# Simulation of Wireless Network using Packet Tracer Tool

*Maher Riyadh Jabbar, maherj@kth.se*
*KTH Royal institute of technology*

## Abstract

Nowadays the internet provides many services such as Emails, chats, E-learning, E-health, online banking, and multiplayers online games. Computer networks in these services plays an important role as they allow the exchange information among many connected devices. So, in this report, a simple wireless network will be implemented and simulated using a network simulator tool, i.e. Cisco packet tracer, while focusing on how packets move among different devices to understand various concepts, such as connectivity by visualizing ICMP and TCP packet flow and analyze broadcasts.

## Contents



## Preface

I would like to thank Mr. G.Q. Maguire Jr. for a very rewarding and interesting course that made us learn interesting information about the relationship between human and internet worlds.

## 1. Introduction

The Local Area Network (LAN) is the most basic computer network that can be used for interconnection with wide area networks. A LAN permits sharing of data processing equipment such as mass storage media, and printers. Resource sharing is probably equally as important as the role of a LAN in providing access the Internet. Generally, computer networking was borne out of the need to use computers for sharing information within an organization in form of messages, files, data bases and so forth. Wireless communication is used across a wide range of distances, and unlike the situation in wired networking where a single technology (Ethernet) dominates, wireless networking utilizes multiple technologies, many with similar characteristics.

LAN consists of: physical links, common interfacing hardware connecting the hosts to the links, and protocols to make everything work together. Every LAN node is able to communicate with every other LAN node using Access Control List (ACL) that specifies which nodes (or users) are granted access to others nodes, as well as what operations are allowed on given node. Sometimes this will require the cooperation of intermediate nodes acting as switches or routers. To support universal connectivity, internet protocol (IP) provides a global mechanism for addressing and routing, so that packets can be delivered from any host to any other host. IP addresses (for the most-common version 4, which we denote IPv4) are 4 bytes (32 bits) and are part of the IP header that generally follows the Ethernet header. In the case of IEEE 802.3 (Ethernet) and IEEE 802.11 networks the Ethernet header only stays with a packet for one hop; the IP header stays with the packet for its entire journey across the Internet [1].

The International Standards Organization (ISO) divides network communication into seven layers. Layers 1-4 are considered the lower layers, and mostly concern themselves with moving data around. Layers 5-7, the upper layers, deal with application-level data. Networks operate on one basic principle: "pass it on." Each layer takes care of a very specific job, and then passes the data onto the next layer. This model is called open systems interconnection (OSI). In the OSI model, control is passed from one layer to the next, starting at the application layer (Layer 7) in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. The OSI model takes the task of inter-networking and divides the process up into what is referred to as a vertical stack that consists of the following 7 layers [2]:

- Application (Layer 7): This Layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Layer 7 Application examples include WWW browsers, HTTP, and FTP.
- Presentation (Layer 6): This layer provides independence from differences in data representation (such as encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer. Layer 6 Presentation examples include encryption, ASCII, EBCDIC, TIFF, GIF, PICT, and JPEG.
- Session (Layer 5): This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination. Layer 5 Session examples include NFS, NetBIOS names, RPC, and SQL.
- Transport (Layer 4): Layer 4 provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer. Layer 4 Transport examples include SPX, TCP, and UDP.
- Network (Layer 3): Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing. Layer 3 Network examples include AppleTalk DDP, IP, and IPX.
- Data Link (Layer 2): At layer 2, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control, and frame synchronization. The data link layer is divided into two sub layers: Media

Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control, and error checking. Layer 2 Data Link examples include PPP, ATM, IEEE 802.X, and HDLC.

- Physical (Layer 1): Layer 1 conveys the bit stream - electrical impulse, light, or radio signal through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards, and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components. Layer 1 Physical examples include Ethernet, FDDI, V.35, V.24, and RJ45.

TCP/IP protocols map to a four-layer conceptual model known as the DARPA model (Fig.1). The four layers of the DARPA model are: Application, Transport, Internet, and Network. In fact, the OSI Model's top three layers - that is: Application, Presentation, and Session - are essentially collapsed into the Application layer in TCP/IP. Additionally, the bottom two layers - Physical and Data Link - are combined into the Network Access layer for TCP/IP.

Generally, the three building blocks of a wireless LAN are: access points (AP), which are informally called base stations, an interconnection mechanism, such as a switch or router used to connect access points, and a set of wireless hosts, also called wireless nodes or wireless stations. A switch also performs routing operations. Usually a switch operates at layer 2 (the Data Link layer) while routers operate at layer 3 (the Network layer). In principle, two types of wireless LANs are possible [3]:

- *Ad hoc* — wireless hosts communicate among themselves without a base station
- Infrastructure — a wireless host only communicates with an access point, and the access point relays all packets

Due to limitation of *ad hoc* wireless networks (minimal security against unwanted incoming connections, inability to monitor the strength of signals, and often run slower than infrastructure mode), a service provider deploys a set of access points, and each wireless host communicates through one of these access points as shown in in Fig.2.

