Locator/ID SPlit (LISP)

Łukasz Bromirski
lbromirski@cisco.com

Polish Network Operators' Group

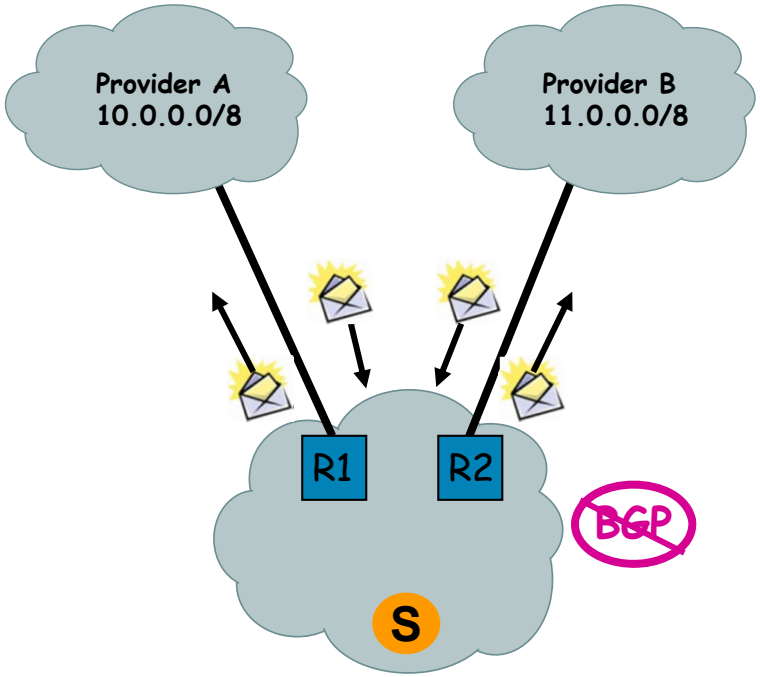
LISP?

- Problem który LISP stara się rozwiązać, to skalowalność tablic routingu
  - międzyplanetarny internet?
- Wnioski ze spotkania Internet Architect Board w październiku 2006 opisano w RFC4984… i już ☺
- LISP jest próbą stworzenia technologii typu OTN – niezależną od protokołu warstwy trzeciej – IPv4 i IPv6

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Multihoming?

- Istniejące mechanizmy multihomingu nie są idealne
  - kontrola ruchu wchodzącego i wychodzącego – zarówno z perspektywy operatora jak i klienta
  - protokół – BGP
  - adresacja PI w IPv4 i IPv6 – rozłączenie adresu od operatora od którego on pochodzi
- …a gdyby tak jeszcze zmniejszyć tablice routingu?



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Oddzielenie adresacji

- Znaczenie pól w adresie można zmienić – lub rozszerzyć:

ID i lokalizacja

IPv6: 2001:0102:0304:0506:1111:2222:3333:4444

Locator ID

ID i lokalizacja

IPv4: 209.131.36.158.10.0.0.1

Locator ID

Dla PI – nowy ‘locator’,
dla PA – nowe ID

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Definicja znaczeń

- **ID lub EID**

  adres konkretnego hosta lub routera

  pojawiają się w rekordach DNS

  nowa przestrzeń adresowa – nie pojawia się w globalnej tablicy routingu

- **Locator**

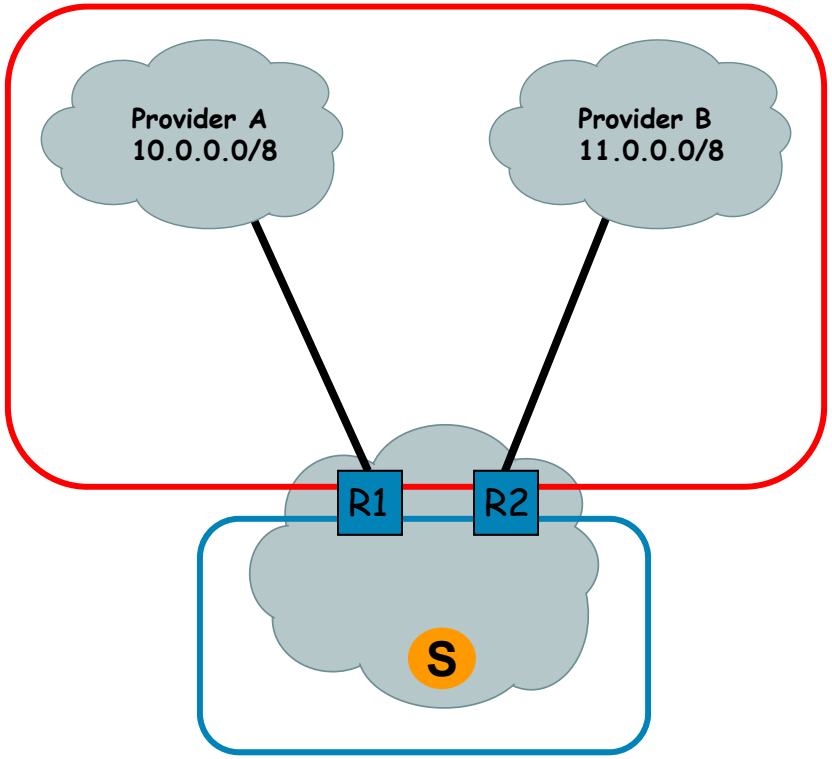
  Adresy infrastruktury – routerów LISP i dostawców

  Hosty nie muszą wiedzieć o tej przestrzeni adresowej

  Znajdują się w globalnej tablicy routingu i podlegają najlepszym praktykom routingu (w szczególności – agregacji)

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

LISP – podział adresacji



W szkielecie („Internecie”) wykorzystywane są adresy typu ‘Locator’

Hosty używają ID/EID

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Czym jest zatem LISP?

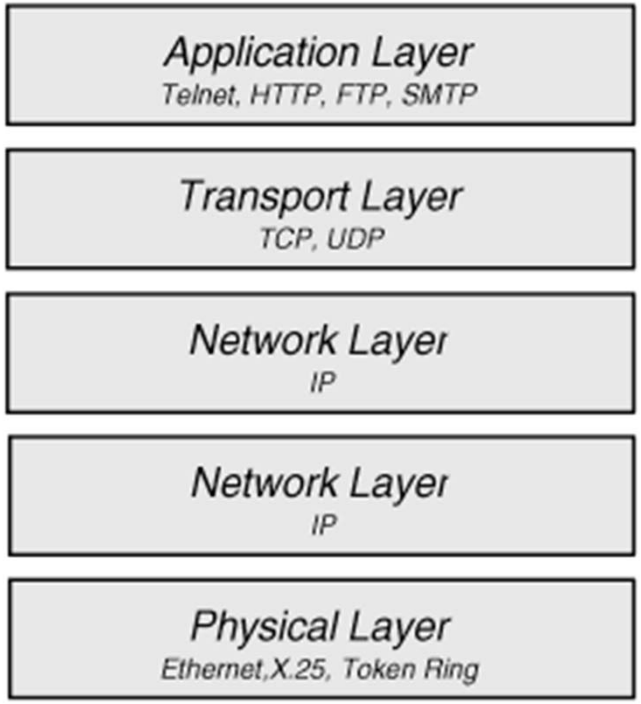
- Protokołem zapewniającym separację adresów – Locator od ID
- Podstawowe cele z jakimi tworzony był LISP
  - Rozwiązanie oparte o sieć
  - Stos protokołów po stronie hostów nie ulega modyfikacji
  - Żadnych zmian w adresacji hostów
  - Mało zmian w konfiguracji urządzeń sieciowych
  - Możliwy do przyrostowego wdrożenia
  - Niezależny od protokołu L3 – IPv4 i IPv6

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Jak „wygląda” LISP?

