IP Fast Reroute

Jozef Papán*
Department of InfoComm networks
Faculty of Management Science and Informatics
University of Žilina
Univerzitná 1, 010 26 Žilina, Slovakia
jozef.papan@fri.uniza.sk

Abstract

In this work, a new innovative Multicast Repair (M-REP) IPFRR mechanism, which uses an IP multicast technology, is presented. The proposed M-RER mechanism uses Protocol Independent Multicast - Dense Mode (PIM-DM) with modified algorithm of the Reverse Path Forwarding (RPF). The key contribution of this work is the fact that the proposed M-REP IPFRR mechanism is independent of the link-state routing protocols and the internal algorithm does not explicitly calculate the alternative path.

Categories and Subject Descriptors

C.2.0 [**Computer - communication Networks**]: GeneralSecurity and protection; C.2.3 [**Computer - communication Networks**]: Network Operations-Network management

Keywords

IP Fast Reroute; IPFRR; multicast; RPF; PIM-DM

1. IP Fast Reroute

After a link or node failure, a process of network convergence starts in a network, during which routers must update their routing tables. The overall time of network convergence might take from a few milliseconds up to tens of seconds. During this process, several destinations in the network might become unavailable, packet loss might increase or even routing loops might occur. Several solutions have been introduced and developed for solving these negative impacts - these mechanisms are called by a common term Fast Reroute (FRR) mechanisms.

The first FRR mechanism was Multiprotocol Label Switching (MPLS) FRR, which uses an explicit backup routes. However, since the MPLS mechanisms are not used in every network and MPLS is not scalable enough, the next development lead towards the IPFRR mechanisms.

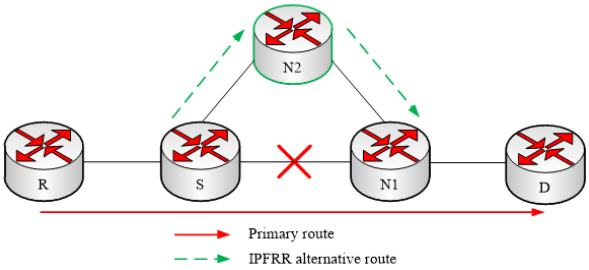

Figure 1: Basic IPFRR principle

The main goal of all IPFRR mechanisms is to minimize the network recovery time after a node or link failure. The key feature of these mechanisms is the calculation of alternative route before the failure occurs [13, 9]. The computation of alternative route requires network topology information and therefore most of the existing IPFRR mechanisms strongly depend on the usage of link-state routing protocols.

When there is a link failure in the network, the IPFRR mechanism routes the packets to a pre-computed alternative route until the network converges, Figure 1. During this time, the routing protocol makes updates about the network topology changes. This update of routing protocols happens in the background. After its completion, the routing protocol takes back the control over the routing of packets.

An important factor in IPFRR is the recovery time after the node or link failure. This time should be one of the key factors when evaluating the IPFRR mechanisms. The average reaction time of current IPFRR mechanisms for fast recovery is 50ms [10, 3].

Many IPFRR mechanisms have been proposed. They can be categorized into three main groups:
- Loop Free Alternates (LFA) mechanisms [5],
- Equal Cost Multiple Paths (ECMP) mechanisms [11],
- Multihop solutions: Tunnels, Multiple Routing Configurations (MRC), Maximally Redundant Trees (MRT), PQ-Space, U-Turn Alternative, Remote LFA (rLFA) [6, 4].

Modern network routing protocols use a relatively slow

*Thesis supervisors: doc. Ing. Pavel Segeč, PhD., Ing. Peter Palúch, PhD.
Defended at Faculty of Management Science and Informatics, University of Žilina on August, 2015.

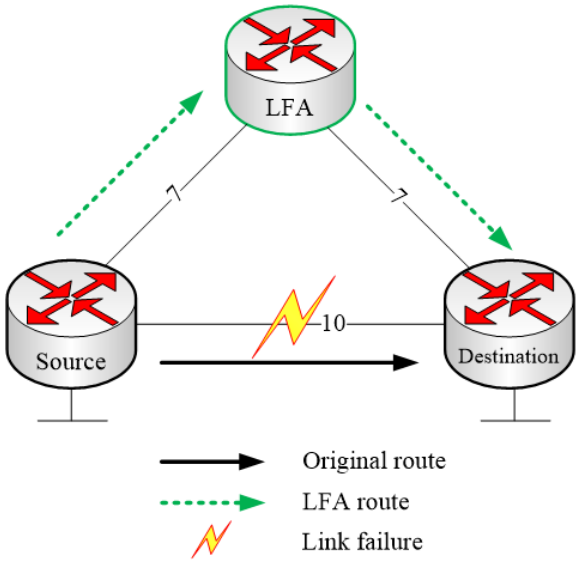

Figure 2: LFA

and complex hello mechanism. The failure detection time of routing protocols alone is insufficient for rapid rerouting requirements. Therefore, fast failure detection is an important part of an IPFRR mechanism. There is a number of existing alternative failure detection mechanism approaches that can be used [13]:
- Physical detection mechanism (loss of carrier, loss of light, increase in bit error rate, etc.),
- Independent detection mechanism (Bidirectional Failure Detection protocol) [12],
- Routing protocol detection (Hello mechanisms).

