Chapter 1: Exploring the Network

* 1. **1. Networking Today**
* **Network in our Daily Lives: Methods to communicate are constantly changing and evolving. Every1 can connect, share, and diff**
* **Technology Then vs now:** Benefits of Internet (games, info, videos, destination route, online shopping, bank balance etc.)

**Fixed Computing:** You go to device **BOYD:** Device goes with you **Internet of Things:** Age of devices **Internet of Everything:** ppl, data

* **Global Community: Create a world in which national borders, geographic distances and physical limitations become less relevant.**

**CISCO refers to this as human network, centers on impact of internet and networks on people and business.**

* **Network support the way we learn: Robust and reliable networks support and enrich students learning experience.**

**Support creation of virtual classrooms, provide on-**demand video, enable collaborative learning spaces, enable Mobile Learning

In Addition to benefit for students, networks have improved management and administration courses as well. (Student enrollment)

* **Network support the way we communicate:** Globalization of internet caused new forms of communication that empower individuals to create information that can be accessed by a global audience

1. **Instant Messaging: IM and texting, both enable instant real-time communication between 2 or 2+ people. also file transfer, voice**
2. **Social Media:** Consist of interactive websites where people communicate, create, and share user-generated content with friends,
3. **Collaboration Tools:** Opportunity for people to work on shared documents. They can share text, graphics and edit doc together
4. **Weblogs:** Web pages that are easy to update and edit. Gives means to communicate their thoughts to a global audience without technical knowledge of web design. Blogs are available for almost every topic
5. **Wikis:** web pages that group of people can edit and view together. Wiki is group creation. Subject to extensive review and editing. Wikipedia- comprehensive resource, online encyclopedia. Many business use wikis as internal collaboration tool.
6. **Podcasting:** Audio-based medium that originally enabled people to record audio and convert it to use. Allows people to deliver their recordings to a wide audience. Audio file placed on a website, where others can download it and play it
7. **Peer-to-Peer:** Allows people to share files with each other without having to store and download them. User can join P2P network which lets them locate and share files with others. P2P not embraced by every1: concern of violation of copyrighted

* **Network support the way we work: Data networks initially used by business to internally record and manage data.**
* **Network support the way we play: Adoption of internet by entertainment and travel industries enhances ability to enjoy. Traditional forms of entertainment: listen to recording artists, preview, or view motion pics, read entire book, Live events, concert**

**New forms of entertainment: online games, online competition that the game designer sets. Even Offline activities enhanced: share common experiences and hobbies, Sports fans. Online markets and auction site provide opportunity to buy, sell etc.**

**1.1.2. Providing Resources in a Network**

* **Networks of Many Sizes: Comes in all sizes, simple networks installed in homes enable sharing of resources, documents etc. between few local computers, home office networks and small office networks to connect corporate network or other centralized resources. Communication over traditional forms of communication is less expensive and more efficient, mail, phone. In Business and large organizations, networks used on broader scale to provide employees with consolidation, storage and access to network servers, many organizations use their network to provide products and services to customers through their connection to internet. Internet means “Network of Networks”. An interconnected private and public networks**
* **Clients and Servers: All Computers connected to network directly participate network communication of host/end devices.**

**Hosts can send and receive messages on network. Software installed on computer decides what role the computer plays. Servers are hosts that have software installed to provide info. Each service requires separate server software. Clients are computer hosts that have software installed that enable to request and display info obtained from server. Example: Web browser**

**A single computer can run multiple types of server software. In a home or small business, one computer to act as file, web server**

**A single computer can run multiple types of client software. Must be client software for every service required. With multiple clients installed, a host can connect to multiple servers at a time. Example: user can check email as well as open web page**

* **Peer-to-Peer: Client and server software possible to run on one computer, carry both roles in home and small businesses.**

**Simplest peer-to-peer is two directly connected computers using wired or wireless connection. Multiple PCs can also be connected to create a larger peer-to-peer network but will require networking device, such as hub to interconnect devices.**