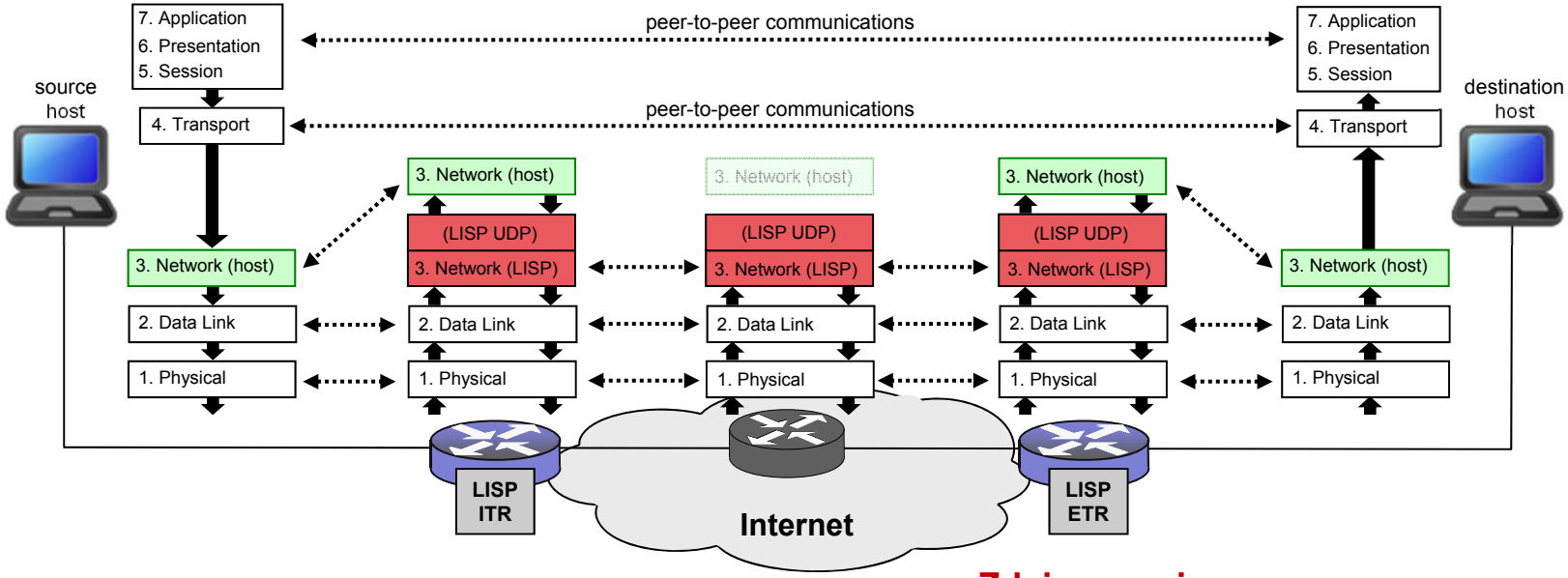
Stos hosta:
dodaje ID

Stos routera:
dodaje ‘locator’
wraz z nowym
nagłówkiem



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Jak „wygląda” LISP dokładniej?



Dodawanie nagłówka LISP

Zdejmowanie nagłówka LISP

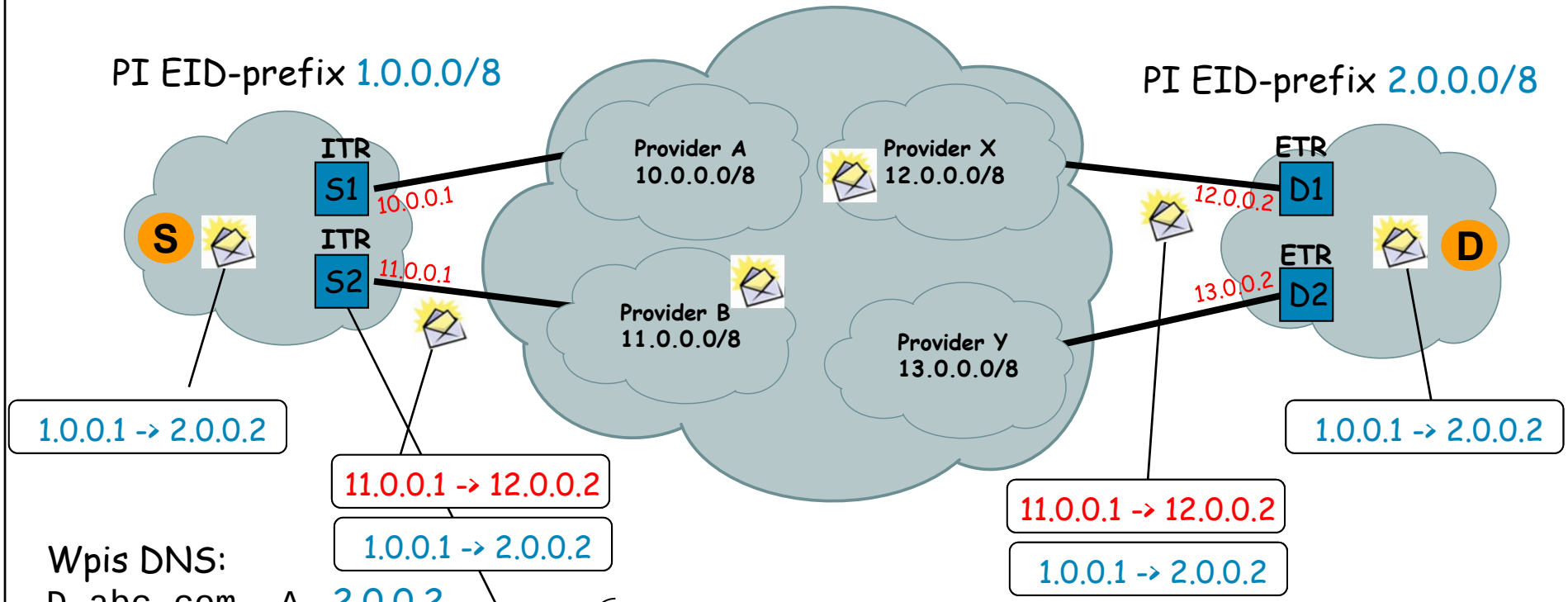
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Elementy sieciowe LISP