1.1 Loop Free Alternates

When the source router S detects a link failure, it sends traffic to an alternate back up router - also called an LFA (see Figure 2). The selection of the LFA router is precomputed in advance. An LFA router must be directly connected to the source router S. The LFA router must provide a loop-free path to forward packets to the destination D. The source router may have precomputed more than only one next-hop LFA router [5].

The LFA router election is defined by two criteria. These conditions guarantee that LFA router provides a loop free path:

Loop-Free Criterion:

$$Cost(N, D) < Cost(N, S) + Cost(S, D) \qquad (1)$$

Downstream Path Criterion:

$$Cost(N, D) < Cost(S, D) \qquad (2)$$

where S is a source router, N is a potential LFA router, D is the destination router and $Cost(N, D)$ is the cost of the shortest path from N to D, $Cost(N, S)$ is the cost of the shortest path from N to S, $Cost(S, D)$ is the cost of the shortest path from S to D. LFA mechanism has good

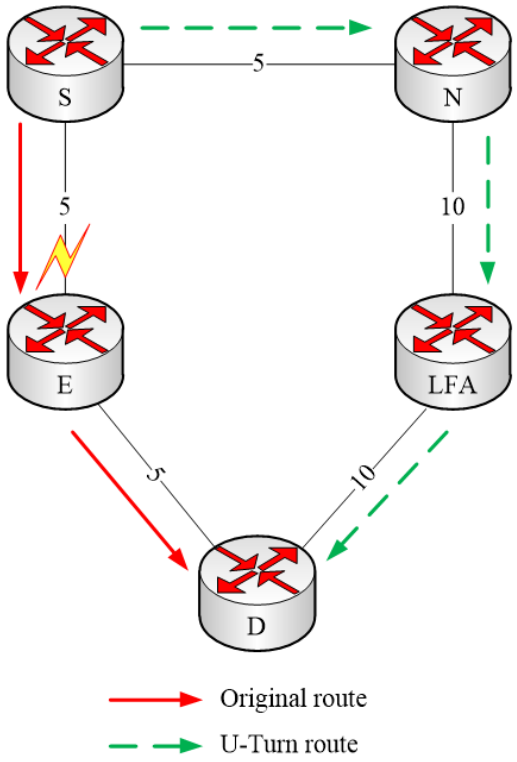

Figure 3: U-Turn

basic protection against a link or a node failure. Other LFA mechanisms improvements allows the locations of the LFA backup router more than one hop away from the source router (for example Remote LFA mechanism).

1.2 U-Turn Alternative

LFA mechanisms usually use directly connected neighboring routers to send data traffic around the failed link. When an LFA router is not available, the U-Turn mechanism can be used instead [9]. The mechanism allows the source router S to send traffic to a so-called U-Turn alternative router N (see Figure 3).

U-Turn router (N) then recognizes the special traffic from the source router S and this traffic will not be dropped. When the U-Turn router receives packets from the source router S, packets will be forwarded to the LFA router of router N. The LFA router then sends these packets to destination.

In the case the router U does not implement the U-Turn mechanism, packets from router S can be blackholed, misrouted or looped.

The U-Turn alternative candidate must pass following condition [9]: Node Selection Criterion:

$$Cost(N, D) \geq Cost(N, S) + Cost(S, D) \qquad (3)$$

where S is a source router, N is a potential U-Turn router, D is a destination router and $Cost(N, D)$ is the cost of the shortest path from N to D, $Cost(N, S)$ is the cost of the shortest path from N to S, $Cost(S, D)$ is the cost of the shortest path from S to D.

A U-Turn router must be able to recognise the traffic from the source router S, either in implicit or in explicit

way. Implicit detection means that the U-Turn router has a special algorithm for recognition of an IP FRR traffic sent from a source router S. The algorithm tells the router which traffic from source router S is sent over a backup path as opposed to normal routing.

Explicit detection occurs when the source router S will somehow modify header of packets and the U-Turn router is able to receive and recognize these modified packets. Modification of packet headers may possibly cause problems with compatibility among other routers within the network.

In the next section, we focus on analyzing the disadvantages of existing IPFRR mechanisms.

2. Problem specification

2.1 Pre-computing

The basic principle of IPFRR mechanisms is based on the fast detection of the link failure and precomputed alternative routes. The complexity of these pre-calculations is not trivial.

The computational complexity increases with the number of the routers in the network. The computations need to be performed again after topology change in order to update the alternative routes. The routers usually perform these calculations as processes with low priority during the idle time of the router CPU. The additional alternative route calculations thus consume time and system resources of the router. Therefore we consider these pre-computations to be one of the problematic areas of the existing IPFRR mechanisms.

2.2 Dependence on link-state routing protocols

Another important factor is that many of the existing IPFRR algorithms require the topology information about the network in order to pre-compute the alternative route. This fact limits the usage of IPFRR mechanisms to the networks with link-state routing protocol. Majority of existing IPFRR mechanisms depend on the link-state routing protocols.

2.3 Research direction

The analysis of existing solutions shows that the existing mechanisms meet the basic IPFRR requirements, but they are complicated. Our goal was therefore to develop a new simpler mechanism that would meet the basic IPFRR requirements. One of the possibilities that has not been used in the current IPFRR mechanisms is the multicast technology [7]. This was the starting point of our search for a new mechanism that would bring a new principle into IPFRR area. After we had made the decision to use the multicast technology, the question was which multicast protocol to use? We have focused our efforts mostly on the PIM protocol. The PIM protocol can work either in sparse [8] or dense [2] mode.

