Solution for the Default Gateway Protection within Fault-Tolerant Routing in an IP Network

Preliminary Communication

Oleksandr Lemeshko
Kharkiv National University of Radio Electronics,
Faculty of Infocommunications, Department of Infocommunication Engineering
Nauka Ave., 14, Kharkiv, Ukraine
oleksandr.lemeshko@nure.ua

Oleksandra Yeremenko
Kharkiv National University of Radio Electronics,
Faculty of Infocommunications, Department of Infocommunication Engineering
Nauka Ave., 14, Kharkiv, Ukraine
oleksandra.yeremenko.ua@ieee.org

Nadia Tariki
Kharkiv National University of Radio Electronics,
Faculty of Infocommunications, Department of Infocommunication Engineering
Nauka Ave., 14, Kharkiv, Ukraine
nadotariki@gmail.com

Abstract *– In this paper, the consistent solution for default gateway protection within fault-tolerant routing in an IP network is presented, and it is based on development of the appropriate flow-based mathematical model. Within the framework of the proposed model, a fault-tolerant routing problem has been reduced to the solution of the optimization problem of nonlinear programming. Fault-tolerance functions are implemented by introducing additional routing variables responsible for the calculation of a backup default gateway and the corresponding path (multipath) in the transport network. Several examples have demonstrated features of the application of the proposed model in solving default gateway protection within fault-tolerant routing for the case of realization of single path and multipath routing. The results have confirmed the efficiency of the proposed model and adequacy of the calculation results obtained.*

Keywords *– access network, default gateway, edge router, fault-tolerance, flow-based model, routing, transport network, virtual router*

1. INTRODUCTION

One of the ways to improve network availability is to implement fault-tolerant routing. However, as a rule, fault-tolerant routing in IP/MPLS networks is realized on the access level of the transport network due to default gateway protection schemes, and at the level of the transport network itself – due to Fast ReRoute decisions [1-5]. The problematics of research lies in the fact that the existing fault-tolerant routing protocols have rather limited capabilities for providing fault-tolerant solutions in the network, which cannot perform scaled adaptation to changes in the network state. In addition, the basic factors causing changes in the communication network include its overload, violation of the security level and requirements to the Quality of Service, compromising network elements or failures in network equipment. It is usually conditioned by ineffective traffic management, available link and buffer resources of the network. The reason for such situation is the lack of adequate mathematical models and valid methods of fault-tolerant routing, which could underlie mathematical, software-algorithmic and protocol support of network equipment. The major requirements imposed to such mathematical models and methods include accountability of the specifics of processes in modern communication networks, support of different routing strategies, implementation of known fault-tolerance schemes based on protection (redundancy) of network elements and its bandwidth.

In this regard, the task of finding an effective solution for protecting the default gateway within fault-tolerant routing in the IP network on the edge of the transport network when multiple flows arrive from the access network in conditions of possible failures is necessary if additional redundancy of edge routers is required. The structure of the present paper is as follows. Section 2 is devoted to the analysis of theoretical solutions for fault-tolerant routing, including a comparative charac-

teristic of protocol solutions for protecting the default gateway. Section 3 describes a graph model of the fault-tolerant IP network. Section 4 introduces a fault-tolerant IP routing model for network core and edge, presented to describe the interaction of access networks and the transport network. Section 5 directly presents the default gateway protection scheme in fault-tolerant IP routing. In Section 6, within the framework of the proposed optimization statement of the problem of fault-tolerant routing, a composite optimality criterion of fault-tolerance for core and edge of the IP network is presented, with the rationale for choosing the weight coefficients of its terms. In addition, the classification of solved optimization problems is presented. Section 7 is a numerical study and it contains examples of default gateway protection for single path and multipath routing strategies.

2. ANALYSIS OF WORK RELATED TO FAULT-TOLERANT ROUTING

Analysis of the results obtained by other scientists in the field of fault-tolerant routing [6-9] has shown that in the current conditions of use they have several disadvantages. For example, in [7-9], solutions are proposed to improve network fault-tolerance, but they are only adapted for implementation of single path routing, which adversely affects the Quality of Service. In [8, 9], solutions on fault-tolerant routing over the paths that do not overlap are given. However, this does not contribute to the efficient use of available network resources, load balancing in the network and maximizing the Quality of Service.

A specific feature in the construction of modern heterogeneous networks is their division into the access network (AN) and the transport network (TN). Hence, when transmitting packets from the AN to the TN, it is important to select a default gateway. At the same time, in the analyzed solutions, fault-tolerant routing does not provide a solution to the problem of selecting and protecting the default gateway.

