Evoluce RTBH v NIX.CZ

Petr Jiran – NIX.CZ

IT17 Praha
20170621

NIX·CZ | 20 YEARS

Co to je NIX.CZ/SK

- NIX.CZ = *Neutral Internet eXchange of the Czech Republic*
- NIX.SK = *Neutral Internet eXchange of the Slovak Republic*
- IXP = *Internet eXchange Point → platforma pro propojovaní ISP (Internet Service Provider)*

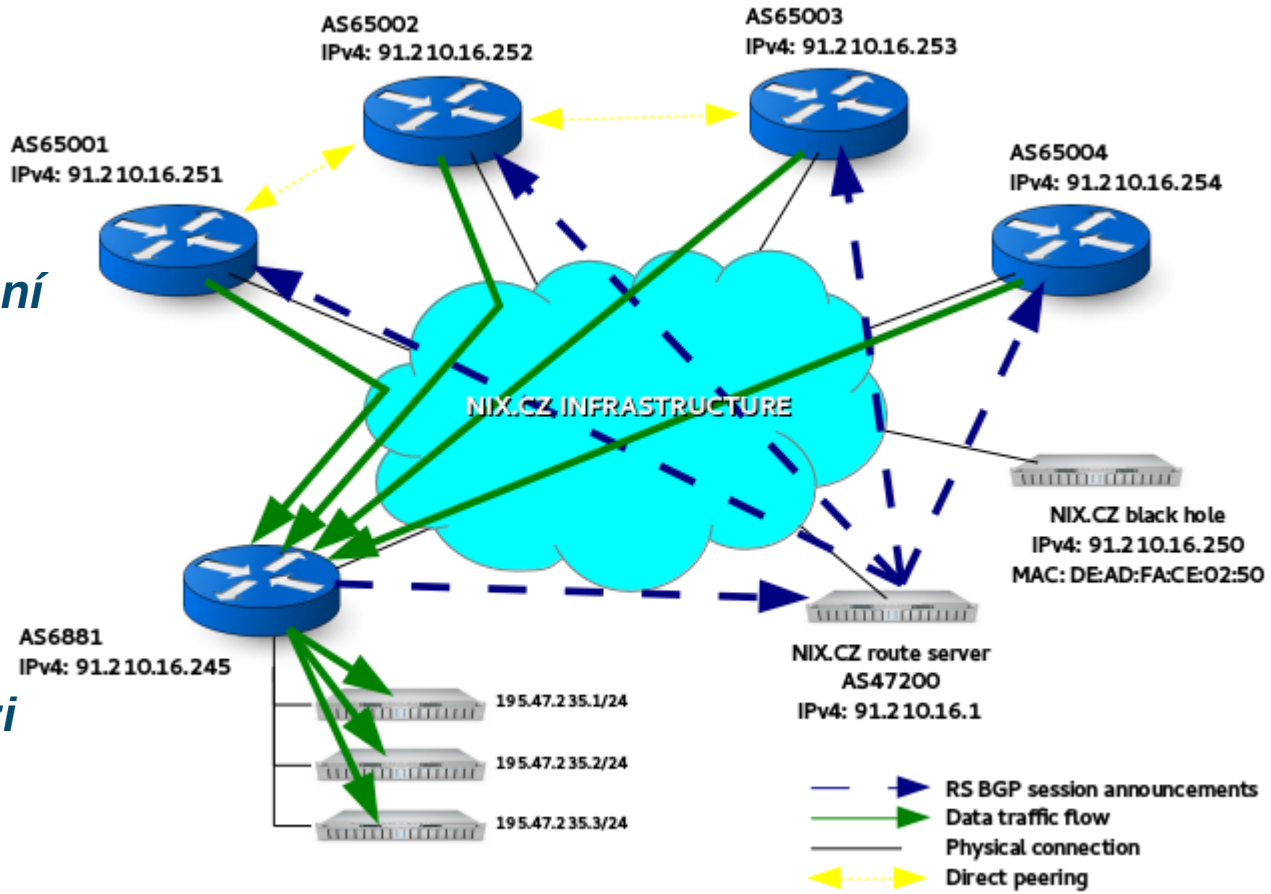
- Založen 1996
- 6x PoP v Praze
- 146 připojených ASN
- 247 připojených portů – 12x 100GE
- 2692 Gb/s připojené kapacity
- 529 Gb/s max. datový tok
- 7 .TLD operátorů
- L2 topologie – virtualizovaná dvojitá hvězda
- Veřejný peering, Privátní VLAN, .TLD housing, multicast VLAN, Partner Program a Fenix projekt
- Člen Euro-IX, RIPE a projektu Atlas

