Project:

ATTENDANCE MANAGEME­­NT

**Table of Contents**

**Acknowledgement**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Student Declaration**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Table of Contents**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Cisco Packet Tracer**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. **Devices used in the network\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
3. **Switches\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
4. **Routers\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
5. **Server\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
6. **Addressing\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
7. **IP Addressing\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
8. **MAC Addressing\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
9. **Configuring a wireless router\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
10. **Abstract**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
11. **Introduction\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
12. **LAN Networking**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
13. **Software Requirements**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
14. **Working** (through screenshots)\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ACKNOWLEDEGEMENT**

It would not have been possible without the kind support and help of many individuals and our institution. I would like to extend my sincere thanks to all of them.

I am highly indebted to BMIET for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.

I would like to express my gratitude to Ms. Nehafor her kind co-operation and training which helped me in completion of this project.

I would like to express my special gratitude and thanks to our teachers for giving me such attention and time.

My thanks and appreciations also go to my team members in developing the project and people who have willingly helped me out with their abilities.

**STUDENT’S DECLARATION**

I am Anurag hereby declare that I have been a part of this project team and contributed to its completion with best of my efforts, in partial fulfillment of requirements for the award of degree of B.Tech (Computer Science Engineering) at **B.M Institute of Engineering and Technology**, **Sonepat**. The work which is being presented in the training report submitted to Department of **Computer Science Engineering** at **B.M Institute of Engineering and Technology, Sonepat** is an authentic record of our own work.

Signature of student

Anuragl

CSE/16/108

**COMPUTER NETWORKS PROJECT DOCUMENTATION**

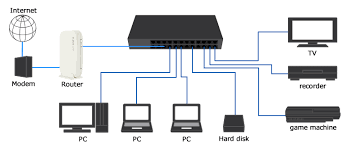
**CISCO PACKET TRACER:**

**Packet Tracer** is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.Packet Tracer can be run on Linux and Microsoft Windows.

Similar Android and iOS apps are also available. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices.

**DEVICES USED IN OUR PROJECT:**

**SWITCHES:**

 ****

A network switch (also called switching hub, bridging hub, officially MAC bridge is a computer networking device that connects devices on a computer network by using packet switching to receive, process, and forward data to the destination device.

A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Some switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

Switches for Ethernet are the most common form of network switch.. Switches also exist for other types of networks including Fibre Channel, Asynchronous Transfer Mode, and InfiniBand.

Unlike less advanced repeater hubs, which broadcast the same data out of each of its ports and let the devices decide what data they need, a network switch forwards data only to the devices that need to receive it.

**LAYER SPECIFIC FUNCTIONALITY**

**Layer 1:**

A **layer 1** network device transfers data, but does not manage any of the traffic coming through it, an example is Ethernet hub. Any packet entering a port is repeated to the output of every other port except for the port of entry. Specifically, each bit or symbol is repeated as it flows in. A repeater hub can therefore only receive and forward at a single speed. Since every packet is repeated on every other port, packet collisions affect the entire network, limiting its overall capacity.

By the early 2000s, there was little price difference between a hub and a low-end switch. Hubs remained useful for a time for specialized applications, such supplying a copy of network traffic to a packet analyzer. A network tap may also be used for this purpose and many network switches now have a port mirroring feature that provides the same functionality.

**Layer 2:**

A **layer 2** network device is a multiport device that uses hardware addresses, MAC address, to process and forward data at the data link layer (layer 2)

A switch operating as a network bridge may interconnect devices in a home or office. The bridge learns the MAC address of each connected device. Bridges also buffer an incoming packet and adapt the transmission speed to that of the outgoing port. While there are specialized applications, such as storage area networks, where the input and output interfaces are the same bandwidth, this is not always the case in general LAN applications. In LANs, a switch used for end user access typically concentrates lower bandwidth and uplinks into a higher bandwidth.

Interconnect between switches may be regulated using spanning tree protocol (STP) that disables links so that the resulting local area network is a tree without loops. In contrast to routers, spanning tree bridges must have topologies with only one active path between two points. Shortest path bridging is a layer 2 alternative to STP allows all paths to be active with multiple equal cost paths.

**Layer 3:**

A **layer-3** switch can perform some or all of the functions normally performed by a router. Most network switches, however, are limited to supporting a single type of physical network, typically Ethernet, whereas a router may support different kinds of physical networks on different ports.

A common layer-3 capability is awareness of IP multicast through IGMP snooping. With this awareness, a layer-3 switch can increase efficiency by delivering the traffic of a multicast group only to ports where the attached device has signalled that it wants to listen to that group.

**Layer-3** switches typically support IP routing between VLANs configured on the switch. Some layer-3 switches support the routing protocols that routers use to exchange information about routes between networks.

**Layer 4:**

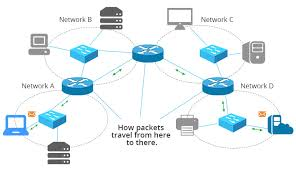
While the exact meaning of the term layer-4 switch is vendor-dependent, it almost always starts with a capability for network address translation,[citation needed] and may add some type of load distribution based on TCP sessions or advanced QoS capabilities.

The device may include a stateful firewall, a VPN concentrator, or be an IPSec security gateway.

**Layer 7:**

Layer-7 switches may distribute the load based on uniform resource locators (URLs), or by using some installation-specific technique to recognize application-level transactions. A layer-7 switch may include a web cache and participate in a content delivery network (CDN).

**ROUTERS:**

** **

A **wireless router** is a device that performs the functions of a router and also includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network. Depending on the manufacturer and model, it can function in a wired local area network.

**Most current wireless routers have the following characteristics:**

1.One or multiple NICs supporting Fast Ethernet or Gigabit Ethernet integrated into the main SoC.

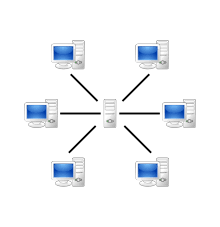
2.Some newer routers feature Link Aggregation allowing two ports to be used together improving throughput and redundancy.

3.One or multiple WNICs supporting a part of the IEEE 802.11-standard family also integrated into the main SoC or as separate chips on the printed circuit board. It also can be a distinct card connected over a MiniPCI or MiniPCIe interface.

4.Some dual-band wireless routers operate the 2.4 GHz and 5 GHz bands simultaneously.

**Generic Router** is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links or point-to-multipoint links over an Internet Protocol network.

**SERVER:**

** **

In computing, a server is a computer program or a device that provides functionality for other programs or devices, called "clients". This architecture is called the client–server model, and a single overall computation is distributed across multiple processes or devices. Servers can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers. A client process may run on the same device or may connect over a network to a server on a different device. Typical servers are database servers, file servers, mail servers, print servers, web servers, game servers, and application servers.

Client–server systems are today most frequently implemented by (and often identified with) the request–response model: a client sends a request to the server, which performs some action and sends a response back to the client, typically with a result or acknowledgement. Designating a computer as "server-class hardware" implies that it is specialized for running servers on it. This often implies that it is more powerful and reliable than standard personal computers, but alternatively, large computing clusters may be composed of many relatively simple, replaceable server components.

A **media access control address** (MAC address) of a device is a unique identifier assigned to a network interface controller (NIC). For communications within a network segment, it is used as a network address for most IEEE 802 network technologies, including Ethernet, Wi-Fi, and Bluetooth. Within the Open Systems Interconnection (OSI) model, MAC addresses are used in the medium access control protocol sublayer of the data link layer. As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or no separator (see Notational conventions below).

**ADDRESSING REQUIRED FOR CONFIGURING DEVICES:**

**MAC ADDRESSING :**

A **MAC address** may be referred to as the burned-in address, and is also known as an Ethernet hardware address, hardware address, and physical address (not to be confused with a memory physical address).

A network node with multiple NICs must have a unique MAC addresses for each. Sophisticated network equipment such as a multilayer switch or router may require one or more permanently assigned MAC addresses.

MAC addresses are most often assigned by the manufacturer of network interface cards. Each is stored in hardware, such as the card's read-only memory or by a firmware mechanism. A MAC address typically includes the manufacturer's organizationally unique identifier (OUI). MAC addresses are formed according to the rules of one of two numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): EUI-48 (it replaces the obsolete term MAC-48)and EUI-64.EUI is an abbreviation for Extended Unique Identifier.

**IP ADDRESSING:**

An **Internet Protocol address** (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.An IP address serves two principal functions: host or network interface identification and location addressing.

Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number. However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address, was developed in 1995,and standardized in December 1998.In July 2017, a final definition of the protocol was published. IPv6 deployment has been ongoing since the mid-2000s.

IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 in IPv4, and 2001:db8:0:1234:0:567:8:1 in IPv6. The size of the routing prefix of the address is designated in CIDR notation by suffixing the address with the number of significant bits, e.g., 192.168.1.15/24, which is equivalent to the historically used subnet mask 255.255.255.0.

The IP address space is managed globally by the Internet Assigned Numbers Authority (IANA), and by five regional Internet registries (RIRs) responsible in their designated territories for assignment to end users and local Internet registries, such as Internet service providers. IPv4 addresses have been distributed by IANA to the RIRs in blocks of approximately 16.8 million addresses each. Each ISP or private network administrator assigns an IP address to each device connected to its network. Such assignments may be on a static (fixed or permanent) or dynamic basis, depending on its software and practices.

**DHCP SERVER:**

A**DHCP Server** is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

A DHCP server automatically sends the required network parameters for clients to properly communicate on the network. Without it, the network administrator has to manually set up every client that joins the network, which can be cumbersome, especially in large networks. DHCP servers usually assign each client with a unique dynamic IP address, which changes when the client’s lease for that IP address has expired.

**When to use a router/switch as your DHCP Server**  
There are many enterprise companies who are still using DHCP for IPv4 on their routers/switches.  This is typically done by the network administrator who needs to get a DHCP capability up and running quickly but does not have access to a DHCP server. Most routers/switches have the ability to provide the following DHCP server support:

a DHCP client and obtain an interface IPv4 address from an upstream DHCP service

a DHCP relay and forward UDP DHCP messages from clients on a LAN to and from a DHCP server

a DHCP server whereby the router/switch services DHCP requests directly. However, there are limitations to using a router/switch as a DHCP server

Running a DHCP server on a router/switch consumes resources on the network device.  These DHCP packets are handled in software (not hardware accelerated forwarding).  The resources required make this practice not suitable for a network with a large number (> 150) of DHCP clients.

Does not support dynamic DNS.  The router/switch DHCP server cannot create an entry into DNS on behalf of the client based on the IPv4 address that was leased to the client.

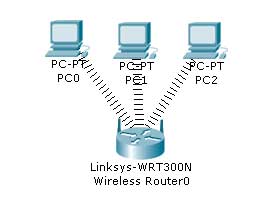
No ability to e asily manage the scope and see the current DHCP bindings and leases across multiple routers.  Administrator must log into the switch/router individually to get information about DHCP bindings.

No high availability or redundancy of the DHCP bindings.  This could cause problems if the current DHCP server and default gateway fails.

It is more difficult to configure DHCP options on router/switch platform.

The DHCP service running on a router/switch is not integrated with IP address management (IPAM) for address tracking and scope utilization or security forensics.

**CONFIGURING A WIRELESS ROUTER:**



To Setup the Wireless network, you need a wireless network adapter.

By default the Wireless Router will be having DHCP configured and enabled, which will be in certain range.

The Computers are configured to receive IP from the DHCP Server.

So all the PCs shall receive the IP address.

The default credentials for the Wireless Router are as below:

SSID: default

Username: admin

Password: admin

We will connect from the PC0 and using the web browser, we will configure the wireless router. In Packet tracer, Under Desktop Tab, Click Web browser and in the URL space give the IP of the Wireless Router.

Login with the credentials: admin / admin

In the GUI for the Router configuration, Scroll down and under the DHCP setting, select the “Disabled” Option.

Now, let’s change the configuration to be static and have the configuration as below:

Username: admin

Password: certilogy

Now under the Administration tab, change the default admin password for the router, so no one else can login.

We keep username as “admin” and change the password to “certilogy”

Once you save this setting and continue, you will again be prompted for the password as the credentials have changed and you need to provide the new credentials.