There exist specific protocols for failure protecting default gateways, where preference is given to Fault-Tolerant IP Routing protocols, which include the Hot Standby Router Protocol (HSRP), the Virtual Router Redundancy Protocol (VRRP), and the Gateway Load Balancing Protocol (GLBP). In addition, the Common Address Redundancy Protocol (CARP) is widely used as an alternative to the previous solutions. The features of the so-called first hop redundancy protocols are compared in Table 1 [10-13].

The main goal of such protocols is to enhance the accessibility of TN edge routers. The TN edge routers, in turn, act as default gateways for multiple access networks. Moreover, each AN has a formed virtual router (Virtual Router, VR). It is responsible for connecting certain interfaces of edge routers. For instance, when VRRP is applied, the network state is analyzed and a VR interface is determined. The VR interface is used by the access network to connect to the transport network. Therefore, load balancing across multiple interfaces of the virtual router is able to increase availability and reliability of connection; however, such functionality is not peculiar to all existing protocols (Table 1) [10-13].

Table 1. Comparison of the First Hop Redundancy Protocols.

Property	HSRP	VRRP	GLBP	CARP
Scope	Cisco Proprietary	IEEE Standard	Cisco Proprietary	Not a standard (BSD based OS)
Standard	RFC 2281	RFC 5798	None	None
OSI	Layer 3	Layer 3	Layer 2	Layer 3
Load Balancing	No	Yes	Yes	Yes
IPv6	Yes	Yes	Yes	Yes
Advantages	• easy to configure; • low network overhead	• simplified network management; • high adaptability; • low network overhead; • load balancing; • minimizes the duration of black holes; • minimizes bandwidth overhead and processing complexity	• efficient use of network resources; • high availability; • automatic load balancing; • lower administration cost; • effective Access-layer design	• open alternative to HSRP and VRRP; • provides failover redundancy for firewalls and routers; • load balancing
Disadvantages	• not effective for real time traffic; • weak security; • Cisco proprietary	• weak security (does not currently include any type of authentication)	• Cisco proprietary; • high complexity of network management	• incompatibility with standards; • weak security

There are some considerable disadvantages in Fault-Tolerant IP Routing solutions:

- lack of consideration of the network traffic flow-based nature;
- limited ability for load balancing with a need of administrative configuration;
- no consistent solution for interrelated problems of default gateway selection and routing in the transport network.

For example, as shown in [10], the following methods can be used to provide load balancing on default gateways interfaces:

- Round Robin (GLBP);
- Weighted (GLBP);
- Host-dependent (GLBP, VRRP).

The Round Robin method assumes line balancing of the load across all interfaces of the virtual gateway, which is an acceptable solution only in the case of approximately the same availability of TN edge routers. Otherwise, it is advisable to use weighted load balancing, in which the traffic coming from the AN is distributed among virtual gateway interfaces in proportion to their administrative weight. The host-dependent method implements pseudo-balancing when a specific virtual gateway interface for one AN is a primary interface, and for another AN it is a backup one. Thus, to provide uneven load balancing between the TN edge routers with different availability, it is necessary to administratively conduct additional configuration of the equipment.

These balancing methods significantly reduce the speed of network response to possible failures and limit the functionality of network solutions for gateway protection. In addition, even with optimal load balancing for gateway protection, there is no guarantee that after the gateway has been selected, there is a route in the TN that has the necessary bandwidth to provide QoS. This is due to the fact that the known solutions for default gateway protection with TN routing decisions are not consistent and implemented sequentially, but independently of each other.

Therefore, in Fault-Tolerant IP Routing we propose a model for default gateway protection. This model should provide an agreed solution for tasks related to both the selection of the default gateway with optimization of load balancing, and the definition of routes in the transport network. The goal of the proposed model consists of improvement of the availability of virtual router interfaces and network performance on the whole. This is also considered to be an additional extension of the approach proposed in [14, 15].

3. FAULT-TOLERANT IP NETWORK GRAPH MODEL

We assume that the graph $G = (M, L)$ describes the structure of communications system and $M = R \bigcup V$ is the set of vertices comprising two disjoint subsets [14]:

- $R = \{R_i, i = \overline{1,m}\}$ is the set of vertices modeling transport network routers;
- $V = \{V_j, j = \overline{1,v}\}$ is the set of vertices modeling access networks in the communications system.

There are also two subsets in the set R: R^+ is the set of vertices modeling edge routers of the transport network, i.e. the routers, which can be connected to the access networks, where $m^+ = |R^+|$ is the total number of edge routers in the TN, and R^- is the set of vertices modeling transit routers of the transport network, where $m^- = |R^-|$ is the total number of transit routers in the TN.

