IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.86119

A Study on Networking Devices

Monica Eswar[1], Srivaths JM[2], Dr. Geetha K S[3]

Student, Department of Electronics and Communication, RV College of Engineering, Bangalore, India[1]

Student, Department of Electronics and Communication, RV College of Engineering, Bangalore, India[2]

Professor and Head of the Department, Department of Electronics and Communication, RV College of Engineering, Bangalore, India[3]

Abstract: Networking devices, in a broader sense, are the end devices that are connected to one another across a network and allow communication to flow. Hubs, switches, and access points are examples of network devices. These devices must be set up and have firmware that needs to be updated. They require adequate bandwidth and consistent connectivity, as well as, preferably, redundant connections in the case that one or more of the devices or connections fails. This study primarily focuses on the working of the most commonly used network devices in offices and sometimes in households. Cisco Packet Tracer simulations are demonstrated for the working of hubs, switches and access points.

Keywords: Hubs, switches, access points.

I. INTRODUCTION

Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network [1]. Computer networks are the backbones of most business enterprises. Therefore, a proper planning is a must for a ensuring proper interconnections of devices in a network.

The survey conducted in 1997 as shown in [2] shows theadvantages and disadvantages of communicating with computer networks as compared to traditional fax or telephones.Computer networks are classified in terms of various criteria, [3]. Some of these include the medium of transmission used to carry signals (wired of wireless), bandwidth usage, communications protocols, the number of devices in the network, the network topology, mechanism employed to control network traffic, and organizational applications. Computer networks are employed in wide range of applications and services like access to the World Wide Web, Voice overIP (VoIP), audio/video conferencing etc.

The first attempts to standardize computer networks was in 1977 when International Organization for Standardization (ISO) founded the Open Systems Interconnection model (OSI model), [4]. Analyzing raw packets or datastreams requires deeper understanding of the OSI or TCP/IP model, [5]. The seven layers described in OSI model laid the foundation for networking. The data-stream in any packet is divided into frames where each frame corresponds to a layer in the OSI model. TCP/IP model gained popularity as it combined a few layers into application layer [6]. A bottom-up approach, describing all the protocols (from physical layer upto application layer) can be seen in [7].

Through an in-depth study of TCP/IP protocol stack principles and ideas along with the actual situation of embedded devices, it can be observed in [6] that the existing TCP/IP is cut out, and by using the layered, modular design the specific implementation of the embedded TCP/IP protocol stack is described in detail. As networks progressed from wired networks to wireless networks, more focus was on the WLAN networks which became a standard which is popularly known as IEEE 802.11. [8] studies IEEE 802.11 wireless LANs in the rate adaptation scheme. Various networking devices that are used for communication between hardware on a computer network are discussed.

II. HUBS

Hubs are devices that connect many computer networking devices. A hub also serves as a repeater, amplifying signals that have deteriorated due to vast distances travelled through connected cables. A hub connects various LAN components with identical protocols hence it is considered as the simplest networking device. Figure 1 shows the packets received by the hub.

A hub can be configured to support both digital and analog data inputs. The hubs passes the inputs as a packet if the incoming data is in digital format. If the incoming data is in analog format then the data is converted to signal form and then transmitted.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.86119

The packets are not filtered by the hubs and the addressing functions also are not differentiated. Figure 2 shows the packets that are sent through all ports. They directly send data to all connected devices irrespective of the requirements. The hubs are of two types simple and multiple hubs which operate on physical layer of OSI model.

