Najlepsze praktyki zabezpieczania sieci klasy operatorskiej

Przewodnik praktyczny

Łukasz Bromirski
lbromirski@cisco.com

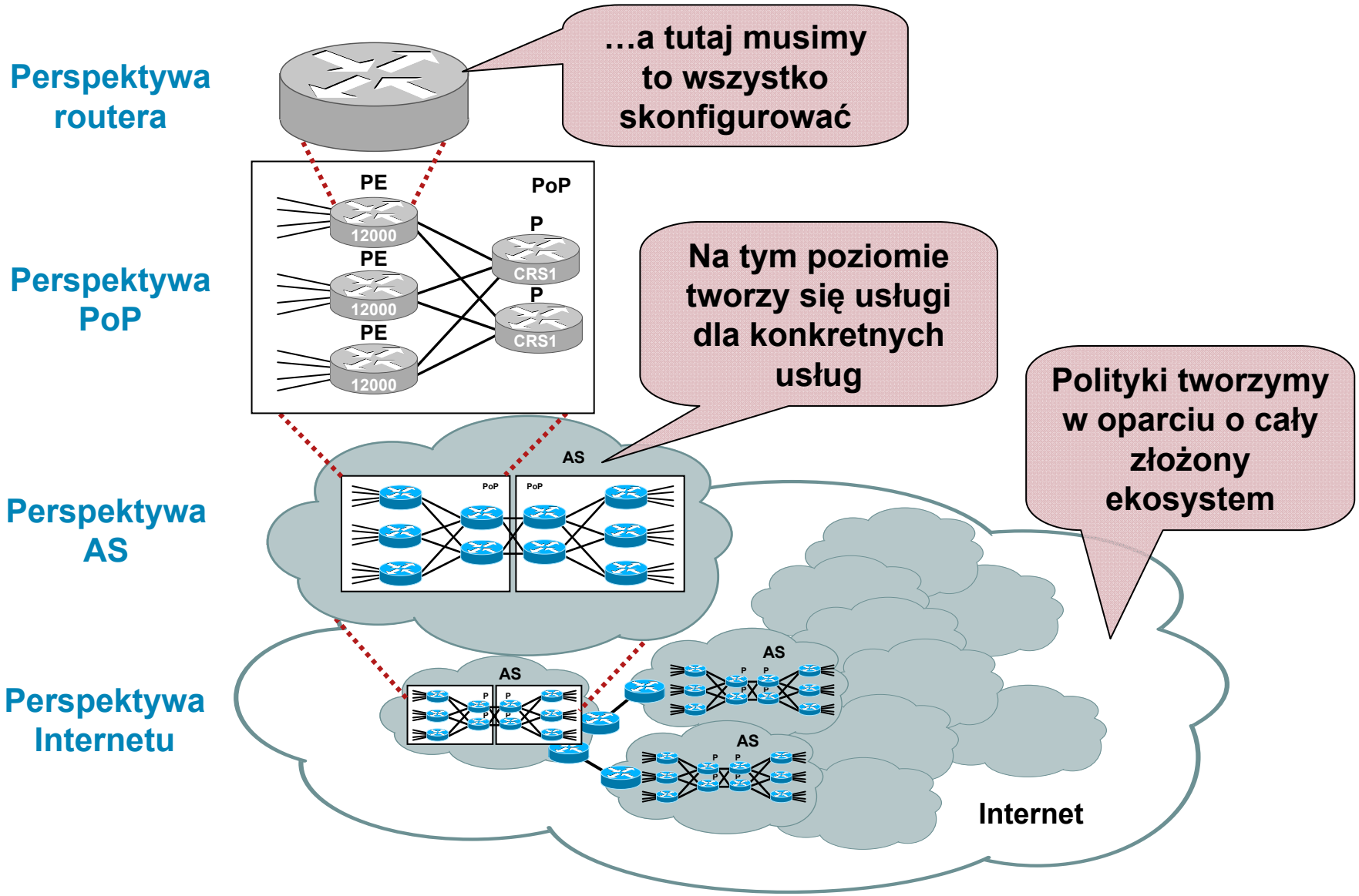
Warszawa, 01/2009

Agenda

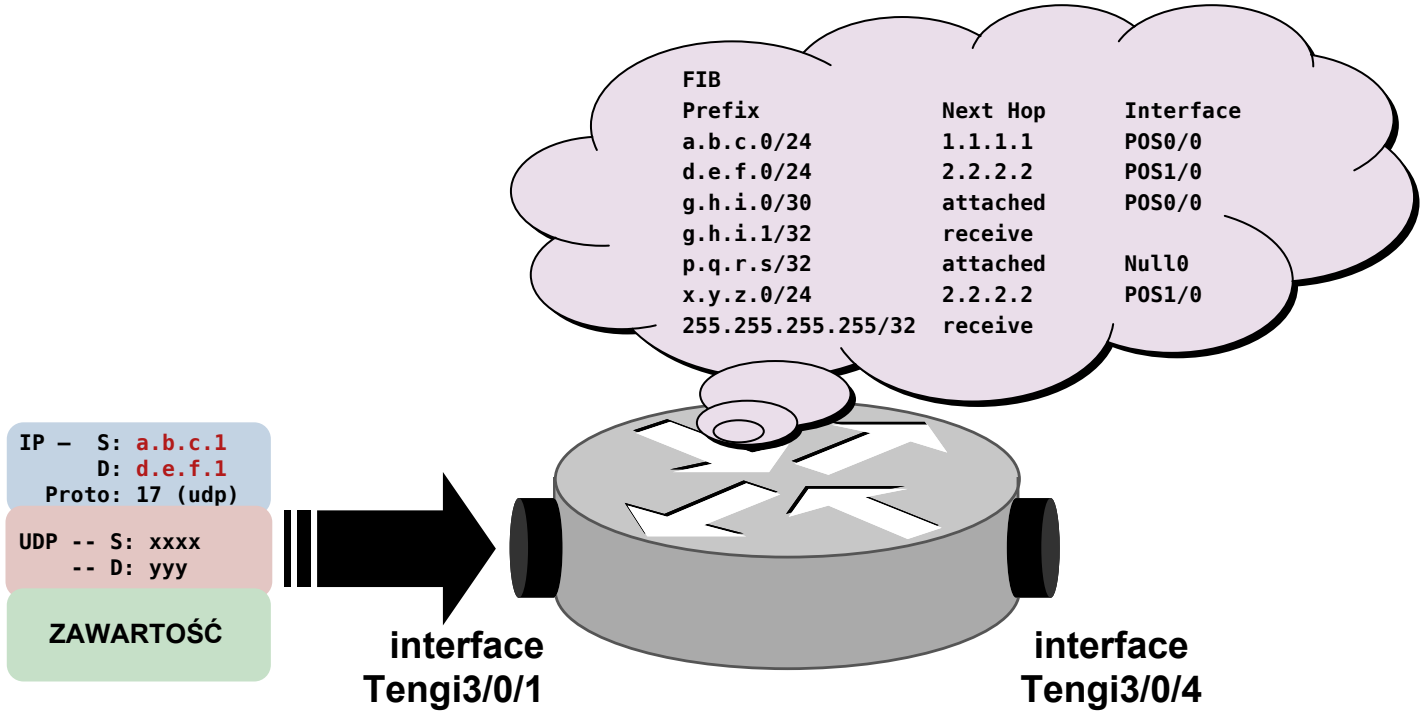
- Obsługa ruchu w sieci – perspektywa inżyniera
- BCP
  - hardening
  - uRPF
  - iACL
  - VRF i MPLS
  - CoPP
  - Bezpieczeństwo mechanizmów routingu
  - Blackholing
  - IP Anycast i dystrybucja polityk QoS przez BGP

Obsługa ruchu w sieci – perspektywa inżyniera

Hierarchia w sieci oczami inżyniera



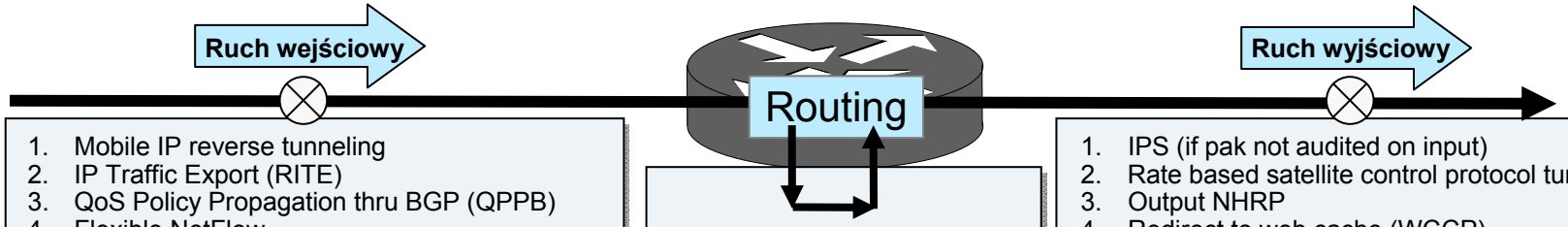
W tym wszystkim chodzi o pakiet…



- Gdy pakiet już trafi do Internetu, jakieś urządzenie, gdzieś będzie musiało zrobić jedną z dwóch rzeczy: [1] przekazać pakiet dalej* lub [2] odrzucić pakiet

*** przy okazji może wykonać różnego rodzaju operacje (QoS/etc)**

Przejście ruchu przez router Cisco



1. Mobile IP reverse tunneling
2. IP Traffic Export (RITE)
3. QoS Policy Propagation thru BGP (QPPB)
4. Flexible NetFlow
5. Virtual Fragmentation Reassembly
6. STILE (NBAR)
7. Input QoS Classification (CCE)
8. Ingress NetFlow
9. Intercept ACLs (LI)
10. IOS IPS Inspection
11. Input Stateful Packet Inspection (IOS FW)
12. Input Authentication Proxy Check
13. Input ACL check
14. Input CCE (common classification engine)
15. Flexible Packet Matching (FPM)
16. Crypto
17. EZVPN connect ACL
18. Unicast RPF check
19. Input QoS Marking
20. Input Policing (CAR)
21. Input MAC/Precedence Accounting
22. NAT-PT (IPv4-to-IPv6)
23. NAT Outside to Inside
24. Fwd packts to NM-CIDS
25. SSG
26. Policy Routing Check
27. WCCP
28. CASA
29. Idle timer
30. URD Intercept
31. GPRS ingress policy
32. CDMA PDSN ingress address filtering
33. Mobile IP Home Agent intercept

Mechanizmy dodatkowe

1. BGP Policy Accounting
2. TCP MSS fix
3. NAT Virtual Interface (NVI)

1. IPS (if pak not audited on input)
2. Rate based satellite control protocol tunnel
3. Output NHRP
4. Redirect to web cache (WCCP)
5. QOS classification/CCE egress
6. Output copy to NM-CIDS
7. Inside-to-outside NAT
8. STILE (NBAR)
9. Output DSCP Classification for AutoQoS
10. BGP Policy Accounting
11. Intercept ACLs (LI)
12. Crypto map check (mark for encryption)
13. Output QoS Classification
14. Output “fixup” for IOS FW
15. Output ACL check
16. Output Common Classification Engine (CCE)
17. Output FPM
18. Output TCP MSS tweak
19. DoS tracking
20. Output Stateful Packet Inspection (IOS FW)
21. IOS FW AuthProxy Intercept
22. Output TCP Intercept
23. Mobile IP Home Agent Intercept
24. Output QoS Marking
25. Output accounting
26. RSVP Netflow hook
27. Output Policing (CAR)
28. MAC/Precedence accounting
29. IPSec Encryption
30. Egress NetFlow
31. Flexible NetFlow
32. Output GPRS
33. Ouput IPHC
34. Egress RITE
35. Queuing (CBWFQ, LLQ, WRED)

Dwie/trzy warstwy logiczne

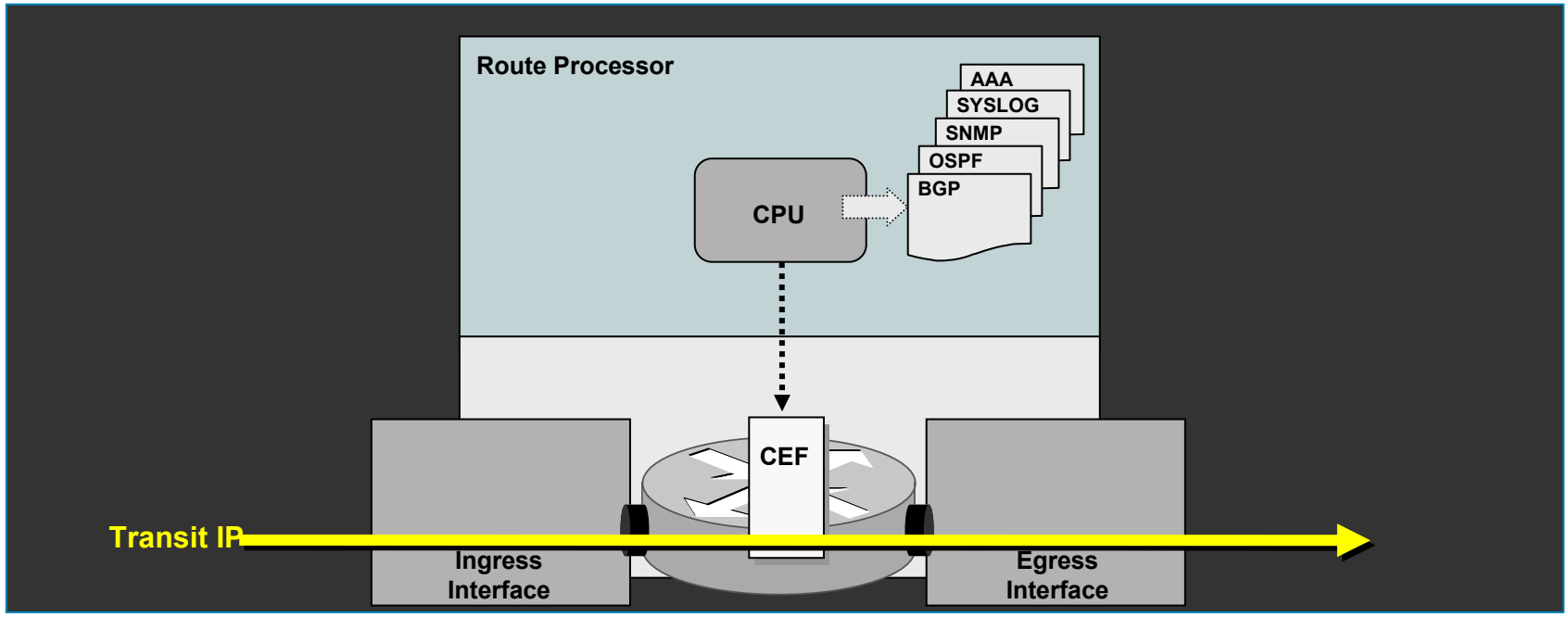
- Logiczne oddzielenie od siebie funkcji ułatwia zrozumienie działania nowoczesnych routerów i podział dużego problemu na mniejsze

  IETF RFC3654 definiuje dwie ‘warstwy’: kontroli i przekazywania ruchu

  ITU X805 definiuje trzy ‘warstwy’: kontroli, zarządzania i użytkownika

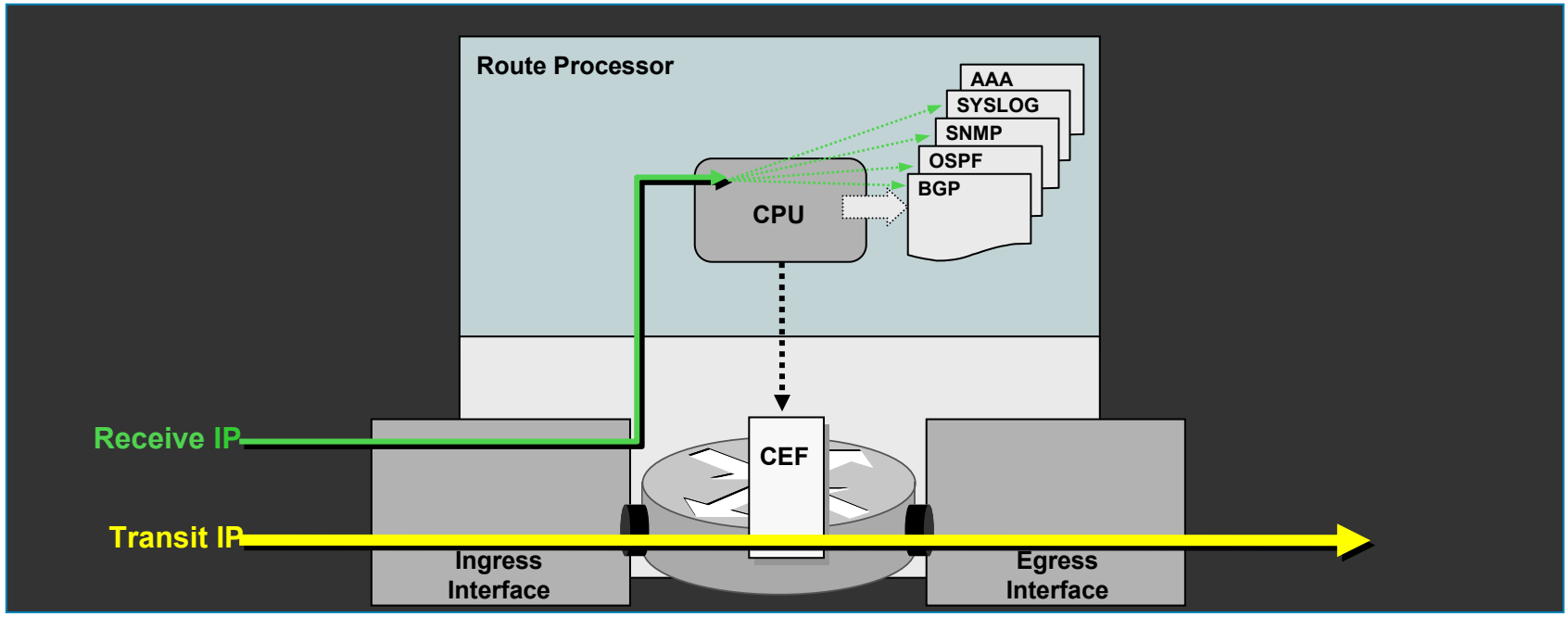
Ruch tranzytowy

- Poprawne pakiety IP, które można obsłużyć za pomocą standardowego routingu, opartego o docelowy adres IP i nie wymagają dodatkowej obróbki.
- Docelowy adres IP nie jest adresem urządzenia, jest zatem przekazywany pomiędzy interfejsem wejściowym a wyjściowym
- Ruch pakietów obsługiwany jest przez mechanizm CEF (Cisco Express Forwarding) i (gdy to możliwe) specjalizowane układy sprzętowe.