Assume that R_j^+ is a subset of the set R^+. It models edge routers (their interfaces), which form a virtual router for the jth access network described by the vertex V_j. Then $m_j^+ = |R_j^+|$ is the total number of edge routers (their interfaces) that make up a virtual router for the jth AN. Let us consider an example. Suppose that for the first access network V_1 a set of routers represented by vertices R_1, R_2, and R_3 is used as a virtual router (Fig. 1), i.e. $m_1^+ = 3$; for the second network V_2 a virtual router is formed by router interfaces modeled by nodes R_2 and R_3, i.e. $m_2^+ = 2$. Thus, it can be seen that there is a possibility for sets R_j^+ ($j = \overline{1,v}$) to overlap due to the fact that the interfaces of the same edge router can take part in different virtual routers.

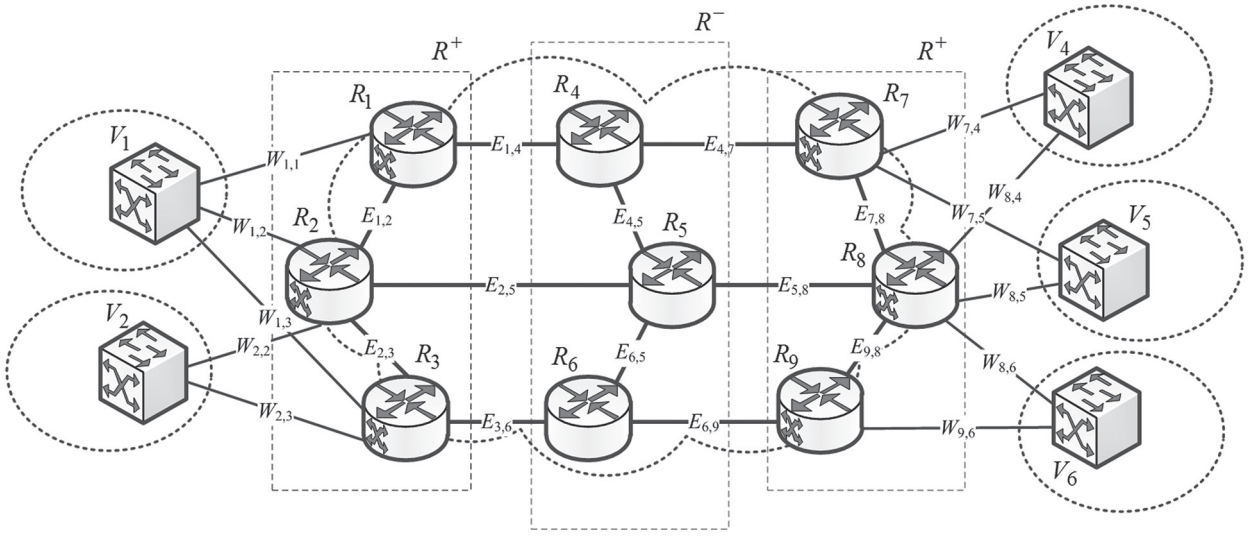


Fig. 1. Example of the network structure

In turn, the set of arcs $L = E \bigcup W$ of the original graph G also includes two subsets:

$E = \left\{E_{i,j}, i, j = \overline{1,m}, i \neq j\right\}$ is the set of TN links;

$W = \left\{W_{i,j}, i = \overline{1,v}, j = \overline{1,m^+}\right\}$ is the set of access lines that connect AN and TN edge routers.

Then $|E| = n$ is the number of links in the TN. Each arc $E_{i,j} \in E$, which models the corresponding link of the transport network, possesses associated link capacity $\varphi_{i,j}$.

4. FAULT-TOLERANT IP ROUTING MODEL FOR NETWORK CORE AND EDGE

Let us consider K as the set of flows incoming to edge routers from access networks; the following parameters correspond to each kth flow from the set K: V_s^k is the access network and the source of the kth flow; V_d^k is the access network and the destination of the kth flow; and λ^k is the mean packet rate of the kth flow in packets per second (1/s).

Thus, when solving the problem of Fault-Tolerant IP Routing with the help of the proposed model, the following three types of control variables should be calculated [14, 15]:

- $x_{i,j}^k$ is the routing variable that characterizes the fraction of the kth flow in the link represented by the arc $E_{i,j}$;
- $y_{i,j}^k$ is the access variable that characterizes the fraction of the kth flow in the access line, which is in turn represented by the arc $W_{i,j}$, i.e. from the ith AN to the jth edge router of the TN;
- $z_{j,i}^k$ is the access variable that characterizes the fraction of the kth flow in the access line, which is represented by the arc $W_{j,i}$, i.e. from the jth edge router of the TN to the ith AN.

The number of routing variables $x_{i,j}^k$ corresponds to the product $|K| \cdot |E|$; the total number of access variables $y_{i,j}^k$ and $z_{j,i}^k$ is determined as $v \cdot m^+ \cdot |K|$.

