Jak skonfigurować open peering TPIX?

Konfiguracja krok po kroku po stronie uczestnika i Orange

Piotr Siemdaj
Konrad Plich

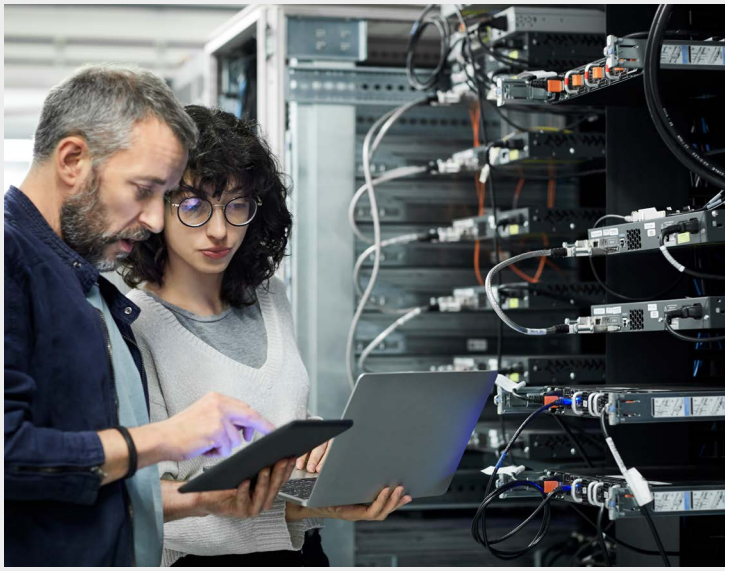
orange™

Dla operatorów

Punkty, czy też platformy wymiany ruchu internetowego (ang. Internet eXchange Point, IXP) pozwalają na wygodną wymianę ruchu z ogromną bazą uczestników. W tym gronie jest także wielu znaczących dostawców treści.

Skorzystanie z open peeringu wymaga, poza fizycznym połączeniem sieci, posiadania własnego numeru ASN (Autonomous System Number) i zestawienia sesji za pomocą protokołu BGP (Border Gateway Protocol).

Konfiguracja połączenia jest bardzo podobna w przypadku praktycznie każdego IX. W naszym e-booku pokazujemy, jak można skonfigurować wymianę ruchu w ramach platformy TPIX. Dowiesz się, jak zestawić sesję BGP pomiędzy swoim routerem a route serverem Orange, na podstawie której wymieniane są informacje routingowe.



Czym jest open peering TPIX?

W odniesieniu od modelu OSI można uznać, że open peering to pojedyncza, szeroka domena broadcastowa L2, do której podłączone są routery wszystkich uczestników. Zatem urządzenia te w swoich tablicach ARP posiadają wpisy bezpośrednio wskazujące na wszystkie pozostałe routery. Rozwiązanie to zasadniczo różni się od, np. klasycznych połączeń tranzytowych, w których vlan skonfigurowany jest wyłącznie pomiędzy routerem dostawcy i klienta, a interfejsy zaadresowane są wąską adresacją połączeniową /30 lub /31 pod zestawienie sesji eBGP.

Adresowanie IP oraz route servery

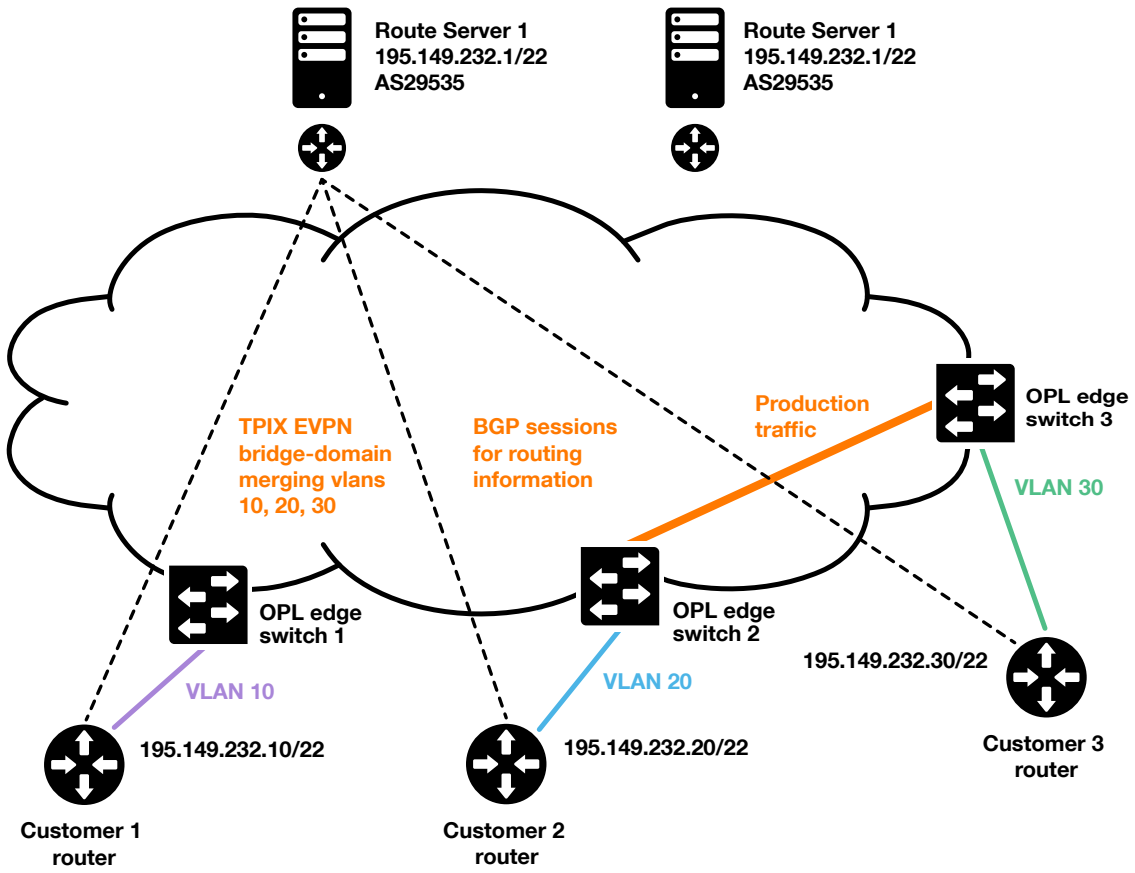
W open peeringu każdemu uczestnikowi przypisany jest adres z szerokiej klasy /22. Uczestnicy mogą wymieniać się routingiem bezpośrednio pomiędzy sobą, chociażby poprzez zestawienie bezpośrednich sesji BGP, jednak w szczególności każdy z nich powinien nawiązać sesję eBGP i rozgłosić swoje prefixy do route serverów TPIX:

