Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Research of Services of Communication Operators for Creation of Corporate Data Transmission Networks

[1]Ziraddin Qasimov, [2]Elman Imamaliev,[3]Nizami Cafarov ,[4]Metanet Huseynova,[6]Nigar Jabrayilova

[1]Department of Computer Technologies, Associate Professor, Azerbaijan, Baku,

[2]Department of Computer Technologies, Associate Professor, Azerbaijan, Baku,

[3]Department of Computer Technologies, Associate Professor, Azerbaijan, Baku,
[4]Department of Computer Technologies, Associate Professor, Azerbaijan, Baku,
[6]Department of Computer Technologies, Azerbaijan, Baku,
[1,2,3,4,5,6]Azerbaijan Technical University (ATU), Azerbaijan

Abstract. The article discusses various ways to connect and build corporate data networks, explores their features and capabilities. In particular, the typical range of services of telecom operators, their features, and the possibilities of their use in a corporate data network are examined. Methods of connecting to data networks include: dial-up access, physical leased line, digital leased line in the telecom operator's network. All these communication channels have positive and negative sides, both in the speed and quality of communication, and in the cost and recovery methods. This article discusses the most universal and accessible type of communication - L3 Multiprotocol Label Switching multiprotocol label switching (MPLS) / Virtual Private Network - virtual private network (VPN) solutions for combining networks at the IP level or L2 MPLS \VPN solutions for combining networks at the IP level link level. If it is necessary to encrypt Ethernet traffic, special solution requires the installation of additional high-performance network equipment.

***Keywords*:** corporate network, VPN channel, critical traffic, virtual router, multiprotocol switching.

Introduction

It is known that any corporate network has its own characteristics, but they also have a lot in common. o build distributed corporate data networks (DCDN), services provided by data network operators are usually used. The specific service ordered from the operator depends on a number of requirements, including the availability of the service at the desired location. This article discusses the typical range of services of telecom operators offered for the construction of DCDN, their features, and the possibility of their use in a corporate data network.

It is known that different subsystems can be united by different, most suitable, communication channels. The connection method should be selected based on the requirements for the data network from the applications used in the company.[2]

Methods of connecting to data networks include: dial-up access, physical leased line, digital leased line in the telecom operator's network. All of these listed communication channels have their pros and cons both in the speed and quality of communication, as well as in the cost and recovery methods.

Among the methods considered, the most universal and affordable type of communication is the use of L3 Multiprotocol Label Switching multiprotocol label switching (MPLS) / Virtual Private Network - virtual private network (VPN) solutions for combining networks at the IP level or L2 MPLS \VPN solutions for combining networks at the IP level link level. Let's consider these types of communications separately.[4]

L3 VPN channel is currently the most actively developing service provided by data transmission operators. MPLS

networks continued the logical development of VPN networks based on FR and ATM channels. The MPLS network has the internal logic of IP networks - MPLS routers use IP addressing, and specially adapted IP routing protocols are used within the MPLS network.

Connecting to an MPLS network for a client looks like connecting to a regular IP network. At the same time, the provider can provide the client with a number of features that, when put together, make MPLS networks more attractive than connections via Frame Relay and ATM networks, these are, first of all:[3]

- end-to-end support within the operator network for several classes of service;

- the ability to save your own IP addressing plan;

- the ability to route IP traffic between the Customer's offices in the operator's network;

- organization of Internet access.

End-to-end support for multiple classes of service. Now in corporate networks there is an active transition to the so-called convergent data networks. This means that customers want to transfer all their data over a single network, from Internet and intranet traffic to voice and video traffic. Each traffic has its own special technical requirements for speed, delays, delay variations, acceptable packet losses and other parameters. If the customer is able to independently control these parameters within the LAN of each office, then when transmitting data through the global network he does not have this opportunity. This problem does not arise when using "clean channels", in which packets are transmitted sequentially, it is only important that the packets are sent in the right order. In the case of a packet data network, the customer wants to be sure that his priority traffic will be served by the provider first and with the required quality.[6]

Currently, all MPLS network providers support at least three classes of service. They can be called differently, but the main classes are as follows:

- real-time traffic class: the service parameters of this class provide for meeting the requirements for voice and video traffic. This means that the lowest latency is guaranteed for this class. In this case, a certain percentage of packet loss is acceptable (usually about 1%);

- critical traffic class: intended for the transmission of traffic that is critical for the customer's business (for example, database transactions, transmission of application data on which the customer's activities depend).

Typically, this class guarantees low latency and a minimum percentage of packet loss;

- "default" class: for this traffic class, usually only a threshold is set, which should not exceed packet loss (0.5_3%). This class should include customer traffic that is not business-critical or delay-sensitive (data received from the Internet, email, etc.).

Some providers support additional classes of service, such as a data class with a lower priority than the default class. The described feature allows the user to organize data transfer between offices with the required quality of service. Typically, the user must independently assign data to a particular class of service before transmitting it to the telecom operator's network. This is done by marking IP packets with one or another operator-agreed value of the DSCP field in the IP packet header.[5]

Classes of service support is present in Frame Relay networks, but by default there is only high- and low-priority traffic, which determines which packets can be dropped first when congestion occurs on the link. If there is a need to provide a larger number of classes of service, then you will need to organize several virtual channels between all nodes and independently distribute traffic of different priorities over them.

