HOW TO ATTACK, DEFEND AND 0wN NETWORK FOR FUN, FUN & FUN

Łukasz Bromirski
lukasz@bromirski.net

Agenda

- **Bezpieczeństwo sieciowe**

  (definicja problemu i parę dobrych rad wujka Dobra Rada)

- **Ataki L2**
- **Ataki L3**
- **L4 i powyżej**
- **Q&A**

Ta sesja...

- **...stanowi podsumowanie najczęściej stosowanych ataków i technik obrony przed nimi**
- **...nie dotyczy ataków L0/L1/socjotechniki, ale również nie wybiega daleko w L4+ oraz w bezpieczeństwo głosu i WLAN**

BEZPIECZEŃSTWO SIECIOWE

Duże firmy wydają na bezpieczeństwo...

- **...mniej niż na kawę**
- **Dlaczego małe firmy lub osoby prywatne mają wydawać więcej?**

  (i kogo to obchodzi?)
- **Zmiana nastawienia, nawyków i całej kultury związanej z bezpieczeństwem zależy od młodego pokolenia**

Parę porad Wujka Dobra Rada

- **Dobre bezpieczeństwo ma warstwy**

  ...każda z nich potencjalnie spowalnia i zniechęca atakującego

  ...jeden, dwa, trzy mechanizmy mogą zawieść – pięć lub sześć zawodzi bardzo rzadko

- **Bezpieczeństwo jest procesem**

  ...to oczywiście wygodny sposób na wyciąganie pieniędzy, ale wystarczy zajrzeć na ulubioną listę poświęconą bezpieczeństwu by zdać sobie sprawdę, że nowe zagrożenia pojawiają się co chwila (i tu ma zastosowanie traktowanie bezpieczeństwa jak procesu)

Parę porad Wujka Dobra Rada

- **Wybierając dowolne rozwiązanie komercyjne sprawdź czy producent:**

  ...informuje o błędach publicznie i natychmiast bez czekania na „drugi wtorek miesiąca”?

  ...należy i aktywnie uczestniczy w pracach instytucji zaangażowanych w implementowanie i rozwój systemów bezpieczeństwa?

  ...zapewnia pomoc techniczną w przypadku problemów z bezpieczeństwem?

  ...posiada własny zespół zajmujący się bezpieczeństwem produktów?

  I jak wygląda jego reputacja na podstawie danych, które potrafisz zebrać?

Przydatne jeśli chodzi o bezpieczeństwo jest...

- **...pamiętać, że:**

  Bezpieczeństwo Sieciowe to System

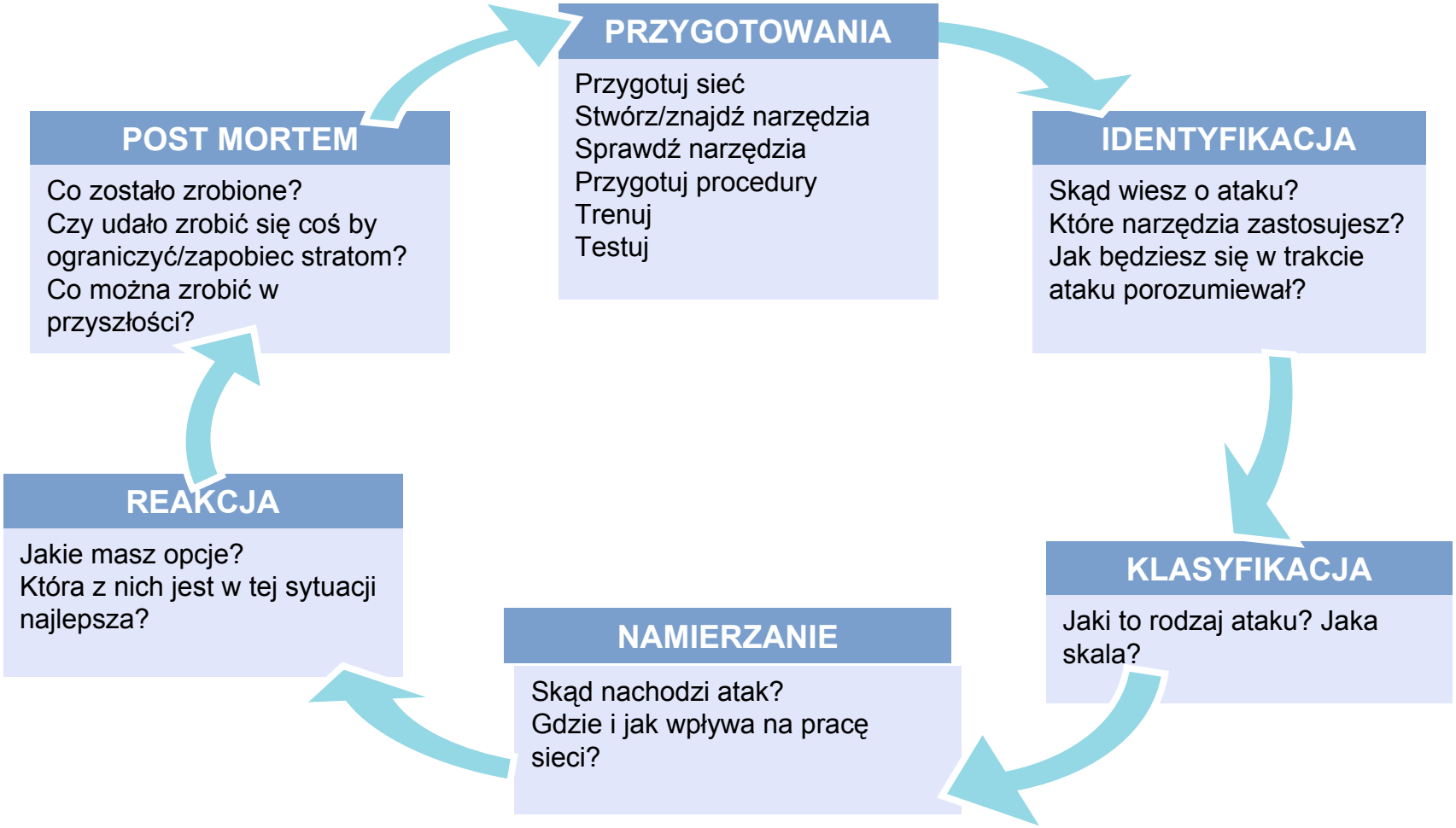
  Wszystko jest Celem lub Bronią

  Łatwiej jest bronić i zarządzać rzeczami prostymi

  „Security Through Obscurity” to proszenie się o kłopoty

  „Poufność” != „Bezpieczeństwo”

Jak sobie radzić ze stresem w trakcie ataku?



ATAKI L2

Ataki L2

- **DoS urządzenia:**

  dziury w usługach (SNMP, Telnet/SSH, HTTP/HTTPS etc.) i protokołach firmowych (CDP/VTP/etc.)

  śmieciowy ruch wprost na IP urządzenia jeśli przetwarzaniem zajmuje się CPU (99,8% tanich rozwiązań)

- **Przechwytywanie/wstrzykiwanie ruchu:**

  przepełnianie tablicy CAM, ataki na (r)STP, DHCP spoofing

  podwójne tagowanie (VLAN hopping)

ATAKI NA MAC

Adres MAC

Adres unikalny dla warstwy drugiej modelu OSI – 48 bitów

1234.5678.9ABC

Pierwsze 24 bity = przydzielane przez IEEE, kod producenta

0000.0cXX.XXXX

Drugie 24 bity – przydzielane przez producenta, unikalne dla niego

0000.0cXX.XXXX

Wszystkie 48 bitów ustawione na 1 = broadcast

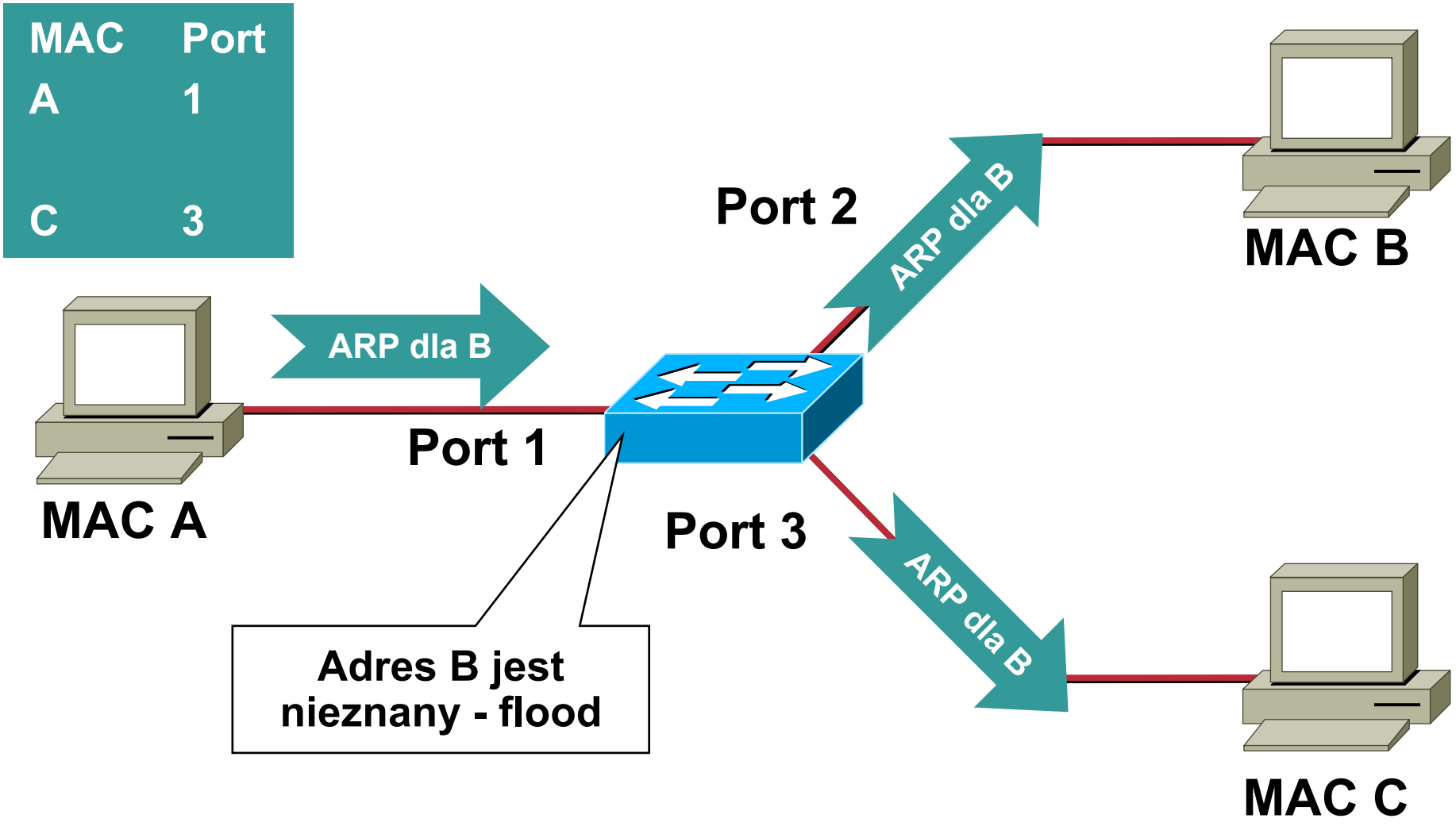
FFFF.FFFF.FFFF

- **Przełącznik przechowuje mapowania port-MAC w pamięci podręcznej**
- **Pamięć ma zwykle ograniczony (programowo lub sprzętowo) rozmiar**
- **Po jej przepełnieniu:**

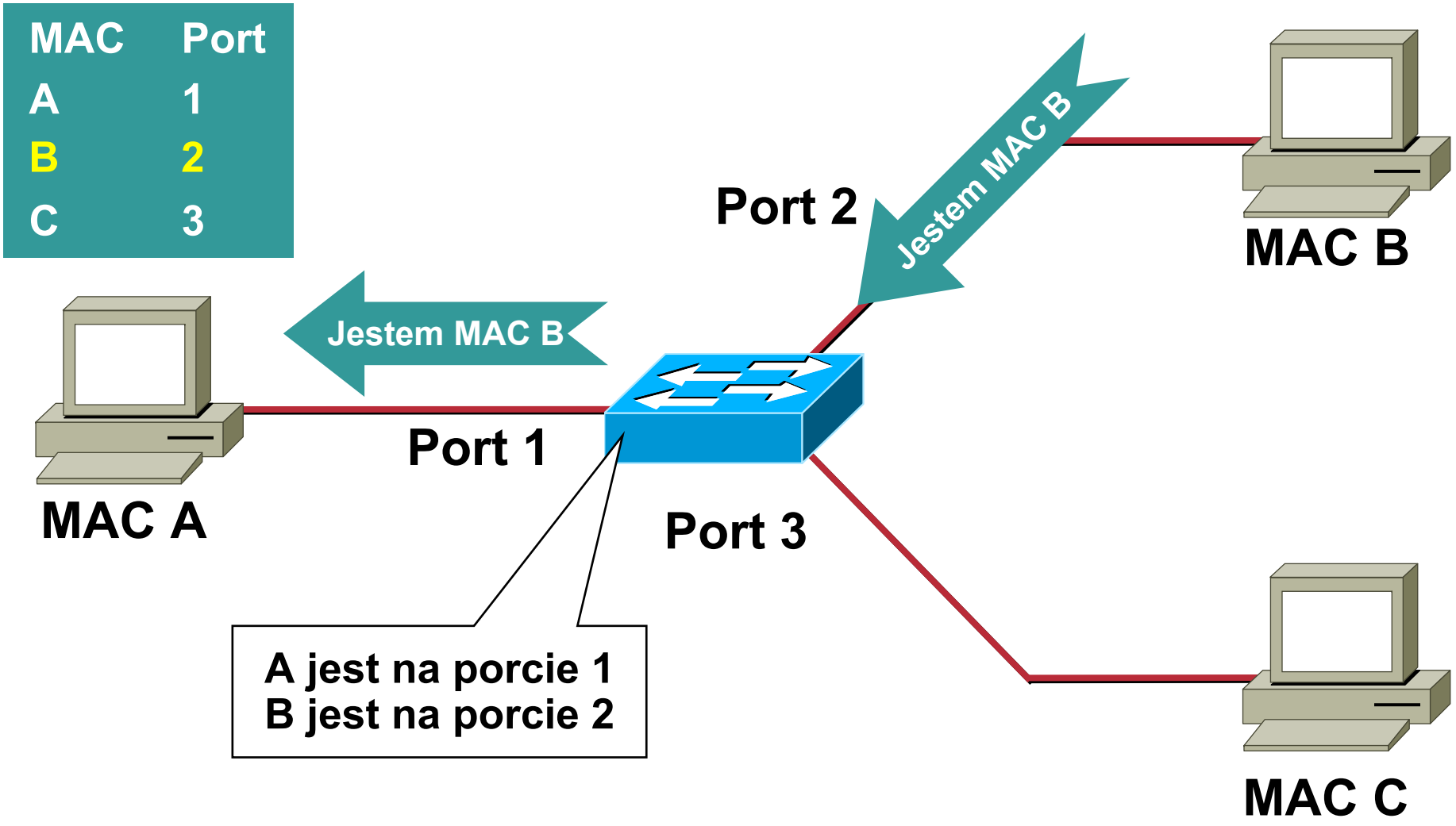
  wyrzucamy szybciej stare wpisy (skracamy timeout)

