ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (373-377), Month: April-June 2014, Available at: www.researchpublish.com

An Introduction to Computer Networking

Sumit Ahlawat[#1], Anshul Anand[#2]

[#1]M.Tech Student, [#2]Asst. Professor
Department of CSE, Shri Baba Mastnath Engineering College, Rohtak (INDIA)

***Abstract*: Computer networks are a system of interconnected computers for the purpose of sharing digital information. The concept of a network began in 1962 when a server at the Massachusetts Institute of Technology was connected to a server in Santa Monica, California. Since that time the proliferation of computers and computer networks has increased significantly. One of the most significant challenges to networks is attacks on their resources caused by inadequate network security. In this research paper we highlight and overview concept of computer networks.**

***Keywords:* Computer networks, protocols, network security.**

I. INTRODUCTION

A computer network or data network is a telecommunications network that allows computers to exchange data. In computer networks, networked computing devices pass data to each other along data connections. The connections (network links) between nodes are established using either cable media or wireless media. The best-known computer network is the Internet. Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices are said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other. Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications. Computer networks differ in the physical media used to transmit their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent.

II. HISTORY

Making devices talk to each other for the purposes of communication is nothing new. Early forays into telephony such as the telegraph and telephone have since evolved into more complicated devices, and now a computer can be networked to the Internet, another PC, or even a home stereo. In the early 1960s, individual computers had to be physically shared, making the sharing of data and other information difficult. Seeing this was impractical, researchers developed a way to "connect" the computers so they could share their resources more efficiently. Hence, the early computer network was born.

Through the then-new communication protocol known as packet switching, a number of applications, such as secure voice transmission in military channels became possible. These new circuits provided the basis for the communication technologies of the rest of the 20th century, and with further refinement these were applied to computer networks. These networks provided the basis for the early ARPANET, which was the forerunner of the modern Internet. The Advanced Research Projects Agency (ARPA) submitted the proposal for the project on June 3, 1968 which was approved a few weeks later. This proposal entitled "Resource Sharing Computer Networks" would allow ARPA not only the further sharing of their data, but would allow them to further their research in a wide variety of military and scientific fields. After being tested in four locations, the network spread and the new protocols created for its use evolved into today's World Wide Network.

In 1977, early PC-based Local Area Networks, or LANs (Local Area Networks) were spreading, and while initially restricted to academics and hobbyists, they eventually found their way into the workplace and in homes, although the explosion into the latter two arenas is a relatively recent phenomenon. LAN variants also developed, including Metropolitan Area Networks (MANs) to cover large areas such as a college campus, and Wide Area Networks (WANs) for university-to-university communication. With the widespread use of computers in the corporate world, the speed and convenience of using them to communicate and transfer data has forever altered the landscape of how people conduct business. Networks have become an integral part of the corporate world. Ubiquitous computing and Internet-capable cellular phones have allowed people to remain connected, even if the individual is away from a fully wired office environment.

III. PROPERTIES OF COMPUTER NETWORKS

Facilitate communications: Using a network, people can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing. Permit sharing of files, data, and other types of information In a network environment, authorized users may access data and information stored on other computers on the network.

Facilitates interpersonal communications

People can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing.

Allows sharing of files, data, and other types of information

Authorized users may access information stored on other computers on the network. Providing access to information on shared storage devices is an important feature of many networks.

Allows sharing of network and computing resources

Users may access and use resources provided by devices on the network, such as printing a document on a shared network printer. Distributed computing uses computing resources across a network to accomplish tasks.

May be insecure

A computer network may be used by computer Crackers to deploy computer viruses or computer worms on devices connected to the network, or to prevent these devices from accessing the network (denial of service).

May interfere with other technologies

Power line communication strongly disturbs certain [5] forms of radio communication, e.g., amateur radio. It may also interfere with last mile access technologies such as ADSL and VDSL. A complex computer network may be difficult to set up. It may be costly to set up an effective computer network in a large organization.

IV. PROTOCOLS IN NETWORKING

Ethernet: The Ethernet protocol is by far the most widely used one. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other nodes have already transmitted on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant.

Fast Ethernet: To allow for an increased speed of transmission, the Ethernet protocol has developed a new standard that supports 100 Mbps.

Local Talk: Local Talk is a network protocol that was developed by Apple Computer, Inc. for Macintosh computers. The method used by Local Talk is called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). It is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. Local Talk adapters and special twisted pair cable can be used to connect a series of computers through the serial port.

Token Ring: The Token Ring protocol was developed by IBM in the mid-1980s. The access method used involves token-passing. In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next.

FDDI: Fiber Distributed Data Interface (FDDI) is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances. The access method used by FDDI involves token-passing. FDDI uses a dual ring physical topology.

ATM: Asynchronous Transfer Mode (ATM) is a network protocol that transmits data at a speed of 155 Mbps and higher. ATM works by transmitting all data in small packets of a fixed size; whereas, other protocols transfer variable length packets. ATM supports a variety of media such as video, CD-quality audio, and imaging. ATM employs a star topology, which can work with fiber optic as well as twisted pair cable.

Gigabit Ethernet: The most latest development in the Ethernet standard is a protocol that has a transmission speed of 1 Gbps. Gigabit Ethernet is primarily used for backbones on a network at this time. In the future, it will probably also be used for workstation and server connections.

V. APPLICATIONS

Applications of wireless technology:

Mobile telephones

One of the best-known examples of wireless technology is the mobile phone, also known as a cellular phone, with more than 4.6 billion mobile cellular subscriptions worldwide as of the end of 2010.