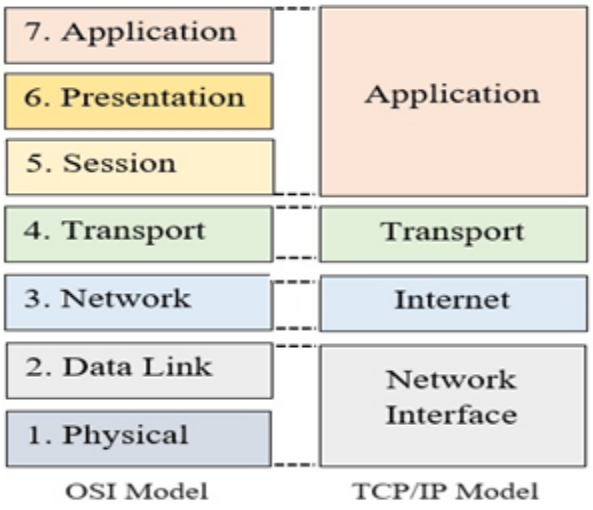



Fig.1 OSI and TCP/IP Layers

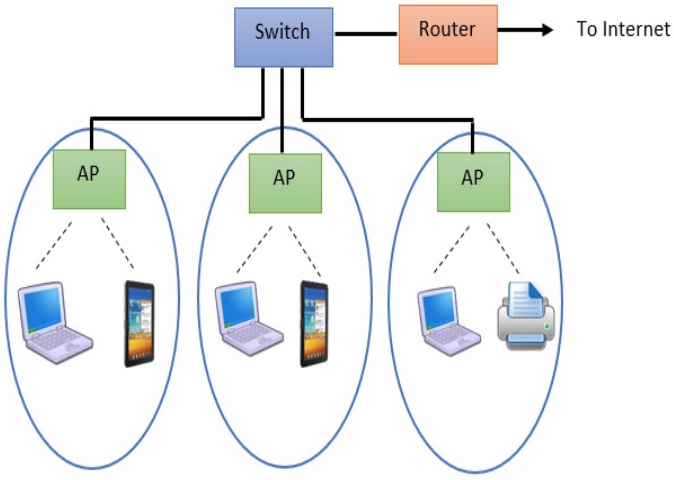



Fig.2 An infrastructure architecture for a wireless network

Generally, the main object of any network is to reduce the number of inaccessible users and workgroups. All terminals should have a capability to communicate with others and should provide desired information. Additionally, physical systems and devices should be able to preserve and provide suitable level of performance, reliability and security. As a result, system managers need expert tools to assist them with the design and maintenance of networks. A simulation tool offers a way to predict the impact on the network when upgrading the hardware, using another network topology [4], or changing in the traffic load. So, in this report, a simple wireless network is designed and simulated using Cisco Packet Tracer.

## 2. Simple Wireless Network

Cisco packet tracer tool is a powerful network simulation program that provides simulation, visualization, authoring, assessment, and collaboration capabilities and facilitates the teaching and learning of complex technology concepts. Packet Tracer allows a user to simulate highly complex networking environments and allows the user to see how packets move between different devices [5]. Fig.3 shows a simple wireless network that has been designed using Cisco packet tracer application [6].

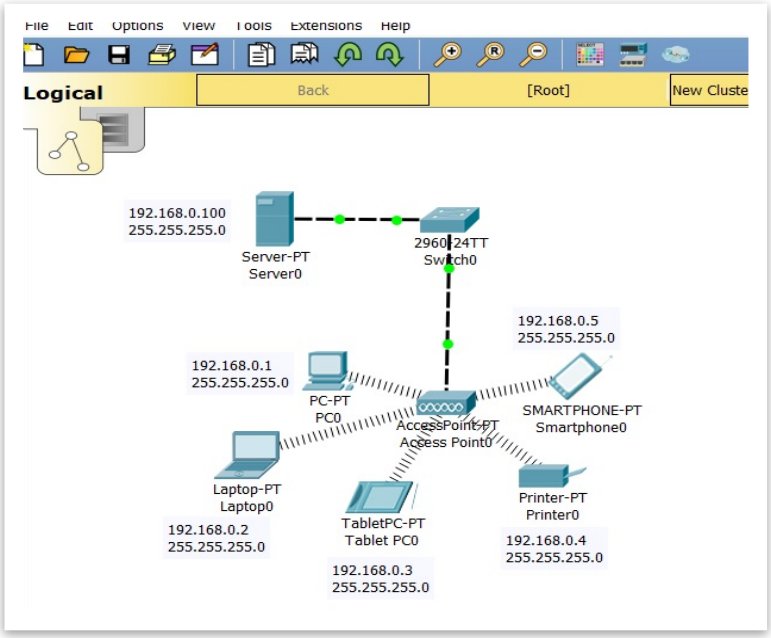



Fig.3 Simple wireless network

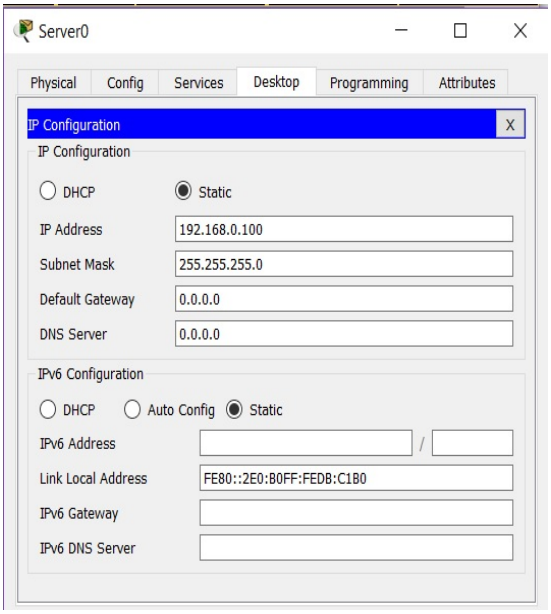



Fig.4 Server's IP address assignment

This network contains a server, switch, one access point, and several wireless terminals. Fig.4 shows how to assign IP address to the server, while Table-1 shows the configuration (IP address and Subnet mask) for each wireless device in the designed LAN.