  floodujemy ramki do nieznanych adresów przez wszystkie porty

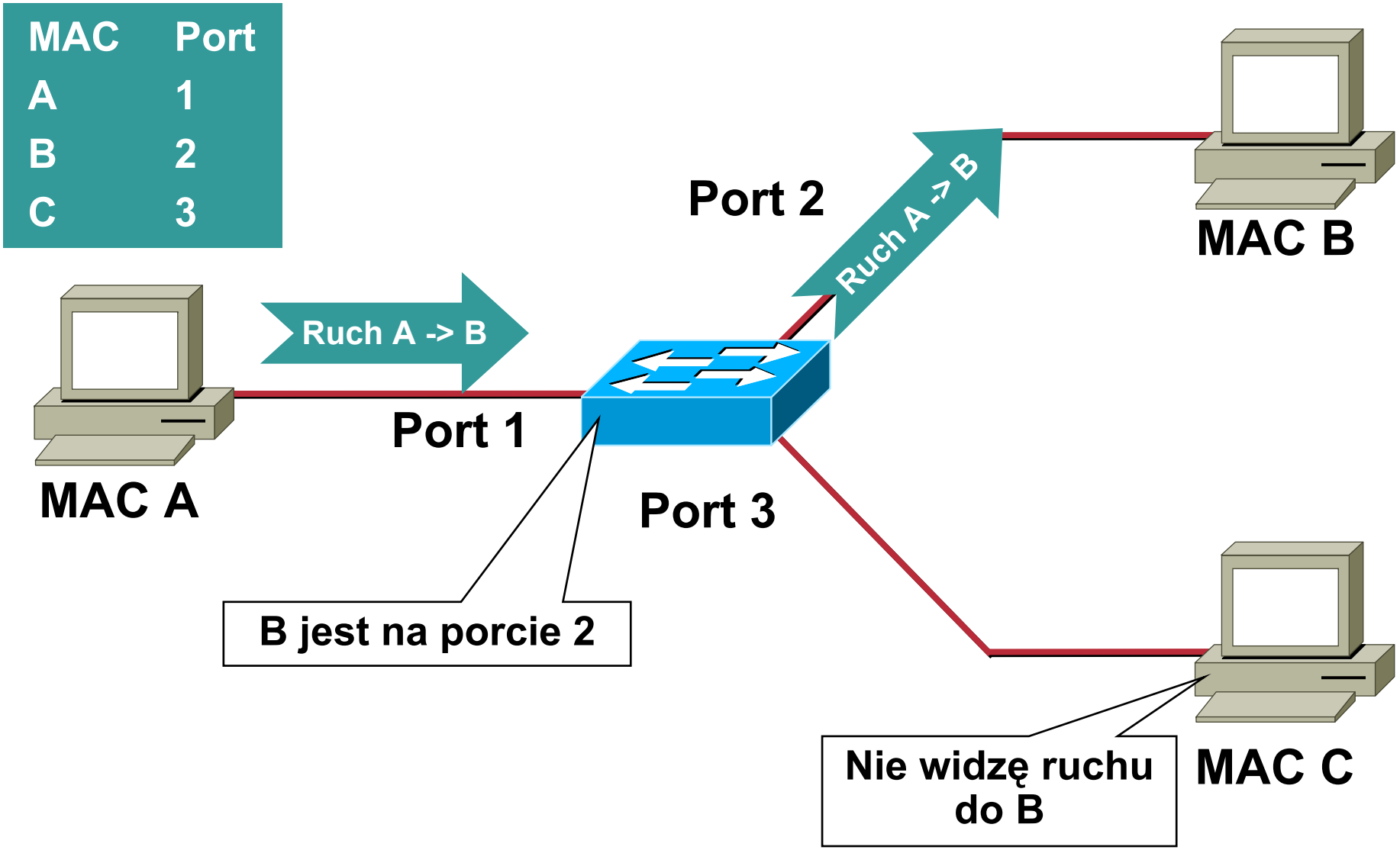
Zachowanie normalne



Zachowanie normalne



Zachowanie normalne



Przepełnienie pamięci podręcznej

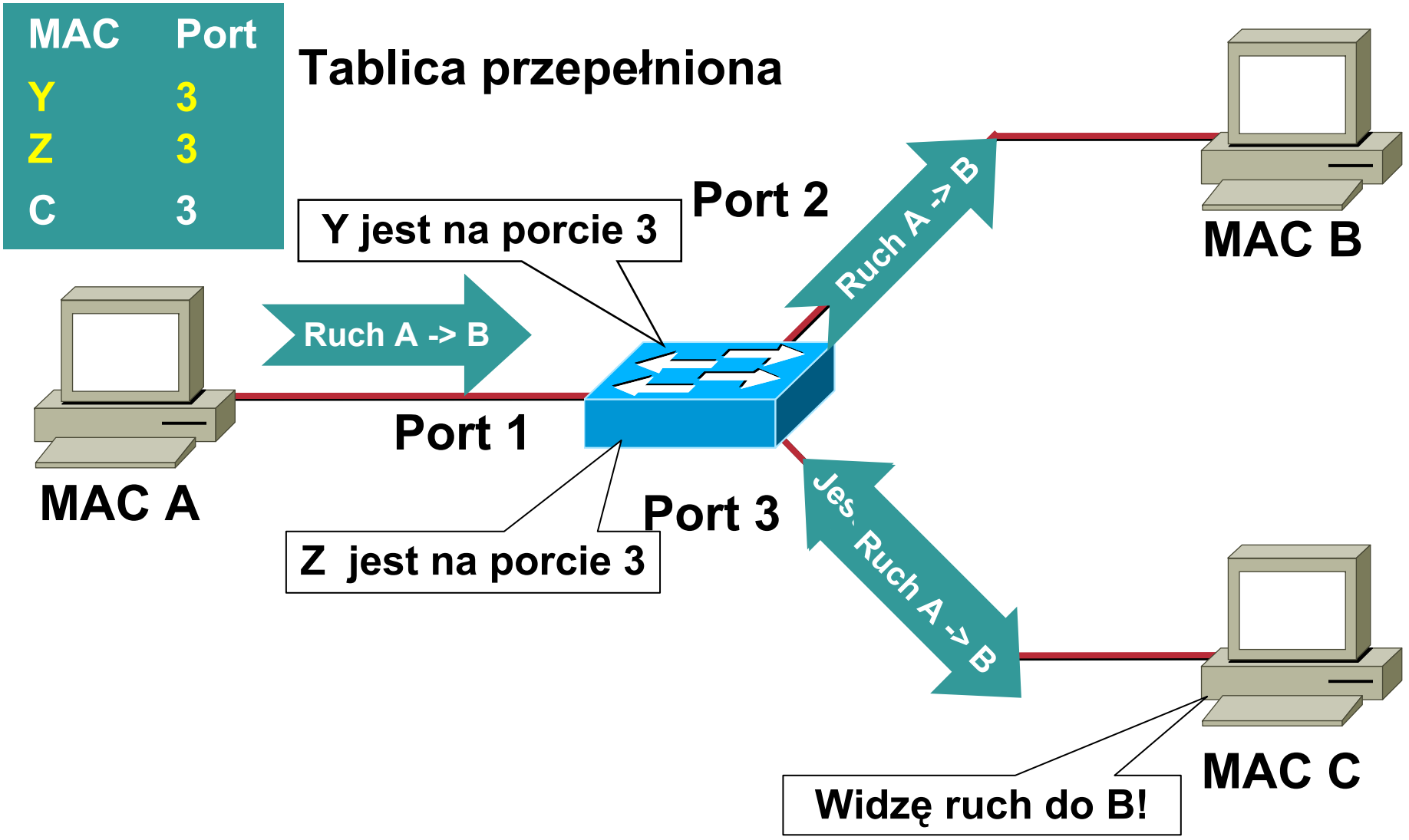
- **macof - od 1999**

  około 100 linijek w Perlu

  inne narzędzie – dsniff, korzysta z niego

- **Atak opiera się o przepełnienie zawartości pamięci podręcznej przełącznika**

Przepełnienie pamięci podręcznej



Atak przy użyciu 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
```

- **...wysyłamy pakiety z losowymi adresami MAC i IP**

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

- **Do pobrania z:**

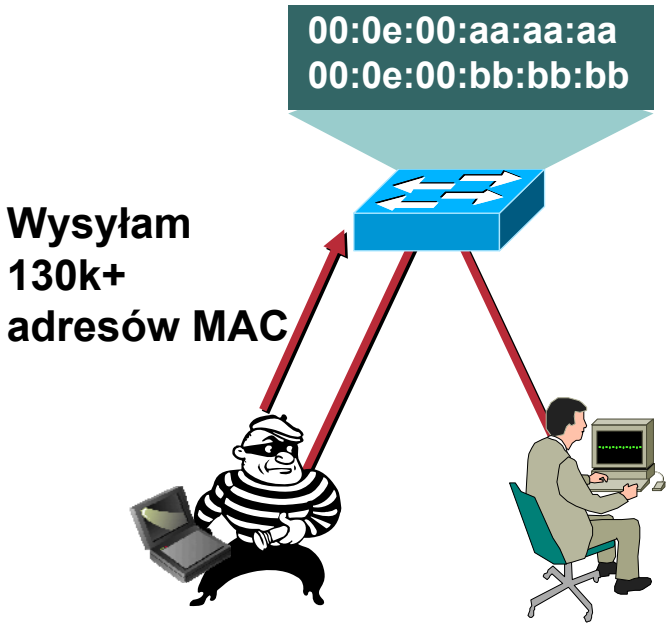
  http://monkey.org/~dugsong/dsniff/

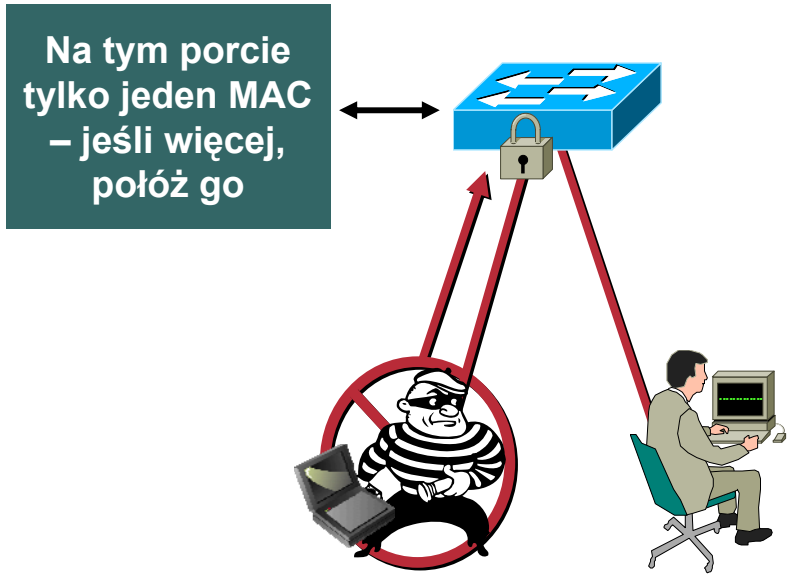
Po przepełnieniu tablicy:

- Ruch do wpisów nieistniejących jest wysyłany na wszystkie porty
- ...zamiast przełącznika = hub
- Dodatkowo, atak ‘przelewa’ się na sąsiednie przełączniki

Obrona

Wykorzystanie funkcjonalność ‘port security’ i PrivateVLAN przełącznika – ograniczenie ilości adresów MAC per port i zamknięcie stacji użytkownika z portem L3 (routera)

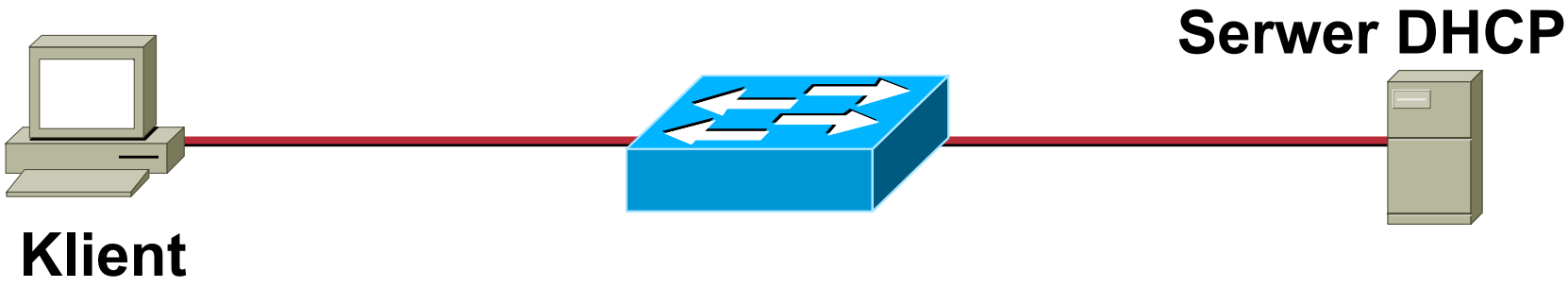




Dodatkowo: arpwatch, wykrywanie adresów IP spoza używanych pól itp.

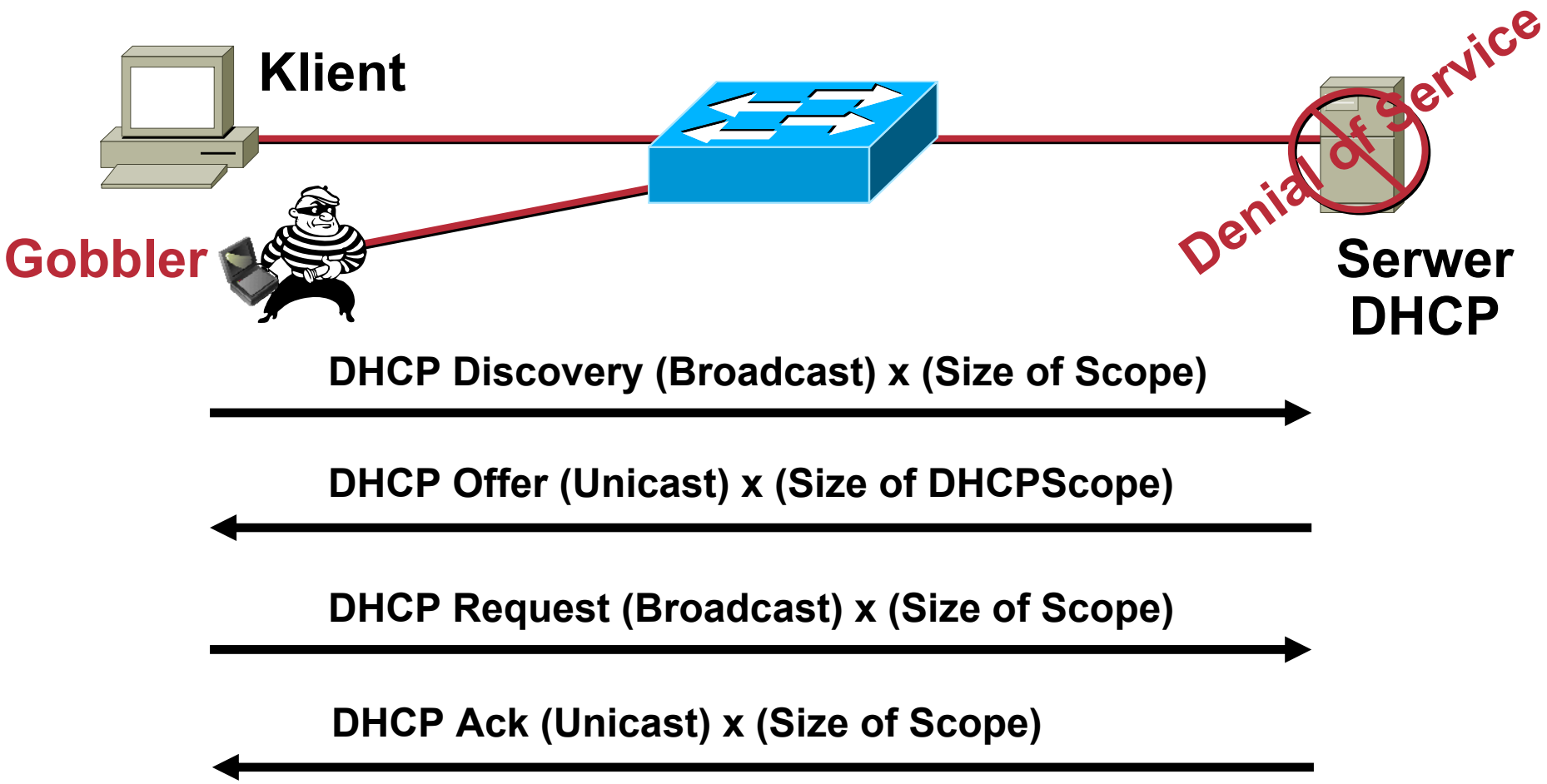
ATAKI DHCP

Jak działa DHCP (z lotu ptaka)?



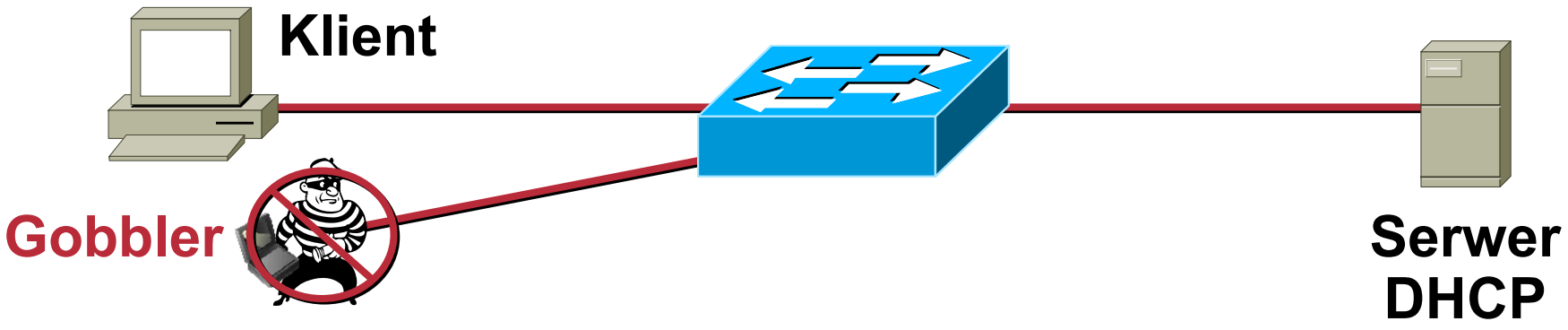
- DHCP jest opisane w RFC 2131

Atak na DHCP - DoS



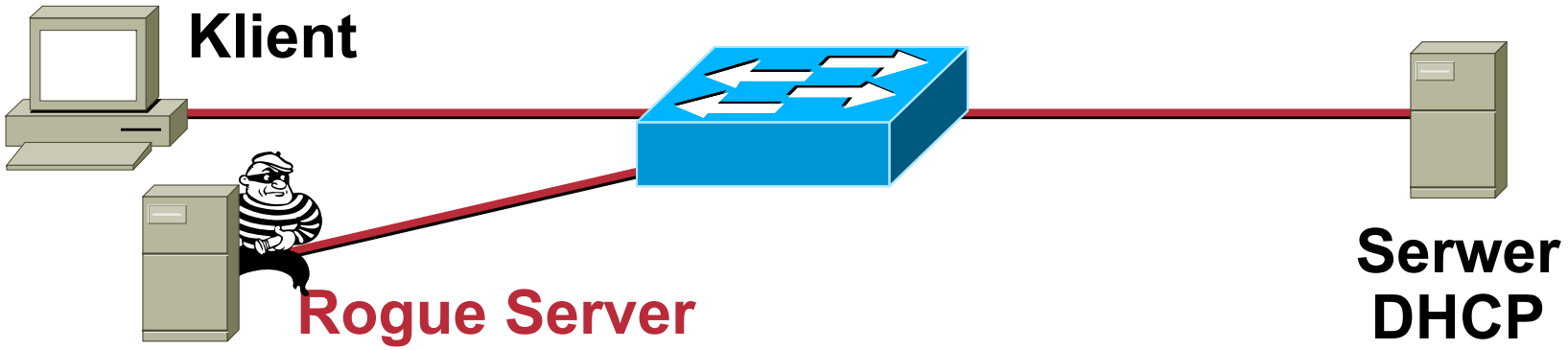
- Gobbler stara się uzyskać od serwera DHCP wszystkie możliwe IP
- Tradycyjny DoS – żadna inna stacja nie będzie się już mogła do sieci dołączyć

Atak na DHCP - obrona



- W każdym pakiecie REQUEST, Gobbler używa innego MACa
- Funkcjonalność ‘port security’ pozwala zatem ponownie się obronić – z jednego portu nie więcej niż X źródłowych MACów
- ...czy pamiętamy o oglądaniu logów z serwera DHCP?

Atak na DHCP – podstawiony serwer



DHCP Discovery (Broadcast)

DHCP Offer (Unicast) z podstawionego serwera

DHCP Request (Broadcast)

DHCP Ack (Unicast) z podstawionego serwera

Atak na DHCP – podstawiony serwer

- **Co możemy ‘zaserwować’?**

Adres IP: 10.10.10.101
Maska: 255.255.255.0
Domyślny router: 10.10.10.1
Serwery DNS: 192.168.10.4, 192.168.10.5
Czas wygaśnięcia: 10 dni

...i inne – np. serwery dla telefonów IP, z których mają pobrać firmware(!)

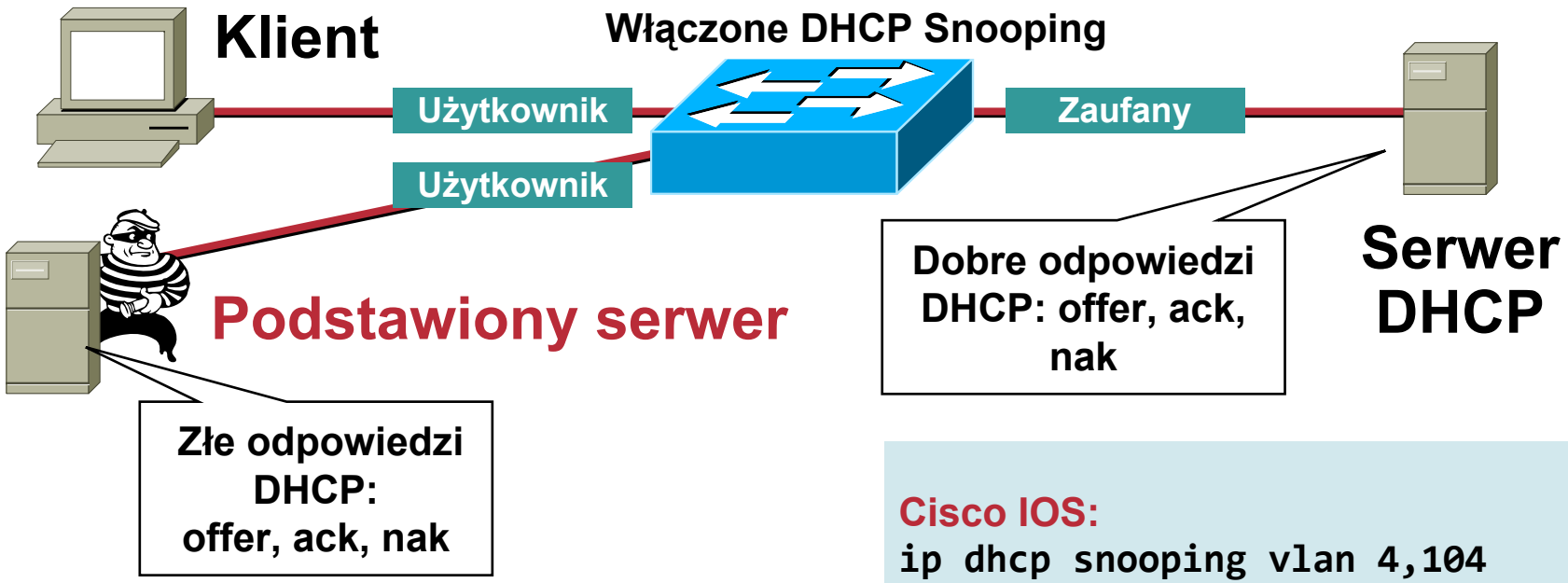
- **Jak to wykorzystać?**

Podstawiona domyślna bramka — atakujący widzi ruch poza podsieć

Podstawiony serwer DNS — atakujący fałszuje rekordy

Podstawione IP — wszyscy dostają np. ten sam (DoS)

Obrona przed podstawionym serwerem



- Inne potencjalne rozwiązania:

  każdy użytkownik = interfejs L3 z routera

Cisco IOS:

