Alternativy ladění sítě

Václav Nesvadba
Faster_3.0

použité technologie

pokročilé
- juniper ...

jednoduché
- mikrotik ...

otevřený HW
- whitebox + (cumulus)linux + BIRD ...

vlastní HW
- unipi.technology PLC/IoT

open source
- linux, freebsd, openvswitch ...

šetřit adresy

BE FASTER.CZ

peering

```
a.b.c.d/30 :(     a.b.c.d/31      a.b.c.d peer e.f.g.h
```

mikrotik

```
ADDRESS             NETWORK          INTERFACE
10.20.188.169/32    10.20.188.168    combo1
```

linux

```
ip ad add 172.30.1.1 peer 172.30.1.128/29 dev swp1
echo 1 >  /proc/sys/net/ipv4/conf/swp1/proxy_arp
ip ro fl type  broadcast dev swp1 src \
 172.30.1.1  table local
# Nezkoušet na IPv6 !
```

šetřit zdroje

BE FASTER.CZ

ochrana proti útokům na neighbor cache (4096)
menší routing table

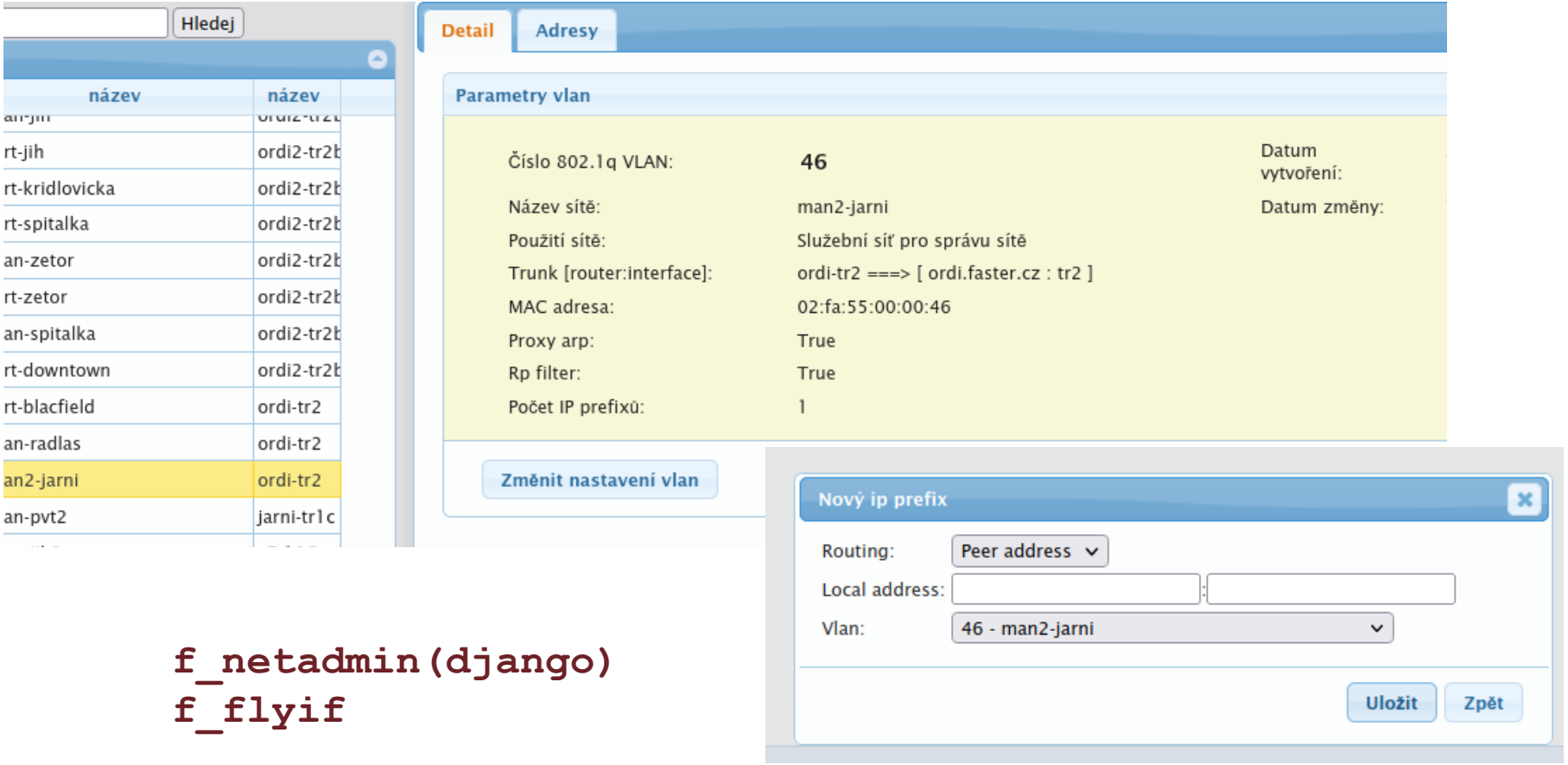
router IP
    default 2a02:e98:10:5410::1/120 (16 subnets)
    up to   /116 (256 subnets)

