INVESTIGATION OF FUNCTIONAL AVAILABILITY FOR THE NETWORK ACCESS POINTS INFRASTRUCTURE

Alexander Berezhnoy, Jelena Levshina

Transport and Telecommunication Institute
Lomonosova str. 1, Riga, LV-1019, Latvia
Ph: +371 29110030, +371 29647434. E-mail: avb@tsi.lv

The given research deals with the analysis of computer network infrastructure for the purpose of outbound access to the company information resources and Internet global network. For this purpose network infrastructure chains supporting the key information services are selected. The construction of the conditions graph for the network access point service chains is carried out. The transformation of conditions graph and evaluation of reliability indexes such as final state probabilities and availability coefficient is made.

Keywords: *reliability, conditions graph, availability, computer network access point, information services*

1. Introduction

Due to the worldwide active development of network technologies there has been significantly changed the key ideas regarding the architecture of corporate communications as well as models of the company's digital information resources' access organization over the last decade. The occurred changes are mainly connected to evolution of bandwidth characteristics of data links, significant expansion of functionality, flexibility of network equipment configuration, and to increase in a degree of reliability of present network connections. Happening at the same time processes of perfection of known network applications and development of new forms of information interaction as a consequence, have led to expansion of network infrastructure evaluation criteria sets and significant strengthening of requirements to construction even typical network solutions.

Considering the modern architecture of a computer network first of all there are taken into account the existing needs of the present business critical applications on which functionality frequently depends on the viability of the whole organization. Providing the functionality and required productivity for the specified applications becomes the actual standard, by ignoring which, leads to failure of implementation for any modern corporate network solution. Along with the listed requirements there is also put a special stress on the demand to reliability, scalability and security of internal components, and the requirement for keeping the selected level of quality of service (QoS). The specified needs have complex nature and are covering both a hardware-software implementation of introduced services, as well as transport infrastructure of a network.

2. Information Resources' Access Organization Service Structure

Historically, at the stage of construction of Internet global public network, user end-point connections over the territorial networks, as a rule, are low speed and low reliable, the number of network services has been strongly limited, and security issues were realized at a primitive level on the Internet-service providers' side. A little bit later there has appeared a practice to accommodate the part of corporate resources, such as a public web-site of the company or Intranet environment on the provider servers. Hence the remote access technology necessary for servers' remote management began to grow. Comparatively simultaneously with the advent of electronic documents systems, the much greater attention began to be paid to protection of information resources located within the frames of a local area network. Modern throughput capacities of data links, provided QoS parameters relevant to levels of delays and frame losses have allowed to offer the alternative form of the company information resources' access organization at which all server segments are moved out to the specialized hosting platforms placed in the Data centres.

Such kind of network reorganization means the change in dislocation of a point for accessibility and maintenance of availability of given services. According to alternative ideology of network construction it is also accompanied by creation of the distributed concept of data protection and maintenance of a high level of availability of the distributed network infrastructure. Thus, for some reasons (for example, because of the cost factor, or because of close logical interdependence of used system resources) the companies frequently feel necessity in accommodation of a part of a server segment directly in the local area network that may lead to some problems that are peculiar only to the distributed network architecture. Realization of the requirement of territorial distribution in case of access reservation only at a level of cabling infrastructure is known as geographical diversification, meaning, that used physical data links of the company headquarters and branches should be completely independent, i.e. to run on various geographical routes and to use various switching units.

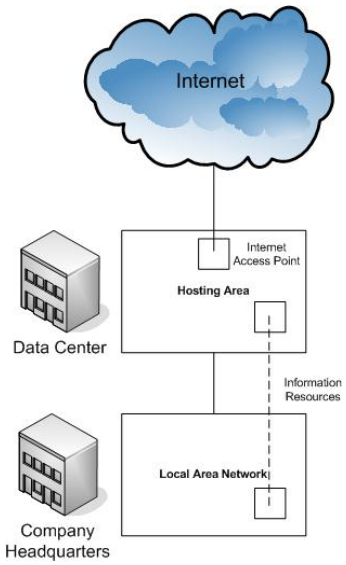

Figure 1. The structure of the access organization to information resources of the company

Needs for the reservation, going from requirements to reliability of the network decision can be satisfied at several levels and may consist only in reservation of data links, both data links and network equipment, or full reservation of all network, services infrastructure and carriers of information resources. In case of duplication of all kinds of resources, the mirror or truncated decision is placed in the other Data centre on a case of refusal of the primary service infrastructure.