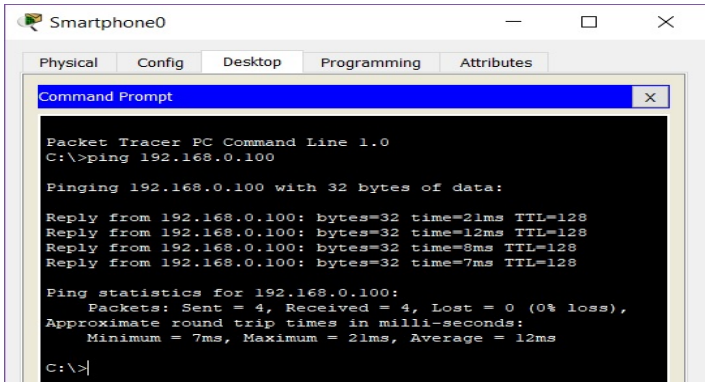
| Device | IP Address | Device | IP Address |
|---|---|---|---|
| Server | 192.168.0.100 | Tablet | 192.168.0.3 |
| PC | 192.168.0.1 | Printer | 192.168.0.4 |
| Laptop | 192.168.0.2 | Smart Phone | 192.168.0.5 |

## 3. Simu

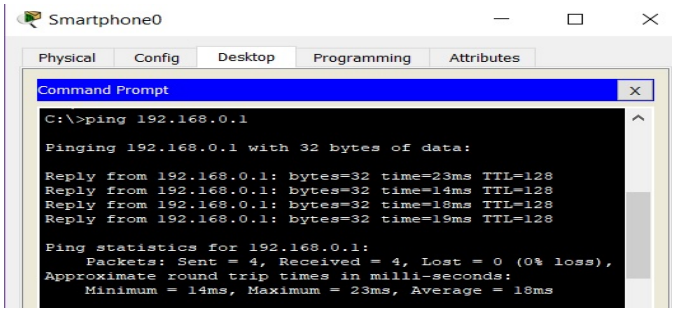
In simulation mode, the Cisco packet tracer simulates the network devices with its environment, so protocols in Packet Tracer are coded to work and behave in the same way as they would on real hardware. The protocols that supported by Packet Tracer can be seen in [5]. After designing the simple wireless LAN and assigning an IP address to each end device, the operation of the LAN will be tested using Cisco Packet Tracer network simulator. This test includes network connectivity tests and analyzing broadcasts in simulation mode using a simple protocol data unit (PDU).

### 3.1.Network connectivity test

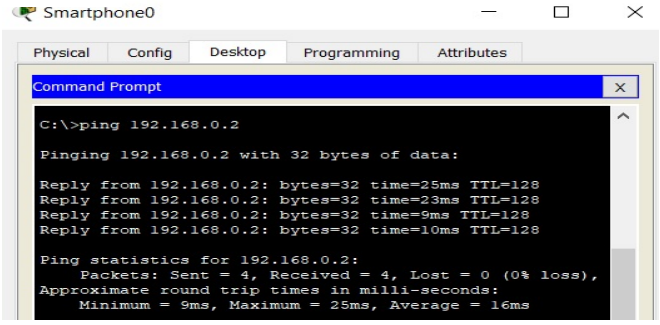
Network connectivity or LAN interconnection can be tested using a ping command (ping is useful to determine if another machine is accessible), followed by the the IP address of the end-device which required to test connectivity to. Fig.5 shows the result of performing a ping to the smart phone device to test the reachability of this device on IP network, and to measure the round-trip time for messages sent from it to destination devices that are echoed back to the source.




(a) Smart Phone to Server




(b) Smart Phone to PC




(c) Smart Phone to Laptop

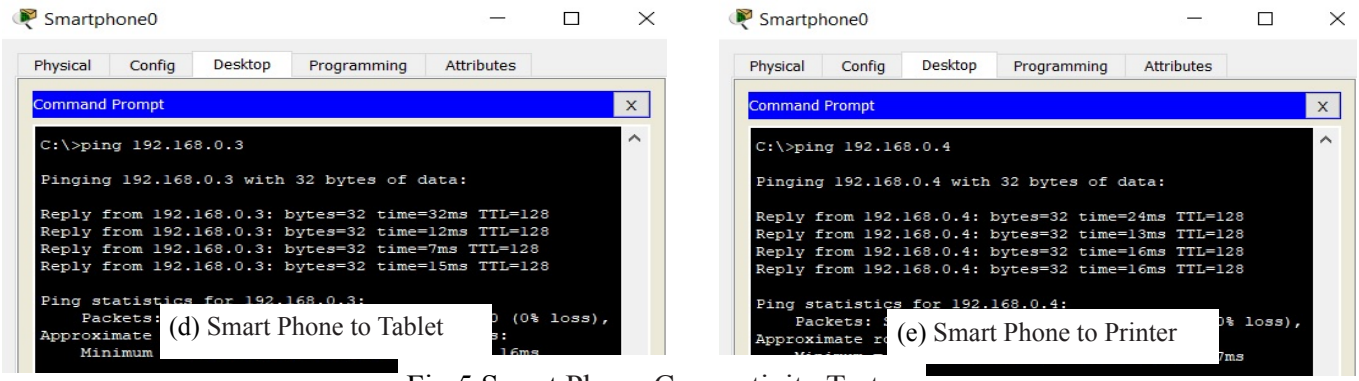



Fig.5 Smart Phone Connectivity Test

From Fig.5, it is observed that all IP address in the wireless network are valid.

