

RPKI v e-infrastruktuře CESNET

Ondřej Caletka



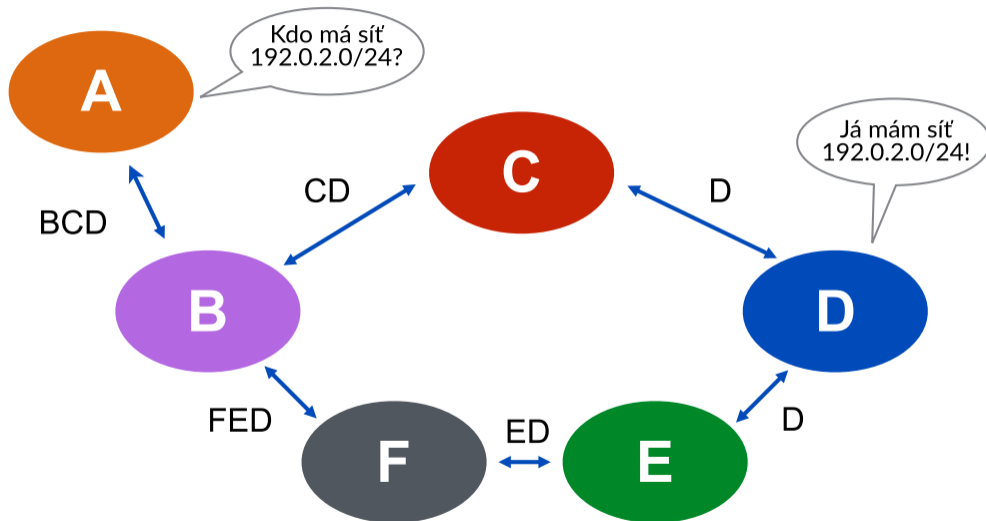
31. ledna 2019



Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

- Internet je síť sítí = vzájemně propojených autonomních systémů
- AS nabízejí své IP adresy sousedům, ti budují směrovací tabulku
- kdokoli může nabízet jakékoli IP adresy
- každý *by měl* nabízet jen svoje IP adresy
- každý *by měl* přijímat jen legitimně nabízené adresy

Budování cesty

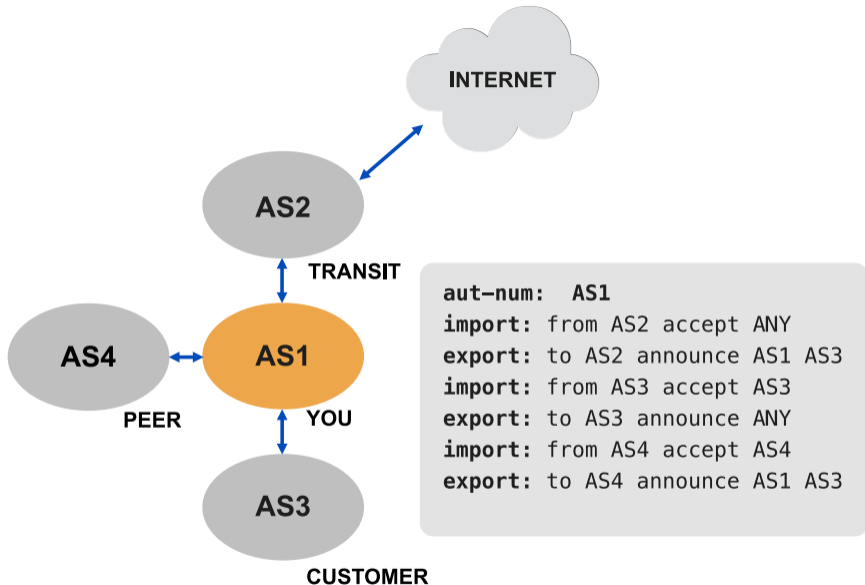


- chyba konfigurace
 - Pakistan Telecom vs. YouTube v roce 2008
- cílený únos
 - nepoužívaných adres pro spamming
 - DNS serverů pro phishing (MyEtherWallet.com v roce 2018)
- cílený odklon provozu
 - za účelem odposlechu/MitM