3. Protocol Independent Multicast - Dense Mode (PIM-DM)

PIM-DM protocol assumes, that all routers in network want to receive multicast traffic. At the beginning of multicast transmission, routers with enabled PIM-DM protocol send multicast packets to all other routers in the network. This process is called flooding [2]. PIM-DM protocol uses Reverse Path Forwarding (RPF) protection mechanism against micro-loops, which can occur during initial flooding of multicast communication. If some routers with enabled PIM-DM do not want to receive specific multicast communication, they send Prune message to upstream router. This process is called pruning.

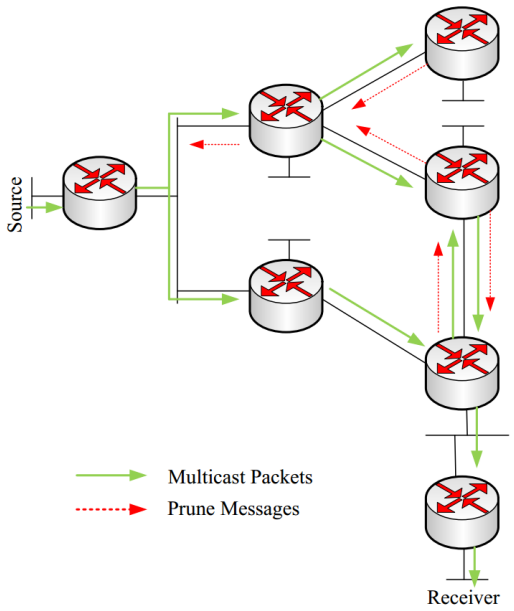

Figure 4: Protocol PIM-DM

Interfaces on routers, which send the Prune message, get to pruned state. Pruned state is valid for a limited period of time. After this period, routers receive the multicast communication again. The prune state is related to a specific multicast (S, G) pair. If a new receiver appears in the pruned area, the PIM-DM protocol uses the PIM Graft message to cancel the pruned state. The PIM Graft message is sent by the corresponding router to its upstream router.

In order to minimize the number of pruning and flooding processes, the PIM-DM protocol uses a State Refresh message. This message is for extension of the pruned state. Flooding and pruning processes cause unwanted traffic in the network. The PIM-DM is more efficient when it is used in a network with dense multicast traffic.

The protocol PIM-DM uses an RPF protection against micro-loops. Multicast packet is accepted by a router only if it passes an RPF check. RPF check in PIM-DM means that a multicast packet is accepted only if it is received via interface, which is used in unicast communication to reach the source of multicast transmission. In other words, the multicast packets are accepted only if they arrive via an interface, which is on the shortest path by unicast routing table to source of multicast transmission.

4. Proposal of new M-REP IPFRR mechanism

At the beginning of flooding multicast communication, the PIM-DM sends packets to all routers with enabled PIM protocol. This fact means, that multicast packets (independently of any failures) will get to the destination router. We want to

use this specific behavior of PIM-DM protocol to develop a new IPFRR mechanism.

4.1 Modification of RPF

The original behavior of RPF mechanism is not compatible with our intended RPF utilization in IPFRR. Under some circumstances, a specific router with original RPF mechanisms may drop our IPFRR communication.

The original RPF mechanism uses information from unicast routing table to select the correct RPF interface for specific multicast (S, G) flow. However, in network, where router or link failure has occurred, the information in unicast routing table may not be correct on the affected routers by failure until the process of network convergence is complete. It means that some router on the original path to destination can drop our IPFRR multicast flow because of RPF check.

Using a simple modification of the original RPF mechanism, we can flood IPFRR communication around the failed link or router. Our new IPFRR mechanism still uses the RPF mechanism in PIM-DM, but it focuses on modification of RPF mechanism, which selects the correct RPF interface for specific multicast communication.

4.2 Description of new IPFRR mechanism

Our new IPFRR mechanism is not designed to provide a link or node protection, but to protect a specific unicast flow (flow protection).

We assume that a customer sends an important flow of data to the destination D. If any router on the path to the destination detects a connection failure (link or node), it becomes the router S - source router.

The source router encapsulates protected unicast flow to a specific multicast flow (specific Source, G pair), which is immediately flooded to all active interfaces with enabled PIM Dense Mode. The router performs this tunneling of unicast flow until the process of convergence in the network is complete.

From the moment, when the link or node failure occurs on the original shortest path between the source and the destination, the routing information in the routing tables is outdated. The result is that the routers do not have the current information about the correct RPF interface, until the convergence process in the network is complete.

If we retain the original RPF mechanism (the packet must enter via interface, which according to the routing table is on the shortest path back to the sender of the packet), one of our routers on original shortest path can drop our specific multicast flow because of RPF check failure.

When the first multicast packet for a group G enters on a specific interface of router (non-S), this interface becomes the RPF interface for our IPFRR multicast flow. The term "first packet" denotes a multicast packet, processing of which leads to the creation of a new route record in the multicast routing table for a specific (Source, G) pair. In other words, the RPF interface of all routers, will be the **interface of the first arrival**, 6 of specific IPFRR multicast packets for a specific (Source, G) pair. After the selection of the RPF interface, routers forward multicast packets to all other PIM enabled interfaces 5.