subnety
   zak-A 2a02:e98:10:5410::20/124
          (použít adresy 22 ... 2e/64 pro stěhování)
   zak-B 2a02:e98:10:5410::30/124
          (routovat net /60+ via ::32)

peering
                185.146.4.112/31
             2a02:e98:1:4::112/127

efektivní rekonfigurace

BE FASTER.CZ



f_netadmin(django)
f_flyif

efektivní rekonfigurace

BE FASTER.CZ

ansible + f_modules(bird,juniper,switch,firewall...)

```
- name: swp50
  descr: "downlink xx101 40G-1/0/3"
  type: trunk
  options: ["mtu 9000","link-autoneg on" ]..
  units:
   - id: 2384
     descr: "peer xx3"
     addr: [  "55.66.5.105/31","2a12:e88:1:5::105/127" ]

   - id: 2381
     descr: "downlink to zzz+yyy"
     addr: [  "55.66.8.235/32" ]
     options: [ "mtu 1500" ]
```

```
# ---- NIX  -----
- name: NIX5v6
  ip: 2001:7f8:14::11
  ip2: 2001:7f8:14::12
  as: "47200"
  local_as: "{{faster_as}}"
  no_bfd: true
  med: 66

  options:
    - "import rpki"
    - "import from-ebgp"
    - "export to-ebgp"
    - "remove-private all"
```

ifupdown2

zvýšit dostupnost - VRRP

BE FASTER.CZ

keepalived

```
/etc/keepalived/keepalived.conf
  vrrp_instance swp1 {
  notify notify-broifc.sh
  interface swp1.1234
  state BACKUP
  virtual_router_id 106
  priority 100
      authentication {
      ...
      } }
```

```
---- status ----
admin@rc6xx:mgmt:~# vrrp-show
/var/run/vrrp.pid:3811
/var/run/vrrp.swp1:MASTER
/var/run/vrrp.swp5:BACKUP
/var/run/vrrp.swp51:BACKUP
/var/run/vrrp.swp53:BACKUP
```

f_cl-ifc

```
swp1.1024 UP,LOWER_UP 172.16.8.1:172.16.8.176/29 10.168.128.17:10.168.128.9/32
2a02:e98:0:5001::1/64
swp1.1025 UP,LOWER_UP 192.168.229.209/28 192.168.228.57/29
swp1.1026 UP,LOWER_UP 192.168.244.209/29 192.168.244.169/29 192.168.229.249/29
192.168.244.233/29
swp5.1027 UP,LOWER_UP 192.168.229.65/28
```

