**15CSE312- Computer Networks**

**Case study Document**

Group No:

|  |  |  |  |
| --- | --- | --- | --- |
| **RegNo** | **Name** | **Email ID** | **Contribution** |
| **CB.EN.U4CSE17004** |  |  | Architecture Diagram,  Cisco Packet Tracer,  Prism algorithm with ARP, Python implementation of RIP(Distance Vector) |
| **CB.EN.U4CSE17058** |  |  | Implementation of the network architecture in JavaScript code, Analytical Questions |
|  |  |  | Performance Parameters - Bandwidth, Throughput, Packet Loss, Propagation Delay, |
|  |  |  | Performance Parameters - Transmission Time, Processing Delay, Queueing Delay, Jitter, Applications of the algorithm, |

**Project Title : The need of Wi-Fi 802.11ax over 802.11ac**

**Module Name : (Individual module name of the student)**

**Abstract:**

(a) Problem statement of the work:

  We explore the need of Wi-Fi 802.11ax also known as Wi-Fi 6 over the old Wi-Fi 802.11ac (Wi-Fi 5). The Wi-Fi 6 is an emerging technology with great potential for research.

### (b) Analytical questions: -

* Why Wi-fi 6 is needed?

The need of Wi-Fi 6 is because of the increase in mobile wireless users from day to day. The number of users increased exponentially from the last update of Wi-fi which is in 2013. Since the 802.11ac cannot handle many devices at a time and the network will be slow when the number of devices increases. This created the need for Wi-fi 6. The main reason is the increase in IoT devices.

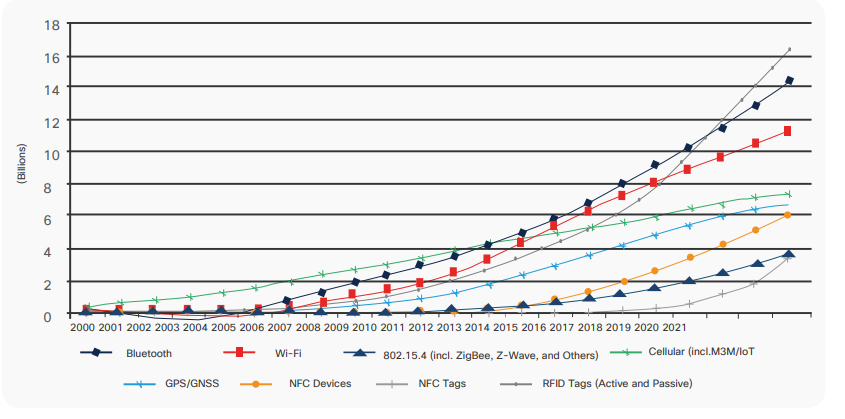


Figure 1: IoT trend Courtesy: Cisco

* Are there any security improvements?

Because of the increase in IoT and wireless devices security becomes a major concern. So, the 802.11.ax adopts WPA3 standard which is the successor to widely used WPA2 standard. The Wi-Fi 6 in WPA3 certified technology.

* How it is greater than Wi-fi 5 (802.11ac)?

Wi-fi 6 gives a more consistent and reliable network compared to Wi-fi 5. The latency time is reduced drastically which is ideal for voice, video and gamming traffic.

It offers a better coverage area which is ideal for IoT devices.

It offers Higher Capacity i.e. it can connect up to 4 times more devices than any other previous standards. This is because of OFDMA and MU-MIMO features.

The Wi-fi 6 communicates in parallel with devices but the existing methods communicate only one at a time.

The power efficiency is increased in the clients. The devices consume by up to two third less power than the existing standards. So , the devices will have a longer battery life because of using Target Wake Time.

In prior generations of 802.11, low-power devices such as mobile phones were accommodated with Unscheduled Automatic Power Save Delivery (U-APSD) or Wi-Fi Multi Media Power-Save (WMM-PS). A client in this mode can have the access point buffer transmissions to it instead of sending it immediately. Instead, the access point signaled availability of data in periodic beacons through a Traffic Indication Message (TIM), which allows the client to keep its radio receiver off (saving power) and waking-up only periodically to receive beacons (generally a multiple of every 102.4 ms). However, this strict adherence to beacons limits the potential energy-saving potential for IoT devices that don’t require regular channel access like a mobile phone yet must always be ready to receive a phone call. With 802.11ax and the new OFDMA scheduling capability of 802.11ax, we can devise a new power-savings mode called Target-Wakeup Time (TWT). With TWT, there is no longer a tight relationship between access-point beacons and the sleep time of the device. Generally, the station can request a schedule to wake up at any time in the future. The result is significant power savings for battery-powered devices, particularly those in the IoT space.

A related but significant benefit of TWT is that it can also be used as an uplink scheduling method akin to UL-OFDMA. That is, because TWT effectively puts clients to sleep with a predetermined wake-up time (based on their request), deterministic transmission times and hence uplink scheduling is possible. The access point can use this ability to both reduce contention (more distributed channel usage) and address delay sensitivity of applications.

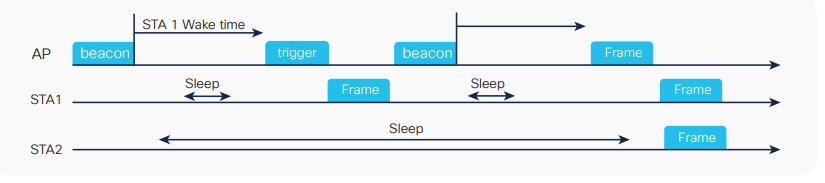


Figure 2: TWT operation Courtesy: Cisco

The speed my increase up to 4 times in average throughput in congested wireless networks than 802.11ac.

