CCIE.PL
POWERING your KNOWLEDGE.

ATM SI

IPv6 – dwa kliknięcia i działa



Piotr Wojciechowski (CCIE #25543)
Starszy Konsultant ds. Sieci
PLNOG 2011, Warszawa, 16-17 Marca 2011

Agenda

- Czy jesteśmy gotowi na IPv6?
- Jedno kliknięcie i działa – ale czy bezpiecznie?
- Kilka modeli wdrożenia IPv6 u operatora
- WLAN na konferencji PLNOG

Czy jesteśmy gotowi na IPv6?

- TAK!
  - Coraz więcej urządzeń obsługuje IPv6
  - Coraz więcej zasobów dostępnych jest po IPv6
  - Coraz więcej firm i operatorów przejmuje się problemem braku adresacji IPv4 i testuje modele wdrożenia IPv6
  - Adresacja IPv6 sprzedawana jest „w pakiecie”
  - Systemy operacyjne i urządzenia CE dojrzewają do IPv6

Czy jesteśmy gotowi na IPv6?

- NIE!
  - Nadal spora liczba urządzeń sieciowych (modemy, routery) nie wspiera IPv6
  - Zastraszająco duża liczba urządzeń sieciowych nie oferuje mechanizmów ochrony sieci IPv6
  - Użytkownicy wyłączają firewalle na swoich komputerach
  - Administratorzy nie są przystosowani do utrzymywania infrastruktury i serwisów działających w oparciu o IPv6
  - Niedobór narzędzi diagnostycznych i monitorujących

IPv6 z punktu widzenia operatora

- Technikalia
  - Routery i routing
  - Adresacja i jej przydział
- Content
  - Dostęp do zasobów po IPv6
- Bezpieczeństwo
  - Autoryzacja i blokowanie użytkowników
  - Zabezpieczenie treści
  - VPNy

IPv6 z punktu widzenia przeciętnego użytkownika

- „Panie, co mi Pan o jakimś IPv6 mówi, mówię, że mi Internet nie działa bo nie mogę się do ulubionej strony dostać”
  - Przeciętny Kowalski nie ma pojęcia o IPv4 i IPv6
  - Przeciętny Kowalski kupuje usługę pt. Internet i oczekuje, że będzie mógł skutecznie otworzyć ulubioną stronę czy pogadać przez Skype

Agenda

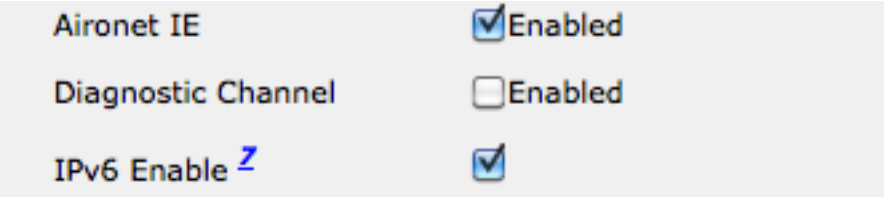
- Czy jesteśmy gotowi na IPv6?
- **Jedno kliknięcie i działa – ale czy bezpiecznie?**
- Kilka modeli wdrożenia IPv6 u operatora
- WLAN na konferencji PLNOG

IPv6 – jedno kliknięcie i działa

- Uruchomienie IPv6 nie stwarza problemów:

```
Router(config)#ipv6 unicast-routing
Router(config)#interface Fa0/0
Router(config-if)#ipv6 enable
```

- Transparentne przenoszenie protokołu IPv6 w większości urządzeń działa domyślnie, na niektórych trzeba je aktywować ręcznie (chyba, że ruch IPv6 jest domyślnie odrzucany)



IPv6 – protekcja przed atakami od strony klienta

- Większość urządzeń sieciowych jest nieprzygotowana na ataki mogące pochodzić od naszych klientów
- Specyfikacja ICMPv6 nie przewidziała zabezpieczenia przed atakami na ten protokół pochodzącymi z sieci lokalnej – potencjalnie każdy użytkownik może nam napsuć krwi.
- Rozwiązanie - *SEcure Neighbor Discovery (SEND) – RFC 3971*
  - Zaprzęgnięcie kryptografii w proces tworzenia adresu hosta
  - Para kluczy dla każdego węzła uwierzytelniające adres IPv6
  - Linux wspiera SEND, Windows XP I Vista nie.
  - Cisco i Juniper wspierają SEND na swoich platformach

