ISSN 2278-3091

Volume 9, No.4, July – August 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse07942020.pdf

https://doi.org/10.30534/ijatcse/2020/07942020

Local Area Network Monitoring: The Issue of Broadcast Storm

Maxim Sergeevich Logachev[1], Ivan Vladimirovich Voronin[2], Valentina Valentinovna Britvina[1,3], Sergey Alexandrovich Tichtchenko[4], Alexei Valerievitch Altoukhov[4]

[1]Moscow Polytech University, Moscow, Russia

[2]P.M. Vostrukhin College of communications no. 54, Moscow, Russia

[3]MSTU STANKIN, Moscow, Russia

[4]Lomonosov Moscow State University (MSU), Moscow, Russia

ABSTRACT

This article describes the main methods of analysis of local area network (LAN). Detection of broadcast storm is an issue upon such monitoring. Storm is one of the main failure causes of operation of corporate LAN, which can result in property and reputation damage if it is not prevented at the level of monitoring of network resources or at the level of network settings. This work describes in details the tools and mechanisms of revealing, elimination, prevention of storm spreading. The results are presented as formal models reflecting execution of business processes at the enterprise while organizing monitoring (BPMN diagrams) and reflecting system of planning and resource usage upon implementation of respective process (EPC diagrams). The main protocols of LAN monitoring are analyzed, which is an important factor to understand settings of equipment and overall LAN. The obtained results can be applied for designing and development of comprehensive system of failure prediction or monitoring of corporate LAN.

Key words: network, process model, network protocols, network monitoring, local area network, network segmentation, VLAN.

1. INTRODUCTION

Operation of modern companies requires for IT infrastructure providing not only data transfer but also capability to adopt decisions and to execute various business operations. Integration of such infrastructure into unified network would provide the following:

- resource sharing by means of granting access for a set of end users to one and the same device;
- data sharing by granting access for users in accordance with their professional duties and levels of access;
- software sharing for efficient operation of each company officer [1, 2].

Routing in such network can be both static and dynamic. In the case of static routing, it is possible to perform rapid and simple configuration only in small sized networks due to moderate load on network processor [3, 4]. Herewith, it should be understood that scaling capability is complicated because of necessity to create numerous route entries. In addition, it will be required to keep records on routing, fault tolerance will decrease, arrangement of reserve channels will be complicated [5].

In the case of dynamic routing, fault tolerance is high, configuration of reserve channels is relatively simple, it is possible to maintain automated traffic balancing. As a consequence, the load on network processors increases, unpredictable results can occur during debugging of such network [6].

While designing network, it is required to account for all possible risks, which can occur upon further operation of network. More often, already at the designing stage, the loads on future network are not considered and possible scaling up is not implanted. However, during network operation it is necessary to carry out continuous monitoring of all constituents of the network. Sufficiently wide range of modern and scientifically substantiated technical and engineering solutions should be used for their analysis and monitoring [7].

Nowadays the network monitoring systems are characterized by certain drawbacks. Thus, scaling leads to the decreased network monitoring, not complying with initially preset parameters, including such important variable as maximum time of error detection [8]. This can be attributed to increased intervals between polling of network equipment. Available software uses free resources not optimally and is not adapted to various networks. In most cases, monitoring is based on resources already used by other applications at this time [9].

2. METHODS

Specialized software is used to detect problems occurring in corporate LAN. The most popular monitoring systems are listed below [10]:

