MODEL OF THE CORPORATE NETWORK OF THE ENTERPRISE FOR PROTECTION FROM UNAUTHORIZED ACCESS

Sayfullaev Sh.B.
TUIT named after
Muhammad al-Khwarizmi

Annotation. This article discusses the corporate network model and network types, linear network construction with common channels.

Key words. Network, non-sectional access, model, corporate network

To define the concept of “corporate network model”, we need to define the concept of “corporate network”. Recently, this phrase has become quite common and has even begun to lose its meaning. The most detailed definition is as follows. A corporate network is an internal private network of an organization that unites the computing, communication and information resources of this organization and is designed to transmit information of various types (digital, audio, video and other information) [2]. A corporate network is usually geographically distributed, that is, it unites departments and structures located at a significant distance from each other. Often, corporate network nodes are located in different cities, and sometimes countries. A special policy is defined within the corporate network, describing the hardware and software used, the rules for gaining user access to network resources, the rules for managing the network, monitoring the use of resources and the further development of the network. A corporate network combines a huge number of different components, among which, in the most general case, we can highlight:

- cable systems;
- information transmission networks;
- telecommunication systems (including automatic telephone exchanges);
- information system servers and workstations;
- system software;
- application software;

- security and life support systems.

The main tasks of a corporate network are the interaction of system applications located in different nodes and access to them by remote users. Applications are understood as both system software - databases, mail systems, computing resources, file services, etc. - and the tools that the end user works with.

One of the main problems that has to be solved when creating a corporate network is organizing communication channels. If within one city you can count on renting dedicated lines, including high-speed ones, then when moving to geographically remote nodes, the cost of renting channels increases sharply, and their quality and reliability often turns out to be very low.

The simplest solution to this problem is to use existing global networks. In this case, it is enough to provide channels from offices to the nearest network nodes. The global network will then take on the task of delivering information between nodes. Even when creating a small network within one city, you should keep in mind the possibility of further expansion and use technologies compatible with existing global networks: X.25, Frame Relay, ATM, Internet.

The ideal option for a private network is to create communication channels only in those areas where they are needed, and to transmit any network protocols required by the running applications. At first glance, this is a return to leased communication lines, but there are technologies for building data transmission networks that allow you to organize channels within them that appear only at the right time and in the right place. Such channels are called virtual. It is natural to call a system that unites remote resources using virtual channels a virtual network. Today, there are two main technologies for virtual networks - circuit-switched networks and packet-switched networks [3]. The former include the regular telephone network, ISDN and a number of other technologies. Packet-switched networks are represented by X.25, Frame Relay and - more recently - ATM technologies. It is too early to talk about the use of ATM in geographically distributed networks due to its fairly high cost. Other types of virtual (in various combinations) networks are widely used in building corporate information systems.

Circuit-switched networks provide the subscriber with several communication channels with a fixed bandwidth for each connection. For example, a telephone network provides one communication channel between subscribers. If it is necessary to increase the number of simultaneously available resources, it is necessary to install additional telephone numbers, which is very expensive. Even if we forget about the low quality of communication, the limitation on the number of channels and the long time to establish a connection do not allow using telephone communication as the basis of a corporate network. For connecting individual remote users, this is a fairly convenient and often the only available method.

Another example of a virtual circuit-switched network is ISDN (Integrated Services Digital Network). ISDN provides digital channels (64 kbps) that can transmit both voice and data. A basic ISDN connection (Basic Rate Interface) includes two such channels and an additional control channel with a speed of 16 kbps (this combination is designated as 2B+D). It is possible to use a larger number of channels - up to thirty (Primary Rate Interface, 30B+D), but this leads to a corresponding increase in the cost of equipment and communication channels. In addition, the costs of renting and using the network increase proportionally. In general, the restrictions on the number of simultaneously available resources imposed by ISDN lead to the fact that this type of communication is convenient to use mainly as an alternative to telephone networks. In systems with a small number of nodes, ISDN can also be used as the main network protocol. However, it should be borne in mind that access to ISDN in our country is still the exception rather than the rule due to its high cost.

