MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL TECHNICAL UNIVERSITY

"KHARKIV POLYTECHNICAL INSTITUTE"

DEPARTMENT OF SOFT ENGINEERING AND INFORMATION TECHNOLOGY OF MANAGEMENT

Project work

On subject: «Computer network»

Done by

Student of the group CS-36a

Bodnia Yevhen

Checked out:

Tarasova Anna

KHARKIV 2018

**Table of contents**

[**Introduction.**…………………………………………………………………..…...…](#_Toc500926339)3

[**1 Text**](#_Toc500926341)……………………………………………………………………………….…4

Properties……………………………………………………………………..…..….4

Network packet………………………………………………………………...….…4

Network topology………………………………………….……………………...…5

Communication protocols………………………………………….…………….....11

Geographic scale…………………………………………………….…………..….13

Routing………………………………………………………………………...……16

Network performance…………………………………………………………....….17

[**2 List of vocabulary**](#_Toc500926344)…………………………………………………………………19

[**3 List of the questions to the text**](#_Toc500926353)…………………………………………………...22

[**4**](#_Toc500926353) **References**………………………………………………………………………….24

**Introduction**

A computer network, or data network, is a digital telecommunications network which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections between nodes (data links.) These data links are established over cable media such as wires or optic cables, or wireless media such as Wi-Fi.

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. In most cases, application-specific communications protocols are layered (i.e. carried as payload) over other more general communications protocols. This formidable collection of information technology requires skilled network management to keep it all running reliably.

Computer networks support an enormous number of applications and services such as access to the World Wide Web, digital 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. Computer networks differ in the transmission medium used to carry their signals, communications protocols to organize network traffic, the network's size, topology, traffic control mechanism and organizational intent. The best-known computer network is the Internet.

**Properties**

Computer networking may be considered a branch of electrical engineering, electronics engineering, telecommunications, computer science, information technology or computer engineering, since it relies upon the theoretical and practical application of the related disciplines.

A computer network facilitates interpersonal communications allowing users to communicate efficiently and easily via various means: email, instant messaging, online chat, telephone, video telephone calls, and video conferencing. 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 or use of a shared storage device. 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. Distributed computing uses computing resources across a network to accomplish tasks.

A computer network may be used by security hackers 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.

**Network packet**

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. Packets are sent through the network to their destination. Once the packets arrive they are reassembled into their original message.

Packets consist of two kinds of data: control information, and user data. 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.

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 other users, and so the cost can be shared, with relatively little interference, provided the link isn't overused. 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.

**Network topology**

The physical layout of a network is usually less important than the topology that connects network nodes. Most diagrams that describe a physical network are therefore topological, rather than geographic. The symbols on these diagrams usually denote network links and network nodes.

**Network links**

The transmission media used to link devices to form a computer network include electrical cable, optical fiber, and radio waves. In the OSI model, these are defined at layers 1 and 2 — the physical layer and the data link layer.

A widely adopted family of transmission media used in local area network (LAN) technology is collectively known as Ethernet. The media and protocol standards that enable communication between networked devices over Ethernet are defined by IEEE 802.3. Ethernet transmits data over both copper and fiber cables. Wireless LAN standards use radio waves, others use infrared signals as a transmission medium. Power line communication uses a building's power cabling to transmit data.

**Wired technologies**

The orders of the following wired technologies are, roughly, from slowest to fastest transmission speed.

