Ministry of Education of the Republic of Belarus
Educational Institution
Belarusian State University of Informatics and
Radioelectronics

UDC 004.42:629.33

AL-Arkawazi Ali Jalil Ali

ANALYSIS OF ENTERPRISE-LEVEL IP NETWORK TRAFFIC

ABSTRACT

for master's degree in technical sciences by specialty 1-45 80 02 «Telecommunication systems and computer networks»

Scientific adviser
Phd, V.K.Konopelko

Minsk, 2020

INTRODUCTION

Nowadays in the era of technological progress the effective functioning of any enterprise depends a lot on the IT infrastructure of the organization. The world observes the rapidly growing need for the organization of local networks.

A corporate network is a network which main purpose is to support the functioning of a particular enterprise owning this network. Users of a corporate network are only the employees of this enterprise. Enterprise-wide networks integrate a large number of computers from all the territories of the organization. The corporate network includes also the branches of the enterprise in various cities (countries).

A modern corporate network is not only a data transmission network, but also a complex of various services which allows to solve a lot of tasks of key processes at the enterprise such as: quick access to information arrays of the general information space of the company (enterprise); the ability to carry out the analysis of the state and management of business processes from a single analytical center; exchange of information and settlement documents; continuous automated monitoring and management; infocommunication system resources from a single center. To provide continuous operation and automation of production processes in their branches, enterprises need local area networks that meet the following characteristics: fault tolerance; cryptographic security; the flexibility of the network architecture, when it is possible to change the network topology when moving and connecting new users; high throughput.

In the field operations, the degree of protection of data transmitted over the network plays an important role due to the ever-growing number of cyber crimes. All nodes connected to the network through third-party providers must be protected by advanced encryption methods, as well as flexible access rules not only from outside, but also inside the organization.

Due to all these facts creation of a reliable and fully functional corporate network of an enterprise is very important.

GENERAL CHARACTERISTIC

The purpose of this dissertation is to model a corporate local network taking into account modern security requirements, fault tolerance and continuous transmission of all types of network traffic. To achieve the goal of the work the following tasks were solved: the analysis of technologies for building local and corporate computer networks and the analysis of the principles of construction and characteristics of computer network equipment were carried out; modeling tools for the local network were selected; a local network model taking into account modern security requirements, fault tolerance and continuous transmission of all types of network traffic was modeled.

In the first chapter of the dissertation "Analysis of initial data for building a corporate network" the essence, the main characteristics of a corporate network and the basic principles of building corporate networks are disclosed. The modular approach to building a network structure based on a composite network model of the enterprise provided by Cisco Systems is described. Also in this chapter the encryption in private virtual networks is considered, the specific features of VPN connections use are analyzed.

In the chapter 2 of the dissertation "Selection of equipment to develop a local computer network" the main requirements for routing services, switch and firewall are described. The main types of switches, the ways of switch placement are mentioned, the models of switches with basic speed are described. The network security mechanisms to protect the corporate network are disclosed in this section.

In the chapter 3 of the dissertation "Selection of software to model the network" advantages and the disadvantages of the GNS3 graphic network simulator and the EVE-NG graphic network emulator are considered.

The next part of the dissertation devoted to the description of the designing a local network. So in the chapter 3 of the work the specific features of the network setup at the Head Office were analyzed on the base on the analysis network zones, branch network areas and organization of communication with the head office were identified. The process of designing an ATM network and organizing communications with the head office and processing center are shown.

In the last chapter 5 of the dissertation “Estimated cost of desinging a local computer network” the calculation of the remuneration of employees, the estimates of design costs, the expenses for materials and components, the basic salary of production and installation personnel, the estimates of installation are presented.

SUMMARY

A corporate network is a network which main purpose is to ensure the functioning of a particular enterprise that owns this network. Users of a corporate network are only employees and customers of the enterprise. Corporate networks do not provide services to enterprises and other users, unlike the networks of providers.

The corporate data transmission network (CDTN) is a unified information system of the enterprise that allows you to share the company's network resources – servers, computers and other devices connected to the network (such as printers, plotters, modems), as well as provide the necessary business applications such as network databases, file sharing, email, IP-telephony, customer relationship management (CRM), management systems (ERP-systems).

The basic principles of building corporate networks are: the transmission of all types of traffic should occur through a single communication channel; the corporate network should be built on the basis of open standards and interfaces in order to ensure the possibility of expanding the network and combining it with other networks; the corporate network must be a packet-switched network.

