WiFi w wydaniu operatorskim

Piotr Chomczyk

piotr.chomczyk@cisco.com

PLNOG #7, Kraków 28-29 września 2011

O czym dzisiaj

- WiFi w wydaniu operatorskim
  - Dlaczego…
- Architektury i technologie
  - Od ręcznego przełożenia…
  - … po pełną automatyzację…
  - …przez kilka faz pośrednich
- Podsumowanie

Słowem wstępu

Wzrost (globalny) ruchu mobilnego

Prognozy mówią o 5mld urządzeń mobilnych i 2mld M2M do 2015

Wolumen ruchu mobilnego ma wzrosnąć 26X, do 6.3 EB/mies

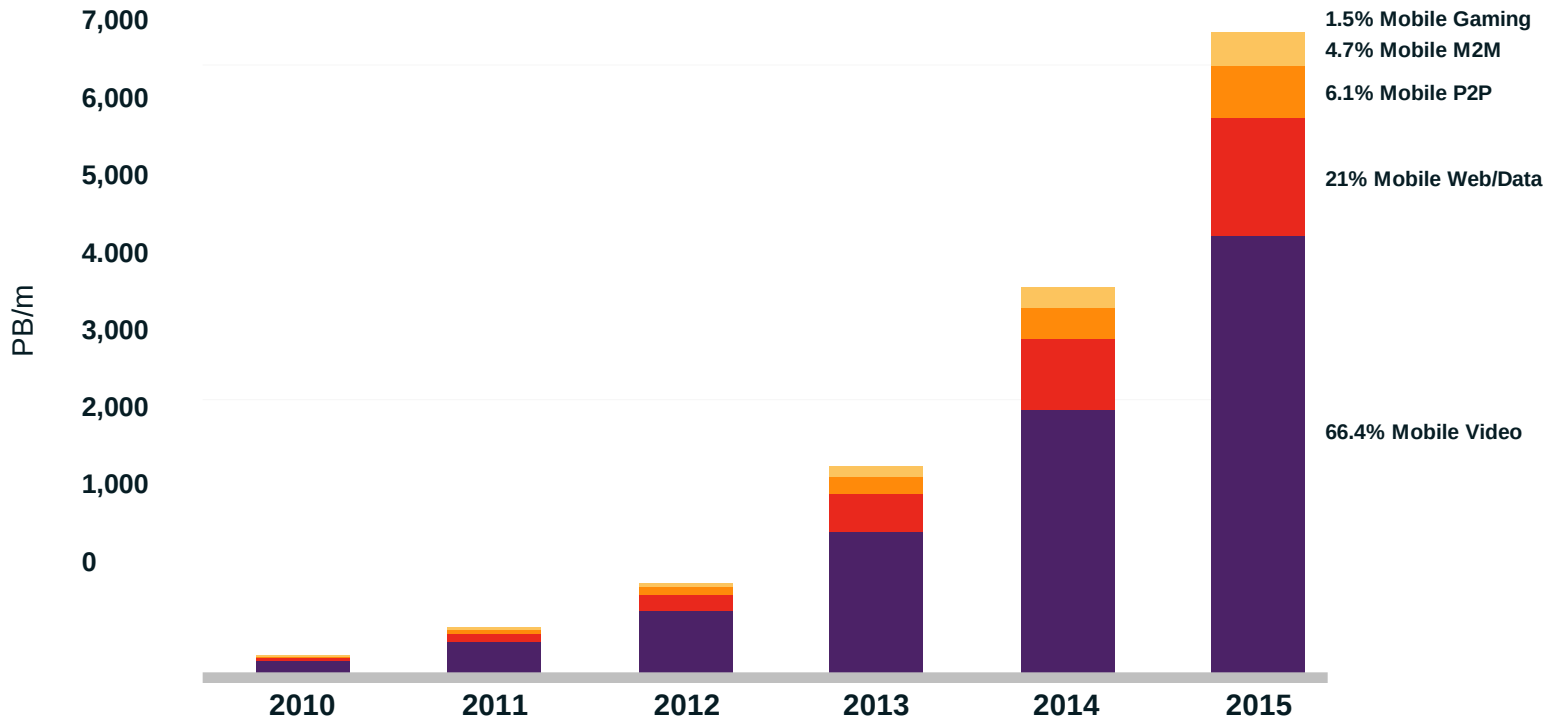
Udział ruchu wideo w 2015 ma przekroczyć 2/3

Źródło: Cisco Visual Networking Index (VNI) Global Mobile Data Forecast, 2010–2015