An alternative to circuit-switched networks is packet-switched networks. With packet switching, a single communication channel is shared by many users in a time-sharing mode, much like the Internet. However, unlike networks like the Internet, where each packet is routed separately, packet-switched networks require a connection to be established between end resources before information can be transmitted. Once a connection is established, the network “remembers” the route (virtual channel) along which information must be transmitted between subscribers and remembers it until it receives a signal to break the connection. For applications running in a packet-switched network, virtual channels look like regular communication lines—the difference is that their throughput and introduced delays vary depending on network load. The classic packet-switching technology is the X.25 protocol.

At present, there are practically no X.25 networks using speeds higher than 128 kbit/sec. The X.25 protocol includes powerful error correction tools, ensuring reliable delivery of information even on poor lines and is widely used where there are no high-quality communication channels. In our country, they are almost everywhere. Reliability is not cheap - in this case, the speed of network equipment and relatively large, but predictable, delays in the distribution of information. At the same time, X.25 is a universal protocol that allows you to transfer almost any type of data. "Natural" for X.25 networks is the operation of applications using the OSI protocol stack. These include systems using the 43 X.400 (e-mail) and PTAM (file exchange) standards, as well as some others. Tools are available that allow you to implement interaction between Unix systems based on OSI protocols.

Another standard feature of X.25 networks is communication via regular asynchronous COM ports. In other words, the X.25 network extends the cable connected to the serial port, extending its connector to remote resources. Thus, virtually any application that can be accessed via a COM port can be easily integrated into the X.25 network. Examples of such applications include not only terminal access to remote host computers, such as Unix machines, but also interaction between Unix computers (C, IISR), Lotus Notes-based systems, cc:Mail and MS Mail e-mail, and so on.

To unite LANs in nodes connected to an X.25 network, there are methods of packing ("encapsulating") information packets from the local network into X.25 packets. Some service information is not transmitted, since it can be unambiguously restored on the recipient's side. The standard encapsulation mechanism is considered to be the one described in RFC 1356. It allows various local network protocols (IP, IPX, etc.) to be transmitted simultaneously through one virtual connection. This mechanism (or its older implementation RFC 877, which allows only IP transmission) is implemented in almost all modern routers [113].

There are also methods for transmitting other communication protocols via X.25, in particular SNA, used in IBM mainframe networks, as well as a number of private protocols from various manufacturers. Thus, X.25 networks offer a universal transport mechanism for transmitting information between virtually any applications. In this case, different types of traffic are transmitted via one communication channel, “knowing” nothing about each other. When combining LANs via X.25, it is possible to isolate individual fragments of a corporate network from each other, even if they use the same lines.

44 connections. This facilitates the solution of security and access control problems that inevitably arise in complex information structures. In addition, in many cases there is no need to use complex routing mechanisms, shifting this task to the X.25 network.

Today, there are dozens of global public X.25 networks in the world, their nodes are located in almost all large business, industrial and administrative centers. In Russia, X.25 services are offered by Sprint Network, Infotel, Rospak, Rosnet, Sovam Teleport and a number of other providers. In addition to connecting remote nodes, X.25 networks always provide access means for end users. In order to connect to any X.25 network resource, a user only needs a computer with an asynchronous serial port and a modem. At the same time, there are no problems with authorization of access in geographically remote nodes - firstly, X.25 networks are sufficiently centralized and by concluding an agreement, for example, with Sprint Network or its partner, you can use the services of any SprintNet node, and these are thousands of cities around the world, including more than a hundred in the territory of the former USSR. Secondly, there is a protocol for interaction between different networks (X.75), which takes into account, among other things, payment issues. Thus, if a resource is connected to an X.25 network, it can be accessed both from the service provider's nodes and through nodes of other networks - that is, from almost anywhere in the world.

In terms of information transfer security, X.25 networks offer a number of very attractive opportunities. First of all, due to the network structure itself, the cost of intercepting information in an X.25 network is high enough to serve as a good defense. The problem of unauthorized access can also be solved quite effectively by means of the network itself. If any, even the smallest, risk of information leakage is unacceptable, then it is necessary to use encryption tools, including real-time encryption. Today, there are encryption tools created specifically for X.25 networks that allow working at fairly high speeds - up to 64 kbps. Such equipment is manufactured by Racal, Cylink, Siemens. There are also domestic developments created under the auspices of FAPSI. An example of the use of real-time encryption technology is the global information banking system SWIFT (The Society for Worldwide Interbank Financial Telecommunications).