- Ingress Tunnel Router (ITR)
  - Odnajduje mapowanie EID na ‘Locator’
  - Tuneluje ruch do odpowiedniego ‘Locatora’
- Egress Tunnel Router (ETR)
  - Odnajduje mapowanie EID i adresów ‘Locator’ów
  - Rozpakowuje tunel i przesyła dane do hosta
- xTR – router LISP bez rozróżniania kierunku obsługiwanego ruchu
  - Typowe wdrożenie składa się z routerów xTR

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Przekazywanie ruchu unicastowego



Wpis DNS:
D.abc.com A 2.0.0.2

Wpis mapujący:
- EID-prefix: 2.0.0.0/8
- Locator-set:
  - 12.0.0.2, priority: 1, weight: 50 (D1)
  - 13.0.0.2, priority: 1, weight: 50 (D2)

Polityka Kontrolowana przez hosta docelowego

Legenda:
- EID -> Niebieskie
- Locator -> Czerwone

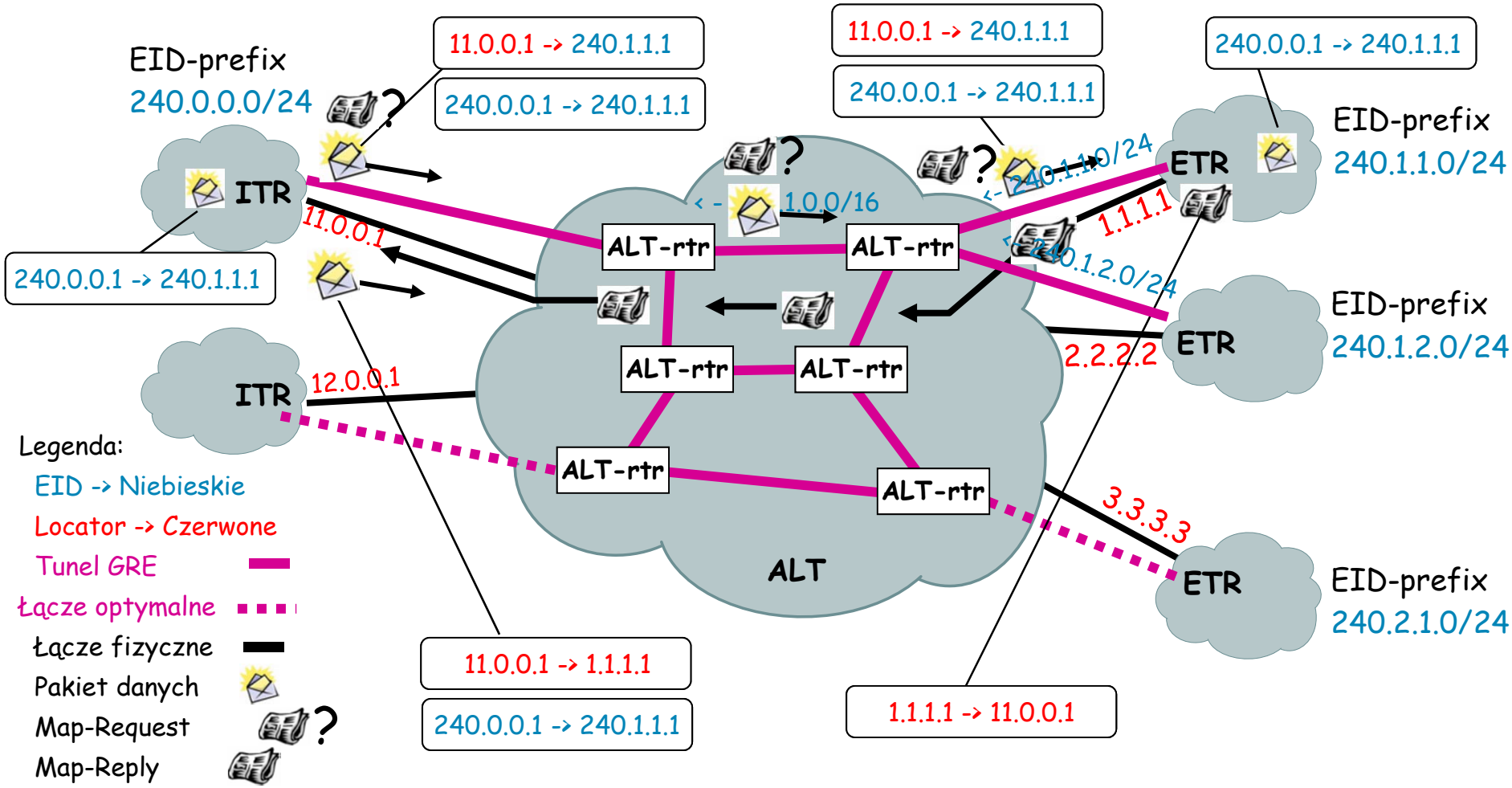
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

LISP + ALT?

- Dana lokalizacja używa przestrzeni adresowej EID
- Sieć operatora używa przestrzeni adresowej ‘Locatorów’
- Musi istnieć mechanizm tworzenia mapowań po stronie routerów LISP
- Rozgłaszanie prefiksów EID w alternatywnej topologii tuneli GRE – przez protokół BGP
- Wejściowe routery LISP (ITR) otrzymują mapowania
  (map-request) w topologii ALT od routerów wyjściowych (ETR)

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Jak to działa razem?



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

LISP+ALT+ … Internet?

- LISP będzie wdrażany przyrostowo
- Sieci wspierające/wykorzystujące LISP będą musiały komunikować się z Internetem
- Mamy dwie podstawowe drogi:
  - LISP Network Address Translators (LISP-NAT)
  - Proxy Tunnel Routers (PTRs)

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

LISP – gdzie jesteśmy dzisiaj?

- Pierwsze prace implementacyjne w marcu 2007 na praskim spotkaniu IETF
- W czerwcu 2007 rozpoczął się pilot
  - Platforma NX-OS na urządzeniach Cisco
  - OpenLISP na platformie FreeBSD
  - Prowadzone są prace nad implementacją w Cisco IOS i IOS-XR
- Sieć pilotażowa działa – 24 lokalizacje w 5 krajach
  - Dwa prefiksy: 153.16.0.0/16 i 2610:00d0::/32
  - LISP-ALT używa 32-bitowych numerów AS: 32656.x

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Użytkownicy LISPa

- Google
- Facebook
- Cisco
- PLNOG ☺

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Gdzie szukać informacji?