Zmiana środowiska

Eksplozja mobilnego wideo

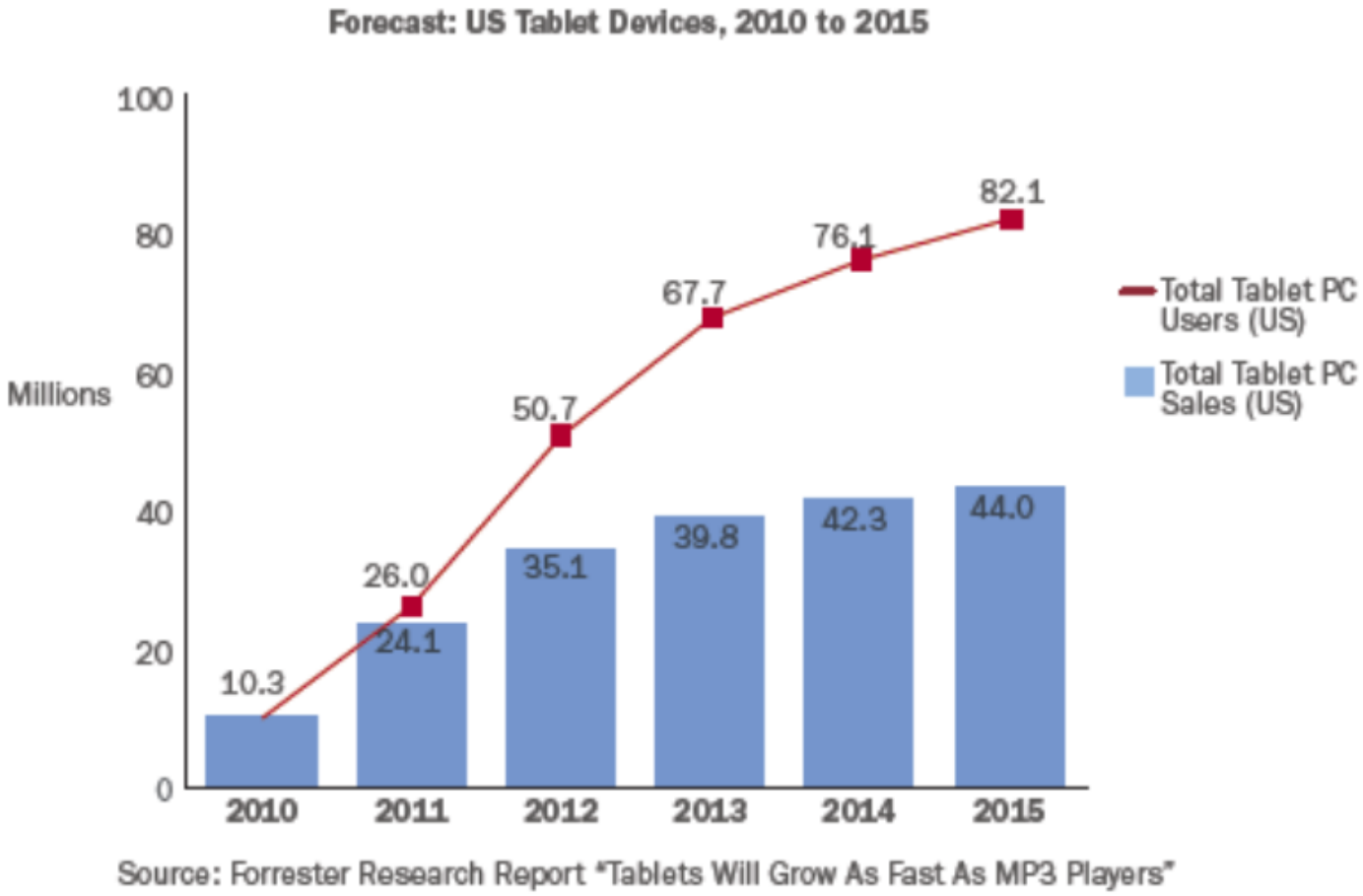
92% CAGR 2010–2015



VoIP - 0.4% ruchu mobilnego w 2015

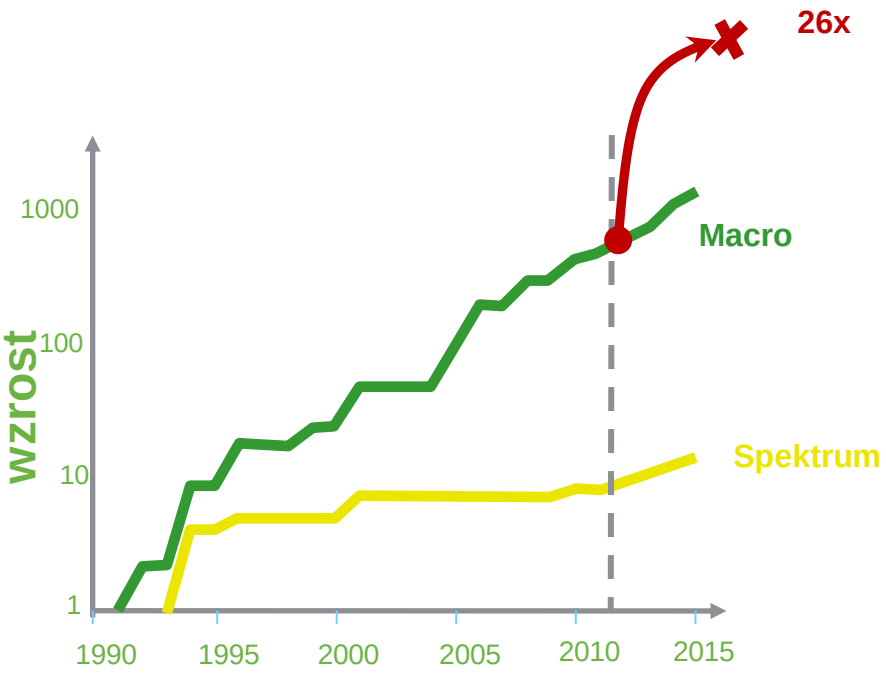
Źródło: Cisco Visual Networking Index (VNI) Global Mobile Data Forecast, 2010–2015