Username: admin

Password: certilogy

Now let’s change the SSID so we remember it as our Wireless Network (change it to “certilogy” and also change security mode to “WEP” and provide a key “0987654321”. Thus when any computer will try to connect to this Wireless Router, It will have to choose the SSID as “certilogy” and when asked for PIN / Key “0987654321”

Under the Wireless Security, select WEP as Security Mode and assign a Key.

Now Click on PC wireless on the Desktop Menu and Connect to the WIFI Network.

And Click on the WIFI Network and Connect to it with the WEP Key

We see that we have now successfully connected to the Wireless Network.

**Abstract**

In the past, we used to call the name of members for the purpose of attendance checking by instructors. They verify the identity of member's participation by human recognition using facial and voice matching. This approach is time-consuming because the number of members is getting increased. Moreover, they may have to recheck any of the students’ presence at the end of the lecture manually. In this research, we offer a convenient attendance checking method to take advantage of Wi-Fi technology. Our network initiates Wi-Fi service for checking and uploading attendance of users by instructors. By this way managers/instructors can easily check the member's attendance. In addition, this research proposes a novel concept that unlimited number of devices can be supported. We make use of Wireless routers and smart devices, resulting in an enhanced scalability.

**Introduction**

The most common means of tracking student attendance in the classroom is by enforcing the students to manually sign the attendance sheet, which is normally passed around the classroom while the lecturer is conducting the lecture. There are numerous disadvantages of using such system. The attendance sheet is passed around the class; some students may accidentally or purposely sign another student's name. Another issue of having the attendance record in a hardcopy form is that a lecturer may lose the attendance sheet. As a consequence of that, lecturer can no longer trace the students overall attendance record throughout the particular semester. In this system faculty report the student’s attendance via application and notification of attendance is passed to the server and thus to HOD office and Principal office.

All HOD PC’s are LAN connected to the Principal office. So that Principal get a master copy of whole day activity and can know about the every lecture conducted by concern faculty and take action on lecturer who does not taken lecture. The application has a lot of advantages, such as unique, permanent, good anti-fake and easy to use. So it is recognized increasingly by people.

**LAN Networking**

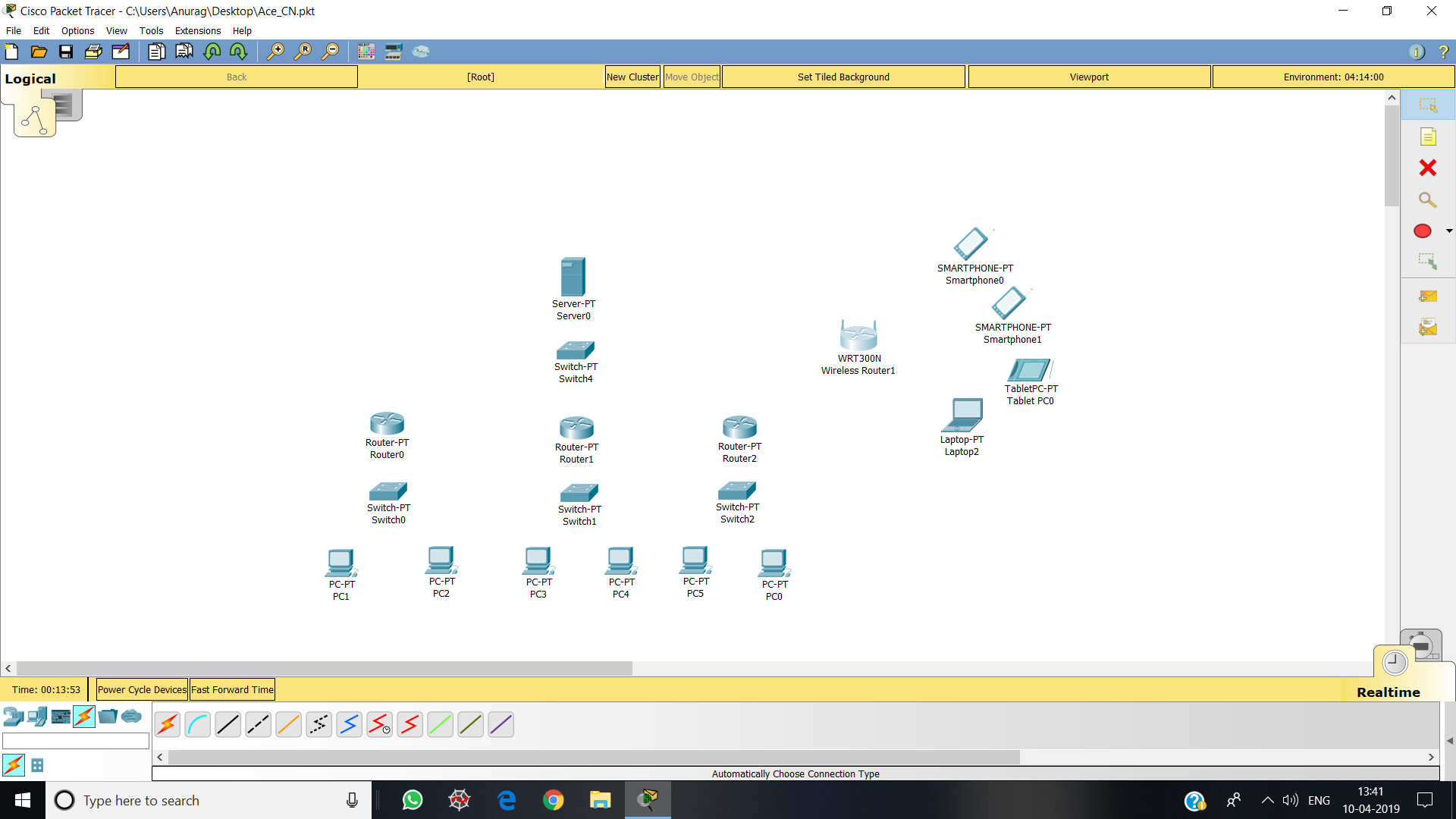
A local-area network (LAN) is a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings; however, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN). Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which itexecutes programs, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions. LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line; but the distances are limited, and there is also a limit on the number of computers that can be attached to a single LAN.

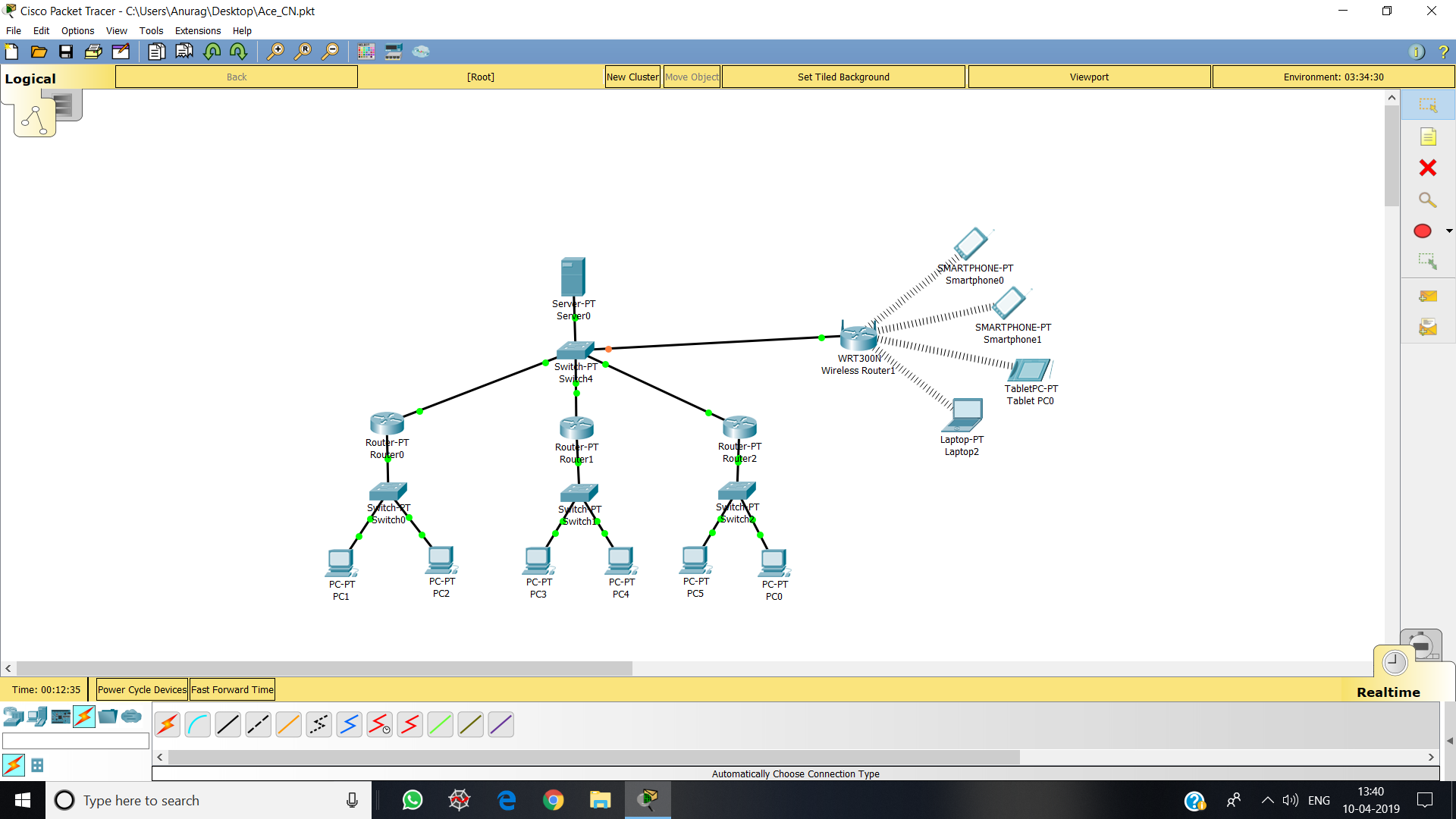
**SOFTWARE REQUIREMENTS**

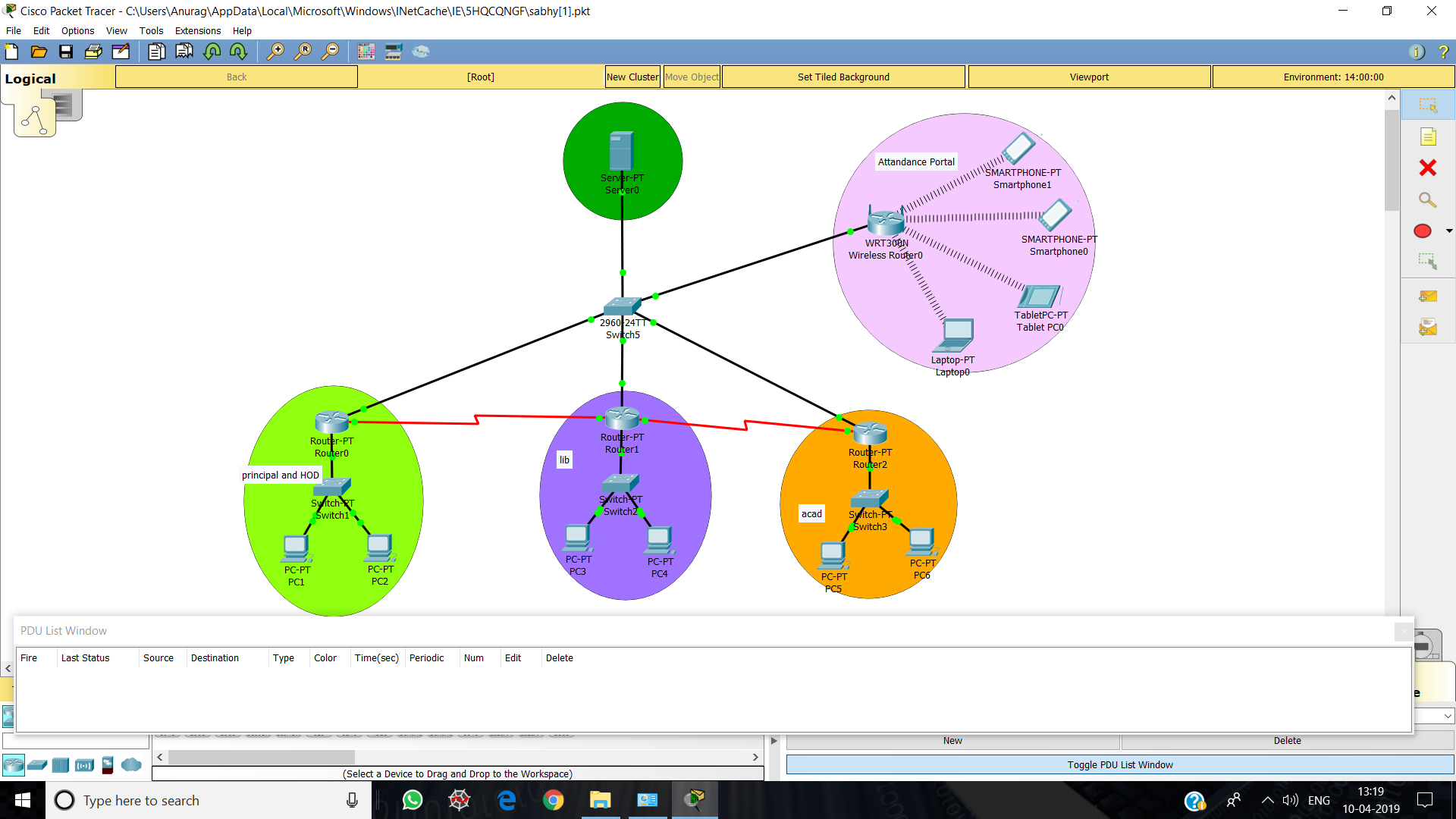
* Cisco Packet Tracer 7.1
* Microsoft Office