```
ip dhcp snooping vlan 4,104
ip dhcp snooping
interface fastethernet 0/6
 description Port uzytkownika
 no ip dhcp snooping trust
 ip dhcp snooping limit rate 10
interface fastethernet 0/24
 description Port serwera
 ip dhcp snooping trust
```

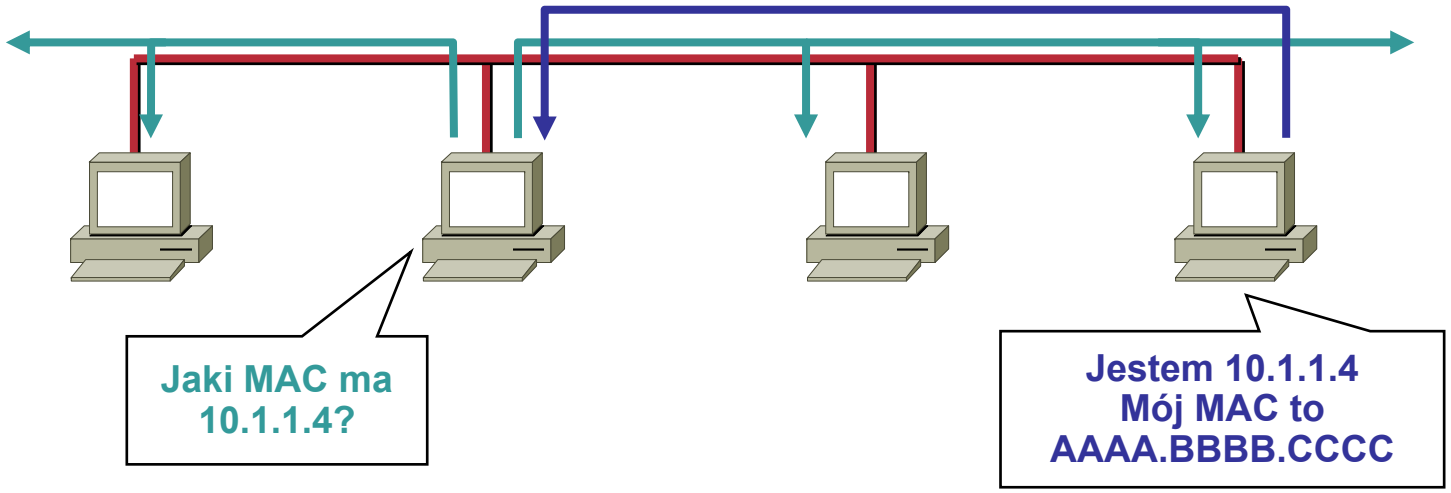
ATAKI ARP

Co to jest i jak działa, ARP?

- Zanim stacja korzystająca z Ethernetu będzie mogła porozmawiać z inną stacją, musi zapytać przez ARP (Address Resulution Protocol) o mapowanie IP<>MAC

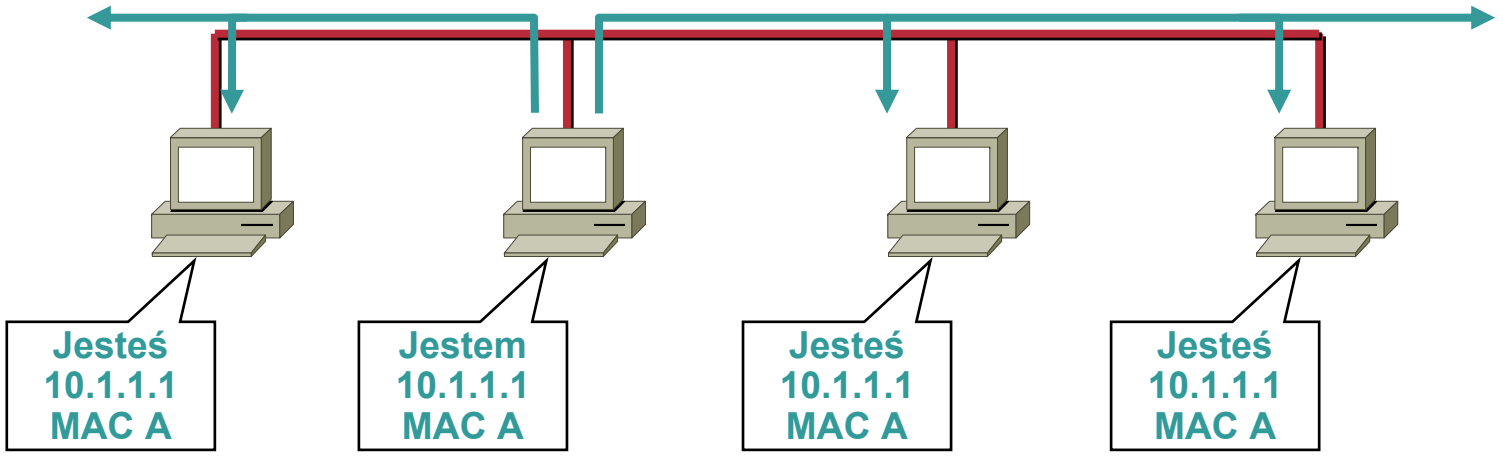
  protokół numer 0x0806

- Ramka jest broadcastem – wszystkie komputery ją słyszą, ale tylko ‘właściwy’ powinien odpowiedzieć



Co to jest i jak działa, ARP?

- Zgodnie z RFC, klient może wysłać odpowiedź w imieniu innego hosta, lub nawet nie pytany
- Każdy może stwierdzić, że jest dowolną kombinacją IP/MAC
- ...dzięki czemu można przekierować ruch



„ARP Attack”

- **Popularne narzędzia, pozwalające na ‘fajne rzeczy’:**

  dsniff—http://monkey.org/~dugsong/dsniff/

  ettercap—http://ettercap.sourceforge.net/index.php

  Cain&Abel - http://www.oxid.it/cain.html

  yersinia - http://www.yersinia.net/

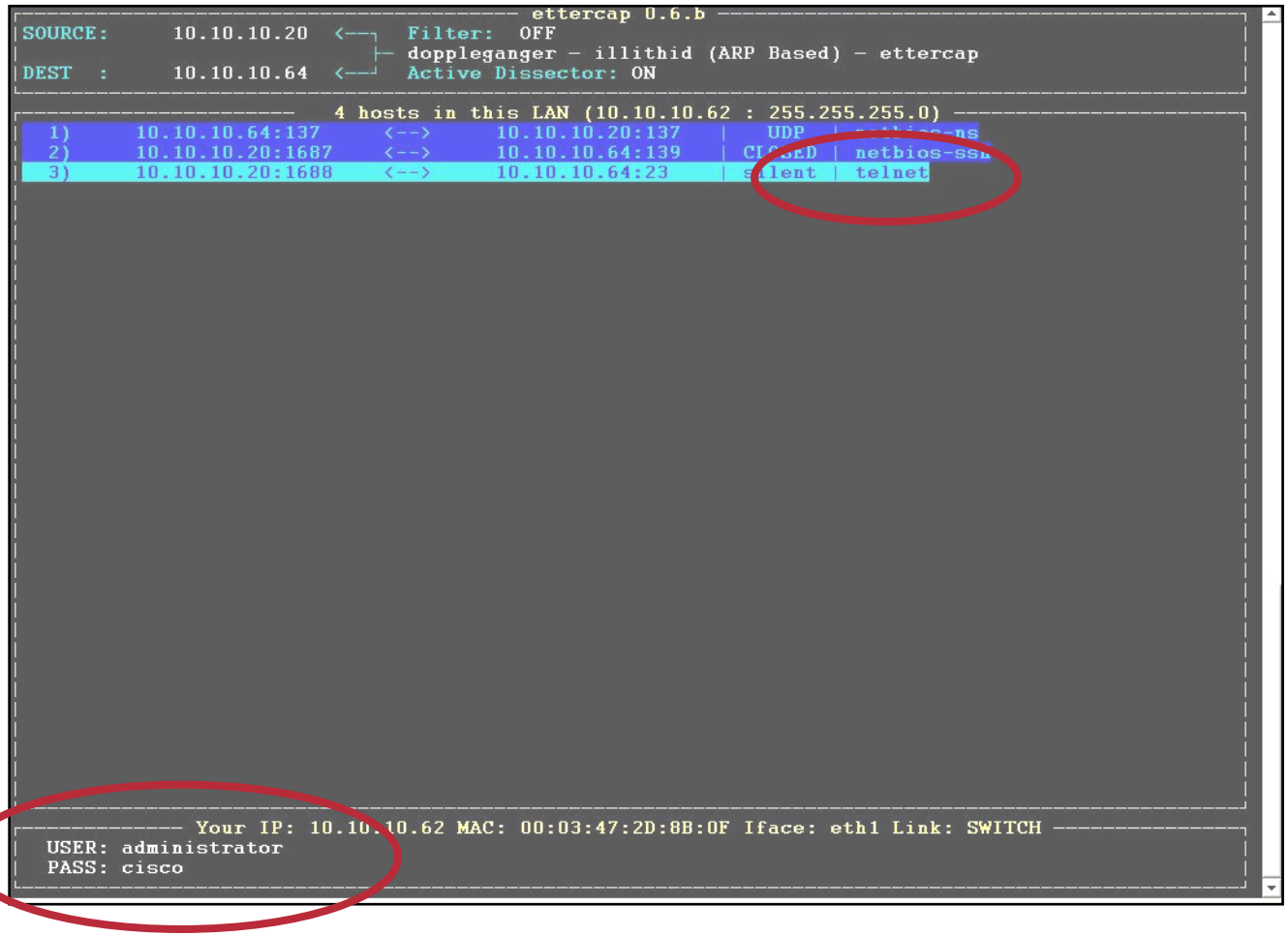
- **Możliwości przechwytywania i odszyfrowywania haseł dla protokołów:**

  FTP, Telnet, SMTP, HTTP, POP, NNTP, IMAP, SNMP, LDAP, RIP, OSPF, PPTP, MS-CHAP, SOCKS, X11, IRC, ICQ, AIM, SMB, Microsoft SQL

- **Możliwość ataków na niezabezpieczone protokoły L2/L3 – Spanning Tree, Rapid Spanning Tree, CDP, HSRP itp.**

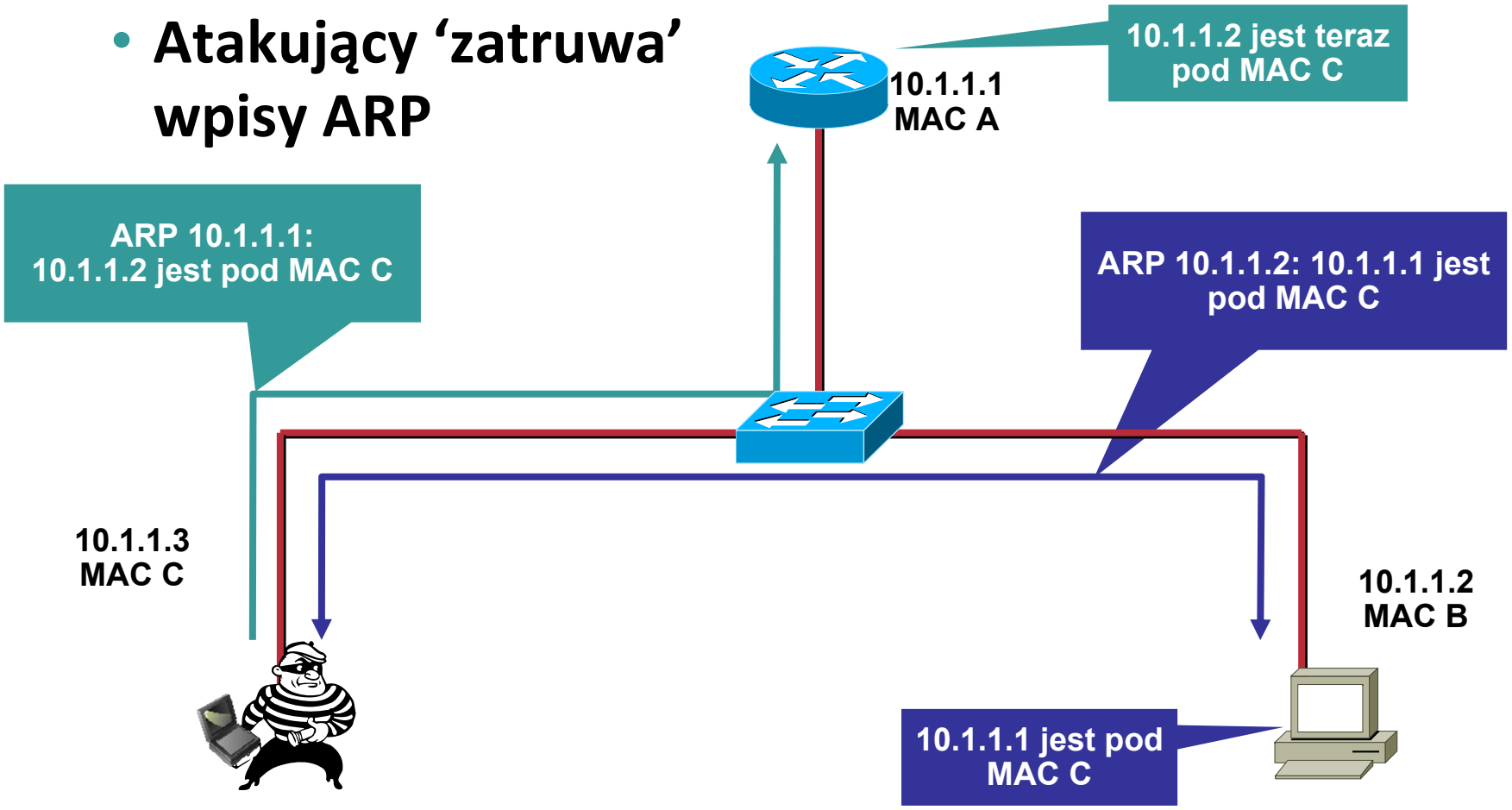