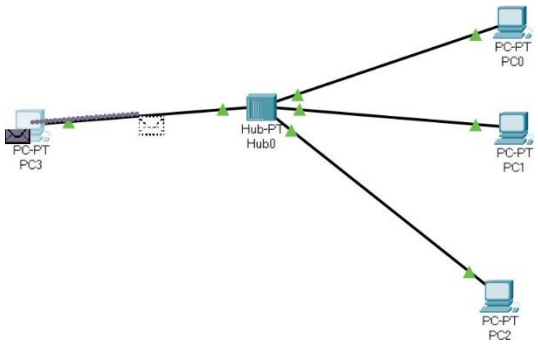

Fig. 1. Packet received by hub

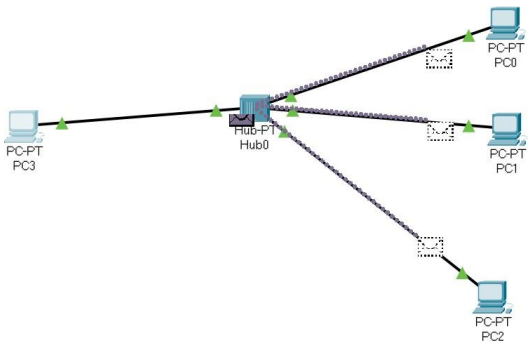

Fig. 2. Packets sent through all port

III. SWITCHES

Switches play a more intelligent role than hubs in most cases. A switch is a device having multi-port that increases the efficiency of a network. Figure 3 shows the packets being sent to the switch. The routing information about internal network nodes are limited by the switch and facilitates connections to systems such as hubs and routers. Switches are commonly used to link LAN strands. In most cases, switches can read the hardware addresses of incoming packets and forward them to the correct destination. Figure 4 shows that the packets are being sent to only to matching devices.

Switches have the ability to create virtual circuits, they are more efficient than hubs or routers in terms of network efficiency. Switches also increase network security by making it more difficult to investigate virtual circuits with network monitors. A switch can be thought of as a device that combines the greatest features of routers and hubs. In the OSI model, a switch can operate at either the Data Link layer or the Network layer. A multilayer switch is one that can work on both layers, meaning it may be used as a switch and a router. A multilayer switch is a high-capacity device that uses the same routing protocols as routers.

Switches are vulnerable to Distributed Denial of Service (DDoS) assaults, and flood guards are used to keep malicious traffic from shutting down the switch. Switch port security is critical, thus make sure you secure the following switches: Use DHCP snooping, ARP inspection, and MAC address filtering to disable all unneeded ports.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.86119

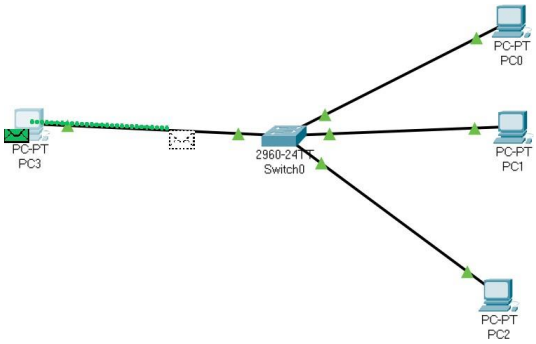

Fig. 3. Packet sent to the switch

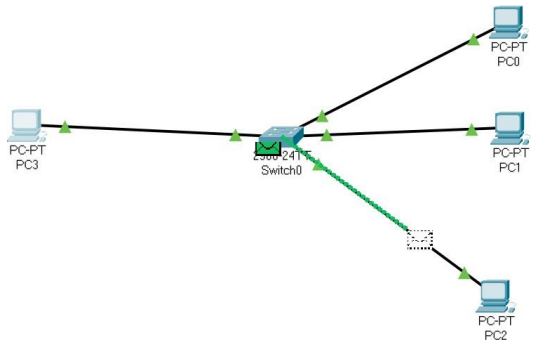

Fig. 4. Packet sent only to the matching device

IV. ACCESS POINTS

An Access Point (AP) can be a wired or wireless device, it is most usually used to refer to a wireless device. The Data Link layer of the OSI model is where the access point operates. It acts as a bridge that links a wired network to a wireless device. It also supports routers in transmitting data from one point to another in a network. Figure 5 shows the packets that are sent to AP.

