Computer Networks

Digital Assignment

Simulation of Wireless Network using Packet Tracer Tool

Abstract

In the present era, the internet offers a wide range of services, including email, instant messaging, online learning, telemedicine, internet banking, and multiplayer online gaming. Computer networks play a crucial role in facilitating communication and information exchange among multiple interconnected devices. This report aims to create and simulate a basic wireless network using a network simulator tool called Cisco Packet Tracer. The focus will be on understanding various concepts related to packet movement between different devices, such as connectivity visualization through ICMP and TCP packet flow, as well as analyzing broadcast communication.

Contents

1. Introduction

- The Local Area Network (LAN) serves as a fundamental computer network that enables connectivity with wide area networks. It allows for the sharing of data processing equipment such as storage devices and printers. Apart from granting access to the internet, LANs play a crucial role in facilitating resource sharing within organizations. Initially, computer networking emerged from the necessity to share information within an organization, including messages, files, and databases. Wireless communication encompasses various technologies utilized over different distances. Unlike wired networking dominated by Ethernet, wireless networking incorporates multiple technologies, many of which possess similar characteristics.

- A LAN comprises physical links, common interfacing hardware connecting hosts to these links, and protocols that ensure their seamless collaboration. Access Control Lists (ACLs) specify which nodes or users have access to others and determine the operations allowed on specific nodes. Switches or routers may be involved in this process to facilitate connectivity.

- To achieve universal connectivity, the internet protocol (IP) provides a global addressing and routing mechanism, enabling packet delivery between any two hosts. IP addresses, particularly the most common IPv4 version, consist of 4 bytes (32 bits) and are part of the IP header, which typically follows the Ethernet header. In Ethernet (IEEE 802.3) and IEEE 802.11 networks, the Ethernet header only accompanies a packet for a single hop, while the IP header remains with the packet throughout its journey across the internet.

- The International Standards Organization (ISO) divides network communication into seven layers, with layers 1-4 referred to as the lower layers and layers 5-7 as the upper layers, focusing on application-level data. Networks operate on the principle of "pass it on," where each layer performs specific tasks and passes the data to the next layer. This model is known as the open systems interconnection (OSI) model. The OSI model comprises seven layers, including:

- Application (Layer 7): Supports application and end-user processes, handling identification, quality of service, user authentication, privacy, and data syntax. It provides services for applications such as file transfers and email.

- Presentation (Layer 6): Translates data between application and network formats, ensuring compatibility and dealing with data formatting and encryption.

- Session (Layer 5): Establishes, manages, and terminates connections between applications, coordinating conversations and exchanges.

- Transport (Layer 4): Enables transparent data transfer between hosts, ensuring error recovery and flow control.

- Network (Layer 3): Utilizes switching and routing technologies to create logical paths (virtual circuits) for transmitting data between nodes, handling addressing, internetworking, error handling, congestion control, and packet sequencing.

- Data Link (Layer 2): Encodes and decodes data packets into bits, managing transmission protocols, error handling, and frame synchronization. It consists of the Media Access Control (MAC) and Logical Link Control (LLC) sub-layers.

- Physical (Layer 1): Transmits data at the electrical and mechanical level through the network, providing the necessary hardware components.

- TCP/IP protocols align with a four-layer conceptual model known as the DARPA model, which includes the Application, Transport, Internet, and Network layers. The top three layers of the OSI model (Application, Presentation, and Session) are merged into the Application layer in TCP/IP, while the bottom two layers (Physical and Data Link) are combined into the Network Access layer.

- A wireless LAN encompasses three main components: access points (AP) or base stations, an interconnection mechanism like a switch or router to connect access points, and wireless hosts (nodes or stations). Switches operate at the Data Link layer (Layer 2), while routers operate at the Network layer (Layer 3). Two types of wireless LANs are commonly used: ad hoc networks, where wireless hosts communicate directly with each other without a base station, and infrastructure networks, where wireless hosts communicate only through access points. Infrastructure networks are preferred due to enhanced security against unwanted connections, signal strength monitoring capabilities, and improved performance compared to ad hoc networks.