**WORKING** (Through Screenshots)

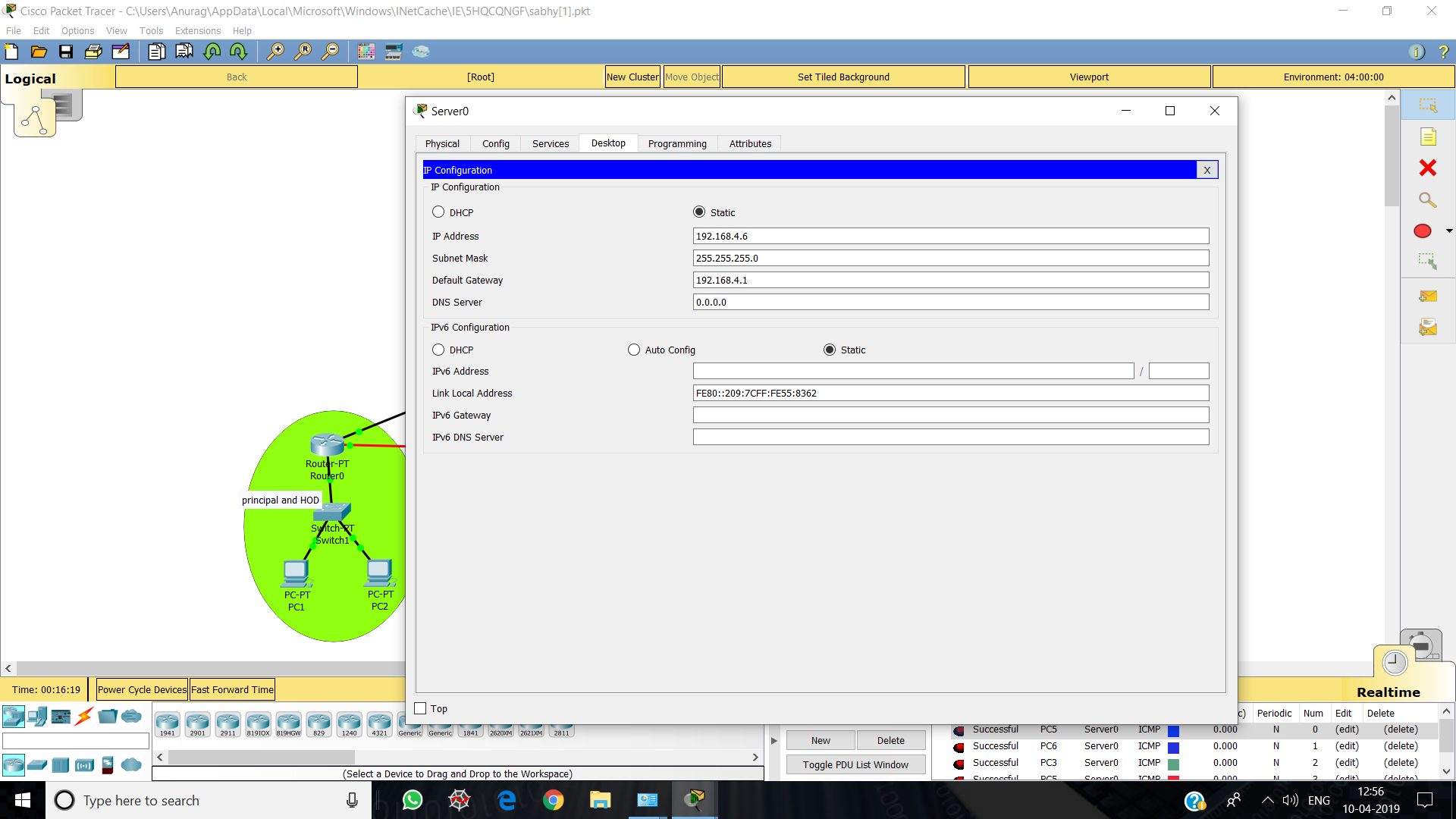
This is the network representing the entire attendance management system in our college. We have represented the online attendance portal using a wireless router. Also, we have represented the HOD office, the Principal office, Library, Accounts and Academics office using different routers connected with each other as needed.