A Wireless LAN (WLAN) is formed by combining a transmitter and a receiver by the Wireless Access Points(WAPs).A dedicated network devices with a built-in antenna, transmitter, and adaptor are known as access points. To provide a connection point between WLANs, APs use the wireless infrastructure network mode. They also contain many ports, allowing users to expand the network to accommodate more clients. Figure 6 shows that the packets are being broadcasted through the wireless network. One or more APs may be required to give full coverage, depending on the size of the network. Additional access points are used to provide access to more wireless clients and to extend the wireless network's range.

An APs transmission range is the distance a client can be from the AP such that they are still receiving an acceptable signal. The data processing speed is also regulated by each AP's transmission range. Figure 7 shows that the desired device responds accordingly. The actual distance between the client and the AP is determined by the wireless standard, impediments, and ambient circumstances. High-powered antennas on higher end APs allow them to extend the range of the wireless transmission.

Many ports may be available on APs, which can be utilised to expand the network's capacity, firewall capabilities, and Dynamic Host Configuration Protocol (DHCP) service. As a result, we have access points that operate as a switch, DHCP server, router, and firewall.

A Service Set Identifier (SSID) name is required to connect to a wireless AP. The SSID is used by 802.11 wireless networks to identify all systems that belong to the same network, and client stations must be set with the SSID in order to connect to the AP. The AP may broadcast the SSID, making it visible to any wireless clients in the region.

APs can be configured not to broadcast the SSID for security concerns, which implies that an administrator must provide the SSID to client computers rather than letting it to be detected automatically. SSIDs, security settings, channels, passwords, and usernames are all established by default on wireless devices. Because many internet sites display the default settings used by manufacturers, it is strongly recommended that you change these default settings as soon as possible for security reasons. There are two types of access points: fat and thin.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.86119

Fat APs, which are still often referred to as autonomous APs, must be manually setup with network and security settings before being left to serve clients until they can no longer function. Thin APs can be configured remotely using a controller. Thin clients can be readily adjusted and monitored because they do not require manual configuration. Controller-based or stand-alone access points are both possible.

