Bezpieczeństwo sieci

(a raczej zaledwie parę przykładów)

Łukasz Bromirski
lukasz@bromirski.net

SecureCON 2007, Wrocław

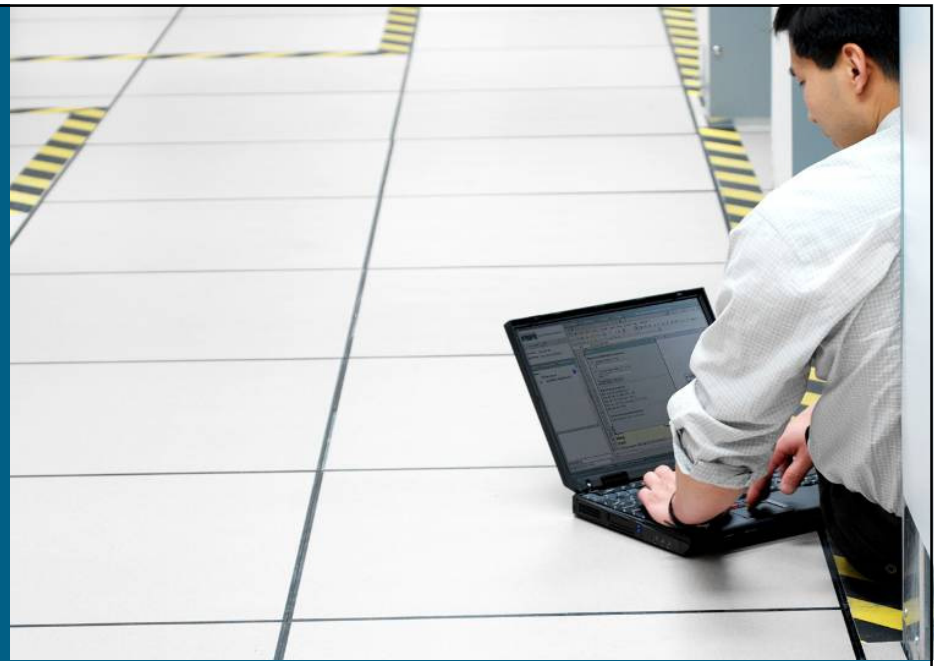
Disclaimer ☺

Sesja zawiera ilustracje jedynie wybranych ataków w warstwie drugiej i trzeciej.

Nie stanowi kompendium, a jedynie zestaw powiązanych zagadnień dających się poruszyć w ciągu 120 minut.

Agenda

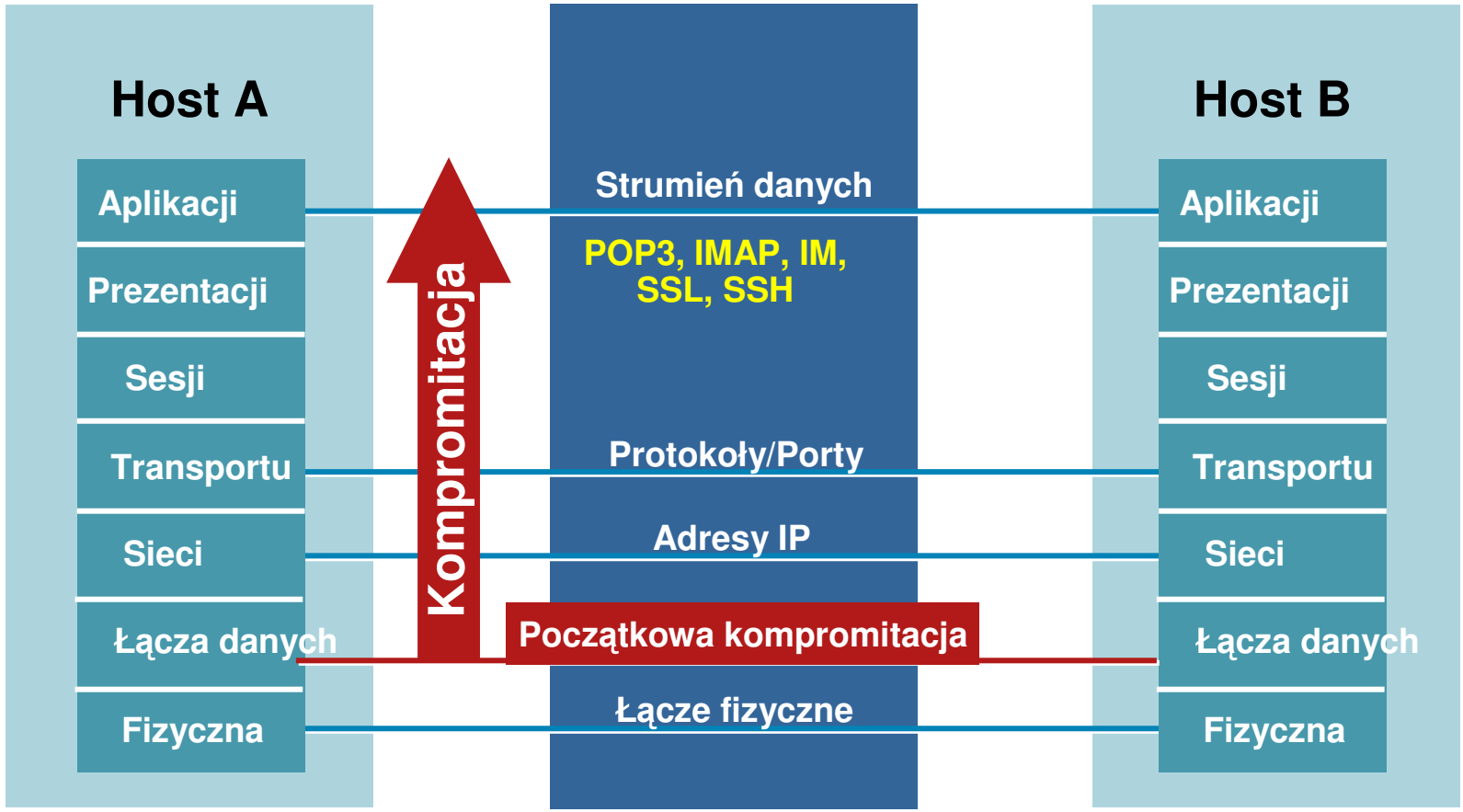
- Ataki w warstwie dostępowej
  - MAC/ARP spoofing, DHCP spoofing
  - Spanning Tree
- Ataki w warstwie IP
  - uRPF
  - filtrowanie prefiksów
  - ochrona protokołów routingu (MD5) / GTSM
  - BGP blackholing



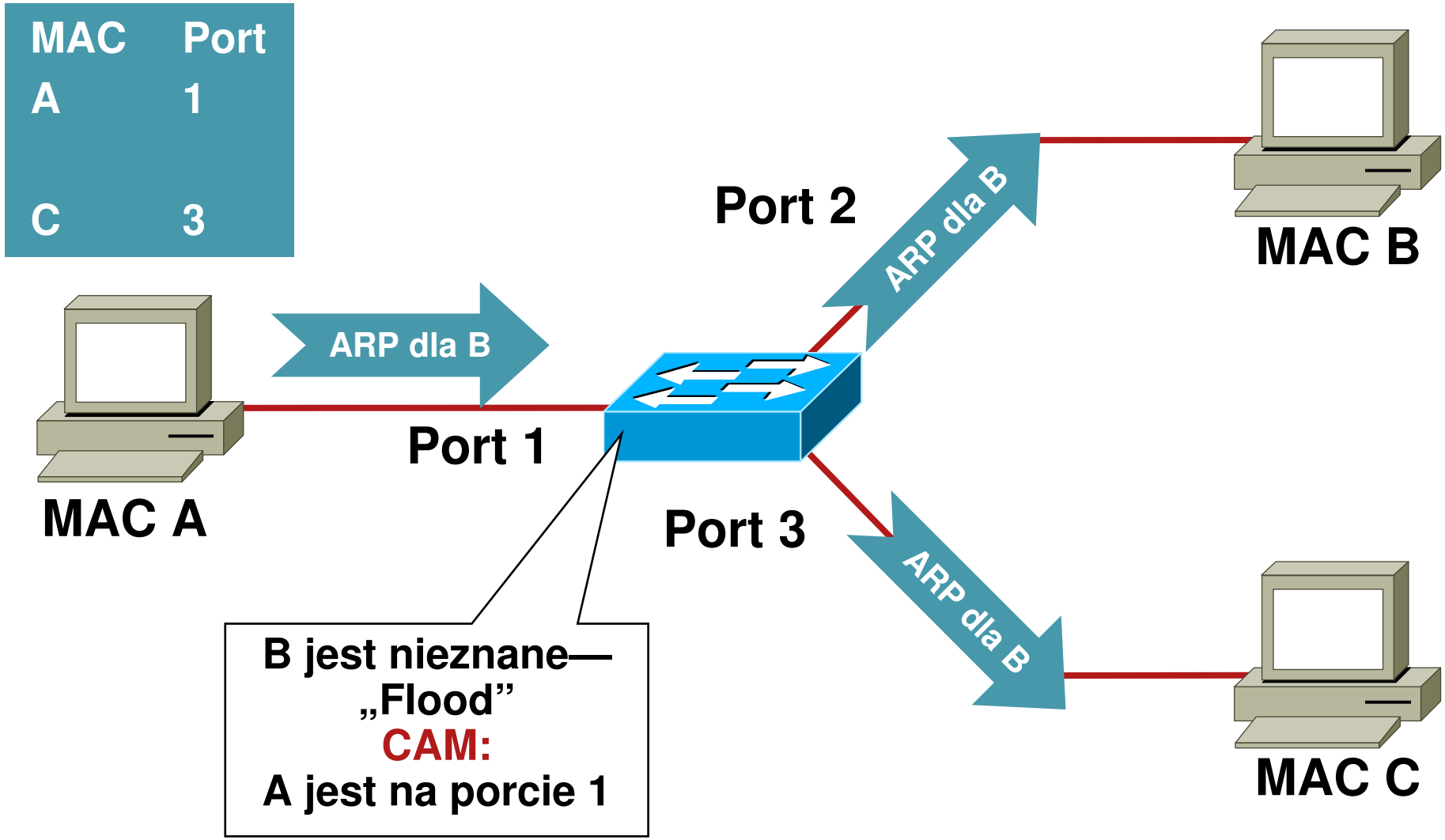
Dlaczego L2 jest ważne?

Warstwy niższe OSI wpływają na wyższe

- Kompromitacja warstwy wyższej otwiera wyższe na atak – nie są tego świadome
- Bezpieczeństwo jest tak dobre, jak najsłabsze ogniwo architektury
- Warstwa 2 może być bardzo słabym ogniwem

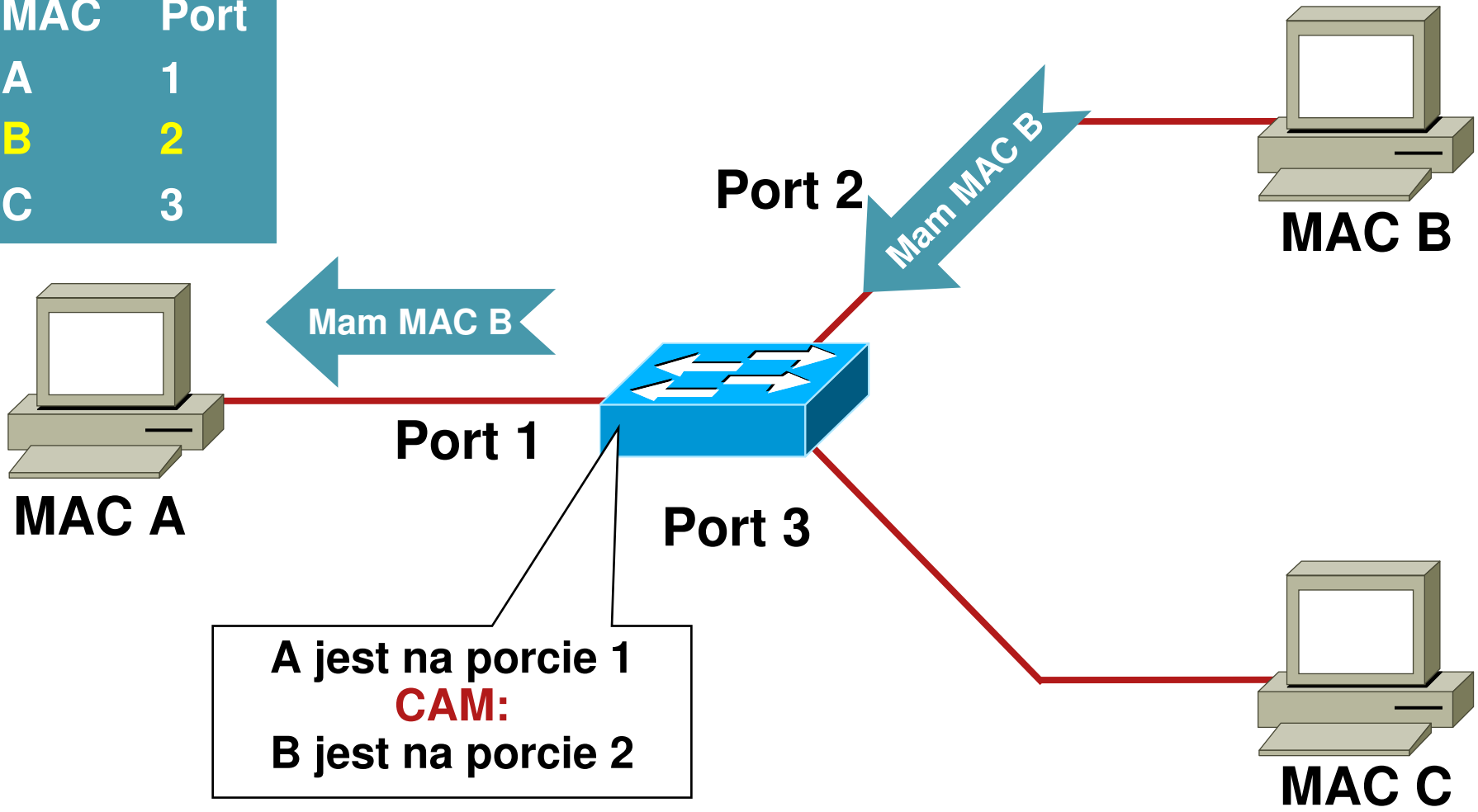


Normalne zachowanie tablicy CAM (1/3)



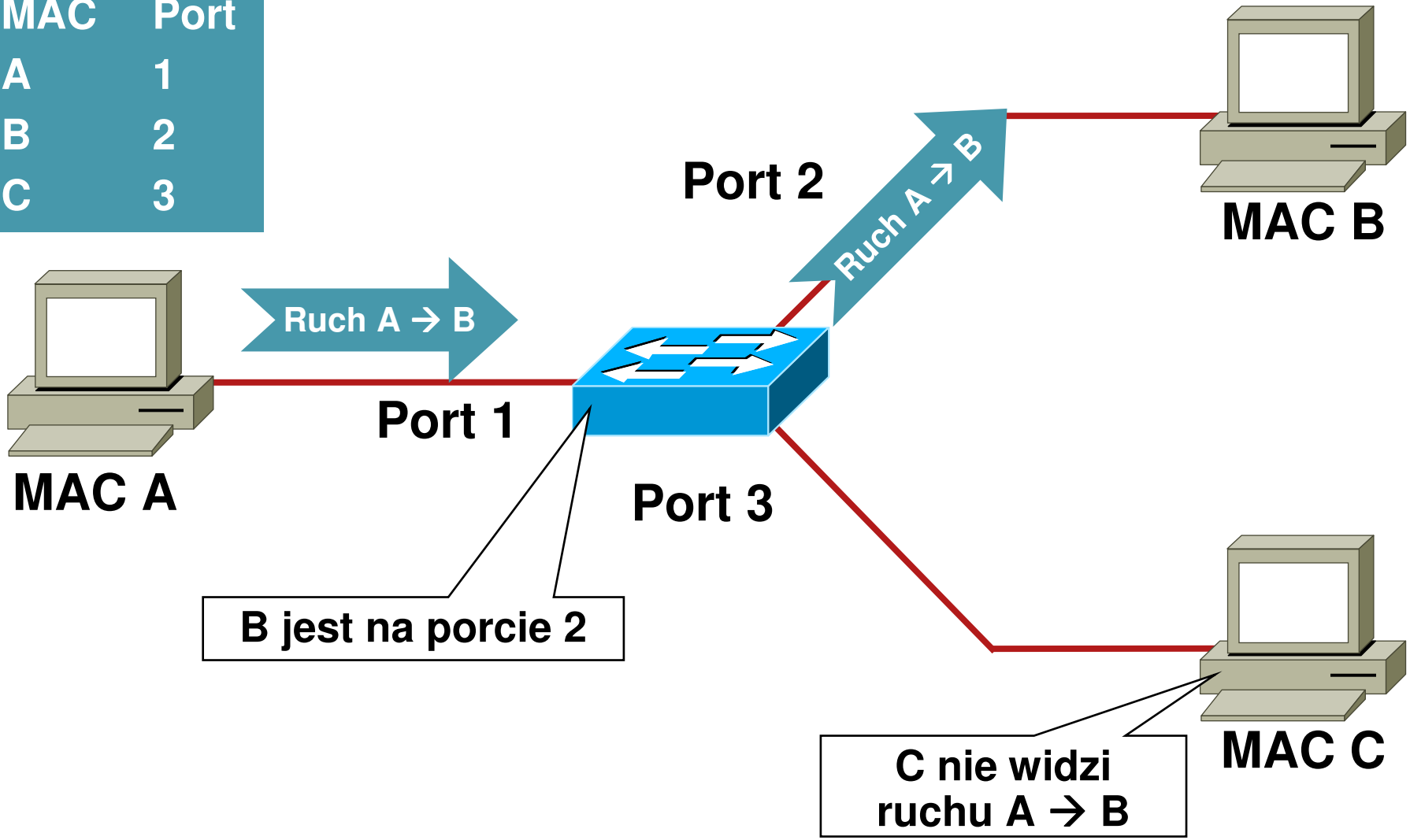
Normalne zachowanie tablicy CAM (2/3)

MAC	Port
A	1
B	2
C	3



Normalne zachowanie tablicy CAM (3/3)

MAC	Port
A	1
B	2
C	3



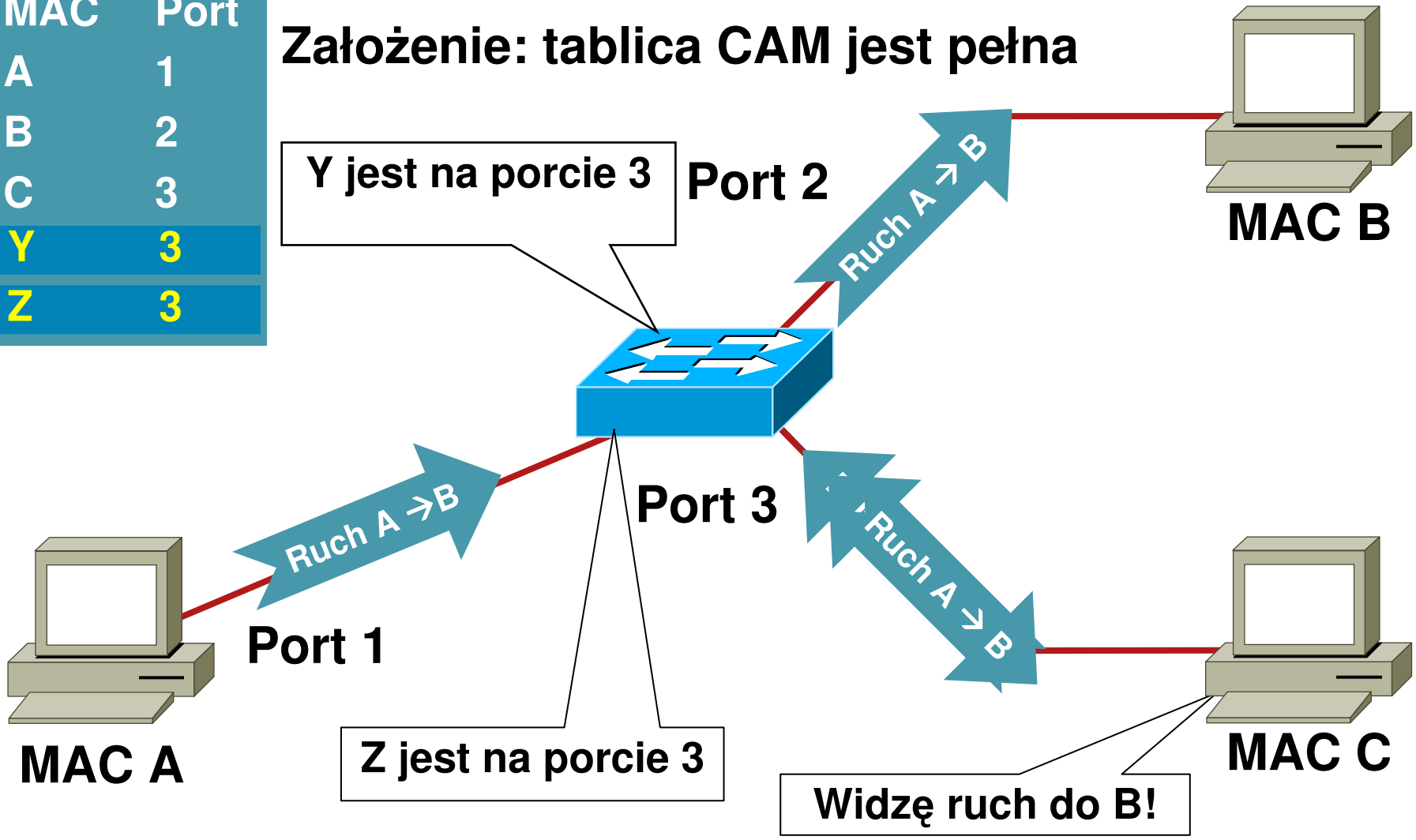
Ataki na tablicę CAM (1/2)