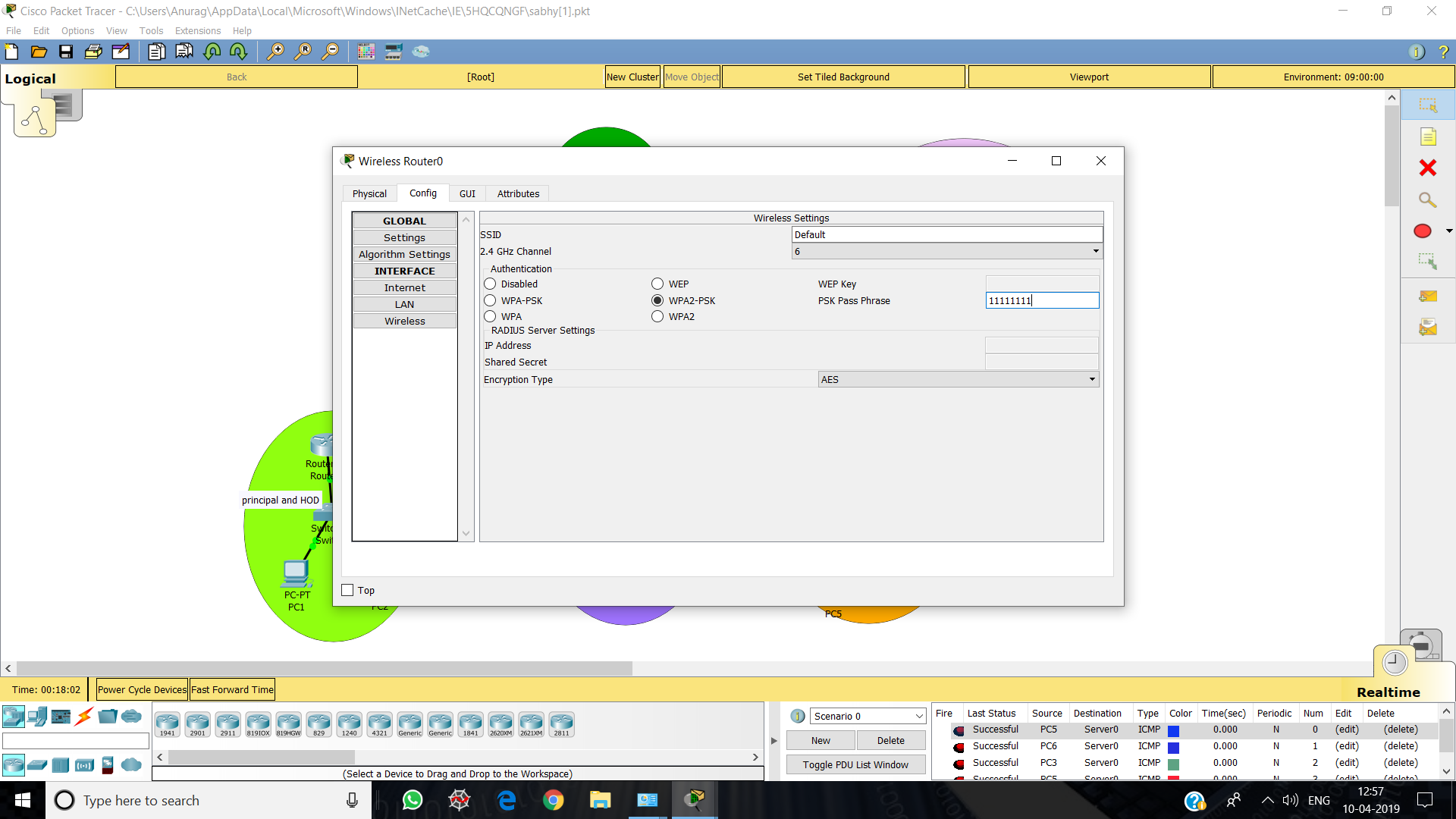


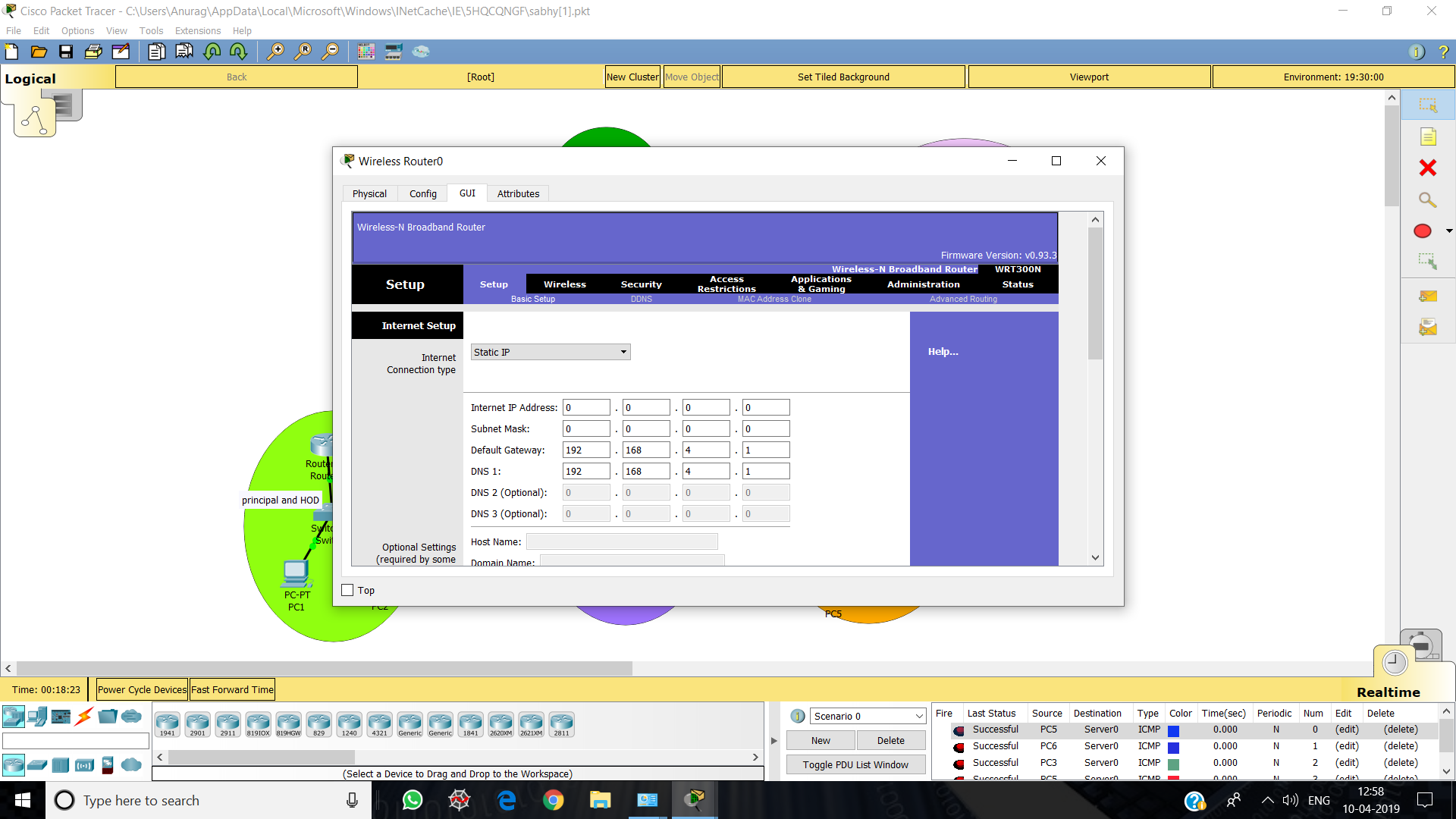


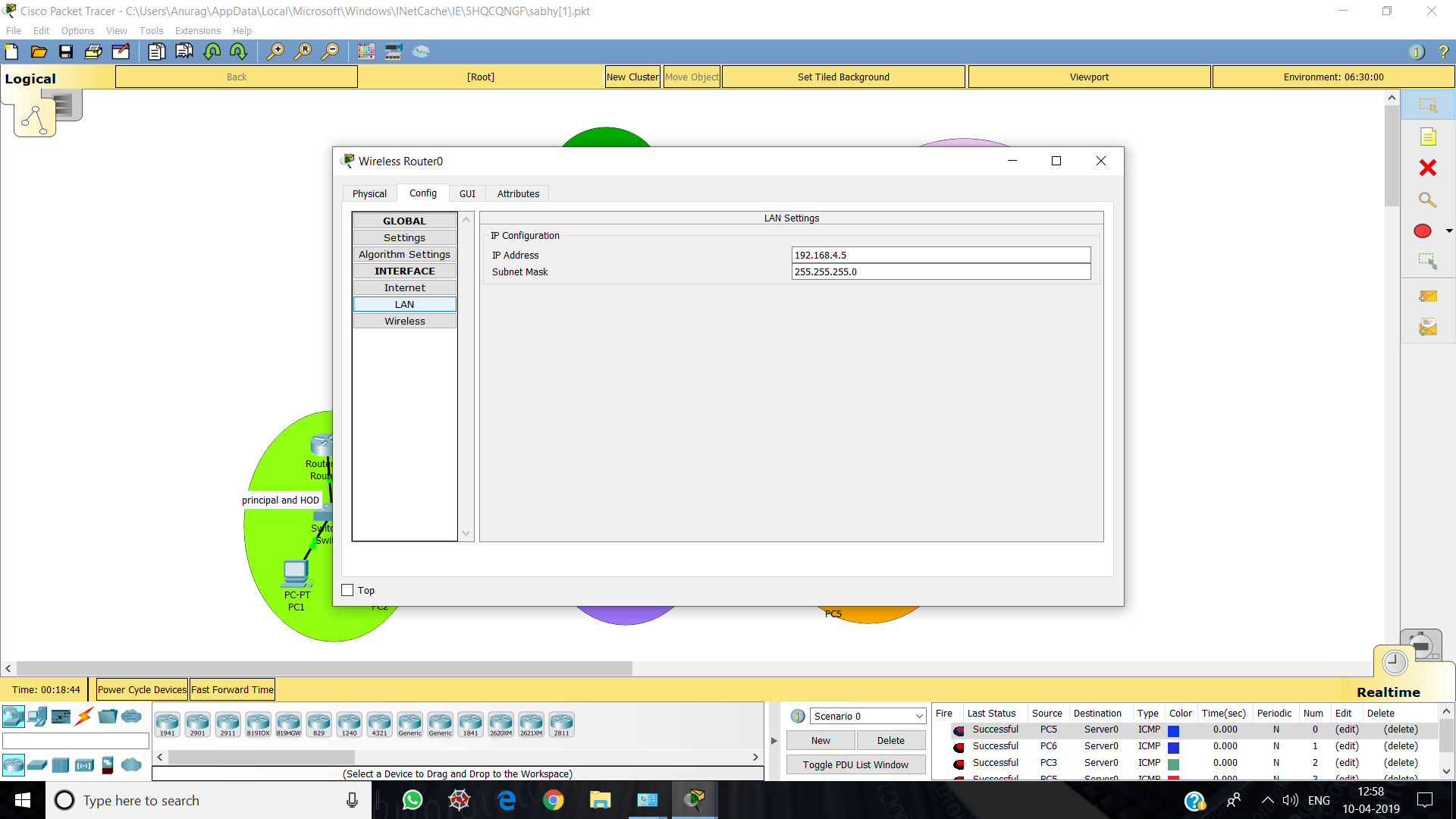
**Server** – The Server in this network stores and provides information regarding the attendance records of all the students, student profiles and the dues of the students, namely, account dues and library dues.

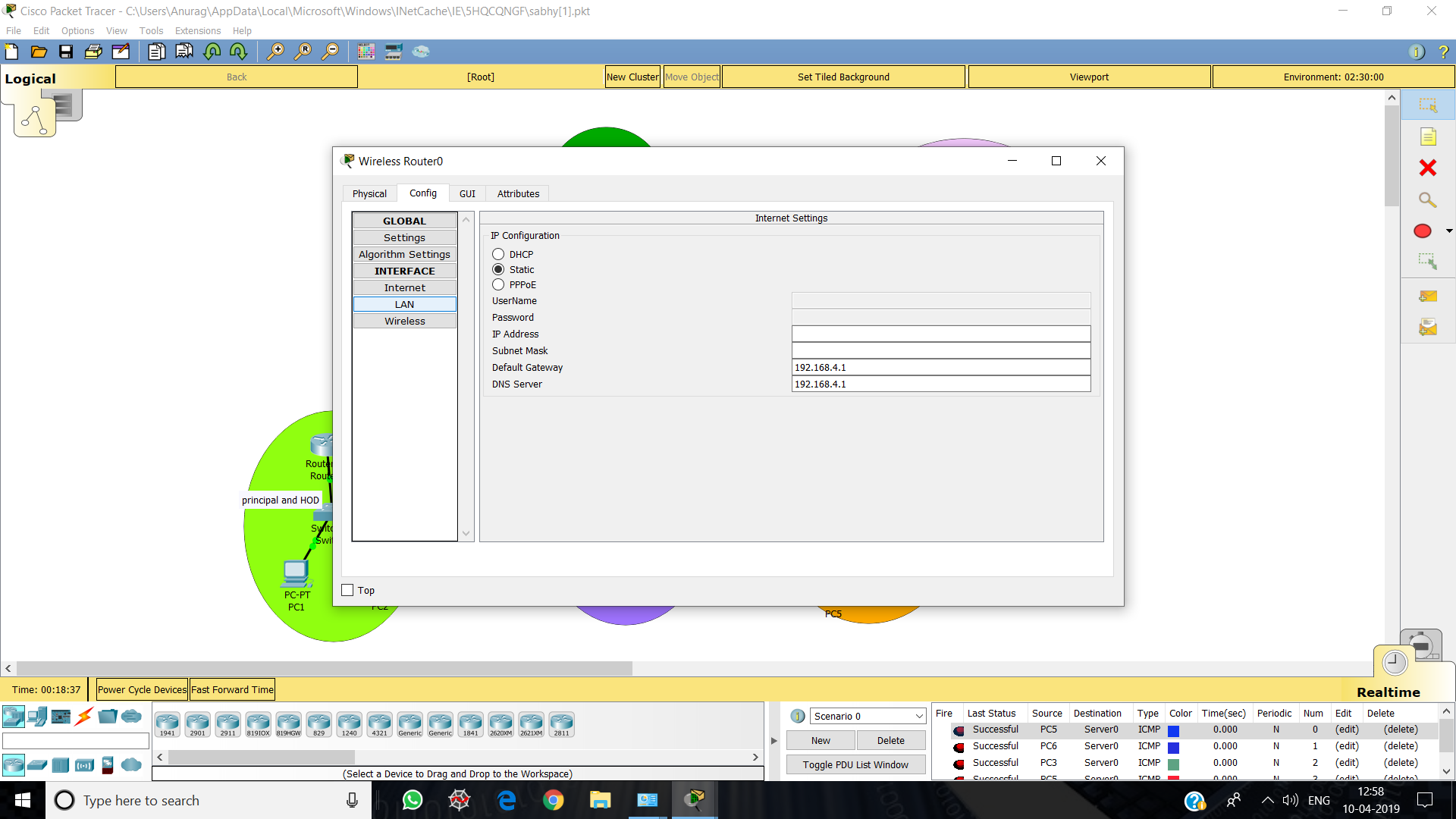


**Wireless Router (Attendance Portal)** - We have used wireless router so as to provide access to all portable smart devices and all to web application. The attendance portal can be accessed by the students to check their current attendance and can be accessed by the faculty to upload and modify student’s attendance.