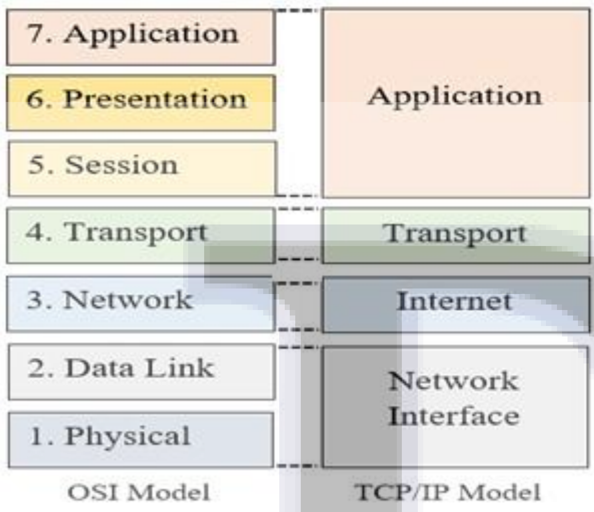


Fig.1 OSI and TCP/IP Layers

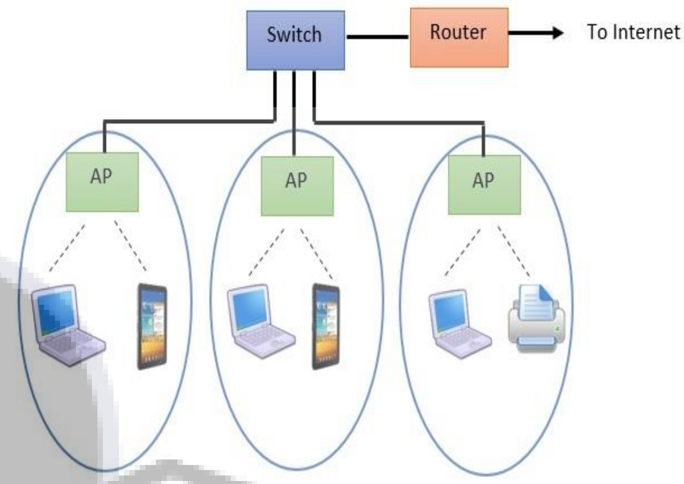


Fig.2 An infrastructure architecture for a wireless network

The primary objective of any network is to minimize the number of users and workgroups that are inaccessible. All terminals within the network should possess the capability to communicate with one another and provide the necessary information. Furthermore, the physical systems and devices involved should ensure optimal performance, reliability, and security. Consequently, system managers require expert tools to aid them in network design and maintenance. Simulation tools offer a means to predict the impact on the network when implementing hardware upgrades, altering network topologies, or adjusting traffic loads. Therefore, this report focuses on the design and simulation of a basic wireless network using Cisco Packet Tracer.

2. Simple Wireless Network

Cisco Packet Tracer is an advanced network simulation program that offers a wide range of capabilities to simulate, visualize, author, assess, and collaborate on network designs. It serves as a powerful tool in the education and training of complex technology concepts related to networking.

One of the key features of Packet Tracer is its ability to simulate highly intricate networking environments. Users can create virtual networks, consisting of routers, switches, servers, PCs, and other network devices, and configure their settings and connections. The tool provides a realistic simulation environment where users can observe how data packets traverse the network and how devices interact with one another.

By visualizing packet movements, users gain a deeper understanding of how information flows within a network. They can analyze the routing paths, observe the behavior of different protocols, and troubleshoot connectivity issues. This hands-on approach enables users to grasp the concepts of network operation and troubleshooting in a practical and interactive manner.

Packet Tracer also offers a collaborative platform, allowing multiple users to work together on a network design or troubleshooting scenario. This feature enhances teamwork and enables instructors to assess students' understanding of network concepts and their ability to solve network-related problems.

Furthermore, Packet Tracer supports the creation of complex network topologies, enabling users to design networks with multiple interconnected devices, VLANs, wireless networks, and even virtual private networks (VPNs). This versatility allows users to simulate real-world network scenarios and evaluate the impact of different network configurations and technologies.