1. Cacti is an open-source tool allowing to plot network load on the basis of selected statistical data. It has not only standard templates for equipment monitoring (for instance, servers, routers, switches, etc.) but also facilitates development of additional templates by third-party developers. The default settings of the software are SNMP protocol and Perl or PHP scenarios. With the aim of monitoring, data can be visualized in the form of plots per any time interval (including online mode), showing, for instance, traffic loading by network equipment. Internal solutions for gathering information on CPU load and RAM usage are not provided. The main drawback is no response to events and their automatic correction.
2. Nagios is a software for system and network administrators supported by users and third-party developers. It provides wide range of functions for LAN monitoring (for instance, controlling disk space on server, checking load of RAM and CPU). Flexible mechanism of notifications by e-mail and messengers is available. The software allows displaying controllable active network equipment in logical presentation of respective network. Basic version of the software provides monitoring of workstations, their CPU load, usage of HD space. A significant drawback of Nagios is configuration tuning using only command line as well as unavailability of data storage after monitoring.
3. Zabbix is a network monitoring software with web interface. Its operation is supported by program agents installed in controlled hosts, or by using SNMP protocol. Hosts for checking are added manually or automatically. The software operation is based on various templates, monitoring can be performed only for certain (meaningful) network properties, certain network issues can be eliminated using trigger settings, plots of capacity data for network objects are displayed (for instance, network capacity, CPU load); customized cards, monitors, and slide show are supported to display current state of equipment.
4. 10-Strike LANState Pro is a monitoring system of remote LAN, verifying accessibility of hosts, servers with subsequent notification of fault or failure in the form of report (notifications can be sent to e-mail). Numerous parameters are monitored, including CPU load. Templates for various checks can be used by the software (for instance, analyzing statistics on traffic usage with variations using NetFlow protocol).

Analysis of the LAN monitoring software has demonstrated that functional capabilities of the products are similar. Table 1 summarizes the obtained results (only basic versions are considered without additional plugins).

Table 1: Specifications of LAN monitoring programs

	Cacti	Nagios	Zabbix	10-Strike LANState Pro
Type	Open source	Open source	Open source	Shareware
Web interface	+	+	+	+
Response to network events	–	+	+	+
Templates	+	+	+	–
Hardware monitoring	–	+	+	+
Notifications	E-mail	E-mail, SMS	E-mail, SMS	E-mail, SMS
Network traffic analysis	–	–	–	+
Long-term data storage	+	–	+	+
GUI	+	–	+	+

Application of this or that software depends on the properties of corporate LAN and problems solved by its monitoring [11]. Herewith, a significant drawback of all mentioned software products (and many others, not reviewed here) is unavailability to trace and to prevent broadcast storm.

Broadcast storm nearly instantly blocks transfer of useful traffic in all network and swamps the port bandwidth with exponentially increasing data packets [12]. The reason of such situations can be both hacker attacks and errors upon adjustment of equipment as well as protocol faults.

Active network equipment is generally examined in order to detect reasons of broadcast storm [13]. At least two experts are involved in this procedure. Model of checking of all active equipment is illustrated in Figure 1.

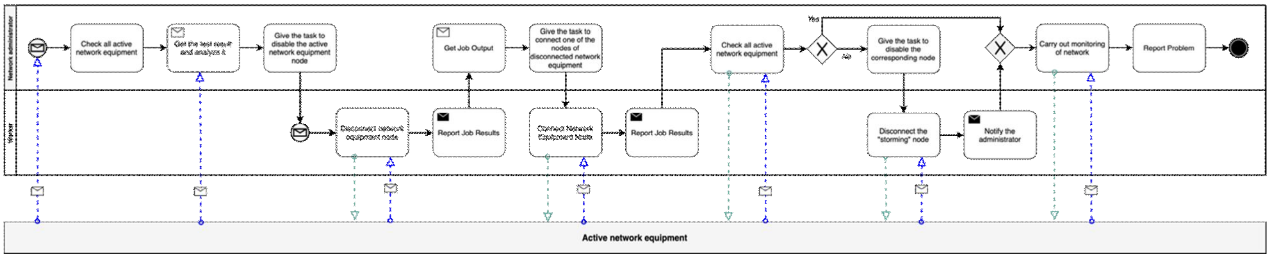
Network administrator
Worker
Check all active network equipment
Get the test result and analyze it
Give the task to disable the active network equipment node
Disconnect network equipment node
Report Job Results
Get Job Output
Give the task to connect one of the nodes of disconnected network equipment
Connect Network Equipment Node
Report Job Results
Check all active network equipment
Yes
No
Give the task to disable the corresponding node
Disconnect the "storming" node
Notify the administrator
Carry out monitoring of network
Report Problem
Active network equipment