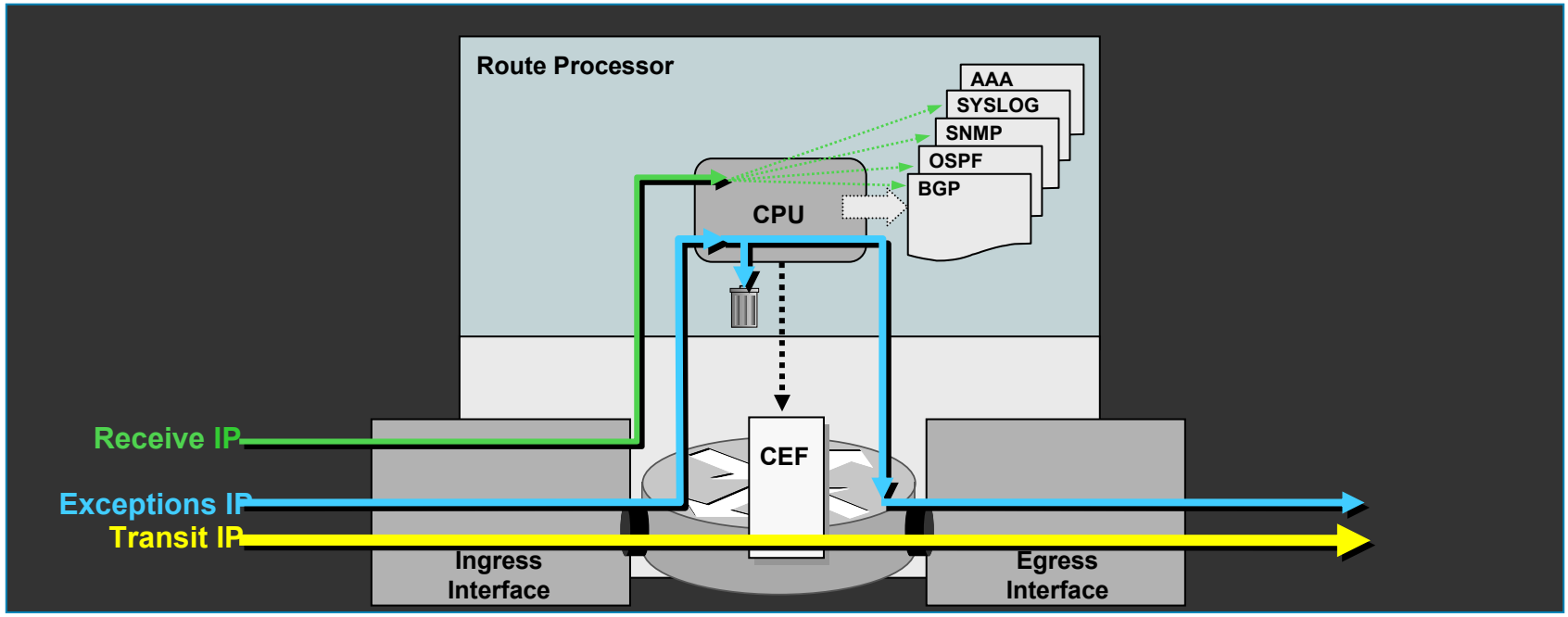
Ruch do routera – ‘receive’

- Pakiety IP z adresem docelowym jednego z interfejsów lub usług uruchomionych na routerze.
- Docierają do procesora (na dedykowanym RP lub współdzielonego dla całej platformy) do konkretnego procesu pracującego w Cisco IOS
- Adresy IP ‘nasłuchujące’ ruchu oznaczone są w tablicy CEF terminem ‘receive’. Proces przesłania ich z interfejsów do konkretnej usługi to ‘punt’



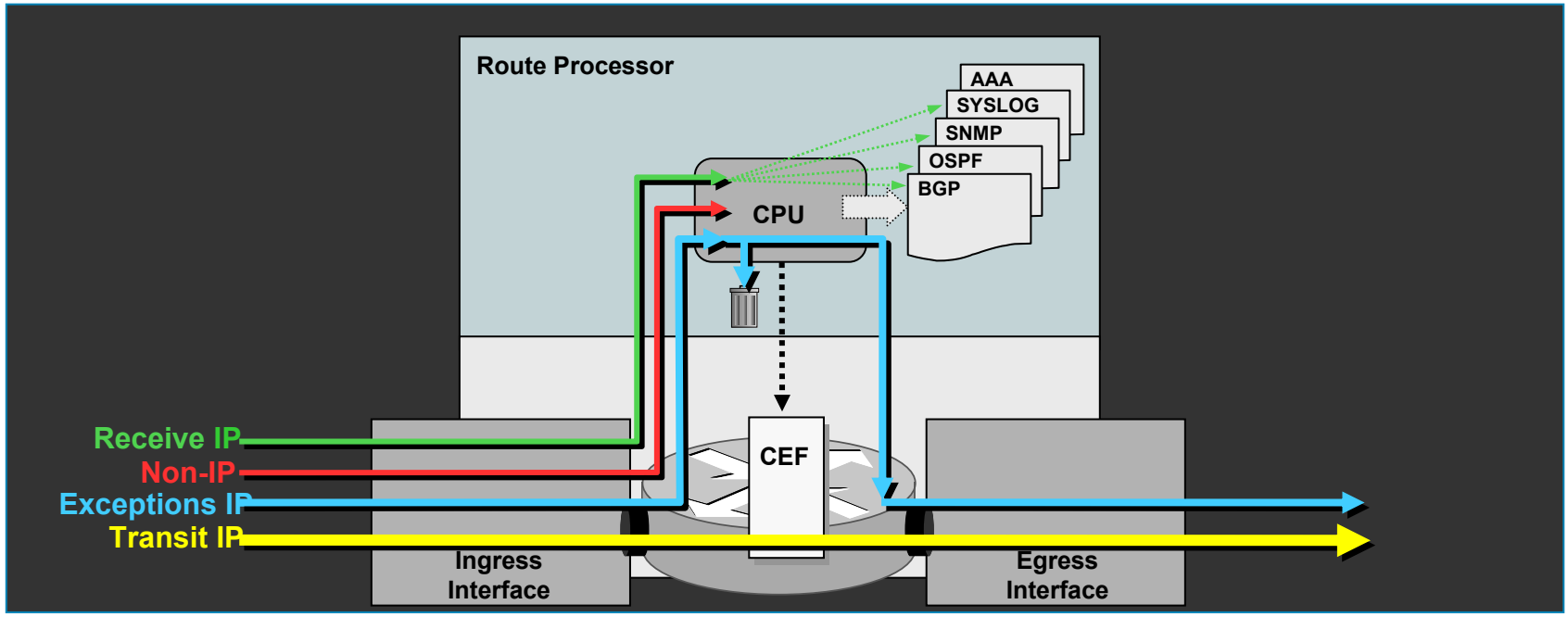
Wyjątki – ‘exceptions’

- Wyjątki to np. pakiety zawierające opcje, pakiety z wygasającym TTL. W niektórych przypadkach i architekturach mogą to być również pierwsze pakiety nowej sesji – np. pierwszy pakiet multicast, sesja tworząca wpis NAT itp.
- Wszystkie pakiety tego typu obsługiwane są przez RP



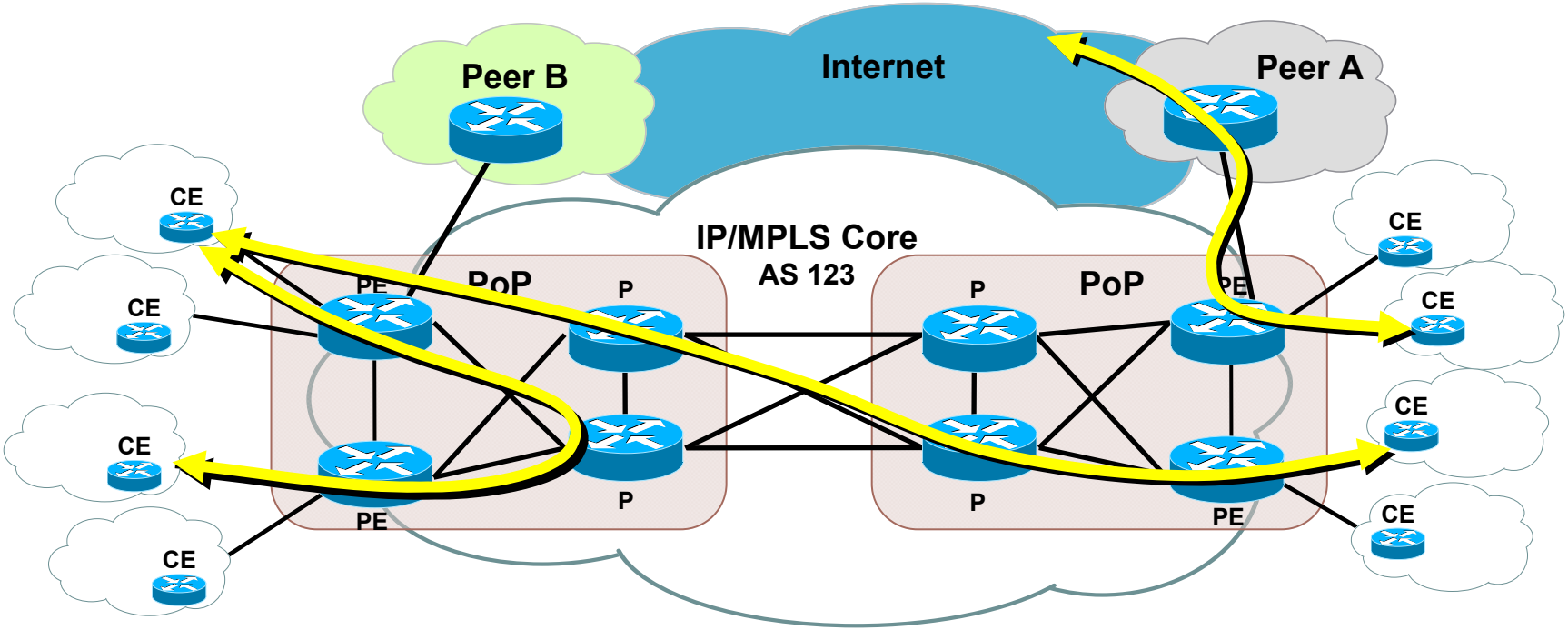
Ruch nie-IP

- Przykłady ruchu nie-ip to pakiety keepalive L2, pakiety ISIS, CDP, PPP LCP
- Wszystkie pakiety tego typu obsługiwane są przez RP



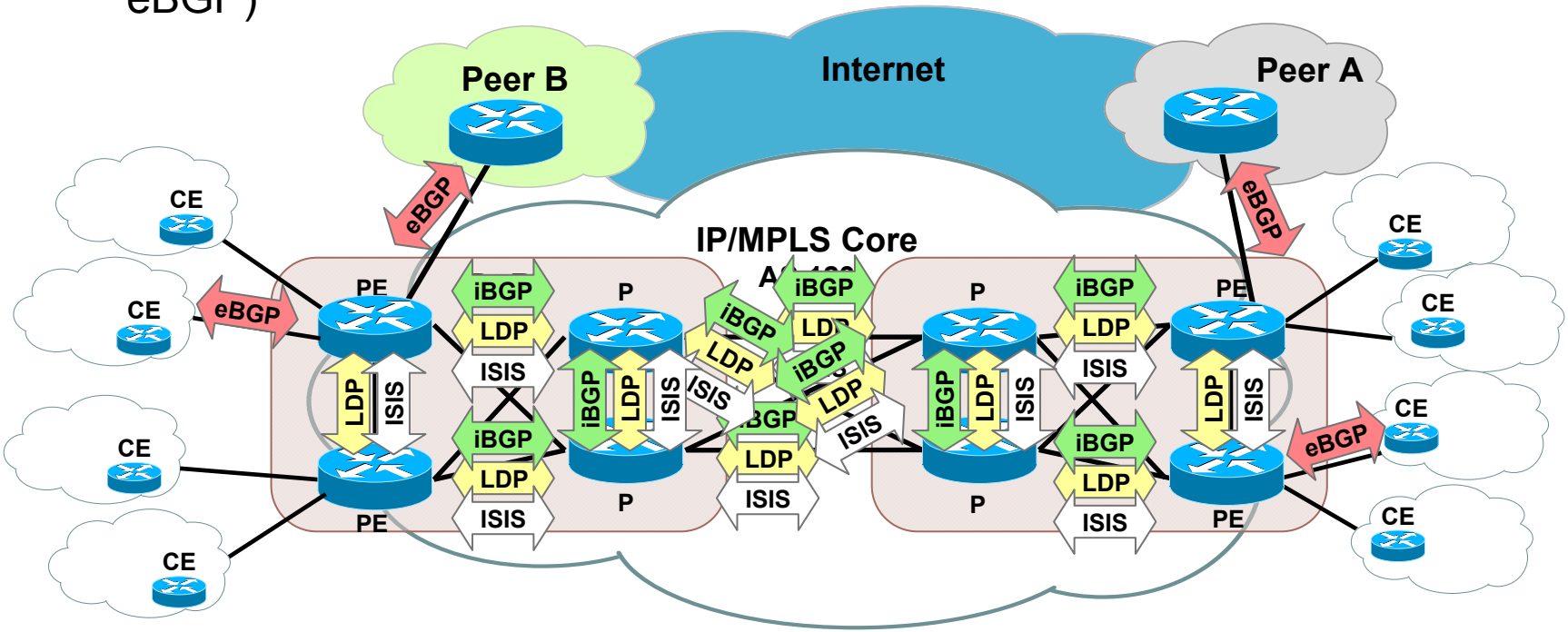
Warstwa danych IP

- Logiczna grupa zawierająca ruch generowany przez aplikacje klienta – ruch powstający i terminowany w sieciach klienta
- Ruch warstwy danych traktowany jest zawsze jako tranzytowy przez elementy sieciowej.



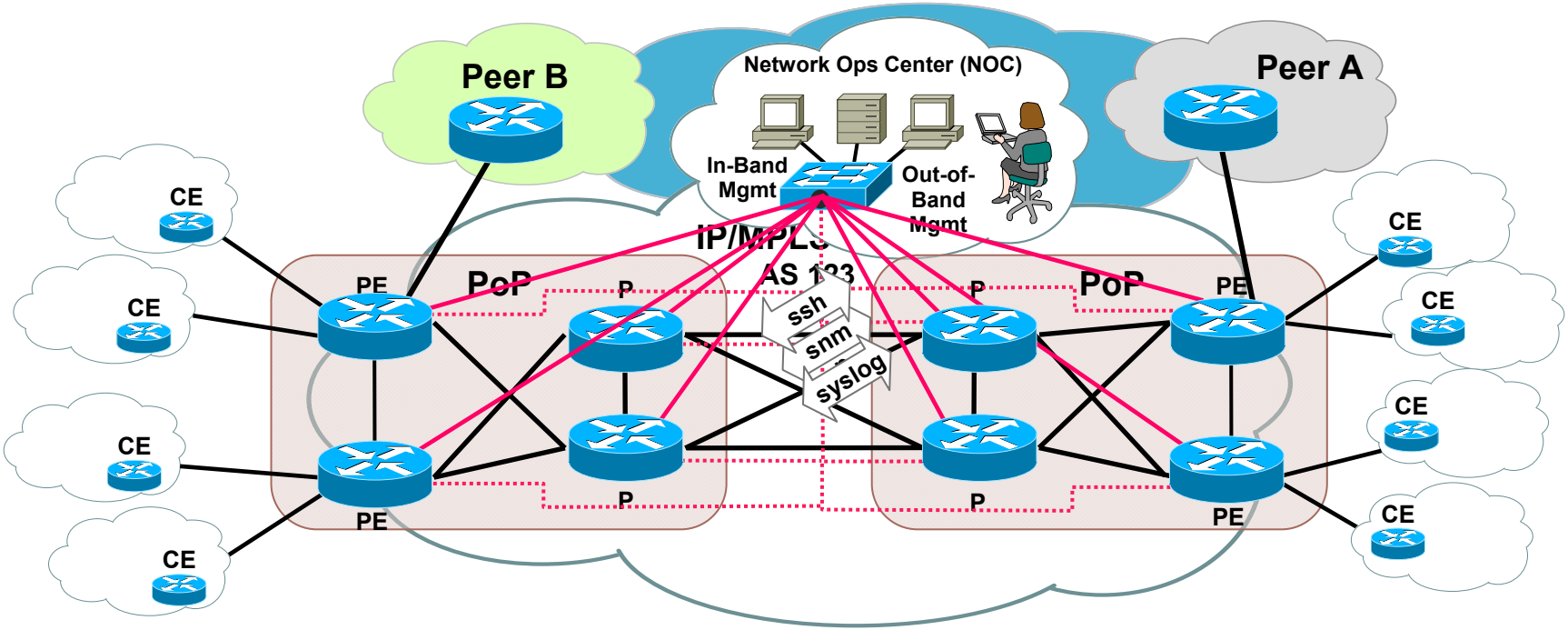
Warstwa kontrolna

- Logiczna grupa zawierająca ruch protokołów routingu, sygnalizacji, utrzymania łącz (i ich stanu) – wszystko co powoduje że sieć wykorzystująca protokoły takie jak BGP, OSPF, LDP, IS-IS, ARP, Layer 2 keepalives, ATM OAM czy ramki PPP LCP
- Ruch w warstwie kontrolnej zawiera pakiety klasyfikowane jako ‘receive’, ale logicznie zawiera również część ruchu tranzytowego (np. multihop eBGP)



Warstwa zarządzania

- Logiczna grupa zawierająca ruch służący do zarządzania, provisioningu, utrzymania i monitoringu sieci. Warstwa zawiera ruch taki jak SSH, FTP, SNMP, Syslog, TACACS+ i RADIUS, DNS, NetFlow, ROMMON, CDP itd.
- Ruch w warstwie kontrolnej zawiera pakiety klasyfikowane jako ‘receive’, ale logicznie zawiera również część ruchu tranzytowego (np. SSH)



Koncepcja ‘pasma’
Inżynieria „PPS” – Packets Per Second

- Ile można maksymalnie wysłać ramek na sekundę dysponując interfejsem Gigabit Ethernet?

  Minimalny ładunek ramki to 46 bajtów, a węzeł może osiągnąć maksymalną przepustowość w kanale bez kolizji. Ramka składa się zatem z 72 bajtów z 12 bajtową przerwą pomiędzy ramkami – minimalna ‘długość’ to zatem 84 bajty

- Jaką maksymalną wydajność można uzyskać posługując się interfejsem Gigabit Ethernet?

  Maksymalny ładunek Ethernet to 1500 bajtów, a węzeł może osiągnąć maksymalną przepustowość w kanale bez kolizji. Ramka składa się zatem z 1526 bajtów i 12 bajtową przerwą pomiędzy ramkami – łącznie 1538 bajtów.

