Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 6): pp. 4772-4777
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.06.464

Critical Analysis On Computer Networks

K. Abdul Rasak , Joseph Deril K.S

ABSTRACT:

A computer network is a setup that joins a lot of separate computers together to share resources and information. User communication is made easier by the integration of computers and other technologies. A collection of two or more interconnected computer systems is referred to as a computer network. Cable or wireless media can be used to create a network connection. Computers and tools are connected in any network using hardware and software. A computer network is made up of different types of nodes. Nodes in a computer network can include servers, networking equipment, personal computers, and other specialised or general-purpose hosts. Network addresses and hostnames are used to identify them.

KEYWORDS : network , computers , interconnected , equipment , optics.

I COMPUTER NETWORK:

A computer network is a collection of interconnected computers that can send and receive data. Anything from smartphones to servers is considered a computing device. These gadgets can communicate wirelessly or via hardwires like fibre optics.

In the late 1960s, the U.S. Department of Défense supported the development of the first functional network, which came to be known as ARPANET. Back when computers were bulky and cumbersome to transport, government researchers would pool their resources and share what they had learned. Today's advanced networks are a far cry from those early attempts. The internet is the hub of modern society; it is a network of networks that links together countless electronic gadgets all over the globe. Networks are used by businesses of all kinds to link the personal devices of workers with the office's shared resources, such as printers.

Cities' traffic monitoring systems are examples of large-scale computer networks. These systems send out notifications to officials and first responders on traffic conditions and occurrences. Google Drive and similar collaboration tools make it easy to exchange papers with faraway co-workers. A computer network is active whenever we make a video call, watch a movie online, transfer data, use instant messaging, or just browse the web.

The study of computer networks, including their design, implementation, operation, and protection, is known as computer networking. Computer science, computer engineering, and telecommunications all come together to form this field.

II USES OF COMPUTER NETWORK:

Here are eight vital objectives associated with building and running a computer network.

- Cost Savings: Computer networks steer clear of huge expensive mainframes, preferring to employ processors at selected points. Processors are cheaper and faster, so users save time and increase efficiency.

- Error Reduction: Since all the organization's data comes from one source, there is an element of consistency and continuity, which in turn reduces the likelihood of mistakes.

- Increased Storage Capacity: In these days of big data, organizations need all the data storage they can get.

- Performance Management: The more a company grows, the heavier its data-related workload. By adding additional processors, the IT department boosts performance.

- Resource Availability and Reliability: Networks give users access to resources via multiple access points, not stored in inaccessible data silos. Also, multiple machines provide an excellent backup in case one piece of hardware fails.

- Resource Sharing: Users can now share data and services regardless of where they are. Geography is no longer an issue.

- Secured Remote Access: This objective has gained an additional level of importance thanks to the global pandemic. As a result, users can safely access their work from home.

- Streamlined Collaboration and Communication: Computer networks make it easier for staff from different departments to talk, plan, share, and collaborate.

III KEY COMPONENTS OF A COMPUTER NETWORK:

Nodes, or network devices, and connections are the fundamental building elements of every computer network. The ties join together two or more nodes. Communication protocols specify the format in which these connections transmit data. Ports are commonly used to refer to the devices at each end of a communication path.

