Bezpieczeństwo sieci klasy operatorskiej

Łukasz Bromirski
Dyrektor Techniczny
lbromirski@cisco.com
CCIE #15929 R&S/SP, CCDE 2012::17
Cisco ISP-SWAT

Usługi Informatyczne
Uniwersytetu Warszawskiego

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

Agenda

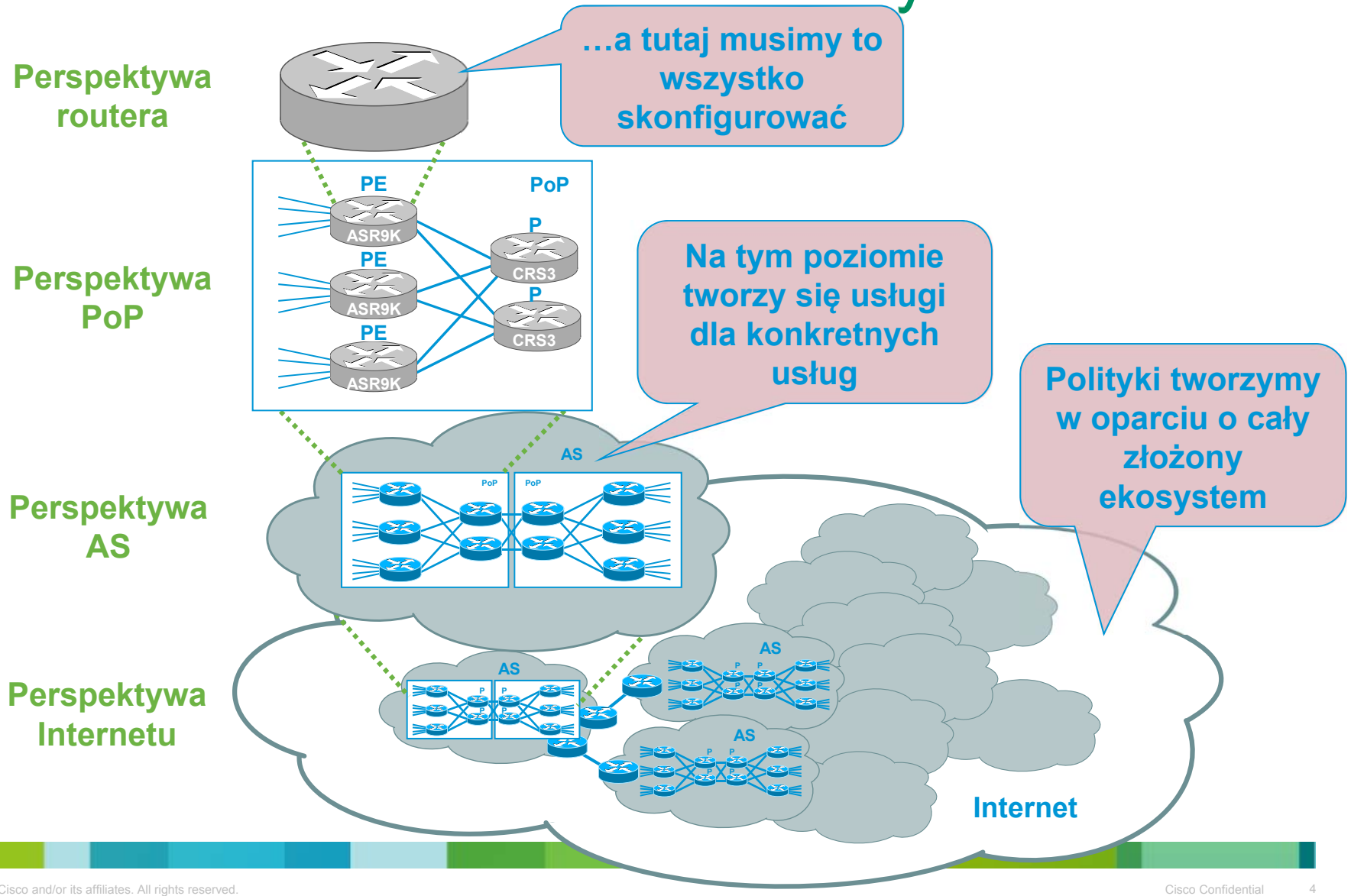
- Bezpieczeństwo
- Warstwa kontroli (control plane)
- Warstwa danych (data plane)
- Warstwa zarządzania (management plane)
- Warstwa usług (services plane)
- Q&A

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

Bezpieczeństwo
Ogólne zalecenia

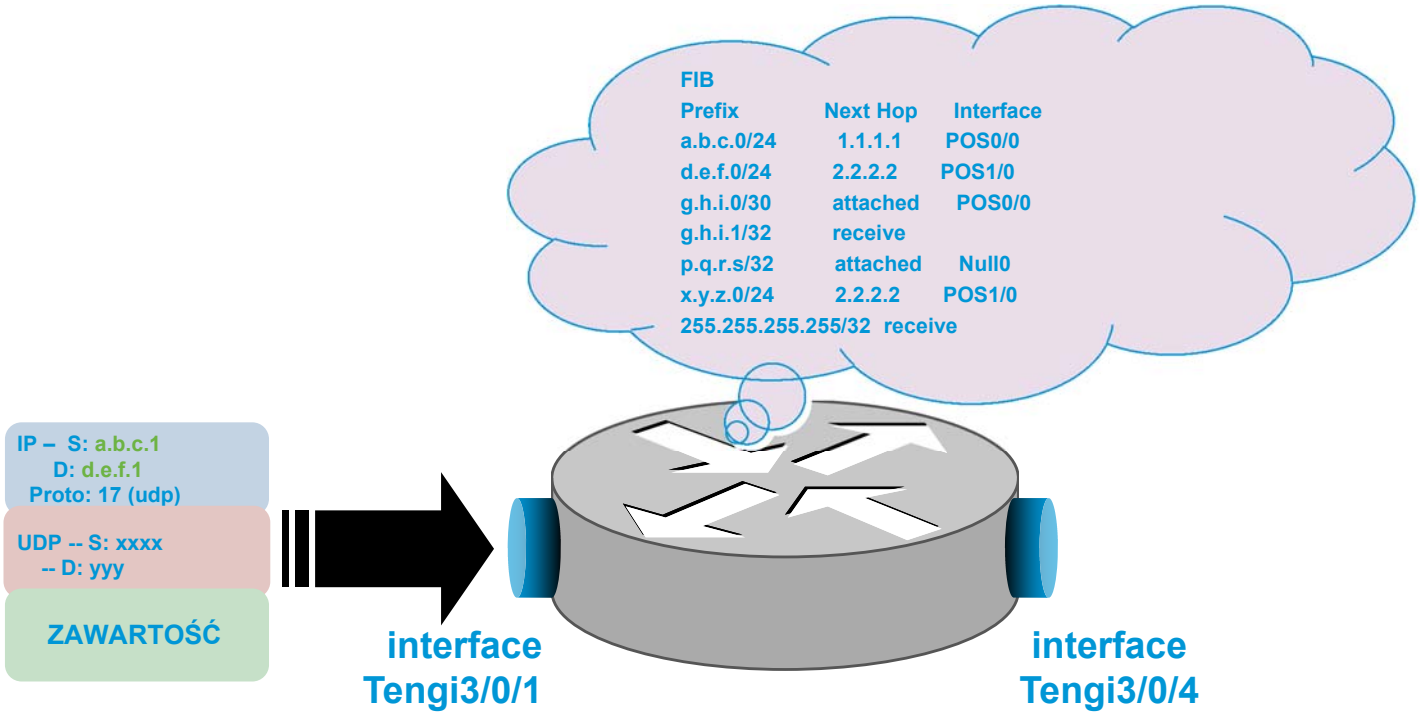
© 2010 Cisco and/or its affiliates. All rights reserved.

Hierarchia w sieci oczami inżyniera



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

W tym wszystkim chodzi o pakiet…



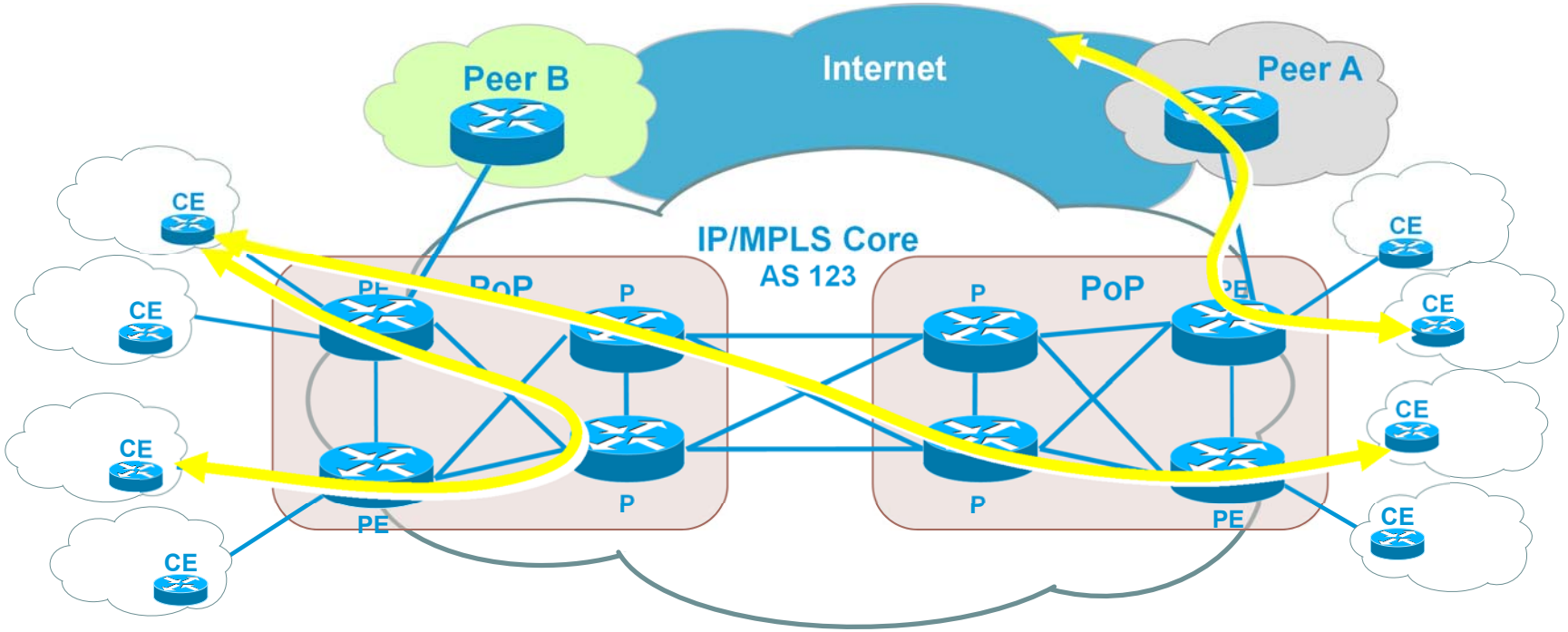
Gdy pakiet już trafi do Internetu, **jakieś urządzenie**, **gdzieś** będzie musiało zrobić jedną z dwóch rzeczy:
[1] **przekazać pakiet dalej*** lub [2] **odrzucić pakiet**

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

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

Warstwa danych IP

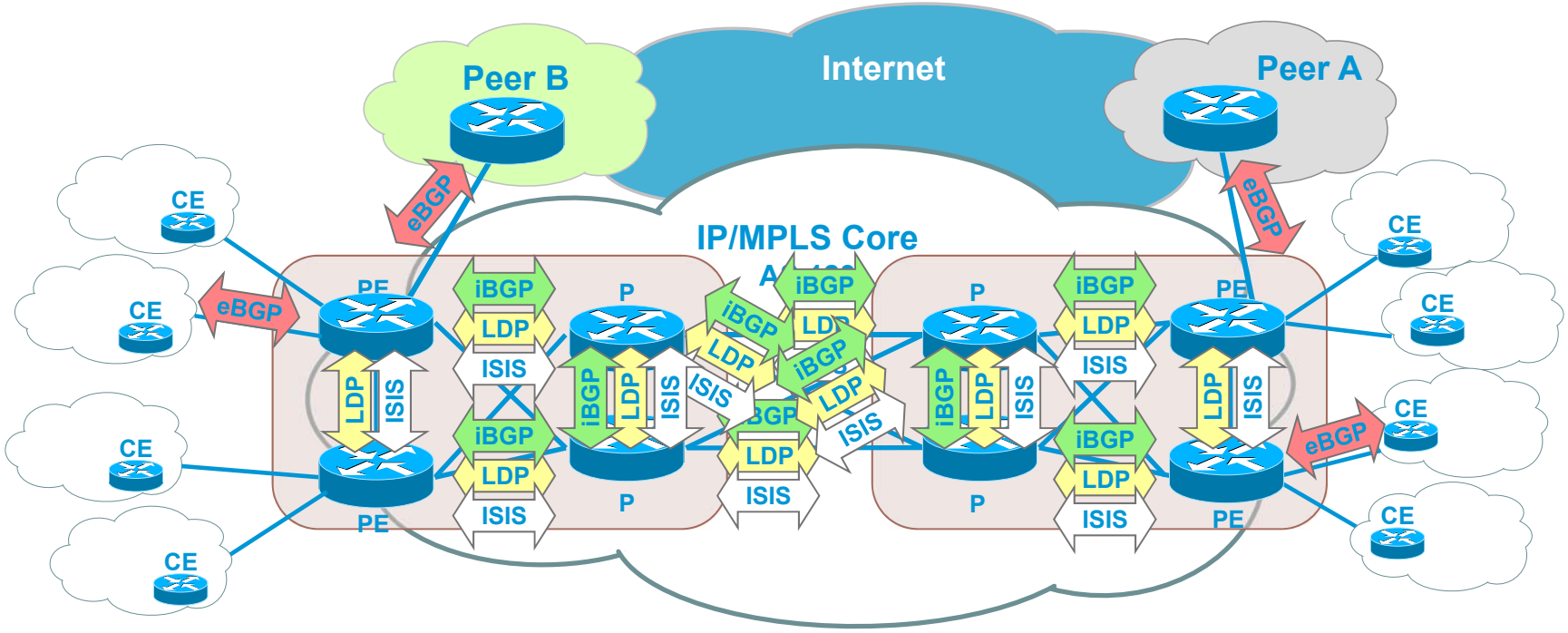
- Logiczna grupa zawierająca ruch generowany przez aplikacje klienta – ruch powstający i terminowany w sieciach klienta
- Ruch warstwy danych traktowany jest zawsze jako tranzytowy przez elementy sieciowej.



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

Warstwa kontrolna

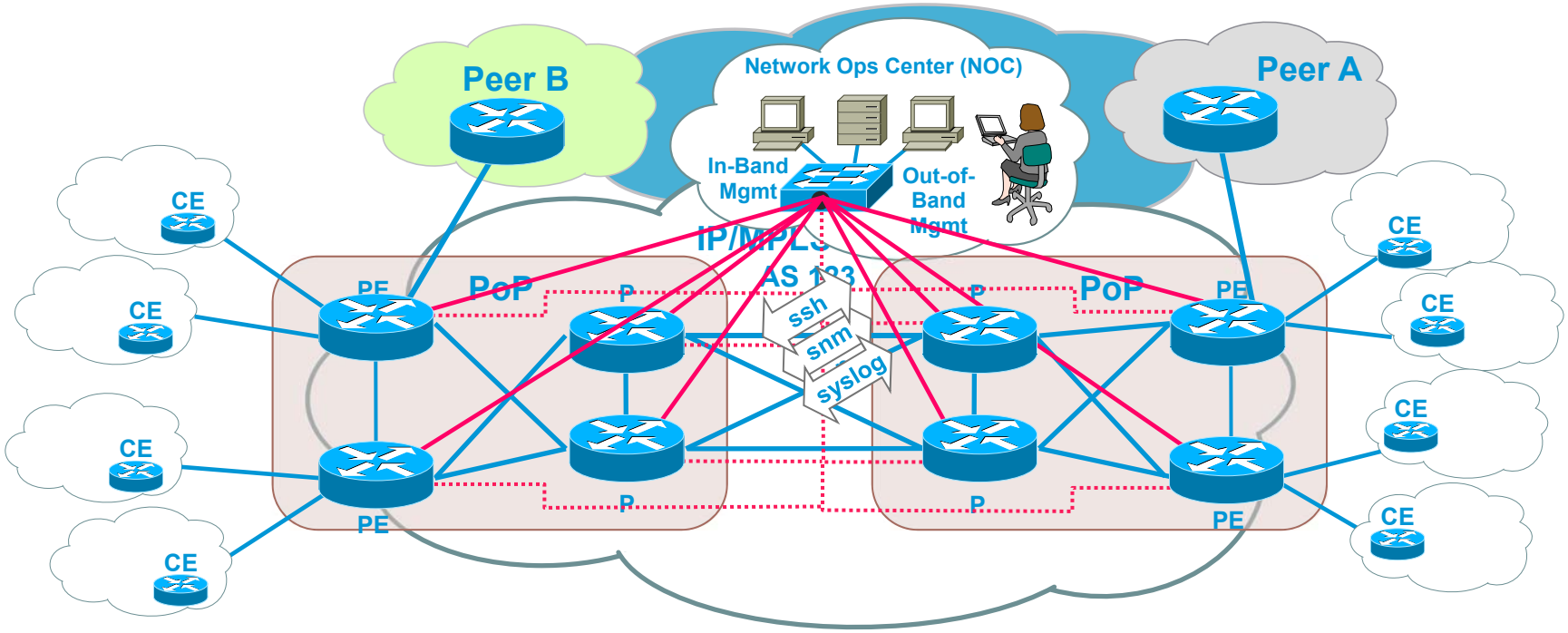
- Logiczna grupa zawierająca ruch protokołów routingu, sygnalizacji, utrzymania łącz (i ich stanu) – wszystko co powoduje że sieć wykorzystująca protokoły takie jak BGP, OSPF, LDP, IS-IS, ARP, Layer 2 keepalives, ATM OAM czy ramki PPP LCP
- Ruch w warstwie kontrolnej zawiera pakiety klasyfikowane jako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