„ARP Attack”

- Przykładowe przechwycenie hasła w sesji telnet
- Ettercap podszywa się pod ofiarę i serwer, ale przekazuje ruch pod właściwe adresy MAC (żeby utrzymać sesję)



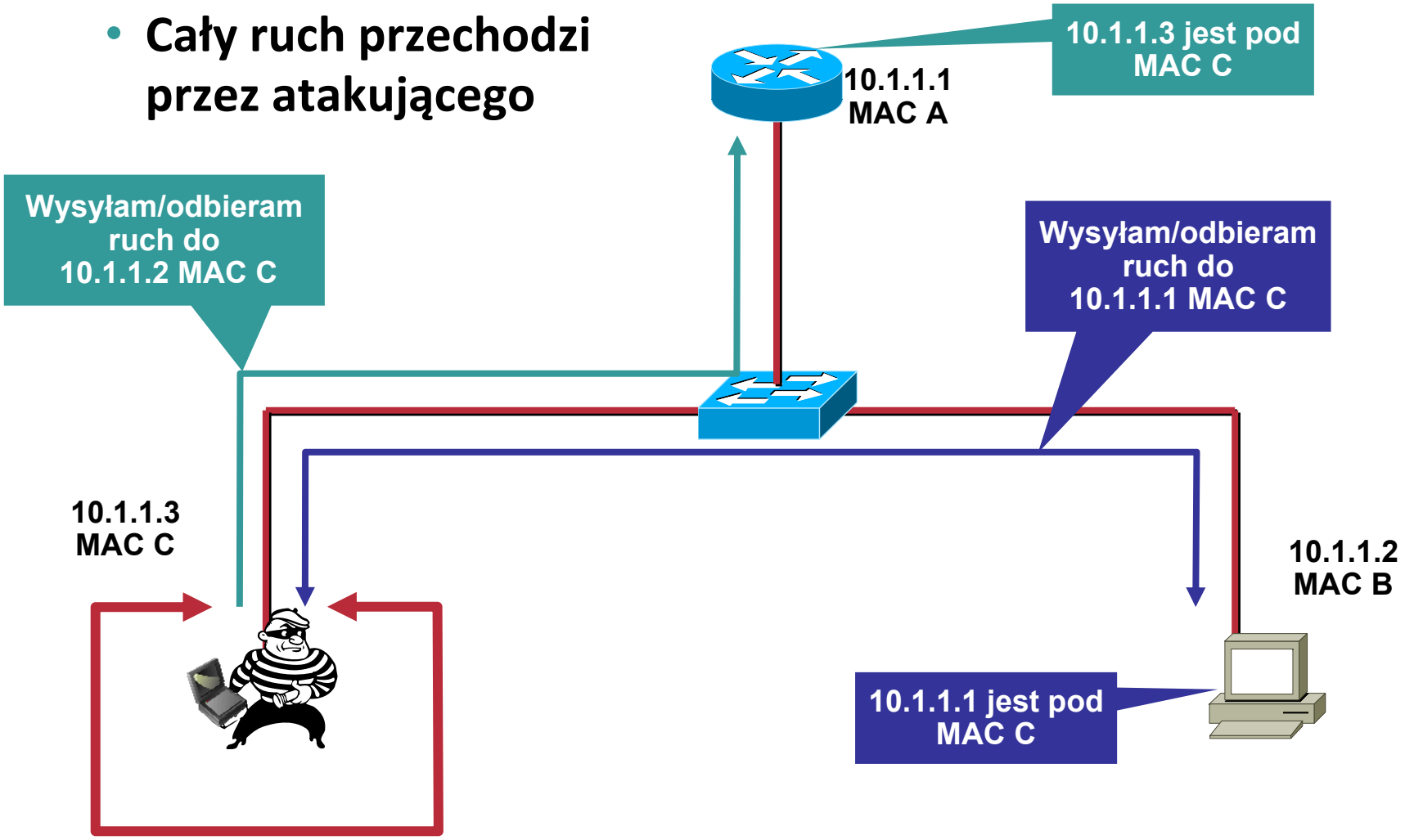
Jak to działa?

- Atakujący ‘zatruwa’ wpisy ARP



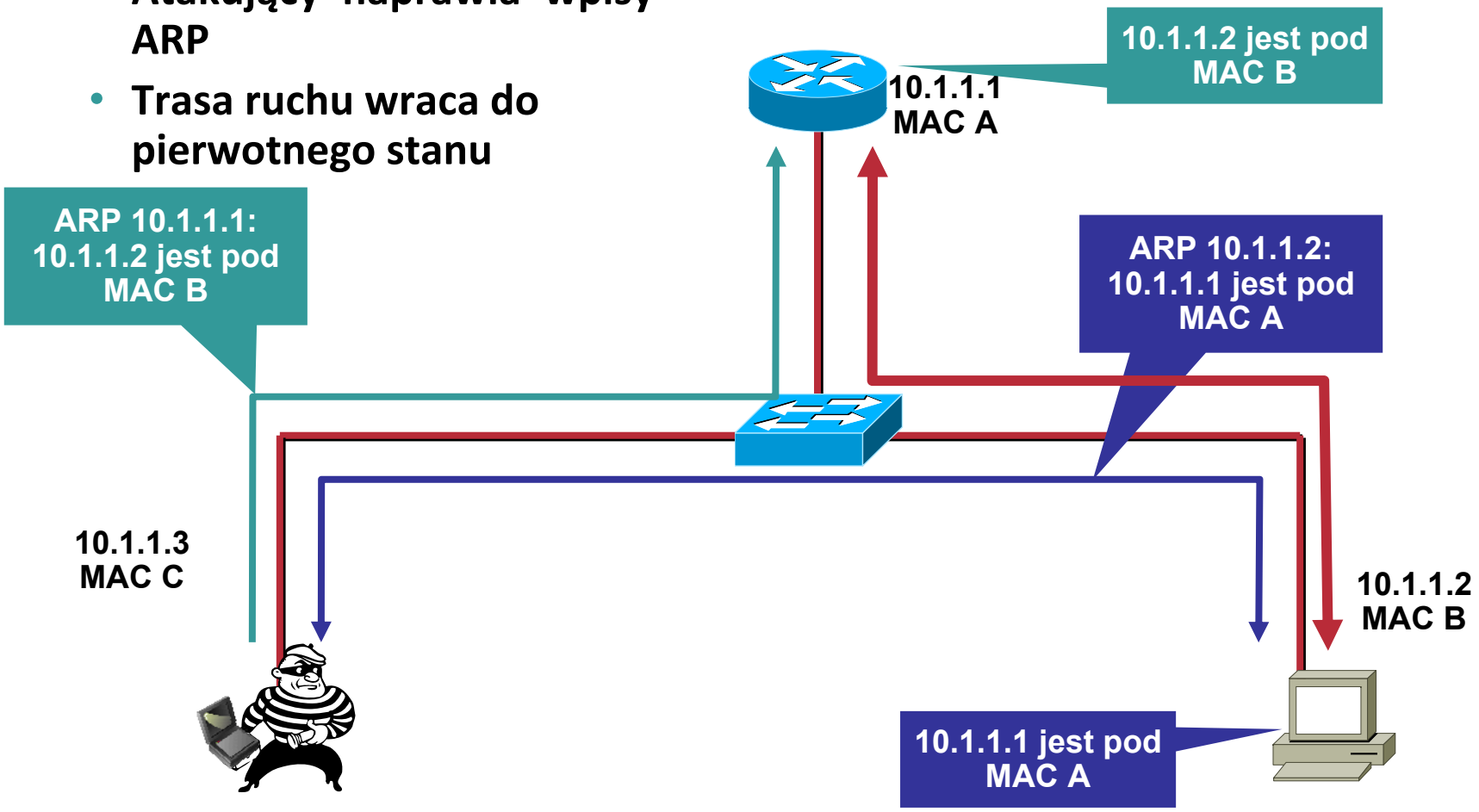
Jak to działa?

- Cały ruch przechodzi przez atakującego

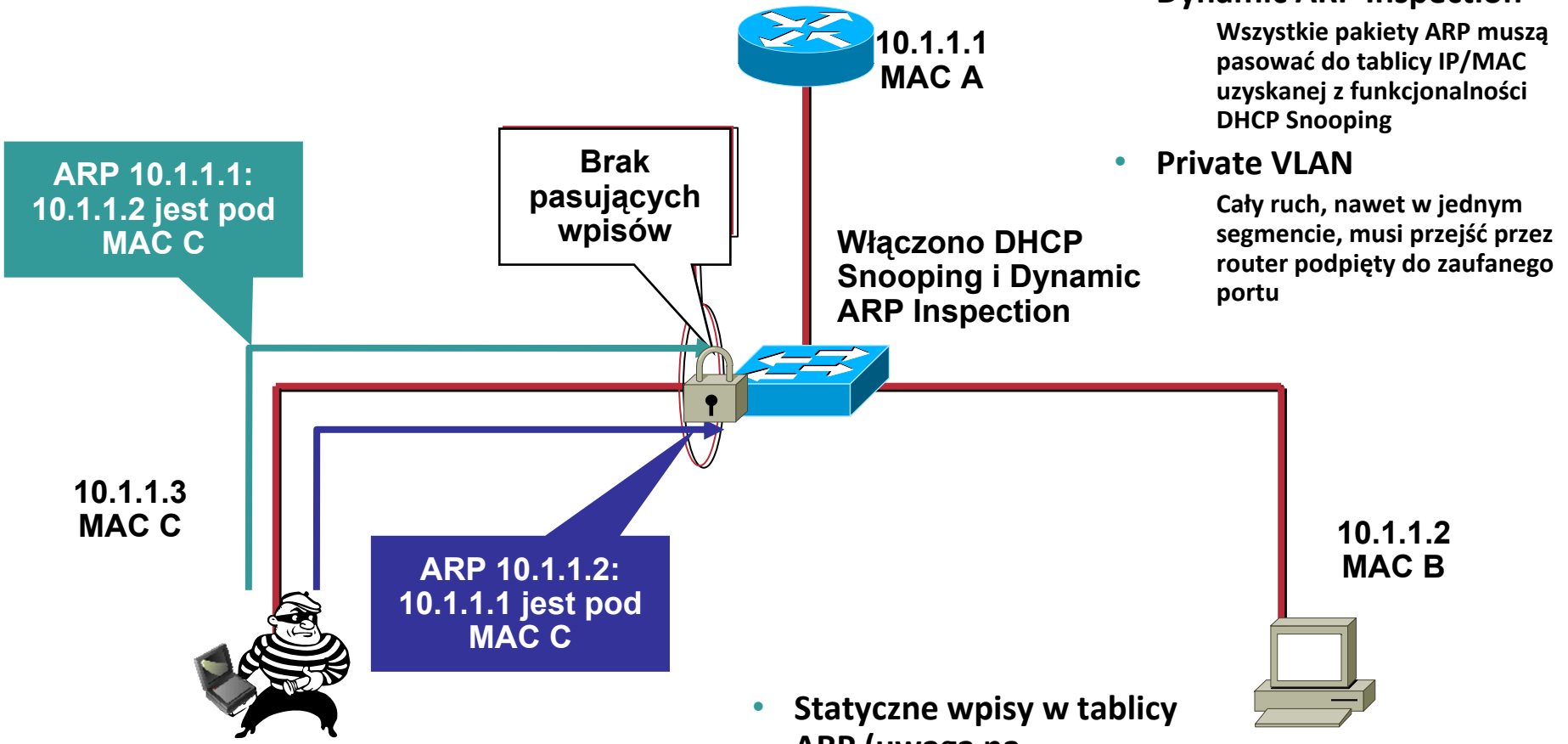


Posprzątamy...

- Atakujący ‘naprawia’ wpisy ARP
- Trasa ruchu wraca do pierwotnego stanu



Jak się bronić przed atakiem ARP?

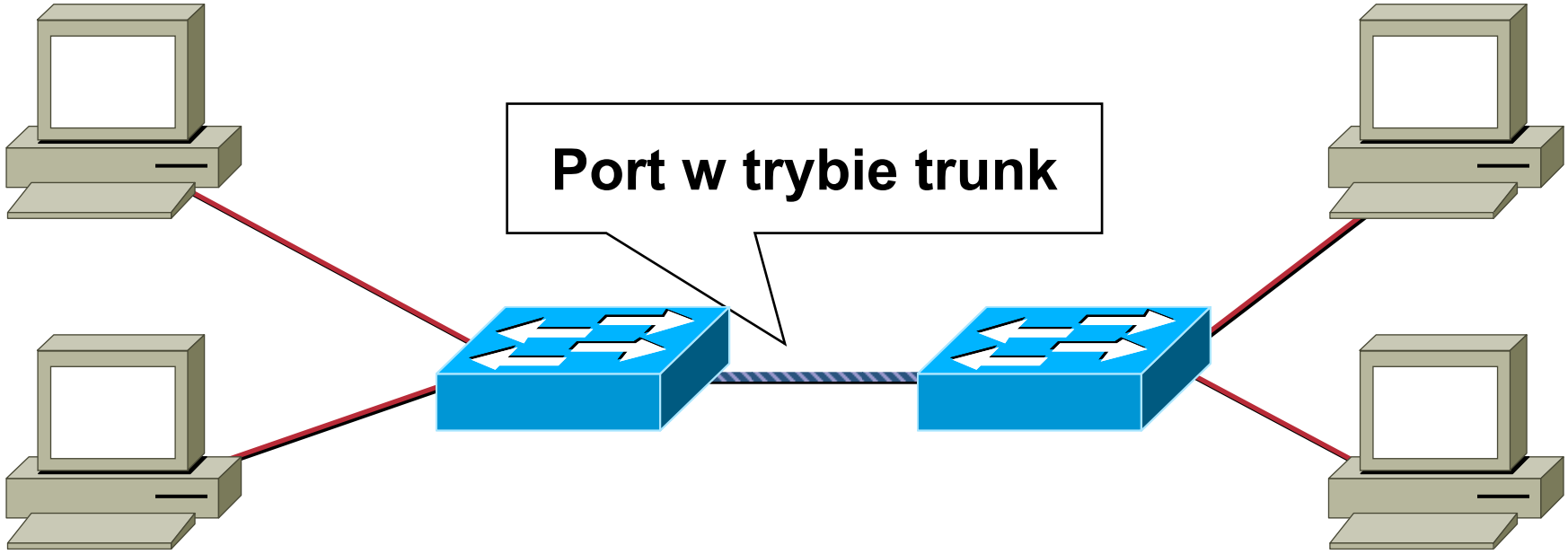


- **Dynamic ARP Inspection**
  - Wszystkie pakiety ARP muszą pasować do tablicy IP/MAC uzyskanej z funkcjonalności DHCP Snooping
- **Private VLAN**
  - Cały ruch, nawet w jednym segmencie, musi przejść przez router podpięty do zaufanego portu

- **Statyczne wpisy w tablicy ARP (uwaga na Windowsy...)**

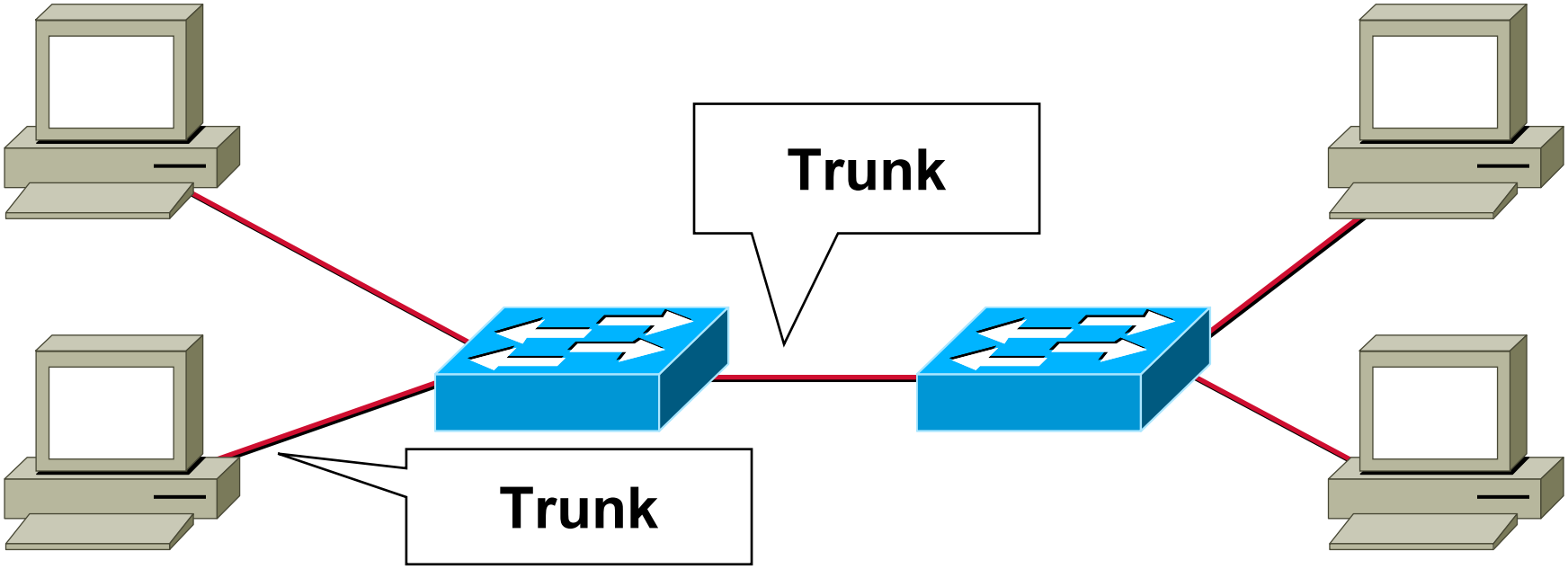
VLAN HOPPING

Czym jest trunk?



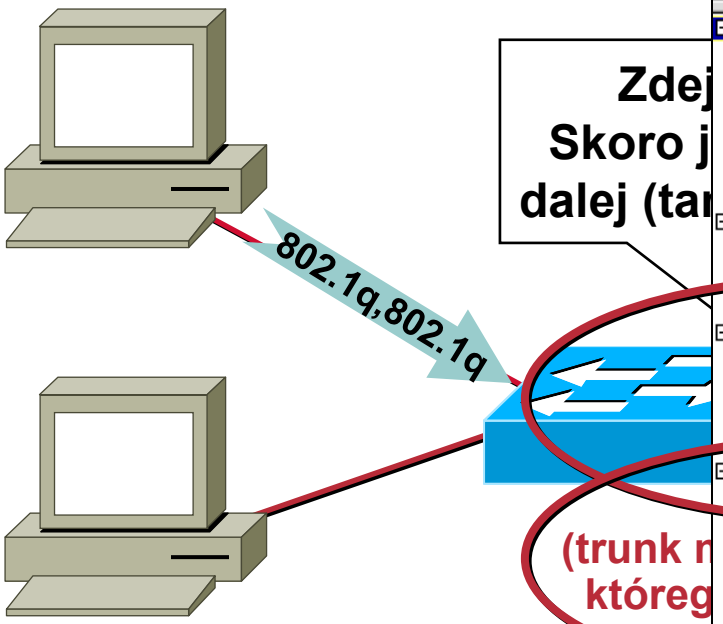
- **Porty trunk przenoszą tagowane ramki dla VLANów**
  - **domyślnie przenoszą wszystkie VLANy**
- **Standardem połączeń trunk jest IEEE 802.1Q, jest jeszcze Cisco ISL**

Jak przenieść ruch pomiędzy VLANami bez routera?



- Stacja końcowa może udawać przełącznik z portem trunk – innymi słowy, wysyłać otagowane ramki (podwójnie)
- yersinia ma przygotowany atak tego typu

Atak VLAN hopping



Zdej
Skoro j
dalej (tar

(trunk n
któreg

No.	Time	Source	Destination	Protocol	Info
1	0.000000	1.2.3.9	1.2.3.4	ICMP	Echo (ping) request

