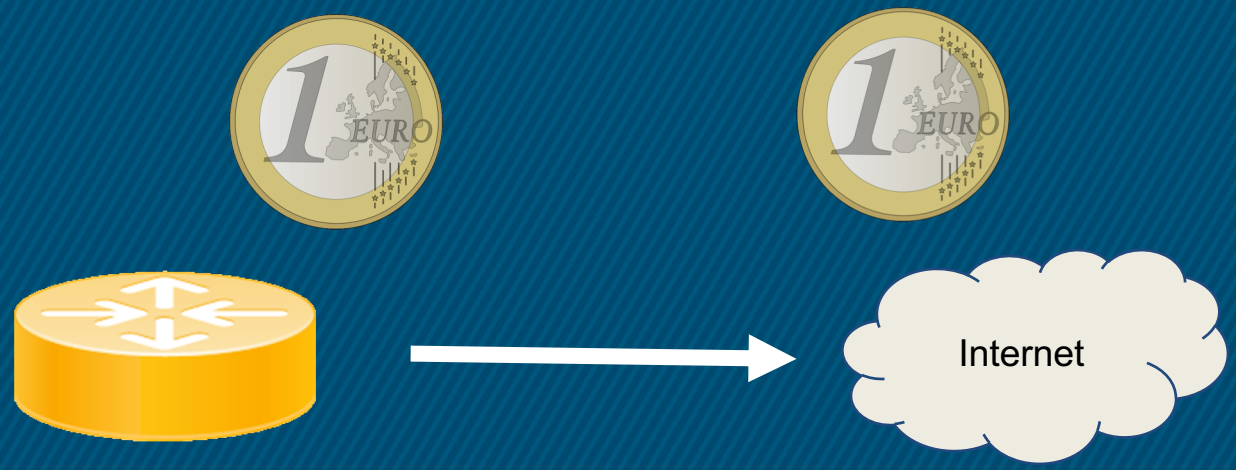
Bezpečnost peeringu

Marian Rychtecký - NIX.CZ
mr@nix.cz / @MarianRychtecky

NIX·CZ

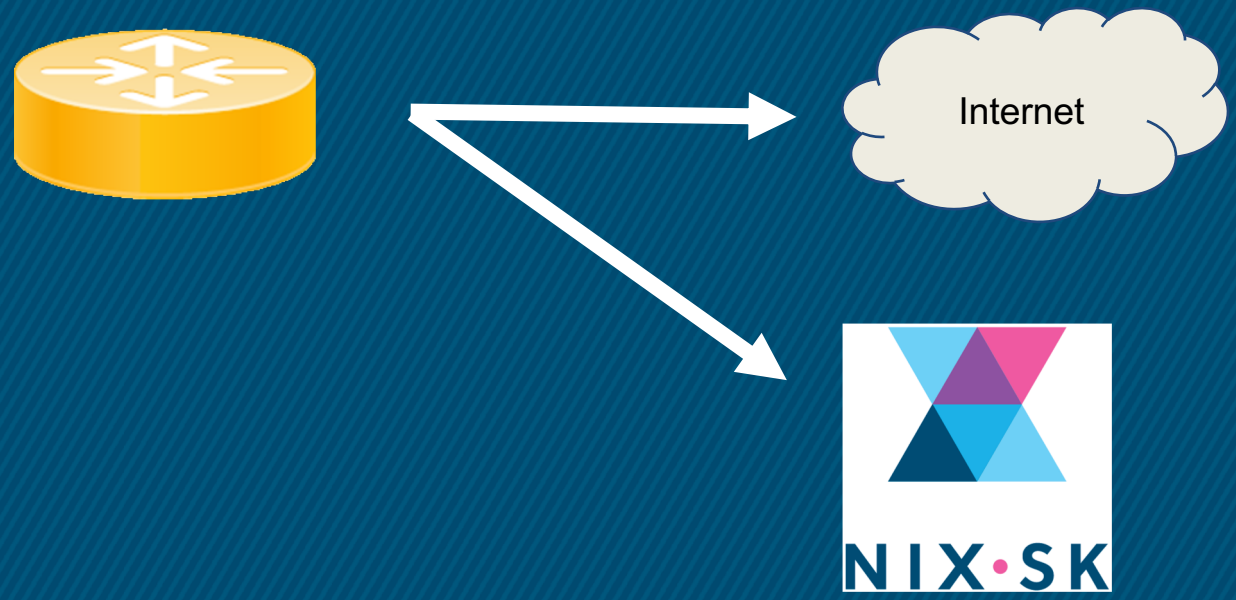
Co je “peering”