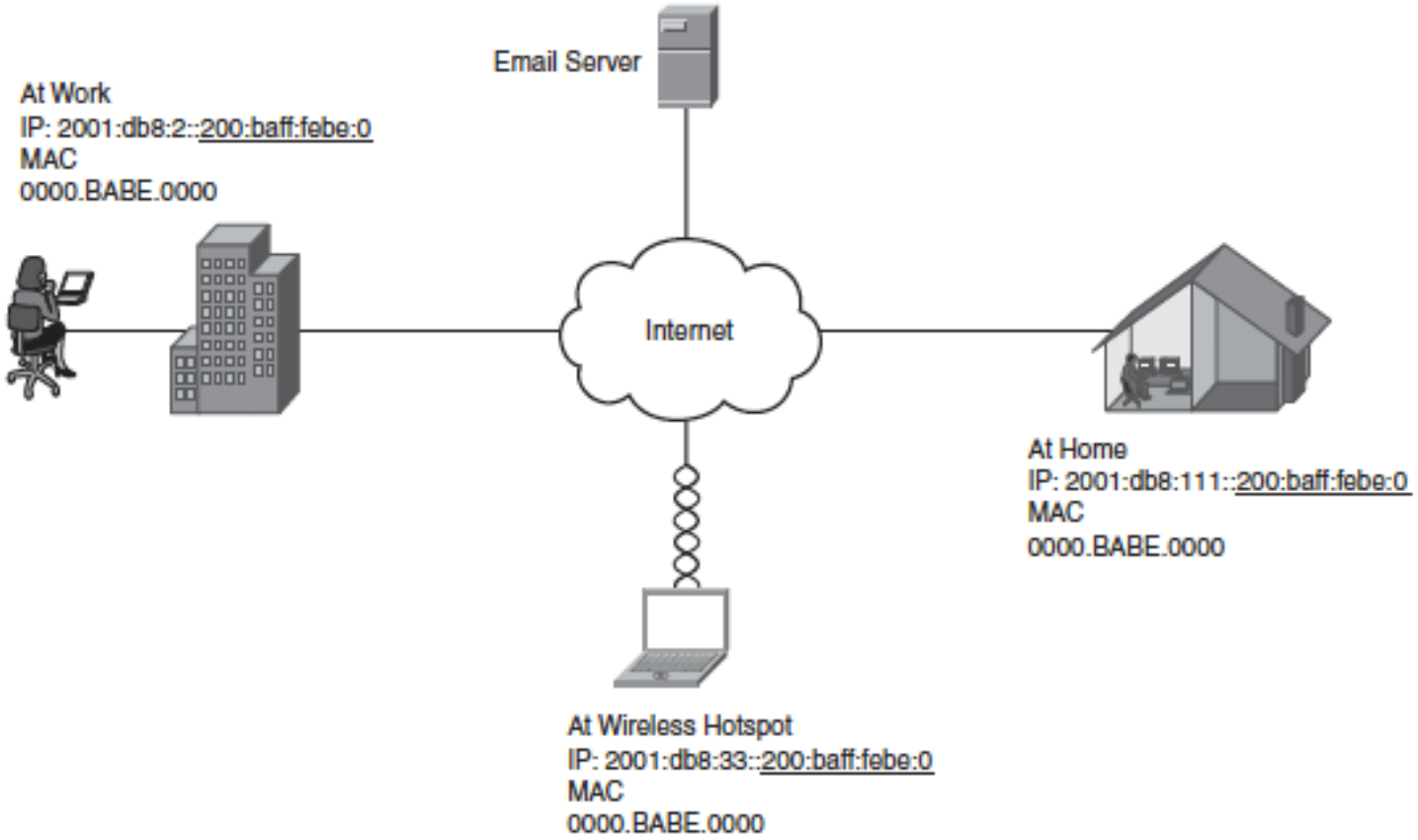
IPv6 – protekcja przed atakami od strony klienta

- Wykrywanie *Rogue RA Messages*
  - Niektóre IDSy mają odpowiednie sygnatury – ale taki sensor musimy mieć w każdym segmencie sieci co jest nieefektywne ekonomicznie
  - Istnieją darmowe rozwiązania – NDPMon, Rafixd
- Mechanizmy protekcji powinny być wbudowane w przełączniki tak jak to ma miejsce dla adekwatnych protokołów IPv4
  - IPv6 VLAN ACL
  - IPv6 port ACL
  - IPv6 RA Guard (RFC 6105, February 2011)
  - DHCPv6 Snooping
  - Dynamic NA Inspection
- Używajmy adresacji link-local wszędzie gdzie to możliwe (np. BGP)

IPv6 – protekcja klientów

- Klient otrzymuje adres publiczny jego komputer jest więc zagrożony
- Większość systemów operacyjnych ma zapory sieciowe, które klienci lubią wyłączać
- Zaatakowany komputer użytkownika końcowego to potencjalne zagrożenie dla bezpieczeństwa naszej sieci.

Prywatność w sieciach IPv6



Source: IPv6 Security, CiscoPress

IPv6 – Privacy Issue with EUI-64 Address

- Problem opisany w 1999, ubrany w formułę RFC 3041 “Privacy Extensions for Stateless Address Autoconfiguration in IPv6” w 2001 roku, zaaktualizowany przez RFC 4941
- Rozwiązanie – generowanie części adresu bazującego na EUI-64 przy użyciu funkcji hashującej MD5.
- Prawie zerowe prawdopodobieństwo wystąpienia zduplikowanych adresów – a nawet jeżeli to mamy DAD
- Hosty okresowo generują nowy adres IPv6 zachowując przy tym stary dla ciągłości już aktywnych transmisji

IPv6 – Privacy Issue with EUI-64 Address

- Windows XP, Vista, 7 domyślnie używają rozszerzeń prywatności przy generowaniu adresów IPv6.
- Większość dystrybucji Linuxa także z nich domyślnie korzysta
- MacOS X Snow Leopard domyślnie generuje adres w sposób standardowy!
- Funkcjonalność ta często jest wyłączana w politykach korporacyjnych