- **RS1: 195.149.232.1**
- **RS2: 195.149.233.1**
- **AS29535**

Głównym zadaniem route serverów jest wymiana NLRI (Network Layer Reachability Information), czyli listy prefiksów pomiędzy uczestnikami. Nie jest zatem konieczne, aby zestawiali oni wiele sesji BGP pomiędzy sobą (full mesh) – wystarczą dwie sesje eBGP do RS TPIX.

Warto zaznaczyć, że ruch produkcyjny nie przechodzi przez route servery lecz kierowany jest bezpośrednio na interfejs uczestnika, dla którego został wskazany next-hop.

Ponadto, w atrybucie AS-PATH pośredni AS29535 jest ukrywany. W rezultacie uczestnik open peeringu „widzi” prefixy innego uczestnika bezpośrednio w AS-PATH. Zabieg ten w naturalny sposób przesuwa ruch w stronę IX względem, najczęściej droższych, łączy tranzytowych.



Realizacja usługi klienckiej

Zasięg transportowych sieci Orange – Metro Ethernet / Carrier Ethernet – jest ogólnopolski. Za ich pomocą realizowane jest połączenie vlan od routera klienta do najbliższego, dostępowego switcha TPIX/IPMPLS – standardowo do najbliższego miasta wojewódzkiego.

Jak skonfigurować uczestnika open peeringu?

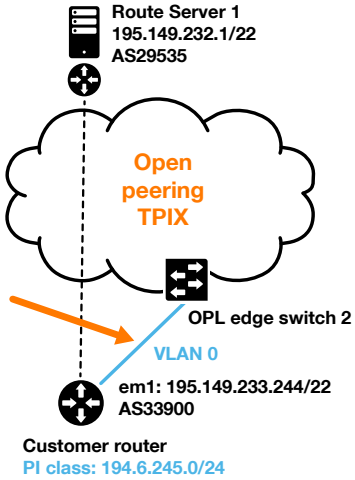
Konfiguracja krok po kroku:

1. **Zestawienie połączenia do platformy TPIX**
2. **Konfiguracja routera po stronie uczestnika i Orange**
3. **Kwarantanna**
4. **Przeniesienie do produkcji**
5. **Uzupełnienie baz danych**

Konfiguracja po stronie Orange i uczestnika

Dla omawianego przykładu konfiguracji usługi open peering po stronie uczestnika, wykorzystaliśmy router Juniper w wersji Junos OS 21. Tym niemniej koncepcja konfiguracji interfejsu, vlan, protokołu BGP wraz z politykami import/export, jest podobna dla różnych producentów urządzeń.

1. Konfiguracja interfejsu i subinterfejsu w stronę Orange



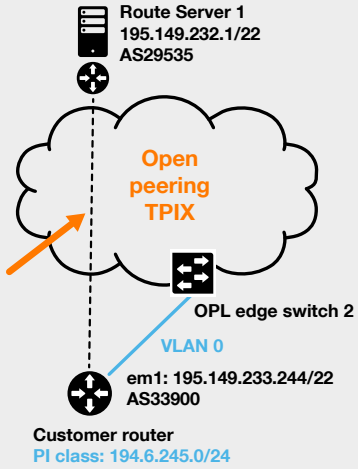
Dla uproszczenia uznajemy, że połączenie pomiędzy routerem klienta a dostępowym switchem Orange realizowane będzie w oparciu o połączenie nietagowane – uczestnik odbiera pojedynczy serwis IX na całym interfejsie skonfigurowanym jako acces, unit 0. Oczywiście dopuszczamy realizację usługi na porcie trunk, jako kolejne połączenie vlan obok innych usług.

Klient otrzymał adres połączeniowy 195.149.233.244/22 a konfiguracja subinterfejsu zobrazowana jest poniżej.

```
siemdpio@vrr-rko> show configuration logical-systems LS-TPIX
interfaces
em1 {
        unit 0 {
                family inet {
                        filter {
                                input FF-V4-PROTECT-IN;
                        }
                        address 195.149.233.244/22;
                }
        }
}
```

Poprawnie skonfigurowany interfejs na routerze L3 Juniper nie będzie wysyłał niedozwolonych protokołów, o których pisaliśmy w poprzednim punkcie.

2. Konfiguracja protokołu BGP



Konfigurację sąsiedztwa BGP w stronę obu route serverów należy wykonać w hierarchii „protocols bgp group”, nadając odpowiednią nazwę grupy oraz definiując dwóch neighborów, tj. adresy IP obu route serverów.

Na poniższej ilustracji widoczny jest odpowiedni fragment konfiguracji. Najważniejsze i wymagane parametry to:

- type external; sesje do route serverów to sesje eBGP,
- peer-as 29535; ASN TPIX,
- wspólna polityka importu oraz exportu dla obu sesji,
- local-address 195.149.233.244, czyli adres przydzielony od Orange,
- w hierarchii routing-options autonomous-system skonfigurowano lokalny ASN jako 33900. W tym miejscu zrezygnowano z konfiguracji router-ID, zostawiając ten parametr domyślny.

```
siemdpio@vrr-rko> show configuration logical-systems LS-TPIX
protocols bgp
group BGP-V4-RS {
        type external;
        description "RS Openpeering TPIX IPv4";
        local-address 195.149.233.244;
        family inet {
                unicast;
        }
        export TO-TPIX-OPENPEERING;
        neighbor 195.149.232.1 {
                description RS1;
                import FROM-TPIX-OPENPEERING;
                peer-as 29535;
        }
        neighbor 195.149.233.1 {
                description RS2;
                import FROM-TPIX-OPENPEERING;
                peer-as 29535;
        }
}
```

3. Konfiguracja polityk BGP import / export

Konfiguracja polityki BGP import: „loose policy”

Uczestnik może filtrować prefixy otrzymywane ze strony route serverów na podstawie as-set RIPE: AS29535:AS-TPIX. Jeżeli z pewnych powodów nie chce lub nie może tworzyć na routerze prefix listy zawierającej dużo rekordów, można zastosować tzw. „loose policy” na sesji TPIX open peering.