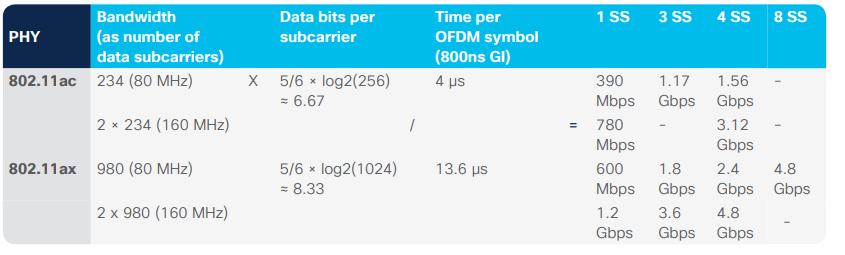


Figure 3: Speed Comparison Courtesy: Cisco

Security is updated with the WPA3 standard.

What OFDMA is?

Orthogonal Frequency-Division Multiple Access is a type of frequency division which uses the subcarriers more efficiently than the existing OFDM. In the OFDM each user got one time slot, or the whole bandwidth channel. So, each user should wait in line for their packet to be delivered. Because of this when the number of clients increase the delay also increases. In easy terms OFDM sends one truck for each user to deliver the packet whereas in OFDMA one truck is sent to deliver all the packet.

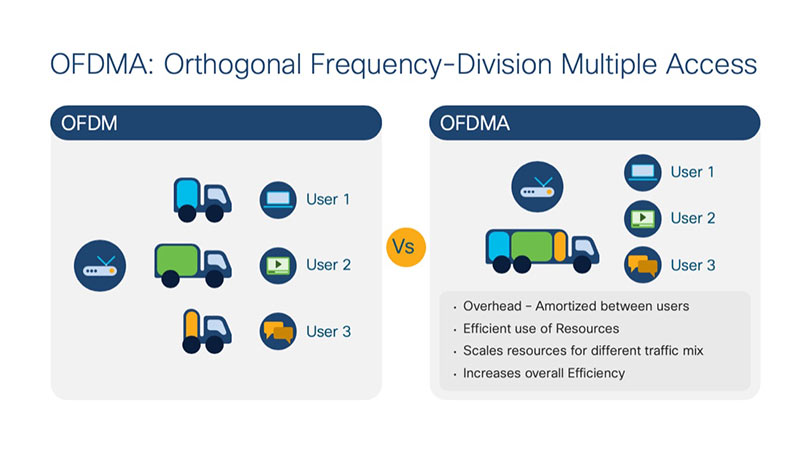


Figure 4: OFDM vs OFDMA Courtesy: Cisco

In 802.11ac, multiple users are separated by space and time. In the time domain, transmission opportunities are allocated to clients and access points alike in a distributed fashion using EDCA. In the spatial domain, downlink\ multiuser Multiple-Input-Multiple-Output (MIMO) techniques are used for isolation and simulcast capabilities limited by the number of transmit antennas (typically up to 4). Both techniques are applied on a per Multiuser Physical layer Protocol Data Unit (MU-PPDU) basis. In 802.11ax, we inherit the same space and time separation as 802.11ac but we add a third multiuser dimension: frequency division. With 802.11ac, the Wi-Fi channel (20, 40, 80, or 160 MHz) was broken down into a collection of smaller OFDM sub-channels to mitigate interference. At any given point in time, a single user is allocated all of those sub-carriers in each PPDU. However, with OFDMA (802.11ax), individual groups of subcarriers are individually allocated to clients as a resource unit on a per-PPDU basis.

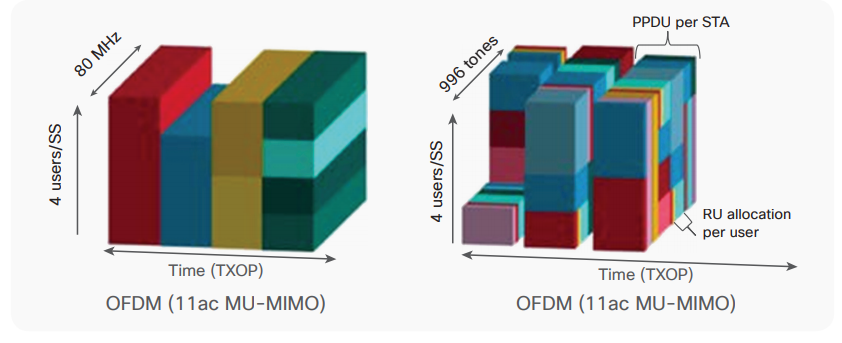


Figure 5 Courtesy: Cisco

This third dimension (OFDMA) has many advantages, such as determinism and increased efficiency through reduction of collisions and contention. But it also revolutionizes the way in which you can deliver Quality of Service (QoS). Previously, with 802.11ac, if an access point wished to deliver a certain throughput to one client but more throughput to another, the best it could do was schedule the correct number of downlink PPDUs in the time domain (for example, with queuing and shaping techniques) and “hope” the client would be able to allocate a sufficient number of TXOPs for UL-PPDUs. This inefficiency and unpredictability makes it difficult to provide any assurance around throughput and other KPIs such as delay and jitter. With OFDMA we now have both a more granular downlink resource unit of time + frequency and also for the first time a way of explicitly allocating resource units in the uplink. This bidirectional resource-unit allocation ability is akin to the LTE Resource Block (RB) and allows the formation of a virtual resource or “slice” in 5G terminology. As can be imagined, this 802.11ax slice could have various attributes such as bandwidth, delay, and jitter, allowing finer-grained QoS than previously available with 802.11ac.