* Coaxial cable is widely used for cable television systems, office buildings, and other work-sites for local area networks. The cables consist of copper or aluminum wire surrounded by an insulating layer, which itself is surrounded by a conductive layer. The insulation helps minimize interference and distortion. Transmission speed ranges from 200 million bits per second to more than 500 million bits per second.
* ITU-T G.hn technology uses existing home wiring (coaxial cable, phone lines and power lines) to create a high-speed (up to 1 Gigabit/s) local area network
* Twisted pair wire is the most widely used medium for all telecommunication. Twisted-pair cabling consist of copper wires that are twisted into pairs. Ordinary telephone wires consist of two insulated copper wires twisted into pairs. Computer network cabling (wired Ethernet as defined by IEEE 802.3) consists of 4 pairs of copper cabling that can be utilized for both voice and data transmission. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed ranges from 2 million bits per second to 10 billion bits per second. Twisted pair cabling comes in two forms: unshielded twisted pair (UTP) and shielded twisted-pair (STP). Each form comes in several category ratings, designed for use in various scenarios.
* An optical fiber is a glass fiber. It carries pulses of light that represent data. Some advantages of optical fibers over metal wires are very low transmission loss and immunity from electrical interference. Optical fibers can simultaneously carry multiple wavelengths of light, which greatly increases the rate that data can be sent, and helps enable data rates of up to trillions of bits per second. Optic fibers can be used for long runs of cable carrying very high data rates, and are used for undersea cables to interconnect continents.

Price is a main factor distinguishing wired- and wireless-technology options in a business. Wireless options command a price premium that can make purchasing wired computers, printers and other devices a financial benefit. Before making the decision to purchase hard-wired technology products, a review of the restrictions and limitations of the selections is necessary.

**Wireless technologies**

* Terrestrial microwave – Terrestrial microwave communication uses Earth-based transmitters and receivers resembling satellite dishes. Terrestrial microwaves are in the low gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 48 km (30 mi) apart.
* Communications satellites – Satellites communicate via microwave radio waves, which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically in geosynchronous orbit 35,400 km (22,000 mi) above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.
* Cellular and PCS systems use several radio communications technologies. The systems divide the region covered into multiple geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area.
* Radio and spread spectrum technologies – Wireless local area networks use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area.
* Free-space optical communication uses visible or invisible light for communications. In most cases, line-of-sight propagation is used, which limits the physical positioning of communicating devices.

**Network nodes**

Apart from any physical transmission media there may be, networks comprise additional basic system building blocks, such as network interface controllers (NICs), repeaters, hubs, bridges, switches, routers, modems, and firewalls. Any particular piece of equipment will frequently contain multiple building blocks and perform multiple functions.

**Network interfaces**

A network interface controller (NIC) is computer hardware that provides a computer with the ability to access the transmission media, and has the ability to process low-level network information. For example, the NIC may have a connector for accepting a cable, or an aerial for wireless transmission and reception, and the associated circuitry.

The NIC responds to traffic addressed to a network address for either the NIC or the computer as a whole.

In Ethernet networks, each network interface controller has a unique Media Access Control (MAC) address—usually stored in the controller's permanent memory. To avoid address conflicts between network devices, the Institute of Electrical and Electronics Engineers (IEEE) maintains and administers MAC address uniqueness. The size of an Ethernet MAC address is six octets. The three most significant octets are reserved to identify NIC manufacturers. These manufacturers, using only their assigned prefixes, uniquely assign the three least-significant octets of every Ethernet interface they produce.

**Repeaters and hubs**

A repeater is an electronic device that receives a network signal, cleans it of unnecessary noise and regenerates it. The signal is retransmitted at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable that runs longer than 100 meters. With fiber optics, repeaters can be tens or even hundreds of kilometers apart.

A repeater with multiple ports is known as an Ethernet hub. Repeaters work on the physical layer of the OSI model. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay that affects network performance and may affect proper function. As a result, many network architectures limit the number of repeaters that can be used in a row, e.g., the Ethernet 5-4-3 rule.

Hubs and repeaters in LANs have been mostly obsoleted by modern switches.

**Bridges**

A network bridge connects and filters traffic between two network segments at the data link layer (layer 2) of the OSI model to form a single network. This breaks the network's collision domain but maintains a unified broadcast domain. Network segmentation breaks down a large, congested network into an aggregation of smaller, more efficient networks.

Bridges come in three basic types:

* Local bridges: Directly connect LANs
* Remote bridges: Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers.
* Wireless bridges: Can be used to join LANs or connect remote devices to LANs.