Propojování sítí



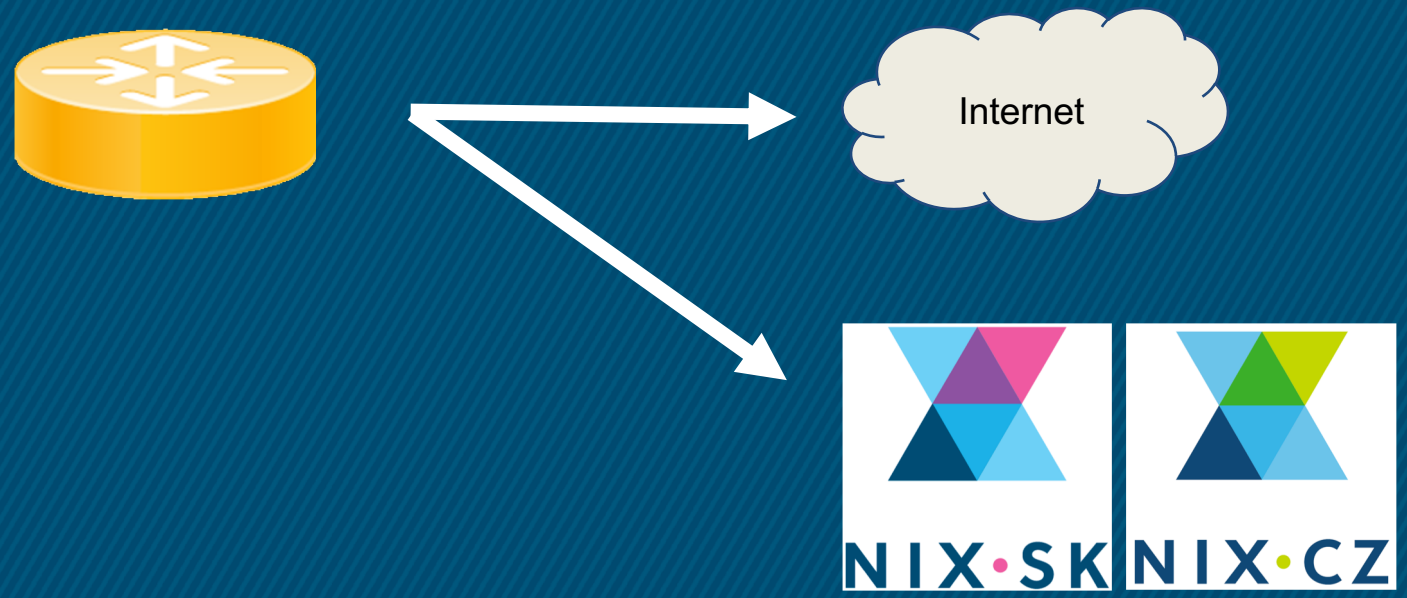
Co je “peering”