```
Frame 1 (64 on wire, 64 captured)
    Arrival Time: Jul 27, 2002 19:40:39.934687000
    Time delta from previous packet: 0.000000000 seconds
    Time relative to first packet: 0.000000000 seconds
    Frame Number: 1
    Packet Length: 64 bytes
    Capture Length: 64 bytes
Ethernet II
    Destination: 00:03:47:b9:6f:ae (Intel_b9:6f:ae)
    Type: 802.1Q Virtual LAN (0x8100)
802.1q Virtual LAN
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0000 0000 0001 = ID: 1
    Type: IP (0x0800)
802.1q Virtual LAN
    111. .... .... .... = Priority: 7
    ...0 .... .... .... = CFI: 0
    .... 0000 0000 0010 = ID: 2
    Type: IP (0x0800)
    Trailer: 0000000000000000000081C1A10F
Internet Protocol, Src Addr: 1.2.3.9 (1.2.3.9), Dst Addr: 1.2.3.4 (1.2.3.4)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 28
    Identification: 0x00f2
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (0x01)
    Header checksum: 0x71df (correct)
    Source: 1.2.3.9 (1.2.3.9)
    Destination: 1.2.3.4 (1.2.3.4)
⊞ Internet Control Message Protocol
```

- **Wysyłamy podwójnie**

  czasami działa tagowa

- **Ruch tylko w jedną st**

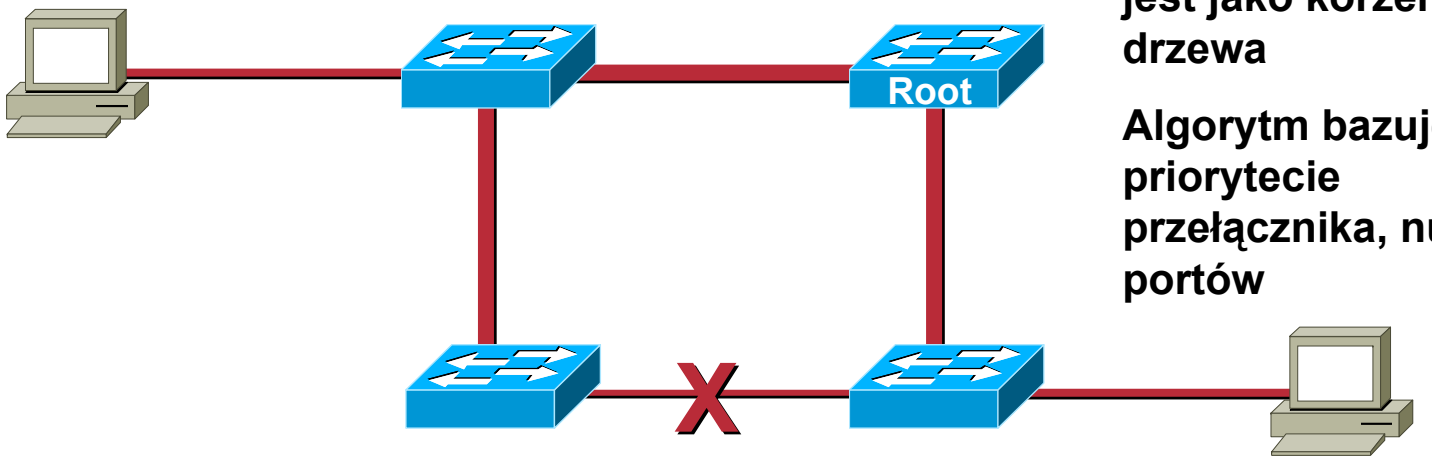
Jak sobie z tym radzić?

- Używaj unikalnego VLAN ID dla portów, które są trunkami
- Wyłącz nieużywane porty i wrzuć je do nieużywanego VLANu
- Unikaj VLANu 1 – do czegokolwiek
- Na portach które mają być tagowane – ustaw to na sztywno, dla konkretnej listy VLANów
- Porty dostępowe ustaw w tryb dostępowy

IEEE SPANNING TREE

Po co nam Spanning Tree?

- Zapewnić topologię bez pętl w warstwie drugiej ISO



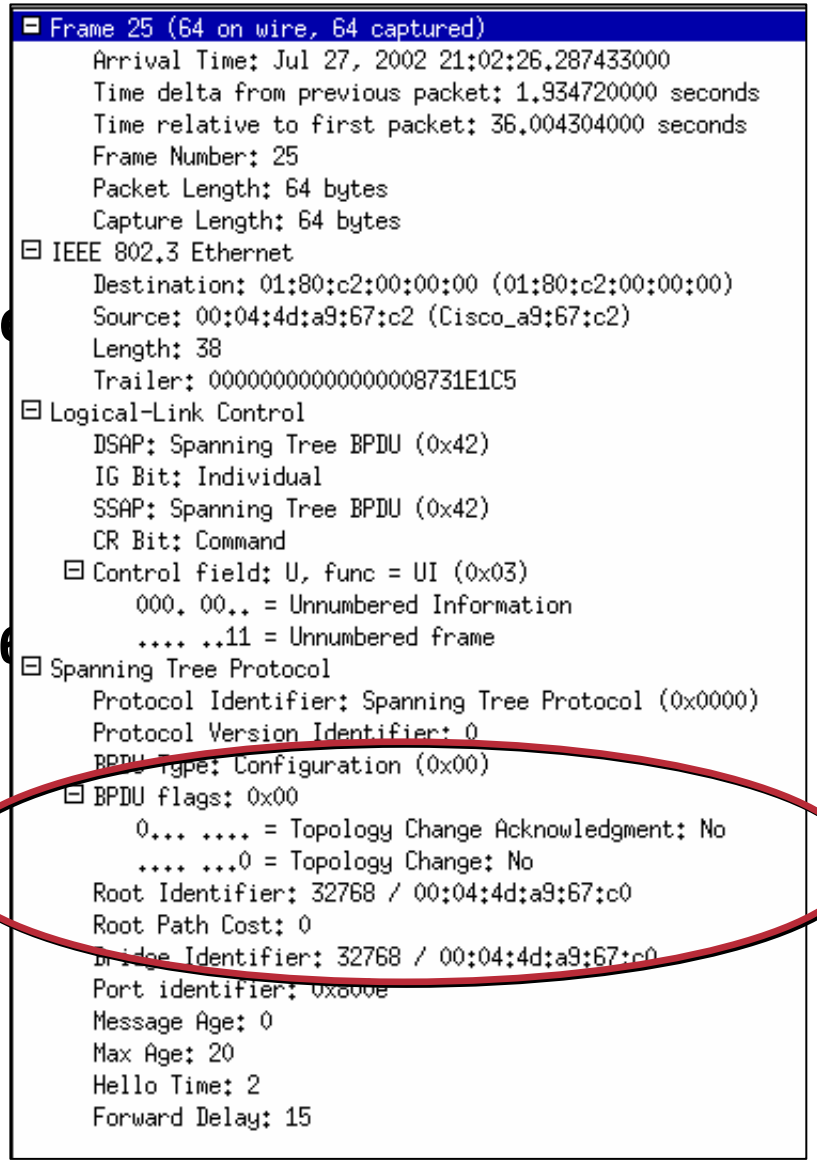
Przełącznik wybierany jest jako korzeń drzewa

Algorytm bazuje na priorytecie przełącznika, numerze portów

- STP jest bardzo proste – przesyła dane w ramkach Bridge Protocol Data Units (BPDU), podstawowe typy to: Configuration BDPU, Topology change notification/ack (TCN/TCA)
- Ramki Ethernet nie mają pola TTL znanego z IP – mogłyby krążyć wiecznie, a broadcasty z czasem stawałyby się sztormami

Przykład ataku na Spanning Tree

- **Warunek: dwa interfejsy sieciowe do dwóch różnych przełączników, lub podpięcie do koncentratora**
- **Wysyłamy odpowiednio spreparowane BPDU:**
  - **niski priorytet (domyślnie 327**



Przykład ataku na Spanning Tree

- **Widzimy ramki, których nie powinniśmy:**
  - **możliwe stają się ataki typu MITM, DoS itp. – trudne lub niemożliwe do wykrycia przez użytkowników podłączonych do przełączników**
  - **trzeba zapewnić odpowiednią wydajność stacji, która ma przenosić ruch (i poza atakiem DoS, a wszczególności dla MITM, trzeba go przenosić!)**

Jak sobie radzić?

- Jeśli się da – projektuj sieci bez pętl w L2 ☺
- Nie wyłączaj STP w sytuacjach z pętlami/potencjalnymi pętlami – jej powstanie i tak spowoduje ‘samoczynny’ atak DoS
- Parę rozwiązań, w zależności od producenta:
  - Cisco: BPDU guard, BPDU filter, Root Guard
  - Inni producenci: zwykle jeśli już, filtr dla BPDU
- Na interfejsie routera Linux/BSD ustawionym w tryb PROMISC, wykrycie ramki BPDU oznacza jedną z dwóch rzeczy:
  - ktoś podłączył przełącznik żeby ‘rozdzielić’ Internet
  - ktoś bawi się narzędziami, którymi nie powinien...

Podsumowanie – ataki L2

- **Wiele problemów rozwiązuje wdrożenie 802.1X**
  - **brak darmowych supplicantów dla starszych systemów Win***
  - **‘problematyczność’ w sieciach osiedlowych – po pierwsze klienci, po drugie zarządzalny przełącznik z funkcjonalnością 802.1X**
- **Samo PPPoE jest możliwe do przejęcia i potencjalnie* możliwe do zaatakowania, jeśli przełącznik nie da się zabezpieczyć**
  - **w szczególności kwestia wynegocjowania CHAP->PAP rozwiązuje wiele problemów ☺**
  - **brak darmowych klientów PPPoE dla starszych systemów Win***
- **Skompromitowane L2 = brak kontroli w wyższych**

ATAKI L3

Ataki L3

- **DoS urządzenia:**

  dziury w usługach (SNMP, Telnet/SSH, HTTP/HTTPS etc.) i protokołach firmowych (CDP/VTP/etc.)

  śmieciowy ruch wprost na IP urządzenia jeśli przetwarzaniem zajmuje się CPU (99% ogólnodostępnych rozwiązań)

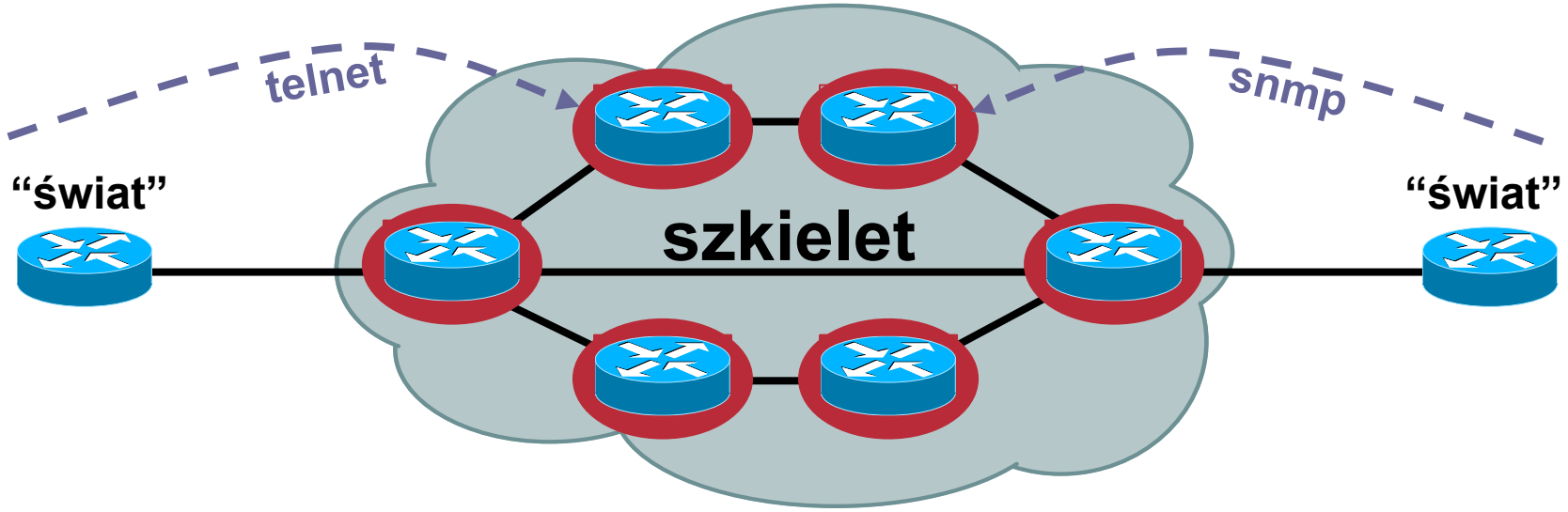
- **Przechwytywanie/wstrzykiwanie ruchu:**

  ataki na protokoły routingu dynamicznego

  błędy/luki w filtrowaniu pakietów

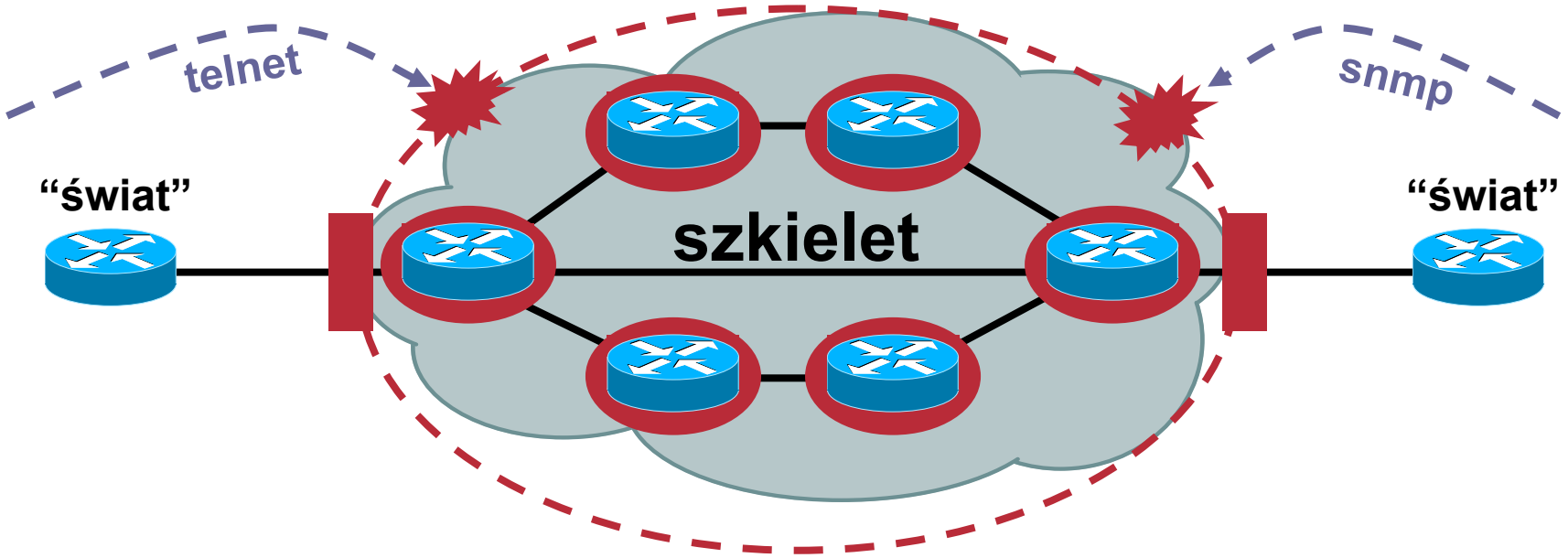
  spoofing

Stary sposób myślenia o sieciach IP



- Każdy z routerów zabezpieczony osobno
