RPKI v e-infrastruktuře CESNET

Ondřej Caletka

cesnet

11. února 2020

Úvod do RPKI

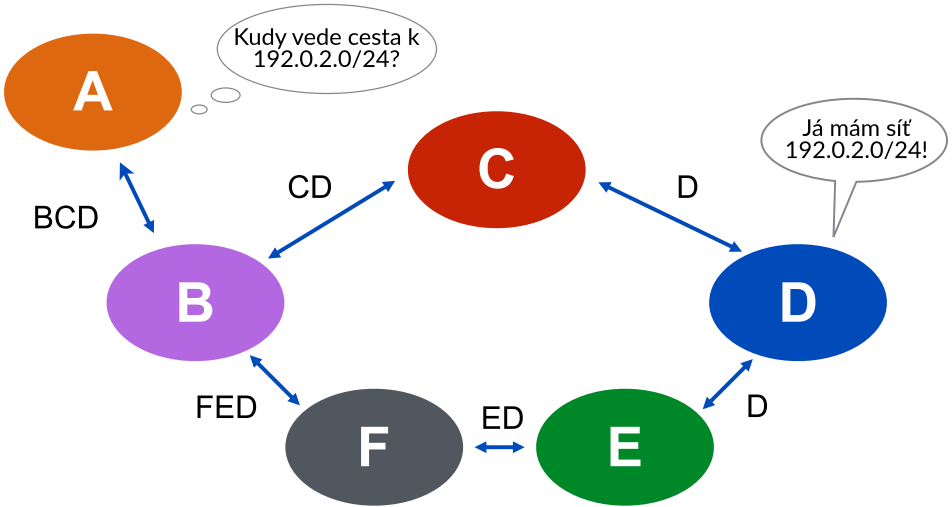
cesnet

Úvod do RPKI

- 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

cesnet

Budování cesty



Zdroj: RIPE NCC BGP Operations and Security training

cesnet

Incidenty v globálním routingu

- 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

cesnet

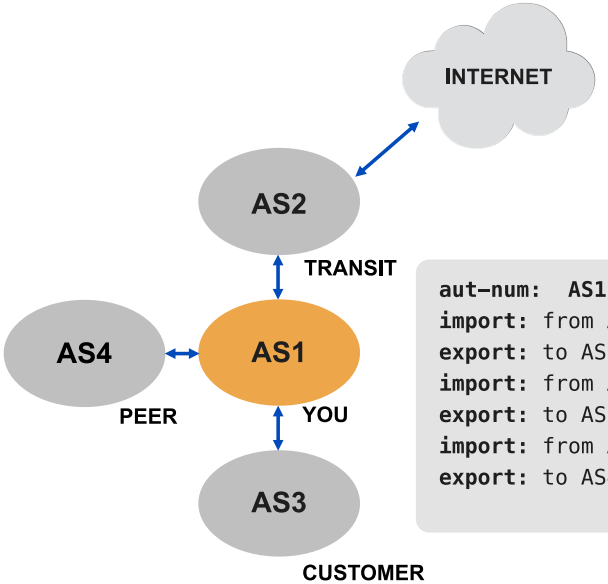
Internet Routing Registry

- 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
```

cesnet




```
aut-num:  AS1
import: from AS2 accept ANY
export: to AS2 announce AS1 AS3
import: from AS3 accept AS3
export: to AS3 announce ANY
import: from AS4 accept AS4
export: to AS4 announce AS1 AS3
```

Zdroj: RIPE NCC BGP Operations and Security training

cesnet

Problémy IRR

- neexistuje **globální důvěryhodná databáze**
- spousta databází je provozována nezávislými institucemi
- minimální nebo žádné ověření oprávněnosti editace
- často zastaralá data

cesnet

Search

AS Number: 2852

Prefixes

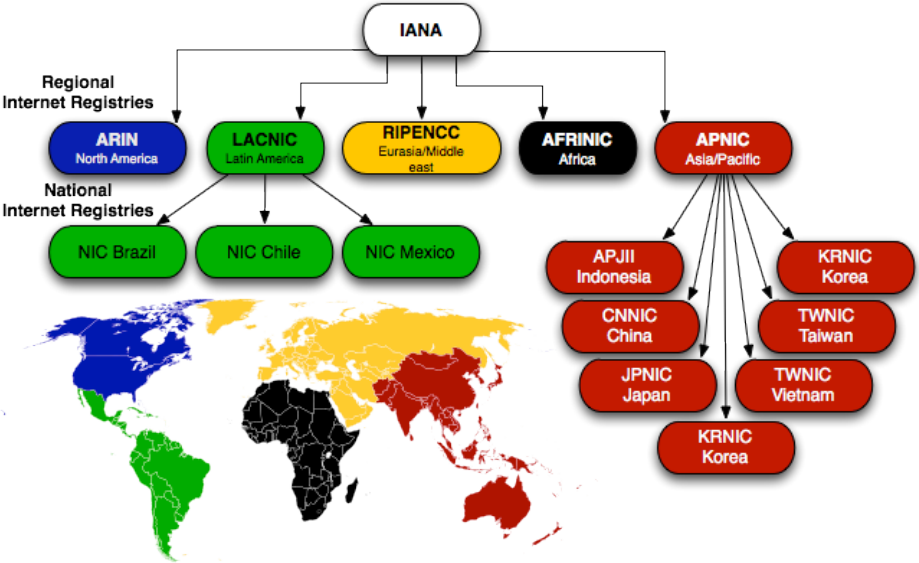
prefix	bgp	ripe_managed	radb	rpki	ripe	advice
78.128.128.0/17	2852	✓	2852	2852	2852	Perfect
2001:718:ffff::/48		✓		65533		Route objects in foreign registries exist, but no BGP origin. Consider moving IRR object to RIPE DB or deleting them.
2001:718::/32	2852	✓	2852	2852	2852	Perfect
195.178.64.0/19	2852	✓	2852	2852	2852	Perfect
195.113.0.0/16	2852	✓	2852	2852	2852	Perfect
194.50.26.0/23		✓		2852		Route objects in foreign registries exist, but no BGP origin. Consider moving IRR object to RIPE DB or deleting them.
193.84.80.0/22	2852	✓	2852	2852	2852	Perfect

cesnet

Resource Public Key Infrastructure

- 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

cesnet



Zdroj: Mapping Autonomous Systems to Organizations: CAIDA's Inference Methodology

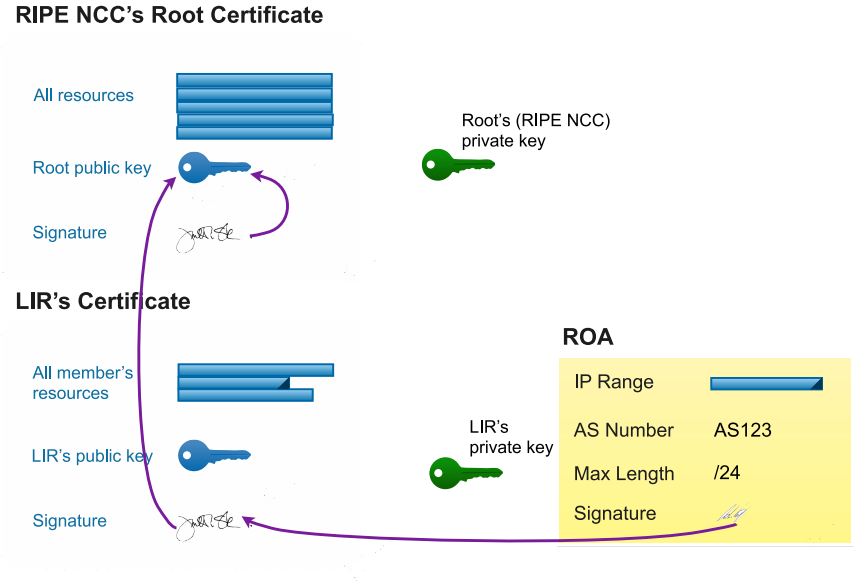
Podepsání přidělených adres

- certifikační autorita (RIR) vystaví každému držiteli certifikát
- v certifikátu jsou zapsány všechny prostředky přidělené danému držiteli
- držitel certifikátu může podepsat objekty *Route Origin Authorization*
- platná jsou pouze ROA obsahující podmnožinu adres uvedených v certifikátu

Obsah ROA

- adresní prefix
- maximální povolená délka prefixu
- číslo zdrojového autonomního systému (není omezené certifikátem)

cesnet



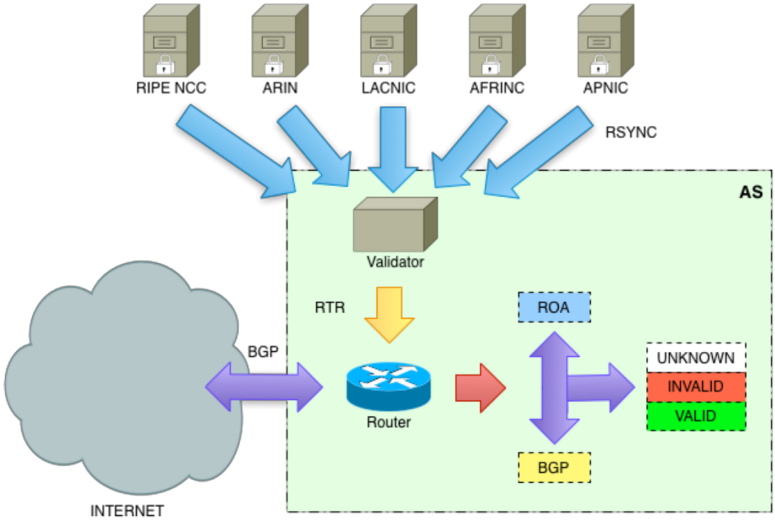
Zdroj: RIPE NCC BGP Operations and Security training

Validace RPKI

- samostatné validátory (*Relying Party*) mimo síťové prvky
- nutné importovat *Trust Anchor Locator* pro každý RIR
  - obsahuje veřejný klíč a adresu serveru
  - ARIN vyžaduje před stažením souhlas se smluvními podmínkami
- výstupem je pravidelně aktualizovaný seznam *Validated ROA Payloads*