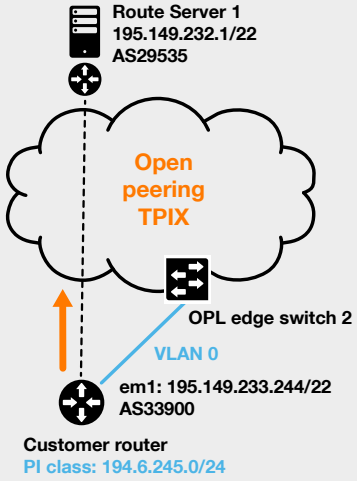
Zgodnie z zaleceniami RFC7454 (BCP-BGP Operations and Security) zaakceptowane mogą zostać wszystkie prefixy z wyjątkiem:

- prefiksów, które nie powinny pojawić się w publicznej sieci Internet (REJECT-MARTIANS), np. prefixy private use, muliticast, link local,
- swoich własnych prefixów, należących do local-as (REJECT-MYPREFIXES),
- default route (REJECT-DEFAULT),
- prefixów, które są za wąskie. Dobrą praktyką jest odrzucenie wszystkich prefixów krótszych od /24 (TOO-SPECIFIC).

Po prawej przykład polityki importu, która może być zastosowana na routerze uczestnika. Uwzględniono w niej wyżej wymienione nazwy termów.

```
siemdpio@vrr-rko> show configuration logical-systems LS-TPIX
policy-options policy-statement FROM-TPIX-OPENPEERING
term REJECT-MARTIANS {
        from {
                prefix-list-filter PFX-V4-MARTIANS orlonger;
        }
        then reject;
}
term REJECT-MYPREFIXES {
        from {
                prefix-list-filter PFX-V4-MYPREFIXES orlonger;
}
        then reject;
}
term REJECT-DEFAULT {
        from {
                route-filter 0.0.0.0/0 exact;
        }
        then reject;
}
term TOO-SPECIFIC {
        from {
                route-filter 0.0.0.0/0 upto /24;
        }
        then accept;
}
term END {
        then reject;
}
```

Konfiguracja polityki eksportu



Polityka exportu w stronę route serverów jest prosta. W analizowanym przypadku uczestnik TPIX powinien rozgłosić wyłącznie swój prefix, czyli 194.6.245.0/24 (należący do prefix-listy PFX-V4-MYPREFIXES).

Po prawej przykład implementacji polityki exportu.

```
siemdpio@vrr-rko> show configuration logical-systems LS-TPIX
policy-options policy-statement TO-TPIX-OPENPEERING
term MY-PREFIXES {
        from {
                prefix-list-filter PFX-V4-MYPREFIXES exact;
        }
        then accept;
}
term REJECT {
        then reject;
}
```

4. Weryfikacja stanu sesji BGP oraz propagacji informacji routingowych

Weryfikacja drożności L2/L3 po przeniesieniu usługi do produkcji

Po przeniesieniu przez Orange usługi do produkcji, router uczestnika powinien zbudować tablicę ARP zawierającą połączeniowe adresy IP oraz MAC adresy routerów wszystkich innych uczestników TPIX, w tym route serverów.

Router uczestnika:

```
siemdpio@vrr-rko> show arp no-resolve logical-system LS-TPIX
MAC Address          Address             Interface           Flags
6a:b6:8b:08:d4:27    195.149.232.1       em1.0               none
64:64:9b:6a:e0:f0    195.149.232.5       em1.0               none
f4:b5:2f:72:57:f0    195.149.232.7       em1.0               none
cc:ed:4d:56:26:40    195.149.232.9       em1.0               none
3c:2c:30:0b:80:82    195.149.232.11      em1.0               none
08:4f:a9:dc:ce:dd    195.149.232.13      em1.0               none
c0:d6:82:36:16:b5    195.149.232.14      em1.0               none
9c:e0:41:69:61:60    195.149.232.15      em1.0               none
                              ...
Total entries: 390
}
```

Po stronie Orange, route server TPIX wpisze do tablicy ARP MAC adress oraz IP uczestnika. Weryfikacja ping ostatecznie potwierdza drożność połączenia.

Route Server TPIX:

```
[siemdpio@tpix_rsl_kaz ~]$ arp -a | grep 195.149.233.244
? (195.149.233.244) at 66:d2:60:b1:43:99 [ether] on ens19
[siemdpio@tpix_rsl_kaz ~]$ ping 195.149.233.244
PING 195.149.233.244 (195.149.233.244) 56(84) bytes of data.
64 bytes from 195.149.233.244: icmp_seq=1 ttl=64 time=1.22 ms
64 bytes from 195.149.233.244: icmp_seq=2 ttl=64 time=1.31 ms
64 bytes from 195.149.233.244: icmp_seq=3 ttl=64 time=1.02 ms
```

Weryfikacja stanu sesji BGP

Zarówno route server TPIX jak i router BGP uczestnika odnotowały stan sesji BGP jako pożądany stan „Established”.

Na ilustracji zaznaczone są informacje warte uwagi takie jak: stan sesji BGP, local oraz remote IP/ASN, polityki import/export przypisane do neighbora TPIX.