A number of restrictions are imposed to the control variables in accordance with their physical meaning. For the case of using single path routing of flows in the TN, the next conditions take place

$$x_{i,j}^k \in \{0;1\} \tag{1}$$

To implement multipath routing, we have

$$0 \le x_{i,j}^k \le 1 \tag{2}$$

that is, packets of the same flow can be transmitted simultaneously over a set of paths [14, 15].

Therefore, in order to ensure a balanced network load and improve the QoS in the communications system as a whole, multipath routing should be implemented in accordance with the Traffic Engineering concept.

If the access network is connected only to one virtual router interface at a time, as realized, e.g. in the HSRP protocol (Table 1), the access variables are restricted as follows:

$$\begin{cases} y_{i,j}^k \in \{0;1\}; \\ \sum\limits_{j:R_j \in R_i^+} \prod\limits_{k \in K} y_{i,j}^k = 1; \end{cases} \text{and} \begin{cases} z_{j,i}^k \in \{0;1\}; \\ \sum\limits_{j:R_j \in R_i^+} \prod\limits_{k \in K} y_{i,j}^k = 1. \end{cases} \tag{3}$$

Given a possibility of load balancing over all available interfaces of the virtual router by analogy with the protocols VRRP, GLBP and CARP (Table 1), condition (3) is replaced by

$$0 \le y_{i,j}^k \le 1 \text{ and } 0 \le z_{j,i}^k \le 1 \tag{4}$$

Moreover, to prevent packet loss in areas "AN – TN virtual router" (5) and "TN virtual router – AN" (6), the following conditions are introduced:

$$\sum_{R_j \in R_p^+} y_{p,j}^k = 1 \quad , \quad V_p = V_s^k \tag{5}$$

$$\sum_{R_j \in R_h^+} z_{j,h}^k = 1 \quad , \quad V_h = V_d^k \tag{6}$$

The consistency in the calculation of control variables, which are responsible for the implementation of fault-tolerant IP routing, is ensured due to the fulfillment of flow conservation conditions [15]:

$$\begin{cases} \sum\limits_{j:E_{i,j} \in E} x_{i,j}^k - \sum\limits_{j:E_{j,i} \in E} x_{j,i}^k = 0; k \in K,\ R_i \in R^-; \\ \sum\limits_{j:E_{i,j} \in E} x_{i,j}^k - \sum\limits_{j:E_{j,i} \in E} x_{j,i}^k = y_{p,i}^k; k \in K,\ R_i \in R^+, V_p = V_s^k; \\ \sum\limits_{j:E_{i,j} \in E} x_{i,j}^k - \sum\limits_{j:E_{j,i} \in E} x_{j,i}^k = -z_{i,h}^k; k \in K,\ R_i \in R^+, V_h = V_d^k. \end{cases} \tag{7}$$

In (7), index j indicates the number of input or output interfaces of the ith router through which the kth flow arrives or departs through the router accordingly. Conditions (7) ensure that there are no packet losses on TN transit routers and the communications system as a whole, as well as the fact that the flow of any user from the AN will be accepted and served by the TN.

To improve IP routing fault-tolerance, in which the AN is connected with the TN through (a) certain virtual router interface(s), it is necessary to introduce additional control variables that determine a backup path with the same root [10-12]. From the mathematical point of view, it is necessary to calculate the following additional control variables:

- $\overline{x}_{i,j}^k$ is the routing variable, which characterizes a portion of the kth flow in the link $E_{i,j}$ of the backup path with arguments (1) or (2) in the core network;

- $\bar{y}_{i,j}^k$ is the access variable, which characterizes the fraction of the *k*th flow in the backup access line from the *i*th AN to the jth edge router of the TN;
- $\bar{z}_{j,i}^k$ is the access variable, which characterizes the fraction of the *k*th flow in the backup access line from the jth edge router of the TN to the ith AN.

$$\frac{1}{2}\sum_{k\in K}\left(\lambda^k\left[(x_{i,j}^k+\bar{x}_{i,j}^k)+\sqrt{(x_{i,j}^k-\bar{x}_{i,j}^k)^2}\right]\right)\le\varphi_{i,j} \quad (8)$$

where $\varphi_{i,j}$ is associated with the TN link capacity.

Thus, the fulfillment of conditions (8) allows us to prevent overload of communication links in the network, even when if not all, but only some of the flows, switch from the primary to the backup route. In this case, some part of the bandwidth of backup routes will always remain unused for these flows, thereby implementing a bandwidth protection scheme in the organization of fault-tolerant routing [16].

5. DEFAULT GATEWAY PROTECTION SCHEME IN FAULT-TOLERANT IP ROUTING

To protect one of the routers forming a virtual router, the following backup-schemes have been presented. To implement the protection scheme of the default gateway with the possibility of load balancing over all available interfaces of the virtual router, we have introduced the model in the following nonlinear terms:

$$\sum_{i:V_i\in V} y_{i,j}^k\bar{y}_{i,j}^k+\sum_{i:E_{i,j}\in E} x_{i,j}^k\bar{x}_{i,j}^k=0\ ,\ R_j\in R^+ \quad (9)$$

If the given conditions are fulfilled, it is guaranteed that the *j*th edge router (i.e. all incident links to this node from the AN and the TN) is used by either the primary or the backup path.