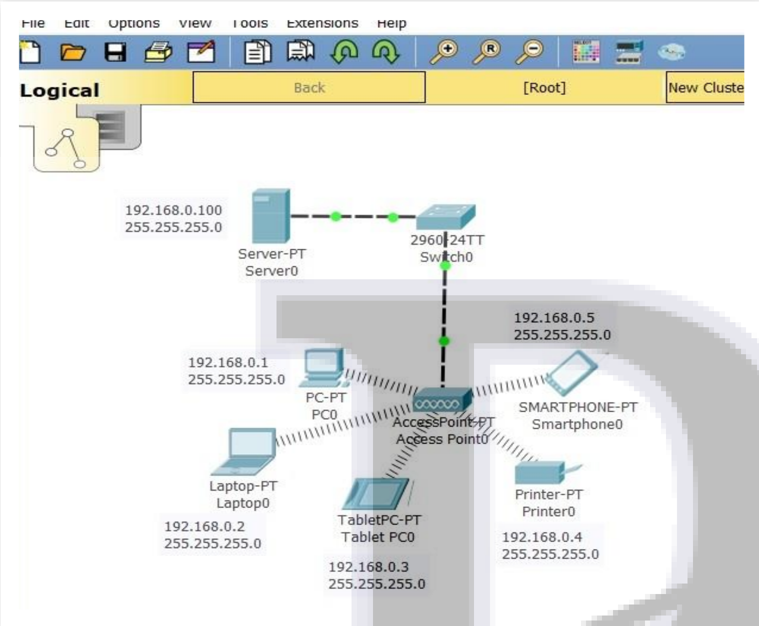


Fig.3 Simple wireless network

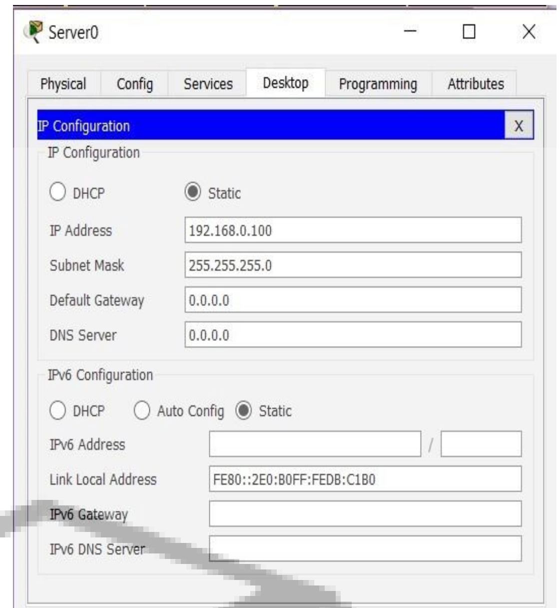


Fig.4 Server's IP address assignment

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

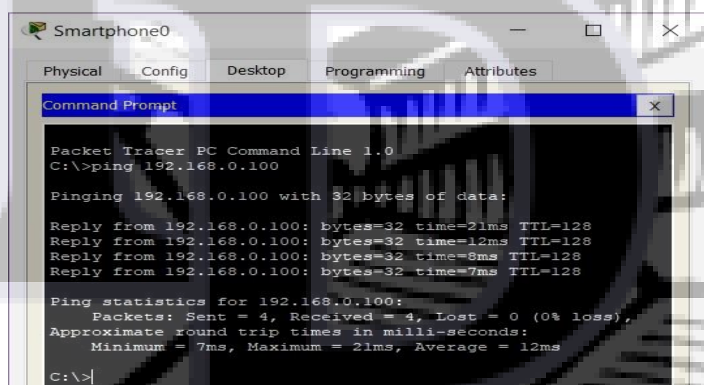
Table.1 LAN IP address assignment (Subnet mask: 255.255.255.0)

3. Simulation process

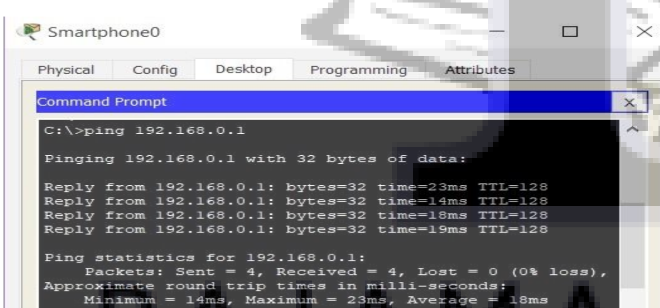
In simulation mode, the Cisco packet tracer simulates the network devices with its environment, so protocols in Packet Tracer are coded to work and behave in the same way as they would on real hardware. The protocols that supported by Packet Tracer can be seen in [5]. After designing the simple wireless 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

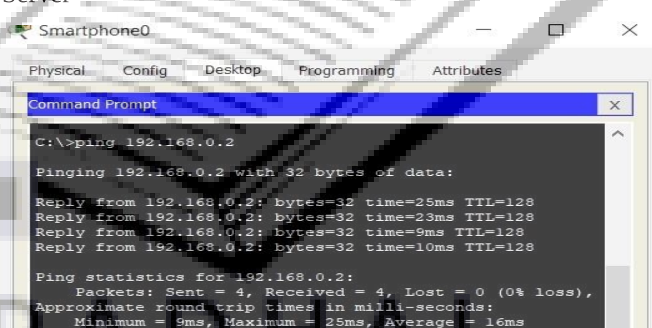
Network connectivity or LAN interconnection can be tested using a ping command (ping is useful to determine if another machine is accessible), followed by the the IP address of the end-device which required to test connectivity to. Fig.5 shows the result of performing a ping to the smart phone device 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.