Propojování sítí



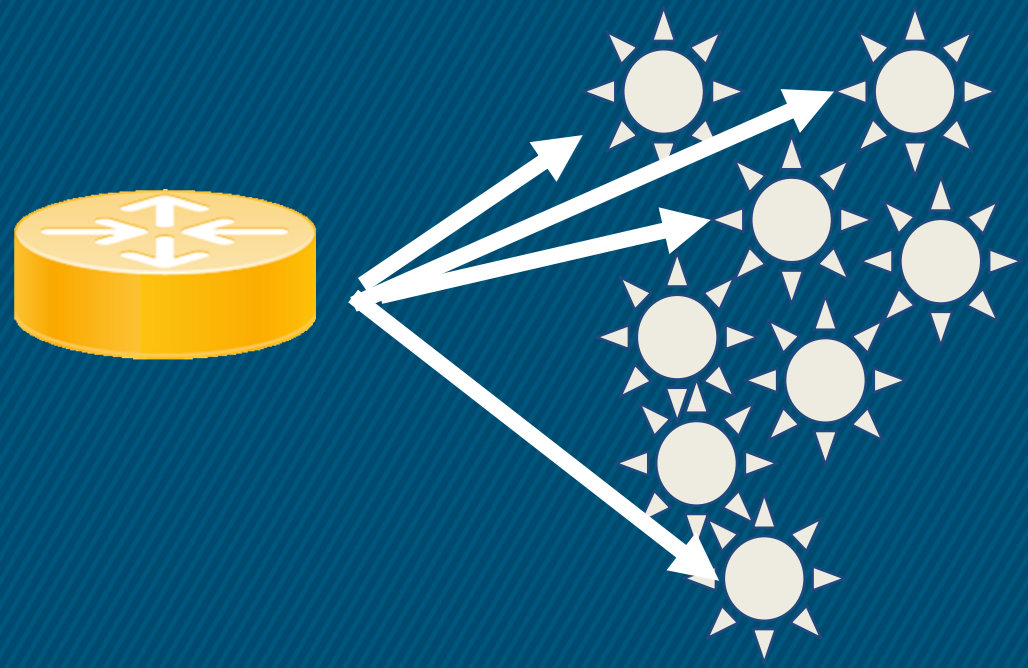
Co je “peering”

Propojování sítí



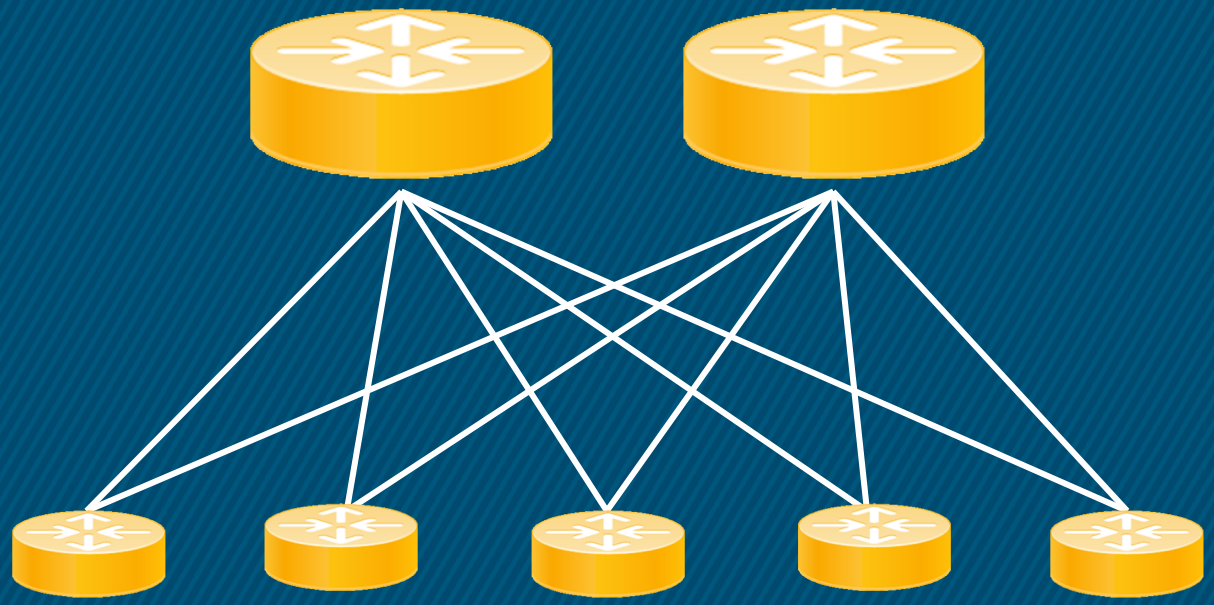
Co je “peering”