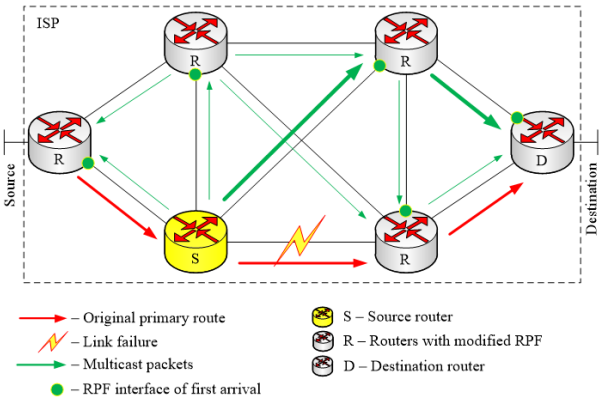

Figure 5: M-REP IPFRR mechanism

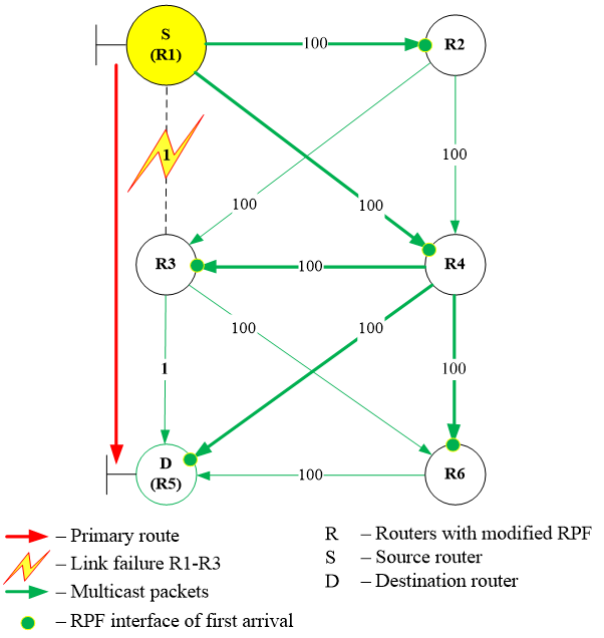

Figure 6: The rule of first arrival

Each router can have only one RPF interface. It can be proved that for a network with point-to-point links, our modified RPF mechanism provides loop-free paths to all other routers in the network, including the destination router D. In dissertation work is mathematical proof, which proved, that our modification of original RPF mechanism does not cause micro-loops during initial flooding of multicast packets.

The alternative path, which is created by selection of modified RPF interface, is a randomly generated path. In other words, the created path may not be the shortest possible path (IPFRR techniques generally do not provide the shortest alternative paths).

The IPFRR encapsulated packets must be restored back to the original format while leaving the network domain. The restoration process of IPFRR communication is performed by the destination router (D). Router D is the router, which has directly connected the original recipient of unicast packet. Router D performs the necessary decapsulation, which means that the end of IPFRR multi-

cast distribution tree is on this router. After this process, the packet can be sent to its original destination.

Our modification of the original RPF mechanism for specific multicast (Source, G) flow does not cause micro-loops between routers with point-to-point links. Requirements of our new IPFRR mechanism for physical network topology are:
- point-to-point links between routers,
- router D, original destination of protected flow, must be directly connected to this router.

We note that the original pruning process in the PIM-DM protocol is not modified. If a router receives unnecessary protected multicast flow, for which it does not have a recipient, it prunes from the multicast distribution tree. The final result of the flooding process is only one route created from the router S (performs tunnelling communication) to the router D (performs restoration of communication).

Tunnelling mechanism of IPv4 unicast communication is one of the many possible solutions how to back up information of original source and destination of the packet.

Another way how to backup the original source and destination of the protected unicast flow in IPv6 is the use of next headers, in which we can backup this information. This information can then be restored by router D from the next header of the packet.

4.3 Multiple failures

Protocol PIM-DM uses the Graft message to re-initialize the distribution tree and cancel the Prune state. In the classical PIM-DM, the Graft message is sent through the RPF interface. In our mechanism, we need to deal with the loss of the RPF interface and therefore we have modified the terms of use of the Graft message.

In the following example, we show the application of the modified RPF procedure and Graft mechanism M-REP. Suppose we have the topology shown in Figure 7, and the first link failure happens on router R2. The router which detects this failure, becomes router S and starts encapsulating unicast communication for specific multicast specified by pair (Source, G). Suppose the alternative route created using the rule of first arrival is S $\rightarrow$ R1 $\rightarrow$ R2 $\rightarrow$ R3 $\rightarrow$ R4 $\rightarrow$ D. The routers, which receive the unwanted multicast communication, send the Prune message. When there is another failure in the network, this time router R4, the router D must restore the alternative route. The question arises, which interface should be selected on router D as the RPF interface for sending the Graft message to its upstream router.

