Bezpieczeństwo routerów i sieci IP

Najlepsze praktyki

Łukasz Bromirski
lbromirski@cisco.com

© 2012 Cisco and/or

Agenda

- Przetwarzanie ruchu przez routery
- Control, Management i Data Plane – zabezpieczanie w sposób zorganizowany
- BGP blackholing – IPv4 i IPv6
- IP anycast
- Q&A

© 2012 Cisco and/or its affiliates. All rights reserved.

Obsługa ruchu w sieci – perspektywa inżyniera

© 2012 Cisco and/or its affiliates. All rights reserved.

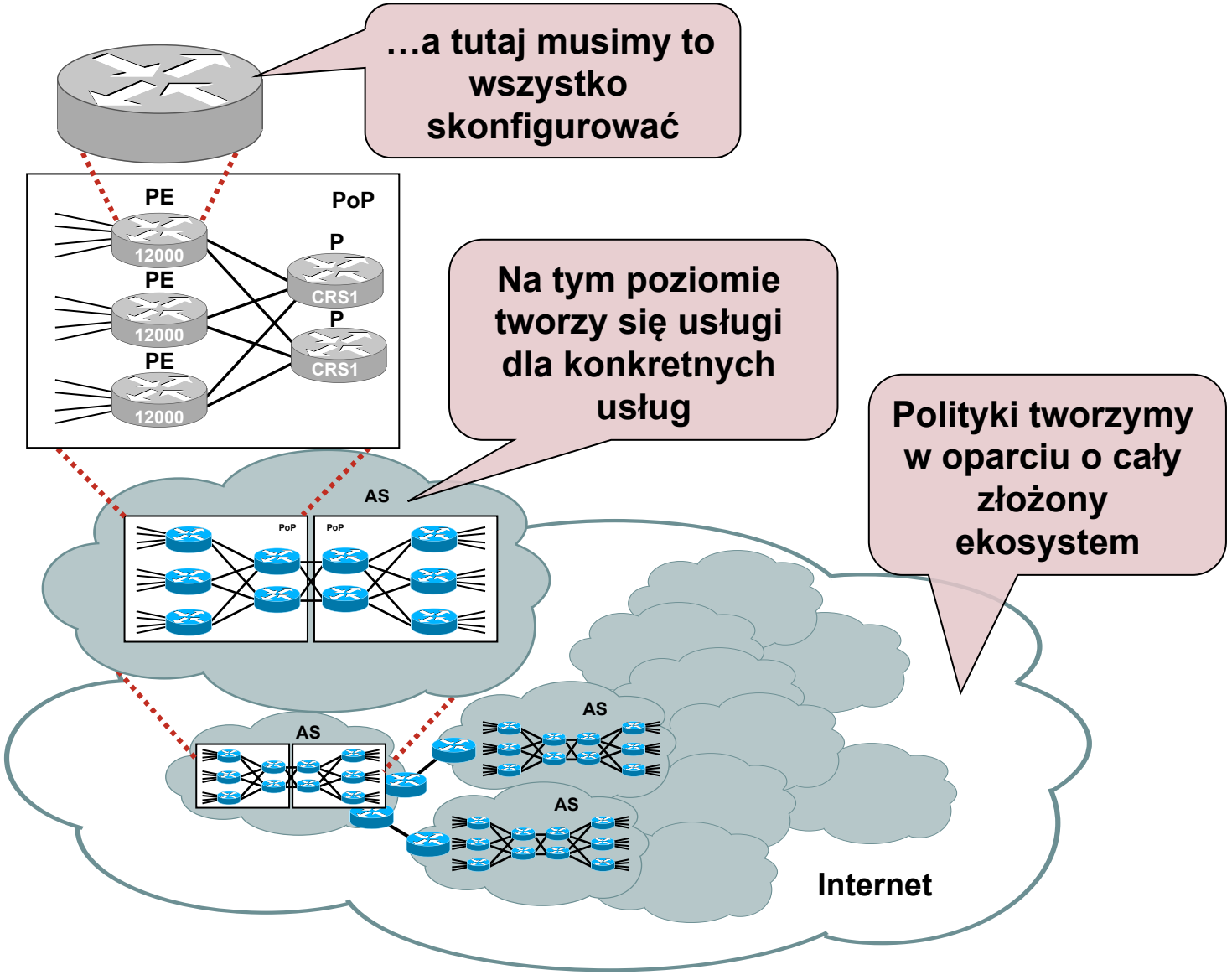
Hierarchia w sieci oczami inżyniera

Perspektywa routera

Perspektywa PoP

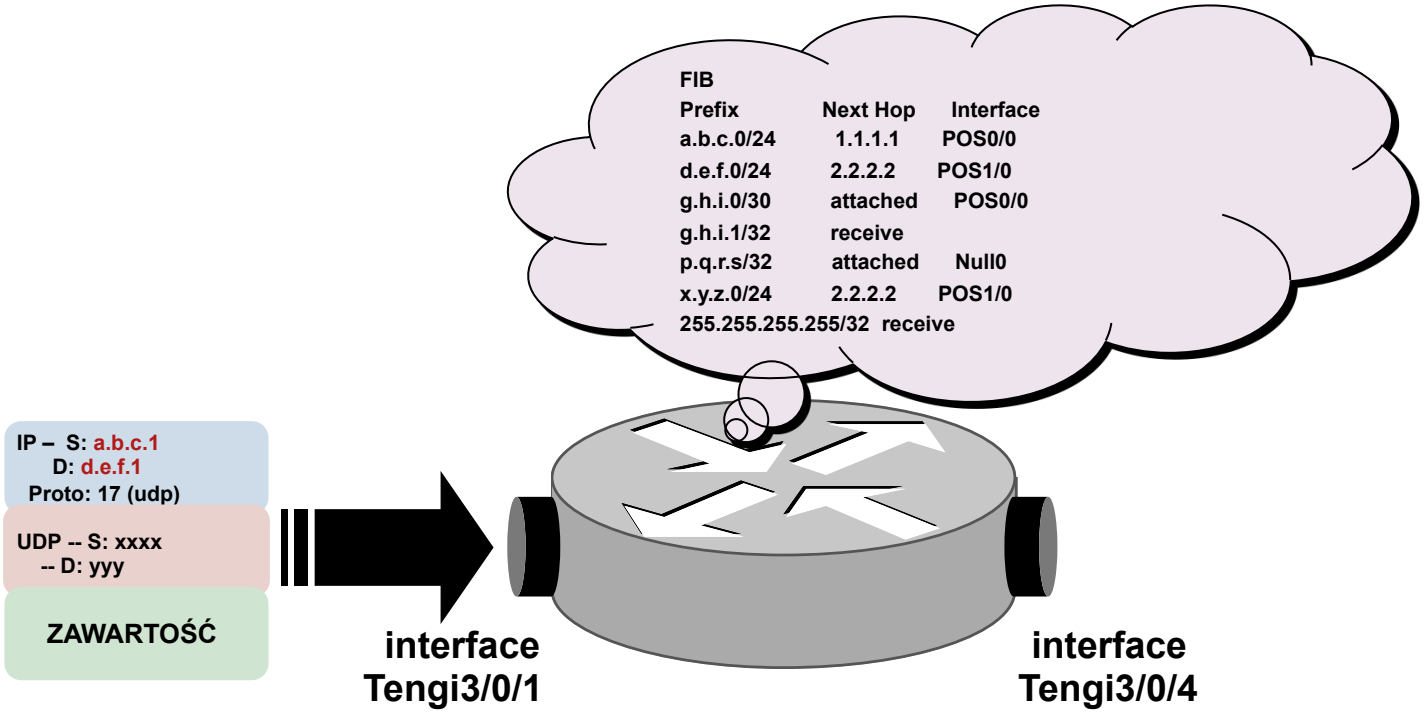
Perspektywa AS

Perspektywa Internetu



© 2012 Cisco and/or its affiliates. All rights reserved.

W tym wszystkim chodzi o pakiet…

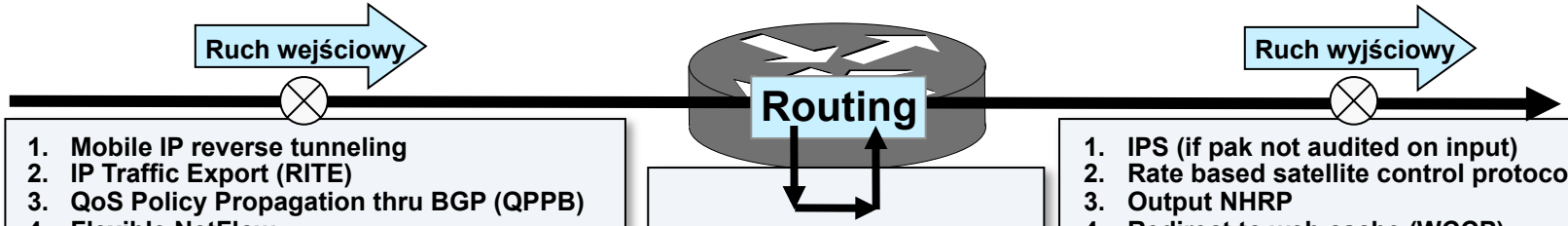


- Gdy pakiet już trafi do Internetu, jakieś urządzenie, gdzieś będzie musiało zrobić jedną z dwóch rzeczy: [1] przekazać pakiet dalej* lub [2] odrzucić pakiet

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

© 2012 Cisco and/or its affiliates. All rights reserved.

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)

© 2012 Cisco and/or its affiliates. All rights reserved.

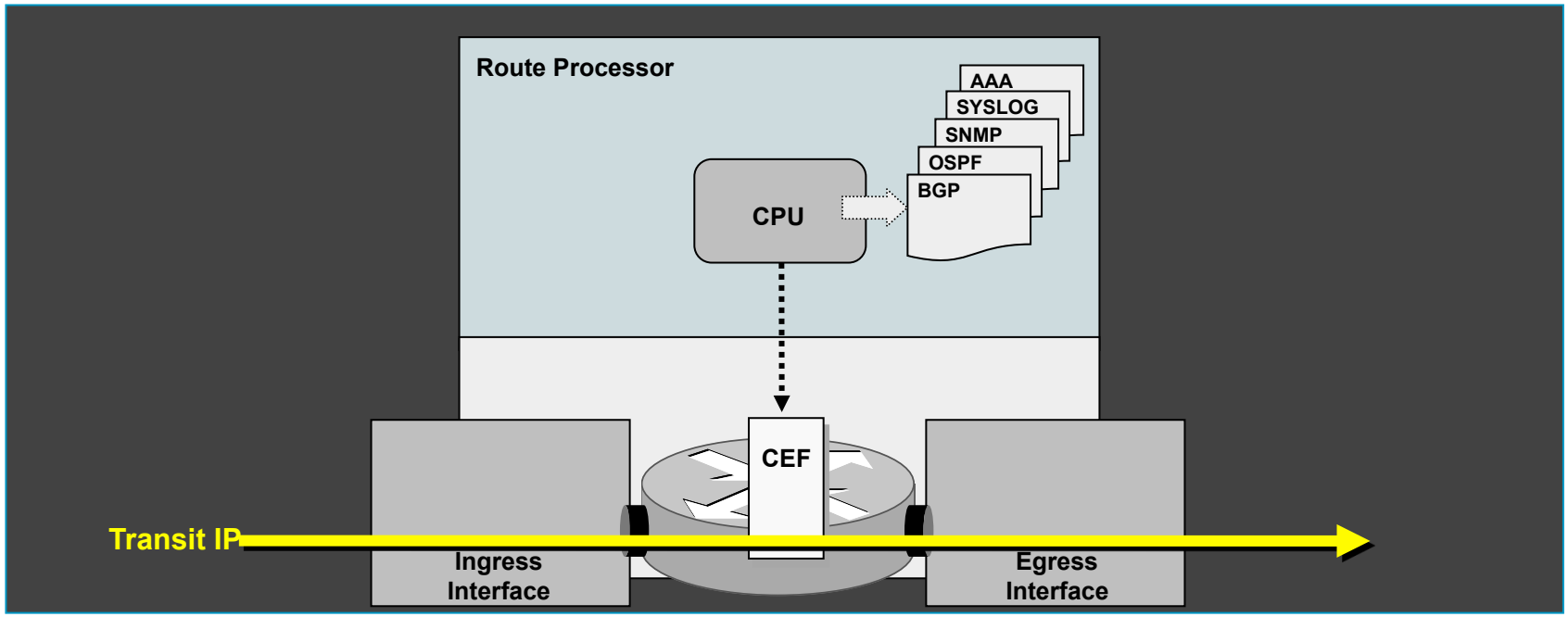
Dwie/trzy warstwy logiczne

- 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

© 2012 Cisco and/or its affiliates. All rights reserved.

Ruch tranzytowy

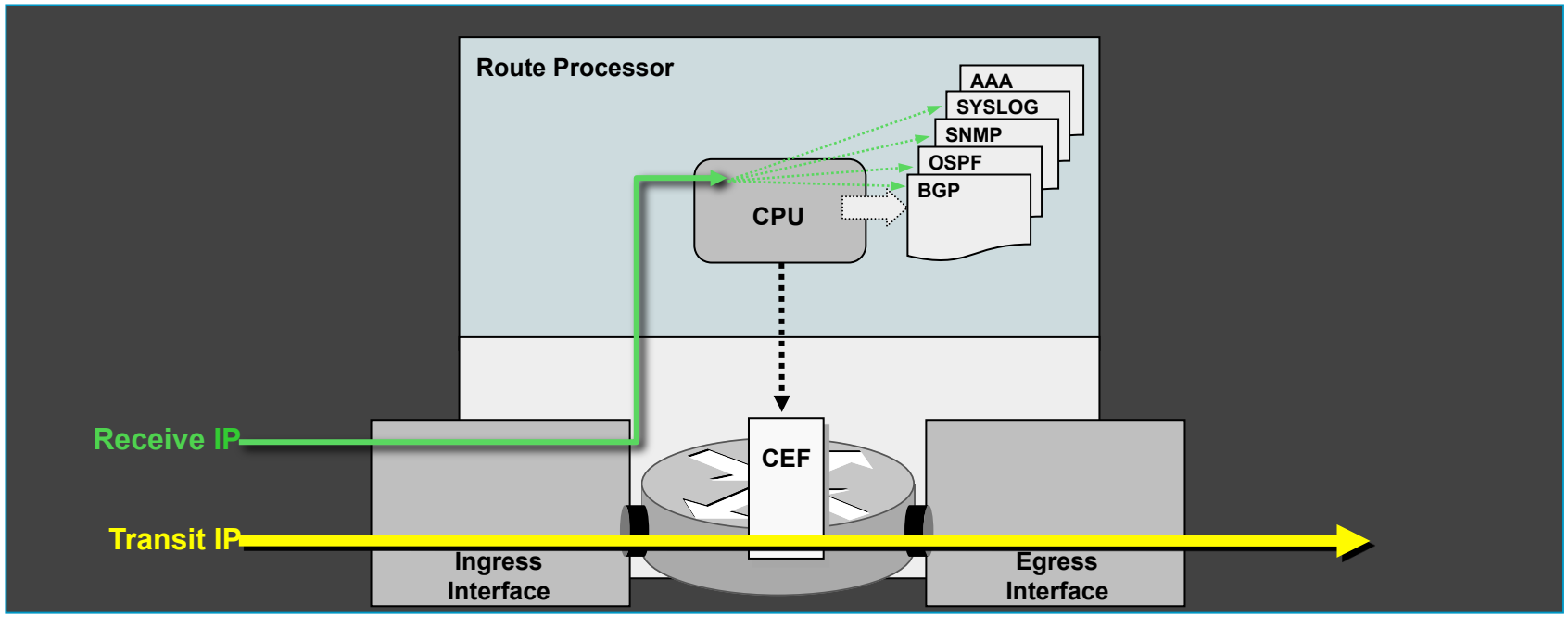
- Poprawne pakiety IP, które można obsłużyć za pomocą standardowego routingu, opartego o docelowy adres IP i nie wymagają dodatkowej obróbki.
- Docelowy adres IP nie jest adresem urządzenia, jest zatem przekazywany pomiędzy interfejsem wejściowym a wyjściowym
- Ruch pakietów obsługiwany jest przez mechanizm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



© 2012 Cisco and/or its affiliates. All rights reserved.

