Simulating of Fault-Tolerant Gateway Based on VRRP Protocol in OMNeT++ Environment*

Ilya I. Noskov[1][0000-0002-5489-4092] and Vladimir A. Bogatyrev[1][0000-0003-0213-0223]

[1] Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics, Kronverksky prospect, 49, Saint Petersburg, 197101, Russian Federation
noskovii@mail.ru

Abstract. Ways of improving the fault-tolerance of local computer network gateways using the Virtual Router Redundancy Protocol (VRRP) are considered. VRRP protocol is analyzed in the OMNeT++ simulation environment that has models of real communication channels and TCP/IP network protocols. The method of constructing computer network models with a fault-tolerant gateway based on the VRRP protocol in the OMNeT++ environment is proposed in the paper. The paper provides a description of all the main stages of creating and carrying out experiments with a computer network model. All windows of the simulation environment in which the model is parameterized and settings are considered in detail. The paper also describes the internal language of the OMNeT++ environment for the development of computer network models - NED. The process of creating scripts that allow simulating various events in the simulation process, such as the break of the communication channel between devices or the failure of the device is considered in detail. ANSA-INET is the OMNeT++ framework, which contains many modules and implementations of network protocols, including the FHRP family of protocols. This framework is used as the main framework for developing models in this paper. Capabilities of this framework are shown while simulating the VRRP protocol for creating a fault-tolerant gateway in the local area network.

Keywords: Simulating, Fault-Tolerant Gateway, Computer Networks, VRRP, OMNeT++.

1 Introduction

At present, the number of real-time systems with high requirements for functional and structural reliability has significantly increased in conditions of destructive impacts on the channel or active network equipment [1-4]. That is why reliability and fault-tolerance researching of information and communication systems and networks is carrying out nowadays [5-6]. The choice of design solutions for the construction of information and communication systems is based on analytical or simulation modeling [7-10].

* Copyright 2019 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-2522/paper11.pdf

Gateway is an important element for traffic forwarding in local area computer networks because it links this network with others. Failure of this element can lead to the inoperability of the entire subnet and the loss of large amounts of data. To ensure gateway reliability in local computer networks, it is necessary to use device redundancy and using specialized gateway protocols for developing a cluster of routers.

For effective interaction of computer nodes of distributed systems, it is necessary to build networks with a redundancy of elements of active network equipment, with the support of multipath routing [11-14] with the possibility of choosing an alternative route to the destination node for balancing traffic. The transport coding allows reducing the average delays of messages in the network with the multipath coupling of nodes [15–16]; the effect is achieved due to the coding that it is possible to recover the entire message without repeating transmissions. In redundant real-time information and communication systems, increasing the likelihood of timeliness and reducing the average latency of servicing requests allows for redundant maintenance, which creates copies of requests made by different nodes of the system or by different sequences of nodes [17-19]. Redundant query service can be effectively applied in cluster architecture systems and in multipath data transmission systems that are sensitive to delays.

The aim of this work is building reliable fault-tolerant network solutions based on the development of simulation models in the OMNeT++ environment, which allow using real communication tools and network protocols to ensure the fault-tolerant of gateways [20-24].

2 Fault-tolerance of gateways

The fault-tolerance of computer networks at the network level is ensured by the reservation of active network equipment and/or communication channels, as well as the use of specialized protocols. There are a whole family of First Hop Redundancy Protocols (FHRP) protocols that allow building fault-tolerant computer networks with redundant switching nodes. This is achieved by combining several routers into one virtual router that responds to ARP requests and distributes traffic to currently active router from the entire cluster. If the active router fails, another router from the group assumes its role, and the traffic actually continues through the other router. Thus, in a computer network, reliability, and probability of delivery of packages to the destination node increase.

3 Virtual Router Redundancy Protocol

VRRP is a network protocol from the FHRP family designed to increase the availability of routers acting as a default gateway. This is achieved by combining a group of routers into one virtual router and assigning them a common IP address, which will be used as the default gateway for computers on the network.