If the router D selects fa 0/0 as the RPF interface and uses it to send the Graft message, the router R5 cannot use it to restore the alternative route, because it would lose the connectivity with the upstream router R4. This means that the router D cannot determine the proper RPF interface in this situation. Therefore the router D does not select any RPF interface for the specific (Source, G) multicast flow and sends the Graft message through all remaining interfaces and removes the item for (Source, G) from its own multicast routing table. After receiving the Graft message, the router R6 sets the given interface

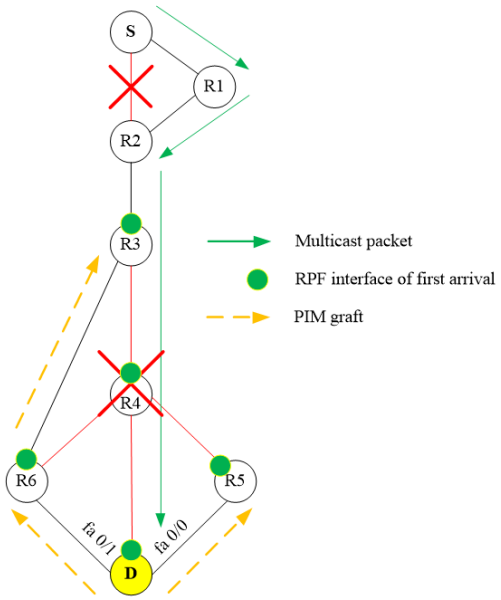

Figure 7: Solution to subsequent failures

to forward and uses its own RPF interface of the first arrival to send the next Graft message to the upstream router. When the router D receives the specific (Source, G) multicast flow again (clearly from router R6), it sets its new RPF interface. The alternative route is restored and it will be S$\rightarrow$ R1 $\rightarrow$ R2 $\rightarrow$ R3 $\rightarrow$ R6 $\rightarrow$ D. Packets will be delivered to their destination only after the multicast distribution tree is restored. Until the specific (Source, G) multicast distribution tree is restored, the packets are thrown away by router R3 or any of its upstream routers.

If we modify previous topology to topology on picture (Figure 8), problem may arise if we use same scenario as in previous case. Assume, that in time of failure or router R4 another link failure between routers R3 and R7 occurs.

When router R7 detects failure on its RPF interface of first arrival, it sends Graft message to all other PIM enabled interfaces, which means in given topology sending Graft message to router R6. In classical PIM-DM router, which receives Graft message via RPF interface, wonâĂŹt accept it. Therefore we must modify behavior of router, which receives Graft message via RPF interface of first arrival. If router receives Graft message via its RPF interface of first arrival, it removes specific (Source, G) record in multicast routing table, cancel current RPF interface of first arrival and sends Graft message to all other remaining interface. After arrival of new specific (Source, G) packet router sets new RPF interface based on first arrival again. Final alternative route will be S $\rightarrow$ R1 $\rightarrow$ R2 $\rightarrow$ R3 $\rightarrow$ R6 $\rightarrow$ D.

5. Testing

In this section, we describe the testing of the M-REP IPFRR mechanism in the OMNeT++ simulator (version 4.5). We have used the existing implementation of the PIM-DM protocol from the ANSA library (version 2.2) [1] as the basis for the simulations and we have then implemented the M-REP mechanism functionality into the ANSA library.

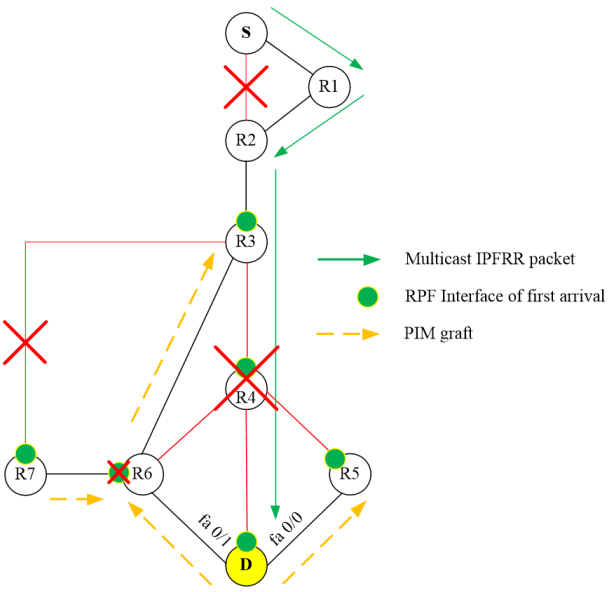

Figure 8: Solution to subsequent failures part 2

To generate the data flow, we use the Source1 in the simulations and Host2 is the recipient of the generated flow. The data flow from Source1 to Host2 is protected by the proposed M-REP mechanism. The primary route for this data flow is R1 → R3 → R5, Figure 9.

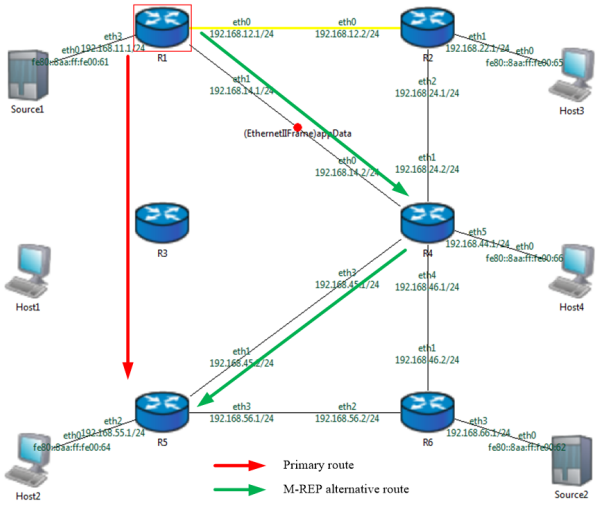

Figure 9: The rule of first arrival

We simulate the failure of the whole router that lies on the primary path to the destination. This scenario represents the disconnection of all links connected to the router R3. Table 1 shows the breakdown of the R3 failure time.

