

AN INTRODUCTION TO COMPUTER NETWORKING

Harinder Singh Tiwana¹, Parminder Kaur²

^{1,2} Department of Computer Science & Applications
Desh Bhagat University, Mandi Gobindgarh

ABSTRACT

Computer networks are systems of interconnected computers designed for sharing digital information. The concept of networking began in 1962 when a server at the Massachusetts Institute of Technology was connected to a server in Santa Monica, California. Since then, the proliferation of computers and computer networks has increased significantly. One of the key challenges is attacks on network resources due to inadequate security. This paper provides an overview of computer networks.

Keywords: Computer networks, protocols, network security

I. INTRODUCTION

A computer network or data network is a telecommunications system allowing computers to exchange data. Networked computing devices pass data along network links using either cable or wireless media.

Network Nodes: Devices that originate, route, and terminate data are called network nodes, including hosts (PCs, phones, servers) and networking hardware. Devices are networked together when they can exchange information, even without a direct connection.

Applications:

- Access to the World Wide Web
- Shared use of storage and application servers, printers, fax machines
- Email and instant messaging

Networks differ by physical media, communication protocols, size, topology, and organizational intent.

II. HISTORY

Early attempts at communication include the telegraph and telephone. In the 1960s, sharing computing resources was inefficient, prompting the development of computer networks.

Packet Switching: Enabled applications such as secure military voice transmission and formed the basis for ARPANET, the precursor to today's Internet. ARPA submitted the proposal "Resource Sharing Computer Networks" on June 3, 1968.

LANs, MANs, WANs:

- 1977: Early Local Area Networks (LANs) emerged, later expanding to workplaces and homes
- Metropolitan Area Networks (MANs) cover large areas like campuses

- Wide Area Networks (WANs) enable university-to-university communication

Ubiquitous computing and mobile devices allow continuous connectivity outside traditional wired environments.

III. PROPERTIES OF COMPUTER NETWORKS

1. **Facilitate Communications:** Email, instant messaging, chat, voice, and video calls.
2. **Share Files and Data:** Authorized users can access data on other networked devices.
3. **Share Network and Computing Resources:** Distributed computing and shared printers enhance efficiency.
4. **Potential Insecurity:** Networks can be exploited to deploy viruses, worms, or denial-of-service attacks.
5. **Interference:** Certain network technologies may interfere with radio communication or last-mile access technologies.
6. **Setup Complexity:** Large-scale networks can be costly and difficult to configure effectively.

IV. PROTOCOLS IN NETWORKING

- **Ethernet:** Uses CSMA/CD to listen before transmitting; widely used.
- **Fast Ethernet:** Supports 100 Mbps transmission speed.
- **LocalTalk:** Developed by Apple; uses CSMA/CA to signal intent before transmission.
- **Token Ring:** Developed by IBM; uses token-passing in a logical ring.
- **FDDI:** Fiber Distributed Data Interface; dual-ring topology for LAN interconnection.
- **ATM:** Asynchronous Transfer Mode; transmits fixed-size packets at ≥ 155 Mbps, supports video and audio.
- **Gigabit Ethernet:** Latest Ethernet standard, 1 Gbps transmission, used in network backbones.

V. APPLICATIONS

Wireless Technology Applications:

1. **Mobile Telephones:** Over 4.6 billion subscriptions globally (as of 2010).
2. **Wireless Data Communications:** Supports mobile computing with Wi-Fi, cellular data (3G, EDGE, CDMA2000), and satellite communications.
3. **Wireless Sensor Networks:** Monitor and collect data, aiding decision-making.
4. **Wireless Energy Transfer:** Transfers power without wires using far-field (beam, radio, microwave) or near-field (induction) methods.
5. **Wireless Medical Technologies:** Mobile Body Area Networks (MBAN) monitor vital signs wirelessly.
6. **Computer Interface Devices:** Wireless keyboards, mice, and peripherals communicate via RF or Bluetooth, offering convenience but with minor latency and security concerns.

VI. NETWORK SECURITY

Definition: Activities designed to protect the usability, reliability, integrity, and safety of networks and data.

Common Threats:

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

Security Measures: Multiple layers of hardware and software protect networks. Components often include:

- Anti-virus and anti-spyware
- Firewalls
- Intrusion Prevention Systems (IPS)
- Virtual Private Networks (VPNs)

VII. CONCLUSION

Computer Networks and Protocols have transformed the way humans work, communicate, and live. Digital networking continues to expand into new areas, enabling innovation and efficiency. While many current protocols have existed for decades, future developments in standards and applications will further enhance network capabilities.

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>
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