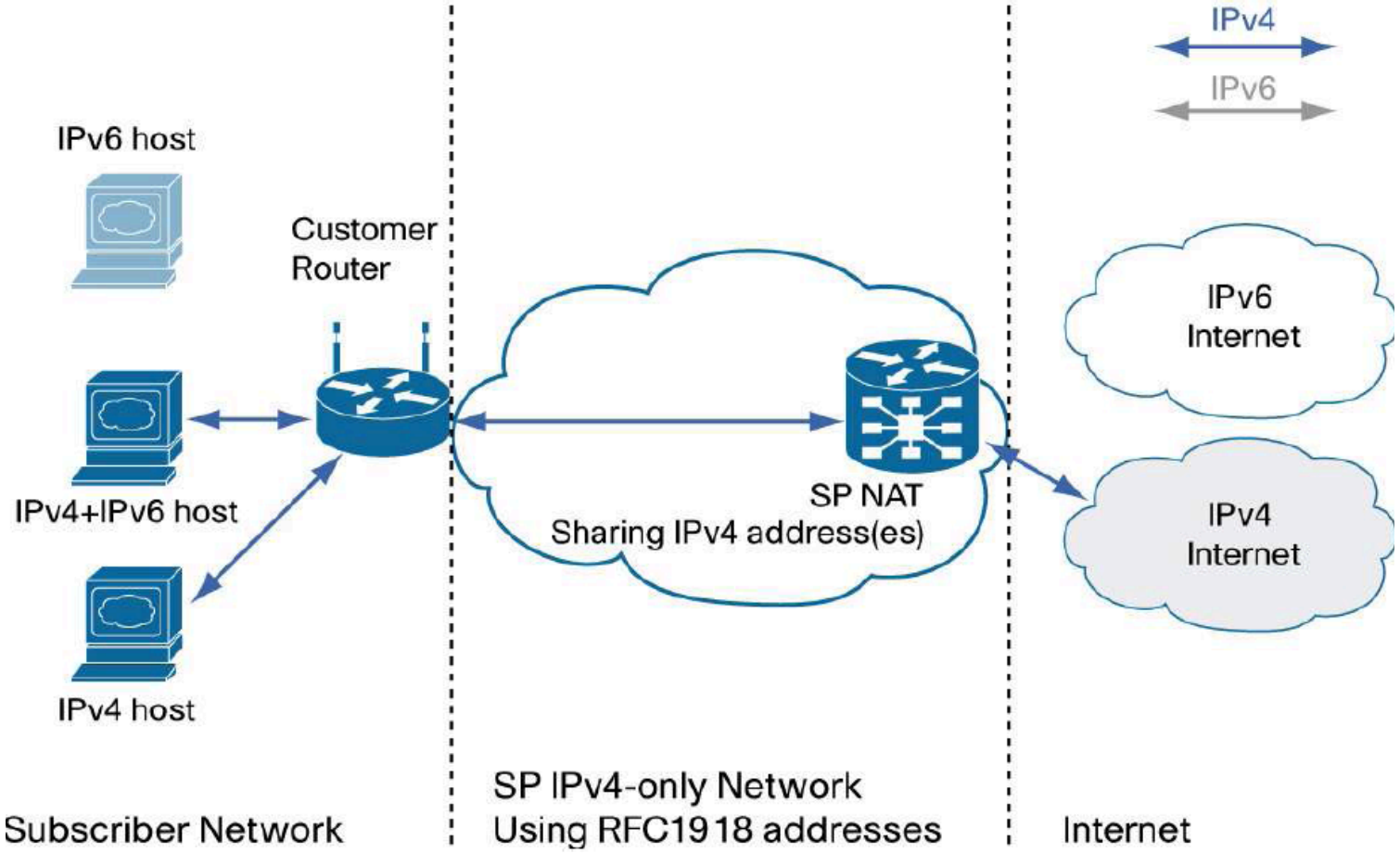
Agenda

- Czy jesteśmy gotowi na IPv6?
- Jedno kliknięcie i działa – ale czy bezpiecznie?
- **Kilka modeli wdrożenia IPv6 u operatora**
- WLAN na konferencji PLNOG