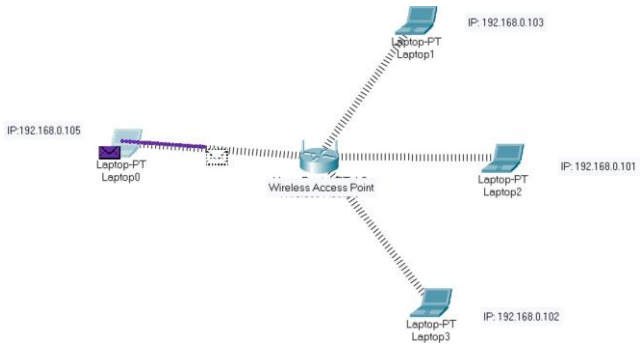

Fig. 5. Packet sent to AP

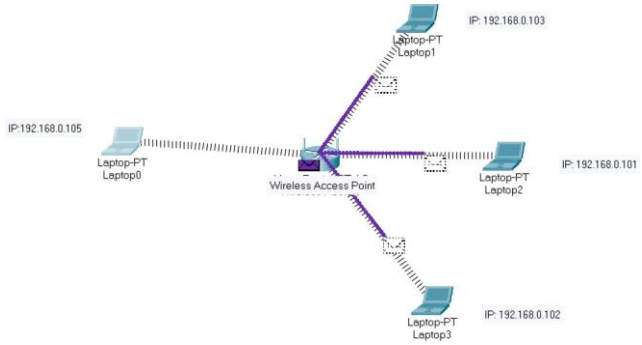

Fig. 6. Broadcast through wireless channel

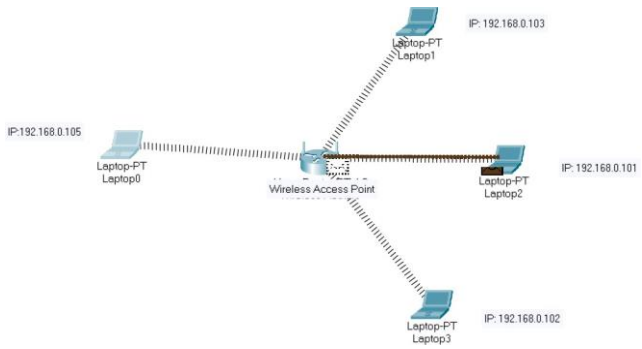

Fig. 7. Desired device responds

V. CONCLUSION

Computer communication has laid the foundation for a completely new . Having a strong understanding of the types of network devices accessible will assist users in designing and constructing a secure network. Every organization has a dedicated IT department where good knowledge on networking is crucial. Whenever network issues arise, experience with network devices comes in handy. This study primarily focuses on the working of the most commonly used network devices in offices and sometimes in households.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.86119

Hubs are the basic devices operating on the physical layer of the OSI model. Hubs consists of physical ports, generally ethernet ports, where the information sent on one port is blindly repeat the packets onto all the other ports. Hubs are cheap devices, but they waste a lot of bandwidth as devices are often forced to wait for the undesired packets to be streamed inorder to avoid collision, [9].
Switches solves the issues posed by hubs by associating the mac address of a device with the ethernet port it is connected to. Switches operate on the datalink layer and cannot read layer 3 data such as IP address.

Access Points are network layer devices which provides both wired and wireless connectivity among devices in a network. As demonstrated by Cisco Packet Tracer simulations, APs broadcast the packets in wireless channels. Common channel bands used by APs are 2.4 GHz and 5 GHz. Selection of suitable APs depending on the applications and bandwidth requirements is discussed in [10] and [11].

REFERENCES

[1] Wikipedia contributors, 2021. Networking hardware Wikipedia, the free encyclopedia. [Online; accessed 15-June-2021].

[2] Chou, C., 1997. “Computer networks in communication survey research”. IEEE Transactions on Professional Communication, 40(3), pp. 197–208.

[3] Wikipedia contributors, 2021. Computer network — Wikipedia, the free encyclopedia. [Online; accessed 15-June-2021].

[4] Balasubramaniam, D., 2015. “Computer networking: A survey”. International Journal of Trend in Research and Development,, 2, 09.

[5] Li, Y., Li, D., Cui, W., and Zhang, R., 2011. “Research based on osi model”. In 2011 IEEE 3rd International Conference on Communication Software and Networks, pp. 554–557.

[6] RiLi, H., 2011. “Research and application of tcp/ip protocol in embedded system”. In 2011 IEEE 3rd International Conference on Communication Software and Networks, pp. 584–587.

[7] Stevens, W. R., and Fall, K., 2009. TCP/IP Illustrated: The Protocols v. 1, 2nd ed. Addison-Wesley Publishing Company, USA.

[8] Li, Y., and Fu, Y., 2012. “Research and improvement on ieee 802.11 wlan mac protocol”. In 2012 Fourth International Conference on Computational and Information Sciences, pp. 827–829.

[9] Cocco, G., Ibars, C., Gu¨ndu¨z, D., and Herrero, O., 2011. “Collision resolution in multiple access networks with physical-layer network coding and distributed fountain coding”. pp. 3120 – 3123.

[10] Glisic, S., 2016. Access Point Selection. 05, pp. 446– 477.

[11] Vasudevan, S., Papagiannaki, K., Diot, C., Kurose, J., and Towsley, D., 2005. “Facilitating access point selection in ieee 802.11 wireless networks”. pp. 293–298.

[12] Judd, G., and Steenkiste, P., 2002. “Fixing 802.11 access point selection”. Computer Communication Review, 32, 07, p. 31.