The disadvantage of X.25 technology is the presence of a number of fundamental limitations on speed. The first of them is connected precisely with the developed possibilities of correction and restoration. These means cause delays in information transmission and require high computing power and productivity from X.25 equipment, as a result of which it simply “does not keep up” with high-speed communication lines. Although there is equipment with a port speed of 2 Mbit/s, the speed they actually provide does not exceed 250 - 300 kbit/s per port. On the other hand, for modern high-speed communication lines, X.25 correction means are redundant and when they are used, the equipment capacity often works idle.

The second feature that makes us consider X.25 networks as slow is the peculiarities of LAN protocol encapsulation (primarily IP and IPX). All other things being equal, the connection of local networks via X.25 is, depending on the network parameters, 15-40 percent slower than when using HDLC technology over a dedicated line. Moreover, the worse the communication line, the higher the loss of productivity. Again, we are dealing with obvious redundancy: LAN protocols have their own means of correction and recovery (TCP, SPX), but when using X.25 networks, this has to be done again, losing speed.

It is on these grounds that X.25 networks are declared slow and obsolete. But before saying that any technology is obsolete, it should be specified for what applications and under what conditions. On low-quality communication lines, X.25 networks are quite effective and provide a significant advantage in price and capabilities compared to dedicated lines. On the other hand, even if we count on a rapid improvement in communication quality - a necessary condition for X.25 obsolescence - then investments in X.25 equipment will not be wasted, since modern equipment includes the ability to switch to Frame Relay technology.

Frame Relay technology appeared as a means of realizing the advantages of packet switching on high-speed communication lines. The main difference between Frame Relay networks and X.25 is that they exclude error correction between network nodes. The tasks of restoring the information flow are assigned to the end equipment and user software. Naturally, this requires the use of high-quality communication channels. It is believed that for successful work with Frame Relay, the error probability in the channel should be no worse than 10'6-10'7, i.e. no more than one bad bit per several million. The quality provided by conventional analog lines is usually one to three orders of magnitude lower.

The second difference between Frame Relay networks is that today almost all of them implement only the mechanism of permanent virtual connections (PVC). This means that when connecting to a Frame Relay port, it is necessary to determine in advance which remote resources need access. The principle of packet switching - many independent virtual connections in one communication channel - remains here, but it is impossible to select the address of any subscriber of the network. All available resources are determined when configuring the port. Thus, on the basis of Frame Relay technology, it is convenient to build closed virtual networks used to transmit other protocols, by means of which routing is carried out.

A virtual network being "closed" means that it is completely inaccessible to other users operating on the same Frame Relay network. For example, in the United States, Frame Relay networks are widely used as backbones for the Internet. However, a private network can use Frame Relay virtual circuits on the same lines as Internet traffic - and be isolated from it.

Like X.25 networks, Frame Relay provides a universal transmission medium for virtually any application. The main area of application for Frame Relay today is the unification of remote LANs. In this case, error correction and information recovery are performed at the level of LAN transport protocols - TCP, SPX, etc. Losses for encapsulation of LAN traffic in Frame Relay do not exceed two to three percent. Methods for encapsulating LAN protocols in Frame Relay are described in the RFC 1294 and RFC 1490 specifications. RFC 1490 also defines the transmission of SNA traffic via Frame Relay.

The Annex G specification of ANSI T 1.617 describes the use of X.25 over Frame Relay networks. In this case, all the functions of addressing, correction and restoration of X.25 are used - but only between end nodes implementing Annex G. In this case, a permanent connection over a Frame Relay network appears as a "direct wire" over which X.25 traffic is transmitted. X.25 parameters (packet size and window) can be chosen in such a way as to obtain the minimum possible propagation delays and speed losses when encapsulating LAN protocols.

The absence of error correction and complex packet switching mechanisms typical of X.25 allows information to be transmitted via Frame Relay with minimal delays. Additionally, it is possible to enable a prioritization mechanism, allowing the user to have a guaranteed minimum data transfer rate for a virtual channel. This capability allows Frame Relay to be used to transmit information that is critical to delays, such as voice and video in real time. This relatively new capability is becoming increasingly popular and is often the main argument when choosing Frame Relay as the basis of a corporate network.