- Strona projektu LISP4:

  http://lisp4.cisco.com/

- Demon OpenLISP dla FreeBSD:

  http://gforge.info.ucl.ac.be/projects/openlisp/

- Narzędzie diagnostyczne LIG:

  http://www.github.com/davidmeyer/lig

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Gdzie szukać draftów/API?

Locator/ID Separation Protocol (LISP) - draft-ietf-lisp-07; 25-Apr-2010
http://tools.ietf.org/html/draft-ietf-lisp-07

LISP Map Server - draft-ietf-lisp-ms-05; 26-Apr-2010
http://tools.ietf.org/html/draft-ietf-lisp-ms-05

LISP ALT - draft-ietf-lisp-alt-04; 26-Apr-2010
http://tools.ietf.org/html/draft-ietf-lisp-alt-04

LISP Interworking - draft-ietf-lisp-interworking-00; 26-May-2009
http://tools.ietf.org/html/draft-ietf-lisp-interworking-00

LISP Multicast - draft-ietf-lisp-multicast-03; 16-Apr-2010
http://tools.ietf.org/html/draft-ietf-lisp-multicast-03

LISP Mobility Architecture - draft-meyer-lisp-mn-01; 01-Feb-2010
http://tools.ietf.org/html/draft-meyer-lisp-mn-01

LISP Internet Groper (LIG) – draft-ietf-lisp-lig-00;10-Apr-2010
http://tools.ietf.org/html/draft-ietf-lisp-lig-00

LISP CanonicalAddressFamily (LCAF) – draft-farinacci-lisp-lcaf-00; 13-Apr-2010
http://tools.ietf.org/html/draft-farinacci-lisp-lcaf-00

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Secure Inter-Domain Routing

Łukasz Bromirski
lbromirski@cisco.com

Polish Network Operators' Group

Agenda

- Problem
- Rozwiązanie

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Problem

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

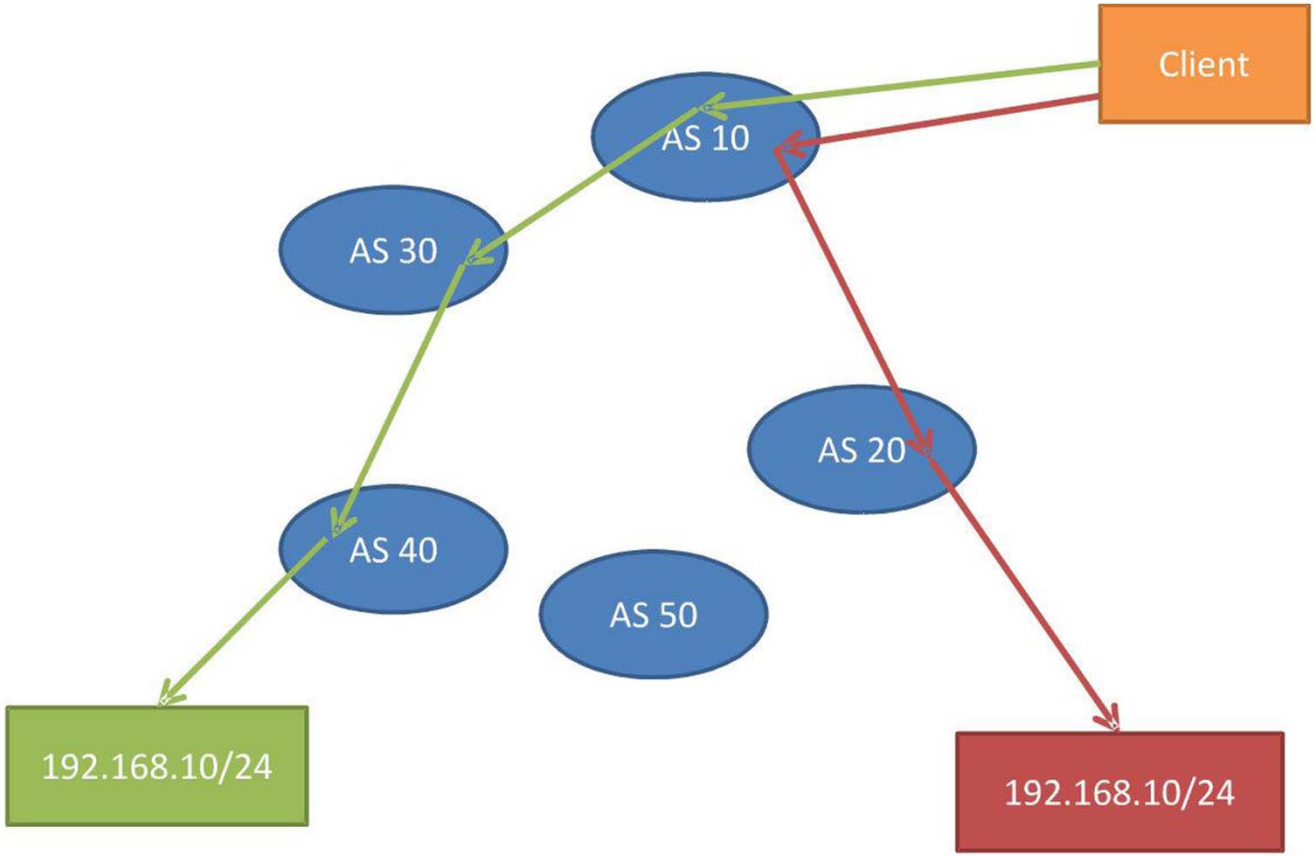
Porywanie prefiksów

- Możemy rozgłosić AS kogoś innego
- Możemy rozgłosić przestrzeń adresową należącą do kogoś innego
- W ten sposób można ściągnąć do siebie ruch „ofiary”...

  ...być może potem przekierować go nawet od właściwego odbiorcy – oczywiście po zgraniu, obejrzeniu i „zachowaniu na później”?