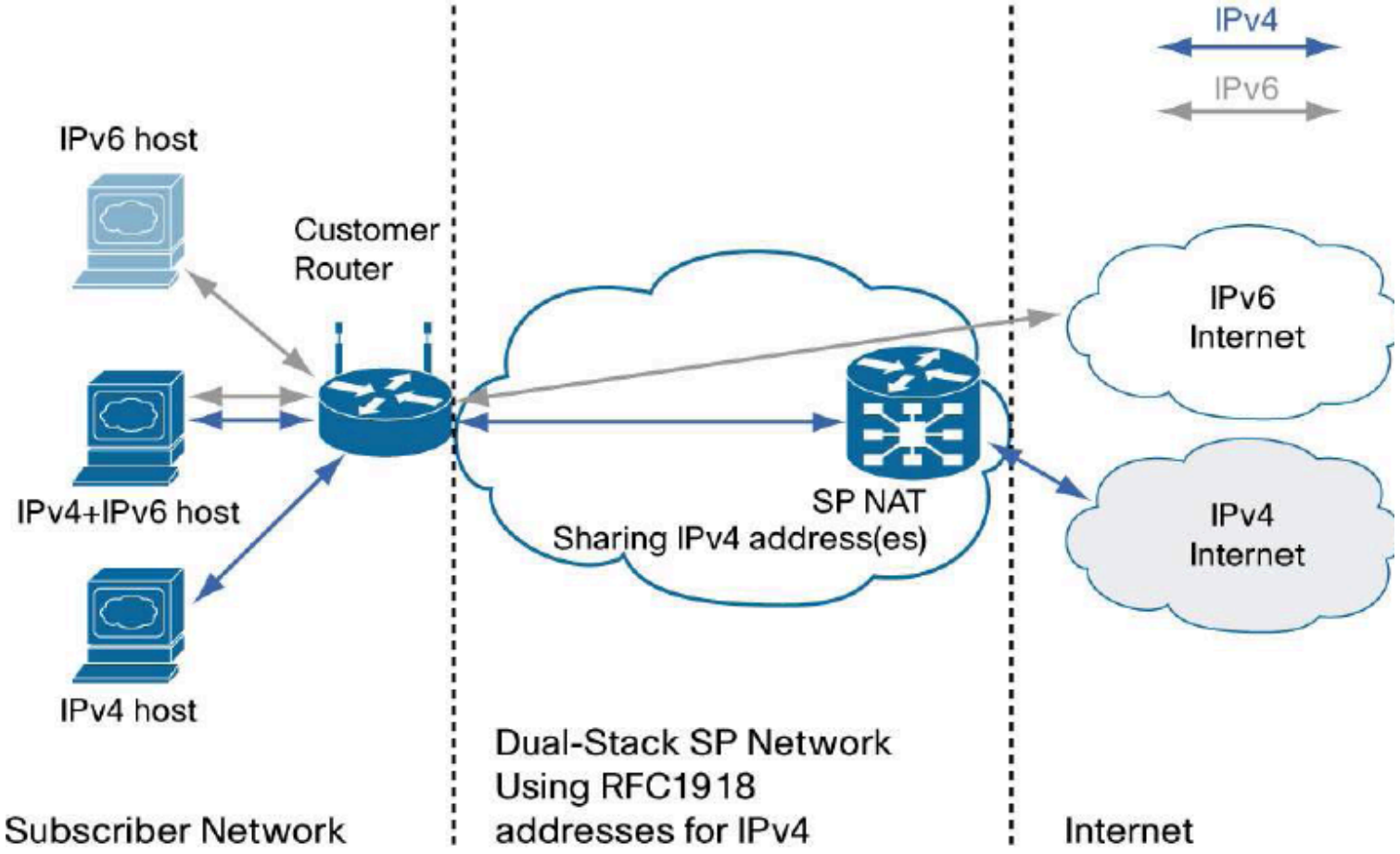
Podejście do braku adresacji IPv4

- Co może zrobić provider, gdy skończą się adresy IPv4
  - Nic, gdyż nie oczekuje rozwoju swojego biznesu
  - Przedłużać życie adresacji IPv4
    - Przejąć adresy od innej firmy
    - Współdzielić adresację pomiędzy wielu swoich klientów (NAT44)
  - Wdrażać IPv6 dla nowych klientów zapewniając połączenie i translację pomiędzy sieciami IPv6 i IPv4
- Podejścia te nie są rozłączne!
- Ponad 16 dobrze opisanych modeli migracji do IPv6

Przykładowe modele wdrożeń
IPv4 only + NAT44



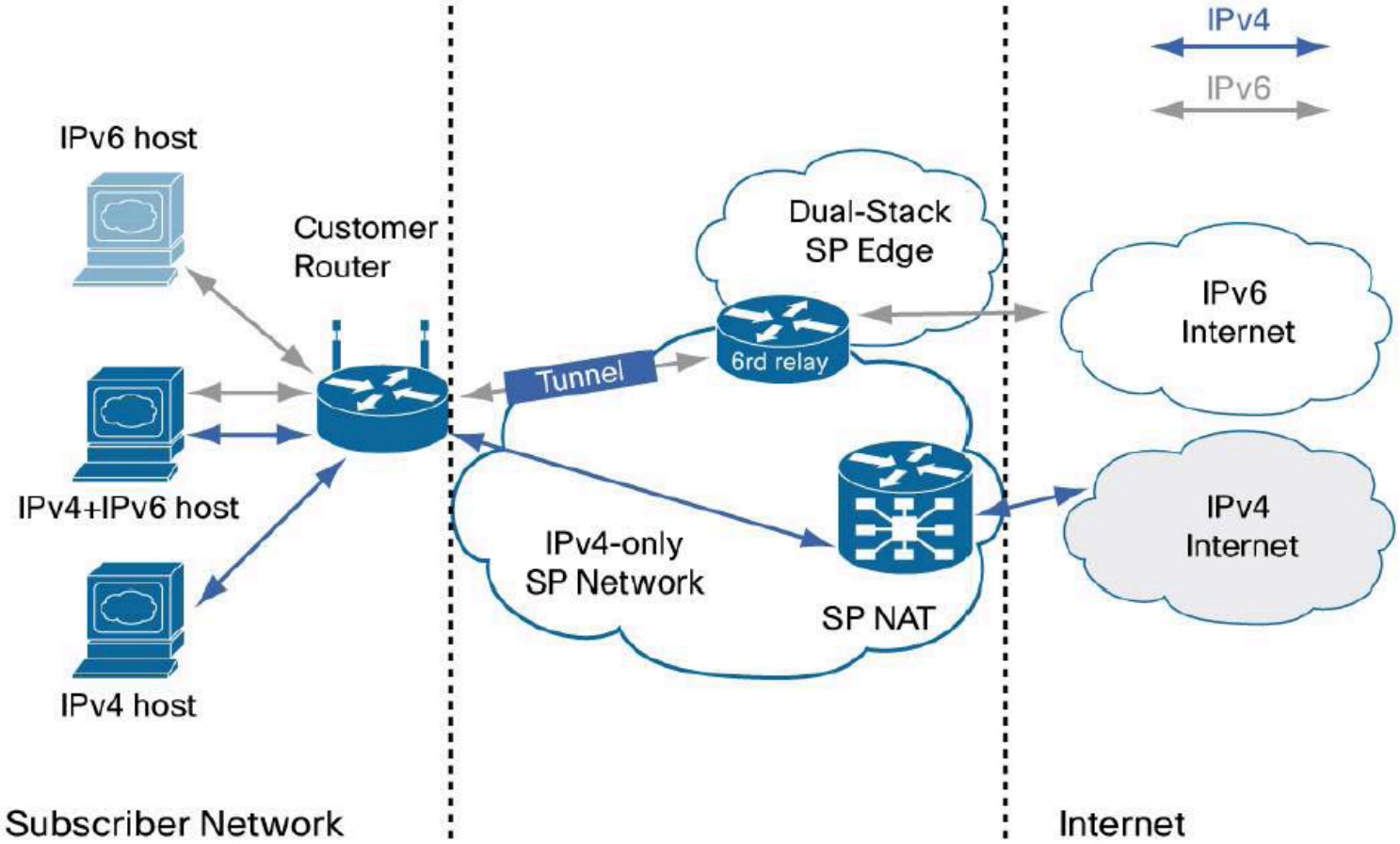
Przykładowe modele wdrożeń
Dual-Stack + NAT44



