ANNUAL OF ASSEN ZLATAROV UNIVERSITY, BURGAS
BULGARIA, 2021, v. L (1)

GENERALIZED NETS MODEL FOR MARKING PACKETS FOR FURTHER PROCESSING

Ivelina Vardeva, Stoyan Dimitrov
E-mail: ivardeva@btu.bg

ABSTRACT

The article describes the mangle method used to mark packets and connections, as well as several special changes that can be applied to network traffic passing through the MikroTik firewall. The apparatus for generalized networks was used to describe the processes of the method. Generalized networks are used by means of constructing flexible and structured models of systems in which time-parallel processes consisting of multiple interacting components take place.

Key words: *marking package, mangle rule, generalized net*

INTRODUCTION

The mangle rule is used for packet and connection marking as well as a few special changes that can be applied to traffic passing through the MikroTik firewall.

Mangle rule is a kind of 'marker' that marks packets for future processing with special marks. Many other facilities in RouterOS make use of these marks, e.g. queue trees, NAT, routing. They identify a packet based on its mark and process it accordingly. The mangle marks exist only within the router, they are not transmitted across the network.

In the present research we develop Generalized Net [1, 3] models for marking packets for further processing. Indexed matrices are used to describe the states of the token [2]. The generalized network is built of many transitions, containing conditions under which the nuclei pass from the input to its output places [1, 3].

EXPOSITION

The main functions that are available there are to place special marks on packages or links. Depending on the type of marking, bookmarks can be used for other services within the router itself. For example, packet marking, links, and routing marks can be used as filter conditions, packet marking can be used in Queues quality management or QoS, and routing marks in routing tables. Under the terms of the Mangle policy, predefined chains are also available that determine when to place the marker. The chains are:

• Forward - marking is performed before a filter in the forward chain;

• Input - marking is performed before a filter in the input circuit;

• Output - marking is performed before a filter in the output circuit;

• Postrouting - marking is performed before a filter in the src-nat circuit;

• Prerouting - marking is performed before a filter in the dst-nat circuit;

Diagram mangle rule for packet and connection marking is shown in Fig. 1.

The actions that can be performed after creating appropriate conditions are twenty, and those that place markers are:

• mark-connection - puts a marker, which is set to the parameter new-connection-mark, on the whole connection, for which compliance is found in the conditions;

• mark-packet - places a marker, which is set to the new-packet-mark parameter, on each package for which compliance with the conditions is found;

• mark-routing - sets a marker that is set to the new-routing-mark parameter. Such tokens are used in managing the routing process through policies.

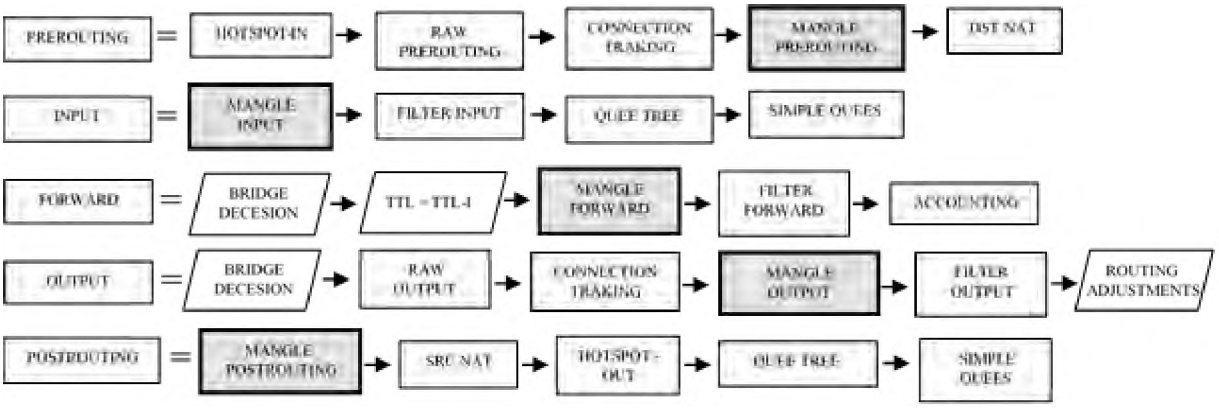

Fig.1. Diagram mangle rule for packet and connection marking

This article presents a model described forward chain when using mark-connection and mark-packet. Rules must first be applied to mark the required connections, and then a rule must be executed to mark the packets in them [4, 5, 6]. Thus, it will not be necessary to process all traffic by the packet marking rule presented in Table 1.