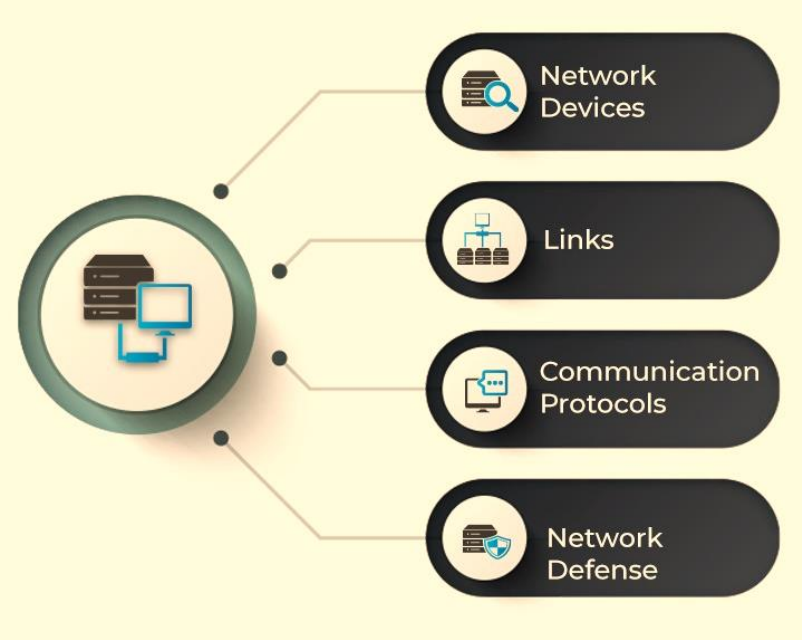

Figure 1: Main Components of a Computer Network

1. Network Devices:

Network devices or nodes are computing devices that need to be linked in the network. Some network devices include:

- **Computers, mobiles, and other consumer devices**: These are end devices that users directly and frequently access. For example, an email originates from the mailing application on a laptop or mobile phone.

- **Servers**: These are application or storage servers where the main computation and data storage occur. All requests for specific tasks or data come to the servers.

- **Routers**: Routing is the process of selecting the network path through which the data packets traverse. Routers are devices that forward these packets between networks to ultimately reach the destination. They add efficiency to large networks.

- **Switches**: Repeaters are to networks what transformers are to electricity grids—they are electronic devices that receive network signals and clean or strengthen them. Hubs are repeaters with multiple ports in them. They pass on the data to whichever ports are available. Bridges are smarter hubs that only pass the data to the destination port. A switch is a multi-port bridge. Multiple data cables can be plugged into switches to enable communication with multiple network devices.

- **Gateways**: Gateways are hardware devices that act as 'gates' between two distinct networks. They can be firewalls, routers, or servers.

2. Links:

Links are the transmission media which can be of two types:

- **Wired**: Examples of wired technologies used in networks include coaxial cables, phone lines, twisted-pair cabling, and optical fibers. Optical fibers carry pulses of light to represent data.
- **Wireless**: Network connections can also be established through radio or other electromagnetic signals. This kind of transmission is called 'wireless'. The most common examples of wireless links include communication satellites, cellular networks, and radio and technology spread spectrums. Wireless LANs use spectrum technology to establish connections within a small area.

3. Communication Protocols:

A communication protocol is a set of rules followed by all nodes involved in the information transfer. Some common protocols include the internet protocol suite (TCP/IP), IEEE 802, Ethernet, wireless LAN, and cellular standards. TCP/IP is a conceptual model that standardizes communication in a modern network. It suggests four functional layers of these communication links:

- **Network access layer**: This layer defines how the data is physically transferred. It includes how hardware sends data bits through physical wires or fibers.
- **Internet layer**: This layer is responsible for packaging the data into understandable packets and allowing it to be sent and received.
- **Transport layer**: This layer enables devices to maintain a conversation by ensuring the connection is valid and stable.
- **Application layer**: This layer defines how high-level applications can access the network to initiate data transfer.

Most of the modern internet structure is based on the TCP/IP model, though there are still strong influences of the similar but seven-layered open systems interconnection (OSI) model.

IEEE802 is a family of IEEE standards that deals with local area networks (LAN) and metropolitan area networks (MAN). Wireless LAN is the most well-known member of the IEEE 802 family and is more widely known as WLAN or Wi-Fis.

4. Network Défense:

While nodes, links, and protocols form the foundation of a network, a modern network cannot exist without its defenses. Security is critical when unprecedented amounts of

data are generated, moved, and processed across networks. A few examples of network defense tools include firewall, intrusion detection systems (IDS), intrusion prevention systems (IPS), network access control (NAC), content filters, proxy servers, anti-DDoS devices, and load balancers.