- Založen 2015
- 2x PoP v Bratislavě
- 37 připojených ASN
- 49 připojených portů
- 265 Gb/s připojené kapacity
- 19 Gb/s max. datový tok
- 2 .TLD operátoři
- L2 topologie
- Veřejný peering, Privátní VLAN, .TLD housing, multicast VLAN

Peering @ IXP

- ASN = *Autonomní systém*
- Network / Prefix = *IP adresy sítě*
- Peering IP = *IP adresa hraničního routeru*
- Next-hop IP = *IP adresa dalšího skoku v cestě*
- Peering = *Navázání vztahu mezi ISP pro předávání informací o cestách*
- BGP = *Routovací protokol používaný v peeringu*
- Route server peering = *Navázání přímé*

  BGP relace mezi route serverem a routerem ISP
- Black hole = *Černá díra*
- Direct peering = *Navázání přímé BGP relace mezi routery dvou ISP*

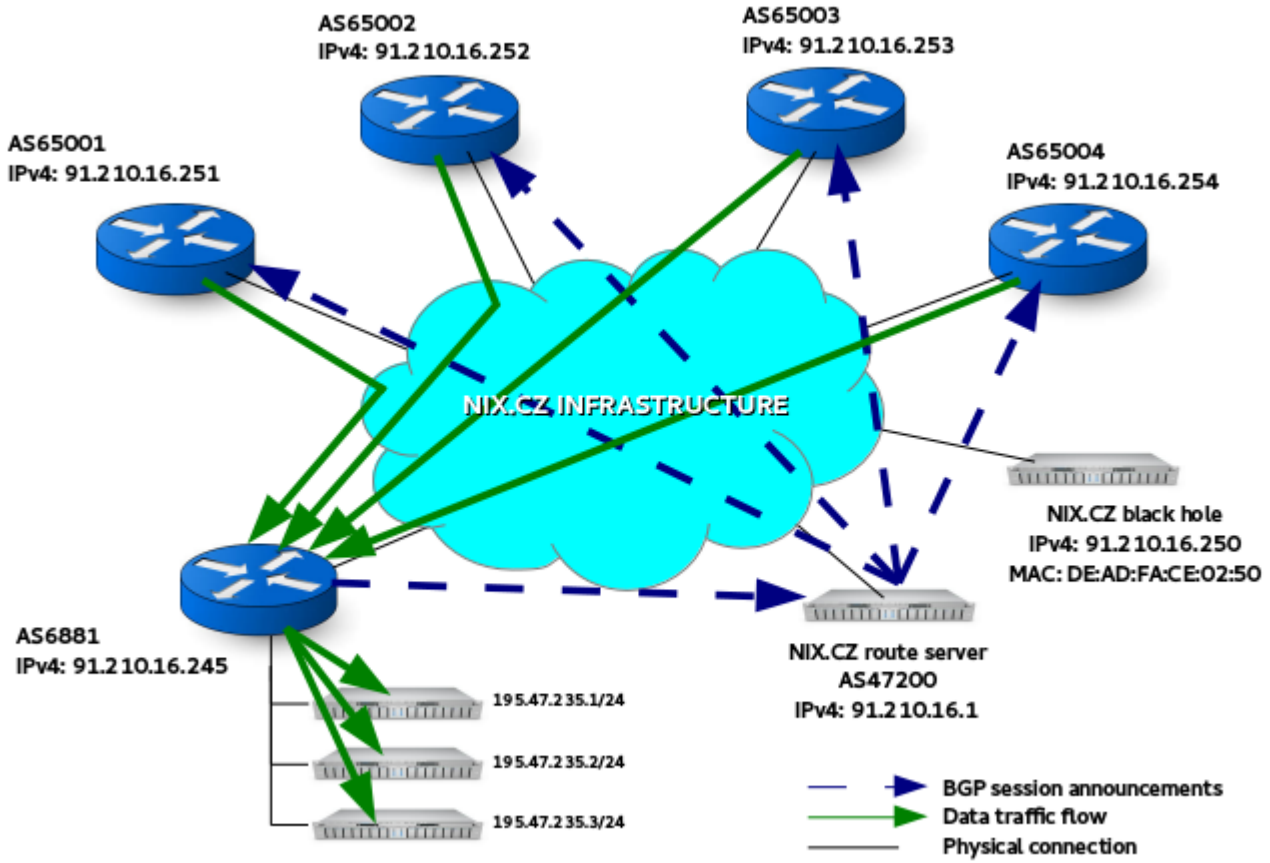


RTBH @ NIX.CZ

- RTBH = Remotely Triggered Black Hole filtering
  - RTBH v praxi znamená, přesměrování toku dat na jiný next-hop (black hole), kde je zahozen
  - Výsledkem je, že provoz směrovaný na původní cíl ho nedosáhne a tím jsou sítě těchto hostitelů chráněny