* What is needed for the implementation of Wi-Fi 6?

Wi-fi 6 enabled access points (AP) and Wi-fi 6 capable clients.

* Where this technology is useful?

This technology increases the normal day to day network experience but will serve well in mission critical operations. And makes a turning point in Augmented Reality, Virtual Reality.

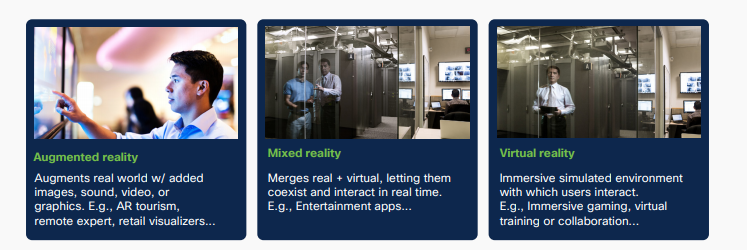
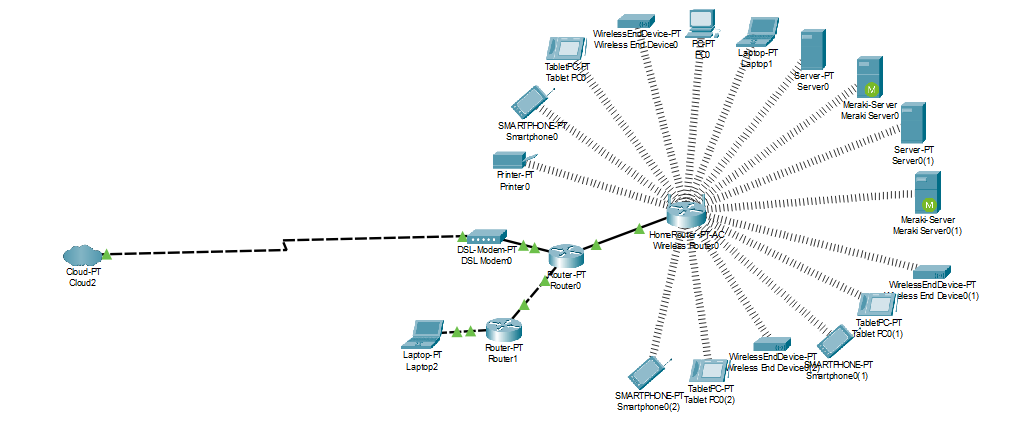


Figure 6: AR, VR Courtesy: Cisco

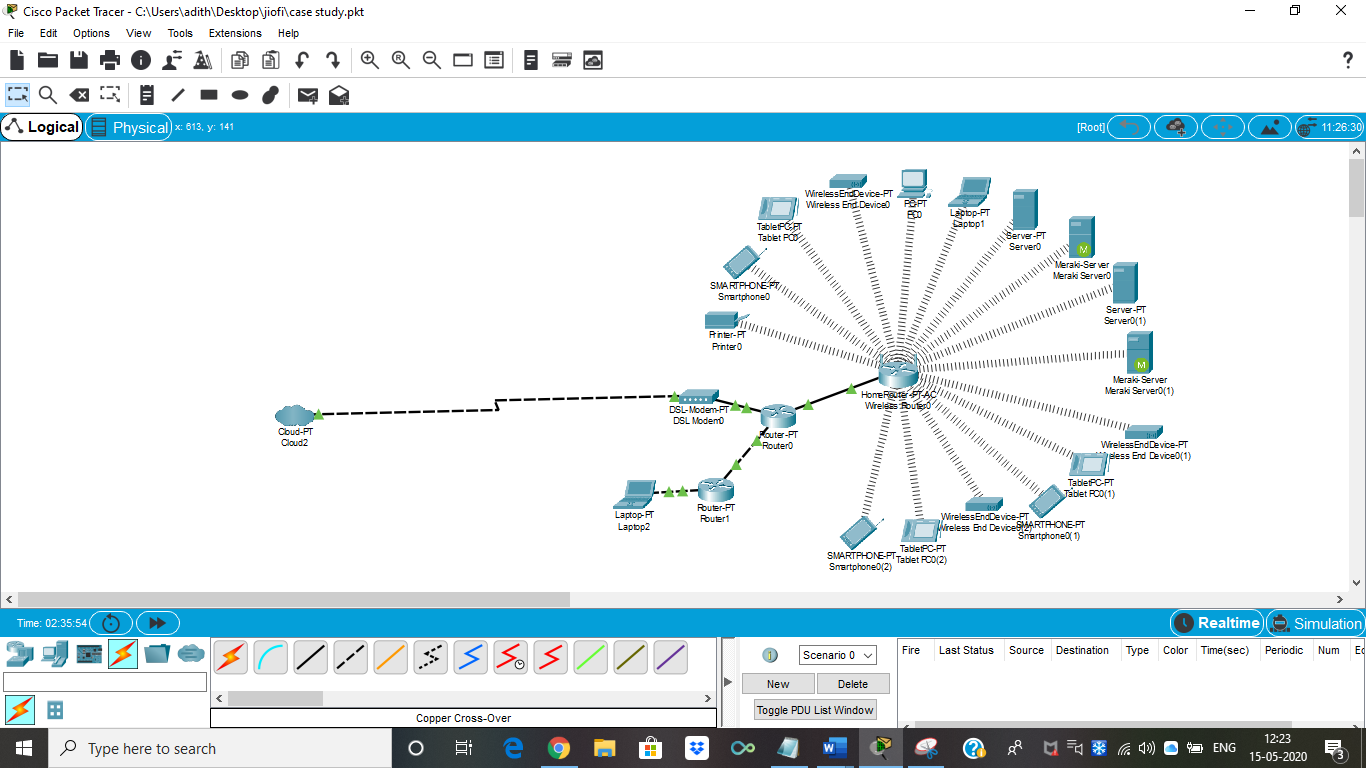
**Model Diagram of the 802.11ac Network design**:



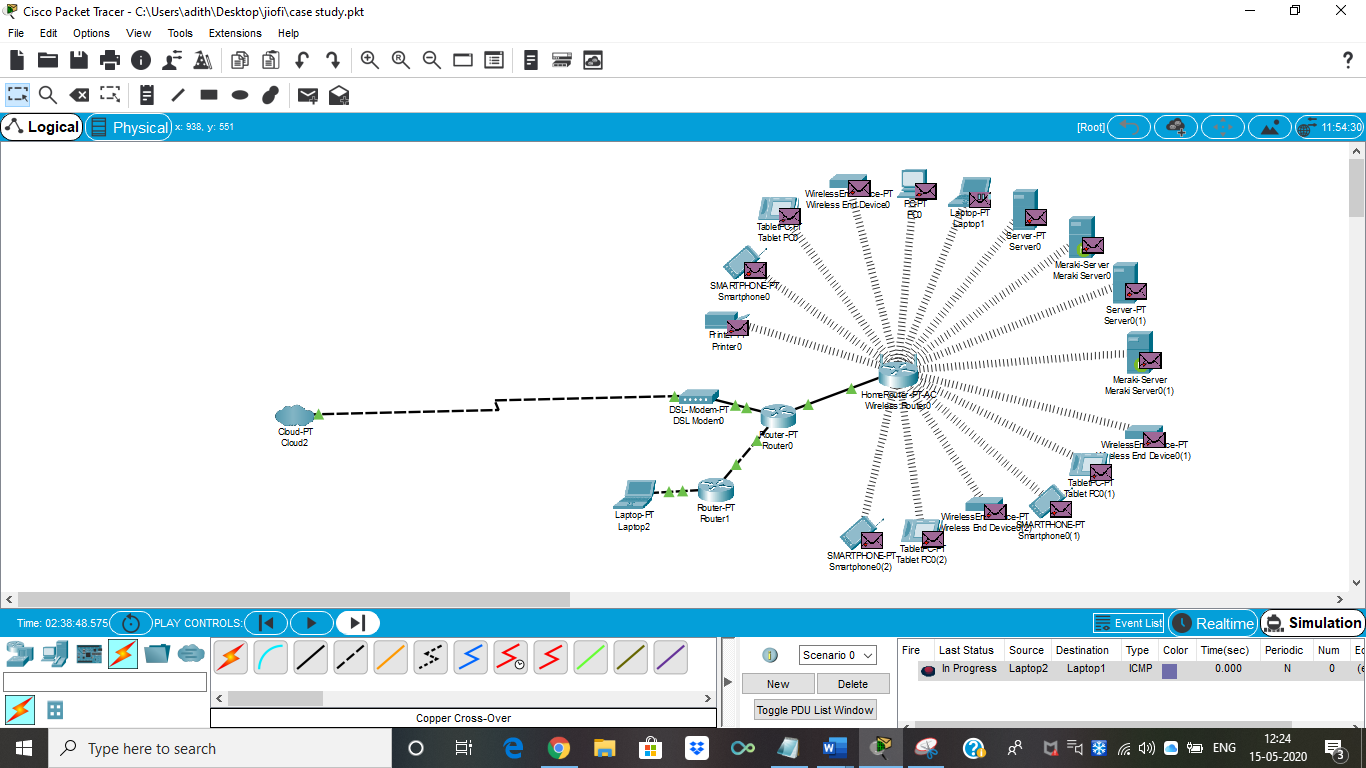
### 

### 

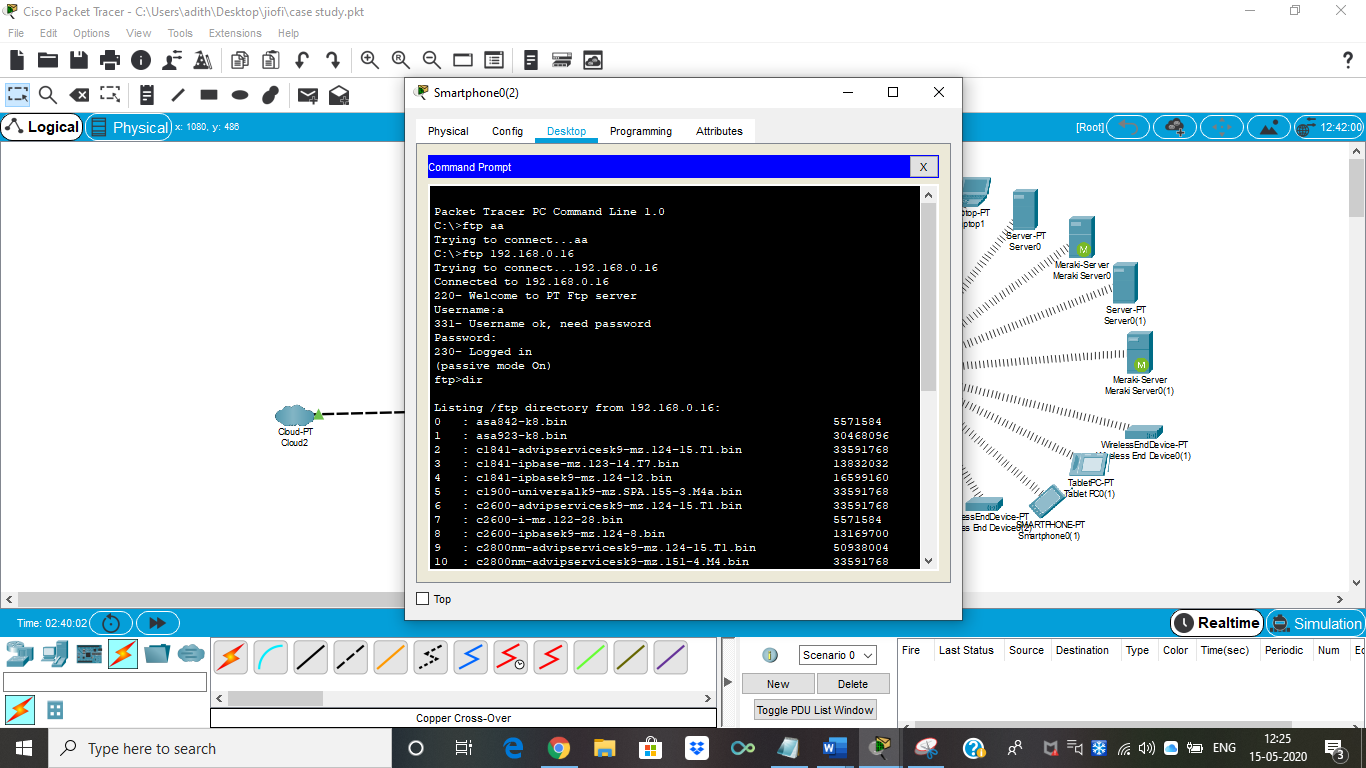
### (a) Network Design in CISCO packet Tracer (screenshot )