Ruch do routera – ‘receive’

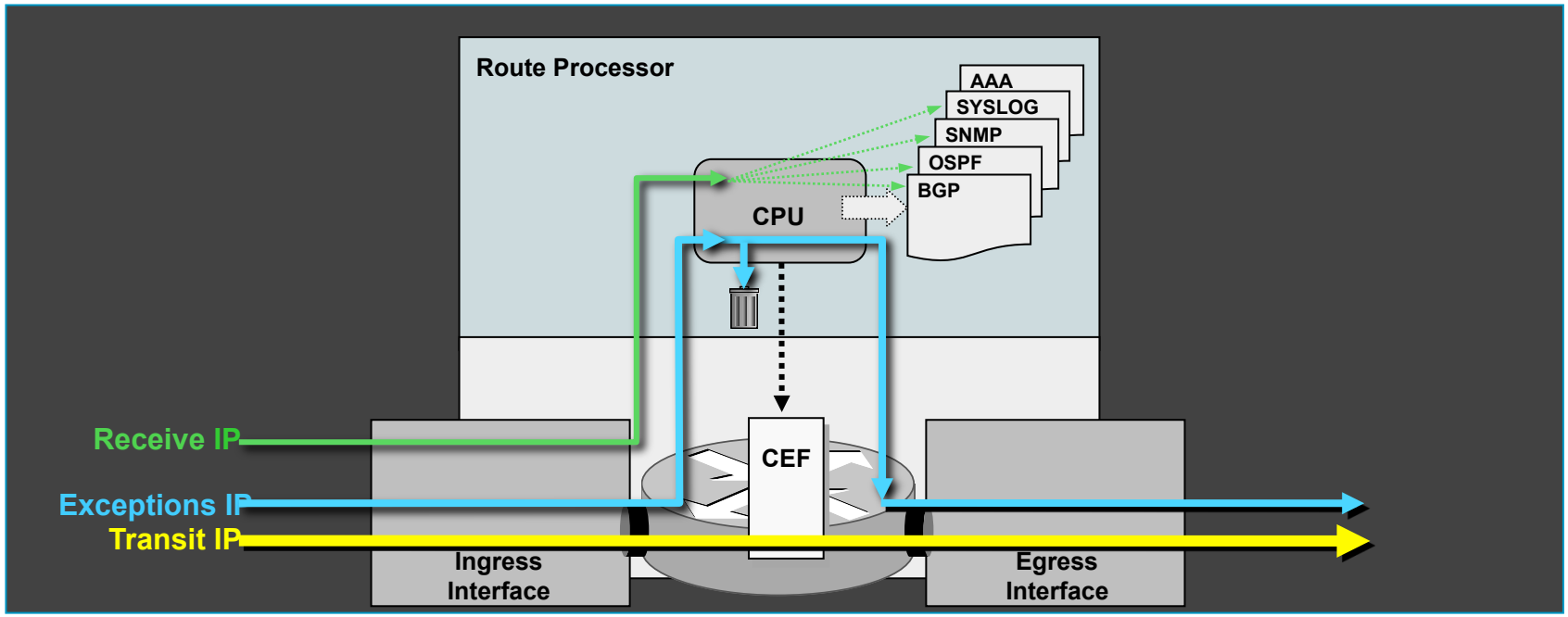
- Pakiety IP z adresem docelowym jednego z interfejsów lub usług uruchomionych na routerze.
- Docierają do procesora (na dedykowanym RP lub współdzielonego dla całej platformy) do konkretnego procesu pracującego w Cisco IOS
- Adresy IP ‘nasłuchujące’ ruchu oznaczone są w tablicy CEF terminem ‘receive’.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



© 2012 Cisco and/or its affiliates. All rights reserved.

Wyjątki – ‘exceptions’

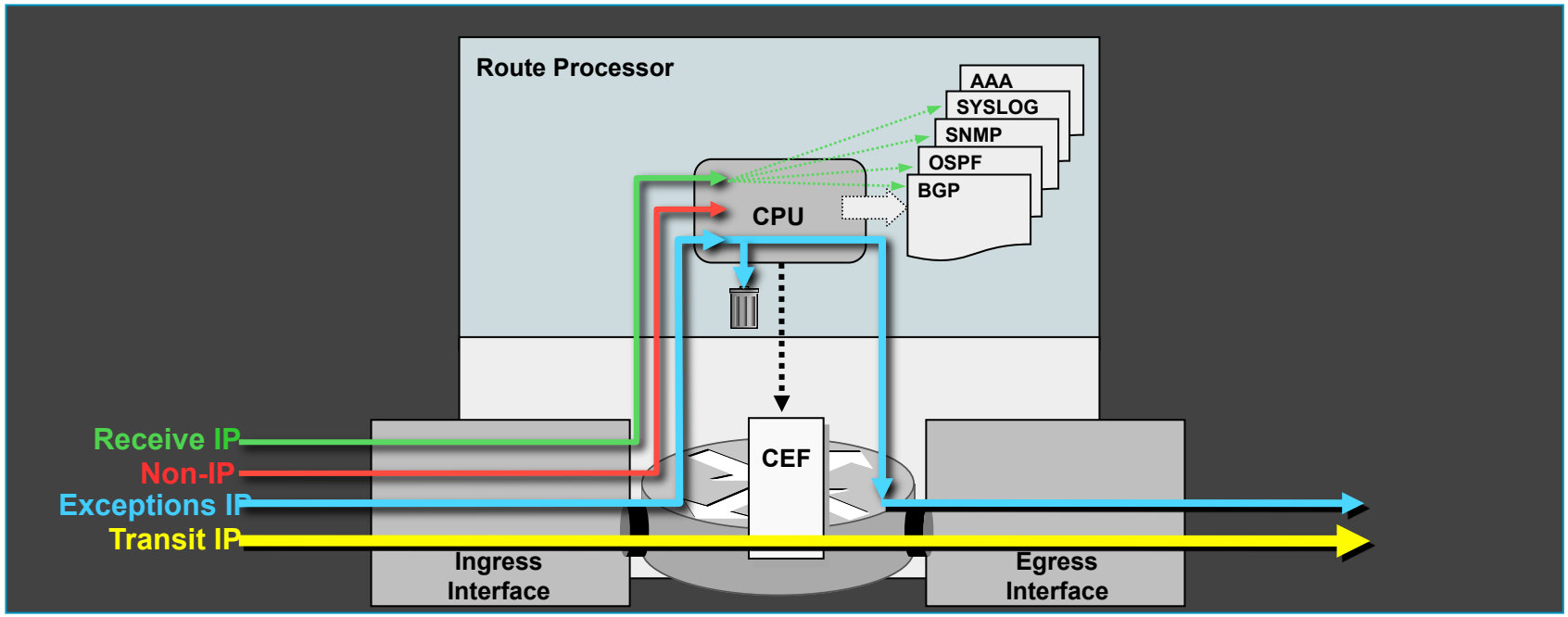
- Wyjątki to np. pakiety zawierające opcje, pakiety z wygasającym TTL. W niektórych przypadkach i architekturach mogą to być również pierwsze pakiety nowej sesji – np. pierwszy pakiet multicast, sesja tworząca wpis NAT itp.
- Wszystkie pakiety tego typu obsługiwane są przez RP



© 2012 Cisco and/or its affiliates. All rights reserved.

Ruch nie-IP

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



© 2012 Cisco and/or its affiliates. All rights reserved.

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:

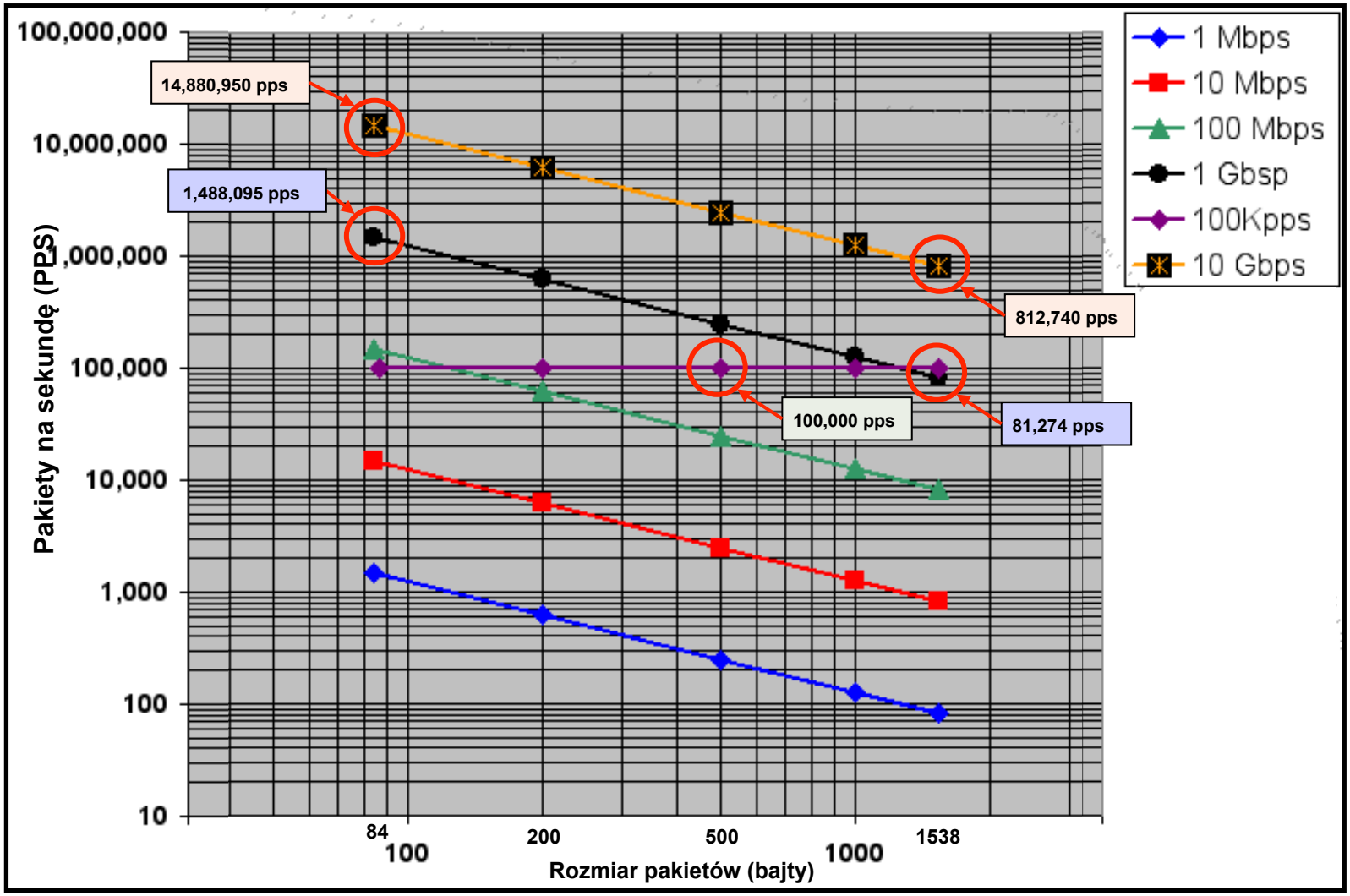
  1,000,000,000 bps/(84 B * 8 b/B) = 1,488,096 fps

- …a dla ruchu 1538 bajtów:

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

© 2012 Cisco and/or its affiliates. All rights reserved.

Koncepcja ‘pasma’ – PPS a długość PDU



© 2012 Cisco and/or its affiliates. All rights reserved.

Modele zagrożeń i ataków

	Opis
Atak wyczerpania zasobów	Atak klasy DoS, w którym atakujący stara się wyczerpać zasoby atakowanego służące do świadczenia usługi – można go przeprowadzić bezpośrednio na ofiarę, w ramach tranzytu dużej ilości ruchu lub w wyniku odbić (z ew. wzmacnianiem)
Atak fałszowania adresu źródłowego	Atak wykorzystujący pakiety z losowym adresem IP – atakujący stara się ukryć swoją tożsamość, zaciemnić obraz ataku lub wykorzystać relacje pomiędzy stronami oparte o adresy
Ataki na protokoły transportowe	Atak mający na celu zatrzymanie komunikacji między węzłami, lub przejęcie/wstrzyknięcie własnej informacji do sesji.
Ataki na protokoły routingu	Ataki mające na celu zatrzymać lub utrudnić/spowolnić pracę routera – formowanie się nowych sąsiedztw, zrywanie istniejących, przekierowywanie ruchu i wstrzykiwanie ruchu nieprawidłowego.

© 2012 Cisco and/or its affiliates. All rights reserved.

Hardening urządzeń

© 2012 Cisco and/or its affiliates. All rights reserved.

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/

© 2012 Cisco and/or its affiliates. All rights reserved.

Mechanizmy do wykorzystania

- Filtrowanie i ograniczanie ruchu
  - Filtry ruchowe (ACL)
  - uRPF
- Nadużycia na poziomie protokołów warstwy danych
  - Filtrowanie opcji IP – dla IPv4/IPv6
  - Fragmenty
- Tradycyjne rekomendacje dla operatorów
  - Ochrona połączenia CE<>PE
  - Ukrywanie szkieletu sieci
- Bardziej zaawansowane rozwiązania
  - BGP Blackholing & Sinkholing
  - QoS Policy Propagation z BGP
  - IP Anycast

© 2012 Cisco and/or its affiliates. All rights reserved.

Filtrowanie ruchu – BCP38 i uRPF

© 2012 Cisco and/or its affiliates. All rights reserved.

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

© 2012 Cisco and/or its affiliates. All rights reserved.

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

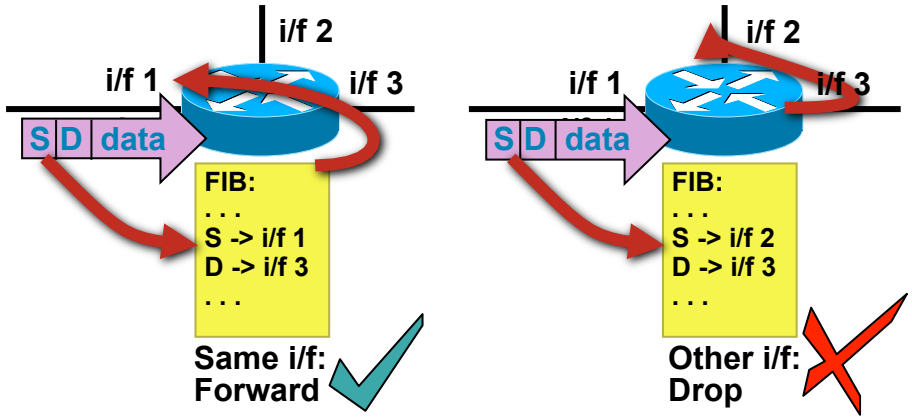
- uRPF “VRF Mode”

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

© 2012 Cisco and/or its affiliates. All rights reserved.