IV TYPES OF COMPUTER NETWORKS:

Computer networks can be classified based on several criteria, such as the transmission medium, the network size, the topology, and organizational intent. Based on a geographical scale, the different types of networks are:

1. **Nanoscale networks**: These networks enable communication between minuscule sensors and actuators.
2. **Personal area network (PAN)**: PAN refers to a network used by just one person to connect multiple devices, such as laptops to scanners, etc.
3. **Local area network (LAN)**: The local area network connects devices within a limited geographical area, such as schools, hospitals, or office buildings.
4. **Storage area network (SAN)**: SAN is a dedicated network that facilitates block-level data storage. This is used in storage devices such as disk arrays and tape libraries.
5. **Campus area network (CAN)**: Campus area networks are a collection of interconnected LANs. They are used by larger entities such as universities and governments.
6. **Metropolitan area network (MAN)**: MAN is a large computer network that spans across a city.
7. **Wide area network (WAN)**: Wide area networks cover larger areas such as large cities, states, and even countries.
8. **Enterprise private network (EPN):** An enterprise private network is a single network that a large organization uses to connect its multiple office locations.
9. **Virtual private network (VPN)**: VPN is an overlay private network stretched on top of a public network.
10. **Cloud network**: Technically, a cloud network is a WAN whose infrastructure is delivered via cloud services.

Based on organizational intent, networks can be classified as:

1. **Intranet**: Intranet is a set of networks that is maintained and controlled by a single entity. It is generally the most secure type of network, with access to authorized users alone. An intranet usually exists behind the router in a local area network.

2. **Internet**: The internet (or the internetwork) is a collection of multiple networks connected by routers and layered by networking software. This is a global system that connects governments, researchers, corporates, the public, and individual computer networks.

3. **Extranet**: An extranet is similar to the intranet but with connections to particular external networks. It is generally used to share resources with partners, customers, or remote employees.

4. **Darknet**: The darknet is an overlay network that runs on the internet and can only be accessed by specialized software. It uses unique, customized communication protocols.

REFERENCES:

[1] Adedokun, Emmanuel & Adamu, Hamisu A. & Shaibu, Idris. (2018). Modified Token Based Congestion Control Scheme for Opportunistic Networks. Journal of Computing and Information Technology. 26. 7-17. 10.20532/cit.2018.1003825.

[2] B. S. Vishwanath Hari Kumar Naidu, K. Thanushkodi, M. B. Sanjay Pandey, G.Vasanth. (2010), "The Novel Application of Artificial Neural Networks for a Reliable Secure Wireless Multicast Routing in Mobile Ad-Hock Networks"

[3] Basheer, Shajahan & Alavandar, Srinivasan. (2018). Congestion Controller for Best Effort Networks Using Fuzzy Inference System. Journal of Computational and Theoretical Nanoscience. 15. 40-46. 10.1166/jctn.2018.7053.

[4] Bathla, Neha & Kaur, Amanpreet & Singh, Gurpreet. (2014). Congestion Control Techniques in TCP: A Critique.

[5] C. Chrysostomou, A Pitsillides, G. Hadjipollas, A. Sekercioglu and M. Polycarpou, (2006). "Fuzzy Logic Congestion Control In TCP/IP Best Effort Networks".

[6] C. Partridge and T. Shepard. (1997), "TCP/IP performance over satellite links. In IEEE Network Magazine", pp. 44–49.

[7] Dvir, Amit & Vasilakos, Athanasios. (2010). Backpressure-based Routing Protocol for DTNs. Computer Communication Review - CCR. 40. 405-406. 10.1145/2043164.1851233.

[8] Ibrahim, Dogan. (2016). An Overview of Soft Computing. Procedia Computer Science. 102. 34-38. 10.1016/j.procs.2016.09.366.

[9] J. Postel.(1981), "Transmission Control Protocol. RFC 793", 1981.