Table 1: Description of router failure scenario

	Time (sims)	Component	Action
1	50	Source1	Source1 sends data to Host2, period 1sims
2	52	R3	Failure of router R3
3	54	R3	Restoration of router R3

The expected behavior of the M-REP mechanism is that after the R3 failure, it finds an alternative route bypassing the failed router and delivers the protected unchanged unicast data flow to the destination Host2. Figure 9 shows the topology after the R3 failure.

Router R1 detects the link failure on the original path to destination and starts modifying the packets designated to go to Host2. R1 sends the packets to all output interfaces (except the incoming one).

Every router in the network receives the packets (Table 2, green color, lines 9 to 18). Router R5 determines that it is directly connected to the destination and restores the packets as previously described.

The alternative route that is created using the rule of the first arrival of specific multicast packets is R1 → R4 → R5 (Table 2, lines 9 to 18, lines 25 to 28). Table 2 shows the communication in the network before and after the router R3 failure.

Table 2: Network communication after the router failure

	Time (sims)	Action	Type of message
1	50.00001162	Source1 → R1	appData
2	50.00003497	R1 → R3	appData
3	50.00005832	R3 → R5	appData
4	50.00008167	R5 → Host2	appData
5	51	Source1 → R1	appData
6	51.00001173	R1 → R3	appData
7	51.00002346	R3 → R5	appData
8	51.00003519	R5 → Host2	appData
9	52	Source1 → R1	appData
10	52.00001173	R1 → R2	appData
11	52.00001173	R1 → R4	appData
12	52.00002346	R2 → R4	appData
13	52.00002346	R4 → R2	appData
14	52.00002346	R4 → R5	appData
15	52.00002346	R4 → R6	appData
16	52.00003519	R5 → Host2	appData
17	52.00003519	R5 → R6	appData
18	52.00003519	R6 → R5	appData
19	52.000036099999	R2 → R4	PIMJoinPrune
20	52.000036099999	R4 → R2	PIMJoinPrune
21	52.000041909999	R2 → R1	PIMJoinPrune
22	52.000047829999	R5 → R6	PIMJoinPrune
23	52.000047829999	R6 → R5	PIMJoinPrune
24	52.000053639999	R6 → R4	PIMJoinPrune
25	53	Source1 → R1	appData
26	53.00001173	R1 → R4	appData
27	53.00002346	R4 → R5	appData
28	53.00003519	R5 → Host2	appData
29	54	Source1 → R1	appData
30	54.00002335	R1 → R3	appData
31	54.0000467	R3 → R5	appData
32	54.00005843	R5 → Host2	appData

This scenario represents a situation that often happens also in the real ISP operation. The test has confirmed that the M-REP mechanism is able to protect the specific unicast flow against router failure. The dissertation thesis also contains other tests, e.g. subsequent failures of links or routers in the network.

6. Benefits of M-REP IPFRR mechanism

The main benefit of our new IPFRR mechanism is the fact, that it is independent of pre-computation. Alternative path is not calculated by internal algorithm as in existing IPFRR mechanisms. Due to this feature, we can say that M-REP IPFRR mechanism is currently unique.

According to analysis of existing IPFRR mechanisms only a few are implemented in operating systems of routers. By utilizing of existing multicast protocol PIM-DM, its minimum modification of RPF logic and modification of Graft mechanism, M-REP mechanism can be implemented in real routers.

In the following sections we discuss important benefits of our M-REP mechanism, problem areas and future research.

6.1 Independent of pre-computation

Most of existing IPFRR mechanisms are based on pre-computation of alternative paths. M-REP mechanism does not require pre-computation of alternative route. We use a specific multicast address and the process of flooding/pruning in PIM-DM to send protected traffic around the failed link or router.

For existing IPFRR mechanisms, the network size affects the amount of pre-computation. This means that the size of network increases the number of preparatory calculations of alternative backup paths.

Proposed M-REP mechanism is independent of pre-computation of alternative path, which means, it is not affected by size of the network

6.2 Independent of routing protocols

With pre-computation of alternative route there is also the related dependence on routing protocols. Some of the existing IPFRR mechanisms require network topology information for calculation of alternative backup path. That means, they are dependent on usage of link-state routing protocols. M-REP IPFRR mechanism does not require preparatory calculations of alternative route and construction of multicast distribution tree is not also based on information from unicast routing table, which means, that it is independent of routing protocols. It supports static routing, distance-vector routing protocols and link-state routing protocols.

6.3 100% repair coverage

Another advantage of M-REP IPFRR mechanism is, that it solves the problem of multiple failures in network. Protected unicast flow, which is encapsulated as specific multicast traffic, floods via functional links in the network. When multiple link or node failures occur and there is only one possible path from source to destination, our M-REP IPFRR mechanism is able to find it and use it. In other words, M-REP mechanism provides 100 percent repair coverage.

6.4 Subsequent link or node failures in network

Existing IPFRR mechanism are tested mostly against link or node failure. M-REP mechanism is based on multicast protocol PIM-DM with modified RPF and Graft mechanism. M-REP mechanism was tested against multiple, e.g. subsequent failures within network at different times. Simulations in simulator OMNeT++ proved that proposed mechanism can provide alternative path after multiple, e.g. subsequent link or node failures.

