CAMPUS NETWORK SECURITY AND MANAGEMENT

1S. Sudharsan, 2M. Naga Srinivas, 3G. Sai Shabareesh, P.Kiran Rao

1 Department of Computer science
2Department of Computer science
3Department of Computer science

ABSTRACT
This project is totally dedicated to the Network Engineer for new and smart learning of the Network Structure. In this concept it is possible for the networker to check the Network Structure of a company spread in the big campus area. The incoming & the outgoing traffic can be maintained along with some security concepts as well. In this logic we use the multiple Routing Protocols in different areas of the company. The practical shows us the proper movement of the packet from one part of the company to the other part of the company. The project comprises of the different Departments of a Campus spread in different buildings. Multiple Routing protocols have been used in different branches of and all the departments can communicate with other different departments through the redistribution among different Routing Protocols. It has a DHCP server for assigning the IP Addresses to the Hosts in the building as well as a DHCP server has been used in the other Buildings as well. The Internet Service Provider has been used for Communication of the Buildings of Campus with the Data Centre & Internet through ISP, using the Frame Relay Switching Technology available for Wide Area Network. Routing Protocols EIGRP along with the Synchronous Number, Static Routing & its concepts including the Default Routing as well has been applied. The different Routing Protocols are running and which has been synchronized to work with Frame Relay Switching Technology.

1.INTRODUCTION
A network is defined as devices connected together to share information and services. The types of data/services that can be shared on a network is endless - documents, music, email, websites, databases, printers, faxes, telephony, videoconferencing, etc.

Networks are generally broken down into two types:
LANs (Local Area Networks):- a high-speed network that covers a relatively small geographic area, usually contained within a single building or campus. A LAN is usually under the administrative control of a single entity/organization.

WANs (Wide Area Networks):-The book definition of a WAN is a network that spans large geographical locations, usually to interconnect multiple LANs. A more practical definition describes a WAN as a network that traverses a public network or commercial carrier, using one of several WAN technologies. Thus, a WAN can be under the administrative control of several entities or organizations, and does not need to “span large geographical distances.”

MAN (Metropolitan Area Network):- A MAN is defined as a network that spans several LAN’s across a city-wide geographic area. The term “MAN” is less prevalent than either LAN or WAN. Generally a network is purely based on what TOPOLOGY it is using, generally a computer network topology is the way various components of a network (like nodes, links, peripherals, etc) are arranged. Network topologies define the layout, virtual shape or structure of network, not only physically but also logically. The way in which different systems and nodes are connected and communicate with each other is determined by topology of the network. Topology can be physical or logical. Physical Topology is the physical layout of nodes, workstations and cables in the network; while logical topology is the way information flows between different components. In general, physical topology relates to a core network whereas logical topology relates to basic network.

Types of Physical Network Topologies
• Bus Topology
• Star Topology
• Ring Topology
• Mesh Topology
• Tree Topology
• Hybrid Topology

Factors to be taken into consideration while choosing a Network topology
• Scale of your project (in terms of number of components to be connected).
• Amount of traffic expected on the network.
• Budget allotted for the network i.e. amount of money you are willing to invest.
• Required response time

What is Campus Network Security and Management?
In this concept for the networker has to check the Network Structure of a company spread in the campus area. The outgoing & the incoming traffic can be maintained along with the some security concepts. Here we use the Routing Protocols in different areas of the campus. The proper movement of the packet from one part of the company to the other part of the company is the main criteria. This project comprises of the various departments of a Campus spread in different buildings. Multiple
Routing protocols are being used in different branches of and all of them can communicate with other different buildings through the redistribution between different Routing Protocols. It comprises a DHCP server to assign the IP Addresses among the Hosts in the building as well as between the DHCP server that has been used in the other buildings. The Internet Service Provider [ISP] has been used to Communicate between the Buildings of Campus with the Data Centre & Internet through ISP, using the Frame Relay Switching Technology available to Wide Area Network. Routing Protocols EIGRP, Synchronous Number, Static Routing & its various concepts which include the Default Routing have been applied. This comprises the entire view of the Campus Network Management and Security.

Existing Campus Network Security and Management

Present Campus Network Security and Management is entirely based on Bus topology. Generally a bus network is an arrangement with a local area network (LAN) in which each node (workstation or other device) is connected to a main cable or link called the bus. The illustration shows a bus network with five nodes. Each node is shown as a sphere, the bus appears as a heavy horizontal line, and connections to the bus appear as vertical lines. A bus network is simple and reliable. If one node fails to operate, all the rest can still communicate with each other. For a major disruption to take place, the bus itself must be broken somewhere. Bus networks are easy to expand. Additional nodes can be added anywhere along the bus. There are several limitations to the bus network topology. The length of the bus is limited by cable loss. A bus network may not work well if the nodes are located at scattered points that do not lie near a common line. Though it is easy to set-up and extend bus network, cable length required for this topology is the least compared to other networks, costs very less and good for LAN. It has some drawbacks like:

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.
- There is a limit on central cable length and number of nodes that can be connected.
- Dependency on central cable in this topology has its disadvantages. If the main cable (i.e. bus) encounters some problem, whole network breaks down.
- Proper termination is required to dump signals. Use of terminators is must.
- It is difficult to detect and troubleshoot fault at individual station.
- Maintenance costs can get higher with time.
- Efficiency of Bus network reduces, as the number of devices connected to it increases.
- It is not suitable for networks with heavy traffic.

