Разпределение на трафика (Load balancing)

- Обща представа
- Реализация с политики за маршрутизация

София, MUM България 2014

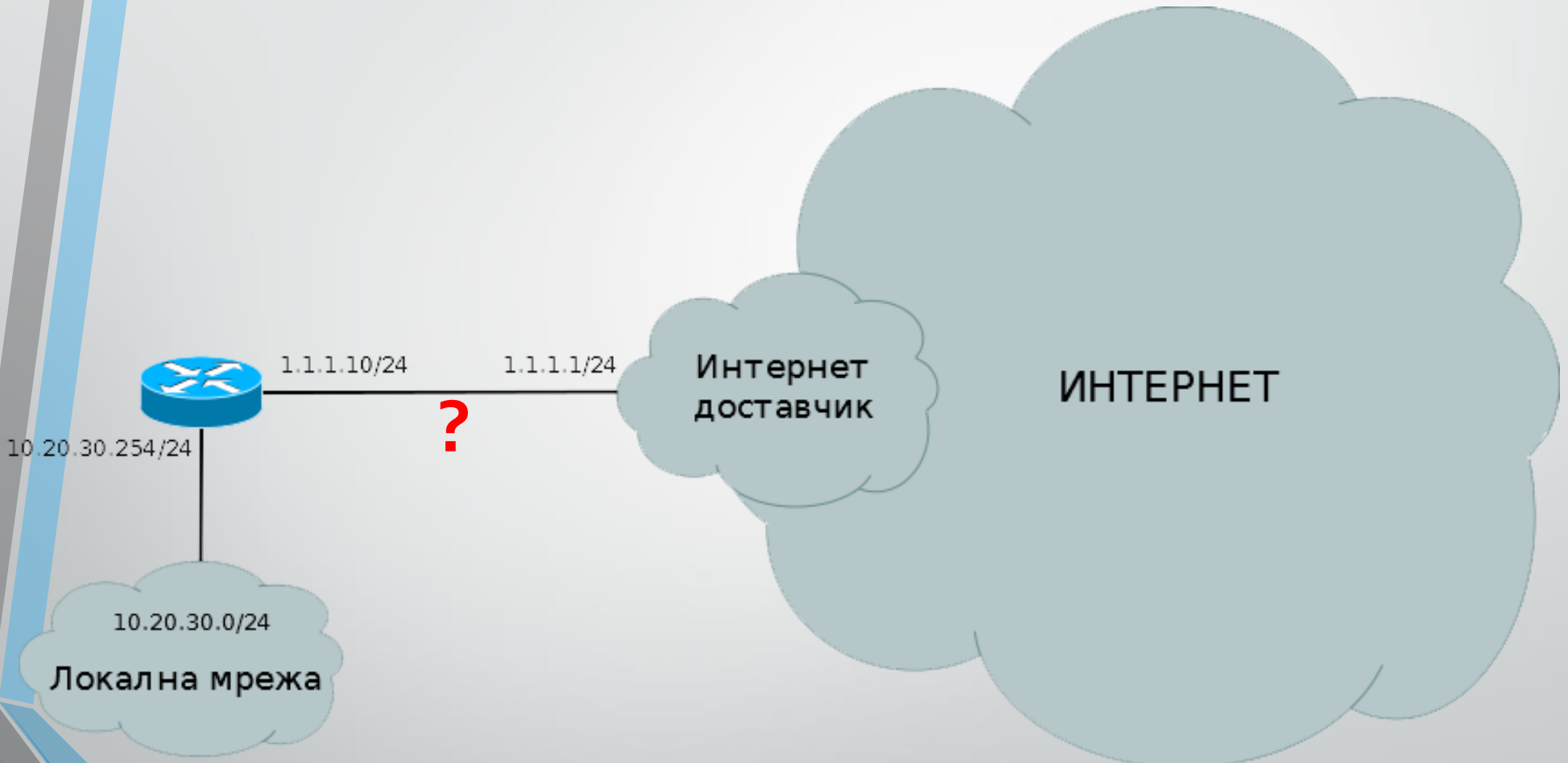
За мен:

Петър Димитров

ПГ НЕТ ПРО ЕООД

- Опит с MikroTik от 2005 г.
- MikroTik Certified Trainer от 2013 г.