6.5 Simple implementation

M-REP mechanism uses existing multicast protocol PIM-DM. By simple modification of RPF logic for selecting

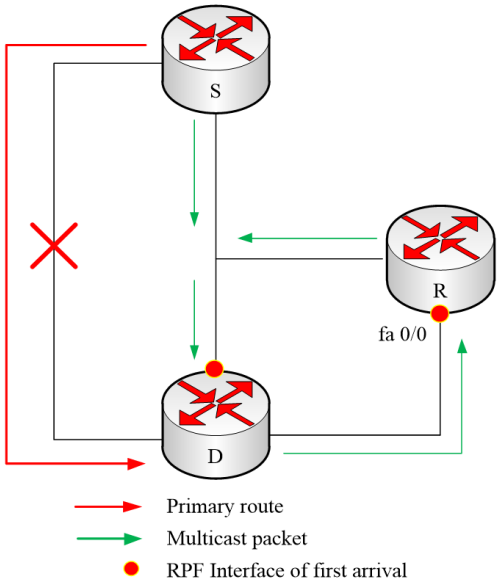

Figure 10: Micro-loops in multi-access segment

RPF interface as well as the modification of Graft mechanism modification in this protocol, we used its native behavior in new IPFRR area. PIM-DM protocol is currently supported by many important manufacturers of routers. One advantage of M-REP mechanism is thus its simple implementation.

6.6 Problem areas and future research

Problem areas of M-REP mechanism are related to its specified requirements on physical topology of network. The first requirement for network topology is the existence of point-to-point links between routers.

6.6.1 Multi-access networks

The proposed M-REP mechanism uses modified RPF logic so that RPF interface on the router is determined by the rule of first arrival. This means that for our specific IPFRR multicast group we do not use information from unicast routing table. This information is based on shortest paths to destinations. If we use M-REP mechanism in multi-access networks, micro-loops can occur.

We have a give topology, Figure 10, where router S sends IPFRR packet on network with multi-access. If the router R first receives the IPFRR packet via interface fa 0/0 from router D, according our RPF rule of first arrival, this interface will be chosen for RPF interface. A micro-loop might occur between routers D and R.

Therefore, this issue needs further research in future. We note that some of existing IPFRR mechanisms have also problems in multi-access networks (for example Remote LFA).

6.6.2 Random alternative route

Existing IPFRR mechanisms use SPF algorithm to calculate the alternative shortest path from source to destinations. These calculations require the processing power of router, but calculated alternative route is the shortest possible route.

Original PIM-DM protocol creates Shortest Path Tree (SPT). The creation of these SPT trees provides RPF mechanism in PIM-DM. RPF mechanism in M-REP do not use information from unicast routing table to verify the correct RPF interface, but the RPF interface is selected by the rule of first arrival of specific unicast (Source, G) packet. Multicasts packets reach the destination, but it is not possible to guarantee the shortest path. Multicast data may or may not get to destination by shortest path.

The second requirement of M-REP mechanism is that router D must have directly connected destination on its output interfaces. Original unicast flow of data is delivered to this destination. Destination router is identified by this requirement. Specific multicast (Source, G) tree is created from the source to destination router.

6.6.3 Packet encapsulation

Our mechanism uses in IPv4 encapsulation of protected unicast flow with additional IP header (multicast tunneling). In IPv6 can be used the same principle or new IPv6 header can proposed for this purpose. Modifications of original packets brings problems with MTU, increased CPU load and other problems. However, it should be noted that most of existing IPFRR mechanism also encapsulates packets or modify specific bits in packet header. Encapsulation of packets is one of the biggest disadvantages of existing IPFRR mechanism, but in present this technology is most common.

6.6.4 Flooding/pruning process in PIM-DM

PIM-DM protocol at the beginning of multicast transmission sends multicast packets to all routers in administrative domain (flooding process). Routers, which donâĂŹt have recipients for specific multicast communication, prune from multicast distribution tree (pruning process). Besides these processes, PIM-DM periodically sends "Hello" messages to other routers. Flooding and pruning processes brings unnecessary load in the network. However, M-REP IPFRR mechanism encapsulates protected unicast flow to specific (Source, G) multicast flow until process of network convergence is complete. When the process of network convergence is complete, routing protocol routes packets again.

6.7 Future research

Companies such as Cisco Systems and Juniper Networks focus they future development on IPFRR technology, because the requirements on ISP grow every day. Future research should focus on further validation of the proposed mechanism M-REP, solving of the problem areas and implementation in an experimental environment Quagga. The current requirements of M-REP mechanism for point-to-point links or directly connected destination may be sometimes limiting.

The proposed M-REP IPFRR mechanism is designed to protect a specific unicast flow. Therefore, further research should focus on verification whether it is possible to protect all flows, whose primary route lead through the failed link.

7. Conclusion

This work presents a new M-REP IPFRR mechanism that solves some of the disadvantages of existing IPFRR mechanisms. The new M-REP IPFRR mechanism relies on the innovative use of multicast PIM-DM protocol. At the beginning of the multicast transmission (flooding), the PIM-DM protocol delivers the multicast data to every PIM router in the network (regardless of failure). This is the specific property of the PIM-DM protocol that we have used when designing the new M-REP mechanism. This mechanism is primary designed to protect the specific unicast flow using the backup multicast distribution tree defined by the unique multicast address.