Router uczestnika:

```
siemdpio@vrr-rko> show bgp neighbor 195.149.232.1 logical-system
LS-TPIX
Peer: 195.149.232.1+179 AS 29535 Local: 195.149.233.244+50646 AS
33900
Description: RS1
Group: BGP-V4-RS1          Routing-Instance: master
Forwarding routing-instance: master
Type: External             State: Established        Flags: <Sync>
Last State: OpenConfirm            Last Event: RecvKeepAlive
Last Error: None
Export: [ TO-TPIX-OPENPEERING ] Import: [ FROM-TPIX-OPENPEERING ]
Options: <LocalAddress AddressFamily PeerAS Refresh>
Options: <GracefulShutdownRcv>
Address families configured: inet-unicast
Local Address: 195.149.233.244 Holdtime: 90 Preference: 170
Graceful Shutdown Receiver local-preference: 0
Number of flaps: 0
Peer ID: 195.149.232.1     Local ID: 194.6.245.33     Active
Holdtime: 90
Keepalive Interval: 30     Group index: 0    Peer index: 1
SNMP index: 0
```

Route Server TPIX:

```
[siemdpio@tpix_rsl_kaz ~]$ birdc show protocols R233_244
BIRD 1.6.8 ready.
Access restricted
name       proto      table    state      since         info
R233_244   BGP        T33800   up         2023-09-12    15:44:16
Established
```

Weryfikacja propagacji informacji routingowych

Router uczestnika:

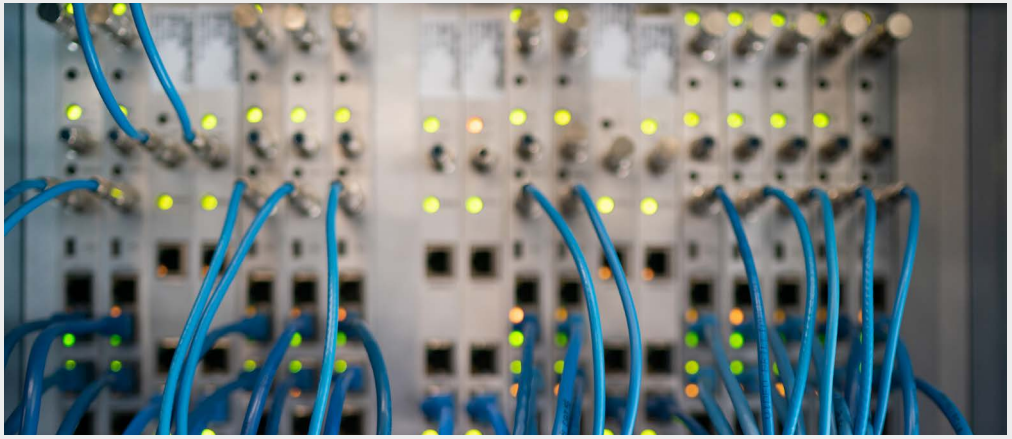
```
siemdpio@vrr-rko> show route receive-protocol bgp 195.149.232.1
logical-system LS-TPIX | count
Count: 119829 lines
```

Router uczestnika otrzymuje od strony route servera TPIX informacje o około 120 tysiącach prefixów IPv4, co jest pożądaną wartością dla usługi open peering. Nie jest to pokazane na powyższej ilustracji, jednak otrzymywane prefixy w atrybucie AS-PATH mają ukryty AS TPIX AS29535.

Route Server TPIX:

```
[siemdpio@tpix_rsl_kaz ~]$ birdc show route protocol R233_244
table T33900
BIRD 1.6.8 ready.
Access restricted
194.6.245.0/24    via 195.149.233.244 on ens19 [R233_244 2023-09-
12 15:44:16] * (100) [AS33900i]
```

Route server TPIX otrzymuje pojedynczy prefix /24 należący do uczestnika. Prefix ma poprawny AS-PATH, jest akceptowany i wybierany. Potwierdza to poprawną konfigurację polityki export na routerze klienta.

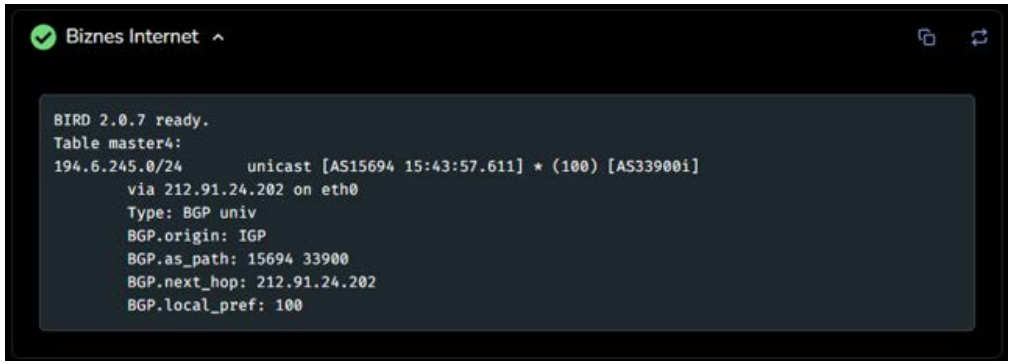


Weryfikacja propagacji informacji routingowych – Looking Glass

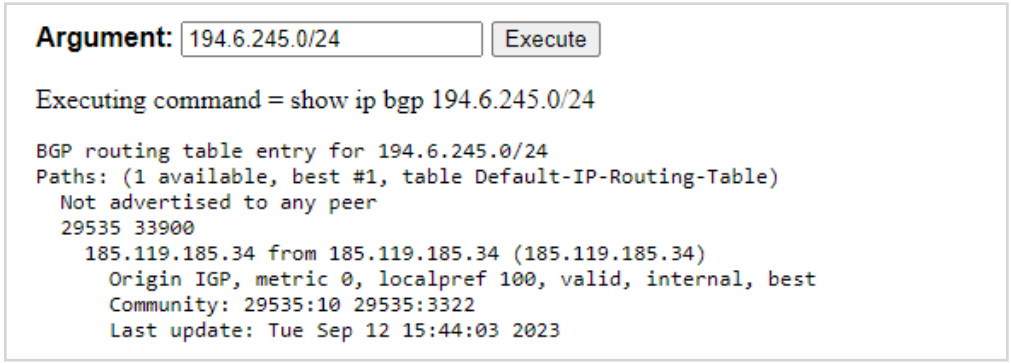
Do weryfikacji poprawności rozgłaszania informacji routingowych można wspomóc się narzędziami Looking Glass udostępnionymi przez innych uczestników TPIX. W analizowanym przypadku wybrano LG: Atman oraz Actus.