Propojování sítí - přímý peering



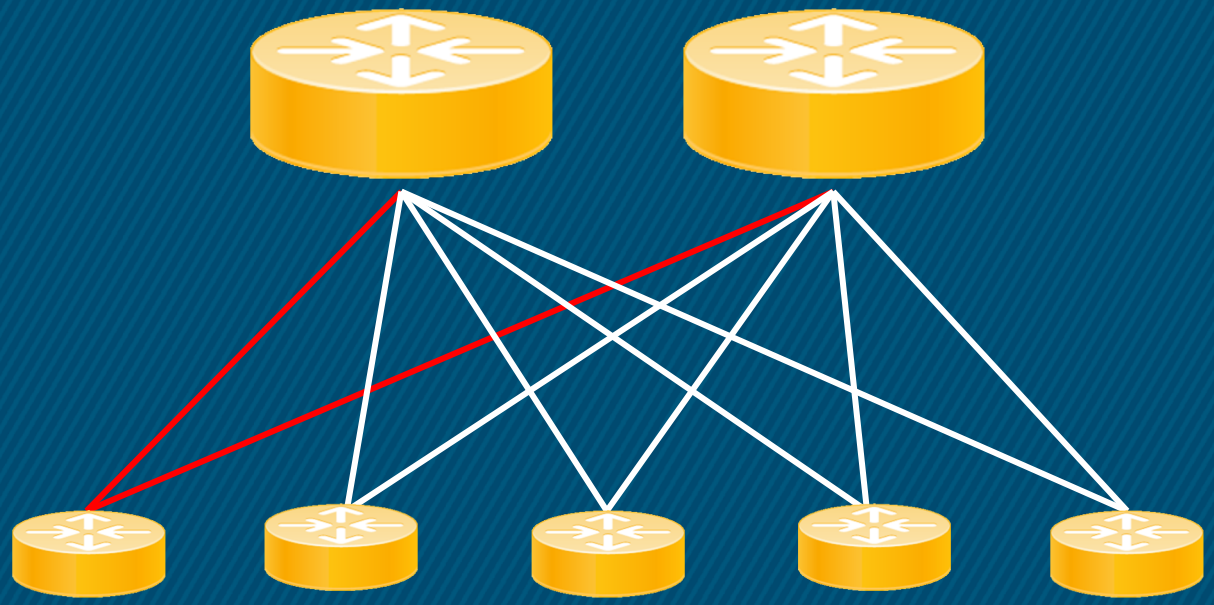
Co je “peering”

Propojování sítí - route servery



Co je “peering”

Propojování sítí - route servery



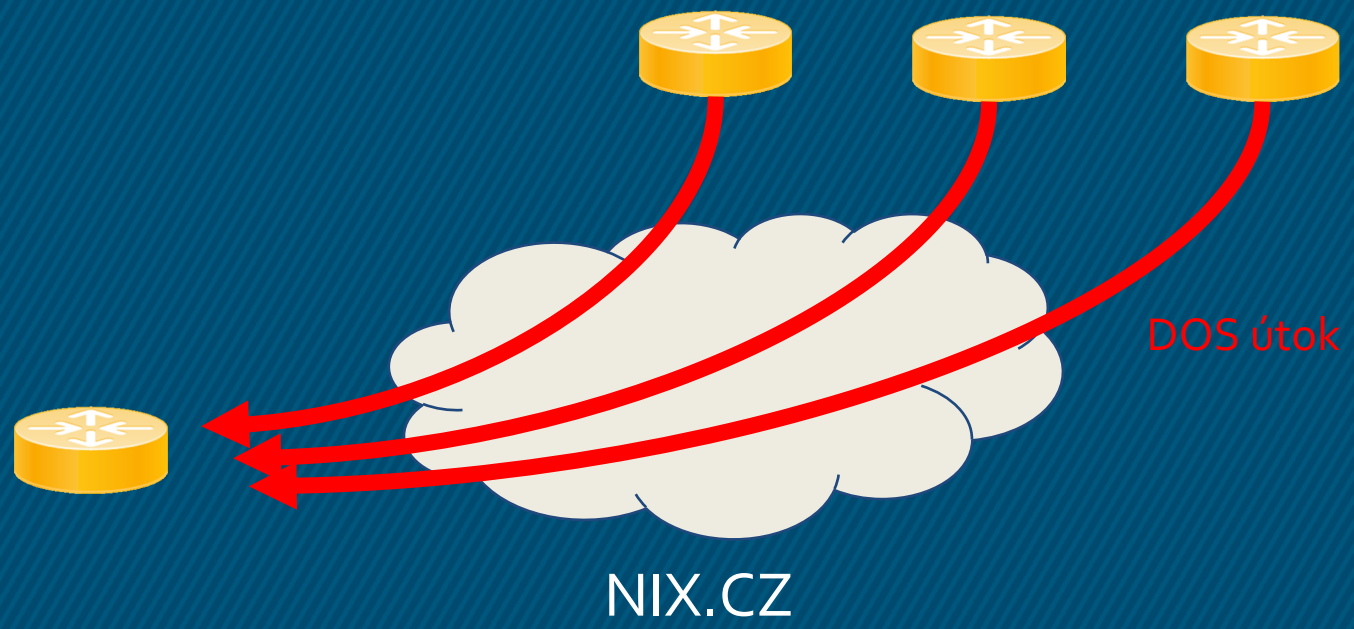
Co je “peering”