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

Warstwa zarządzania

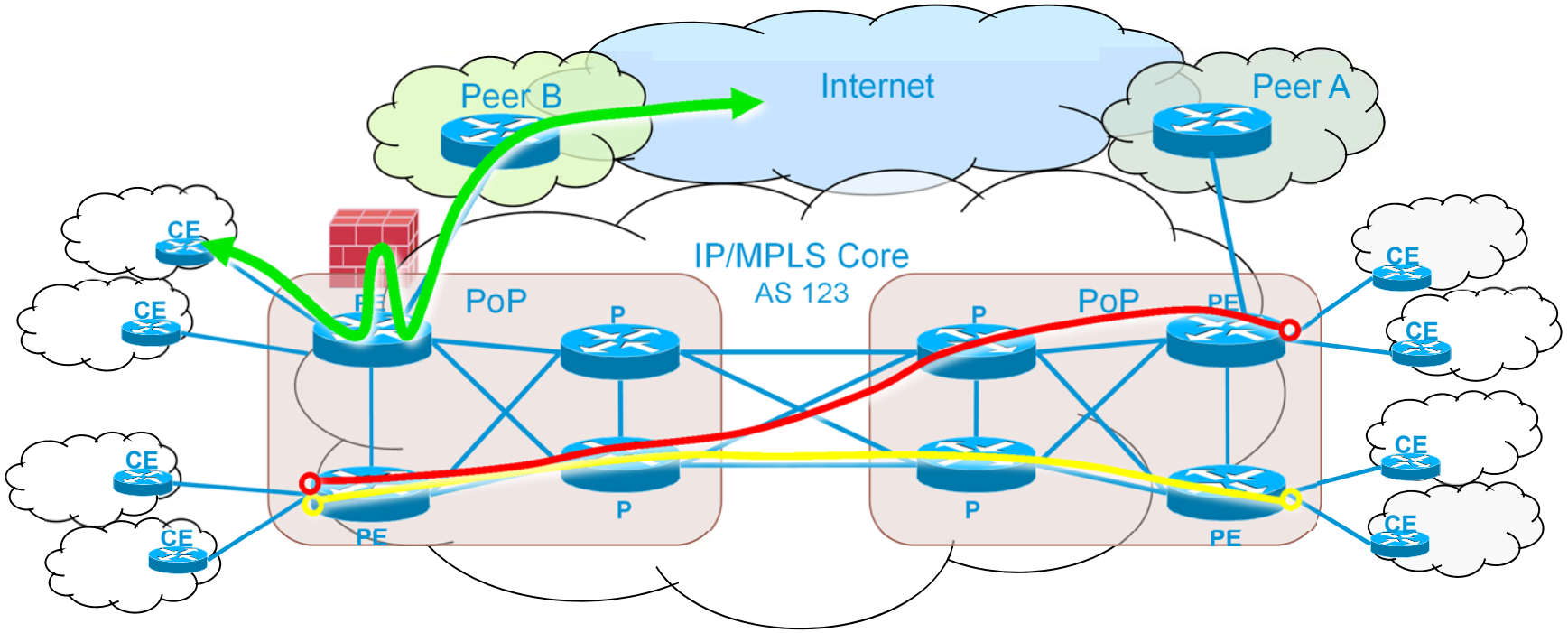
- Logiczna grupa zawierająca ruch służący do zarządzania, provisioningu, utrzymania i monitoringu sieci. Warstwa zawiera ruch taki jak SSH, FTP, SNMP, Syslog, TACACS+ i RADIUS, DNS, NetFlow, ROMMON, CDP itd.
- Ruch w warstwie kontrolnej zawiera pakiety klasyfikowane jako ‘receive’, ale logicznie zawiera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



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

Warstwa usługowa

- Warstwa zawierająca ruch użytkowników sieci (jak warstwa danych), ale z dodatkowymi usługami zapewniającymi funkcjonalności – np. DNS, firewall, IPS, CDN



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

Koncepcja ‘pasma’

- 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:

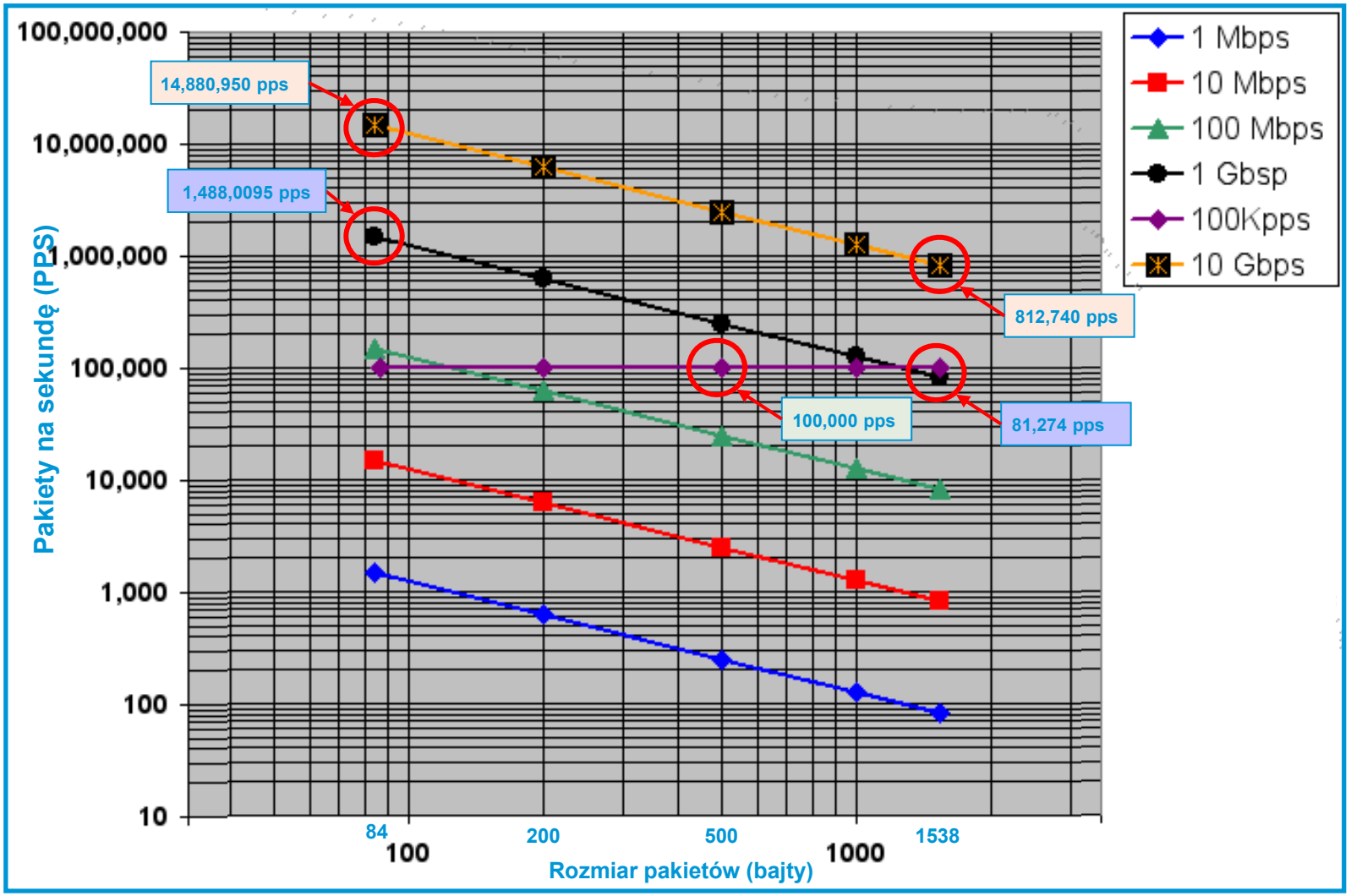
  1,000,000,000 bps/(84 B * 8 b/B) = 1,488,096 fps

- …a dla ruchu 1538 bajtów:

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

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

Koncepcja ‘pasma’ – PPS a długość PDU



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

Bezpieczeństwo

Warstwa kontrolna

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

Bezpieczeństwo warstwy kontrolnej

- Bezpieczeństwo samej warstwy kontroli:
  - Zmninimalizować ilość usług na węźle
  - Odfiltrować ruch do RP węzła (iACL/rACL)
  - Control Plane Policing i Rate-Limiting (CoPP)
  - Local Packet Transport Services (LPTS)
- Bezpieczeństwo protokołów routingu:
  - Uwierzytelnianie sąsiadów (TCP-AO, MD5)
  - Generalized TTL Security Mechanism (GTSH)
  - Selective Packet Discard (SPD)
  - Secure InterDomain Routing (SIDR)
- Bezpieczeństwo innych protokołów:
  - Label Distribution Protocol (LDP)
  - Resource Reservation Protocol (RSVP)

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

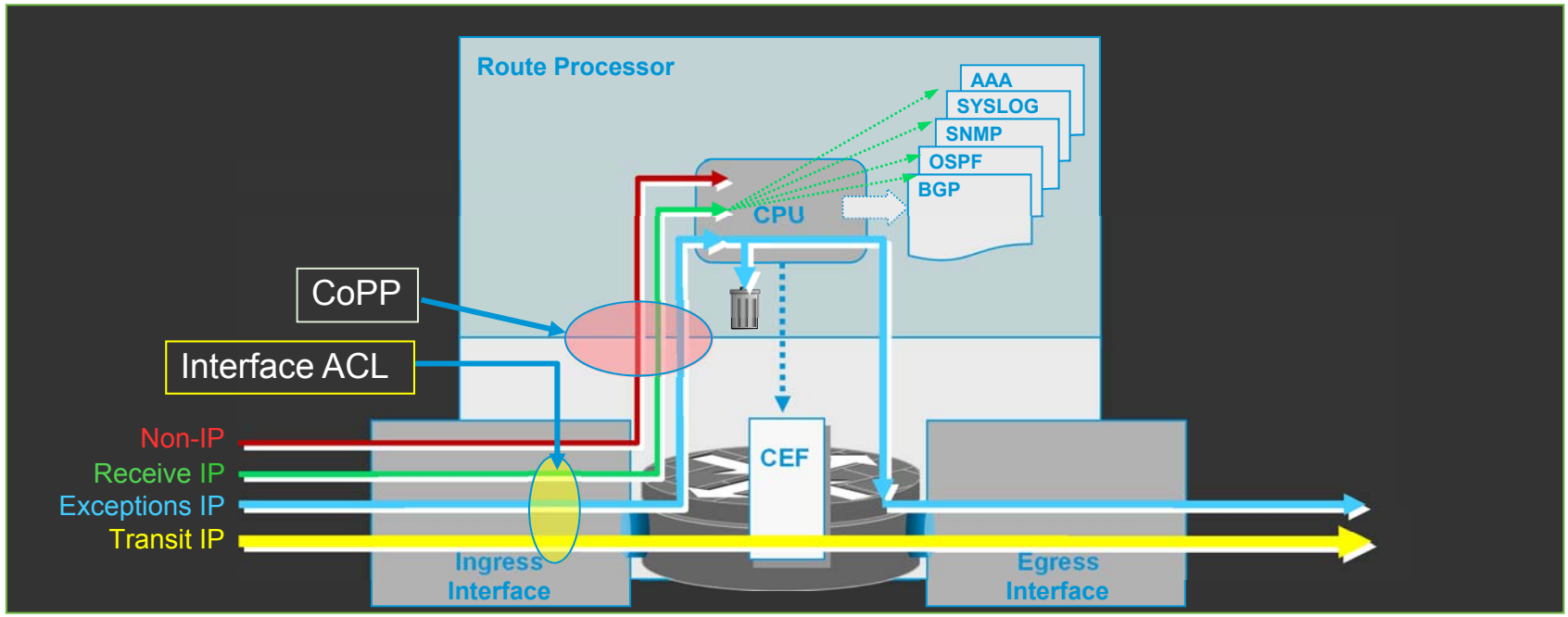
Zabezpieczanie routerów

- 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/

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

Control Plane Policing (CoPP)

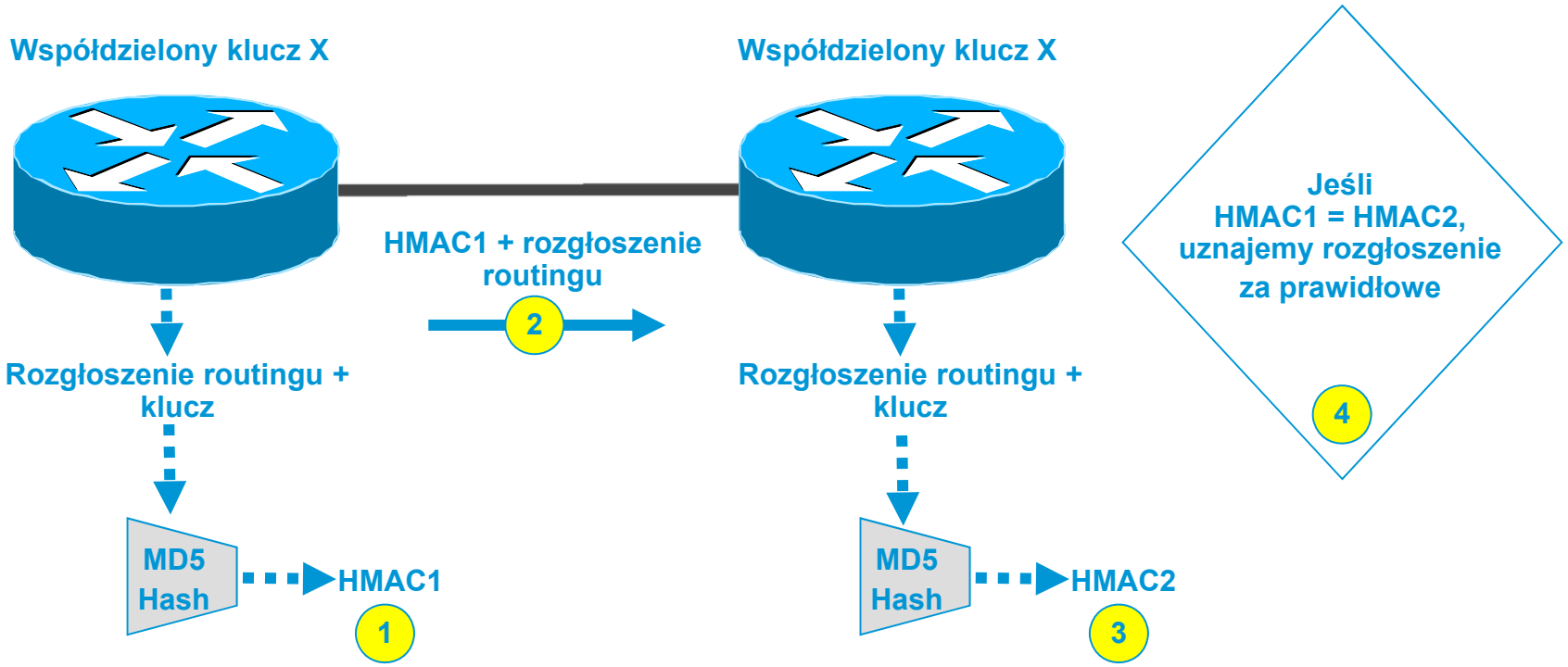
- Ruch docierający do RP węzła należy odpowiednio kontrolować
  - Parametry wydajnościowe węzła są czasami zapisane na stałe w sprzęcie
  - Mechanizmy takie jak CoPP (węzły software'owe Cisco) i LPTS (systemy pracujące pod kontrolą IOS-XR) pozwalają dostosować konfigurację do wymaganej polityki



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

Uwierzytelnianie protokołów routingu

- Uwierzytelnianie protokołów routingu za pomocą hasha MD5: BGP, OSPF, LDP, RIPv2, IS-IS, HSRP, EIGRP, MSDP
- Dodatkowo można zmieniać klucze w czasie za pomocą TCP-AO



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

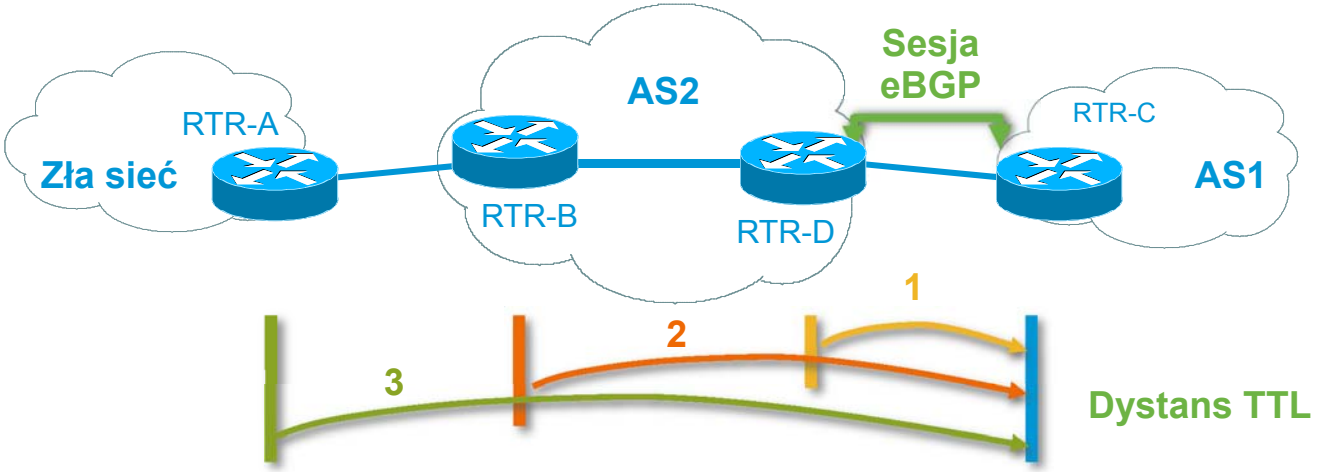
Dodatkowe mechanizmy bezpieczeństwa

- Dodatkowe mechanizmy bezpieczeństwa w szczególności dotyczące protokołu BGP to między innymi:
  - Filtry prefiksów
  - Limity na prefiksy
  - Limity na AS-PATH
  - Generalized TTL Security mechanism (RFC 3682)
  - Secure InterDomain Routing (SIDR)