At any time, only one of the physical routers performs traffic routing, that is, it becomes the main VRRP router, the rest of the routers in the group become redundant. If the main router becomes unavailable, then one of the backup ones assumes its role - the one with the highest priority.

The basic concepts of the VRRP protocol are:

- VRRP Router — a router with running VRRP protocol. It can participate in one or more virtual routers.
- Virtual Router (VR) — is an abstract object managed by VRRP protocol. Performs the role of the default router for computers in the network. A virtual router is a group of router interfaces that are on the same network and share a Virtual Router Identifier (VRID) and a virtual IP address.
- IP Address Owner — VRRP router that uses the IP address assigned to the virtual router as the real IP address assigned to the interface.
- ADVERTISEMENT — messages that are sent by the Master-router.
- Virtual IP address — is the IP address assigned to the interface of one of the routers that make up the Virtual Router. Also known as Primary IP Address. VRRP adverts always use the virtual IP address as the sender's address.
- VRRP Master router — is VRRP router that is responsible for sending packets sent to an IP address that is associated with a virtual router and for responding to ARP requests sent to this address. If the owner of the IP address is available, then it always becomes the Master.
- VRRP Backup router — is a group of routers that are in standby mode and are ready to take on the role of the VRRP Master router as soon as the current VRRP Master router becomes unavailable.
- Virtual MAC address — is 0000: 5E00: 01xx, where xx is the number of the VRRP group.

VRRP is designed to increase the availability of routers that use as a default gateway in the local area network.

For a group of routers, they are configured to belong to a virtual router. In fact, a virtual router is a group of router interfaces that are on the same network and share a Virtual Router Identifier (VRID) and virtual IP address.

A VRRP router can be in multiple virtual routers, each with a unique VRID/IP address combination. The correspondences between the VRID and the IP address must be the same on all routers on the same network.

At any given time, only one of the physical routers performs traffic routing, that is, it becomes a VRRP Master router, the rest of the routers in the group become a VRRP Backup router. If the current VRRP Master router becomes unavailable, then one of the VRRP Backup routers - the one with the highest priority - assumes its role. Setting priority allows you to define more priority routers administratively.

The backup router will not attempt to intercept the role of the master router unless it has a higher priority than the current master router. VRRP allows administrative blocking of the master-router role. The only exception to this rule is that the VRRP router will always become the Master if it owns the IP address that is assigned to the virtual router.

In each virtual router, only the master sends periodic VRRP messages to the reserved group address 224.0.0.18. At the data link layer, the virtual MAC address is used as the MAC address of the sender of VRRP announcements.

For researching of this protocol, it is necessary to develop models for the simulation-modeling environment, which will allow a detailed review of the operation of the protocol on various network configurations and topologies.

4 Develop a simulation model and carry out experiments

The specialized environment for computer network simulating OMNeT++ was chosen for creating and researching simulation models of computer networks with fault-tolerant gateway because it is cross-platform, contains a large library of network components and models of network protocols in different network layers, has a convenient graphical interface and detailed English-language documentation.

OMNeT++ simulating environment is a cross-platform specialized environment for simulating computer networks for various purposes. This program is written in C++ language and allows modifying its modules in this language, as well as building models using a graphical editor or a specialized model description language. The simulation results are available to the user in the form of tracing events or data arrays, from which you can automatically build informative graphs and charts. Since this environment is an open-source environment, the user has access to many different libraries and modules written by various developers and researchers. It has a great number of different implementations of the vast majority of network protocols from the OSI stack. In addition, it has components of the VRRP protocol based on router models that support this protocol.