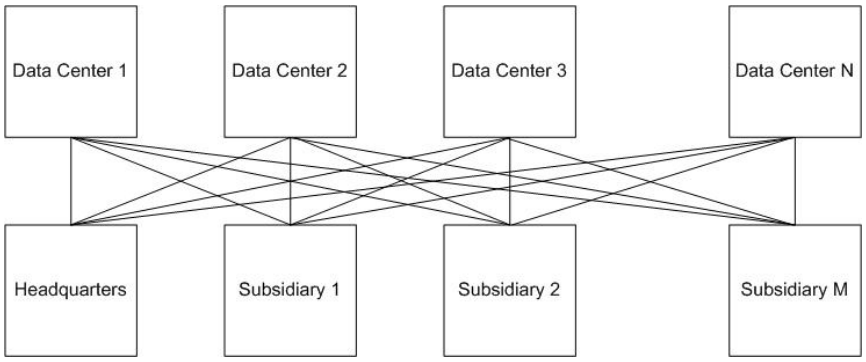

Figure 2. The block diagram of the organization of access to electronic resources of a network of the company having branches

Theoretically, thus it becomes possible to provide repeated reservation having put in parallel N Data centres; however in practice even the large companies introduce reasonable restrictions on the amount of hosting platforms, which are solving a problem of a hot reservation. It is a special case dealing with a cluster decisions, when using of the various Data centres decides not only the redundancy tasks for the information reserve storage and maintenance of uninterrupted availability of services, but also increases the services productivity due to balancing user data flows having territorial distribution. It is quite easy to count up that for the organization of the company connections possessing M branches it is required $L = N \cdot (M + 1)$ communication links.

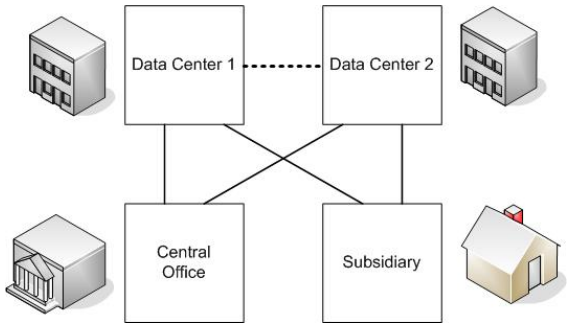

Figure 3. Synchronization channels of in the distributed network solution

Switching of data links between Data centres, as a rule, is performed in two general modes – hot passive reservation (Hot Standby), or hot active reservation (Active/Active). Hot active reservation is realized as more complex scenario supposing that services of both sides (the Fig. 3) are traffic loaded and functioning in an operating conditions as simultaneously, as in case of falling down of one of the sides. At turning-off of the service in one of Data centres all loading is operatively switched to the remained centres in a chain of a reservation. It is also expected that Data centres should be territorially diverse on a case of accident capable to stop work of one of hosting platforms. In case of the hot passive reservation scenario, the same is that switching is carried out automatically, but in a normal functioning mode all active streams of the data pass only through one Data centre. In the reserve Data centre from the primary one there should be performed a regular reserve copying under the given scheme. Thus it is constantly kept the time synchronization. Besides there should be present a binding link between Data centres, on which the synchronizing information and signals of malfunction of the equipment is transferred at both operation modes.

3. Architecture of the Information Resources' Access Solution

As it has been already stated before, while changing the dislocation of network access point to the company information resources and to the Internet global network at the Data centre, it is put forward a lot of criteria, which should be satisfied for a high-grade information activity of the company. One of typical decisions of a reliability maintenance problem is regarded to be hot reservation by means of network and information infrastructure duplication in the various Data centres. However the question of reliability maintenance strongly depends on internal functioning scheme of the outsourced network solution. One of possible architectural realizations of a network access point is resulted on Fig. 4. From the viewpoint of reliability the examined technical system is complex and is characterized by multi functionality.

The schematic solution of the remote point of network access organization is based on division of several zones of access within the framework of which processing of information flows before its further sending to destination addressees is carried out. Interaction with a company local area network is carried out through the encrypted data links. Streams of data of the central office on the part of the Data centre are terminated on the router, which acts as entrance access gateway. Segmentation of a network takes place at the gateway brandmauers separating physically and logically streams of the data intended for various servers, which are allocated in different de-militarised zones.

According to existing international requirements in the field of security, the functional roles should not be united within each of hardware devices. Differently, the router, capable to carry out blocking of the traffic should not manage it, and hardware firewalls should not be engaged in a filtration of a content, despite of presence of the similar built-in functionality. For the given reason service chains of communications may be extended enough that negatively influences final reliability of the decision.

Switching to the reserve data link in case of primary data link failure occurs on the basis of dynamic routing protocols (e.g., BGP, RIP, OSPF, etc.), Hot standby router protocol (HSRP), or application of events triggers notifying the reserve equipment about refusals. At presence of the several Data centres, where the network infrastructure of the primary network decision is duplicated, the information on infringement of service functioning or on refusal of the single device is transferred to the reserve Data centre by means of using the centre to centre synchronization channel. The most remarkable is the structure of the service functioning in case of failure of activity of one or several elements of a functional chain. Two alternatives are available – full switching to the network of other Data centre or flow redirection to the similar efficient device on other side with the subsequent return of the information stream to a network of the primary Data centre on the synchronization link, or with the further data processing in the reserve centre are possible.

From the viewpoint of reliability, the considered decision, first of all, should provide readiness of key services. In order to reveal the most critical services from the point of the company activities the matrix of information flows is constructed. A background for drawing up of a data flow matrix is a listing of used services: Mail, DNS, Web, File Transfer, IP Telephony, Video Conference, Remote Access, File Sharing, Skype, Internet Banking, LDAP, DHCP, Database Service, Custom applications, Terminal Services, etc. Time of continuous work of key services should be as long as possible.