As previously mentioned, the majority of the IPFRR mechanisms requires pre-computing of alternative routes for the case of various failure of links or routers in the network. These preparatory calculations have undesired effects, e.g. loading of router CPU, dependence on the link-state routing protocols etc.

M-REP mechanism does not require preparatory calculations of backup routes, because it uses the PIM-DM protocol's flooding process to floods the multicast communication. With respect to the specific conditions and purposes, under which this system is supposed to operate, it was necessary to modify the RPF mechanism in PIM-DM. RPF interface is chosen based on the arrival of the first packet with special multicast address. All routers in the administrative domain must have exactly one RPF interface for specific (Source, G) flow.

Protocol PIM-DM with modified RPF mechanism explicitly creates a tree, which means that no routing loops are created among the routers. The alternative route is created using the rule of the first arrival of the specific multicast packet. The protected unicast communication is encapsulated until the network convergence process is completed.

The new M-REP IPFRR mechanism solves the problem of performing the pre-comutations by the existing IPFRR mechanisms, the dependence on routing protocols and problem of multiple failures in the same network, e.g. subsequent failures. Other advantages are the 100% repair coverage and simple implementation into the existing operating systems of routers.

References

[1] Fakulta informačných technológií VUT Brno. ANSA extension above INET framework for OMNeT++, 2014. https://github.com/kvetak/ANSA.

[2] A. Adams, J. Nicholas, and W. Siadak. Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised). *RFC 3973, Network Working Group*, pages 4–10, 2010.

[3] S. Antonakopoulos, Y. Bejerano, and P. Koppol. A simple IP fast reroute scheme for full coverage. *BellLabs, Murray Hill, USA*, page 1, 2012.

[4] A. Atlas. U-turn Alternates for IP/LDP Fast-Reroute. *Google, Internet-Draft, Network Working Group*, pages 1–8, 2006.

[5] A. Atlas and A. Zinin. Basic Specification for IP Fast Reroute: Loop-Free Alternates. *Alcatel-Lucent, RFC 5286, Standards Track, Network Working Group*, pages 3–5, 2008.

[6] S. Bryant, C. Filsfils, S. Previdi, and M. Shand. IP Fast Reroute using tunnels. *Cisco Systems, Network Working Group, Internet-Draft*, pages 1–10, 2010.

[7] S. Deering. Host Extensions for IP Multicasting. *Stanford University, RFC 1112, Network Working Group*, pages 1–5, 2006.

[8] B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas. Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised). *RFC 4601, Standards Track, Network Working Group*, pages 1–146, 2006.

[9] M. Gjoka, V. Ram, and X. Yang. Evaluation of IP Fast Reroute Proposals. *COMSWARE 2007. 2nd International Conference*, pages 1–8, 2007.

[10] A. T. Hassan. Evaluation of Fast Reroute Mechanisms in Broadband Networks. *Master of Electrical and Computer Engineering, University of Ottawa*, page 1, 2007.

[11] C. Hopps. Analysis of an Equal-Cost Multi-Path Algorithm. *NextHop Technologiest, RFC 2992, Informational, Network Working Group*, pages 1–5, 2000.

[12] D. Katz and D. Ward. Bidirectional Forwarding Detection (BFD). *Juniper Networks, Request for Comments: 5880, Standards Track, IETF, ISSN: 2070-1721*, pages 1–50, 2010.

[13] M. Shand and S. Bryant. IP Fast Reroute Framework. *RFC 5714, Internet Engineering Task Force, Informational, ISSN: 2070-1721, Cisco Systems*, pages 5–7, 2010.

Selected Papers by the Author

J. Papán, P. Segeč, P. Palúch. Utilization of PIM-DM in IP Fast Reroute. In *ICETA 2014: 12th IEEE International Conference on Emerging eLearning Technologies and Applications*, ISBN 978-1-4799-7739-0, IEEE, 373–378, 2014.

J. Papán, P. Segeč, P. Palúch. Tunnels in IP Fast Reroute. In *Digital Technologies: The 10th International Conference*, ISBN 978-1-4799-3301-3, IEEE, 281–285, 2014.

J. Papán, P. Segeč, P. Palúch. Multicast in IP Fast Reroute. In *ELEKTRO 2014: Proceedings of 10th International Conference*, ISBN 978-1-4799-3720-2, IEEE, 81–85, 2014.

P. Segeč, P. Palúch, J. Papán, M. Kubina. The integration of WebRTC and SIP: Way of Enhancing Real-time, Interactive Multimedia Communication. In *ICETA 2014: 12th IEEE International Conference on Emerging eLearning Technologies and Applications*, ISBN 978-1-4799-7739-0, IEEE, 437–442, 2014.

J. Papán, M. Jurečka, J. Milanová. WSN for Forest Monitoring to Prevent Illegal Logging. In *FedCSIS: Proceedings of the Federated Conference on Computer Science and Information Systems*, ISBN 978-83-60810-51-4, IEEE, 809–812, 2012.

M. Drozdová, M. Mokryš, M. Kardoš, Z. Kurillová, J. Papán. Change of Paradigm for Development of Software Support for eLearning. In *ICETA 2012: 10th IEEE International Conference on Emerging eLearning Technologies and Applications*, ISBN 978-1-4673-5123-2, IEEE, 2012.