Na załączonej ilustracji widać, że w przypadku Atmana, prefix jest osiągany bezpośrednio przez open peering, jednak w przypadku Actus w AS-PATH widnieje AS29535 (TPIX). Wynika to stąd, że w chwili wykonywania testu Actus miał rozłączone sesje BGP z route serverami i prefix był widoczny na łączu tranzytowym Internet.optimum (także terminowanym w AS29535).

Atman:



Actus:



Zanim zostaniesz uczestnikiem open peering

Zanim zaczniesz korzystać z usługi wykonujemy jeszcze dwa działania:

1. Kwarantanna

W tym kroku vlan kliencki znajduje się w routing-instance kwarantanny. Sesje BGP z route serverami jeszcze się nie zestawią. Po odebraniu vlanu IX i zaadresowaniu subinterfejsu adresacją /22, uczestnik proszony jest o wyłączenie protokołów innych niż IPv4, IPv6, ARP. Następnie rozpoczyna się monitoring ruchu otrzymywanego na tym połączeniu i jeżeli na tym vlanie uczestnik nie wysyła w stronę Orange „zakazanych" pakietów, wówczas można przejść do kolejnego kroku.

2. Przeniesienie do produkcji

Po pomyślnych testach w kwarantannie, VLAN open peeringowy przenoszony jest do routing-instance produkcyjnej. Router kliencki widzi już pełną tablicę ARP wraz z wpisami odpowiadającymi wszystkim innym uczestnikom oraz adresy IP route serverów, do których może zestawić sesje BGP i rozgłosić swoje prefixy.

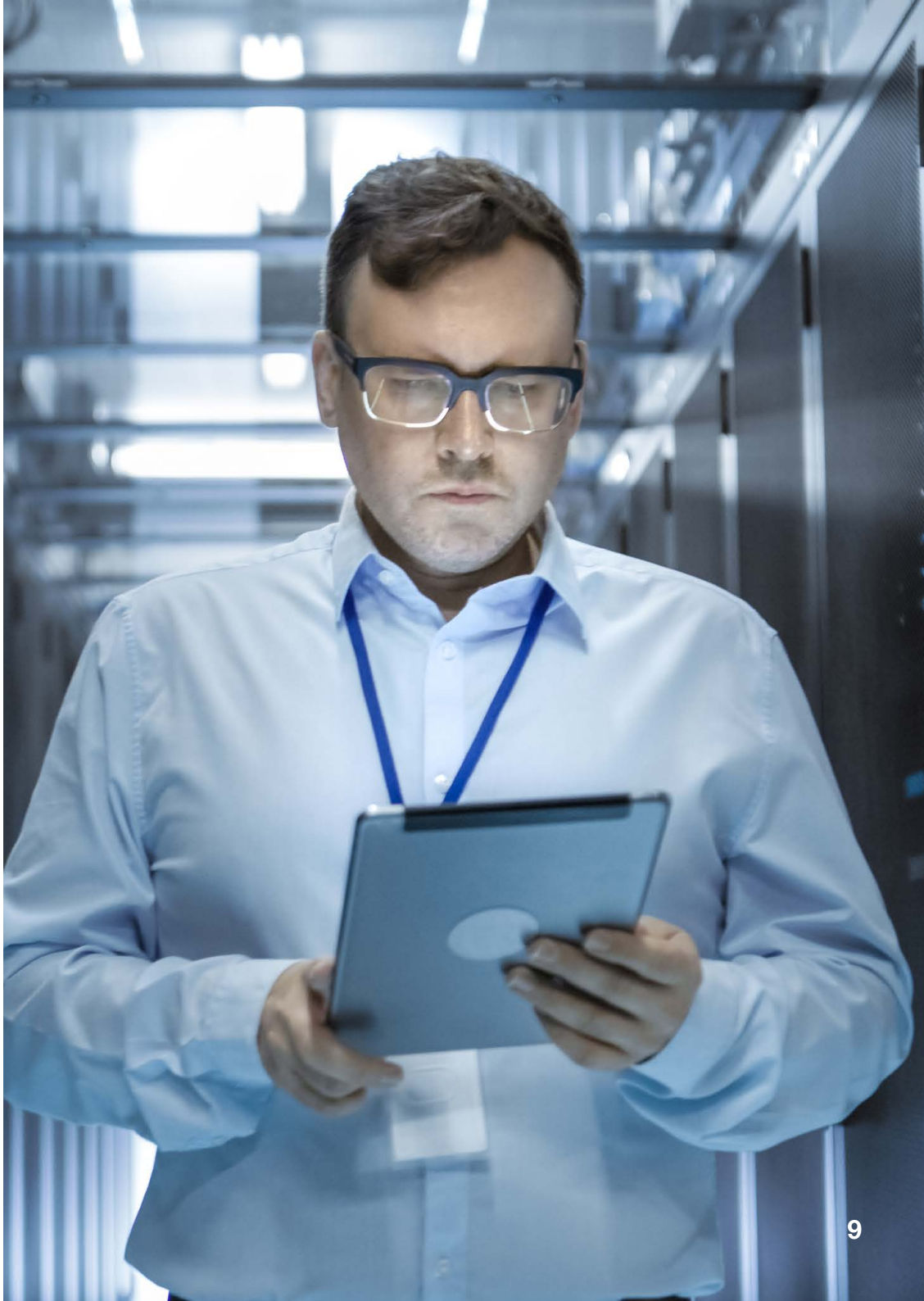
Dla zabezpieczenia przed tworzeniem się pętli w L2, w open peeringu TPIX stosujemy następujące mechanizmy zabezpieczające:

- Jeden dozwolony MAC address routera uczestnika dla pojedynczego vlanu open peeringowego (wpisany „na sztywno" w ACL po stronie Orange).
- Filtr na subinterfejsie – dopuszcza jedynie pakiety protokołów IPv4, IPv6 i ARP od uczestnika.
- MAC learning = 1 – ograniczenie tylko do jednego adresu MAC, tak by wykluczyć zwrotne zaczytanie wszystkich adresów na pojedynczym subinterfejsie uczestnika.
- MAC pinning – funkcjonalność, dzięki której w sytuacji, gdy tablica ARP nauczyła się konkretnego adresu MAC na danym interfejsie, to jeżeli ten sam adres MAC pojawi się na innym interfejsie, a pierwszy jeszcze nie wygasł, dropowany będzie nowy adres MAC, tak aby uniknąć kolizji adresów.