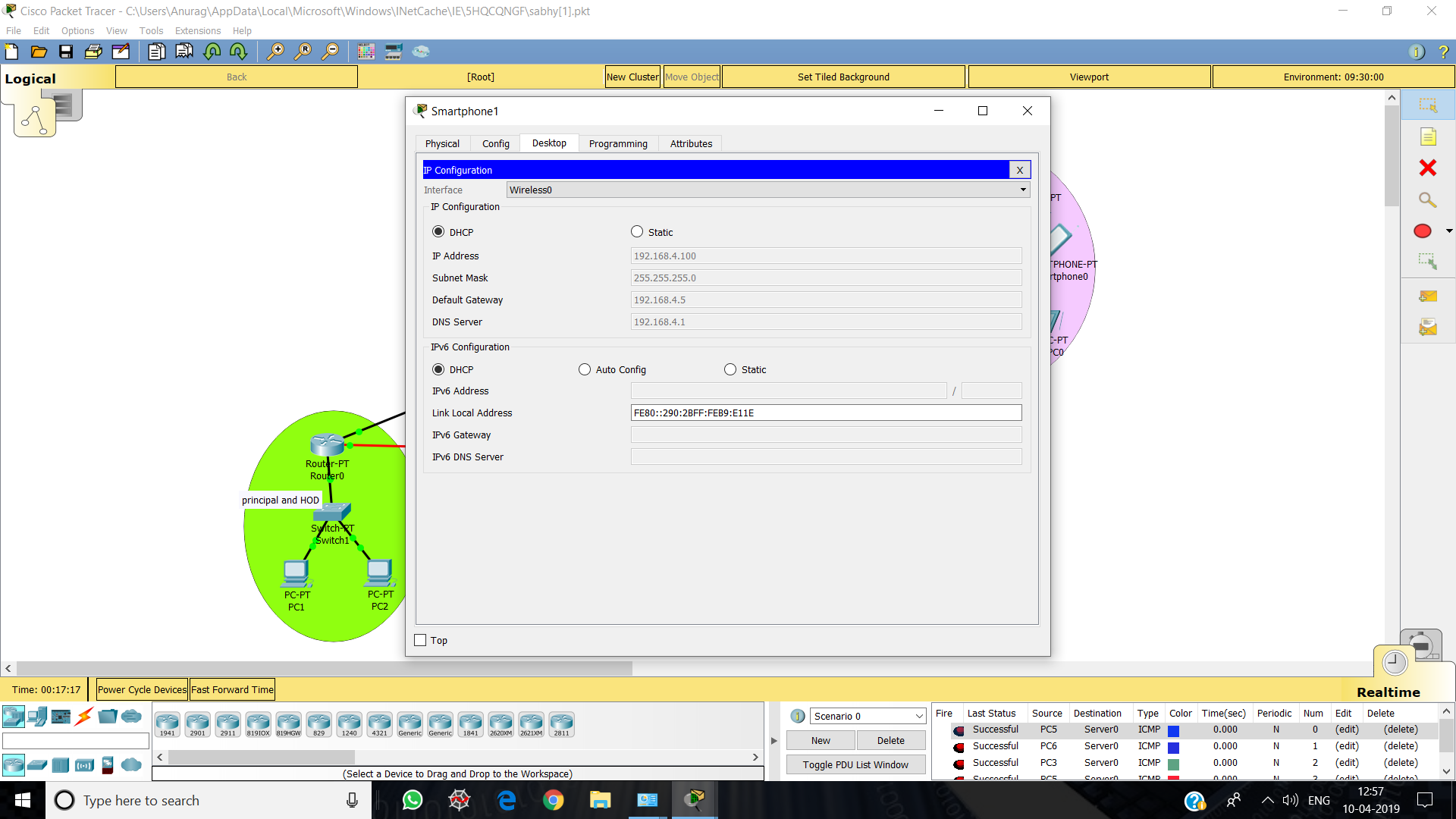




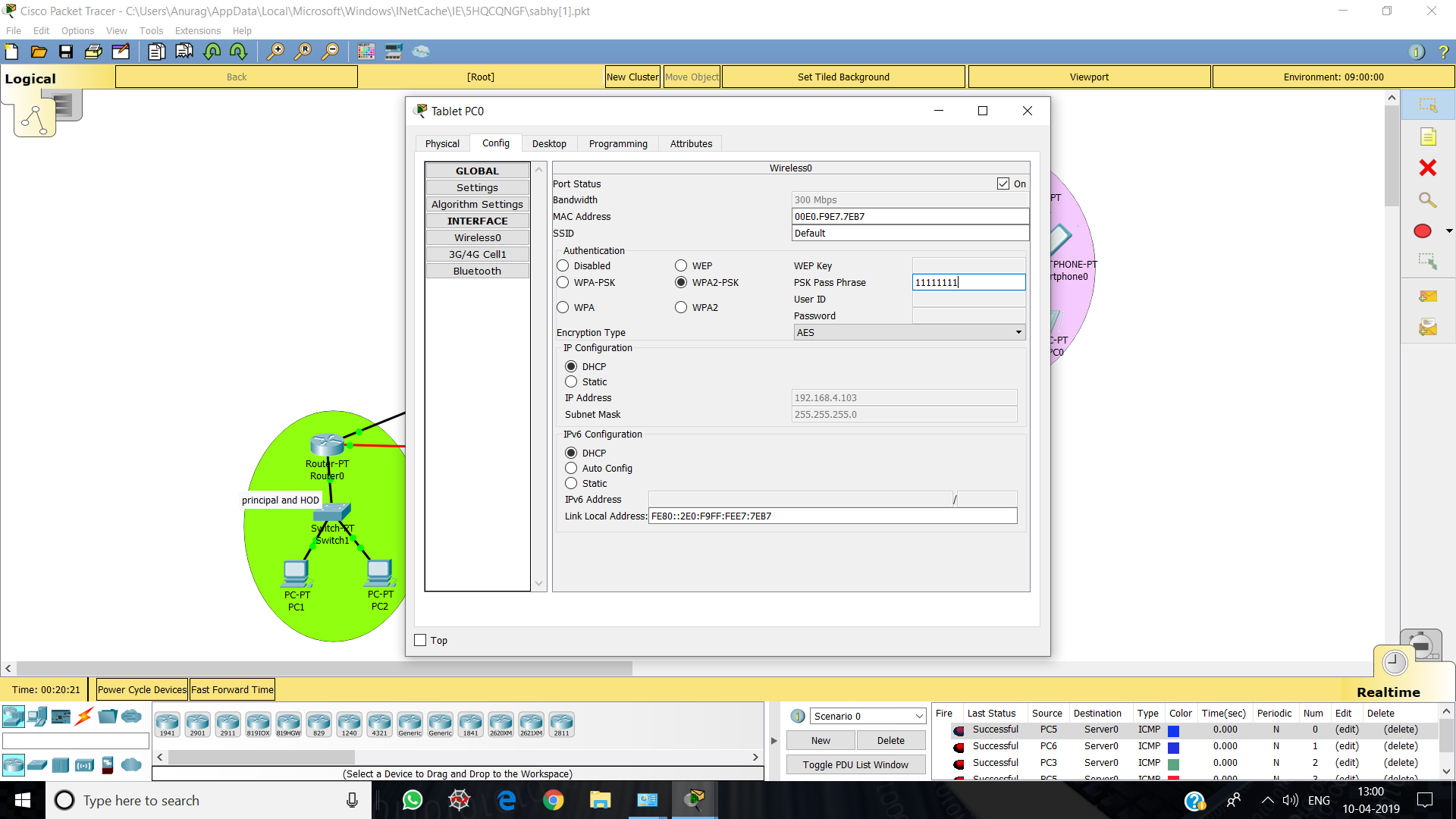


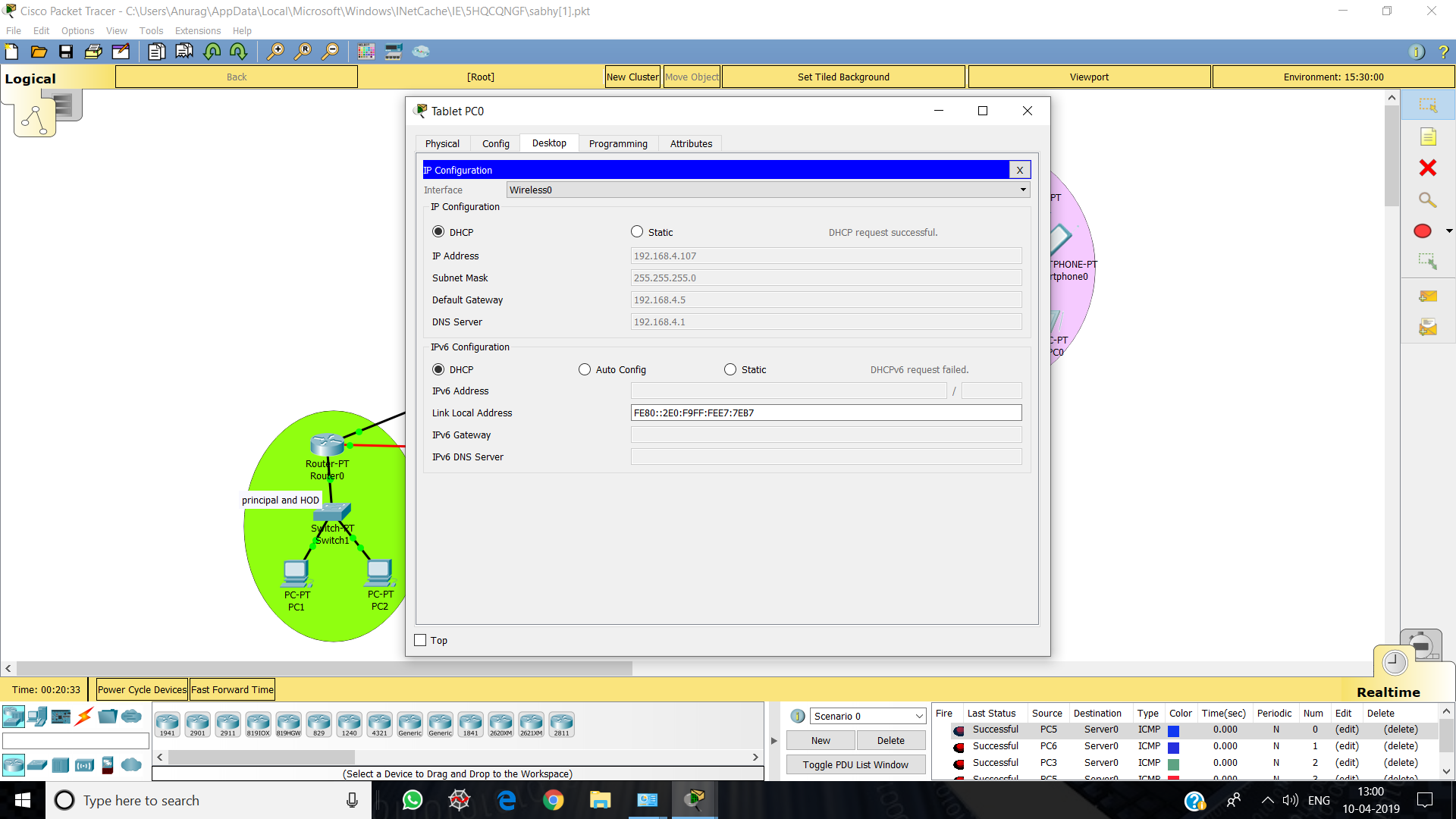


**Smartphone –** This represents the access of portable devices.

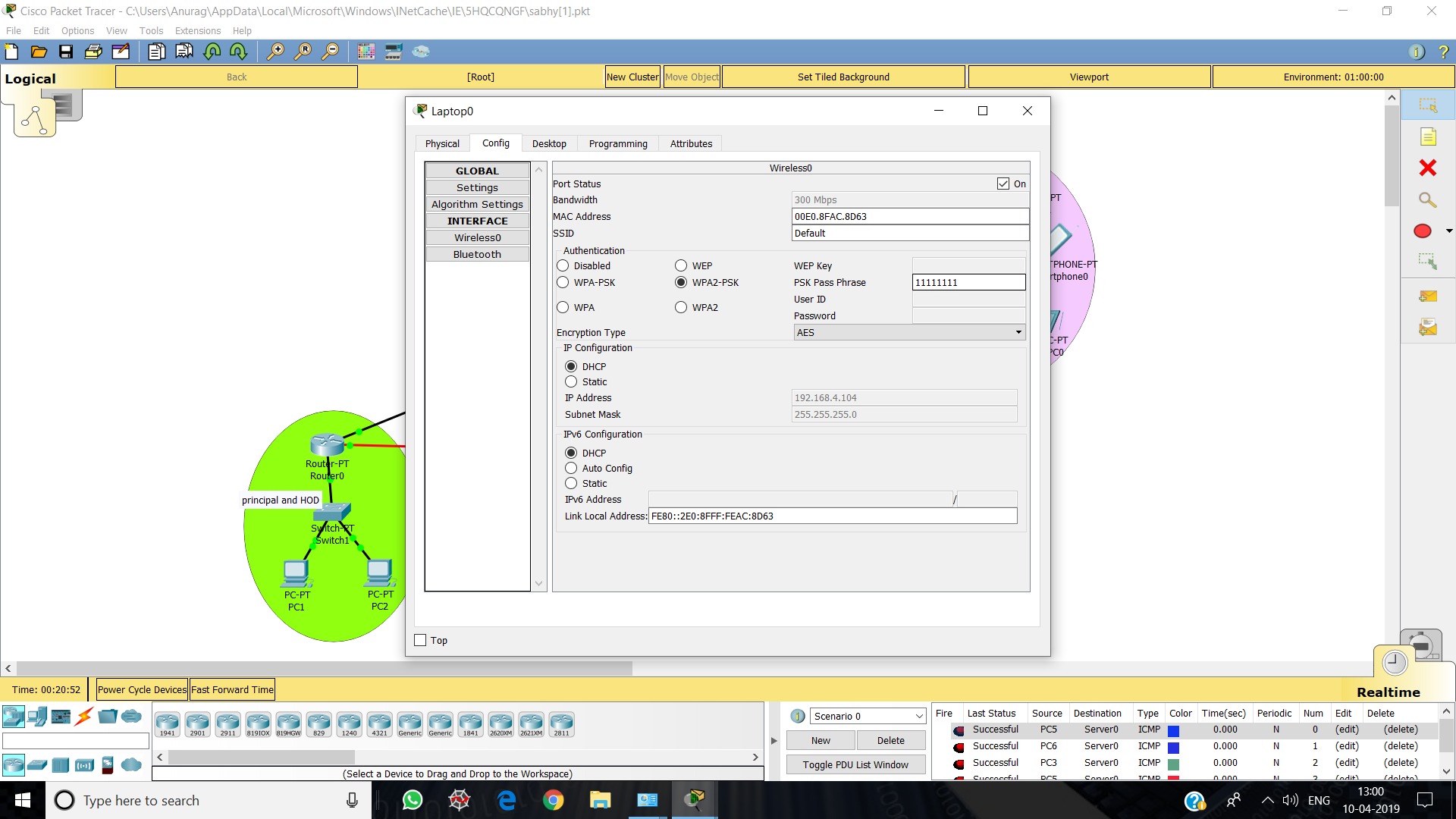


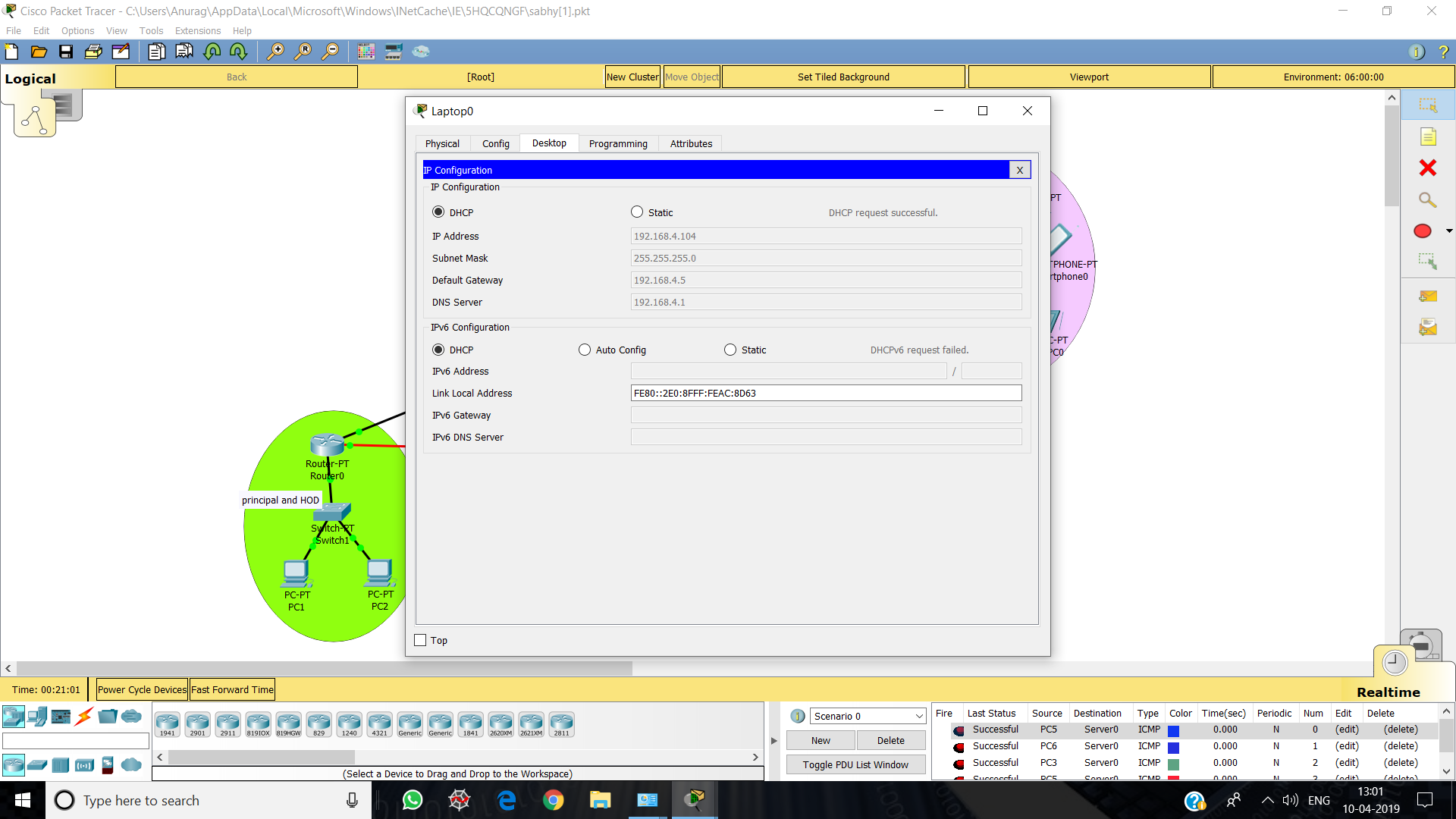