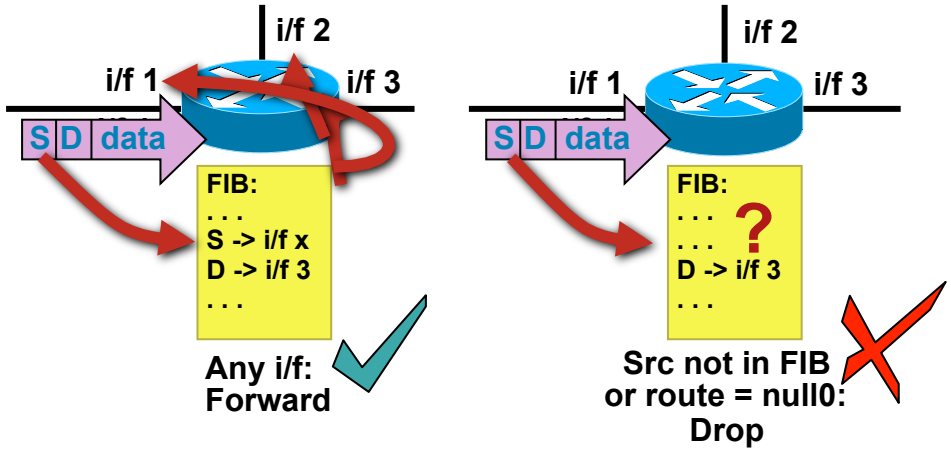
uRPF strict i uRPF loose

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



"Strict Mode"
(aka "v1")

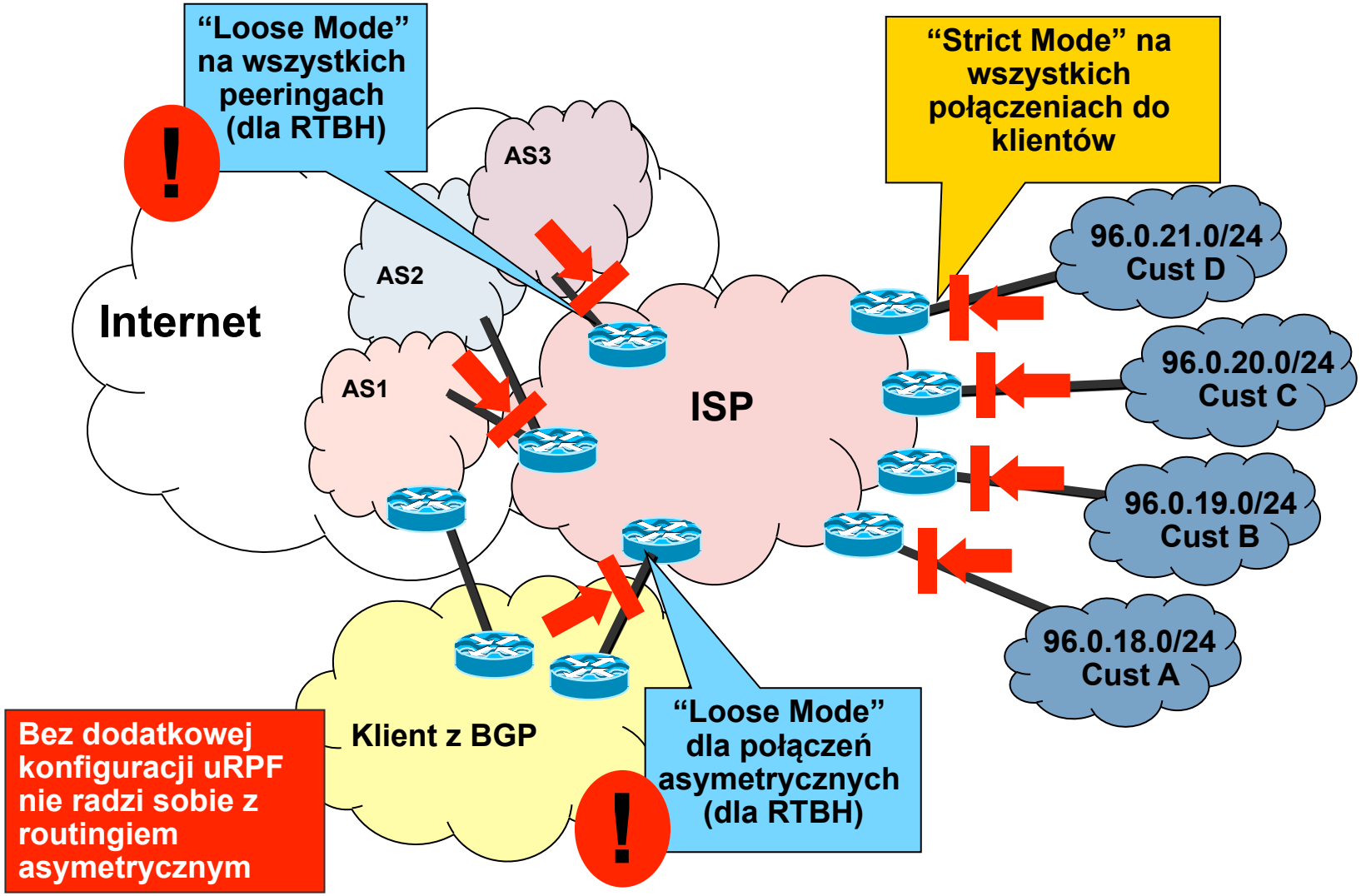
router(config-if)# ip verify unicast source reachable-via any



"Loose Mode"
(aka "v2")

© 2012 Cisco and/or its affiliates. All rights reserved.

Gdzie stosować uRPF?



© 2012 Cisco and/or its affiliates. All rights reserved.

Mechanizmy ochrony i separacji: iACL i VRF

© 2012 Cisco and/or its affiliates. All rights reserved.

Czym jest VRF?

- Virtual Routing & Forwarding

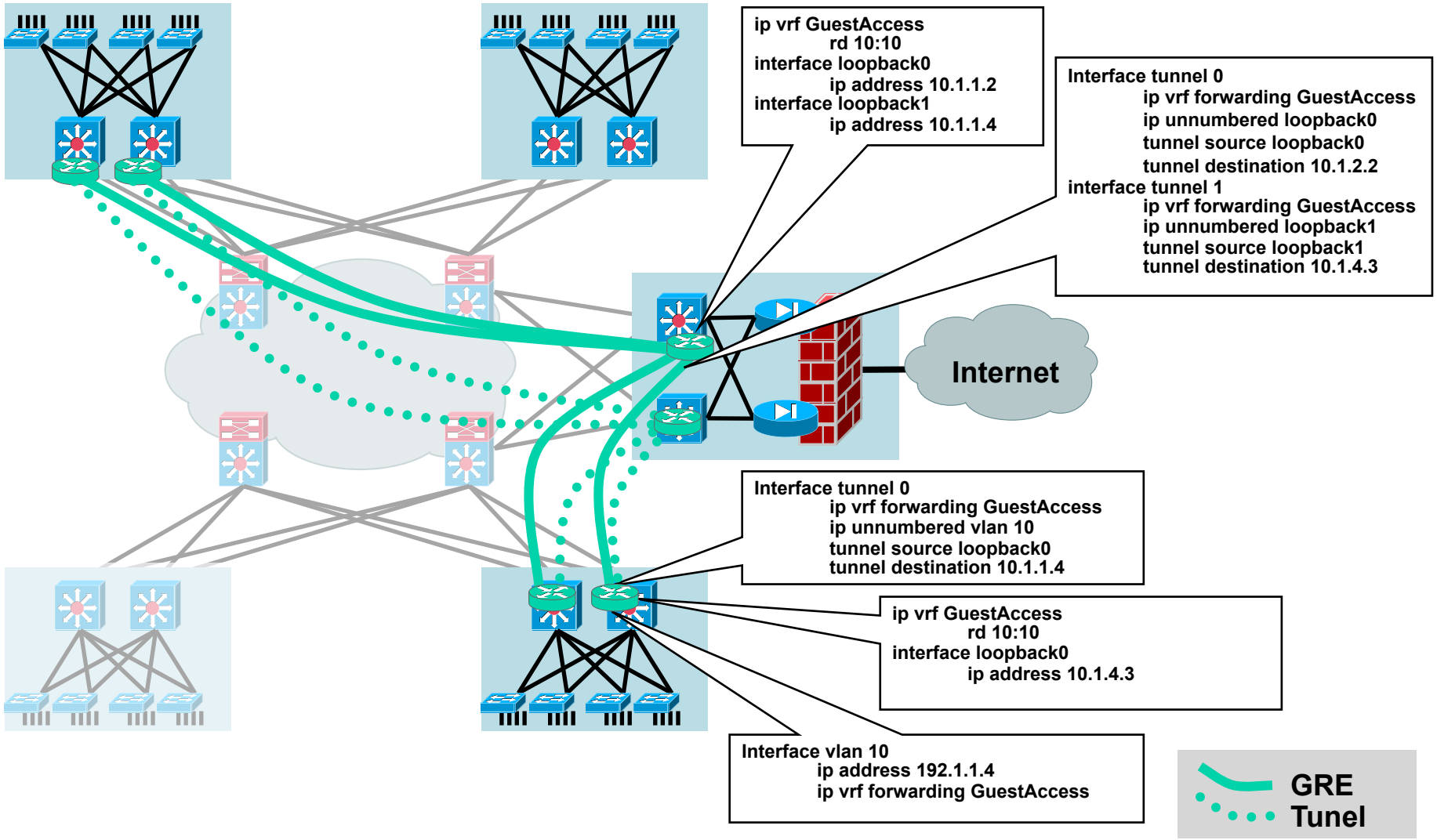
  osobna tablica routingu, do której przynależą interfejsy – może zawierać własne instancje routingu i wymieniać selektywnie informacje o osiągalności z innymi VRFami, w tym – VRFem globalnym

- 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

© 2012 Cisco and/or its affiliates. All rights reserved.

Separacja w firmie z wykorzystaniem VRF



© 2012 Cisco and/or its affiliates. All rights reserved.

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

W tym VRF…

… zaakceptuj do 50 prefiksów,…

```
ip vrf red
 maximum routes 50 90
```

…i zaloguj ostrzeżenie po dojściu do 90% (z 50),…

© 2012 Cisco and/or its affiliates. All rights reserved.

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:

Od tego sąsiada…

… zaakceptuj do 45 prefiksów a powyżej zrestartuj sesję …

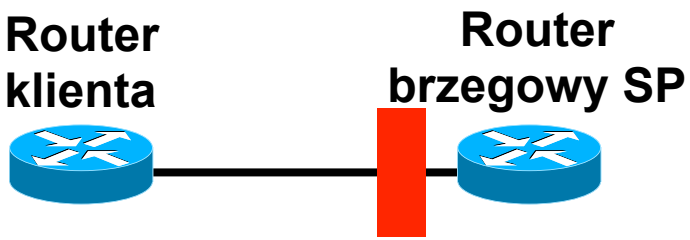
```
router bgp 13
  neighbor 140.0.250.2 maximum-prefix 45 80 restart 2
```

...logując ostrzeżenie po osiągnięciu 80% 45 prefiksów...

… po dwóch minutach od wystąpienia przepełnienia

© 2012 Cisco and/or its affiliates. All rights reserved.

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

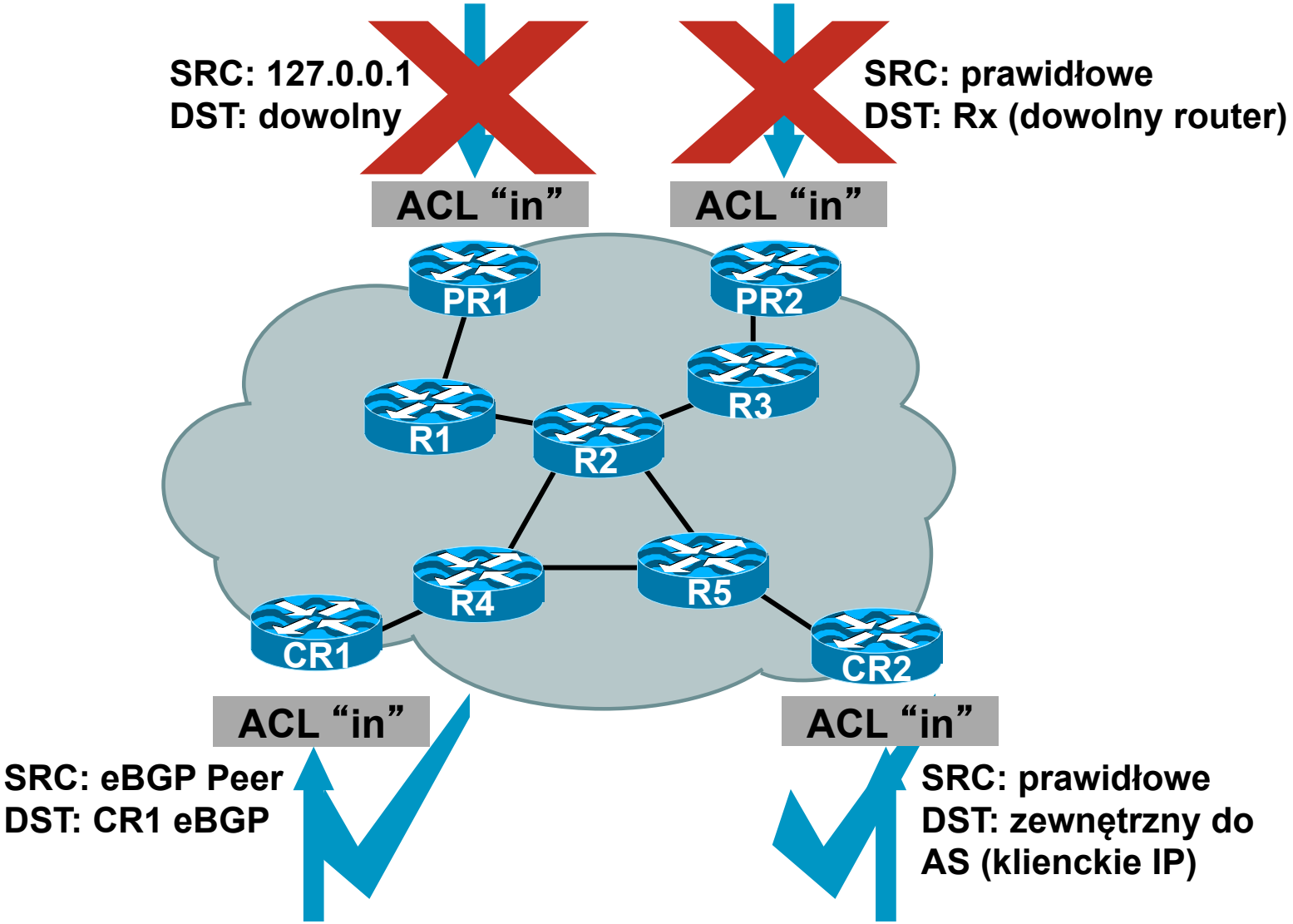
© 2012 Cisco and/or its affiliates. All rights reserved.

