**15CSE312-Computer Networks**

**Secured Enterprise Network for**

**Faculty of University**

|  |  |  |  |
| --- | --- | --- | --- |
| **Registration No.** | **Name** | **Email-ID** | **Contribution** |
| CB.EN.U4CSE17017 | Pretham D | prethamdantuluri416@gmail.com | Architecture Diagram , Qos Parameters |
| CB.EN.U4CSE17031 | Vijay Mani Dev K | vijayjonathan143@gmail.com | Cisco Packet Tracer, Analytical Questions |
| CB.EN.U4CSE17036 | Harsha Saketh K | konjetisaketh24@gmail.com | Cisco Packet Tracer,Design |
| CB.EN.U4CSE17050 | Sai Akhil Y | saiakhil.yerramsetty@gmail.com | Cisco Packet Tracer,Ip Addressing Tables |

**Title:** Secured Enterprise Network for Faculty of a University

**Abstract:**

Our proposed system is about designing a secured enterprise network for faculty of university. The aim of this study is to develop a scalable, available, and manageable enterprise network for the faculty of a university.

**Problem Statement:**

To compete globally, the faculty needs to build and setup a secured enterprise network solution to show the technological advancement of the university

### 

### **Software :**

* Cisco Packet Tracer to simulate network topologies and imitate the functioning of a network.
* Cloud Services like Amazon web services

### **Analytical questions:**

1. What is the average time to send data from department to department in the same subnet?
2. What is the average time to send data from department to department across different subnets?
3. How does one prevent bottlenecks in the network, i.e., manage flow control?

* Here are four modern ways that engineers ease congestion throughout various parts of an enterprise network.
* ****Load balancing****

The Border Gateway Protocol (BGP) is often implemented in large enterprise networks  to take advantage of **[internet load sharing](http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13762-40.html" \t "https://www.networkcomputing.com/data-centers/_blank)**.

* ****WAN optimization and SD-WAN****

The first method, WAN optimization, is deployed via  appliances installed at either end of the WAN connection. The appliances use a series of software-based optimization tools to squeeze out as much efficiency on a link as possible. Techniques include compression, caching, data deduplication, and traffic shaping.The next evolution of WAN optimization is **[SD-WAN](http://www.networkcomputing.com/networking/top-4-sd-wan-myths/1072744350)**, which adds another layer of software-based optimization intelligence into the mix. An SD-WAN architecture creates a virtual overlay where multiple WAN connectivity options are aggregated together.

* ****Virtual Port Channel (vPC)****

Port channeling – a **[link aggregation](http://www.networkcomputing.com/networking/link-aggregation-terminology-explained/721978943)** technique -- is the process of logically combining multiple physical links together to increase bandwidth between two network devices.

* ****Leaf-spine architectures****

The bandwidth between compute, storage and the network is a major concern. One way to address this bottleneck is to move from a traditional three-tier network design to a leaf-spine architecture in the data center. This technique creates a full mesh of network connectivity between the data center access layer (leaf nodes) and the aggregation layer (spine nodes). Since all nodes are connected, every resource within the data center is the same number of hops away. Additionally, each uplink between the leaf and spine nodes can be utilized to its fullest extent.

1. How to quantify the scalability of the network?

To answer this, we need some scalability metrics, such as the following:

* *Throughput*—the rate at which transactions are processed by the system
* *Resource usage*—the usage levels for the various resources involved (CPU, memory, disk, bandwidth)
* *Cost*—the price per transaction

1. **How DHCP server assigns IP address to a host?**

* **DHCPDISCOVER:** When a new node is connected to the network, it broadcasts the DHCPDISCOVER message which contains the source address as 0.0.0.0 to every node on the network including server. DHCP server on receiving the message, returns the DHCPOFFER message to the requested host which contains the server address and new IP address to the node.
* **DHCPOFFER:** If there are multiple servers on the network, host receives multiple DHCPOFFER messages. It is up to the host to select a particular message.
* **DHCPREQUEST:**  The requested host on receiving the offer message, it again broadcasts the DHCPREQUEST message on the network with the address of the server whose offer message is accepted by the host. The server which pertains to that server address sent by the host checks whether the address to be assigned to the node is available in the data storage.
* **DHCPACK :** If the address is assigned , it marks the IP address in the storage as unavailable to ensure consistency. Now, the server sends DHCPACK packet to the requested host which contains network information(IP address, subnet mask, gateway address). In case, if the address is assigned to other machine meanwhile, then the server sends the packet DHCPNAK to the requested host indicating that the IP address is assigned to some other machine.
* **DHCPRELEASE :** And finally, If the host wants to move to other network or if it has finished  its work, it sends the DHCPRELEASE packet to the server indicating that it wants to disconnect. Then the server marks the IP address as available in the storage so that it can be assigned to other machine.