## 3.2. Visualizing ICMP packet flow

To visualize packet flow, a simple PDU will be used in the simulation. The simulation will keep track every frame or event in the network. As a result, one can see packets flowing from one node to another and can also click on a packet to see detailed information categorized by OSI layers. An Internet Control Message Protocol (ICMP) packet will be selected to be visible in a packet flow process as shown in Fig.6. ICMP is an error-reporting protocol and when broadcasting in the network it used to generate error messages to the source IP address when network problems prevent delivery of IP packets (reporting errors is not used here in simulation, but rather the Echo request/response messages).

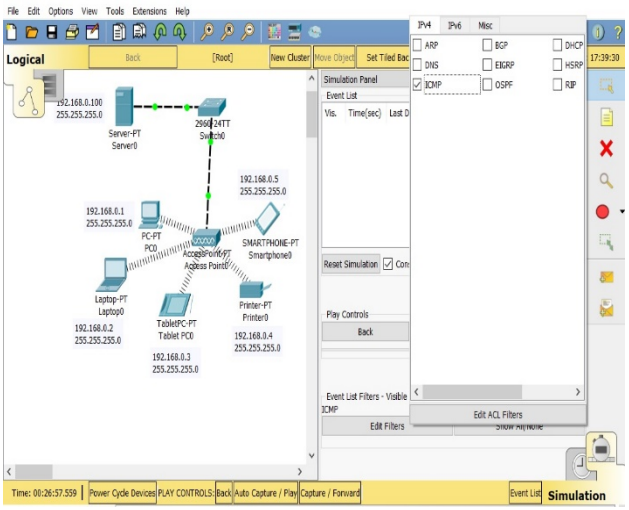



Fig.6 Selecting ICMP event

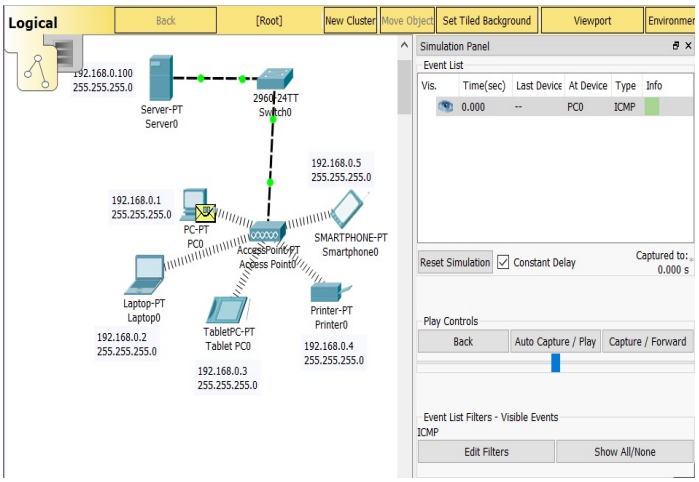



Fig.7 Sending PDU from PC to Laptop

The simple PDU message will be sent from PC device to Laptop device. Fig.7 illustrates the first step of sending and receiving process while Fig.8 shows the PDU details. In PDU (layer 3) there is a source IP address (PC: 192.168.0.1) and destination IP address (Laptop: 192.168.0.2).

