hanáčkéonet

High availability network services using MikroTik RouterOS

by Martin Pína

MUM Poland, Warsaw, 16th March, 2012

High Availability

- things have to work
- budget is limited
- need to keep setups simple

How to achieve it?

- primary/secondary server
  (DNS, NTP, RADIUS)
- cluster
- use underlying protocols to do the work
  DHCP – broadcast

  VRRP – special protocol

  anycast (?)

Dark side

- usage of secondary option usually means some timeout
- what is not offered by default (primary/secondary) has to be done by somebody, it is expensive (extra hardware, extra software, administrators' time)
- there is no cluster solution for everything

Anycast is the (interesting) way

- easy to setup
- scalable
- secure

Easy to setup

- puts main burden on underlying network layer
- does not differentiate between L7 protocols
- is not as complicated as cluster
- in effect, you will use the same configuration for clients network-wide

Scalable

- routing usually done to provide service from the “nearest“ server, small latency, low load
- you can have your services distributed geographically
- you can use more platforms for the same purpose
- if one server fails, not a problem, there is another one ready
- if there is really problem, it only affects “near“ clients

Secure

- if server gets compromised, just turn it of, there is enough of its clones
- if DDoS is made to your service, it has only local impact
- you can create fake server as honeypot for attacks

Is it so perfect? Of course not.

- there is not much intelligence, having working L3, does not mean there is L7 service running
- it is usable maily for the simple tasks like DNS/NTP/RADIUS, the client does not care where the information is from, but administrator has to take care
- even if you want dedicated virtual servers using MikroTik's KVM, RouterOS is 32bit system, 2GB of RAM maximum

Is it new approach? Not at all

- anycast is not something that much special itself, only special usage of unicast
- IPv6
- already used worldwide (?)

Root nameservers example

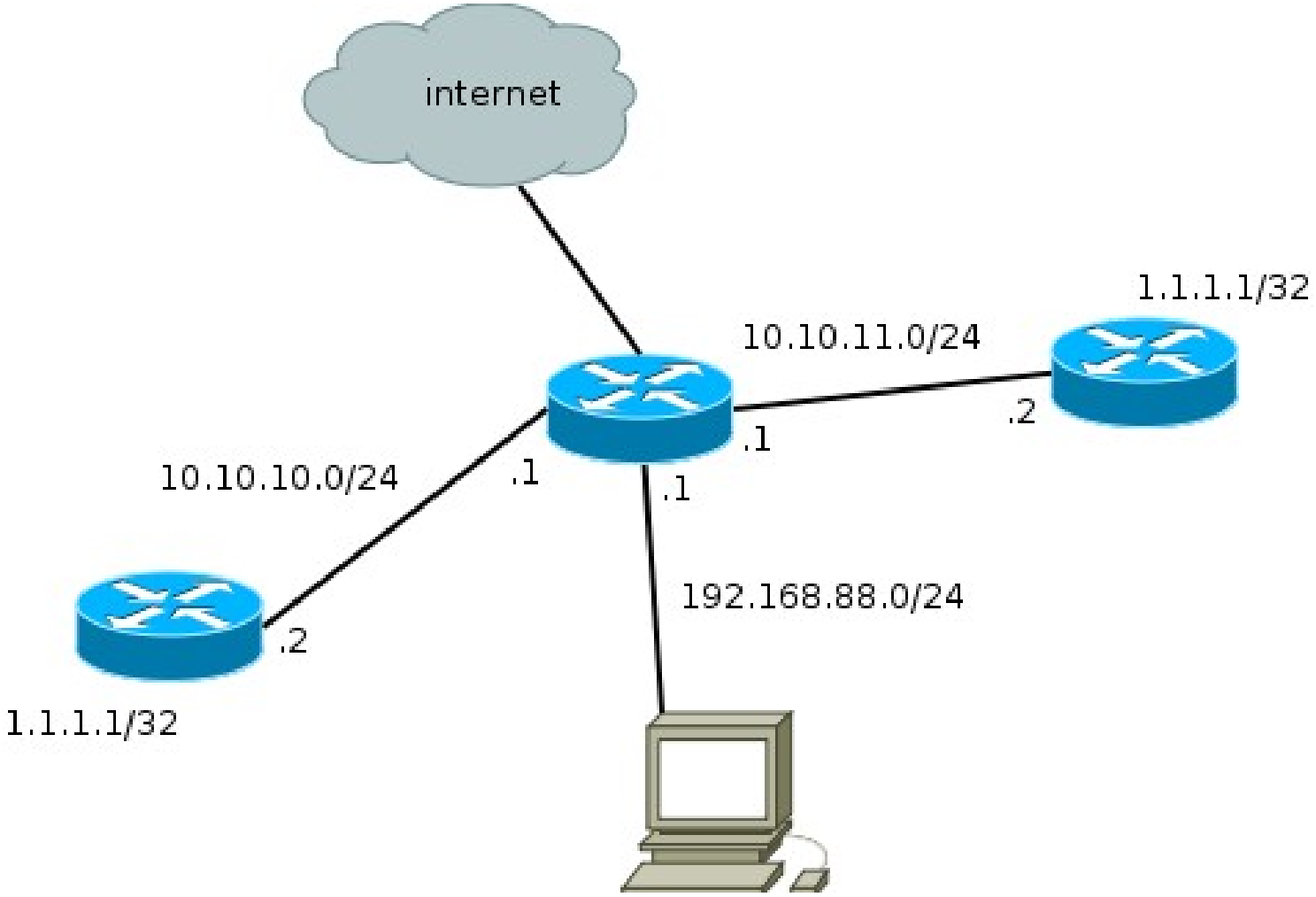
Why RouterOS?

- it is a router, who else should take care of where to send the requests
- it already has the mostly crucial server functionality like DNS or NTP
- if the inbuild servers are not enough, there is always MetaROUTER or KVM available for endless possibilities

Example study case

- it is only about routing, no special package, no special configuration menu
- dynamic routing is done by OSPF
- it is the most easiest way, no special hardware, no virtualization
- DNS is the network service

Topology


internet
1.1.1.1/32
10.10.11.0/24
.2
.1
10.10.10.0/24
.1
.1
192.168.88.0/24
.2
1.1.1.1/32

3 possible scenarios

- network service in router itself, only special loopback bridge interface created for the anycast address
- virtual RouterOS created in MetaROUTER or KVM to do the network service server and nothing else, or possibly special Linux/Windows one-purpose server installed in KVM (Linux in MetaRouter)
- network service servers are not hosted by MikroTik RouterOS, but routers redistribute routing information about them

Recommendations

- segregate network and services
  - either via virtualization
  - or via physical segregation
- do have management IP address for network service server to be able to easily turn-on/off the anycast address
- use this technique sensibly
- be careful about ECMP

Troubleshooting

- good understanding of routing solves everything
- traceroute is your friend

Resources

- http://en.wikipedia.org/wiki/Anycast
- http://www.root-servers.org/
- www.sanog.org/resources/sanog5-woody-anycast-v10.pdf

Thanks for your attention (patience)

- Questions... ?

hanácké.net®