Една връзка към интернет

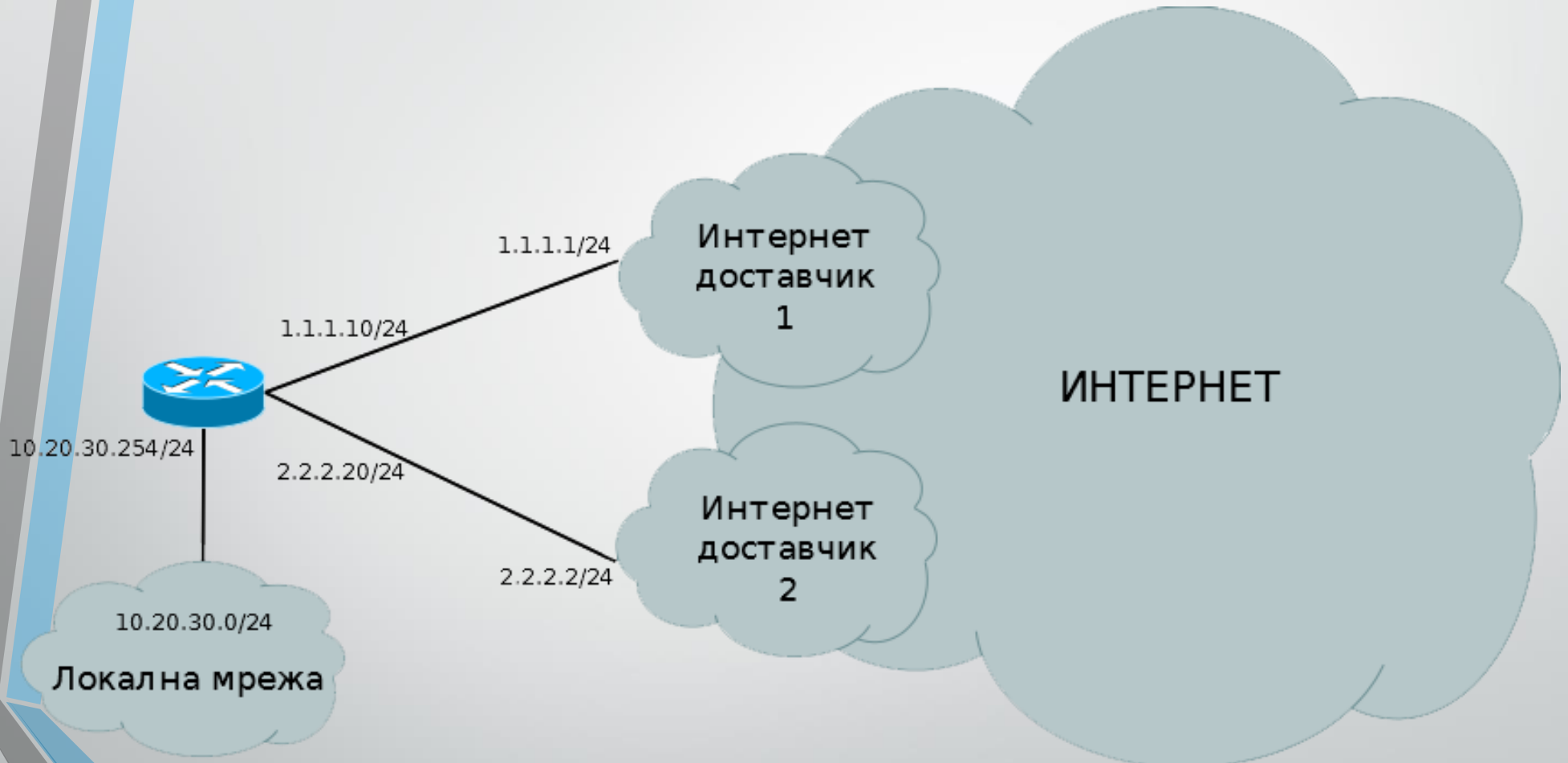


Повече от една връзка

- За осигуряване на безотказност
- За осигуряване на по-голям капацитет

В практиката, когато разполагате с повече от една връзка, желаете да осигурите и двете

Интернет с два доставчика



Разпределение на трафика осигуряване на безотказност

- Equal Cost Multi Path (ECMP) маршрути
- Протоколи за динамична маршрутизация
- Политики за маршрутизация

Какво ще ни бъде необходимо?