Propojování sítí - route servery

1. Odfiltrovat malé prefixy (default je >/24 pro IPv4 a > /48 pro IPv6), jež neobsahují RTBH nebo DDOS
2. Odfiltrovat martians/bogons (*) prefixes
3. Odfiltrovat prefixy, které nemají alespoň 1 ASN a mají více než 64 ASN v cestě
4. Odfiltrovat prefixy, které nemají stejné ASN peeru a prvního hopu v cestě
5. Odfiltrovat prefixy, které nemají shodnou IP adresu next-hop a peer IP (next-hop hijacking)
6. Odfiltrovat prefixy známých Tier1 ASN (**)
7. Odfiltrovat prefixy, které nemají zdrojové ASN mezi AS daného AS-SETu
8. RPKI
    1. Validní - akceptovat
    2. Invalidní - zahodit
9. RPKI unknown - procesovat dále podle seznamu AS-SETů a IRRDB

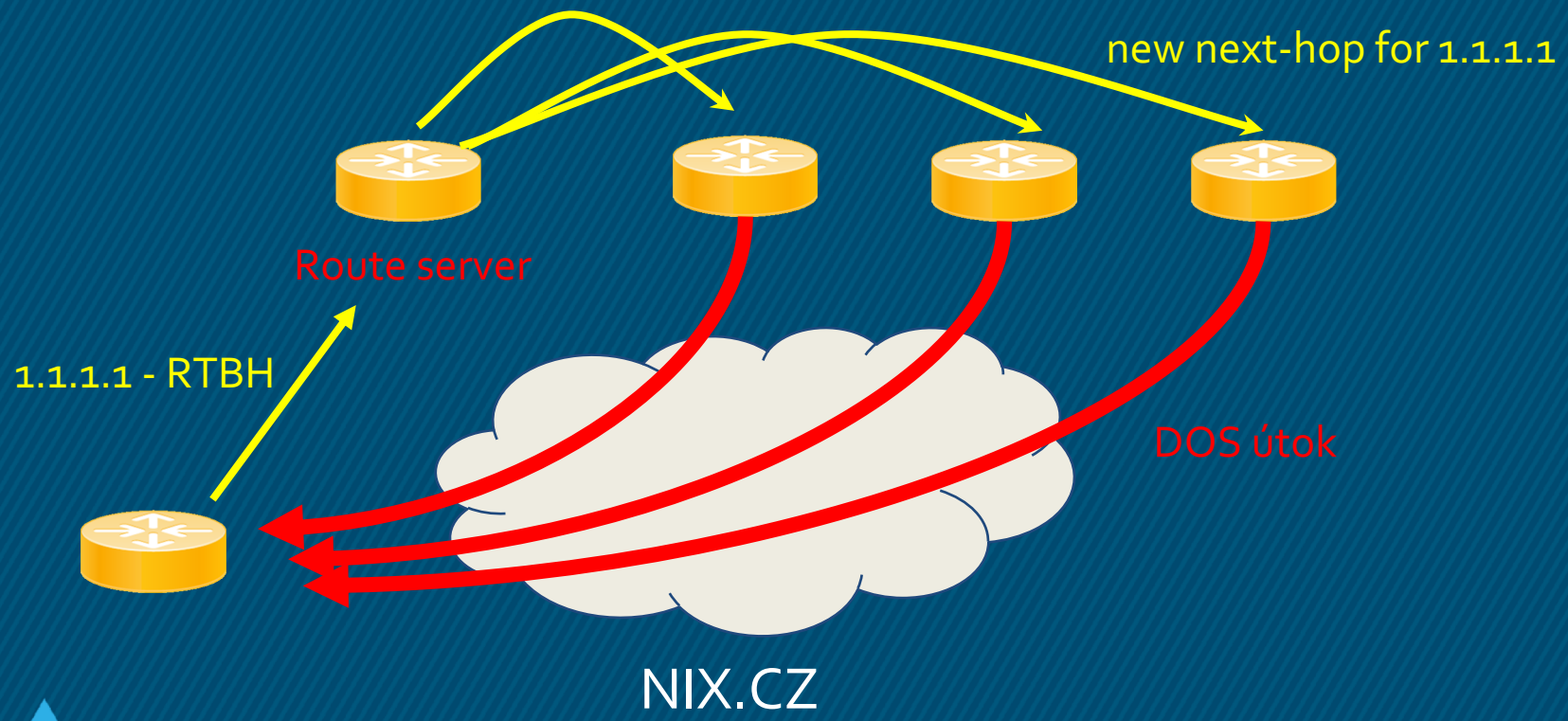
Routing policy

Propojování sítí -
RTBH (Remotely Triggered Black Hole)