Table 1. Data flow matrix

Incoming traffic (protocols)		**Outgoing traffic (protocols)**	
Internet	LAN	LAN	Internet
POP3, IMAP, DNS, HTTP/HTTPS, FTP/TFTP/SFTP, H.323, RTP, SIP, SMB, etc.		SMTP, DNS, HTTP/HTTPS, FTP/TFTP/SFTP, H.323, RTP, SIP, SMB, etc.	
Servers	LAN	LAN	Servers
POP3, IMAP, DNS, HTTP/HTTPS, FTP/TFTP/SFTP, SMB, RDP/Telnet/SSH, SNMP, Syslog, etc.		DNS, HTTP/HTTPS, FTP/TFTP/SFTP, SMB, RDP/Telnet/SSH, SNMP, etc.	

Incoming traffic (protocols)		**Outgoing traffic (protocols)**	
Internet	Servers	Servers	Internet
SMTP Relay, NTP, HTTP/HTTPS, SFTP, PPTP/L2F/L2TP, RDP/Telnet/SSH, etc.		SMTP, HTTP/HTTPS, SFTP, PPTP/L2F/L2TP, RDP/Telnet/SSH, etc.	
Internet	Subsidiaries LAN	Subsidiaries LAN	Internet
POP3, IMAP, DNS, HTTP/HTTPS, FTP/TFTP/SFTP, H.323, RTP, SIP, SMB, etc.		SMTP, DNS, HTTP/HTTPS, FTP/TFTP/SFTP, H.323, RTP, SIP, SMB, etc.	
Servers	Subsidiaries LAN	Subsidiaries LAN	Servers
POP3, IMAP, DNS, HTTP/HTTPS, FTP/TFTP/SFTP, SMB, etc.		DNS, HTTP/HTTPS, FTP/TFTP/SFTP, SMB, etc.	
Subsidiaries LAN	LAN	LAN	Subsidiaries LAN
SNMP, DNS, PPTP/L2F/L2TP, H.323, RTP, SIP, SMB, etc.		DNS, PPTP/L2F/L2TP, RDP/Telnet/SSH, NTP, H.323, RTP, SIP, SMB, etc.	