W warstwie IP:

- Akceptujemy tylko prefixy należące do ASN uczestnika i ewentualnie do operatorów, których tranzytuje w ramach as-set (RFC 7454).
- RPKI: walidacja obiektów ROA (planowane wdrożenie akceptacji prefixów ze statusem valid oraz unknown w 2024).

Co jeszcze warto wiedzieć?



Dodatkowe, potencjalne przydatne funkcjonalności

Jeżeli nie chcesz aby Twoje prefixy były rozgłaszane do innego, konkretnego uczestnika, wystarczy, że rozgłosisz prefixy oznaczone community 0:ASN.

Poniżej zaprezentowano implementację polityki exportu, tak aby prefix nie był rozgłaszany do Atmana. Pełną listę udostępnionych community w TPIX można w prosty sposób znaleźć w bazie RIPE dla rekordu AS29535.

```
siemdpio@vrr-rko> show configuration logical-systems
LS-IPIX policy-options policy-statement TO-TPIX-
OPENPEERING term MY-PREFIXES
from {
       prefix-list-filter PFX-V4-MYPREFIXES exact;
}
then {
       community add NO-ATMAN;
       accept;
}
siemdpio@vrr-rko> show configuration logical-systems
LS-TPIX policy-options community NO-ATMAN
members 0:15694;
```

BFD na sesji z route serverami

W TPIX wspieramy funkcjonalność BFD na sesjach z route serverami. Na życzenie możemy skonfigurować taką sesję domyślnie z parametrami 5x500 ms.

Poniżej zamieszczony jest przykład konfiguracji na klienckim Juniperze. Całkowitą konfigurację wykonuje się dla konkretnego BGP neighbora w odpowiedniej grupie dla protocols bgp.

Zalecane parametry to 5x500 ms

```
siemdpio@vrr-rko> show configuration logical-systems LS-TPIX protocols bgp group
BGP-V4-RS neighbor 195.149.232.1
description RS1;
import FROM-TPIX-OPENPEERING;
peer-as 29535;
bfd-liveness-detection {
       minimum-receive-interval 500;
       multiplier 5;
       transmit-interval {
              minimum-interval 500;
       }
}
```

```
siemdpio@vrr-rko> show bfd session
                                                  Detect  Transmit
Address                  State   Interface        Time    Interval        Multiplier
195.149.232.1            Up      eml.0            3.000    0.500              5
```

rs1_kaz: show bfd sessions

Search: 233.244

IP address	State	Since	Interval	Timeout
195.149.233.244	Up	2023-09-29 13:50:56	0.500	2.500

Rejestracja w IRR oraz PeeringDB

Prefixy, które rozgłasza klient powinny mieć odpowiednie wpisy w IRR (w przypadku Europy jest to RIPE) oraz PeeringDB. Tylko w ten sposób można zagwarantować, że będą one akceptowane i poprawnie rozgłaszane w open peeringu.

RIPE:

```
route:          194.6.245.0/24
descr:          TP IPVPN
descr:          for abuse: abuse@tpnet.pl
origin:         AS33900
mnt-by:         AS5617-MNT
created:        2004-11-03T15:15:00Z
last-modified:  2004-11-16T10:46:52Z
source:         RIPE
```

PeeringDB (https://www.peeringdb.com/ix/482):

Peers at this Exchange Point

Filter

Peer Name IPv4	ASN IPv6	Speed	Policy
"Info-Net" Uslugi Teleinformatyczne S.C. 195.149.232.207	48712	1G	Open
Actus 195.149.233.161	197790	10G	Open
Agora 195.149.232.33	8535 2001:7f8:27::8535:1	10G	Open

Wpis w IRR (Internet Routing Registry), RIPE

Rozgłaszany prefix powinien mieć w RIPE utworzony odpowiedni obiekt route wskazujący na ASN operatora. Przykład odpowiedniego rekordu dla adresacji 194.6.245.0/24 można znaleźć na grafice powyżej. W TPIX nasz prefix-automat filtruje prefixy wejściowe właśnie po obiektach route z RIPE.

Dopisanie peeringu w TPIX w PeeringDB

Po przeniesieniu usługi do produkcji uczestnik proszony jest o dopisanie się jako uczestnik TPIX w PeeringDB. Odpowiedni rekord można znaleźć na stronie: **https://www.peeringdb.com/ix/482**

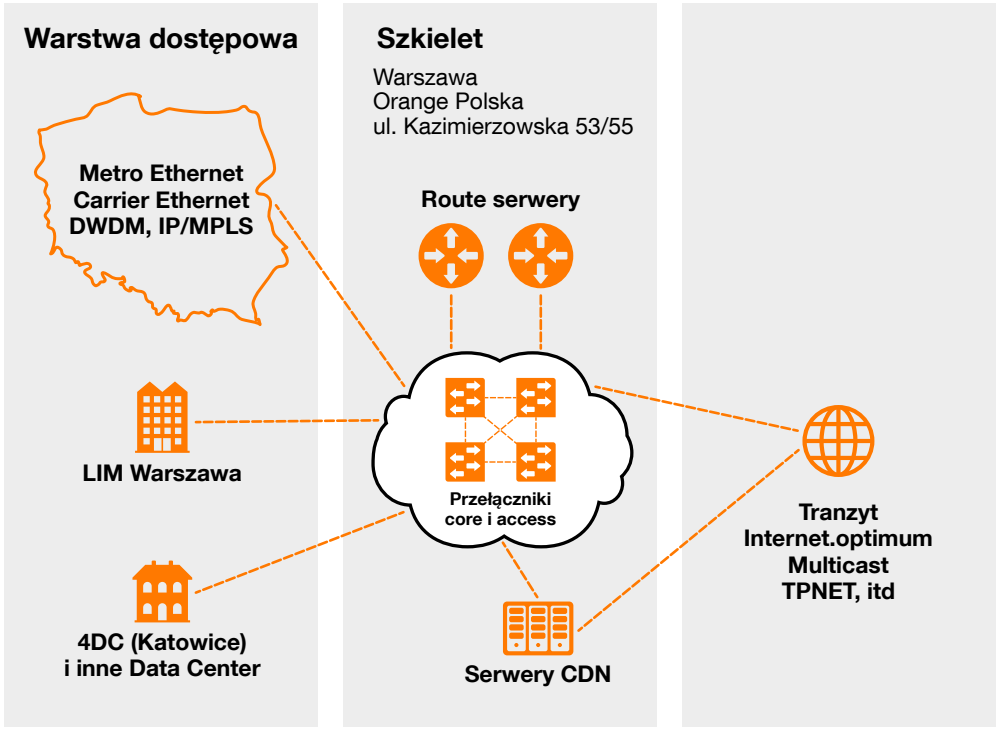
Utworzenie obiektów ROA dla swoich prefiksów w RPKI