**Switches**

A network switch is a device that forwards and filters OSI layer 2 datagrams (frames) between ports based on the destination MAC address in each frame. A switch is distinct from a hub in that it only forwards the frames to the physical ports involved in the communication rather than all ports connected. It can be thought of as a multi-port bridge. It learns to associate physical ports to MAC addresses by examining the source addresses of received frames. If an unknown destination is targeted, the switch broadcasts to all ports but the source. Switches normally have numerous ports, facilitating a star topology for devices, and cascading additional switches.

Multi-layer switches are capable of routing based on layer 3 addressing or additional logical levels. The term switch is often used loosely to include devices such as routers and bridges, as well as devices that may distribute traffic based on load or based on application content.

**Routers**

A router is an internetworking device that forwards packets between networks by processing the routing information included in the packet or datagram (Internet protocol information from layer 3). The routing information is often processed in conjunction with the routing table (or forwarding table). A router uses its routing table to determine where to forward packets. A destination in a routing table can include a "null" interface, also known as the "black hole" interface because data can go into it, however, no further processing is done for said data, i.e. the packets are dropped.

**Modems**

Modems are used to connect network nodes via wire not originally designed for digital network traffic, or for wireless. To do this one or more carrier signals are modulated by the digital signal to produce an analog signal that can be tailored to give the required properties for transmission. Modems are commonly used for telephone lines, using a Digital Subscriber Line technology.

**Firewalls**

A firewall is a network device for controlling network security and access rules. Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in cyber attacks.

**Network structure**

Network topology is the layout or organizational hierarchy of interconnected nodes of a computer network. Different network topologies can affect throughput, but reliability is often more critical. With many technologies, such as bus networks, a single failure can cause the network to fail entirely. In general the more interconnections there are, the more robust the network is; but the more expensive it is to install.

**Common layouts**

Common layouts are:

* A bus network: all nodes are connected to a common medium along this medium. This was the layout used in the original Ethernet, called 10BASE5 and 10BASE2.
* A star network: all nodes are connected to a special central node. This is the typical layout found in a Wireless LAN, where each wireless client connects to the central Wireless access point.
* A ring network: each node is connected to its left and right neighbour node, such that all nodes are connected and that each node can reach each other node by traversing nodes left- or rightwards. The Fiber Distributed Data Interface (FDDI) made use of such a topology.
* A mesh network: each node is connected to an arbitrary number of neighbours in such a way that there is at least one traversal from any node to any other.
* A fully connected network: each node is connected to every other node in the network.
* A tree network: nodes are arranged hierarchically.

**Overlay network**

An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay network are connected by virtual or logical links. Each link corresponds to a path, perhaps through many physical links, in the underlying network. The topology of the overlay network may (and often does) differ from that of the underlying one. For example, many peer-to-peer networks are overlay networks. They are organized as nodes of a virtual system of links that run on top of the Internet.

Overlay networks have been around since the invention of networking when computer systems were connected over telephone lines using modems, before any data network existed.

The most striking example of an overlay network is the Internet itself. The Internet itself was initially built as an overlay on the telephone network. Even today, each Internet node can communicate with virtually any other through an underlying mesh of sub-networks of wildly different topologies and technologies. Address resolution and routing are the means that allow mapping of a fully connected IP overlay network to its underlying network.

Another example of an overlay network is a distributed hash table, which maps keys to nodes in the network. In this case, the underlying network is an IP network, and the overlay network is a table (actually a map) indexed by keys.

Overlay networks have also been proposed as a way to improve Internet routing, such as through quality of service guarantees to achieve higher-quality streaming media. Previous proposals such as IntServ, DiffServ, and IP Multicast have not seen wide acceptance largely because they require modification of all routers in the network. On the other hand, an overlay network can be incrementally deployed on end-hosts running the overlay protocol software, without cooperation from Internet service providers. The overlay network has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes that a message traverses before it reaches its destination.