Ability to save your own IP addressing. This feature is important for companies that already have their own LANs and use their own, non-routable addresses to the Internet (and such companies are currently the absolute majority). This problem does not arise at all when using dedicated (physical or digital) channels. Support for traffic routing between offices lies in the fact that the provider's network can be presented to the customer in the form of some "distributed virtual router" that "knows" about the addresses used within the network and routes traffic between them.[7]

Customer networks can use static or dynamic routing to communicate with the provider's network. In this case, the provider usually allows the customer to configure interaction with his network using dynamic routing protocols and maintains a routing table for each customer separately. Dynamic routing ensures the organization of a fault-tolerant connection of customer office networks with automatic rerouting of traffic when part of the channels or equipment fails.

Typically, BGP is used as the communication protocol. The customer's network uses other dynamic routing protocols OSPF, EIGRP or RIP, or static routing. In this case, the customer must arrange for the transfer of information about available routes from one routing protocol to another.

Thus, it should be concluded that MPLS\VPN networks currently most fully provide the corporate customer with the necessary services for creating a distributed corporate data transmission network.

Two points should be noted as features of this connection:

1. IP traffic transmitted over the operator’s network is marked to place it in a particular service class by the customer himself using his equipment.

2. The customer must ensure traffic transmission at a speed not exceeding the agreed upon one. This requirement appears when the provider

a connection to the network is ordered at a speed of several megabits per second, and the connection is made via a Fast Ethernet interface with a physical speed of 100 Mbit/s. In terms of security level, VPN connections organized through the MPLS network are equal to Frame Relay channels, i.e. it is assumed that the traffic of one client cannot be accessed by other clients.

L2 VPN channel (usually Metro Ethernet) – to connect corporate networks at the Ethernet level, the most suitable solution would be to use either high-speed leased channels or L2 VPN services. For the customer, connection to L2 VPN channels is usually presented in the form of a connection to an Ethernet port (at a speed of 10 or 100 Mbit/s). In this case, the telecom operator’s network acts as a “virtual switch” that forwards packets between the LANs of individual offices. The number of offices is theoretically unlimited. It is possible to organize connections between offices using Ethernet trunks (IEEE 802.1q standard). In this case, the provider uses technology to encapsulate user VLANs into one of its VLANs using Q technology.[3]

However, with such a connection, it is often difficult to organize backup channels due to the fact that the provider may not allow the customer’s BPDU packets to pass through its network and there is a threat of loops in its Ethernet network. The advantages of such solutions for corporate users include low channel costs compared to similar solutions based on MPLS networks, ease of equipment configuration and cost, and the ability to transmit non-IP traffic.

The relatively low cost of organizing high-speed Ethernet channels allows us to consider this connection method for connecting customer networks at the IP level with the installation of routers at the end of the channel, which are often entrusted with the task of encrypting transmitted traffic.

Data sharing between clients in operator's Metro Ethernet networks is based on the use of VLAN-ID tags in the provider's networks. If sensitive data is transmitted over the network, additional measures are usually taken to ensure its security. A solution for encrypting Ethernet traffic at high speeds is not common. Therefore, if it is necessary to encrypt Ethernet traffic, special solutions are used. In particular, it uses encapsulation of Ethernet frames into IP packets, which are then encrypted before being transmitted to the Metro Ethernet network channels. This solution requires the installation of additional high-performance network equipment.[5]

It is often easier and less expensive to initially plan a data network so that connections between offices are made at the network (IP) level, or that data that requires additional security is encrypted before being transferred to the network at the application level.

References

[1] Information systems. News bulletin. – . Journal №2. (2008).

[2] «Cisco Voice Over IP. Student Guide», Cisco Systems. (2007).

[3] "Microsoft Internet Information Server. "Channel Trading Ltd.". (2017).

[4] Petrovski M. “Internet Information Server 4.0” - Transl. from English - K.: Publishing group "BHV". (2018).

[5] D. Awduche, J. Malcolm, J. Agogbua, M. O’Dell, and J. McManus, “RFC 2702, MPLS Traffic Engineering,” IETF, September (1999).

[6] C. Semeria, “RSVP Signaling Extensions for MPLS Traffic Engineering,” White Paper, Juniper Networks, Inc. (2000).

[7] Minoli, A Collection of Potential Network-Based Data Services, Bellcore/Telcordia

[8] Special Report, SR-NPL-000790, Piscataway, NJ. (1987).

[9] Fundamentals of modern cryptography. Barichev S., Serov R. Moscow-2001,

[10] https://cryptoworld.su/lesons-of-cryptography-1/

[11] Cryptographic interfaces and their use. Khorev P.B. - 2007 278 pp.

[12] https://avidreaders.ru/book/kvantovaya-kriptografiya.html

[13] Abdullaev S.G. (2007). Evaluating the effectiveness of the distance learning system. Telecommunications and informatization of education. No. 3. c. 85.

[14] Andreev A.A. (2003). Introduction to Internet education: textbook. allowance. M.: Logos. 76 p.

[15] Vasiliev V. (2004). Distance learning: an activity-based approach. Distance and virtual learning. No. 2. c. 6-7.

[16] Olnev A.S. (2011). Using new technologies in distance learning. Current problems of modern science. No. 1. c. 96.

[17] Samari S.M. (2009). Ways of using distance learning in the education system. Graduate student and applicant. No. 5. c. 84-88.