- **Narzędzie Macof,1999**
  - **100 linii w perlu**
  - **Jest częścią pakietu "dsniff"**
- **Atak na tablicę CAM – strukturę o <u>skończonej</u> wielkości**
- **Yersinia - narzędzie do ataków w L2 – STP, CDP, DTP, DHCP, HSRP, 802.1q, 802.1x, ISL, VTP**

Pokaz: Atak CAM Overflow

MAC	Port
A	1
B	2
C	3
Y	3
Z	3

Założenie: tablica CAM jest pełna



Atak MAC Flooding – narzędzie macof

```
macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

- **Macof generuje i wysyła ramki z losowym MAC i IP**
- **Wersja ‘szybsza’ ☺**

  `macof -i eth1 2> /dev/null`

- **macof (część dsniff)— http://monkey.org/~dugsong/dsniff/**

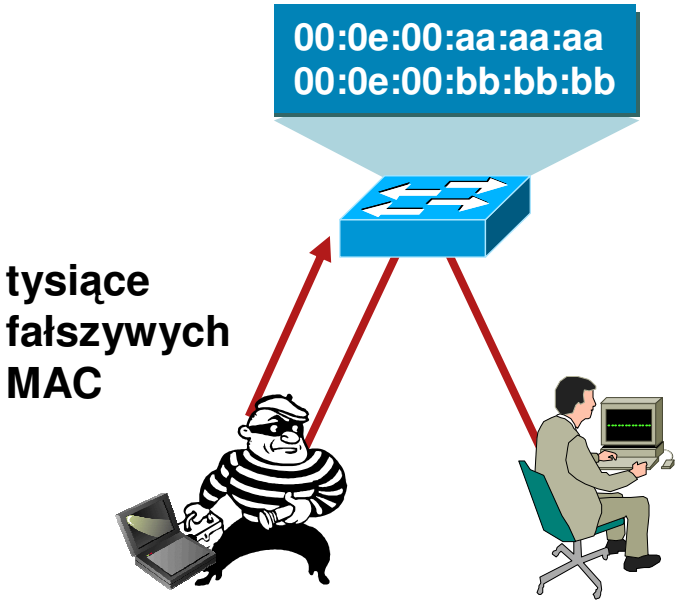
A gdy tablica CAM jest pełna…

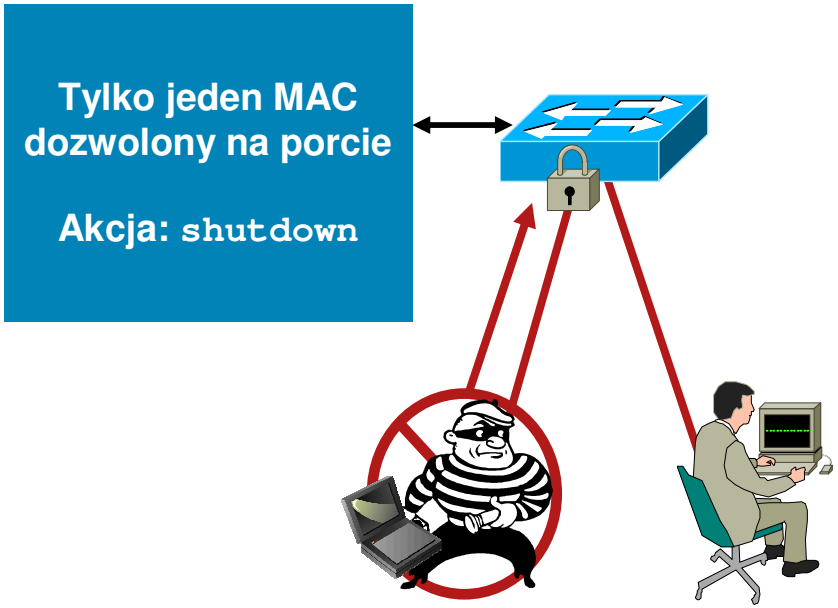
- Kiedy tablica CAM ulegnie przepełnieniu, ramki skierowane do nieznanego adresu MAC są kopiowane na wszystkie porty w danym VLANie
- Dla każdego VLANu przełącznik zaczyna działać jak hub
- Atak przepełni również tablice CAM sąsiednich przełączników

```
10.1.1.22 -> (broadcast) ARP C Who is 10.1.1.1, 10.1.1.1 ?
10.1.1.22 -> (broadcast) ARP C Who is 10.1.1.19, 10.1.1.19 ?
10.1.1.26 -> 10.1.1.25  ICMP Echo request (ID: 256 Sequence number: 7424) ← OOPS
10.1.1.25 -> 10.1.1.26  ICMP Echo reply (ID: 256 Sequence number: 7424) ← OOPS
```

Obrona przed atakami na tablicę CAM

Port Security ogranicza ilość adresów MAC na interfejsie

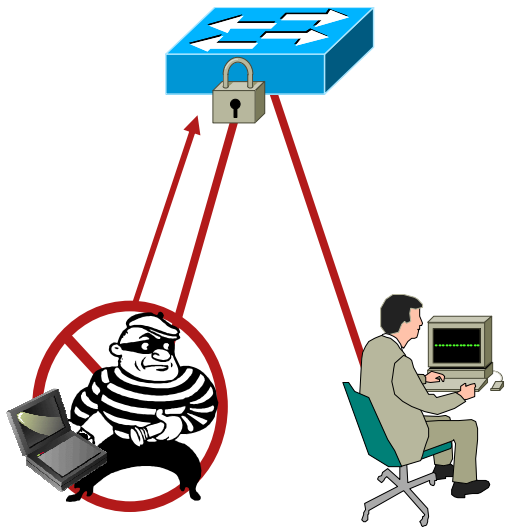




Rozwiązanie:

- **Mechanizm Port security ogranicza atak MAC flood, wsyła wiadomość SNMP i wyłącza port**

Port Security: przykładowa konfiguracja



IPT będzie działała podczas ataku

```
CatOS
set port security 5/1 enable
set port security 5/1 port max 3
set port security 5/1 violation restrict
set port security 5/1 age 2
set port security 5/1 timer-type inactivity

IOS
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

- `maximum` chroni przełącznik przed atakiem
- W zależności od polityki bezpieczeństwa – wyłączenie portu może być preferowane, nawet dla VoIP

Jeżeli pojawi się błąd Error-Disable, logowana jest wiadomość :

4w6d: %PM-4-ERR_DISABLE: Psecure-Violation Error Detected on Gi3/2, Putting Gi3/2 in Err-Disable State

Budujemy warstwy obrony

- **Port Security zapobiega atakom na tablicę CAM i serwer DHCP (starvation attack)**

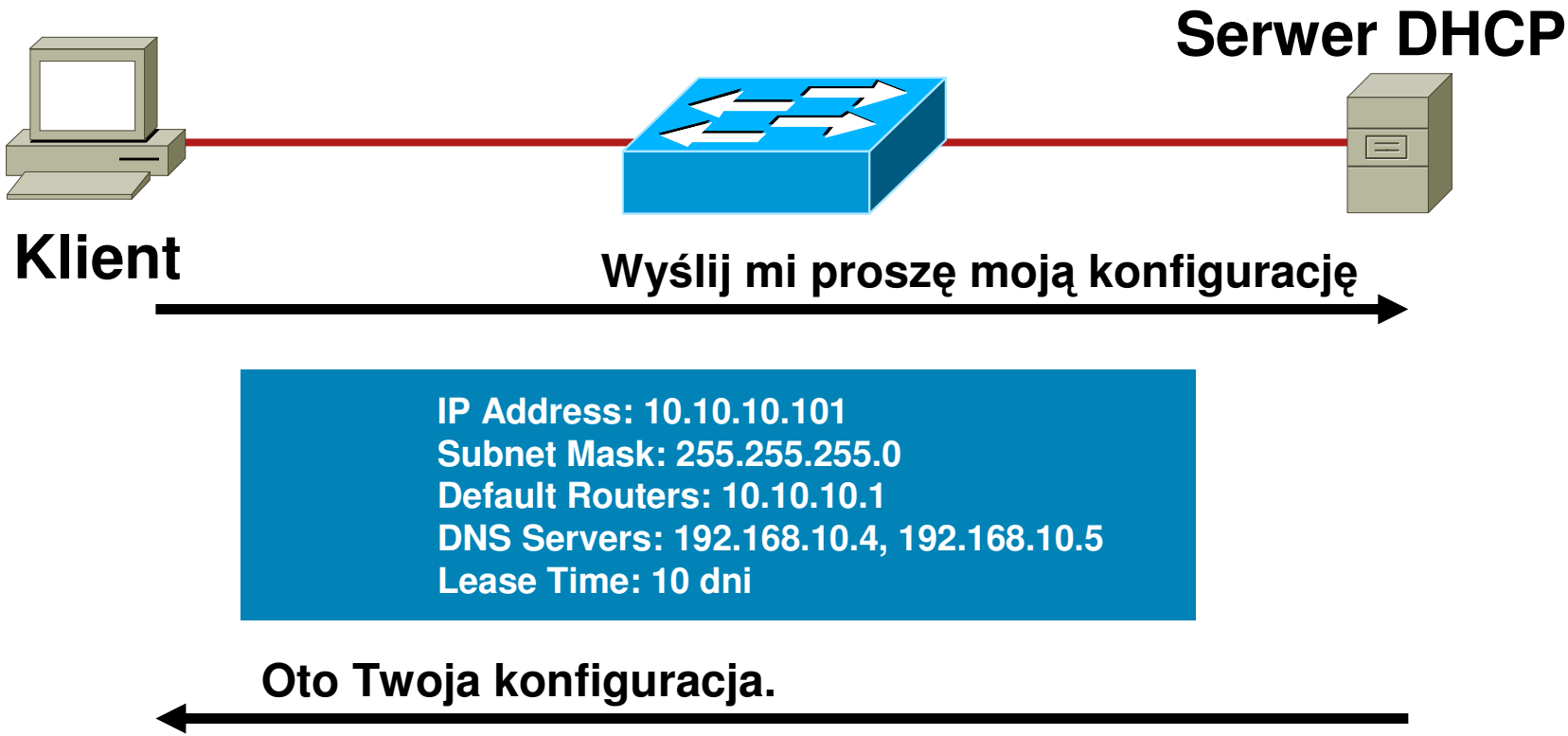
Demonstracja #1

- macof i narzędzia pochodne a mechanizm port-security

Agenda

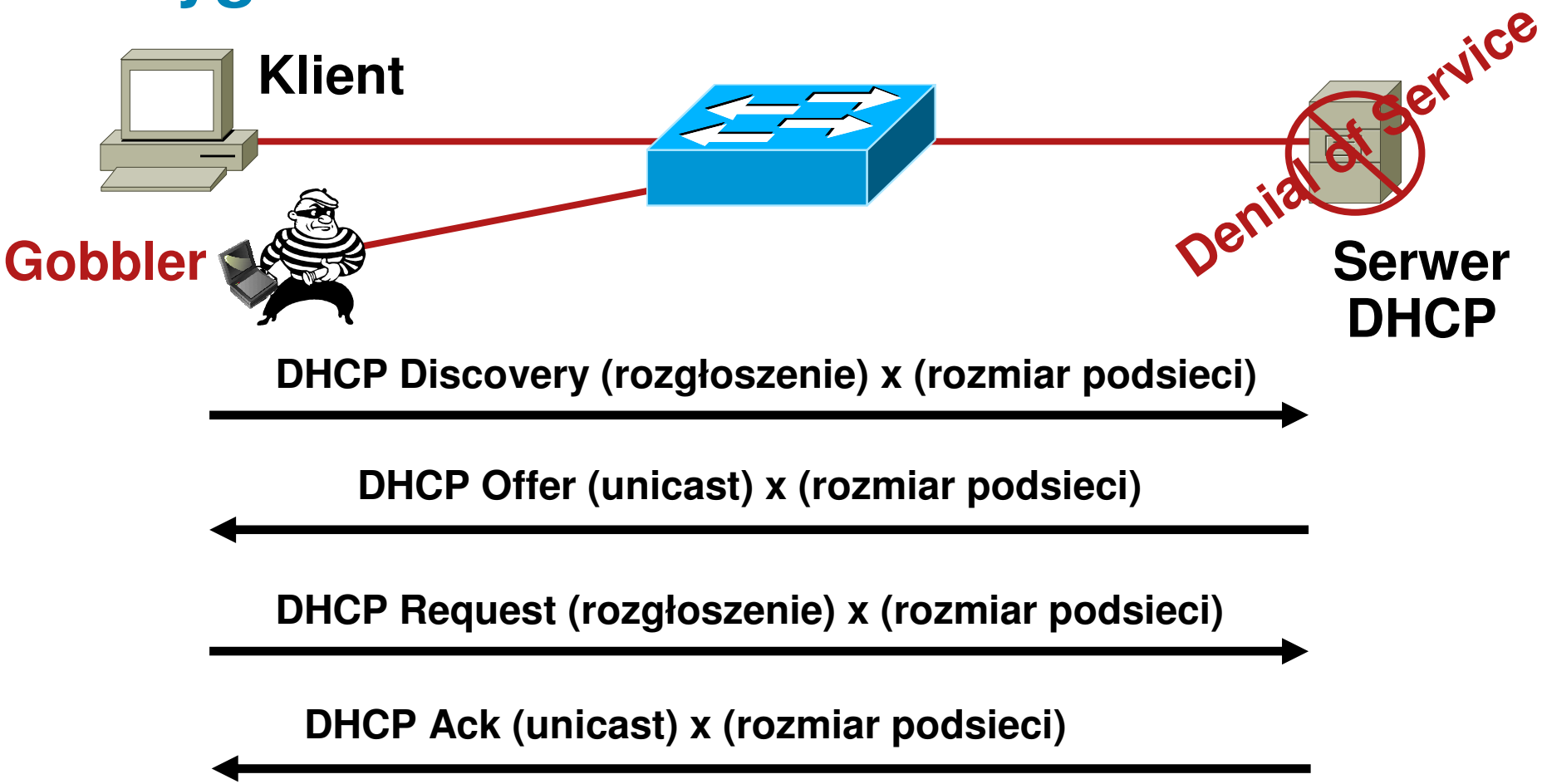
- **Ataki L2 i metody przeciwdziałania**
  - **Ataki MAC**
  - **Ataki na usługę DHCP**
  - **Ataki na ARP**
  - **Ataki typu Spoofing**
  - **Inne ataki (VLAN Hopping, STP, CDP, VTP, zarządzanie)**

Działanie DHCP z lotu ptaka



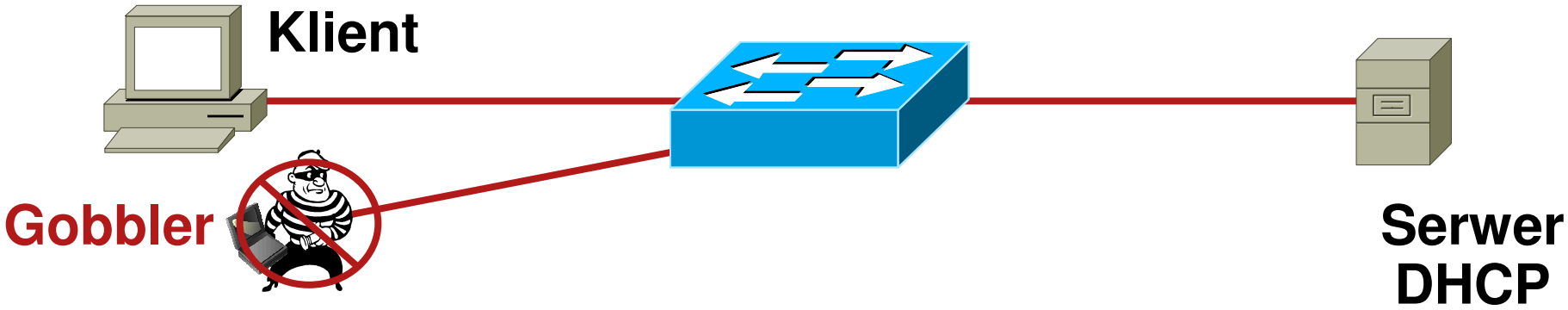
- Serwer przyznaje dynamicznie adres IP na żądanie
- Administrator tworzy pule dostępnych adresów
- Adres jest przyznawany na czas dzierżawy
- DHCP dostarcza innych parametrów i informacji (opcje)

Typy ataków DHCP (1)
Wygłodzenie serwera DHCP



- Gobbler/DHCPx determinuje pulę dostępnych adresów i stara się wydzierżawić wszystkie możliwe adresy z tej puli
- Jest to atak typu Denial od Service na pulę dostępnych adresów

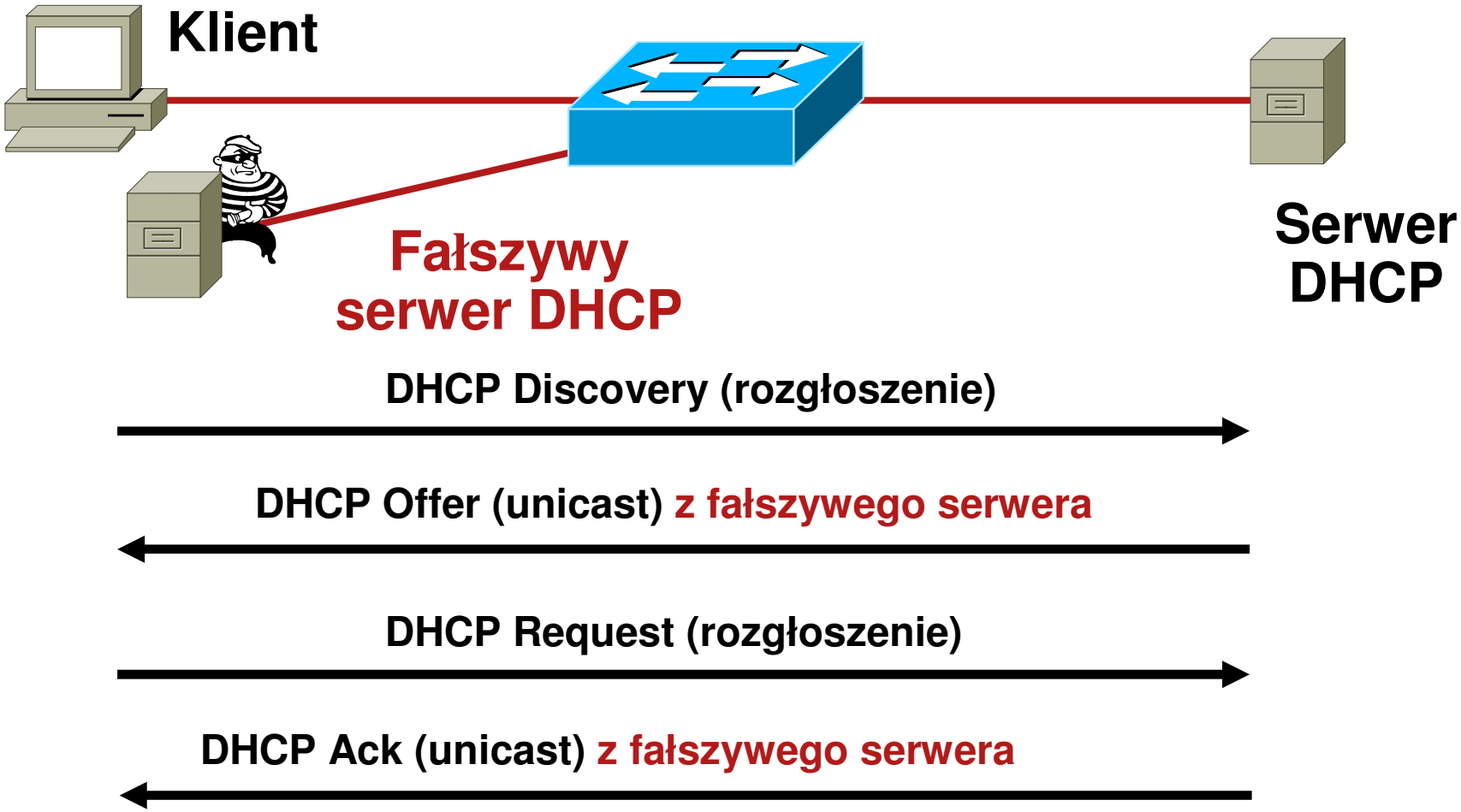
Wygłodzenie serwera DHCP – Obrona: port-security



