



Akademie

DNS anycast

Zbyněk Michl
<*zbynek.michl@nic.cz*>

Ondřej Surý
<*ondrej.sury@nic.cz*>

10. února 2011

CZ...
nic :

Co je to anycast?

- Směrování jeden zdroj → více cílů
- Více (všechny) cíle propagují stejný IP rozsah
- Vždy je vybrán nejbližší server
 - Nikoli geograficky
 - Potencionálně pro každý paket jiný
- Nejlepší pro nestavové protokoly (UDP)
 - Při stabilním směrování lze použít i TCP



Proč použít anycast?

- Zvýšená spolehlivost
 - Jednoduchý load balancing
 - Pomalá konvergence
 - Snížení síťové latence
 - Zvýšená odolnost pro DoS a DDoS
 - Zátěž je distribuována
- Ideální aplikace pro DNS (UDP zprávy)



Útoky na root servery

- Březen 2007
- 6 kořenových serverů pod masivním DDoS
- Nejhorší byly postiženy unicast servery



Implementace anycastu

- Nezávisí na směrovacím protokolu
 - Nejčastěji BGP
 - Teoreticky i jiné protokoly, ale ty se v core internetu nepoužívají
- Je zapotřebí PI rozsah (/24)
 - Ze speciálního rozsahu kvůli filtrování
- DNS server musí umět BGP (bird, quagga, openbgpd)
 - nebo směrovač před ním



RIPE anycast policy

- 2006 – 2009
 - Pouze jeden /24 prefix
- Červen 2009 – nyní
 - CZ.NIC společně s Nominetem zahájil změnu policy
 - CZ.NIC – max 4 prefixy
 - Nominet – prefixy i pro ENUM operátory
 - 4x IPv4 /24 a 4x IPv6 /48 rozsahy

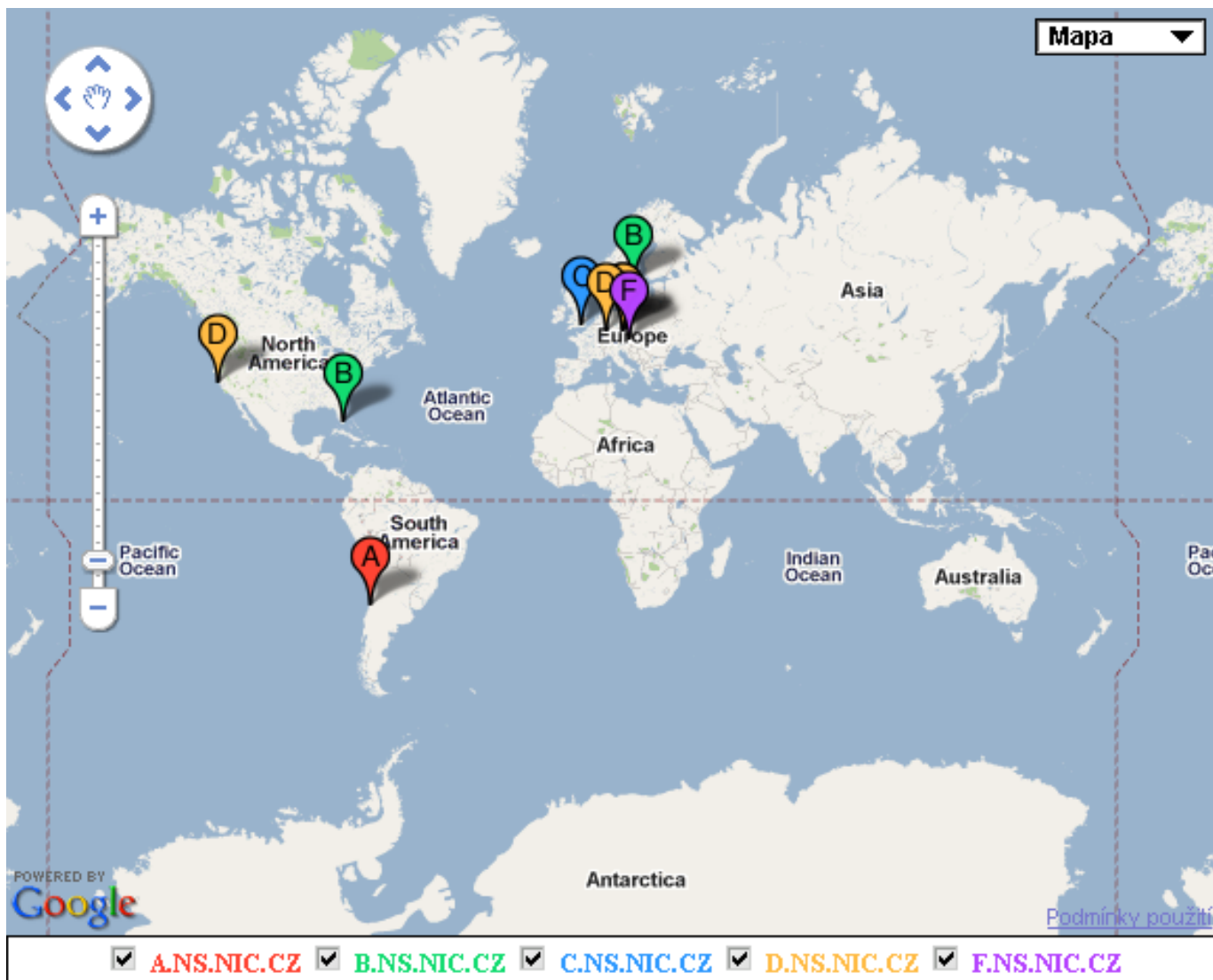


.CZ DNS

- 6 nameserverů (a-f.ns.nic.cz) → 4 (a-d)
- 1 unicast
 - f: Vídeň
- 4 anycast
 - a: Praha, Santiago
 - b: Miami, Stockholm
 - c: Londýn
 - d: Praha, Frankfurt, Redwood City



.CZ DNS



AS112

- AS112 – speciální autonomní systém (BGP)
- Černá díra pro:
 - PTR dotazy na privátní adresy (RFC1918)
 - Jinou nevalidní komunikaci na root servery
- Od roku 2004 přítomno v NIX.CZ



Jiné použití

- Rozložení zátěže rekurzivních serverů
 - Vhodné pro větší ISP
 - Více serverů v síti ISP, směrování např. OSPF
 - BGP má pro tyto účely pomalou konvergenci
 - Alternativa místo load-balancerů