The ANSA-INET library contains models of routers with the implementation of the VRRP protocol for simulating computer networks with a fault-tolerant gateway. Fig. 1 shows the computer network model that was developed in the OMNeT++ environment:

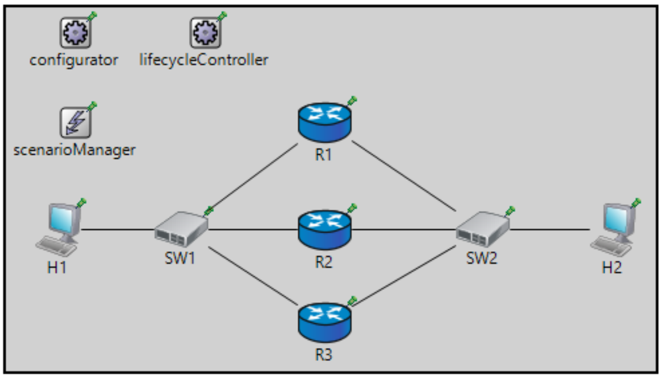
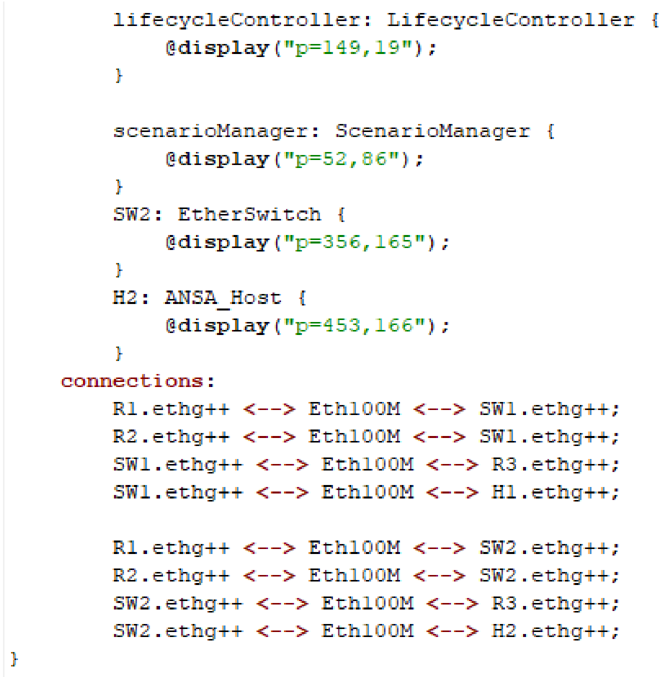


Fig. 1. Model of a computer network

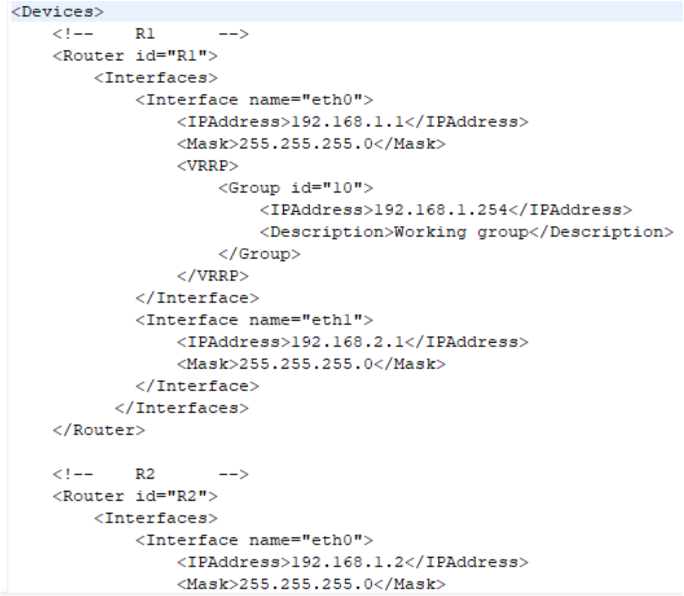
The OMNeT++ simulation environment allows you to build computer network models not only using a graphical user interface but also with using specialized NED language. This language has a C-like language and allows us to create models without using a graphical environment. This can be useful when we build large networks consisting of a big amount of different nodes. Fig. 2 shows an example of a network configuration that was built via this language.



```
        lifecycleController: LifecycleController {
            @display("p=149,19");
        }

        scenarioManager: ScenarioManager {
            @display("p=52,86");
        }
        SW2: EtherSwitch {
            @display("p=356,165");
        }
        H2: ANSA_Host {
            @display("p=453,166");
        }
    connections:
        R1.ethg++ <--> Eth100M <--> SW1.ethg++;
        R2.ethg++ <--> Eth100M <--> SW1.ethg++;
        SW1.ethg++ <--> Eth100M <--> R3.ethg++;
        SW1.ethg++ <--> Eth100M <--> H1.ethg++;

        R1.ethg++ <--> Eth100M <--> SW2.ethg++;
        R2.ethg++ <--> Eth100M <--> SW2.ethg++;
        SW2.ethg++ <--> Eth100M <--> R3.ethg++;
        SW2.ethg++ <--> Eth100M <--> H2.ethg++;
}
```