Wireless data communications

Wireless data communications are an essential component of mobile computing. The various available technologies differ in local availability, coverage range and performance, and in some circumstances, users must be able to employ multiple connection types and switch between them.

Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to the Internet. Standardized as IEEE 802.11 a,b,g,n, Wi-Fi approaches speeds of some types of wired Ethernet. Wi-Fi has become the de facto standard for access in private homes.

Cellular data service offers coverage within a range of 10-15 miles from the nearest cell site. Speeds have increased as technologies have evolved, from earlier technologies such as GSM, CDMA and GPRS, to 3G networks such as W-CDMA, EDGE or CDMA2000.

Mobile Satellite Communications may be used where other wireless connections are unavailable, such as in largely rural areas or remote locations. Satellite communications are especially important for transportation, aviation, maritime and military use.

Wireless Sensor Networks are responsible for sensing noise, interference, and activity in data collection networks. This allows us to detect relevant quantities, monitor and collect data, formulate meaningful user displays, and to perform decision-making functions

Wireless energy transfer

Wireless energy transfer is a process whereby electrical energy is transmitted from a power source to an electrical load that does not have a built-in power source, without the use of interconnecting wires. There are two different fundamental methods for wireless energy transfer. They can be transferred using either far-field methods that involve beam

power/lasers, radio or microwave transmissions or near-field using induction. Both methods utilize electromagnetism and magnetic fields

Wireless Medical Technologies

New technologies such as mobile body area networks (MBAN) the capability to monitor blood pressure, heart rate, oxygen level and body temperature, all with wireless technologies. The MBAN works by sending low powered wireless signals to receivers that feed into nursing stations or monitoring sites. This technology helps with the intentional and unintentional risk of infection or disconnection that arise from wired connections.

Computer interface devices

Answering the call of customers frustrated with cord clutter, many[who?] manufacturers of computer peripherals turned to wireless technology to satisfy their consumer base [citation needed]. Originally these units used bulky, highly limited transceivers to mediate between a computer and a keyboard and mouse; however, more recent generations have used small, high-quality devices, some even incorporating Bluetooth. These systems have become so ubiquitous that some users have begun complaining about a lack of wired peripherals. [who?] Wireless devices tend to have a slightly slower response time than their wired counterparts; however, the gap is decreasing. [citation needed]

Computer interface devices such as a keyboard or mouse are powered by a battery and send signals to a receiver through a USB port by way of a radio frequency (RF) receiver. The RF design makes it possible for signals to be transmitted wirelessly and expands the range of effective use, usually up to 10 feet. Distance, physical obstacles, competing signals, and even human bodies can all degrade the signal quality. Concerns about the security of wireless keyboards arose at the end of 2007, when it was revealed that Microsoft's implementation of encryption in some of its 27 MHz models was highly insecure.

V. NETWORK SECURITY

What is network security? How does it protect you? How does network security work? What are the business benefits of network security? You may think you know the answers to basic questions like, What is network security? Still, it's a good idea to ask them of your trusted IT partner. Why? Because small and medium-sized businesses (SMBs) often lack the IT resources of large companies. That means your network security may not be sufficient to protect your business from today's sophisticated Internet threats.

What Is Network Security?

In answering the question What is network security? your IT partner should explain that network security refers to any activities designed to protect your network. Specifically, these activities protect the usability, reliability, integrity, and safety of your network and data. Effective network security targets a variety of threats and stops them from entering or spreading on your network. What Is Network Security and How Does It Protect Your network? Many network security threats today are spread over the Internet. The most common include:

1. Viruses, worms, and Trojan horses
2. Spyware and adware
3. Zero-day attacks, also called zero-hour attacks
4. Hacker attacks
5. Denial of service attacks
6. Data interception and theft
7. Identity theft

You need multiple layers of security. If one fails, others still stand. Network security is accomplished through hardware and software. The software must be constantly updated and managed to protect you from emerging threats. A network security system usually consists of many components. Ideally, all components work together, which minimizes maintenance and improves security.

Network security components often include:

1. Anti-virus and anti-spyware
2. Firewall, to block unauthorized access to your network
3. Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks
4. Virtual Private Networks (VPNs), to provide secure remote access

V. CONCLUSION

While the age-old concept of the network is foundational in virtually all areas of society, Computer Networks and Protocols have forever changed the way humans will work, play, and communicate. Forging powerfully into areas of our lives that no one had expected, digital networking is further empowering us for the future. New protocols and standards will emerge, new applications will be conceived, and our lives will be further changed and enhanced. While the new will only be better, the majority of digital networking's current technologies are not cutting-edge, but rather are protocols and standards conceived at the dawn of the digital networking age that have stood solid for over thirty years.

REFERENCES

[1] http://en.wikipedia.org/wiki/Computer_network

[2] http://gimnetwork.wordpress.com/2013/01/19/properties-of-computer-networks/

[3] http://www.goldgroup.co.uk/brief-history-networking/

[4] http://www.edrawsoft.com/Network-Protocol.php

[5] http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6157406&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5449605%2F6157403%2F06157406.pdf%3Farnumber%3D6157406

[6] http://infpower.wordpress.com/

[7] http://www.ecii.edu/wp-content/uploads/2013/10/Tantillo_1_Pantani_Network_Security_Through_Open_Source_Intrusion_Detection_Systems_May2012.pdf