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

© 2012 Cisco and/or its affiliates. All rights reserved.

Jak działają iACL?



© 2012 Cisco and/or its affiliates. All rights reserved.

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
```

© 2012 Cisco and/or its affiliates. All rights reserved.

Mechanizmy ochrony Control Plane i Management Plane

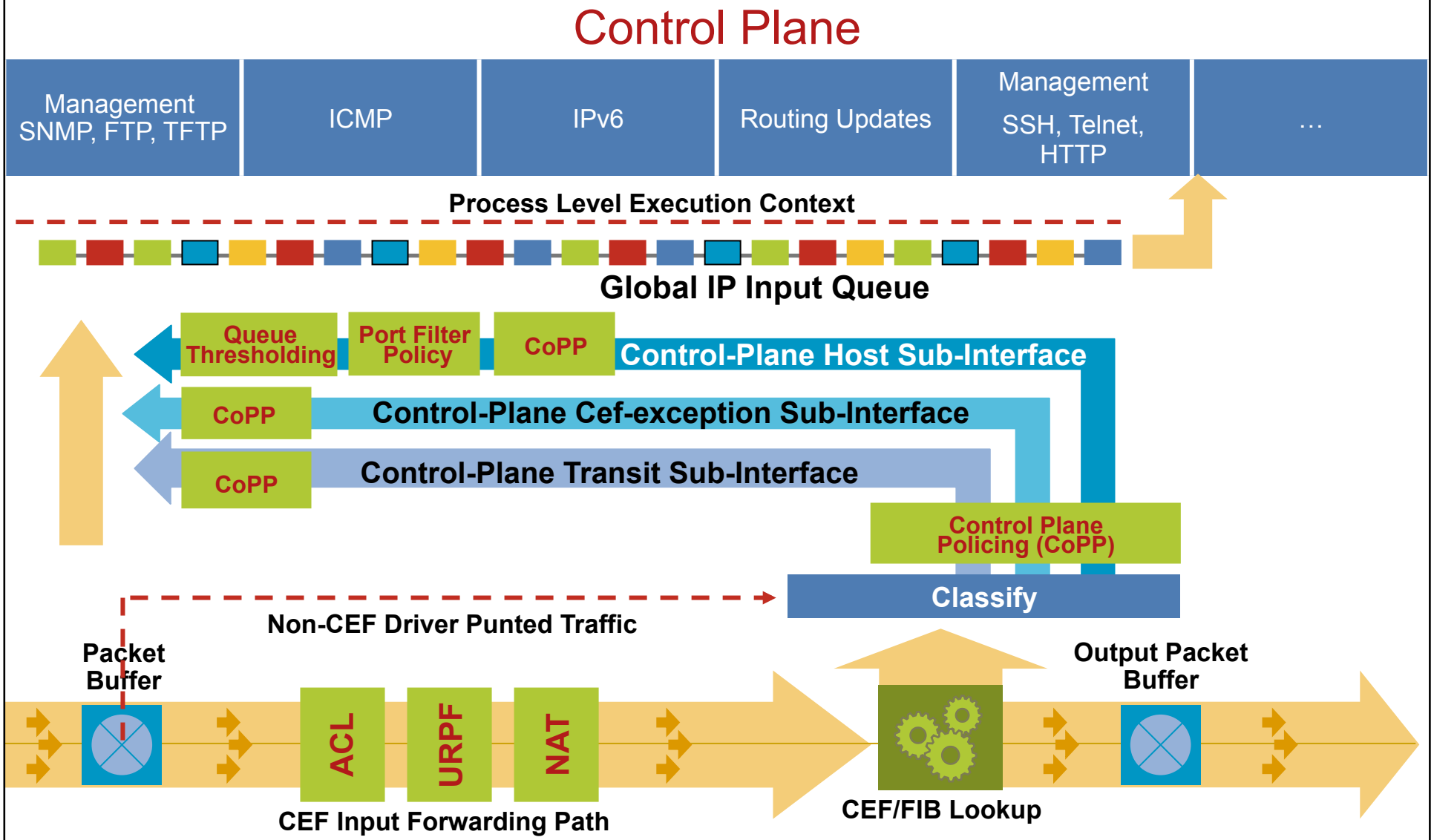
© 2012 Cisco and/or its affiliates. All rights reserved.

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)

© 2012 Cisco and/or its affiliates. All rights reserved.

Trzy interfejsy CPPr – host, transit, cef



© 2012 Cisco and/or its affiliates. All rights reserved.

Warstwa kontroli i zarządzania - ochrona

- CoPP/CoPPr – Cisco IOS/IOS-XE/NX-OS
- LPTS – Cisco IOS-XR
- MPP – ochrona interfejsów przez które odbywa się zarządzanie urządzeniami (dla Cisco IOS/IOS-XE oraz IOS-XR)
- Podpisane cyfrowo obrazy z oprogramowaniem
- Głęboka integracja weryfikacji oprogramowania i sprzętu wzajemnie

© 2012 Cisco and/or its affiliates. All rights reserved.

Bezpieczeństwo mechanizmów routingu

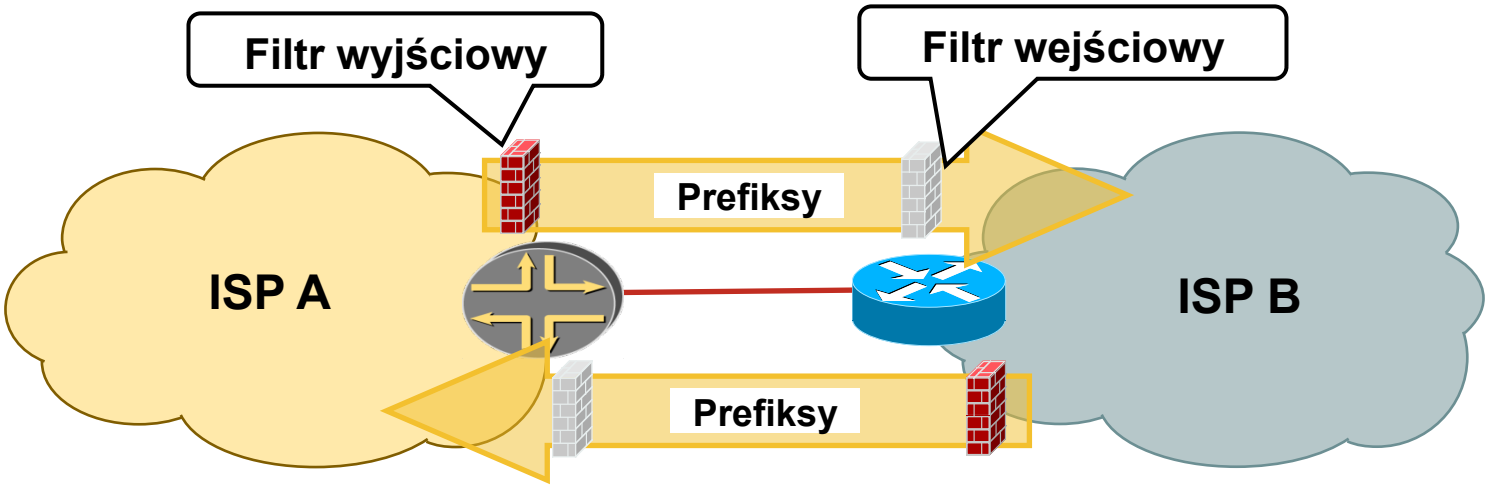
© 2012 Cisco and/or its affiliates. All rights reserved.

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)

© 2012 Cisco and/or its affiliates. All rights reserved.

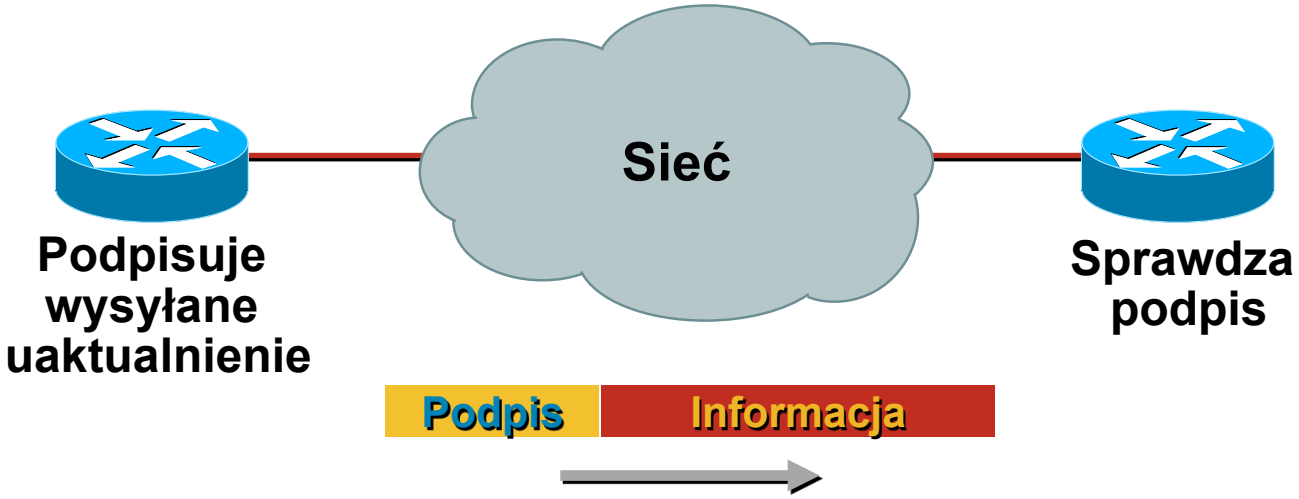
Ograniczone zaufanie...



- 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

© 2012 Cisco and/or its affiliates. All rights reserved.

Uwierzytelnianie pakietów routingu



Certyfikuje Autentyczność sąsiada i Integralność informacji routingowej

© 2012 Cisco and/or its affiliates. All rights reserved.

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

© 2012 Cisco and/or its affiliates. All rights reserved.

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
```

© 2012 Cisco and/or its affiliates. All rights reserved.

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
```

© 2012 Cisco and/or its affiliates. All rights reserved.

Przykład uwierzytelniania

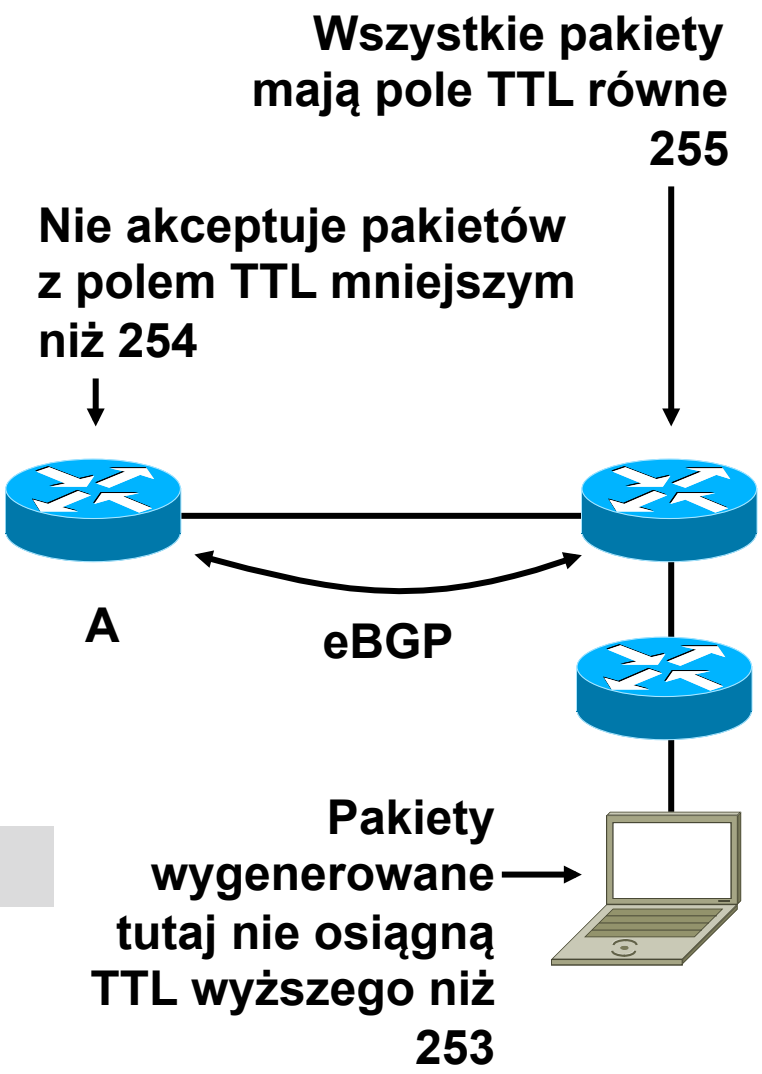
```
router bgp 200
 no synchronization
 neighbor 4.1.2.1 remote-as 300
 neighbor 4.1.2.1 description Link to Excalibur
 neighbor 4.1.2.1 send-community
 neighbor 4.1.2.1 version 4
 neighbor 4.1.2.1 soft-reconfiguration inbound
 neighbor 4.1.2.1 route-map Community1 out
 neighbor 4.1.2.1 password 7 q23dc%$#ert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

© 2012 Cisco and/or its affiliates. All rights reserved.