Table 1. Packet marking rule

```
/ip firewall mangle
add action=mark-connection chain=forward connection-state=new src-address=192.168.100.0/24 \
passthrough=yes new-connection-mark=netN
add action=mark-packet chain=forward connection-mark=netN new-packet-mark=clients-netN \
passthrough=yes
```

Thus, the first rule checks the IP header and look for compliance in the new requests, adding a connection token in those for which there is compliance. The next rule no longer checks the IP header of each packet, but will simply check the connection token and mark the packets if it finds a match. The latest action added by MikroTik in Mangle is called route: its function is to redirect packets to the IP address specified in the rule on the next router, ignoring the normal routing process. The route action can only be used with the prerouting circuit because it works before the routing process decides.

As illustrated in Fig. 2, we study a GNs model containing four transitions, which correspond to the following aspects of the above-described mangle rule for forward chain:

$A = \{Z_1, Z_2, Z_3, Z_4, Z_5, Z_6\}$,

where the transitions describe the following processes:

Z_1= "Represents the chain forward";
Z_2= "Represents the bridge decision";
Z_3= "Represents the TTL";
Z_4= "Represents the mangle forward";
Z_5= "Represents the filter forward"
Z_6= "Represents the accounting"

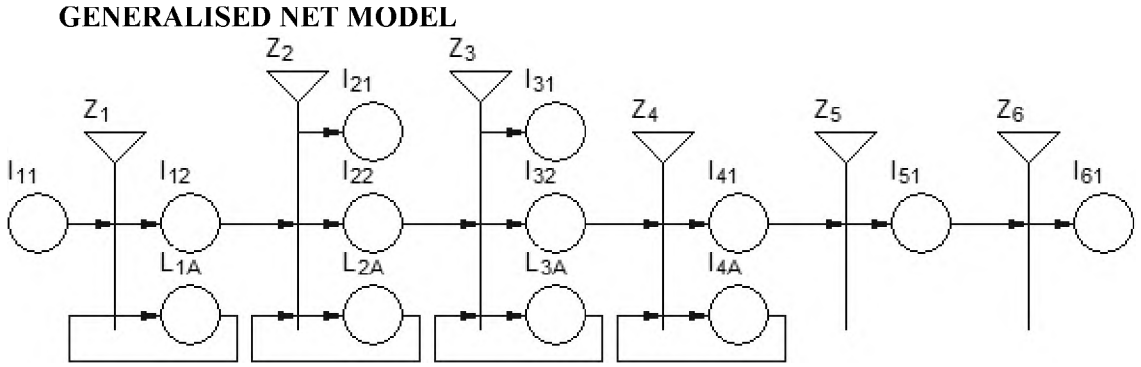

Fig. 2 Generalized net model for processing the received packets

In place l_{11} token α with characteristic "received package for chain forward".

What follows is a description of the transitions of the net.

The transitions have the following description:

$Z_1 = \langle\{l_{11}, L_{1A}\}, \{l_{12}, L_{1A}\}, R_1, \vee(l_{11}, L_{1A})\rangle$,

Where:

R_1	l_{12}	L_{1A}
l_{11}	*false*	*true*
L_{1A}	$W_{L_{1A},l_{12}}$	*true*

$W_{L_{1A},l_{12}}$ = "there is a package from a forward chain".

When the predicate $W_{L_{1A},l_{12}}$ has truth value "true" the α token from place l_{11} enters place L_{1A} with characteristic "*request to forward chain*".