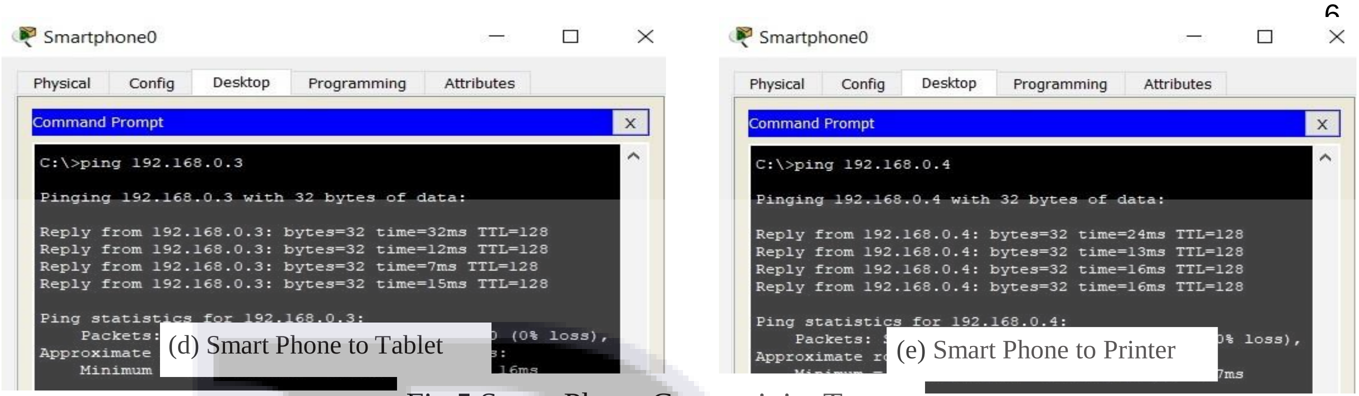
(a) Smart Phone to Server



(b) Smart Phone to PC



(c) Smart Phone to Laptop



(d) Smart Phone to Tablet (e) Smart Phone to Printer

Fig.5 Smart Phone Connectivity Test

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

3.2Visualizing 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).

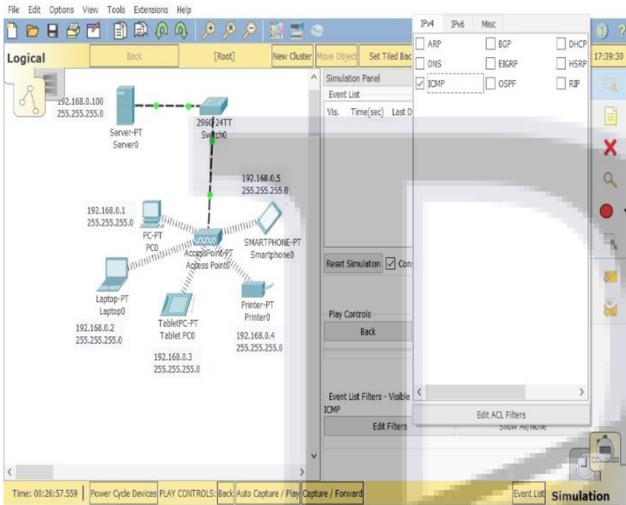


Fig.6 Selecting ICMP event

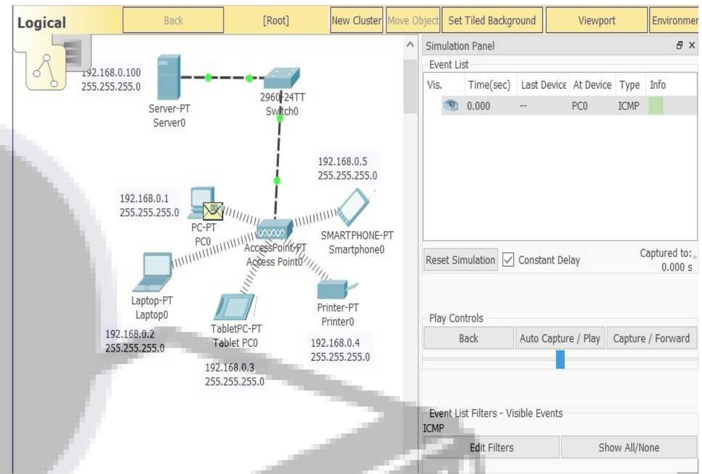


Fig.7 Sending PDU from PC to Laptop

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).