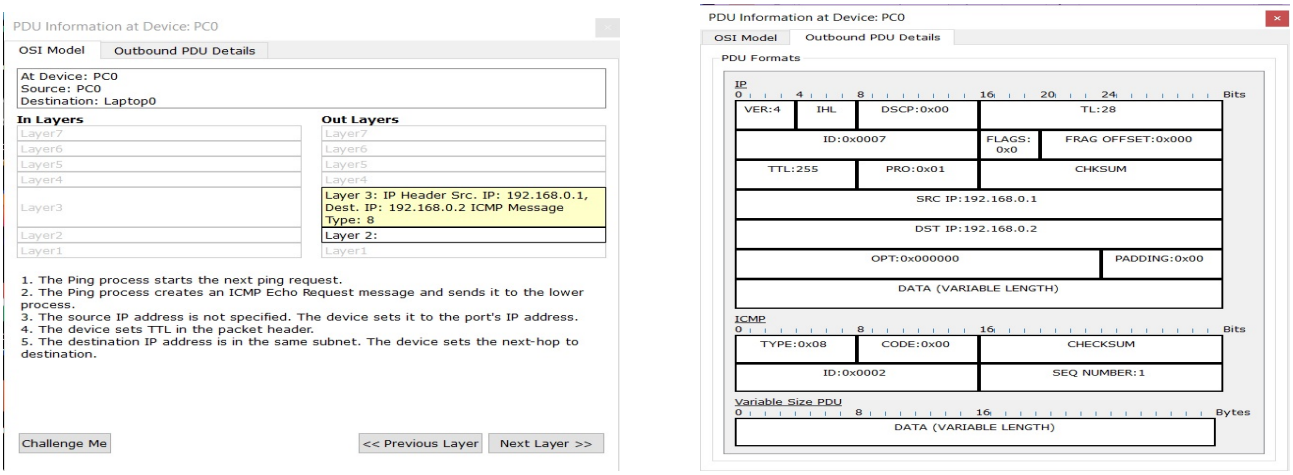



Fig.8 PDU details

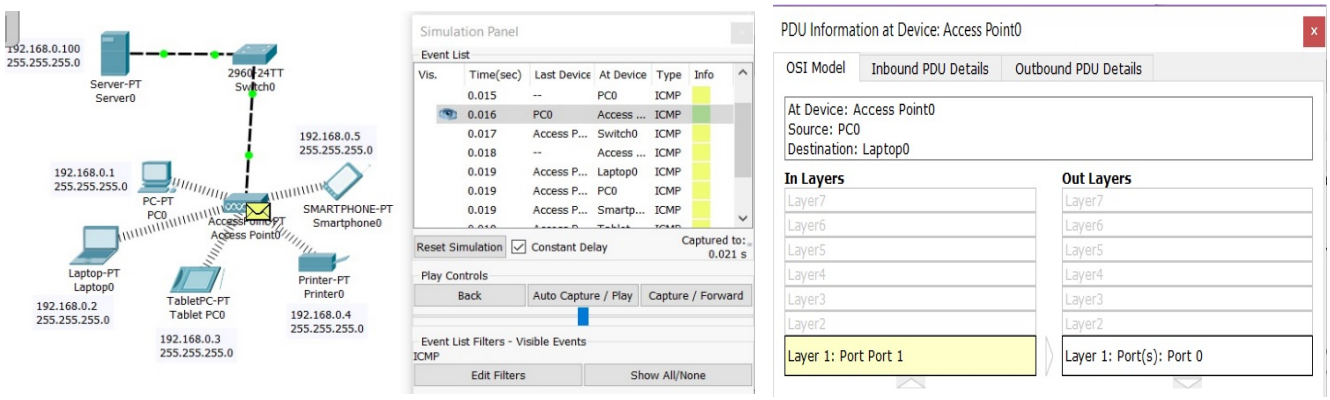
Fig.9 shows all steps of this process for sending an ICMP echo request message from the PC to the Laptop. In (Fig.9.a) PDU has been sending to AP. At AP, the wireless port (layer-1) receives the frame while Ethernet port (layer-1) sends out the frame to the switch (Fig.9.b). In Switch device, Ethernet port (layer-1) receives the frame and the frame source of media access control (MAC) address was found in the MAC table of Switch (layer-2). In fact, this is a unicast frame. Switch looks in its MAC table for the destination MAC address. After that the Switch drops the frame because outgoing port and incoming port are the same. AP then will broadcast PDU to all devices in the network (Fig.9.c). Only Laptop will receive the message while other devices will drop the frame. As an example, at Printer device the wireless port (layer-1) receives the frame but in layer-2 the frame's destination MAC address does not match the receiving port's MAC address, the broadcast address, or any multicast address. So, the Printer device drops this frame. In Fig.9.d, the process of sending/receiving PDU information at Laptop device will be:

- In Layers (Laptop device):
    1) In layer-1, the wireless port receives the frame.
    2) In layer-2, the frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address. The device encapsulates the PDU from the Ethernet frame.
    3) In layer-3, the packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet. Since this packet is an ICMP packet, The ICMP processes it. Finally, ICMP process received an Echo Request message.
- Out Layers (Laptop device):

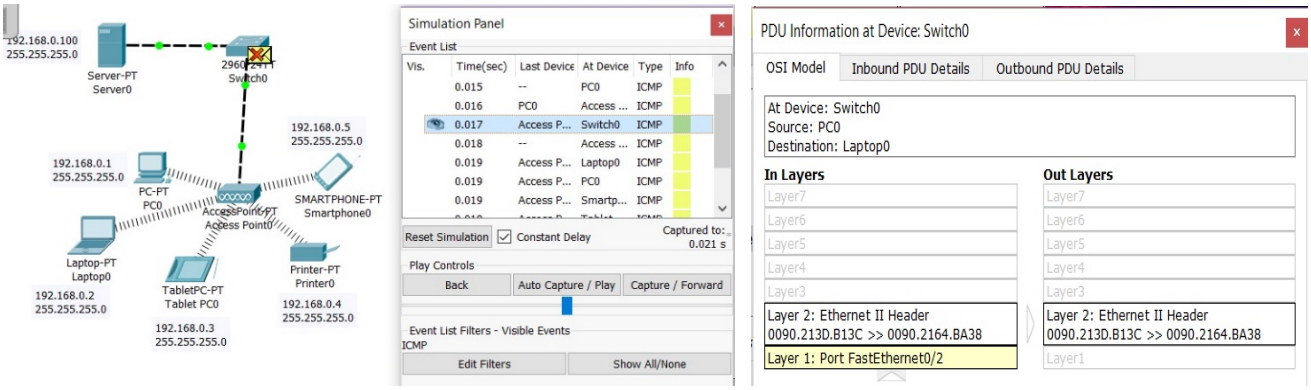
1) In layer-1, the wireless port is sending another frame at this time. The device buffers the frame to be sent later.

2) In layer-2, the next-hop IP address is a unicast. The address resolution protocol (ARP) process looks it up in the ARP table. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table. The device encapsulates the PDU into an Ethernet frame.

