UNIT 3. NETWORKS

I. Make sure that you know the following words:

Direct connection, include hosts, personal computers, differ in, to carry signals, transmission medium, communication protocols, digital audio, printers, fax machines, use of email, to the destination, instant messaging, chat rooms, video telephone calls, video conferencing, service attack, control information.

II. Learn the following terms:

- **to exchange data** — обмениваться информацией
- **data link** — канал передачи данных
- **wireless medium** — беспроводной носитель данных
- **network node** — главный узел
- **shared use of applications** — совместное использование приложений
- **to organize network traffic** — организовывать сетевой трафик
- **application-specific communications protocol** — специализированный протокол связи
- **point-to-point telecommunication link** — канал связи «точка-точка»
- **packet switched network** — сеть с пакетной коммутацией
- **bandwidth of the transmission medium** — полоса пропускания передающей среды
- **network address** — сетевой адрес
- **error detection code** — код с обнаружением ошибок
- **to deliver user data** — оставлять сообщения, содержащие информацию для пользователя
- **packet header** — заголовок пакета
- **trailer** — трейлер — запись с контрольной суммой в конце массива данных
- **shared storage device** — совместно используемое запоминающее устройство
- **to accomplish a task** — выполнить задание
- **computer cracker** — взломщик компьютерных систем, злоумышленник

III. Read and translate the text:

A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices exchange data with each other using a data link. The connections 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 can be 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 differ in the transmission medium used to carry their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent.

Computer networks support an enormous number of applications such as access to the World Wide Web, video, digital audio, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications as well as many others. In most cases, application-specific communications protocols are layered (i.e. carried as payload) over other more general communications protocols.

Computer communication links that do not support packets, such as traditional point-to-point telecommunication links, simply transmit data as a bit stream. However, most information in computer networks is carried in packets. A network packet is a formatted unit of data (a list of bits or bytes, usually a few tens of bytes to a few kilobytes long) carried by a packet-switched network.

In packet networks, the data is formatted into packets that are sent through the network to their destination. Once the packets arrive they are reassembled into their original message. With packets, the bandwidth of the transmission medium can be better shared among users than if the network were circuit switched. When one user is not sending packets, the link can be filled with packets from others users, and so the cost can be shared, with relatively little interference, provided the link isn't overused.

Packets consist of two kinds of data: control information, and user data (payload). The control information provides data the network needs to deliver the user data, for example: source and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers, with payload data in between.

Often the route a packet needs to take through a network is not immediately available. In that case the packet is queued and waits until a link is free.

A computer network facilitates interpersonal communications allowing users to communicate efficiently and easily via various means: email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing. Providing access to information on shared storage devices is an important feature of many networks. A network allows sharing of files, data, and other types of information giving authorized users the ability to access information stored on other computers on the network. A network 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. 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 via a denial of service attack.

IV. Answer the following questions:

1. What does computer network allow computers to do?
2. What devices exchange data with each other using a data link?
3. How are connections between nodes established?
4. What computer devices are called network nodes?
5. What devices do nodes include?
6. How do computer networks differ in?
7. What applications do computer networks support?
8. How is most information in computer networks carried?
9. What is a network packet?
10. What kinds of data do packets consist of?
11. How does computer network allow users to communicate via various means?
12. What is an important feature of many networks?
13. Who may a computer network be used by to deploy computer viruses or computer worms?

V. Retell the text briefly using the new words and expressions from ex. II.

VI. Fill in the gaps with the words given below. Use the dictionary if necessary.

Future Initiatives

a) media, b) to evolve, c) to outsource, d) applications, e) YouTube,
f) efficiently, g) "the cloud", h) consumption, i) functions, j) powerful

Network software ... (1) including Twitter and ... (2) have been rapidly replacing traditional ... (3) as a source for news, information, training and entertainment. As the Internet continues to grow as the primary network platform, the role of network software will continue ... (4). A trend toward "cloud-based computing" seeks to ... (5) network and application management from the corporate premises to data centers. Traditional network software ... (6) including application hosting, communication, administration and backups will be outsourced to ... (7) where they can be performed more ... (8). Network software platforms are becoming more ... (9) targeting new objectives to reduce the number of servers, cooling requirements and power ... (10) requirements of corporations and data centers. This concept of "Green I/T" is a new and evolving purpose of network software technologies.

Grammar revision: Relative clauses with a participle

VII. Rewrite each of these sentences like this:

1. A gateway is an interface (enable) dissimilar networks to communicate.
2. A bridge is a hardware and software combination (use) to connect the same type of networks.
3. A backbone is a network transmission path (handle) major data traffic.
4. A router is a special computer (direct) messages when several networks are linked.
5. A network is a number of computers and peripherals (link) together.
6. A LAN is a network (connect) computers over a small distance such as within a company.
7. A server is a powerful computer (store) many programs (share) by all the clients in the network.
8. A client is a network computer (use) for accessing a service on a server.
9. A thin client is a simple computer (comprise) a processor and memory, display, keyboard, mouse and hard drives only.
10. A hub is an electronic device (connect) all the data cabling in a network.

VIII. Link these statements using a relative clause with a participle.

1. a) The technology is here today.
   b) It is needed to set up a home network.
2. a) You only need one network printer.
   b) It is connected to the server.
3. a) Her house has a network.
   b) It allows basic file-sharing and multi-player gaming.
4. a) There is a line receiver in the living room.
   b) It delivers home entertainment audio to speakers.
5. a) Eve has designed a site.
   b) It is dedicated to dance.
6. a) She has built-in links.
   b) They connect her site to other dance sites.
7. a) She created the site using a program called Netscape Composer.
   b) It is contained in Netscape Communicator.
8. a) At the center of France Telecom’s home of tomorrow is a network.
   b) It is accessed through a Palm Pilot-style control pad.
9. a) The network can simulate the owner’s presence.
   b) This makes sure vital tasks are carried out in her absence.
10. a) The house has an electronic door-keeper.
    b) It is programmed to recognize you.
    c) This gives access to family only.