  - Takto rešený blackholing je účinný způsob, jak zmírnit dopady Distributed Denial of Service (DDoS) útoků, atd.
- Tato funkce byla v roce 2014 nasazena v projektu FENIX a následně 2016 v peeringu NIX.CZ
- Princip fungování RTBH je u různých IXP v podstatě stejný, na začátku však neexistoval standard, jak RTBH signalizovat
- Signalizace RTBH probíhá převážně pomocí BGP komunit, kterými lze řídit propagaci oznam. sítí
- Pokud tedy hovoříme o evoluci RTBH, jedná se spíše o vývoj signalizace než jeho principu

RTBH filtrování @ NIX.CZ

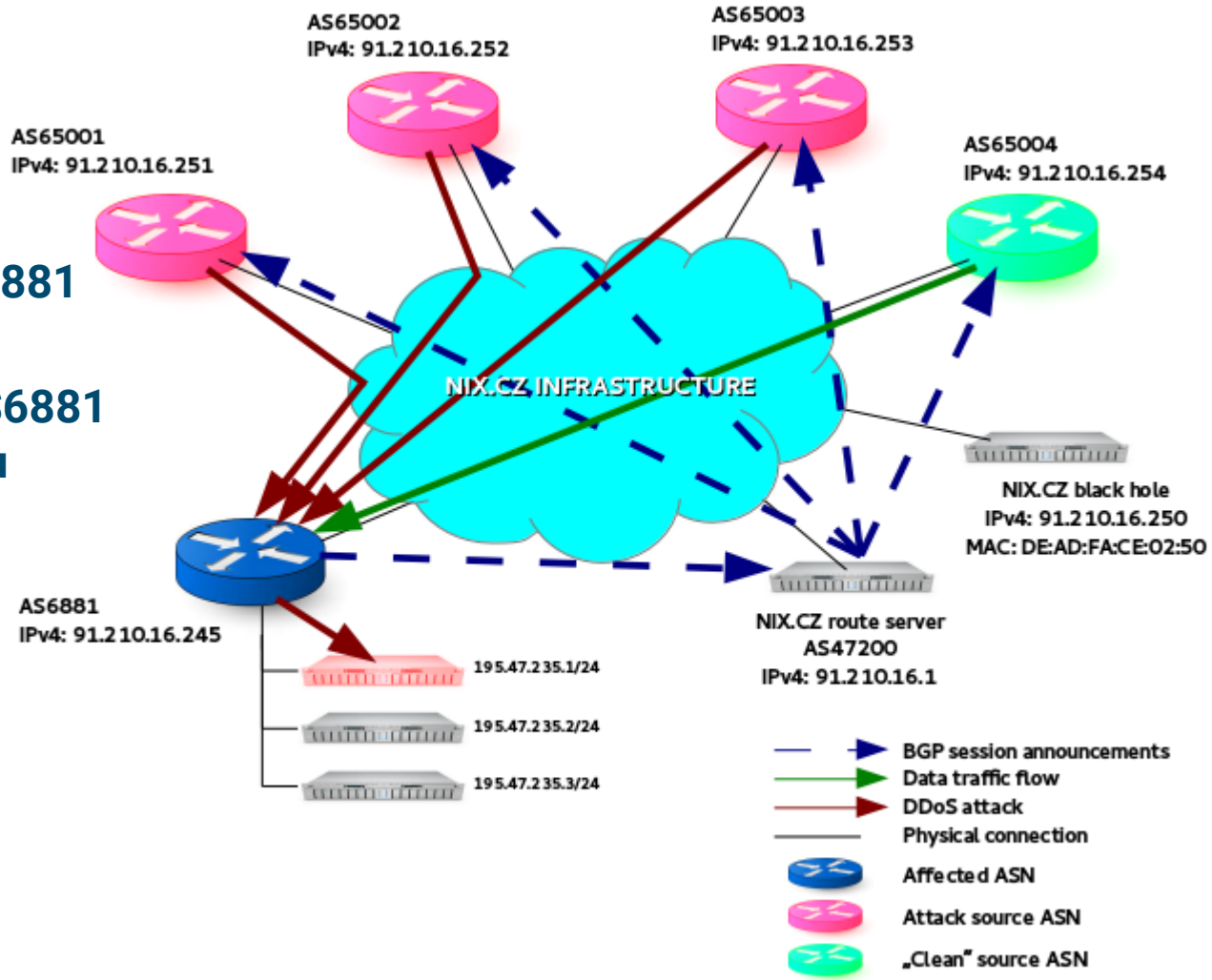
- Standardní situace:
  - → AS6881 propaguje pfx. 195.47.235.0/24 směrem k RS bez BGP komunit
  - → RS propaguje tento pfx. všem klientům
  - → Prefix je přijímán/akceptován a zvolen jako best-path
  - → Odpovídající next-hop IP (91.210.16.245) a MAC jsou naučeny pomocí ARP
  - → Zákaznický provoz teče přes NIX.CZ infrastrukturu do AS6881