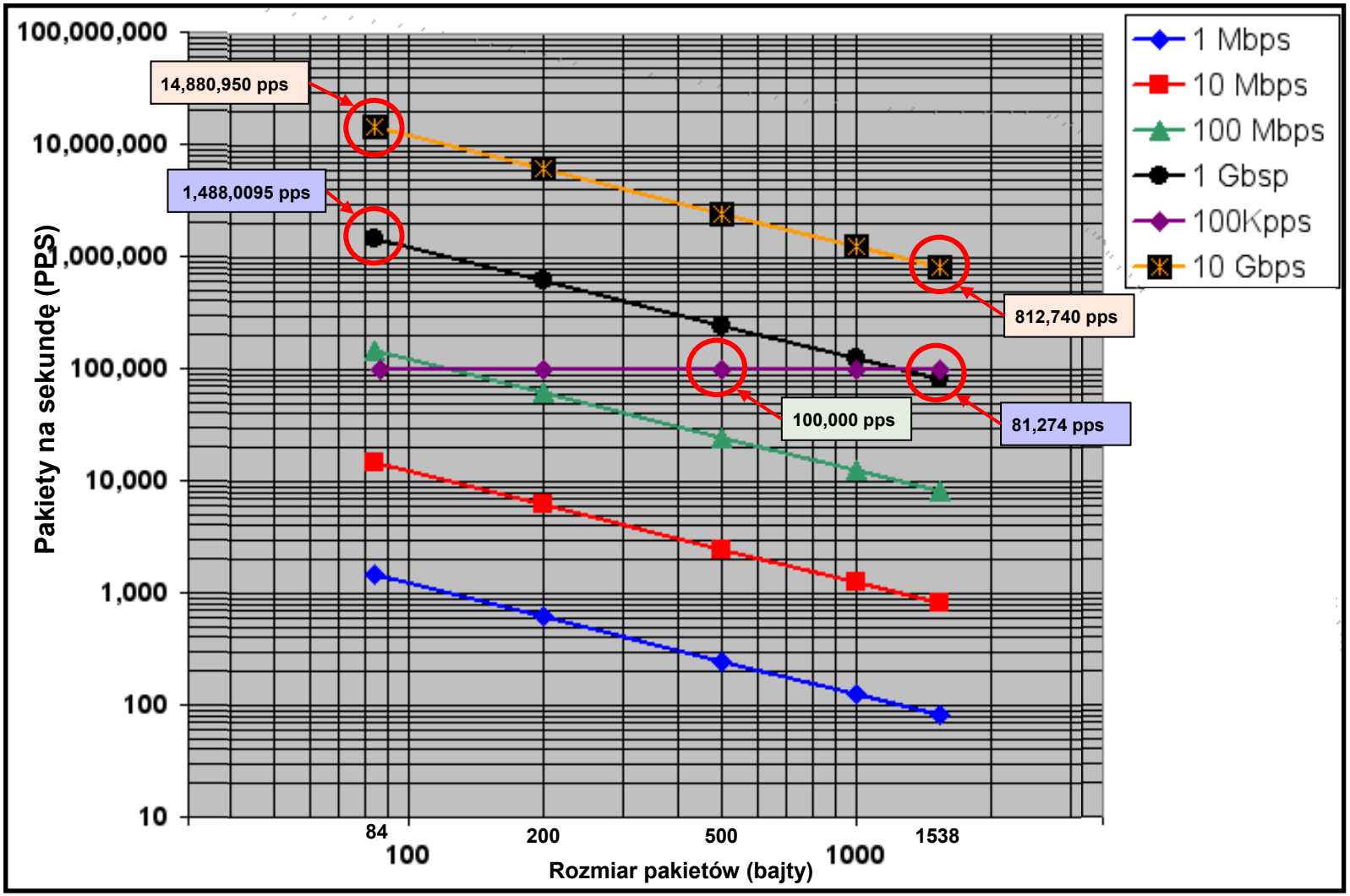
- Zatem – dla ruchu 84 bajtów:

  1,000,000,000 bps/(84 B * 8 b/B) = 1,488,096 fps

- …a dla ruchu 1538 bajtów:

  1,000,000,000 bps/(1538 B * 8 b/B) = 81,274 fps

Koncepcja ‘pasma’ – PPS a długość PDU



BCP - hardening

Zabezpieczanie routerów
Najlepsze praktyki

- Wiele organizacji publikuje własne zalecenia dotyczące najlepszych praktyk

  http://www.first.org/resources/guides/

  http://www.sans.org/resources/policies/

  http://www.ietf.org/html.charters/opsec-charter.html

- Dokumenty te opisują ‘hardening’ platformy, nie kompleksowe podejście do zapewnienia sieci bezpieczeństwa
- Cisco również opublikowało w przeszłości taki dokument:

  ftp://ftp-eng.cisco.com/cons/isp/essentials/

Zabezpieczanie routerów
Najlepsze praktyki

- Data plane
- Control plane
- Management plane
- Services plane

Mechanizmy warstwy danych (data plane)

Interface Access Control Lists (iACLs)	Filtrowanie ruchu wchodzącego i wychodzącego
Unicast Reverse Path Forwarding (uRPF)	Automatyczne filtrowanie ruchu z adresów ‘sfałszowanych’
IP Options [ignore | drop]	Kontrola ruchu IPv4 z ustawionymi opcjami
IP source-route	Kontrola ruchu IPv4 z ustawioną opcją routingu na podstawie źródłowa
IP directed-broadcast	Kontrola ruchu IPv4 skierowanego broadcastu
Zmiana klasyfikacji QoS dla pakietu IP	Klasyfikacja i reklasyfikacja ruchu dzięki IP DSCP/ToS
Remote Triggered Blackholing	Rozwiązanie dynamicznego filtrowania ruchu przy pomocy BGP

Zabezpieczanie routerów
Najlepsze praktyki

Data plane
Control plane
Management plane
Services plane

Mechanizmy warstwy kontrolnej (control-plane)

Receive-Path Access List (rACL)	ACL obsługujące ruch do wpisów ‘receive’ w linii 12.0S
Control Plane Policing (aCoPP and dCoPP)	Mechanizmy klasyfikacji i nakładania ograniczeń na ruch do RP
Selective Packet Discard (SPD)	Wewnętrzny mechanizm nadawania priorytetów ruchowi krytycznemu
Polecenia związane z BGP	
IP Prefix List	Filtrowanie prefiksów za pomocą prefix-list
IP Community List	Filtrowanie/nakładanie polityki w oparciu o wartości community
IP AS-Path Access Lists	Filtrowanie prefiksów za pomocą AS-path
Route Map	Możliwość nakładania polityk na prefiksy wchodzące/wychodzące z routera
Class Map	Mechanizm klasyfikacji ruchu i przypisania ograniczeń
Policy Map	Mechanizm łączący wiele class-map w jedną politykę
Trasy statyczne na Null0	Mechanizm routingu w sprzęcie (jeśli dostępne) dla ruchu niechcianego

- Data plane
- Control plane
- Management plane
- Services plane

Zabezpieczanie routerów
Najlepsze praktyki

Mechanizmy warstwy kontrolnej (control-plane)

RSVP	Nakładanie ograniczeń związanych z bezpieczeństwem na RSVP
PIM	Nakładanie ograniczeń związanych z bezpieczeństwem na PIM
IGMP	Nakładanie ograniczeń związanych z bezpieczeństwem na IGMP
IP icmp rate-limits	Ograniczanie ilości generowanego ruchu ICMP w odpowiedzi
IP redirects	Generowanie informacji ICMP redirect
IP unreachables	Generowanie informacji ICMP unreachable
IP mask-reply	Generowanie informacji ICMP mask-reply
IP information-reply	Generowanie informacji ICMP information-reply
IP proxy-arp	Mechanizm proxy-arp na interfejsie
Key Chain	Uwierzytelnianie kluczami zmiennymi w czasie

Zabezpieczanie routerów
Najlepsze praktyki

- Data plane
- Control plane
- Management plane
- Services plane

Mechanizmy warstwy zarządzającej (management-plane)

SNMP	Polecenia związane z SNMP
AAA	Polecenia związane z AAA
TACACS+	Polecenia zwiazane z TACACS+
NTP	Polecenia związane z NTP
Baza danych użytkowników lokalnych	Lokalna baza użytkowników (np. na wypadek awarii, upgrade'ów/etc)
Syslog	SYSLOG
TCP	Tuning stosu TCP
SSH	Bezpieczne zdalne zarządzanie
HTTP/HTTPS	Kontrola serwera HTTP i HTTPS
FTP/TFTP/SCP	Przesyłanie plików do/z routera
VTY/Console/Aux / Management-interface	Kontrola dostępu zdalnego i lokalnego
Banner	Definicja banneru powitalnego/logowania/etc
NetFlow	Mechanizm NetFlow z raportowaniem lokalnym i/lub eksportowanym
Embedded Event Manager	Polecenia związane z EEM
IP Source Tracker	Polecenia związane z mechanizmem IP Source Tracker

- Data plane
- Control plane
- Management plane
- Services plane

Zabezpieczanie routerów
Najlepsze praktyki

Mechanizmy warstwy zarządzającej (management-plane)

Kontrola procesów w IOSie	
scheduler allocate	Konfiguracja podziału czasu pomiędzy procesy a routing
memory free low-watermark processor	Informacje o osiągnięciu krytycznie niskich wartości wolnej pamięci
process cpu threshold	Informacje o osiągnięciu krytycznego obciążenia CPU
Konfiguracje globalnych serwisów	
boot system flash <*filename*>	Wskazanie miejsca obrazu binarnego IOS
service password-encryption	„Zaciemnienie” (to nie jest szyfrowanie!) hasła
service compress-config	Kompresja pliku z konfiguracją
service timestamps <poziom-logowania>	Oznaczanie logów stemplami czasowymi
no service pad	Funkcjonalność PAD
no ip finger	Funkcjonalność IP finger
no logging console	Logowanie na konsolę
no ip bootp server	Obsługa usługi BOOTP
no cdp run	Cisco Discovery Protocol
maximum routes	Ilość tras (maksymalnie) per VRF
no mpls ip propagate-ttl	Propagacja wartości pola TTL pakietu przez sieć MPLS
mpls ldp advertise-labels	Bezpieczeństwo konfiguracji rozgłaszania etykiet
mpls ldp neighbor labels accept	Konfiguracja jakie etykiety akceptujemy od sąsiadów

Zabezpieczanie routerów
Zarządzanie platformą

- Dostęp do interfejsu zarządzającego
- IOS:

```
control-plane host
 management-interface Fa0/0 allow ssh snmp
```

- IOS-XR:

```
control-plane
 management-plane
  inband
   interface Gig 0/0/01
    allow ssh peer address ipv4 10.0.1.0/24
    allow https peer address ipv4 10.0.1.0/24
```

Zabezpieczanie routerów
Zarządzanie platformą

- Archiwizacja / rollback konfiguracji
- IOS:

12.3(7)T/12.2(25)S/12.2(31)SB/12.2(33)SRA/12.2(33)SXH

```
archive
[…]
config replace running-config [list] [time x]
```

- IOS-XR – domyślnie aktywne

BCP - uRPF

unicast Reverse-Path Filtering

- Mechanizm blokujący klasę ataków, w których adres źródłowy jest losowy lub sfałszowany
- Opiera swoje działanie o tablicę routingu

  działa równie dobrze dla IPv4 jak i IPv6
- Pojawił się jako podstawowy element ‘dobrych praktyk’ w RFC 2827 / BCP 38

uRPF w trzech trybach

- uRPF “Strict Mode”

  Prawidłowy wpis w FIB wskazujący dokładnie na interfejs, którym pakiet dotarł do routera

  Jeśli wpis w FIB nie istnieje, lub wskazuje na inny interfejs – pakiet jest odrzucany

- uRPF “Loose Mode”

  Prawidłowy wpis w FIB wskazujący na dowolny interfejs, którym pakiet dotarł do routera

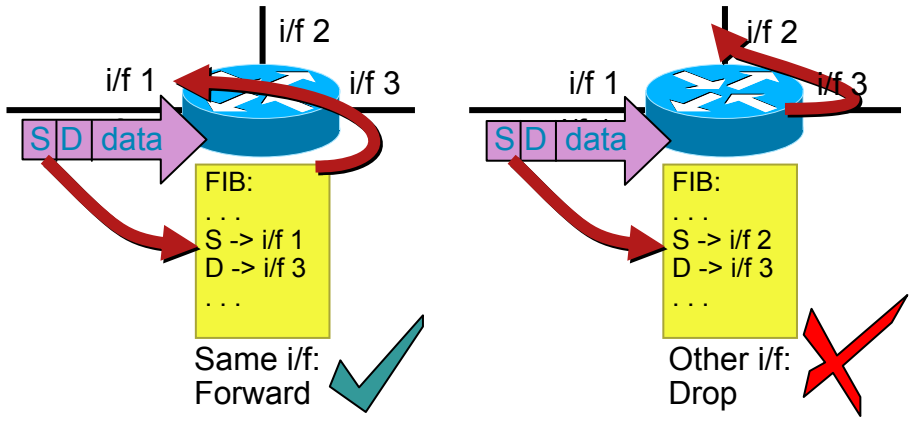
  Jeśli wpis w FIB nie istnieje, lub wskazuje na interfejs Null0 – pakiet jest odrzucany

- uRPF “VRF Mode”

  Wymaga aby źródłowy adres IP był wymieniony na białej lub czarnej liście w danym VRFie

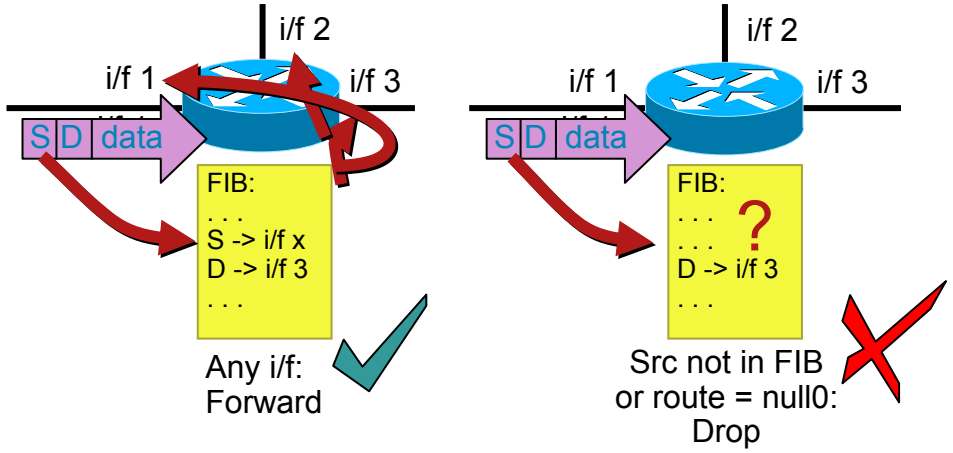
uRPF strict i uRPF loose

router(config-if)# ip verify unicast source reachable-via **rx**



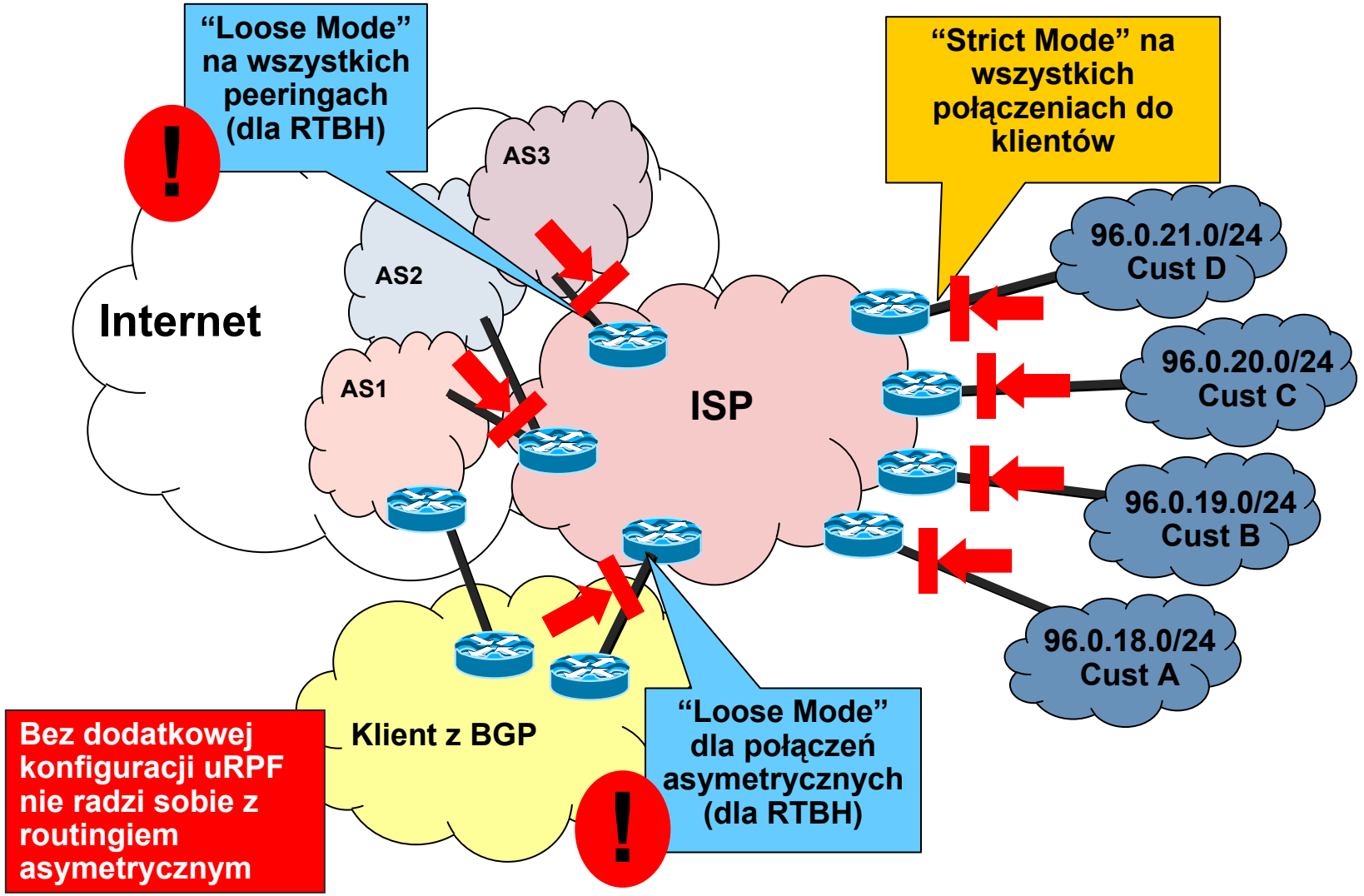
"Strict Mode"
(aka "v1")

router(config-if)# ip verify unicast source reachable-via **any**



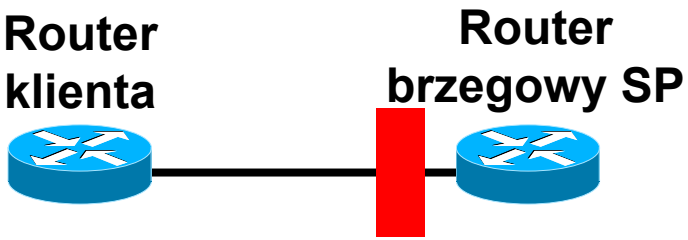
"Loose Mode"
(aka "v2")

Gdzie stosować uRPF?



BCP - iACL

ACL do infrastruktury (iACL)



- Na brzegu:

  deny ip any <zakres_adresów_sieci_szkieletowej>

  wyjątki: protokoły routingu, być może ICMP

- Idea zastosowania:

  „skoro nie możesz wygenerować ruchu do urządzeń, nie będziesz ich w stanie zaatakować”

- Stanowi dobre odseparowanie, ale jest trudny w utrzymaniu a DoS jest nadal możliwy - ruchem tranzytowym

ACL do infrastruktury

- Konkretny zestaw ACL pozwoli na ruch tylko wymaganym protokołom i zablokuje całą resztę komunikacji do przestrzeni adresowej sieci szkieletowej

  pozwalamy na np.: eBGP peering, GRE, IPSec, itp. itd.

