# KAPITEL 2 / *CHAPTER 2* [2]
# BUILDING CORPORATE NETWORKS FOR FOOD INDUSTRY ENTERPRISES

**DOI: 10.30890/2709-2313.2023-22-01-031**

## Introduction

Computer networks are an important part of modern information technologies. Today, most businesses use networks to deliver information to employees, suppliers, and customers. A computer network is a group of two or more computer systems connected by communication channels to exchange data and information. Modern networks often connect thousands of users and can carry audio and video as well as data. Networks include clients and servers. A client is a program that runs on a personal computer or workstation. It depends on a server that manages network resources or performs special tasks such as storing files, managing one or more printers, or handling database queries. Any network user can access the server's capabilities. By simplifying and accelerating the exchange of information, networks have created new ways of working and improving productivity. They provide a more efficient use of resources, allowing communication and collaboration across distance and time. When exchanging files, all employees, regardless of location, have access to the same information. Shared databases also eliminate duplication of effort. Employees at different facilities can "screen share" computer files, working with data as if they were in the same room. Their computers are connected by telephone or cable lines, they all see the same thing on their displays, and each can make changes that the other participants see. Employees can also use video conferencing networks. Networks allow companies to run enterprise software, large programs with built-in modules that manage all of the corporation's internal operations. Enterprise resource planning systems work in networks. Typical subsystems include finance, human resources, engineering, sales and order distribution, and order and procurement management. These modules work independently of each other and then automatically share information, creating an enterprise-wide system that includes current delivery dates, inventory status, quality control and other critical information. Let's now look at the main types of networks that companies use to transfer data – LANs and WANs – and popular networking applications such as intranets and virtual private networks.

[2]***Authors:*** *Lemeshko Andriy Viktorovych, Antonenko Artem Vasylovych, Golubenko Oleksandr Ivanovych Tonkykh Oleksii Grygorovych, Balvak Andrii Anatolijovych, Tsvyk Oleksandr Serhiyovych, Korotkov Serhii Stanislavovych, Ivanov Oleksandr Pavlovich, Prysiazhniuk Vladyslav Dmytrovych Petrenko Vladyslav Valentinovych, Drahun Vladyslav Petrovych, Demchenko Maksym Ruslanovych Hafanovych Vladyslav Oleksandrovych*

## 2.1. Corporate networks for food industry enterprises

Information systems are necessary for organizations to support their core and support activities with information and communications. Therefore, before discussing the structure and function of information systems, it is necessary to clarify the purpose and goals of the organization itself in order to understand what needs to be automated.A computer network consists of 1 communication line connecting several computers in a limited range (for example, in a house in the same room or nearby). Today, most computer networks are based on a client/server computer model , which is a local network located in the same office building. A network connection consists of 2 computers for communication and a path between them. It is also possible to build a network using wireless technology, but this is not common. In the client / server model, network communication is divided into 2 areas: on the client side and on the server side. By definition, the client requests information and services from the server. The server responds to the client's request. In the client / server model, in many cases each party can act as both a server and a client. When building a computer network, it is necessary to select various components that determine the software and hardware used to form a corporate network. The computer network is an integral part of the modern business infrastructure, and the corporate network is only one of the applications used there, and therefore should not be the only factor that determines the choice of network components. The components required for an intranet must be added without significant changes to the architecture of the existing network.The scalability of your network determines how your enterprise manages your network. There are several management methods. A local area network is divided into 2 types: a peer-to-peer network and a hierarchical (multi-level) network, depending on how it is managed.

Peer-to-peer networks In a peer-to-peer network, all computers are equal, there is no hierarchy between computers, and there is no dedicated server. As a rule, each computer serves as both a client and a server at the same time. In other words, there are no individual computers responsible for managing the entire network. Each user decides what data on the computer to publish on the network. A peer-to-peer network is also called a workgroup. A working group is a small group, and a peer-to-peer network usually contains no more than 30 computers. A peer-to-peer network is relatively simple. Since each computer is both a client and a server, there is no need for such a powerful central server as is required for a more complex network. Peer-to-peer networks are usually cheaper than server networks, but require more powerful (and more expensive) computers. Peer-to-peer networks typically have lower performance and security requirements for network software than dedicated server

networks.

Hierarchical Networks A hierarchical network has 1 or more servers that store information shared by different users. To improve storage reliability, the server makes 2 disks redundant in parallel, allowing one of them to be automatically replaced in the event of a failure. File server in this case, the server hosts common files or (and) common programs. An example of a file server application is the hosting of MS Office applications. In this case, only a small part of these programs (clients) is hosted on the workstation and few resources are required. Programs that allow such modes of operation are called network programs. Database server. In this case, the database (Consultant Plus, Guarantor, bank accounts, etc.) is placed on the server. The database on the server can be filled with information from different workstations or (...) publish information on request from workstations. Hierarchical network clients can use Windows XP, Windows Vista, and Windows 7 operating systems, but the server requires a special server version of the operating system.

Corporate networks have a rather complex structure that uses various types of communications, communication protocols, methods of connecting resources, etc. All data network equipment is broadly divided into peripheral equipment for connecting endpoints to the network and backbone or core equipment responsible for the main functions of the network (linking, routing, etc.). There is no clear distinction between these types, and the same device can be used for different purposes or in combination with each other. It should be noted that trunk equipment usually has higher requirements for reliability, performance, number of ports, and even scalability. Peripheral devices are an integral part of a corporate network. The functionality of the trunk node can be intercepted by the global data network to which the resource is connected. Typically, trunk nodes will appear as part of a corporate network only if you use a dedicated line or create your own access node. Peripheral devices in corporate networks are also divided into two types according to their functions. First, routers are responsible for connecting similar local area networks (usually IP or IPX) to the global data network. In networks based on IP and IPX, especially on the Internet, routers are also used as backbone devices to connect different communication channels and protocols. Routers include a single computer-based device and software and a special communications adapter. The second is the widespread use of gateway peripherals that implement interfaces that work in different types of networks. A full-featured gateway should always provide the software interface required by your application, so it is always part of the hardware and software. All major networking vendors offer a suite of products that provide enterprise networking capabilities for IT administrators. It includes various sets of hardware (hubs, routers, switches) focused on creating systems

for the latest communication technologies, such as high-speed Ethernet, asynchronous automated teller machine (ATM) and virtual networks... We aim to increase throughput by implementing these technologies in large-scale information systems.