- Базова конфигурация на вътрешната мрежа и двата доставчика
- Дефиниране на отделни маршрутни таблици, маршрутизиращи трафика към всеки от доставчиците
- Разпределяне на трафика към двете маршрутни таблици
- Осигуряване на механизъм за безотказност

Базова конфигурация

/ip address

add address=10.20.30.254/24 interface=ether5-LAN

add address=1.1.1.10/24 interface=ether2-ISP1

add address=2.2.2.20/24 interface=ether3-ISP2

/ip firewall nat

add action=masquerade chain=srcnat out-interface=ether2-ISP1

add action=masquerade chain=srcnat out-interface=ether3-ISP2

/ip dns set allow-remote-requests=yes servers=1.1.1.1,2.2.2.2

Дефиниране на маршрутни таблици

Ще дефинираме следните маршрути:

/ip route

add gateway=1.1.1.1

add gateway=2.2.2.2

add gateway=1.1.1.1 routing-mark=ISP1

add gateway=2.2.2.2 routing-mark=ISP2

Маршрути за директно свързани мрежи

- При добавяне на IP адрес към интерфейс, се добавя автоматично динамичен маршрут само в маршрутна таблица main.
- Трафика за локалните мрежи, насочен към таблиците ISP1 и ISP2, ще попада на маршрутите по подразбиране в тези таблици.
- Ще осигурим маршрути за директно свързаните мрежи в маршрутните таблици, различни от main.

Маршрути за директно свързани мрежи

/ip route

add dst-address=10.20.30.0/24 gateway=ether5-LAN routing-mark=ISP1

add dst-address=1.1.1.0/24 gateway=ether2-ISP1 routing-mark=ISP1

add dst-address=2.2.2.0/24 gateway=ether3-ISP2 routing-mark=ISP1

add dst-address=10.20.30.0/24 gateway=ether5-LAN routing-mark=ISP2

add dst-address=1.1.1.0/24 gateway=ether2-ISP1 routing-mark=ISP2

add dst-address=2.2.2.0/24 gateway=ether3-ISP2 routing-mark=ISP2

Разпределяне на трафика

- Чрез /ip route rule
- Чрез mark-routing в /ip firewall mangle
  - По протоколи или други критерии
  - На база адресни листи
  - Чрез nth или per-connection-classifier

/ip route rule

Съдържа правила за маршрутизация, указващи какво действие да се извърши с трафик, отговарящ на определени условия:

- Трафика може да се разграничава по адрес на източника/местоназначението, маркировка за маршрутизация или входящ интерфейс
- Трафика може да се унищожи (drop, unreachable) или обработи в определена маршрутна таблица (lookup, lookup only in table)

Пример за прилагане на /ip route rule

Да маршрутизираме първата половина от адресното пространство на локалната мрежа през ISP1, втората половина – през ISP2:

/ip route rule

add src-address=10.20.30.0/25 table=ISP1

add src-address=10.20.30.128/25 table=ISP2

Почистване на конфигурацията

Премахваме правилата в /ip route rule:

/ip route rule remove [/ip route rule find]

/ip firewall mangle

Правилата в /ip firewall mangle работят на принципа "ако-тогава".

Условията в частта "ако" ще използваме за да разграничим трафика според желанието ни, действията в частта "тогава" - за да поставим съответната маркировка.

Маркировка за маршрутизация може да се постави само във вериги prerouting и output

/ip firewall mangle

- Маркировката за маршрутизация указва за местоназначението на маркирания пакет в коя маршрутната таблица да се търси маршрут.
- Маркировката на връзки предоставя възможност за оптимизация на mangle, както и за работа с всички пакети, принадлежащи на определена връзка.