Figure 1: BPMN diagram of checking active network equipment in order to detect broadcast storm

3. RESULTS

Numerous procedures are available to eliminate broadcast storms in LAN. They are as follows [14]:

1. Limiting of broadcast traffic to 10% (or 1%). This indicator depends on the model of active network equipment. This is a simple and low efficient method.
2. Activation of loopback detection on switches. A special frame is transferred to LAN, when it returns, it is assumed that the port is switched to storming segment. The drawback of this method is comprised of frequent failures, since at wide-scale storms the LAN is completely paralyzed.
3. LAN segmentation. Figure 2 illustrates the model of LAN segmentation, which allows to create isolated virtual segments.

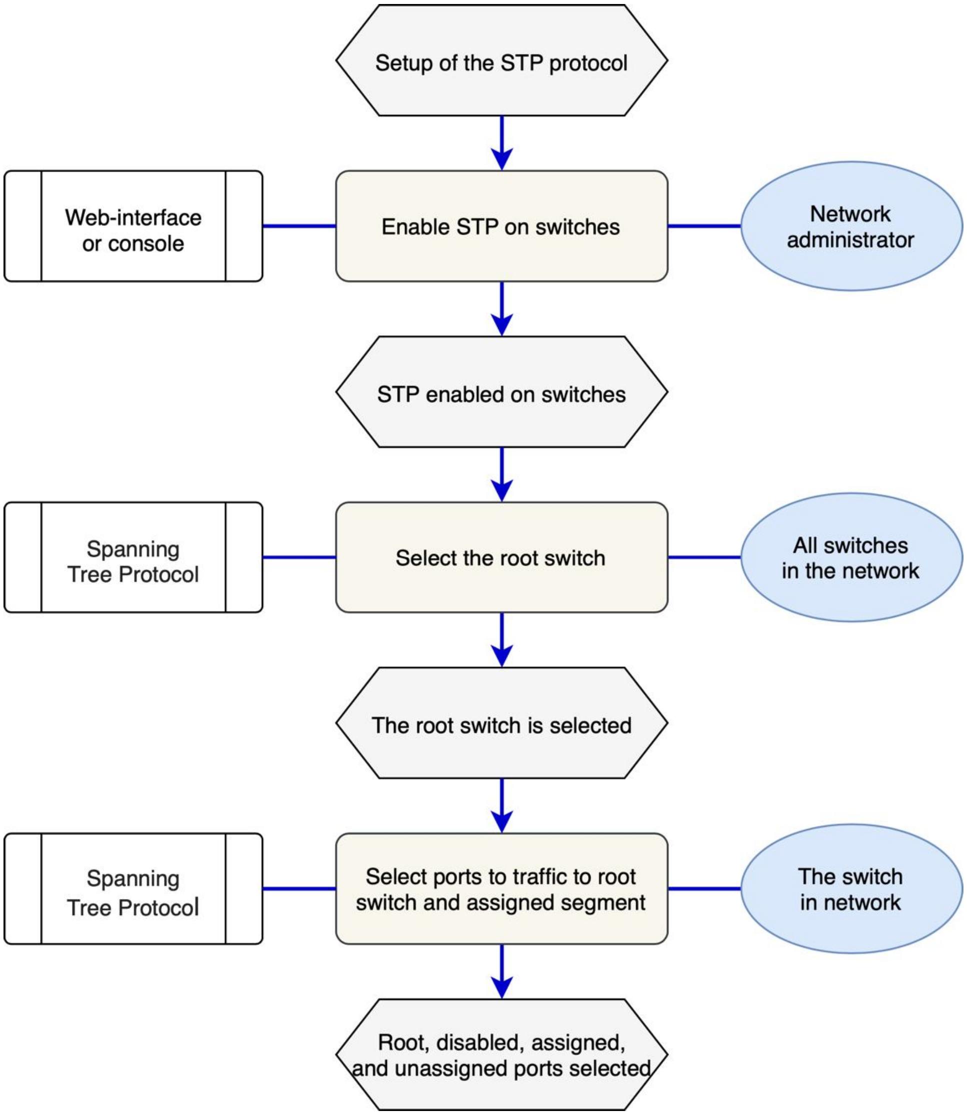
Setup of the STP protocol
Web-interface or console
Enable STP on switches
Network administrator
STP enabled on switches
Spanning Tree Protocol
Select the root switch
All switches in the network
The root switch is selected
Spanning Tree Protocol
Select ports to traffic to root switch and assigned segment
The switch in network
Root, disabled, assigned, and unassigned ports selected