- ACL powinny również zapewniać usługi antyspoofingowe (jeśli uRPF jest niemożliwy do wprowadzenia):

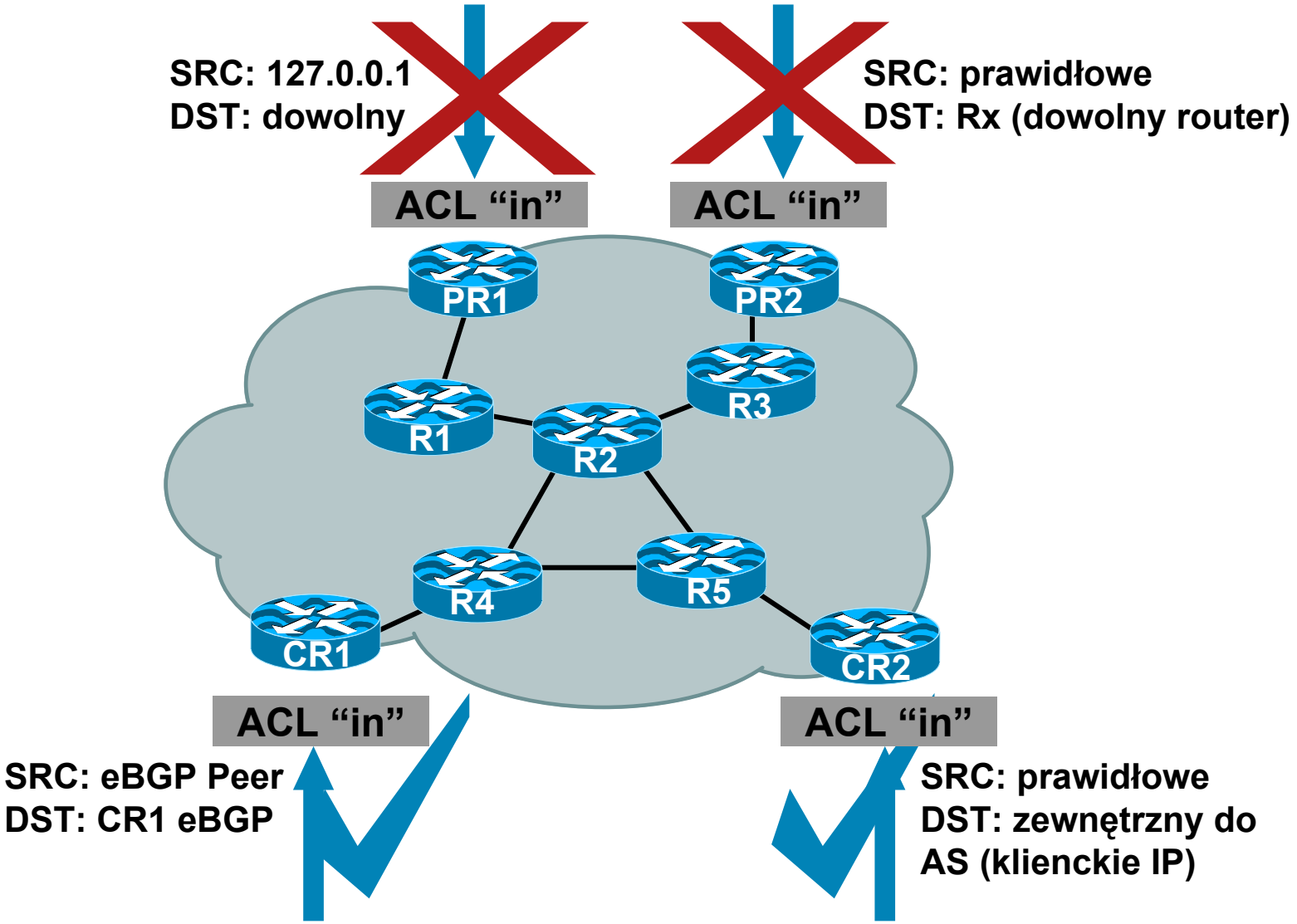
  odrzucać ruch przychodzący z zewnątrz, ale z Twoimi adresami IP

  odrzucać ruch z RFC1918

  odrzucać ruch multicastowy (224/4)

  ...i ruch opisany w RFC3330

Jak działają iACL?



Przykład: ACL do infrastruktury

```
! odrzuć naszą przestrzeń adresową w adresach źródłowych
access-list 101 deny ip our_CIDR_block any
! odrzuć ruch z adresów 0.0.0.0 i 127/8
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
! odrzuć klasy adresowe z RFC1918
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.0.15.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
! zezwól na zestawienie sesji eBGP
access-list 101 permit tcp host peerA host peerB eq 179
access-list 101 permit tcp host peerA eq 179 host peerB
! zablokuj dowolny inny ruch do naszej infrastruktury
access-list 101 deny ip any core_CIDR_block
! przepuść ruch tranzytowy
access-list 101 permit ip any any
```

BCP - VRFy

Czym jest VRF?

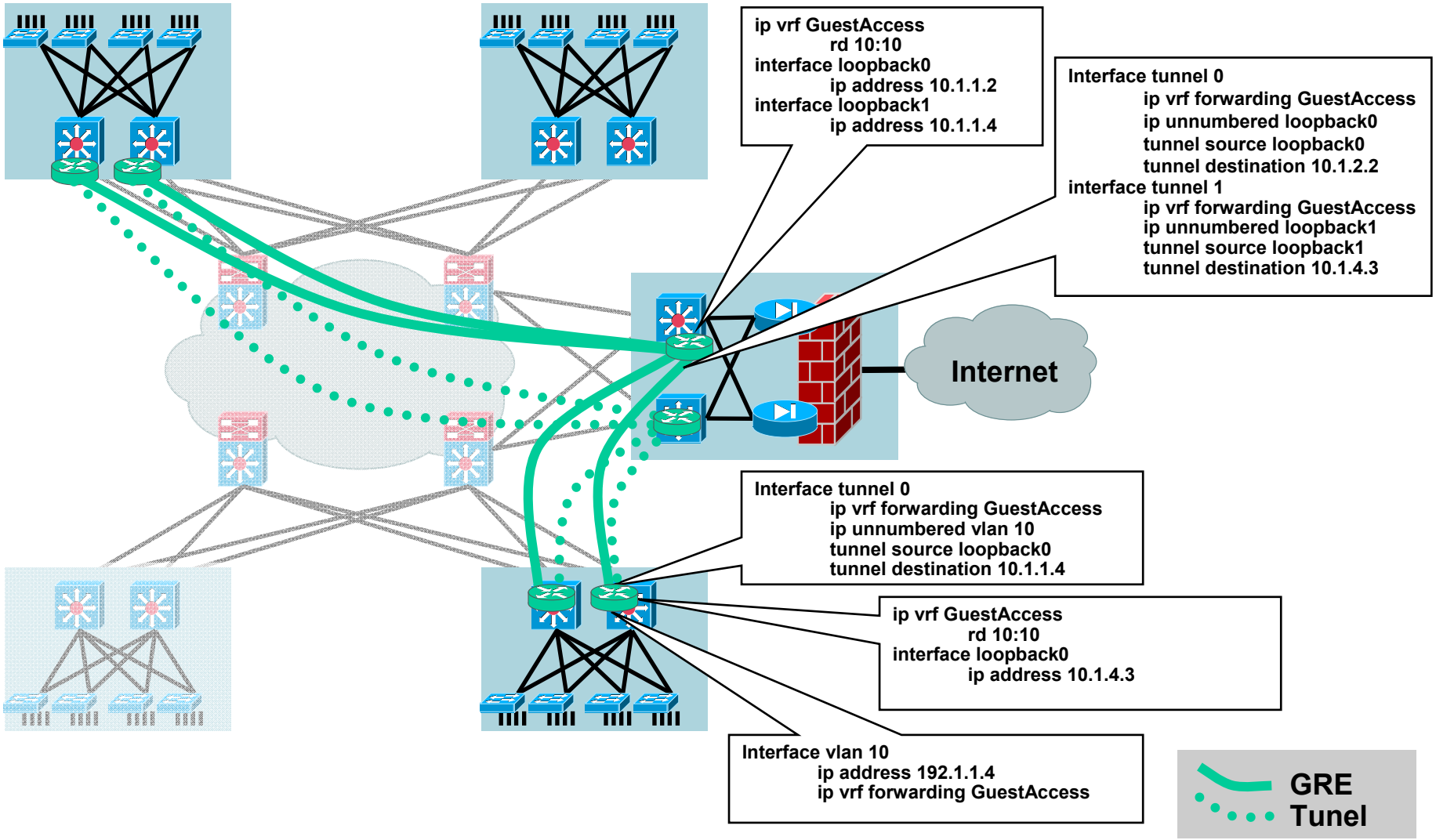
- Virtual Routing & Forwarding

  osobna tablica routingu, do której przynależą interfejsy – może zawierać własne instancje routingu i wymieniać selektywnie informacje o osiągalności z innymi VRFami, w tym – VRFem globalnym

- VRF = VRF wykorzystywany w połączeniu z MPLS
- VRF-lite = VRF wykorzystywany bez MPLS do separacji podsieci

  coraz popularniejsze rozwiązanie w firmach typu enterprise, hotelach, kampusach etc

Separacja w firmie z wykorzystaniem VRF



Bezpieczeństwo sieci MPLS

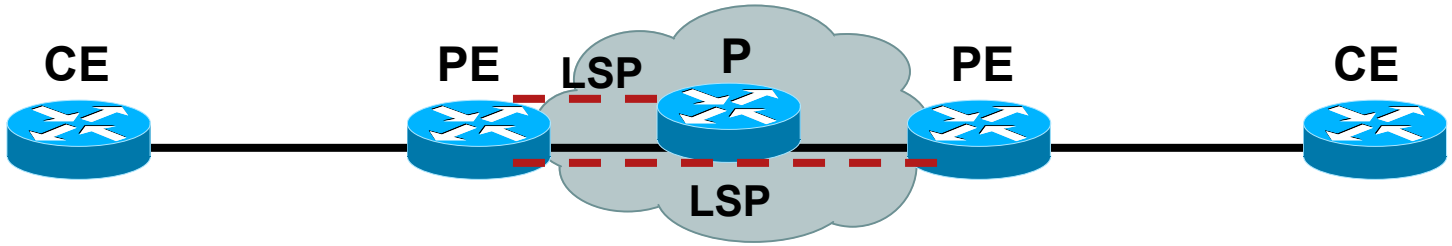
- Sam MPLS nie jest rozwiązaniem kompletnym dla ukrycia sieci operatora

  no mpls ip propagate-ttl to ‘security by obscurity’

- Wszystcy klienci, łącznie z Internetem powinni znaleźć się w osobnych VRFach

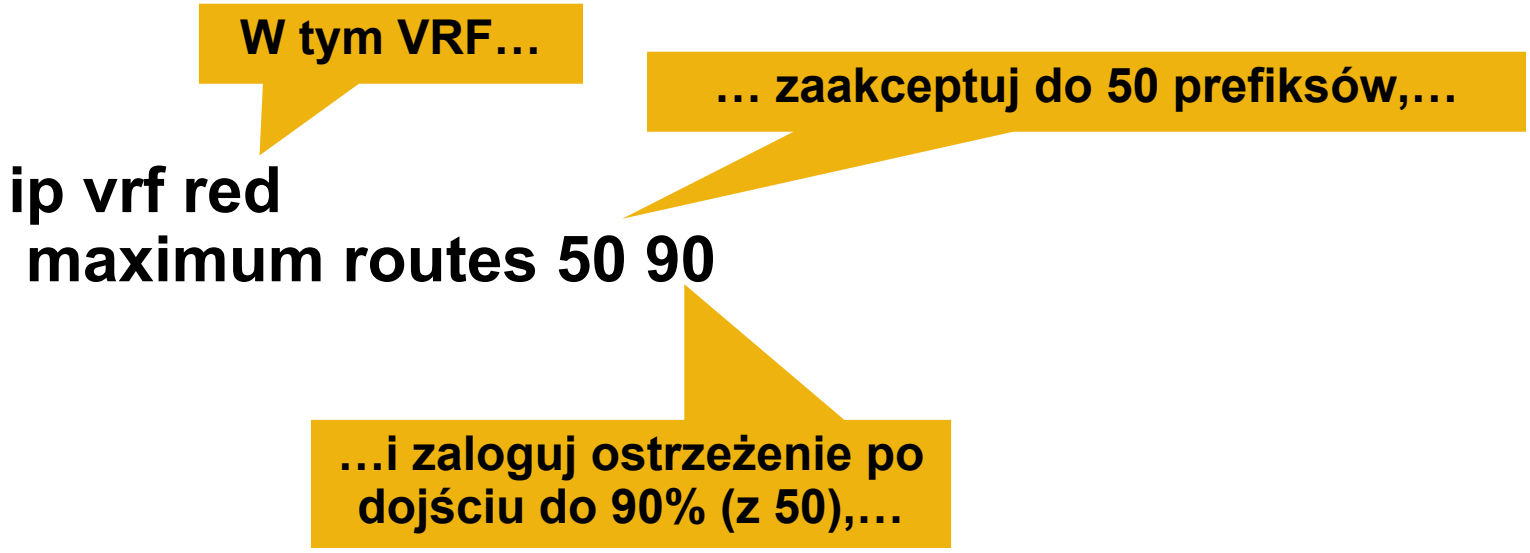
  routery P znikają z celownika

  routery PE należy odpowiednio zabezpieczyć



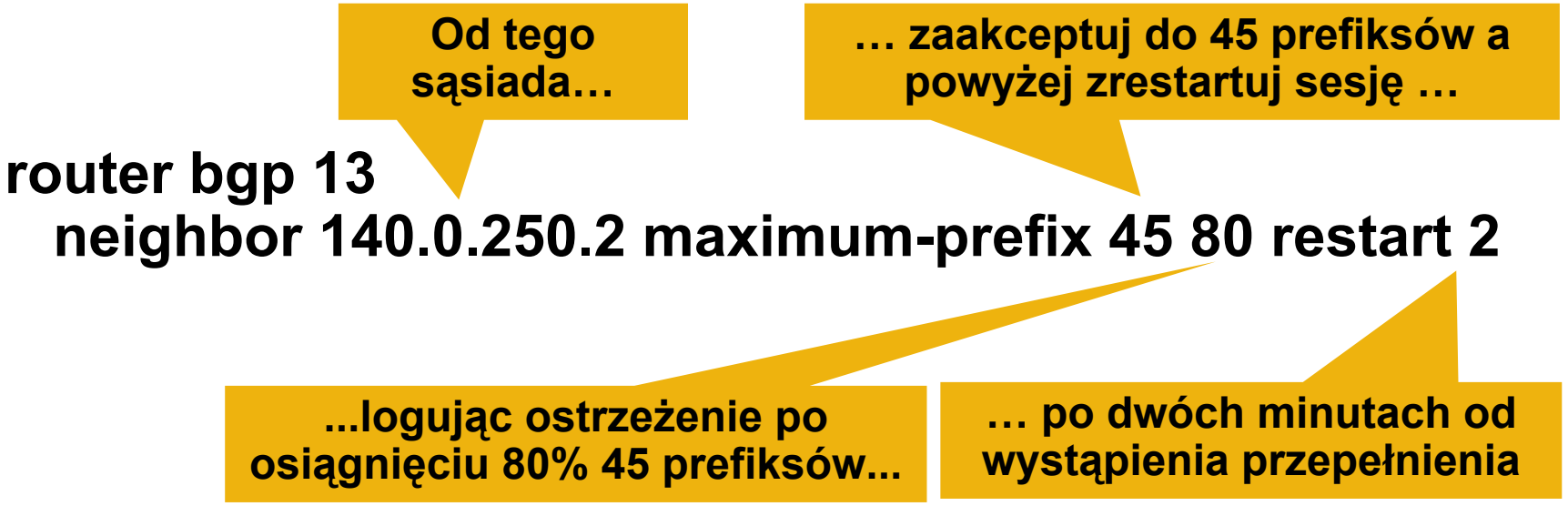
Ograniczenie ilości prefiksów w VRF

- Pobranie zbyt wielu prefiksów w VRFie może doprowadzić do potencjalnego przepełnienia pamięci (ataku DoS)
- Dla każdego VRFu można ograniczyć ilość akceptowanych prefiksów



Ograniczenie ilości prefiksów w sesji BGP

- Pobranie zbyt wielu prefiksów w sesji BGP może również doprowadzić do potencjalnego przepełnienia pamięci (ataku DoS)
- Dodatkowe polecenie dotyczące sąsiada w konfiguracji sesji BGP:



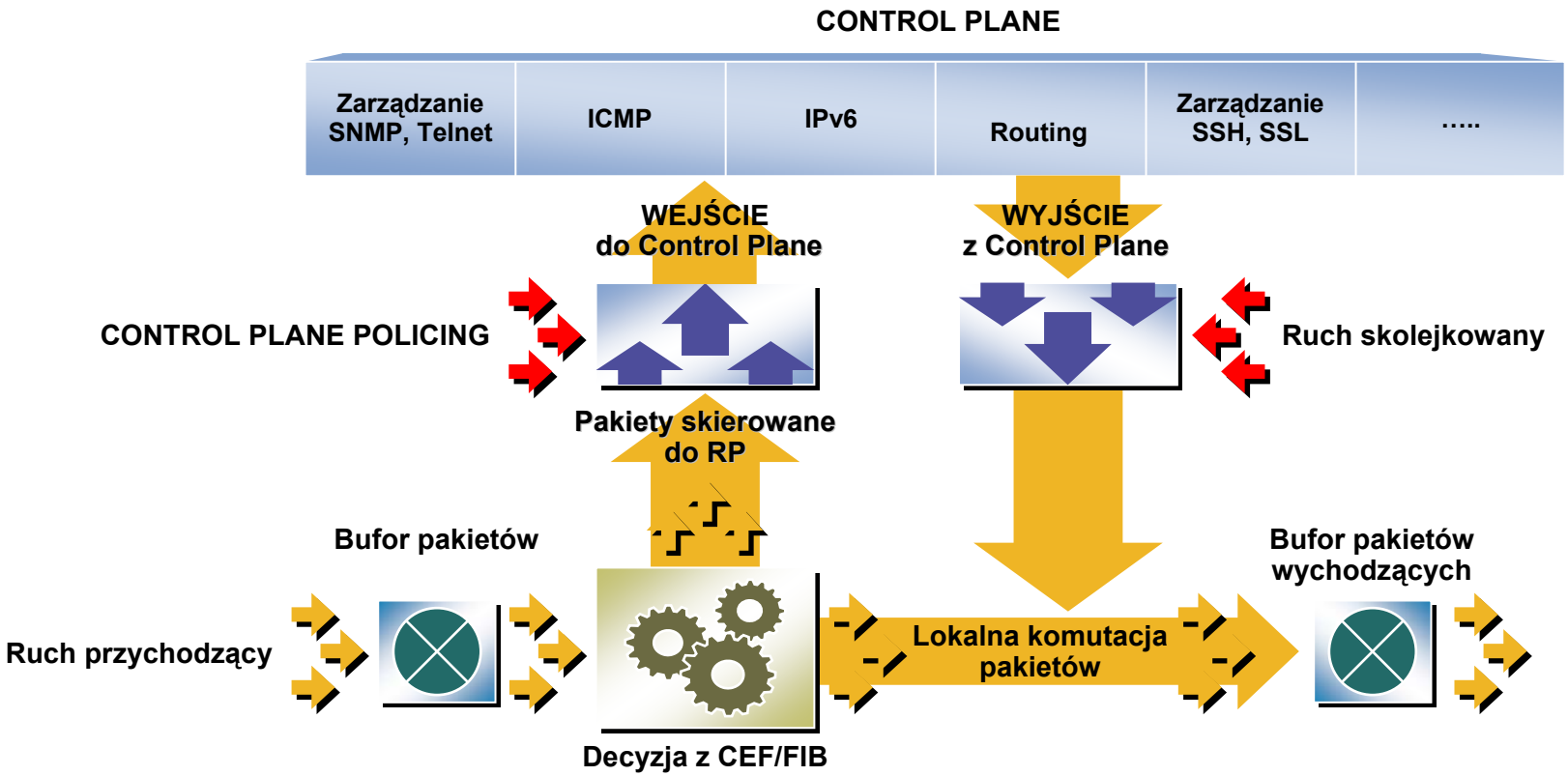
BCP - CoPP

Control Plane Policing (CoPP)

- Control Plane = „inteligencja” routera
- Mechanizm pozwala wykorzystać mechanizmy QoS Cisco IOS do ograniczenia ruchu do RP
- Pozwala efektywnie i relatywnie prosto ograniczyć możliwość wpływu ruchu sieciowego na pracę routera

  uwaga na cały ruch obsługiwany bezpośrednio przez RP, czyli np. początki sesji NAT (bez CEF)

Control Plane Policing
Jak to działa?