NIX·CZ | 20 YEARS

RTBH filtrování @ NIX.CZ

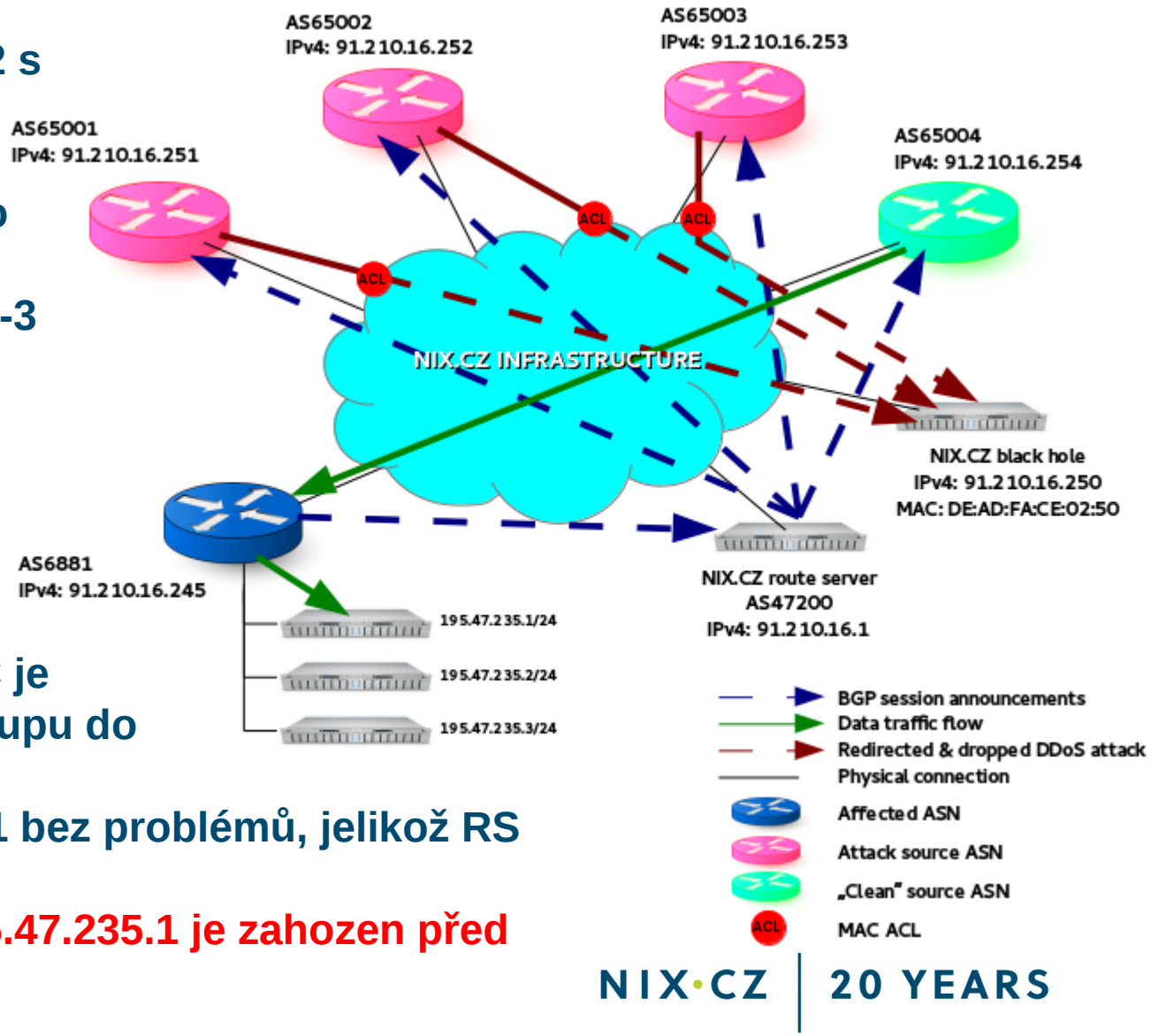
- DDoS útok:
  - → AS65001-3 jsou zdroje zákeřného (“dirty”) provozu útočícího na server 195.47.235.1 v AS6881
  - → AS65004 je zdroj normálního (“clean”) provozu proudícího na server 195.47.235.1 v AS6881
  - → Server 195.47.235.1 je přetížen a jeho služby jsou nedostupné pro všechny klienty
  - → Ostatní IP AS6881 mohou být tímto útokem postiženy také
  - → Zahlcení portů, přetížení CPU routeru, “flapování” BGP relací, atd.