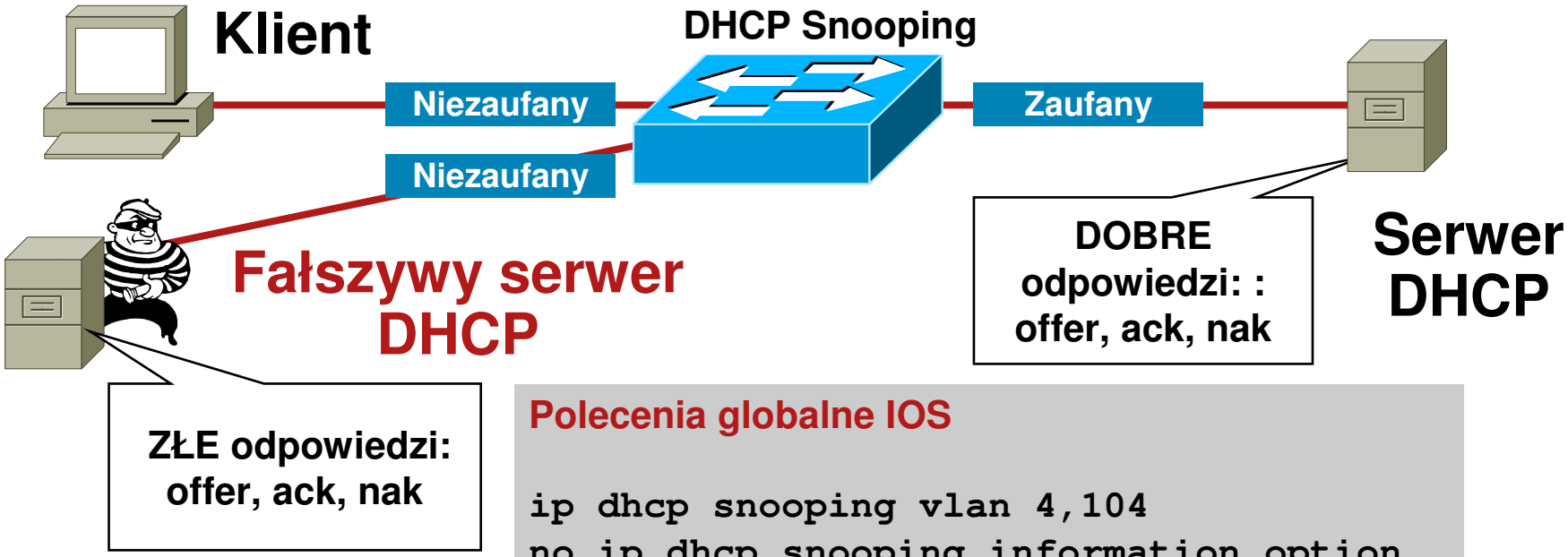
- Gobbler używa nowego adresu MAC dla każdego żądania DHCP
- Ogranicz ilość adresów MAC na porcie
- Ilość przyznanych adresów IP = ilość adresów MAC na porcie
- Atakujący otrzyma jeden adres IP z serwera DHCP

```
CatOS
set port security 5/1 enable
set port security 5/1 port max 1
set port security 5/1 violation restrict
set port security 5/1 age 2
set port security 5/1 timer-type inactivity
IOS
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

Typy ataków DHCP (2)
Fałszywy serwer DHCP (Rogue DHCP)



Fałszywy serwer DHCP
Obrona: DHCP Snooping (1)



Polecenia globalne IOS

```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
```

DHCP Snooping – port niezaufany

Polecenia na porcie niezaufanym

```
no ip dhcp snooping trust (Default)
ip dhcp snooping limit rate 10 (pps)
```

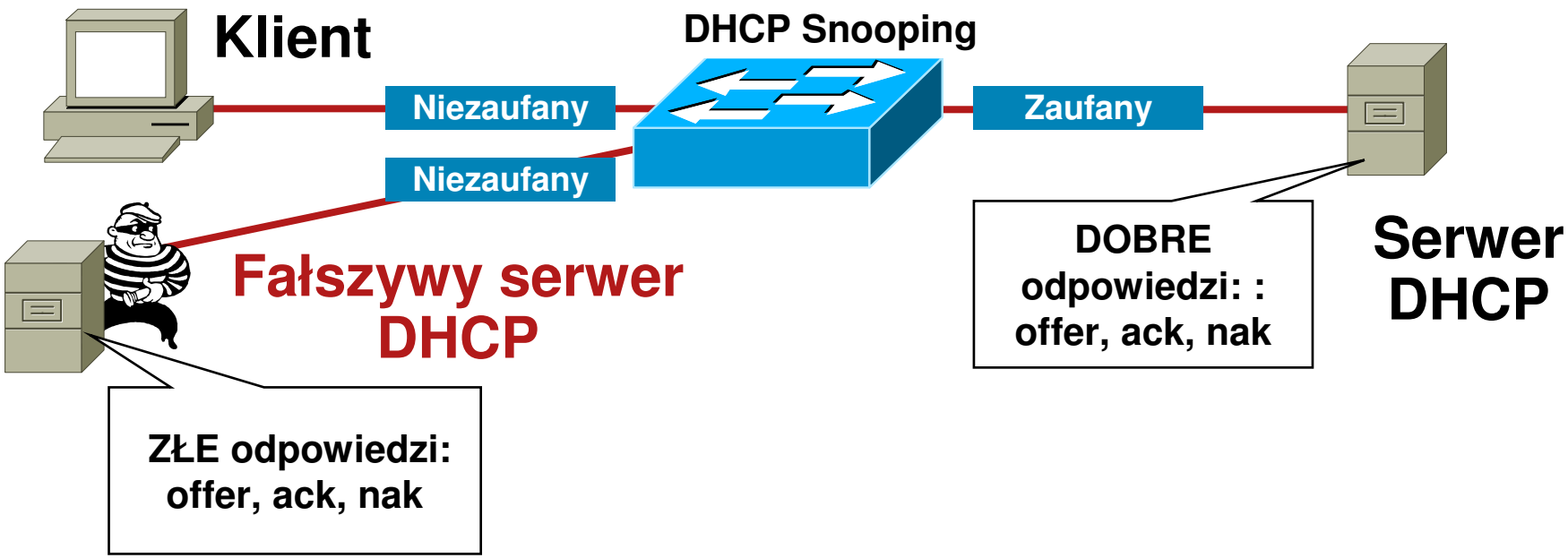
DHCP Snooping – uplink lub serwer

Polecenia na porcie zaufanym

```
ip dhcp snooping trust
```

- **Domyśnie wszystkie porty w VLANie są niezaufane**

Fałszywy serwer DHCP
Obrona: DHCP Snooping (2)



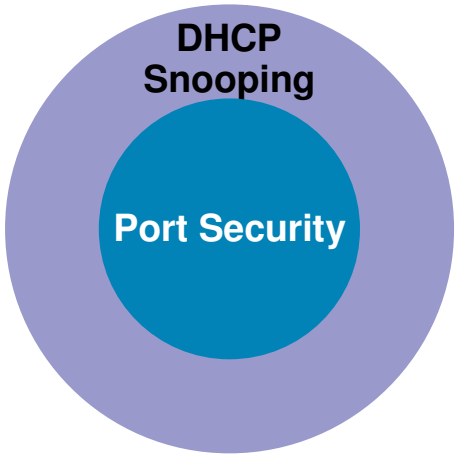
Tablica dowiązań DHCP Snooping:

```
sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10      193185      dhcp-snooping  4     FastEthernet3/18
```

- **Tablica jest budowana przez „snooping” odpowiedzi DHCP w stronę klienta**
- **Wpisy w tablicy pozostają na czas trwania dzierżawy**

Budujemy warstwy obrony

- Port Security zapobiega atakom na tablicę CAM i serwer DHCP (starvation attack)
- **DHCP snooping zapobiega atakom na DHCP**



Demonstracja #2

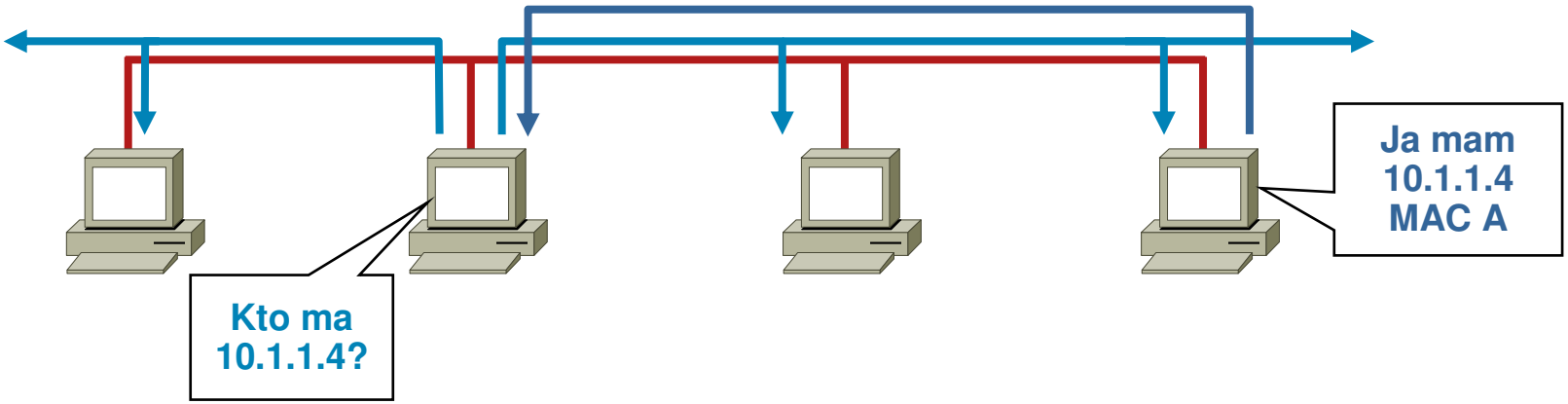
- DHCP DDoS a mechanizm port-security

Agenda

- **Ataki L2 i metody przeciwdziałania**
  - Ataki MAC
  - Ataki na usługę DHCP
  - Ataki na ARP
  - Ataki typu Spoofing
  - Inne ataki (VLAN Hopping, STP, CDP, VTP, zarządzanie)

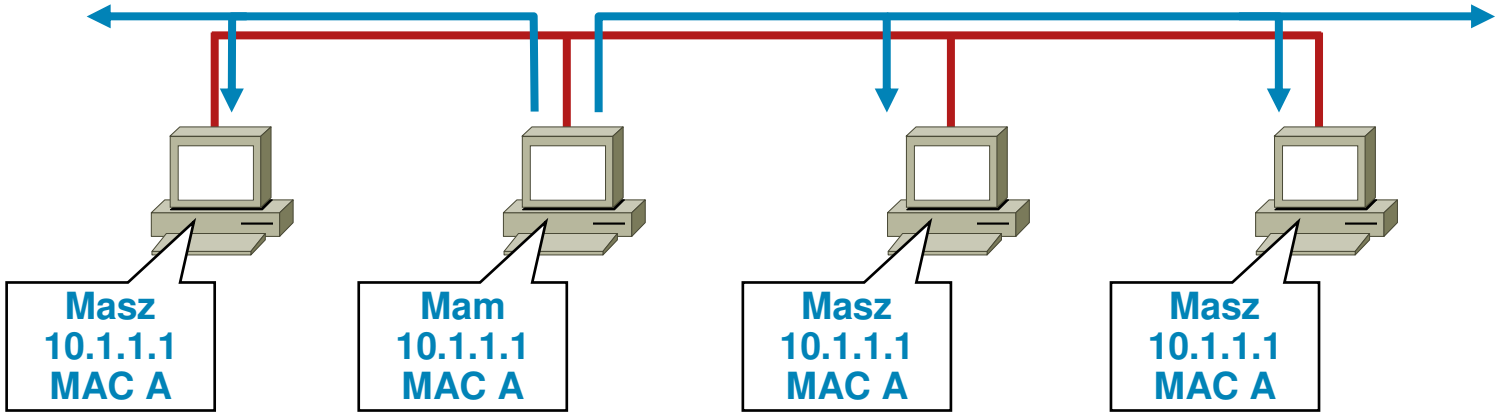
Działanie ARP – z lotu ptaka

- Zanim stacja zacznie nadawać, musi znać adres MAC drugiej strony. Wysyła zapytanie ARP
  - Zapytanie ARP jest rozgłoszeniem, protokół 0x0806
- Wszystkie stacje w podsieci otrzymują zapytanie ATP i je przetwarzają. Na zapytanie odpowiada stacja o adresie IP zawartym w zapytaniu.



Działanie ARP

- Zgodnie z ARP RFC, klient może wysłać odpowiedź ARP bez żądania (ARP „grzecznościowy” – Gratuituous ARP). Inne hosty w podsieci mogą zachować tę informację w swoich tablicach ARP
- W efekcie każdy może podać się za posiadacza dowolnego adresu IP/MAC
- Ataki na ARP umożliwiają przekierowanie ruchu

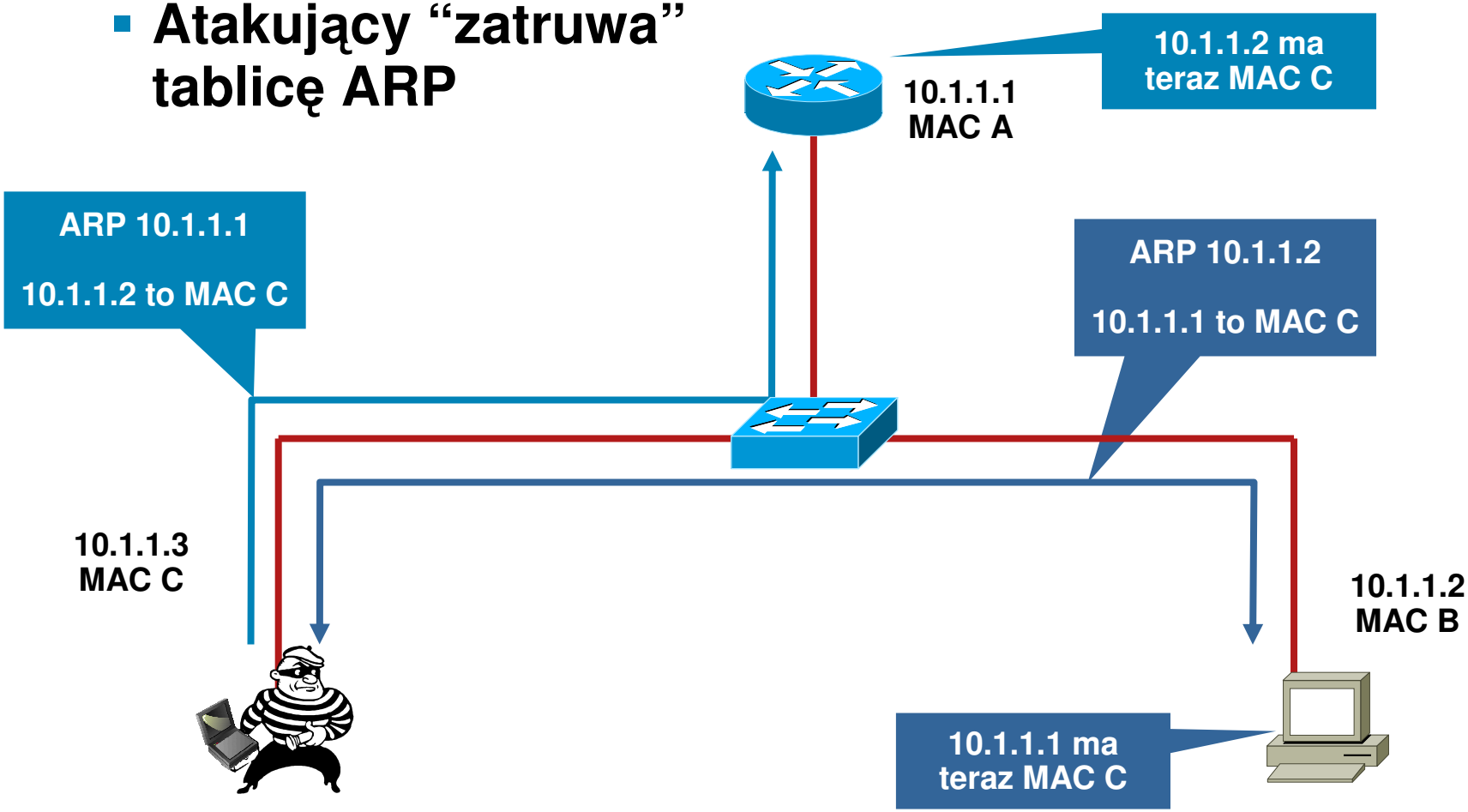


Ataki na ARP: narzędzia (1)

- Istnieje wiele narzędzi do ataków na ARP
  - Dsniff, Cain and Abel, ettercap, Yersinia, itd.
- ettercap—http://ettercap.sourceforge.net/index.php
  - Większość posiada przyjemny interfejs GUI
- Wszystkie przechwytują hasła w ruchu aplikacyjnym
  - FTP, Telnet, SMTP, HTTP, POP, NNTP, IMAP, SNMP, LDAP, RIP, OSPF, PPTP, MS-CHAP, SOCKS, X11, IRC, ICQ, AIM, SMB, Microsoft SQL, itd.

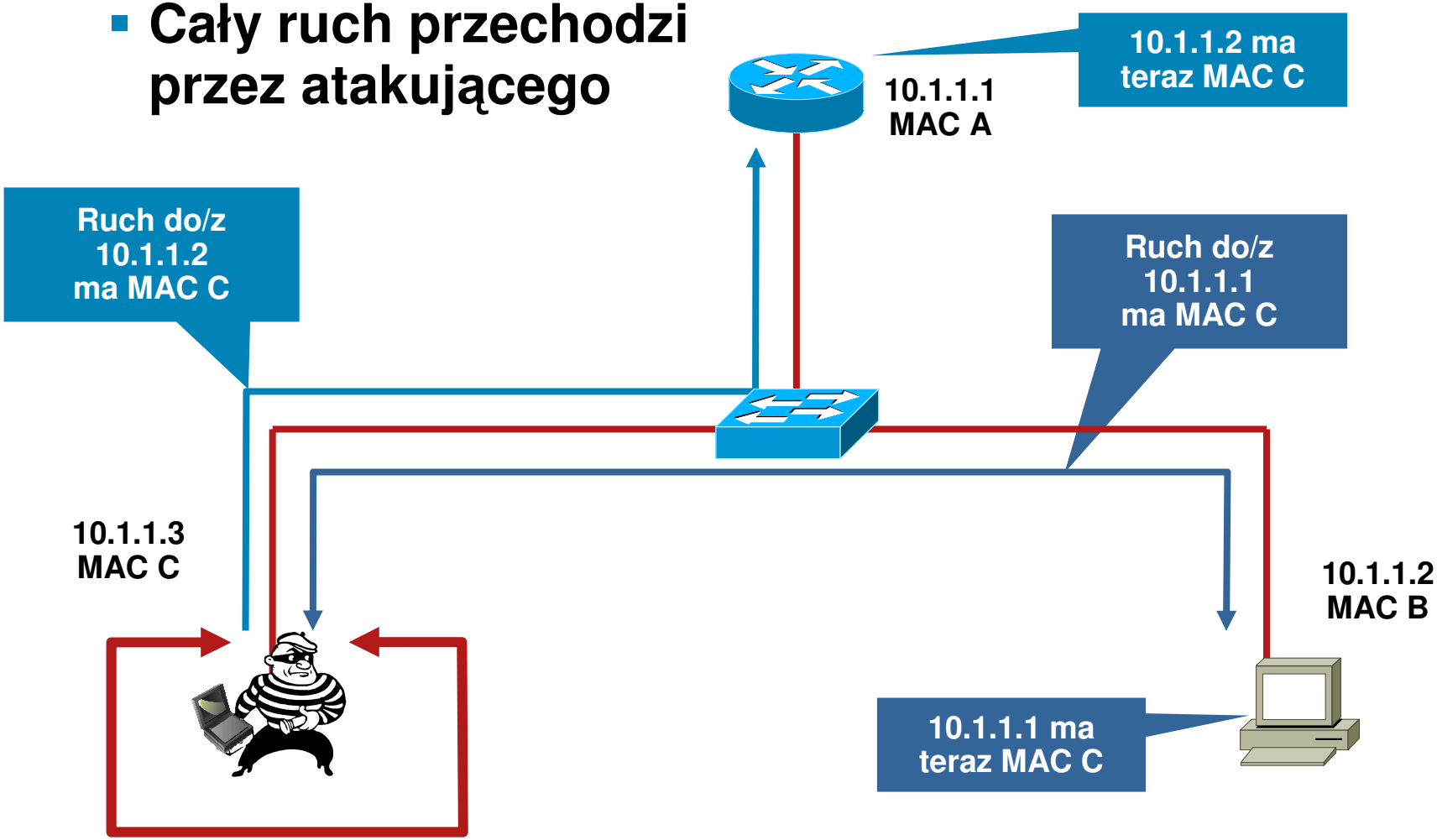
Atak na ARP w działaniu

- Atakujący “zatruwa” tablicę ARP



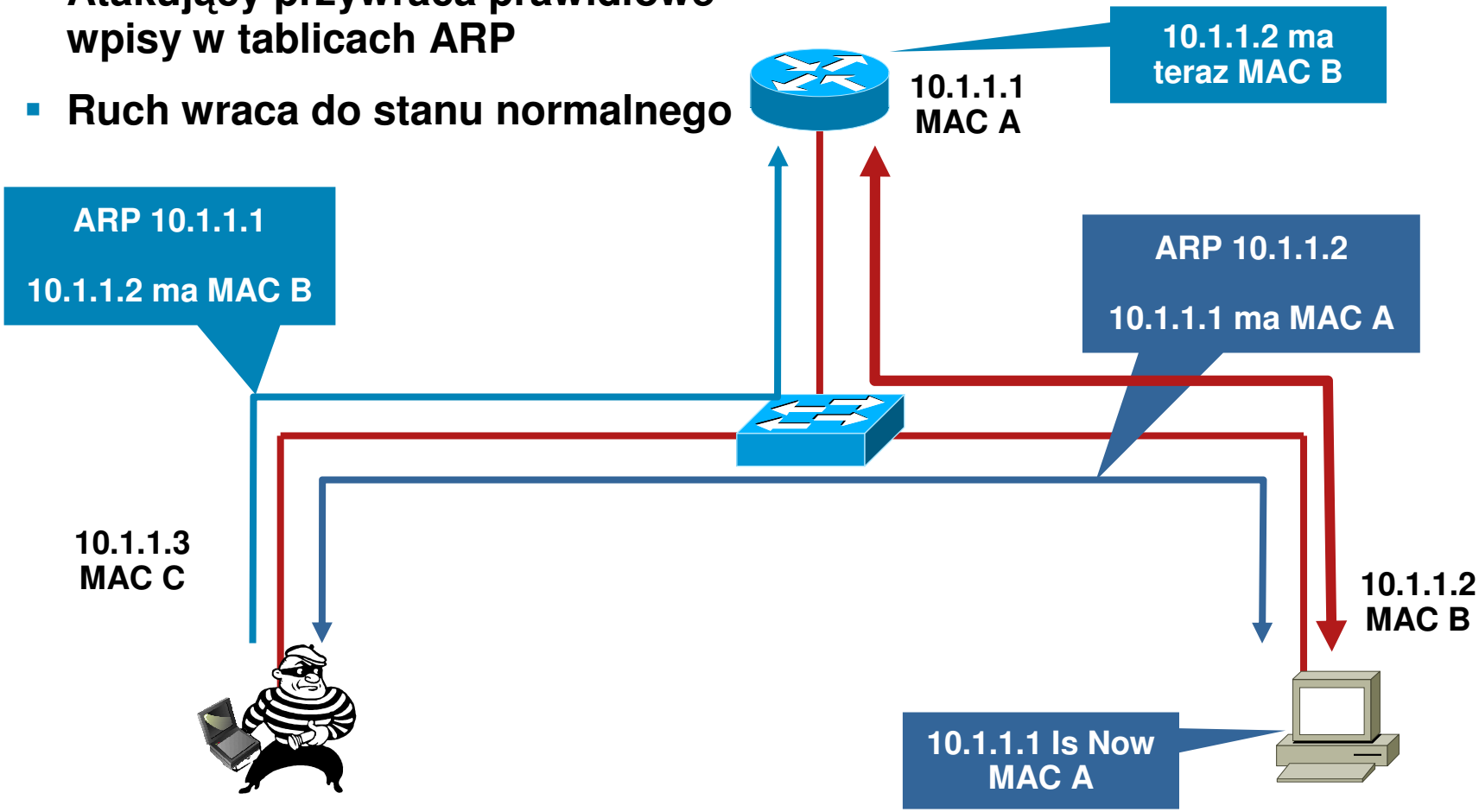
Atak na ARP w działaniu

- Cały ruch przechodzi przez atakującego

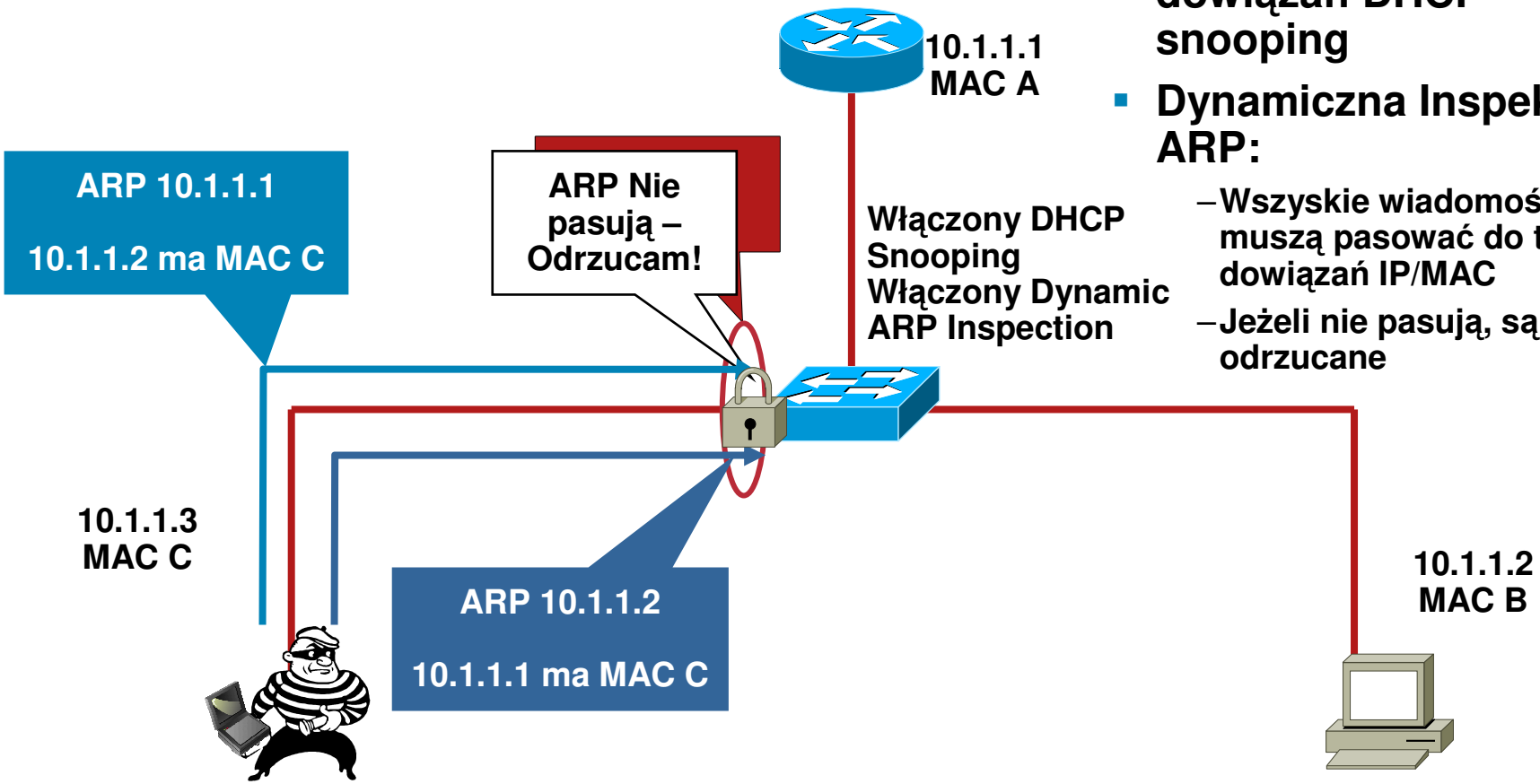


Atak na ARP: zakończenie

- Atakujący przywraca prawidłowe wpisy w tablicach ARP
- Ruch wraca do stanu normalnego



Dynamic ARP Inspection – DAI
Obrona przed atakami na ARP (1)



- Wykorzystuje tablicę dowiązań DHCP snooping
- Dynamiczna Inspekcja ARP:
  - Wszyskie wiadomości ARP muszą pasować do tablicy dowiązań IP/MAC
  - Jeżeli nie pasują, są odrzucane

Dynamic ARP Inspection – DAI
Obrona przed atakami na ARP (2)

- **Wykorzystuje wpisy w tablicy dowiązań DHCP snooping**