Jak wdrożyć CoPP

- Jaki poziom ruchu na TCP/179 jest akceptowalny?
- Przed wdrożeniem CoPP potrzebne jest dobre zaplanowanie i rozeznanie co jest normalne a co nie jest normalne w sieci

  SNMP, NetFlow, etc.
- Dokładne zaplanowanie polityki będzie trudne w przypadku bardzo dynamicznie zmieniających się warunków sieciowych oraz sposobu obsługi ruchu przez poszczególne platformy

  np. ograniczenia bit/s a pps (na Catalyst 6500 tylko bit/s)

  dla ograniczenia ruchu ISIS w CoPP należy stworzyć klasę dodatkową pasującą do całego ruchu IP, dzięki czemu w klasie class-default otrzymamy tylko ruch nie-IP (ISIS używa CLNS)

Jak wdrożyć CoPP

- CoPP jest dostępny od:

  12.3(4)T i 12.2(18)S

  Distributed CoPP - 12.0(30)S

  Cisco Catalyst 65xx/76xx - 12.2(18)SXD1

- Dokumenty wdrożeniowe:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a008052446b.html

  http://www.cisco.com/en/US/products/ps6642/products_white_paper0900aecd804fa16a.shtml

  http://www.cisco.com/warp/public/732/Tech/security/docs/nfpcatalyst.pdf

Przykładowa klasyfikacja ruchu

1. Znany ruch niepożądany—ruch który spodziewamy się ‘otrzymać’ - odrzucamy
2. Ruch krytyczny—protokoły routingu dynamicznego (control-plane)—zwykle bez rate-limit
3. Ruch ważny—SNMP, SSH, AAA, NTP (management plane)—być może rate-limit jest dobrym pomysłem
4. Normalny ruch—pozostały ruch który nie musi być złośliwy – np. ping i pozostały ICMP—rate-limit
5. Reaktywnie obsługiwany ruch niepożądany—niespodzianki – np. nowa luka bezpieczeństwa —odrzucany
6. Catch-all—cały pozostały ruch IP—rate-limit
7. Default—pozostały ruch nie-IP—być może rate-limit

Control Plane Protection (CPPr)

- Rozszerzenie CoPP pozwalające dokładniej badać ruch docierający do control-plane

  Pozwala na odrzucanie ruchu skierowanego do portów nieaktywnych

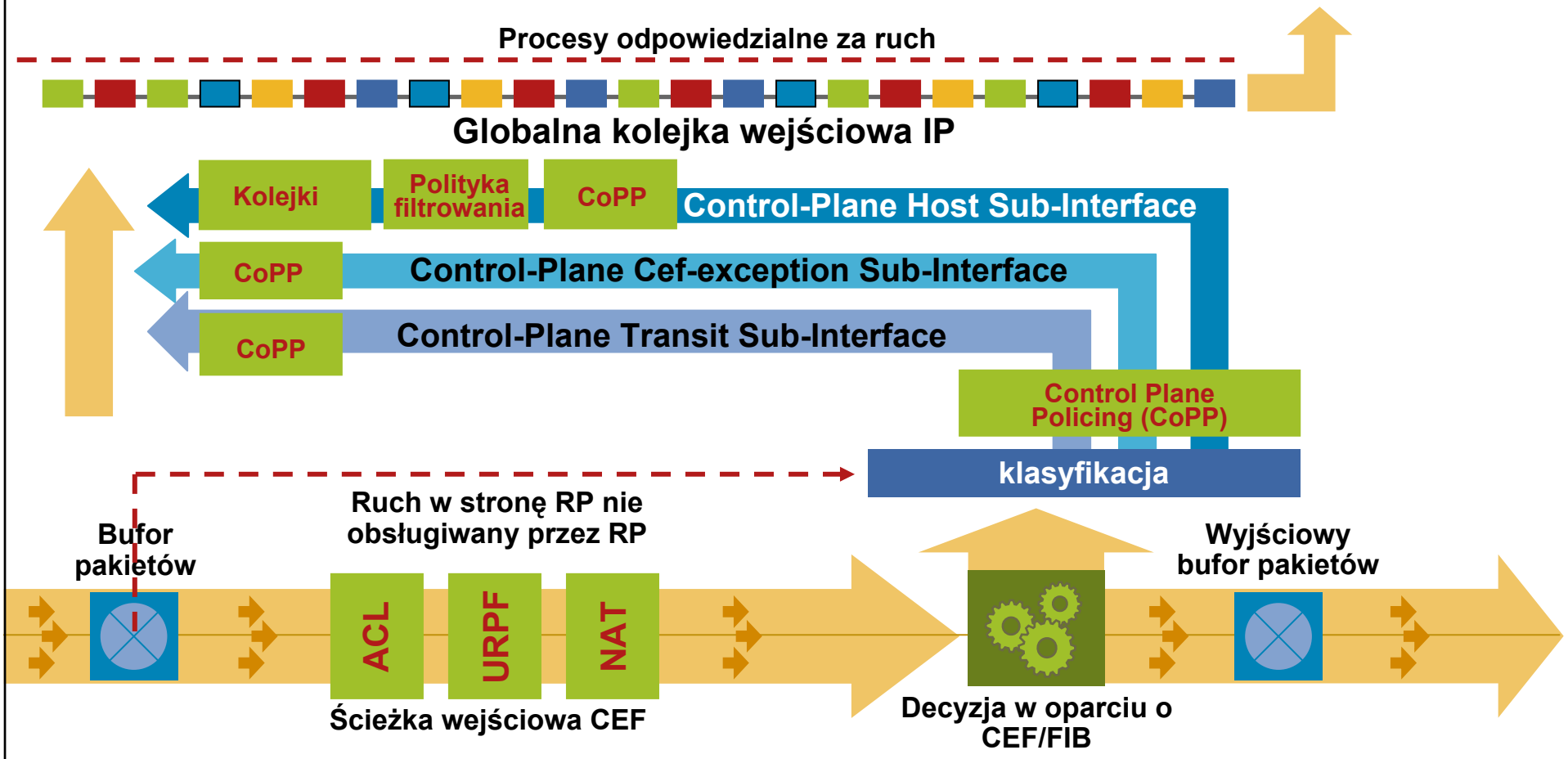
  Możliwość ograniczenia zużycia kolejek protokołów

  Jeśli CoPP i CPPr są aktywne jednocześnie, CoPP działa pierwszy

Trzy interfejsy CPPr – host, transit, cef

Warstwa kontrolna

Zarządzanie: SNMP, FTP, TFTP	ICMP	IPv6	Uaktualnienia routingu	Zarządzanie: SSH, Telnet, HTTP	…



Trzy interfejsy CPPr – host, transit, cef

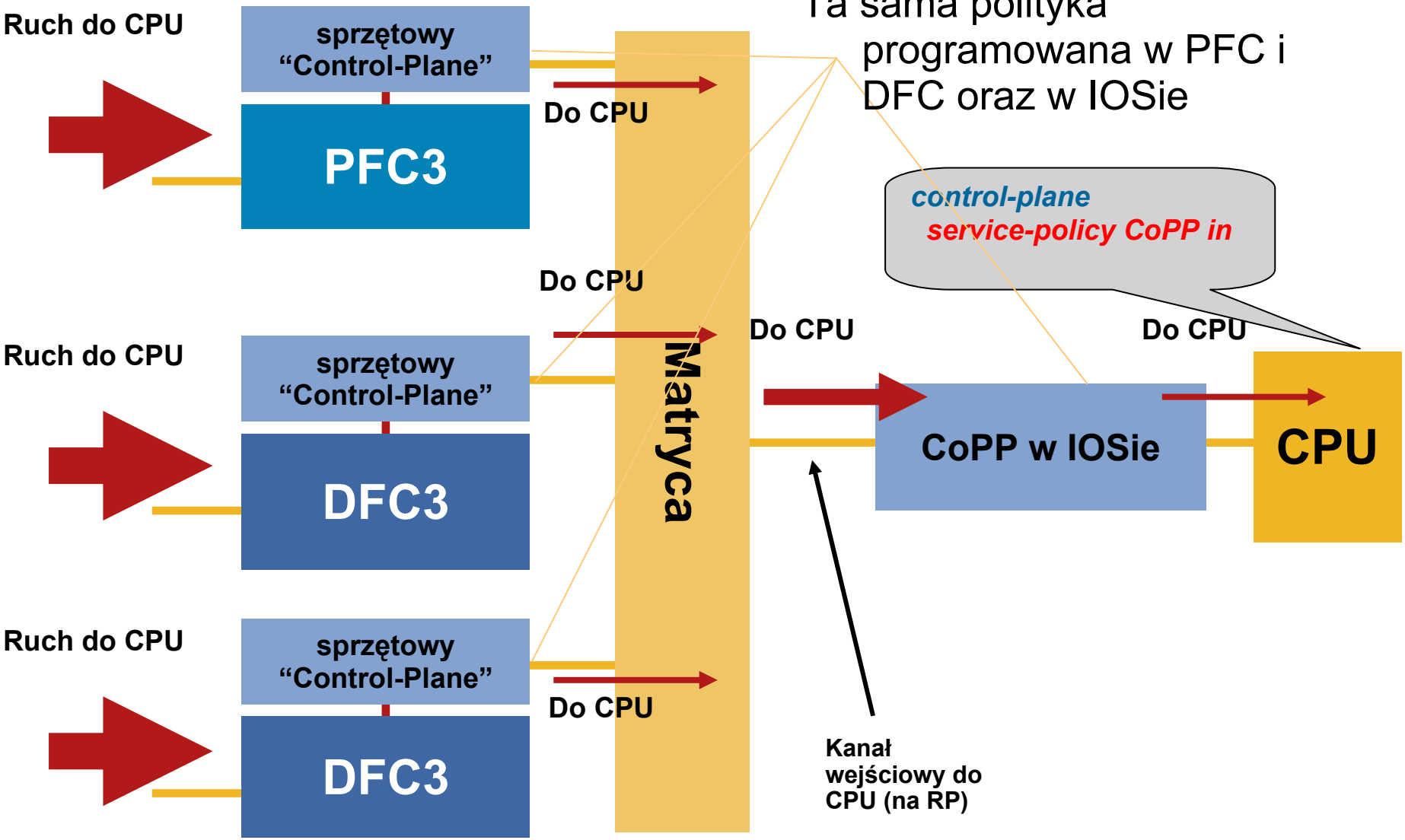
- Host – ruch otrzymywany w ramach ‘receive’ – ruch zarządzający i routingowy
- CEF exception – pakiety przekierowane do RP przed wykonaniem sprawdzenia tablicy routingu
  - Skonfigurowana funkcjonalność wymagała dodatkowej pracy
  - Pakiety miały opcje IP lub TTL=0 bądź 1
  - Pakiety przekierowane do sterownika interfejsu – ARP, keepalive dla L2
- Transit – ruch tranzytowy wysłany do RP po wykonaniu sprawdzeniu tablicy routingu ale przed wysłaniem ruchu dalej – np. CBAC czy logowanie ACL

Control Plane Protection (CPPr)

Ciekawa funkcjonalność mechanizmu – utrzymuje tablicę wszystkich otwartych portów na routerze:

```
router# show control-plane host open-ports
Active internet connections (servers and established)
Prot      Local Address      Foreign Address             Service    State
 tcp               *:22                *:0         SSH-Server   LISTEN
 tcp               *:23                *:0              Telnet   LISTEN
 tcp            *:44095       172.16.2.1:179                 BGP ESTABLIS
 tcp               *:80                *:0          HTTP CORE   LISTEN
 tcp              *:179                *:0                 BGP   LISTEN
 tcp              *:443                *:0          HTTP CORE   LISTEN
 udp               *:67                *:0       DHCPD Receive   LISTEN
 udp              *:123                *:0                 NTP   LISTEN
 udp              *:161                *:0             IP SNMP   LISTEN
 udp              *:162                *:0             IP SNMP   LISTEN
 udp            *:56837                *:0             IP SNMP   LISTEN
  .                  .                   .                   .         .
  .                  .                   .                   .         .
```

CoPP na platformie 6500/7600



CoPP na platformie 6500/7600

Ograniczenia zastosowania:

- Nie obsługuje microflow policing
- Nie obsługuje sprzętowo ruchu multicast, broadcastów w L2
- Nie obsługuje wyjątków związanych z TTL, MTU czy RPF
- Rate-limiting obsługuje tylko bit/s, nie obsługuje pps

    sprzętowy (mls) rate-limiting obsługuje pps

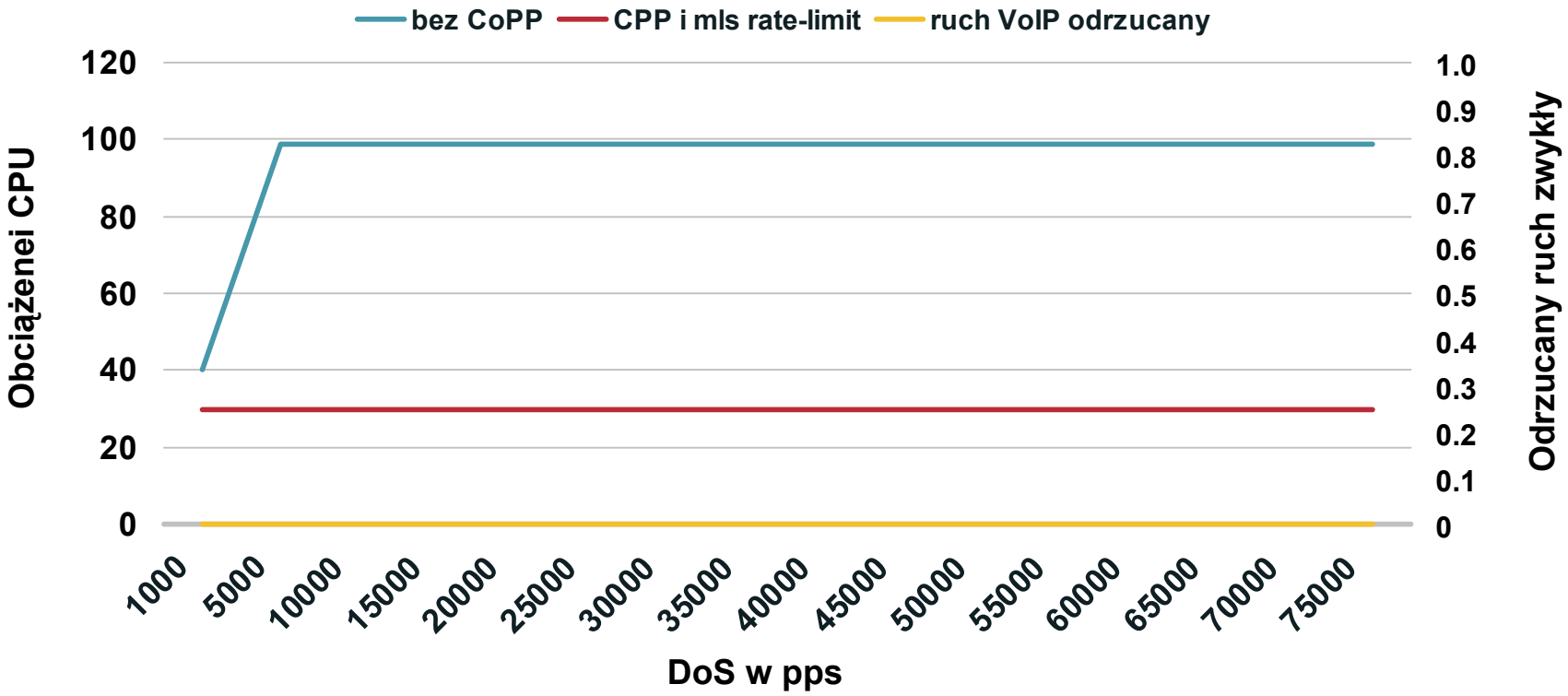
CoPP na platformie 6500/7600

Rekomendowane ustawienia - show mls rate-limit

```
switch# show mls rate-limit
   Rate Limiter Type            Status                Packets/s            Burst     Sharing
   --------------------         ----------            ---------            -----      -----
         MCAST NON RPF          Off                                -          -          -
        MCAST DFLT ADJ          On                     10000                  10         Not sharing
      MCAST DIRECT CON          Off                                -          -          -
        ACL BRIDGED IN          On                     500        10          Group:1 S
       ACL BRIDGED OUT          On                     500        10          Group:1 S
           IP FEATURES          Off                     -         -          -
          ACL VACL LOG          Off                               -          -          -
           CEF RECEIVE          Off                               -          -          -
             CEF GLEAN          On                     10000                  10         Not sharing
      MCAST PARTIAL SC          On                     10000      10          Not sharing
        IP RPF FAILURE          On                     500        10          Group:0 S
           TTL FAILURE          On                     500        10          Not Sharing
ICMP UNREAC. NO-ROUTE On                  500          10         Group:0 S
ICMP UNREAC. ACL-DROP On                  500          10         Group:0 S
         ICMP REDIRECT          On                     100        10          Group:0 S
           MTU FAILURE          Off                               -          -          -
       MCAST IP OPTION          On                     10         1          Not Sharing
       UCAST IP OPTION          On                     10         1          Not Sharing
           LAYER_2 PDU          On                     1000       100        Not Sharing
            LAYER_2 PT          Off                     -         -          -
             IP ERRORS          On                     500        10          Group:0 S
           CAPTURE PKT          Off                     -         -          -
            MCAST IGMP          On                     5000       10          Not Sharing
                        ----- output truncated ------
```

Wpływ CoPP na platformę

- Wiele równoległych ataków (multicast z TTL=1, częściowe skróty dla multicastu, opcje IP, fragmenty do wpisu ‘receive’, flood TCP SYN)
- CPU nadal trzyma się na akceptowalnym poziomie mimo trwającego ataku



Sprzętowe mechanizmy limitowania
Cisco 6500/7600

Ruch unicast	
CEF Receive	Traffic destined to the router
CEF Glean	ARP packets
CEF No Route	Packets with not route in the FIB
IP Errors	Packets with IP checksum or length errors
ICMP Redirect	Packets that require ICMP redirects
ICMP No Route	ICMP unreachables for unroutable packets
ICMP ACL Drop	ICMP unreachables for admin deny packets
RPF Failure	Packets that fail uRPF check
L3 Security	CBAC, Auth-Proxy, and IPSec traffic
ACL Input	NAT, TCP Int, Reflexive ACLs, Log on ACLs
ACL Output	NAT, TCP Int, Reflexive ACLs, Log on ACLs
VACL Logging	CLI notification of VACL denied packets
IP Options	Unicast traffic with IP Options set
Capture	Used with optimized ACL logging

Ruch multicast	
Multicast FIB-Miss	Packets with no mroute in the FIB
IGMP	IGMP packets
Partial Shortcut	Partial shortcut entries
Directly Connected	Local multicast on connected interface
IP Options	Multicast traffic with IP Options set
V6 Directly Connect	Packets with no mroute in the FIB
V6*, G M Bridge	IGMP packets
V6*, G Bridge	Partial shortcut entries
V6 S, G Bridge	Partial shortcut entries
V6 Route Control	Partial shortcut entries
V6 Default Route	Multicast traffic with IP Options set
V6 Second Drop	Multicast traffic with IP Options set

Ruch L2	
L2PT	L2PT encapsulation/decapsulation
PDU	Layer 2 PDUs

Ogólnego przeznaczenia	
MTU Failure	Packets requiring fragmentation
TTL Failure	Packets with TTL<=1

Czym są Receive ACL (rACLs)?