Generalised TTL Security Mechanism
RFC 3682

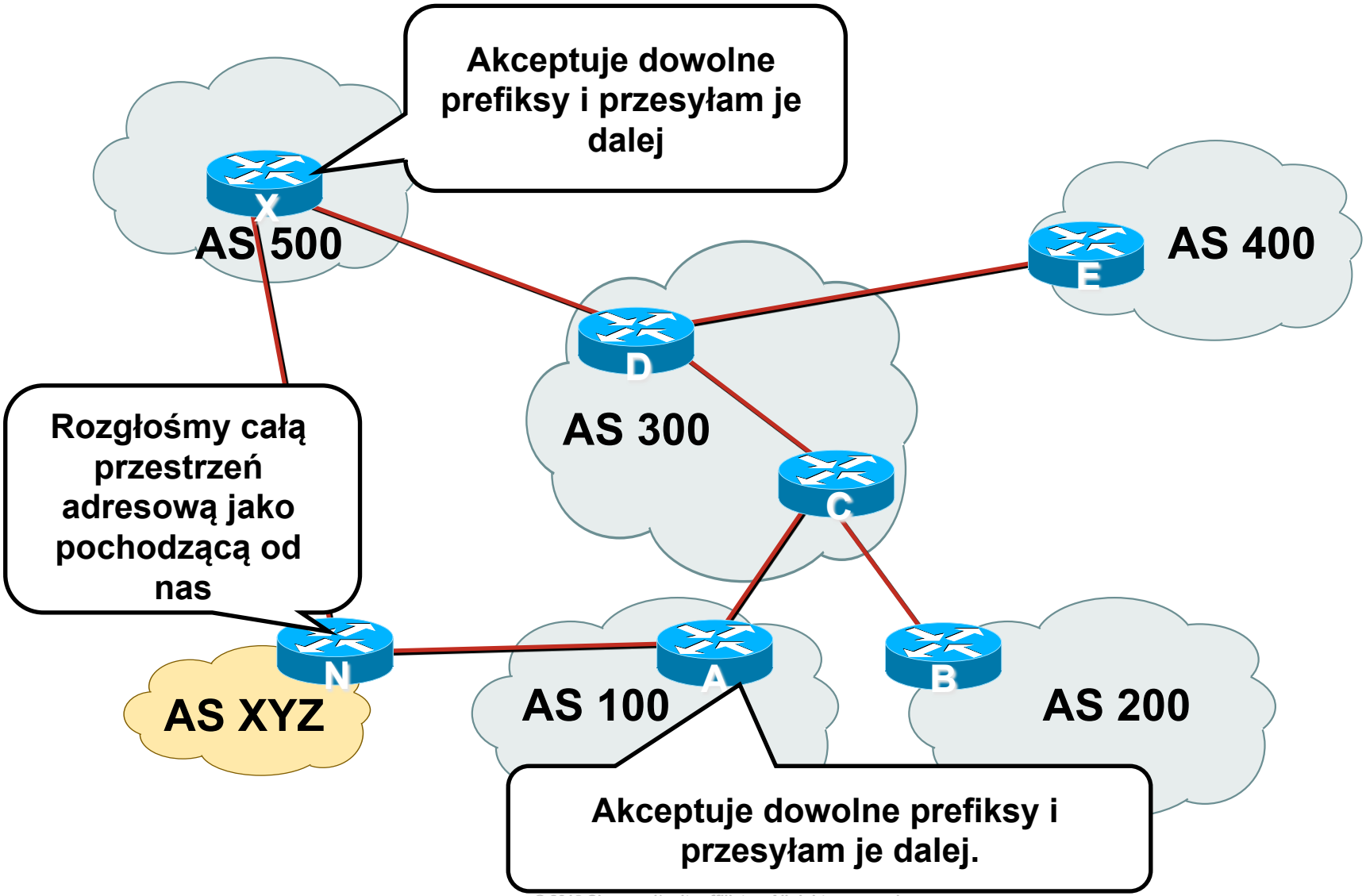
- GTSM chroni sesje BGP przed atakami z oddalonych stacji/ sieci
- Routery wymieniają się pakietami IP z polem TTL ustawionym na 255, wartości poniżej 254 są automatycznie odrzucane
- Urządzenie nie podłączone bezpośrednio pomiędzy routerami nie może wygenerować takiego ruchu

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



© 2012 Cisco and/or its affiliates. All rights reserved.

Garbage in – Garbage Out ?



© 2012 Cisco and/or its affiliates. All rights reserved.

Secure InterDomain Routing

- Każdy router BGP może wstrzyknąć fałszywą informację routingową (o osiągalności prefiksu)
  - zwykle jest to błąd (Pakistan Telecom i YouTube)
  - może być jednak działanie świadome (podsłuchiwanie ruchu do popularnych serwisów czy nawet – krajów)
- Tak czy inaczej, ruch do danego AS może zostać przekierowany lub wręcz zablokowany
- Prefiks można przekierować do siebie w BGP za pomocą dokładniejszego prefiksu, lub skonstruowania krótszej ścieżki do docelowego AS
- SIDR = mechanizm "uwierzytelniania" możliwości rozgłaszania danego prefiksu

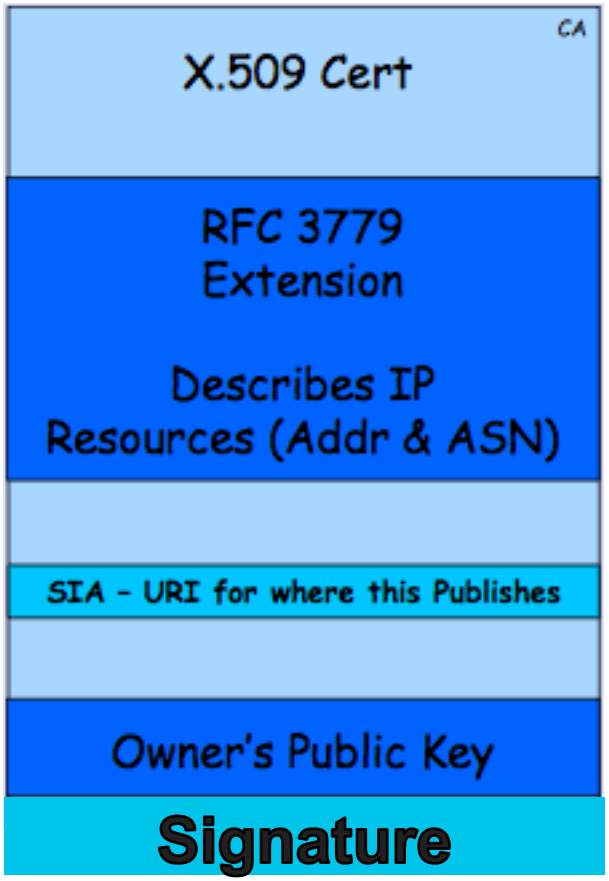
© 2012 Cisco and/or its affiliates. All rights reserved.

Certyfikaty RPKI

- Każdy RIR generuje certyfikat dla każdego przydzielonego prefiksu i dystrybuuje go z prefiksem

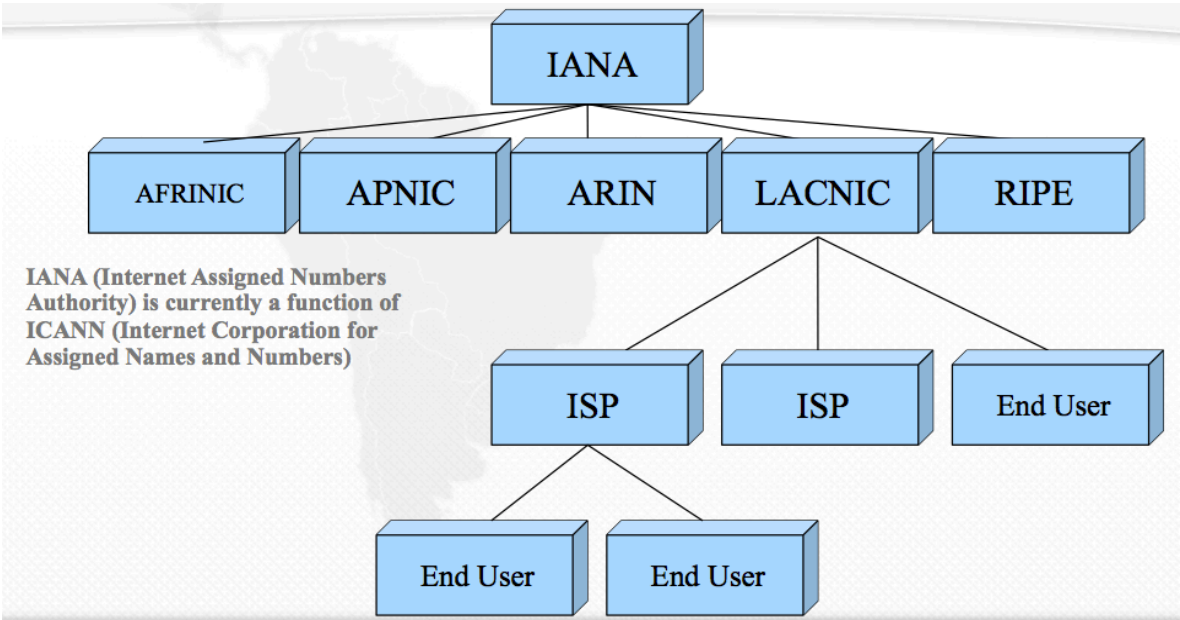
  Certyfikat oznacza: będąc klientem "K" masz prawo rozgłaszać prefiks "P" ponieważ wystawiłem i podpisałem Ci certyfikat

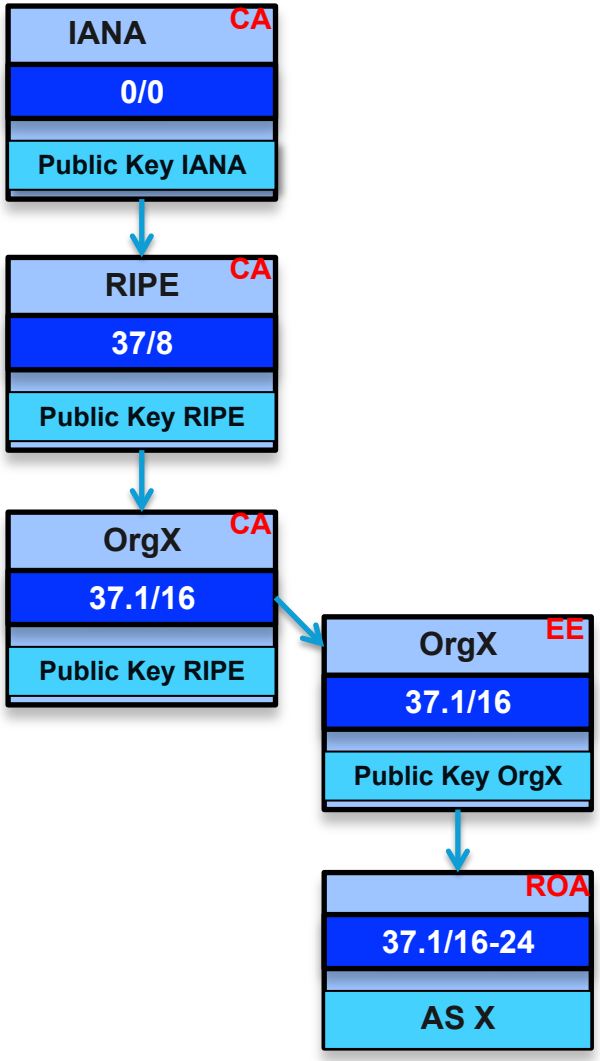
- Uzyskanie klucza publicznego jest proste dzięki infrastrukturze PKI
- Każdy z ISP przydzielających podsieci z tego prefiksu również wykonuje analogiczną procedurę



© 2012 Cisco and/or its affiliates. All rights reserved.

Schemat certyfikacji





© 2012 Cisco and/or its affiliates. All rights reserved.

Zmiany w BGP i infrastrukturze

- Osobny protokół (TCP lub SSH), którym routery brzegowe BGP transportują informacje o certyfikacji
- Prefiks w tablicy BGP może znaleźć się w jednym z trzech stanów:

  VALID – prefiks rozgłoszono w ramach ograniczeń na długość maski z właściwym Origin AS

  INVALID – rozgłoszenie jest dokładniejsze niż umożliwia to certyfikat, bądź nie zgadza się Origin AS

  NOT FOUND – nie znaleziono dla prefiksu danych w bazie certyfikacyjnej

© 2012 Cisco and/or its affiliates. All rights reserved.

Weryfikacja działania BGP SIDR

- Podsumowanie stanu:

```
router# show ip bgp summary
BGP router identifier 192.176.2.28, local AS number 65001
BGP table version is 407551, main routing table version 407551
Path RPKI states: 3214 valid, 377828 not found, 2504 invalid
```

- Prefiksy w BGP RIB:

```
router# show ip bgp
...
RPKI validation codes: V valid, I invalid, N Not found
     Network      Next Hop        Metric LocPrf Weight Path
*> N1.0.4.0/22    134.222.88.226 0       31592  286    4323 7545 56203 I

...

*> N1.0.28.0/22   134.222.88.226 0       31592  286    2914 2519 i
```

© 2012 Cisco and/or its affiliates. All rights reserved.

Weryfikacja za pomocą BGPmon

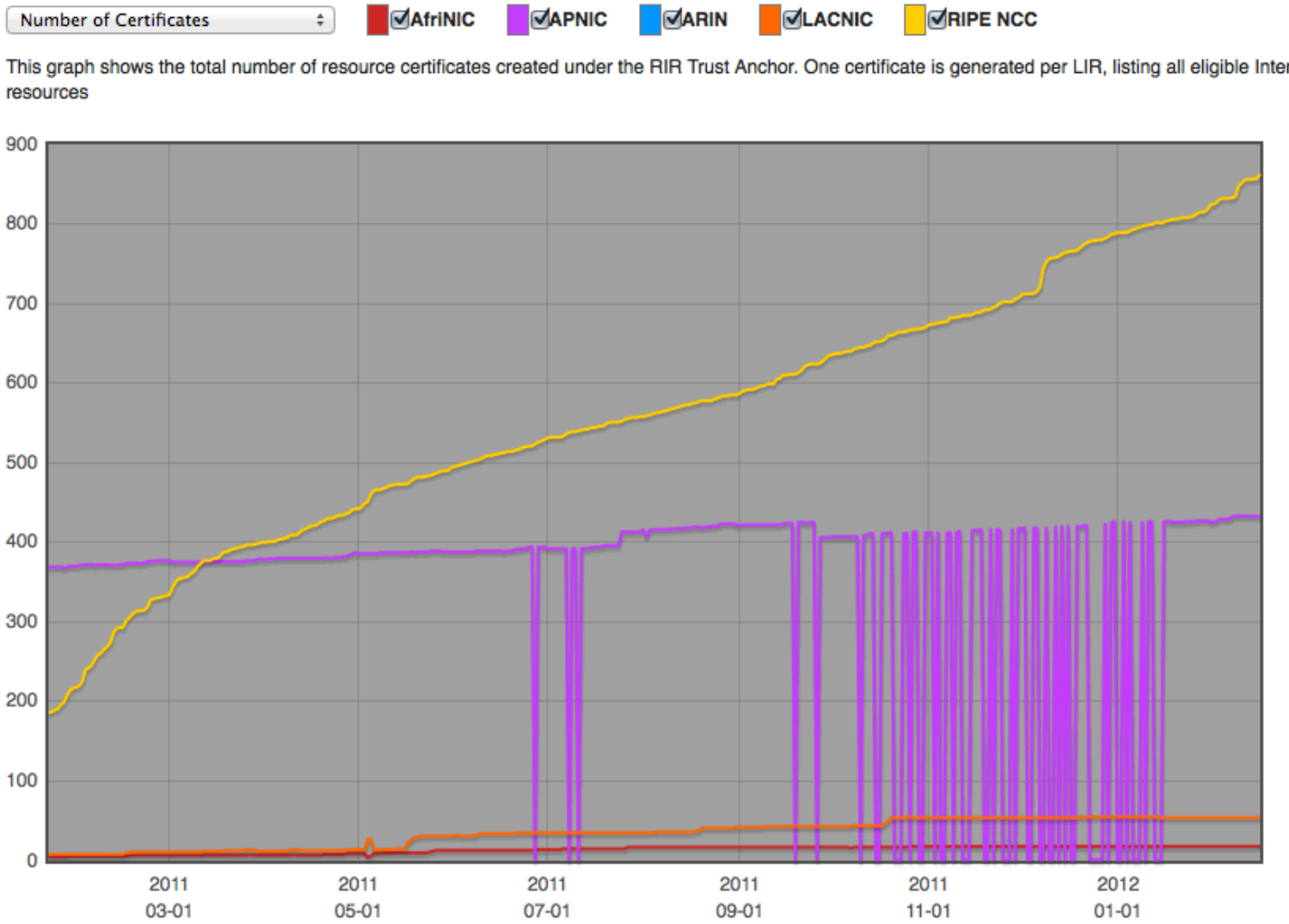
```
[szopen@r2d2 ~]$ whois -h whois.bgpmon.net 217.97.0.0

% This is the BGPmon.net whois Service
% You can use this whois gateway to retrieve information
% about an IP adress or prefix
% We support both IPv4 and IPv6 address.
%
% For more information visit:
% http://bgpmon.net/bgpmonapi.php

Prefix:                217.97.0.0/16
Prefix description:    for abuse: abuse@tpnet.pl
Country code:          PL
Origin AS:             5617
Origin AS Name:        TPNET Telekomunikacja Polska S.A.
RPKI status:           No ROA found
First seen:            2011-10-19
Last seen:             2012-2-15
Seen by #peers:        122
```

© 2012 Cisco and/or its affiliates. All rights reserved.