NIX·CZ | 20 YEARS

RTBH filtrování @ NIX.CZ

- Obrana proti DDoS útoku:
  - → AS6881 začne propagovat pfx. 195.47.235.1/32 s BGP komunitou 47200:65004 65535:666 směrem k RS
  - → RS přijme tuto komunitu a změní next-hop pro tento pfx. 195.47.235.1/32 na black hole IP (91.210.16.250) pouze pro klienty AS65001-3
  - → AS65001-3 přijmou/akceptují a zvolí prefix 195.47.235.1/32 jako best-path
  - → AS65001-3 se naučí odpovídající black hole next-hop IP a MAC via ARP
  - → AS65001-3 začnou směrovat svůj provoz na black hole IP (91.210.16.250)
  - → Provoz směrovaný na cílovou black hole MAC je pomocí vstupního L2 ACL zahozen již na vstupu do infrastruktury NIX.CZ
  - → AS65004 posílá "čistý" provoz na 195.47.235.1 bez problémů, jelikož RS nezměnil tomuto klientovi next-hop
  - → Veškerý provoz + DDoS z AS65001-3 na IP 195.47.235.1 je zahozen před tím, než dosáhne AS6881



NIX·CZ | 20 YEARS

Konfigurace RTBH @ NIX.CZ

- **Příklad konfigurace routeru a výstupní route-mapy:**

(Cisco – IPv4)
ip prefix-list RTBH seq 5 permit <*blackholed pfx.*>
!
router bgp <*your ASN*>
no bgp enforce-first-as
neighbor <*RS IP*> remote-as <*NIX.CZ RS ASN*>
!
address-family ipv4
network <*blackholed prefix*>
neighbor <*RS IP*> route-map RTBH-MAP out
exit-address-family
!
route-map RTBH-MAP permit 10
match ip address prefix-list RTBH
set community 47200:65004 65535:666
#

- **Příklad konfigurace routeru a vstupní route-mapy akceptující /(>=32) pfx.:**

(Cisco – IPv4)
ip community-list standard BLACKHOLE permit 65535:666
ip prefix-list IPv4-/24 seq 5 permit 0.0.0.0/0 le 24
ip prefix-list IPv4-/32 seq 5 permit 0.0.0.0/0 le 32
!
route-map AS<*your ASN*>-RS-IPv4-IN permit 10
match ip address prefix-list IPv4-/32
match community BLACKHOLE
set local-preference 666
set community no-export
!
route-map AS<*your ASN*>-RS-IPv4-IN permit 20
match ip address prefix-list IPv4-/24
set local-preference 10
#