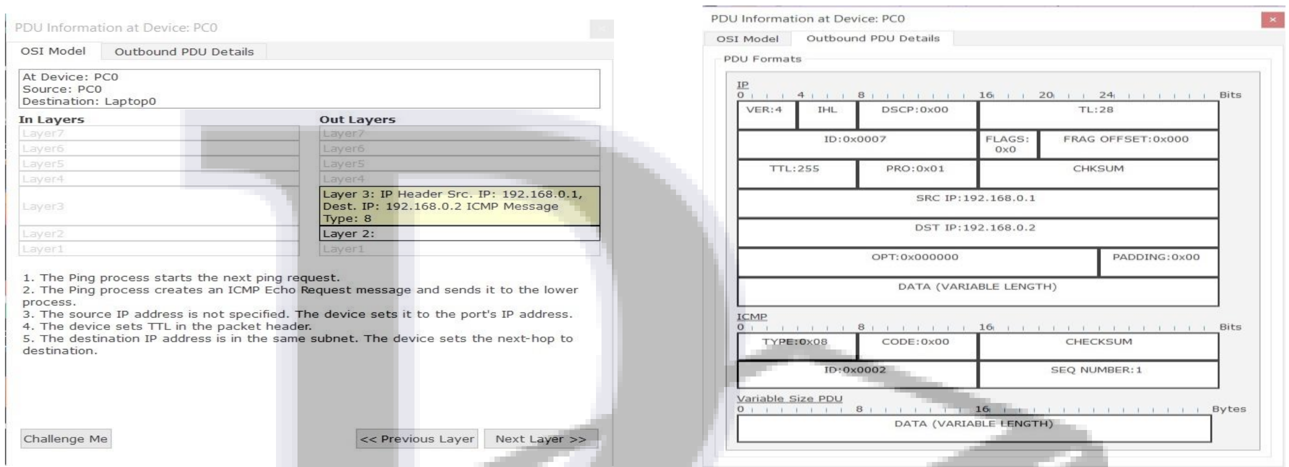


Fig.8 PDU details

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):

  3.2.1 In layer-1, the wireless port receives the frame.

  3.2.2 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.

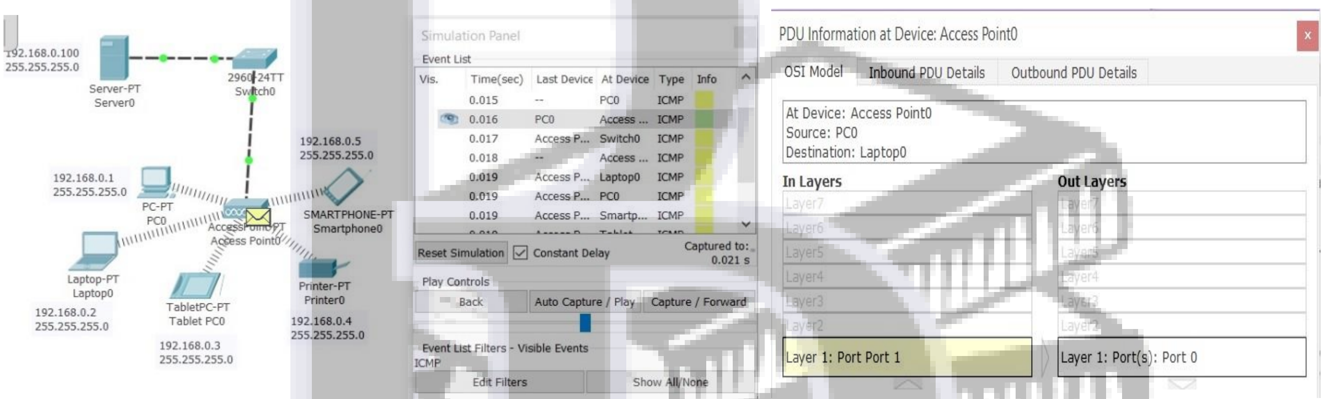
  3.2.3 In layer-3, the packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet. Since this packet is an ICMP packet, The ICMP processes it. Finally, ICMP process received an Echo Request message.

- Out Layers (Laptop device):

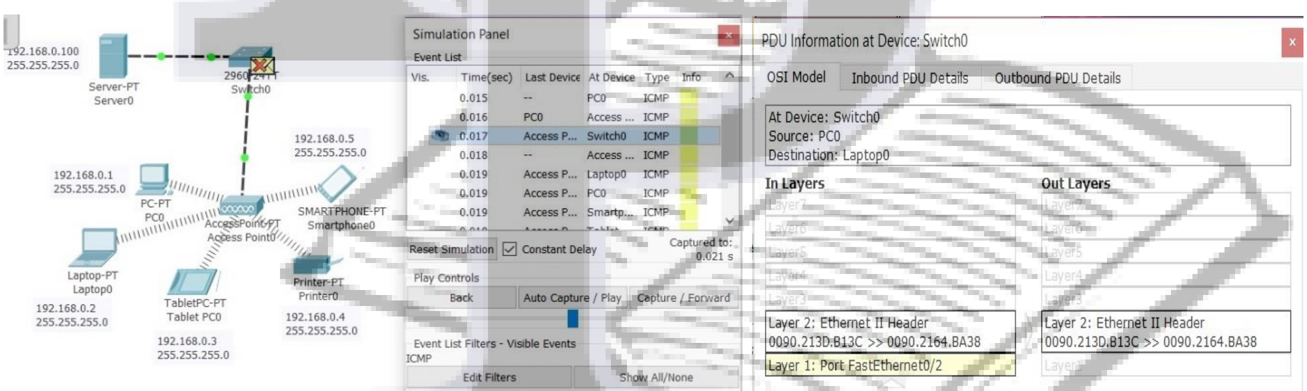
1) In layer-1, the wireless port is sending another frame at this time. The device buffers the frame to be sent later.