Nowe urządzenia == więcej połączeń



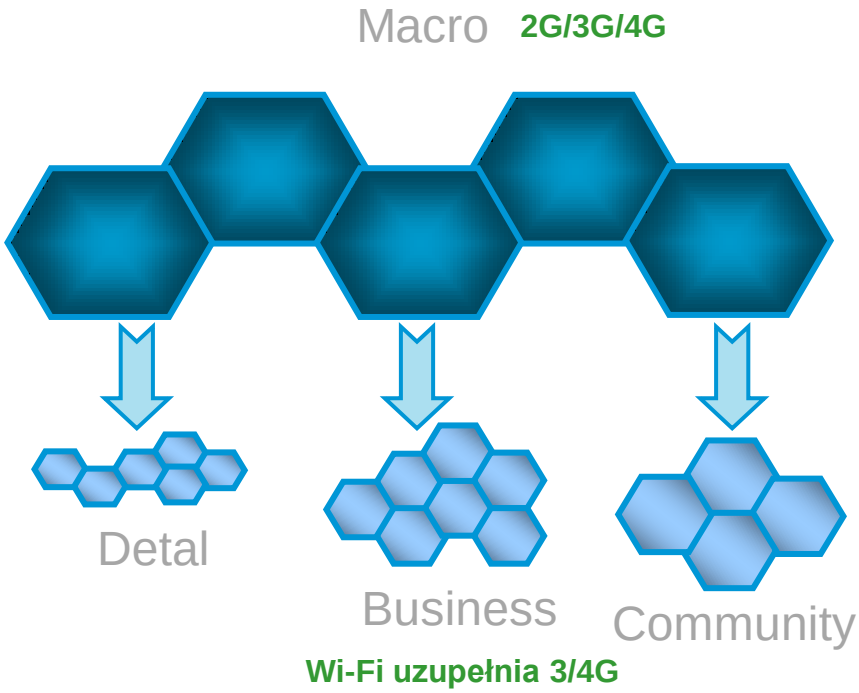
Prognoza sprzedaży PC na 2015 = 38.9M

Pojemność sieci nie nadąża za oczekiwaniami odbiorców



Źródło: Agilent

Małe komórki zwiększają pojemność



Wi-Fi

- MO potrzebują efektywniejszych kosztowo technologii radiowych
- Wi-Fi jest globalne – +/- te same zakresy częstotliwości
- Wi-Fi wbudowane w urządzenia końcowe
- Wi-Fi daje ~5x pasma (MHz) niż technologie komórkowe
- WiFi oferuje platformę do implementacji nowego portfolio usług