**Disadvantage: performance of host can be slowed down if it is acting both a client and server at the same time**

Diagram

Description automatically generated

* 1. **LANs, WANs, and the internet**
* **Components of Network: Network infrastructure consist of 3 categories of components: Devices, Media, Services.**
* **Devices and media: Physical elements, hardware. Visible components like PC, laptop etc. however wireless media, messages are transmitted through air using invisible radio frequency or infrared waves**
* **Services: Network components used to provide services and processes. These are communication programs, software. Network services provide info in response to a request. Email hosting and web hosting services. Processes less obvious, but critical**
* **End Devices: Devices that form interface between users and underlying communication network. Examples, Computers, Network printers, VoIP phones, Telepresence endpoint, Security cameras, Mobile handheld devices. A Host device is either source or destination of message transmitted over the network. Each host is distinguished through its address. When host initiates a communication, it uses address of destination host to specify where the message should be sent.**
* **Intermediary Network Devices: Interconnect end devices. These devices provide connectivity and work behind scenes to ensure that data flows across the network. Examples, Network access (switches and wireless access points), Internetworking (routers), Security (firewall). Management of data as it flows through network is also a role of intermediary devices. They use destination host address along with info about network interconnections, to determine path that message should be sent. Processes running on intermediary devices perform these actions:**
* **Regenerate and retransmit data signals**
* **Maintain info about what pathways exist though the network and internetwork.**
* **Notify other device of errors and communication failures.**
* **Direct data along the alternate pathways when there is a link failure**
* **Classify and direct messages according to Quality of Service (QoS) priorities**
* **Permit or deny the flow of data, based on security settings**
* **Network Media: Communications across network are carried out by medium. Medium provide the channel over which message travels from source to destination. Usually, 3 types of media to interconnect devices: Metallic wire within cables (transmitted encoding the data into electrical impulses that match specific patterns), Glass or plastic fibers (relies on pulses of light, within infrared or visible ranges), Wireless transmission (patterns of electromagnetic waves depict various bit values).**

**Criteria for choosing Network Media: Distance media can successfully carry a signal, The environment where the media is installed, amount of data and speed at which it must be transmitted, cost of media and installation**

* **Network Representations: Topology: Diagram representation of network. Important terms to remember.**
* **Network Interface Card- a NIC, or LAN adapter, provides physical connection to network at PC/ host device. The media connecting the PC to networking device plugins directly into the NIC**
* **Physical Port: A connector or outlet on a networking device where the media is connected to a host or other networking device**
* **Interface: Specialized ports on internetworking devices that connect to individual networks. Routers are interconnect networks, the ports on a router are referred to as network interfaces**
* **Two Types of Topology Diagrams: Physical Topology Diagram (Identify Physical location of intermediary devices, configured ports and cable installation), Logical Topology Diagram (Identify devices, ports, and IP addressing scheme)**
* **Types of Networks: Networks can vary based on 1. Size of Area Covered 2. Number of Users connected 3. Number and types of services available**

**Two most Common types of Networks:**

* **Local Area Network (LAN): a network infrastructure provides access to users and end devices in a small geographical area. (Home, office etc.), administered by a single organization or individual, governs security and access control policies are enforced on the network level. LANs provide high bandwidth to internal end devices and intermediary devices**
* **Wide Area Network (WAN): a network infrastructure provides access to other networks over a wide geographical area. (Cities, provinces, states, etc.). WANs are administered by multiple service providers. Slower speed links than LAN**

**Other Types of Networks:**

* **Metropolitan Area Network (MAN): network infrastructure that spans bigger than LAN but smaller than WAN (Eg: a city)**
* **Wireless LAN (WLAN): Like LAN but wirelessly interconnects users and end points in small geographical area.**
* **Storage Area Network (SAN): network infrastructure designed to support file servers, provide data storage, retrieval etc. It involves high-end servers, multiple disk arrays, and Fibre Channel interconnection technology.**
* **The Internet: Worldwide collection of interconnected networks, cooperating with each other to exchange info using common standards. There are many agencies built up to maintain structure and standardization of internet protocols and processes. Eg: Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), Internet Architecture Board (IAB) etc. internet =multiple networks interconnected, Internet =Global system of interconnected computer network**
* **Intranet: Refers to private connection of LANs and WANs belonging to an organization. Intranet only accessible from within org.**
* **Extranet: An org. can provide safe and secure access to individuals who work in diff org. but require company data. Examples: company providing access to outside suppliers/contractors, Hospital providing booking sys to doctors to make appointments.**
* **Connecting to the Internet: Home users, teleworkers and small offices typically require connection to ISP (broadband cable, Broadband digital subscriber line (DSL)), Organizations typically require access to other corporate sites and internet. Fast connections are required for that. Business-class interconnections provided by SP, (Example: DSL, leased lines, Metro Ethernet)**
* **Connecting Remote users to the internet:**
* **Cable: Typically offered by cable television SP, provides high bandwidth, always connected to internet, Special cable modem separates Internet data signals from other signals carried on cable and provides Ethernet connection to host computer/LAN**
* **DSL: Provides high bandwidth, always on network, requires high-speed modem that separates DSL signals from telephone signal and provide ethernet to host computer. DSL runs on telephone line, split into 3 different channels: 1. Voice telephone calls 2. Faster download Channel 3. Sending/Uploading info. The quality and speed of DSL depends on telephone line**
* **Cellular: Uses cellphone network to connect. When you can access cellular signal, you can receive cellular internet access. Performance limited by capabilities of phone and cell tower to which it is connected. Used where there is no other internet conn.**
* **Satellite: Good for homes or offices that do not have Cable/DSL. Satellite requires clear line of sight. Speed varies on contract, generally good. Equipment and installation cost is high.**
* **Dial-up Telephone: Inexpensive option uses phone line and a modem. To connect to ISP, user calls ISP access phone number. The low bandwidth provided is usually not sufficient for big file data transfer. Should be consider only if higher speed conn. Not there**
* **Connecting Business to the internet:**
* **Dedicated Leased line: dedicated connection from SP to customer premise. They are reserved circuits that connect geographically separated offices and data networking. Circuits are rented based on monthly/yearly rate which make it expensive**
* **Metro Ethernet: Typically, available from a provider to customer premise over a dedicated copper or fiber connection providing bandwidth speed of 10 Mb/s to 10 Gb/s. Ethernet over Copper (EoC) is more economical than fiber optic. Fiber optic ethernet service delivers the fastest connections available at economical price per megabit. Still many areas where this is not there**
* **DSL**
* **Satellite** 
  1. **Converged Networks**
* **Advances in technology are enabling us to consolidate diff types of networks onto one platform (converged network). Converged networks can deliver voice, video streams, text and graphics between many different types of devices over the same communication channel and network structure. This platform provides wide range of alternative and new communication methods that enable people to interact directly with each other almost instantaneously. (One common network infrastructure)**
* **Reliable Network: Network Architecture: refers to technologies that support infrastructure and programmed services and rules, or protocols that move messages across the network**