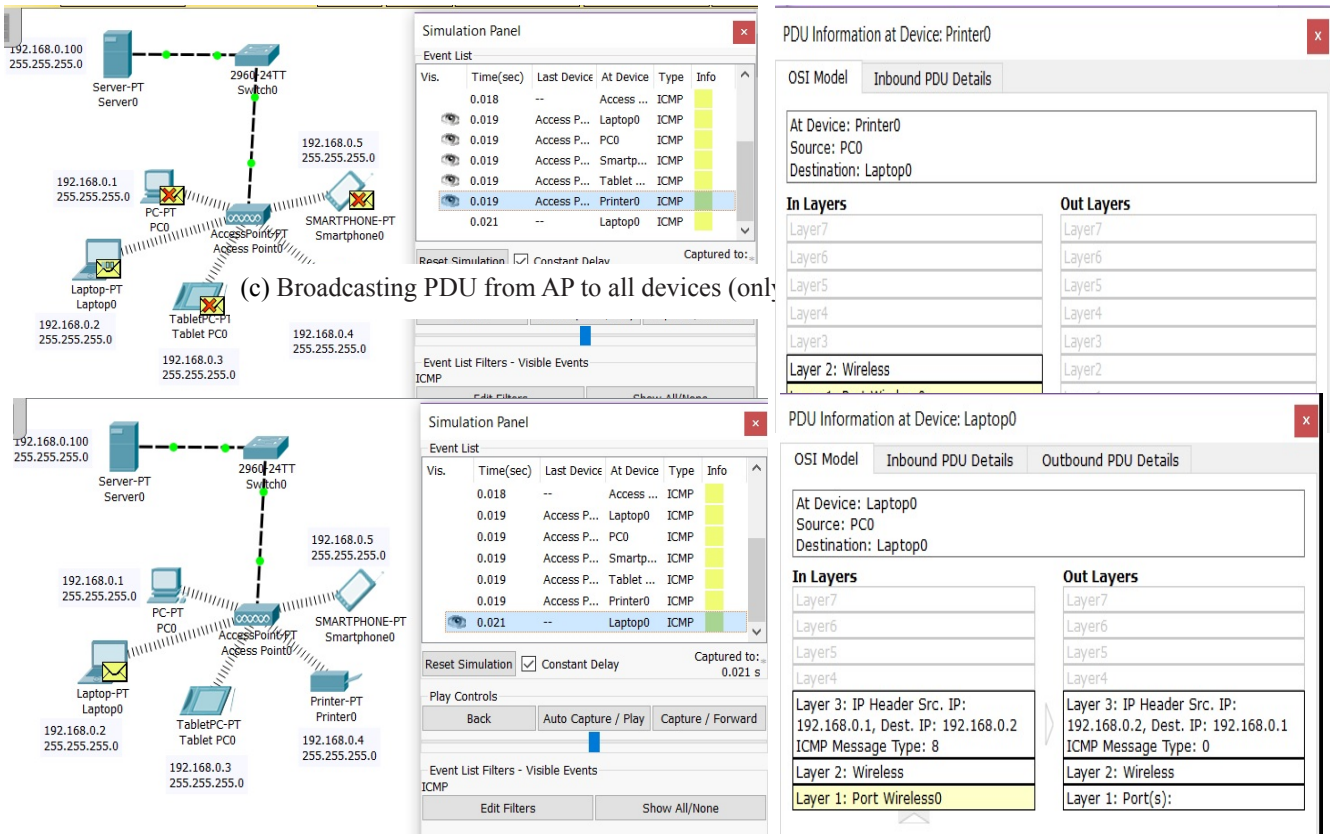
3) In layer-3, the ICMP process replies to the Echo Request by setting ICMP type to Echo Reply. The ICMP process sends an Echo Reply. Finally, the destination IP address is in the same subnet. The device sets the next-hop to destination.




(a) Broadcasting PDU from PC to AP




(b) Broadcasting PDU from AP to the switch




(c) Broadcasting PDU from AP to all devices (only

(d) Broadcasting PDU from AP to Laptop

Fig.9 Process of broadcasting PDU from Pc (source) to Laptop (destination)

## 3.3.Visualizing of HTTP traffic

To simulate HTTP traffic, a web browser will be selected for PC device to show the server page shown in Fig.10. The HTTP service in packet tracer offers a web server that supports both HTTP and HTTPS protocols (Fig.12). This service provides options to create and edit static HTML pages and display these pages when this server is accessed through the web browser utility of other end devices. To show how the data is exchanged in the network, the transmission control protocol (TCP) will be tracked in the simulation and PDU traffic generated as shown in Fig.12. The traffic generator is used to create customized packets and send them at periodic intervals and it is useful for simulating a real environment. The destination IP address is selected as the server's address, while the source IP is selected as PC address. Fig.13 shows the processing of HTTP traffic (http://192.168.0.100) between the server and PC device which indicates that the data exchanged between server and host (PC device) is working properly.