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

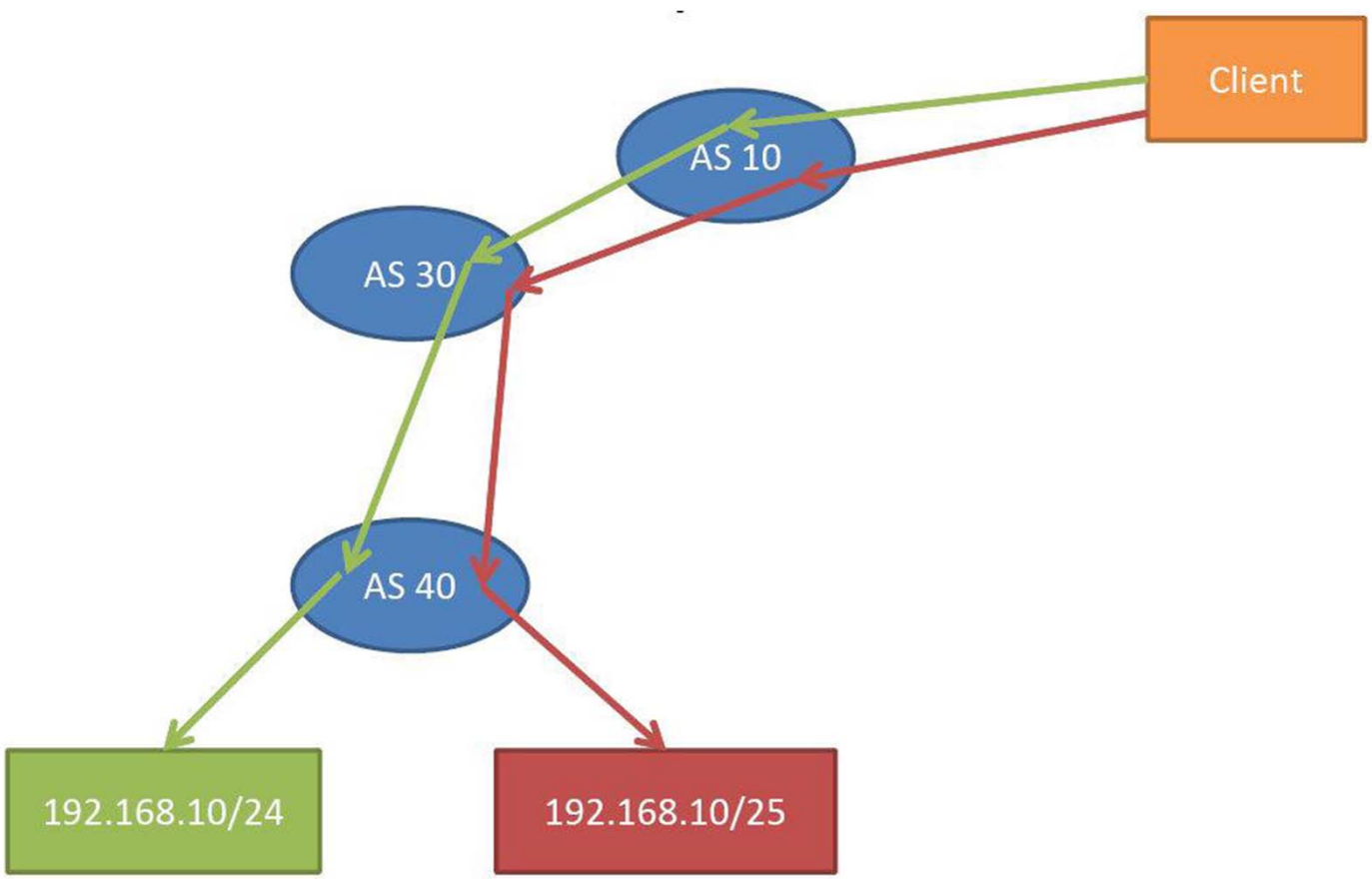
Ten sam prefiks – wygrywa krótsza AS_PATH



Źródło: prezentacja z NANOG46

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Ten sam prefiks – bardziej dokładny



Źródło: prezentacja z NANOG46

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

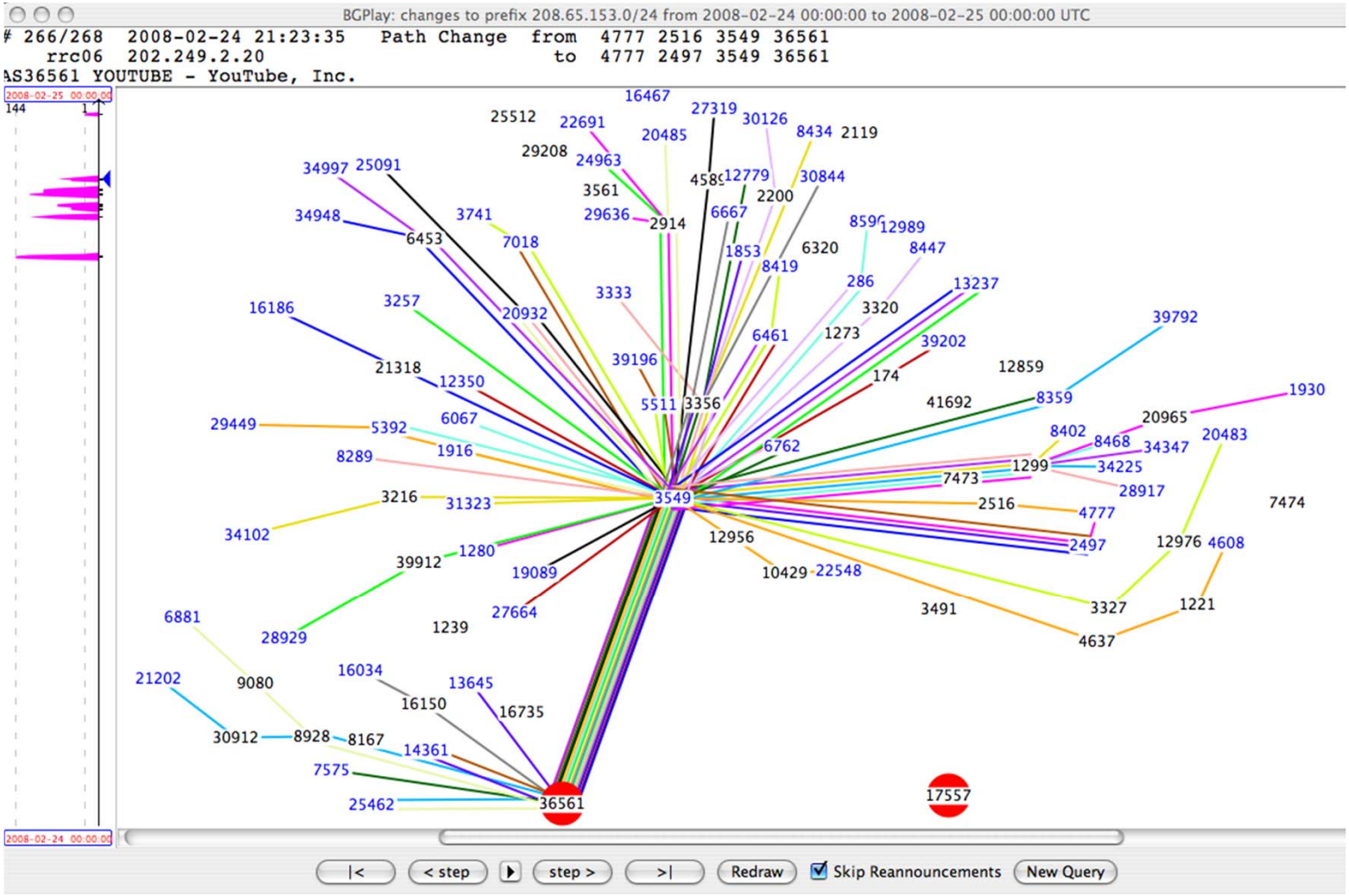
Przykłady „porywania” prefiksów

- W niedzielę, 24’ego lutego 2008 Pakistan Telecom (AS17557) rozpoczął rozgłaszanie prefiksu 208.65.153.0/24.
- Jeden z operatorów tranzytowych PT - PCCW Global (AS3491) zaakceptował i przesłał to rozgłoszenie dalej – co spowodowało „porwanie” prefiksu należącego do YouTube w większości internetu
  - Wina PT czy PCCW?
  - BGP blackholing?