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.

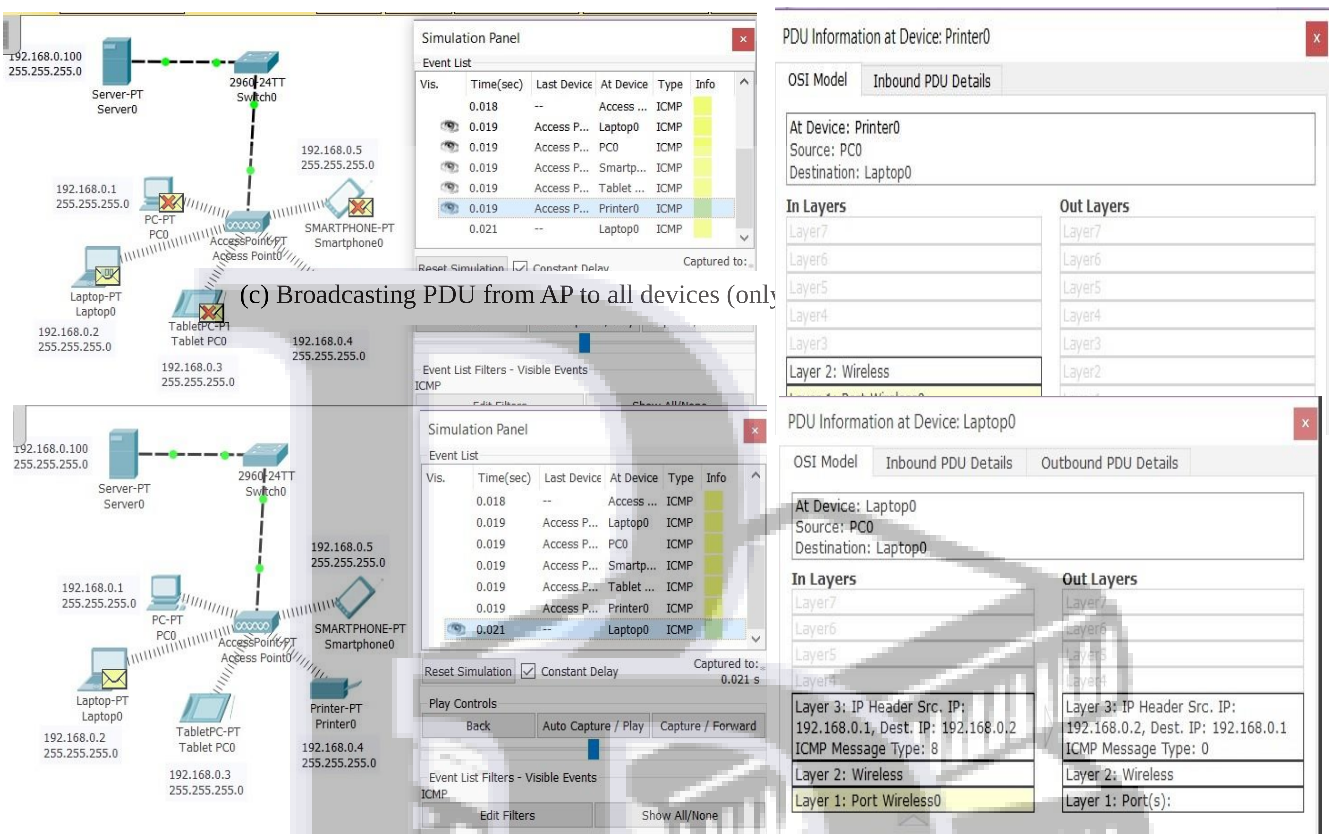
3) In layer-3, the ICMP process replies to the Echo Request by setting ICMP type to Echo Reply. The ICMP process sends an Echo Reply. Finally, the destination IP address is in the same subnet. The device sets the next-hop to destination.