Security is very low because all the computers receive the sent signal from the source. These drawbacks do not help to maintain effective Campus Network Security and Management.

Proposed Campus Network Security and Management

The proposed Campus Network Security and Management is based on STAR topology. Generally a STAR network is a local area network (LAN) in which all nodes (workstations or other devices) are directly connected to a common central computer. Every workstation is indirectly connected to every other through the central computer. In some star networks, the central computer can also operate as a workstation. The illustration shows a star network with five workstations (or six, if the central computer acts as a workstation). Each workstation is shown as a sphere, the central computer is shown as a larger sphere, and connections are shown as straight lines. The connections can be wired or wireless links. The star network topology works well when workstations are at scattered points. It is easy to add or remove workstations. In a star network, a cable failure will isolate the workstation that it links to the central computer, but only that workstation will be isolated. All the other workstations will continue to function normally, except that they will not be able to communicate with the isolated workstation. If any workstation goes down, none of the other workstations will be affected.

It has many advantages like:

- As compared to Bus topology it gives far much better performance, signals don’t necessarily get transmitted to all the workstations. A sent signal reaches the intended destination after passing through no more than 3-4 devices and 2-3 links. Performance of the network is dependent on the capacity of central hub.
- Easy to connect new nodes or devices. In star topology new nodes can be added easily without affecting rest of the network. Similarly components can also be removed easily.
- Centralized management. It helps in monitoring the network.
- Failure of one node or link doesn’t affect the rest of network. At the same time it is easy to detect the failure and troubleshoot it.

This helps to maintain effective Campus Network Security and Management.

The goal of any networking project is to enable you to do the following:

- Build implementations of the Internet protocols
- Generalize this knowledge to other networking protocols.
- Be a competent network and systems programmer.
- Think like a networking practitioner
- Read and judge articles on networking in trade magazines
- Begin to read and judge research and technical articles on networking
- Create simplicity and reliability out of complexity and unreliability
Project Description
It consists of a First Building (FB), an Second Building (SB), and a Data Center (DC), all connected through a frame relay switch. The Data Center is connected to the ISP to get to the simulated Internet (it's just a 4.2.2.0/24 network). All the IP subnets are indicated in a little legend key. Of course, you may wish to use whatever IP scheme you want.

The Steps:
First Building
1 Switches: IP addresses
Configure IP addresses for the switches which will be in VLAN 1, subnet 172.16.1.0/24). Their default gateway will be 172.16.1.254.

2 Switches: VTP and VLANs
Configure the ports connected between the switches to trunk ports. Create VLANs 30 and 40 on one switch, name them DATA1 and DATA2 respectively. Configure the VTP domain "WB" on the switch (and optionally VTP password "1234"; you'll have to configure the password on the other switches). Assign the ports that will have PCs attached to the VLANs (check topology image).

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, 30 and 40). Optional: Configure ports that are/will be connected to PCs/routers to port fast.

4 Routers: Router-on-a-stick
Configure the (CME labeled) router's Fast-Ethernet port on VLAN 1, and two sub interfaces for each of VLANs 30 (subnet 172.16.30.0/24) and 40 (subnet 172.16.40.0/24);

5 Routers: Gateway Router/DHCP
Configure it's Fast-Ethernet port on the VLAN 40 subnet; don't forget to configure the port on the switch on VLAN 40. Configure DHCP pools for VLANs 30 and 40 (I'm not sure if this was in the CCNA syllabus, but it's pretty cool and easy. Otherwise, forget about this and just statically assign IPs to the PCs in their respective VLAN subnets. If you do however go with the DHCP, you'll have to configure one extra command on the router-on-a-stick router for the VLAN 30 PCs to obtain IPs.

6 Routers: Routing protocol
I used EIGRP. You may use anything else. After configuring routing protocols on both routers, verify by show ip route on the Gateway router. You can verify by ping (for example, ping from Gateway router [VLAN 40] to one of the switches [VLAN 1]) to verify inter VLAN routing. Also, ping from a PC on one VLAN to another PC on the other VLAN.

Second Building
Same thing as First Building. I chose the VTP domain "EB", VLANs 35 and 45 instead, different IP subnets; refer to the topology image. Use the same routing protocol.

Data Center
This is pretty straight forward. There is no VTP here, no STP, and you don't even have to have DHCP (I did). Configure static IPs. Refer to the image. Use the same routing protocol. Configure the serial interface that will connect to the ISP with the IP address.