- protokol RPKI-RTR pro přenos dat mezi validátorem a směrovačem
- směrovač na základě dat přidělí přijatým síťovým prefixům jeden ze stavů:

VALID	nalezena odpovídající ROA
INVALID	v konfliktu s ROA
UNKNOWN	pro danou adresu žádná ROA neexistuje

cesnet



Zdroj: RIPE NCC BGP Operations and Security training

Nakládání s výsledkem validace

- záleží na lokálním nastavení
- snížení preference prefixům ve stavu INVALID nemá velký účinek
  - specifičtější prefix vždy vyhraje
- pouze zahazování INVALID prefixů vede ke kýženému efektu
  - nemusí pomoci, pokud je validní i nevalidní prefix míří stejnou cestou
  - proto musí validovat pokud možno všichni

cesnet

Nasazení RPKI v e-infrastruktuře CESNET

cesnet

Podepsání prefixů

- využíváme hostované služby přímo od RIPE NCC
  - RIPE NCC drží náš privátní klíč a vydává ROA podle zadání
- jeden držitel = jeden certifikát = samostaný portál RPKI
  - CESNET je i správce PI a Legacy adres svých členů
- problém s agregovanými PI bloky – nelze získat společný certifikát
  - `ČVUT  (147.32/16) + VŠCHT (147.33/16) = 147.32/15`
  - `TUL  (147.230/16) + CAS  (147.231/16) = 147.230/15`
  - `UNOB (160.216/16) + JČU  (160.217/16) = 160.216/15`
- podle aktuálních pravidel není možné ani založit takto agregovaný `route` objekt v RIPE databázi
- prozatím používáme ROA pro `/16`
- zvažujeme deagregování uvedených prefixů

cesnet

Validace RPKI

- dvojice validátorů na virtuální infrastruktuře
  - RIPE NCC validator 3.1
  - Routinator 3000
- problémy se staršími verzemi RIPE NCC validátoru
  - velká spotřeba prostředků
  - vyřešeno v upstreamu změnou databázového backendu
- přenos filtrovacích pravidel protokolem RPKI-RTR na směrovače Cisco a Nokia
  - **nešifrovaný protokol** bez pevně určeného čísla portu
  - nemožnost navázat protokol na loopbackovou adresu na směrovačích Cisco

cesnet

Zahazování INVALID prefixů

Vážení uživatelé e-infrastruktury CESNET,
rádi bychom vám předem oznámili, že v souladu **aktuálními bezpečnostními standardy zavádíme od 24. června 2019 v rámci sítě CESNET technologii RPKI**.

Tato změna se vás přímo netýká a na vaší straně není potřeba žádného administrativního zásahu.

Zavedením technologie RPKI chceme zamezit únosům IP adres během BGP peeringu, ke kterým průběžně dochází jak kvůli chybám konfigurace, tak i za účelem odposlechu či pozměňování komunikace. Zavedením striktních validací RPKI na páteřních směrovačích e-infrastruktury CESNET nebudou síťové prefixy s nevalidním RPKI podpisem v síti akceptovány.

Ve výjimečných případech může dojít k problémům se spojením do vaší sítě z adres, jejichž RPKI podpisy nejsou validní.

Kontrola pomocí https://lg.cesnet.cz