http://www.ripe.net/news/study-youtube-hijacking.html

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

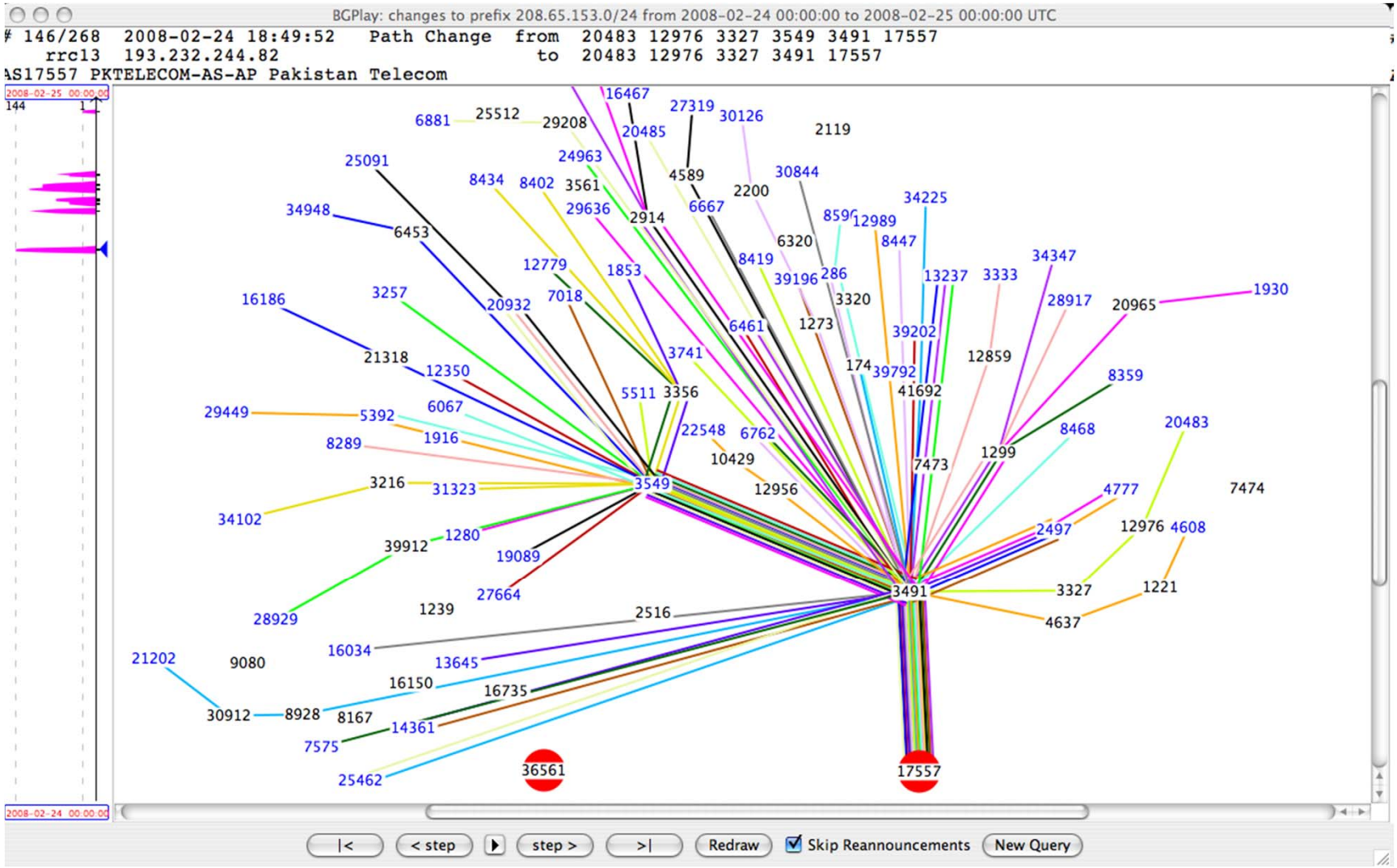
Youtube – powinno być tak



Obrazki dzięki RIPE BGPlay

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Youtube – było tak



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Rozwiązanie

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Prace standaryzacyjne

- IETF Security Inter Domain Routing WG
- Weryfikacja rozgłaszającego AS

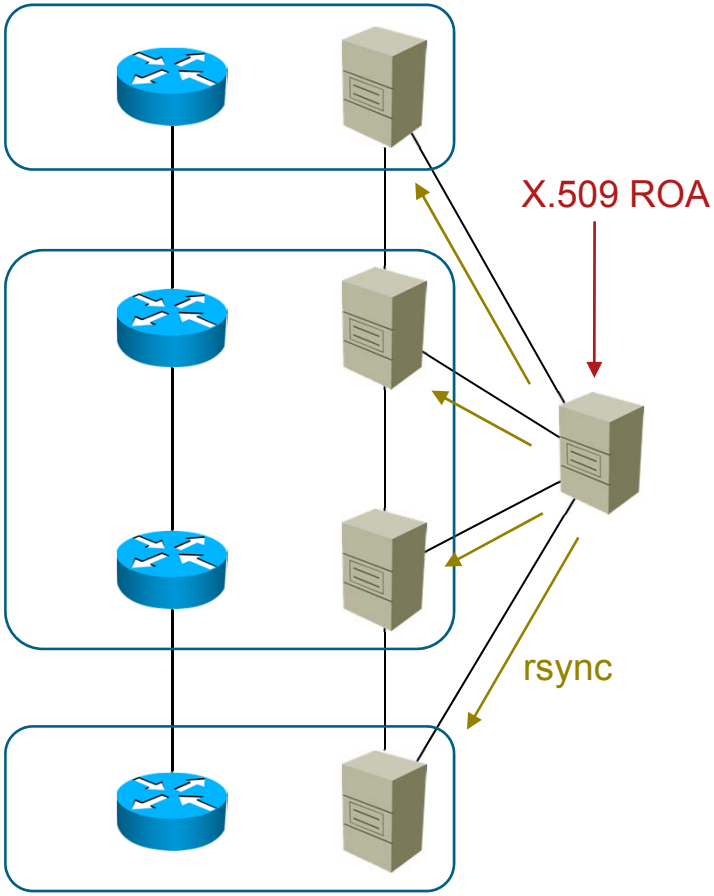
  draft-pmohapat-sidr-pfx-validate-xx.txt

  draft-ymbk-rpki-rtr-protocol-xx.txt
- Zdefiniowano infrastrukturę opartą o PKI służącą do weryfikacji „źródła pochodzenia”
  - Globalna, dystrybuowana baza autoryzowanych (prefiks<>AS) mapowań które są cyfrowo zweryfikowane
  - Router/oprogramowanie BGP wykonuje werfyikację lokalnie

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Jak zabrać się do problemu?