See http://www.cisco.com/web/about/security/intelligence/protecting_bgp.html

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

Generalized TTL Security Mechanism



- GTSM wymusza minimalną wartość TTL którą musi mieć pakiet żeby został przekazany do procesu BGP
- Ograniczamy ilość „inteligencji” po stronie węzła oszczędzając zasoby RP

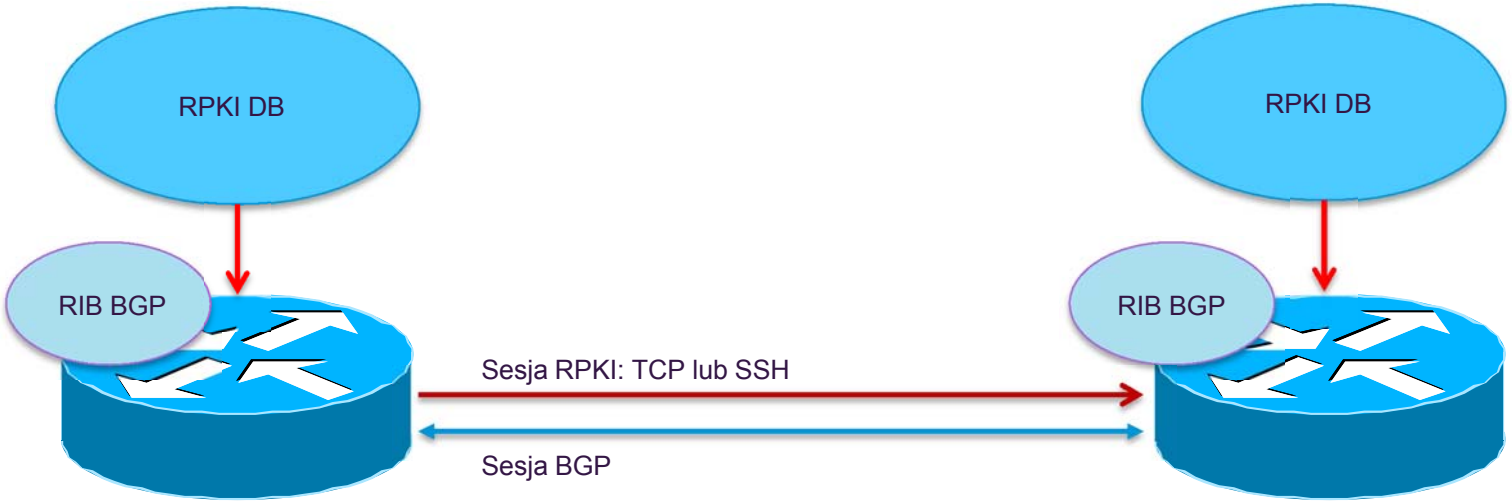
© 2010 Cisco and/or its affiliates. All rights reserved.

Po co nam SIDR i co to jest?

- Dowolny AS może rozgłosić dowolny prefiks
  - zwykle przez pomyłkę
  - złośliwie
- Tak czy inaczej, AS „porywa” przestrzeń rozgłoszoną i zaczyna otrzymywać, który powinien był docierać do kogoś innego
  - Na straży stoją tutaj filtry prefiksów generowane z baz RIRów...
  - Przykłady (YouTube i Pakistan Telecom) pokazują, że nie zawsze działa to dobrze
- SIDR to pomysł na uwierzytelnienie rozgłoszeń i kontrolę tych rozgłoszeń

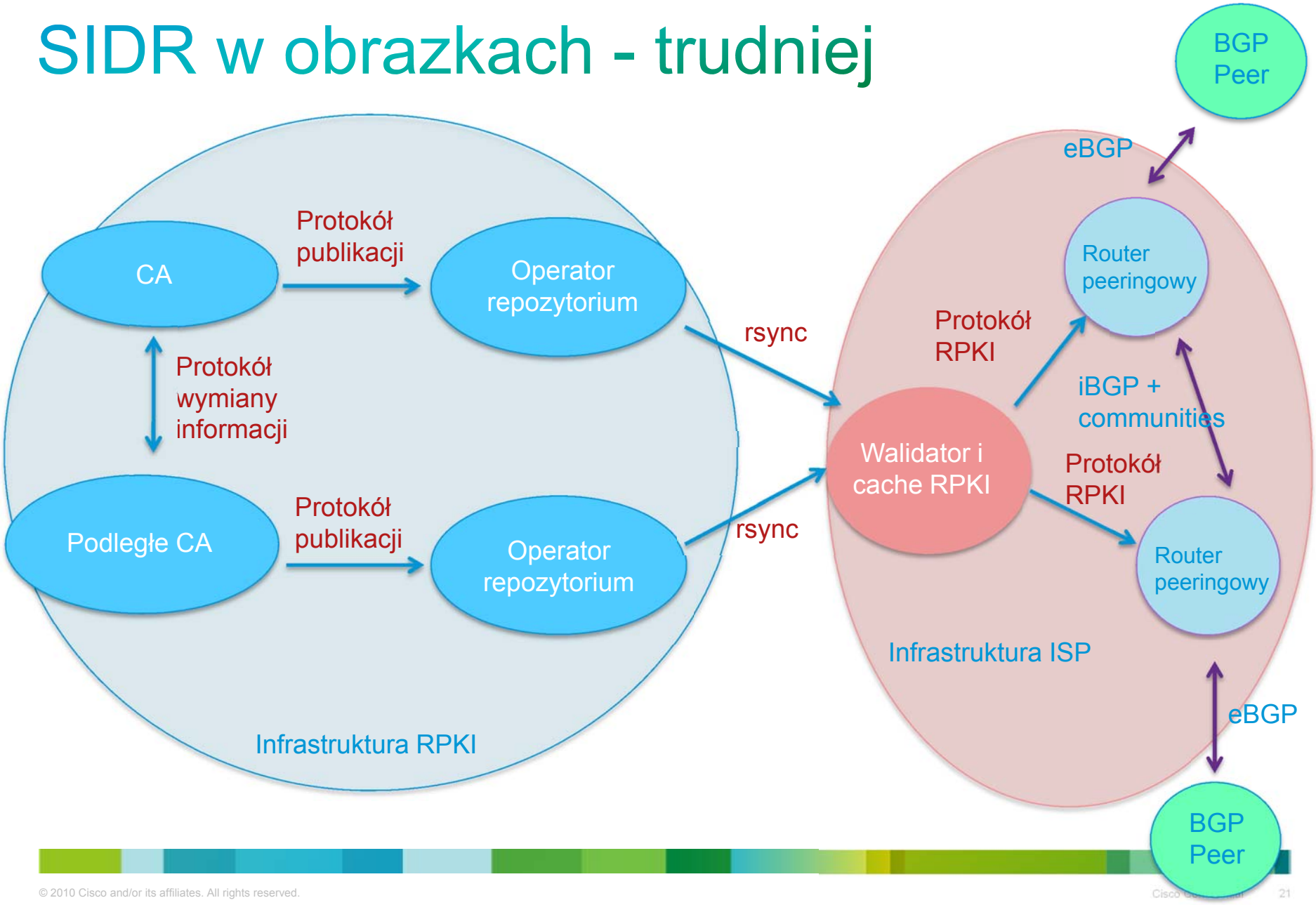
© 2010 Cisco and/or its affiliates. All rights reserved.

SIDR w obrazkach - prościej



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

SIDR w obrazkach - trudniej



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

SIDR – stan prefiksu

- VALID

  Prefiks rozgłoszono w zakresie określonym przez limity masek i przez właściwy Origin AS

  Certyfikat jest ważny

- INVALID

  Prefiks nie zawiera się w długości maski określonej przez certyfikat

  Origin AS jest zły

  Certyfikat jest nieważny, lub łańcuch certyfikatów nie jest prawidłowy

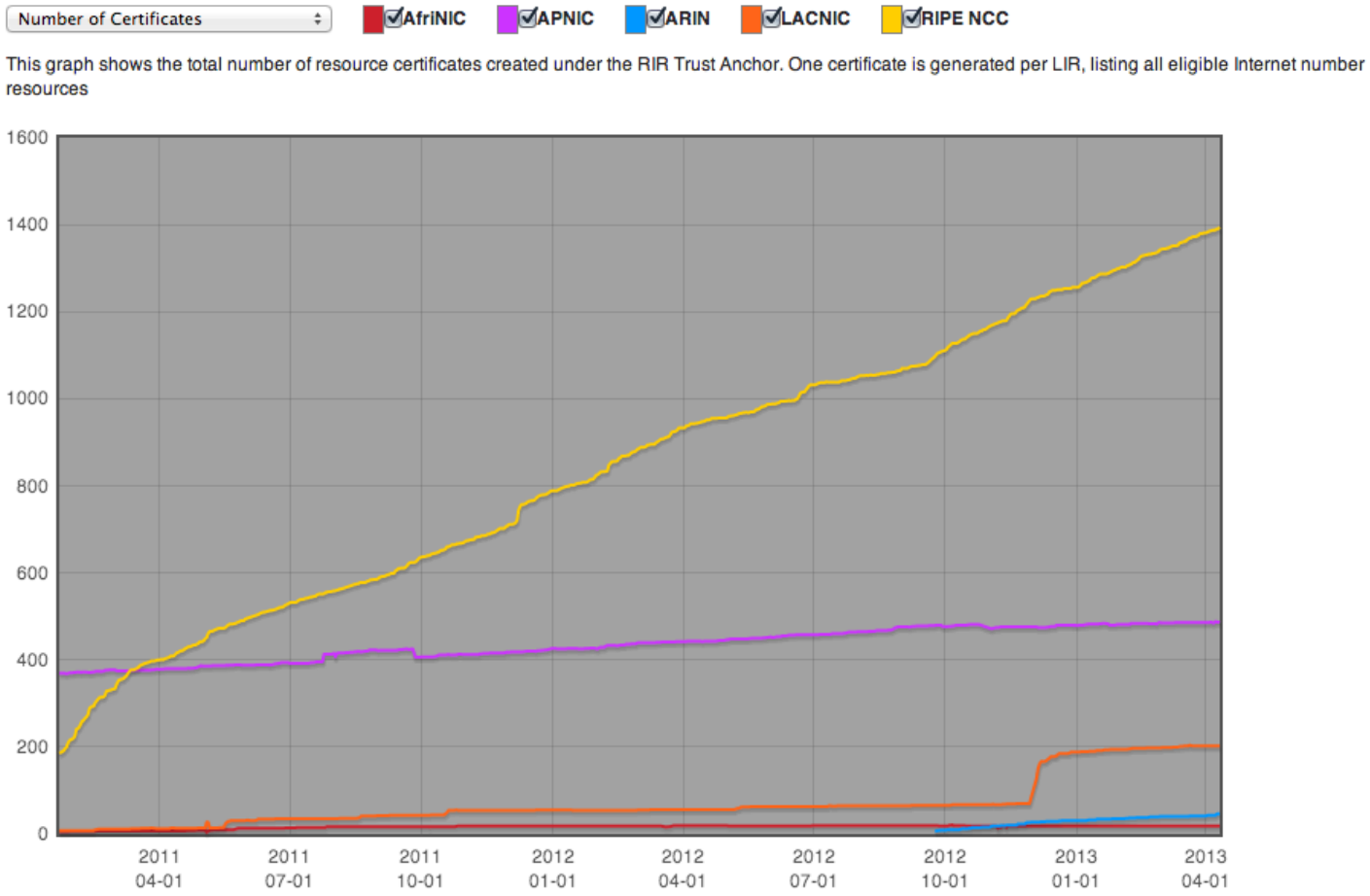
- NOT FOUND

  Prefiks nie został znaleziony w bazie i nie może zostać zweryfikowany

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

RPKI – statystyki w RIPE

http://certification-stats.ripe.net/



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

Bezpieczeństwo
Warstwa zarządzania

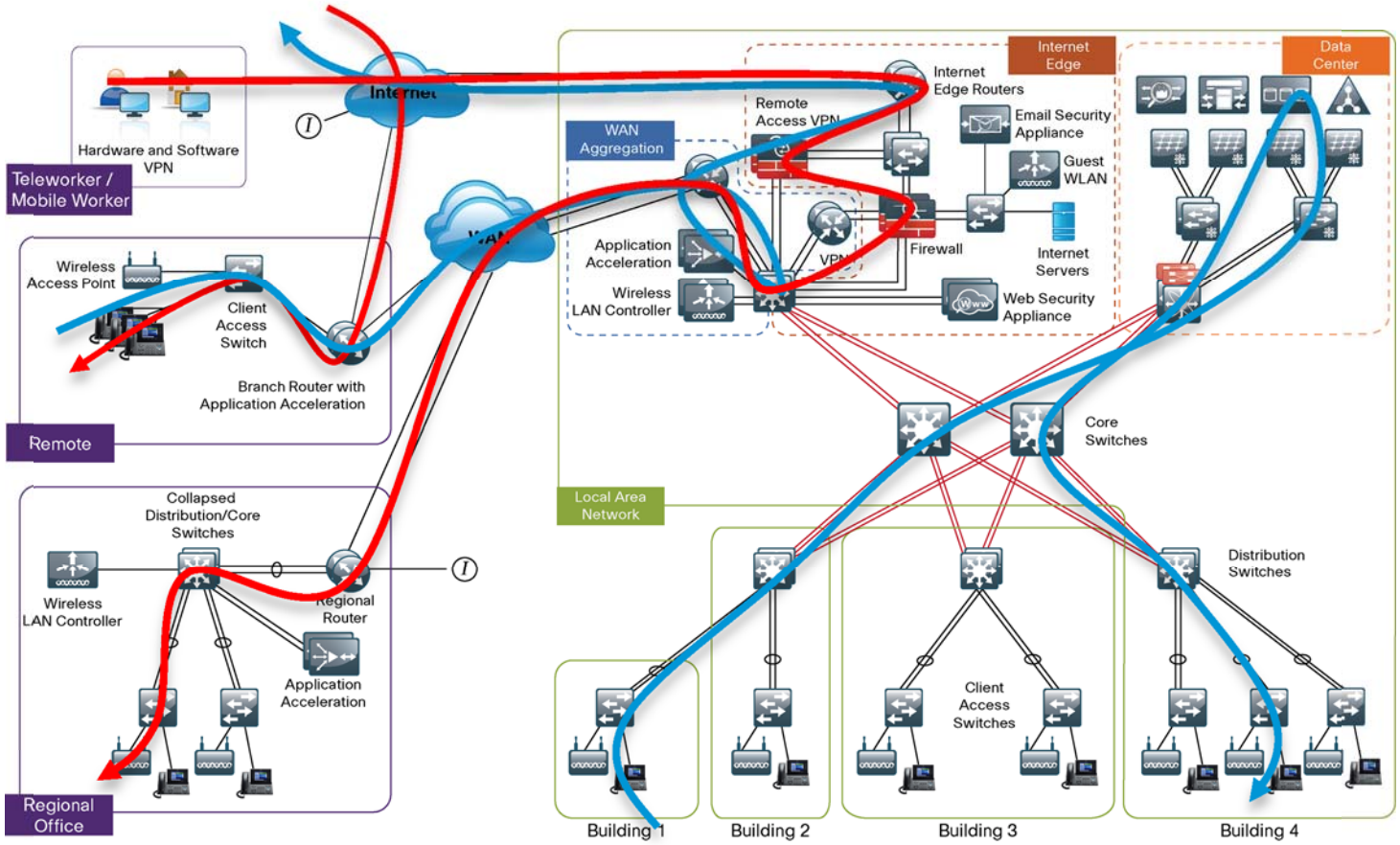
© 2010 Cisco and/or its affiliates. All rights reserved.

