Mikrotik RouterOS:

Řízení datových toků

Obsah

- Platné verze
- Úvod
- Queues
- Mechanismy omezování
- Rozdíl mezi simple queues a queue tree a případy jejich použití
- Nastavení queue types
- Nastavení simple queues
- Nastavení queue tree

Platné verze

RouterOS verze od verze 2.8. Předchozí verze < 2.8 používaly odlišný systém práce s queues.

Úvod

Ethernet, jak jej známe dnes, nedokáže stoprocentně zajistit kvalitu služeb (QoS). Musíme se proto spoléhat na tzv. best effort, tedy „nejlepší snahu“. RouterOS se s tímto obecným problémem, či spíše vlastností, ethernetu, vypořádává nadmíru dobře a jeho administrátoři dostávají do rukou mocný nástroj pro řízení datového toku, tzv. Queues.

Umožnit kontrolu nad datovými toky procházejícími směrovačem, dnes patří k základní výbavě IP routeru. Čím dál častěji se ovšem setkáváme s implementací řízení toku i do síťových přepínačů, jejichž funkce donedávna nepřesahovala rámec druhé síťové vrstvy. RouterOS můžeme také chápat buď jako směrovač, či bridge. V obou režimech nám totiž umožní řídit datový provoz. Je tedy na Vás, zda-li zvolíte transparentní, či netransparentní řízení datového toku.

Queues

Řízení datového toku v RouterOS řeší submenu queues. To umožňuje ošetřit následující činnost:

- Omezování (popř. upřednostňování) rychlostí jednotlivých IP
- Omezování rychlosti (popř. upřednostňování) jednotlivých protokolů, portů a na nich běžících služeb
- Vytváření sdílených linek
- Řízení provozu P2P systémů (viz Howto RouterOS: Problematika výměnných sítí)
- Vytvářet statistiky o přenesených datech (viz Howto RouterOS: Vizualizace datových toků)

Mechanismy omezování

Mikrotik podporuje několik mechanismů omezování a řízení síťového provozu. Dokument, který si právě čtete, si neklade za cíl překládat originální anglické návody Mikrotik RouterOS, má být pouze vodítkem pro pochopení práce s queues a jejich základní nastavení. Více informací naleznete na www.mikrotik.com/docs2.8/root/queue.simple

- PFIFO (packets first-in first-out) a bfifo (bytes first-in first-out)
- SFQ (stochastic fair queueing)
- RED (random early detection)
- PCQ (per connection queue)
- HTB (hierarchical token bucket)

PFIFO a BFIFO posílá pakety tak, jak je dostane. Obecně se příliš nehodí pro omezování rychlosti, můžou vést k zahlcování linky špičkami. Jejich použití je především v oblasti statistik.

SFQ funguje na principu rovnoměrného přidělování přenosového pásma všem sessions, které jsou otevřené. Obecné doporučení je pro přetížené linky, kdy se tímto způsobem dostane na každého. Nevýhoda tohoto mechanismu je, že přiděluje pásmo jednotlivým sessions, nikoliv počítačům (IP adresám).

RED je zřejmě nejpoužívanějším mechanismem. Dokáže ohleduplně řídit vytížení linky, která díky tomu nechodí na „dorazy“. Statisticky zahazuje pakety, díky čemuž dokáže přinutit jednotlivé toky nevybíhat do špiček. Nicméně má mechanismy (tzv. burst), které umožní jednorázově přenést více paketů (např. pro rychlé načtení webové stránky)

PCQ je protokol, který značným způsobem usnadňuje nastavení většího počtu stejných nesdílených linek. Ve vlastnostech PCQ je třeba nastavit identifikátor rozpoznání jednotlivých uživatelů (většinou cílová adresa). Poté se nastaví jedna queue, která zahrne rozsah IP adres, které chceme omezovat a nemusíme nastavovat pro každou IP adresu vlastní queue.

HTB se používá pro sofistikované řízení provozu, kdy chceme řídit jednotlivé protokoly nebo porty.

Queues jsou aplikovány vždy v případě, kdy paket prochází směrovačem přes dvě různá síťová rozhraní. Queues NEJSOU aplikovány při komunikaci dvou bezdrátových klientů v rámci jednoho AP. RouterOS tuto funkci v současné době nepodporuje. Queues jsou rovněž aplikovány i v případě, kdy RouterOS pracuje v režimu bridge. To nám dává možnost nastavit transparentní shaper, stejně jako firewall bridge.