Statystyki certyfikacji dla RIPE



© 2012 Cisco and/or its affiliates. All rights reserved.

BGP blackholing – IPv4 i IPv6

© 2012 Cisco and/or its affiliates. All rights reserved.

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’

© 2012 Cisco and/or its affiliates. All rights reserved.

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

© 2012 Cisco and/or its affiliates. All rights reserved.

Krok 1: przygotowanie routerów

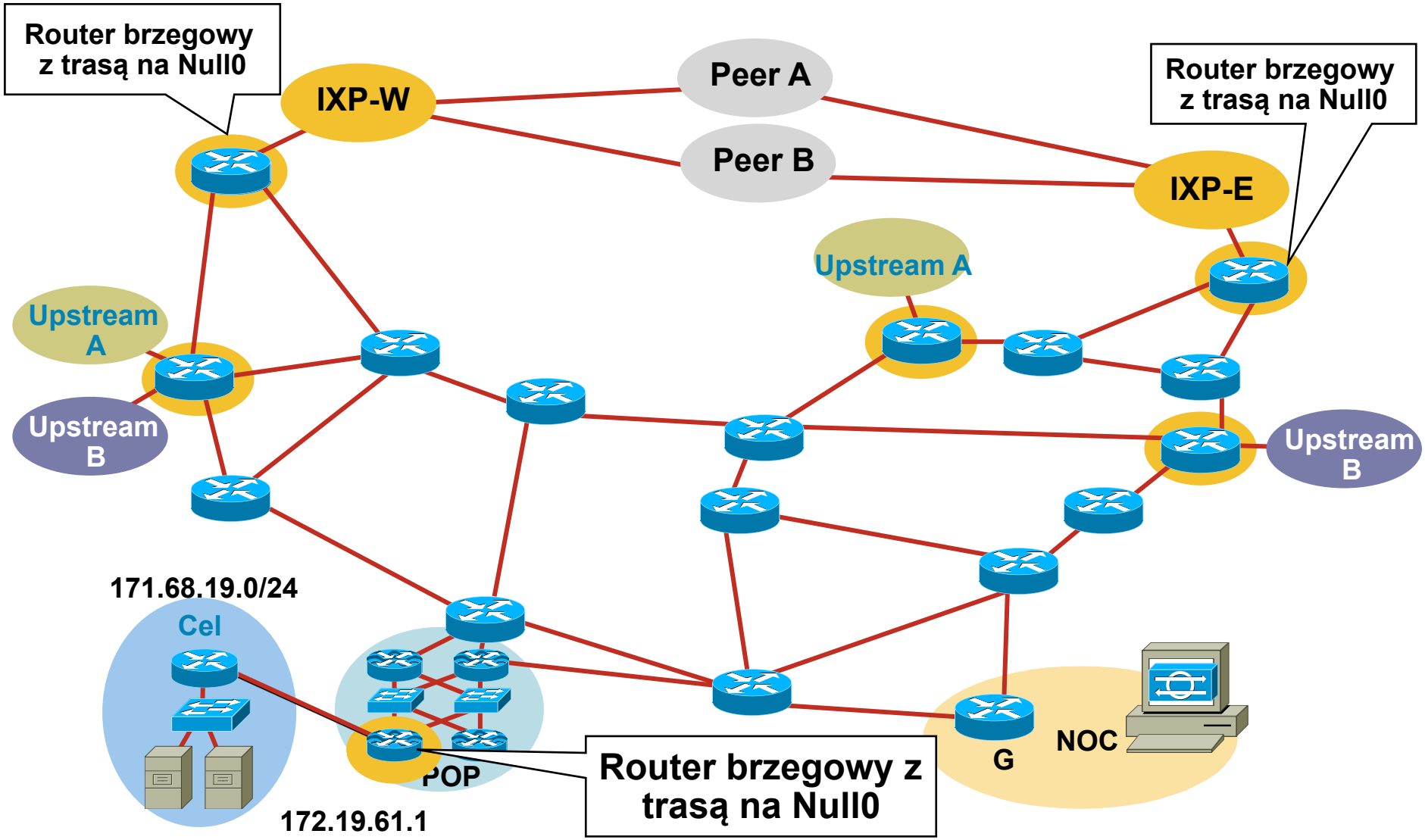
- Wybierz mały blok adresów nie używany w Twojej sieci do niczego innego – pula 192.0.2.0/24 jest zwykle optymalna
- Na każdym z routerów który w przypadku ataku ma odrzucać ruch, zdefiniuj trasę statyczną wskazującą na wybrany adres (adresy) i interfejs Null0

```
ip route 192.0.2.1 255.255.255.255 Null0
```

© 2012 Cisco and/or its affiliates. All rights reserved.

Krok 1

Przygotowanie routerów



© 2012 Cisco and/or its affiliates. All rights reserved.

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)

© 2012 Cisco and/or its affiliates. All rights reserved.

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

© 2012 Cisco and/or its affiliates. All rights reserved.

Krok 3:
Konfiguracja ‘klientów’ – brzegowych routerów BGP

```
ip bgp new-format
ip route 192.0.2.1 255.255.255.255 null0
!
interface null 0
 no ip unreachables
!
ip community-list 1 permit 65535:666
!
route-map BGP-BH permit 10
 match community 1
 set ip next-hop 192.0.2.1
route-map BGP-BH permit 20
!
router bgp 65535
 neighbor 123.123.123.3 route-map BGP-BH in
```

Ta sama trasa na Null0 (adres IP może być inny)

Nie wysyłamy do źródła ataku pakietów unreachable (self-DDoS)

BGP community którego użyjemy w route-map

„Jeśli prefiks oznaczony jest community 65535:666 to ustaw next-hop na 192.0.2.1”

Przeglądane mają być wszystkie prefiksy rozgłaszane przez sąsiada

© 2012 Cisco and/or its affiliates. All rights reserved.

Krok 4:
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

© 2012 Cisco and/or its affiliates. All rights reserved.

Aktywacja blackholingu – widok z FIB

Prefiks z BGP—172.19.61.1 next-hop = 192.0.2.1

Trasa statyczna na routerze brzegowym—192.0.2.1 = Null0

172.19.61.1= 192.0.2.1 = Null0

ruch do adresu 172.19.61.1 jest routowany do Null0

© 2012 Cisco and/or its affiliates. All rights reserved.

RTBH wzbogacone o community

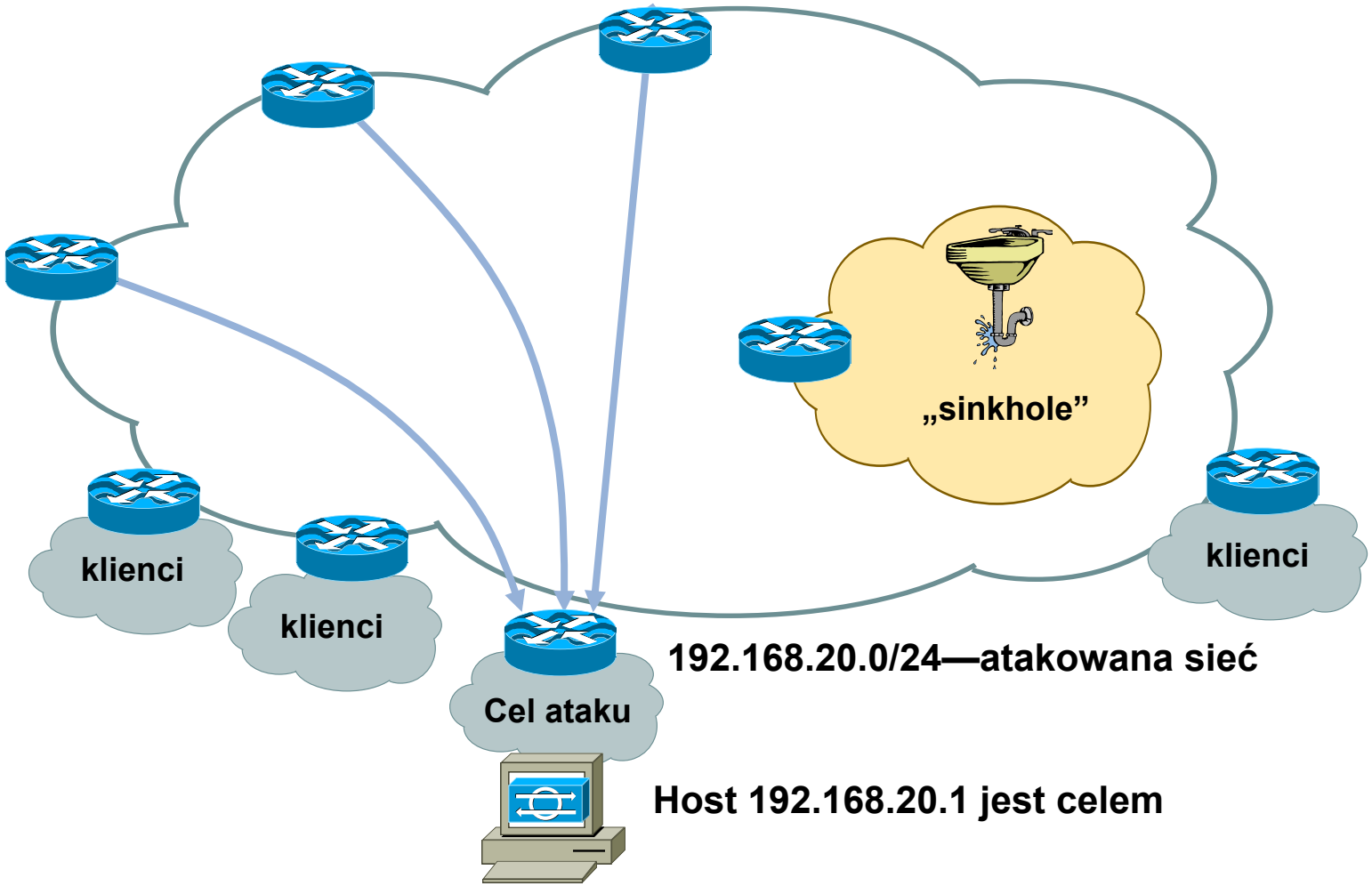
- Wykorzystanie atrybutu community w BGP pozwala wydzielić różne ‘klasy’ ruchu odrzucanego i/lub zróżnicować rodzaj wykonywanej akcji
- Na routerach brzegowych wymaga to wskazania za pomocą route-mapy, że prefiksy akceptowane z konkretnym community mają być odrzucane (lub traktowane w inny, szczególny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

  64999:666 – ruch do odrzucenia

  64999:777 – ruch do przekierowania do specjalnej lokalizacji

© 2012 Cisco and/or its affiliates. All rights reserved.

Routery/sieci ‘sinkhole’



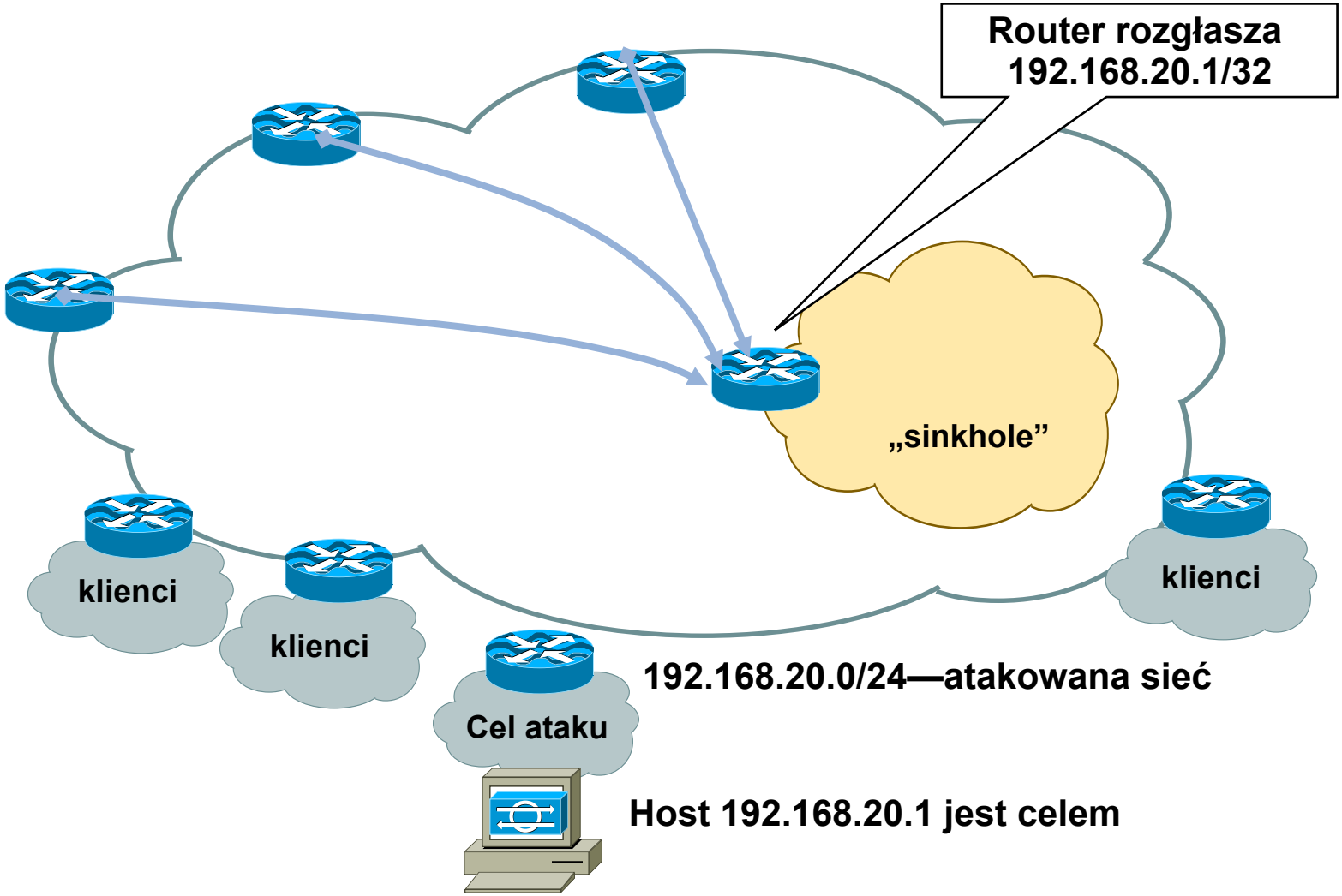
© 2012 Cisco and/or its affiliates. All rights reserved.

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

© 2012 Cisco and/or its affiliates. All rights reserved.

Routery/sieci ‘sinkhole’



© 2012 Cisco and/or its affiliates. All rights reserved.

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

© 2012 Cisco and/or its affiliates. All rights reserved.