Fig.10 Server Page

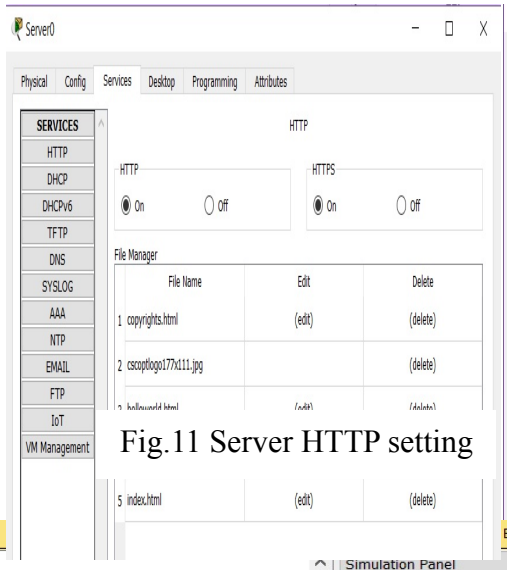



Fig.11 Server HTTP setting

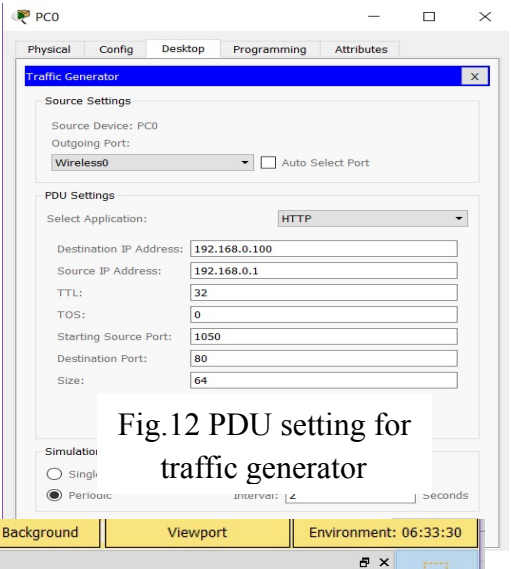



Fig.12 PDU setting for traffic generator

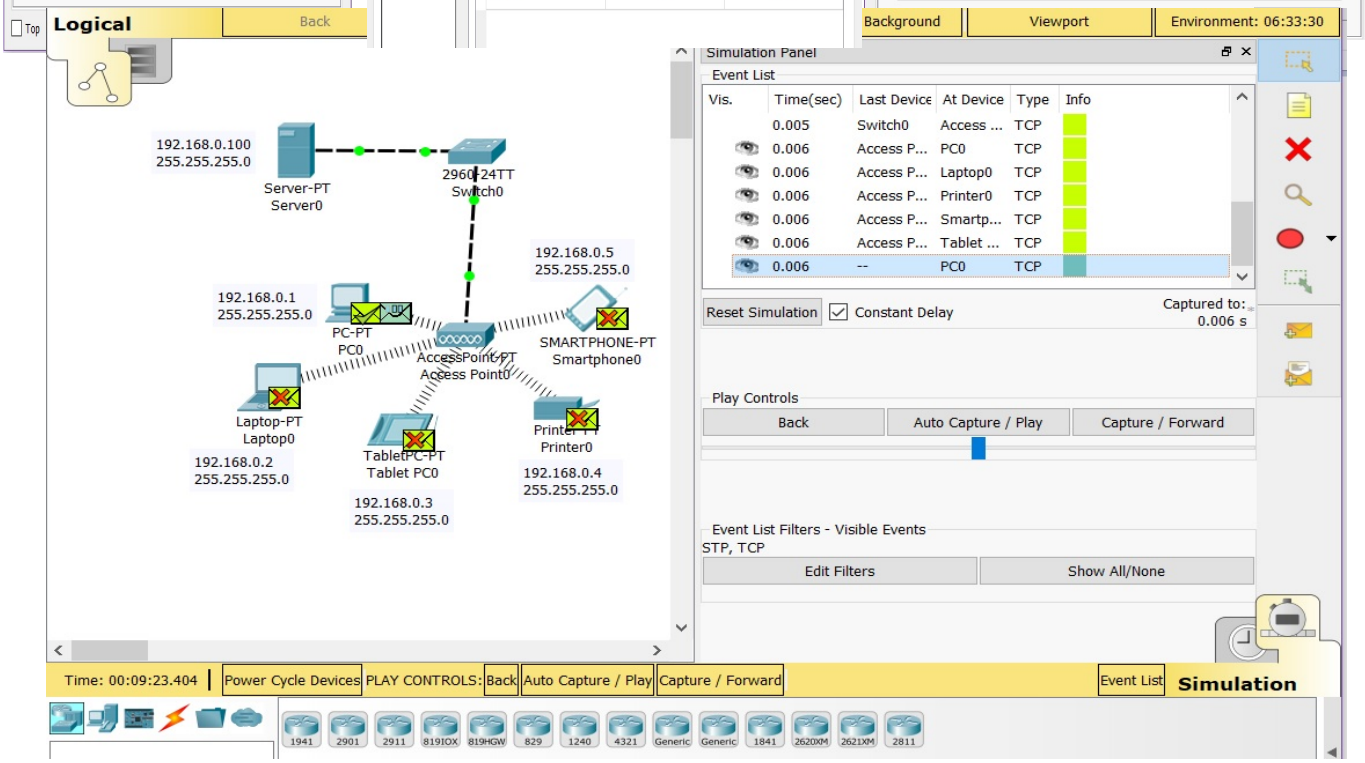



Fig.13 Exchange of HTTP traffic between the Server and PC

Fig.14 shows the PDU information (for PC device) in the last step in the exchange of HTTP traffic with inbound and outbound PDU details.