```
sh ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type            VLAN  Interface
------------------  --------------  ----------  -------------   ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10     193185      dhcp-snooping   4     FastEthernet3/18
00:03:47:c4:6f:83   10.120.4.11     213454      dhcp-snooping   4     FastEthermet3/21
```

- **Zagląda do pól MacAddress i IpAddress, aby sprawdzić, czy wiadomośc ARP pochodzi od istniejącej stacji. Jeżeli nie – ARP jest odrzucany**

Dynamic ARP Inspection – Konfiguracja

IOS
Polecenia globalne

```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 4,104
ip arp inspection log-buffer entries 1024
ip arp inspection log-buffer logs 1024 interval 10
```

Na interfejsie zaufanym

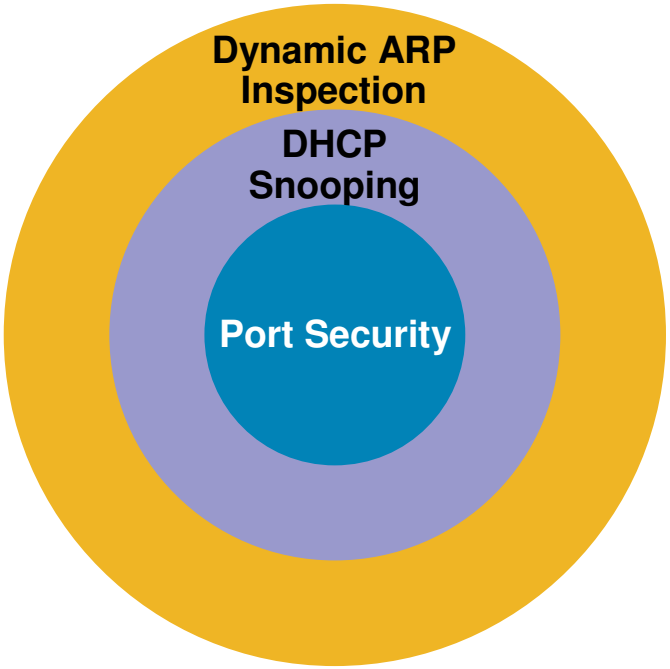
```
ip dhcp snooping trust
ip arp inspection trust
```

IOS
Na interfejsie w stronę niezaufanego klienta