Zastosowanie mechanizmu IP Anycast

© 2012 Cisco and/or its affiliates. All rights reserved.

Ochrona serwerów root DNS anycastem

ICANN

Factsheet

Root server attack on 6 February 2007

On 6 February 2007, starting at 12:00 PM UTC (4:00 AM PST), for approximately two-and-a-half hours, the system that underpins the Internet came under attack. Three-and-a-half hours after the attack stopped, a second attack, this time lasting five hours, began.

At least six root servers were attacked but only two of them were noticeably affected: the "g-root", which is run by the U.S. Department of Defense and is physically based in Ohio, and the "l-root" run the Internet Corporation for Assigned Names and Numbers (ICANN), which is physically based in California.

The reason why these two were particularly badly affected was because they are the only root servers attacked that have yet to install Anycast (a further three root servers without Anycast were not attacked this time).

© 2012 Cisco and/or its affiliates. All rights reserved.

Trochę o historii…

To nic nowego, ale nadal działa dobrze ☺

- Wykrywanie nowych usług – SNTPv4 (RFC 2030) oraz NTP "manycast" (RFC 4330)
- Pierwszy mechanizm przechodzenia na IPv6 (RFC 2893) a potem 6to4 (RFC 3068)
- Użycie anycastów dla RP – MSDP i PIM (RFC 4610)
- W IPv6 pierwsze RFC (RFC 1884, 2373 i 3513) zabraniały używania adresu anycastowego jako adresu źródłowego; zniesiono to ograniczenie w RFC 4291
- Zastosowanie anycastów w systemie DNS (RFC 3258) wspomina wykorzystanie "shared unicast"

© 2012 Cisco and/or its affiliates. All rights reserved.

IP Anycast

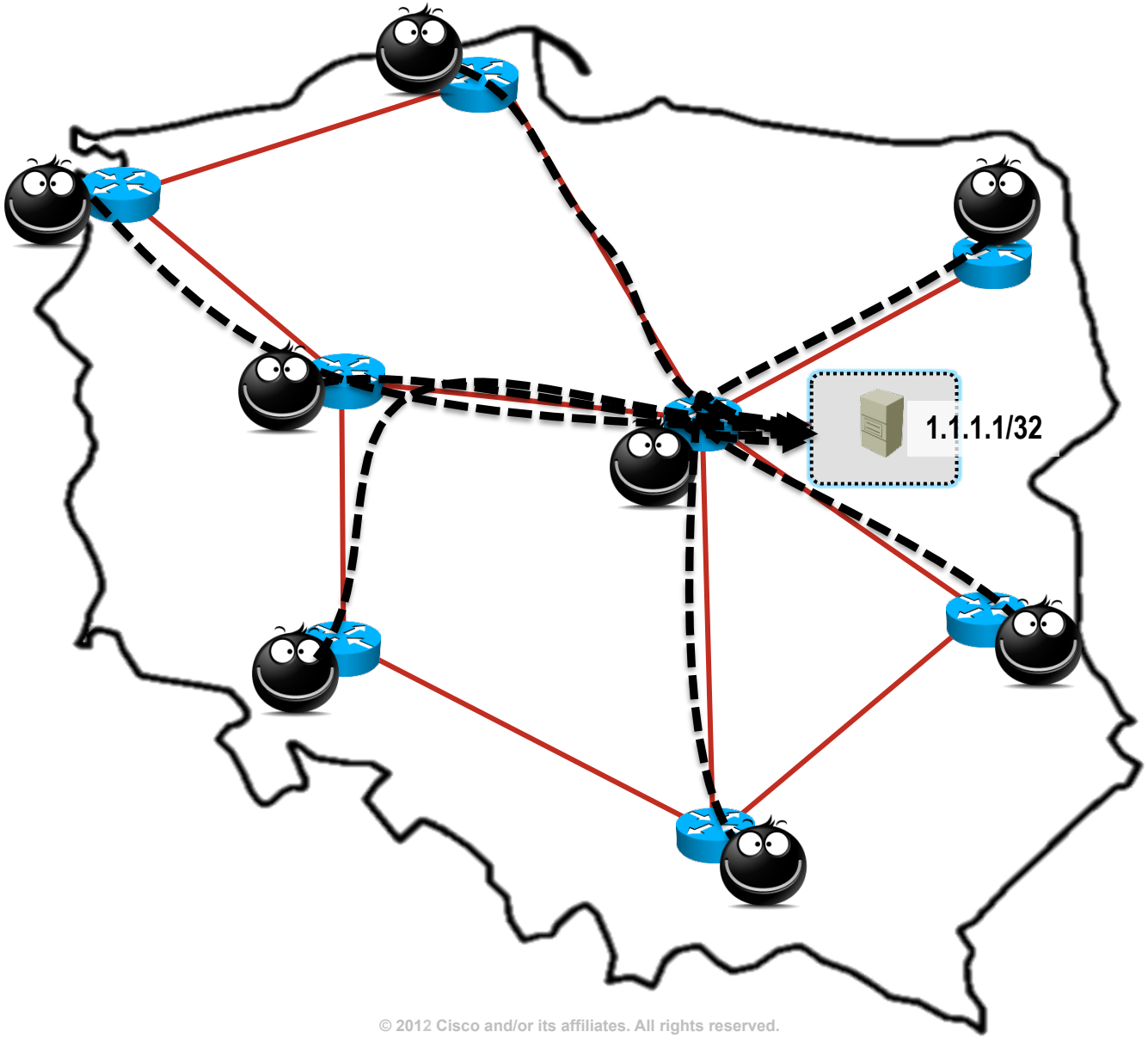
- Prosty, efektywny, szeroko używany ☺
- Niezależny od warstwy trzeciej

  zarówno IPv4 jak i IPv6 działają – po prostu

  RFC mówi o specjalnych adresach anycast – ale większość technik skalowania, w tym te najpowszechniejsze – wykorzystują podejście 'shared unicast'

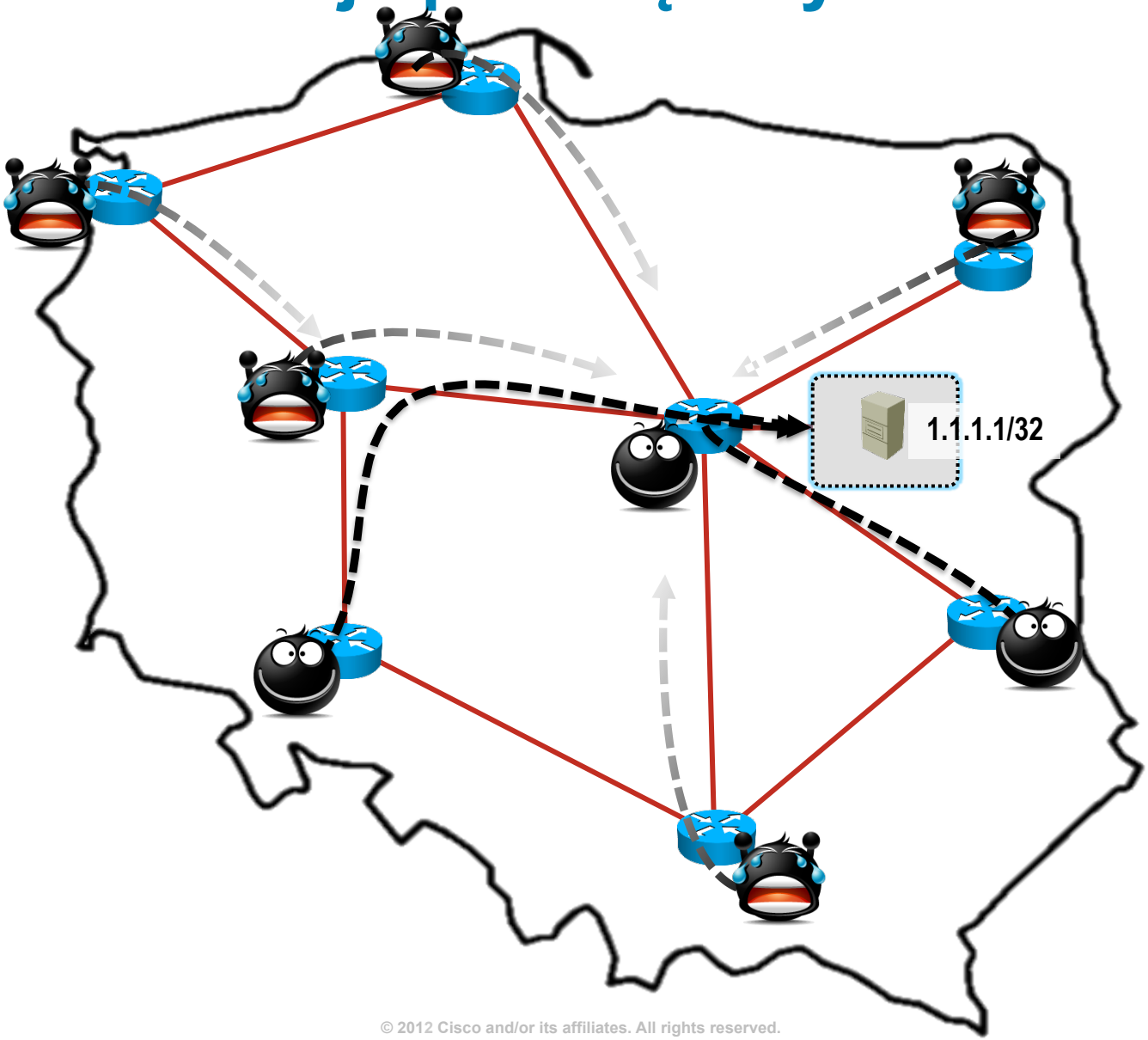
© 2012 Cisco and/or its affiliates. All rights reserved.

Typowe zastosowanie



© 2012 Cisco and/or its affiliates. All rights reserved.

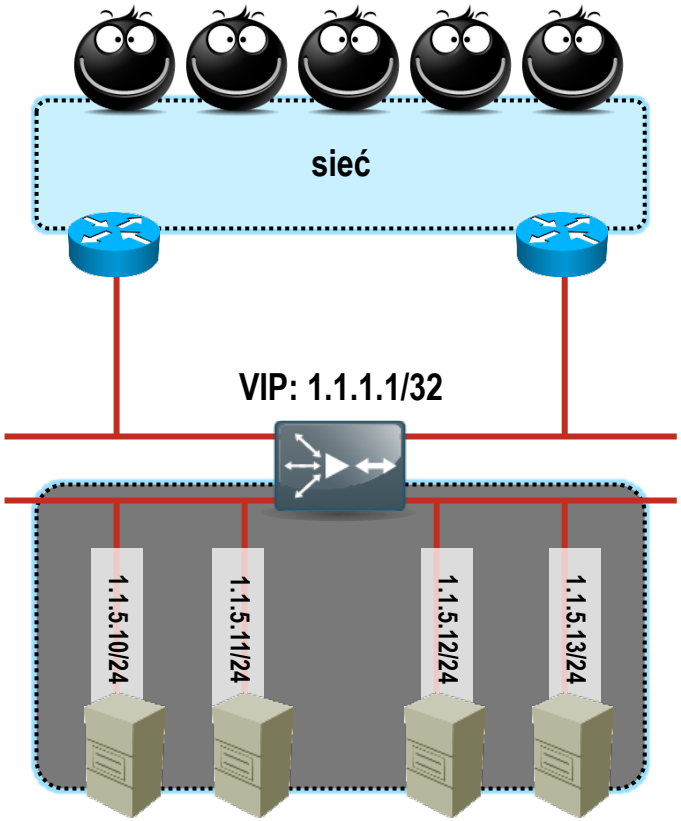
Serwer zostaje przeciążony



© 2012 Cisco and/or its affiliates. All rights reserved.

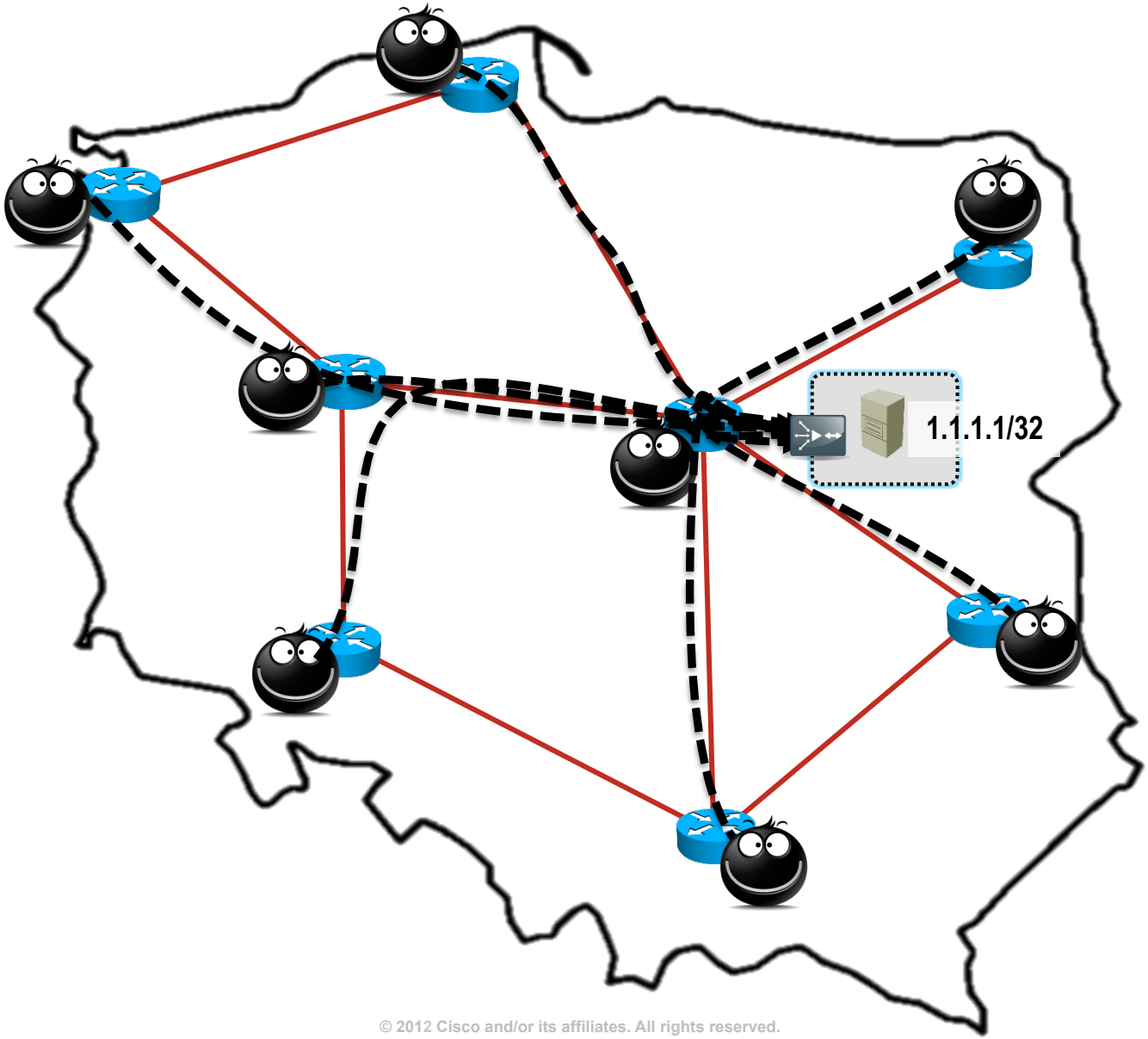
Rozwiązanie pierwsze: rośniemy wszerz

"Zainstalujmy loadbalancer i dodajmy serwerów"