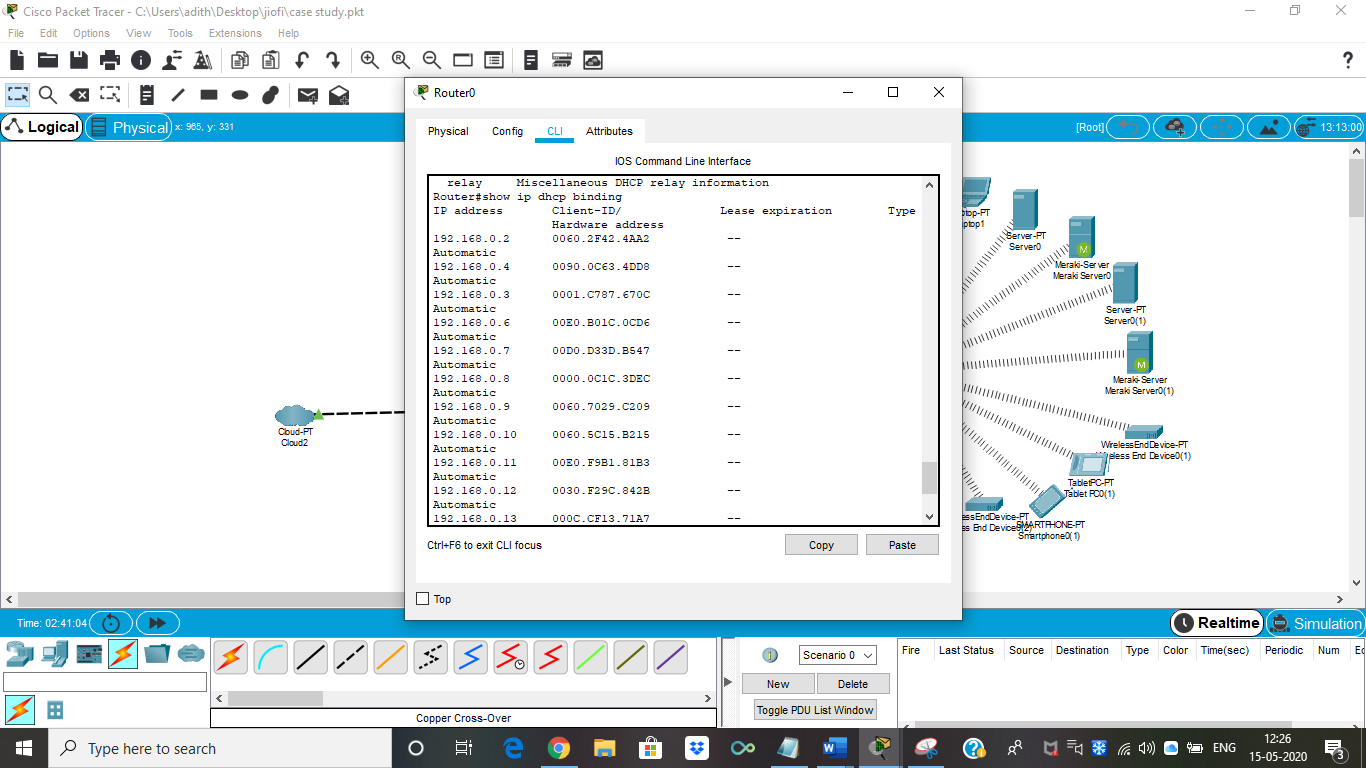
Main Network Simulation



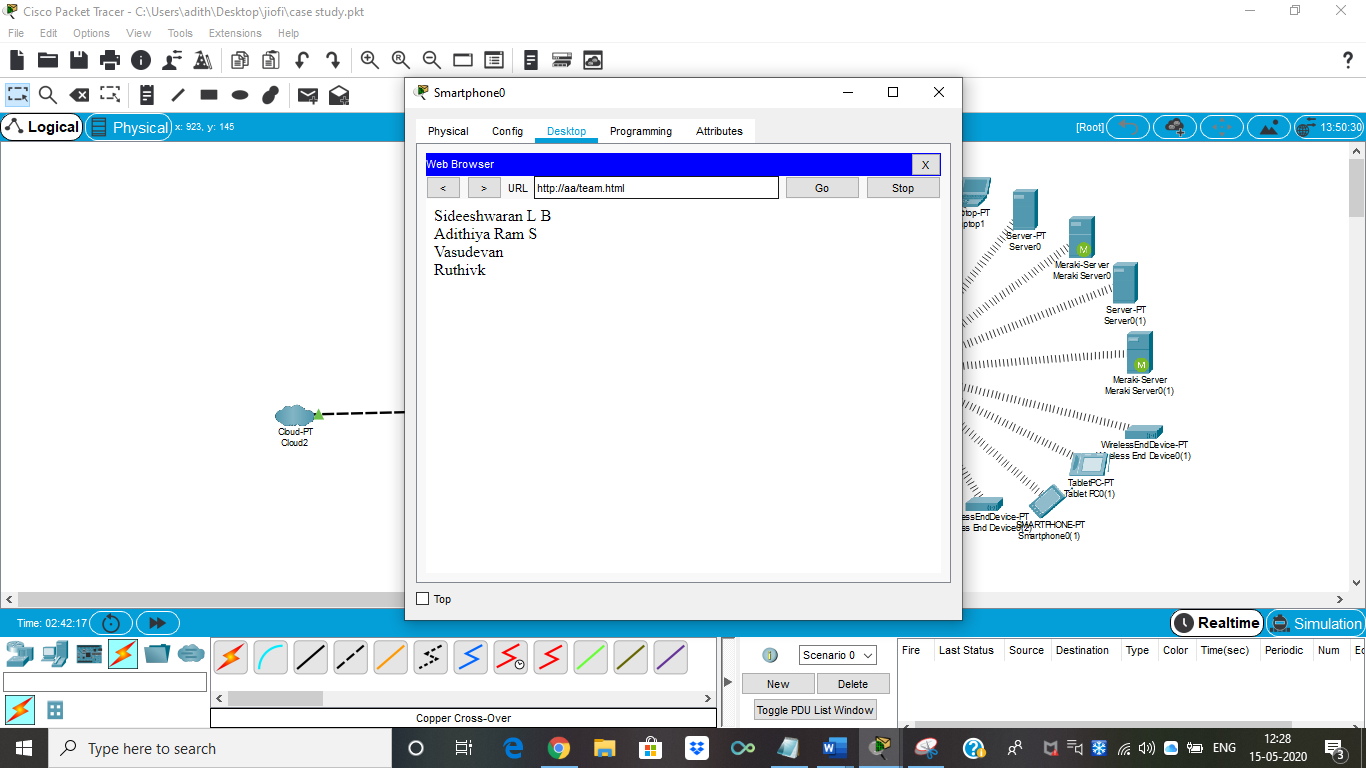
FTP Connection Established



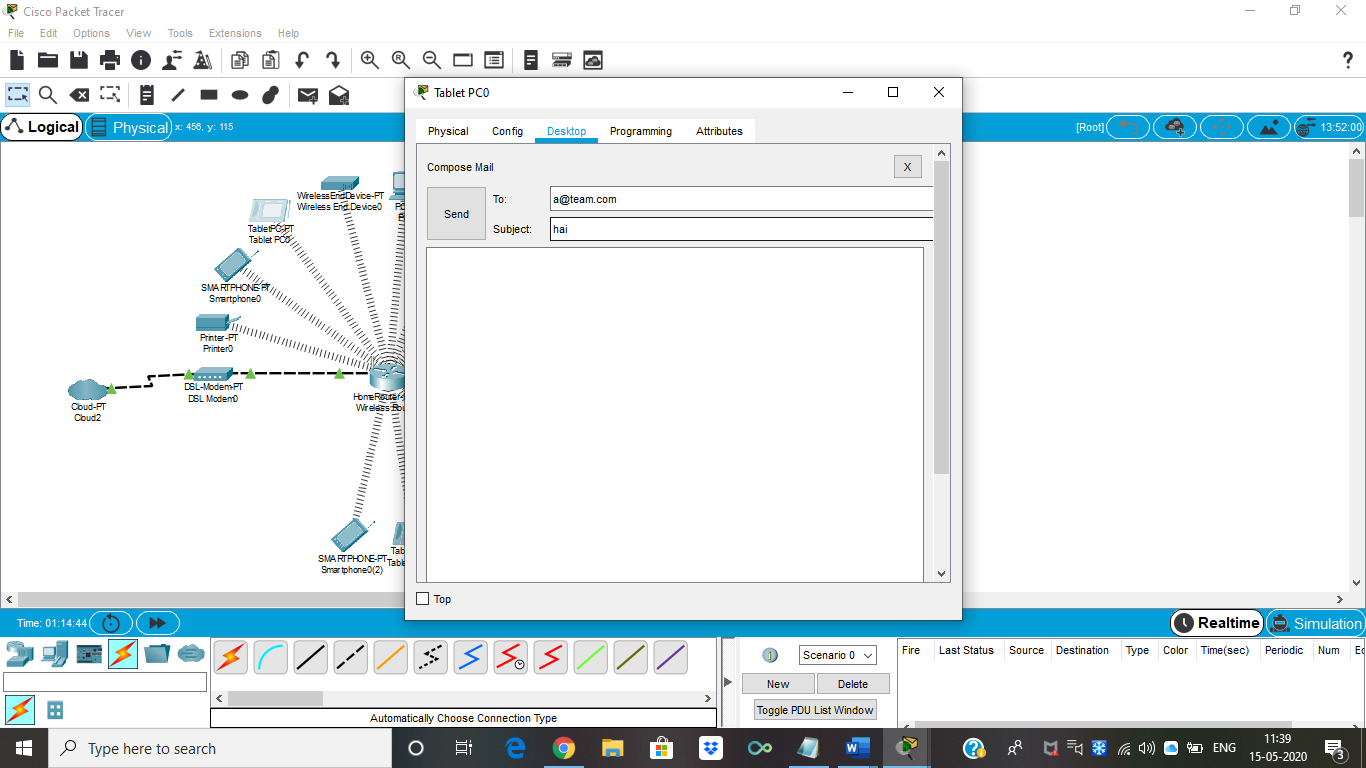
DHCP Server Established

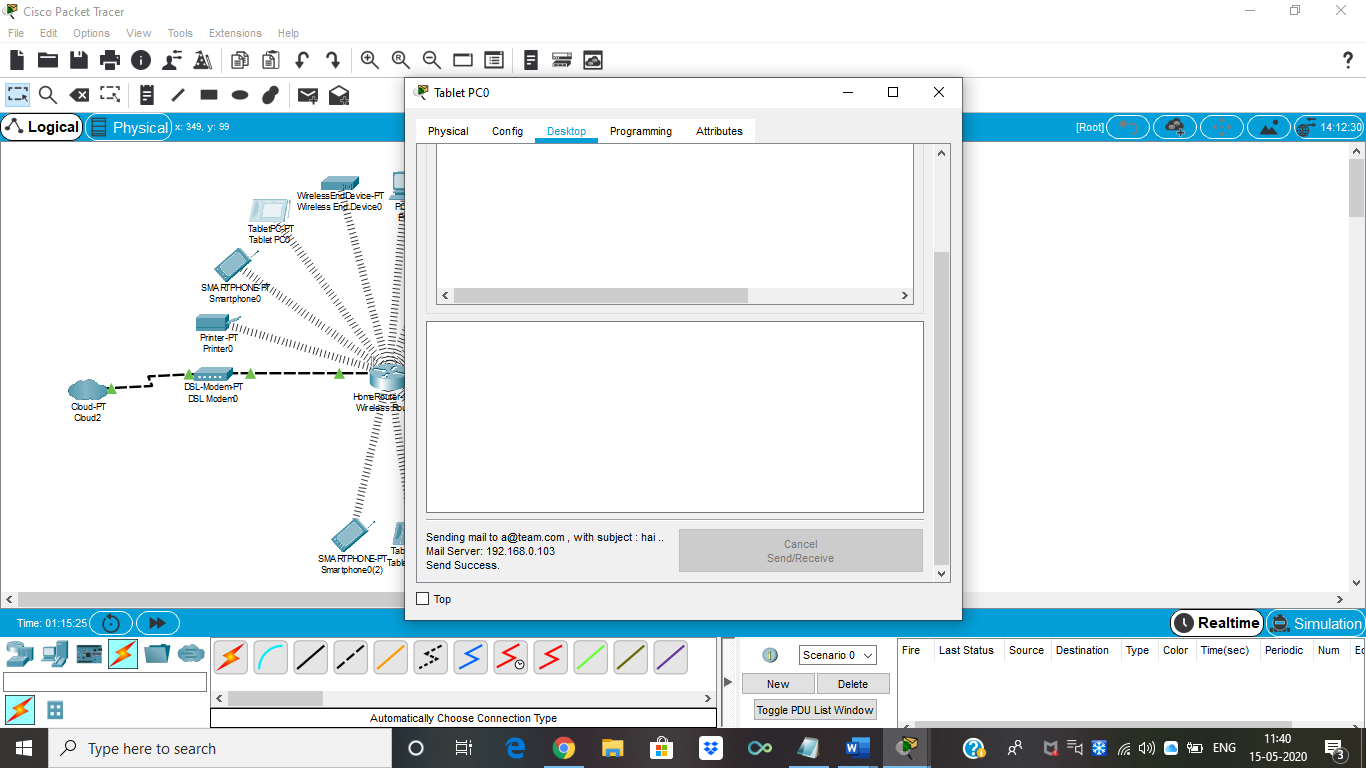


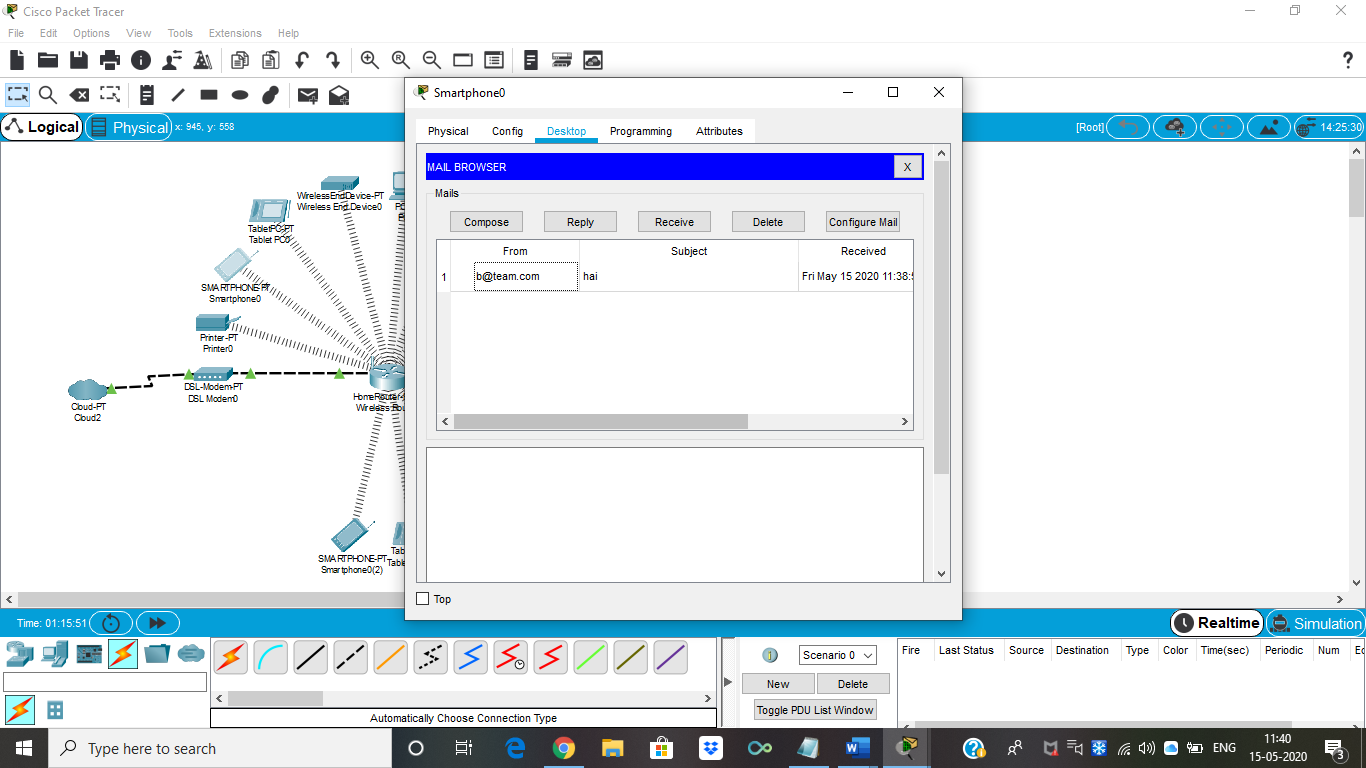
Enabling HTTP Services



Mail Server Configuration:







Ip Address Implementation:

|  |  |
| --- | --- |
| Departments/ SubNetwork Name | IP Address Range |
| Server | 192.168.0.16 255.255.255.255 |
| Wireless LAN | 192.168.0.0 255.255.255.0 |
| LAN 1 | 192.168.3.0 255.255.255.0 |
| Router Network | 192.168.2.0 255.255.255.0 |

#### 

#### (a) Routing Algorithm

The routing algorithm is OSPF (Open Shortest Path First).

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) standardized by the Internet Engineering Task Force (IETF) and commonly used in large Enterprise networks. OSPF is a link-state routing protocol providing fast convergence and excellent scalability. Like all link-state protocols, OSPF is very efficient in its use of network bandwidth.