It should be remembered that today Frame Relay network services are available in our country in no more than fifteen cities, while X.25 is available in about two hundred. There is every reason to believe that as communication channels develop, Frame Relay technology will become more widespread - primarily in places where X.25 networks currently exist. Unfortunately, there is no single standard describing the interaction of various Frame Relay networks, so users are tied to one service provider. If it is necessary to expand the geography, it is possible to connect to networks of different providers at one point - with a corresponding increase in costs.

There are also private Frame Relay networks operating within a single city or using long-distance, usually satellite, dedicated channels. Building private networks based on Frame Relay allows for a reduction in the number of leased lines and the integration of voice and data transmission [1].

When using the Internet as a basis for a corporate data transmission network, you need to keep in mind the following. The Internet is not a single network, but a set of networks. That is, if you look inside the Internet, you can see that information passes through many completely independent and mostly non-commercial nodes connected through the most diverse channels and data transmission networks. The rapid growth of services provided on the Internet leads to an overload of nodes and communication channels, which sharply reduces the speed and reliability of information transmission. At the same time, Internet service providers do not bear any responsibility for the functioning of the network as a whole, and communication channels are developing extremely unevenly and mainly where the state considers it necessary to invest in this. Accordingly, there are no guarantees of the quality of network operation, data transfer speed, or even just the accessibility of computers. For tasks in which reliability and guaranteed time of information delivery are critical, the Internet is far from the best solution. In addition, the Internet binds users to one protocol - IP. This is good if you use standard applications that work with this protocol. Using any other systems with the Internet turns out to be a difficult and expensive matter.

Another major Internet problem that has been widely discussed recently is security. If we are talking about a private network, it seems natural to protect the information being transmitted from prying eyes. The unpredictability of information paths between many independent Internet nodes not only increases the risk of data theft (technically, this is not that difficult), but also makes it impossible to determine the location of the information leak. Encryption tools solve the problem only partially, since they are mainly applicable to mail, file transfer, etc. Solutions that allow information to be encrypted in real time at an acceptable speed (for example, when working directly with a remote database or file server) are difficult to access and expensive.

Another aspect of the security problem is related to the decentralization of the Internet - there is no one who could restrict access to the resources of a private network. Since it is an open system where everyone sees everyone, anyone can try to get into a private network and gain access to data or programs. Of course, there are means of protection (they are usually called Firewalls). However, they should not be considered a panacea - it is enough to remember viruses and antivirus programs. Any protection can be broken, as long as it covers the cost of hacking.

It should also be noted that it is possible to make a system connected to the Internet inoperative without intruding into the network itself. There are known cases of unauthorized access to network node management, or simply using the peculiarities of the Internet architecture to disrupt access to a particular server.

Thus, it is impossible to recommend the Internet as a basis for systems that require reliability and privacy. Connecting to the Internet within a corporate network makes sense if access to a huge information space is needed.

Let us consider exactly this case. Given a corporate network consisting of one or several segments (parts), which are local networks of the corporation's divisions. Each segment is operational independently of the others. All network segments have access to the Internet (Fig. 1).

The analysis will be conducted using the example of one of the corporate network segments. As mentioned earlier, a corporate network segment is a local network of a corporate division. The mathematical model of a local network (or simply a network) is a graph [1]. The graph nodes represent terminal equipment (computers, hubs, routers, switches, etc.), and the graph branches are communication channels (Fig. 2). According to topological properties, the following types of networks can be distinguished [1]:

■ Fully connected graph, or "each with each" (Fig. 3). In a network of this type, there is a communication channel between each pair of nodes. Such a network has maximum survivability in providing transit data transmission through its nodes. Survivability is understood as the property of a network with a given probability of providing information delivery with some deterioration in service when individual branches or nodes of the network fail [2]. A network of this type is capital-intensive to create.