Bezpieczeństwo warstwy zarządzania

- AAA
  - TACACS+, RADIUS, konta lokalne (także jako zapas przy awarii!)
- Bezpieczeństwo węzła
  - Informacje przy logowaniu
  - Mechanizm RBAC – IOS/IOS-XE/IOS-XR/NX-OS i mechanizm widoków
  - Bezpieczny system plików
  - Podpisane kryptograficznie pliki binarne
- Zarządzanie węzłem
  - SNMP, EEM, SYSLOG, Telnet, SSH, SCP, FTP, TFTP
  - Zarządzanie OoB
- Telemetria sieciowa
  - NetFlow v9 / Flexible NetFlow
  - Zliczanie ruchu IPv4/IPv6

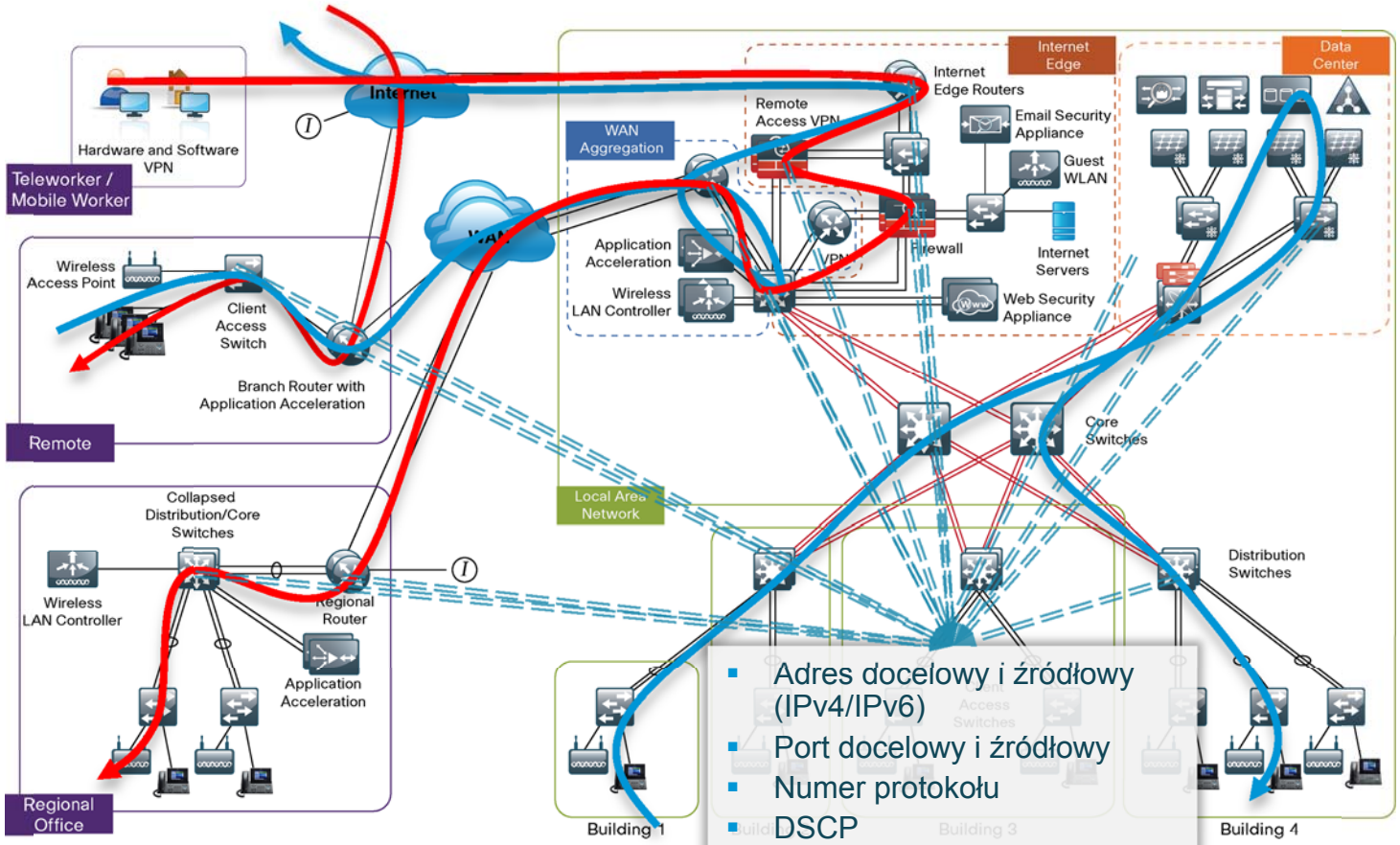
© 2010 Cisco and/or its affiliates. All rights reserved.

Jak dobrze monitorować ruch w sieci?



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

Jak dobrze monitorować ruch w sieci?



- Adres docelowy i źródłowy (IPv4/IPv6)
- Port docelowy i źródłowy
- Numer protokołu
- DSCP
- Interfejs wejściowy
- Pole next-hop z BGP
- Informacje z etykiety MPLS
- Informacje o multicaście
- Informacje z L2 (tag 802.1q, pole CoS, etc)

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

NetFlow?

- Narzędzie do zbierania informacji o ruchu w sieci IP w ujęciu sesji danych (jednocześnie – protokół eksportowy)
  - NetFlow v5 i v9
- Coraz doskonalsze narzędzia opierające się o NetFlow połączony z dodatkowymi algorytmami klasyfikacji aplikacji (NBAR/NBAR2/AVC) pozwalają na szczegółowe rozliczanie i monitoring – dla wielu równoczesnych odbiorców
  - np. dział bezpieczeństwa zbiera informacje o dużej ilości krótkich sesji
  - np. dział monitoringu zbiera informacje o skuteczności inżynierii ruchowej w sieci
  - np. dział biznesowy otrzymuje informacje o krytycznych danych nowej aplikacji działającej dla pewnej grupy klientów

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

NetFlow – pola kluczowe tworzące „flow”

Pola kluczowe	Pakiet 1
Źródłowe IP	1.1.1.1
Docelowe IP	2.2.2.2
Port źródłowy	23
Port docelowy	22078
Protokół L3	TCP - 6
Bajt ToS	0
Inne pola	
Długość	1250

- Pola kluczowe są unikalne dla danej sesji
- Pola nie będące kluczowymi są atrybutami danej sesji
- Jeśli pola kluczowe są unikalne (nie istnieją do tej pory w pamięci podręcznej) – tworzony jest nowy „flow” czyli sesja

Pola kluczowe	Pakiet 2
Źródłowe IP	3.3.3.3
Docelowe IP	4.4.4.4
Port źródłowy	80
Port docelowy	22079
Protokół L3	TCP - 6
Bajt ToS	0
Inne pola	
Długość	519

SRC IP	DST IP	IF	Protokół	ToS	…	Pkts
1.1.1.1	2.2.2.2	GE1/0	6	0	…	11000

SRC IP	DST IP	IF	Protokół	ToS	…	Pkts
3.3.3.3	4.4.4.4	GE2/1	6	0	…	50
1.1.1.1	2.2.2.2	GE1/1	6	0	…	11000

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

Bezpieczeństwo
Warstwa danych

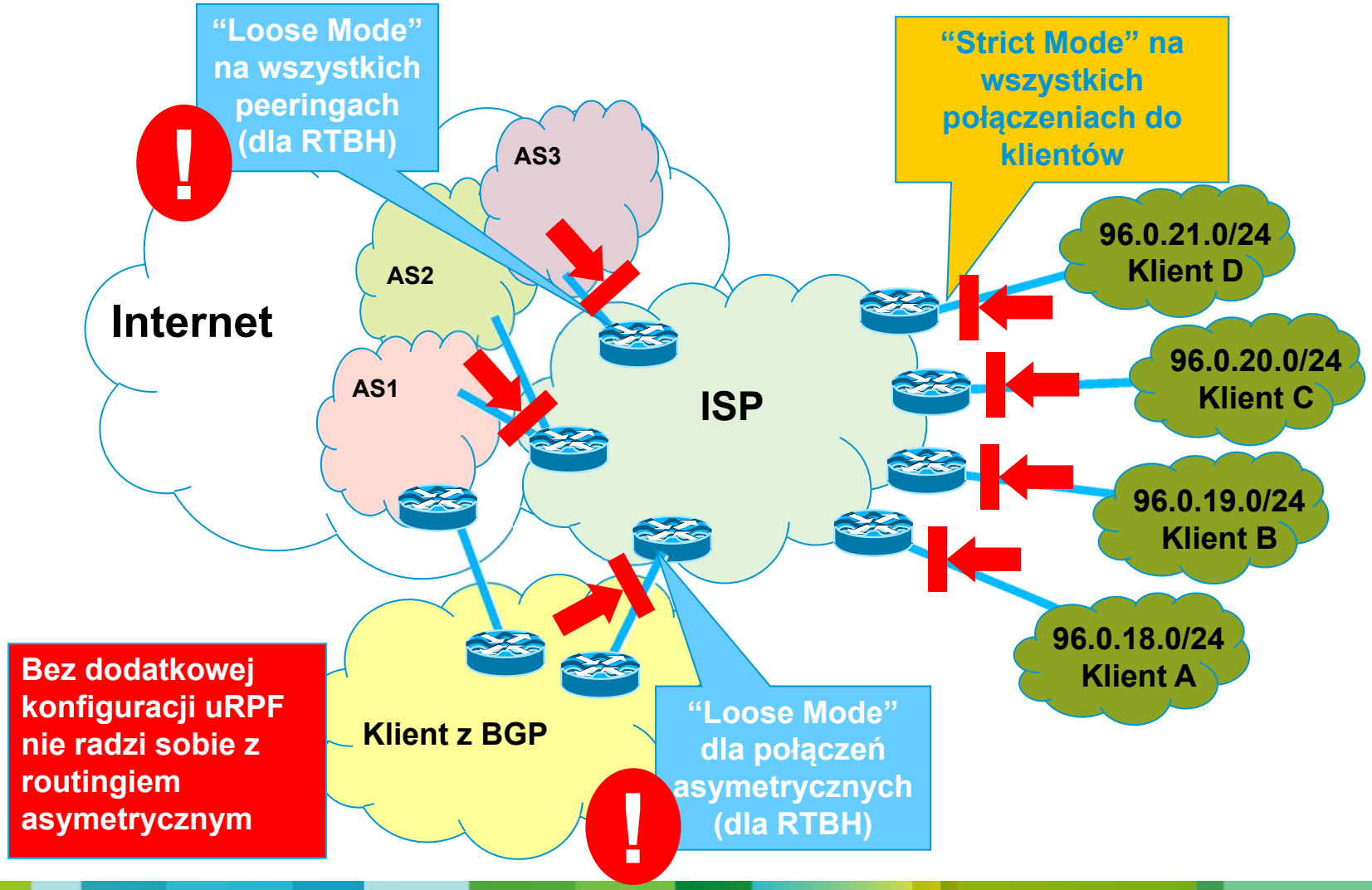
© 2010 Cisco and/or its affiliates. All rights reserved.

Bezpieczeństwo warstwy danych

- Filtrowanie i ograniczanie ruchu
  - ACL i uRPF (BCP38)
  - Wykorzystanie mechanizmów QoS (policing)
- Wykorzystanie protokołów i interakcji pomiędzy nimi
  - Filtrowanie opcji – dla IPv4 & IPv6
  - Ataki na bramki IPv4<>IPv6 i protokoły stanowe
- Ogólne rekomendacje dla róznych scenariuszy/topologii
  - Połączenia PE-CE dla sieci MPLS
  - Ukrywanie szkieletu
- Bardziej zaawansowane mechanizmy i narzędzia
  - BGP Blackholing i Sinkholing
  - QoS Policy Propagation with BGP (QPPB)

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

Gdzie stosować uRPF?



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

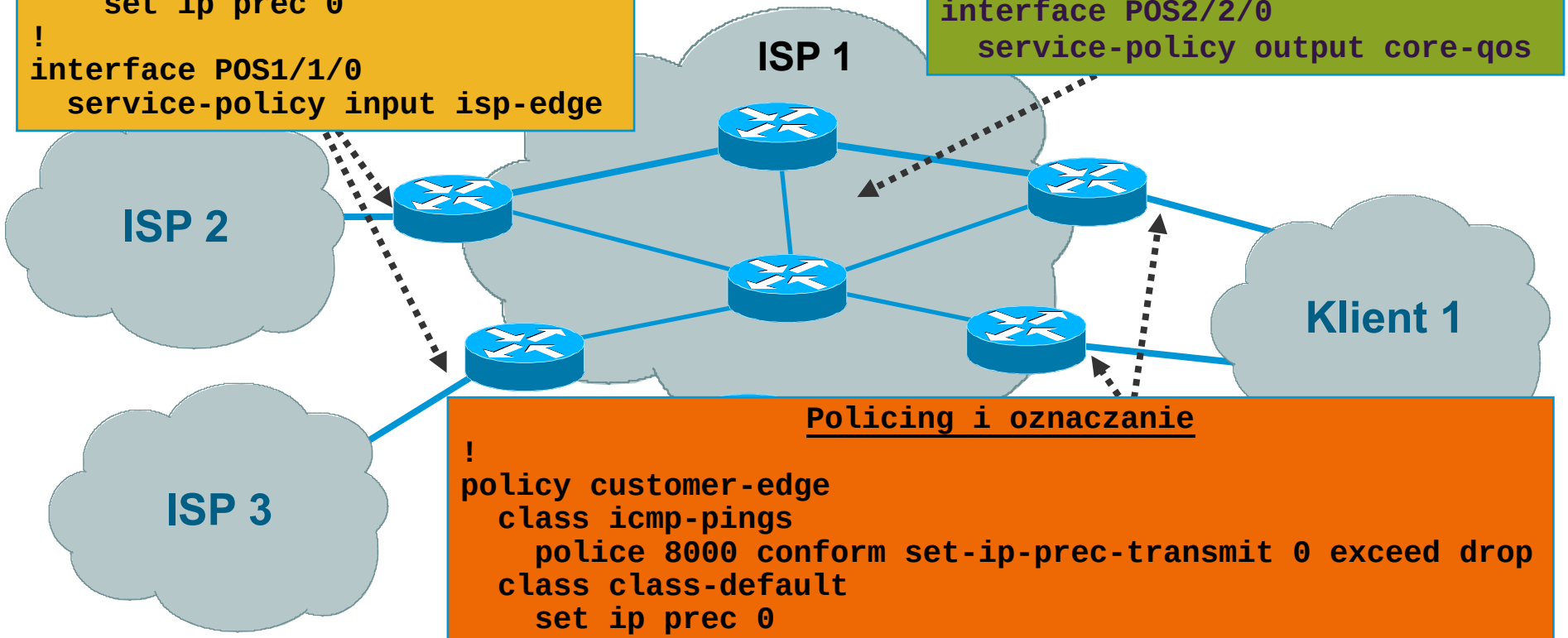
Wykorzystanie QoS

Oznaczanie (marking)

```
!
policy isp-edge
  class class-default
    set ip prec 0
!
interface POS1/1/0
  service-policy input isp-edge
```

Kolejkowanie

```
!
policy core-qos
  class prec6-control
    bandwidth percent 25
  class prec0-data
    bandwidth percent 75
!
interface POS2/2/0
  service-policy output core-qos
```



Policing i oznaczanie

```
!
policy customer-edge
  class icmp-pings
    police 8000 conform set-ip-prec-transmit 0 exceed drop
  class class-default
    set ip prec 0
!
interface POS3/3/0
 service-policy input customer-edge
```

© 2010 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’

© 2010 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

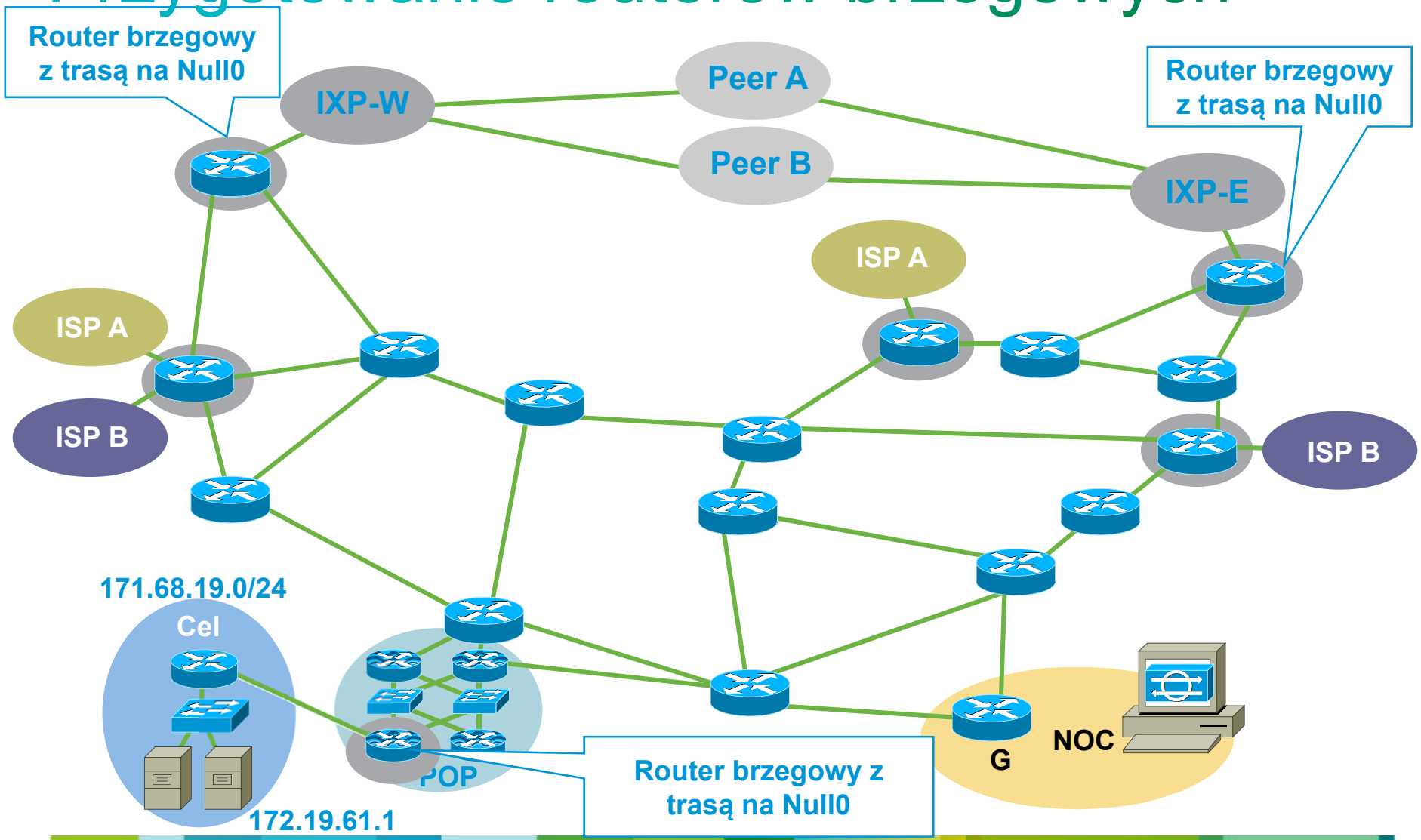
Trasa statyczna na routerze brzegowym—192.0.2.1 = Null0