Communication channels are the means by which people in an organization communicate and interact with each other. Without the right channels of communication, it becomes extremely difficult to align employees with business goals, bridge disparities, and innovate in the workplace. In addition, the communication channels you use in your workplace directly affect the quality of employee service, employee engagement, and your ability to help your employees improve their productivity, leadership, and communication skills.

The fact is that with the transition to remote work, communication in the workplace has become more difficult in the last few weeks. As a result, many employers are struggling to understand how information flows through different channels, which results in communication becoming much more difficult. It's no surprise that using the wrong channels for workplace collaboration, peer-to-peer communication, and top-down communication can affect a company's success. Considering all possible communication channels, we can divide them into two main groups.

Communication channels for formality. There are three different channels of communication based on formality: formal, informal and informal. Formal communication involves sharing information such as the organization's goals, policies, and procedures. Some of the more common examples of formal communication include company business plans, strategy, goals, annual reports, agreements, company-wide communications, workplace safety rules and procedures, board presentations, etc.

Informal communication channels are also used to transmit official business messages, but in a more casual way. Some examples of informal communication include conversations at work about various problems that team members may have, conversations over lunch, and ongoing collaboration between team members. Unofficial channels of communication. In addition to official communication channels, there is also an informal way of communication that is quite common in the workplace. Informal communication includes communication between employees outside the work environment on topics not related to work. Communication channels by means. In addition to formality, communication channels can be divided by means. In other words, the way and tools employees use to communicate with each other.

Let's look at the 3 main means of communication in the workplace. Digital communication channels. Electronic communication includes various online tools that employees use to stay in touch with each other and keep abreast of company news and

updates. Today, digital communication channels are the most popular and most frequently used channels in the workplace. Some examples include email, internal communication platforms, employee collaboration software, and intranets.

Face-to-face communication. Although electronic means of communication in the workplace are gaining ground, face-to-face communication is extremely important. This tool is much more personal, and it has more of a human touch. Related: Interpersonal Communication: Definition, Importance, and Required Skills Written communication. This type of communication is almost completely dead in organizations. However, written communication is still necessary when important policies, letters, memos, manuals, notices and announcements are communicated to employees.

## 2.2. Network equipment for food industry enterprises

Network equipment is used to combine, divide, switch, amplify, or route packets of information through a computer or telecommunications network. This product area includes hubs, switches, routers, bridges, gateways, multiplexers, receivers and firewalls. In addition to device type, network equipment is defined by protocol (eg Ethernet) and port or interface type (eg T1).

Network equipment connects devices so that data can be exchanged between them. The layout or topology of these connected devices defines the design or structure of the network. Common topologies for computer networks include bus, ring, star, tree, and mesh. Hybrid topologies are also used. In wireless networks, devices exchange data using radio waves and require a physical connection. Wired networks use cables. These cables are equipped with connectors of a specific port or interface type. For example, the connection unit interface (AUI) cables are equipped with 15-pin connectors that connect to a 15-pin socket on network receivers. Computer networks process data according to protocols, which are the fundamental mechanisms of network interaction. Network protocols define the software attributes of data transmission, including the structure of packets and the information they contain. Depending on the type of network, packets may be called blocks, cells, frames, or segments. Network protocols may also dictate some or all of the performance characteristics of the network equipment on which they run.

There are different types of network devices used in a computer network, including the following: network hub, rule switch, modem, network router, bridge, repeater, network hub.

A network hub is a type of network device in a computer network that is used to communicate with different network hosts as well as transfer data. Data transfer in a computer network can be carried out as packets. Whenever data processing can be performed from the host to the network hub, data can be transmitted to all connected ports. Likewise, all ports identify the data path, resulting in inefficiencies and losses. Because of this operation, the network hub can be so safe and reliable. Also, copying data packets to all ports will make the hub slower, which will use up the switch. Network hubs are divided into two types such as active hub and passive hub.

An active hub has its own power supply and these hubs are used to clean, amplify and transmit the signal over the network. It works as a switching center and repeater. Active hubs play a key role in increasing the distance between nodes.

The passive hub collects wiring from the power supply unit and various nodes of the active hub. These hubs transmit signals over the network without enhancing or cleaning them. These hubs are not suitable for increasing the distance between nodes like an active hub.

A network switch, like a hub, works at the local network level, and a switch is more intelligent than a hub. Because a hub is used to transmit data, while a switch is used to filter and forward data. So it's a smarter way to deal with data packets. Whenever a data packet is received from the interfaces in the switch, the data packet can be filtered and forwarded to the proposed receiver interface. For this reason, the switch maintains a table of addressable memory contents to store system configuration as well as memory. This table is also called FIB (Forwarding Information Base), otherwise Forwarding Table.

Modem is the most important network device and is used every day in our life. If we notice that the internet connection to the houses was provided by wire. the wire then carries internet data from one location to another. But every computer outputs digital or binary data in the form of zeros and ones. The full form of a modem is a modulator and a demodulator. Thus, it modulates and demodulates the signal between the computer and the telephone line because the computer generates digital data while the telephone line generates an analog signal.

A network router is a type of network device on a computer network that is used to route traffic from one network to another. These two networks can be private to a public network. For example, here the router is considered as a traffic police at an intersection, it directs heterogeneous network traffic in different directions.

A bridge in a computer network is used to connect two or more network segments. The main function of the bridge in the network architecture is storage, and even transfer of frames between different segments. Bridges use MAC (Media Access Control)

equipment to transmit frames.