RTBH signalizace @ IXP/ISP

- V roce 2014 signalizovali RTBH IXP a ISP různými způsoby
  - → Pomocí oznamování změněného next-hopu daného pfxu.
  - → Pomocí BGP komunit
  - → Kombinací obou výše uvedených variant

- Neexistovala žádná standardizace → každý rešil po svém:
  - IXP – Internet eXchange Point

    NIX.CZ = next-hop + 65511:47200
    DE-CIX = next-hop
    MSK-IX = 0:666
    TPIX = 29535:666
    Netix = 65499:999

    - ISP – Internet Service Provider

      Hurricane Electric = 6939:666
      NTT = 2914:666
      Init7 = 65000:666
      Team Cymru = 64496:666

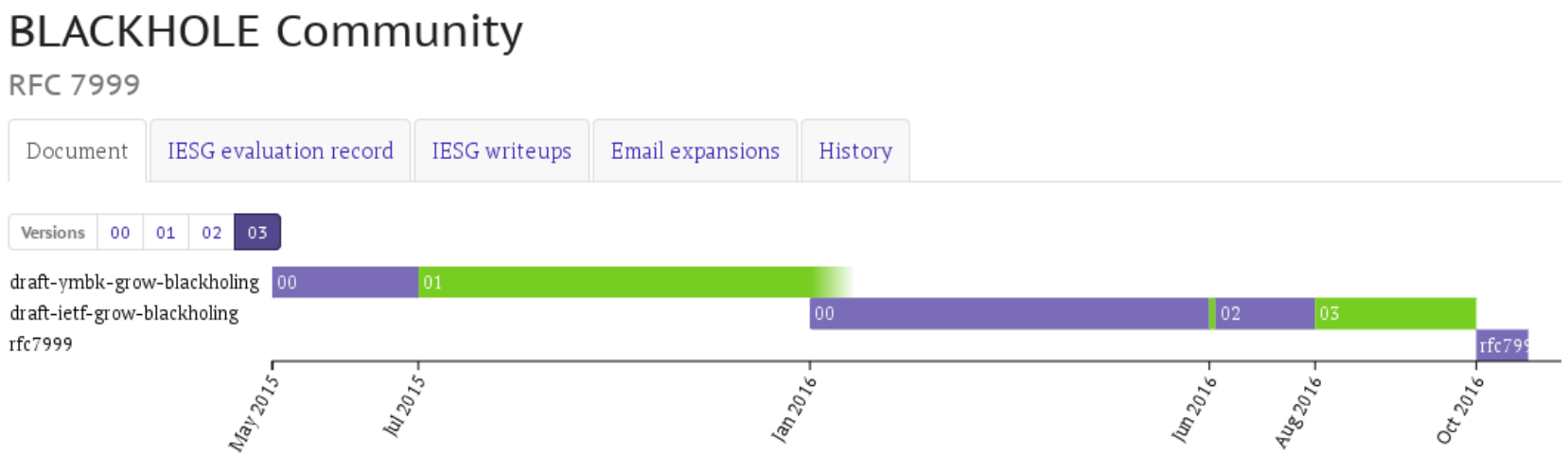
Standardizace RTBH @ Euro-IX

- **2014 na půdě Euro-IX začala diskuze o standardizaci RTBH**
  - **→ Diskuze zda RTBH v IXP vůbec podporovat**
  - **→ Diskuze jak by měla BGP komunita vypadat**
  - **→ Záležitost spíše ISP než IXP**
- **RTBH je u ISP využíváno jak v peeringu, tak směrem k upstream a downstream partnerům**
  - **→ Nejednotnost v implementaci není efektivní**

euro-IX
European Internet Exchange Association

RTBH @ IETF

- Thomas King (DE-CIX) – 2015 IETF draft pro standardizaci tzv. well-know BGP community
- Dohoda IXP a ISP používajících RTBH na:
  - → 65535:666 well-known komunitě
  - → NO_EXPORT / NO_ADVERTISE
- Není v konfliktu se stavajícími koncepty RTBH
- 2016 standardizováno pod RFC 7999 (https://tools.ietf.org/html/rfc7999)



RFC 7999 @ IANA

- **Výsledkem standardizace RFC 7999 je registrace BLACKHOLE well-known komunity u organizace IANA.**

http://www.iana.org/assignments/bgp-well-known-communities/bgp-well-known-communities.xhtml