```
BGP routing table entry for 2001:1488::/32
Paths: (21 available, best #3)
…
Path #3: Received by speaker 0
…
Advertised IPv6 Labeled-unicast paths to peers:
  195.113.144.5   195.113.144.6
25192, (aggregated by 25192 217.31.205.211)
  2001:7f8:14::e:2 from 2001:7f8:14::11 (91.210.16.1)
    Origin IGP, metric 100, localpref 150, valid, external,
                                    atomic-aggregate, best, group-best
    Received Path ID 0, Local Path ID 1, version 226789860
    Community: 2852:666
    Origin-AS validity: valid
```

cesnet

Zkušenosti

- přes 5000 zahozených prefixů
- žádná stížnost způsobená zahazováním RPKI
- *zatím* žádný incident, který by RPKI pomohlo zastavit

Občas se někdo překlepne

There are alerts about BGP announcements with your certified address space for cz.ten-34 in the Resource Certification (RPKI) service.

These are BGP announcements with your certified address space that have the status **Unknown**. You should create a ROA for each authorised announcement to make them Valid:

AS Number	**Prefix**
AS8218	2000::/12

Díky za pozornost

Ondřej Caletka
Petr Adamec
Josef Verich

Prezentace je již nyní k dispozici ke stažení na `https://ondřej.caletka.cz/slidy/`