Figure 2: Model of network segmentation using U type topology

Safety level can be increased by application of FHRP protocols and U type topology at the access level. In some cases, it is quite difficult to refuse loopback since it is required to arrange fault tolerant infrastructure, for instance, with connection to the Cloud. Client virtual networks are located inside the cloud infrastructure between all hosts of virtualization cluster obtaining complete duplication of all LAN elements [12, 15]. Two solutions to the problem can exist in this case. Models of problem elimination are illustrated in Figure 3.

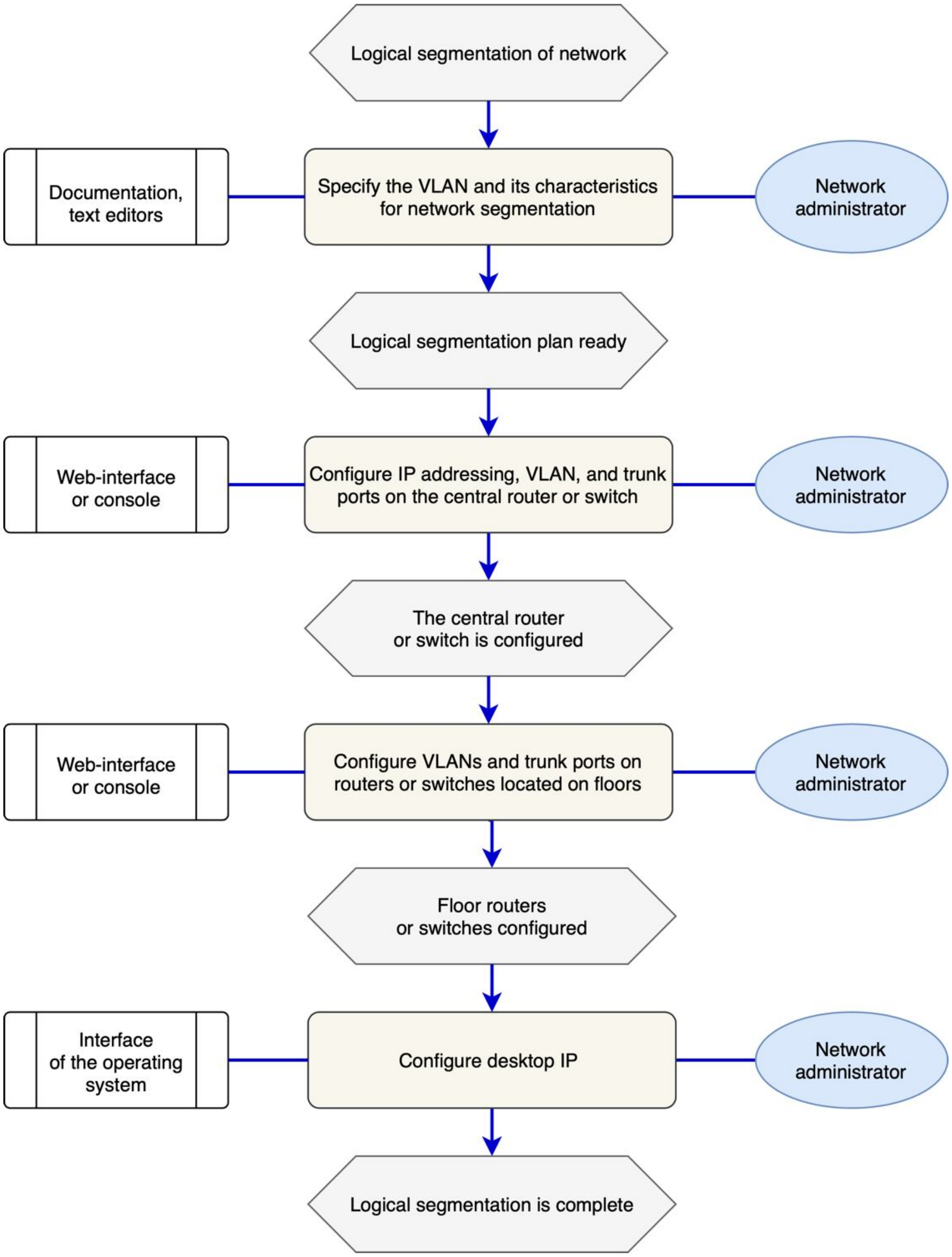
Logical segmentation of network
Documentation, text editors
Specify the VLAN and its characteristics for network segmentation
Network administrator
Logical segmentation plan ready
Web-interface or console
Configure IP addressing, VLAN, and trunk ports on the central router or switch
Network administrator
The central router or switch is configured
Web-interface or console
Configure VLANs and trunk ports on routers or switches located on floors
Network administrator
Floor routers or switches configured
Interface of the operating system
Configure desktop IP
Network administrator
Logical segmentation is complete