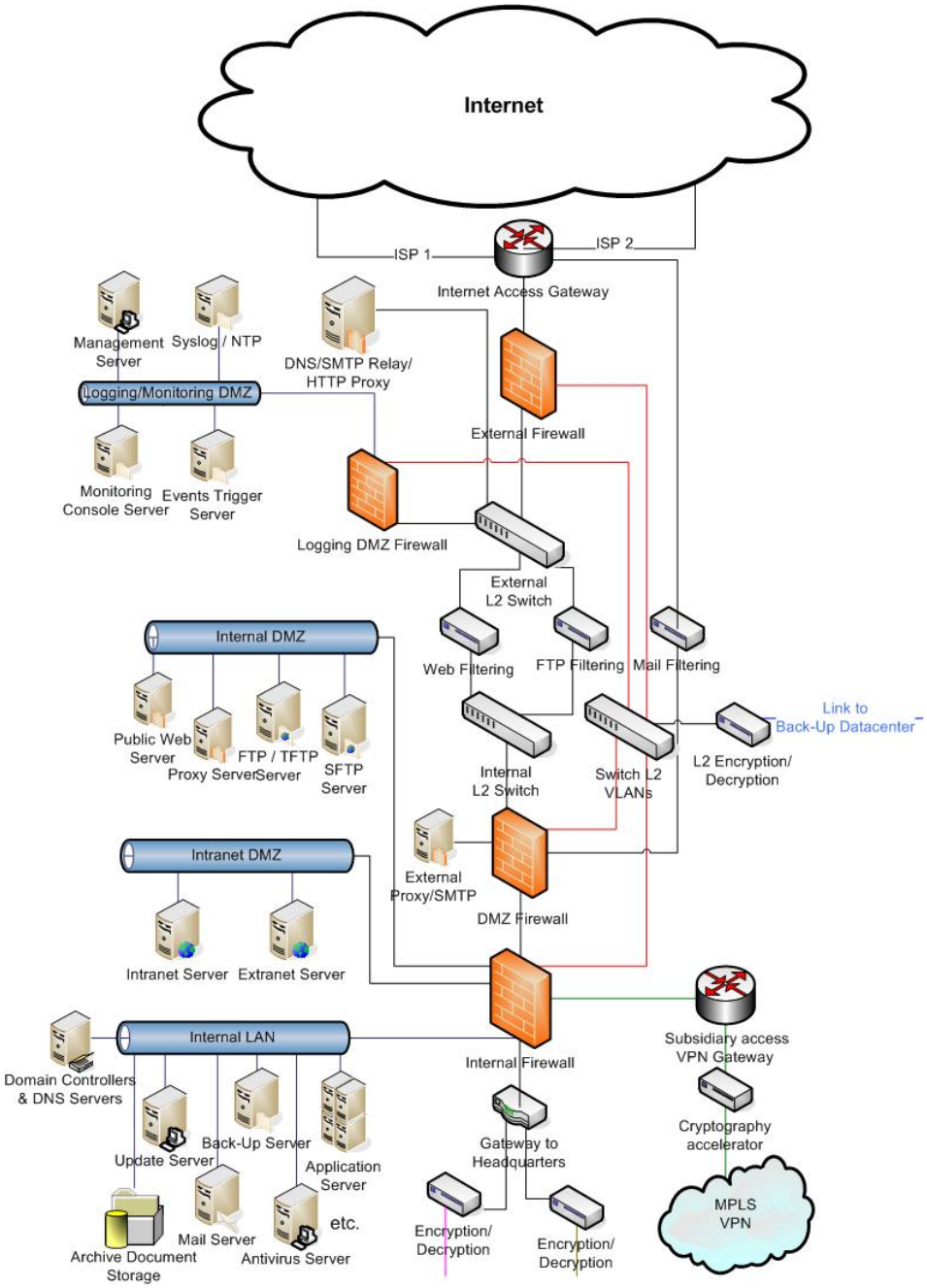

Figure 4. A functional chart of the company's network access solution

Constructing the network access solution the FCAPS (fault, configuration, accounting, performance and security) concept should be applied. Being the ISO model for network management, FCAPS provides a functional approach that segments management areas into discrete categories, which allows the network manager or management framework to address each in turn and ensure that no area is overlooked. According to the pointed base model, implemented services and serviceability of the equipment should be constantly supervised. For these purposes on some part of the equipment SNMP- and the Zabbix-agents are installed, allowing transferring trigger updates about all arising refusals and events, being the indicators of proper operation of devices in a real-time mode.

4. Services Reliability Analysis

For carrying out of the analysis of reliability of given services it is required to draw up chains of devices through which data flows are passing individually for each of selected services. We shall construct an example of revealing of functional bindings for the e-mail, web and ftp traffic (see Fig. 5, 7). On the block diagram λ represents failure rate of the corresponding unit, and μ corresponds to intensity of its restoration.

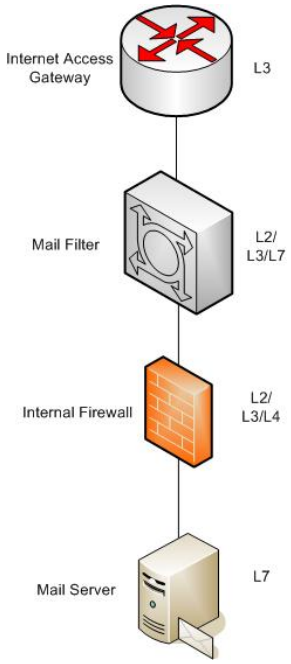

Figure 5. Mail traffic processing chain

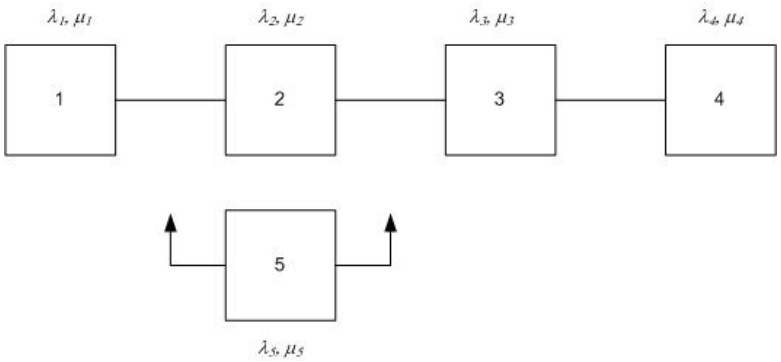

Figure 6. Mail service structure scheme

Let's designate as x_1, x_2, x_3, x_4 – conditions of system elements. For the block diagram of the mail service we shall make the table of the validity on four binary variables (Tab. 2). As y, it is designated the function of logics algebra for a system without reservation, and as y^* – for the system with the non-loaded (cold back-up) reserve (see Fig. 6).

Table 2. The table of validity of the mail service chain

x_1	x_2	x_3	x_4	y	y^*
0	0	0	0	0	0
0	0	0	1	0	0
0	0	1	0	0	0
0	0	1	1	0	0
0	1	0	0	0	0
0	1	0	1	0	0
0	1	1	0	0	0
0	1	1	1	0	0
1	0	0	0	0	0
1	0	0	1	0	0
1	0	1	0	0	0
1	0	1	1	0	1
1	1	0	0	0	0
1	1	0	1	0	0
1	1	1	0	0	0
1	1	1	1	1	1

In Table 2, "0" – corresponds to a failure condition of an element, and "1" – to a serviceable condition of an element. The efficient condition of system is described by the following logics algebra functions:

$y = x_1 x_2 x_3 x_4$, and $y^* = x_1 x_2 x_3 x_4 \vee x_1 \overline{x_2} x_3 x_4$.

Replacing disjunction and conjunction operations in the perfect disjunctive normal form of record to algebraic operations of multiplication and addition, and logic variables to corresponding probabilities of elements conditions, we shall receive probabilities of non-failure operation of system:

$$P_y = p_1(t) \cdot p_2(t) \cdot p_3(t) \cdot p_4(t),\ P_{y^*} = p_1(t) \cdot p_2(t) \cdot p_3(t) \cdot p_4(t) + p_1(t) \cdot q_2(t) \cdot p_3(t) \cdot p_4(t).$$

For the presented chain of mail service we shall construct the graph of conditions for the direct, inverse and set priorities of service. In case of the set priority of service as a priority element subject the device of a mail filtration is selected as primary for restoration. Thus for the set priority of service of the 2nd element, the graph of conditions will coincide completely with the graph of conditions of system with a direct priority of service.