**Communication protocols**

A communication protocol is a set of rules for exchanging information over a network. In a protocol stack, each protocol leverages the services of the protocol layer below it, until the lowest layer controls the hardware which sends information across the media. The use of protocol layering is today ubiquitous across the field of computer networking. 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.

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.

**IEEE 802**

IEEE 802 is a family of IEEE standards dealing with local area networks and metropolitan area networks. 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.

**Ethernet**

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**

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.

**Internet Protocol Suite**

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.

**Asynchronous Transfer Mode**

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.

**Geographic scale**

A network can be characterized by its physical capacity or its organizational purpose. Use of the network, including user authorization and access rights, differ accordingly.

**Nanoscale network**

A nanoscale communication network has key components implemented at the nanoscale including message carriers and leverages physical principles that differ from macroscale communication mechanisms. Nanoscale communication extends communication to very small sensors and actuators such as those found in biological systems and also tends to operate in environments that would be too harsh for classical communication.

**Personal area network**

A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles. A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters. A wired PAN is usually constructed with USB and FireWire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

**Local area network**

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as a home, school, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Wired LANs are most likely based on Ethernet technology. Newer standards such as ITU-T G.hn also provide a way to create a wired LAN using existing wiring, such as coaxial cables, telephone lines, and power lines.

The defining characteristics of a LAN, in contrast to a wide area network (WAN), include higher data transfer rates, limited geographic range, and lack of reliance on leased lines to provide connectivity. Current Ethernet or other IEEE 802.3 LAN technologies operate at data transfer rates up to 100 Gbit/s, standardized by IEEE in 2010. Currently, 400 Gbit/s Ethernet is being developed.

A LAN can be connected to a WAN using a router.

**Home area network**

A home area network (HAN) is a residential LAN used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a cable TV or digital subscriber line (DSL) provider.

**Storage area network**

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network by other devices. The cost and complexity of SANs dropped in the early 2000s to levels allowing wider adoption across both enterprise and small to medium-sized business environments.

**Campus area network**

A campus area network (CAN) is made up of an interconnection of LANs within a limited geographical area. The networking equipment (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling, etc.) are almost entirely owned by the campus tenant / owner (an enterprise, university, government, etc.).

For example, a university campus network is likely to link a variety of campus buildings to connect academic colleges or departments, the library, and student residence halls.

**Backbone network**

A backbone network is part of a computer network infrastructure that provides a path for the exchange of information between different LANs or sub-networks. A backbone can tie together diverse networks within the same building, across different buildings, or over a wide area.

For example, a large company might implement a backbone network to connect departments that are located around the world. The equipment that ties together the departmental networks constitutes the network backbone. When designing a network backbone, network performance and network congestion are critical factors to take into account. Normally, the backbone network's capacity is greater than that of the individual networks connected to it.

Another example of a backbone network is the Internet backbone, which is the set of wide area networks (WANs) and core routers that tie together all networks connected to the Internet.

**Metropolitan area network**

A Metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.

**Wide area network**

A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances. A WAN uses a communications channel that combines many types of media such as telephone lines, cables, and air waves. A WAN often makes use of transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

**Enterprise private network**

An enterprise private network is a network that a single organization builds to interconnect its office locations (e.g., production sites, head offices, remote offices, shops) so they can share computer resources.

**Virtual private network**

A virtual private network (VPN) is an overlay network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.

**Global area network**

A global area network (GAN) is a network used for supporting mobile across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off user communications from one local coverage area to the next. In IEEE Project 802, this involves a succession of terrestrial wireless LANs.

**Routing**

Routing is the process of selecting network paths to carry network traffic. Routing is performed for many kinds of networks, including circuit switching networks and packet switched networks.

In packet switched networks, routing directs packet forwarding through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing.

There are usually multiple routes that can be taken, and to choose between them, different elements can be considered to decide which routes get installed into the routing table, such as (sorted by priority):

* Prefix-Length: where longer subnet masks are preferred
* Metric: where a lower metric/cost is preferred
* Administrative distance: where a lower distance is preferred

Most routing algorithms use only one network path at a time. Multipath routing techniques enable the use of multiple alternative paths.