- Lokalna baza danych uwierzytelnionych prefiksów
  - Obecnie rozważa się bazę certyfikatów/podpisanych obiektów (ROA)
- W pamięci routera BGP prosta baza mapowań prefiksów na AS
- BGP powinno sprawdzać tą strukturę przed zaakceptowaniem każdego prefiksu



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Przykład konfiguracji

- IOS-XR:

```
router bgp 4128
   bgp router-id 198.180.152.251
   bgp rpki cache 198.180.150.1 42420 refresh-time 600
   address-family ipv4 unicast
     bgp dampening collect-statistics ebgp
     redistribute static route-policy vb-ebgp-out
    ...
```


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Przykład weryfikacji prefiksów

- IOS-XR:

```
RP/0/5/CPU0:ios# show bgp rpki prefix-validation database
Wed Oct 19 12:54:16.812 UTC
Network          Maxlen          Origin-AS      Valid
8.0.0.0/4        6               200            Y
1.1.0.0/16       24              1              Y
3.0.0.0/24       24              2              N
4.0.0.0/8        8               3              N/A
12.0.0.0/8       24              7018           Y
20.137.0.0/21    21              4238           N
```


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Wynik weryfikacji

- Valid

  Odnaleziono mapowanie dla prawidłowego certyfikatu dla wskazanego ASN

- Invalid

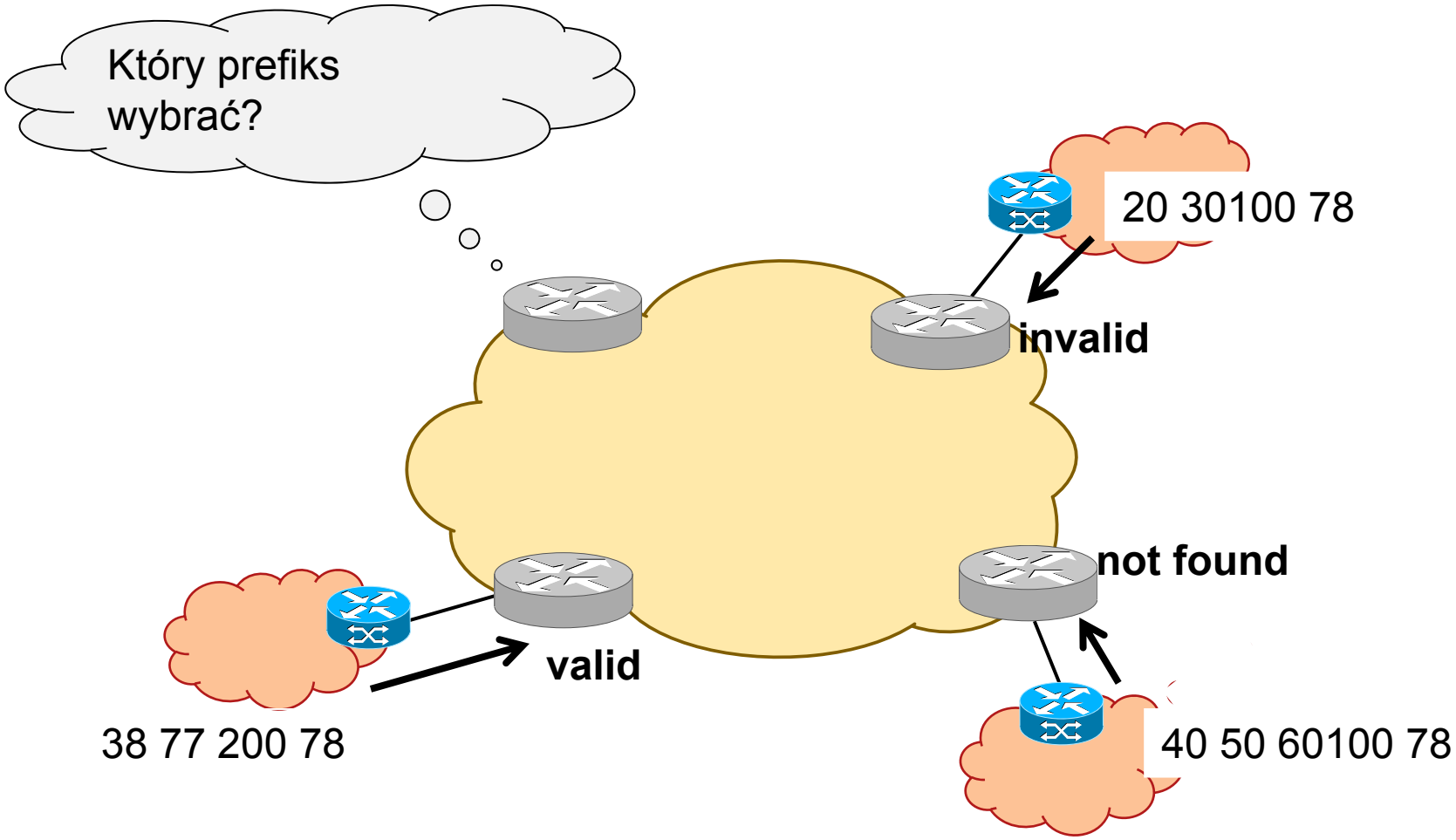
  Odnaleziono mapowanie dla certyfikatu, ale nie zgadzał się ASN lub certyfikat był nieważny

- Not found/available

  Nie odnaleziono pasującego mapowania

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Docelowe rozwiązanie



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IOS-XR – Prefiks Valid

```
RP/0/1/CPU0:r0.dfw# show bgp 192.158.248.0/24
    BGP routing table entry for 192.158.248.0/24
    Versions:
        Process bRIB/RIB SendTblVer
        Speaker 132327 132327
    Last Modified: Oct 2 01:06:47.630 for 13:33:12
    Paths: (6 available, best #3)
        Advertised to peers (in unique update groups):
                 204.69.200.26
    Path #1: Received by speaker 0
    2914 1299 6939 6939 27318
        157.238.224.149 from 157.238.224.149 (129.250.0.85)
                 Origin IGP, metric 0, localpref 100, valid, external, \
                       origin validity state: valid
                 Community: 2914:420 2914:2000 2914:3000 4128:380
    Path #2: Received by speaker 0
    ...
```