W celu dodatkowej protekcji przed niepożądanym działaniem Route Hijackingu sugerujemy, aby dla prefixów rozgłaszanych w open peeringu, utworzyć obiekty ROA w RPKI. W 2024 roku planujemy wdrożyć walidację prefixów otrzymywanych od klientów w TPIX właśnie po RPKI. Na początku akceptowane będą rekordy VALID i UNKNOWN jednak docelowo zaakceptujemy jedynie prefixy VALID.

TPIX – nie tylko open peering

Dostęp do platformy TPIX można zrealizować na wiele sposobów. Wybór zależy przede wszystkim od Twoich potrzeb, możliwości, zasobów i lokalizacji.

Topologia TPIX

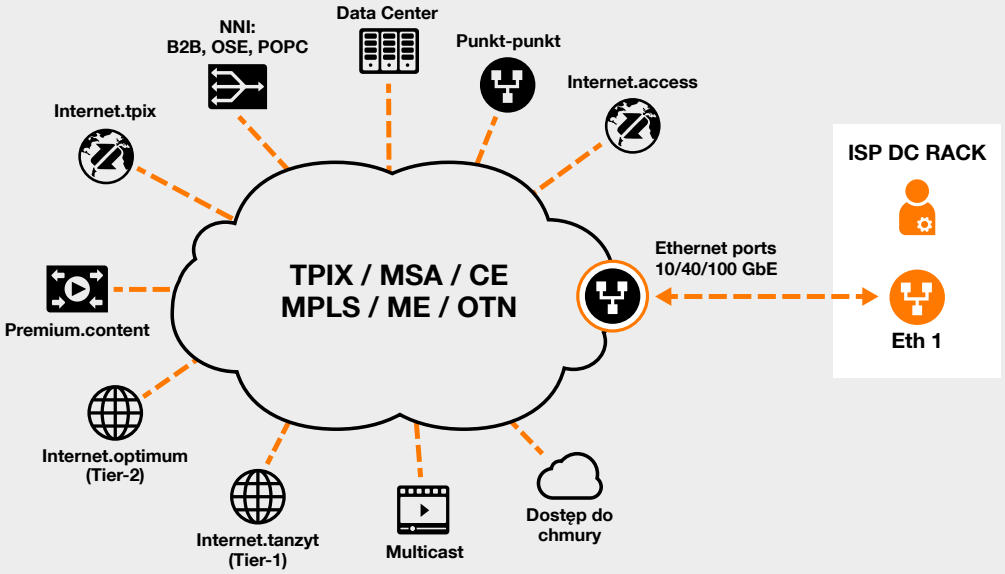


TPIX to nie tylko open peering, czyli możliwość wymiany ruchu z ogromną bazą uczestników oraz znaczącymi dostawcami treści (CSP). Korzystając z naszej platformy możesz uzyskać dostęp do m.in.:

- Multicast TV,
- peeringu z TPNET AS5617,
- NNI do innych operatorów,
- usług Orange Polska (dostęp do internetu, połączenie punkt-punkt i wiele innych).

Usługi te realizowane są jako dodatkowy VLAN na tym samym porcie. VLAN dostarczamy też do dowolnych lokalizacji w Polsce na bazie usług Transmisji danych Orange Polska (port Ethernet).

Warstwa dostępowa TPIX
Ogólnopolski Ethernet Orange Polska



Zalety

- **Wiele usług na jednym porcie**
- **Optymalizacja kosztów**
  - jeden łącznik
  - jeden port
  - mniej hardware'u
  - mniejsze zużycie energii
- **Możliwość dodawania nowych VLAN**, np. dostęp do chmury, kontent

Unikalny content w open peering TPIX

Zestawienie bezpośredniej wymiany ruchu ze znaczącymi dostawcami treści obecnymi na platformie TPIX pozwala zwiększyć ruch w open peeringu oraz poprawić jakość i zmniejszyć koszty zakupu usług tranzytowych. Bliskość źródeł treści i możliwość z nich skorzystania ma także olbrzymie znaczenie dla użytkownika końcowego.

Stale powiększamy liczbę i jakość źródeł w ramach platformy TPIX. Część z nich nie wykorzystuje połączeń do route servera TPIX, przez co ich ruch nie pojawia się automatycznie na połączeniu uczestnika z open peering TPIX.

Aby wymienić ruch z danym dostawcą treści konieczne jest zestawienie z nim prywatnej sesji BGP, zgodnie z jego polityką peeringową. Sesje zestawiamy na bazie tego samego VLAN open peering, na którym uczestnik ma sesję BGP z route serverami TPIX i wymienia ruch z typowymi uczestnikami TPIX.

Warto przy tym pamiętać o rejestracji w PeeringDB. Niektórzy z dostawców treści mogą bowiem odmówić niezarejestrowanym podmiotom prośbie o prywatną sesję BGP.

Szczegółowe informacje na temat zestawienia private peeringu zamieszczamy w serwisie TPIX, na stronie **Konfiguracja usług**
link: https://hurt-orange.pl/tpix/informacje-techniczne/konfiguracja-uslug/#private-peering

Znaczący dostawcy treści na platformie TPIX

aws amazon CLOUDFLARE Google Limelight NETWORKS Microsoft Meta

Słowniczek

Adres MAC (Media Access Control Address) – adres warstwy łącza danych, który jest wymagany dla każdego portu lub urządzenia podłączonego do LAN.