The following linear conditions are obtained in the model offered when implementing a connection of the access network to only one virtual router interface at the present time, by analogy with [9]:

$$\begin{cases} x_{n,j}^k+\bar{x}_{n,j}^k\le 1; \\ y_{n,j}^k+\bar{y}_{n,j}^k\le 1. \end{cases} \quad (10)$$

The fulfillment of these conditions guarantees that the link $W_{i,j}$ will be used by a single path, either primary or backup.

6. COMPOSITE OPTIMALITY CRITERION OF FAULT-TOLERANCE FOR CORE AND EDGE OF THE IP NETWORK

Like the analogy in [15] and [16], it is offered to choose a minimum of the following objective function as the optimality criterion of the solutions obtained for fault-tolerant routing:

$$\begin{aligned} J=&\sum_{k\in K}\sum_{E_{i,j}\in E}c_{i,j}^k x_{i,j}^k+\sum_{k\in K}\sum_{E_{i,j}\in E}\bar{c}_{i,j}^k\bar{x}_{i,j}^k+\\ &+\sum_{k\in K}\sum_{W_{i,j}\in W}b_{i,j}^k y_{i,j}^k+\sum_{k\in K}\sum_{W_{i,j}\in W}\bar{b}_{i,j}^k\bar{y}_{i,j}^k+\\ &+\sum_{k\in K}\sum_{W_{j,i}\in W}a_{j,i}^k z_{j,i}^k+\sum_{k\in K}\sum_{W_{j,i}\in W}\bar{a}_{j,i}^k\bar{z}_{j,i}^k-\\ &-\sum_{k\in K}\sum_{E_{i,j}\in E}d_{i,j}^k x_{i,j}^k\bar{x}_{i,j}^k\ , \end{aligned} \quad (11)$$

where $n_{i,j}^k$ and $\bar{n}_{i,j}^k$ are link metrics applied in the calculation of the primary and backup paths, respectively, in the TN; and the seventh term is introduced to the objective function to improve scalability [16] by maximization of the coincidence between the primary and backup paths over non-protected links, whereas $d_{i,j}^k > c_{i,j}^k$ and $d_{i,j}^k > \bar{c}_{i,j}^k$. The weighted coefficients $b_{i,j}^k$ and $a_{j,i}^k$, in their turn, are the set of access metrics for the *k*th flow that determine the conditional cost of AN's connection to the edge router when choosing the default gateway; $\bar{b}_{i,j}^k$ and $\bar{a}_{j,i}^k$ have the same physical sense but for the backup access lines. The selection of these metrics is determined as the inverse functions of access line availabilities within the proposed solution.

Then the first and second terms in expression (11) describe the conditional cost of the use of TN links (primary and backup paths), and the terms from the third to sixth terms reflect the conditional cost of using the primary and backup access lines for incoming traffic to the TN or outgoing traffic from the TN, respectively.

Therefore, when solving the technological problem of Fault-Tolerant IP Routing, it is necessary to solve the mixed integer nonlinear programming problem (MINLP) during minimization (11) considering conditions (1), (3), (5)-(10) or the nonlinear programming problem (NLP) with constraints (2), (4)-(9) (Table 2).

Table 2. Classification of optimization problems.

Constraints	Optimization Problem Class
(1), (3), (5)-(10)	MINLP
(2), (4)-(9)	NLP

With conditions (1) and (3), the given model uses the strategy of the access network connection at the present time to only one virtual router interface. At the same time, the implementation of (2) and (4) provides a possibility of load balancing over all available interfaces of the virtual router.

7. EXAMPLES OF DEFAULT GATEWAY PROTECTION FOR SINGLE PATH AND MULTIPATH ROUTING

Let us demonstrate the functioning of the default gateway protection scheme on the structure shown in Fig. 1 for the cases of single path and multipath routing. The initial data for the research are presented in Tables 3 and 4.

Table 3. Initial data for the research.

Access Line	$W_{1,1}$	$W_{1,2}$	$W_{1,3}$	$W_{8,6}$	$W_{9,6}$
$A_{i,j}$	0.999	0.9999	0.998	0.9995	0.999

There are availabilities provided for every access line that have to determine the choice of the virtual router interface. Thus, the value $A_{i,j}$ defines the availability of the (i, j) network interface. In turn, capacity $\varphi_{i,j}$ is associated with every transport network link $E_{i,j}$, and corresponding values are presented below (Table 4).