$Z_2 = \langle\{l_{12}, L_{2A}\}, \{l_{21}, l_{22}, L_{2A}\}, R_2, \vee(l_{12}, L_{2A})\rangle$,

Where:

R_2	l_{21}	l_{22}	L_{2A}
l_{12}	*false*	*false*	*true*
L_{2A}	$W_{L_{2A},l_{21}}$	$W_{l_{2A},l_{22}}$	*true*

$W_{L_{2A},l_{21}}$ = "bridge decision is rejected",

$W_{l_{2A},l_{22}}$ = "bridge decision is allowed".

In place l_{12} token α obtains the characteristic "available is package from bridge decision". After transition α token enters l_{22} the place obtains the characteristic "*allowed incoming package*".

$Z_3 = \langle\{l_{22}, L_{3A}\}, \{l_{31}, l_{32}, L_{3A}\}, R_3, \vee(l_{22}, L_{3A})\rangle$,

Where:

R_3	l_{31}	l_{32}	L_{3A}
l_{22}	*false*	*false*	*true*
L_{3A}	$W_{L_{3A},l_{31}}$	$W_{l_{22},l_{32}}$	*true*

$W_{L_{3A},l_{31}}$ = "verified TTL is reject".

$W_{L_{3A},l_{32}}$ = "verified TTL is allowed".

In place l_{22} token α obtains the characteristic "verified the incoming package from TTL". After transition α token enters l_{32} the place obtains the characteristic "allowed TTL from package".

$Z_4 = \langle\{l_{32}, L_{4A}\}, \{l_{41}, L_{4A}\}, R_4, \vee(l_{32}, L_{4A})\rangle$,

Where:

R_4	l_{41}	L_{4A}
l_{32}	*false*	*true*
L_{4A}	$W_{L_{4A},l_{41}}$	*true*

$W_{L_{4A},l_{41}}$ = "packed is marked".

In place l_{32} token α obtains the same characteristic "allowed TTL from package". When the predicate $W_{L_{4A},l_{41}}$ has truth value "true" the α token from place l_{41} enters place with characteristic "*marked packed with mangle rule*".

$Z_5 = \langle\{l_{41}\}, \{l_{51}\}, R_5, \vee(l_{41})\rangle$,

Where:

R_5	l_{51}
l_{41}	$W_{l_{41},l_{51}}$

$W_{l_{41},l_{51}}$ = "filter forward is available".

When the predicate $W_{l_{41},l_{51}}$ has truth value "true" the α token from place l_{51} enters place with characteristic "*proceed filter forward*".

$Z_6 = \langle\{l_{51}\}, \{l_{61}\}, R_6, \vee(l_{51})\rangle$,

Where:

R_6	l_{61}
l_{51}	$W_{l_{51},l_{61}}$

$W_{l_{51},l_{61}}$ = "accounting is available".

When the predicate $W_{l_{41},l_{51}}$ has truth value "true" the α token from place l_{61} enters place with characteristic "*accounting*".

CONCLUSION

Creating complex tasks related to traffic authorization, routing through policies, etc. impose a requirement to work with various elements of RouterOS. This type of tasks requires not only to achieve the desired result, but also to optimize the available resources to attain good results.

The presented GN model describes the place of special marks on packages or links depending on the type of marking or bookmarks. The developed model can help examination, analyzing and optimizing the flowing processes in exchanging such data in the router rules.

REFERENCES

1. Atanassov K., Generalized nets, World Scientific, Singapore, 1991
2. Atanassov K., Index Matrices: Towards an Augmented Matrix Calculus, Springer, Berlin, 2014

3. Atanassov K., On Generalized Nets Theory, "Prof. M. Drinov" Academic Publ. House, Sofia, 2007
4. Boyadzhiev D., MikroTik RouterOS Basics (book), FOR THE LETTERS, ISSN: 978-619-185-252-9, 2016, Sofia
5. Petrov Y., Determining the area of the automobile tire contact footprint using generalized nets, Annual of Assen Zlatarov University, Burgas, Bulgaria, 2020, v. XLIX
6. Staneva, Liliya Anestieva. "Minimising using the Method of Quine-McCluskey with Generalised Nets." 2019 29th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE). IEEE, 2019