1. What is the network topology and why is it important?

A network topology is a substantial arrangement of a network in which all the nodes are connected with each other using network links or connecting lines. Apart from just describing how the nodes are interconnected, network topology also explains how the data is transferred in a network.

## **Importance of network topology**

* Plays a significant role in the functioning of networks.
* Plays a crucial role in performance.
* Helps reduce the operational and maintenance costs such as cabling costs.
* A network topology is a factor in determining the media type to be used to cable a network.
* Error or fault detection is made easy using network topologies.

### **Data Tables :**

|  |  |
| --- | --- |
| **Parameter** | **Specifications** |
| Number of nodes | N number of nodes |
| Type of addressing | Classless addressing |
| Network devices | Switches, routers and server |
| Routing protocols | RIP |
| IP address range | 172.16.0.0/16 |
| Communication media | Ethernet Cable(copper) |
| Type of network | VLAN, client-server, VPN |

**Hardware:**

1. Switch:

* Model: Cisco 2960 .
* Bandwidth Limit: 10Mbps
* RAM: 64 MB
* Cabling Type: Ethernet 100Base-TX, Ethernet 10Base-T
* Ports Quantity: 24 ports
* Communication Mode: Half-duplex, Full-duplex
* Switching Protocols: Ethernet

1. Router 1941

* 2 integrated 10/100/1000 Ethernet ports
* 2 enhanced High-Speed WAN Interface Card slots that can host 2 single wide or 1 double wide and 1 single wide (e)HWIC
* 1 Internal Services1 Internal Services Module slot
* Fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE) and Cisco Enhanced PoE
* Security Embedded hardware-accelerated VPN encryption
* Secure collaborative communications with Group Encrypted Transport VPN, Dynamic Multipoint VPN, or Enhanced Easy VPN
* Integrated threat control using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, and Cisco IOS Content Filtering

1. Cisco Adaptive security appliance(ASA) 5505

* SSL and IPsec VPN Services
* 8 port 10/100 switch with 2 Power over Ethernet (PoE) ports
* Memory: 512 MB; Maximum Firewall throughput (Mbps): 150 Mbps
* Packets Per Second (64 byte): 85,000
* Maximum 3DES/AES VPN Throughput: 100 Mbps
* SSL VPN User Sessions: 2 Bundled/25 Max
* Content Security (Anti-virus, Anti-Spyware, File Blocking): Not available