An example of single path fault-tolerant routing, obtained by using the proposed model and realizing the default gateway protection scheme, is presented in Fig. 2. Here the access network V_1 represents the source of the flow of 300 1/s, arriving into the transport network through the default gateway, which is the virtual router interface modeled by the node R_2, while the destination of this flow is the access network V_6. The rates of the flows of packets are shown in the gaps of network links (Fig. 2).

Table 4. Initial data for the research.

Transport Network Link	$E_{1,2}$	$E_{2,3}$	$E_{1,4}$	$E_{2,5}$	$E_{3,6}$	$E_{4,5}$
$\varphi_{i,j}$, 1/s	150	110	350	400	400	300
Transport Network Link	$E_{6,5}$	$E_{4,7}$	$E_{5,8}$	$E_{6,9}$	$E_{7,8}$	$E_{9,8}$
$\varphi_{i,j}$, 1/s	200	200	800	350	100	120

Then the primary path is formed by the routers of the transport network as follows: $R_2 \rightarrow R_5 \rightarrow R_8$. The choice of this solution is determined on the one hand by a more reliable default gateway for the access networks V_1 and V_6 (according to the availabilities from Table 3), and on the other hand, by path selection in a transport network with the maximum bandwidth. In this case, metrics $c_{i,j}^k$ and $\bar{c}_{i,j}^k$ were chosen by analogy with the IGRP protocol, namely $10^7/\varphi_{i,j}$, for all corresponding transport network links. In the case of a failure of the default gateway R_2, the transmitted flow will be switched automatically to the router R_1. Then the backup path in the transport network will be formed by the routers $R_1 \rightarrow R_4 \rightarrow R_5 \rightarrow R_8$.

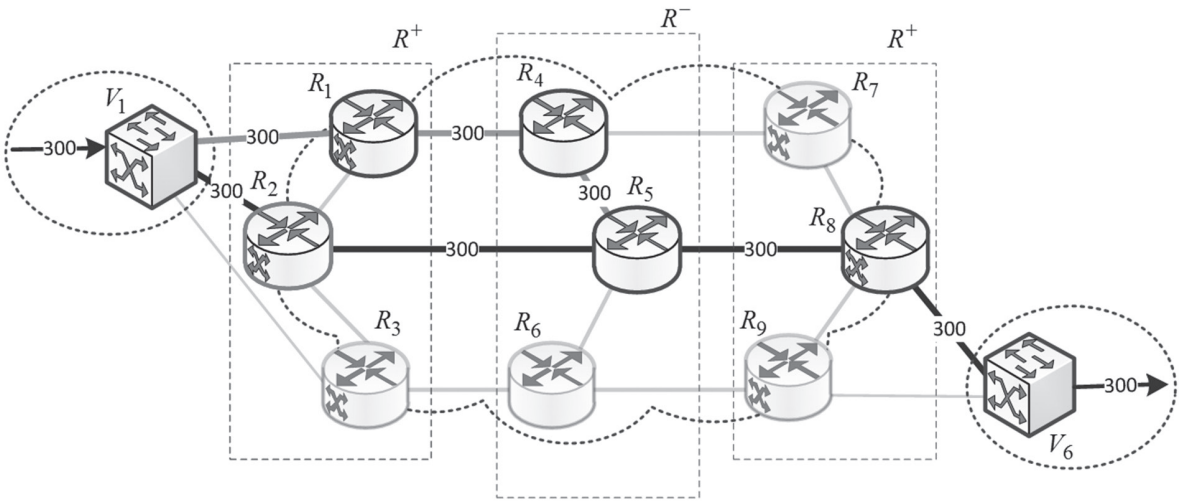


Fig. 2. Single path fault-tolerant routing example

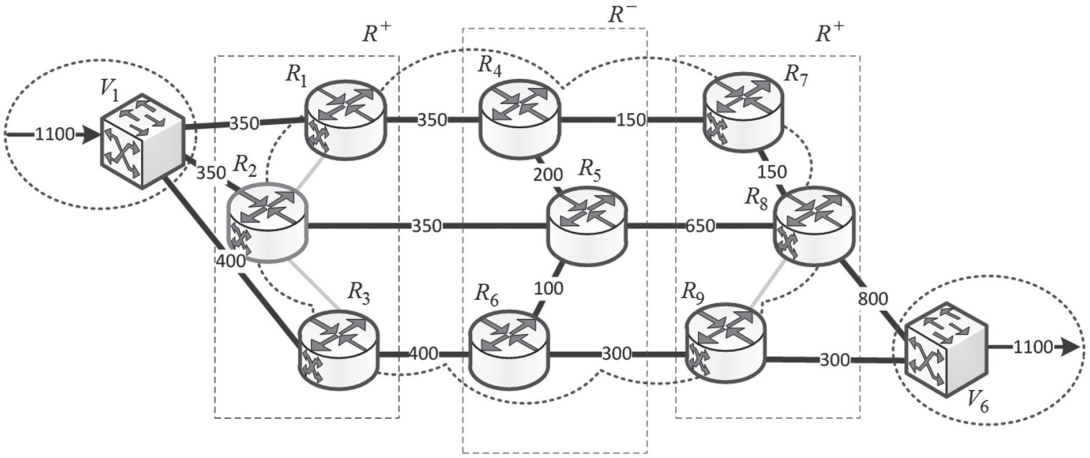
Next, let us consider the example of multipath fault-tolerant routing obtained by using the proposed model and realizing the default gateway protection scheme, which is shown in Figures 3a and 3b. In this case, the access network V_1 represents the source of the flow of 1100 1/s, arriving into the transport network, when the load is balanced over all interfaces of virtual routers R_1, R_2, and R_3, while the destination of this flow is the access network V_6. Then the primary multipath consists of the following paths:

- Path #1: $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_8$, where the packet rate is 150 1/s;
- Path #2: $R_1 \rightarrow R_4 \rightarrow R_5 \rightarrow R_8$, where the packet rate is 200 1/s;
- Path #3: $R_2 \rightarrow R_5 \rightarrow R_8$, where the packet rate is 350 1/s;
- Path #4: $R_3 \rightarrow R_6 \rightarrow R_5 \rightarrow R_8$, where the packet rate is 100 1/s;
- Path #5: $R_3 \rightarrow R_6 \rightarrow R_9$, where the packet rate is 300 1/s.

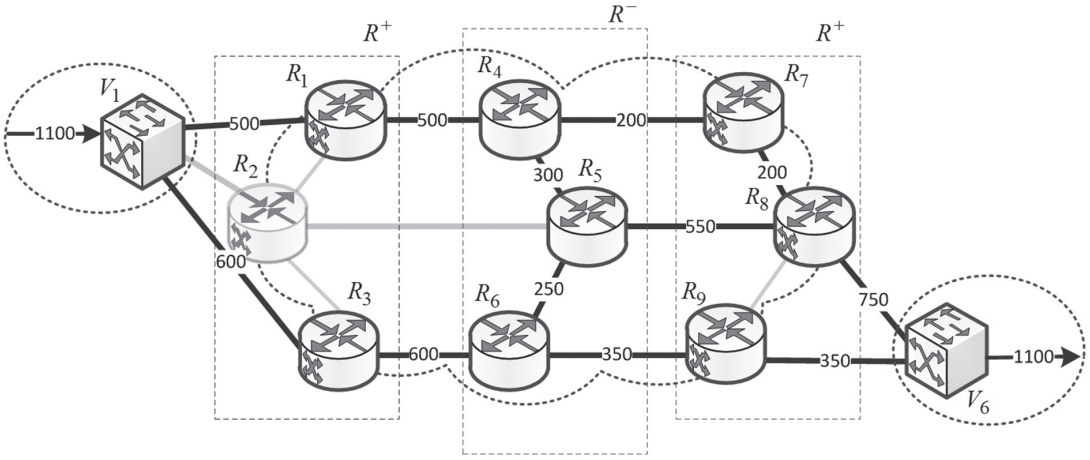
This solution is based on the possibility of providing load balancing over all available interfaces of virtual routers R_1, R_2, and R_3 for the access network V_1, and R_8, R_9 for V_6, respectively. This is also accompanied by the use of a multipath routing strategy in the transport network.

Here, in the case of the failure of default gateway R_2 in accordance with the calculations obtained in the framework of the proposed model, the transmitted flow will be rerouted automatically to the backup multipath excluding the route with R_2:

- Path #1: $R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_8$, where the packet rate is 200 1/s;
- Path #2: $R_1 \rightarrow R_4 \rightarrow R_5 \rightarrow R_8$, where the packet rate is 300 1/s;
- Path #3: $R_3 \rightarrow R_6 \rightarrow R_5 \rightarrow R_3 \rightarrow$, where the packet rate is 250 1/s;
- Path #4: $R_3 \rightarrow R_6 \rightarrow R_9$, where the packet rate is 350 1/s.



a)



b)

Fig. 3. Multipath fault-tolerant routing example

8. CONCLUSION

In this paper, we present the consistent solution for default gateway protection within fault-tolerant routing in the IP network based on the development of an appropriate flow-based mathematical model (1)-(11). Within the framework of the proposed model, the fault-tolerant routing problem has been reduced to the solution of the optimization problem of nonlinear programming with the objective function (11) and restrictions (1)-(10). Part of control variables (3), (4) is responsible for the selection of the default gateway in the access network, and part (1), (2) is responsible for the selection of the path or the multipath in the transport network.