Rozdíl mezi Simple Queues a Queue Tree a případy jejich použití

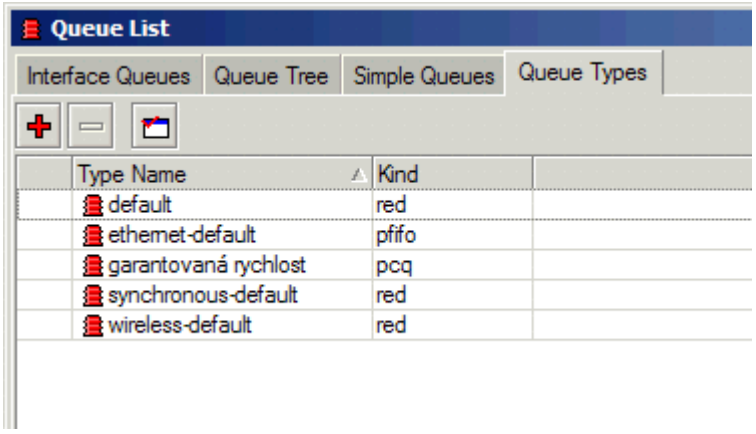
Simple Queues jsou již dle názvu určeny pro základní řízení provozu. Pokud chcete pouze omezovat rychlosti jednotlivým IP adresám, popř. jejich rozsahům (pouze v rámci subnetů sítě, tzn. IP adresy musí být vedle sebe), je ideální použít Simple Queues.

Queue Tree slouží pro sofistikované řízení toků. Pokud chcete vytvářet sdílené linky, upřednostňovat jednotlivé protokoly nebo služby běžící na určitých portech, budete muset použít Queue Tree. Jejich nevýhoda je v určité složitosti konfigurace.

Simple Queue a Queue Tree mohou být zkombinovány pro vzájemný provoz vedle sebe. Je však nutné mít na paměti, že vzájemnou kooperaci je vhodné vyzkoušet. V praxi platí, že se aplikuje přísnější pravidlo (pokud se pravidla překrývají).

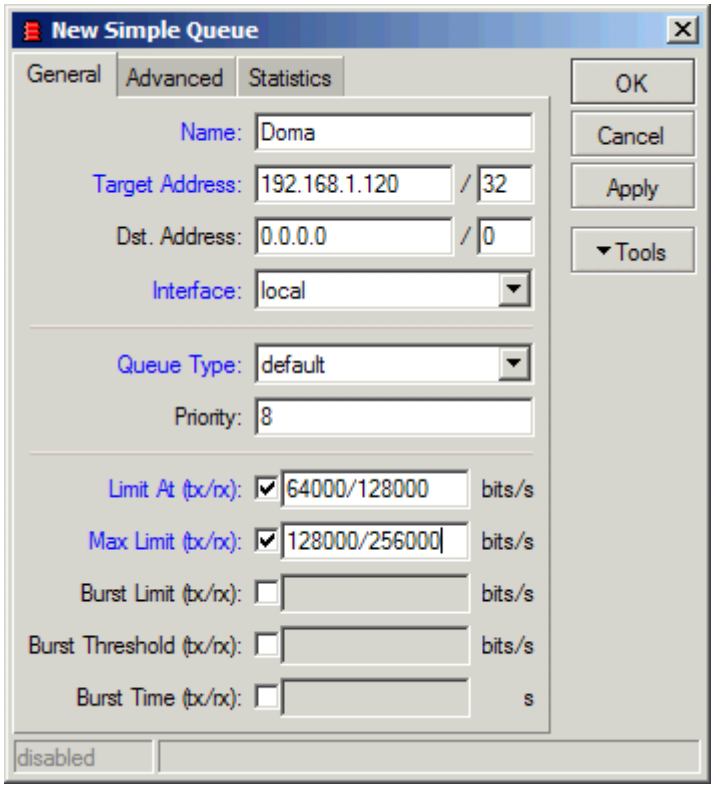
Nastavení Queue Types

V této záložce si můžete nastavit mechanismy, které budete používat v pravidlech Queues. Defaultně jsou zde nastavené čtyři typy, které můžete měnit, popř. můžete přidat své vlastní. Defaultní hodnoty jednotlivých mechanismů jsou ve většině případů vyhovující.