Przykładowe modele wdrożeń
Dual-Stack + NAT44

- Zalety:
  - Świadczymy obecnym klientom usługi po IPv4 (adres publiczny lub prywatny i SP NAT)
  - Uruchamiamy obecnym klientom dual-stack dając im dostęp do zasobów IPv6
  - Uczymy siebie i swoich klientów czym jest IPv6 – nie opóźniamy światowej migracji do nowego protokołu
  - Ograniczenia dt. NAT nie obejmują usług IPv6
- Wady:
  - Wszystkie problemy z NAT44, w tym konieczność wdrażania CGN u dużych dostawców
  - Dodatkowy koszt utrzymania sieci IPv4 i IPv6 jednocześnie

Przykładowe modele wdrożeń
Dual-Stack + 6rd + NAT44



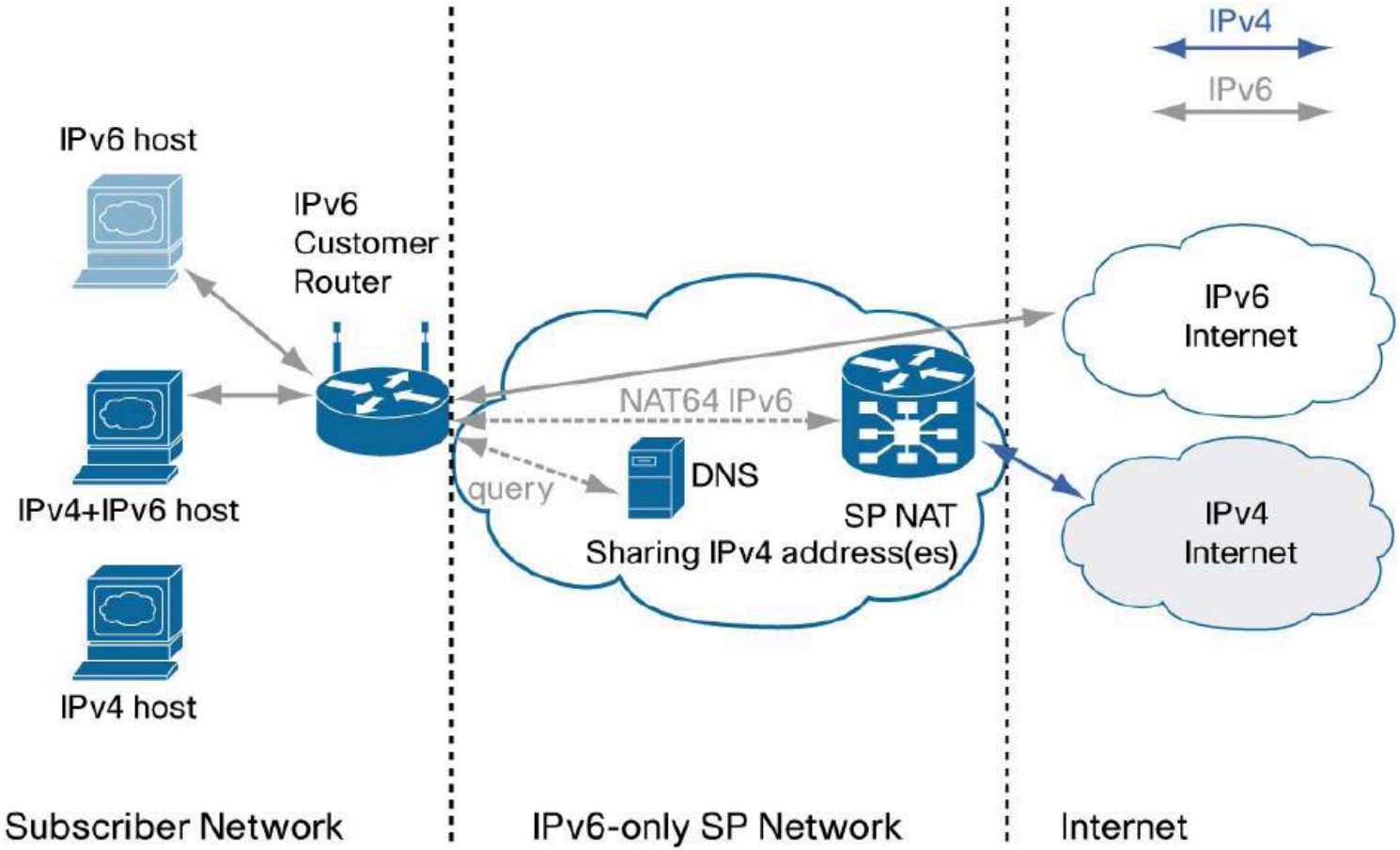
Przykładowe modele wdrożeń
Dual-Stack + 6rd + NAT44

- Zalety:
  - 6rd da się wdrożyć szybko i nie wymaga aktywacji IPv6 w całym szkielecie
  - Nie potrzebuje IPv6 w sieci dostępowej i agregacyjnej
  - 6rd działa jako stateless, więc nie wymaga bardzo dużych zasobów
  - Na rynku są urządzenia zarówno CPE jak i operatorskie
  - 6rd to nie są tunele 6to4 (i całe szczęście) – nie wymaga prefiksu 2002::/16, można skonfigurować dowolną pulę z adresacji unicast operatora
  - Dostęp do zasobów IPv4 może być za pomocą adresacji publicznej jak i prywatnej

Przykładowe modele wdrożeń
Dual-Stack + 6rd + NAT44

- Wady:
  - Tunelowanie musi zostać usunięte gdy IPv6 zostanie wdrożone w szkielecie operatora
  - Firmware urządzeń CPE może wymagać aktualizacji by wspierać 6rd
  - Trzeba wdrożyć jeden lub więcej punktów terminacji dla tuneli
  - Masa tuneli w sieci – potencjalnie masa kłopotów

Przykładowe modele wdrożeń
NAT64 (Statefull AFT)



Przykładowe modele wdrożeń
NAT64 (Statefull AFT)