Figure 3: Model of reservation of communication channels and corporate infrastructure

RSTP protocol can be used for storm elimination, it allows to detect and to break broadcast loops [12, 16, 17]. Such variant is more preferable for data centers, not for companies with continuously increasing number of clients. Such companies can apply MSTP protocol allowing to combine several VLAN into one STP process (additional operator with corresponding qualification is required for administration) [18, 19].

An alternative to MSTP can be, for instance, FlexLinks allowing to reserve switch links or stack under single control. The model of such tool is illustrated in Figure 4*a*. Figure 4*b* illustrates the alternative to this model.

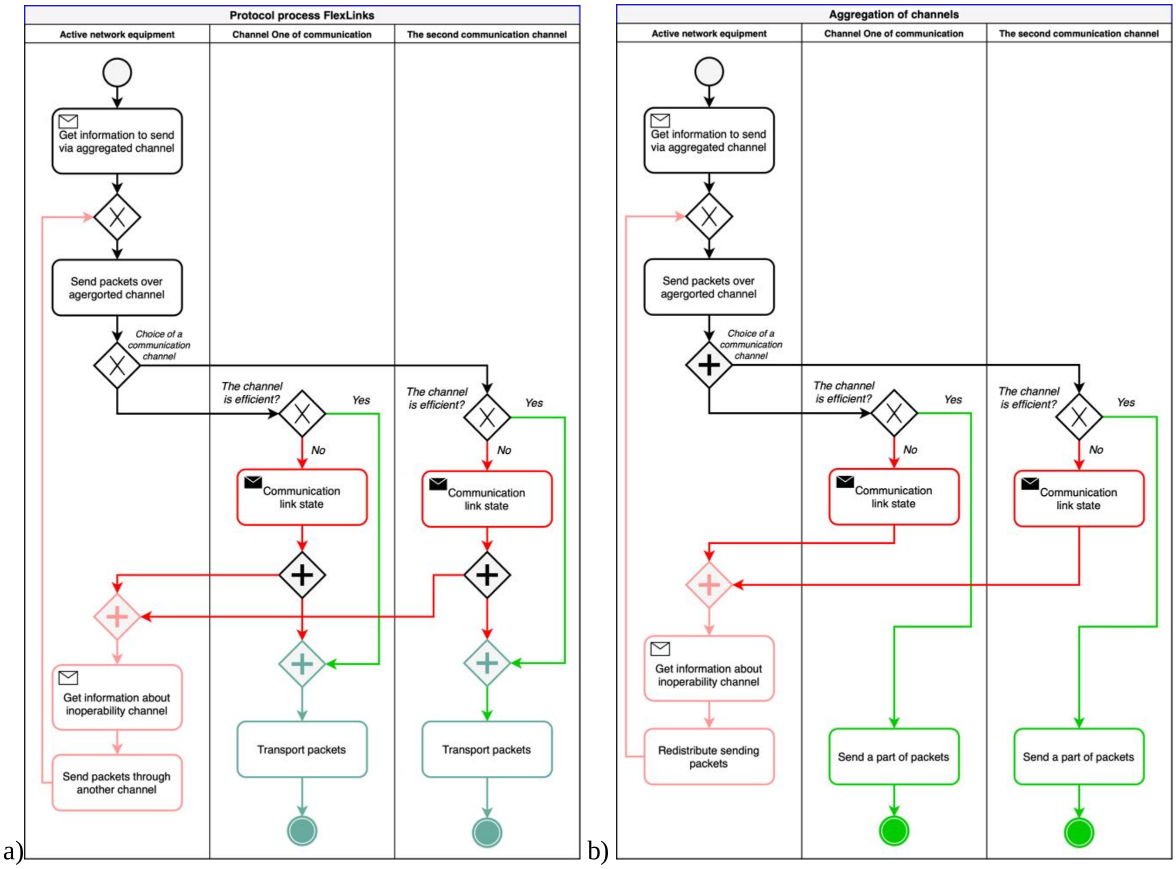
Protocol process FlexLinks
Active network equipment
Channel One of communication
The second communication channel
Get information to send via aggregated channel
Send packets over agergorted channel
Choice of a communication channel
The channel is efficient?
Yes
No
Communication link state
Get information about inoperability channel
Send packets through another channel
Transport packets
a)
Aggregation of channels
Active network equipment
Channel One of communication
The second communication channel
Get information to send via aggregated channel
Send packets over agergorted channel
Choice of a communication channel
The channel is efficient?
Yes
No
Communication link state
Get information about inoperability channel
Redistribute sending packets
Send a part of packets
b)

Figure 4: Models of link integrations: a) FlexLinks, b) mLag

In this case all available links are used, combined into one logical channel. Thus, a switching cluster is obtained where control module of a switch controls all cluster links. If a switch fails, its rights are transferred to the next active switch. Such approach is used in CiscoVSS [16, 20], NexusvPS, Juniper virtual router and other mLag technologies [21]. Therefore, monitoring of corporate LAN parameters can be presented by the model illustrated in Figure 5.