Nastavení Simple Queues

Po kliknutí Přidat se vám zobrazí okno se třemi záložkami, `General`, `Advanced` a `Statistics`:



Name – název Queue

Target Address – IP adresa zařízení, jehož provoz má být omezen, POZOR, musí být uvedena správně maska sítě (pro jednu IP adresu maska 32)

Dst. Address – Cílová adresa pro Queue, můžete omezovat provoz buď globálně (0.0.0.0/0), nebo k jednotlivým zařízením v síti

Interface – Rozhraní, kterým komunikace opouští směrovač. V případě Simple Queues by to mělo být rozhraní, kam je připojeno omezované zařízení. V případě použití rozhraní spojených do bridge je lepší použít nastavení All

Queue Type – mechanismus omezování

Priority – priorita v udělování volného pásma. Priorita u Simple queues označuje prioritu v rozdělování volného pásma pro Max Limit! Dokud nejsou uspokojeny požadavky všech Queues v rámci Limit At, jsou si všechny Queues rovny. V Queue Tree se Priority chová jinak (viz Nastavení Queue Tree).

Limit At (tx/rx) – garantovaná rychlost ve tvaru upload/download

Max Limit (tx/rx) – maximální rychlost ve tvaru upload/download

Tyto nastavení stačí pro správné fungování Simple Queues. Ostatní nastavení mohou mít pouze vliv na chování burst režimu. Mechanismus RED má metodu BURST integrovanou již v sobě.

Na záložce Advanced můžete definovat celkové hodnoty parametrů Queue (upload i download dohromady)

Na záložce Statistics vidíte aktuální rychlost a přenesené byty/pakety.

Simple queues jsou zpracovávány v pořadí, v jakém jsou zadány. Můžete tedy nejdříve zadat pravidla pro jednotlivé IP a na konec zadat globální pravidlo pro celou síť, kterým omezíte provoz všem ostatním IP adresám.

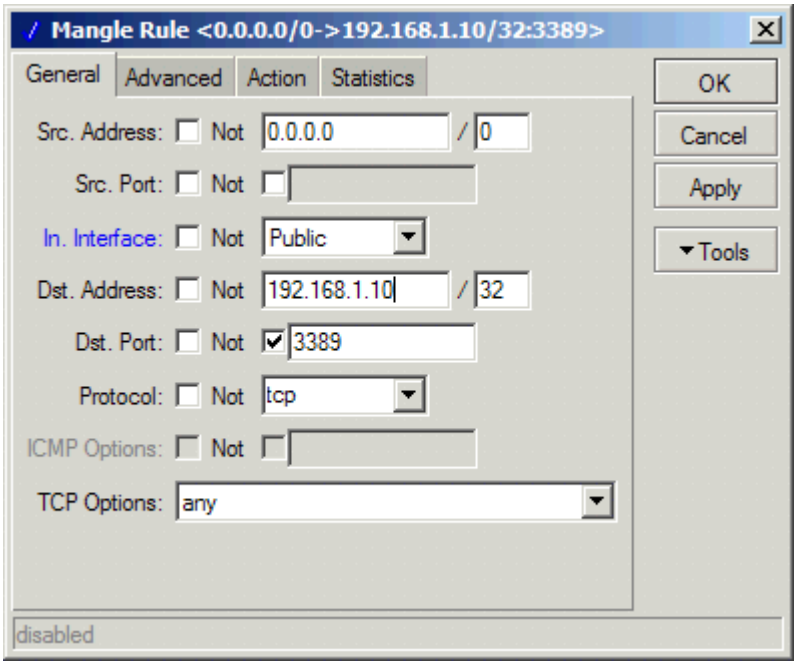
Nastavení Queue Tree

Queue Tree používají ve verzi 2.8.x protokol HTB. Pro bližší informace o tomto mechanismu najdete na http://luxik.cdi.cz/~devik/qos/htb/ (v angličtině)

Pro použití Queue Tree musíte nejprve označit požadované pakety, které chcete řídit. Značkování paketů se provádí v /ip firewall mangle. Mikrotik RouterOS disponuje širokými možnostmi označování paketů. Pro řízení datového toku musíte zadat vždy dvojici pravidel, jedno pro upload a jedno pro download. Pokud označujete pakety v překládané síti (NAT), je nutné použít tři pravidla, viz níže. V Queue Tree můžete posléze tyto označené pakety řídit.