- ...ale każdy osiągalny z zewnątrz

Nowy, zalecany sposób – obrona warstwowa



- Każdy z routerów nadal zabezpieczony

  ...ale obecna również ochrona infrastruktury

- Routery/infrastruktura niedostępna z zewnątrz

Przygotować sieć – co robić?

- **Zabieraj włamywaczowi opcje**
  - Filtruj ruch wchodzący i wychodzący
  - Zastosuj mechanizm uRPF – uniemożliwiając spoofing IP
  - Filtrowanie zgodnie z RFC2827
  - Na stykach BGP z operatorem – filtruj otrzymywane prefiksy, filtruj wysyłane prefiksy
- **Baw się, analizując ataki prowadzone codziennie**
  - Co sieć robi normalnie? Czym szczególnym różni się w trakcie ataku?
  - Analiza i korelacja logów, współpraca, trenowanie

Jeszcze raz - co wynika z BCP 38 (RFC2827)?

- **Filtruj tak blisko brzegu jak możesz – idealnie, dla każdego użytkownika osobna /30 lub /31 na logicznej instancji interfejsu z włączonym uRPFem**
- **Filtruj tak dokładnie jak się da**
- **Filtruj zarówno adresy źródłowe jak i docelowe, ruch wchodzący i wychodzący**

  ...w granicach rozsądku oczywiście

BGP Blackholing

- **Użyj iBGP pomiędzy routerami wewnętrznymi**

  każdy z nich powinien mieć odpowiednią route-mapę pozwalającą zaznaczony ustalonym community prefix skierować do /dev/null (sprawdź to!)

  każdy z nich powinien mieć włączony uRPF – odrzucać ruch zarówno do jak i z prefiksu

  sesje zabezpiecz MD5 lub IPsec

- **Dwa zastosowania:**

  odrzuć ruch, nie dbając co to było – większość DoSów

  skieruj ruch do specjalnej stacji – ze stale włączonym tcpdumpem na docelowym interfejsie – pozwala zanalizować co to był za ruch, jaki trojan, skąd przyszedł i jak dokładnie chciał zaatakować zasoby

Protokoły routingu wewnętrznego

- **Protokoły IGP, jeśli nie oddzielono ruchu użytkowników od ruchu ‘administracyjnego’ mogą zostać zaatakowane – świadomie bądź nie**
- **Zwykle relatywnie łatwo atakuje się niezabezpieczone sesje routingu RIP czy OSPF**
  - **Sąsiedzi sygnalizują sobie przecież stan**
  - **Router może nie przeżyć odpowiednio zniekształconego pakietu**
  - **Algorytm maszyny stanów protokołu routingu może nie przewidywać nieoczekiwanych zachowań**

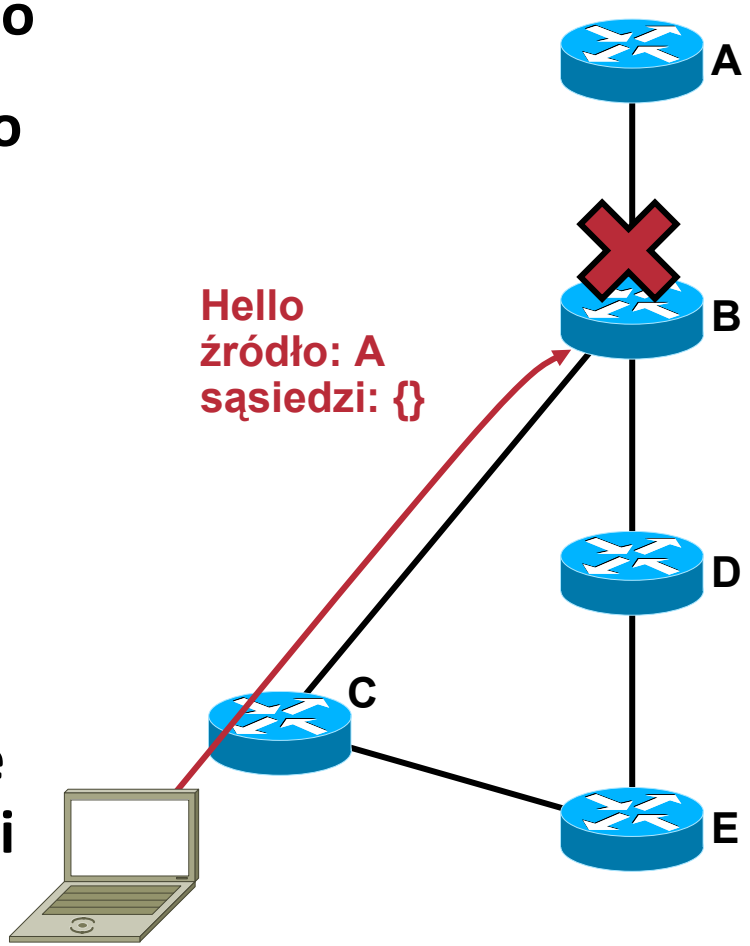
Przykład - OSPF

- Można zresetować sąsiedztwo
- Atakujący wysyła pakiet Hello do routera B

  ...w źródle ustawiając adres routera A

- B otrzymując pakiet zrywa sesję z A

- Inny przykład: zniekształcone LSA ze sfałszowanymi danymi nadawcy

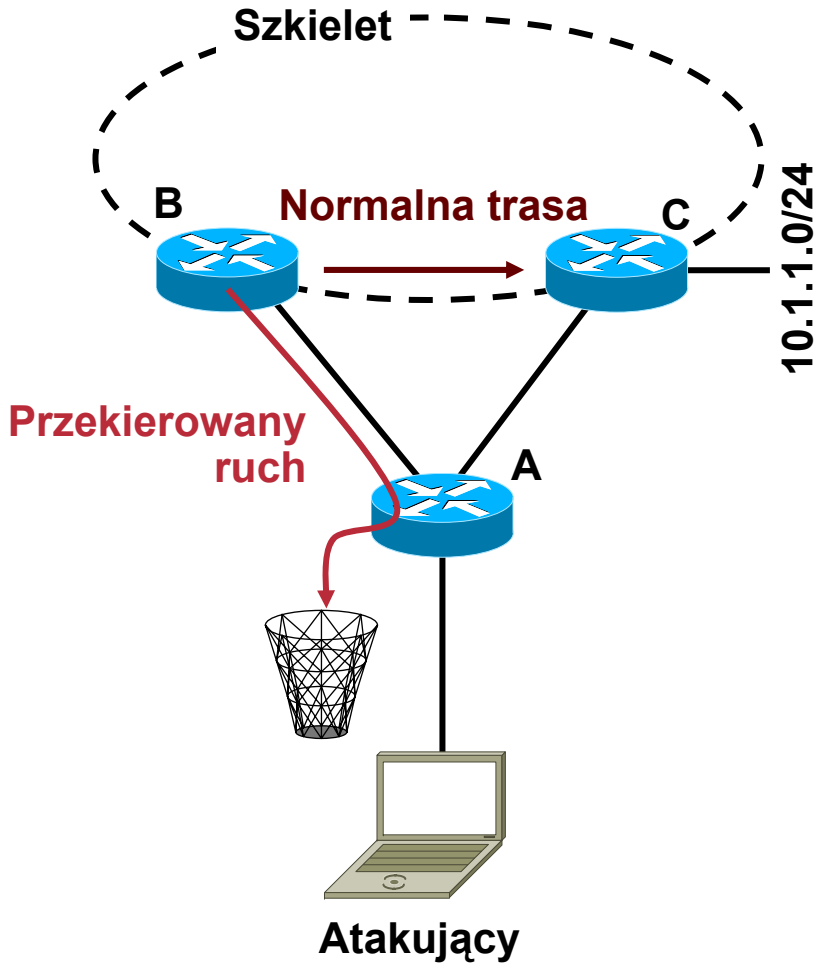


Przykład ataku na zawartość tablic routingu

- Atakujący przekierowuje (np. na siebie) ruch do konkretnego (atakowanego) zasobu

  ...wykorzystując dokładniejszą ścieżkę – np. z maską /32 (jeden host)

- Ruch nie dociera do właściwej lokalizacji – DoS, oraz mozliwość zebrania poufnych danych

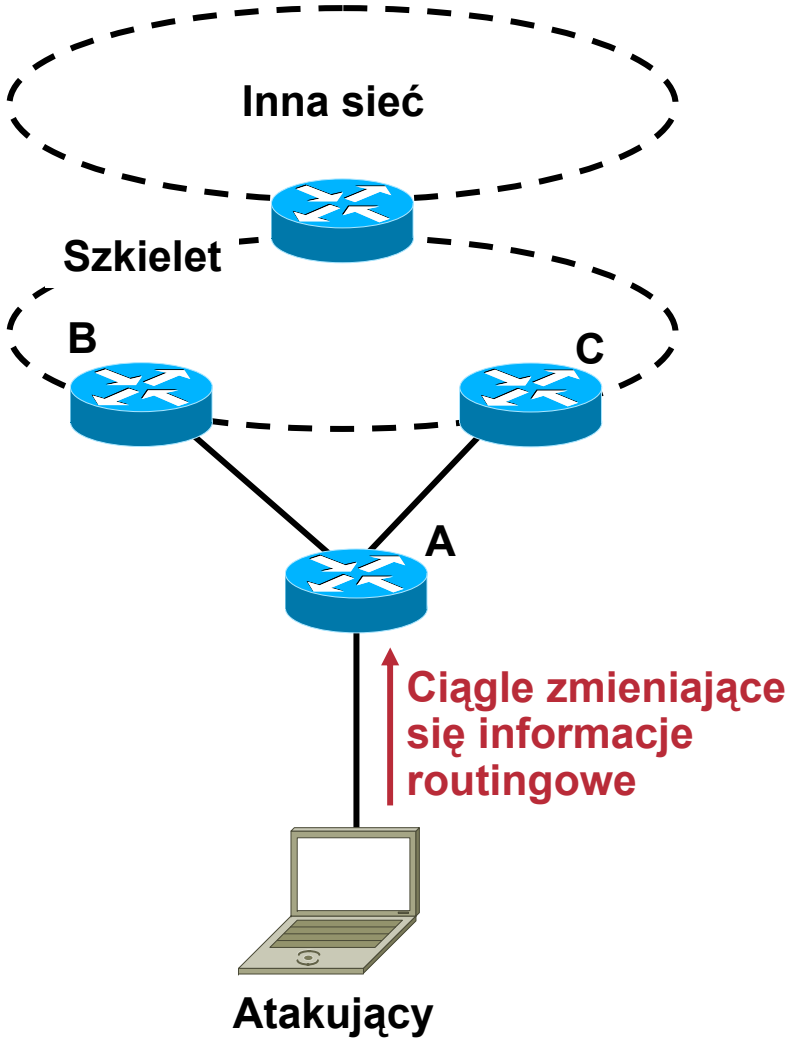


Przykład ataku na protokół routingu i CPU

- Atakujący nawiązuje sesję (dla OSPF/BGP)
- Zaczyna rozgłaszać i za chwilę wycofywać jakiś prefiks, grupę prefiksów

  przeciążając CPU
- Rozgłasza tysiące prefiksów

  przeciążając CPU i pamięć



Jak bronić protokoły routingu?

- Odseparować ruch użytkowników od ruchu administracyjnego
- Tagi MD5 dodawane do pakietów protokołów routingu ochronią przed:
  - pakietami uszkodzonymi i ze sfałszowanymi informacjami
- ...nie ochronią niestety przed:
  - resetowaniem sesji w ramach ataków DoS
  - wstrzykiwaniem błędnych informacji przez urządzenie, które zostało skompromitowane
- Podobnie jest niestety z ochroną sesji przez IPsec
- ...wraca kwestia separacji ruchu

Filtrowanie na brzegu Internetu

- **Upewnij się, że Twoje IGP:**
  - **nie wysyłają żadnych danych do Internetu**
  - **nie pozwalają wstrzelić żadnych danych z Internetu**
  - **nie pozwolą zestawić sąsiedztwa z routerami z Internetu**
- **Do nawiązywania sesji ze światem zewnętrznym wykorzystuj tylko BGP**
  - **ma relatywnie proste ale potężne mechanizmy kontroli rozgłaszanych i akceptowanych prefiksów**
  - **jest w stanie 'wytrzymać' wiele tysięcy, dziesiątek i setek tysięcy prefiksów w przeciwieństwie do np. RIPa czy OSPFa**

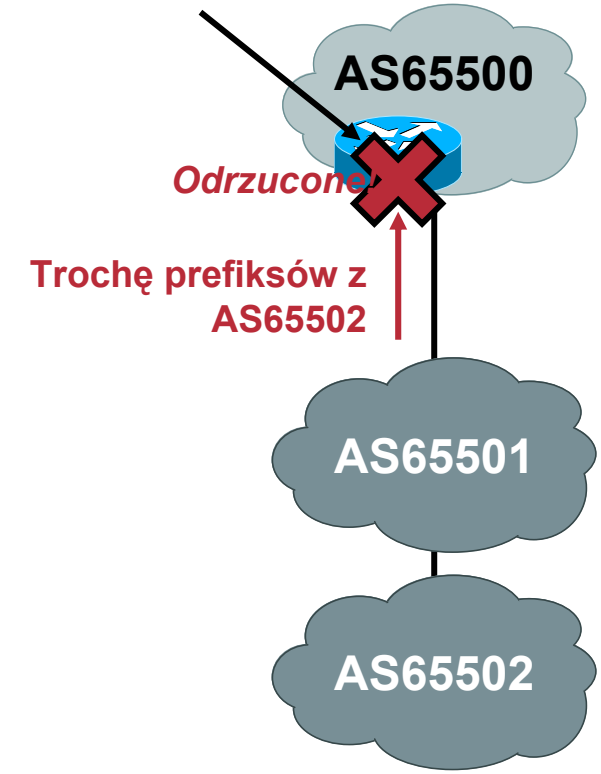
Filtrowanie na brzegu - BGP

- **Filtruj korzystając z AS Path**

  to podstawowy mechanizm zapobiegający pętlom w BGP

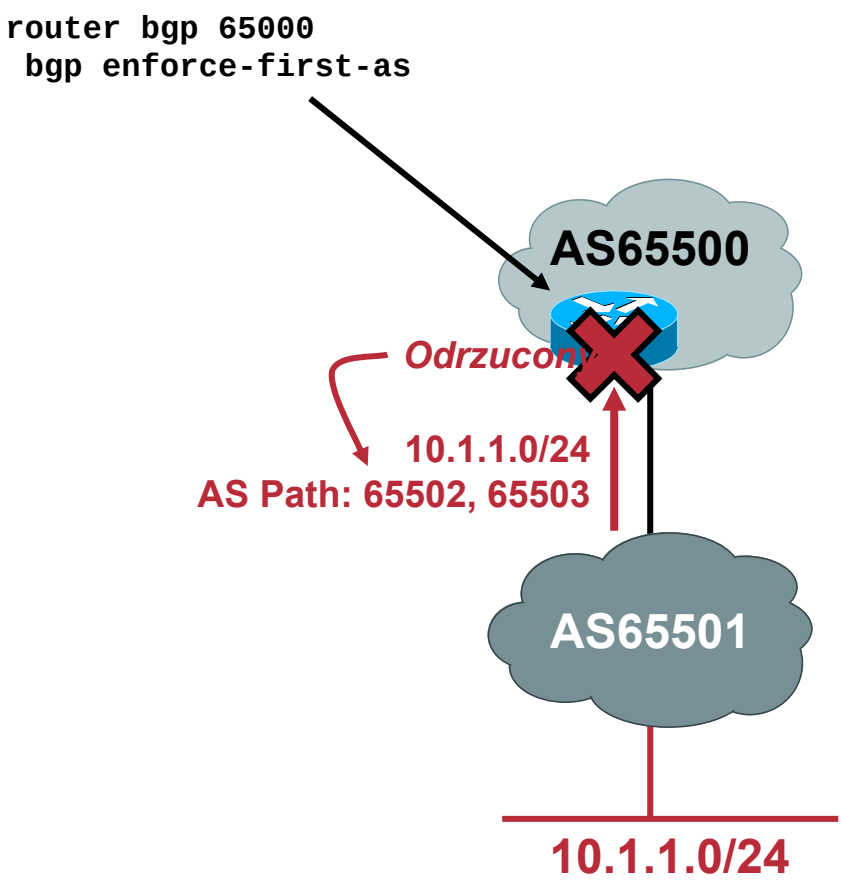
  pozwala określić politykę routingu z punktu widzenia ASów (firm) a nie prefiksów