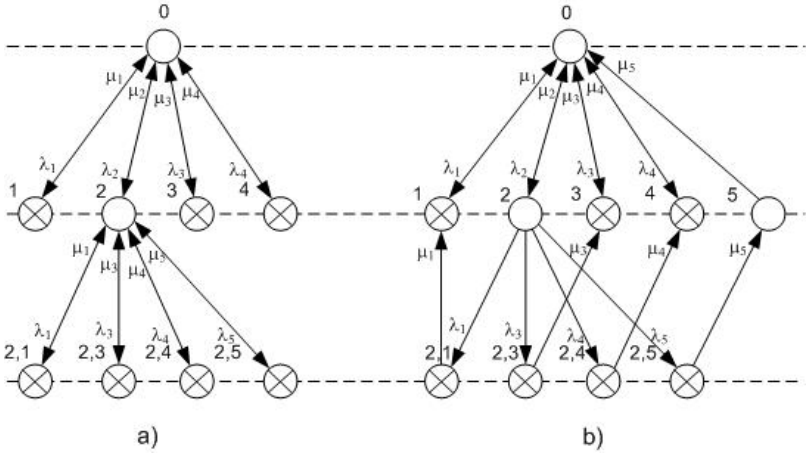

Figure 7. Graphs of conditions for a chain of mail service: a) with a inverse priority of service; b) with a direct priority of service

From the point of system's function it is important to note that filtration devices for information flows can be started both on data link, and on network layers of the open systems interconnection reference model. At realization of system at a data link layer, the filtration of the traffic occurs in transparent mode that does not allow applying the reservation protocols providing the automatic switching of a reserve. In order to keep the serviceability of the chain, application of such reservation protocols as STP (Spanning Tree Protocol) or RST (Rapid Spanning Tree), which are realized by configuring the corresponding protocols at switching devices becomes reasonable (Fig. 9).

Under condition of presence of superfluous financial resources some equipment like firewalls as the most expensive and labour-consuming in a configuration might also be reserved. But as against a problem of traffic filtration when refusal of function is not so critical for serviceability of the whole decision and the objective is to

provide uninterrupted connections, in case of firewalls failure the network becomes vulnerable. Therefore in such situation application of a cold reserve is more preferable (Fig. 10).

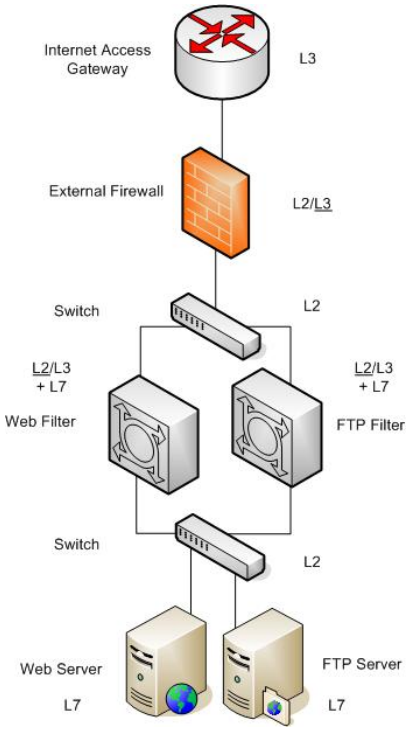

Figure 8. The chain of processing for the Web and FTP traffic

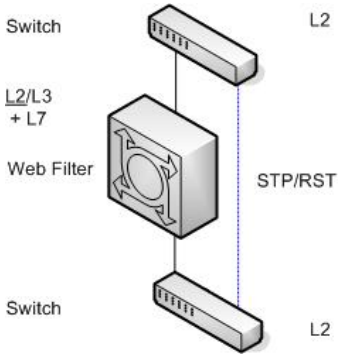

Figure 9. Reservation of connection in a chain of a Web-filtration

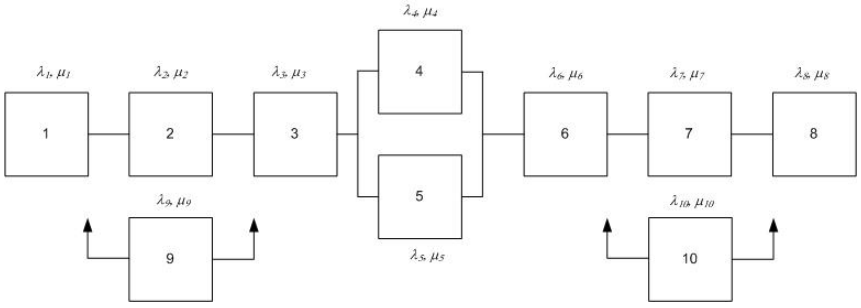

Figure 10. The block diagram of web-service

Similarly to an example with Mail service, we shall make the table of the validity for definition of serviceability in case of a Web-service chain. For this purpose we shall designate system elements conditions as $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$. As y it is designated the function of logics algebra for system (Fig. 10) only with the loaded reservation, and as y^* it is designated the function for the system with simultaneous use both loaded, and non-loaded reserve.