They are also used to connect two physical LANs to a larger local LAN. In the OSI model, bridges operate at the link and physical layers to divide networks from larger to smaller networks, controlling the flow of data between them. In recent years, bridges have been replaced by switches to provide greater functionality.

The work of the repeater can be performed physically. The main function of this device is to reproduce the signal in the same network before the signal becomes weak, otherwise it is damaged. An important point to note about these devices is that they do not amplify the signal. Whenever the signal gets weak, they play it back with real strength. A repeater is a two-port device.

A gateway typically operates at the session and transport layers of the OSI model. Gateways offer conversion between network technologies such as OSI (Open System Interconnection) and TCP/IP. Because of this, they are connected to two or many autonomous networks, where each network has its own domain name service, routing algorithm, topology, protocols, and network administration and policy procedures. Gateways perform all the functions of routers. A router with additional conversion functions is actually a gateway, so the conversion between different network technologies is known as a protocol converter.

A brouter is also called a bridge router, and its main function is to combine the functions of a router, a bridge, and a router. It works either at the network layer or at the data link layer. When it works as a router, it is used to route network packets, while it works as a bridge; it is used to filter local network traffic.

Network equipment must be selected in accordance with the requirements of the designed network, taking into account such parameters as the amount of transmitted traffic, the possibility of expanding the network, equipment compatibility, as well as a number of other parameters. It is also necessary to take into account the type of equipment, in the case of a router or a switch, and its characteristics. The device must meet the requirements regarding the number of interfaces and their type, bandwidth, and supported protocols. We choose the type of device based on its position in the network, with the necessary characteristics, taking into account the manufacturer's recommendations.

Cisco offers a wide range of Gigabit switch routers, including the GSR1200 series, which we often recommend for developing and implementing new services while reducing overall capital requirements. It is a useful tool for an intelligent modular network. If you need scalability, consider options like the GSR1200, which can scale from 2.5 Gbps to nx 10 Gbps per slot. Carrier IP and MPLS networks are easy to maintain with this model.

The Cisco 3800 Series Integrated Services Routers are great for businesses and branch offices. Refurbished 3800 models can provide simultaneous T3/E3 leading speed for your wireless, data, security, video and voice networks. You also get reduced costs and deployment, as well as simple network management. The devices support up to 112 10/100 Mbps switch ports.

Juniper's MX Series routers (MX240, MX480, and MX960) offer high-density, high-bandwidth platforms that can run on multiple cores in peripherals and data centers, as well as on campuses. They are characterized by high network availability and are equipped with a high-quality broadband network gateway with multi-level switching and VPN support.

The Juniper T320/T640 router series is an end-of-life router series that provides Gigabit Ethernet, SONET/SDH and similar high-speed interfaces for large networks and their applications. It is designed with the needs of Internet service providers in mind and supports up to 64 gigabit ports. Maximum aggregate bandwidth starts at 160 Gbps in full-duplex mode and can be a smart choice for cost-effective and efficient expansion of your network.

Cisco offers many models of Layer 2 and Layer 3 switches. For brevity, this section highlights a few popular models used in campus, backbone, and data center environments.

The Cisco Catalyst 6500 family of switches are the most popular switches ever produced by Cisco. They can be found in various installations, not only in campuses, data centers and backbone networks, but also in service deployments, WANs, branch offices, etc. in both enterprise and service provider networks.

The Cisco Catalyst 4500 family of switches is an extremely popular modular switch used in many campus networks at the distribution level or in core networks of small and medium-sized networks. Collapsed kernel structures combine the kernel and distribution layers into a single domain. The Catalyst 4500 is one step below the Catalyst 6500, but supports a wide range of Layer 2 and Layer 3 features.

The Cisco Catalyst 4948G, 3750, and 3560 family of switches are popular switches used in campus networks for fixed-port scenarios, most commonly at the access layer.

The Cisco Catalyst 2000 family of switches are Layer 2-only switches that support few Layer 3 features in addition to Layer 3 routing. These features are often found at the access layer in campus networks.

The Nexus 7000 family of switches are Cisco's best switches for data centers. Product launch in 2008; Therefore, Nexus 7000 software does not yet support all Cisco IOS features.

The Nexus 5000 and 2000 family of switches are low-latency switches designed for deployment at the data center access layer. Today, these switches are only layer 2 switches, but support end-to-end switching for low latency. Nexus 5000 switches are designed for 10-Gigabit Ethernet applications and also support Fiber Channel over Ethernet (FCOE).

This router processes fewer packets. Instead, it is often used to provide other functions. The architecture of the Cisco 2900 family of integrated services routers is based on the architecture of the Cisco 2600 series of powerful multiservice access routers, offering additional built-in security features, significantly improved performance and expanded memory, as well as new high-density interfaces. Working under the management of Cisco IOS software, the Cisco 2900 series routers support the concept of a network with Cisco Self-Defending Network capabilities - thanks to improved security functions and management capabilities, such as hardware encryption acceleration, IPSecVPN support. Provided on all routers of the Cisco 2900 series, the intuitive control system with the Cisco Router and Security Device Manager (SDM) web interface greatly facilitates the management and configuration of the router.

An uninterruptible power supply (UPS) is a device that allows the computer to continue to operate for at least a short time when the incoming power is interrupted. As long as electricity is supplied, it also replenishes and maintains the energy storage. The more energy stored, the more power can be sustained, with practical limitations to be discussed later. The differences between UPS systems lie in the technology that allows them to do their job.

The three main types of uninterruptible power supplies - stand-alone UPS, on-line UPS and line-interactive UPS (Line-Interactive) are the most common uninterruptible power sources.