172.19.61.1= 192.0.2.1 = Null0

Ruch do adresu 172.19.61.1 jest routowany do Null0

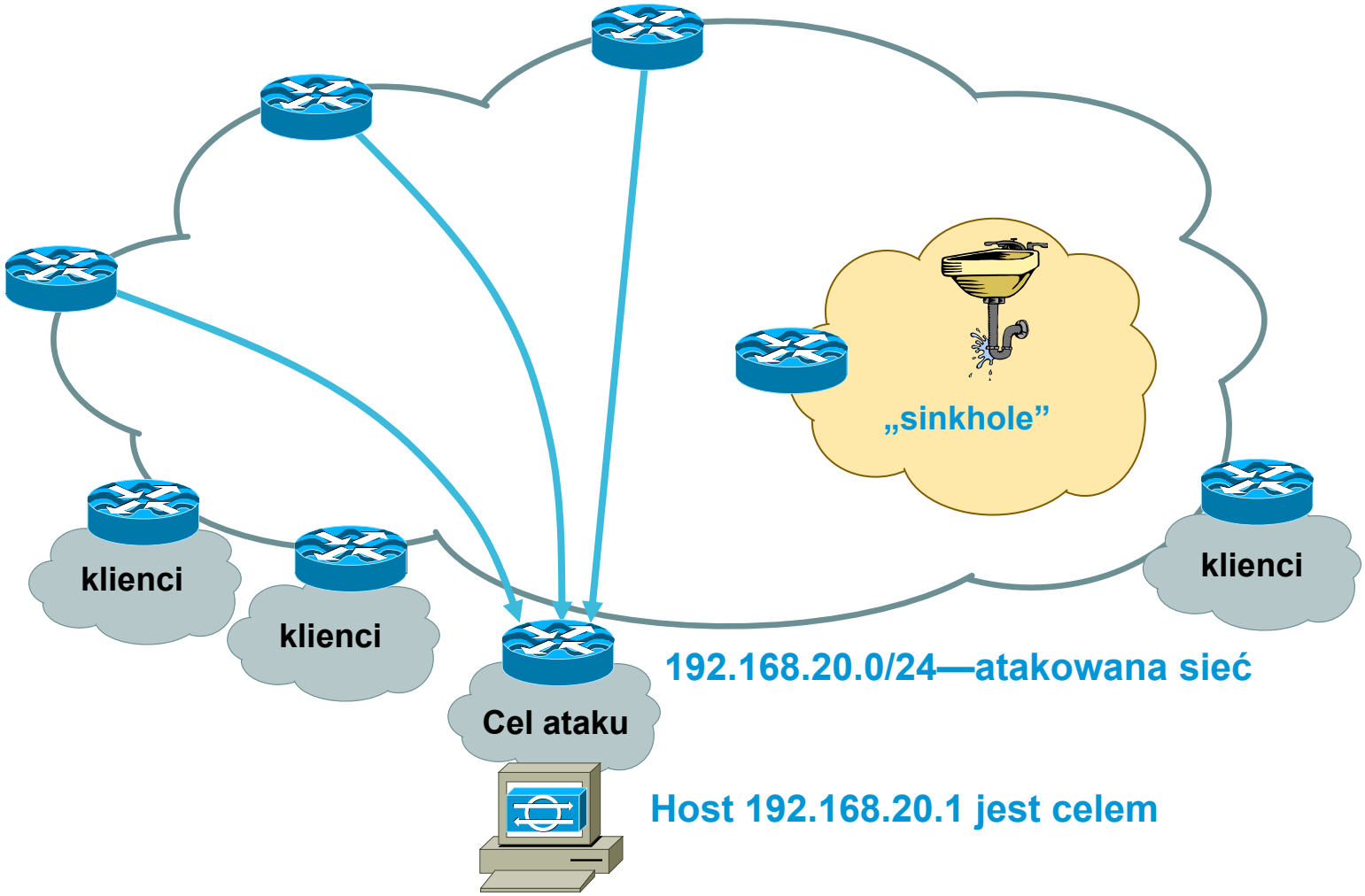
© 2010 Cisco and/or its affiliates. All rights reserved.

Przygotowanie routerów brzegowych



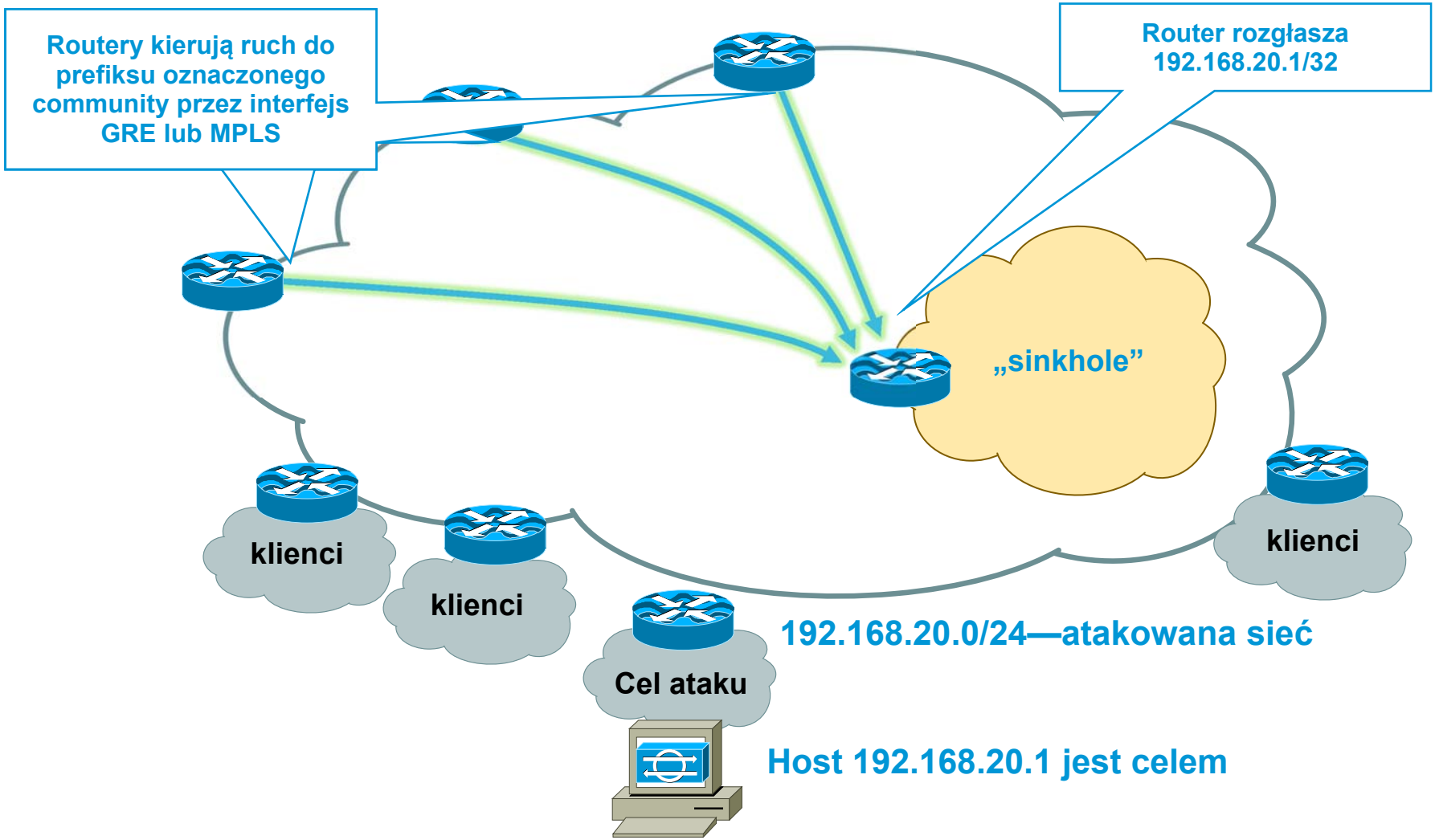
© 2010 Cisco and/or its affiliates. All rights reserved.

Routery/sieci ‘sinkhole’



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

Routery/sieci ‘sinkhole’



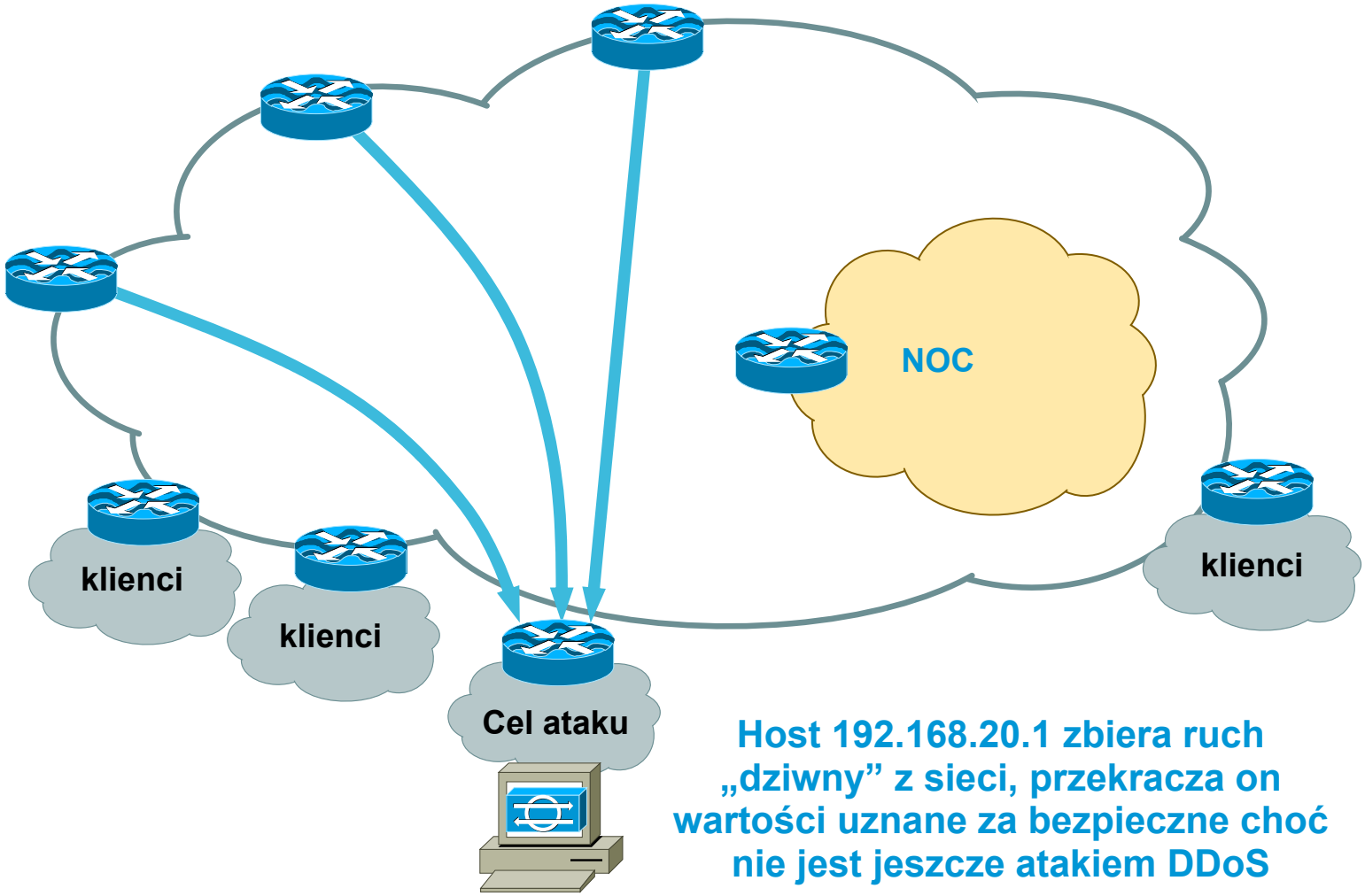
© 2010 Cisco and/or its affiliates. All rights reserved.

QoS policy propagation with BGP

- Możliwość dystrybucji polityki QoS na wiele routerów jednocześnie i sterowania nią za pomocą wartości community
- 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, realizowania kolejkowania, reklasyfikacji, etc.

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

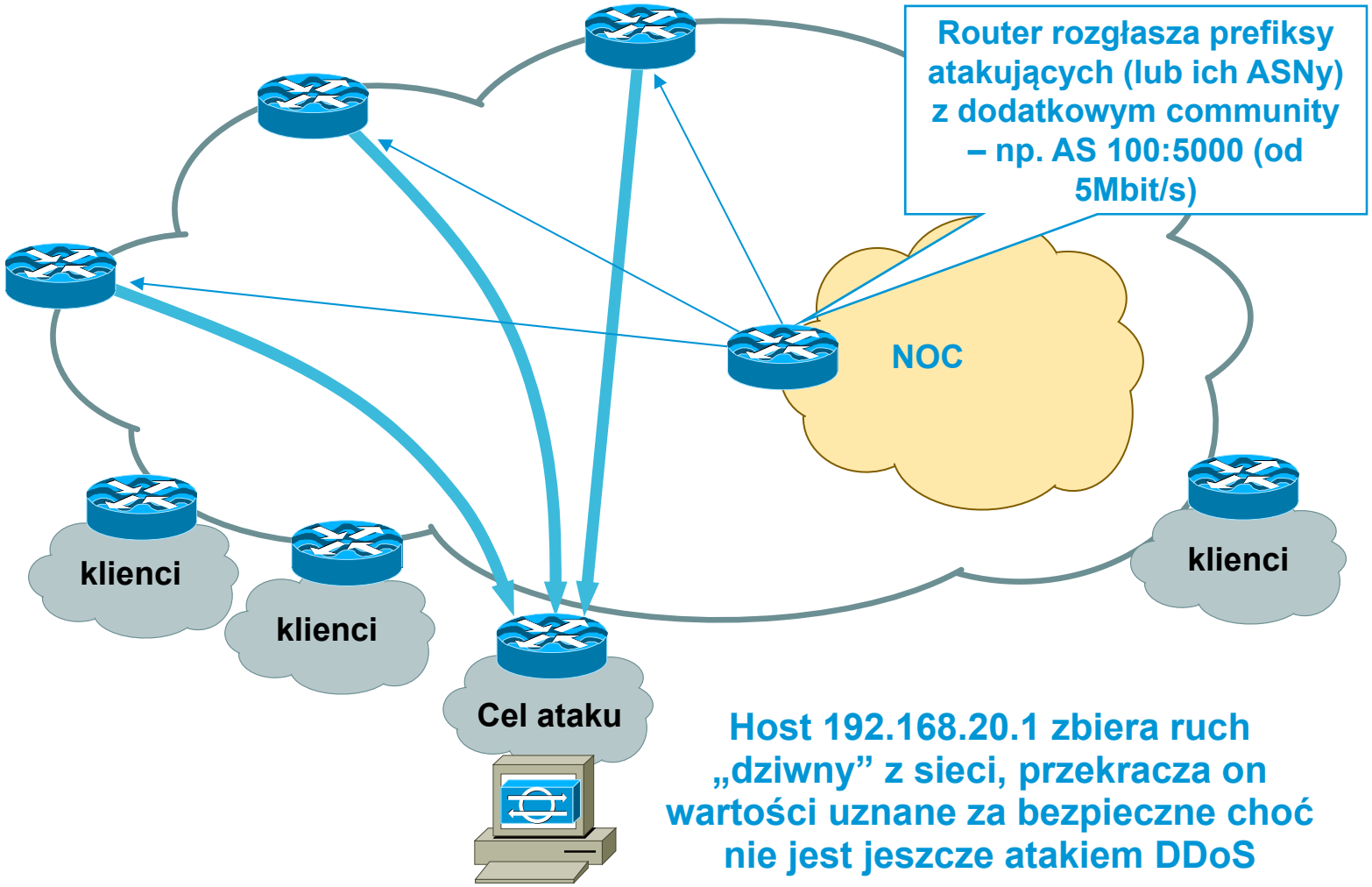
QoS Policy Propagation with BGP



Host 192.168.20.1 zbiera ruch „dziwny” z sieci, przekracza on wartości uznane za bezpieczne choć nie jest jeszcze atakiem DDoS

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

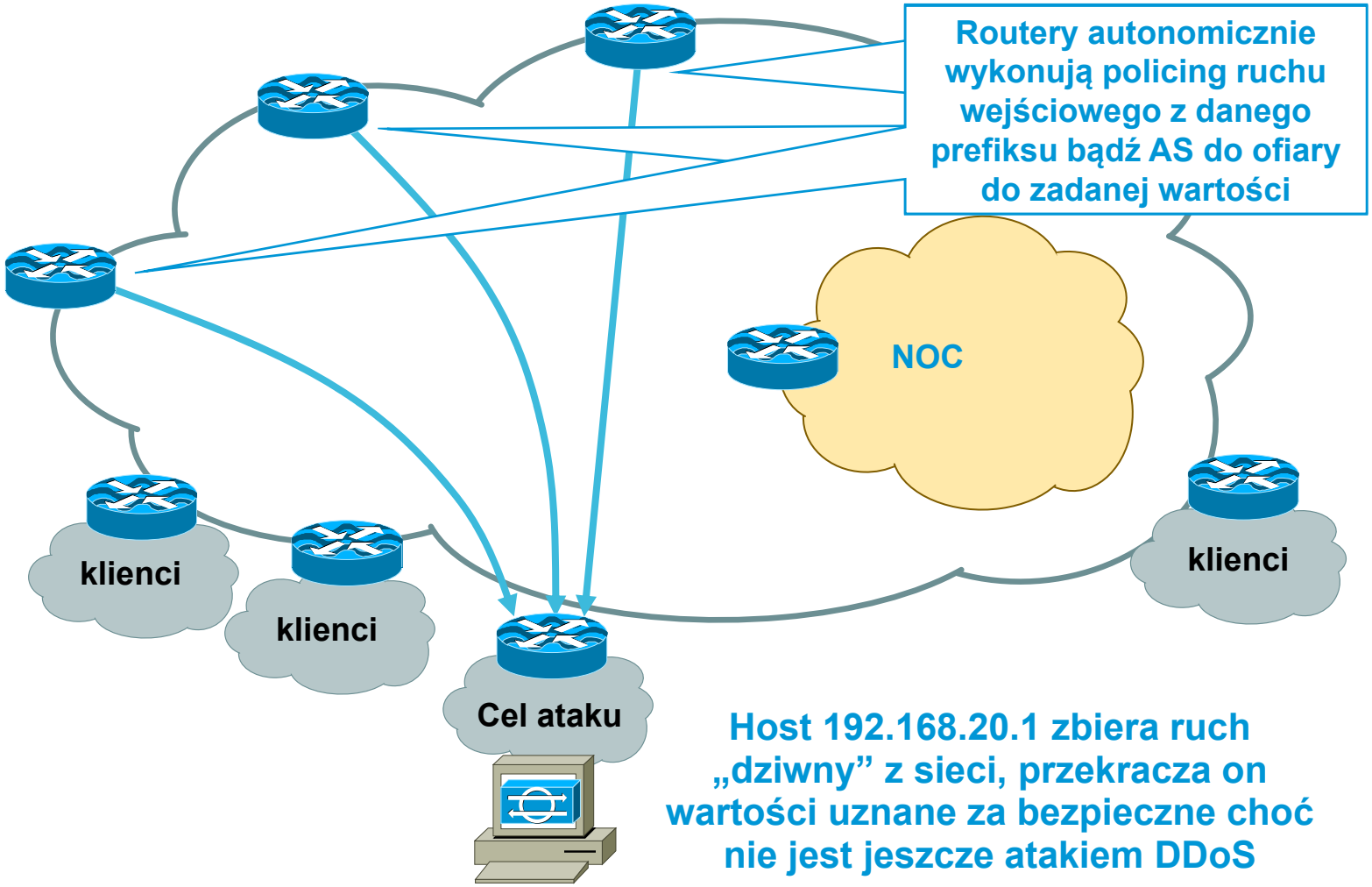
QoS Policy Propagation with BGP



Host 192.168.20.1 zbiera ruch „dziwny” z sieci, przekracza on wartości uznane za bezpieczne choć nie jest jeszcze atakiem DDoS