Table 3. The validity of web-service chain

№	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	y	y^*
173	1	0	1	0	1	1	0	1	0	1
175	1	0	1	0	1	1	1	1	0	1
181	1	0	1	1	0	1	0	1	0	1
183	1	0	1	1	0	1	1	1	0	1
189	1	0	1	1	1	1	0	1	0	1
191	1	0	1	1	1	1	1	1	0	1
237	1	1	1	0	1	1	0	1	0	1
239	1	1	1	0	1	1	1	1	1	1
245	1	1	1	1	0	1	0	1	1	1
247	1	1	1	1	0	1	1	1	0	1
253	1	1	1	1	1	1	0	1	0	1
255	1	1	1	1	1	1	1	1	1	1

The efficient condition of system is described by the following function of logics algebra:

$$y = x_1x_2x_3\overline{x_4}x_5x_6x_7x_8 \vee x_1x_2x_3x_4\overline{x_5}x_6x_7x_8 \vee x_1x_2x_3x_4x_5x_6x_7x_8,$$

and

$$y^* = x_1x_2x_3x_4x_5x_6x_7x_8 \vee x_1x_2x_3x_4x_5x_6\overline{x_7}x_8 \vee x_1x_2x_3x_4\overline{x_5}x_6x_7x_8 \vee x_1x_2x_3x_4\overline{x_5}x_6\overline{x_7}x_8 \vee x_1x_2x_3\overline{x_4}x_5x_6x_7x_8 \vee$$
$$\vee x_1x_2x_3\overline{x_4}x_5x_6\overline{x_7}x_8 \vee x_1\overline{x_2}x_3x_4x_5x_6x_7x_8 \vee x_1\overline{x_2}x_3x_4x_5x_6\overline{x_7}x_8 \vee x_1\overline{x_2}x_3x_4\overline{x_5}x_6x_7x_8 \vee x_1\overline{x_2}x_3x_4\overline{x_5}x_6\overline{x_7}x_8 \vee$$
$$\vee x_1\overline{x_2}x_3\overline{x_4}x_5x_6x_7x_8 \vee x_1\overline{x_2}x_3\overline{x_4}x_5x_6\overline{x_7}x_8.$$

According to the block diagram submitted on Fig. 10 let's construct the graph of system conditions, assuming that the type of service with an inverse priority is chosen. The probability to find restored system in a condition i during the fixed moment of time t in Laplace's transformation can be written down in the following form:

$$P_i(s) = \frac{\Delta_i(s)}{\Delta(s)} = \frac{B_{0i}s^{m_i} + B_{1i}s^{m_i-1} + \ldots + B_{mi}}{s\left[A_0s^{n-1} + A_1s^{n-2} + \ldots + A_{n-1}\right]},$$

where $\Delta(s)$ – the main determinant of the differential equations system, written down in Laplace's transformations; $\Delta_i(s)$ – a partial determinant of system [1].