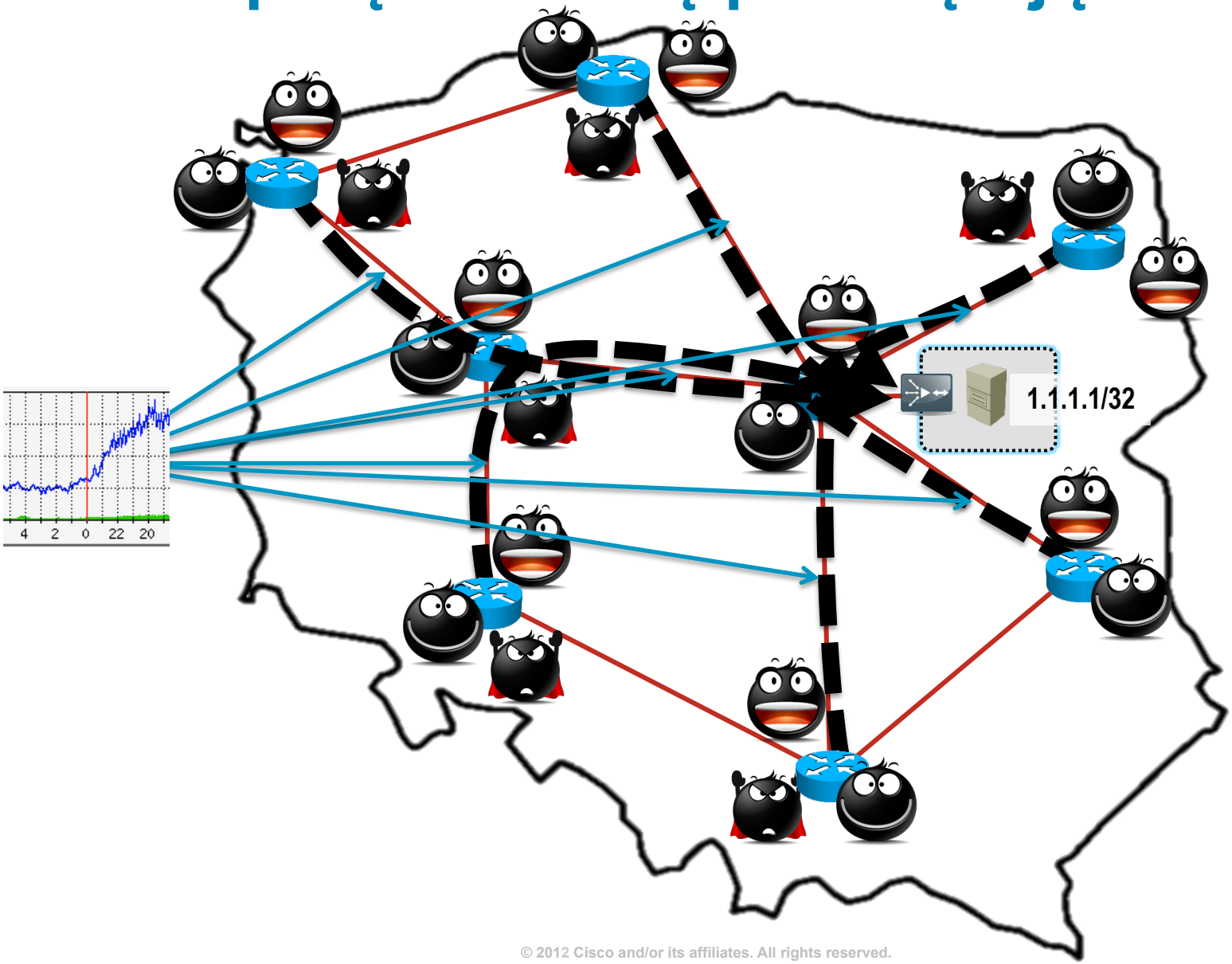
© 2012 Cisco and/or its affiliates. All rights reserved.

Po zastosowaniu VIPa i serwerów



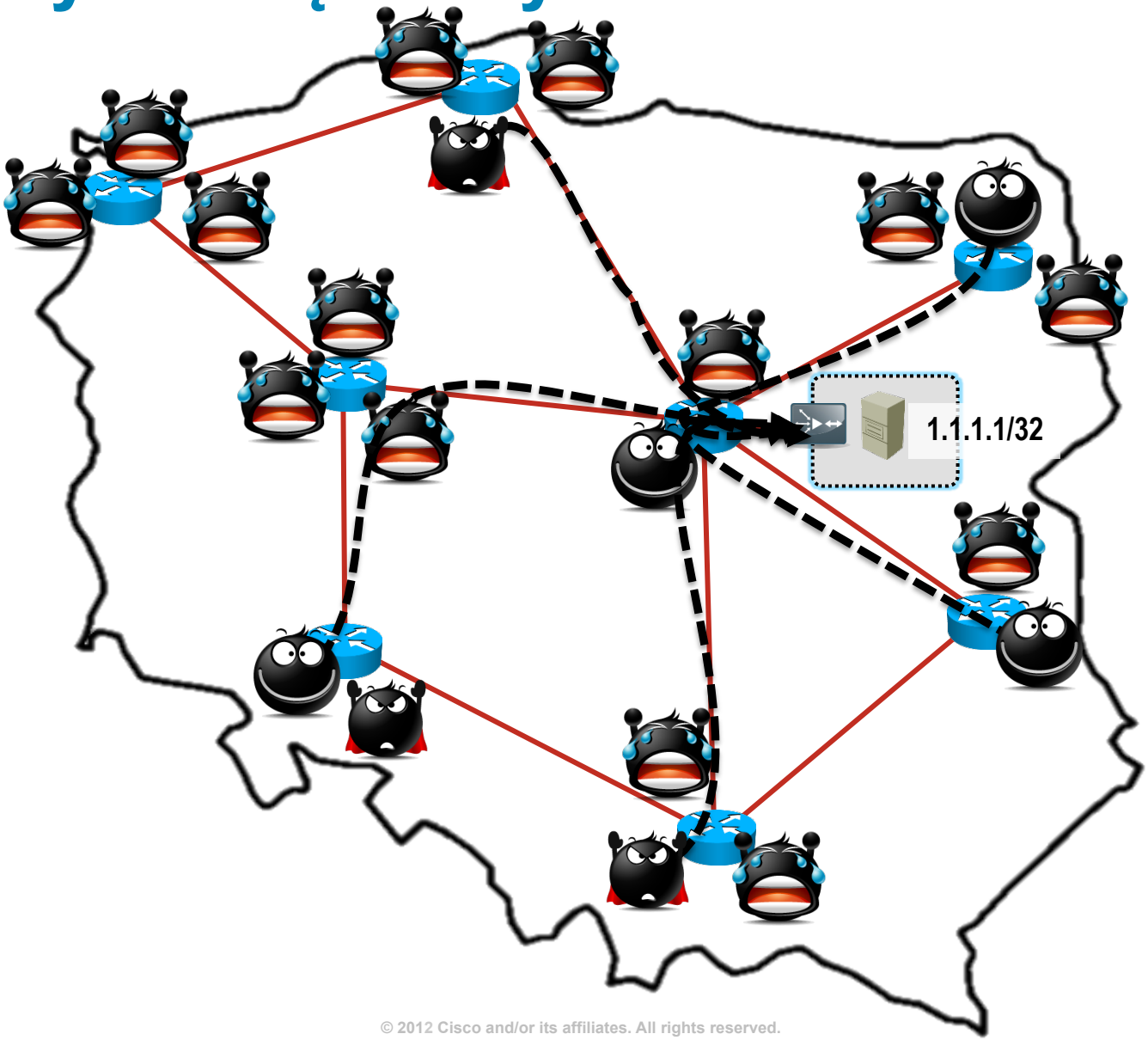
© 2012 Cisco and/or its affiliates. All rights reserved.

…ale połączenia się przeciążają…



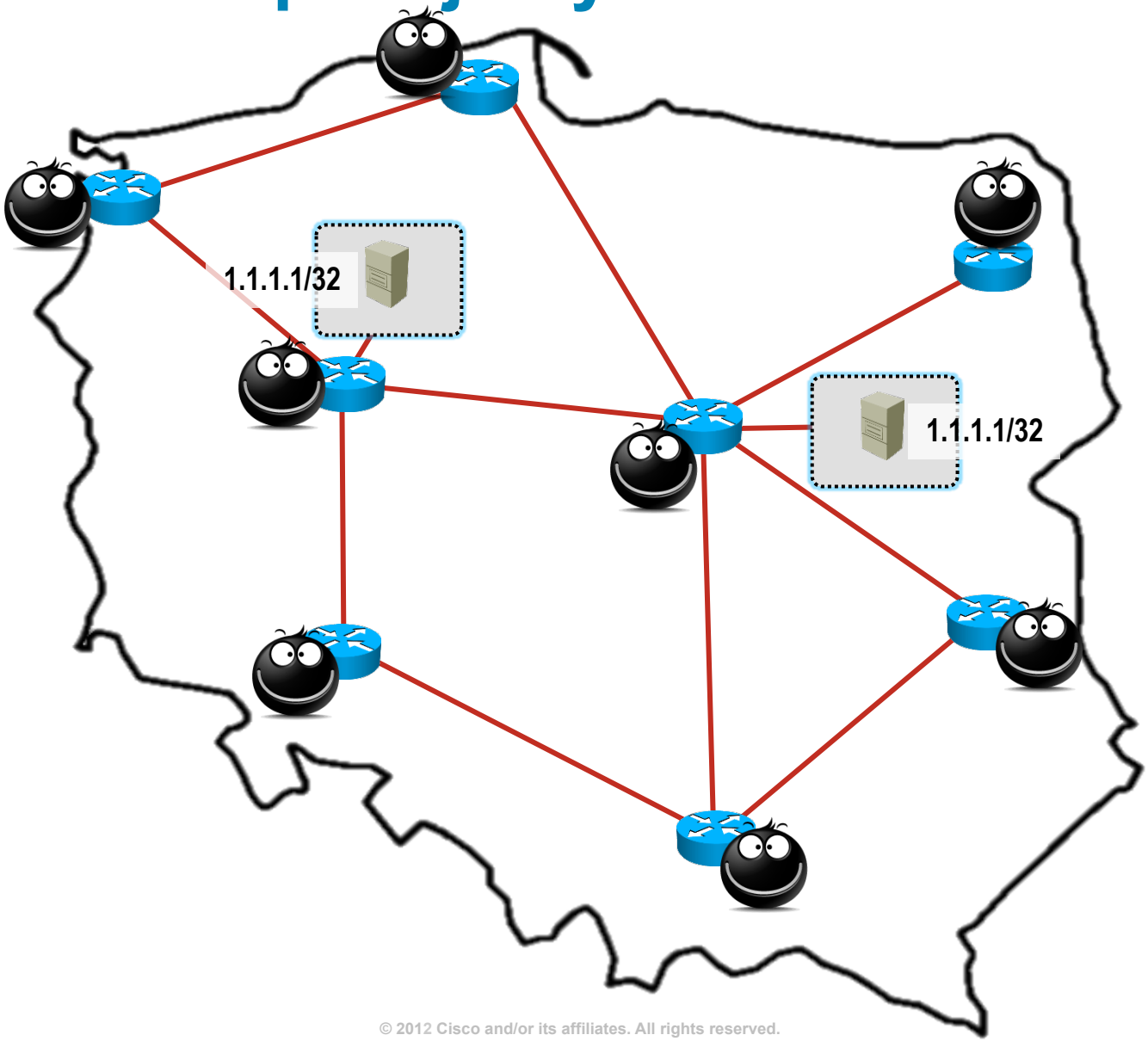
© 2012 Cisco and/or its affiliates. All rights reserved.

…i tylko część użytkowników ma dostęp



© 2012 Cisco and/or its affiliates. All rights reserved.

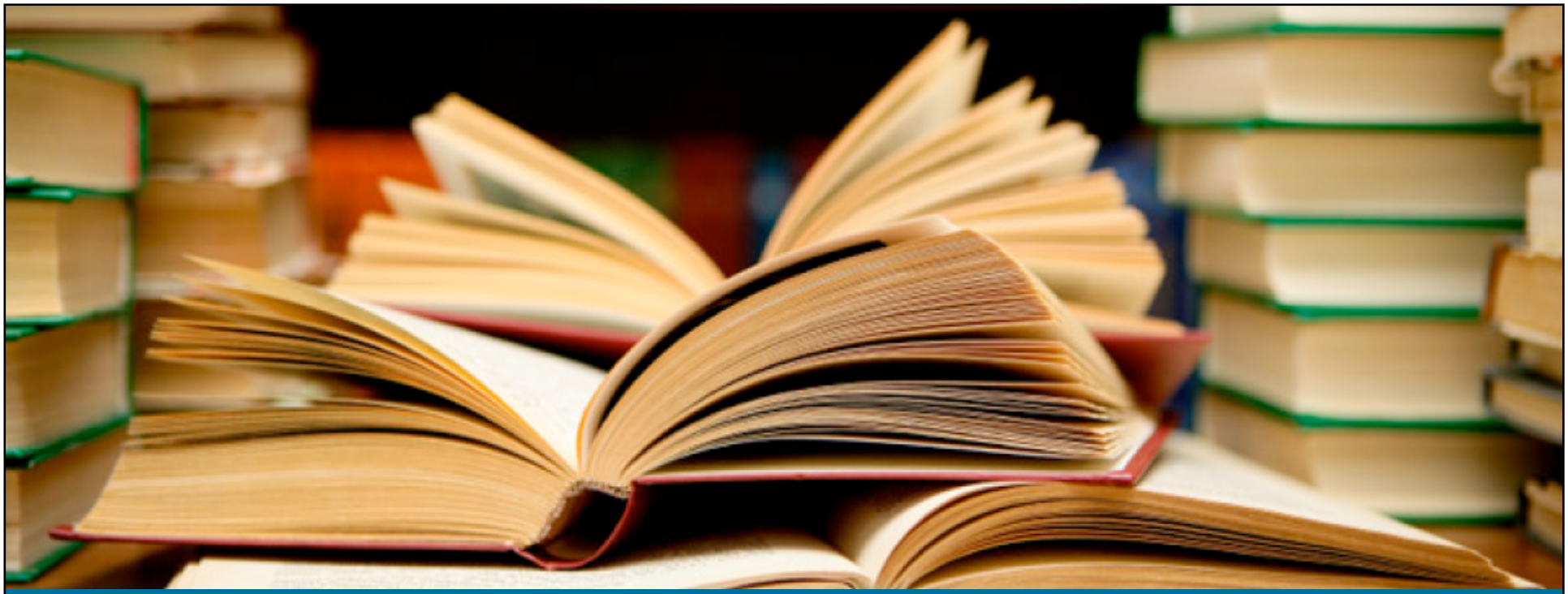
A może zreplikujemy to samo IP?



© 2012 Cisco and/or its affiliates. All rights reserved.

Co jeszcze interesuje operatora?

© 2012 Cisco and/or its affiliates. All rights reserved.



Q&A

© 2012 Cisco and/or its affiliates. All rights reserved.