Oczami architekta

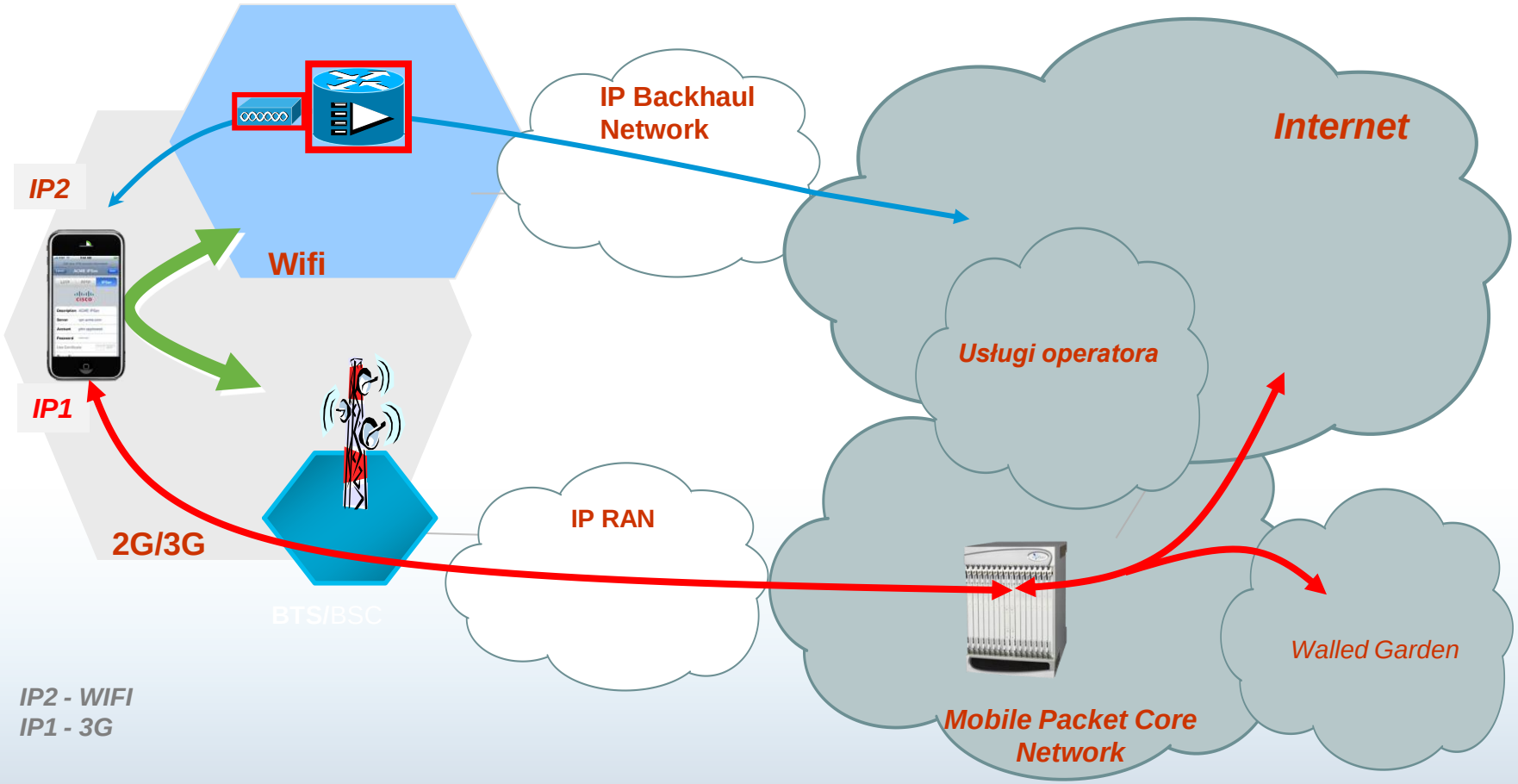
Definiując roaming i mobilność

Roaming

- Użytkownik mobilny (MU) może zostać zautoryzowany w sieci 3G/WiFi, uzyskać dostęp do odpowiednich zasobów i na tej podstawie zostać odpowiednio obciążony
- Adres IP różny dla sieci 3G i WiFi:
  - 3G: IP przydzielone przez HA
  - Wifi: IP przydzielone przez bramę WiFi
- Brak utrzymania połączenia przy przejściu między sieciami WiFi i 3G; może wystąpić konieczność restartu aplikacji (np. klient poczty, VPN)

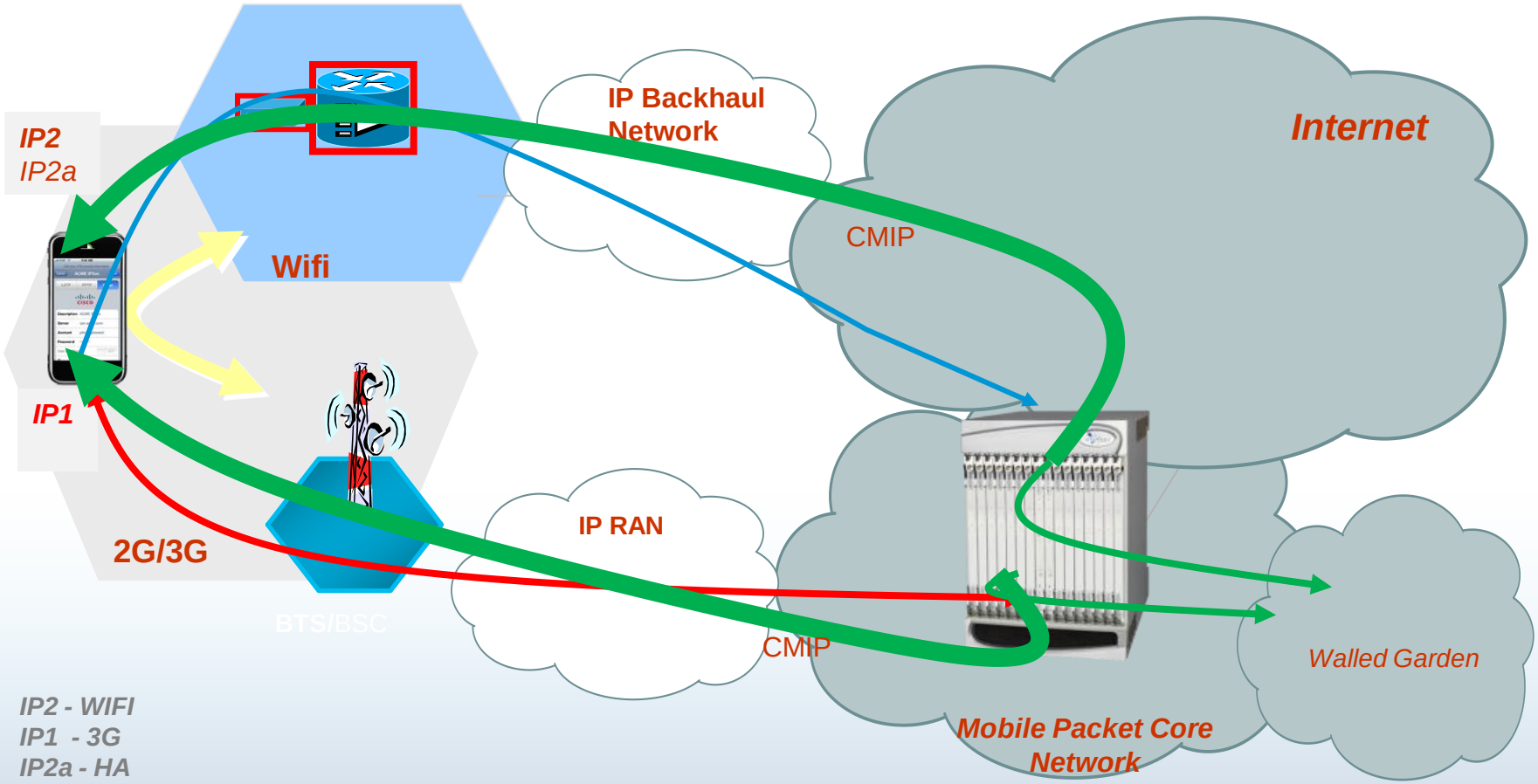
- Mobilność
  - MU może zostać zautoryzowany w sieci 3G/WiFi, uzyskać dostęp do odpowiednich zasobów i na tej podstawie zostać odpowiednio obciążony
  - Adres IP ten sam w 3G i WiFi; przydzielony przez Home Agent
  - Zachowane połączenie na poziomie aplikacji
  - Mobile IP