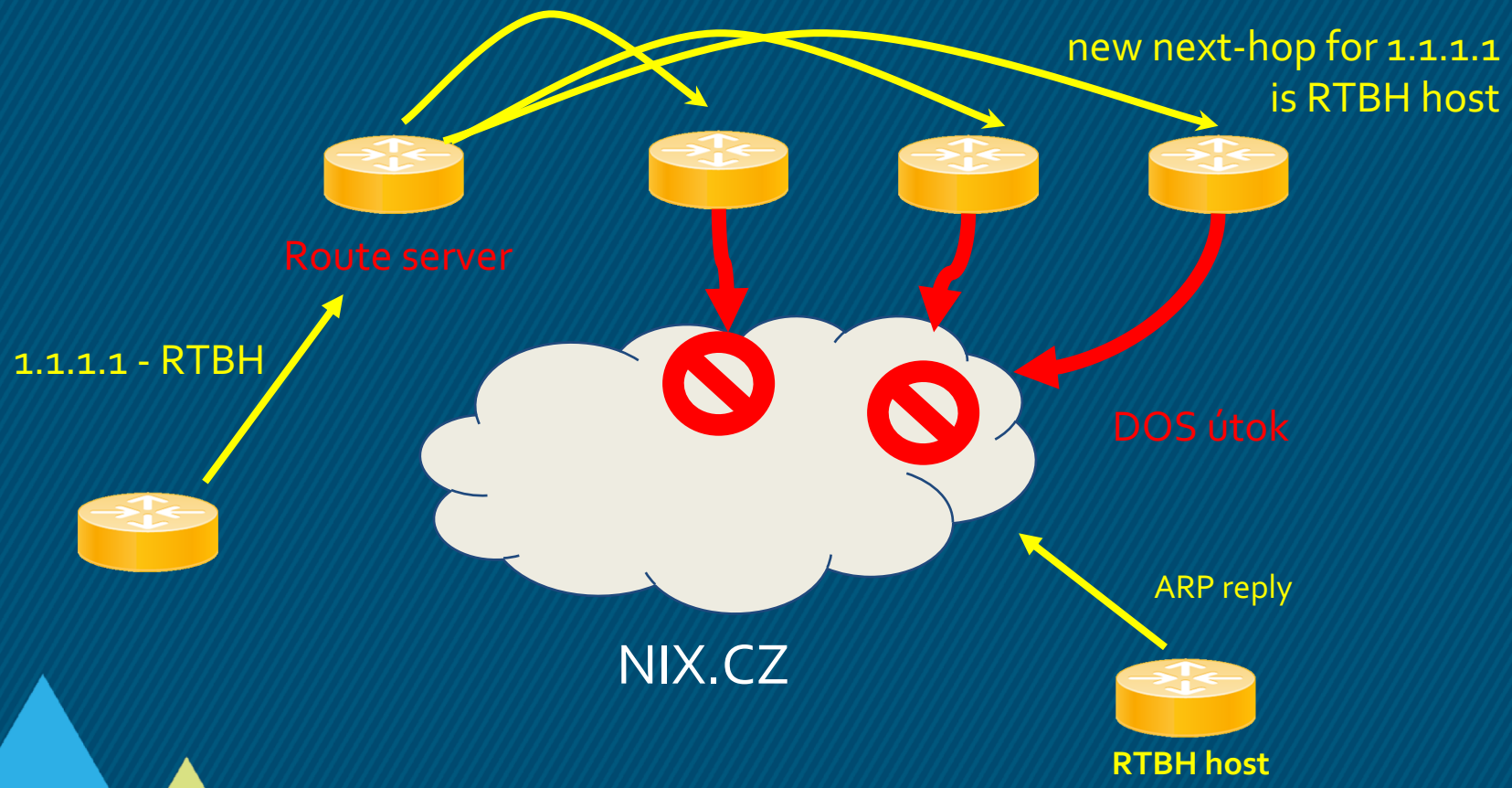
RTBH

Propojování sítí - RTBH (Remotely Triggered Black Hole)



