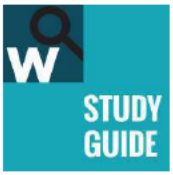
HOME › NETWORKING

Vangie Beal

February 17, 2015

Networking fundamentals teaches the building blocks of modern network design. Learn different types of networks, concepts, architecture and design.



Networking fundamentals teaches computer science students the building blocks of modern network design. Typically you will learn about the many different types of networks, networking concepts, network architecture, network communications and network design.

NETWORK FUNDAMENTALS CHECKLIST

Jump to a topic:

Tweet This Study Guide!

Webopedia study guides offer quick facts to help students prepare for computer science courses. Did you find this guide useful? Click to share it with friends and classmates on Twitter.

GETTING STARTED: KEY TERMS TO KNOW

The following definitions will help you to better understand computer networks:

- network
- networking
- stub network
- star network
- ring network
- bus network
- network map

DEFINING A NETWORK

A network is a group of two or more computer systems or other devices that are linked together to exchange data. Networks share resources, exchange files and electronic communications. For example, networked computers can share files or multiple computers on the network can share the same printer.

DIFFERENT TYPES OF NETWORKS

There are many types of computer networks. Common types of networks include the following:

- **Local-area network** (LAN): The computers are geographically close together (that is, in the same building).
- **Wide-area network** (WAN): The computers are farther apart and are connected by telephone lines or radio waves.
- **Metropolitan-area networ**k (MAN): A data network designed for a town or city.
- **Home-area network** (HAN): A network contained within a user's home that connects a person's digital devices.
- **Virtual private networ**k (VPN): A network that is constructed by using public wires usually the Internet to connect to a private network, such as a company's internal network.
- **Storage area network** (SAN): A high-speed network of storage devices that also connects those storage devices with servers.

Recommended Reading: *Webopedia's Virtual Private Network (VPN) Study Guide*.

THE IMPORTANCE OF NETWORK STANDARDS

Network standards are important to ensure that hardware and software can work together. Without standards you could not easily develop a network to share information. Networking standards can be categorized in one of two ways: formal and de facto (informal).

Formal standards are developed by industry organizations or governments. Formal standards exist for network layer software, data link layer, hardware and so on. Formal standardization is a lengthy process of developing the specification, identifying choices and industry acceptance.

There are a several leading organizations for standardization including The International Organization for Standardization (ISO) and The American National Standards Institute (ANSI). The most known standards

organization in the world is the Internet Engineering Task Force (IETF). IETF sets the standards that govern how much of the Internet operates.

The second category of networking standards is de facto standards. These standards typically emerge in the marketplace and are supported by technology vendors but have no official backing. For example, Microsoft Windows is a de facto standard, but is not formally recognized by any standards organization. It is simply widely recognized and accepted.

NETWORK COMPONENTS, DEVICES AND FUNCTIONS

Networks share common devices and functions, such as servers, transmission media (the cabling used to connect the network) clients, shared data (e.g. files and email), network cards, printers and other peripheral devices.

The following is a brief introduction to common network components and devices. You can click any link below to read the full Webopedia definition:

Server: A computer or device on a network that manages network resources. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks.

Client: A client is an application that runs on a personal computer or workstation and relies on a server to perform some operations.

Devices: Computer devices, such as a CD-ROM drive or printer, that is not part of the essential computer. Examples of devices include disk drives, printers, and modems.

Transmission Media: the type of physical system used to carry a communication signal from one system to another. Examples of transmission media include twisted-pair cable, coaxial cable, and fiber optic cable.

Network Operating System (NOS): A network operating system includes special functions for connecting computers and devices into a local-area network (LAN). The term network operating system is generally reserved for software that enhances a basic operating system by adding networking features.

Operating System: Operating systems provide a software platform on top of which other programs, called application programs, can run. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

Network Interface Card (NIC): An expansion board you insert into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.

Hub: A common connection point for devices in a network. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Switch: A device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model.

Router: A router is a device that forwards data packets along networks. A router is connected to at least two networks and is located at gateways, the places where two or more networks connect.

Recommended Reading: *The Difference Between Hubs, Switches and Routers*

Gateway: A node on a network that serves as an entrance to another network.

Bridge: A device that connects two local-area networks (LANs), or two segments of the same LAN that use the same protocol

Channel Service Unit/Digital Service Unit (CSU/DSU): The CSU is a device that connects a terminal to a digital line. Typically, the two devices are packaged as a single unit.

Terminal Adapter (ISDN Adapter): A device that connects a computer to an external digital communications line, such as an ISDN line. A terminal adapter is a bit like a modem but only needs to pass along digital signals.

Access Point: A hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN.

Modem (modulator-demodulator): A modem is a device or program that enables a computer to transmit data over, for example, telephone or cable lines.

Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

Recommended Reading: *The Differences and Features of Hardware and Software Firewalls*

MAC Address: A MAC (Media Access Control) address, sometimes referred to as a hardware address or physical address, is an ID code that's assigned to a network adapter or any device with built-in networking capability.

NETWORK MODELS

To simplify networks, everything is separated in layers and each layer handles specific tasks and is independent of all other layers. Control is passed from one layer to the next, starting at the top layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. Network models are used to define a set of network layers and how they interact. The two most widely recognized network models include the TCP/IP Model and the OSI Network Model.

THE 7 LAYERS OF THE OSI MODEL

The Open System Interconnect (OSI) is an open standard for all communication systems.The OSI model defines a networking framework to implement protocols in seven layers.

This layer conveys the bit stream – electrical impulse, light or radio signal — through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Examples include Ethernet, FDDI, B8ZS, V.35, V.24, RJ45.

Data Link Layer

At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. Examples include PPP, FDDI, ATM, IEEE 802.5/ 802.2, IEEE 802.3/802.2, HDLC, Frame Relay.

Network Layer

This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing. Examples include AppleTalk DDP, IP, IPX.

Transport Layer

This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.Examples include SPX, TCP, UDP.

Session Layer

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. Examples include NFS, NetBios names, RPC, SQL.

Presentation Layer

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. Examples include encryption, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI.

Application Layer

This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Examples include WWW browsers, NFS, SNMP, Telnet, HTTP, FTP

Recommended Reading: *View Webopedia's The 7 Layers of the OSI Model study guide for in-depth descriptions and diagrams.*

THE TCP/IP MODEL

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.