Networks Affect our Lives

In today's world, through the use of networks, we are connected like never before. People with ideas can communicate instantly with others to make those ideas a reality. The creation of online communities for the exchange of ideas and information has the potential to increase productivity opportunities across the globe. The creation of the cloud lets us store documents and pictures and access them anywhere, anytime.

Network Components

All computers that are connected to a network and participate directly in network communication are classified as hosts. Hosts can be called end devices. Some hosts are also called clients. Many computers function as the servers and clients on the network. This type of network is called a peer-to-peer network. An end device is either the source or destination of a message transmitted over the network. Intermediary devices connect the individual end devices to the network and can connect multiple individual networks to form an internetwork. Intermediary devices use the destination end device address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network. The media provides the channel over which the message travels from source to destination.

Network Representations and Topologies

Diagrams of networks often use symbols to represent the different devices and connections that make up a network. A diagram provides an easy way to understand how devices connect in a large network. This type of "picture" of a network is known as a topology diagram. Physical topology diagrams illustrate the physical location of intermediary devices and cable installation. Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.

Common Types of Networks

Small home networks connect a few computers to each other and to the internet. The small office/home office (SOHO) network allows computers in a home office or a remote office to connect to a corporate network, or access centralized, shared resources. Medium to large networks, such as those used by corporations and schools, can have many locations with hundreds or thousands of interconnected hosts. The internet is a network of networks that connects hundreds of millions of computers world-wide. The two most common types of network infrastructures are Local Area Networks (LANs), and Wide Area Networks (WANs). A LAN is a network infrastructure that spans a small geographical area. A WAN is a network infrastructure that spans a wide geographical area. Intranet refers to a private connection of LANs and WANs that belongs to an organization. An organization may use an extranet to provide secure and safe access to individuals who work for a different organization but require access to the organization's data.

Internet Connections

SOHO internet connections include cable, DSL, Cellular, Satellite, and Dial-up telephone. Business internet connections include Dedicated Leased Line, Metro Ethernet, Business DSL, and Satellite. The choice of connection varies depending on geographical location and service provider availability. Traditional separate networks used different technologies, rules, and standards. Converged networks deliver data, voice, and video between many different types of devices over the same network infrastructure. This network infrastructure uses the same set of rules, agreements, and implementation standards. Packet Tracer is a flexible software program that lets you use network representations and theories to build network models and explore relatively complex LANs and WANs.

Reliable Networks

The term network architecture refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data across the network. As networks evolve, we have learned that there are four basic characteristics that network architects must address to meet user expectations: Fault Tolerance, Scalability, Quality of Service (QoS), and Security. A fault tolerant network is one that limits the number of affected devices during a failure. Having multiple paths to a destination is known as redundancy. A scalable network expands quickly to support new users and applications. Networks are scalable because the designers follow accepted standards and protocols. QoS is a primary mechanism for managing congestion and ensuring reliable delivery of content to all users. Network administrators must address two types of network security concerns: network infrastructure security and information security. To achieve the goals of network security, there are three primary requirements: Confidentiality, Integrity, and Availability.

Network Trends

There are several recent networking trends that affect organizations and consumers: Bring Your Own Device (BYOD), online collaboration, video communications, and cloud computing. BYOD means any device, with any ownership, used anywhere. Collaboration tools, like Cisco WebEx give employees, students, teachers, customers, and partners a way to instantly connect, interact, and achieve their objectives. Video is used for communications, collaboration, and entertainment. Video calls are made to and from anyone with an internet connection, regardless of where they are located. Cloud computing allows us to store personal files, even backup an entire drive on servers over the internet. Applications such as word processing and photo editing can be accessed using the cloud. There are four primary types of Clouds: Public Clouds, Private Clouds, Hybrid Clouds, and Custom Clouds. Smart home technology is currently being developed for all rooms within a house. Smart home technology will become more common as home networking and high-speed internet technology expands. Using the same wiring that delivers electricity, powerline networking sends information by sending data on certain frequencies. A Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to a designated access point or hot spot using similar wireless technologies found in home wireless local area networks (WLANs).

Network Security

There are several common external threats to networks:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks
- Threat Actor attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

These are the basic security components for a home or small office network:

- Antivirus and antispyware
- Firewall filtering

Larger networks and corporate networks use antivirus, antispyware, and firewall filtering, but they also have other security requirements:

- Dedicated firewall systems
- Access control lists (ACL)
- Intrusion prevention systems (IPS)
- Virtual private networks (VPN)

The IT Professional

The Cisco Certified Network Associate (CCNA) certification demonstrates that you have a knowledge of foundational technologies and ensures you stay relevant with skill sets needed for the adoption of next-generation technologies. Your CCNA certification will prepare you for a variety of jobs in today's market. At www.netacad.com you can click the Careers menu and then select Employment opportunities. You can find employment opportunities where you live by using the Talent Bridge Matching Engine. Search for jobs with Cisco as well as Cisco partners and distributors seeking Cisco Networking Academy students and alumni.