Fig. 2. NED fragment of the computer network model in the OMNeT++ environment

In this model, H1 and H2 nodes are clients. Clients send network traffic to each other. SW1 and SW2 - switches. These switches connect subnets of H1 and H2 clients. R1, R2, and R3 routers are a group of routers that have VRRP protocol to provide fault-tolerance to the H1 client's subnet gateway. For working with the VRRP protocol, the ANSA-INET framework provides a special type of the ANSA_VRRP_Router router. In the model of this router, we can configure this protocol. The configuration of a cluster of routers with VRRP protocols provides via using a special configuration file, which is provided by the ANSA-INET library. Fig. 3 shows a fragment of the router's configuration.

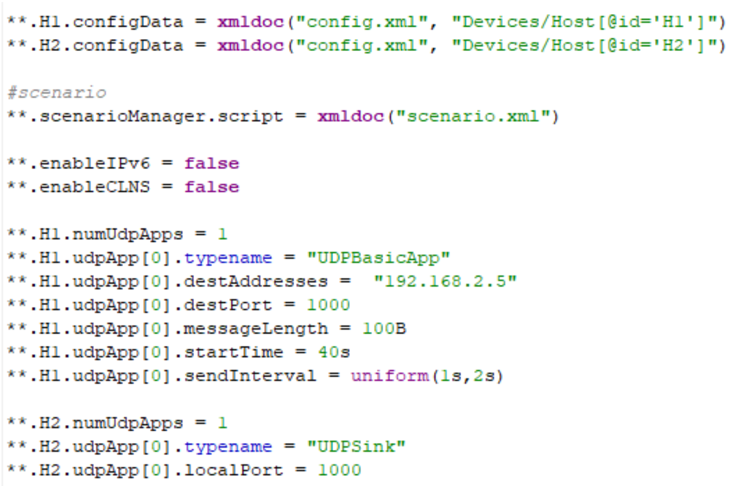


```
<Devices>
    <!--    R1      -->
    <Router id="R1">
        <Interfaces>
            <Interface name="eth0">
                <IPAddress>192.168.1.1</IPAddress>
                <Mask>255.255.255.0</Mask>
                <VRRP>
                    <Group id="10">
                        <IPAddress>192.168.1.254</IPAddress>
                        <Description>Working group</Description>
                    </Group>
                </VRRP>
            </Interface>
            <Interface name="eth1">
                <IPAddress>192.168.2.1</IPAddress>
                <Mask>255.255.255.0</Mask>
            </Interface>
          </Interfaces>
    </Router>

    <!--    R2      -->
    <Router id="R2">
        <Interfaces>
            <Interface name="eth0">
                <IPAddress>192.168.1.2</IPAddress>
                <Mask>255.255.255.0</Mask>
```

Fig. 3. Fragment of routers configuration

The configuration is an XML file that contains the settings of each of the interfaces of the router. In this configuration, we can set their system name, address, description, and other service information. Also in this file, we specify the VRRP settings for the correct operation of the protocol: the virtual IP address of the fault-tolerant router, its id, and description.

The UDP traffic generator is configured for the H1 client node. This generator creates a load flow towards the H2 client node. The UDPSink application is configured at the H2 node. This application receives the traffic flow with the specified address and destination port. In Fig. 4, we can see a fragment of the configuration of client applications.