Prosty Offload



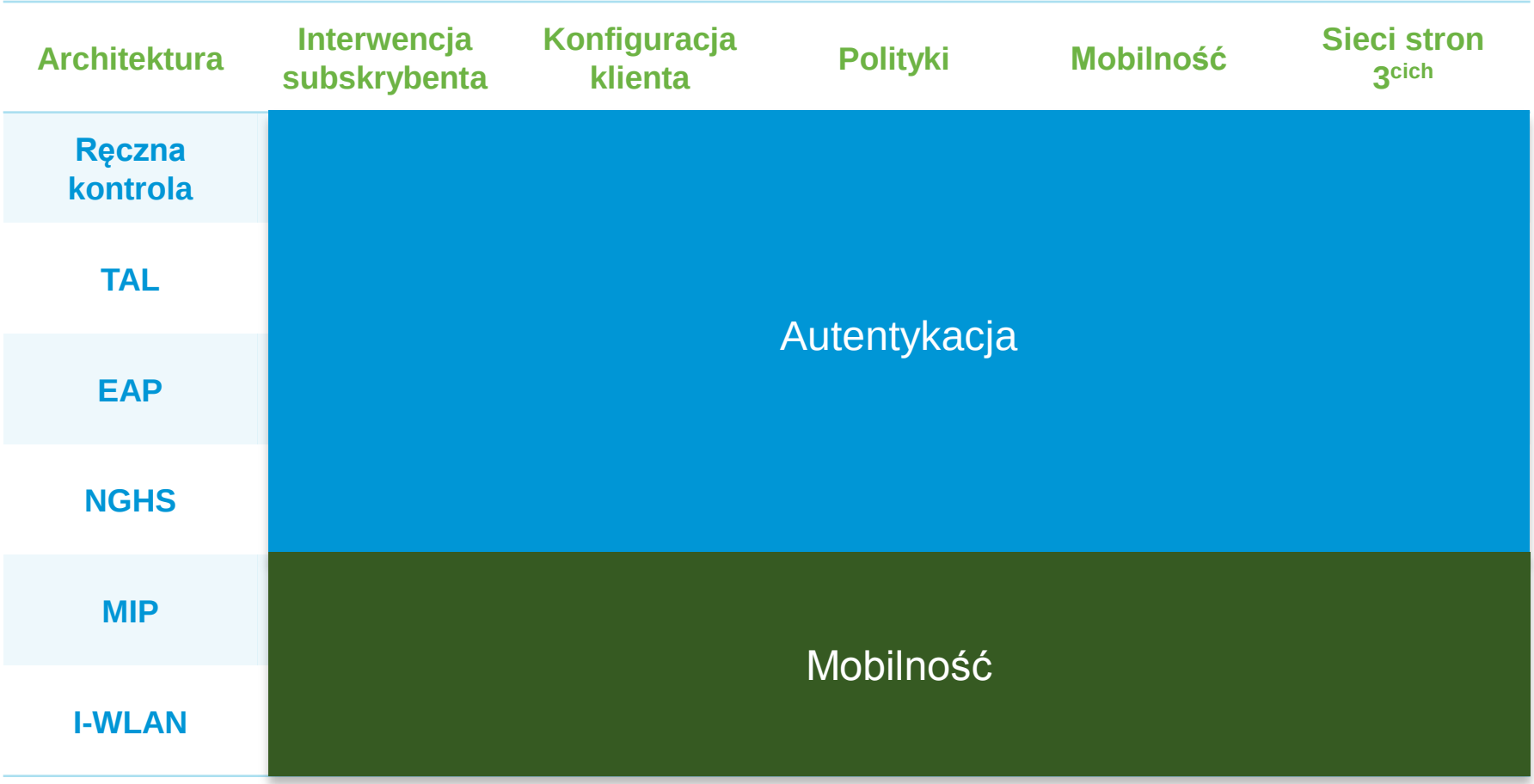
Za	Przeciw
Proste i szeroko obsługiwane	Kiepskie odczucie użytkownika, ręczna konfiguracja
Brak potrzeby stosowania klienta na UE	Bez zachowania sesji
Full offload, backhaul, RAN, Packetcore	Niski % użycia

Offload z Mobile IP



Za	Przeciw
Utrzymanie sesji bez interwencji użytkownika	Wymagany klient
Szerokie wykorzystanie, wysoki % offload	Narzut tunelu
Offload, backhaul, RAN, MVNO	Dociążony Packet Core

Architektury offload



Architektury Offload - charakterystyka

- Wybór zależny głównie od preferencji operatora
  - Własne WiFi czy używamy infrastruktury strony 3ciej?
  - Chcemy obciążać klienta za ruch przez WiFi?
  - Wymagamy autentykacji dla WiFi?
  - Typ urządzeń kwalifikowanych do offload'u (smartphone, PC, dowolne)?
  - Mobilność?
  - Klienci „gościnni"?
- Wybór architektury istotny z punktu widzenia
  - Zapewnienia wykorzystania budowanej infrastruktury (prosta konfiguracja, dostępne urządzenia, benefit dla subskrybenta…)
  - Osiągnięcia odpowiedniego poziomu jakości usług
  - Balansu kosztu rozwiązania vs benefity
  - Osiągnięcia elastyczności przy przyszłej ekspansji