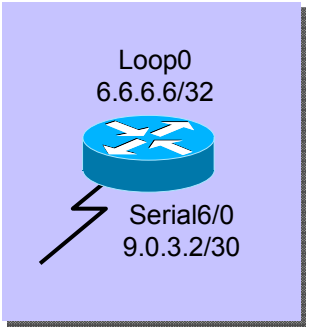
- Receive ACL filtrują ruch skierowany do RP przez wpisy zapisane jako **receive adjacencies** (tylko ruch warstw kontrolnej i zarządzającej)
- rACLs wprost wpuszczają lub blokują ruch IPv4 do RP
- rACLs NIE wpływają na ruch przekazywany przez router
- Ruch jest filtrowany już na karcie liniowej (LC), zanim zostanie przekazany do RP

Receive Adjacencies?

Wpisy w tablicy CEF dla ruchu terminowanego na routerze:

- **Interfejsy fizyczne**
- **Interfejsy loopback**

```
hrnsplab-12008c#sh ip cef
Prefix              Next Hop            Interface
.
6.6.6.6/32          receive             <-- loopback interface
9.0.3.8/30          9.0.3.1             Serial6/0
9.1.1.20/30         9.0.3.1             Serial6/0
9.2.1.8/30          9.0.3.1             Serial6/0
9.2.1.24/30         9.0.3.38            POS0/1
9.2.1.28/30         9.0.3.38            POS0/1
9.0.3.0/30          attached            Serial6/0
9.0.3.0/32          receive
9.0.3.2/32          receive             <-- attached interface
9.0.3.3/32          receive
.
```



Pakiety z polem ‘next hop’ receive są wysyłane do RP

ACL receive

- Wprowadzone w:

  12000: 12.0(21)S2/12.0(22)S

  7500: 12.0(24)S

  10720: 12.0(31)S

  router(config)# ip receive access-list [number]

- Funkcjonalność obsługuje standardowe, rozszerzone i nazwane ACL
- Podobnie jak w zwykłych ACL, widać również ilość trafień w poszczególne wpisy
- Można również używać parametru ‘log’

Działanie rACL na 12000

- CPU kart liniowych obsługuje filtrowanie ze skonfigurowanymi rACL – w czasie ataku obciążenie CPU może się zatem zwiększyć
- Wpływ obciążenia zależy od Engine karty liniowej

  E0/E1/E2: wysokie obciążenie CPU może wpłynąć na routing i ruch L2

  E2 ze specjalnym mikrokodem: wysokie obciążenie CPU → uruchamia mechanizm kolejkowania, tylko ruch oznaczony IP Precedence 6/7 trafi do RP

  E3: jedna z trzech kolejek dedykowana do obsługi ruchu z IP Precedence równym 6/7, druga dla ruchu L2 (keepalive)

  E4/E4+: osiem kolejek, osobne kolejki dla ruchu z IP Precedence 6/7 i L2 keepalives

  E5: jedna z trzech kolejek dedykowana do obsługi ruchu z IP Precedence równym 6/7, druga dla ruchu L2 (keepalive)

- rACL zawsze zwiększają szanse ochrony routera w trakcie ataku

Przykład rACL

```
!---Deny IP fragments---
access-list 177 deny   ip any any fragments
!---SSH---(no telnet allowed!)
access-list 177 permit tcp <NOC block> <loopback block> eq 22
access-list 177 permit tcp <loopback block> <loopback block> eq 22
!---BGP---
access-list 177 permit tcp <loopback block> gt 1024 <loopback block> eq bgp
access-list 177 permit tcp <loopback block> eq bgp <loopback block> gt 1024 established
!--SNMP---
access-list 177 permit udp <NOC server block> <loopback block> eq snmp
!---DNS---
access-list 177 permit udp host <DNS server> eq domain any
!---TACACS+---
access-list 177 permit tcp host <TAC+ server> <loopback block> established
!---NTP---
access-list 177 permit udp host <NTP server> <loopback block> eq ntp
!---FTP---
access-list 177 permit tcp host <FTP server> eq ftp <loopback block>
!---ICMP---
access-list 177 permit icmp any any echo-reply
access-list 177 permit icmp any any ttl-exceeded
access-list 177 permit icmp any any unreachable
access-list 177 permit icmp any any echo
!---TRACEROUTE---(this plus above icmp)
access-list 177 permit udp any gt 10000 any gt 10000
!---Profile Denies---
access-list 177 deny tcp any any
access-list 177 deny udp any any
access-list 177 deny icmp any any
access-list 177 deny ip any any
```

```
! Apply the receive ACL
rtr(config)#ip receive access-list 177
```

Ochrona control plane w IOS-XR

- Od wersji 3.6:

```
configure
 lpts pifib hardware police
  flow ospf unicast default rate 200
  flow bgp configured rate 200
  flow bgp default rate 100
 lpts pifib hardware police location 0/2/CPU0
  flow ospf unicast default rate 100
  flow bgp configured rate 300
```

BCP – bezpieczeństwo mechanizmów routingu

Ataki na protokoły routingu

- Atrakcyjnym dla włamywacza punktem ataku na sieć jest możliwość dowolnego kształtowania polityki routingu w tej sieci
- Możliwe wektory ataku w tej sytuacji to m.in.:

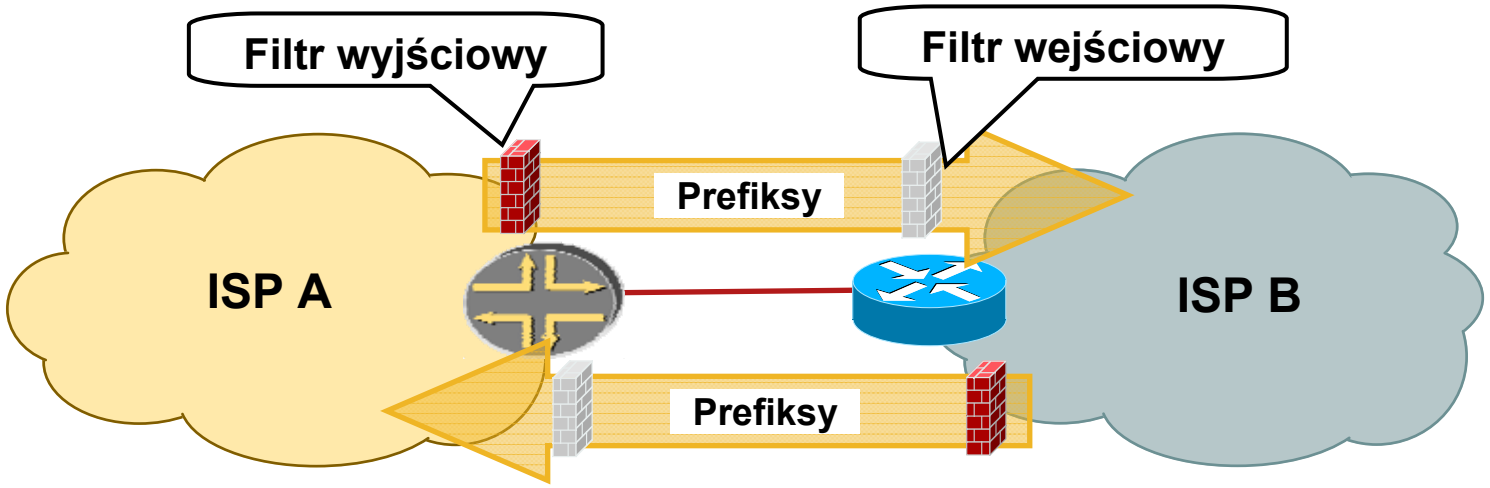
  wysłanie fałszywego uaktualnienia informacji o routingu

  odrzucanie na routerze ruchu do konkretnego prefiksu/prefiksów

  ataki typu MitM – przekierowanie ruchu

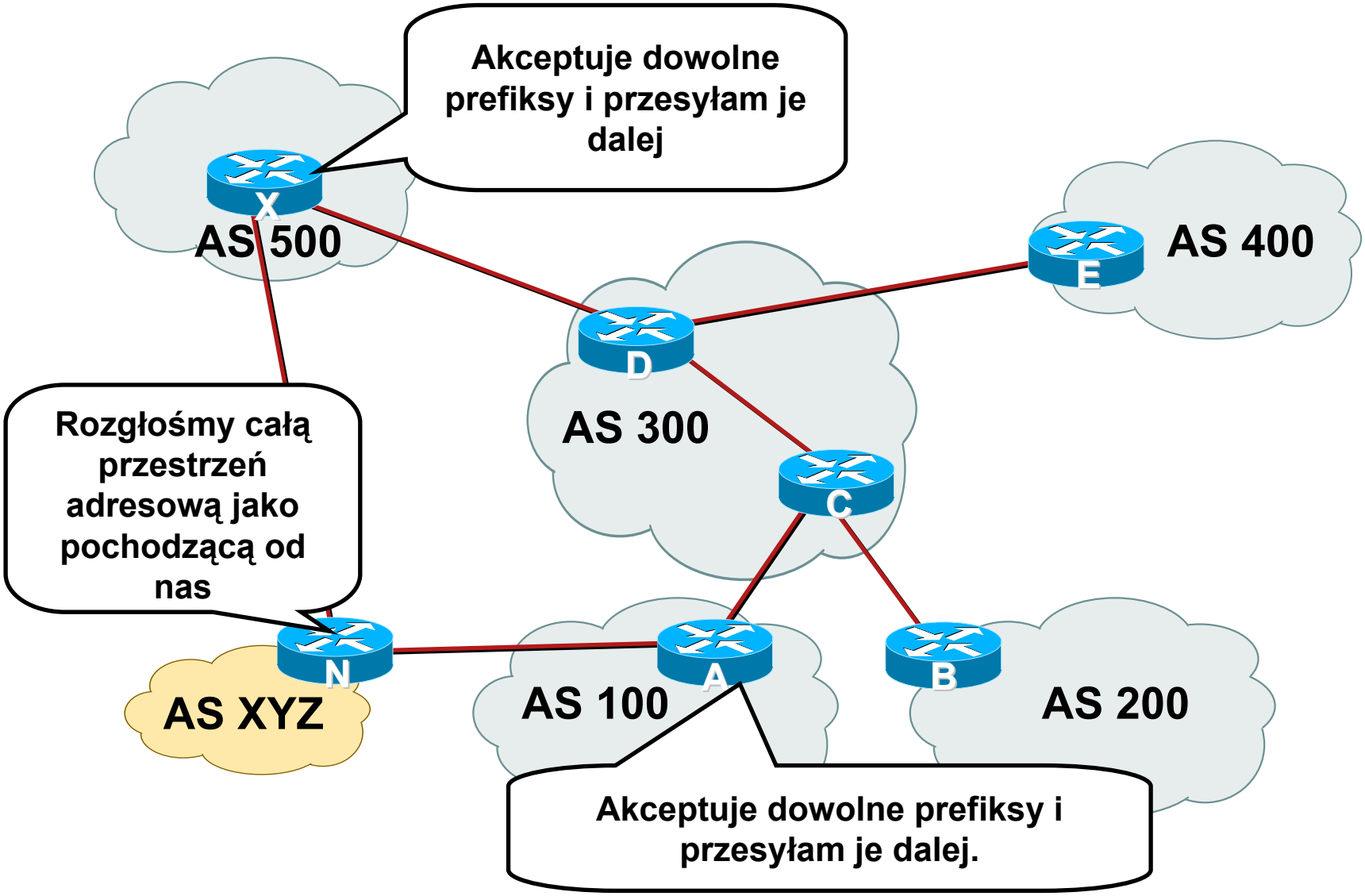
  podsłuchiwanie ruchu (wykorzystanie mechanizmów typu IP Raw Traffic Export czy Lawful Intercept)

Ograniczone zaufanie...



- ISP A akceptuje od ISP B X prefiksów z globalnej tablicy routingu
- ISP B używa filtru wejściowego by upewnić się, że tylko X prefiksów zostało zaakceptowanych
- ISP A stosuje ten sam mechanizm do kontroli prefiksów
- Oba filtry uzupełniają się i stanowią wzajemne zabezpieczenie

Garbage in – Garbage Out ?

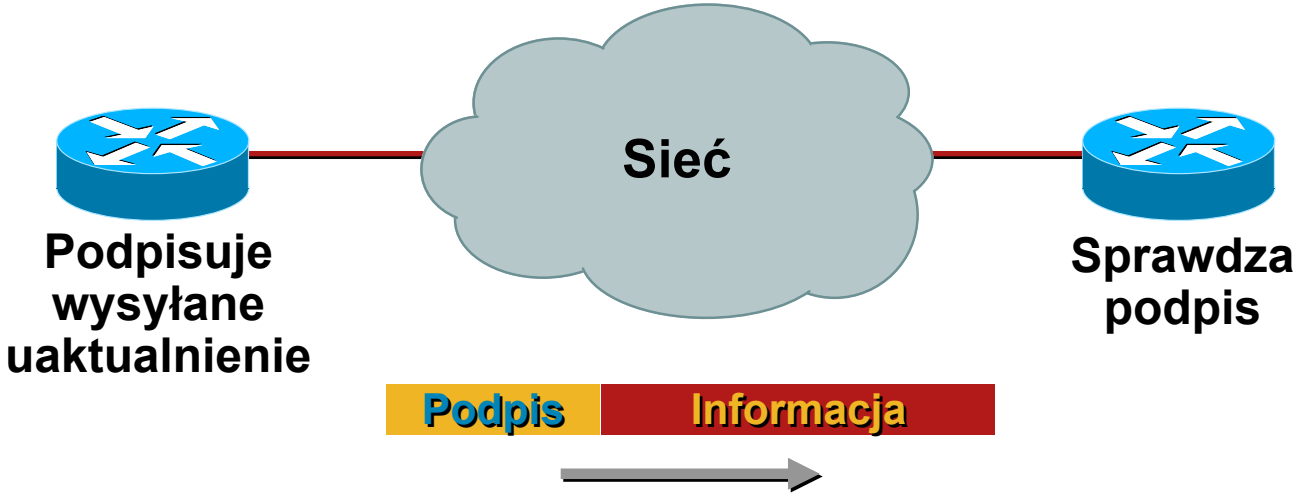


Ochrona przed rozgłoszeniami

- Narzędzia do kontroli akceptowanych per-sąsiad prefiksów to m.in.:
  - prefix-list
  - as-path list (filter-list)
  - route-map dla bardziej złożonych kryteriów

ftp://ftp-eng.cisco.com/cons/isp/security/Ingress-Prefix-Filter-Templates/

Uwierzytelnianie pakietów routingu



Certyfikuje Autentyczność sąsiada i Integralność informacji routingowej

Uwierzytelnianie protokołu routingu

- Współdzielony klucz wymieniany w pakietach

  Czystym tekstem—chroni tylko przed pomyłkami

  Message Digest 5 (MD5)—chroni przed pomyłkami i świadomą próbą ingerencji

- Wsparcie dla protokołów BGP, IS-IS, OSPF, RIPv2, oraz EIGRP

Przykład uwierzytelniania

OSPF

```
interface ethernet1
 ip address 10.1.1.1
255.255.255.0
 ip ospf message-digest-key
100 md5 qa*&gtHH3
!
router ospf 1
 network 10.1.1.0 0.0.0.255
area 0
 area 0 authentication
message-digest
```

ISIS

```
interface ethernet0
 ip address 10.1.1.1
255.255.255.0
 ip router isis
 isis password pe#$rt@s
level-2
```

Przykład uwierzytelniania

```
interface GigabitEthernet0/1
 ip address 10.1.1.1 255.255.255.0
 ip authentication mode eigrp 112 md5
 ip authentication key-chain eigrp 112 112-keys
!
key chain 112-keys
 key 1
  key-string use-strong-password-here
```

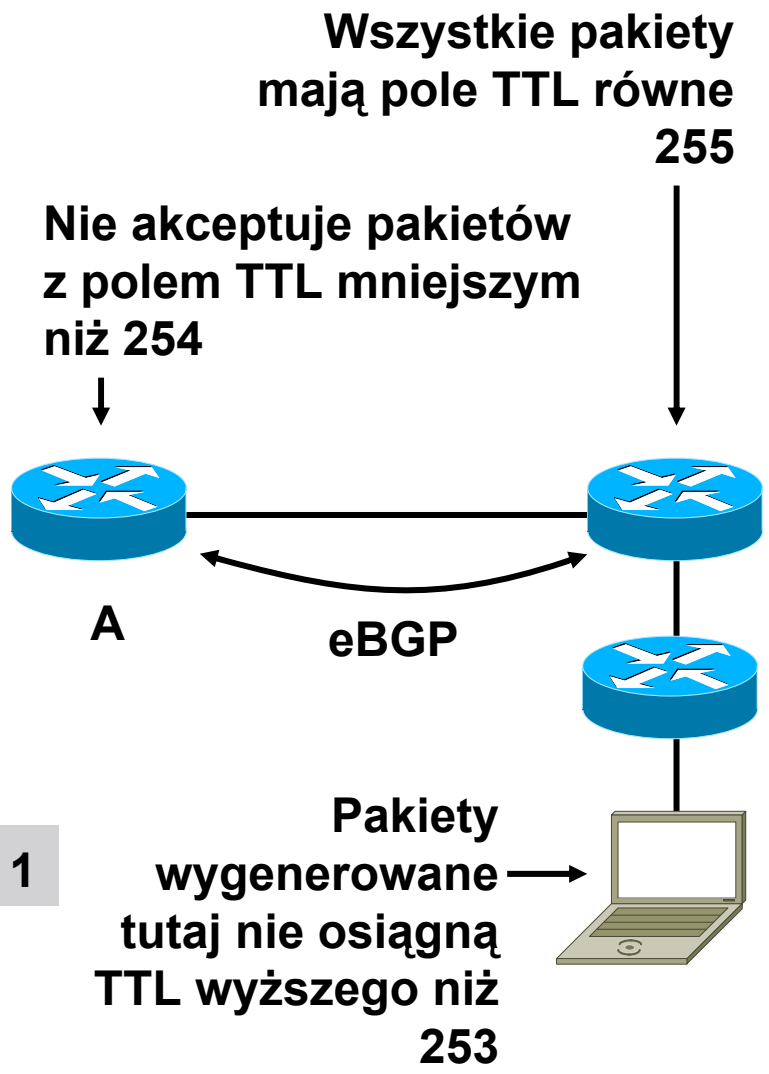
Przykład uwierzytelniania

```
router bgp 200
 no synchronization
 neighbor 4.1.2.1 remote-as 300
 neighbor 4.1.2.1 description Link to Excalibur
 neighbor 4.1.2.1 send-community
 neighbor 4.1.2.1 version 4
 neighbor 4.1.2.1 soft-reconfiguration inbound
 neighbor 4.1.2.1 route-map Community1 out
 neighbor 4.1.2.1 password 7 q23dc%$#ert
```