Uninterruptible power supplies of the Off-Line type. In the normal mode of operation of the Off-Line UPS, power is supplied from the filtered voltage of the primary network. But when the input voltage parameters go beyond the specified range, the device switches to battery mode, regardless of whether there is mains voltage or not. This imposes certain restrictions on the following devices:

Off-Line UPS are applicable only in networks with stable power quality; their disadvantage is poor protection against voltage drops and exceeding its permissible values, changes in the frequency and shape of the input voltage, as well as the impossibility of timely restoration of the battery capacity when frequently switching to battery operation; due to the wide distribution of voltage in the network, especially outside of large cities, the full use of Off-Line UPS is possible only together with an

additional automatic voltage regulator.

Uninterruptible power supplies On-Line type. In normal operation of On-Line UPS (they are also called double-conversion UPS), the mains voltage is rectified and then converted to DC voltage to charge the battery and power the output stage. When the mains voltage is sufficient, the output stage converts the direct voltage into a sinusoidal voltage of 220 V. When the mains voltage is lower, the lack of current is compensated by the battery, but if there is no voltage, the power is supplied only from the battery.

The quality of power supply and reliability of such a device is much higher compared to the previous type. But this device still has disadvantages: low efficiency compared to other types of UPS due to double conversion; high cost; relatively small battery life. Such UPSs are mainly used to support the operation of servers and routers in corporate networks.

Uninterruptible power supplies of the Line-Interactive type. Linear-interactive UPS combines the advantages and, as far as possible, minimizes the disadvantages of Off-Line and On-Line types of uninterruptible power sources. First, the built-in automatic voltage stabilizer of such a UPS provides high-quality power at high or low network voltage, and also protects the equipment from interference and voltage surges in the network. Secondly, when the input voltage parameters go beyond the operating range, as well as the absence of voltage for a short or long time, power is supplied from the battery (batteries), which ensures continuity of power. The non-zero switching time (4-10 ms) on the battery is a disadvantage of the linear-interactive UPS, but in most cases it is not critical for consumers.

UPS type Line-Interactive is divided into UPS with an approximate sine wave output (suitable only for devices with switching power supplies) and a more unified UPS with a correct sine wave shape, which can work with devices that are critical in the form of the input current (with transformers, motors, compressors, etc. ).

Regardless of the size of the premises or IT installation that requires uninterrupted power, it is important to consider the required power quality. The three UPS topologies stand-by, line-interactive, and line-interactive differ in the power quality they can provide and the power problems they can solve without resorting to battery power. Online - UPS, which are considered to provide the maximum level of power supply protection, also differ in their design. Modular UPSs, as a rule, do not contain transformers, and their high efficiency is achieved due to the use of complex power electronics. Monoblock UPS systems can be transformerless or transformer-based with a transformer built into the UPS and providing isolation (galvanic) between critical server loads and power sources. It is impossible to ignore the installation of a UPS

maintenance post. An uninterruptible power supply requires annual maintenance if the system is to operate when it is most needed. The alternative is to crash the system and rush to find and connect emergency uninterruptible power supplies to restore some of your servers and IT network.

In an enterprise, intranet users in departments A and B can communicate with each other and access the Internet. In a small campus network, the S2700 and S3700 switches are typically deployed as access switches (such as ACC1) at the access layer, and the S5700 and S6700 switches as core switches (such as CORE) at the access layer. base layer and AR routers as source routers (eg Router). Access switches are connected to the main switch via an Eth-Trunk for reliability. Each department is assigned a VLAN and services are transferred between departments at Layer 3 through the VLANIF interfaces of the CORE switch. The main switch functions as a DHCP server for allocating IP addresses to users on campus. DHCP snooping is configured on access switches to prevent intranet users from connecting to unauthorized routers to obtain IP addresses. The IPSG feature is configured to prevent intranet users from changing IP addresses.

## 2.3. Analysis of software for food industry enterprises

Enterprise Software means Software licensed by third parties used by the Seller both in the Business and in its other businesses, which is network software or monitoring software, accounting software, general software development software or software for management systems, general enterprise software / back office software, security software, support software. , backup software, general information technology infrastructure software, or used to operate equipment or hardware not included in the acquired assets.

Antivirus software is a type of endpoint protection that protects individual endpoints by detecting and blocking malicious files. A key point of Cyber Security Level 1 is to ensure that the corporate network is protected against the most common cyber threats, such as phishing attacks (links to malicious websites or downloads infected with viruses, attached to emails or instant messages and sent to company employees). and malware (malicious software that enters the company's network via the Internet or e-mail and exists in the form of spyware, ransomware, browser hijackers, etc.). The minimum cyber security measures needed to be implemented is a properly configured firewall working together with regularly updated anti-virus software. Firewalls scan network traffic for anomalous packets or packet fragments.

Antiviruses protect against cyber threats such as ransomware, worms, spyware, and more by scanning every file that employees open or download from the Internet or other sources.

Level 2 cyber security protects the corporate network from non-targeted attacks, for example, malware sent through a range of e-mail addresses, spoofing attacks, spamming, etc. In this case, the attacker's goal is to steal any valuable information from any IP addresses. the address is subject to known security vulnerabilities that may exist on the corporate network. Email Security , which involves various methods (email scanning for malware, spam filtering, etc.) to protect corporate information in both "internal" and "external" e-mails from any cyber-attack using e-mail as an entry point login (spyware, adware, etc.). Network segmentation , such as segmenting a network into departments with segments connected by firewalls that prevent malicious code or other threats from moving from one network segment to another. In addition, network segmentation implies the separation of network assets that store company data from external segments (web servers, proxy servers), which reduces the risk of data loss. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), used to detect and log information about potential security incidents, block them before they spread through network environments, etc. The key task of level 3 cyber security is to protect the corporate network from targeted attacks. This type of cyberattacks (targeted phishing, distribution of advanced malware, etc.) involves specially designed campaigns conducted against a specific organization. Endpoint security. This method of protection involves protecting the access of every device (smartphone, laptop, etc.) that enters the corporate network and thus becomes a potential entry point for security threats. Typically, endpoint security involves installing custom security software on a management server on a corporate network, along with installing client software on each device. The set of these measures allows you to monitor the actions of users when they access the corporate network remotely from their smartphones, tablets and other devices. This way, the company gets the best real-time view of the full range of potential security threats they may have to deal with.