Označkování paketů:

Na kartě General se nastavují základní podmínky výběru paketů, v následujícím příkladu vidíte označení paketů, které přichází na IP adresu 192.168.1.10, port 3389 (Microsoft Terminal Services), pokud chcete označit veškerý provoz, do položky Protocol uveďte „all“:



`Src. Address` – zdrojová IP adresa

`Src. Port` – zdrojový port. Abyste mohli definovat porty, musíte mít zvolený `Protocol` tcp

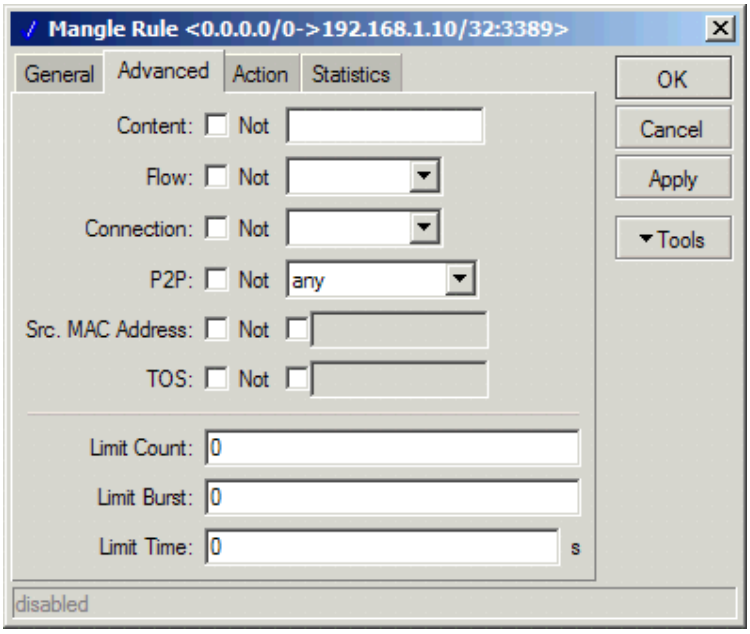
`In. Interface` – rozhraní, kterým paket vstupuje do směrovače

`Dst. Address` – cílová adresa

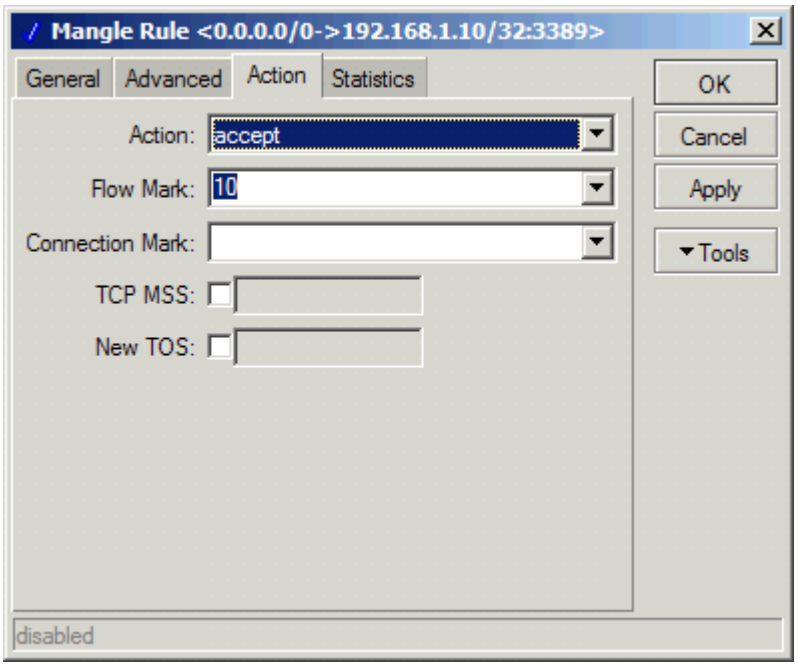
`Dst. Port` – cílový port

`Protocol` – protokol, jehož pakety mají být označovány

Na kartě `Advanced` můžete nastavit pokročilé podmínky pro výběr paketů, např. podle obsahu paketů, zdrojové MAC adresy, omezení platnosti pravidla na počet bytů/paketů popř. čas. Je zde také možnost značkovat pakety provozu výměnných (p2p) sítí.



Na kartě `Action` nastavíte akci, která se má provést v případě, že paket vyhoví zadaným podmínkám



`Action` – typ akce, accept a passthrough. Nastavení `Action` se v případě manglingu chová jinak než ve standardních pravidlech firewallu. Pravidla jsou prováděna v pořadí jak jsou zadána. Pokud má `Action` hodnotu accept, pak se pravidlo aplikuje a další pravidla se již neprovádí. Pokud má hodnotu passthrough, je pravidlo provedeno a systém zkouší další pravidla.