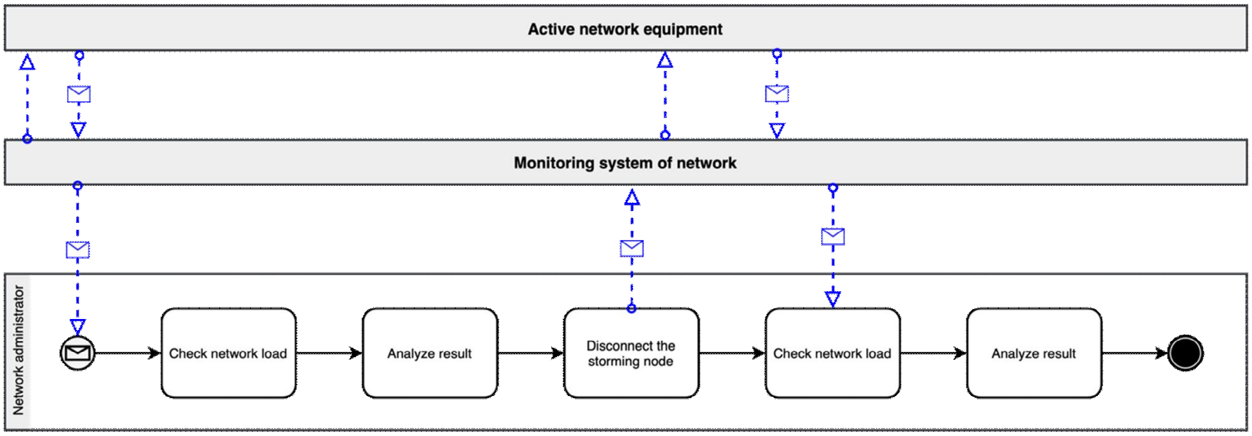

Figure 5: Model of LAN monitoring with accounting for detection of broadcast storm

Monitoring system should provide not only continuous control of LAN state but also possibility of forecasting and diagnostics of state of maintained data systems in short and long terms. Such system should support maximum possible accuracy of analysis of LAN units and not affect the operating data systems (that is, should minimize the impact on intensity of administrative traffic exchange).

Numerous variants are available to monitor LAN. Most of them control switches, servers, databases, etc. This allows not only to obtain online information about failures of communication channels, process shutdowns but also to eliminate a problem prior to its critical status (for instance, data loss).

Any modern monitoring software should be efficient, allowing not only to analyze capacity and behavior of certain devices and overall LAN but also to be a tool to make decision for configuration, prevention of various faults, etc. Analysis of processes in corporate LAN as well as principles of application of existing monitoring systems allows to estimate all features of system operation for faultless operation of overall company.

Analysis of the processes has demonstrated that there exists opportunity to integrate such numerous tools of LAN capacity monitoring into a consolidated system. Combination of the tools in one software makes it possible not only to control LAN capacity but also to create unified data storage, for which reports and intelligent solutions would serve as the basis for further faultless operation of corporate system.

4. CONCLUSION

Therefore, the obtained results are the basis to study the monitoring processes aiming at development of universal platform for LAN monitoring, unified platform-independent routing protocol, control system of active network equipment, improvement of network event analysis system.