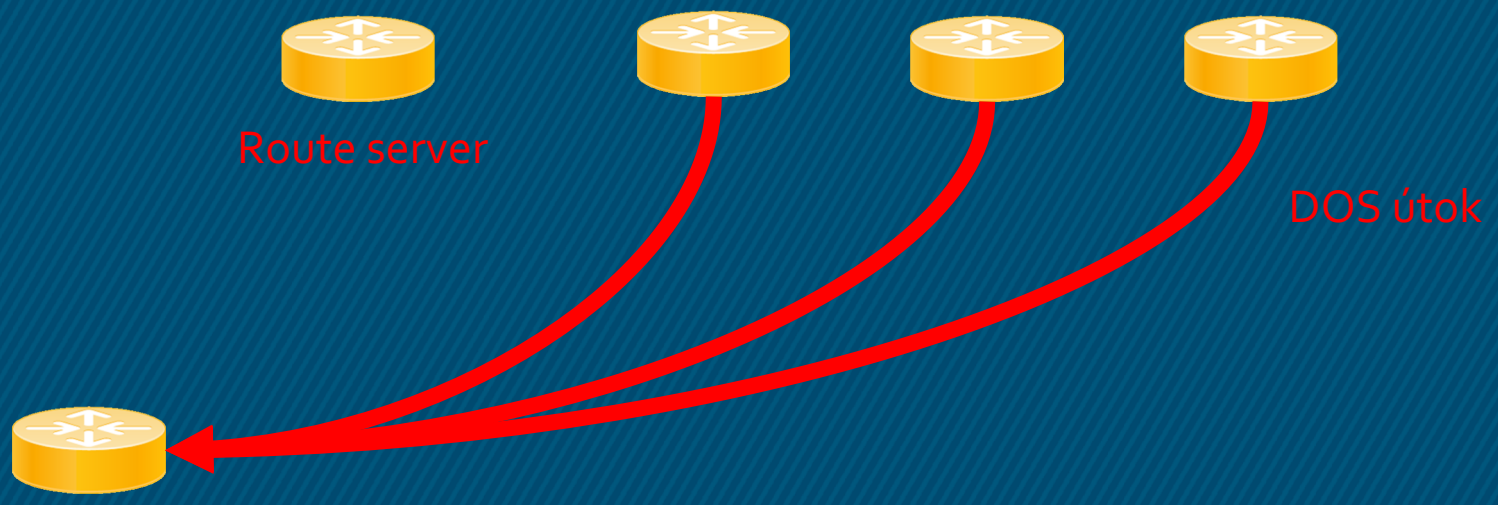
RTBH

Propojování sítí - RTBH (Remotely Triggered Black Hole)