```
no ip arp inspection trust (domyślne)
ip arp inspection limit rate 15(pps)
```

Budujemy warstwy obrony

- Port Security zapobiega atakom na tablicę CAM i serwer DHCP (starvation attack)
- DHCP snooping zapobiega atakom na DHCP
- **Dynamic ARP Inspection zapobiega atakom na ARP**



Demonstracja #3

- Dynamic ARP inspection

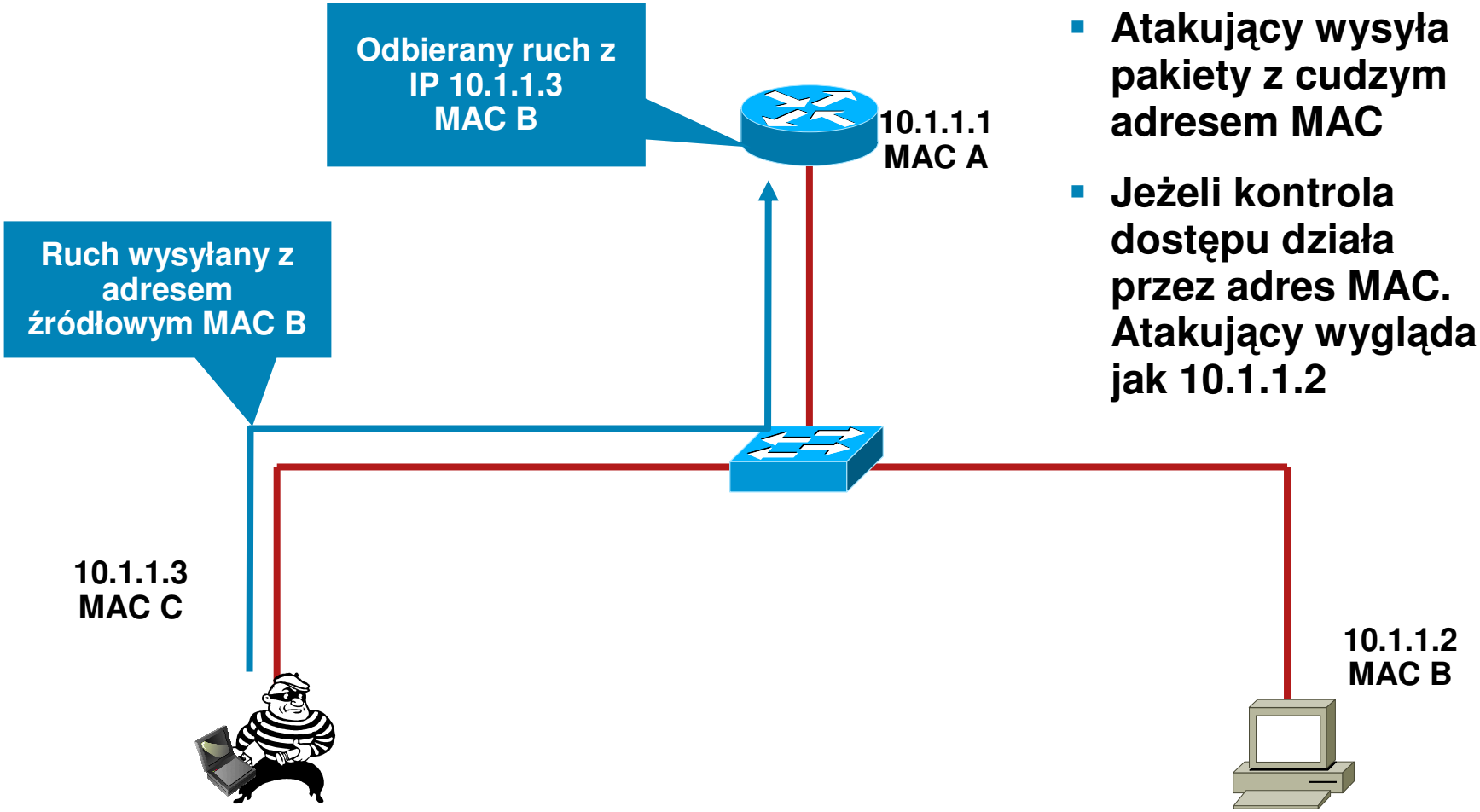
Agenda

- **Ataki L2 i metody przeciwdziałania**
  - Ataki MAC
  - Ataki na usługę DHCP
  - Ataki na ARP
  - Ataki typu Spoofing
  - Inne ataki (VLAN Hopping, STP, CDP, VTP, zarządzanie)

Ataki typu Spoofing – podszywanie się

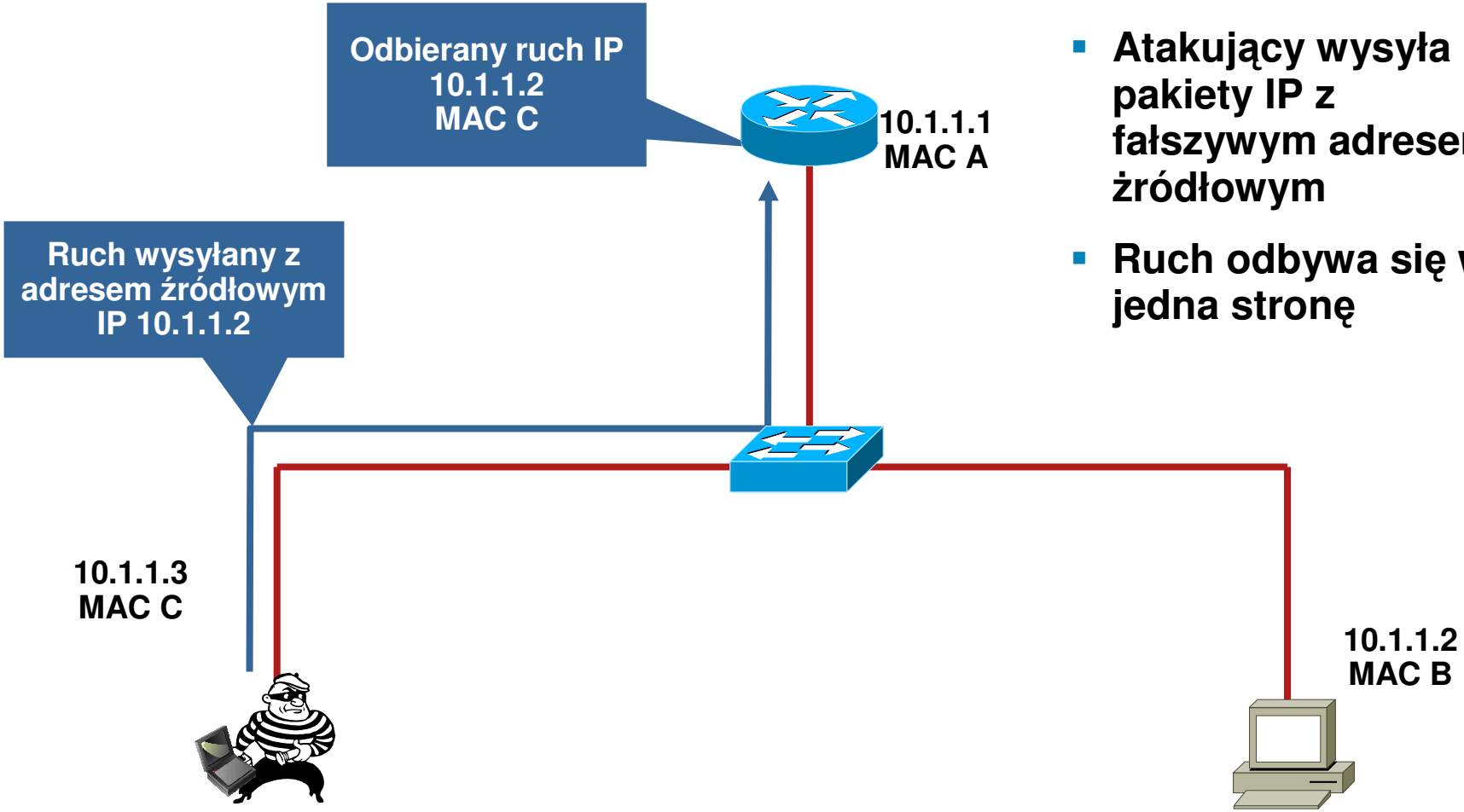
- **MAC spoofing**
  - Jeżeli adresy MAC są używane do identyfikacji – atakujący może uzyskać dostęp do sieci
  - Podszycie się pod istniejącą stację w sieci
- **IP spoofing**
  - Ping of death
  - ICMP unreachable storm
  - SYN flood
  - Podszywanie się pod zaufane adresy IP

Atak MAC Spoofing



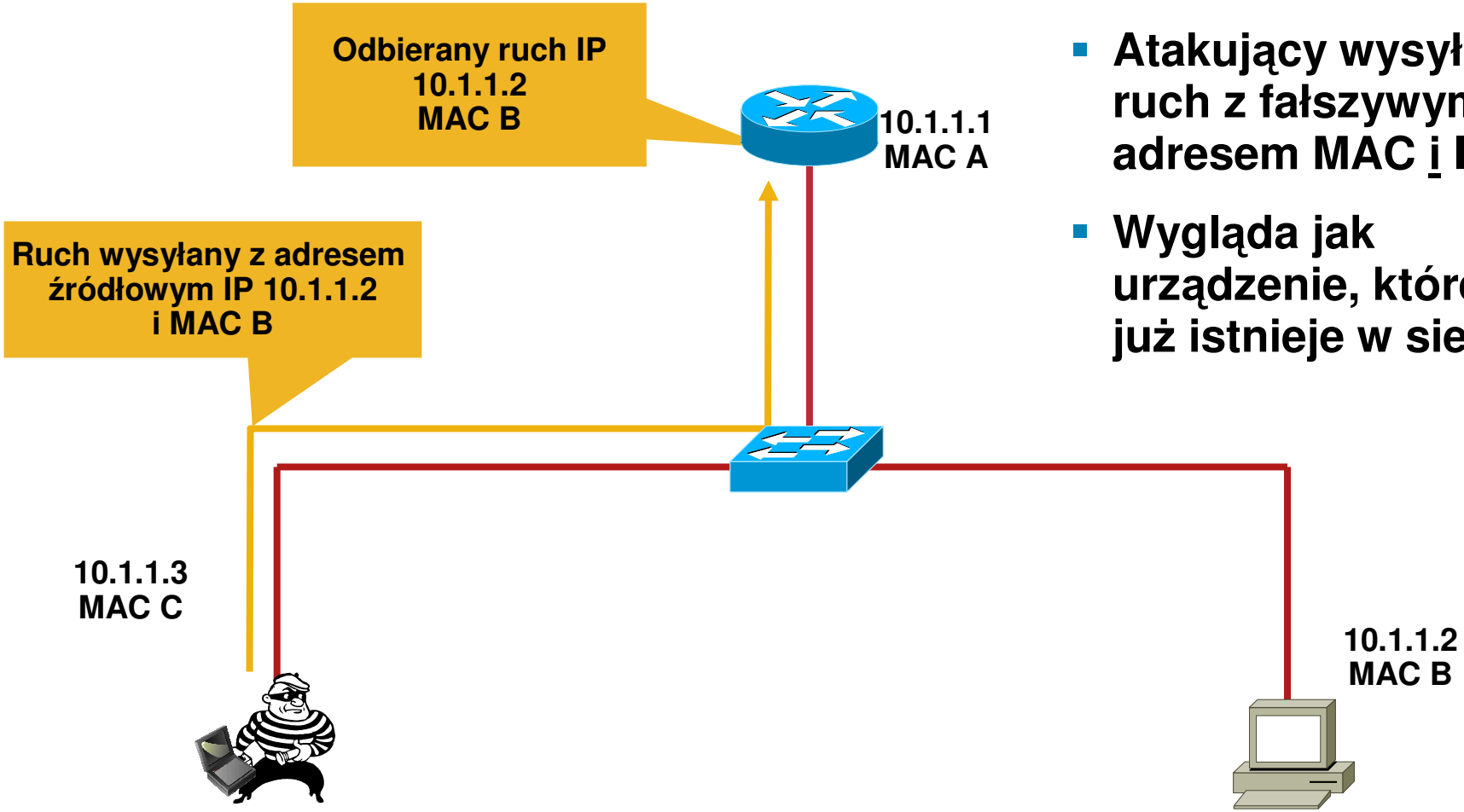
- Atakujący wysyła pakiety z cudzym adresem MAC
- Jeżeli kontrola dostępu działa przez adres MAC. Atakujący wygląda jak 10.1.1.2

Atak IP Spoofing



- Atakujący wysyła pakiety IP z fałszywym adresem źródłowym
- Ruch odbywa się w jedna stronę

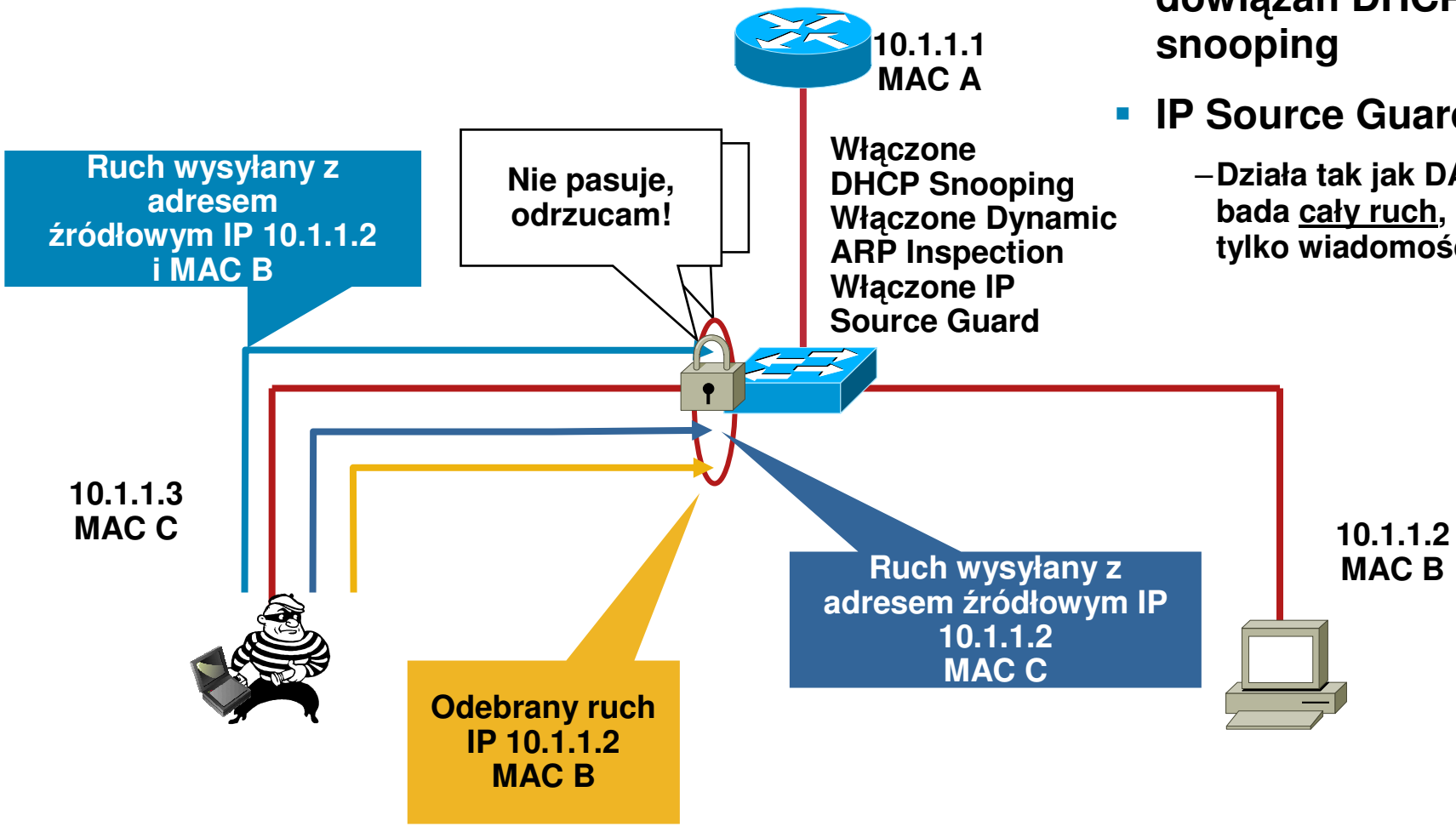
Atak IP/MAC Spoofing



- Atakujący wysyła ruch z fałszywym adresem MAC i IP
- Wygląda jak urządzenie, które już istnieje w sieci

Atak IP/MAC Spoofing – obrona Mechanizm IP Source Guard (1)

- Wykorzystuje tablicę dowiązań DHCP snooping
- IP Source Guard
  - Działa tak jak DAI, ale bada cały ruch, nie tylko wiadomości ARP



Mechanizm IP Source Guard Konfiguracja

IP Source Guard

Konfiguracja IP Source Guard – Weryfikacja IP/MAC (opcja 82)

Globalne Polecenia IOS

```
ip dhcp snooping vlan 4,104
ip dhcp snooping information option
ip dhcp snooping
```

Polecenia interfejsu

```
ip verify source vlan dhcp-snooping
  port-security
```

Konfiguracja IP Source Guard – Weryfikacja IP (bez opcji 82)

Globalne Polecenia IOS

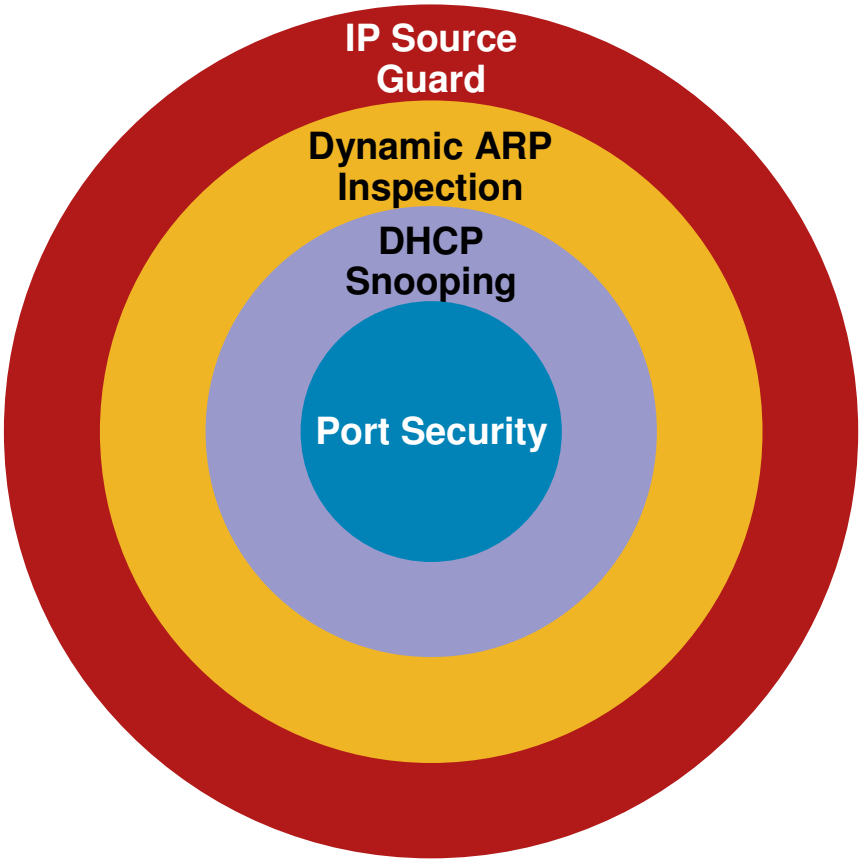
```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
```

Polecenia interfejsu