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

QoS Policy Propagation with BGP



Host 192.168.20.1 zbiera ruch „dziwny” z sieci, przekracza on wartości uznane za bezpieczne choć nie jest jeszcze atakiem DDoS

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

Bezpieczeństwo

Warstwa usług

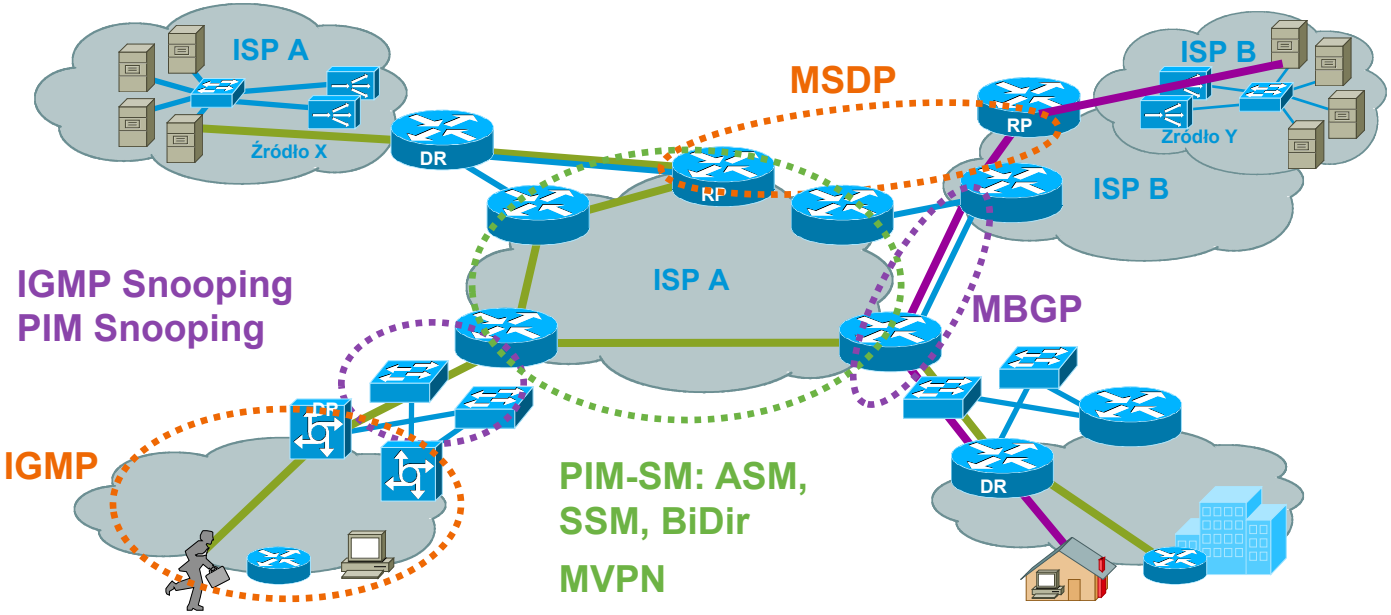
© 2010 Cisco and/or its affiliates. All rights reserved.

Bezpieczeństwo usług

- Bezpieczeństwo multicastu
- Bezpieczeństwo styku MPLS InterAS
- Ataki DDoS w warstwie usługowej

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

Elementy architektury multicastowej



Multicast w sieci LAN/WAN

- Stacje końcowe – router-do-hosta
  - IGMP
- Przełączniki (optymalizacja L2)
  - IGMP snooping i PIM snooping
- Routery (protokół przekazywania)
  - PIM sparse mode lub bidirectional PIM

Multicast między domenami

- Multicast pomiędzy domenami
  - MBGP
- Multicast source discover
  - MSDP with PIM-SM
- Source Specific Multicast
  - SSM

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

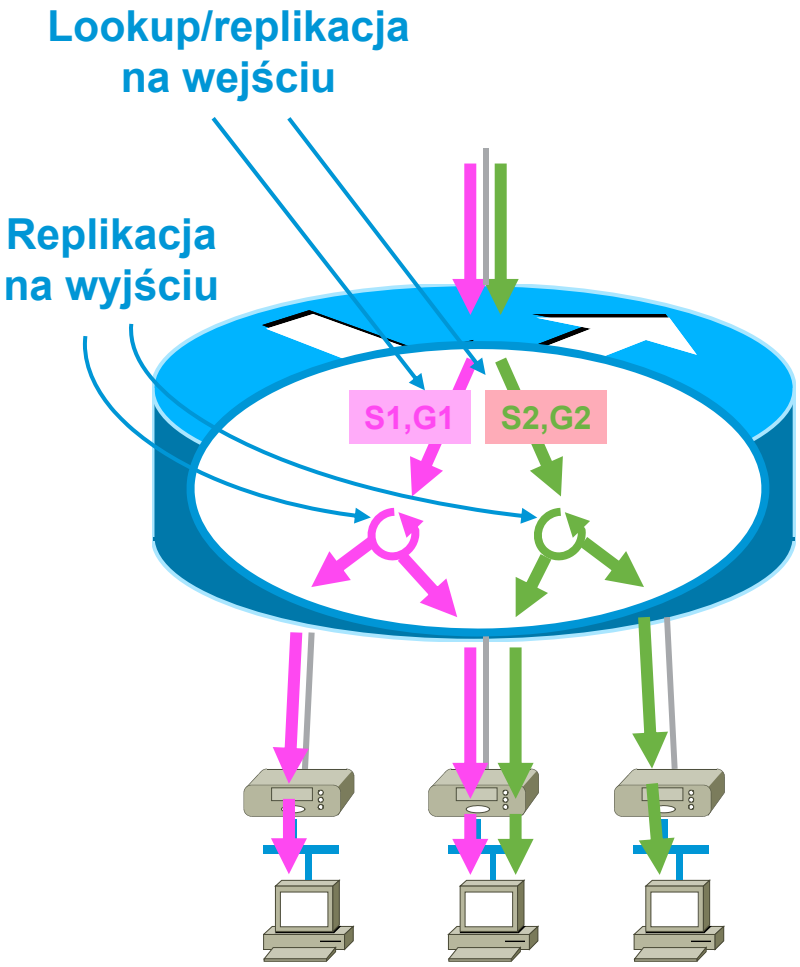
Bezpieczeństwo multicastu

- Z punktu widzenia „warstw” – warstwa kontroli
- Protokoły możliwe do zaatakowania, a w związku z tym konieczne do warstwowego zabezpieczenia:
  - IGMP, MLD
  - PIM, MSDP, AutoRP/BSR/MA
- CoPP/LPTS dla ruchu multicastowego trafiającego do RP
  - przypadki z TTL=1
- „Logika” ruchu multicastowego
  - Dostęp do grup
  - Granice domen multicastowych

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

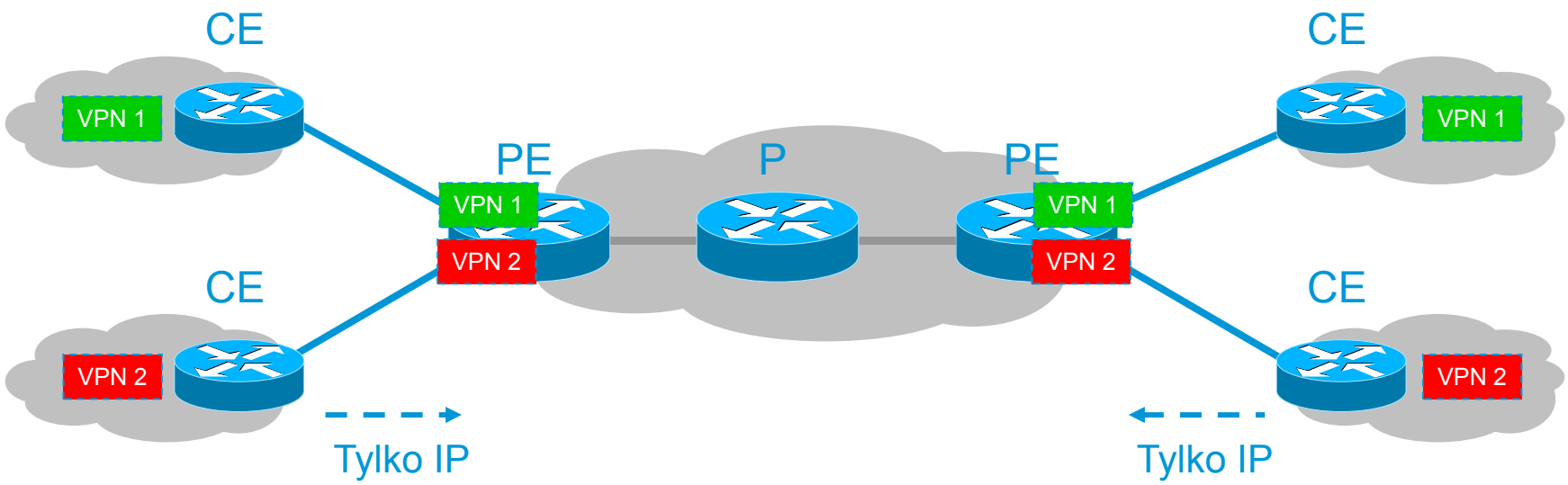
Bezpieczeństwo multicastu

- Stan „wejściowy”
  - per aplikacja/nadawca
- Stan „wyjściowy”
  - per odbiorca/gałąź
- Limity programowe – 100k+
- Limity sprzętowe – 5k-100k
- Limity wydajnościowe
  - Replikacja – gdzie?



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

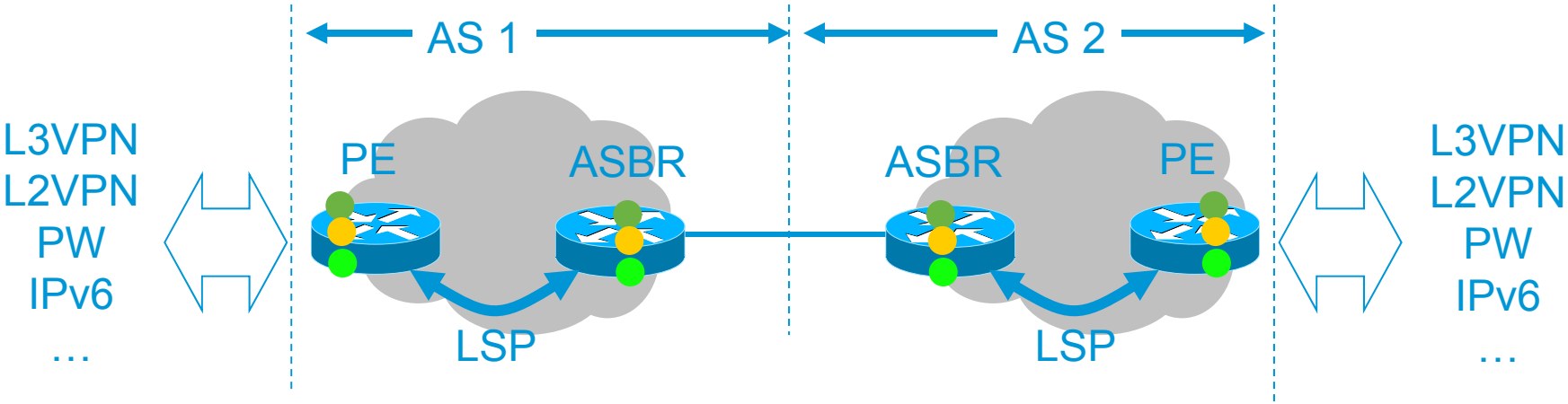
Architektura RFC 2547: bezpieczna*



- Tylko interfejsy IP w stronę klientów, pakiety z etykietami MPLS zostaną odrzucone
- Każdy z pakietów traktowany w kontekście, w jakim został otrzymany (interfejs, VRF)
- Kontrola nad kontekstem: router PE kontrolowany przez operatora

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

Połączenie Inter-AS MPLS VPN



- Duża ilość zagadnień:
  - Styk pomiędzy ASami – VRFy (IP) (A) czy z sygnalizacją via BGP (B i C)?
  - Co jest uruchomione na ASBRach (po co IGP? LDP? – niepotrzebne)

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

Ataki DDoS w warstwie usługowej

- Ataki bezpośrednio na usługi świadczone w infrastrukturze usługowej lub zarządzanej
  - Usługi zarządzane – bezpieczeństwo, backup, (wideo)telefonia i różne inne
  - Dedykowane działy (i mechanizmy), często poza strukturami operatora czy nawet klienta
- Ataki na dostępność – DoS/DDoS
  - „proste” – ruch IP, w tym z użyciem spoofowanych adresów źródłowych
  - „bardziej zaawansowane” – wykorzystujące luki w warstwie aplikacji
  - dwie drogi rozwiązania problemu:
    - maksymalnie ograniczyć możliwości kreowania nadużyć (np. BCP38, odpowiednia konfiguracja usług SMTP i DNS)
    - zapewnienie mechanizmów skalowalnej osiągalności najczęściej atakowanych lub wykorzystywanych do ataków usług

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

Ataki DDoS w warstwie usługowej

- DNS Reflection
  - Wykorzystuje możliwość spoofowania ruchu źródłowego (BCP38!)
    - uRPF
  - Wykorzystuje otwarte resolvery DNS
    - http://openresolverproject.org/

```
dig ANY isc.org @x.x.x.x +edns=0
```

```
; <<>> DiG 9.7.3 <<>> ANY isc.org @x.x.x.x
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5147
;; flags: qr rd ra; QUERY: 1, ANSWER: 27, AUTHORITY: 4, ADDITIONAL: 5
;; QUESTION SECTION:

;isc.org. IN ANY

;; ANSWER SECTION: isc.org. 4084 IN SOA ns-int.isc.org. hostmaster.isc.org.

[....]

;; MSG SIZE  rcvd: 3223
```

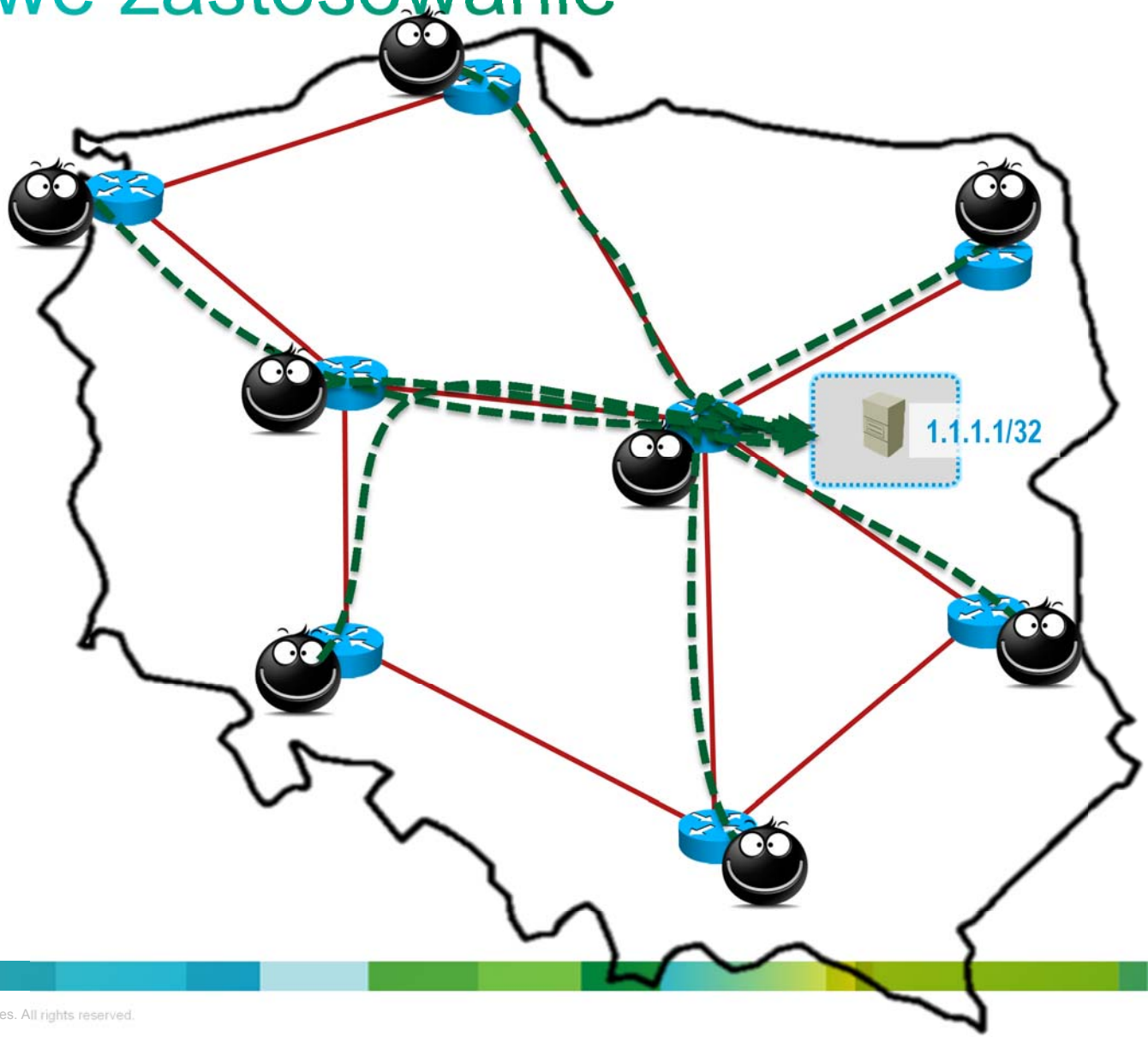
© 2010 Cisco and/or its affiliates. All rights reserved.