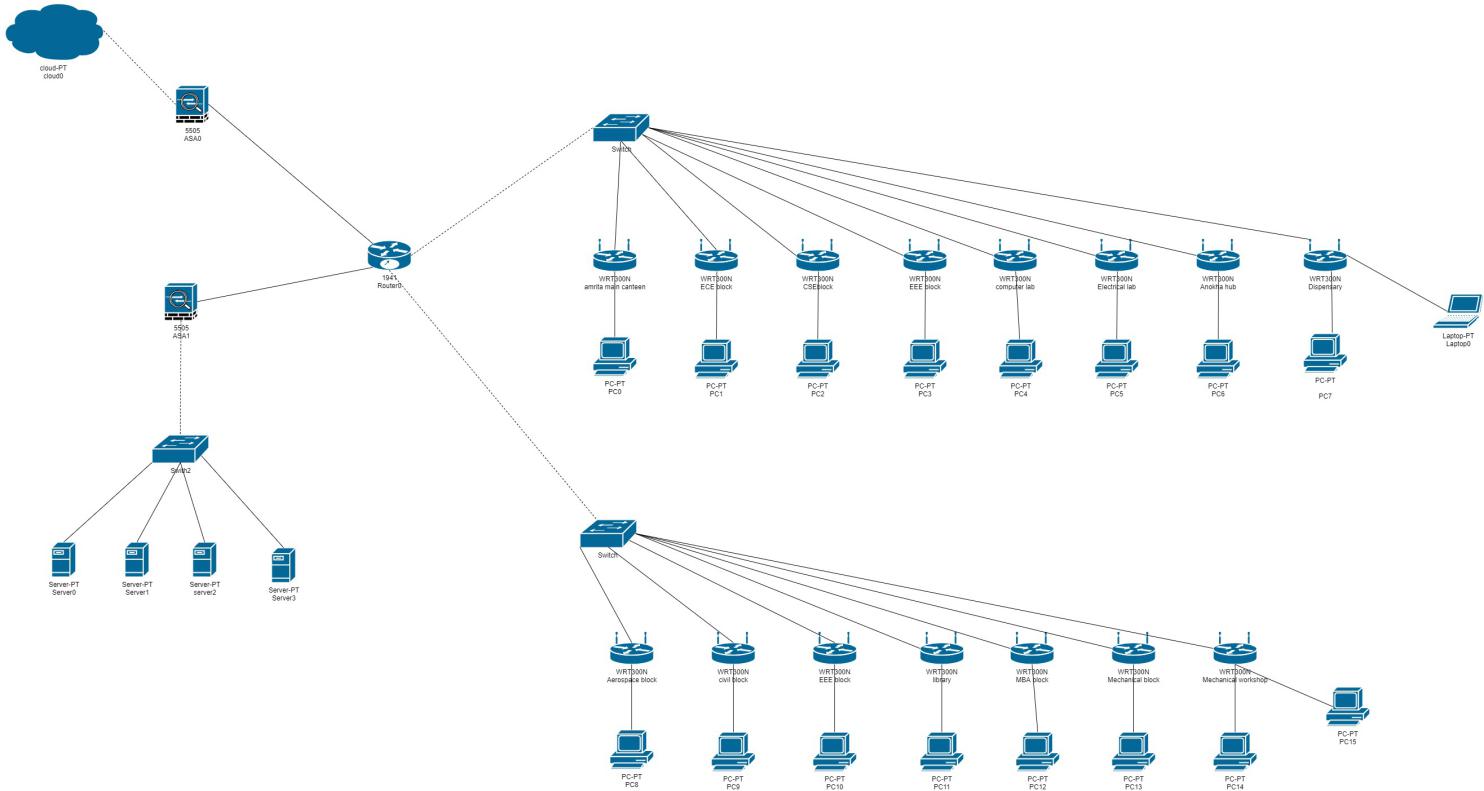
1. PC

* Desktop

Intel i5 7th gen ; 4GB RAM ; 1TB HDD ; Windows ; Integrated Graphics

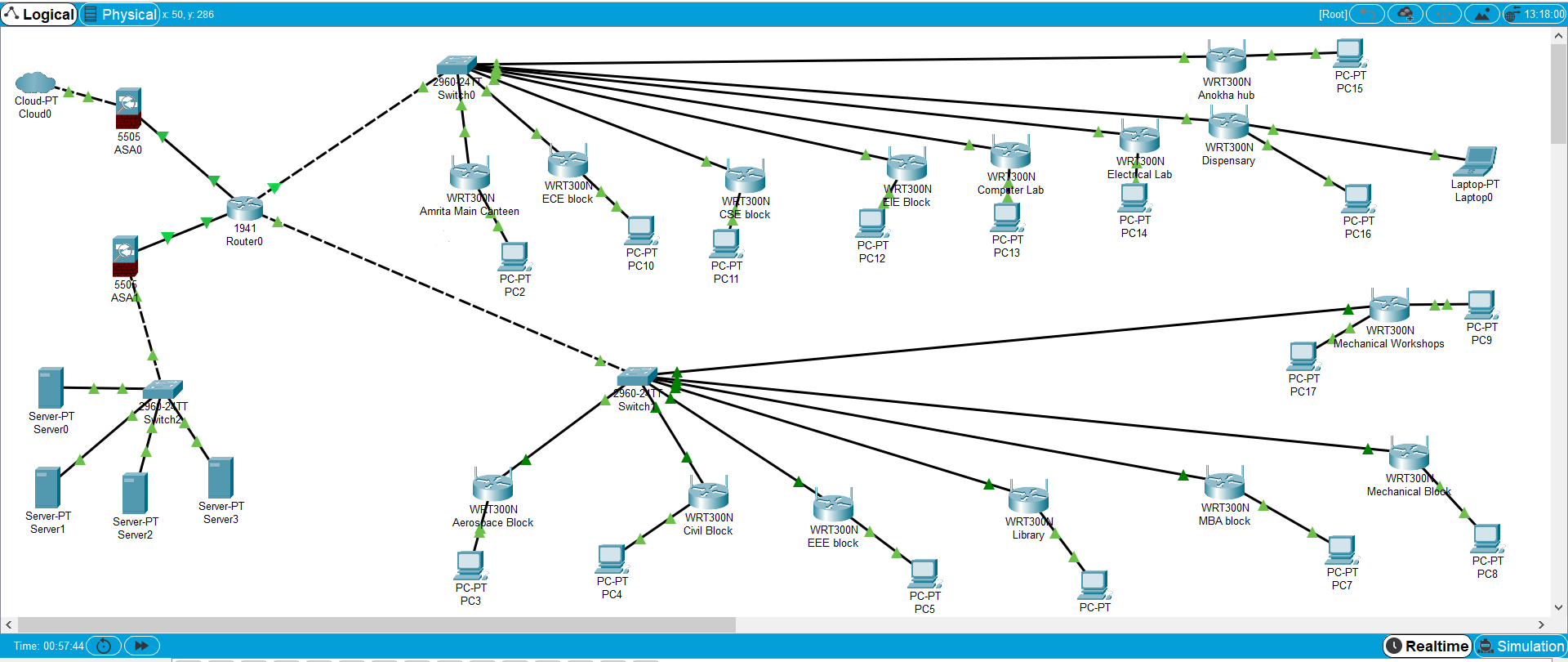
* Any laptop with above specifications

### **Model Diagram of proposed Network design:**



Note: please zoom in to see clearly

### **Network Design in CISCO packet Tracer (screenshot ) :**



**Ip addressing of Network Design :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S No.** | **Network Location** | **Network Address** | **First valid Host** | **Last Valid Host** | **Broadcast Address** |
| 1 | Amrita Main Canteen | 172.16.0.0 | 172.16.0.1 | 172.16.0.254 | 172.16.0.255 |
| 2 | ECE Block | 172.16.8.0 | 172.16.8.1 | 172.16.8.254 | 172.16.8.255 |
| 3 | CSE Block | 172.16.16.0 | 172.16.16.1 | 172.16.16.254 | 172.16.16.255 |
| 4 | EEE Block | 172.16.24.0 | 172.16.24.1 | 172.16.24.254 | 172.16.24.255 |
| 5 | Computer Lab | 172.16.32.0 | 172.16.32.1 | 172.16.32.254 | 172.16.32.255 |
| 6 | Electrical Lab | 172.16.40.0 | 172.16.40.1 | 172.16.40.254 | 172.16.40.255 |
| 7 | Anokha Hub | 172.16.48.0 | 172.16.48.1 | 172.16.48.254 | 172.16.48.255 |
| 8 | Dispensary | 172.16.56.0 | 172.16.56.1 | 172.16.56.254 | 172.16.56.255 |
| 9 | Mechanical Workshop | 172.16.64.0 | 172.16.64.1 | 172.16.64.254 | 172.16.64.255 |
| 10 | Mechanical Block | 172.16.72.0 | 172.16.72.1 | 172.16.72.254 | 172.16.72.255 |