```
ip verify source vlan dhcp-snooping
```

Budujemy warstwy obrony

- Port Security zapobiega atakom na tablicę CAM i serwer DHCP (starvation attack)
- DHCP snooping zapobiega atakom na DHCP
- Dynamic ARP Inspection zapobiega atakom na ARP
- **IP Source Guard zapobiega podszywaniu pod IP/MAC**



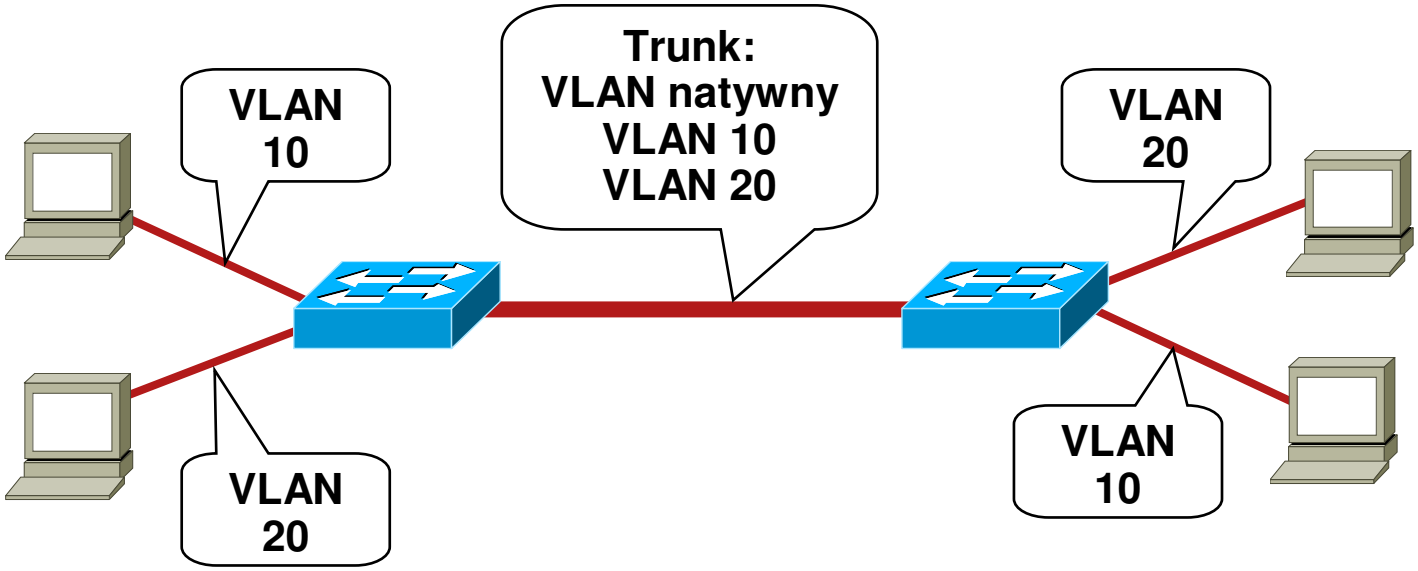
Demonstracja #4

- IP Source Guard

Agenda

- **Ataki L2 i metody przeciwdziałania**
  - VLAN Hopping
  - Ataki MAC
  - Ataki na usługę DHCP
  - Ataki na ARP
  - Ataki typu Spoofing
  - **Inne ataki (VLAN Hopping, STP, CDP, VTP, zarządzanie)**

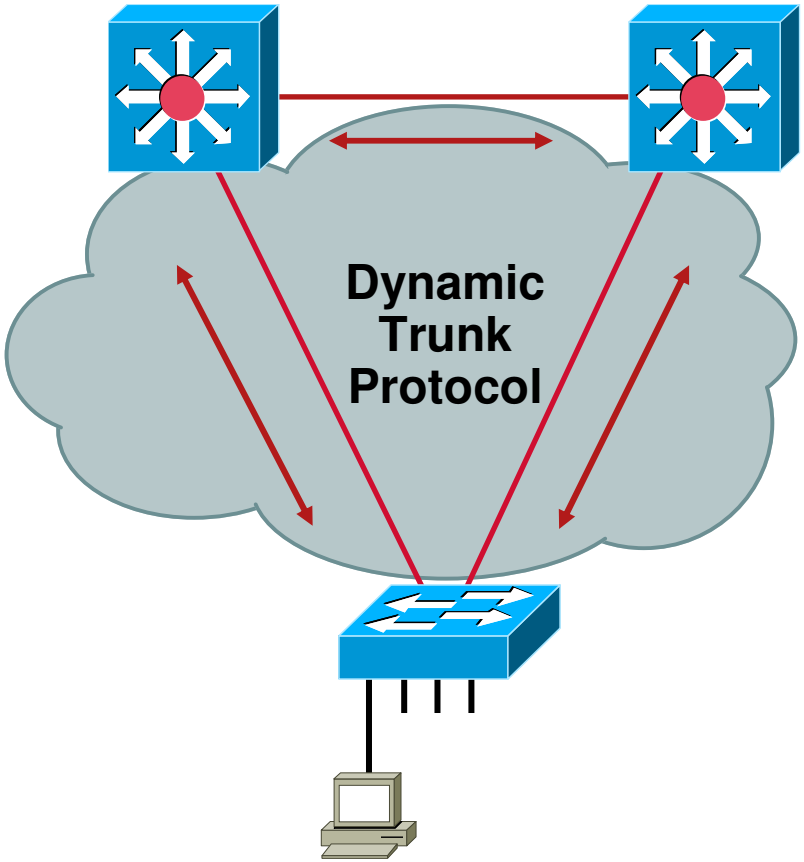
Definicja portu typu trunk



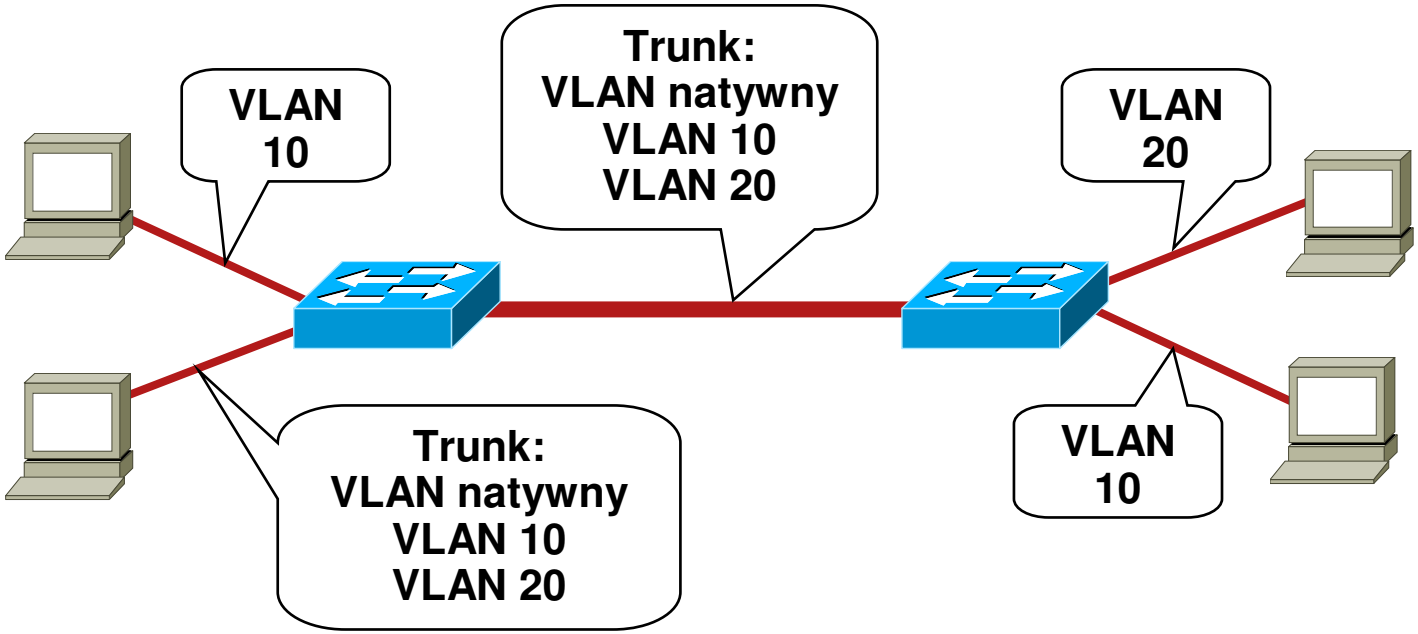
- Porty trunk należą do wszystkich VLANów
- Używane do przenoszenia ruchu z wielu VLANów przez to samo łącze fizyczne (zazwyczaj między przełącznikami lub telefonami IP)
- Enkapsulacja ISL lub 802.1q

Dynamic Trunk Protocol (DTP)

- Co to jest DTP?
  - Automatyzuje konfigurację połączeń typu trunk (802.1q/ISL)
  - Działa pomiędzy przełącznikami (Telefon IP Cisco jest również przełącznikiem)
  - Nie działa na routerach
  - Wsparcie dla DTP jest zależne od platformy
- DTP synchronizuje tryb pracy łącza po obu stronach
- Stan DTP dla 802.1q/ISL można ustalić jako “Auto”, “On”, “Off”, “Desirable”, lub “Non-Negotiate”



Podstawowy atak typu VLAN Hopping



- Stacja końcowa podszywa się pod przełącznik ISL or 802.1q
- Stacja staje się członkiem wszystkich VLANów
- Wymagane jest, aby VLANem natywnym był VLAN1

Atak VLAN Hopping – podwójna enkapsulacja 802.1q

- Atakujący wysyła ramki podwójnie tagowane ramki 802.1q
- Przełącznik dokonuje deenkapsulacji „zewnętrznego” znacznika
- Ruch jednokierunkowy
- Działa nawet, gdy stan DTP portów jest „off”

VLANy i trunking: najlepsze praktyki

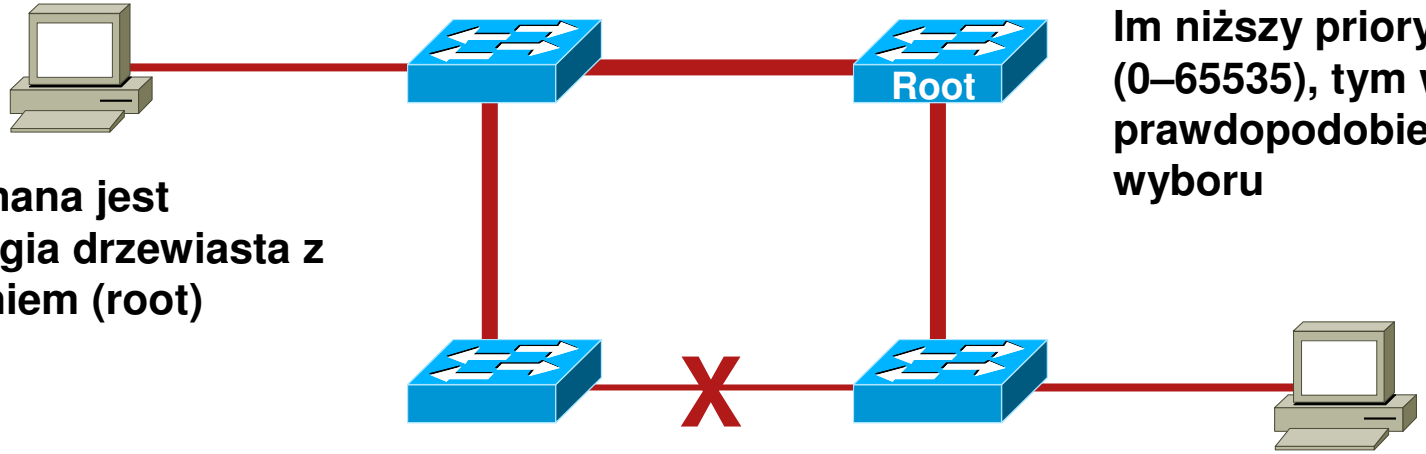
- Zawsze używaj dedykowanego VLANu dla wszystkich portów typu trunk
- Wyłącz nieużywane porty i przenieś je do nieużywanego VLANu
- Bądź paranoikiem: nie używaj VLANu 1 do niczego
- Wyłącz tryb DTP auto na portach użytkowików (DTP off)
- Ręcznie konfiguruj trunking na portach między przełącznikami
- Używaj trybu tagowanego dla VLANów natywnych na łączach typu trunk
- Wyłącz dostęp do Voice VLAN na portach PC
- Używaj `vlan dot1q tag native` na portach typu trunk

Protokół STP – z lotu ptaka

- **Cel STP: Zapewnić przełączaną topologię L2 pozbawioną pętli**

Przełącznik wybrany jako Root

Im niższy priorytet (0–65535), tym większe prawdopodobieństwo wyboru

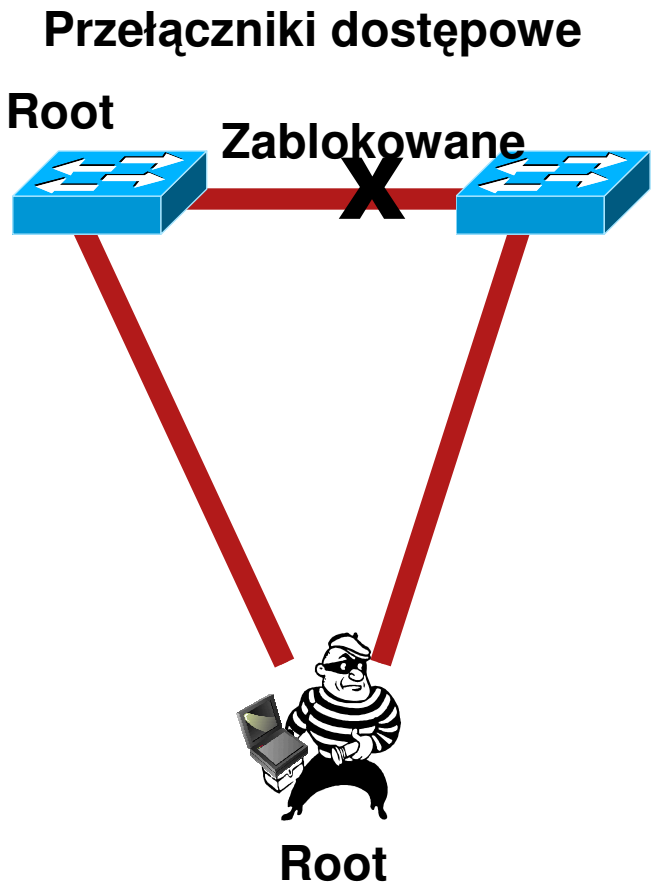


Rozpinana jest topologia drzewiasta z korzeniem (root)

- **Działanie STP: przełączniki wymieniają wiadomości BPDU (Bridge Protocol Data Units). Podstawowe wiadomości: konfiguracja, zmiana topologii (notification/acknowledgment – TCN/TCA).**
- **Ruch rozgłoszeniowy nie wywołuje sztormów**

Atak na Spanning Tree – przykład

- **Atakujący wysyła BPDU, aby stać się root-bridge.**
  - **Atakujący widzi ramki, których nie powinien**
    - **MitM, DoS - <u>wszystko możliwe</u>**
    - **Na atak ma wpływ topologia, trunking, PVST itd.**
    - **Zmiana topologii ze zmianą szybkości (z Gb rdzenia do 10Mb half-duplex)**
    - **Wymagany jest dual-homing. Jeśli użyjemy huba – wystarczy jeden interfejs na stacji atakującego**



Ataki na Spanning Tree – obrona

BPDU Guard

- **STP powinno być włączone zawsze – w możliwie szybkiej implementacji (Rapid STP) i per-VLAN (MST lub PVST/PVST+)**
- **Używaj BPDU Guard ma wszystkich portach dostępowych**
  - **Wykrycie BPDU spowoduje wyłączenie portu**
  - **Włącz na wszystkich portach w trybie portfast**

```
CatOS> (enable)set spantree portfast bpdu-guard enable

IOS(config)# spanning-tree portfast bpduguard
```

Atak na Spanning Tree – obrona

Root Guard

- **Wyłącza port, na którym otrzymano BPDU – jeśli nastąpiłaby zmiana przełącznika root w topologii**
- **Konfigurowane per interfejs**

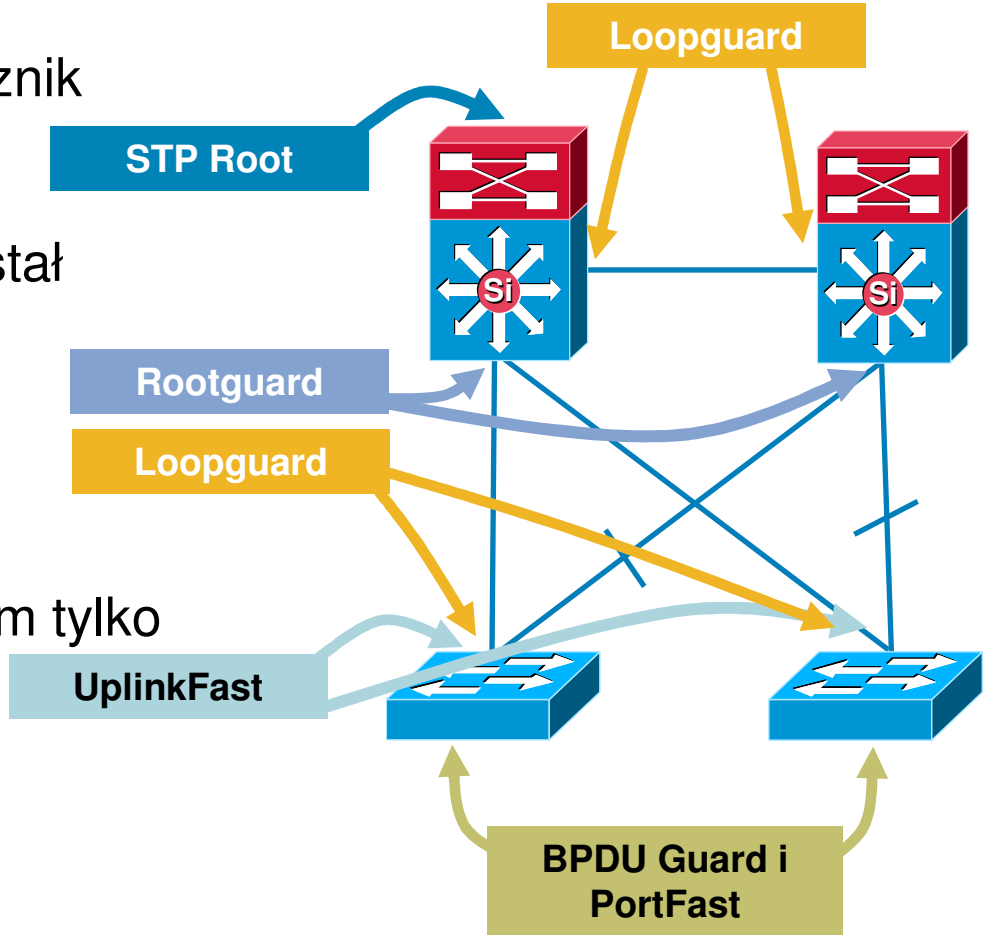
```
CatOS> (enable) set spantree guard root 1/1