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,
- Może być wykorzystywany zamiast lub równocześnie z:
    - równoważeniem obciążenia w L3/L4
    - dodawaniem usług IP w sposób tradycyjny
- W przeciwieństwie do powszechnego przekonania, IP Anycast może być również używany do skalowania usług TCP*

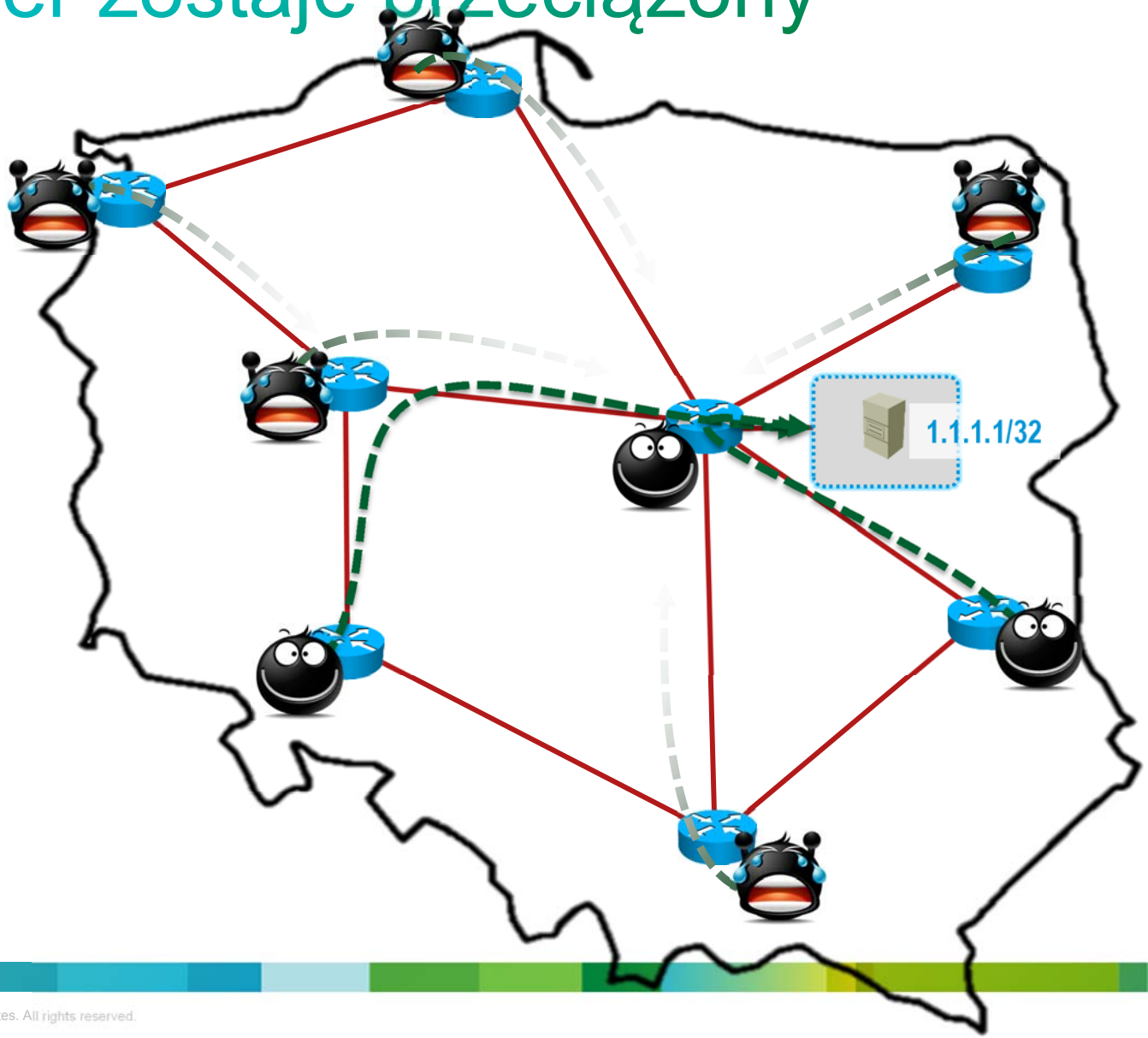
© 2010 Cisco and/or its affiliates. All rights reserved.

Typowe zastosowanie



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

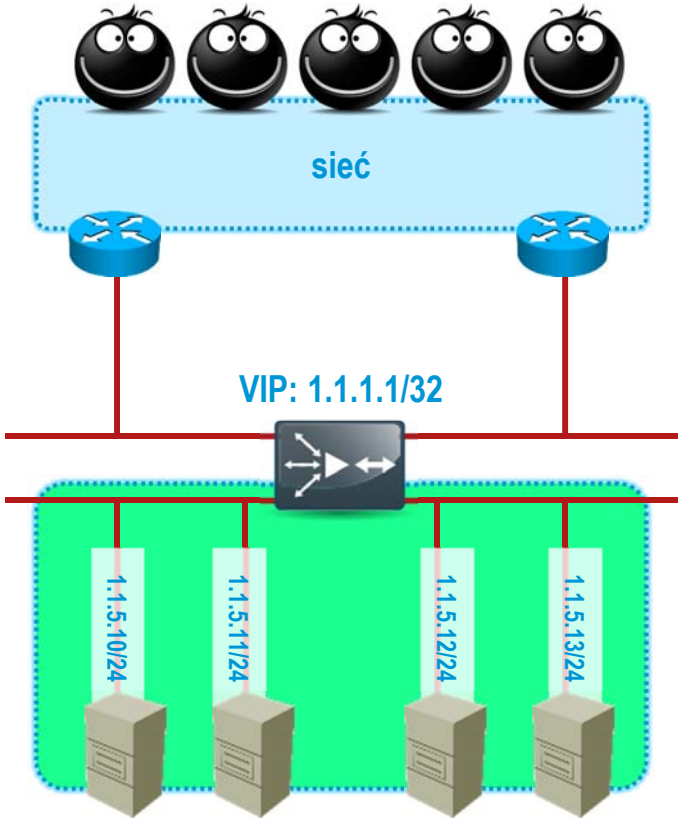
Serwer zostaje przeciążony



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

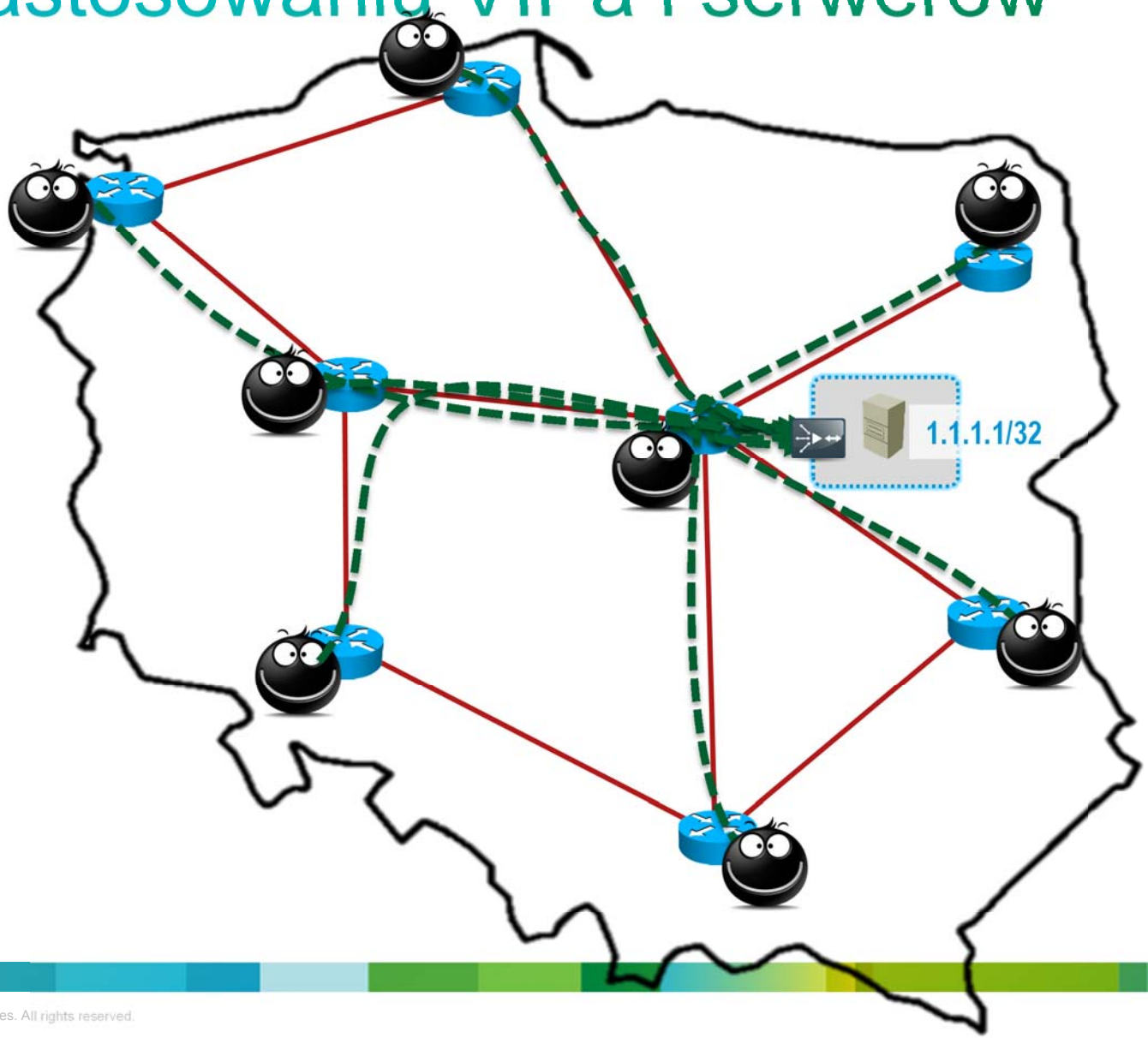
Rozwiązanie pierwsze: rośniemy wszerz

- "Zainstalujmy loadbalancer i dodajmy serwerów"



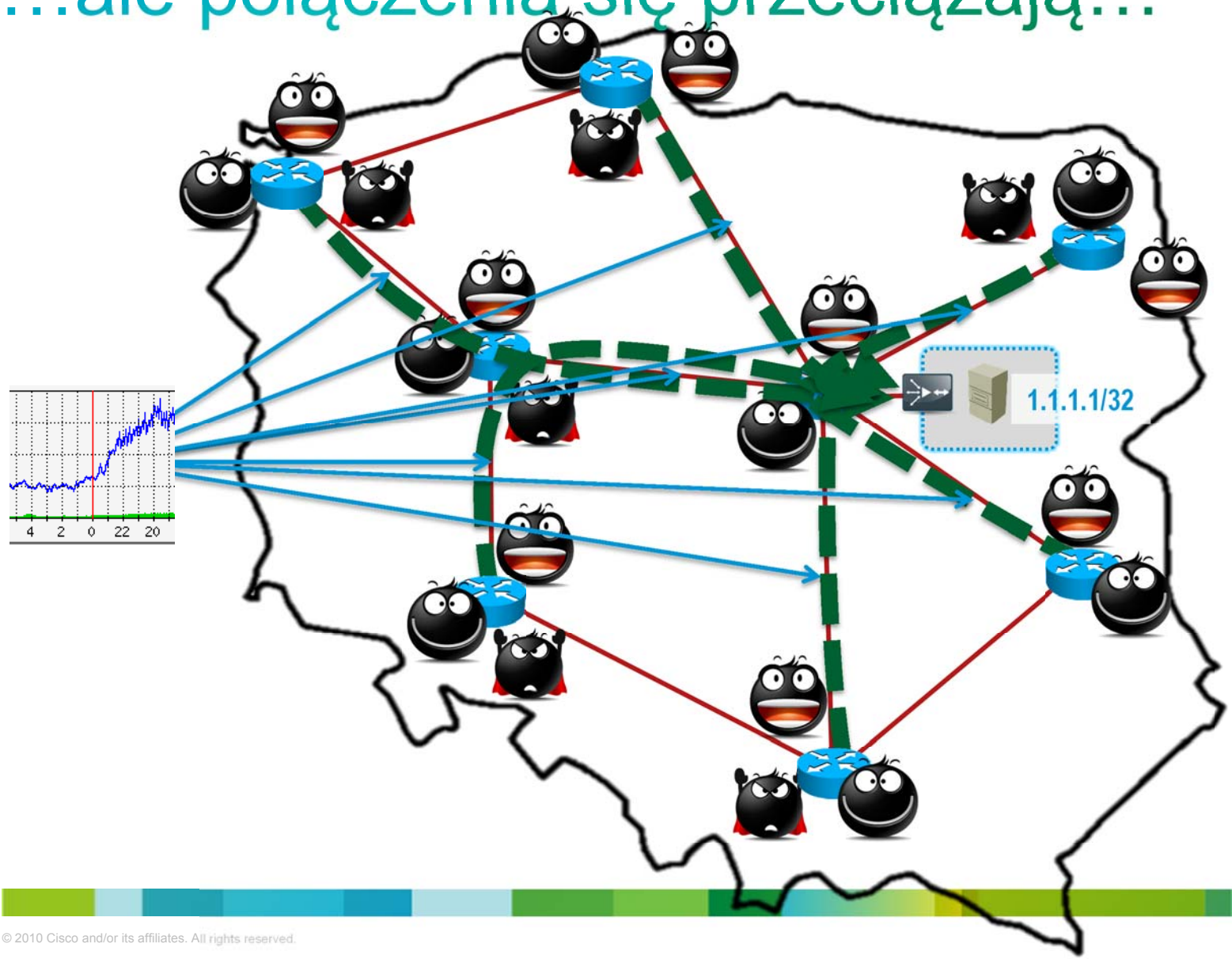
© 2010 Cisco and/or its affiliates. All rights reserved.

Po zastosowaniu VIPa i serwerów



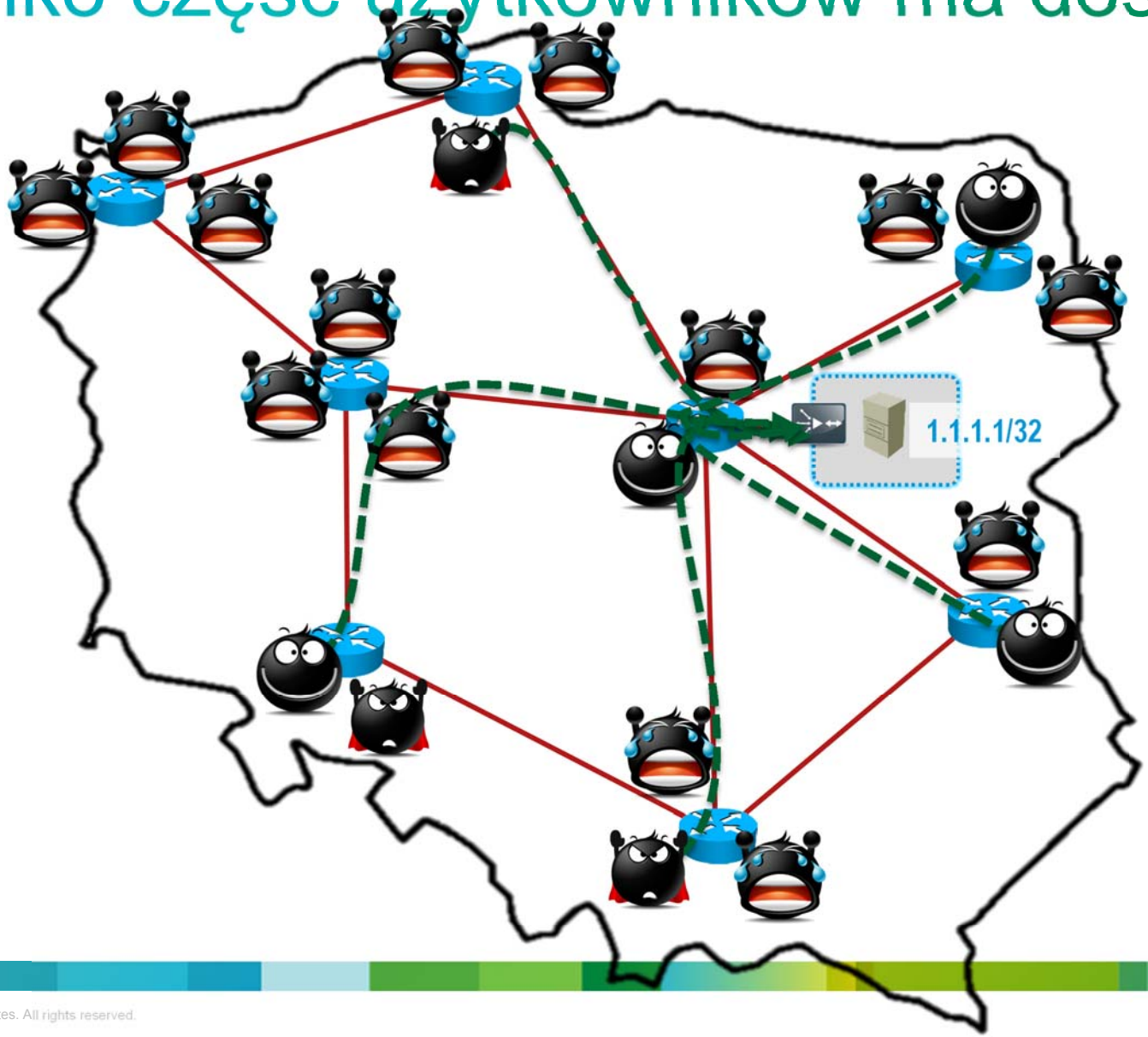
© 2010 Cisco and/or its affiliates. All rights reserved.