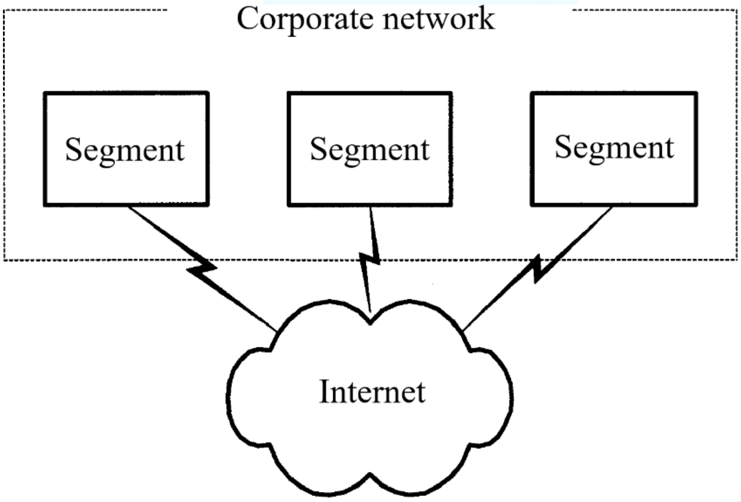

Fig. 1.A corporate network consisting of several segments

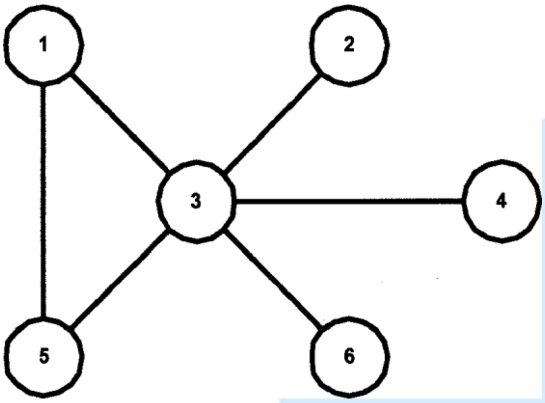

Fig. 2. Mathematical model of a local network - graph

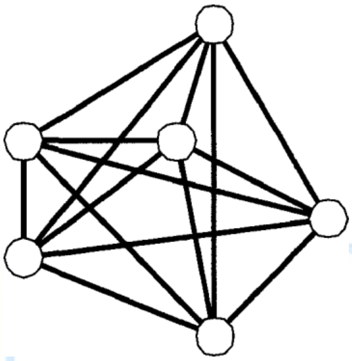

Fig. 3. Network type - fully connected graph

•"Tree" (Fig. 4). This is a network in which there is only one communication channel between each pair of nodes. It has minimal survivability, but is the most optimal in terms of cost.

•"Grid" (Fig. 5). Each node in this type of network is connected only to a few immediate neighboring nodes. The grid has good survivability and average cost.

•Radial-ring network (Fig. 6). One of the "grid" variants, in which each node is connected to a pair of the nearest neighbors and to the central node. It has good survivability, although the number of branches is significantly less than in a fully connected graph.

•Linear construction of a network with common channels (Fig. 7). A special case of such a network is a ring network.

Currently, of the above-mentioned types of topologies, the following are widely used in corporate networks:

•"Star" (Fig. 8). Analog of the "tree" type network. Each network node is connected by a communication channel to the central node - the unifying device. If necessary, several networks with the "star" topology can be combined together, resulting in branched network configurations. In terms of survivability, this topology is not the best solution, since the failure of the central node will lead to the shutdown of the entire network. However, when using the "star" topology, it is easier to find a fault in the cable network. It is the most common topology of modern local networks due to its simplicity, reliability and low cost.

•"Common bus" (Fig. 9). Assumes the use of one cable to which all computers in the network are connected. The cable is used by all stations in turn. Special measures are taken to ensure that when working with a common cable, computers do not interfere with each other's transmission and reception of data. Reliability is higher here, since the failure of individual computers will not disrupt the operation of the network as a whole. Troubleshooting the cable is difficult. In addition, since one cable is used, in the event of a break, the operation of the entire network is disrupted.

●"Ring" (Fig. 10). In this case, data is transmitted from one computer to another as if by relay. If a computer receives data intended for another computer, it transmits it further along the ring. If the data is intended for the computer that received it, it is not transmitted further.