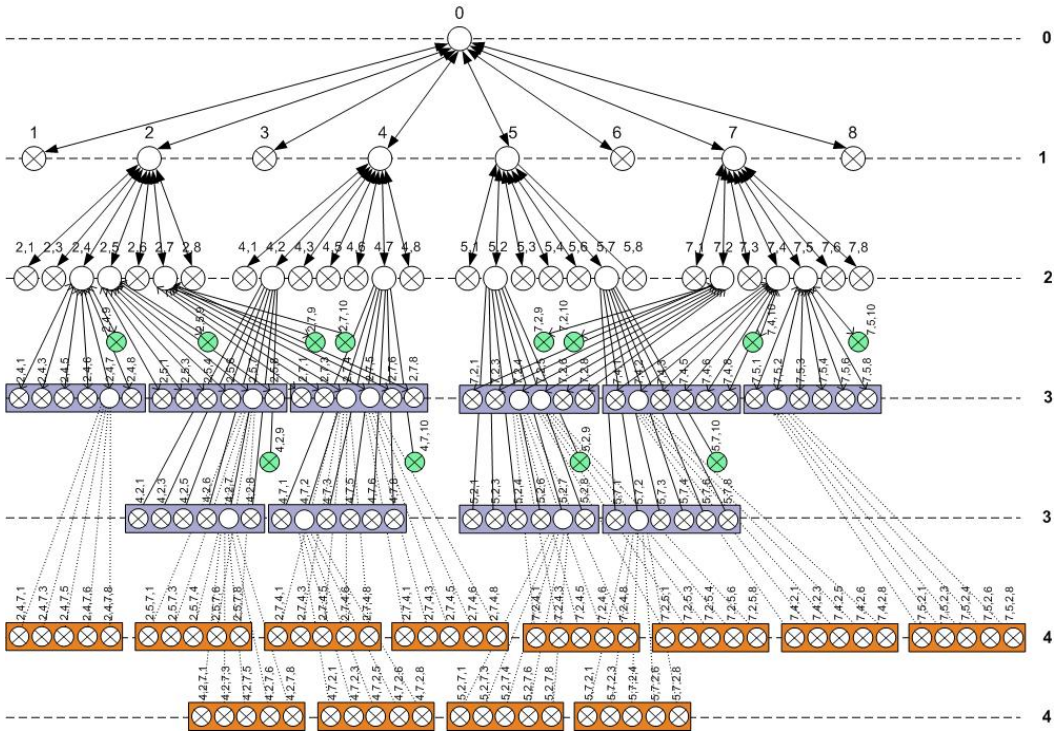

Figure 11. Graph of the system conditions represented on Fig. 10

In practice switching devices designated on plans as switches, as a rule, are virtual segments of one switchboard to which connection of all devices in a chain is made. Besides, occurrence of failure on edge devices is accompanied by automatic switching of a route to the alternative gateway in the other Data centre. Thus, considering the above-stated disclosure, graph of web-service system conditions can be simplified to some extend. It is also important to take into account that in a real life direct or the appointed priority of service more often is used.

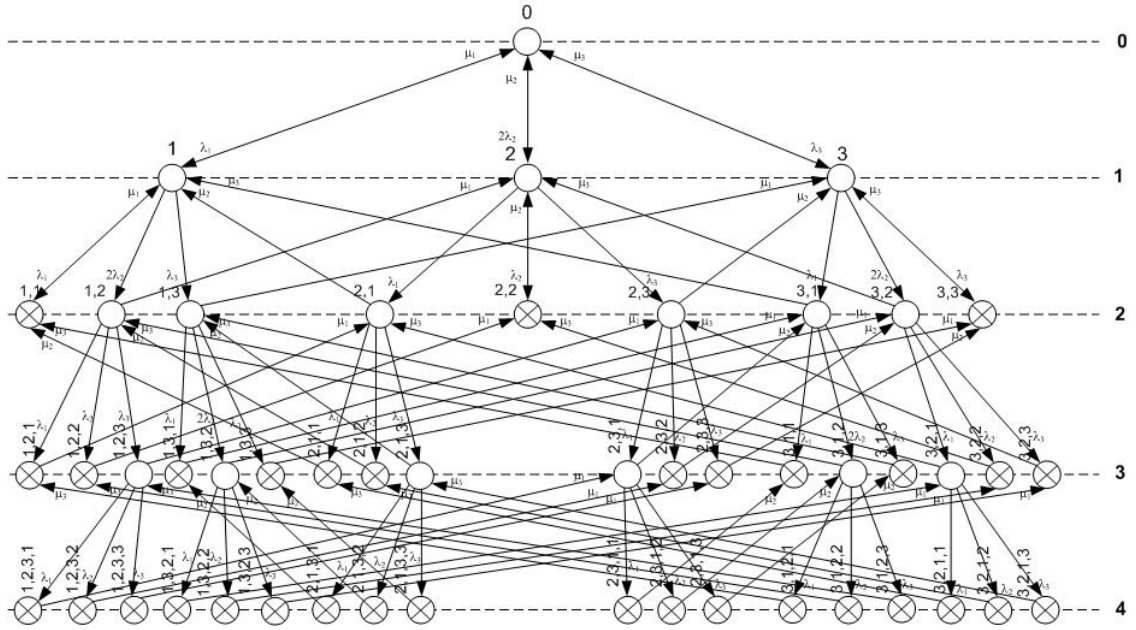

Figure 12. Simplified graph of web-service system conditions for a direct service priority

The investigated system has 49 conditions (Fig. 12). For definition of parameters of its reliability in regard of a service priority it is necessary to solve equations system of the 49-th order. At the chosen type of a service priority the solution can be received directly from the conditions graph.

The availability coefficient described by final probability of system in a serviceable condition is calculated on resulted conditions graph:

$$K_A = \frac{\Delta_p}{\Delta_p + \Delta_q},$$

where Δ_p – the members corresponding to serviceable conditions of system, Δ_q – the members corresponding to failure conditions of system [2].

$$\Delta_p = \mu_1^{16}\mu_2^{16}\mu_3^{16} + \lambda_1\mu_1^{15}\mu_2^{16}\mu_3^{16} + 2\lambda_2\mu_1^{16}\mu_2^{15}\mu_3^{16} + \lambda_3\mu_1^{16}\mu_2^{16}\mu_3^{15} + 2\lambda_1\lambda_2\mu_1^{14}\mu_2^{16}\mu_3^{16} + \lambda_1\lambda_3\mu_1^{14}\mu_2^{16}\mu_3^{16} +$$
$$+2\lambda_1\lambda_2\mu_1^{16}\mu_2^{14}\mu_3^{16} + 2\lambda_2\lambda_3\mu_1^{16}\mu_2^{14}\mu_3^{16} + \lambda_1\lambda_3\mu_1^{16}\mu_2^{16}\mu_3^{14} + 2\lambda_2\lambda_3\mu_1^{16}\mu_2^{16}\mu_3^{14} + 2\lambda_1\lambda_2\lambda_3\mu_1^{13}\mu_2^{16}\mu_3^{16} +$$
$$+2\lambda_1\lambda_2\lambda_3\mu_1^{13}\mu_2^{16}\mu_3^{16} + 2\lambda_1\lambda_2\lambda_3\mu_1^{16}\mu_2^{13}\mu_3^{16} + 2\lambda_1\lambda_2\lambda_3\mu_1^{16}\mu_2^{13}\mu_3^{16} + 2\lambda_1\lambda_2\lambda_3\mu_1^{16}\mu_2^{16}\mu_3^{13} + 2\lambda_1\lambda_2\lambda_3\mu_1^{16}\mu_2^{16}\mu_3^{13}$$