…ale połączenia się przeciążają…



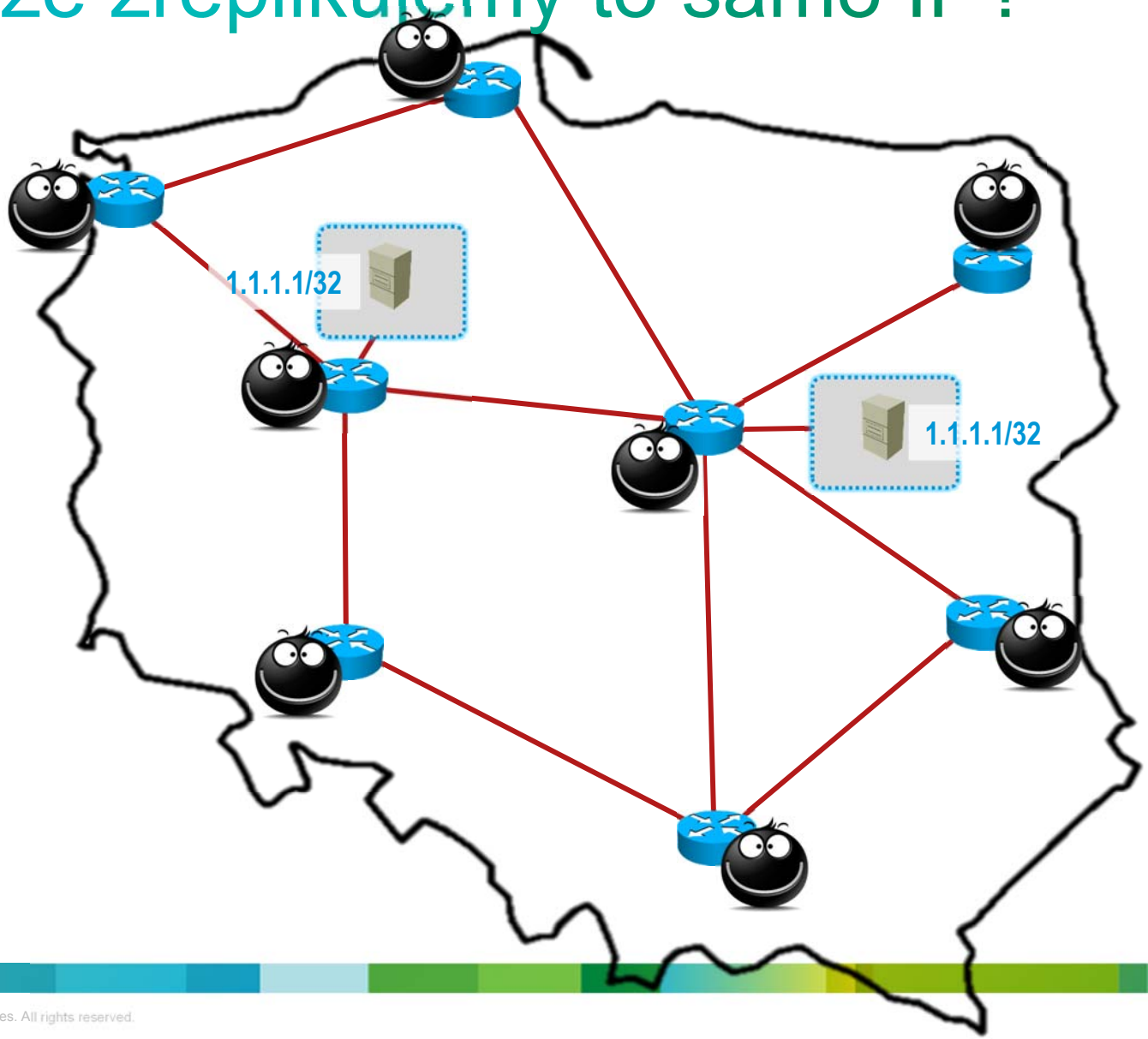
© 2010 Cisco and/or its affiliates. All rights reserved.

…i tylko część użytkowników ma dostęp



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

A może zreplikujemy to samo IP?



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

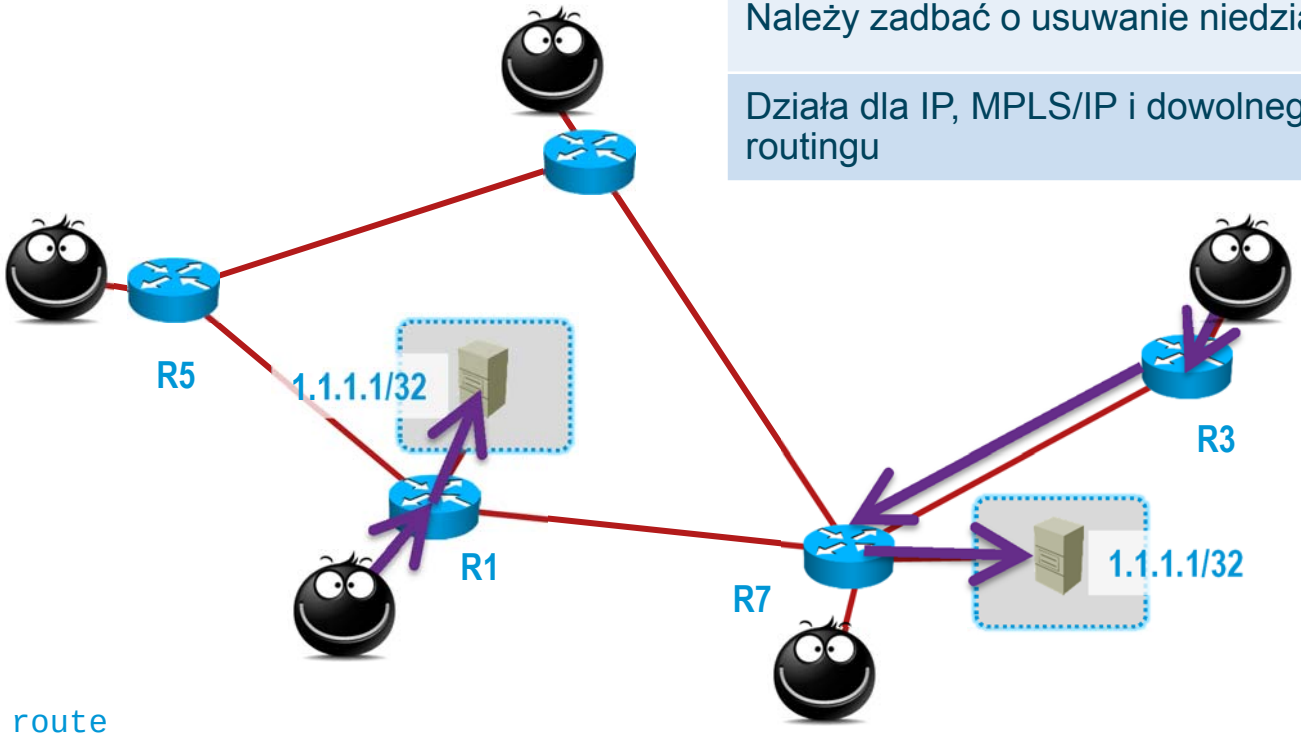
Zreplikowana usługa

Mechanizm routingu wybierze drogę o najmniejszym koszcie pomiędzy klientem a serwerem

Każdy z hostów zostanie skierowany do "najbliższej" instancji usługi

Należy zadbać o usuwanie niedziałających instancji

Działa dla IP, MPLS/IP i dowolnego protokołu routingu




```
R1> show ip route
I    1.1.1.1/32 [115/10] via 192.168.11.6
```

```
R3> show ip route
I    1.1.1.1/32 [115/20] via 192.168.73.7
```

```
R7> show ip route
I    1.1.1.1/32 [115/10] via 192.168.77.6
```

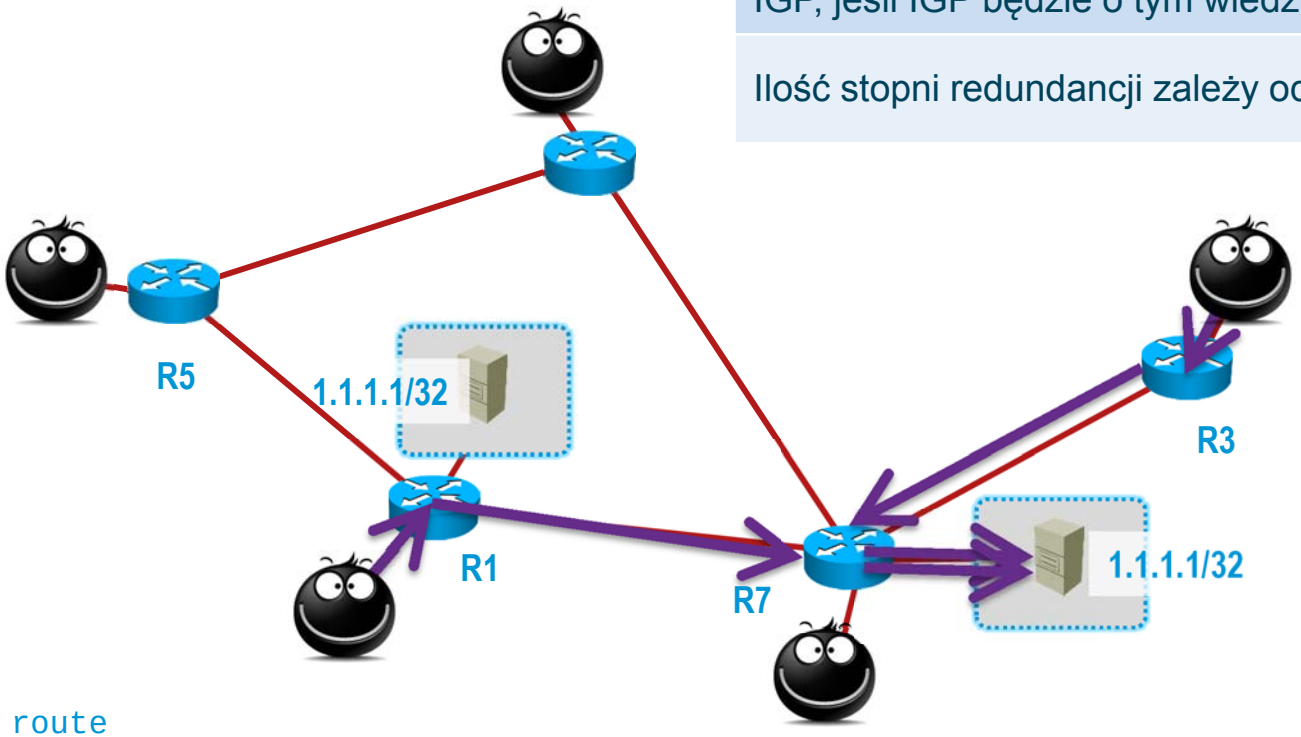
© 2010 Cisco and/or its affiliates. All rights reserved.

Zreplikowana usługa

Replikacja zapewni wysoką dostępność

"Śmierć" jednej instancji spowoduje zniknięcie jej z IGP, jeśli IGP będzie o tym wiedział

Ilość stopni redundancji zależy od ilości instancji




```
R1> show ip route
I    1.1.1.1/32 [115/20] via 192.168.17.7

R7> show ip route
I    1.1.1.1/32 [115/10] via 192.168.77.6
```

```
R3> show ip route
I    1.1.1.1/32 [115/20] via 192.168.73.7

R7> show ip route
I    1.1.1.1/32 [115/10] via 192.168.77.6
```

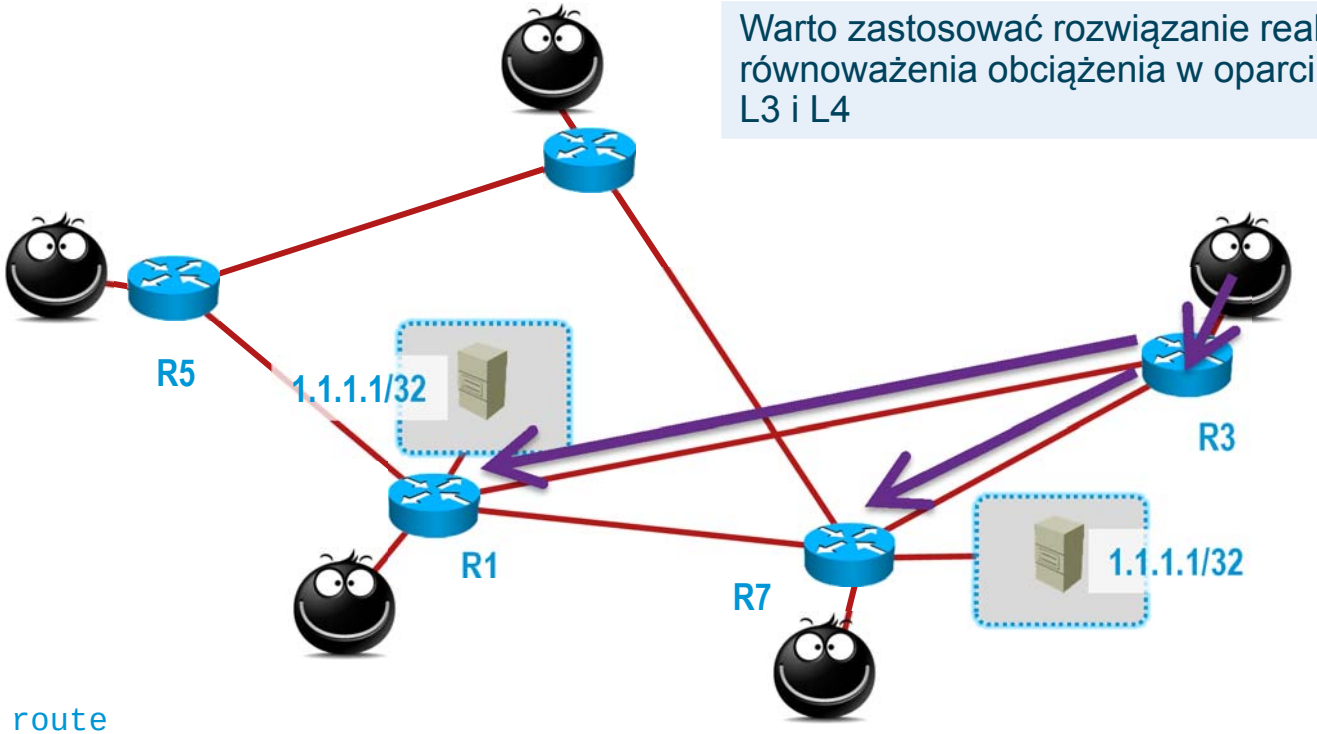
© 2010 Cisco and/or its affiliates. All rights reserved.

Zreplikowana usługa

Automatyczne rozkładanie obciążenia w L3/L4

Uwaga na usługi TCP – oraz ogólnie, na usługi utrzymujące dłuższe połączenia

Warto zastosować rozwiązanie realizujące hash dla równoważenia obciążenia w oparciu o jednocześnie L3 i L4

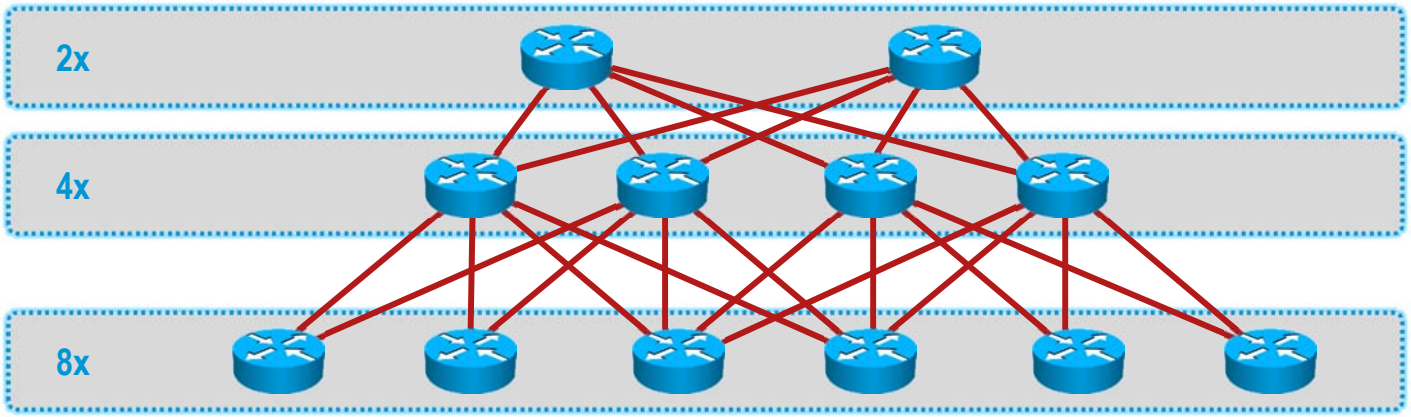



```
R3> show ip route
I    1.1.1.1/32 [115/20] via 192.168.13.1
                         via 192.168.37.7
```

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

W przypadku problemów ze sprzętem

- Ograniczenia ECMP
- Przy ograniczeniach ilości ścieżek równoległych do małych wartości – np. 2 lub 4, można zastosować rozwiązanie wielowarstwowe



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

Q&A

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

Dziękuje bardzo!

CISCO