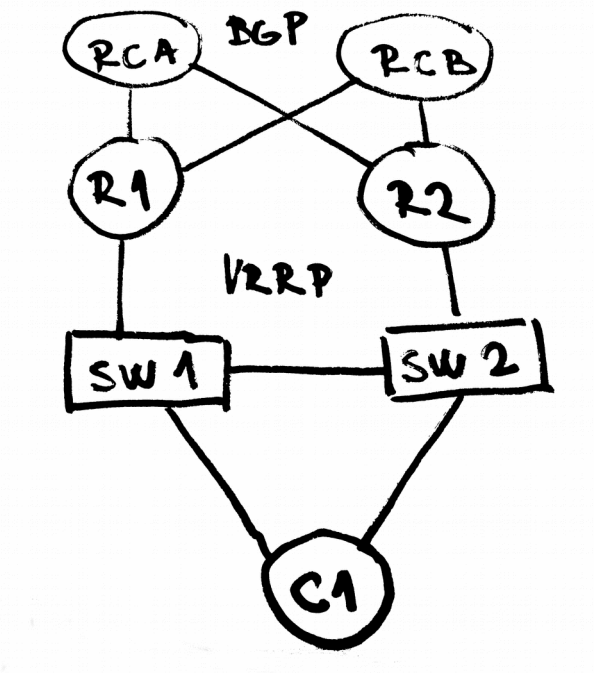
zvýšit dostupnost - VRRP

BE FASTER.CZ

f_brother + f_flyif

/etc/keepalived/brother-hosts.conf
  10.11.7.235 swp51
  10.11.7.237 swp53 swp5

```
 --- log -----
flyif[4721] request  cmd: -r swp5 MASTER
flyif[4721] runnin vrrp_ON cmd: -r swp5 MASTER
flyif[4721]   IFC: swp1 vrrp_ON cmd: -r swp5 MASTER
flyif[4721]   IFC: swp5 vrrp_ON cmd: -r swp5 MASTER
flyif[6125] request  cmd: -r swp5 BACKUP
flyif[6125] waitin  cmd: -r swp5 BACKUP
flyif[4721] finished vrrp_ON cmd: -r swp5 MASTER
flyif[6125] runnin vrrp_ON cmd: -r swp5 BACKUP
flyif[6125]   IFC: swp1 vrrp_ON cmd: -r swp5 BACKUP
flyif[6125] finished vrrp_ON cmd: -r swp5 BACKUP
```



zvýšit dostupnost - VRRP+BGP

BE FASTER.CZ

f_ifwatch

```
ifwatch interface_name  minimum_packet_count watch_time
```

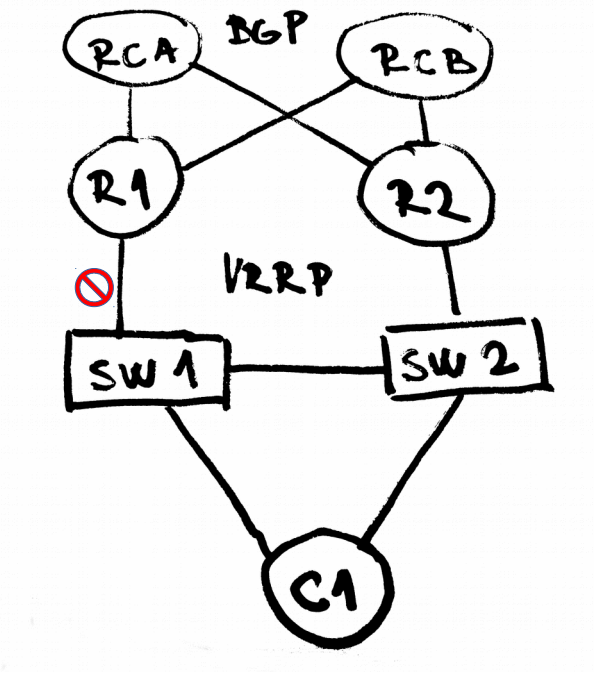
bird R1

/etc/bird/peers/rca.ibgp

```
  ...
  export filter { # to upstreams
     ...
      if ifname ~ "swp1.*" then  {
        include "/etc/bird/prepend.live.swp1";
        }
      if ifname ~ "swp5.*" then  {
        include "/etc/bird/prepend.live.swp5";
        }
     ...
    };
```