ISP
Configure both serial ports with IPs. Do NOT configure a routing protocol. Instead, configure a static route to network 4.2.2.0/24 pointing to the next router (which will be our network on the Internet). This is because we don't want this ISP router to know of ANY of the IPs in the buildings/data center. This will simulate the "internet" experience; so that if it receives a ping from any device, it will not be able to reply back because it doesn't have a route path to the device's IP...this is where NAT will come into play later. At this point, go back to the Data Center router and configure a default static route to point to the ISP router. Then redistribute that route to the other routers.

Internet
Also, straight forward; configure static IPs to the servers and all that. But again, do NOT configure a routing protocol on the router. Instead, just configure a static route to the 68.110.171.132/30 network going through the ISP router.

Frame Relay
Use point-to-point; I had difficulties with the routing protocol when I used multipoint. 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.

NAT and ACLs
Verify that any device will NOT be able to reach the internet (4.2.2.0/24), because we don't have NAT configured. Now, configure NAT on the Data Center router. My ACL was configured as follows: deny VLAN 40 subnet in WB (except routers/admin laptop), deny VLAN 35 subnet in SB (except routers/admin laptop), and permit all the other subnets.

Project scenario

Defining Network Security
People perceive and define network security in a number of different ways. For the purposes of this book, network security includes the detection and prevention of unauthorized access to both the network elements and those devices attached to the network. This includes everything from preventing unauthorized switch port access to detecting and preventing unauthorized network traffic from both inside and outside the corporate network. Confidentiality: only sender, intended receiver should “understand” message contents • sender encrypts message • receiver decrypts message Authentication: sender, receiver wants to confirm identity of each other

Message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection Access and availability: services must be accessible and available to users

Improving the Security:

Security in 802.1x:

Basic description
The architecture compliant to norm 802.1x is using 3 different entities: • The supplicant • The authenticator • The authentication server

The supplicant is the client which wants to use the resources of the network. To be more precise, the client contains a supplicant, which is responsible for responding to Authenticator data that will establish its credentials. The authenticator is the system which controls the access gate. It may be a switch, in the case of a wired network, or an access point, in the case of Wi-Fi. The same remark applies to the authenticator: in fact, the access point contains an authenticator, but is not an authenticator.

Client’s data flows can be separated in two classes:
• Authentication frames, using Extensible authentication Protocol (EAP1– RFC 2284)
• Other frames are blocked, before authentication. Then, the port on the gate is opened, and frames can move freely.

The authentication server is generally a RADIUS server (see RFC 2865). During the authentication, the access point behaves like a simple passive relay, and do not interpret dialog between the supplicant and the RADIUS server. Layer 3 security is not « yet another wireless security protocol ». It’s a set of tools which were developed, or taken from wired world, to satisfy the needs of the security before 802.1x and 802.11i were released. Most of these features work on the IP packets, and that’s why we are talking of Layer 3. However, we won't only focus on Network Layer. Some mechanisms are derived from previously existing in Layer 3, but actually work on Layer 2 (data link) or on Layers 4 / 5 (Transport, application). Two main points will be discussed: PKI (Public Key Infrastructure), VPN (Virtual Private Networks) and encrypted tunnelling via IPSec or SSL.

Public Key Infrastructures a PKI (public key infrastructure) enables users of a basically unsecured public network such as a Wi-Fi network to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

Network security applications
• Authentication Applications
• Web Security Standards
• Authentication application (Kerberos)
• Kerberos is a trusted third-party

Authentication protocol designed for TCP/IP networks (developed at MIT).
• A Kerberos service on the network acts as a trusted arbitrator.
• Kerberos allows clients to access different entities (clients/servers) on the networks.
• Services requiring authentication, as well as their clients, register their secret keys with Kerberos.

Web Security Standard

Web security threads:
• Location
• Server or client (System Security)
• Network traffic (Web Security)
• Type
• Passive attacks.
• Active attacks.
• Campus Network Security and Management Applications

Campus Network Security and Management is applicable in many ways:
• It is applicable to corporate offices to establish a effective network between the different departments of the company.
• It is used in establishing a network between the different blocks of a college so that communication between the different labs of the college may be done.
• It is used in Government sectors to establish a effective network between the different departments in the different parts of a office.

7. CONCLUSION
All the branches are communicating with each other and security is provided to all the departments of the campus to prevent the unauthorized access of the data of other departments and the internet via ISP using internet and network protocols.

8. FUTURE SCOPE
Perhaps the greatest concern companies have in doing business over the Internet is the security risk. Hackers, denial-of-service (DoS) attacks, identity theft, and even cyber-terrorism are very real dangers. In addition, you may wonder how to guarantee the performance and reliability of your Internet-based services. Or, you may not be certain that you have the resources and support needed to deploy and manage e-commerce services and processes. The good news is that a sound network infrastructure can address all these issues. At the foundation of a robust e-commerce infrastructure are the routers and switches. An
integrated approach to routing and switching lets all workers even those at different sites have the same access to business applications, unified communications, and videoconferencing as their colleagues at headquarters. We grow our network over time, adding features and functionality as you need them while ensuring complete investment protection. An added benefit of this integrated approach is that your IT personnel can centrally manage the network from headquarters, which keeps staffing counts low.

REFERENCES