Internet Assigned Numbers Authority

Attribute Value	Attribute	Reference
0x00000000-0x0000FFFF	Reserved	[RFC1997]
0x00010000-0xFFFEFFFF	Reserved for Private Use	[RFC1997]
0xFFFF0000	planned-shut	[draft-francois-bgp-gshut][Pierre_Francois]
0xFFFF0001	ACCEPT-OWN	[RFC7611]
0xFFFF0002	ROUTE_FILTER_TRANSLATED_v4	[draft-l3vpn-legacy-rtc]
0xFFFF0003	ROUTE_FILTER_v4	[draft-l3vpn-legacy-rtc]
0xFFFF0004	ROUTE_FILTER_TRANSLATED_v6	[draft-l3vpn-legacy-rtc]
0xFFFF0005	ROUTE_FILTER_v6	[draft-l3vpn-legacy-rtc]
0xFFFF0006	LLGR_STALE	[draft-uttaro-idr-bgp-persistence]
0xFFFF0007	NO_LLGR	[draft-uttaro-idr-bgp-persistence]
0xFFFF0008	accept-own-nexthop	[Ashutosh_Grewal]
0xFFFF0009-0xFFFF0299	Unassigned	
0xFFFF029A	BLACKHOLE	[RFC7999]
0xFFFF029B-0xFFFFFF00	Unassigned	
0xFFFFFF01	NO_EXPORT	[RFC1997]
0xFFFFFF02	NO_ADVERTISE	[RFC1997]
0xFFFFFF03	NO_EXPORT_SUBCONFED	[RFC1997]
0xFFFFFF04	NOPEER	[RFC3765]
0xFFFFFF05-0xFFFFFFFF	Unassigned	

RFC 7999 @ podpora

- **V současné době vypadá podpora RFC 7999 takto:**
- **Výrobci, ISP a IXP respektujte RFC 7999 !!!**
- **Používejte RFC 7999 a dejte o tom vědět:**

  pj@nix.cz

  https://github.com/tking/BLACKHOLE-BGP-Community

Supporting BGP Speakers

BGP Speaker	Implementation Status
BIRD	Done
GoBGP	Done
OpenBGPD	Done - Usage hint: "allow from any community BLACKHOLE set nexthop blackhole"
ExaBGP	Done
Nokia	Requested
Cisco	Open
Juniper	Open
Brocade	Open
Huawei	Open

Supporting IXPs

IXP	Information
DE-CIX FRA, NYC, MAD, DUS, MUC, HAM, IST, PMO, MRS, DFW	https://de-cix.net/en/services/globepeer/blackholing
NYIIX	http://www.nyiix.net/rtbh/
CIX.HR	https://www.cix.hr/o-cix-u/infrastruktura/route-server
Community-IX	https://www.community-ix.de/technik/
LAIIX	http://www.laiix.net/rtbh/
Equinix Ashburn, Atlanta, Chicago, Dallas, Los Angeles, Miami, New York, Palo Alto, San Jose, Seattle, Toronto, Vienna, Geneva, Paris, Zurich, Hong Kong, Melbourne, Osaka, Singapore, Sydney, Tokyo	http://www.sanog.org/resources/sanog28/SANOG28-Conference_RTBH-Safiudeen.pdf
MSK-IX Moscow, St.-Petersburg, Rostov-on-Don, Stavropol, Samara, Kazan, Ekaterinburg, Novosibirsk, Vladivostok	http://kb.msk-ix.ru/en/ix/services/route-server/#ddos
SIX Seattle	https://www.seattleix.net/blackholing
France IX Paris and Marseille	https://www.franceix.net/en/technical/blackholing/
NIX.CZ	https://www.nix.cz/en/technical#rs

RTBH @ budoucnost

- Prosazování standardu RFC 7999 u ISP a IXP
- Synchronizace používání BGP signalizací u IXP v rámci Euro-IX
- Implementace nového standardu RFC 8092 - BGP Large Communities Attribute
- Vývoj nových (lepších) mitigačních mechanismů
- Spolupráce NIX.CZ na tvorbě nových standardů v rámci Euro-IX a IETF

??? Dotazy ???

Petr Jiran

e-mail: pj@nix.cz

https://www.linkedin.com/in/petrjiran