(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)

3.3Visualizing 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

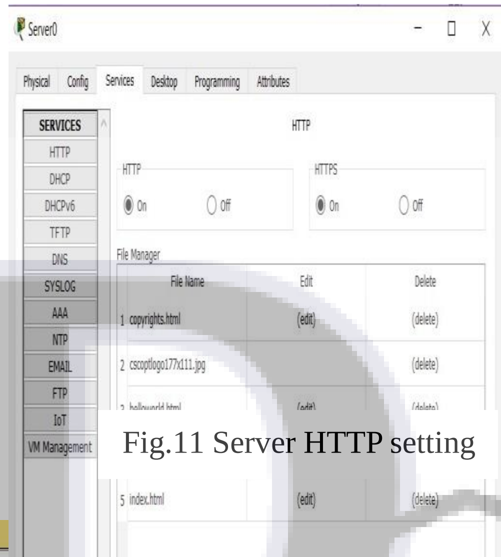


Fig.11 Server HTTP setting

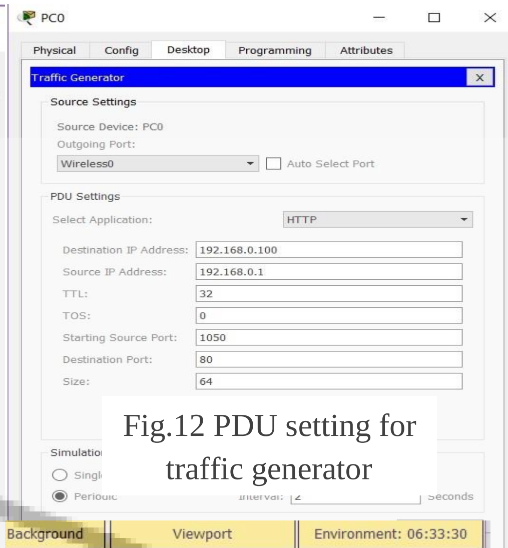


Fig.12 PDU setting for traffic generator

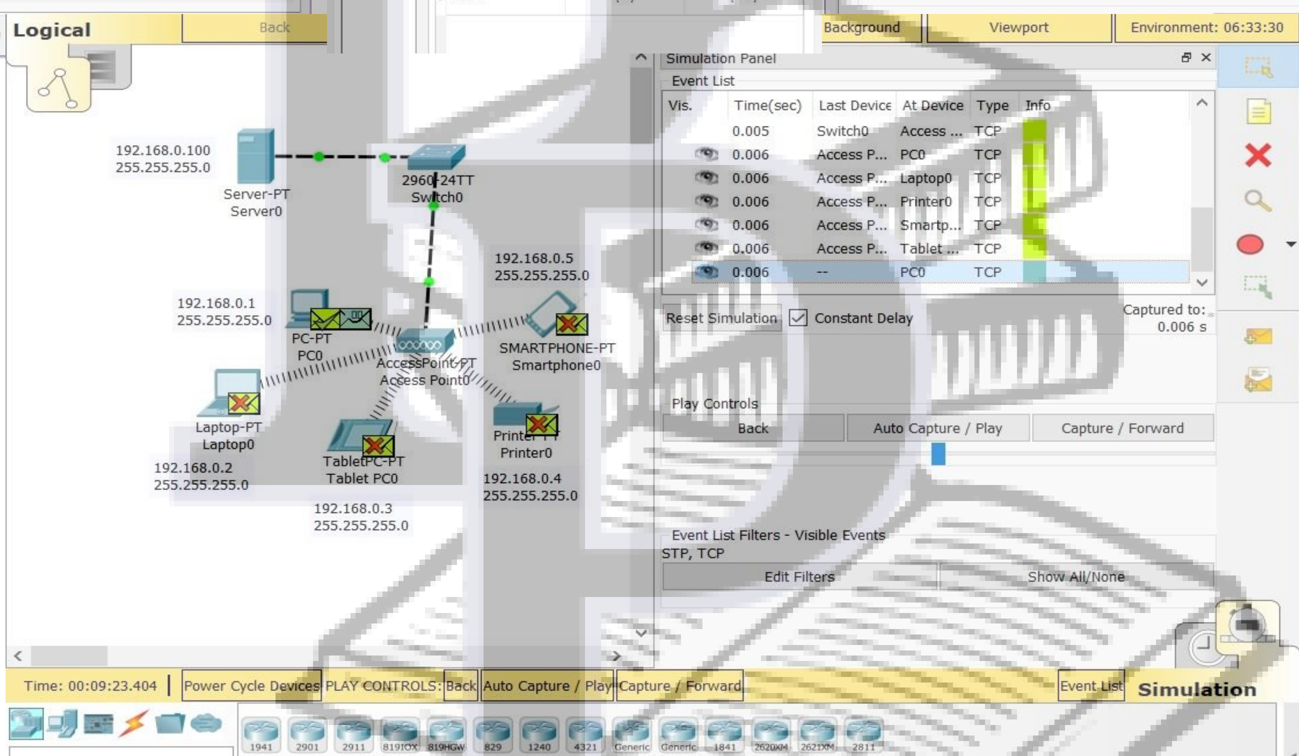


Fig.13 Exchange of HTTP traffic between the Server and PC

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.