The most effective solution for building corporate data networks proposed by Cisco Systems. This solution is a modular approach to building a network structure and is based on a composite network model of the enterprise. This solution allows building both small networks that combine several offices, and large, including hundreds of nodes. This ensures the predictability of the qualitative characteristics of the network during its development by adding new modules or nodes, and requires minimal time for troubleshooting.

Research in the electronic way of communicating from remote locations began back in the 1960s with US military intelligence units. They created a packet switching network called ARPANET (Advanced Research Projects Agency Network) and first used TCP / IP. TCP / IP is described in detail as a packetization of all information, addresses, transmitted and received over the Internet. It utilizes four layers for performance: link, Internet, transport and application.

Clearly, the need for a private network to enhance Internet security has been obvious by that time. Security technology was first researched in 1993 by Professor John Ioannidis and his associates in think-tanks such as Columbia University and AT&T Bell Labs. His activities led to the creation of the Encryption Software (IP encryption software) IP protocol, also known as scrolling, the earliest form of VPN. It was an experimental work that sought to ensure confidentiality, integrity, and authentication for network users. Following this work, Wei Xu began his own research in 1994, focusing on IP security protocols, which ultimately led to the development of the IPsec system.

VPN technology has been developed for several decades. VPNs are used for local networks in which devices are connected to each other, in cases where one needs to use the Internet to make connections. Censorship and geo-restrictions are among key issues plaguing the Internet and innovative VPN technology solutions. The use of censorship in different countries has different reasons, but it usually involves blocking social networks, limited access to Internet media directories, monitoring user activities, email messages or a direct ban on access to the Internet.

IPsec is a set of protocols used to provide privacy and authentication services at the network level of the OSI model. These protocols can be divided into two classes – Protected Data Transfer Protocols (AH, ESP) and Key Exchange Protocols (IKE).

The network should regulate the access of divisions to various resources within the network itself. This regulation is achieved by using access control lists (ACLs) on routing devices. Depending on the configuration, ACLs perform the following tasks: limiting network traffic to improve network performance; traffic flow control; providing a basic level of security with respect to network access; traffic filtering based on the type of traffic; sorting nodes to allow or deny access to certain services.

A very important component of LAN configuration is the routing of traffic between nodes. Modern networks use both static routing protocols and dynamic routing protocols.

Static routing is the easiest way to route traffic between nodes. All routes are entered by the network administrator into the routing tables of the routers manually. Static routing is used only for objects that are not planned to be moved. It also becomes almost impossible to control the fault tolerance of the network, since it is difficult to configure backup channels because there is no one to monitor the availability of a particular network segment. Therefore, most often in networks with a large number of routers and nodes, dynamic routing is used.

There are many dynamic routing protocols. They are classified into two large groups: distance-vector; channel status protocols. Dynamic routing protocols are also divided at the place of application into: IGP (Interior Gateway Protocol) internal; EGP (Exterior Gateway Protocol) external.

The most popular IGP protocol to date is the OSPF (Open Shortest Path First) protocol. OSPF is a channel state protocol that uses the Dijkstra algorithm to find the best route.

To arrange communication between various autonomous systems the most popular is the Border Gateway Protocol (BGP). BGP is very convenient when building redundant access channels to external services through a third-party provider. BGP is currently the only protocol used for communication between autonomous systems.

The chose the most suitable equipment to model a local network several parameters should be considered.

While choosing router its structure should be taken into consideration. Also for the local computer network, it will be sufficient to use one high-speed port on the routing device, since all computers, other routers and firewalls will be connected via switching equipment. The data exchange speed should correspond to the parameters of the Internet connection, the amount of data transferred, and bandwidth is determined by these factors. A large amount of processed data makes it necessary to consider the amount of RAM when making the choice – the larger RAM is, the wider the device’s capabilities are [6].

When choosing switching equipment, one need to clearly understand what purposes it is intended for, how to use it and how to service it. To select a device that optimally meets your goals, and not to overpay the extra money, consider the basic parameters of the switches.

The firewall is designed to protect the user network from intrusions from the outside with traffic filtering mechanisms and setting rules for passing it into the local network. Its place in the network architecture is between the LAN equipment and the provider. In this regard, the starting points in choosing a firewall are the bandwidth of the device (in different modes of operation, it may differ slightly) and quantity: LAN ports, with a given transfer rate; WAN ports, taking into account the needs of redundancy; DMZ ports for server space organization.