IOS(config)# spanning-tree rootguard
```

Atak na Spanning Tree

Świadoma budowa i zabezpieczenie sieci

- Należy zdefiniować przełącznik Root
  - Root Podstawowy/Zapasowy
- Root zawsze tam, gdzie został zdefiniowany:
  - Rootguard
  - Loopguard
  - UplinkFast
  - UDLD
- Na przełączniku dostępowym tylko ruch od klientów:
  - BPDU Guard
  - Root Guard
  - PortFast
  - Port-Security
  - DAI/IP Source Guard



Demonstracja #5

- bpdu-filter i bpdu-guard vs Yersinia

Ataki na warstwę trzecią - IP

Ataki na warstwę trzecią

Drzewo ataku

- Ataki DoS itp. na protokół IP / za pomocą protokołu IP
  - fragmentacja z rozmaitymi wariacjami na ten temat
  - zmniejszanie MTU lub okna TCP
  - resetowanie sesji TCP za pomocą ICMP
- Ataki logiczne na routing (osiągalność prefiksów w sieci IP)
- Ataki na konkretną platformę
  - błędy w implementacji buforów, kolejek, filtrów i obsługi ruchu IPv4/IPv6

Dobre praktyki

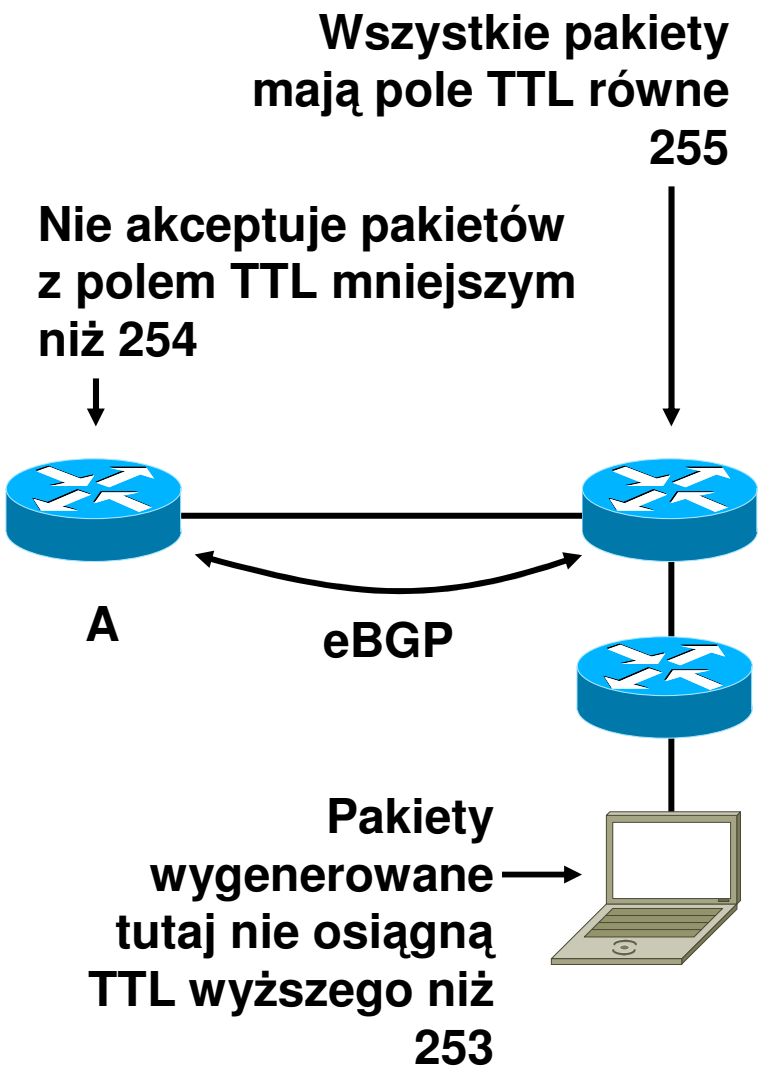
Ochrona protokołów routingu

- Protokoły RIPv2, OSPF, BGP, IS-IS i EIGRP obsługują dodatkowe uwierzytelnianie – sąsiadów lub uaktualnień
- Współdzielony klucz w pakietach protokołów routingu
  - czystym tekstem – chroni tylko przed błędami w konfiguracji
  - Message Digest 5 (MD5)—zapobiega potencjalnym atakom w warstwie protokołu routingu
- Często nie jest wykorzystywane
  - „Nie mieliśmy żadnych ataków”
  - „To obciąża router/ułatwia atak”

Dobre praktyki

Generalised TTL Security Mechanism – RFC 3682

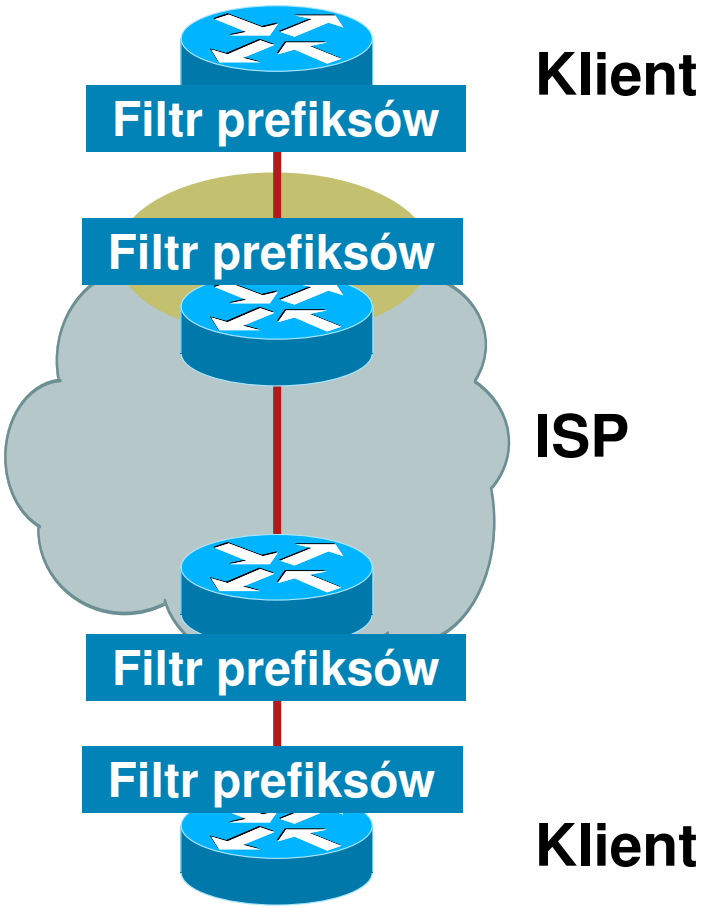
- GTSM chroni sesje BGP przed atakami z oddalonych stacji/sieci
- Routery wymieniają się pakietami IP z polem TTL ustawionym na 255, wartości poniżej 254 są automatycznie odrzucane
- Urządzenie nie podłączone bezpośrednio pomiędzy routerami nie może wygenerować takiego ruchu



Dobre praktyki

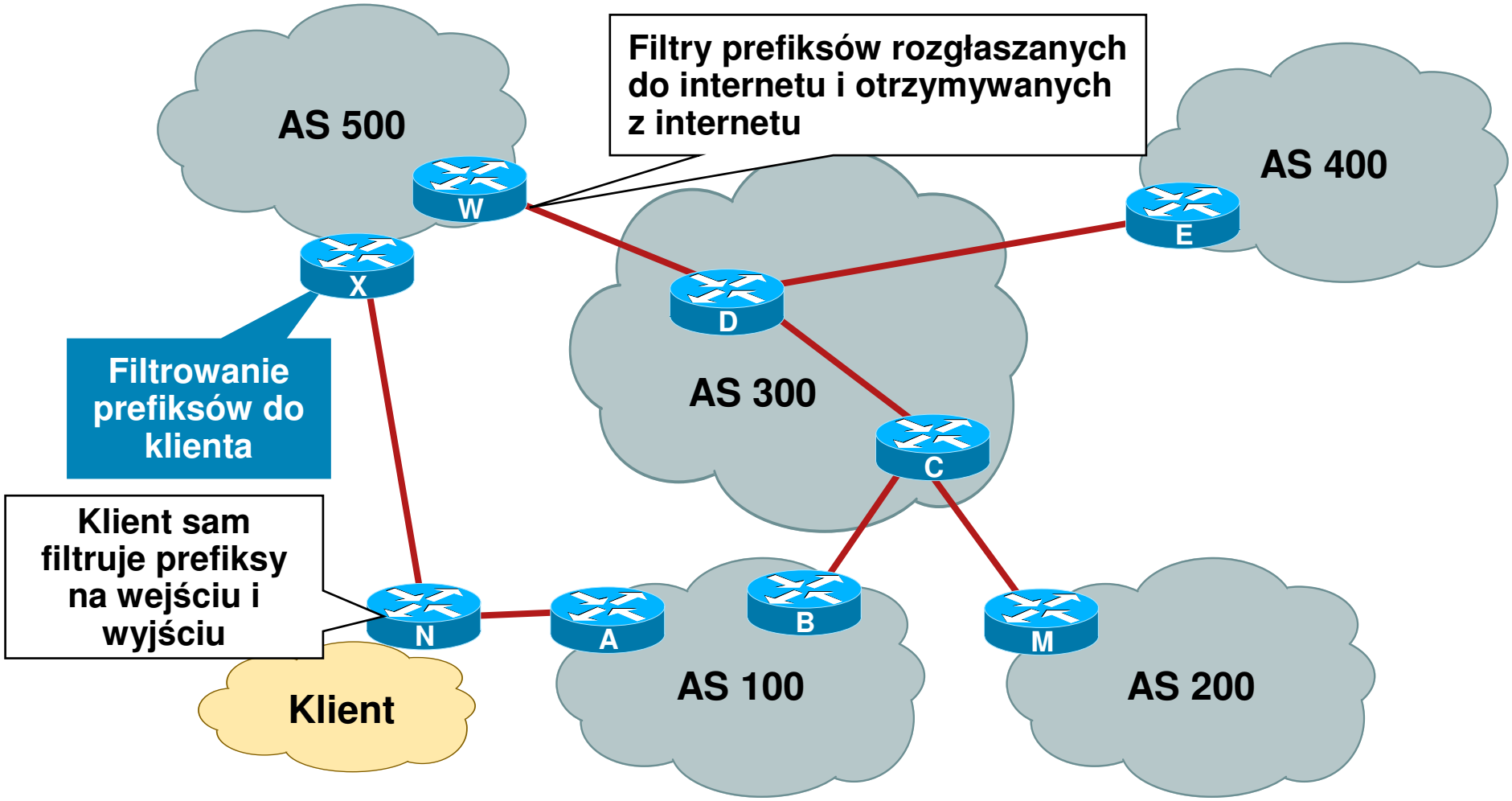
Filtrowanie prefiksów

- Prefiksy otrzymywane od operatorów i wysyłane do operatorów (i klientów) należy kontrolować
  - ...dodatkowy bonus to prawidłowe działanie mechanizmów typu uRPF



Dobre praktyki

Filtrowanie prefiksów – gdzie?



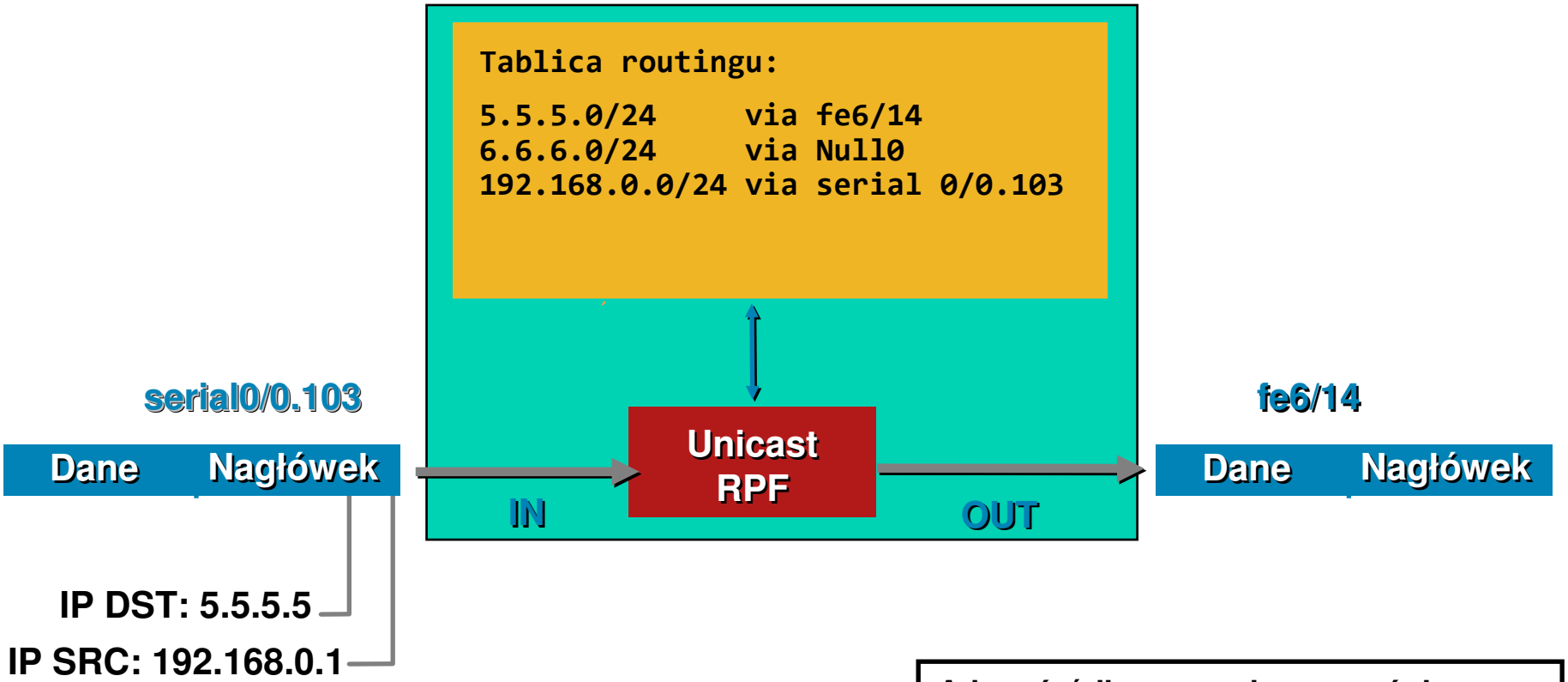
Dobre praktyki

Co i jak można odfiltrować od strony klienta?

- Automatyczne wykrywanie fałszowania adresu źródłowego: unicast Reverse Path Filtering (uRPF)
- Inne pomysły do rozważenia:
  - wycięcie ruchu do/z TCP/UDP 135-139
  - wycięcie ruchu do/z TCP 445 (SMB over TCP)
  - mechanizm QoS – rate limiting per protokół, lub ilość nawiązywanych sesji na sekundę
  - wprowadzenie klas usługowych opartych o oznaczenie pakietów za pomocą IP DSCP – wydzielenie osobnych klas usługowych z nieprzekraczalnym pasmem generowanym od klienta w stronę sieci

unicast Reverse Path Filtering

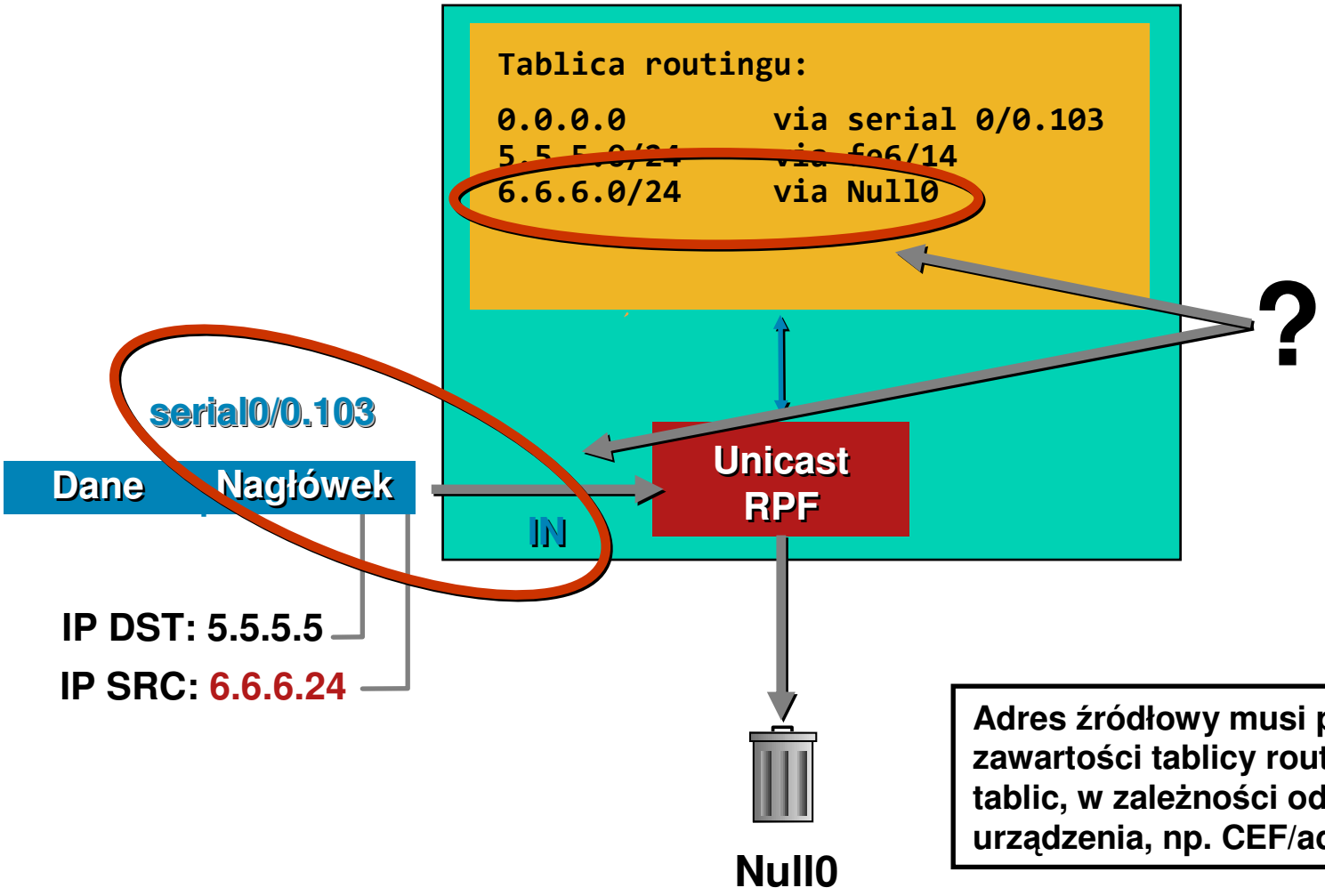
Tryb ‘strict’



Adres źródłowy musi pasować do zawartości tablicy routingu (i innych tablic, w zależności od architektury urządzenia, np. CEF/adj)

unicast Reverse Path Filtering

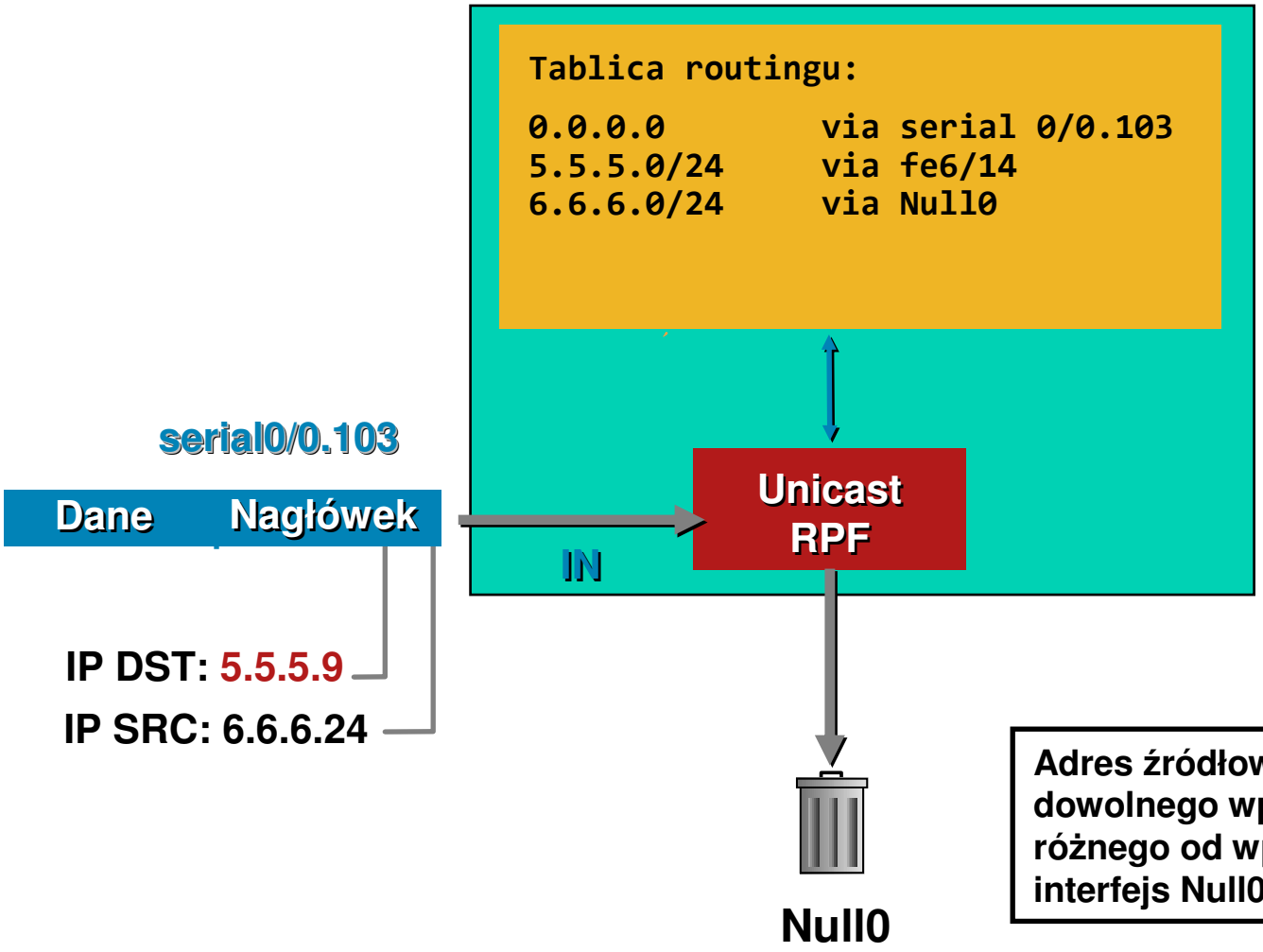
Tryb ‘strict’



Adres źródłowy musi pasować do zawartości tablicy routingu (i innych tablic, w zależności od architektury urządzenia, np. CEF/adj)

unicast Reverse Path Filtering

Tryb ‘loose’



Adres źródłowy musi pasować do dowolnego wpisu w tablicy routingu różnego od wpisu kierującego pakiet na interfejs Null0

unicast Reverse Path Filtering

Konfiguracja

- W zależności od systemu operacyjnego (i często konkretnego filtra pakietów) konfiguracja uRPF:
  - FreeBSD, tryb „strict/loose”:

```
deny log ip from any to any not [verrevpath|versrcpath] in via em0
```

  - Cisco, tryb „strict/loose”:

```
ip verify unicast source reachable via [rx|any] [allow-default]
```

  - Linux, tryb „strict/loose”:

```
echo [1|2] > /proc/sys/net/ipv4/conf/(all|ethX)/rp_filter
```

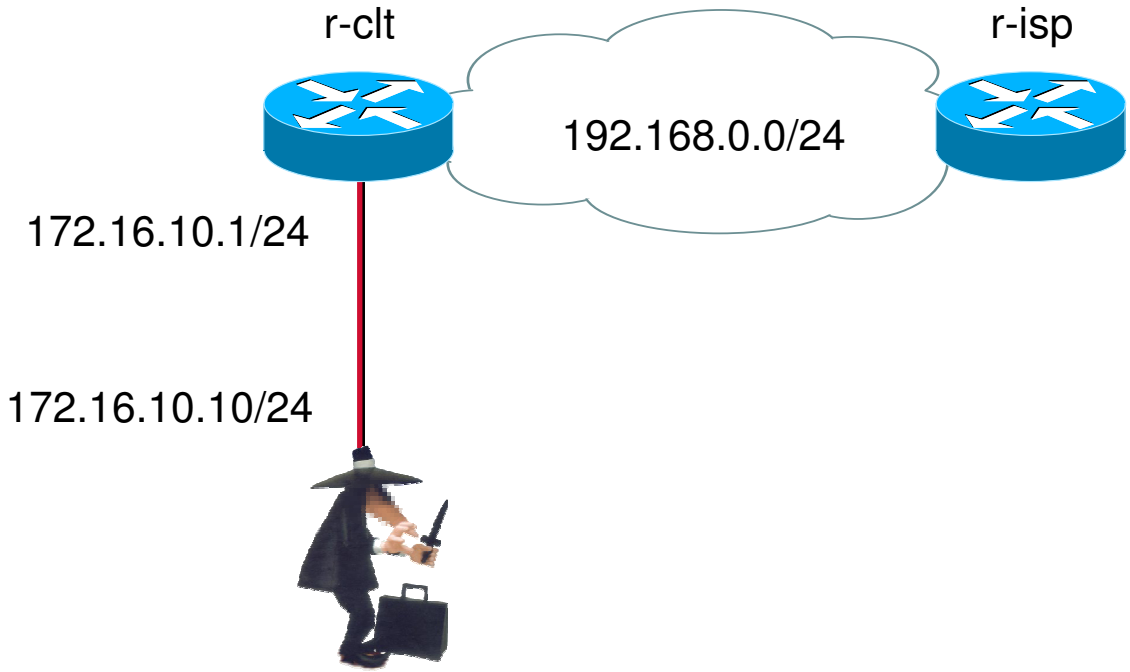
  - JunOS, tryb „strict/loose”:

```
[edit interface ge-0/0/0 unit 0 family inet]
        rpf-check { mode loose; }
```

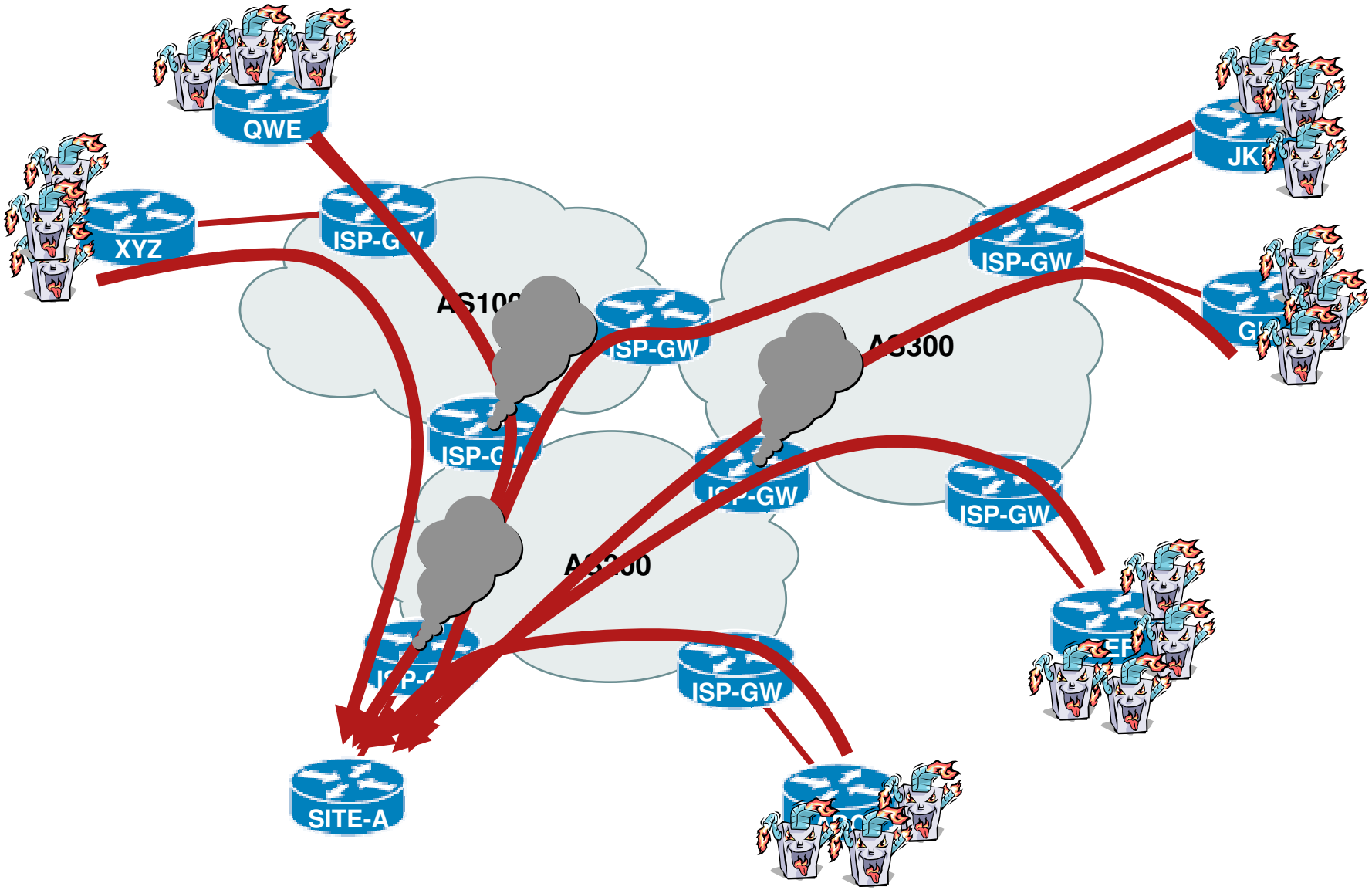
uRPF dla FreeBSD niezależny od filtra pakietów:
http://lukasz.bromirski.net/projekty/patches.html

Demonstracja #6

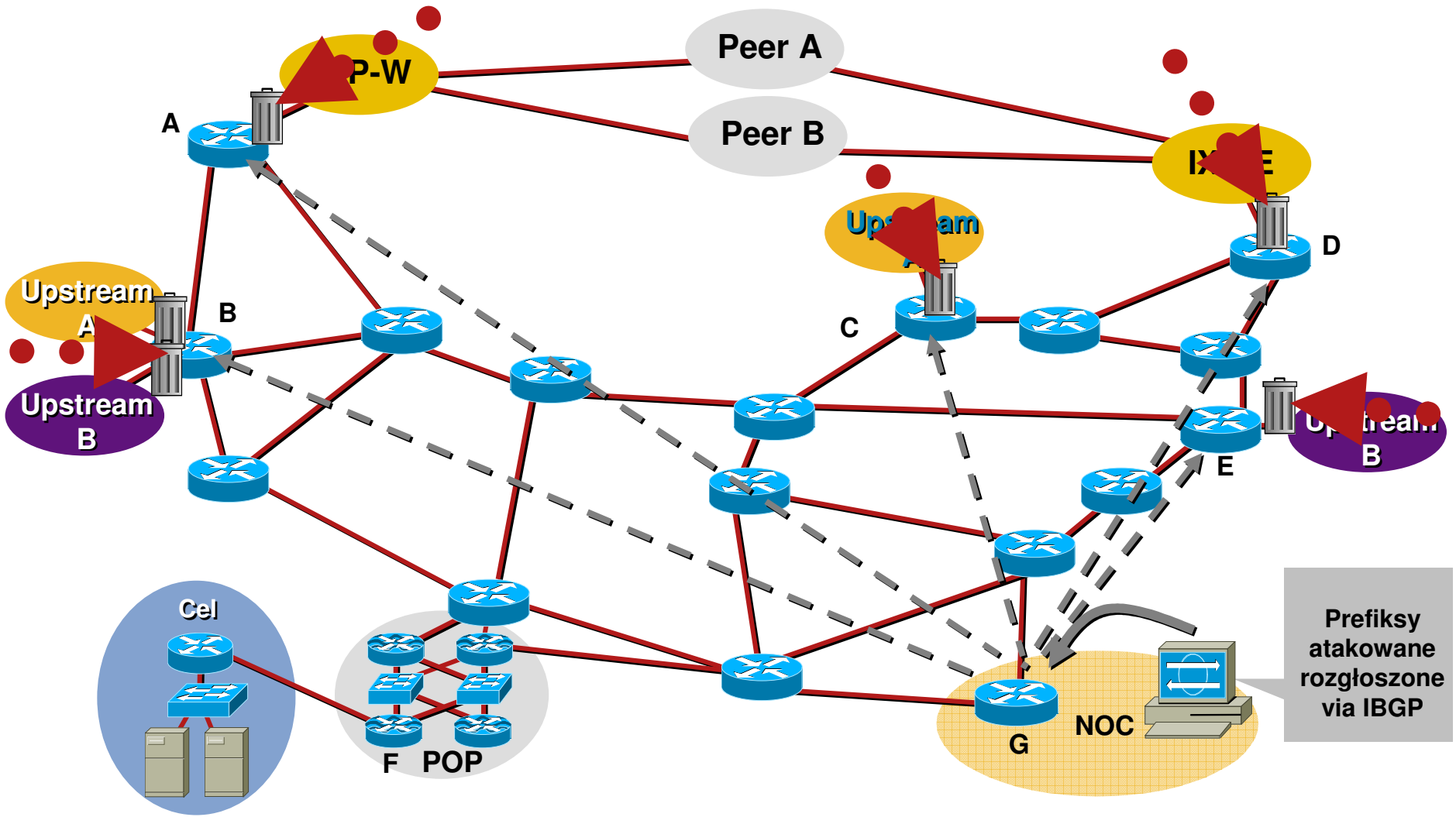
- hping2 vs uRPF



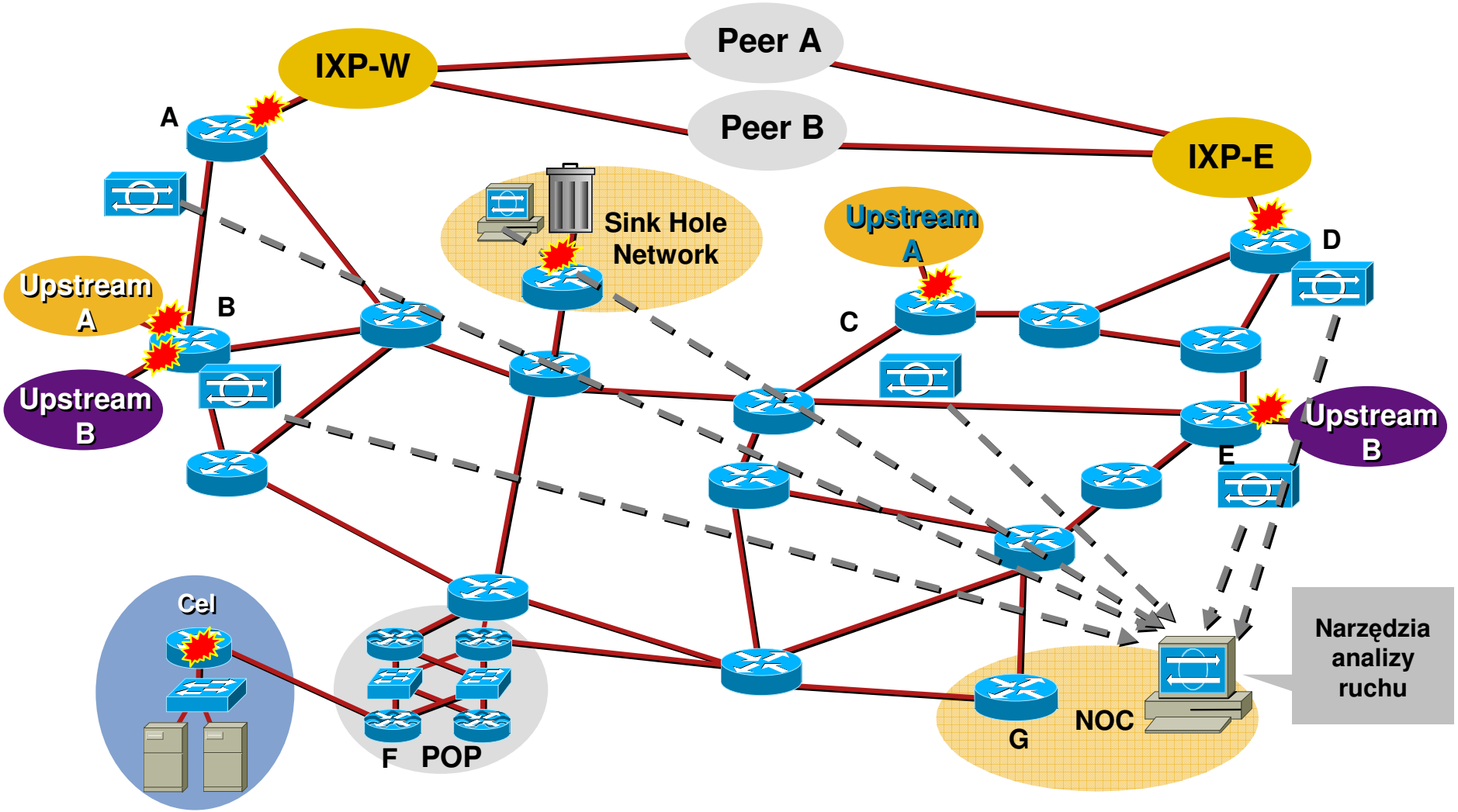
Atak DDoS – jak to się dzieje?



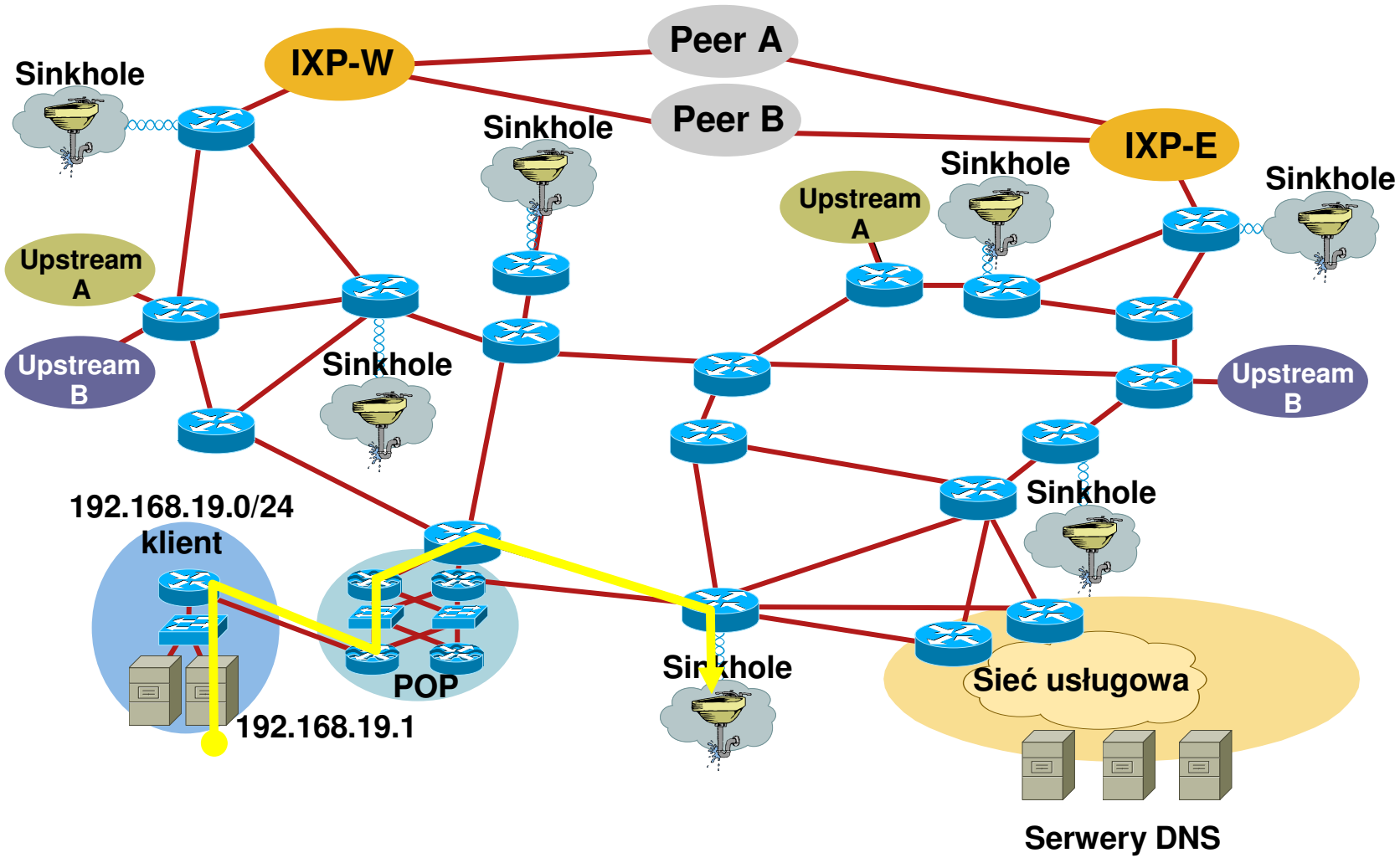
BGP blackholing - filtrowanie



BGP blackholing - przekierowanie

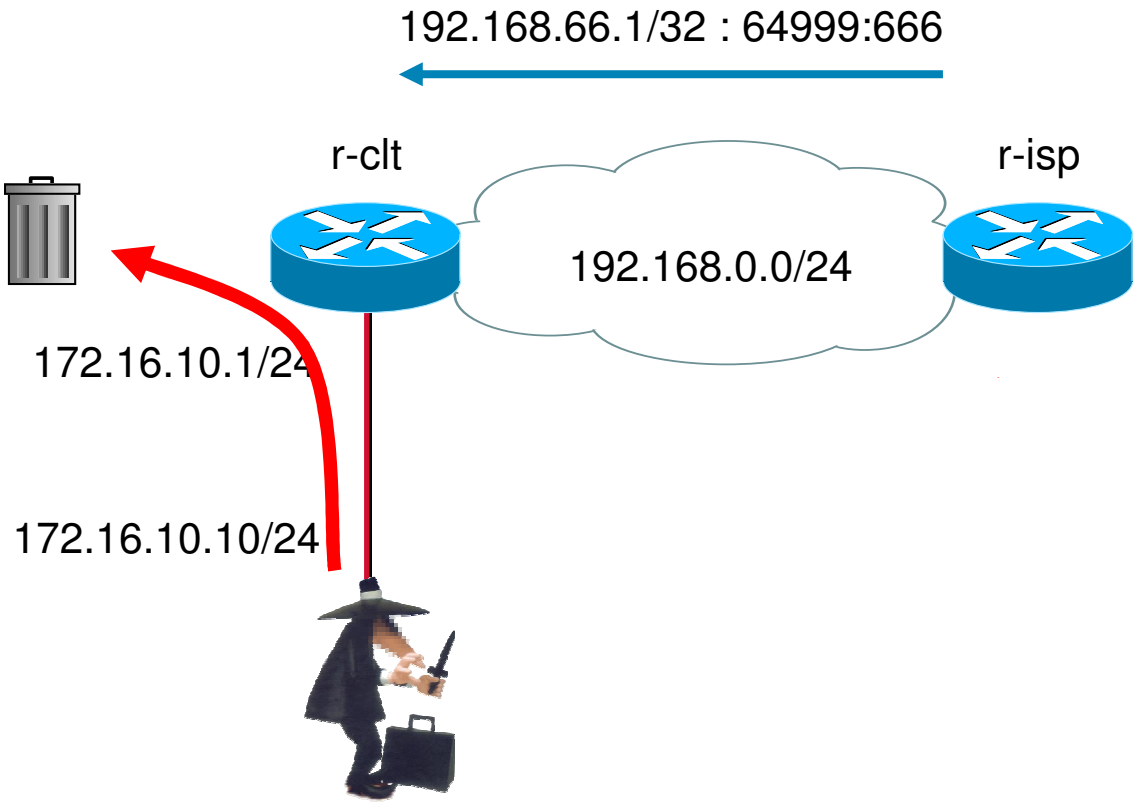


Anycast Sinkhole - przykład



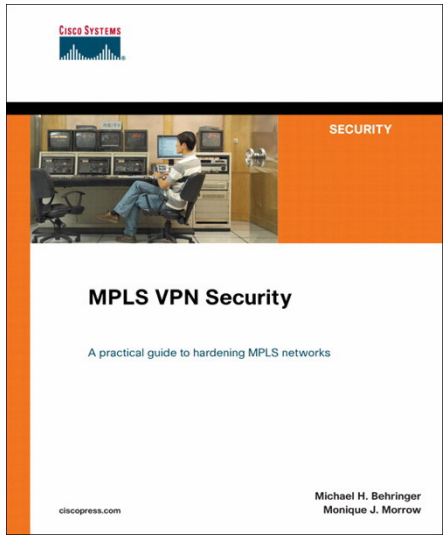
Demonstracja #7

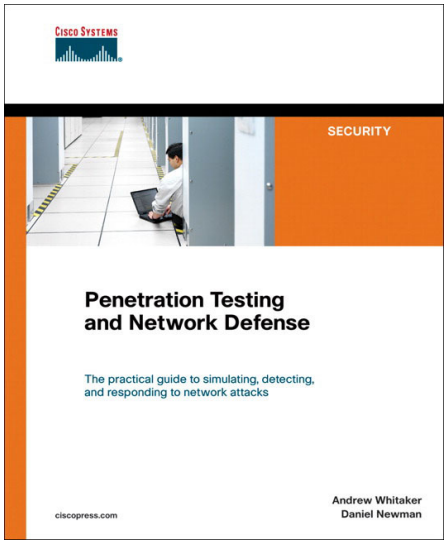
- BGP blackholing

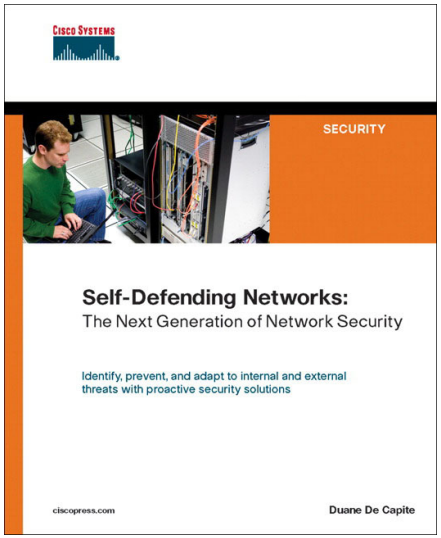


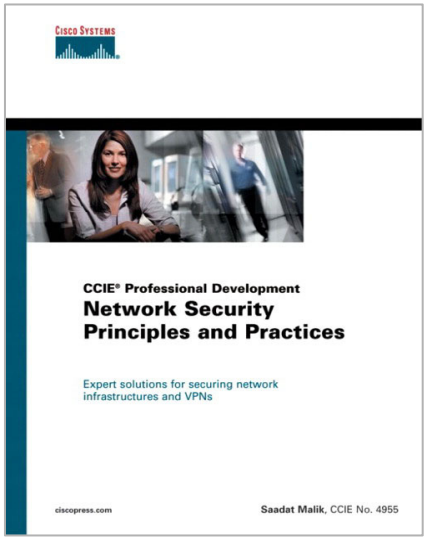
Gdzie znaleźć więcej informacji?

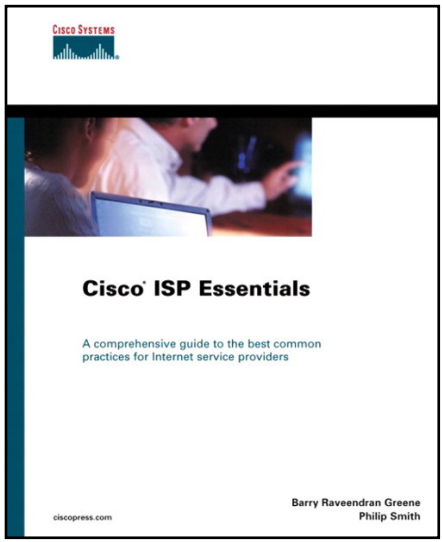
Gdzie warto zajrzeć?











Materiały na WWW

- NANOG (North American Network Operators Group)
  - http://www.nanog.org
- Packet Clearing House
  - http://www.pch.net
- ISP Essentials:
  - ftp://ftp-eng.cisco.com/cons/isp/
- Architektury bezpieczeństwa dla LAN, WLAN, VoIP, CPD, WAN, VPN
  - http://www.cisco.com/go/srnd
- BGP Blackholing PL
  - http://networkers.pl/bgp-blackholing

Q&A


NO
QUESTIONS
VIOLATORS
WILL BE SHOT
SURVIVORS
WILL BE SHOT
AGAIN