ASN (Autonomous System Number) – numer systemu autonomicznego identyfikujący grupę adresów IP rozgłaszanych w jednakowy sposób w protokole routingu dynamicznego BGP.

ARP (Address Resolution Protocol) – zawiera adresy IP komputerów skojarzone z ich adresami fizycznymi MAC i jest wykorzystywany w komunikacji z innymi urządzaniami (np. routerami) połączonymi w sieci.

AS-PATH – lista numerów AS, przez które trzeba przejść aby dostać się do prefiksu.

BFD (Bidirectional Forwarding Detection) – autonomiczny protokół pracujący w oderwaniu od technologii transportujących pakiety, wykorzystywany np. do monitorowania poprawności pracy różnego typu transportu danych.

eBGP – sesja BGP nawiązana między dwoma różnymi AS.

iBGP – sesja BGP nawiązana między dwoma routerami brzegowymi w obrębie jednego AS.

Kwarantanna – wydzielona w infrastrukturze sieć VLAN bez połączenia z podstawową siecią open peering.

Local Preference – wartość od 0 do 4294967295 przekazywana pomiędzy routerami BGP wewnątrz AS. Domyślnie na większości routerów ustawiona na 100.

next-hope – adres, przez który jest przekazywany ruch do danego prefiksu.

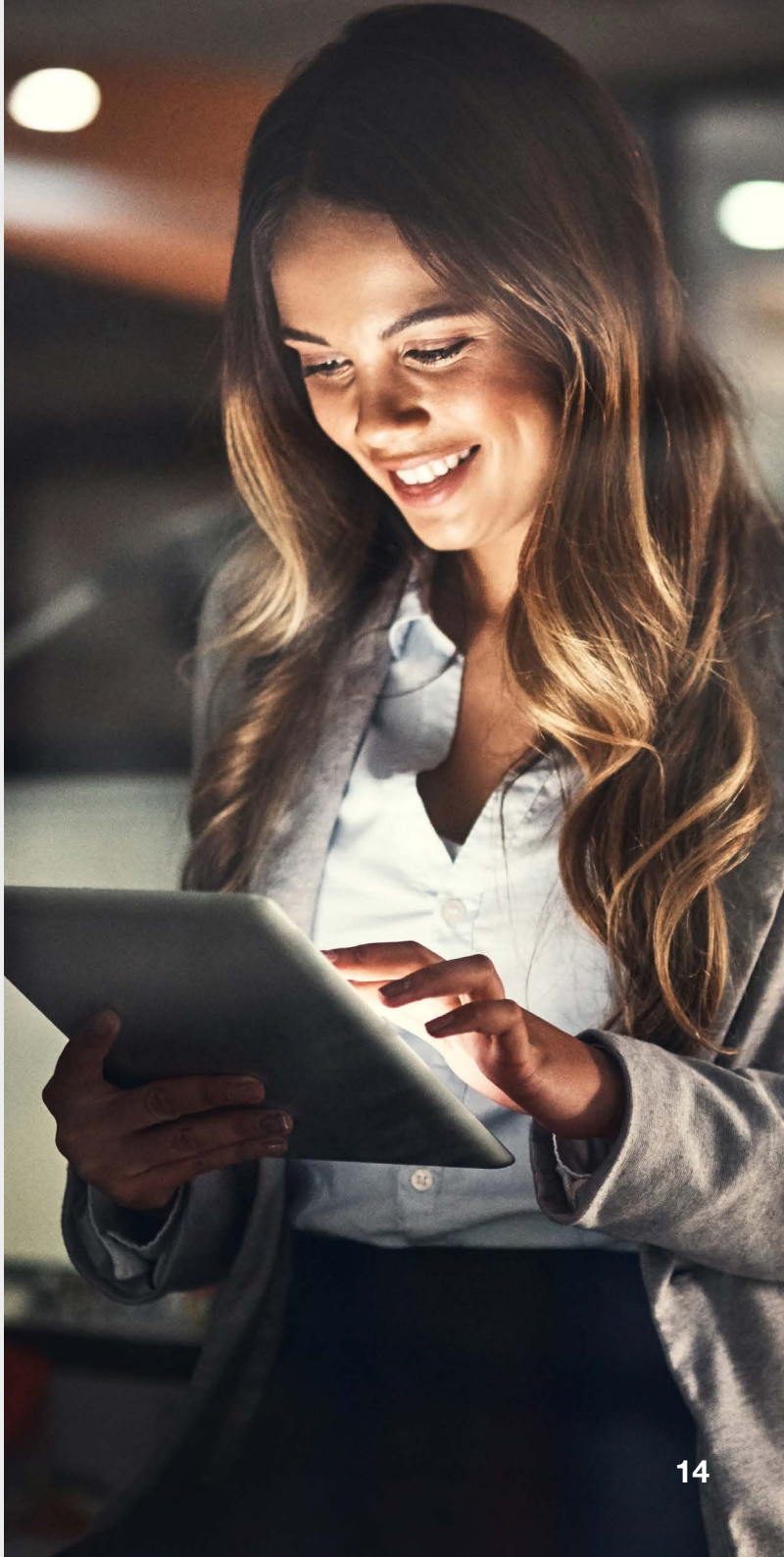
NLRI (Network Layer Reachability Information) – lista prefiksów.

PA (Provider Aggregatable) – unikalne adresy IP przypisane przez RIPE do konkretnego ISP.

PI (Provider Independent) – unikalne adresy IP, które nie są przypisane do konkretnego ISP i mogą być przenoszone między różnymi dostawcami usług.

ROA (Route Origin Authorisations) – obiekty, w których zawarte są takie informacje jak prefiks, maksymalna długość maski podsieci i ASN, który może rozgłosić określony prefiks.

RS (Route Server) – urządzenie TPIX, które poprzez protokół BGP4 komunikuje się z urządzeniami operatora oraz wymienia informacje routingowe podłączonych operatorów, zgodnie z ustaloną przez danego operatora polityką wymiany ruchu.



Infolinia
19 333

www.tpix.pl

www.hurt-orange.pl

orange™

Dla operatorów