Generalised TTL Security Mechanism
RFC 3682

- GTSM chroni sesje BGP przed atakami z oddalonych stacji/sieci
- Routery wymieniają się pakietami IP z polem TTL ustawionym na 255, wartości poniżej 254 są automatycznie odrzucane
- Urządzenie nie podłączone bezpośrednio pomiędzy routerami nie może wygenerować takiego ruchu

neighbor x.x.x.x ttl-security hops 1



BCP – blackholing IPv4 i IPv6

Mechanizm blackholing

- Mechanizm przekazuje pakiety do „nicości”

  ...czyli na interfejs Null0

- Działa tylko dla wskazanych adresów docelowych – tak jak typowy mechanizm routingu
- Ponieważ jest zintegrowany z logiką routingu – układy ASIC odpowiedzialne za ten proces mogą ‘filtrować’ ruch z wydajnością taką, z jaką wykonują routing
- Mechanizm nie jest jednak idealny – w typowym zastosowaniu odrzucany jest cały ruch, a zatem klient zostaje skutecznie ‘zDDoSowany’

Blackholing wyzwalany zdalnie (RTBH)

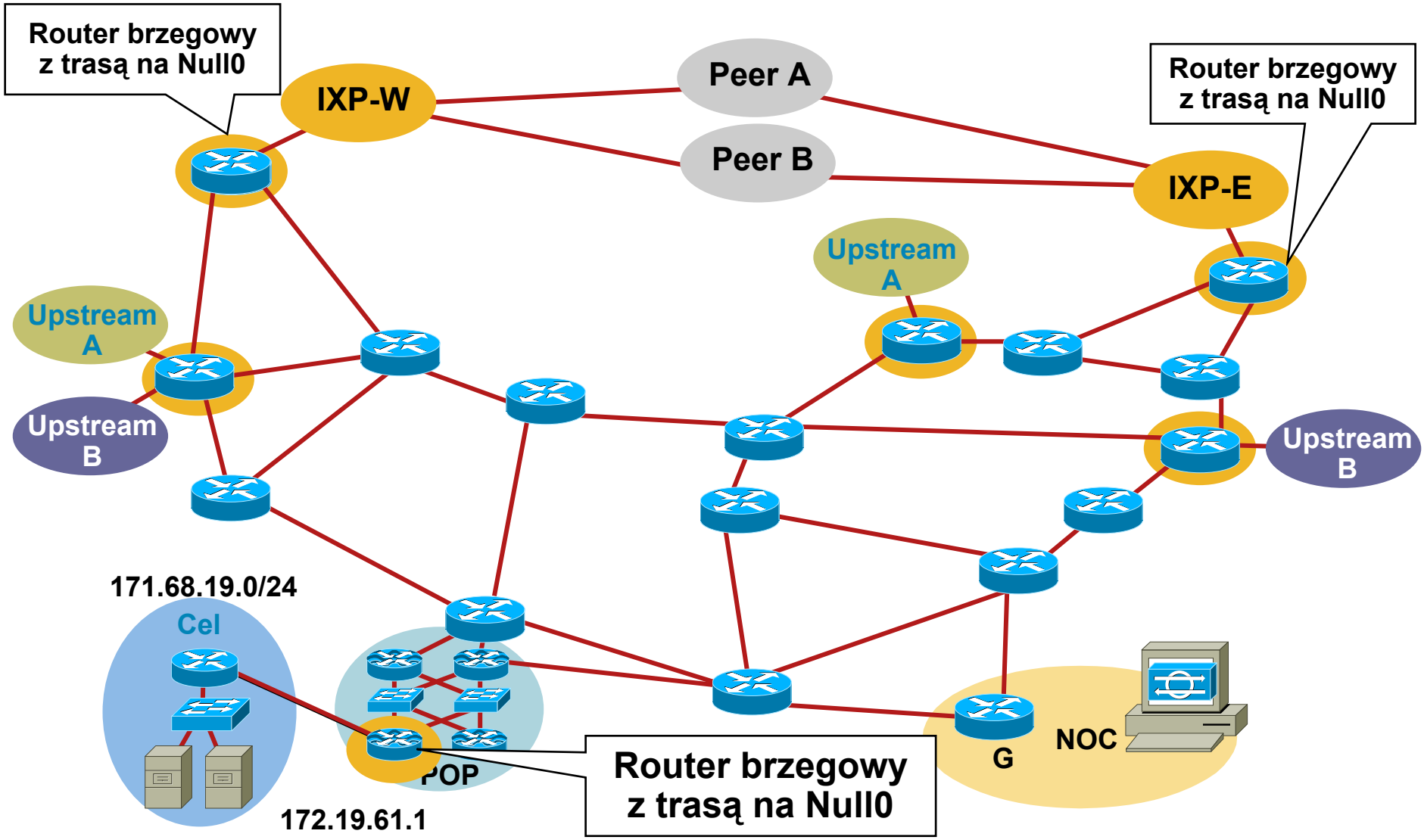
- Do obsługi wykorzystywany jest protokół BGP
- Jeden wpis z definicją routingu statycznego na routerze, przy odpowiedniej konfiguracji, może spowodować odrzucanie konkretnego ruchu w całej, rozległej sieci
- Takie narzędzie pozwala bardzo szybko i efektywnie poradzić sobie z problemami związanymi z bezpieczeństwem – atakami DDoS

Krok 1: przygotowanie routerów

- Wybierz mały blok adresów nie używany w Twojej sieci do niczego innego – pula 192.0.2.0/24 jest zwykle optymalna
- Na każdym z routerów który w przypadku ataku ma odrzucać ruch, zdefiniuj trasę statyczną wskazującą na wybrany adres (adresy) i interfejs Null0

```
ip route 192.0.2.1 255.255.255.255 Null0
```

Krok 1
Przygotowanie routerów



Krok 2

Przygotowanie routera ‘inicjującego’

- Router powinien być częścią siatki iBGP, ale nie musi akceptować żadnych tras
- Może być osobnym, dedykowanym routerem (jest to zalecane)
- Może być dowolnym rozwiązaniem, które obsługuje protokół BGP (programowo/sprzętowym)

Krok 2
Konfiguracja routera ‘inicjującego’

Redystrybucja tras statycznych

```
router bgp 65535
.
 redistribute static route-map static-to-bgp
.
!
route-map static-to-bgp permit 10
 match tag 66
 set ip next-hop 192.0.2.1
 set local-preference 200
 set community 65535:666 no-export
 set origin igp
!
```

Ustawienie pola next-hop

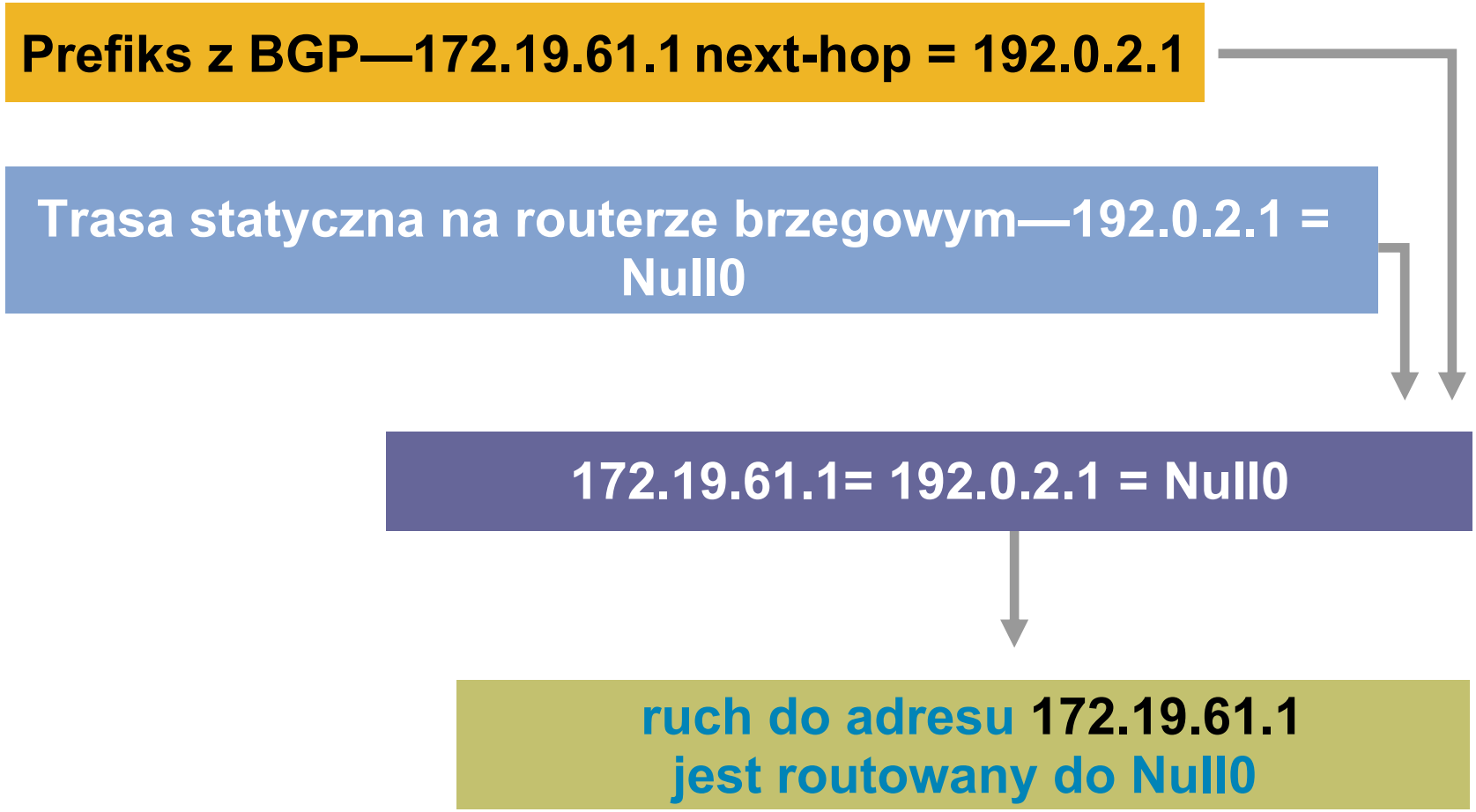
Krok 3
Aktywacja blackholingu

- Dodanie trasy do atakowanego prefiksu z odpowiednim tagiem – w naszym przypadku 66 (tak aby nie wszystkie trasy statyczne podlegały redystrybucji)

```
ip route 172.19.61.1 255.255.255.255 Null0 Tag 66
```

- Router rozgłosi prefiks do wszystkich sąsiadów BGP
- Po otrzymaniu uaktualnienia każdy z routerów przekieruje ruch do prefiksu na interfejs Null0 – efektywnie, odrzucając go bez pośrednictwa filtra pakietów

Aktywacja blackholingu – widok z FIB



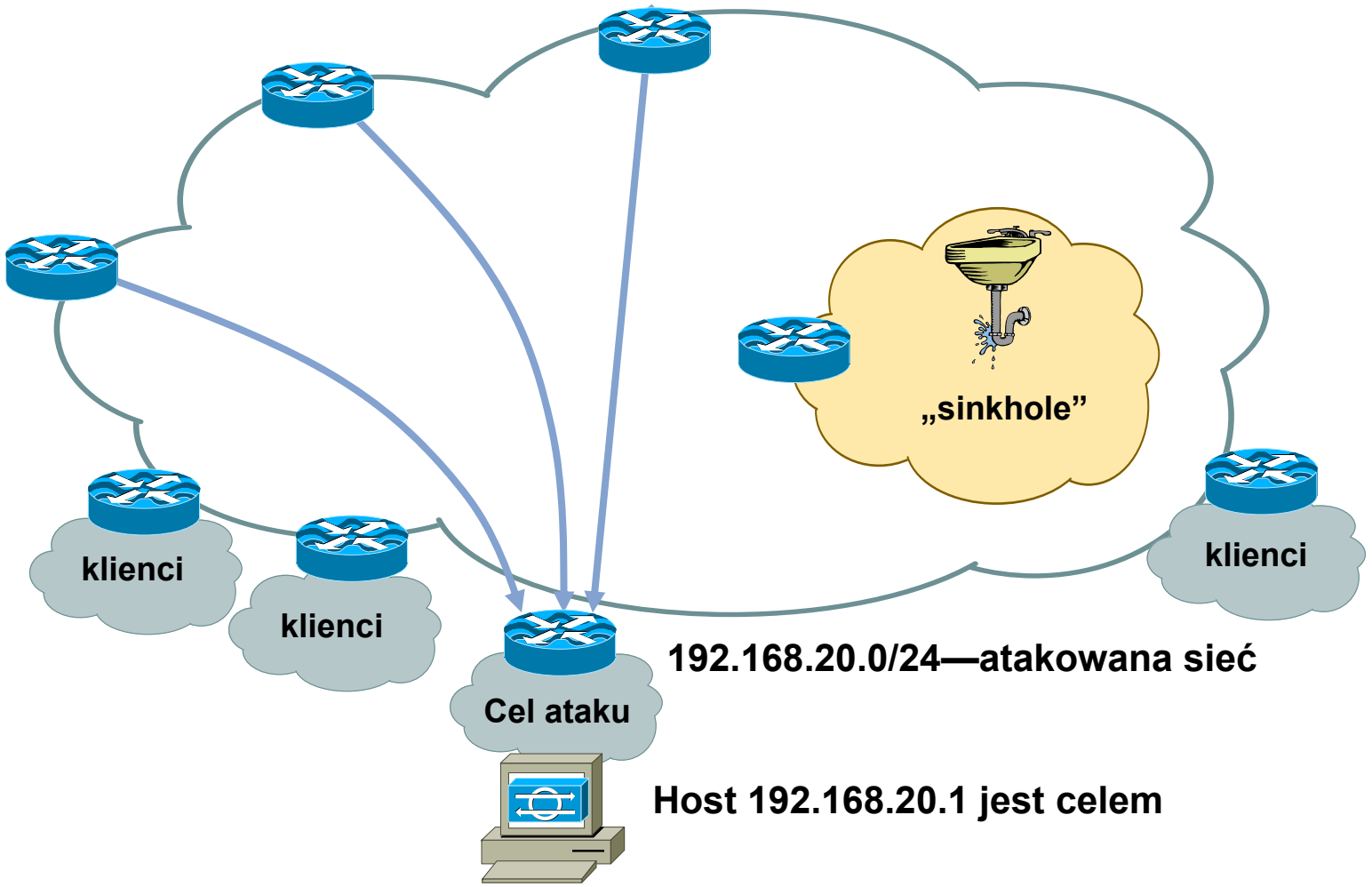
RTBH wzbogacone o community

- Wykorzystanie atrybutu community w BGP pozwala wydzielić różne ‘klasy’ ruchu odrzucanego i/lub zróżnicować rodzaj wykonywanej akcji
- Na routerach brzegowych wymaga to wskazania za pomocą route-mapy, że prefiksy akceptowane z konkretnym community mają być odrzucane (lub traktowane w inny, szczególny sposób)
- Np.:

  64999:666 – ruch do odrzucenia

  64999:777 – ruch do przekierowania do specjalnej lokalizacji

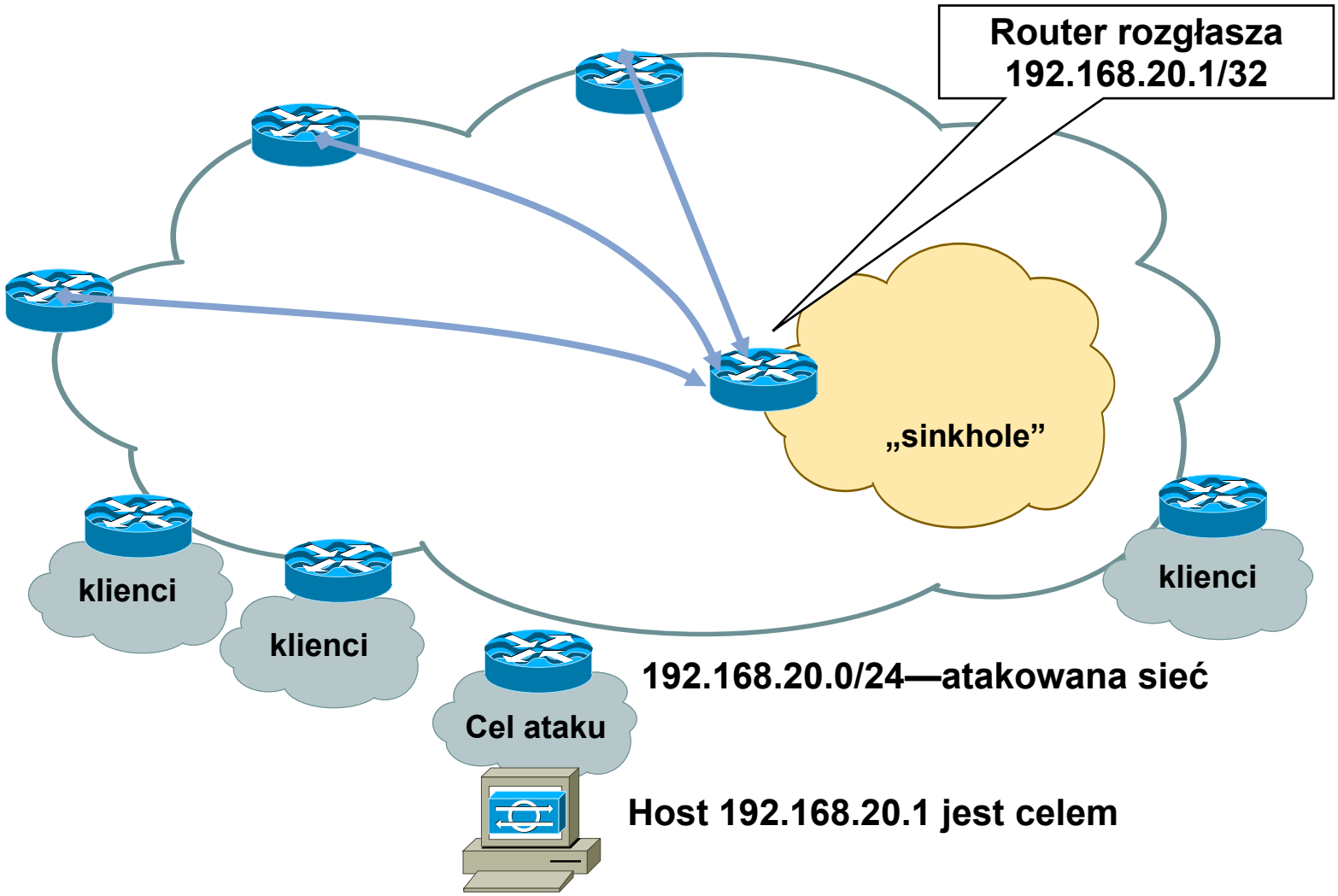
Routery/sieci ‘sinkhole’