The corporate network protection level is determined by the network security mechanisms used, the main of which are as follows:

– built-in protection against IPS intrusions, revealing the facts of unauthorized access to the network, detecting and blocking DoS attacks and malicious traffic;

– NAT-screen that broadcasts traffic based on specified rules, thereby limiting or allowing it, as well as playing the role of a gateway and hiding the corporate network from an external network;

– firewall, i.e. the network filter itself, restricting the transmission of packets on the specified ports and protocols;

– antivirus / anti-spyware and malware – an expanded software package similar in effect to the classic version;

– application control that identifies malicious content, regardless of port, protocol and IP address;

– web-filtering traffic at the source domain name level.

The need to use a certain mechanism determines the functionality of the selected firewall.

Selection of software to model a local network is also very important. In the dissertation advantages and the disadvantages of the GNS3 graphic network simulator and the EVE-NG graphic network emulator are considered. The main reasons GNS3 should be choose to model a local network are the full functionality of emulated devices, the ability to build heterogeneous networks, such characteristic as adding to the network of full-fledged workstations and servers. In general GNS3 is freely available and does not have any restrictions on use. The main advantage of using EVE-NG while modeling a local network is easy and quick creation of virtual environments for specific tasks, there is no need to buy expensive real equipment and software each time.

While designing a local network at the Heads office we took ino the account that the head office is the central point of the local computer network, the servers of which must process data from all remote nodes. To ensure a secure connection, the entire network can be divided into external and internal. The internal network will include the head office network, as well as the subnet of all bank branches.

The central device for routing traffic within the network will be the internal CISCO 3900 router. Through this router, secure channels will be organized to all branches in the bank. An external network is a network of cash machines and exchange points. To route traffic outside the network, it was decided to install an external CISCO 3900 router.

To ensure the safe passage of traffic from outside to the internal network, it is necessary to install the CISCO ASA firewall between the external and internal routers, which will regulate traffic between network zones. These devices will be connected to the switch at the central switch of the head office.

At CISCO ASA, the internal interface will be divided into subinterfaces, each of which will be bound to a separate VLAN.

A demilitarized zone with publicly available bank services, such as a website, a mobile application, etc. will be connected to the firewall. Most often, such a zone is called DMZ. Each DMZ service has its own separate VLAN.

The DMZ network will connect to the firewall through special switches.

Communication with the offices will be held via VPN tunnels, which will be encrypted using the IPSec protocol suite.

To build an internal local network, it is necessary to divide all branches outside the head office into groups and network zones. The general network can be divided into the following zones: head office network; networks of all branches; ATM network; a network of exchange points.

The total address space for the Bank network will be taken from the 10.83.0.0/16 subnet. Next, you need to divide this subnet into subnets for all branches.

According to the results or the research, the estimated cost of designing and implementing infrastructure for the fire alarm system and fire warning is 35,835.96 rubles. The economic effect of the development is the profit of the design and installation organizations ∑ P1 + P2 = 241,051.14 rubles.

CONCLUSION

In the dissertation, an analysis of the technologies for constructing local and corporate computer networks was made, an analysis of the principles of construction and characteristics of the equipment of computer networks, a model of a local computer network was developed and with its help an assessment was made of the working capacity, functionality, security and quality of functioning of the designed local network. In order to clarify the names of technologies (Ethernet, ATM, etc.), the name of the types of equipment (switch, router), simulation environment (GN3), protocols and devices with which security and quality of network operation are ensured (t .e. specific information from section 4 of the dissertation). Based on the results of the research we can make the following conclusions.

1 A corporate network is a network which main purpose is to ensure the functioning of a particular enterprise that owns this network. The basic principles of building corporate networks are: the transmission of all types of traffic through a single communication channel; the corporate network should be built on the basis of open standards and interfaces; the corporate network must be a packet-switched network.

2 To build a local computer network it is very important to select the appropriate equipment which will fulfill all the needed requirements and functions. To choose the most suitable router several parameters should be considered: the structure of the device; the tasks and the number of computers connected to the router, the parameters of the Internet connection, the amount of RAM. To select switching equipment first of all it is necessary to consider the basic parameters of different types of switches (controllable, uncontrollable, configurable) and their placement. To choose the firewall which protects the user network from intrusions from the outside with traffic starting points are the bandwidth of the device (in different modes of operation, it may differ slightly) and quantity.

3 Selection of software to model a local network is also very important. In the dissertation advantages and the disadvantages of the GNS3 graphic network simulator and the EVE-NG graphic network emulator are considered. The main reasons GNS3 should be choose to model a local network are the full functionality of emulated devices, the ability to build heterogeneous networks, such characteristic as adding to the network of full-fledged workstations and servers. In general GNS3 is freely available and does not have any restrictions on use. The main advantage of using EVE-NG while modeling a local network is easy and quick creation of virtual environments for specific tasks, there is no need to buy expensive real equipment and software each time.