| 11 | MBA Block | 172.16.80.0 | 172.16.80.1 | 172.16.80.254 | 172.16.80.255 |
| 12 | Library | 172.16.88.0 | 172.16.88.1 | 172.16.88.254 | 172.16.88.255 |
| 13 | EEE Block | 172.16.96.0 | 172.16.96.1 | 172.16.96.254 | 172.16.96.255 |
| 14 | Civil Block | 172.16.104.0 | 172.16.104.1 | 172.16.104.254 | 172.16.104.255 |
| 15 | Aerospace Block | 172.16.112.0 | 172.16.112.1 | 172.16.112.254 | 172.16.112.255 |

**How our Network Design is sufficient :**

1. the class B private Internet Protocol (IP) Address was specified for each devices on the IP network. This would enable the transmission of packets to the exact location of a user device on the network.
2. Our design uses star topology because its Less expensive, Each device only need one I/O port and needs to be connected with hub with one link.
3. It is robust, if one link fails, other links will work just fine.
4. The design reduced network device load and the time to identify network issues to resolve them.
5. The configured network security provided availability, integrity, and confidentiality.
6. the inclusion of new devices did not affect the transfer of packets.
7. The ASA in Cisco ASA stands for Adaptive Security Appliance. In brief, Cisco ASA is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. It provides proactive threat defense that stops attacks before they spread through the network.