$$\Delta_q = 2\lambda_1^2\lambda_2\lambda_3\mu_1^{12}\mu_2^{16}\mu_3^{16} + 2\lambda_1\lambda_2^2\lambda_3\mu_1^{12}\mu_2^{16}\mu_3^{16} + 2\lambda_1\lambda_2\lambda_3^2\mu_1^{12}\mu_2^{16}\mu_3^{16} + 2\lambda_1^2\lambda_2\lambda_3\mu_1^{12}\mu_2^{16}\mu_3^{16} +$$
$$+2\lambda_1\lambda_2^2\lambda_3\mu_1^{12}\mu_2^{16}\mu_3^{16} + 2\lambda_1\lambda_2\lambda_3^2\mu_1^{12}\mu_2^{16}\mu_3^{16} + 2\lambda_1^2\lambda_2\lambda_3\mu_1^{16}\mu_2^{12}\mu_3^{16} + 2\lambda_1\lambda_2^2\lambda_3\mu_1^{16}\mu_2^{12}\mu_3^{16} +$$
$$+2\lambda_1\lambda_2\lambda_3^2\mu_1^{16}\mu_2^{12}\mu_3^{16} + 2\lambda_1^2\lambda_2\lambda_3\mu_1^{16}\mu_2^{12}\mu_3^{16} + 2\lambda_1\lambda_2^2\lambda_3\mu_1^{16}\mu_2^{12}\mu_3^{16} + 2\lambda_1\lambda_2\lambda_3^2\mu_1^{16}\mu_2^{12}\mu_3^{16} +$$
$$+2\lambda_1^2\lambda_2\lambda_3\mu_1^{16}\mu_2^{16}\mu_3^{12} + 2\lambda_1\lambda_2^2\lambda_3\mu_1^{16}\mu_2^{16}\mu_3^{12} + 2\lambda_1\lambda_2\lambda_3^2\mu_1^{16}\mu_2^{16}\mu_3^{12} + 2\lambda_1^2\lambda_2\lambda_3\mu_1^{16}\mu_2^{16}\mu_3^{12} +$$
$$+2\lambda_1\lambda_2^2\lambda_3\mu_1^{16}\mu_2^{16}\mu_3^{12} + 2\lambda_1\lambda_2\lambda_3^2\mu_1^{16}\mu_2^{16}\mu_3^{12} + 2\lambda_1^2\lambda_2\mu_1^{13}\mu_2^{16}\mu_3^{16} + 2\lambda_1\lambda_2^2\mu_1^{13}\mu_2^{16}\mu_3^{16} +$$
$$+\lambda_1^2\lambda_3\mu_1^{13}\mu_2^{16}\mu_3^{16} + \lambda_1\lambda_3^2\mu_1^{13}\mu_2^{16}\mu_3^{16} + 2\lambda_1^2\lambda_2\mu_1^{16}\mu_2^{13}\mu_3^{16} + 2\lambda_1\lambda_2^2\mu_1^{16}\mu_2^{13}\mu_3^{16} + 2\lambda_2^2\lambda_3\mu_1^{16}\mu_2^{13}\mu_3^{16} +$$
$$+2\lambda_2\lambda_3^2\mu_1^{16}\mu_2^{13}\mu_3^{16} + \lambda_1^2\lambda_3\mu_1^{16}\mu_2^{16}\mu_3^{13} + \lambda_1\lambda_3^2\mu_1^{16}\mu_2^{16}\mu_3^{13} + 2\lambda_2^2\lambda_3\mu_1^{16}\mu_2^{16}\mu_3^{13} + 2\lambda_2\lambda_3^2\mu_1^{16}\mu_2^{16}\mu_3^{13} +$$
$$\lambda_1^2\mu_1^{14}\mu_2^{16}\mu_3^{16} + 2\lambda_2^2\mu_1^{16}\mu_2^{14}\mu_3^{16} + \lambda_3^2\mu_1^{16}\mu_2^{16}\mu_3^{14}.$$

Conclusions

As a result of company information resources' access point network infrastructure analysis there have been noted the key elements that should be reserved in order to perform uninterrupted functioning of the selected services. The conditions graph indicating the possible states of the considered system has been constructing. After making the necessary transformations the reliability analysis of proposed technical solution has been carried out. For this reason the final probabilities for elements of being in the given state have been obtained. And the analytical expressions giving the possibility to calculate the availability coefficient of the investigated key services hardware chains were obtained. Defined coefficients also allow solving the selection problem of the reliable network access point infrastructure. It appears to be useful from the practical point of view at designing or modernizing of access to company's information resources as well as Internet access.

References

1. Polovko, A.M. *The basis of the reliability theory.* St. Petersburg: BXV-Petersburg, 2006. 704 p.; illustr.
2. Kammosev, N.F., Konditerov, P.F. *Investigation of the systems by graph methods*. Riga, 1974.