Spoglądając głębiej

Ręczna kontrola

Infrastruktura strony 3ciej

AP

Internet

Internet

Subskrybent

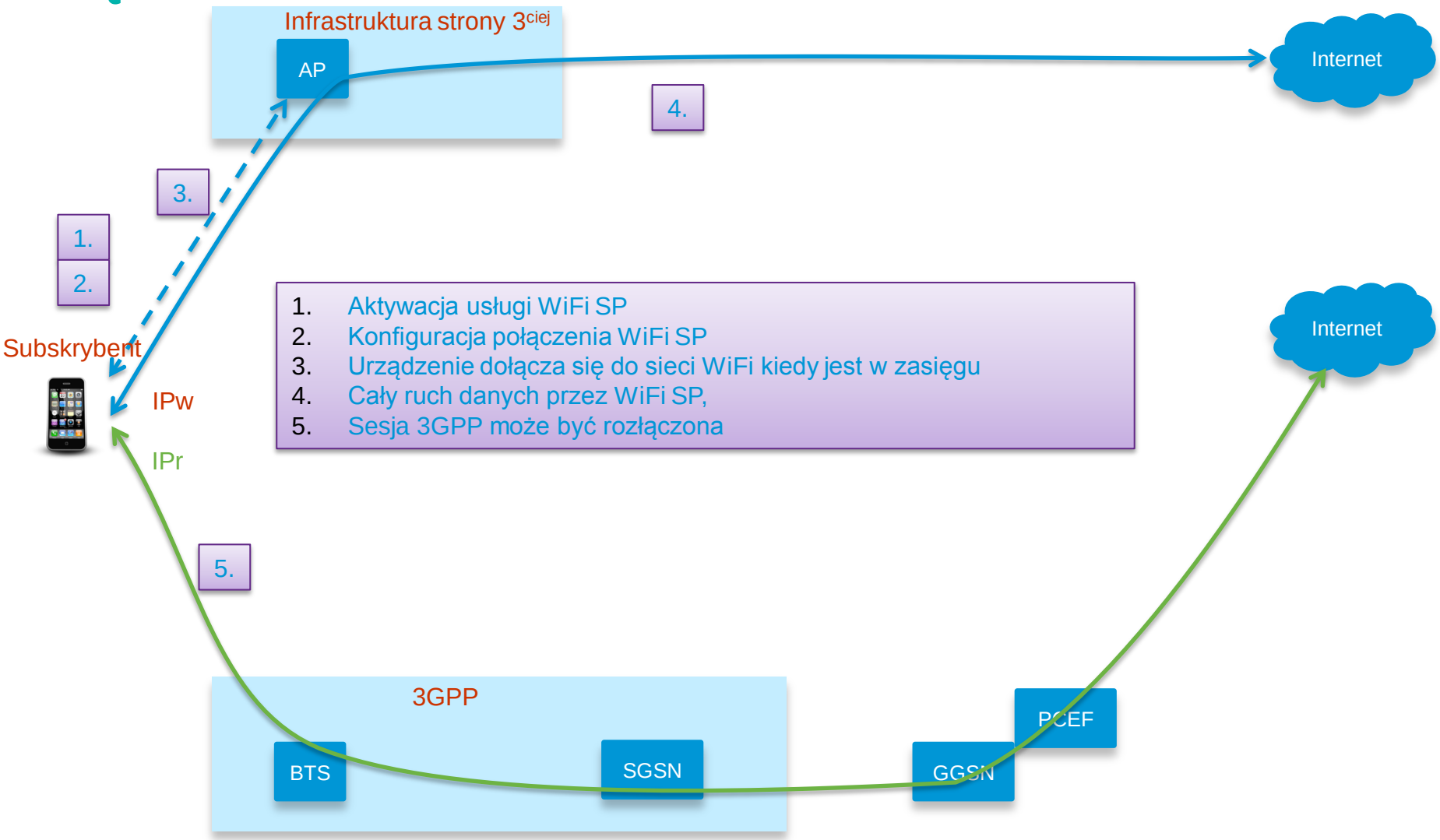
3GPP

BTS

SGSN

GGSN

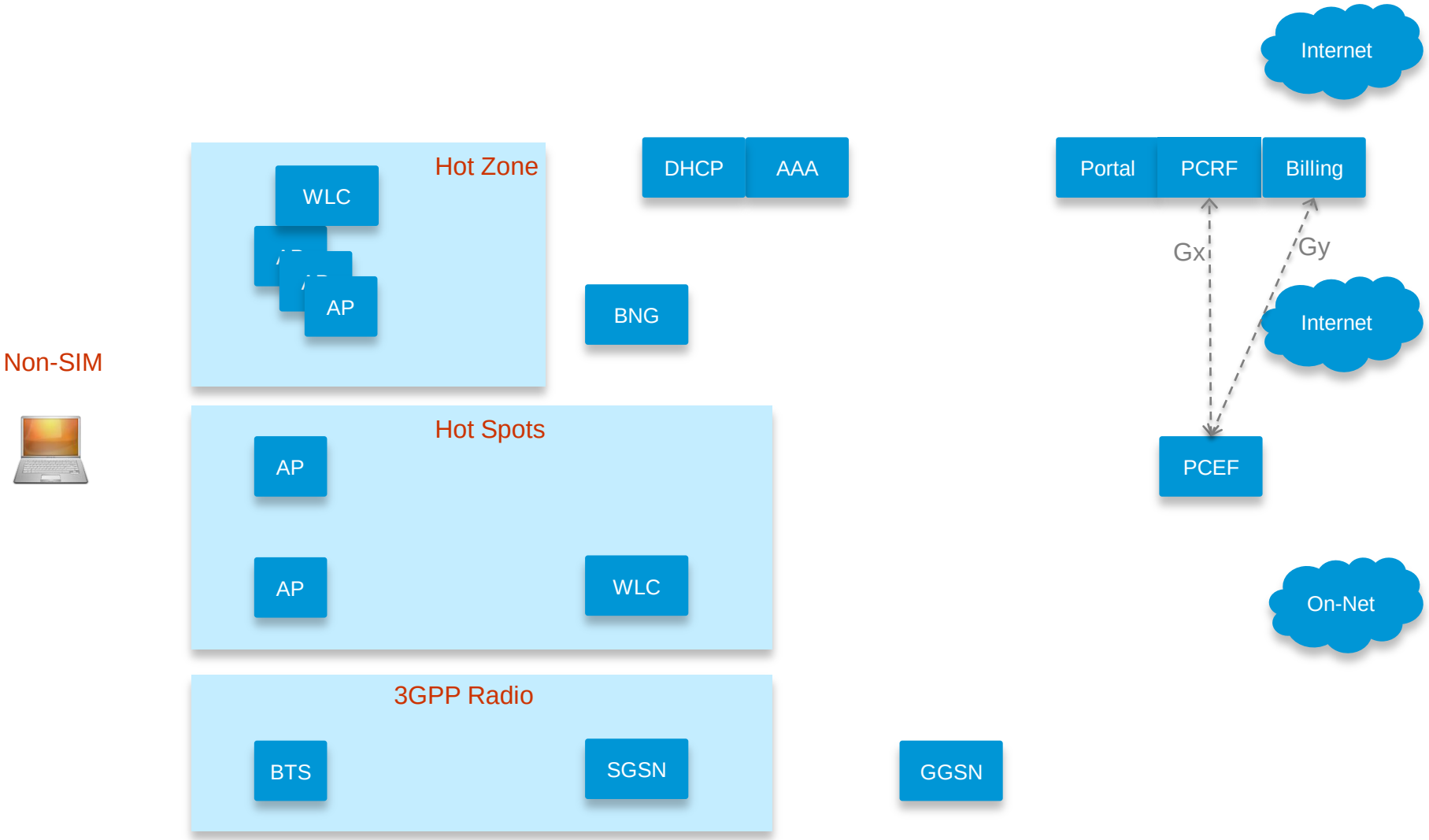
Ręczna kontrola



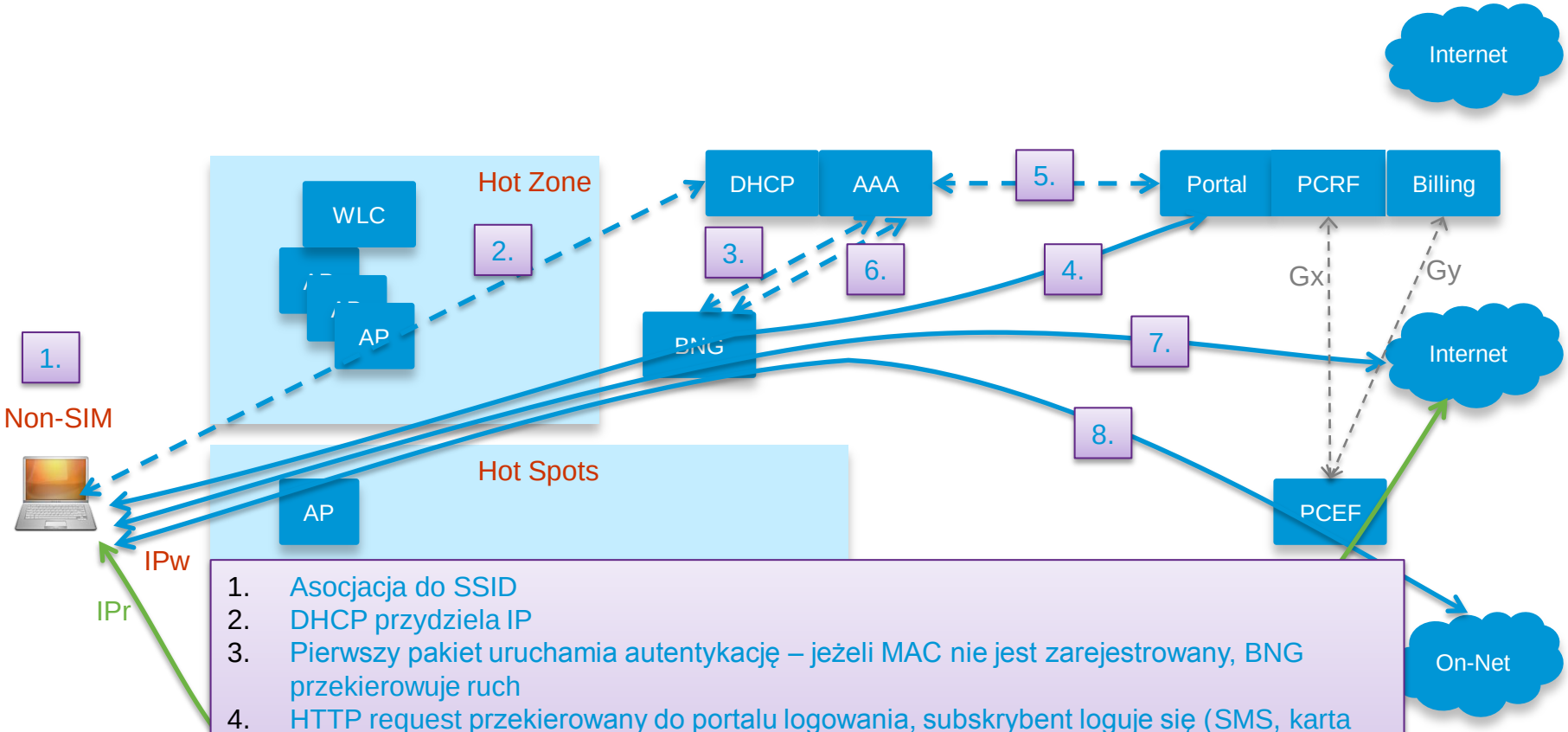
Ręczna kontrola

- **Interwencja subskrybenta**
  - Konieczna konfiguracja usługi strony 3ciej
- **Konfiguracja usługi**