/ip firewall mangle

Ще използваме следния подход:

При установяването на нови връзки, ще маркираме връзките по различен начин, в зависимост от желанието ни през кой доставчик да бъдат маршрутизирани. Ще маркираме всички пакети, принадлежащи на връзки с определена маркировка, с маркировка за маршрутизация през съответния доставчик.

Условия на база протоколи

/ip firewall mangle

add chain=prerouting protocol=tcp dst-port=80 connection-mark=no-mark action=mark-connection new-connection-mark=ISP1

add chain=prerouting connection-mark=ISP1 action=mark-routing new-routing-mark=ISP1 passthrough=no

add chain=prerouting protocol=tcp dst-port=443 connection-mark=no-mark action=mark-connection new-connection-mark=ISP2

add chain=prerouting connection-mark=ISP2 action=mark-routing new-routing-mark=ISP2 passthrough=no

Почистване на конфигурацията

Премахваме правилата в /ip firewall mangle:

/ip firewall mangle remove [/ip firewall mangle find]

Условия на база адресни листи

/ip firewall address-list

add address=10.20.30.1-10.20.30.100 list=isp1

add address=10.20.30.101-10.20.30.200 list=isp2

/ip firewall mangle

add chain=prerouting src-address-list=isp1 connection-mark=no-mark action=mark-connection new-connection-mark=ISP1

add chain=prerouting connection-mark=ISP1 action=mark-routing new-routing-mark=ISP1 passthrough=no

add chain=prerouting src-address-list=isp2 connection-mark=no-mark action=mark-connection new-connection-mark=ISP2

add chain=prerouting connection-mark=ISP2 action=mark-routing new-routing-mark=ISP2 passthrough=no

Условия на база nth

- На условието nth отговаря всеки n-ти пакет, например на nth=2,1 ще отговаря всеки 1-ви от 2 пакета, т.е. 50% от пакетите, попадащи на правилото.
- Директното използване на nth за разпределение на връзките ще доведе до проблеми при комуникация, използваща множество едновременни връзки.

Условия на база nth

- Бихте могли да използвате правила с nth за динамично добавяне в адресни листи
- На правилата, създадени към момента в mangle, ще попада само трафика, идващ от източници, чиито адреси са в адресните листи.
- Ще добавим правила на база nth, които да разпределят равномерно в адресните листи новите адреси, и да маркират трафика

Почистване на конфигурацията

Премахваме статичните записи в /ip firewall address-list:

/ip firewall address-list remove [/ip firewall address-list find]

Условия на база nth

/ip firewall mangle

add chain=prerouting in-interface=ether5-LAN connection-mark=no-mark nth=2,1 action=add-src-to-address-list address-list=isp1 address-list-timeout=1d

add chain=prerouting in-interface=ether5-LAN connection-mark=no-mark nth=2,2 action=add-src-to-address-list address-list=isp2 address-list-timeout=1d

add chain=prerouting src-address-list=isp1 connection-mark=no-mark action=mark-connection new-connection-mark=ISP1

add chain=prerouting connection-mark=ISP1 action=mark-routing new-routing-mark=ISP1 passthrough=no

add chain=prerouting src-address-list=isp2 connection-mark=no-mark action=mark-connection new-connection-mark=ISP2

add chain=prerouting connection-mark=ISP2 action=mark-routing new-routing-mark=ISP2 passthrough=no

Почистване на конфигурацията

Премахваме всички записи в /ip firewall address-list и всички правила в /ip firewall mangle :

/ip firewall address-list remove [/ip firewall address-list find]

/ip firewall mangle remove [/ip firewall mangle find]

Условия на база PCC

- per-connection-classifier изчислява хеш от указаните полета от IP хедъра и остатък при делене на този хеш с посочен делител. Ако остатъка е равен на посочения, пакета отговаря на условието.
- Подходящ критерий за разпределение на трафика би бил по адрес на източника и местоназначението (both-addresses), за осигуряване на комуникация на два хоста през един и същи доставчик