REFERENCES

1. A.A. Lavrov. **Methods and algorithms of LAN monitoring based on combined analysis of time and functional properties of TCP/IP stack**. Synopsis: Cand. Thesis. St. Petersburg State Electrotechnical University "LETI", St. Petersburg, 2013.
2. D.A. Pal'tsin, A.Yu. Tsym. **Monitoring setei svyazi pri pomoshchi kompleksnoi otsenki ikh tekhnicheskogo sostoyaniya** [Communication network monitoring based on integrated assessment of their technical state]. Proceedings of the 12th International conference: Technologies of information community, Moscow, March 4–15, 2018. Moscow: Media Publisher, pp. 223-226, 2018.
3. T.N. Izosimova, Ch.O. Bochko. **Razrabotka avtomatizirovannoi sistemy monitoringa oborudovaniya i programmnogo obespecheniya kompyuternoi seti** [Development of automated monitoring system of hard- and software of computer network]. Proceedings. Innovative development of science and education, Penza, February 15, 2018. Penza: Nauka i Prosveshchenie, pp. 80-82, 2018.
4. A.A. Lavrov, A.R. Liss, V.V. Yanovskiiю ***Monitoring i administrirovanie v korporativnykh vychislitelnykh setyakh*** *[Monitoring and administration in corporate LAN]: Monograph*. St. Petersburg, SPbGETU LETI, 2013.
5. A.K. Skuratov. **Statistic monitoring and analysis of telecommunication networks**: Doctoral Thesis: 05.13.13. Moscow State Institute of Electronics and Mathematics, Moscow, 2007.
6. Networks for children. Linkmeup. Available at: https://linkmeup.ru/
7. M.S. Logachyov. ***Informatsionnye sistemy i programmirovanie. Spetsialist po informatsionnym sistemam. Vypusknaya kvalifikatsionnaya rabota*** *[Information system and programming. IT system technician. Qualifying project] Guidebook*. Moscow: Infra-M, 2020. DOI: 10.12737/1069178
8. V.G. Olifer, N.A. Olifer. ***Kompyuternye seti. Printsipy, tekhnologii, protokoly*** *[Computer networks. Principles, technologies, protocols]: Guidebook*. St. Petersburg: Piter, 2020.
9. M.S. Logachyov. ***Informatsionnye sistemy i programmirovanie. Administrator baz dannykh. Vypusknaya kvalifikatsionnaya rabota*** *[Information system and programming. Database administrator. Qualifying project]: Guide book*. Moscow: Infra-M, 2020.