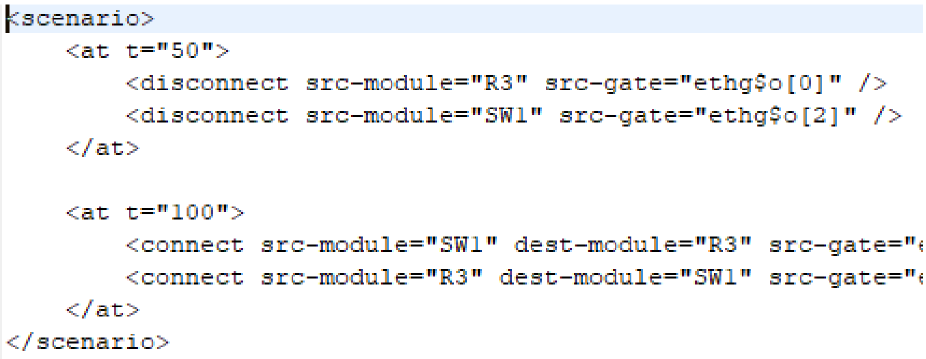


```
**.H1.configData = xmldoc("config.xml", "Devices/Host[@id='H1']")
**.H2.configData = xmldoc("config.xml", "Devices/Host[@id='H2']")

#scenario
**.scenarioManager.script = xmldoc("scenario.xml")

**.enableIPv6 = false
**.enableCLNS = false

**.H1.numUdpApps = 1
**.H1.udpApp[0].typename = "UDPBasicApp"
**.H1.udpApp[0].destAddresses =  "192.168.2.5"
**.H1.udpApp[0].destPort = 1000
**.H1.udpApp[0].messageLength = 100B
**.H1.udpApp[0].startTime = 40s
**.H1.udpApp[0].sendInterval = uniform(1s,2s)

**.H2.numUdpApps = 1
**.H2.udpApp[0].typename = "UDPSink"
**.H2.udpApp[0].localPort = 1000
```

Fig. 4. Simulating parameters and settings of UDP-applications

Also in this file, we set different parameters of routers using the path to the XML configuration file and id of routers.

OMNeT++ simulation environment allows you to write scripts that can influence the model process and simulate various events in the system. A script has been developed for researching fault-tolerance in our computer network. This script simulates the break of the communication channel between the SW1 switch and the R3 router. In Fig. 5, we can see a fragment of developed in the OMNeT++ environment script.



```
<scenario>
    <at t="50">
        <disconnect src-module="R3" src-gate="ethg$o[0]" />
        <disconnect src-module="SW1" src-gate="ethg$o[2]" />
    </at>

    <at t="100">
        <connect src-module="SW1" dest-module="R3" src-gate="
        <connect src-module="R3" dest-module="SW1" src-gate="
    </at>
</scenario>
```

Fig. 5. Fragment of scripts, which simulate the break of the communication channel between the switch and active router

Fig. 6 shows the simulation process before the break of the communication channel.

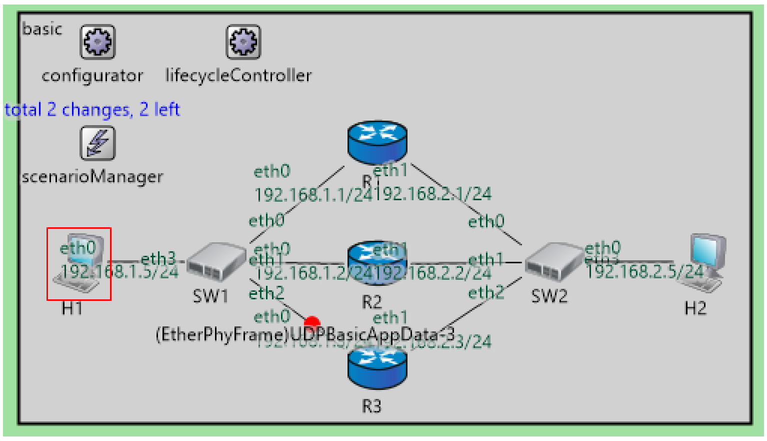


Fig. 6. Simulation before the break of the communication channel

Fig. 6 shows that the traffic from the client H1 goes through the router R3. At each moment only one of the three routers sending traffic - the rest are in standby mode. The script simulates the break of the communication channel between the SW1 switch and the active router R3. Fig. 7 shows the simulation process after the break of the communication link.