**Four basic characteristics that underlying architectures need to address in order to meet user expectations:**

1. **Fault Tolerance – The expectation that Internet is always available to millions of users who rely on it. Requires network architecture to be fault tolerant. Fault tolerant network – fewest number of devices affected by failure, quick recovery. The network depends on multiple paths, if one fails, its instantly sent over a different path.**

**Fault tolerance in circuit-switched connection-oriented Networks: When person called, call first went to a setup process. Process identified the telephone switching locations between source and destination. Temporary path/circuit was created for duration of phone call. If any link or device in circuit failed, the call was dropped. Circuit-switched networks gave priority to existing circuit connections at expense of creating new circuits. After a call is established, even if no communication occurs between persons, the circuit remains connected until one party disconnects the call. The cost to create many alternate paths with enough capacity to support a large simultaneous circuits and technologies necessary to dynamically recreate dropped circuits in event of failure, is why circuit-switched was not optimal for the internet**

**Fault tolerance in packet-switched connection-oriented Networks: The Premise of network is that a single message can be broken into multiple message blocks, with each message containing addressing info to indicate initial and final destination. Using these embedded info message blocks, called packets, are sent through various paths and reassembled reaching final destination.**

**The devices within network are themselves unaware of the content of individual packets. Visible addresses, the IP address are assigned. Reaching the destination, a routing decision is made as to which path to use to forward the packets towards destination**

**Benefit of circuit-switched connection: Quality and consistency of messages transmitted can be guaranteed. Another benefit is that the provider of service can charge users for period the connection is active. Ability to charge users for active connections through network is fundamental premise of telecommunication service industry.**

1. **Scalability – A scalable network can expand quickly to support new users and applications without impacting performance of service being delivered to existing users. Scalability also refers to ability to accept new products and applications. Adherence to standards enables manufacturers of hardware and software to concentrate on product development and improvements in areas of performance and capacity. Current internet architecture, highly scalable, may not always be able to keep up with pace of user demand. New protocols and addressing structures are under development to meet increasing rate at which internet services are being added.**

**3.Quality of Service (QoS)- Networks must provide predictable, measurable and at times, guaranteed services. Needs mechanism to manage congested network traffic. Network Bandwidth is the measure capacity of the network (measured in number of bits that can be transmitted in a single second, or bits per second (bps).**

**Examples of priority decisions for organization may include:**

1. **Time-Sensitive Communication: increase priority for services like telephony or video distribution**
2. **Non Time-Sensitive Communication: decrease priority for web page retrieval or email**
3. **High importance to organization: Increases priority for production control or business transaction data**
4. **Undesirable Communication: Decrease priority or block unwanted activity, like peer-to-peer file sharing or live entertainment**

**4.Security-**

**Consequences of compromising integrity of these assets:**

* **Network outages that prevent comm and transactions from occurring, with consequent loss of business**
* **Intellectual property that is stolen and used by a competitor**
* **Personal or private info that is compromised or made public without users consent**
* **Misdirection and loss of personal or business funds**
* **Loss of important data that takes significant labor to replace, or is impeccable**