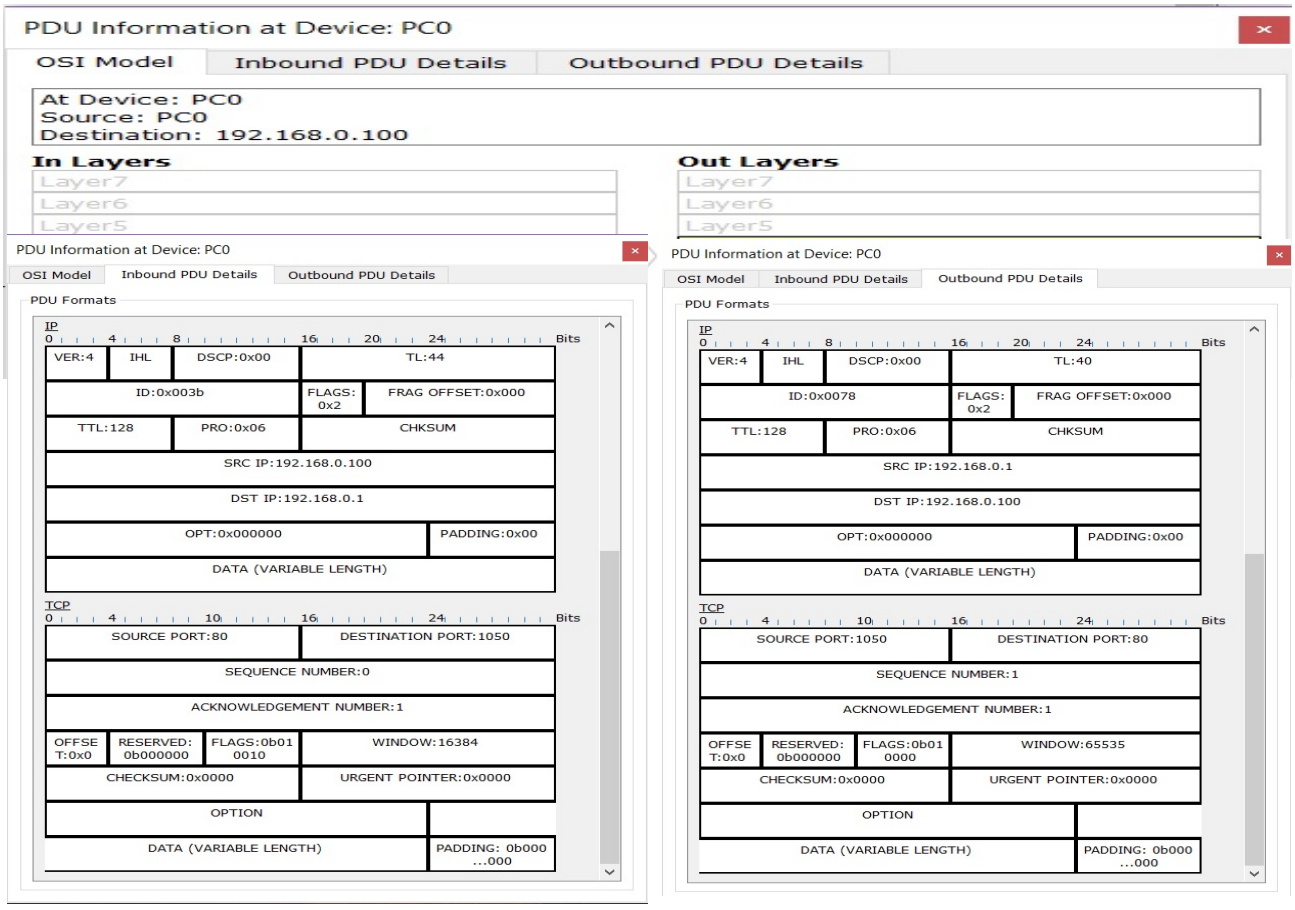



Fig.14 PDU information in PC device

To analyze the HTTP traffic (TCP packet flow), the process of sending/receiving PDU information at PC device can be described as following:

- In Layers (PC device):
    1) In layer-1, the wireless port receives the frame.
    2) In layer-2, the frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address. The device decapsulates the PDU from the Ethernet frame.
    3) In layer-3, the packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet.
    4) In layer-4, The device receives a TCP SYN+ACK segment on the connection to 192.168.0.100 on port 80. Received segment information: the sequence number 0, the ACK number 1, and the data length 24. The TCP segment has the expected peer sequence number. The TCP connection is successful. TCP retrieves the MSS value of 536 bytes from the Maximum Segment Size Option in the TCP header. The device sets the connection state to ESTABLISHED.
- Out Layers (PC device):
    1) In layer-1, the wireless port is sending another frame at this time. The device buffers the frame to be sent later.

2) In layer-2, the next-hop IP address is a unicast. The ARP process looks it up in the ARP table. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table. The device encapsulates the PDU into an Ethernet frame.
3) In layer-3, The destination IP address is in the same subnet. The device sets the next-hop to destination.
**4)** In layer-4, The device sends a TCP ACK segment. Sent segment information: the sequence number 1, the ACK number 1, and the data length 20.

## 4. Conclusion

In this report, a simple wireless network that contains several wireless devices has been implemented using Cisco packet tracer simulator. Packet Tracer provides wireless modules for PCs/laptops and for routers to enable wireless connectivity. This simulation tool offered a way to predict the impact on the network when upgrading the hardware, using another network topology, or changing in the traffic load. It provides a wide range of Cisco switches and routers running on IOS, wireless devices, and several end devices such as PCs and servers with a command line. It also provides physical simulation as well as an assessment tool. The assessment tool can be used to create practical networking questions with a complex scoring model. The physical workspace provided can be used to determine the range of wireless devices. Various tests were performed to simulate the working of a simple wireless network. These tests included network connectivity (ping test), tracking of ICMP flow, and visualizing HTTP traffic (TCP packet flow). All tests have been done by sending a simple PDU from one device to another device in the wireless network.

## References

[1] Peter L. Dordal, “An Introduction to Computer Networks”, Release 1.9.1, Department of Computer Science, Loyola University Chicago, February 19, 2018.
[2] A. S. Tanenbaum, D. J. Wetherall, “Computer Networks”, 5th Ed., Pearson Education Inc., ISBN-13: 978-0-13-212695-3, 2011.
[3] Douglas E. Comer, “Computer Networks and Internets”, Prentice Hall, ISBN 13: 978-0-13-606127-4, 2009
[4] Garima Jain, N. Noorani, N. Kiran, and S. Sharma, “Designing & Simulation of Topology Network using Packet Tracer”, International Research Journal of Engineering and Technology, Vol.2, Issue.2, 2015.
[5] Jesin A., "Packet Tracer Network Simulator", Packt Publishing, ISBN 978-1-78217-042-6, 2014.
[6] “Packet Tracer User Documentation”, https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer