(nie)bezpieczeństwo w IPv6

Łukasz Bromirski
lbromirski@cisco.com

KrakYourNet #4, Kraków, IV.2012

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

Krótkie oświadczenie

- Powinniśmy traktować IPv6 jako po prostu **kolejny protokół** – nie ma w nim problemów wynikających z konstrukcji, ale jak zawsze **wielu mechanizmów trzeba się nauczyć** aby móc zastosować je **w sposób bezpieczny**
- W którymś momencie i tak czeka nas migracja na IPv6 – lepiej zrobić to teraz, niż potem w ostatnim momencie
- **Prawdopodobnie i tak używacie dzisiaj IPv6**, nawet jeśli nieświadomie

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

Agenda

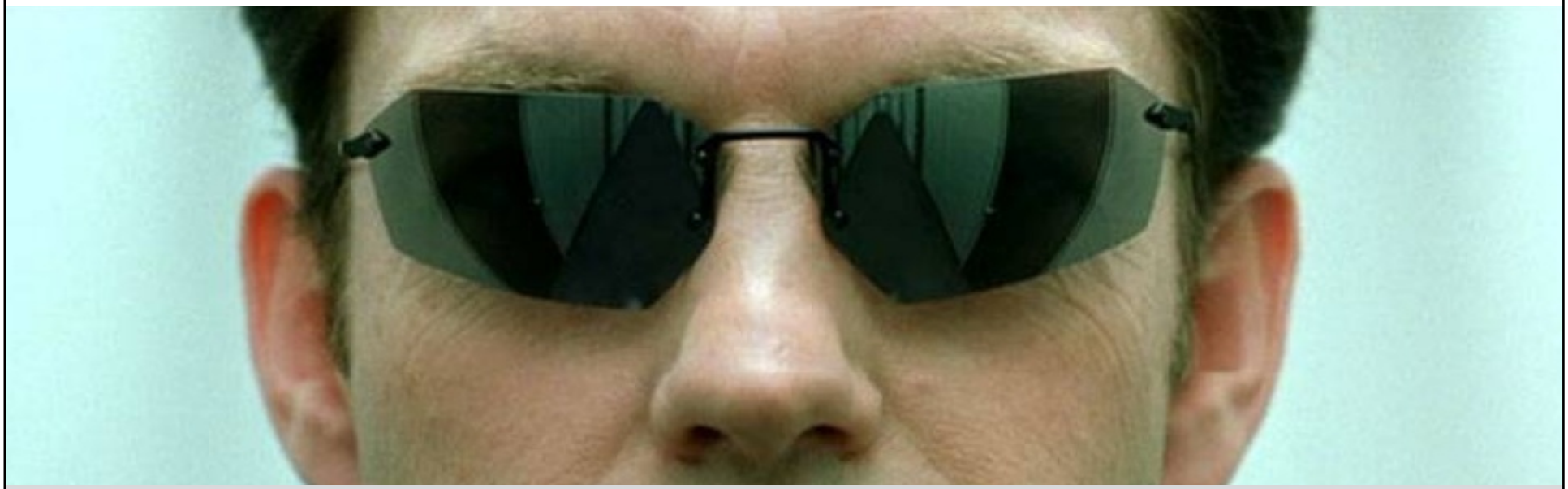
- Problemy bezpieczeństwa IPv4 rozwiązane dzięki wprowadzeniu IPv6
- Bezpieczeństwo IPv6
- Ochrona sieci
  - Warstwa zarządzania
  - Warstwa kontrolna
  - Warstwa danych
- Inne problemy i obszary zainteresowania
- Trochę o praktyce
- Q&A

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

Wdrożenia IPv6 w Polsce

- W 2010 roku – 59 sieci widocznych z 101 przydzielonych
- W 2012 roku – 115 sieci z 178 przydzielonych
- Największym problemem wydaje się nie być infrastruktura sieciowa
  - dostęp do usługi IPv6 od operatora
  - migracja i audyt aplikacji i systemów pod kątem zgodności z IPv6

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



Problemy IPv4 rozwiązane w IPv6

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

Żadne

- Wszystkie warstwy powyżej IPv4 są dokładnie tak samo "niebezpiecznea" w IPv6
- IPv6 robi pewne rzeczy gorzej, pewne lepiej, ale w ogólności – po prostu inaczej
- IPv6 jest bardziej złożony niż IPv4

  złożoność zwykle przynosi **problemy**
- Wszyscy producenci oferujący IPv6 już ogłaszali i zapewne będą jeszcze długo ogłaszać swoje problemy z IPv6

  Cisco, Juniper, Microsoft, Sun/Oracle i dużo różnego rodzaju oprogramowania Open Source

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

Pole bitwy dla IPv6

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

Nic fundamentalnie nowego

- Podsłuchiwanie (ang. sniffing)

  IPv6 oczekuje od implementacji mechanizmów IPsec, ale czy faktycznie włączyliście dla wszystkich połączeń?

- Ataki warstwy aplikacji

  Nawet przy zabezpieczeniu za pomocą szyfrowania i uwierzytelniania zapewnianego przez IPsec i tak większość ataków ma miejsce w warstwie aplikacji – a więc "czy zainstalowaliście już dzisiaj swoje uaktualnienia"?

- Podstawione urządzenia i ataki MITM

  Mogą i będą wykonywane

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

Rozpoznanie w IPv6

Różnica w wielkości podsieci

- Domyślne podsieci w IPv6 mają 2^{64} adresów

  14.8 Mpps (interfejs 10GE) = ~40 000 lat

- Niezbyt wydajne i efektywne
- Bardzo ciekawe obserwacje wyboru adresów IPv6

  Malone, D. *Observations of IPv6 Addresses*. Passive and Active Measurement Conference (PAM 2008), 29–30.IV.2008

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

Rozpoznanie w IPv6

Metody skanowania się zmieniły

- Adresy serwerów muszą być w DNSie
  - Jeszcze więcej informacji zostanie zebrane przez Google…
- Coraz więcej mechanizmów opiera się o dynamiczny DNS
- Aplikacje P2P również pozwolą namierzyć adresy IPv6 z konkretnej podsieci
- Administratorzy używają prostych do zapamiętania adresów
  - granica :1000:, :2000: etc
  - ::1, ::FFFF, ::F00D, ::DEAD, ::C5C0, ::FEED itd
- Oczywiście po przejęciu hosta – nic prostszego tylko skorzystać z pamięci podręcznej ND

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

Skanowanie to problem dla CPU

- Skanowanie będzie problemem dla routerów i wszystkich węzłów L3
  - Proces Neighbor Discovery ma do dyspozycji tylko skończone zasoby sprzętowe (tablicę sąsiadów) i CPU
  - Wbudowane mechanizmy rate-limit to dzisiejsze rozwiązanie, ale nie dotyka ono w ogóle źródła problemu
- Można zastosować ACLki zabraniające ruchu do adresacji przeznaczonej do infrastruktury, ale nie dotyczy to lokalnego segmentu i sprawia problemy przy diagnostyce (traceroute6, etc)

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

Rozpoznanie w IPv6
Zastosowanie multicastu

- 3 adresy site-local

  FF05::2 all-routers, FF05::FB mDNSv6, FF05::1:3 wszystkie serwery DHCP

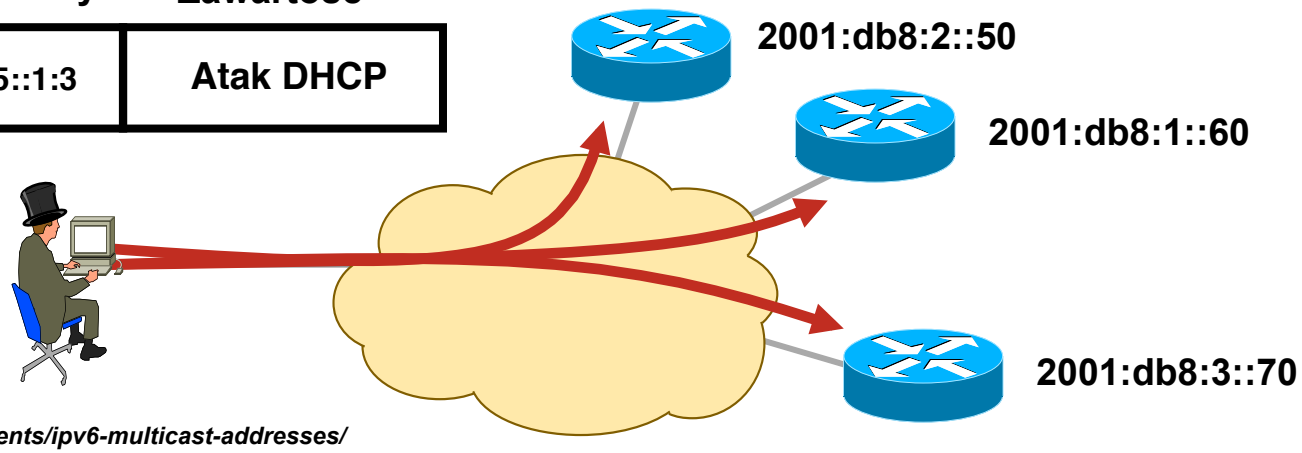
- Parę adresów link-local

  FF02::1 wszystkie węzły, FF02::2 wszystkie routery, FF02::F UPnP, ...

- Niektóre adresy wycofane już (RFC 3879) mogą nadal odpowiadać...

  FEC0:0:0:FFFF::1 DNS server

Adres źródłowy	Adres docelowy	Zawartość
Atakujący	FF05::1:3	Atak DHCP

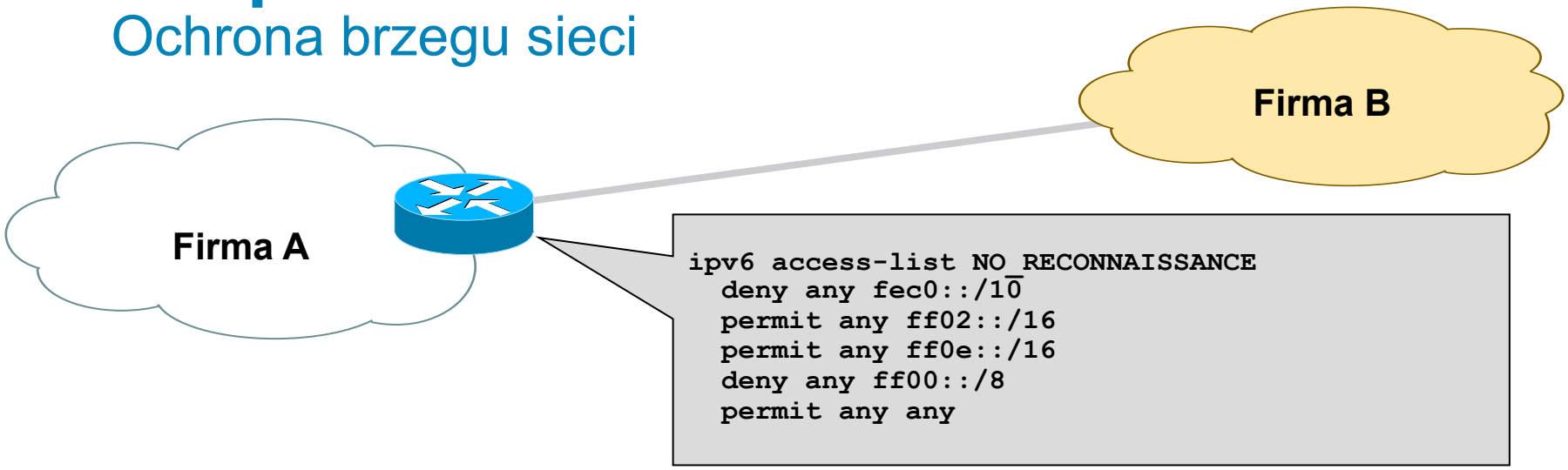


http://www.iana.org/assignments/ipv6-multicast-addresses/

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

Rozpoznanie w IPv6

Ochrona brzegu sieci



- Adresy site-local i anycast warto odfiltrować na brzegu sieci – aby nie były osiągalne zdalnie
- Reguły do rozważenia:

  Blokujemy FEC0::/10 (wycofane adresy site-local)

  Przepuszczamy mcast do FF02::/16 (link-local scope)

  Przepuszczamy mcast do FF0E::/16 (global scope)

  Blokujemy całą resztę

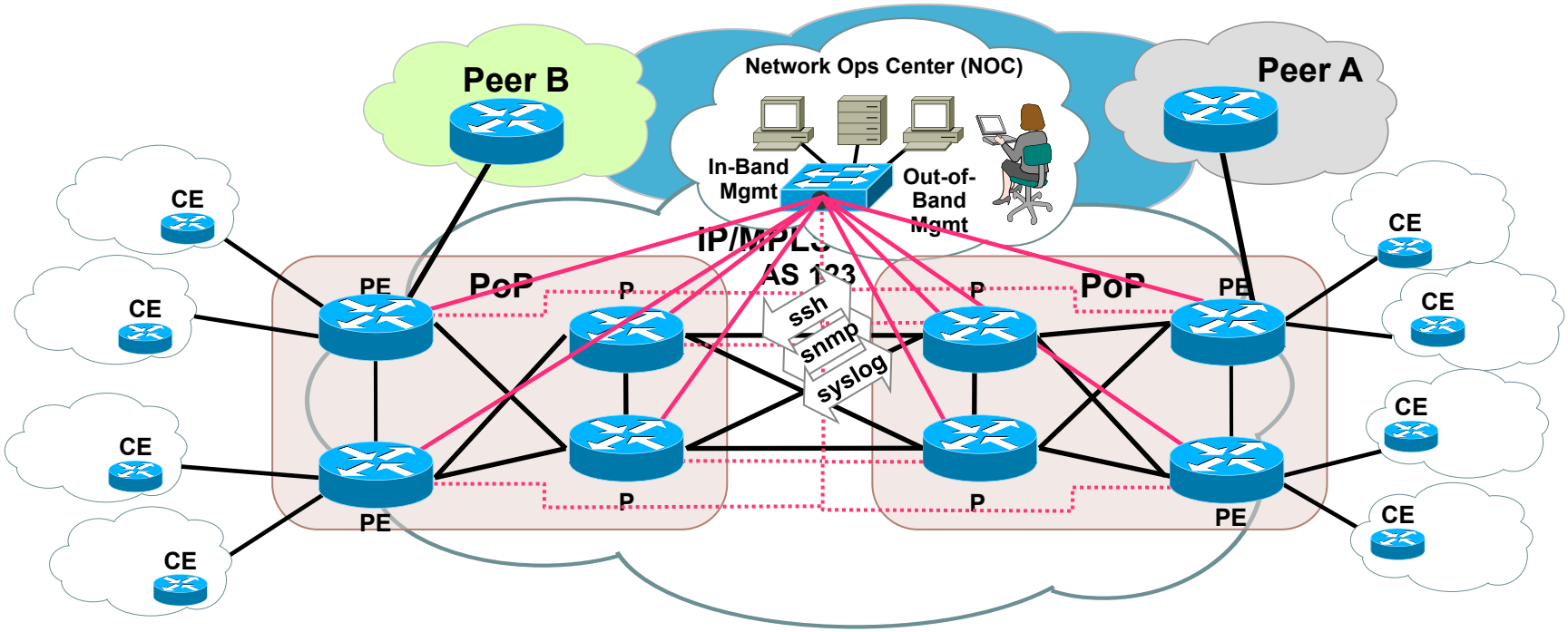
© 2012 Cisco and/or its affiliates. All rights reserved.

Ochrona warstwy zarządzania

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

Warstwa zarządzania

- Zarządzanie, provisioning i monitoring za pomocą protokołów takich jak między innymi: SSH, FTP, SNMP, Syslog, TACACS+ i RADIUS, DNS, NetFlow, ROMMON, CDP, LLDP i innych



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

Zarządzanie po IPv6

- RADIUS, SSH, syslog, SNMP, NetFlow – działają ponad IPv6
- Warstwa zarządzająca dual-stack
  - bardziej odporna: działa nawet gdy jedna z wersji protokołu IP przestaje
  - bardziej odsłonięta: możemy atakować dwa protokoły
- Tam gdzie się da:
  - szyfrujemy
  - filtrujemy dostęp

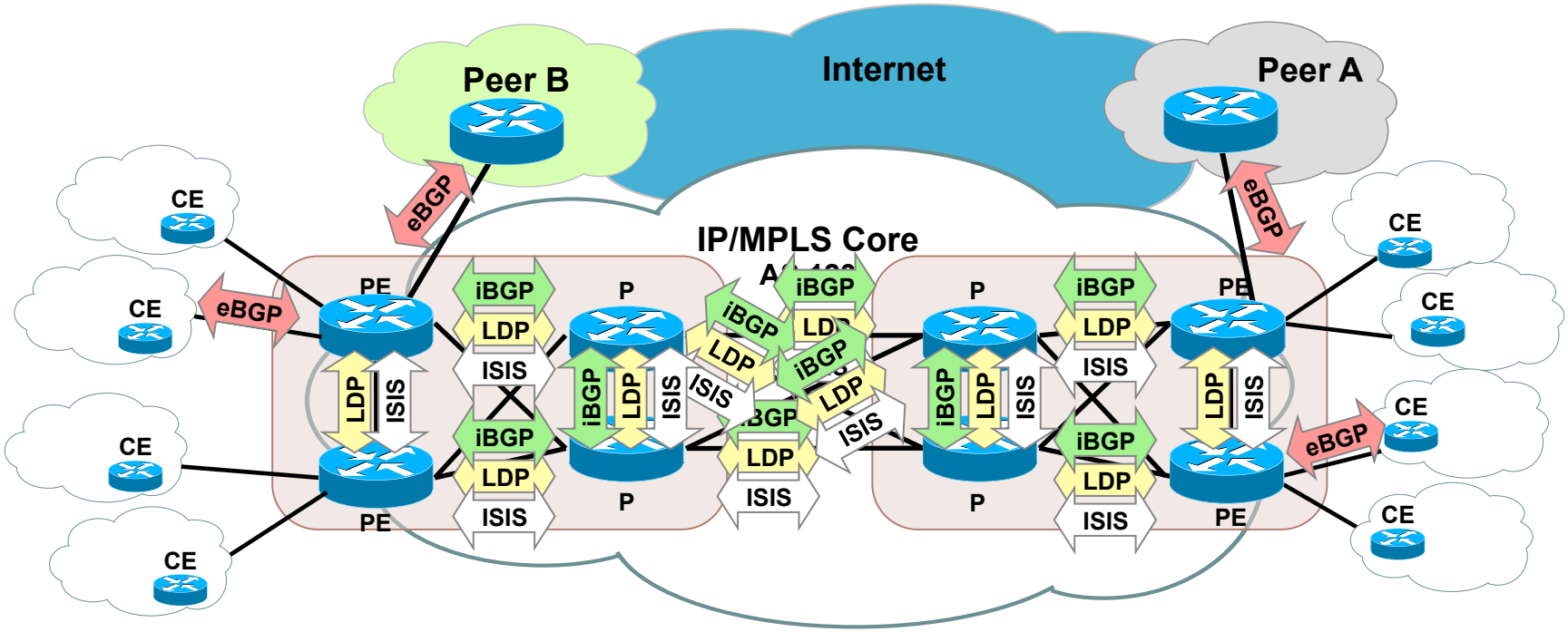
© 2012 Cisco and/or its affiliates. All rights reserved.

Ochrona warstwy kontrolnej

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

Warstwa kontrolna

- Wszystkie protokoły zapewniające sieci inteligencję i działanie – przekazywanie pakietów, nawiązywanie sąsiedztw, etc – protokoły takie jak BGP, OSPF, LDP, IS-IS, ARP, ATM OAM, PPP LCP i inne



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

Zapobieganie atakom na routing

- Dla BGP, ISIS, EIGRP i LDP nic się nie zmienia:
  - do pakietów dodawany tag MD5
- OSPFv3, RIPng i PIM polegają na IPSec
- Tam gdzie się da:
  - szyfrujemy (OSPFv3, RIPng, PIM)
  - uwierzytelniamy (BGP, IS-IS, EIGRP)
  - filtrujemy dostęp

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

Link-Local vs. Global Addresses

- Adresy link-local - fe80::/16, są z definicji izolowane
  - Nie można osiągnąć ich spoza linku
- Można używać ich do adresacji interfejsów
  - Protokoły routingu dla IPv6 używają adresów link-local
  - Warto zapewnić sobie możliwość wykonywania diagnostyki (ping/traceroute)

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

Spoofing ARP to teraz spoofing NDP

- ARP został zastąpiony przez Neighbor Discovery Protocol
  - Nie ma żadnego uwierzytelniania
  - Wpisy statyczne mogą zostać nadpisane przez wpisy dynamiczne
- Bezstanowa autokonfiguracja
  - podstawione/sfałszowane RA
  - wszystkie węzły otrzymują złe informacje
    - DoS
    - przechwycenie ataku
- Istnieją gotowe narzędzia:
  - parasit6
  - fakerouter6
  - ...

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

Spoofing ARP to teraz spoofing NDP

- **ZŁA INFORMACJA**: nie ma jeszcze mechanizmu DAI dla IPv6
- **DOBRA INFORMACJA**: Secure Neighbor Discovery (RFC 3971)

  SEND = NDP + mechnizmy kryptograficzne

  Dostępne w Cisco IOS i w implementacjach open source
- Inne **DOBRE INFORMACJE**:

  Mechanizm Private VLAN działa dla IPv6

  Mechanizm Port Security działa dla IPv6

  801.x działa z IPv6

  Można filtrować ruch ACLkami

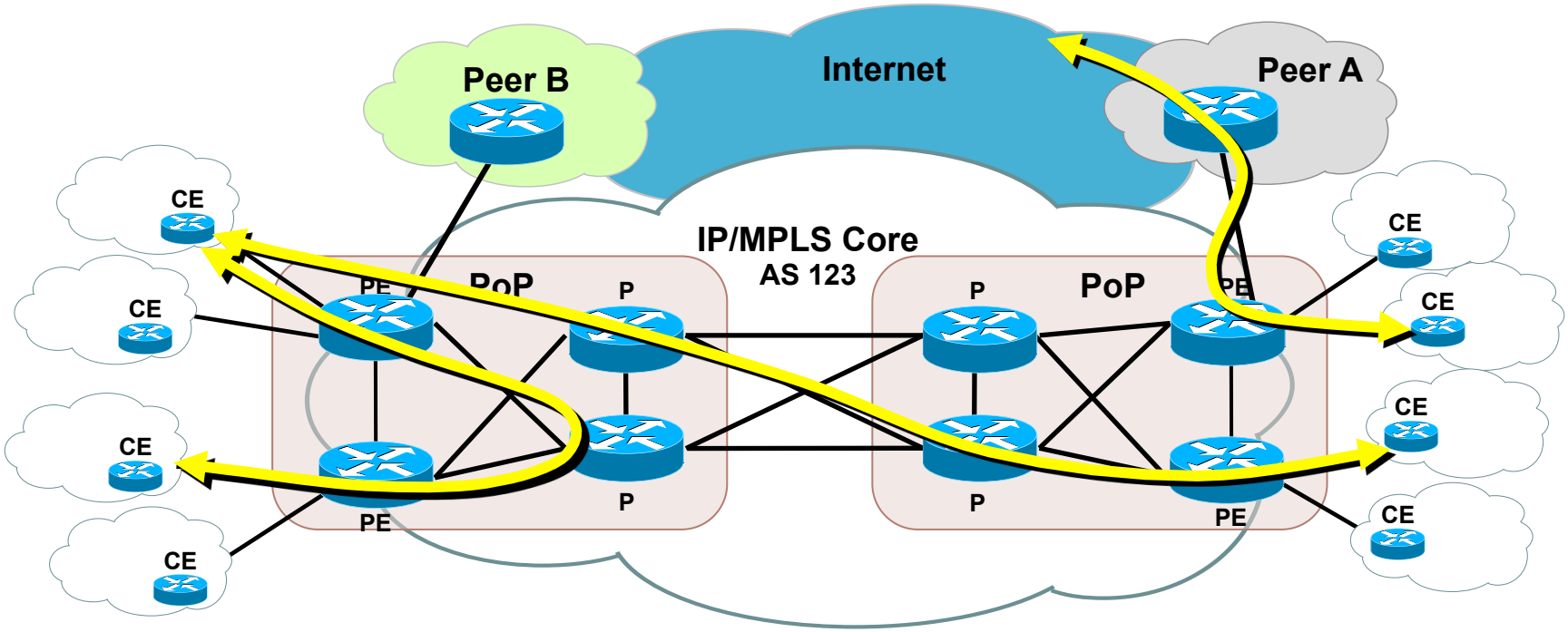
© 2012 Cisco and/or its affiliates. All rights reserved.

Ochrona warstwy danych

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

Warstwa danych

- Wszystko co wymieniane jest między węzłami końcowymi

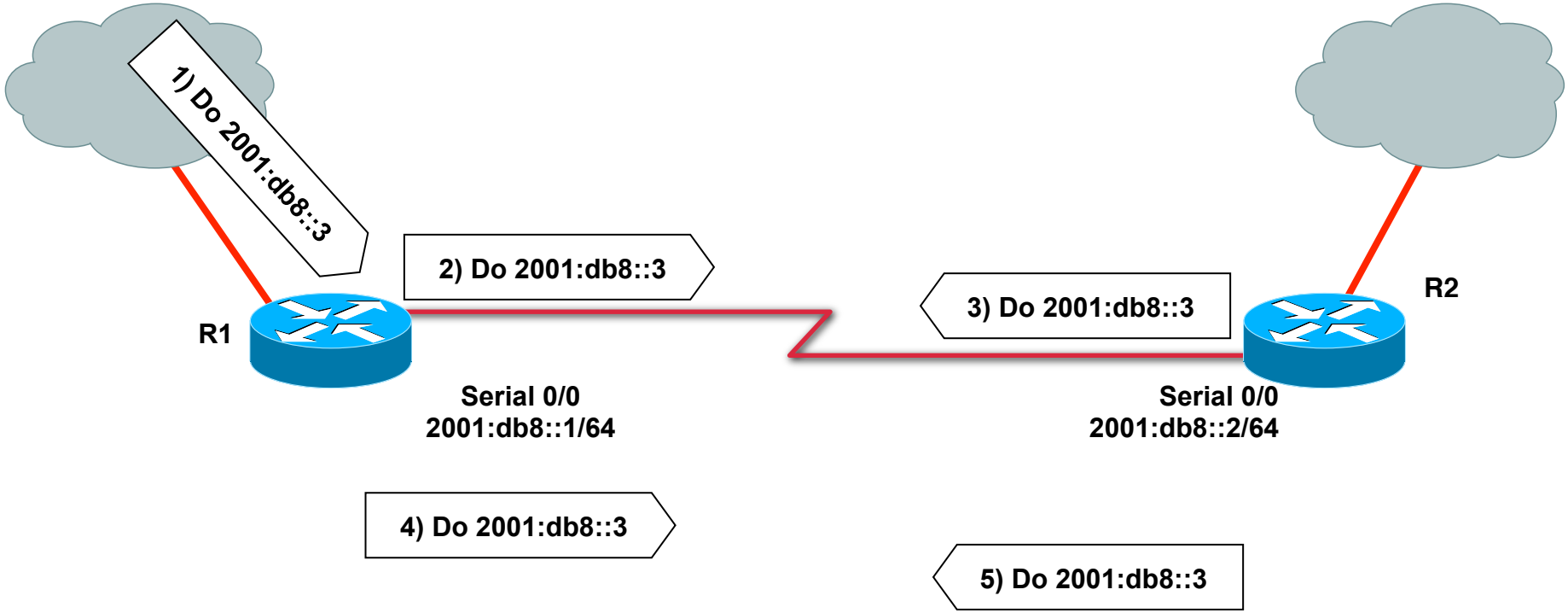


© 2012 Cisco and/or its affiliates. All rights reserved.

Przykład ataku DoS

- Stary stos ICMPv6 może być podatny na taki atak
- Platformy zgodne z RFC 4443 (ICMPv6) nie powinny mieć problemów

  użyj /127 na połączeniach P2P, adresów link-local lub po prostu filtrów ruchowych



....

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

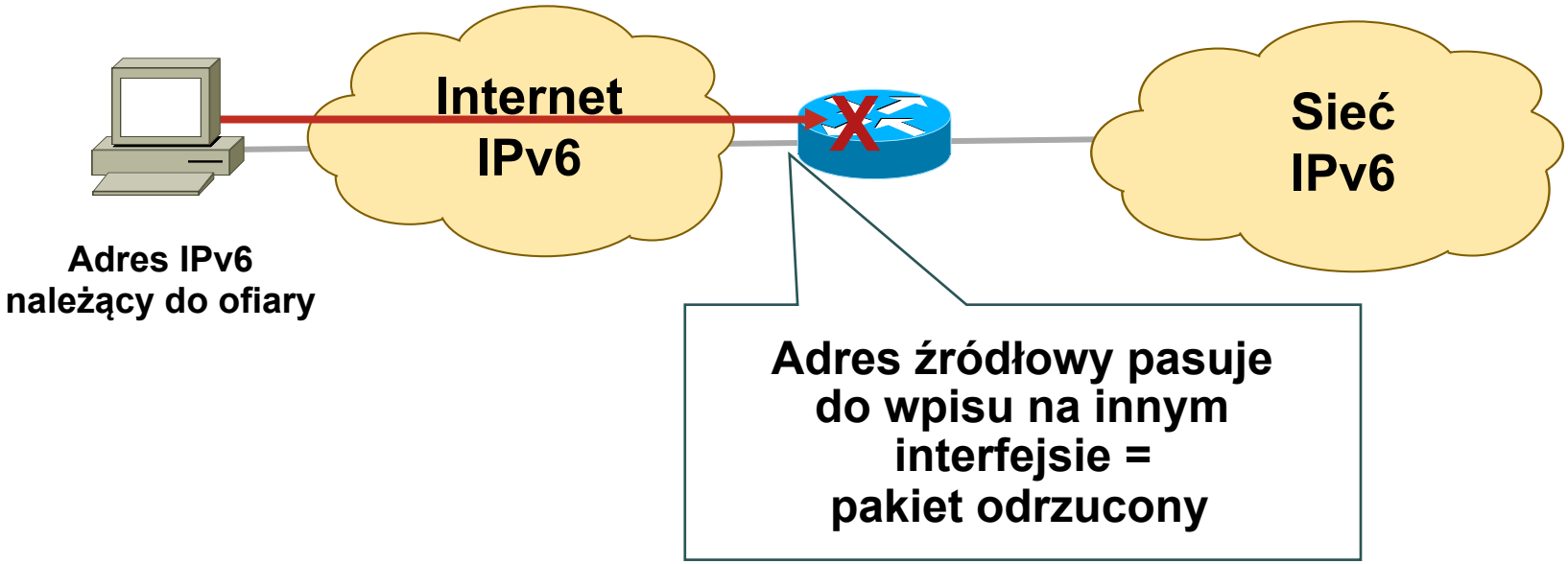
Filtrowanie IPv6 i antyspoofing

- IPv6 również ma swoje "bogony":

  http://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt

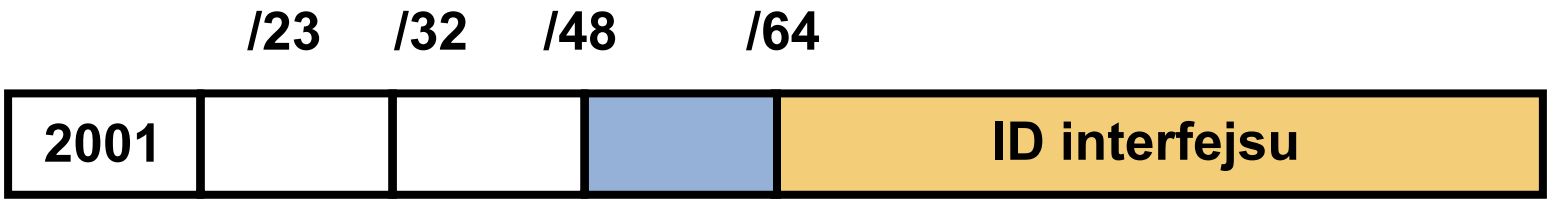
- Sytuacja podobna do tej z IPv6

  jeden styk z trasą domyślną = zastosuj uRPF



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

Rozszerzenia prywatności (RFC 3041)

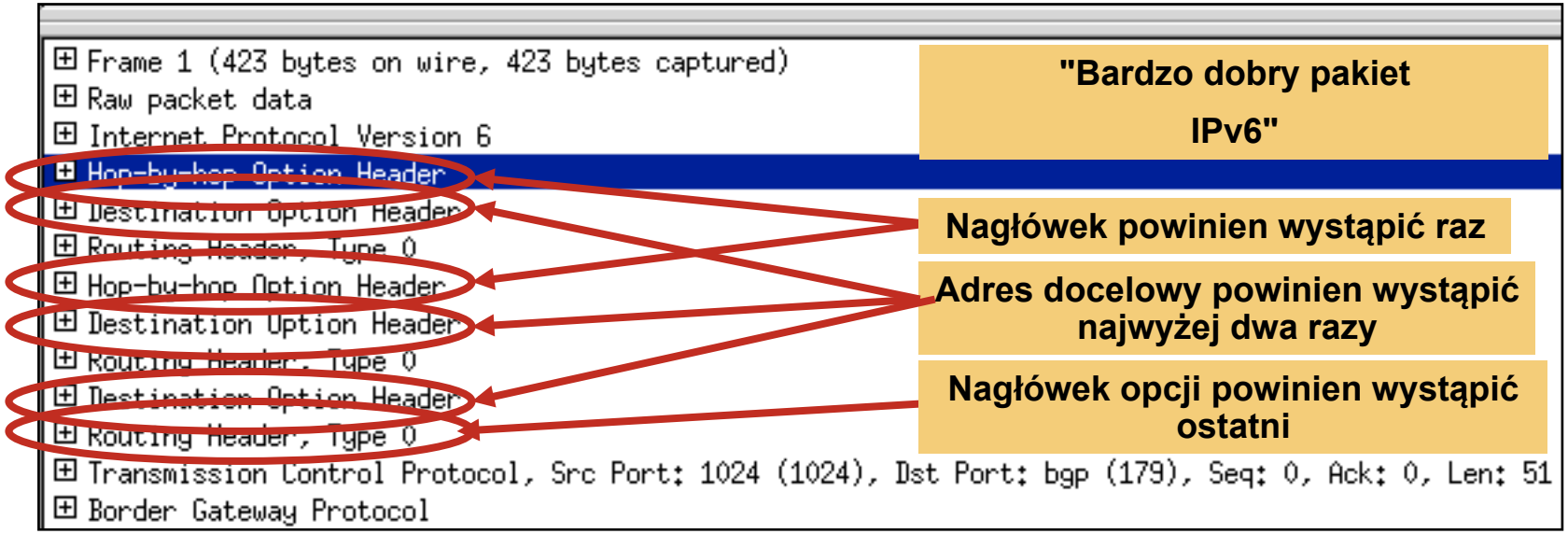


- Adresy tymczasowe IPv6, np. dla kafejek internetowych
  - utrudniają śledzenie hosta
  - losowy 64 bitowy adres przy każdej aktywacji linku
- Problemy przy wdrożeniach w środowiskach firmowych, jeśli jedyną metodą śledzenia aktywności użytkowników jest ich adres IP

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

Manipulacja nagłówkami IPv6

- Nieograniczony rozmiar łańcucha nagłówków może być problematyczny do analizy
- Ciągle odkrywamy dziury w istniejących implementacjach
- Łatwo zaatakować "warstwę kontrolną"

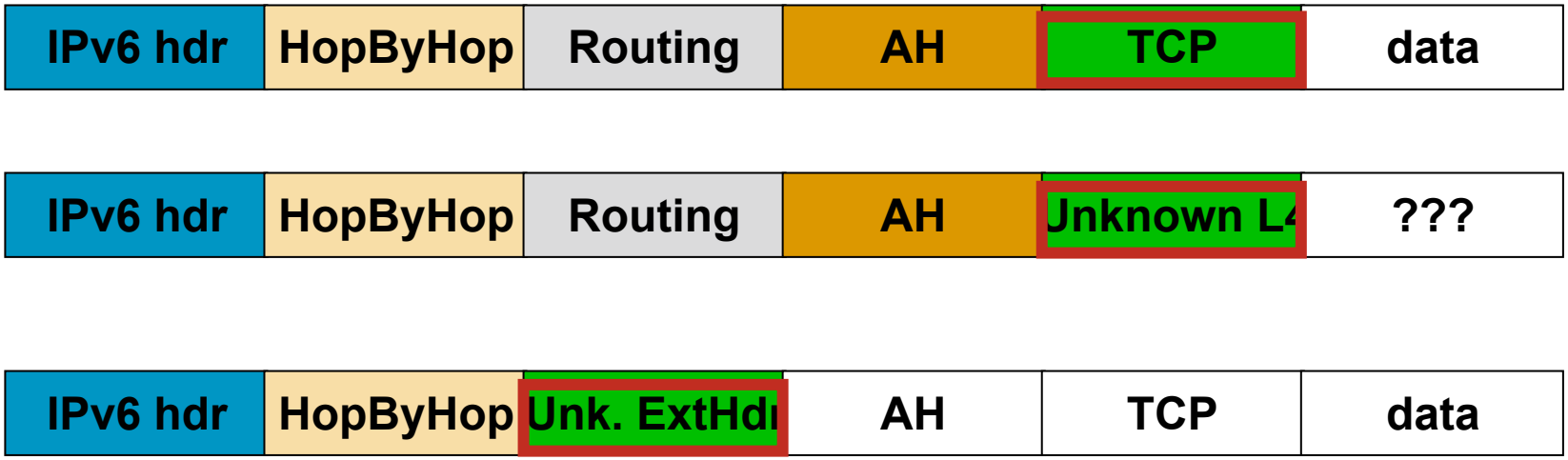


Zajrzyj też pod: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

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

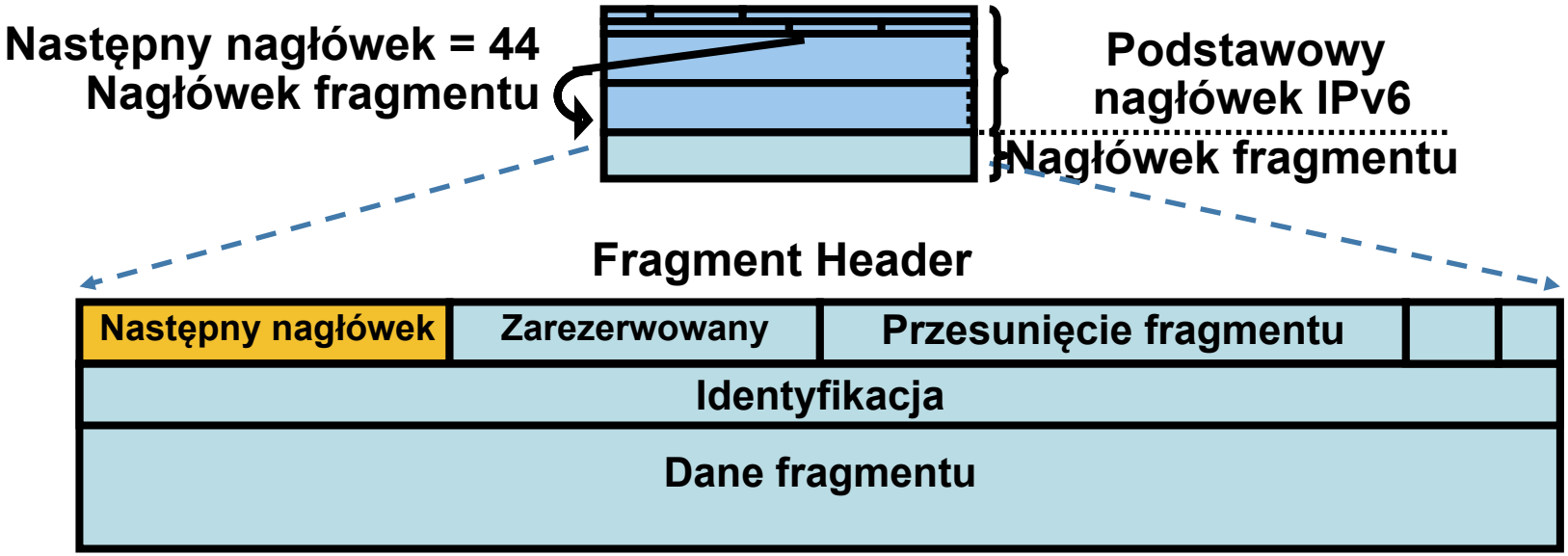
Zabawa w analizę nagłówków IPv6

- Znalezienie informacji o warstwie czwartej nie musi być banalne



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

Sfragmentowany nagłówek IPv6



- W IPv6 fragmentację wykonuje tylko nadawca/router z początkiem tunelu
- Składaniem fragmentów również zajmują się węzły końcowe – jak w IPv4
- Zdarza się i widać to w Internecie, że ruch jest fragmentowany
- Doskonałe narzędzie do zaciemnienia prawdziwej natury ruchu

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

Inne problemy i obszary zainteresowania

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

Przejście z IPv4 do IPv6

- Ponad 16 metod
- Podwójny stos protokołów (ang. dual-stack)
  - dla obu protokołów należy przewidzieć zabezpieczenia
  - nadużycia pomiędzy protokołami
  - odporność i skalowalność (konkurencja o zasoby)
- Tunele
  - Mogą ominąć firewalle (protokół 41 lub UDP)
  - Mogą powodować asymetrię ruchu (utrudniając korelację sesji)

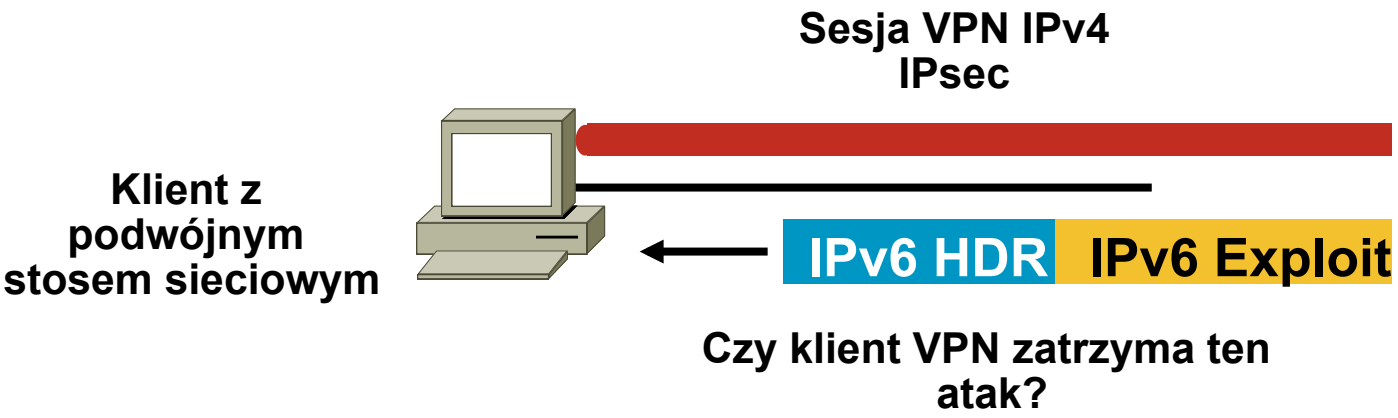
© 2012 Cisco and/or its affiliates. All rights reserved.

Host z podwójnym stosem sieciowym

- Aplikacje mogą stać się ofiarą zarówno dla IPv4 jak i IPv6

  Tylko tak bezpieczne, jak mniej bezpieczna z implementacji

- Rozwiązania typu host firewall, IPS, AV, klienci VPN – powinny być w stanie egzekwować politykę bezpieczeństwa na ruchu z obu protokołów



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

Host z podwójnym stosem sieciowym

- Dzisiejsze nowoczesne systemy operacyjne mają uruchomione IPv6 domyślnie
- W sieci "nie mamy IPv6"
- Założenie: "jesteśmy bezpieczni"
- W rzeczywistości:

  Atakujący w segmencie może rozesłać pakiety RA i skonfigurować obsługę ruchu IPv6 przez siebie

  Host staje się osiągalny zarówno dla atakującego jak i potencjalnie – dla całego internetu (choć sieć obsługuje tylko IPv4)
- **Warto rozważyć świadome wprowadzenie IPv6 do swojej sieci**

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

Włączenie IPv6 na zdalnym hoście

1) Czy są tu jakieś routery IPv6?

2) "włamywacz": tak, oto moje dane

			Destination	Protocol	Info
			ff02::1:ff00:22	ICMPv6	Neighbor solicitati
			ff02::1:ff00:22	ICMPv6	Neighbor solicitati
3	1.568197	2001:db	ff02::1:ff00:22	ICMPv6	Neighbor solicitati
4	99.069381	fe80::215:58	ff02::1	ICMPv6	Router advertisement
5	455.573664	fe80::215:58ff:fe2	1	ICMPv6	Router advertisement
6	880.382347	fe80::20d:93ff:fe3	ff02::2	ICMPv6	Router solicitation
7	880.388487	fe80::20d:93ff:fe3	ff02::fb	MDNS	Standard query response SRV
8	880.578883	fe80::215:58ff:fe2	ff02::1	ICMPv6	Router advertisement
9	880.583454	::	ff02::1:ff38:c874	ICMPv6	Neighbor solicitation
10	880.583602	fe80::20d:93ff:fe3	ff02::2:52a6:75e2	ICMPv6	Multicast listener report
11	880.694784	fe80::20d:93ff:fe3	ff02::2:52a6:75e2	ICMPv6	Multicast listener report
12	883.604742	fe80::20d:93ff:fe3	ff02::2	ICMPv6	Multicast listener done
13	1476.586161	fe80::215:58ff:fe2	ff02::1	ICMPv6	Router advertisement
14	1716.588901	fe80::215:58ff:fe2	ff02::1	ICMPv6	Router advertisement
15	1806.190418	2001:db8:dead::1	ff02::1:ff38:c874	ICMPv6	Neighbor solicitation

```
⊞ Frame 9 (78 bytes on wire, 78 bytes captured)
⊞ Ethernet II, Src: AppleCom_38:c8:74 (00:0d:93:38:c8:74), Dst: IPv6 ghbor-Discovery_ff
⊞ Internet Protocol Version 6
⊟ Internet Control Message Protocol v6
    Type: 135 (Neighbor solicitation)
    Code: 0
    Checksum: 0x48da [correct]
    Target: 2001:db8:dead:0:20d:93ff:fe38:c874
```

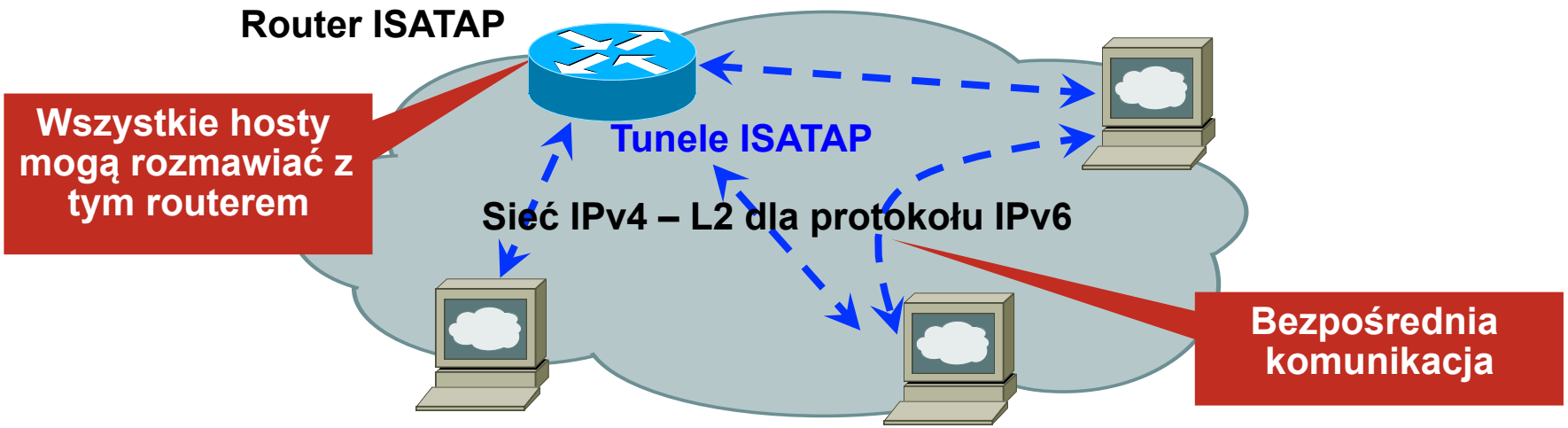
3) Host po włączeniu IPv6 wykonuje proces DAD

4) Pełen adres hosta w sieci IPv6

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

Zagrożenia w trakcie migracji - ISATAP

- Tunele – przechodzą (zwykle) przez firewall – protokół 41
- Infrastruktura IPv4 wygląda jak płaski segment L2 dla wszystkich hostów ISATAP w sieci
  - Ma to swoje implikacje w segmentacji sieci i procesie odkrywania sąsiadów
- ISATAP nie oferuje mechanizmów uwierzytelniania węzłów
  - Windows domyślnie używa nazwy isatap.skonfigurowana-domena
- Adresy IPv6 można zgadnąć na podstawie prefiksu



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

Bezpieczeństwo bramek 6to4

- Wrzucanie ruchu i spoofing IPv6

  Można zapobiec stosując uRPF (blokuje pakiety których adres źródłowy został zbudowany z adresu IPv4 z puli zarezerwowanej

- Przekierowanie i DoS

  Można* zablokować część ruchu ICMPv6 – ND, ruch link-local, redirect

- Ruch jest asymetryczny

  klient/router 6to4 -> relay 6to4 -> serwer IPv6

  routing w sieci IPv4 klienta wybiera relay

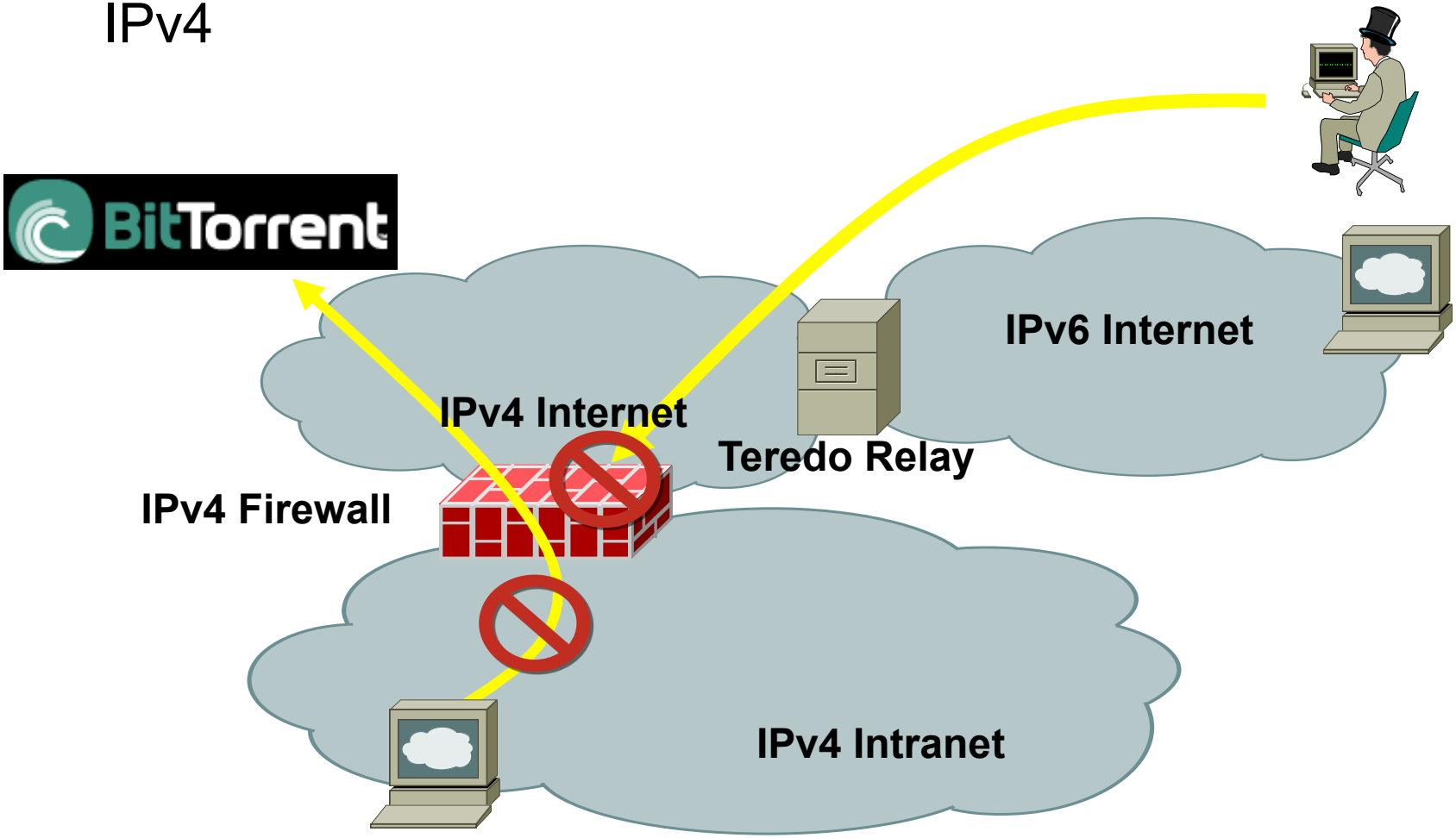
  serwer IPv6 -> relay 6to4 -> klient/router 6to4

  routing w sieci IPv4 serwera wybiera relay

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

Tunele Teredo

- Ruch w sieci jest ściśle kontrolowany – ale tylko ruch IPv4

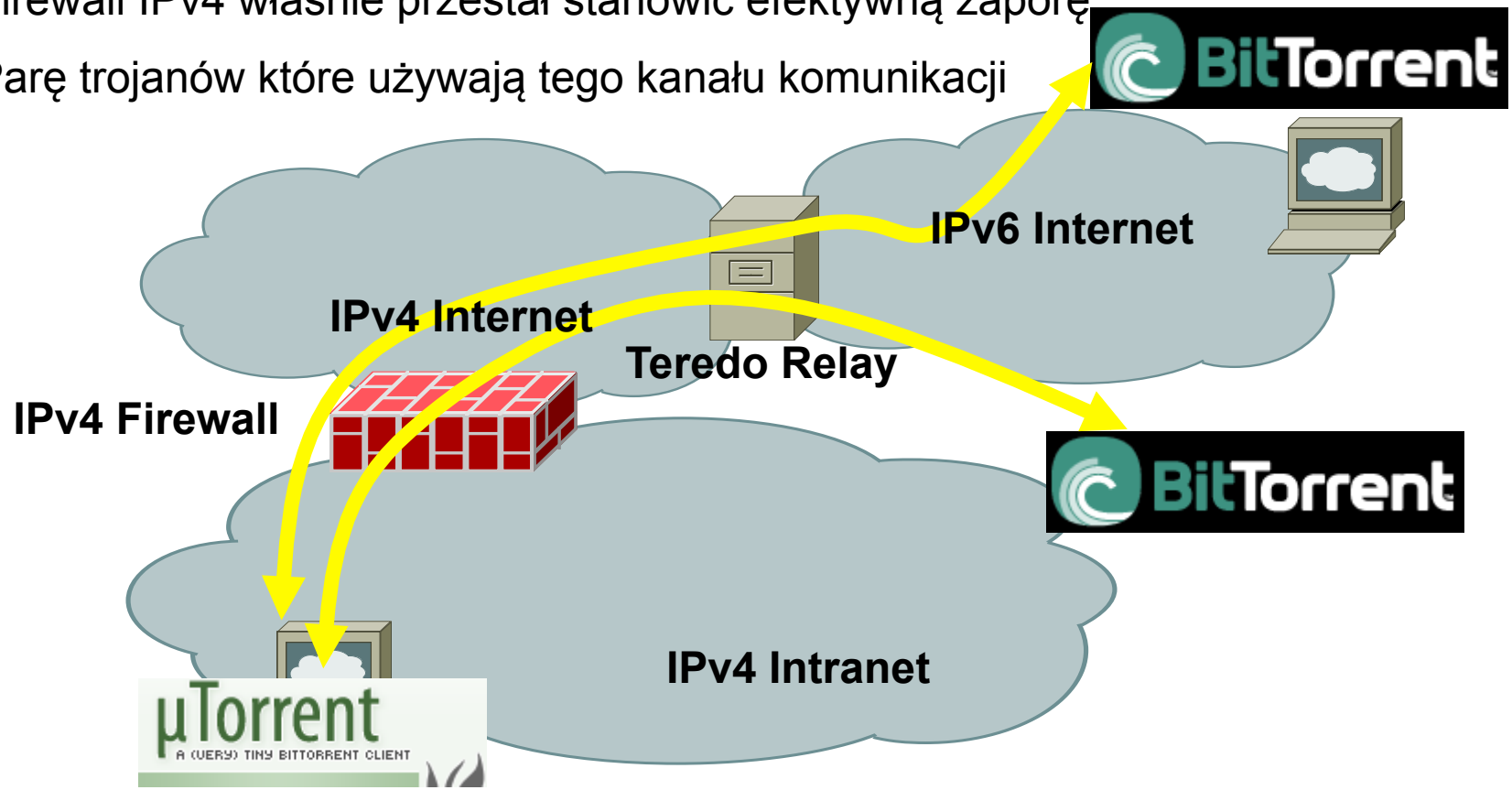


© 2012 Cisco and/or its affiliates. All rights reserved.

Tunele Teredo

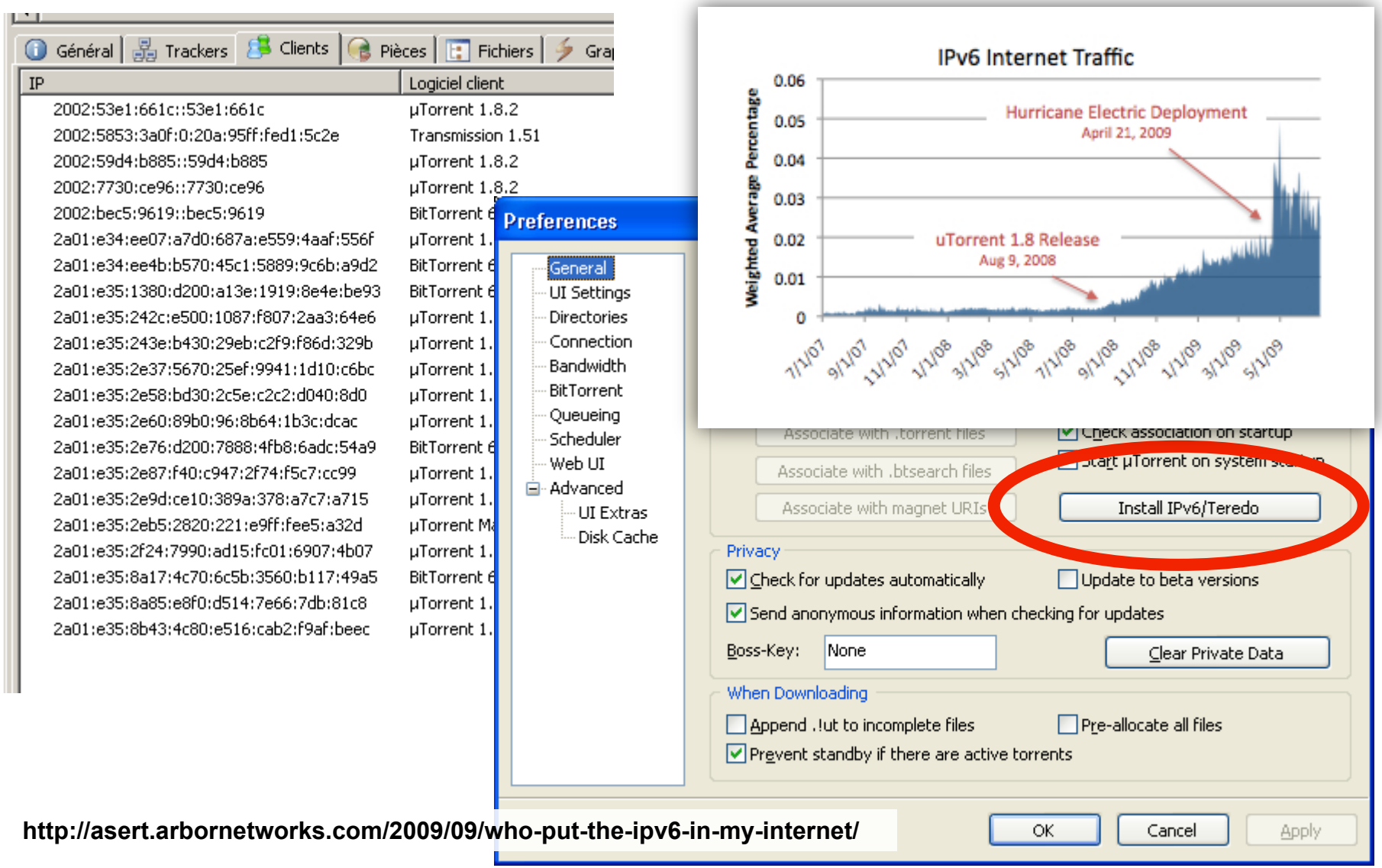
Teredo - IPv6 ponad IPv4/UDP (port 3544)

- Cały ruch IPv6 klienta jest tunelowany w IPv4
- Może być wysyłany na porty popularnych usług (np. 53/udp)
- Firewall IPv4 właśnie przestał stanowić efektywną zaporę
- Parę trojanów które używają tego kanału komunikacji



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

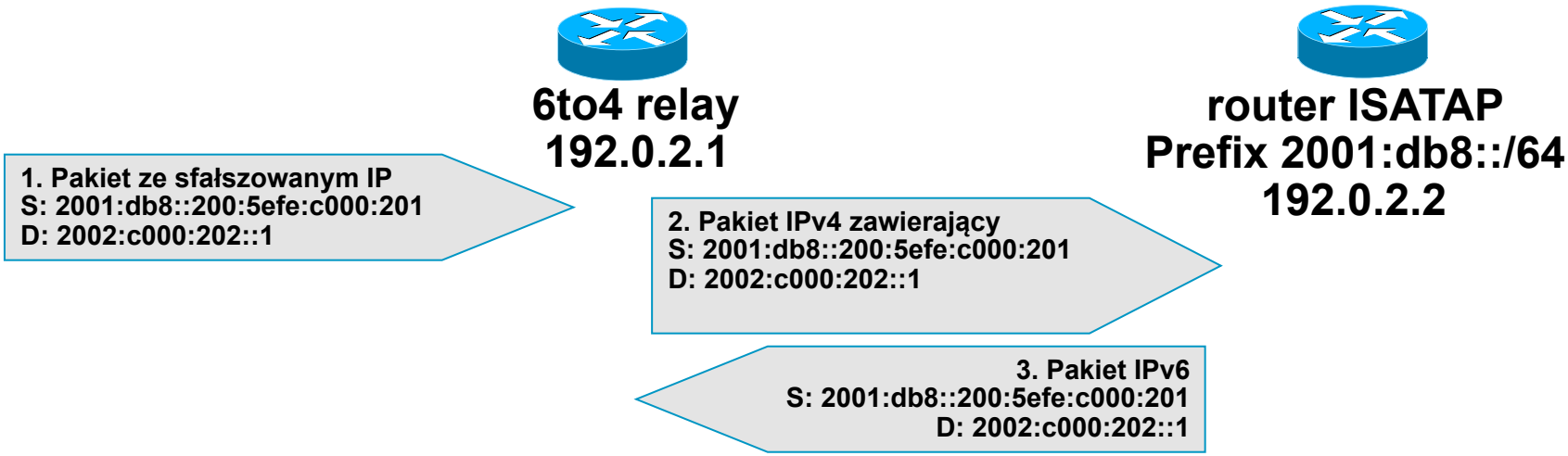
µTorrrent 1.8 (sierpień 2008!)



http://asert.arbornetworks.com/2009/09/who-put-the-ipv6-in-my-internet/

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

Atak zapętlenia pomiędzy ISATAP i 6to4



Pętla do osiągnięcia Hop Limit = 0

- Ten sam protokół (41) ale osadzanie adresu IPv4 w IPv6 dzieje się inaczej
- Router ISATAP akceptuje pakiety 6to4 IPv6 a następnie przekazuje ruch IPv6 z powrotem do relay 6to4
- Ze strony routerów ISATAP: blokujemy pakiety, których adresem źródłowym jest ich adres 6to4
- Dużo trudniejsze na relay'u 6to4 – zablokować wszystkie adresy link-local

http://www.usenix.org/events/woot09/tech/full_papers/nakibly.pdf

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

Gotowe, dzisiaj dostępne narzędzia

- Narzędzia do podsłuchiwania i analizy ruchu
  - Snort
  - TCPdump
  - snoop
  - COLD
  - Wireshark (+pcap/winpcap)
  - Windump
- Zestaw „wszystko w jednym”:
  - THC IPv6 Attack Toolkit: parasite6, alive6, fake_router6, redir6, toobig6, detect-new-ip6, dos-new-ip6, fake_mld6, fake_mipv6, fake_advertiser6, smurf6, rsmurf6
- Skanery
  - IPv6 security scanner
  - Halfscan6
  - Nmap
  - Strobe
  - Netcat
- Narzędzia DoS
  - 6tunneldos
  - 4to6ddos
  - Imps6-tools
- Tworzenie pakietów
  - Scapy6
  - SendIP
  - Packit
  - Spak6

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

Wykrywanie włamań przez IPS dla IPv6

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions			Type	Engine	Retired
						Alert and Log	Deny	Other			
1600/0	ICMPv6 zero length option	✓	Medium	90	67	Alert	Packet		Default	Atomic IPv6	No
1601/0	ICMPv6 option type 1 violation	✓	Medium	75	56	Alert	Packet		Default	Atomic IPv6	No
1602/0	ICMPv6 option type 2 violation	✓	Medium	75	56	Alert	Packet		Default	Atomic IPv6	No
1603/0	ICMPv6 option type 3 violation	✓	Medium	75	56	Alert	Packet		Default	Atomic IPv6	No
1604/0	ICMPv6 option type 4 violation		Medium	75	56	Alert	Packet		Default	Atomic IPv6	No
1605/0	ICMPv6 option type 5 violation	✓	Medium	75	56	Alert	Packet		Default	Atomic IPv6	No
1606/0	ICMPv6 short option data		Medium	75	56	Alert	Packet		Default	Atomic IPv6	No
1610/0	ICMPv6 Echo Request		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1611/0	ICMPv6 Echo Reply		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1612/0	ICMPv6 Destination Unreachable		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1613/0	ICMPv6 Packet Too Big Message		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1614/0	ICMPv6 Time Exceeded Message		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1615/0	ICMPv6 Parameter Problem Message		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1616/0	ICMPv6 Group Membership Query		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1617/0	ICMPv6 Group Membership Report		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1618/0	ICMPv6 Membership Reduction	✓	Informational	100	25	Alert			Default	Atomic IP Advanced	No
1619/0	ICMPv6 Router Solicitation		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1620/0	ICMPv6 Router Advertisement		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1621/0	ICMPv6 Neighbor Solicitation		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1622/0	ICMPv6 Neighbor Advertisement		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1623/0	ICMPv6 Redirect		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1624/0	ICMPv6 Router Renumbering		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1625/0	ICMPv6 Membership Report V2		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1626/0	Large ICMPV6 Traffic		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1627/0	Fragmented ICMPv6 Traffic		Informational	100	25	Alert			Default	Atomic IP Advanced	Yes
1628/0	ICMPv6 Traffic over IPv4	✓	Medium	100	75	Alert			Default	Atomic IP Advanced	No
1630/0	ICMPv6 Packet Too Big	✓	Medium	100	75	Alert			Default	Atomic IP Advanced	No
36606/0	Cisco IOS ICMPv6 Fingerprinting Vulnerability	✓	Low	85	42	Alert			Default	Atomic IP Advanced	No

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

Podsumowanie

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

(nie)bezpieczeństwa związane z IPv6

- Dowolna sieć może być tak bezpieczna, jak osoba, która ją zabezpieczała
- Nie kopiujcie na ślepo zaleceń dla IPv4 do IPv6 – w szczególności konfiguracji
  - trzeba posłużyć się wiedzą i zdrowym rozsądkiem
  - wiele pracy zostało już wykonane, ale czasami wymaga przemyślenia od podstaw
- Nie walczcie z IPv6 – postarajcie się go pokochać ☺
  - NAT nie jest potrzebny, jeden krok mniej przy korelacji/ zabezpieczaniu usług
  - autokonfiguracja, mobilność, publiczna przestrzeń adresowa

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

(nie)bezpieczeństwa związane z IPv6

- Jeśli nie macie jeszcze IPv6 "w domu" – skorzystajcie **DZISIAJ** z Hurricane Electric lub Sixxs

  http://ipv6.he.net/

  http://www.sixxs.net

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

Pytania?

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

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