```
ip as-path access-list 10 permit ^65501$
!
router bgp 65000
 neighbor 10.1.1.1 filter-list 10 in
```



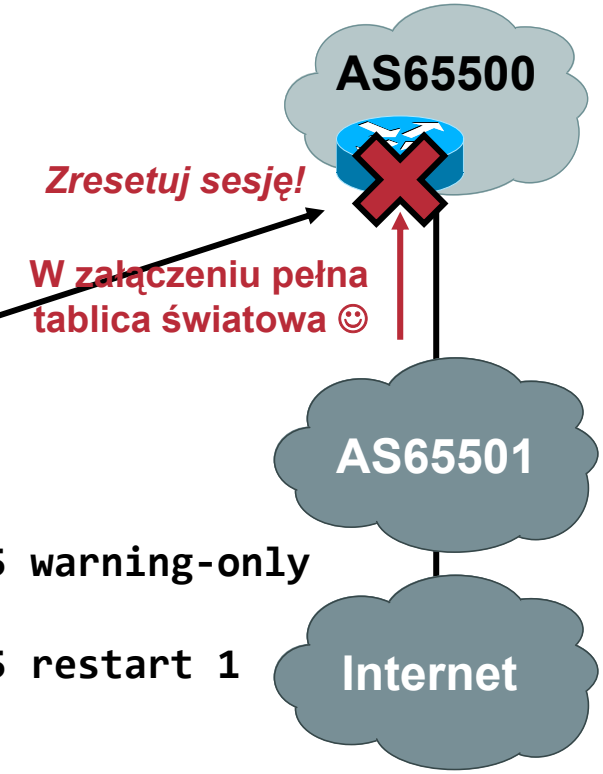
Filtrowanie na brzegu - BGP

- Opcja *bgp enforce-first-as* zapobiega rozgłoszeniu prefiksu jako pochodzącego z innego ASa niż nasz sąsiad
- Warto stosować na wszystkich połączeniach



Filtrowanie na brzegu - BGP

- Ogranicz ilość prefiksów, które zgadzasz się otrzymać od partnera
- Wymaga częstych rewizji
- Pełna tablica światowa – ok. 185k w chwili pisania tego slajdu, za pół roku może 190k a może 195k



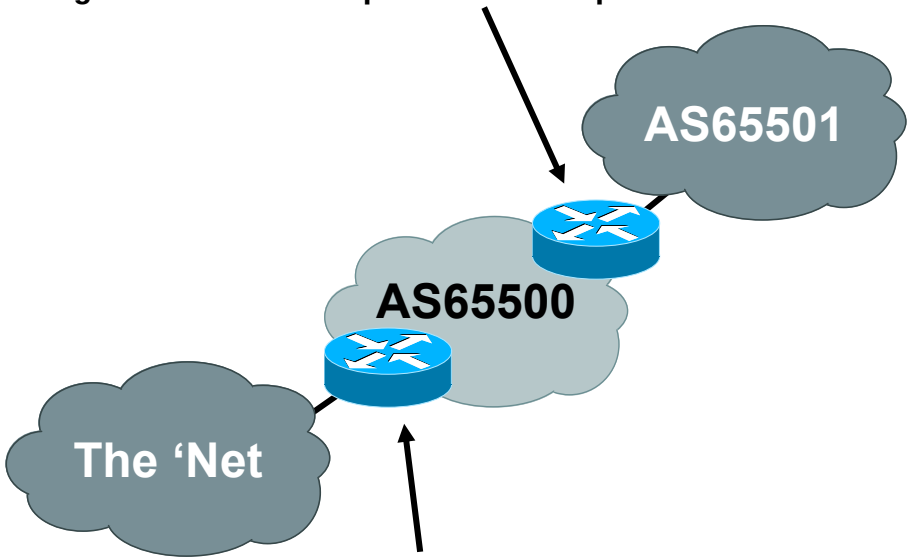