Условия на база PCC

/ip firewall mangle

add chain=prerouting connection-mark=no-mark per-connection-classifier=both-addresses:2/0 action=mark-connection new-connection-mark=ISP1

add chain=prerouting connection-mark=ISP1 action=mark-routing new-routing-mark=ISP1 passthrough=no

add chain=prerouting connection-mark=no-mark action=mark-connection new-connection-mark=ISP2

add chain=prerouting connection-mark=ISP2 action=mark-routing new-routing-mark=ISP2 passthrough=no

Плаващ статичен маршрут

- За задаване на приоритети на маршрути за едно и също местоназначение, се използва опцията "distance" (цена на маршрута)
- При изпращане на пакети, при наличие на повече от един най-специфичен маршрут за дадено местоназначение, се използва маршрут с най-малка цена и достъпен шлюз.
- Опцията "check gateway" позволява на маршрутизатора да следи дали даден шлюз е достъпен.

Механизъм за безотказност

- Ще осигурим за всяка от маршрутните таблици за двата доставчика маршрут по подразбиране с по-висока цена през другия доставчик.

```
/ip route

add gateway=2.2.2.2 distance=2 routing-mark=ISP1

add gateway=1.1.1.1 distance=2 routing-mark=ISP2
```

Механизъм за безотказност

- Ще използваме check-gateway=ping за да следим достъпността на шлюзовете

/ip route set check-gateway=ping [/ip route find dst-address=0.0.0.0/0]

Какво още?

- Ако от Интернет се осъществяват връзки към публичните адреси, трябва да осигурим съответната маркировка:

```
/ip firewall mangle add chain=prerouting in-interface=ether2-ISP1
connection-mark=no-mark action=mark-connection new-connection-
mark=ISP1 place-before=0

/ip firewall mangle add chain=prerouting in-interface=ether3-ISP2
connection-mark=no-mark action=mark-connection new-connection-
mark=ISP2 place-before=0
```

Какво още?

- Ако става въпрос за връзки към самия рутер, тъй като пакетите, създадени от рутера, не минават през верига prerouting, трябва да поставим маркировка за маршрутизация в output:

```
/ip firewall mangle add chain=output connection-mark=ISP1 action=mark-routing new-routing-mark=ISP1 passthrough=no

/ip firewall mangle add chain=output connection-mark=ISP2 action=mark-routing new-routing-mark=ISP2 passthrough=no
```

Проблеми след шлюза на доставчика

- Приложения механизъм за безотказност работи при загуба на връзка до шлюза на доставчика
- Ако има връзка до шлюза, но има проблем някъде след него – в мрежата на доставчика, създадената до тук конфигурация няма да установи проблема и да насочи трафика през другия доставчик

Решение с рекурсивна маршрутизация

- Ще изберем два адреса в интернет, за които ще дефинираме специфични маршрути през двата доставчика – за всеки от тези адреси ще се използва само единия интернет доставчик
- Ще дефинираме рекурсивна маршрутизация през избраните адреси – в този случай опцията check gateway ще следи не дали има връзка до шлюза, а дали има връзка през съответния доставчик до избрания адрес в интернет

Решение с рекурсивна маршрутизация

/ip route add dst-address=8.8.4.4 gateway=1.1.1.1 check-gateway=ping scope=10

/ip route add dst-address=8.8.8.8 gateway=2.2.2.2 check-gateway=ping scope=10

/ip route set gateway=8.8.4.4 [/ip route find dst-address=0.0.0.0/0 gateway=1.1.1.1]

/ip route set gateway=8.8.8.8 [/ip route find dst-address=0.0.0.0/0 gateway=2.2.2.2]

При отпадане на избраните адреси

- Ако двата избрани адреса в даден момент са недостъпни, ще останем без активен маршрут по подразбиране. За да имаме работеща конфигурация и в този случай, можем да добавим един ECMP маршрут с по-висока цена:

```
/ip route add gateway=1.1.1.1,2.2.2.2 check-gateway=ping distance=10
```

Благодаря за вниманието!

Можете да ме потърсите след презентацията, ако имате въпроси.

Петър Димитров

www.pgnetpro.bg