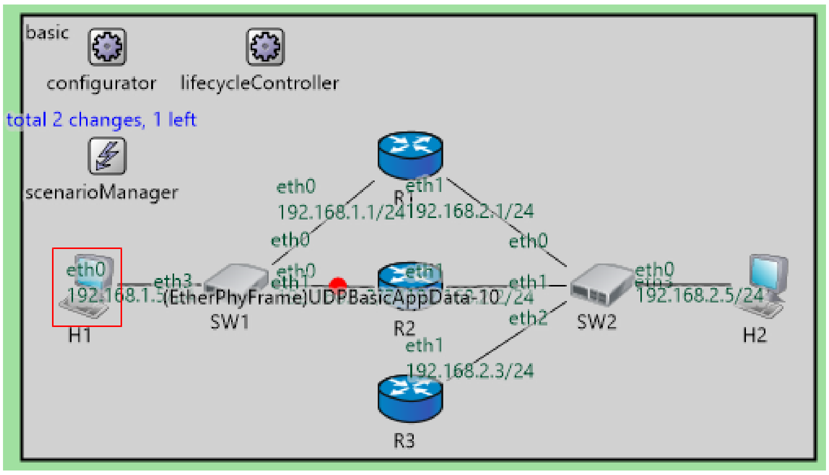


Fig. 7. Simulation after a break of the communication channel.

Traffic from the H1 node is going through an R2 router since the R3 router is unavailable for H1 client. The VRRP algorithm allows us to change active router and traffic from H1 client is sent via the R2 router. Thus, the computer network has the fault-tolerant gateway that allows sending traffic after break communication links and/or network equipment.

5 Conclusion

A computer network model has been developed with a fault-tolerant gateway based on the VRRP protocol. The process of creating and researching computer network models in the OMNeT++ environment is described in the paper. This approach allows building computer network models using real communication tools and computer network protocols of the TCP/IP stack. The algorithm of the VRRP protocol for implementing fault-tolerant gateway in the local area network is described and modeled in detail. The results obtained in this article may be useful to network engineers and designers when building computer networks with a fault-tolerant gateway.

References

1. Sorin D. Fault Tolerant Computer Architecture. Morgan & Claypool 2009. p. 103. DOI: 10.2200/S00192ED1V01Y200904CAC005
2. Coolen, F.P.A., Utkin, LV.: Robust weighted SVR-based software reliability growth model. Reliability Engineering & System Safety 176, 93-101 (2018), DOI: 10.1016/j.ress.2018.04.007.
3. Kopetz H. Real-Time Systems: Design Principles for Distributed Embedded Applications. Springer, pp. 396, 2011. DOI 10.1007/978-1-4419-8237-7.
4. Poymanova, E.D., Tatarnikova, T.M. Models and Methods for Studying Network Traffic 2018 Wave Electronics and its Application in In-formation and Telecommunication Systems, (WECONF) 26-30 Nov. 2018. DOI: 10.1109/WECONF.2018.8604470
5. Aliev T.I. The synthesis of service discipline in systems with limits // Communications in Computer and Information Science. 2016. V. 601. P. 151–156. DOI:10.1007/978-3-319-30843-216.
6. Kutuzov O.I., Tatarnikova T.M. On the Acceleration of Simulation Modeling. XXI International Conference on Soft Computing and Measurements (SCM'2018) 23-25 May 2018
7. Gatchin Y. A., Zharinov I. O., Korobeynikov A. G., Zharinov O. O. Theoretical estimation of Grassmann's transformation resolution in avionics color-coding systems//Modern Applied Science. 2015. Vol. 9, N 5. P. 197-210. ISSN 1913-1844
8. Tatarnikova, T., Kolbanev, M.: Statement of a Task Corporate Information Networks Interface Centers Structural Synthesis. In IEEE EUROCON. Saint Petersburg, pp. 1883–1887 (2009). DOI: 10.1109/EURCON.2009.5167903.
9. Kleinrock, L. Queueing Systems: Volume I – Theory. New York: Wiley Interscience. 1975 p. 417. DOI: 10.3103/S0146411615010022
10. Kleinrock, L. Queueing Systems: Volume II – Computer Applications. New York: Wiley Interscience. 1976 p. 576. DOI: 10.1002/net.3230070308
11. Anders Gunnar & Mikael Johansson. Robust load balancing under traffic uncertainty – tractable models and efficient algorithms // Telecommun Syst. (2011) 48:93–107