**Tablet (**Portable device)





**Laptop –** Access via web application



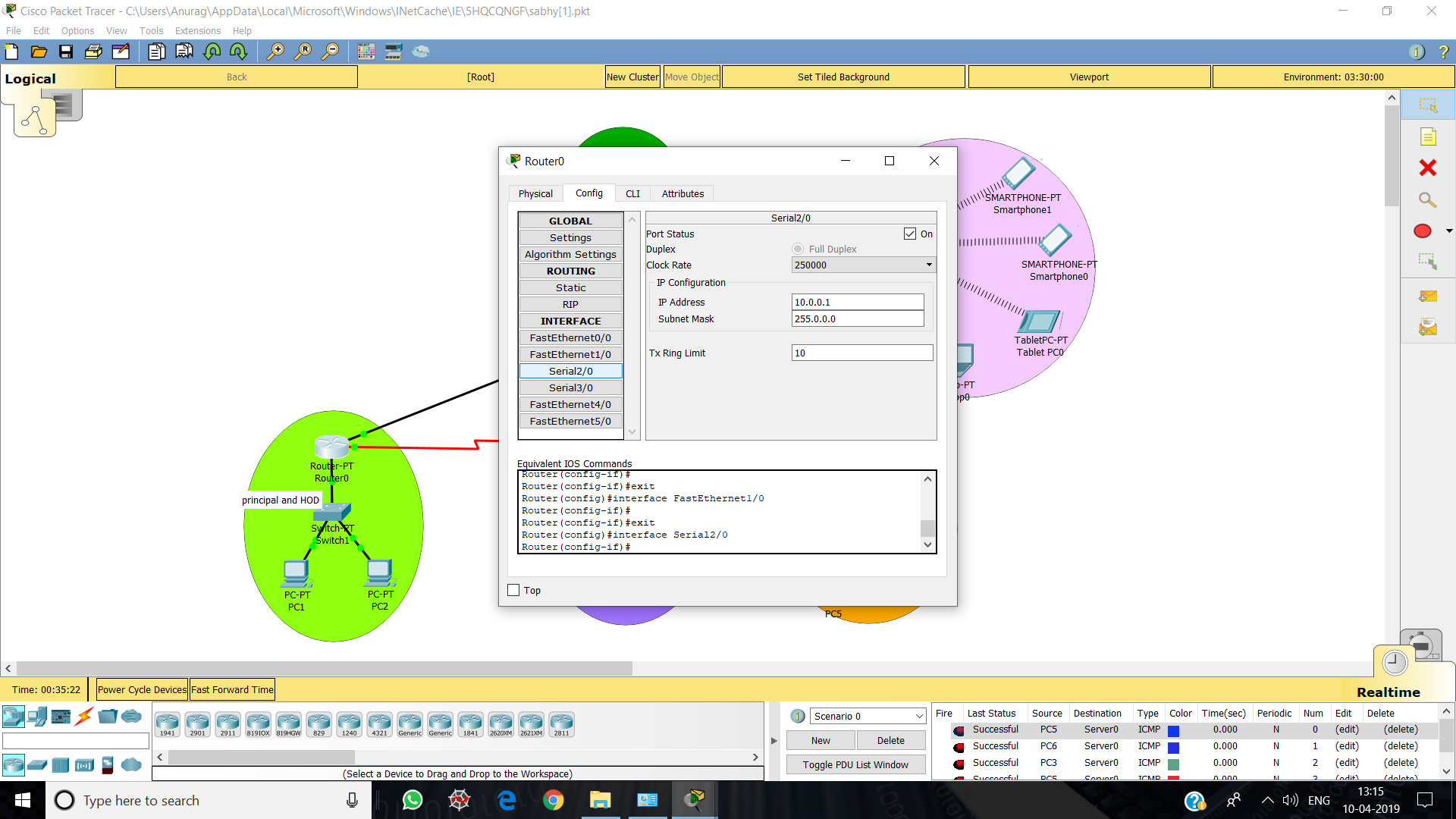


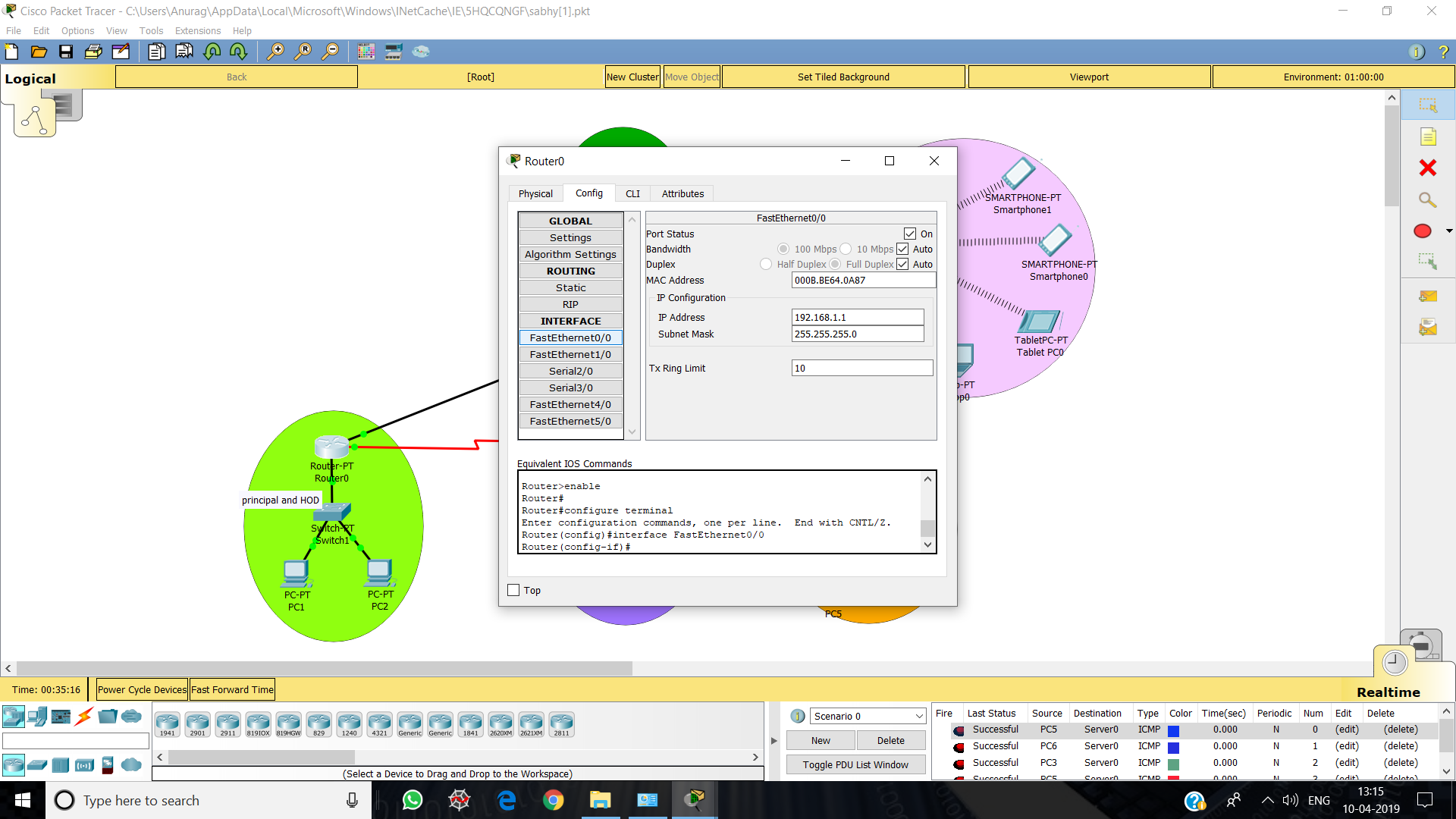
**Router -** Used to route messages and information to and from server to the specific PC as needed.