- veřejné databáze používající jazyk RPSL
- svazují IP adresy s čísly autonomních systémů
- definují vztahy autonomních systémů

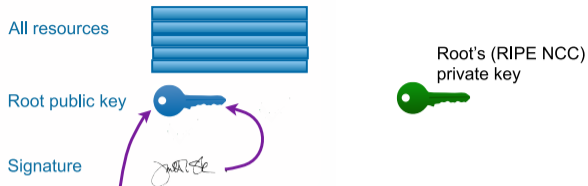
Příklad záznamu

```
$ whois -h whois.radb.net 2001:718::/32
route6:      2001:718::/32
descr:        CESNET6-TCZ
origin:     AS2852
mnt-by:       MAINT-AS2852
changed:      novakv@cesnet.cz 20110531 #19:26:19Z
source:       RADB
```

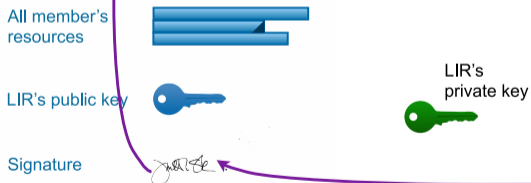


- kryptograficky zabezpečená databáze prefixů a zdrojových AS
- kvalita dat garantovaná regionálními internetovými registry
- omezuje maximální délku prefixu
- odvozeno z PKI
- validace mimo stávající aktivní prvky
- protokol RPKI-RTR pro plnění filtrů ve směrovačích

RIPE NCC's Root Certificate

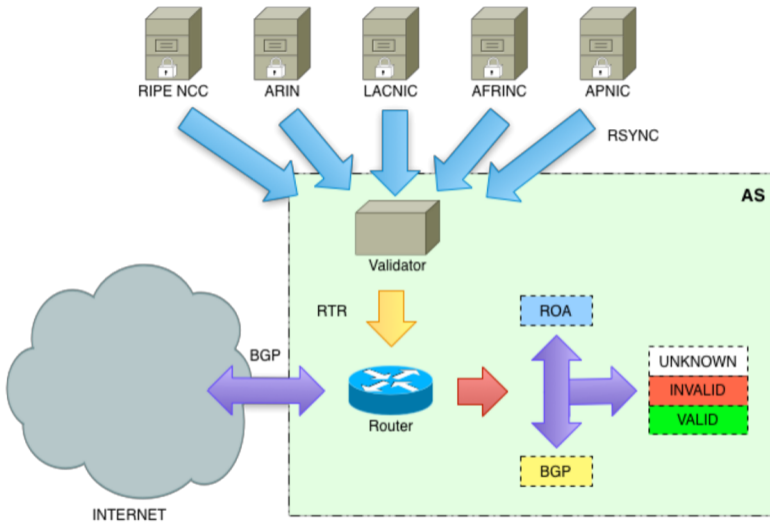


LIR's Certificate



ROA

IP Range	
AS Number	AS123
Max Length	/24
Signature	



- publikujeme ROA pomocí hostované služby RIPE NCC
 - drobná potíž s agregovanými bloky Provider Independent adres
- dvojice validátorů na virtuální infrastrukturu
 - RIPE NCC validator
 - Routinator 3000
- přenos filtrovacích pravidel protokolem RPKI-RTR na směrovače
 - zatím testujeme a vyhodnocujeme
 - později začneme zahazovat prefixy ve stavu INVALID
- pro skutečný efekt musí filtrovat co nejvíce institucí
 - chystá se filtrování na route-serverech NIX-CZ

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
[https://Ondřej.Caletka.cz](https://Ondrej.Caletka.cz)