12. Merindol P. Improving Load Balancing with Multipath Routing / P. Merindol, J. Pansiot, S. Cateloin // Proc. of the 17-th International Conference on Computer Communications and Networks, IEEE ICCCN 2008. – 2008. – P. 54-61. DOI: 10.1109/ICCCN.2008.ECP.30.
13. Rajeev V., Muthukrishnan C.R. Reliable backup routing in fault tolerant real-time networks. Proceedings. Ninth IEEE International Conference on Networks, ICON 2001. DOI: 10.1109/ICON.2001.962338.
14. Banner R., Orda A. Multipath Routing Algorithms for Congestion Minimization, CCIT Report No. 429, Department of Electrical Engineering, Technion, Haifa, Israel, 2004. URL: http://www.ee.technion.ac.il/people/ron/Congestion.pdf
15. Krouk E., Semenov S. Application of Coding at the Network Transport Level to Decrease the Message Delay // Proc. of 3rd Intern. Symp. on Communication Systems Networks and Digital Signal Processing. Staffordshire University, UK, 2002. P. 109—112
16. Kabatiansky G., Krouk E., Semenov S. Error Correcting Coding and Security for Data Networks. Analysis of the Superchannel Concept. Wiley, 2005. 288 p
17. Bogatyrev V.A., Bogatyrev A.V. Functional Reliability of a Real-Time Redundant Computational Process in Cluster Architecture Systems //Automatic Control and Computer Sciences, - 2015, Vol. 49, No. 1, pp. 46-56. DOI:10.3103/S0146411615010022
18. Bogatyrev A.V., Bogatyrev S.V., Bogatyrev V.A. Analysis of the Timeliness of Redundant Service in the System of the Parallel-Series Connection of Nodes with Unlimited Queues // 2018 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) – 2018, DOI: 10.1109/WECONF.2018.8604379
19. Bogatyrev V.A. Increasing the fault tolerance of a multi-trunk channel by means of inter-trunk packet forwarding (1999) Automatic Control and Computer Sciences, 33 (2), pp. 70-76
20. Noskov I.I., Bogatyrev V.A., Slastikhin I.A. Simulation of computer network with switch and packet reservation // CEUR Workshop Proceedings - 2019, Vol. 2344
21. Slastikhin I.A., Bogatyrev V.A., Noskov I.I. The simulation model of the system with aggregated channels and redundant transmissions on the multiple access level // CEUR Workshop Proceedings - 2019, Vol. 2344
22. Slastikhin I.A., Bogatyrev V.A. Redundant Priority Maintenance in the Multi-Channel Systems // 2018 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) - 2018, pp. 1-5. DOI: 10.1109/WECONF.2018.8604301
23. VESELÝ Vladimír, ŠVÉDA Miroslav. L2 protocols in OMNeT++ // IP Networking 1 - Theory and Practice. Žilina: Zilina University Publisher, 2012, pp. 37-40
24. VESELÝ Vladimír, RYŠAVÝ Ondřej, ŠVÉDA Miroslav. Protocol Independent Multicast in OMNeT++ // The International Academy, Research and Industry Association, 2014