Data Loss Prevention (DLP). The application of this measure is extremely important in an enterprise working in the financial or medical field. DLP software protects and prevents the leakage of important, personal, and sensitive data such as customer credit card numbers, social security numbers, and more, giving DLP administrators complete control over the types of data that can be transferred outside the corporate network. DLP can prevent attempts to forward any business email outside the corporate domain, upload corporate files to open source cloud storage, and more.

Information security and event management (SIEM). SIEM solutions monitor,

collect, analyze, and report log and event data about every activity that occurs in the IT environment, helping to avoid "I have no idea what happened" situations in the event of a company network breach. Benefits of SIEM include centralization of collected log data, support for compliance with PCI DSS, HIPAA and other regulations, and real-time incident response.

A virtual network is a network where all connected devices, servers, virtual machines, and data centers are run using software and wireless technology. This allows you to extend your network coverage as much as you need for maximum efficiency, in addition to numerous other benefits.

A local area network, or LAN, is a type of wired network that can typically only reach the domain of a single building. A wide area network, or WAN, is another type of wired network, but the computers and devices connected to the network can span up to a kilometer. Conversely, a virtual network does not follow the normal rules of network organization because it is not connected at all. Therefore, all devices that interact with each other on the network do so using Internet technology, which allows them to have a greater reach than if they were wired. The network itself is as limitless as the Internet.

Virtual networks have many advantages, including: Remote work capabilities. Virtual networks allow people to access their networks from anywhere in the world. Digital security. By using virtual networks, you can make your networks more secure by implementing features such as tunnel encryption and domain shards. Hardware optimization. By using virtual switches to route functions from one location to another, businesses can reduce the amount of hardware needed for access, maintenance, and monitoring. Flexibility and scalability. Because it is a virtual network and does not require a lot of hardware to create a virtual network, it is easier to scale with a lower cost of ownership. Scaling requires a few software tweaks and configurations, but doesn't necessarily require a lot of hardware. Cost savings: By reducing the amount of equipment, businesses benefit by saving money on equipment and maintenance costs.

Performance: Because networks can be configured faster. In a changing world, virtual networks play an important role in any digital business model. It is an evolution of technology that addresses the needs of remote access, security, flexibility, scalability and cost savings. Like many services that enterprises can outsource, this offers benefits in terms of time, money and valuable resources that can be better spent making sure all of your technology meets your business needs. As social conditions require more people to work remotely, virtual networks and NaaS services will become increasingly important to all businesses. Expanding the capabilities of virtual networks can be the next stage of digital transformation for companies that have already gone through the

process of becoming a digital enterprise. For example, expanding your company's virtual network to include more than just a VPN for additional productivity gains is one way businesses can continue to thrive in the digital world.

Choosing a management system for a corporate database is an important element in network development. Basically, there are two types of DBMS: relational and non-relational, also called SQL and NoSQL respectively. Before discussing the most popular database options, let's take a closer look at how relational and non-relational database systems differ in terms of commonly used data structures, performance, scalability, and security. Relational or SQL Databases A relational database is a type of data storage that organizes data in tables that are related to each other, which explains the name. Structured query language is the core of these systems, as it is used to communicate with and manage these databases, giving rise to their second name - SQL databases. RDBMS have a predetermined scheme, that is, data is arranged in rows (records) and columns (attributes) with a strict structure. Here, each record typically contains a value for each attribute, resulting in clear dependencies between different data points. Scalability. Relational databases are usually scaled vertically, that is, data is stored on one server, and scaling is carried out by adding additional computing power (CPU, RAM and RAM) to this one server. However, switching from small machines to larger ones often results in downtime. Scaling a SQL database between multiple servers (horizontal scaling) can be challenging because it requires data structure changes and additional engineering efforts. Performance. Relational databases demonstrate high performance for intensive read/write operations on small and medium-sized data sets. They also provide increased data retrieval speed by adding indexes to data fields for querying and joining tables. However, as the volume of data and user requests increases, performance may suffer. Security. Due to the integrated structure and data storage system, SQL databases do not require much engineering effort to ensure their reliable protection. They are a good choice for building and maintaining complex software solutions where any interaction has a number of consequences. One of the basic principles of SQL is compliance with ACID (atomicity, consistency, isolation, durability). ACID compliance is a better option if you're building, for example, e-commerce or financial applications where database integrity is critical. Non-Relational or NoSQL Databases A non-relational database is a non-tabular database that uses different data models to store, manage, and access data. The most common data models are document-oriented - for storing, extracting and managing data in the form of JSON documents; key-value - for presenting data in the form of a set of key-value pairs, where keys are unique strings with corresponding data values; graph - for storing data in a node-edge-node structure, where nodes are data

points and edges are their relationships; and wide-column — to store data in a tabular format with flexible columns, meaning it can vary from row to row in the same table. Since these databases are not limited to a tabular structure, they are called NoSQL. They allow you to store unstructured data such as texts, photos, videos, PDF files and many other formats. Data is easy to query, but it is not always organized by rows and columns as in a relational database. Scalability. As the amount of data and queries increases, non-relational or NoSQL databases typically scale horizontally by adding additional servers to the pool. They exchange data between different servers, each of which contains only a portion of the data, which reduces the request rate per second to each server. Performance. Non-relational databases are known for their high performance: they have a distributed structure that reduces the load on the system and provides simultaneous access to a large number of users. Such databases can store an unlimited number of sets of all types and forms. They are also quite flexible when it comes to changing data types. Security. Unlike relational systems, NoSQL databases have weak security, which makes them a serious problem for many infrastructures. Although they can provide ACID guarantees, they are usually available within a single database partition, although some DBMSs offer advanced security features that meet strict security and compliance standards.