Routing, in a more narrow sense of the term, is often contrasted with bridging in its assumption that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within localized environments.

**Network performance and congestion**

Network congestion occurs when a link or node is carrying so much data that its quality of service deteriorates. Typical effects include queueing delay, packet loss or the blocking of new connections.

Network protocols that use aggressive retransmissions to compensate for packet loss tend to keep systems in a state of network congestion—even after the initial load is reduced to a level that would not normally induce network congestion. Thus, networks using these protocols can exhibit two stable states under the same level of load. The stable state with low throughput is known as congestive collapse.

Modern networks use congestion control, congestion avoidance and traffic control techniques to try to avoid congestion collapse. These include: exponential backoff in protocols such as 802.11's CSMA/CA and the original Ethernet, window reduction in TCP, and fair queueing in devices such as routers. Another method to avoid the negative effects of network congestion is implementing priority schemes, so that some packets are transmitted with higher priority than others. Priority schemes do not solve network congestion by themselves, but they help to alleviate the effects of congestion for some services. An example of this is 802.1p. A third method to avoid network congestion is the explicit allocation of network resources to specific flows. One example of this is the use of Contention-Free Transmission Opportunities (CFTXOPs) in the ITU-T G.hn standard, which provides high-speed (up to 1 Gbit/s) Local area networking over existing home wires (power lines, phone lines and coaxial cables).

For the Internet RFC 2914 addresses the subject of congestion control in detail.

**Network resilience**

Network resilience is "the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.”