Routery/sieci ‘sinkhole’

- Mechanizm analogiczny do ‘garnków miodu’ (honeypot), ale w odniesieniu do sieci
- Router lub stacja robocza/serwer specjalnie przygotowany do zebrania dużej ilości ruchu
- Idea działania mechanizmu polega na przekierowaniu ataku do tego specjalnego urządzenia/sieci – po to, by go zanalizować i przygotować się na przyszłe ataki
- Wiele ciekawych zastosowań – analiza ‘szumu’ informacyjnego, skanowania sieci, aktywnych prób szukania w ‘ciemnej’ i ‘szarej’ przestrzeni adresowej itp. itd.
- Wykorzystuje opisaną wcześniej dla mechanizmu blackholing infrastrukturę – odpowiednio przygotowane sesje BGP

Routery/sieci ‘sinkhole’



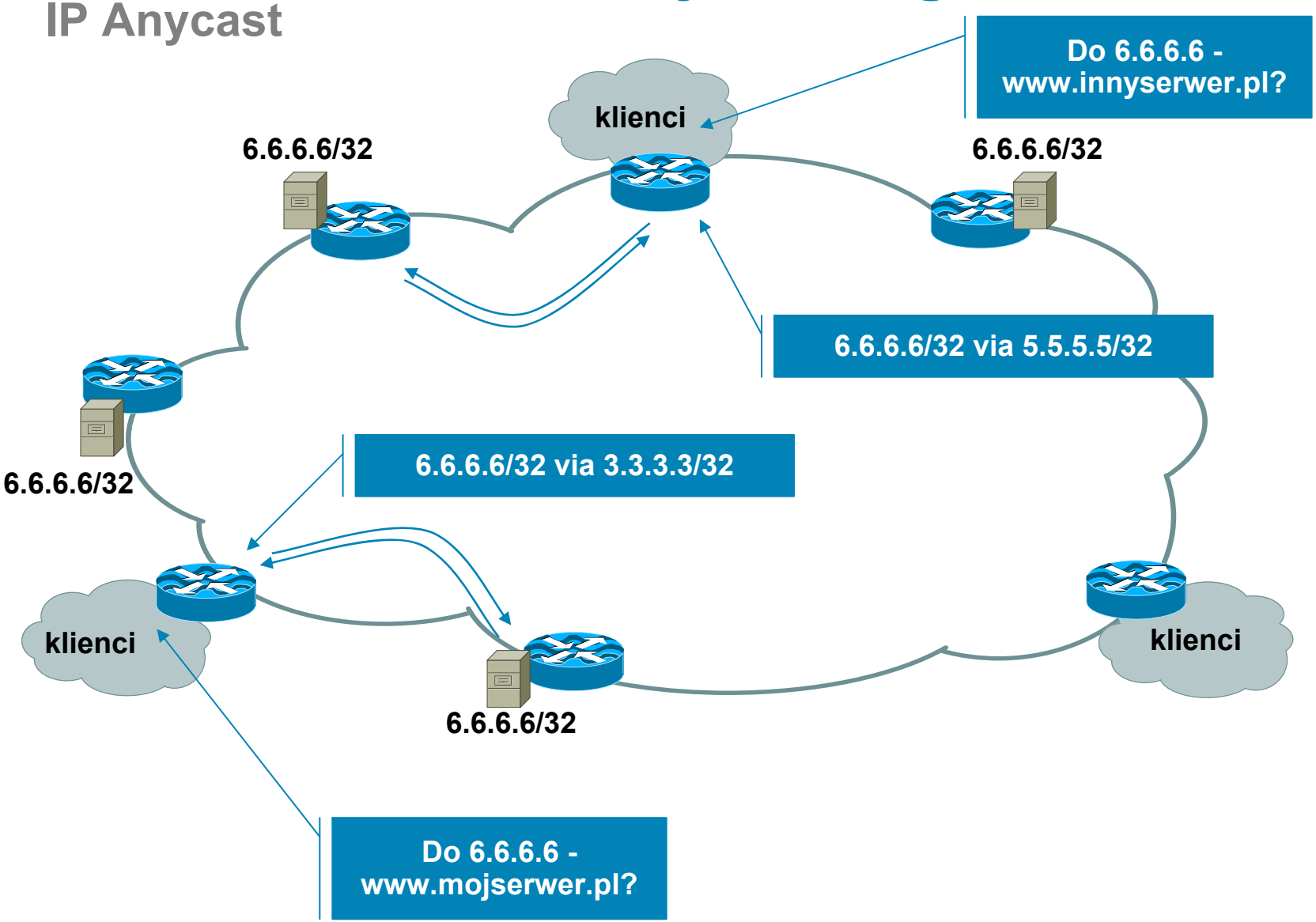
ACL a uRPF (z RTBH)?

- Podstawowe zalety ACL to:
  - dokładne dopasowanie kryteriów (porty, protokoły, fragmenty, etc.)
  - możliwość zbadania zawartości pakietu (FPM)
  - ‘statyczna’ konfiguracja w środowisku – wykluczenie ‘anomalii’
- Statyczne ACL mają jednak wady:
  - ...nie skalują się w dynamicznych środowiskach (w szczególności w trakcie ataku)
  - ...trudno zmieniać je często w sposób zorganizowany na dużej ilości urządzeń
- Wykorzystanie dwóch płaszczyzn: statycznie przypisanych ACL oraz RTBH wykorzystującego uRPF pozwala zbudować stabilną politykę bezpieczeństwa i jednocześnie zapewnić sobie sprawne narzędzie do walki z atakami – z natury dynamicznymi

BCP – ochrona usług

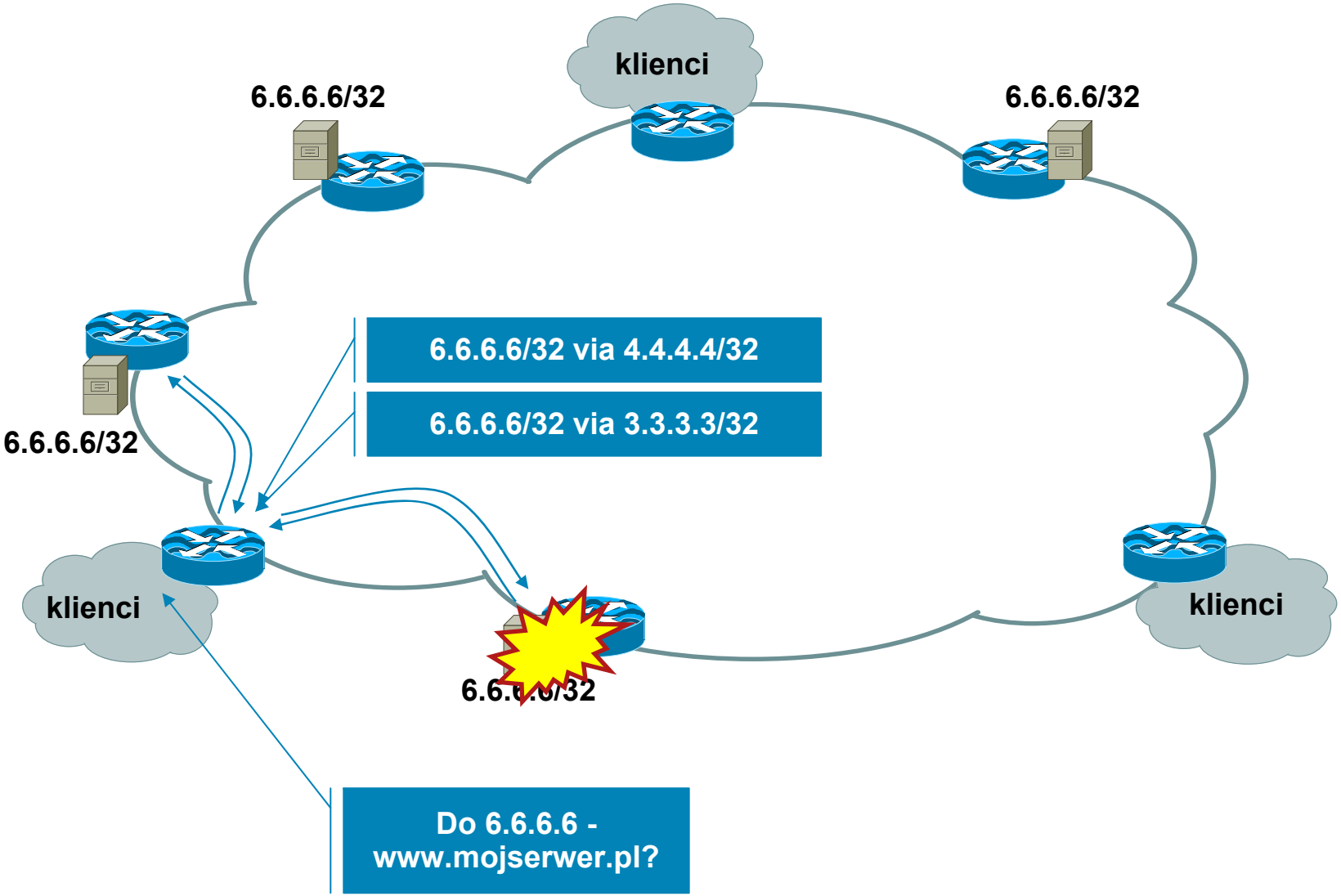
Skalowalnie ochrony - usługa DNS

IP Anycast

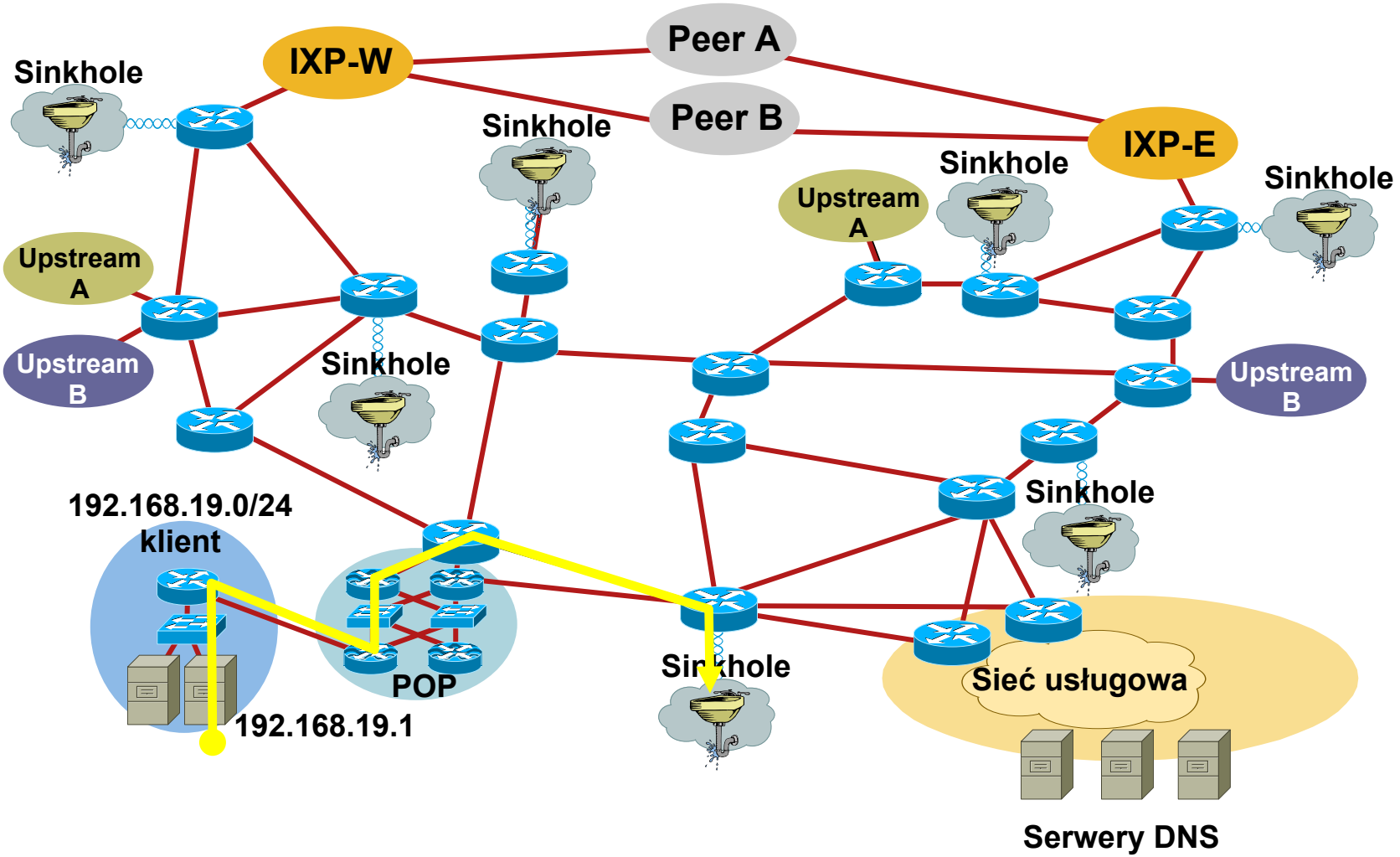


Skalowalnie ochrony - usługa DNS

IP Anycast



Anycast Sinkhole - przykład



QoS policy propagation with BGP

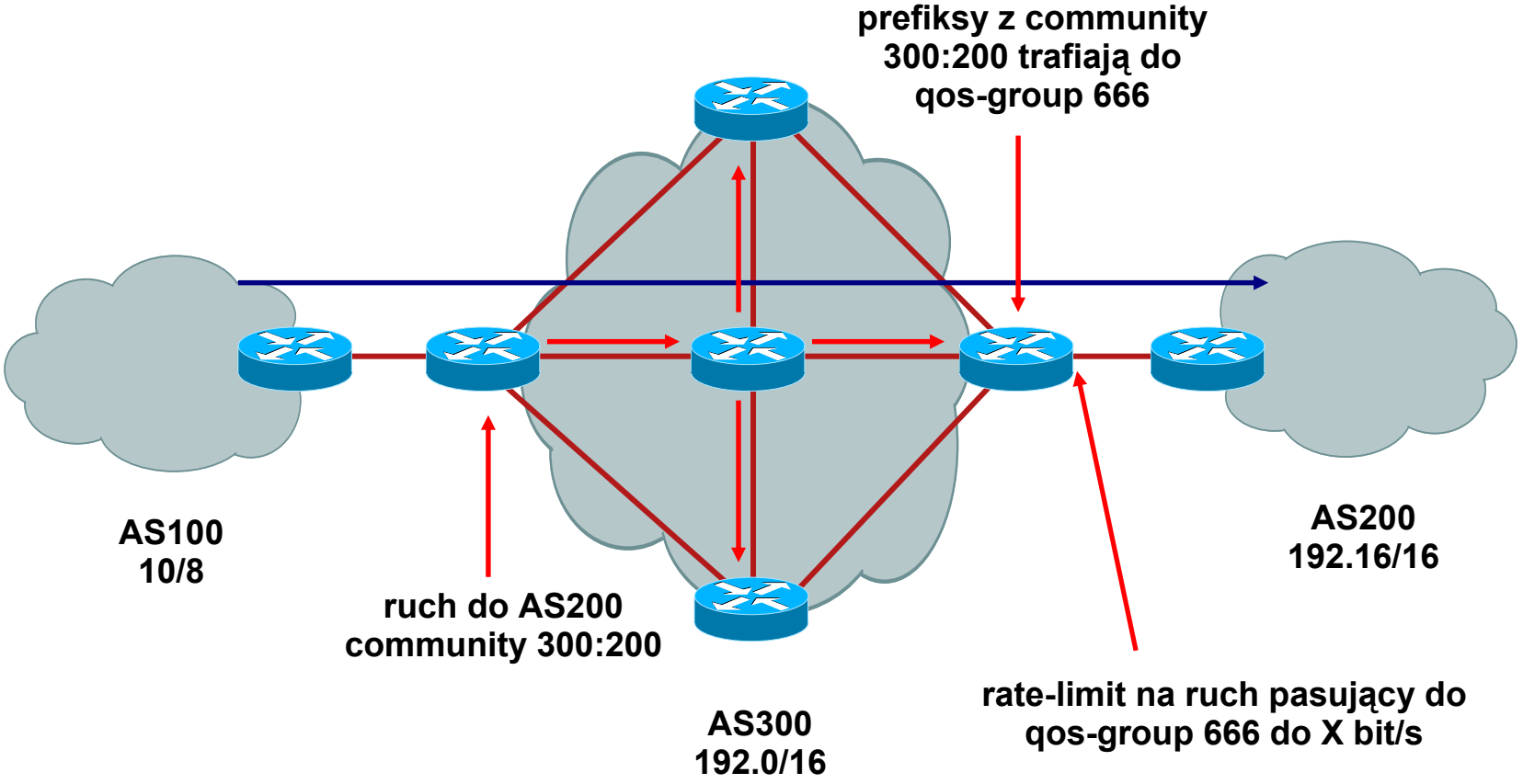
- Możliwość skalowalnej obsługi ruchu na podstawie wartości community przypisanej na wejściu do sieci
- Ruch trafiający do naszej sieci klasyfikujemy

  zostaje mu przypisana wartość community
- Na routerach brzegowych wartość community prefiksu powoduje zakwalifikowanie ruchu do/z niego do określonej QoS-group

  QoS group można wykorzystać w polityce ruchowej interfejsu – do np. ograniczenia pasma

QoS policy propagation with BGP

Topologia rozwiązania



QoS policy propagation with BGP

Konfiguracja rozwiązania – routery brzegowe AS100/AS200

```
router bgp 300
 table-map SET-QOS-POLICY
 neighbour x.x.x.x remote-as 100
 neighbour x.x.x.x route-map SET-AS100-POLICY
 neighbour z.z.z.z remote-as 300
 neighbour z.z.z.z send-community

route-map SET-AS100-POLICY permit 10
 match […]
 set community 300:100

ip community-list 1 permit 300:100
ip community-list 2 permit 300:200

route-map SET-QOS-POLICY permit 10
 match community 2
 set ip qos-group 666

interface serial 1/4
 bgp-policy destination ip-qos-map
 rate-limit input qos-group 666 256000 64000 64000
       conform-action transmit exceed-action drop
```

Pytania?