Because NoSQL databases allow different types of data to be backed up together and scaled by scaling around multiple servers, their continued popularity is understandable. In addition, creating an MVP is a great option for startups with agile, sprint-based development. NoSQL requires no preparation before deployment, making it easy to quickly update the data structure without delay. It is possible to decide which system to use only based on the results of a preliminary information survey. Document management systems are essentially electronic filing cabinets that your organization can use as the basis for organizing all digital and paper documents. Any hard copies of documents can simply be uploaded directly into the document management system using a scanner. Document management systems often allow users to enter metadata and tags that can be used to organize all stored files. Most document management systems have a built-in search engine that allows users to quickly navigate through even the most extensive document libraries to access the appropriate file. Keep confidential documents? Don't worry—most document management systems have permission settings to ensure that only appropriate personnel can access privileged information. Choosing the right document management system starts with an accurate assessment of your organization's needs. The first choice you have to make is whether to choose an on-premise or cloud solution. Each type of system offers the same functionality, but there are several key differences in the way data is maintained and

stored.

An on-premises document management solution requires you to use your own servers and storage, which means you need to do your own maintenance. You will also not be responsible for the security of all your data, so you will need to back up everything. This option usually makes sense for larger companies with dedicated IT resources due to higher technical requirements, but it also gives you direct control over the system. Technical support and software updates from the vendor are usually dependent on whether you continuously renew the annual subscription package.

Pros: The biggest advantage of a stand-alone document management system is that you're always in control of the system and won't be relying on anyone else to keep it up and running. You won't be dependent on the Internet either. If your internet connection goes down, you'll still have access to all your documents.

Disadvantages: The disadvantage is the high initial cost, as well as the additional annual cost of updating the software. Also, you should make sure you have a backup system in place as your files are not automatically stored in the cloud. Another possible drawback is that not all standalone systems work with both Windows and Mac computers; many are only compatible with one or the other.

Cloud-based document management software is hosted by your system vendor and accessible to your organization online. Typically, cloud solutions charge a monthly or annual fee that includes all maintenance and software updates. Depending on the system you choose and the features you need, cloud platforms can range in price from a few dollars to more than $100 per user per month. The biggest advantages are that you don't need your own IT team to install the software and keep it running, and there are no significant upfront costs. You can also access the systems from anywhere you have an internet connection and you won't need to back up your files as they are automatically stored in the cloud. You depend on your ISP to keep your system up and running. If the provider has a problem with the data center, they may prevent you from accessing your files until the situation is resolved. Also, if your Internet connection goes down, you won't be able to access your files. Cloud solutions usually have a storage limit. There are several benefits to using a document management system. Overall, the system should be easy to implement, allow you to run your business more efficiently and make life easier for the business owner. By using a document management system, you can dedicate the time you previously spent organizing and managing documents to more important parts of your business. Security. Cyber security is more important than ever. By backing up documents in an encrypted cloud or on a secure local server, you can protect important and confidential company information and protocols.

As your business grows, so do your storage and document management features. One of the main benefits of document management software is its ability to scale up and down to meet your company's ever-changing needs. Simple document management. Keyword search makes it quick and easy to find important information about your company. Gone are the days of rummaging through file cabinets looking for the right information. Document management systems allow you to access any document more efficiently. Teamwork is the basis of any successful business. Document management software can improve collaboration in the workplace by allowing multiple people to work on the same file at the same time, tracking who makes which changes, and keeping your access to older versions of documents. The document management system is also an important element of the corporate network. Network backup is a system in which selected data from your backup clients (a single computer or a network of computers) is transmitted over a network (also known as the Internet) and sent to a backup server. This server may be privately owned and operated or hosted publicly by a cloud backup provider, as is often the case with most small businesses. Advanced backup systems can also manage backup media connected to a backup server over the network. This type of advanced setup is especially useful for businesses using NAS devices for general data. There are several reasons why you need to use backup for your business. Managing backups for multiple networked computers and devices can be a challenge if you're using physical storage devices, tape drives, or manually backing up each device individually. Here are just a few of the effective, time-saving, and error-reducing benefits of implementing a network backup solution:

Reduces the likelihood of human error. If your company's data is stored on several computers, backup over the network is necessary. If you remember to schedule backups for multiple computers, your business will be prone to errors. It's easy to accidentally skip a day or a week, and then before you know it, you've lost the file forever. Makes storage more scalable and manageable. Because data is sent to one secure location, network backup becomes more manageable and scalable than connecting tape drives to each computer system. With network backup, data is sent to one secure location, making it easy to add new computer systems to your network as your business grows. Automate backups. By using network backup, you simplify your backup processes. If you choose a public backup service provider to manage your backups, the backup software will automatically back up all the devices on your network, from selected computers and laptops to the general data on your NAS devices. Improves your disaster recovery capabilities – Having a detailed disaster recovery plan includes the use of network backup. If everything you had, all your customer and business information was stored locally on an external hard drive or without any backup at all, even a small

mistake would be devastating to your small business. Not only is it smart, but it's incredibly easy to set up network backup for every device you and your employees use. One of the best features of network storage is that you can send all your data to a local server or a remote server over the Internet without the mess, risk, and complexity of physical storage devices. But before you can take advantage of network backup, you need to decide whether you want to back up to your own private server or to a public cloud.

## 2.4. Organization of satellite internet for food industry enterprises

Satellite Internet works through signals, not through hard wires (for example, with cable and fiber optic Internet). An Internet connection here on Earth sends a signal to an orbiting satellite, which then reflects the signal to a dish outside your workplace. Accessibility. DSL is only available within about 22,000 feet of the telephone company's central office. If your business is outside of this range, DSL is most likely not available, and if it is, it may be much slower than it works. Satellite on the other hand is available almost anywhere in the world because it does not use hard lines to send internet services. Even some of the most remote rural areas have access to commercial high-speed satellite Internet, so they don't have to depend on dial-up. Reliability. Satellite Internet can generally be as reliable as DSL in terms of overall signal strength, and it's always on. It works independently of the cables and phone lines leading to your business, so problems with them will not affect your internet connection. The satellite network is much simpler than most other forms of the Internet; There are only four points of contact for the signal: satellite, teleport, network operations center (NOC), and very small aperture terminal (VSAT). Because of this, there are fewer points where a problem can cause a failure. With DSL, thousands of feet of cable travel to your business where road work, weather, animals or other factors can damage the cables and cause your service to be interrupted. Also, with fewer contact points and a very short cable, it's easy for the satellite provider to identify where the problem might be and fix it faster.