10. I.V. Stepanova, M.O.A. Abdulvasea. **Ispolzovanie perspektivnykh tekhnologii dlya razvitiya raspredelennykh korporativnykh setei svyazi** [Advanced technologies for development of distributed corporate communication networks]. *T-Comm*, 6, pp. 10–15, 2017.
11. N.A. Latushko, M.N. Chesnakov, M.V. Mitrofanov. **Sposob povysheniya intellektualizatsii sistem monitoringa sostoyaniya setei svyazi** [Improvement of intellectualization of monitoring systems of communication networks]. Proceedings of the 15th All-Russian Conference: Neurocomputers and their application, Moscow, March 13, 2018. Moscow: MGPPU, pp. 99-100, 2018.
12. "Ideal storm" and how to prevent it. DataLine. Available at: https://habr.com/ru/company/dataline/blog/253609
13. O.Yu. Bogoyavlenskaya. **Raspredelennaya mnogoagentnaya sistema monitoringa i prognozirovaniya proizvoditelnosti transportnogo urovnya setei peredachi dannykh** [Distributed multi-agent system of monitoring and capacity prediction of data transfer networks]. *Programmnaya inzheneriya*, 9(1), pp. 11–21, 2019. DOI: 10.17587/prin.9.11-21
14. A. Tanenbaum, D. Wetherall. ***Computer Networks***. 5th edition. Prentice Hall, Inc., 2011.
15. A. Alkhayal, D.B. Flaks, M.Yu. Perukhin, et al. **Modernizatsiya lokalnoi vychislitelnoi seti**. *Vestnik Kazanskogo tekhnologicheskogo universiteta*, 3, pp. 240–241, 2013.
16. L.T. Yag'yaeva, E.A. Molchanov, L.F. Mubarakshin. **Seti peredachi dannykh [Data transfer networks]**. *Vestnik Kazanskogo tekhnologicheskogo universiteta*, 19, pp. 369–371, 2014.

17. IPRouting. Cisco. Available at: https://www.cisco.com/c/en/us/tech/ip/ip-routing/index.html
18. D.O. Storozhuk. **Methods and algorithms for LAN monitoring systems**: Cand. thesis: 05.13.13. Moscow State Engineering Physics Institute, Moscow, 2008.
19. V.A. Sharai, A.V. Sorokinaю **Algoritmicheskoe obespechenie sistemy adaptivnogo monitoringa kompyuternykh setei** [Algorithmic provision of LAN adaptive monitoring]. *Nauchnye trudy KubGTU*, 3, pp. 396–408, 2018.
20. CiscoIOSNetFlow. Cisco. Available at: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html
21. Traffic monitoring and accounting using NetFlowv5/9. 10-Strike Software. Available at: https://www.10-strike.ru/network-monitor/help/monitoring/netflow.shtml