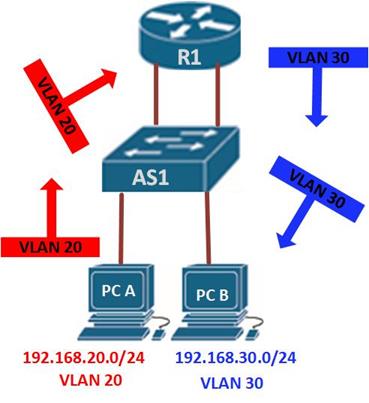
**Implementation:**

<https://github.com/SaiAkhil932/networks>

* The given architecture diagram depicts a pictorial representation of 2 subnets
* Both subnets A and B consists of wireless routers,PCs and Laptops.
* Those 2 subnets are connected to a router
* One link from the router passes through ASA to university servers
* The other link from router passes through another ASA to Cloud

**Inter-VLAN Routing:**

Inter-VLAN routing can be defined as a way to forward traffic between different VLAN by implementing a router in the network. As we learnt previously, VLANs logically segment the switch into different subnets, when a router is connected to the switch, an administrator can configure the router to forward the traffic between the various VLANs configured on the switch. The user nodes in the VLANs forwards traffic to the router which then forwards the traffic to the destination network regardless of the VLAN configured on the switch.The figure below, shows how this process works.



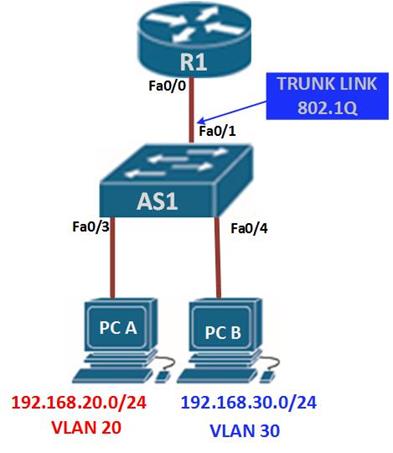
Information destined for PC B, leaves PC A with the VLAN 20 tag, when it gets to R1, the router, changes the format of this message from VLAN 20, to VLAN 30, it then sends it back to the switch and the switch finally sends the message to its intended recipient PC B.

There are two ways in which inter-VLAN routing can be accomplished.

* Traditional inter-VLAN routing
* Router-on-a-stick

One of the 2 ways in which Inter-VLAN routing can be established is traditional inter-VLAN routing.In this type of inter-VLAN routing, a router is usually connected to the switch using multiple interfaces. One for each VLAN. The interfaces on the router are configured as the default gateways for the VLANs configured on the switch.

The other way is Router-on-a-stick. In this type of inter-VLAN routing, the router is connected to the switch using a single interface. The switchport connecting to the router is configured as a trunk link. The single interface on the router is then configured with multiple IP addresses that correspond to the VLANs on the switch. This interface accepts traffic from all the VLANs and determines the destination network based on the source and destination IP in the packets. It then forwards the data to the switch with the correct VLAN information. Our study uses this type.



**QoS parameters :**

|  |  |  |
| --- | --- | --- |
| Parameter | Meaning | Formula |
| Bandwidth | Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time | Expressed in bits per second (bps), modern network links have greater capacity, which is typically measured in millions of bits per second (megabits per second, or Mbps) or billions of bits per second (gigabits per second, or Gbps). |
| Queuing Delay | Time spent by the data packet waiting in the queue before it is taken for execution is called queuing delay. | Queuing Delay is directly proportional to the congestion in the network |

|  |  |  |
| --- | --- | --- |
| Throughput | Throughput measures the percentage of data packets that are successfully being sent; a low throughput means there are a lot of failed or dropped packets that need to be sent again. | Throughput (bits/sec)= sum (number of successful packets)\*(average packet\_size))/Total Time sent in delivering that amount of data. |
| Packet Loss | Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination.Due to network congestion | Efficiency = 100% \* (transferred-retransmitted)/ transferred  Network Loss = 100 - Efficiency |
| Transmission time | The time required for transmission of a message depends on the size of the message and the bandwidth of the channel. | Transmission time =Message size / Bandwidth |
| Propagation Time | Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed. | Propagation time = Distance  /Propagation speed The |
| Processing Delay | Time taken by the processor to process the data packet is called processing delay. | Processing Delay is directly proportional to the processing speed of the processor |