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IOS-XR – Prefiks Invalid

```
RP/0/1/CPU0:r0.dfw#sh bgp 64.9.224.0
        BGP routing table entry for 64.9.224.0/20
        Versions:
                Process bRIB/RIB SendTblVer
                Speaker 0 0
        Last Modified: Oct 2 17:38:27.630 for 4d22h
        Paths: (6 available, no best path)
                Not advertised to any peer
        Path #1: Received by speaker 0
        2914 3356 36492
                157.238.224.149 from 157.238.224.149 (129.250.0.85)
                Origin IGP, metric 2, localpref 100, valid, external,\
                        origin validity state: invalid
                Community: 2914:420 2914:2000 2914:3000 4128:380
```


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IOS-XR – konfiguracja polityki

```
route-map validity 10
     match rpki-invalid
     drop
route-map validity 20
     match rpki-not-found
     set localpref 50
```


© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Co dalej?

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Dostęp do kodu testowego IOS

- Dysponujemy kodem testowym dla IOS i IOS-XR
- Możemy udostępnić dla **celów testowych**

  będziemy chcieli poprosić o parę użytecznych informacji i oczywiście od czasu do czasu odpytać o stabilność ☺

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

RIPE NCC – Narzędzie do weryfikacji

RIPE NCC RIPE NETWORK COORDINATION CENTRE

Site Search | Search

RIPE Labs | Log In | Register

Home • Users • Data Repository • RIPE Database • About

You are here: Home > Users > Amanda Gowland > RIPE NCC Validator for Resource Certification

RIPE NCC Validator for Resource Certification

— filed under: tools, routing, certification

Amanda Gowland — 20 August 2010 10:10

1 tweet retweet

Resource certification can be used to help secure routing. The resource certification system is based on Public Key Infrastructure (PKI) principles. The RIPE NCC Validator for resource certification can help network operators make the necessary routing decisions. You can download the tool below.

Resource Certification
On 1 January 2011, all five Regional Internet Registries (RIRs) will deploy a system that can issue digital certificates along with the assignment or allocation of Internet number resources (IPv4 and IPv6 addresses, as well as Autonomous System Numbers). These "resource certificates" will certify that the holder of the certificate has been officially assigned or allocated the particular resource. The resource certification system is based on Public Key Infrastructure (PKI) principles.

Resource certification can be used to help secure routing. The system will allow holders of Internet resources to sign cryptographically verifiable messages that can help humans or

RIPE NCC Validator for Resource Certific...

RIPE NCC RPKI Validator - ZIP

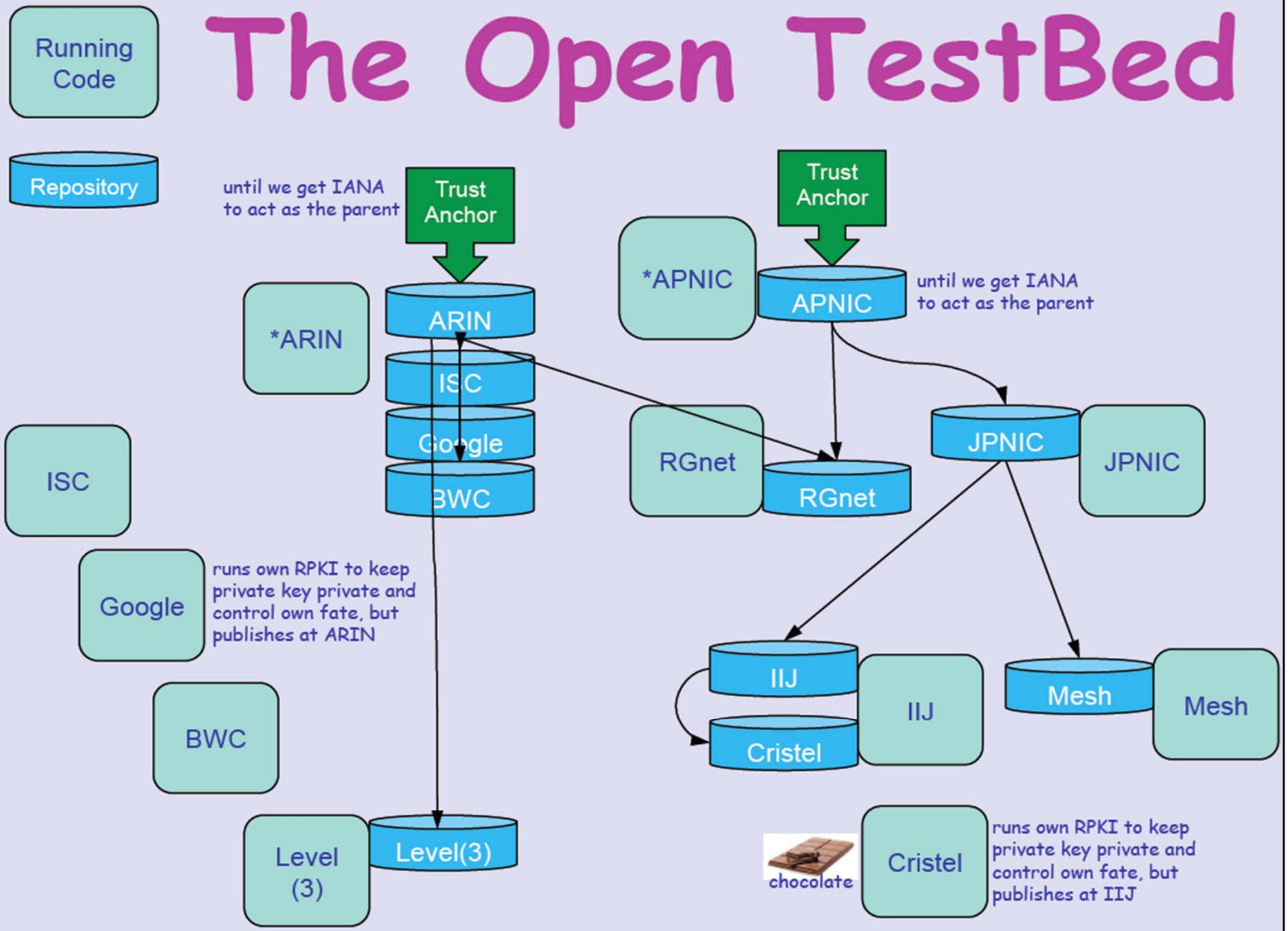
tag cloud

api apnic arin asns cpe dns dnssec database

http://labs.ripe.net/Members/agowland/ripe-ncc-validator-for-resource-certification

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Open TestBed



* APNIC and ARIN are simulations constructed from public data

Q&A

CISCO