Fault-tolerance functions have been implemented by introducing additional routing variables, responsible for the calculation of the backup default gateway with condition (9) and the corresponding path (multipath) in the transport network. This scheme has been implemented aiming at bandwidth protection of the calculated path by introducing condition (8). The implementation of objective function (11) allowed the minimization of the conditional cost of using resources of the access network and

the transport network in solving the fault-tolerant routing tasks. The choice of routing metrics has been performed so that a selection of the default gateway implemented on the maximum availability criterion (Table 3) and the choice of a route in the transport network have been realized according to the criterion of maximum bandwidth (by analogy with the IGRP protocol).

Several examples have demonstrated features of the application of the proposed model to solving default gateway protection within fault-tolerant routing in the IP network for the case of realization of single path (Fig. 2) and multipath routing (Fig. 3). The results have confirmed the efficiency of the proposed model and adequacy (validity) of calculation results obtained.

As a rule, an increase in the number of routers and links in the network leads to an increase in the computational complexity of the solutions obtained. At the same time, the efficiency of using the proposed model is also largely determined by the size of the transport network and the number of access networks. The more options for selecting the default gateway and possible paths in the transport network, the more effective the optimization problem statement of the coordinated solution of these tasks. In these exact conditions, the coordinated solutions provide higher efficiency of fault-tolerant routing in the network compared to the existing solutions in which the gateway selection and routing problems are solved separately.

9. REFERENCES:

[1] I. Hussain, "Fault-Tolerant IP and MPLS Networks", Cisco Press, 2005.

[2] I. Koren, C. Krishna, "Fault-Tolerant Systems", Morgan Kaufmann, 2007.

[3] M. Y. Hariyawan, "Comparison Analysis of Recovery Mechanism at MPLS Network", International Journal of Electrical and Computer Engineering, Vol. 1, No. 2, 2011, pp. 151-160.

[4] A. Sundarrajan, S. Ramasubramanian, "Fast Rerouting for IP Multicast Under Single Node Failures", Proceedings of the 2013 IEEE Global Communications Conference, Atlanta, GA, USA, 9-13 December 2013, pp. 2076-2081.

[5] J. Papán, P. Segeč, P. Palúch, "Analysis of existing IP Fast Reroute mechanisms", Proceedings of the 2015 International Conference on Information and Digital Technologies, Zilina, Slovakia, 7-9 July 2015, pp. 291-297.

[6] J. Rak, "Resilient Routing in Communication Networks", Springer International Publishing, 2015.

[7] D. Tipper, "Resilient network design: challenges and future directions", Telecommunication Systems, Vol. 56, No. 1, 2014, pp. 5-16.

[8] K. Myslitski, J. Rak, Ł. Kuszner, "Network graph transformation providing fast calculation of paths for resilient routing", Proceedings of the 8th International Workshop on Resilient Networks Design and Modeling, Halmstad, Sweden, 13-15 September 2016, pp. 238-244.

[9] T. Gomes, L. Martins, S. Ferreira, M. Pascoal, D. Tipper, "Algorithms for Determining a Node-Disjoint Path Pair Visiting Specified Nodes", Optical Switching and Networking, Vol. 23, Part 2, 2017, pp. 189-204.

[10] J. Pavlik, A. Komarek, V. Sobeslav, J. Horalek, "Gateway redundancy protocols", Proceedings of the IEEE 15th International Symposium on Computational Intelligence and Informatics, Budapest, Hungary, 19-21 November 2014, pp. 459-464.

[11] S. Nadas, Ed. Ericsson, RFC 5798, "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", Internet Engineering Task Force, March 2010.

[12] T. Li, B. Cole, P. Morton, D. Li, RFC 2281, "Cisco Hot Standby Router Protocol (HSRP)", Internet Engineering Task Force (IETF), March 1998.

[13] Cisco Networking Center, First Hop Redundancy Protocol comparison (HSRP, VRRP, GLBP) with the diagram, http:// cisconetworkingcenter.blogspot.com/2013/01/first-hop-redundancy-protocol.html (accessed: 2014)

[14] O. Yeremenko, N. Tariki, A. M. Hailan, "Fault-tolerant IP routing flow-based model", Proceedings of the 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science, Lviv-Slavsko, Ukraine, 23-26 February 2016, pp. 655-657.

[15] O. V. Lemeshko, O. S. Yeremenko, N. Tariki, A. M. Hailan, "Fault-Tolerance Improvement for Core and Edge of IP Network", Proceedings of the 11th International Scientific and Technical Conference Computer Science and Information Technologies, Lviv, Ukraine, 6-10 September 2016, pp. 161-164.

[16] O. Lemeshko, K. Arous, N. Tariki, "Effective solution for scalability and productivity improvement in fault-tolerant routing", Proceedings of the 2nd International Scientific-Practical Conference Problems of Infocommunications Science and Technology, Kharkiv, Ukraine, 13-15 October 2015, pp. 76-78.