**List of vocabulary**

|  |  |  |
| --- | --- | --- |
| Word | Transcription | Translation |
| ability | [əˈbɪlɪti ] | возможность |
| accomplish | [əˈkɒmplɪʃ ] | выполнять |
| adoption | [əˈdɒpʃ(ə)n ] | внедрение |
| affect | [əˈfɛkt ] | влиять |
| application | [ˌæplɪˈkeɪʃ(ə)n ] | применение |
| available | [əˈveɪləbl ] | доступный |
| bandwidth | [ˈbændwɪdθ ] | пропускная способность |
| benefit | [ˈbɛnɪfɪt ] | выгода |
| broadcast | [ˈbrɔːdkɑːst ] | широковещательный |
| challenge | [ˈʧælɪnʤ ] | проблема |
| common | [ˈkɒmən ] | общий |
| conductive | [kənˈdʌktɪv ] | проводящий |
| congestion | [kənˈʤɛsʧən ] | перегрузка |
| consider | [kənˈsɪdə] | рассматривать |
| dedicated | [ˈdɛdɪkeɪt ] | выделенный, преданный |
| delay | [dɪˈleɪ ] | задержка |
| delivery | [dɪˈlɪvəri ] | доставка |
| denial | [dɪˈnaɪəl ] | отказ |
| denote | [dɪˈnəʊt ] | обозначать |
| destination | [ˌdɛstɪˈneɪʃən ] | назначение |
| directly | [dɪˈrɛktli ] | напрямую |
| distribute | [dɪsˈtrɪbju(ː)t ] | распределять |
| diverse | [daɪˈvɜːs ] | разнообразный |
| efficiently | [ɪˈfɪʃəntli ] | продуктивно |
| entirely | [ɪnˈtaɪəli ] | полностью |
| establish | [ɪsˈtæblɪʃ ] | установить |
| exchange | [ɪksˈʧeɪnʤ ] | обмен |
| exist | [ɪgˈzɪst ] | существовать |
| explicit | [ɪksˈplɪsɪt ] | явно |
| facilitate | [fəˈsɪlɪteɪt ] | облегчать |
| feature | [ˈfiːʧə ] | признак |
| filled | [fɪld ] | заполненный |
| flat | [flæt ] | плоский |
| flow | [fləʊ ] | поток |
| formidable | [ˈfɔːmɪdəbl | огромный |
| forward | [ˈfɔːwəd ] | пересылать |
| foundation | [faʊnˈdeɪʃən ] | основа |
| handle | [ˈhændl ] | обрабатывать |
| harsh | [hɑːʃ ] | жесткий, суровый |
| immediately | [ɪˈmiːdiətli ] | сразу |
| increase | [ˈɪnkriːs ] | увеличение |
| infrared | [ˈɪnfrəˈrɛd ] | инфракрасный |
| instant | [ˈɪnstənt ] | мгновенный |
| interference | [ˌɪntəˈfɪərəns ] | помехи |
| layout | [ˈleɪaʊt ] | расположение, макет |
| maintain | [meɪnˈteɪn ] | поддерживать |
| mean | [miːn ] | средство |
| medium | [ˈmiːdiəm ] | среда |
| narrow | [ˈnærəʊ ] | узкий |
| node | [nəʊd ] | узел |
| obstruction | [əbˈstrʌkʃən ] | препятствие |
| occur | [əˈkɜː ] | происходить |
| originate | [əˈrɪʤɪneɪt ] | создавать |
| overuse | [ˌəʊvəˈjuːz ] | злоупотреблять |
| perform | [pəˈfɔːm ] | выполнять |
| performance | [pəˈfɔːməns ] | производительность |
| prevent | [prɪˈvɛnt ] | предотвращать |
| provide | [prəˈvaɪd ] | предоставлять |
| queue | [kjuː ] | очередь |
| rate | [reɪt ] | скорость |
| reassemble | [ˌriːəˈsɛmbl ] | собрать |
| receiver | [rɪˈsiːvə ] | приемник |
| reduce | [rɪˈdjuːs ] | уменьшать |
| relate | [rɪˈleɪt ] | иметь отношение |
| reliability | [rɪˌlaɪəˈbɪlɪti ] | надежность |
| reliable | [rɪˈlaɪəbl ] | надежный |
| rely | [rɪˈlaɪ ] | полагаться |
| remote | [rɪˈməʊt ] | удаленный |
| require | [rɪˈkwaɪə ] | требовать |
| resilience | [rɪˈzɪlɪəns] | устойчивость |
| suite | [swiːt ] | набор |
| surrounded | [səˈraʊndɪd ] | окруженный |
| tenant | [ˈtɛnənt ] | арендатор |
| terminate | [ˈtɜːmɪneɪt ] | ограничивать |
| therefore | [ˈðeəfɔː] | следовательно |
| transmit | [trænzˈmɪt ] | передавать |
| transmitter | [trænzˈmɪtə ] | передатчик |
| unique | [juːˈniːk ] | уникальный |
| variable | [ˈveərɪəbl ] | переменный |
| various | [ˈveərɪəs ] | различный |
| via | [ˈvaɪə] | с помощью |
| vital | [ˈvaɪtl ] | жизненно важный |
| widely | [ˈwaɪdli ] | широко |
| wildly | [ˈwaɪldli ] | совершенно |
| wire | [ˈwaɪə ] | провод |