OSPF uses a shorted path first algorithm in order to build and calculate the shortest path to all known destinations. The shortest path is calculated with the use of the Dijkstra algorithm. The algorithm by itself is quite complicated. This is a very high level, simplified way of looking at the various steps of the algorithm:

1. Upon initialization or due to any change in routing information, a router generates a link-state advertisement. This advertisement represents the collection of all link-states on that router.
2. All routers exchange link-states by means of flooding. Each router that receives a link-state update should store a copy in its link-state database and then propagate the update to other routers.
3. After the database of each router is completed, the router calculates a Shortest Path Tree to all destinations. The router uses the Dijkstra algorithm in order to calculate the shortest path tree. The destinations, the associated cost and the next hop to reach those destinations form the IP routing table.
4. In case no changes in the OSPF network occur, such as cost of a link or a network being added or deleted, OSPF should be very quiet. Any changes that occur are communicated through link-state packets, and the Dijkstra algorithm is recalculated in order to find the shortest path.

The algorithm places each router at the root of a tree and calculates the shortest path to each destination based on the cumulative cost required to reach that destination. Each router will have its own view of the topology even though all the routers will build a shortest path tree using the same link-state database. The following sections indicate what is involved in building a shortest path tree.

#### (b) 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). |

|  |  |  |
| --- | --- | --- |
| 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 |
| 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 |
| Jitter | Jitter is defined as the variation in time delay for the data packets sent over a network. This variable represents an identified disruption in the normal sequencing of data packets. Jitter is related to latency, since the jitter manifests itself in increased or uneven latency between data packets, which can disrupt network performance and lead to packet loss and network congestion. Although some level of jitter is to be expected and can usually be tolerated, quantifying network jitter is an important aspect of comprehensive network | Latency=sum of all delays    To measure Jitter, we take the difference between samples, then divide by the number of samples (minus 1). |

Network latency = N \* ( Nth (Dprop) + Nth (Dtrans))

Units: milliseconds

Where,

N is the number of intermediate nodes

Dprop  is the propagation delay

Dtrans is the transmission delay

Throughput = successful packet deliveries / total number of packets transmitted

References:

<https://www.cisco.com/c/en/us/products/collateral/wireless/e-nb-06-preparing-for-wifi-6-ebook-cte-en.html?oid=ebken019104>

<https://www.cisco.com/c/en/us/products/collateral/wireless/white-paper-c11-740788.pdf>

<https://www.cisco.com/c/en/us/products/ios-nx-os-software/open-shortest-path-first-ospf/index.html>

<https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html#t3>