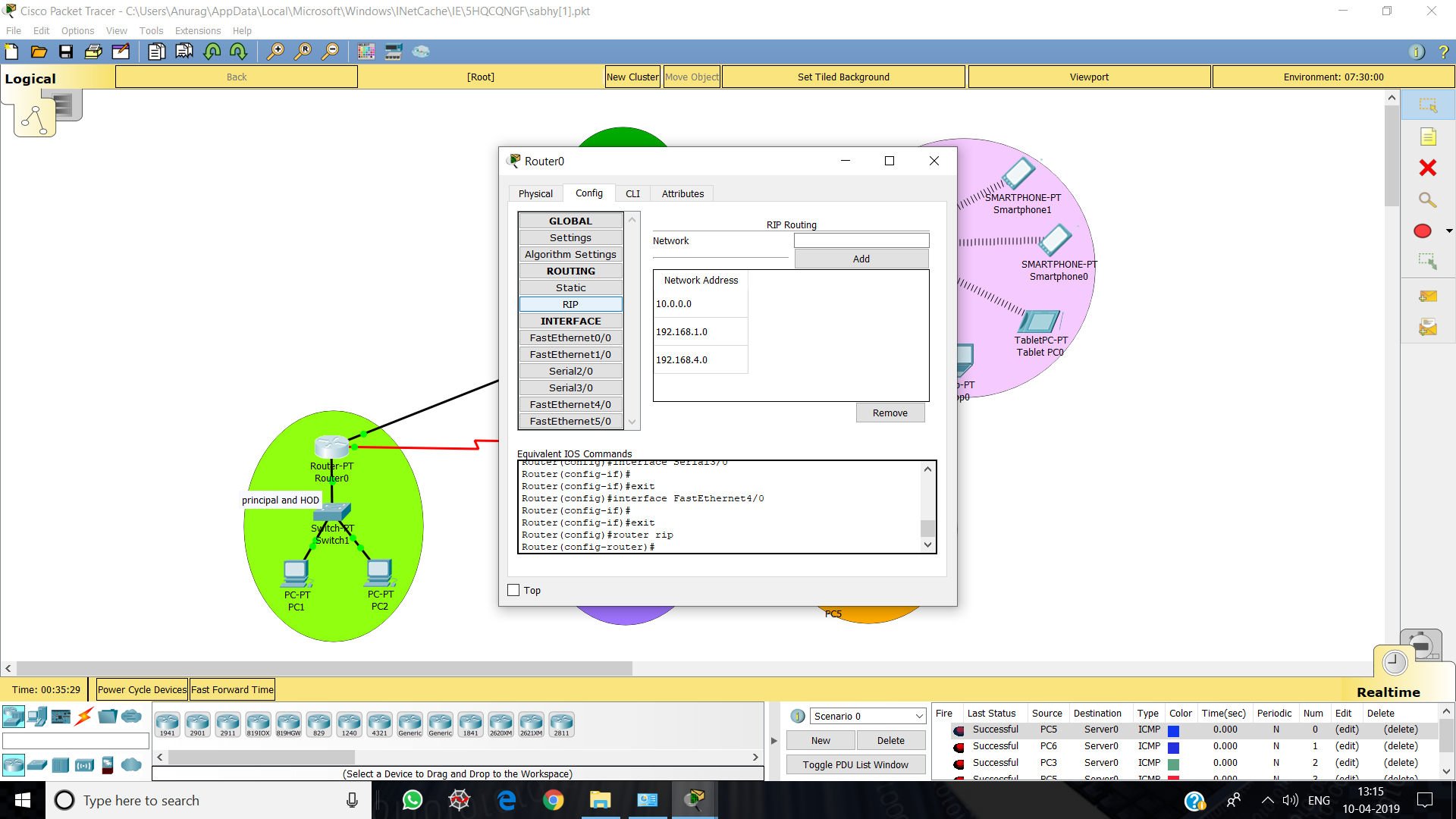
Router0 – Principal and HOD

Router1 – Library

Router2 – Academics and Accounts







**PC** – Systems used to access portal to modify or check attendance.

PC1 – Principal

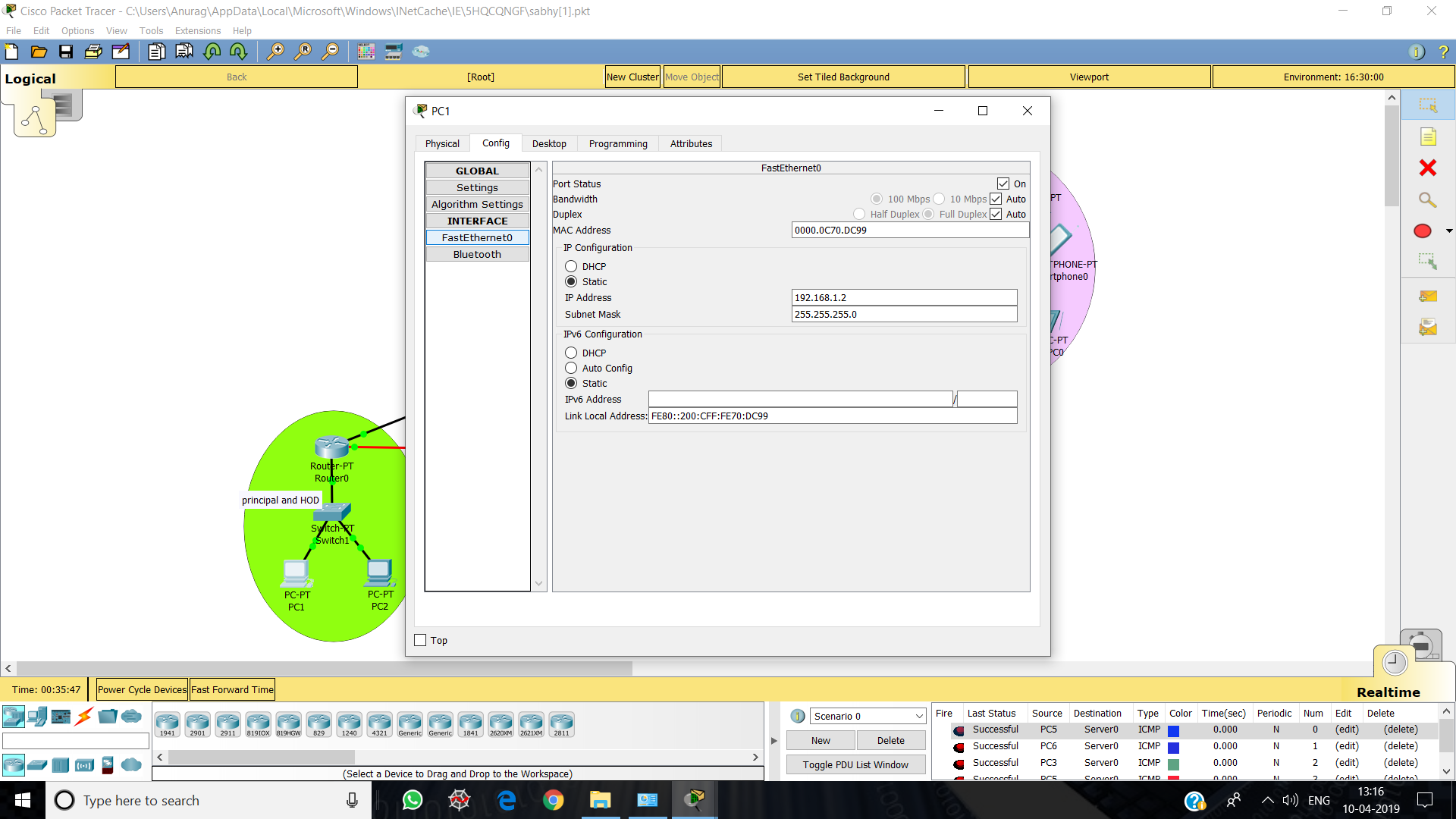
PC2 – HOD

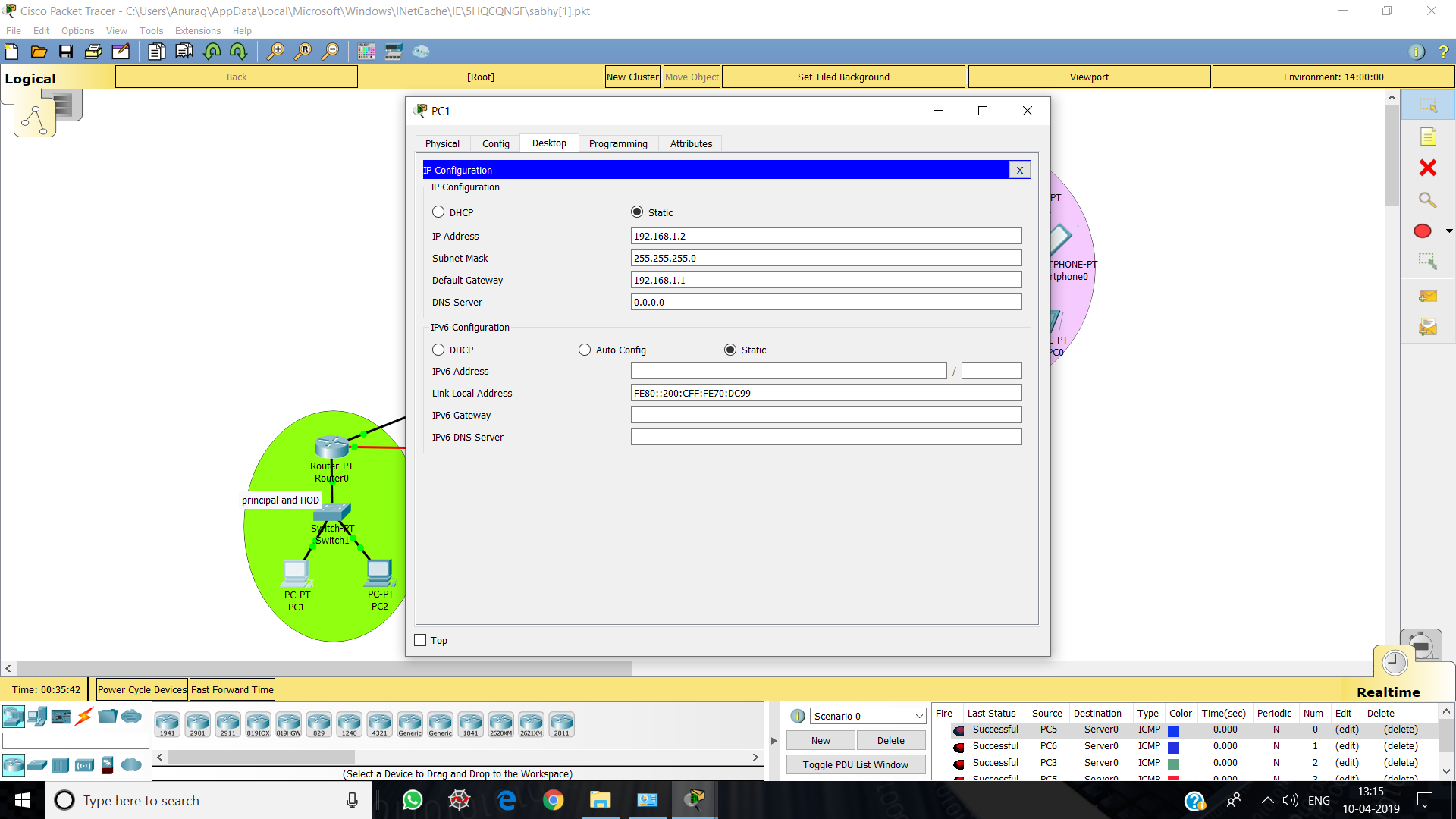
PC3 – Library

PC4 –Library

PC5 – Academics

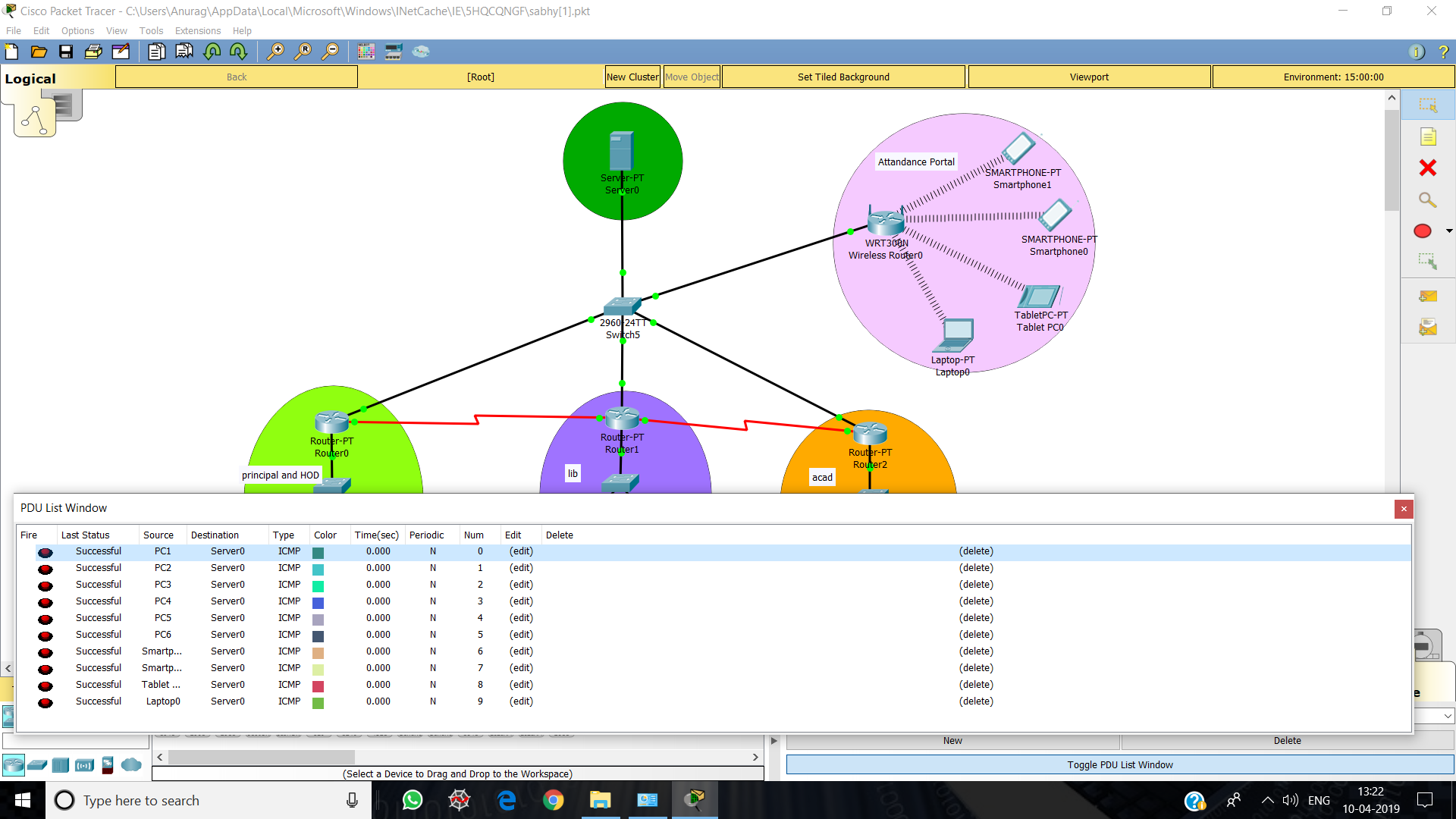
PC6 – Accounts

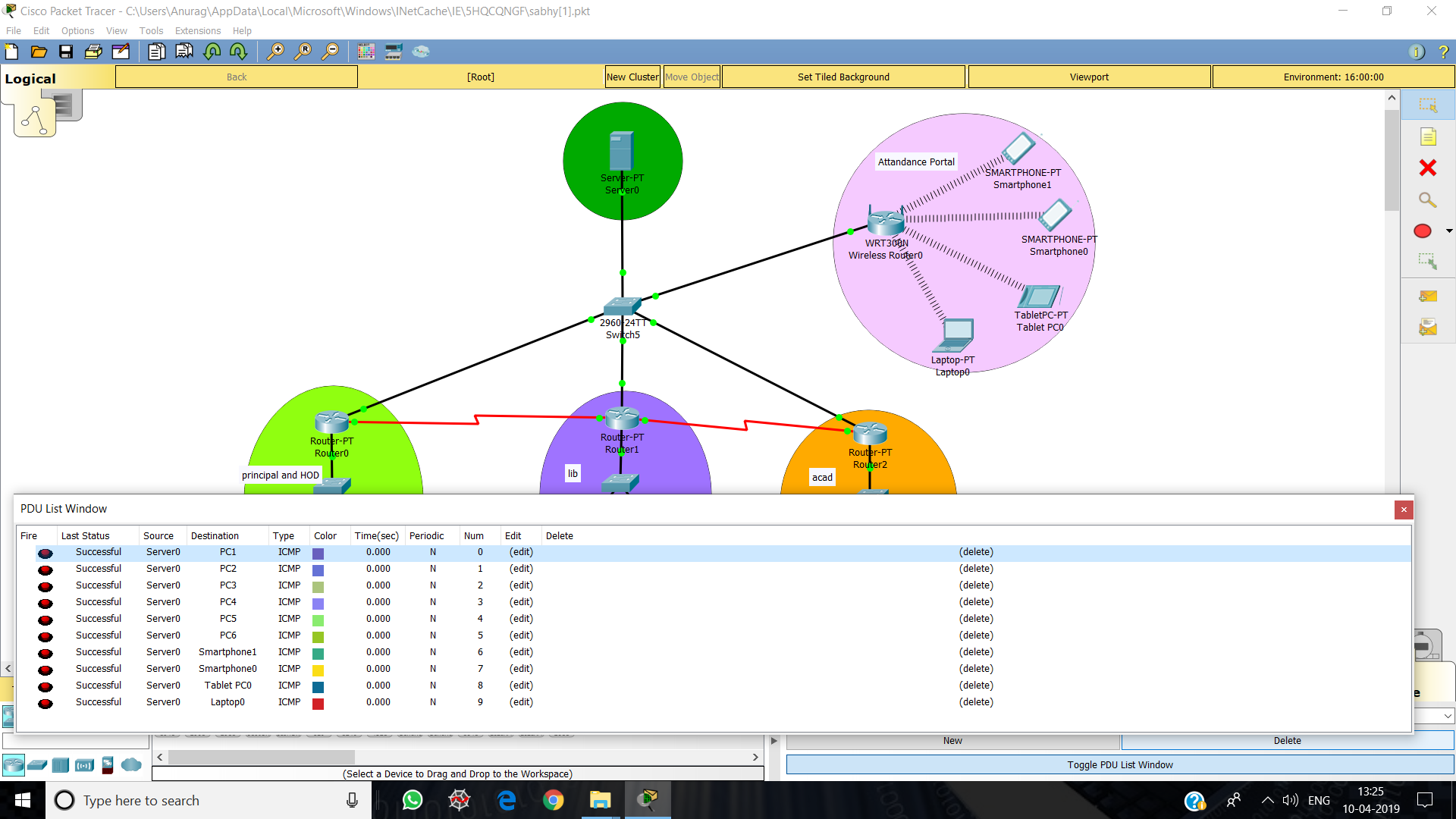


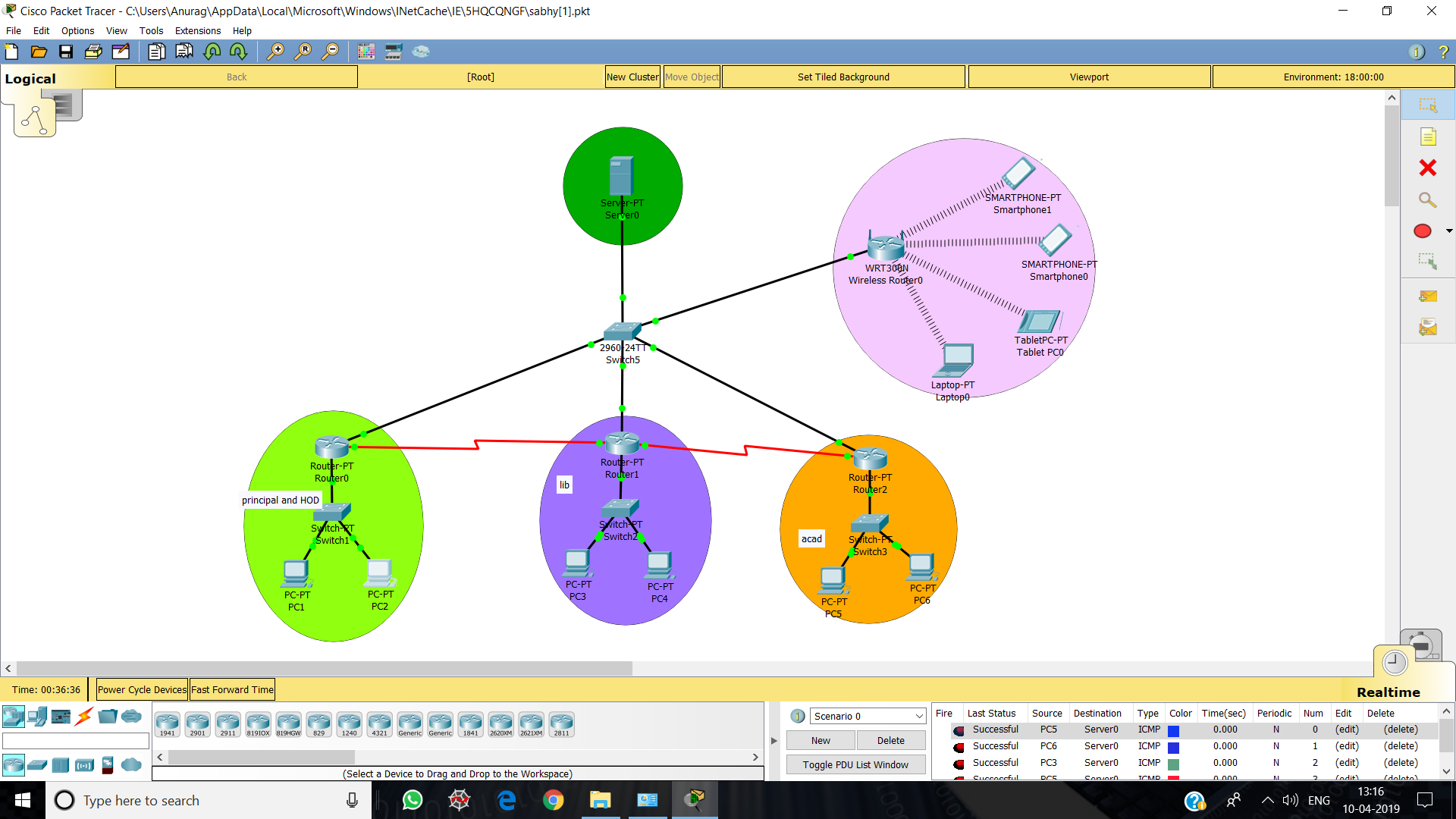


**DATA PACKETS**

Messages and information is needed to be transferred from PC to PC, PC to Server, Wireless Router to Server, portable devices and vice-versa. The network created here successfully transmits messages.







**BIBLIOGRAPHY**

netcademy.com

google.com/network-devices

<https://journals.sagepub.com/doi/full/10.1155/2015/508698>

<https://github.com/landtanin/StudentAttendanceCheck>

**Practical file**

On

ATTENDANCE MANAGEMENT

(Using CISCO PACKET TRACER)

**BACHELOR OF TECHNOLOGY**

*In*

COMPUTER SCIENCE ENGINEERING

*By*

**ANURAG**

**CSE/16/108**



Submitted to:

Ms.Neha Verma

Department of COMPUTER SCIENCE ENGINEERING

B.M Institute of Engineering and Technology

GGSIPU