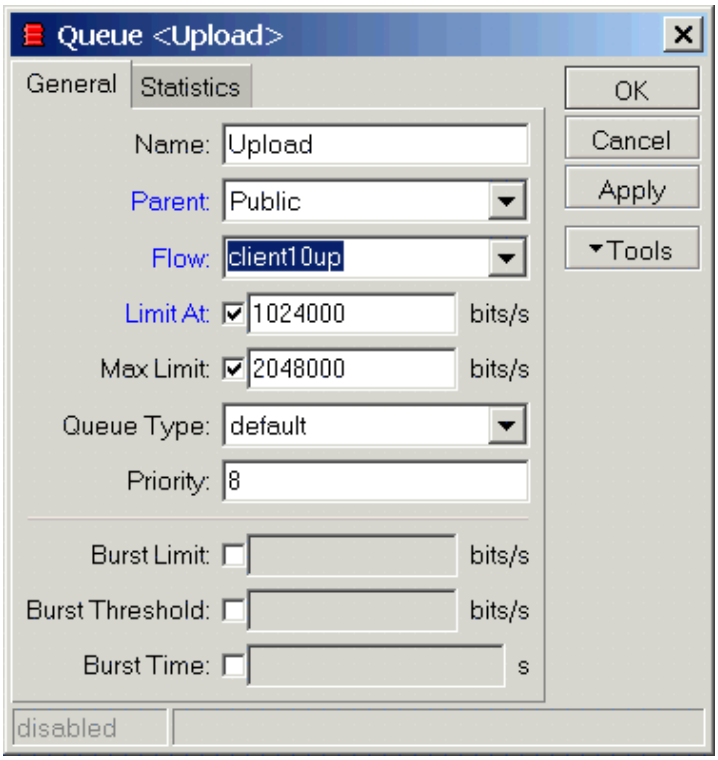
`Flow Mark` – řetězec, kterým je paket označen, pokud vyhoví podmínkám, na základě tohoto řetězce je aplikována Queue Tree

`Connection Mark` – označení paketu pro další práci ve značkovacím procesu, nelze použít přímo v Queue Tree, musí být zkombinováno s druhým pravidlem, který přidá `Flow Mark`, používá se např. pro značkování provozu v síti s překladem adres (NAT)

Pokud chcete označovat provoz v překládané síti (NAT), musíte použít trojici pravidel na každou IP adresu (musí být dodrženo pořadí pravidel):

```
/ ip firewall mangle
add src-address=192.168.1.10/32 action=passthrough mark-connection=client10 \
    comment="Nat IP mark connection" disabled=no
add src-address=192.168.1.10/32 action=accept mark-flow=client10up \
    comment="NAT IP upload" disabled=no
add connection=client10 action=accept mark-flow=client10down \
    comment="NAT IP download" disabled=no
```

Po označení paketů je můžeme řídit v Queue Tree. Po kliknutí Přidat se vám zobrazí okno se dvěma záložkami, `General` a `Statistics`:



`Name` – název Queue

`Parent` – Nadřazená Queue, může být buď jiná Queue, rozhraní, nebo jedno ze dvou virtuálních rozhraní: global-out (zahrnuje všechny odchozí rozhraní) a global-in (příchozí rozhraní)

`Flow` – `Flow mark`, kterým byl paket označen v mangle

`Limit At (tx/rx)` – garantovaná rychlost ve tvaru upload/download

`Max Limit (tx/rx)` – maximální rychlost ve tvaru upload/download

`Queue Type` – mechanismus omezování

`Priority` – priorita v udělování volného pásma. V Queue Tree Priority určuje prioritu získání pásma pro limit-at. Tím získá přednost před ostatními toky.

Ostatní nastavení mají vliv na chování burst režimu. Mechanismus RED má metodu BURST integrovanou již v sobě.

Na záložce `Statistics` vidíte aktuální rychlost a přenesené byty/pakety.

S Queue Tree přichází velká variabilita řízení síťového provozu a není možné uvést všechny případy konfigurací, které mohou nastat. V tomto how-to jste se dozvěděli základní informace o řízení síťového provozu pomocí Mikrotik RouterOS. Pokud budete mít nějaké dotazy o nastavení Queues, obraťte se na pracovníky technické podpory, kteří Vám rádi pomohou s konkrétní konfigurací.