**List of the questions to the text**

1. What is called a network node?
2. What is the purpose of the computer network?
3. What devices can be used in computer networks?
4. What is the most famous computer network for nowadays?
5. What are the functions of the network?
6. What resources does the network use?
7. How can ordinary users use a computer network?
8. Can there be a network hacked?
9. By what means can a network be hacked?
10. In what ways can a computer network protect itself from break-ins?
11. Do the communication links support a point-to-point packet?
12. How are the data transferred by communication links?
13. What is a network packet?
14. How are packets transmitted over the network?
15. What types of data are packets composed of?
16. How is bandwidth shared among users?
17. What are the elements of the network topology?
18. What are the physical media used for?
19. What are the layers of the OSI model protocols?
20. What is the meaning of LAN?
21. What do the media and protocol standards provides?
22. What kinds of waves use the wireless LAN standards?
23. What kinds of wired technology are you aware of?
24. What is a main factor distinguishing wired- and wireless-technology?
25. Are cellular systems the wireless technology?
26. Which factors gives slow two-way communication for exotic's technologies cases?
27. What is network interface controller?
28. Does the network interface controller have a unique media access control address in the Ethernet network?
29. How to avoid address conflicts between network devices?
30. How many octets does the MAC address consist of?
31. How many octets are reserved to identify NIC manufacturers?
32. What is repeater?
33. What is called a repeater with multiple ports?
34. At what layer of the OSI model do repeaters work?
35. What is the function of the network bridge?
36. At what level of the OSI model are network bridges used?
37. What are the main types of network bridges?
38. What is network switch?
39. Is it possible to treat the switch as a multiport bridge?
40. Is the router an internetworking device?
41. What information does the router handle?
42. What is the purpose of the routing table?
43. What is the main function of modems?
44. What are the main purposes of the firewall?
45. What is the common layouts of network structure?
46. What virtual computer network is built on top of another network?
47. What can be an example of an overlay network?
48. What services does the communication protocol use?
49. What characteristics can the communication protocol have?
50. What communication protocols exist?

**References**

1. [https://en.wikipedia.org/wiki/Computer\_network]
2. [https://www.techopedia.com/definition/25597/computer-network]
3. [https://study.com/academy/lesson/types-of-networks-lan-wan-wlan-man-san-pan-epn-vpn.html]
4. [https://www.lifewire.com/what-is-computer-networking-816249]

**Annotation**

The text is entitled “Computer network”. It contains definitions of the main stages of data transfer between computers. In computer networks, [computing devices](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Computing_device&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhg1Xz7zJf-aHBucmtzWJjmiMq7OXw) [exchange data](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Data_transmission&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhj7pBYUOsiQSTvPOXCcS_OnpMocPg) with each other using connections between nodes. These data links are established over [cable media](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Networking_cables&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhhBvnvtAwwuby1zhiBRFtg8AG1--g) such as wires or optic cables, or [wireless media](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Wireless_network&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhixWGHgQZO4mHbWJAygcZKm4aOXYw) such as [Wi-Fi](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/WiFi&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhjHFffQZi6l4t0uwFQujBaHsy_SaQ). Computer networks support an enormous number of [applications](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Application_software&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhg84V5Mo5P2p4c3ch_yPnixMSnkEA) and [services](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Network_service&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhhSY6eh05OfakGz4WTRghFMu_QvPQ) such as access to the [World Wide Web](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/World_Wide_Web&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhhHYGm3lVCybz6-uLQXMoXXQ2DOFA) , [digital video](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Digital_video&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhjH8hETQvodSsHJV1amhZDRwVAKvw) , [digital audio](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Digital_audio&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhgkWh6zlFqyXMbUfmeHqMLrsr-rOw) , shared use of [application and storage servers](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/File_server&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhhDRI_9GnCYUqv7e63WvMGPH2IuuA) , printers, and [fax machines](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Fax&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhgeP1U8raXa6NDzlEMgszMKHHfcPw) , and use of [email](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Email&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhgb5nL_qQcsKlLAFBvcan9HPMt8SQ) and [instant messaging](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Instant_messaging&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhjrcd4PVBRZuISRStBRj5NRXX9Jfg) applications as well as many others. A computer network facilitates interpersonal communications allowing users to communicate efficiently and easily via various means: email, instant messaging, [online chat](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&prev=search&rurl=translate.google.com.ua&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Online_chat&xid=17259,15700002,15700023,15700124,15700149,15700168,15700173,15700186,15700201&usg=ALkJrhjwXFbX-dFSWIwGuIcna5eLn2182Q) , telephone, video telephone calls, and video conferencing.

It is told about various topologies of networks and how they are arranged. The text describes the development of wired and wireless technologies and where we can use such data transmission lines. Investigating this information, we can improve knowledge about computer networks making a conclusion about where they can be used, and what we can expect from their development in the future.