/etc/bird/prepend.live.swp5

```
  bgp_prepend(myas);
```



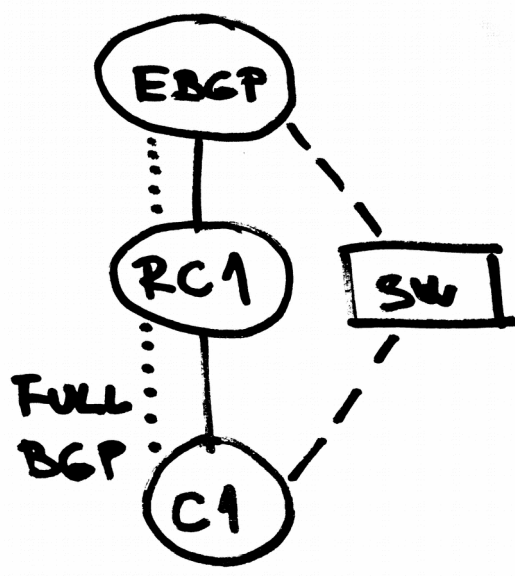
zvýšit dostupnost – FULL BGP

BE FASTER.CZ

bird RC1

2x fullbgp table IPv4+IPv6 < 500MB

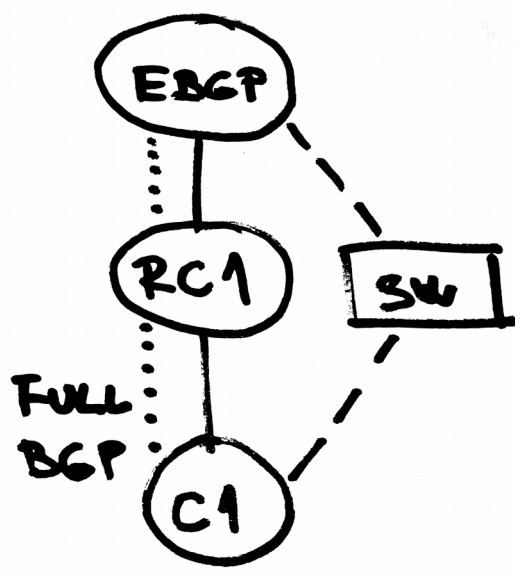
```
/etc/bird/peers/zakaznici.bgp
  protocol bgp c1_a { # peer C1
   table fullbgp;
   import limit 1100000 action block;# upstream
   ...
   import filter {
    # custom
    bgp_community = add(bgp_community,(24641,65199));
      if net = 22.33.98.0/24  then
         bgp_community = add(bgp_community,(24641,2001));
       bgp_accept([55.66.188.48/28,22.33.98.0/24]);
       bgp_reject(ALL);
      };
   ...
   };
```



zvýšit dostupnost – FULL BGP

BE FASTER.CZ

bird RC1




```
/etc/bird/peers/fullbgp.table
  # vymena rout mezi VRF
  table fullbgp;


  protocol pipe fullbgp_pipe {
      peer table fullbgp;

      # export filtruje z main do peer
      export filter {
          reject;
      };

      # import filtruje z peer do main
      import filter {
       if  bgp_community  ~[(24641,65199)] then accept ; else  reject;
      };
  }
```

zvýšit dostupnost - more ...

BE FASTER.CZ

výpadek konektivity upstreamu a defaultgw se pořád propaguje?
  bird: if (fullbgp route count > X) = propaguji defaultgw

problémy s větším počtem RTBH do některých upstreamů
  f_magnet: advertise /24 do lepšího upstreamu + RTBH

interní statistika bajty/pakety/toky, nárust > 250% = DDoS
  f_rtbh_api: automaticky RTBH + ovládání přes dohled

open source HW

Q&A

venca@faster.cz