Ease of use. Satellite Internet service is generally much easier for end users than DSL or fiber, in part because it's always on. A technician comes to your location, sets up the satellite dish and connects it to your computers, and you're done. Usually, all you have to do is turn on your computer and you're connected. Security. Satellite Internet is generally considered more secure than DSL or Wi-Fi because it works over very specific signals. Packets of data are broken up and sent and received over a beam

specifically for transmission to and from your business. Because of this, and because the signal travels to orbit and back, it is very difficult to intercept. Because satellite Internet works using signals transmitted between the Earth's surface and orbit and back, latency (or the time it takes for data to complete a transmission instruction) can be as high as a second or two. Although this does not matter much for research purposes, it can present a problem when trying to conduct real-time transactions and video conferencing, as there can be noticeable delays between sending a message and receiving a response.

Failures depending on the weather. Even commercial-grade satellite Internet can be disrupted by downpours, strong winds, and other weather conditions. These conditions may weaken or completely block your Internet signal until it is unusable. Solutions for enterprises with remote divisions VSAT networks allow the use of solutions for the organization of operational communication of the office (management, administration) of the enterprise with permanent or temporary production sites located outside populated areas, where connection to "terrestrial" communication networks is impossible . It can be, for example: oil and gas fields, gas compressor and oil pumping stations, power grid substations, bases of seismic exploration parties, construction sites (construction of roads and railways, bridges, etc.), stationary gas stations, checkpoints, objects of the agro-industrial complex, telephone and Internet connection via satellite, protection of remote objects and video surveillance via satellite, satellite communication in telemetry and telemechanics systems. Communication via satellite with field parties, the company's own corporate VSAT network, telephone connection and Internet via satellite, a small ground satellite communication station (VSAT station) connected to the Star satellite network is installed at a remote facility. Internet access is a primary service, it is provided automatically. A single computer or computer network can be connected directly to a VSAT satellite earth station using a twisted pair cable. You can use the Internet, e-mail, ICQ-type communicators and other Internet services on any connected computer.

Through a small and inexpensive device - a voice gateway - one or more telephones can be connected. Direct city numbers can be assigned to the user. Outgoing calls from the remote facility and incoming calls to the facility will be made in the same way as if the phone was physically located in one of these cities. Calls from the facility to other cities are paid at IP-telephony rates, which are much cheaper than usual between cities. Thus, connecting to the VSAT satellite communication network not only solves the problem with the Internet and telephone, but also allows you to significantly save on telephone conversations. If the facility is large enough, you can install an office PBX on it and connect its external (city) lines through the voice

gateway to the VSAT satellite station. Thus, by paying the satellite operator 1...4 telephone lines, you can connect up to several dozen telephones, each with access to the city and to the intercity.

Satellite Internet technology has existed for several decades. It involves the transmission of Internet data not by cables, but by radio signals through the vacuum of space. The planet's ground stations transmit signals to satellites in orbit, which can then transmit data to users on Earth. One of the main existing providers was HughesNet, which uses satellites 22,000 miles above the planet. SpaceX's system advances the technology in two important ways: The company wants to use low-Earth orbit satellites that orbit the planet only about 300 miles above the surface. A shortened distance can significantly improve the speed of the Internet, as well as reduce latency. Second, SpaceX wants to launch up to 40,000 satellites in the coming years to power the system, guaranteeing global coverage without service interruption. Starlink uses a SpaceX Falcon 9 rocket to deliver a huge array of satellites into Earth orbit, where they will connect and provide the Internet. However, unlike traditional satellite Internet services, Starlink promises some interesting innovations, including much lower latency than has historically been available from satellite providers, and is already serving a small number of customers through its beta program. Since satellites are much closer to Earth, they also do not have as large a coverage area. That's why the company needs to launch so many smaller satellites, which they call "small satellites." In order for the satellites to communicate, the company has built gateways around the world to help exchange signals, although they are currently experimenting with laser technology that allows the satellites to communicate directly and eliminates the need for a gateway. So for Starlink users, this means that once the Starlink kit is installed, the antenna will automatically find the nearest satellite and connect. As the satellites rotate in a chain, each satellite finds the next and the next, which should create a seamless connection for the user.

The organization of satellite communication will allow effective protection of remote objects, including those that are not serviced. This is especially relevant for enterprises whose facilities are distributed over large territories. For example, a video surveillance system with a security control panel can be organized for a network of gas stations. One security guard, while in the city, will be able to monitor several gas stations located on highways between cities at once. The simplest option for using a terrestrial VSAT satellite station to protect an object is to transmit an alarm signal via satellite communication channels. This requires almost no additional equipment. If a satellite station is already installed at the facility, it is enough to connect an "alarm button" or a loop of security sensors to a free port of the voice gateway. The fact of

opening the loop will be recorded as "hanging up". This signal will be transmitted via the Internet to the security control panel - there the bell or siren will be activated. A small improvement - and after the alarm signal (or instead of it) the loudspeaker communication with the facility will be activated: it will be possible to listen to what is happening there, and if necessary - address the staff or the subject who illegally entered the facility by voice object A more complex scheme is video surveillance of remote objects. IP video surveillance cameras (cameras with a built-in web server and Ethernet interface) or standard analog cameras via an external video server can be connected to the satellite earth station of the VSAT network. One or more stationary cameras can be installed on a remote object - the security guard at the central console will be able to view images from them simultaneously or in turn. You can organize patrolling of a remote object using one rotating PTZ (Pan, Tilt, Zoom) camera. The rotation of the camera can be remotely controlled by the security guard at the security console. And you can program the camera so that it automatically goes around several designated points. A digital video recorder (Digital Video Recorder, DVR) can be installed at the facility. This will make it possible to use satellite communication channels not always, but as needed. In normal mode, images from several cameras are recorded on the recorder's hard disk, and satellite lines are not used. If motion is detected in the camera's viewing area or an external sensor is triggered, a signal is sent to the security control panel. The security guard can immediately receive a picture from one or several cameras at once through the satellite, and if necessary - view the alarm log, view recordings from the cameras, download the necessary recordings from the DVR hard disk and save them as a file on his computer.