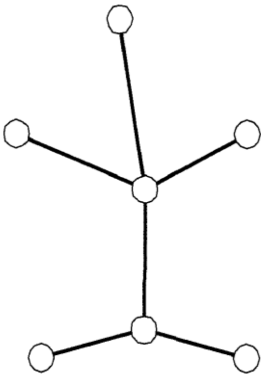

Fig. 4. Network type - "tree"

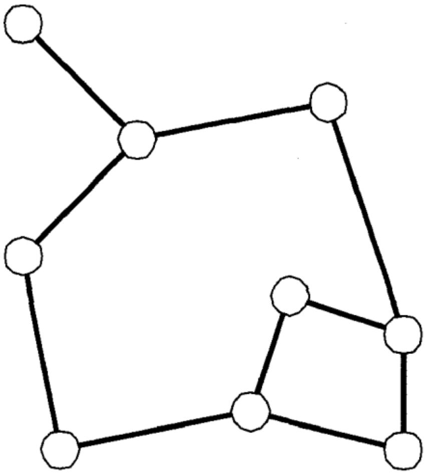

Fig. 5. Network type - "mesh"

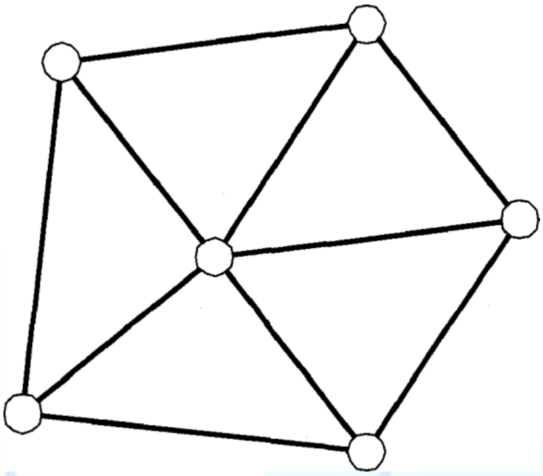

Fig. 6. Network type - radial ring network

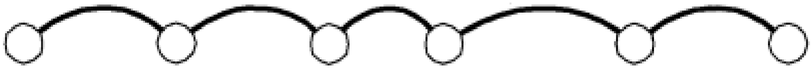

Fig. 7. Linear construction of a network with common channels

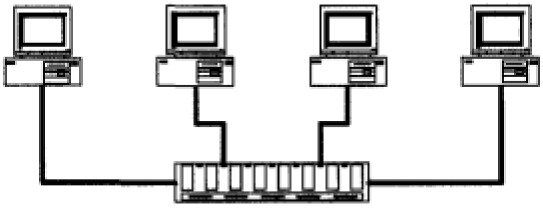

Fig. 8. Network "star"

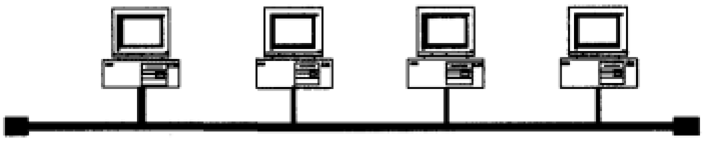

Fig. 9. Common Bus Network

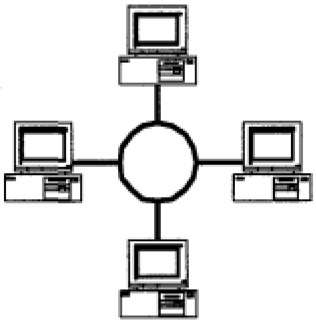

Fig. 10. Ring network

As was stated in the definition at the very beginning of the chapter, a corporate network consists not only of switching equipment (we will call it the physical part of the corporate network), but also of information support (we will call it the logical part of the corporate network), which, in turn, consists of operating systems and software products for expanding the capabilities of these operating systems in order to improve the quality of service. It is the logical part of the corporate network that is subject to an attack in order to gain unauthorized access to some network services. In order to ensure network protection, it is necessary to know what type (kind) of attack can be used to disrupt the operation of corporate network services. Let's move on to their consideration.

Literature

1. Vishnevsky, V.M. Theoretical foundations of designing computer networks. Vishnevsky V.M. - Moscow, Tekhnosfera, 2003. - 512 p.

2. Gorodetsky, A.Ya. Information systems. Probabilistic models and statistical decisions. Textbook. Gorodetsky A.Ya. - St. Petersburg: Publishing house of St. Petersburg State Polytechnical University, 2003. - 326 p.

3. Kuznetsov E.M. Priorities of information processing in a corporate information and computing network Scientific review – Saratov 2013 – No. 11 – P.141-145. http://elibrary.ru/item.asp?id=21219053