```
router bgp 65000
 neighbor 10.10.10.1 maximum-prefix 195000 85 warning-only
 ! lub
 neighbor 10.10.10.1 maximum-prefix 195000 95 restart 1
```

Filtrowanie na brzegu - BGP

- **Nie akceptuj prefiksów ewidentnie ‘dziwnych’:**
  - **z własnego ASa**
  - **z RFC1918**
  - **z nieprzydzielonych jeszcze przez IANA zakresów**
- **Dwa ostatnie punkty plus wiele więcej – projekt BGP blackholing PL (zapraszam na wczorajszą sesję ☺)**

```
ip prefix-list private permit 10.1.0.0/16 le 24

router bgp 65000
 neighbor 10.1.1.1 prefix-list private in
```




```
ip prefix-list public deny 0.0.0.0/0 ge 24
ip prefix-list public deny 10.1.0.0/16
ip prefix-list public deny 122.16.0.0/20
ip prefix-list public deny 192.168.0.0/16
ip prefix-list public permit 0.0.0.0/0

router bgp 65000
 neighbor 10.1.1.1 prefix-list public in
```

Route Flap Damping

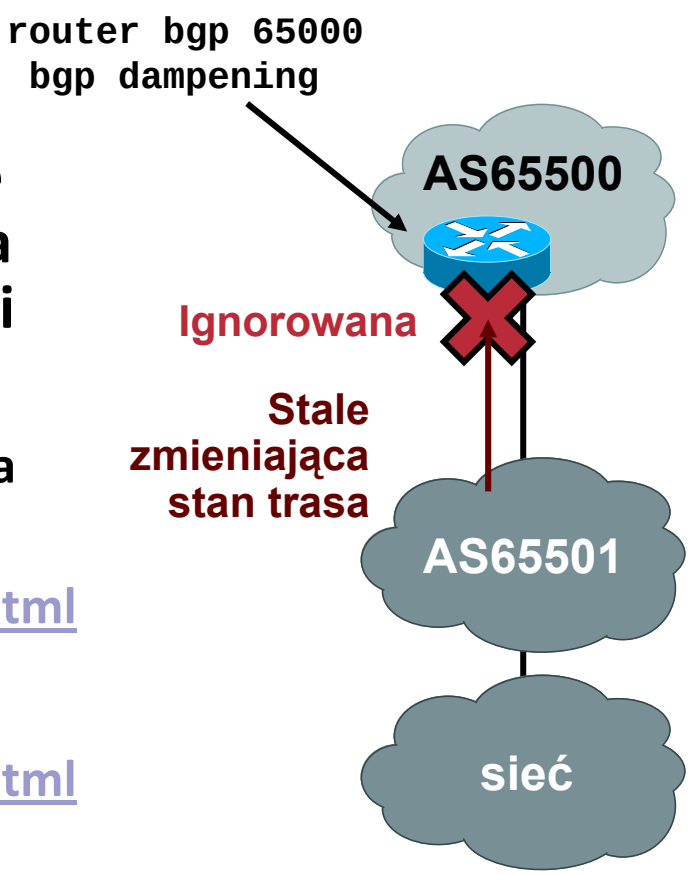
- Mechanizm pozwalający ograniczyć wpływ ‘klapiących’ prefiksów na stabilność pracy routera
- RIPE ma rekomendacje, zalecające wyłączyć z dampeningu istotne dla Internetu zasoby – w szczególności root-serwery DNS

  ...rozbuduj tą listę o zasoby istotne dla Ciebie

  http://www.ripe.net/docs/ripe-229.html

  zastąpiony przez RIPE-378:

  http://www.ripe.net/docs/ripe-378.html



Protokoły first-hop redundancy

- **Standardowe: VRRP**

  standardowe inaczej: CARP

- **Firmowe: HSRP, GLBP**
- **Domyślnie nie chronione w żaden sposób**

  ‘dzisiaj to ja jestem Waszą domyślną bramką!’

- **Używaj dostępnych mechanizmów podpisywania pakietów hello (MD5/SHA1) oraz staraj się niedopuścić do wstrzyknięcia ich z innych segmentów**

ATAKI L4+

Ataki L4+

- **DoS usługi:**

  przepełnienia bufora, itp. itd.

- **Dwa podstawowe rozwiązania:**

  Bezpieczniejsze aplikacje ;)

  HIPS i NIPS – też można je jednak zaatakować

- **Rozwiązania uzupełniające:**

  NetFlow, korelacja logów, systemy eksperckie

- **„Nowe” wyzwania:**

  VoIP, IMy (GG, Skype...)...

GDZIE WARTO RZUCIĆ OKIEM

Zasoby WWW

- **Referencje:**

  Cisco SRND: http://www.cisco.com/go/srnd

  Cisco SAFE: http://www.cisco.com/go/safe

  Cisco NFP: http://www.cisco.com/go/nfp

  SANS.ORG: http://www.sans.org (/rr – Reading Room)

  SecurityFocus.com: http://www.securityfocus.com

  Prezentacje z BlackHat: http://www.blackhat.com/html/bh-multimedia-archives-index.html

  Prezentacje z CanSecWest: http://www.cansecwest.com/

- **Bezpieczeństwo sieciowe w Internecie:**

  http://www.cert.pl

  referencje ‘abuse’ u operatorów

Q&A


NO
QUESTIONS
VIOLATORS
WILL BE SHOT
SURVIVORS
WILL BE SHOT
AGAIN