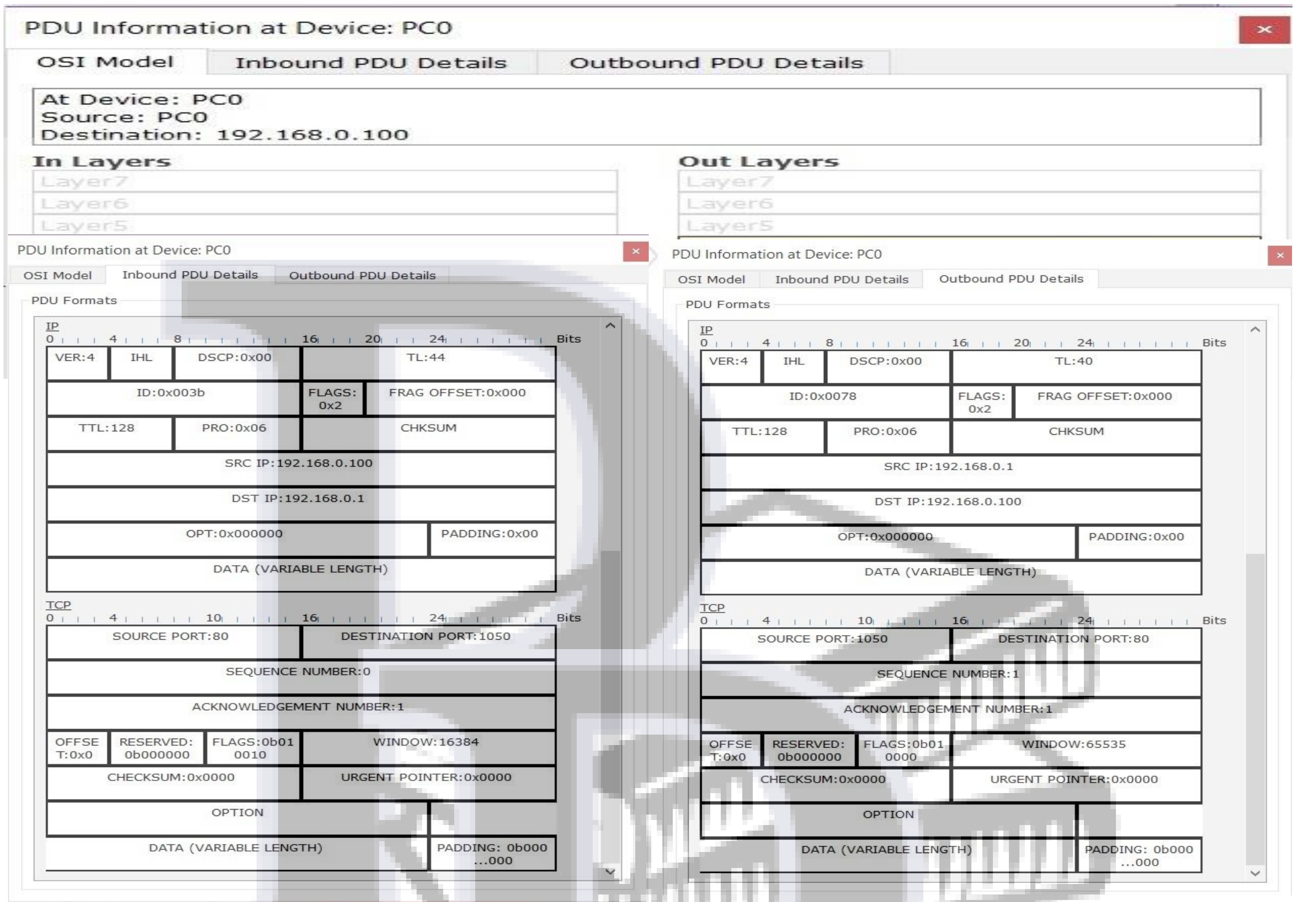


Fig.14 PDU information in PC device

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):
  - 3.3.1 In layer-1, the wireless port receives the frame.
  - 3.3.2 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.
  - 3.3.3 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.
  - 3.3.4 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