IX. Look through the text. Make a short summary of it:

Communications protocols

A communications protocol is a set of rules for exchanging information over network links. In a protocol stack (also see the OSI model), each protocol leverages the services of the protocol below it. An important example of a protocol stack is HTTP (the World Wide Web protocol) running over TCP over IP (the Internet protocols) over IEEE 802.11 (the Wi-Fi protocol). This stack is used between the wireless router and the home user's personal computer when the user is surfing the web.

Whilst the use of protocol layering is today ubiquitous across the field of computer networking, it has been historically criticized by many researchers for two principal reasons. Firstly, abstracting the protocol stack in this way may cause a higher layer to duplicate functionality of a lower layer, a prime example being error recovery on both a per-link basis and an end-to-end basis. Secondly, it is common that a protocol implementation at one layer may require data, state or addressing information that is only present at another layer, thus defeating the point of separating the layers in the first place. For example, TCP uses the ECN field in the IPv4 header as an indication of congestion; IP is a network layer protocol whereas TCP is a transport layer protocol. Communication protocols have various characteristics. They may be connection-oriented or connectionless, they may use circuit mode or packet switching, and they may use hierarchical addressing or flat addressing.

There are many communication protocols, a few of which are described below.

The complete IEEE 802 protocol suite provides a diverse set of networking capabilities. The protocols have a flat addressing scheme. They operate mostly at levels 1 and 2 of the OSI model.

For example, MAC bridging (IEEE 802.1D) deals with the routing of Ethernet packets using a Spanning Tree Protocol. IEEE 802.1Q describes VLANs, and IEEE 802.1X defines a port-based Network Access Control protocol, which forms the basis for the authentication mechanisms used in VLANs (but it is also found in WLANs) — it is what the home user sees when the user has to enter a "wireless access key".

Ethernet, sometimes simply called LAN, is a family of protocols used in wired LANs, described by a set of standards together called IEEE 802.3 published by the Institute of Electrical and Electronics Engineers.

Wireless LAN, also widely known as WLAN or WiFi, is probably the most well-known member of the IEEE 802 protocol family for home users today. It is standardized by IEEE 802.11 and shares many properties with wired Ethernet. The Internet Protocol Suite, also called TCP/IP, is the foundation of all modern networking. It offers connection-less as well as connection-oriented services over an inherently unreliable network traversed by data-gram transmission at the Internet protocol (IP) level. At its core, the protocol suite defines the addressing, identification, and routing specifications for Internet Protocol Version 4 (IPv4) and for IPv6, the next generation of the protocol with a much enlarged addressing capability.

Synchronous optical networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers. They were originally designed to transport circuit mode communications from a variety of different sources, primarily to support real-time, uncompressed, circuit-switched voice encoded in PCM (Pulse-Code Modulation) format. However, due to its protocol neutrality and transport-oriented features, SONET/SDH also was the obvious choice for transporting Asynchronous Transfer Mode (ATM) frames.

Asynchronous Transfer Mode (ATM) is a switching technique for telecommunication networks. It uses asynchronous time-division multiplexing and encodes data into small, fixed-sized cells. This differs from other protocols such as the Internet Protocol Suite or Ethernet that use variable sized packets or frames. ATM has similarity with both circuit and packet switched networking. This makes it a good choice for a network that must handle both traditional high-throughput data traffic, and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins.

While the role of ATM is diminishing in favor of next-generation networks, it sill plays a role in the last mile, which is the connection between an Internet service provider and the home user.

X. Translate the text in written form:

Views of networks

Users and network administrators typically have different views of their networks. Users can share printers and some servers from a workgroup, which usually means they are in the same geographic location and are on the same LAN, whereas a Network Administrator is responsible to keep that network up and running. A community of interest has less of a connection of being in a local area, and should be thought of as a set of arbitrarily located users who share a set of servers, and possibly also communicate via peer-to-peer technologies.

Network administrators can see networks from both physical and logical perspectives. The physical perspective involves geographic locations, physical cabling, and the network elements (e.g., routers, bridges and application layer gateways) that interconnect via the transmission media. Logical networks, called, in the TCP/IP architecture, subnets, map onto one or more transmission media. For example, a common practice in a campus of buildings is to make a set of LAN cables in each building appear to be a common subnet, using virtual LAN (VLAN) technology.

Both users and administrators are aware, to varying extents, of the trust and scope characteristics of a network. Again using TCP/IP architectural terminology, an intranet is a community of interest under private administration usually by an enterprise, and is only accessible by authorized users (e.g. employees). Intranets do not have to be connected to the Internet, but generally have a limited connection. An extranet is an extension of an intranet that allows secure communications to users outside of the intranet (e.g. business partners, customers).

Unofficially, the Internet is the set of users, enterprises, and content providers that are interconnected by Internet Service Providers (ISP). From an engineering viewpoint, the Internet is the set of subnets, and aggregates of subnets, which share the registered IP address space and exchange information about the reachability of those IP addresses using the Border Gateway Protocol. Typically, the human-readable names of servers are translated to IP addresses, transparently to users, via the directory function of the Domain Name System (DNS).

Over the Internet, there can be business-to-business (B2B), business-to-consumer (B2C) and consumer-to-consumer (C2C) communications. When money or sensitive information is exchanged, the communications are apt to be protected by some form of communications security mechanism. Intranets and extranets can be securely superimposed onto the Internet, without any access by general Internet users and administrators, using secure Virtual Private Network (VPN) technology.