- Zalety:
  - Nie jesteśmy ograniczeni brakiem adresacji IPv4 w rozwoju sieci
  - Usługi dostępne natywnie IPv6
  - Sięć operatorska bazuje tylko na IPv6 – IPv6 tylko na styku z CGN
- Wady:
  - Koszt wdrożenia usługi NAT64 (CGN) może być wysoki w zależności od liczby abonentów w siec
  - Infrastruktura DNS wymaga dostosowania do świadczenia usługi NAT64
  - Urządzenia szkieletowe, CPE i klienckie muszą obsługiwać IPv6 – urządzenia IPv4-only nie będą mogły pracować w sieci

Agenda

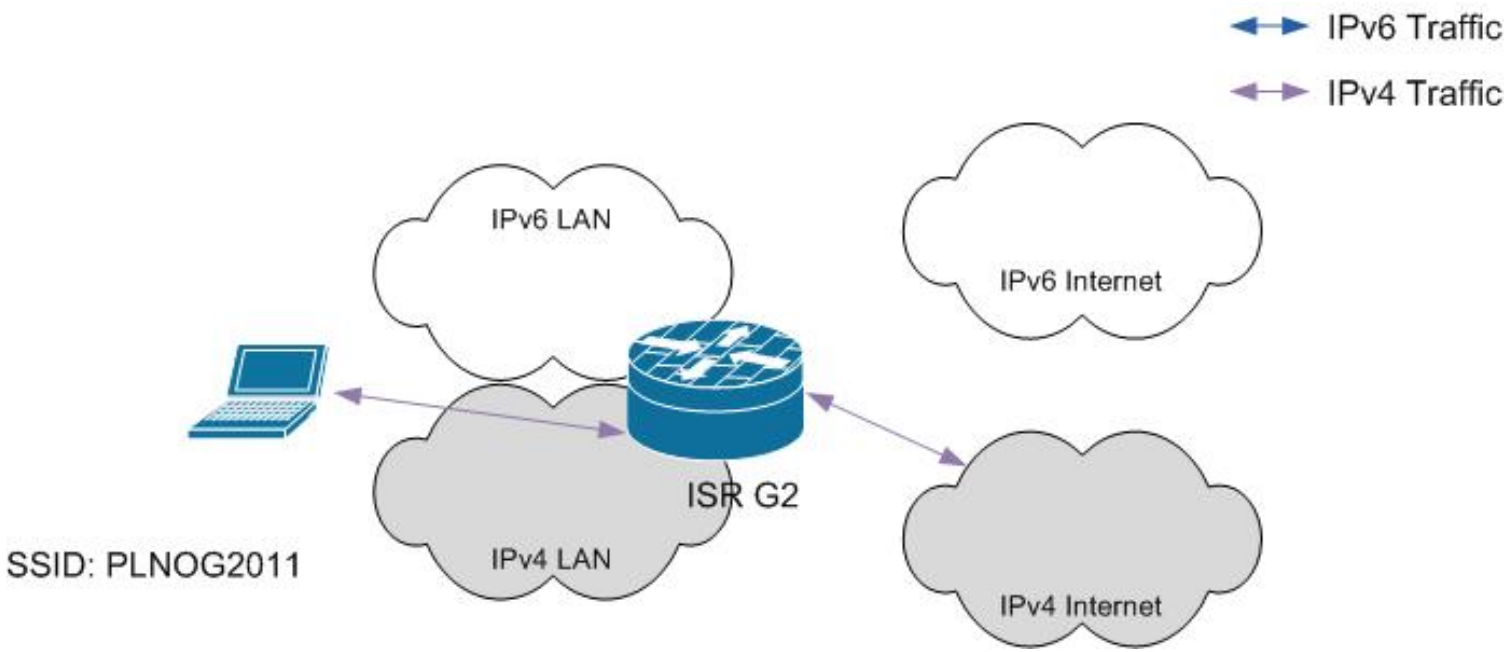
- Czy jesteśmy gotowi na IPv6?
- Jedno kliknięcie i działa – ale czy bezpiecznie?
- Kilka modeli wdrożenia IPv6 u operatora
- **WLAN na konferencji PLNOG**

WLAN PLNOG 2011 w praktyce

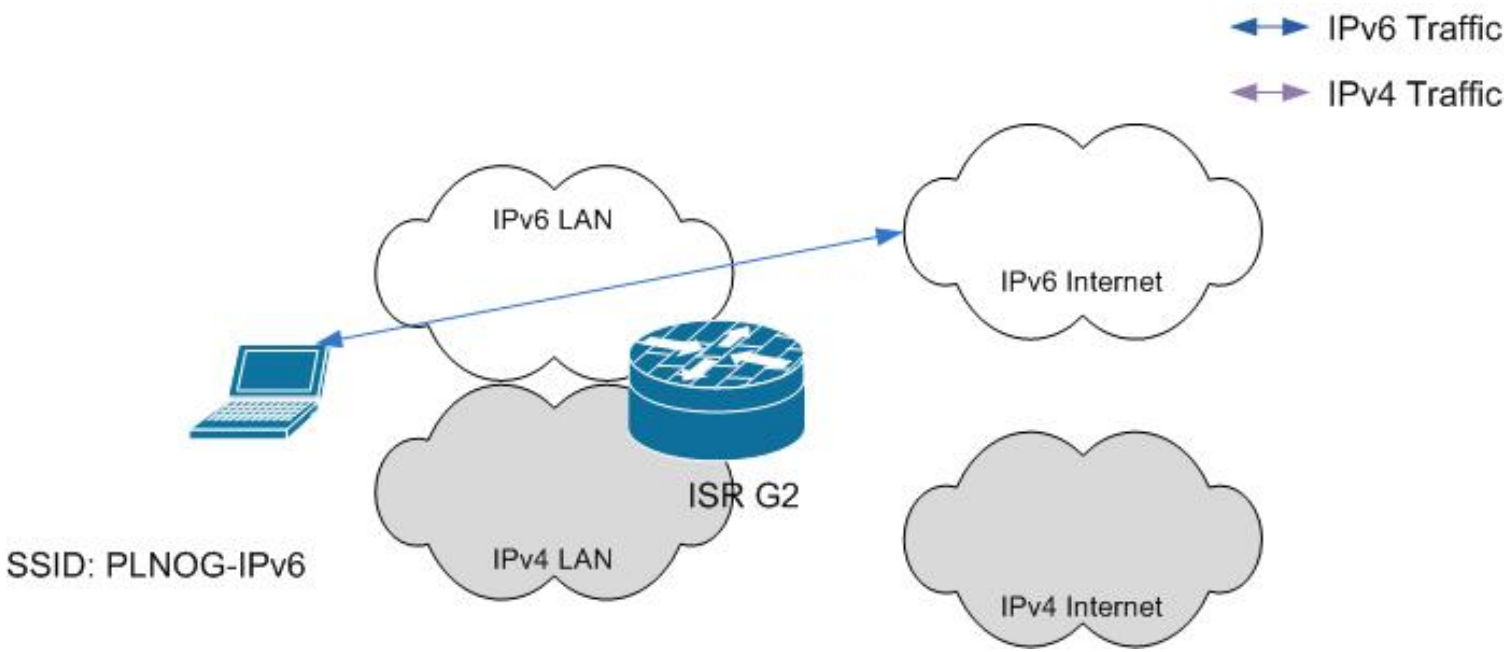
- Co mamy:
  - Kontroler WLC 4402
  - AP 1142
  - Switch
  - Router

- Stworzyliśmy 3 sieci WLAN

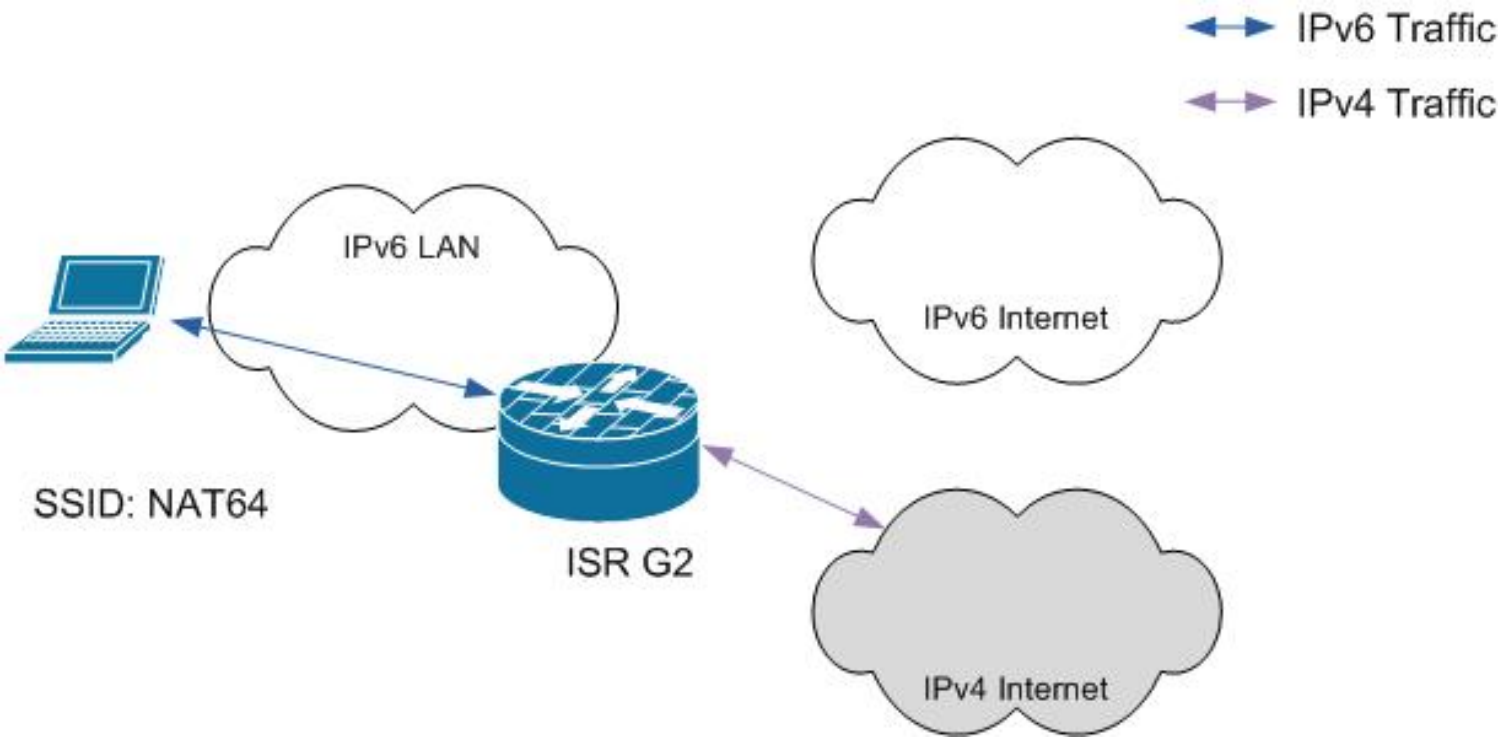
WLAN PLNOG 2011 w praktyce



WLAN PLNOG 2011 w praktyce

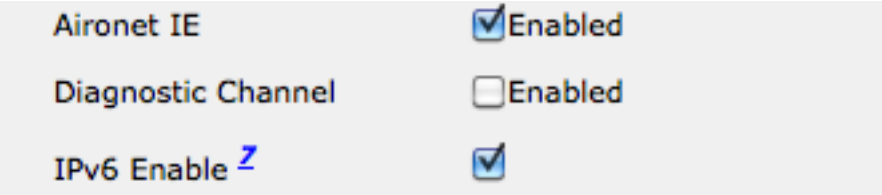


WLAN PLNOG 2011 w praktyce



WLAN PLNOG 2011 w praktyce

- To było proste – jedno kliknięcie w konfiguracji WLC i IPv6 jest transparentnie przenoszone



- Konfiguracja interfejsów i DHCPv6 serwera podręcznikowo prosta :)

WLAN PLNOG 2011 w praktyce
Native IPv6

```
ipv6 dhcp pool IPv6
 dns-server 2001:1A68::55E8:E266
 dns-server 2001:1A68::4D4F:EB66
!
interface GigabitEthernet0/0.6
 description IPv6 native interface
 encapsulation dot1Q 6
 ipv6 address 2A02:2978:1:1::1/64
 ipv6 enable
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
 ipv6 nd ra lifetime 60
 ipv6 nd ra interval 10
 ipv6 dhcp server IPv6
```

WLAN PLNOG 2011 w praktyce
NAT64

```
ipv6 dhcp pool NAT64
 dns-server FC00:64:64::D911:220A
!
interface GigabitEthernet0/0.64
 encapsulation dot1Q 64
 ipv6 address FC00:64::1/64
 ipv6 enable
 ipv6 nd other-config-flag
 ipv6 nat
 ipv6 dhcp server NAT64
!
ipv6 nat v4v6 source 217.17.34.10 FC00:64:64::D911:220A
ipv6 nat v6v4 source list v6 interface GigabitEthernet0/1 overload
ipv6 nat prefix FC00:64:64::/96 v4-mapped v6
!
ipv6 access-list v6
 permit ipv6 FC00:64::/64 FC00:64:64::/96
```

WLAN PLNOG 2011 w praktyce
NAT64 – weryfikacja (podejście inżynierskie)

ATM SI

54	43.904404	Apple_12:cc:0b	Cisco-Li_0c:23:0a	ARP	Who has 192.168.1.254? Tell 192.168.1.5
55	43.905112	Apple_12:cc:0b	Cisco_9d:6c:00	ARP	Who has 10.127.0.1? Tell 10.127.0.11
56	45.892564	fe80::1edf:fff:fe9d:6c00	ff02::1	ICMPv6	Router advertisement from 1c:df:0f:9d:6c:00
57	58.247923	fe80::226:bbff:fe12:cc0b	ff02::2	ICMPv6	Multicast listener done (Unknown (0x00))
58	60.379304	fe80::226:bbff:fe12:cc0b	ff02::1:ff12:cc0b	ICMPv6	Multicast listener report
59	60.382995	Apple_12:cc:0b	Cisco-Li_0c:23:0a	ARP	Who has 192.168.1.254? Tell 192.168.1.5
60	60.383029	Apple_12:cc:0b	Cisco_9d:6c:00	ARP	Who has 10.127.0.1? Tell 10.127.0.11

```
▷ Frame 56: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
▷ Ethernet II, Src: Cisco_9d:6c:00 (1c:df:0f:9d:6c:00), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
▷ Internet Protocol Version 6, Src: fe80::1edf:fff:fe9d:6c00 (fe80::1edf:fff:fe9d:6c00), Dst: ff02::1 (ff02::1)
▽ Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0xf5ca [correct]
    Cur hop limit: 64
  ▽ Flags: 0x48
      0... .... = Not managed
      .1.. .... = Other
      ..0. .... = Not Home Agent
      ...0 1... = Router preference: High
      .... .0.. = Not Proxied
    Router lifetime: 60
    Reachable time: 0
    Retrans timer: 0
  ▽ ICMPv6 Option (Source link-layer address)
      Type: Source link-layer address (1)
      Length: 8
```

WLAN PLNOG 2011 w praktyce
NAT64 – weryfikacja (podejście inżynierskie)

```
nb-382:~ peper$ ifconfig en1
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 00:26:bb:12:cc:0b
        inet6 fe80::226:bbff:fe12:cc0b%en1 prefixlen 64 scopeid 0x6
        inet6 fc00:64::226:bbff:fe12:cc0b prefixlen 64 autoconf
        inet 169.254.217.1 netmask 0xffff0000 broadcast 169.254.255.255
        media: autoselect
        status: active
```

WLAN PLNOG 2011 w praktyce
NAT64 – weryfikacja (podejście inżynierskie)

```
nb-382:~ peper$ mtr fc00:64:64::217.17.34.10 --report
HOST: Anomander.local             Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. fc00:64::1                   10.0%    10    9.4 248.9   6.4 1385. 490.9
  2. fc00:64:64::d911:220a        10.0%    10   20.5 235.2   5.7 1343. 458.2


NAT64-PLNOG#   sh ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      217.17.34.10             FC00:64:64::D911:220A

icmp  46.28.245.82,5252        FC00:64::42A6:D9FF:FE5D:54C9,5252
      217.17.34.10,4160        FC00:64:64::D911:220A,4160

udp   46.28.245.82,51653       FC00:64::42A6:D9FF:FE5D:54C9,51653
      217.17.34.10,53          FC00:64:64::D911:220A,53
```

I prawie się udało czyli odkrycia wdrożenia

- Wszystko działa, ale:
  - MacOS X nie pobiera z DHCPv6 adresów serwerów DNS
  - Systemy operacyjne zgłaszają ograniczoną dostępność sieci, jeżeli dostają jedynie adres IPv6
  - Dodatkowe aplikacje przejmujące od systemu kontrolę nad kartami sieciowymi mogą powodować problemy z DHCPv6 oraz samym IPv6
  - Musieliśmy wyłączyć CEF dla IPv6 by NAT64 zadziałał

DZIĘKUJĘ ZA UWAGĘ