**Two types of network security concerns that must be addressed: network infrastructure security, information security**

* **Network Infrastructure security: physical securing of devices that provide network connectivity, and preventing unauthorized access to the management software that resides on them**
* **Information Security: protecting information contained within packets being transmitted over the network and info stored on network attached devices. Security measures taken in network should:**

1. **Prevent unauthorized disclosure**
2. **Prevent theft of info**
3. **Prevent unauthorized modification of info**
4. **Prevent Denial of Service (DoS)**

* **Three Primary Requirements to achieve goals of network security:**

1. **Ensuring confidentiality: Confidentiality means that only intended or authorized recipients can access and read data. This is accomplished by having a strong system for user authentication, enforcing passwords that are difficult to guess. (also encryption)**
2. **Maintaining communication integrity: Data integrity means having assurance that info is not altered in transmission. Data integrity can be compromised when info has been corrupted- willfully or accidentally. Validate messages/packets during delivery**
3. **Ensuring Availability: Having assurance of timely and reliable access to data services for authorized users. Network firewall devices, server antivirus software can ensure reliability, and robustness to detect, repel, and cope such attacks**

**Network Trends: Top trends: Any device, to any content, Online collaboration, video, cloud computing**

**BYOD: End users having the freedom to use personal tools to access info and communicate across business or campus network. BYOD means any devices, with any ownership, used anywhere.**

**Online Collaboration: Collaboration is defined as the act of working with another or others on a joint project. Improve customer satisfaction, increasing communication choices, optimizing team performance, enable mobile users, improve organizational communications, transform training and event management.**

**Video Communication: critical in collaboration and communication. Another trend in video is video-on-demand and streaming live video. Delivering video over the network lets us see movies and television programs when we want and where we want**

**Cloud Computing: use of computing resources that are delivered as a service over a network. The user’s computer must interface with the cloud using software, which may be a web browser, and cloud’s network take care of rest. Cloud computing means web-based computing. Cloud computing benefits as: Organizational flexibility (Users can access info anytime, anyplace using a web browser), Agility and rapid development (IT department can focus on delivering the tools to mine, analyze, and share info and knowledge from database, files etc.), Reduced cost of infrastructure (technology is moved from on-site to a cloud provider, eliminating the cost of hardware and applications), Refocus of IT resources (Cost savings of hardware and applications can be applied anywhere), Creation of new business models (Applications and resources are easily accessible, so companies can react to customer needs.**

**Data Centers: Data center is facility used to house computer systems and associated components including, Redundant data communications connections, high-speed virtual servers, Redundant storage systems, Redundant or backup power supplies, Environmental controls, Security devices. Virtualization is the creation of virtual version of something, such as hardware platform.**

**Data centers are typically expensive to build and maintain. For this reason, large organizations use private data centers to house their data and provide service to users.**

* **Smart Home Technology: technology that is integrated into everyday appliances allowing them interconnect with other devices, making it more smart or automated**
* **Powerline Networking: uses existing electrical wiring to connect devices**
* **Wireless Broad Band: Wireless internet service provider (WISP) connects subscribers to a designated point or hot spot using similar wireless technologies found in home wireless local networks. Wireless Broadband Service: uses same cellular technology used to access internet with a smart phone/tablet.**

**Network Security: Security a network includes protocols, technologies, devices, tools etc. Most common external threats are**

* **Viruses, works, and trojan horse: Malicious software and arbitrary code running on user device**
* **Spyware and adware: software installed on user device that secretly collects info about the user**
* **Zero-day attacks (zero-hour attacks): an attack that occurs on first day that a vulnerability is known**
* **Hacker Attacks: an attack by a knowledgeable person to user devices or network resources.**
* **Denial of Service attacks: Attacks designed to slow or crash applications and processes on a network device.**
* **Data interception and theft: an attack to capture private info from an organization’s network**
* **Identity Theft: an attack to steal login credentials of a user to access private data**

**Security Solutions for home or small offices:**

* **Antivirus and Antispyware: to protect user devices from malicious software**
* **Firewall fitting: to block unauthorized access to network. Maybe a host-based firewall system or basic filtering service**

**Security Solutions for large Networks and corporate networks:**

* **Dedicated firewall systems:** To provide more advanced firewall capability that can filter large amounts of traffic with granularity
* **Access Control Lists (ACL): to further filter access and traffic forwarding**
* **Intrusion Prevention Systems (IPS): to identify fast-spreading threats, such as zero-day attacks**
* **Virtual Private Networks (VPN): to provide secure access to remote workers.**