RTBH

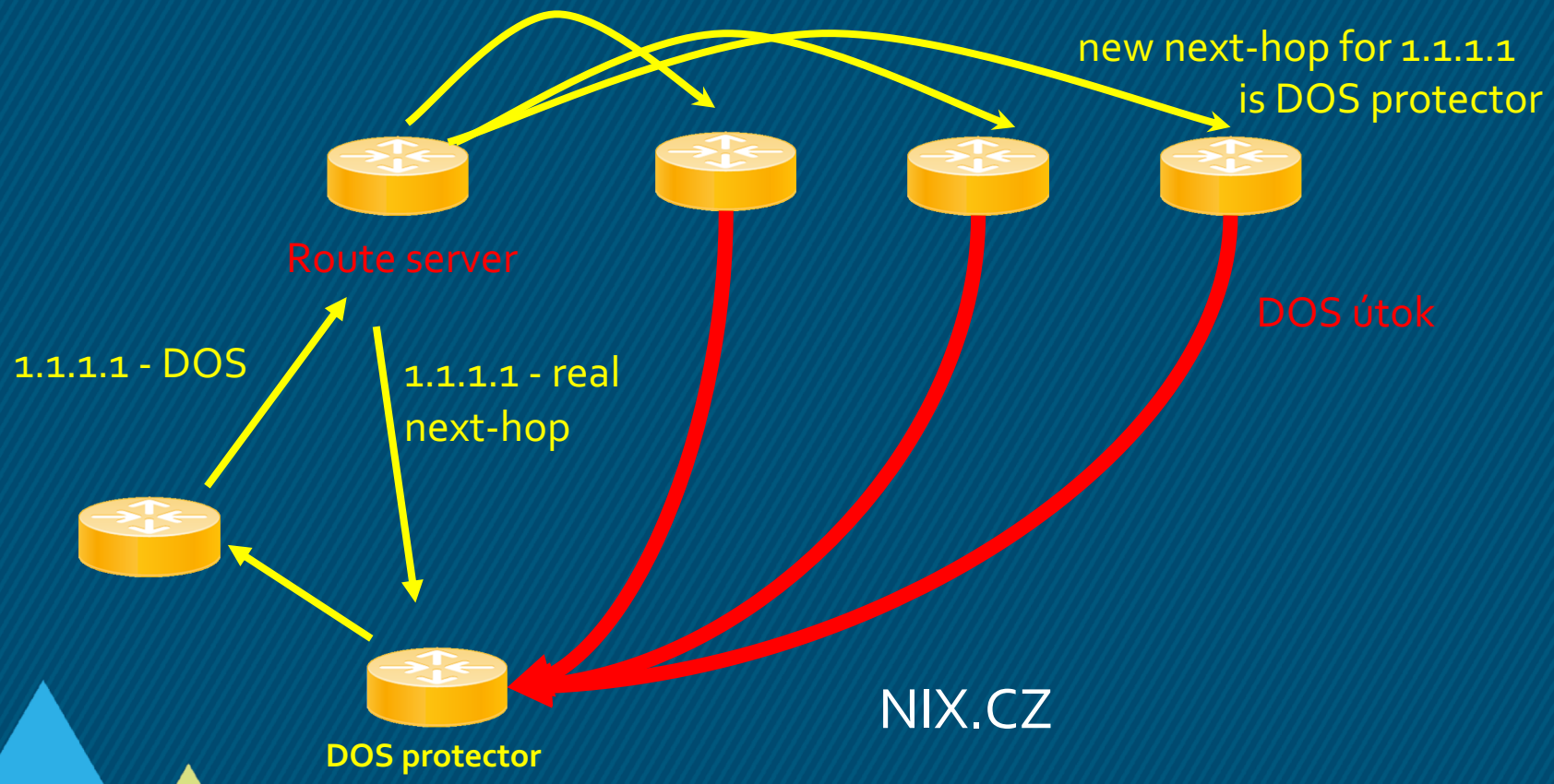
Propojování sítí - DOS protektor



NIX.CZ

Mitigace DOS

Propojování sítí - DOS protektor



NIX.CZ

Mitigace DOS

Propojování sítí

- ~90k IPv4 adres (celkem 800k)
- ~15k IPv6 adres (celkem 16k)
- Google, Facebook, UPC (Vodafone), Orange