Satellite communication can be used for remote control of technological equipment. This solution is successfully used, for example, in automated systems of commercial electricity metering (ASCOE) at power grid substations, railway traction substations, oil pumping stations, etc. Readings of electricity meters from a number of remote objects are transmitted to the central control post via satellite. There, they are analyzed by a special computer program and displayed at the dispatcher's workplace. It is also possible to organize a distributed system of commercial accounting of gas, water, etc. More complex telemetry and telemechanics systems allow you to control several equipment parameters at once (voltage, current, engine speed, temperature, flow of liquids and gases, position of shut-off valves, filling level of containers, etc.). The dispatcher can not only monitor, but also manage the equipment - open/close the valve, start and stop the pump, compressor, fan. For such tasks, existing dispatching hardware and software complexes (SCADA systems) are used. More complex telemetry and telemechanics systems allow you to control several equipment

parameters at once (voltage, current, engine speed, temperature, flow of liquids and gases, position of shut-off valves, filling level containers, etc.). The dispatcher can not only monitor, but also manage the equipment - open/close the valve, start and stop the pump, compressor, fan. Existing hardware and software dispatching complexes (SCADA systems) are used for such tasks. At the same time, the satellite station of the VSAT network provides telephone communication. Therefore, the dispatcher can, if necessary, contact the staff or the repair team. This is a solution for mobile communication with small groups of employees working in the field - for example, geophysicists or surveyors. Usually, for mobile communication in such cases, Thuraya, Iridium, Inmarsat, etc. satellite telephone communication is used. systems It is convenient, but very expensive: a minute of satellite phone communication costs about 1 dollar. If the field parties work at a short distance from the base camp, in which a subscriber satellite station is installed, it is possible to organize a wireless telephone network at its base. Thus, field parties can talk to the base camp without going to the satellite at all, but to the office of the enterprise or to other cities - at IP telephony rates, i.e. cheaper than a regular long-distance call. Here are several options for organizing such a network. In the first version, CB radio stations (27 MHz) are used. One of them (stronger) is installed stationary in the base camp, the others that are carried are in field parties. This decision involves the use of modern radio stations equipped with a digital keyboard and having address call functions - for example, Vertex VX-2500. Such a network provides only voice communication, it is difficult to organize data transmission in it. However, it works reliably even over long distances. The system allows directly from the portable radio stations to go through the satellite to the public telephone network, and vice versa, to make phone calls directly to the portable radio stations. Connecting a computer (Internet), telephone and fax - in the usual way through a voice gateway. A base radio station is connected to this voice gateway through a special device - a telephone line interface. Radio communication of field parties with each other and with the base camp is carried out in the usual order. For a call from a radio station that is carried to the office or to another city, you need to type the access code to the phone line and the phone number on the numeric keypad. The interface will "pick up the phone", broadcast the number from the radio network to the line, connect the line to the base radio station. To call a portable radio station from the office or from another city, you need to dial a phone number and then in tone mode - the personal number of the radio station. During a call, the person talking on the phone cannot press the key of the base radio, so it is controlled by the interface, including the transmission of the voice sound. In the second option, a Wi-Fi wireless computer network is organized around the base camp. Field parties can not only call the office

or other cities, but also transfer data and access the Internet. However, such a network works reliably only over short distances. The range of communication can be increased by using an intermediate repeater in a "mobile" camp - for example, in a car or all-terrain vehicle. Two powerful access points with directional antennas operating in bridge mode are used to connect the base camp with the mobile camp. An intermediate wired Ethernet network is organized in the mobile camp. Another access point with a non-directional antenna is installed to connect the mobile camp with field parties on foot. The functions of mobile phones of field parties are performed by Wi-Fi phones (for example, ALCATEL IP Touch 310). Incoming and outgoing calls from them are made in the same way as from a regular landline. Data received by mobile parties (for example, seismic survey data) can be transmitted directly from the workplace to a mobile camp, base camp, or via satellite - anywhere in the world. In the third option, long-range wireless phones are used, for example, Senao. The base unit of the radio telephone is connected to the VSAT satellite earth station through a free port of the voice gateway. It allows you to work with a remote terminal both in telephone communication mode and in "intercom" mode - for communication between mobile and base camps. An external telephone and fax are connected to the base unit. A remote terminal is brought to the mobile camp, to which, in turn, the base of another radio telephone with a non-directional antenna is connected as an external telephone. Radiotelephone handsets are used in field parties. Data can be sent using a regular modem. A special telephone line interface is connected to the modem for operation with a radio telephone base.

**Conclusions**

We live in a digital age and all transactions are done at the speed of light over the internet. In the food industry, we rely on the Internet for sales and customer service in a variety of industries. For this reason, what is called business continuity (BCC) has become an important priority for companies and industries worldwide. Satellite Internet of the 21st century will become an integral part of the enterprise. When a product or service is complete, the most immediate activities that support it and its "analysis" are complete. Develop plans and strategies that ensure business continuity, thus recovering quickly and efficiently from any type of disruption, regardless of its size or cause. This made it strong. It will be a base in case of an emergency and will give you a sense of stability and security. This is where satellite Internet comes in. While most businesses connect to the Internet over more traditional DSL, fiber optic or wireless networks, having Backup Satellite Internet means your business will never go down. When traditional Internet connections are interrupted, a satellite backup Internet connection can be relevant.