  - SSID, autentykacja – zgodnie z wymaganiami usługodawcy WiFi
  - Opcjonalnie konfiguracja priorytetyzacji połączenia WLAN nad 3GPP i SSID
- **Polityki**
  - Ruchu nie przechodzi przez sieć MO, więc funkcje typu PCEF nie mogą zadziałać
- **Mobilność**
  - Każde radio ma własny adres IP. Konieczna konfiguracja, które ma być używane.
  - Mobilność nie może być osiągnięta, bo z reguły nie ma porozumienia w tym zakresie między operatorem 3G a WLAN
- **Sieć strony 3ciej**
  - Usługa oparta o sieć strony 3ciej

Transparent Auto Login



Transparent Auto Login

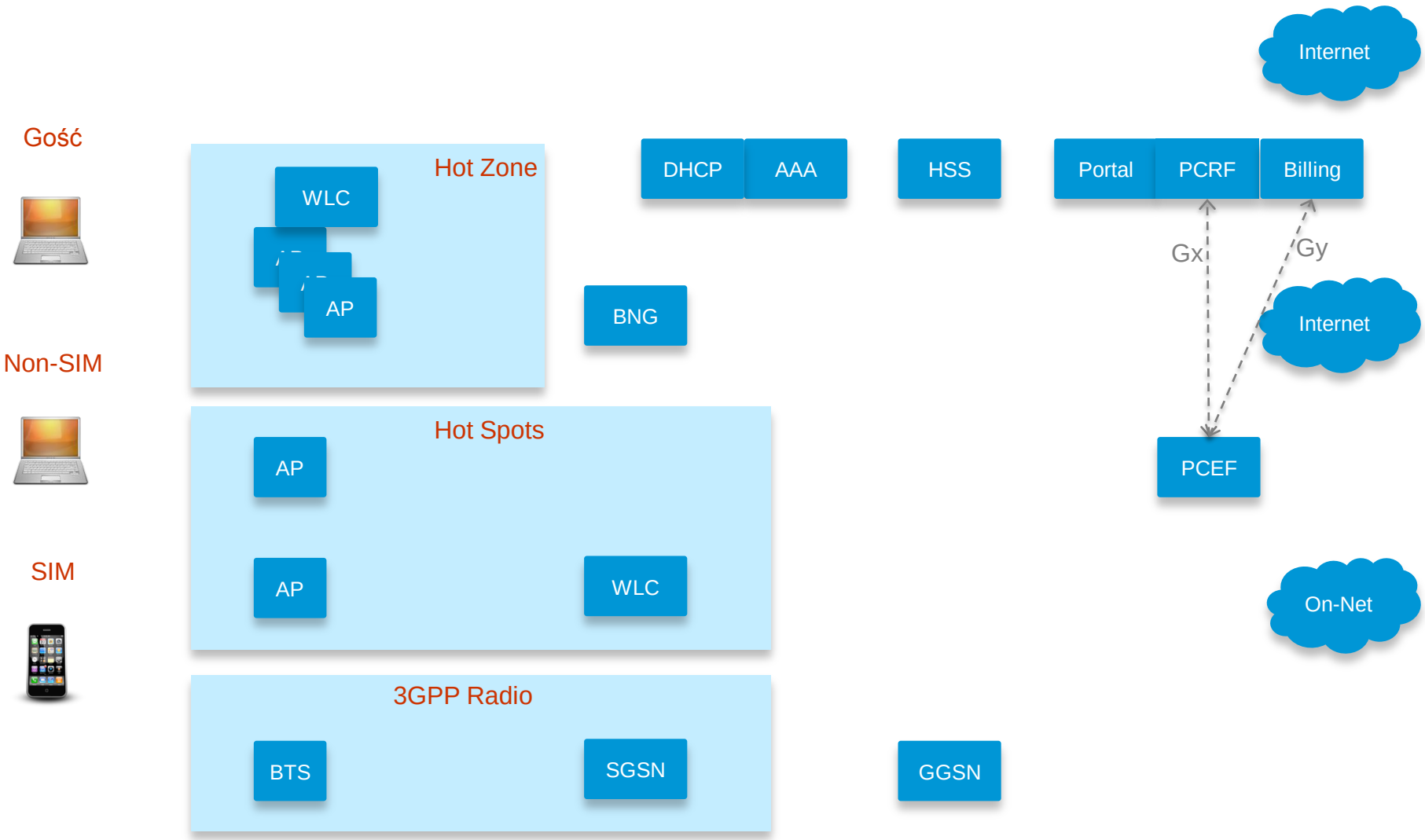


1. Asocjacja do SSID
2. DHCP przydziela IP
3. Pierwszy pakiet uruchamia autentykację – jeżeli MAC nie jest zarejestrowany, BNG przekierowuje ruch
4. HTTP request przekierowany do portalu logowania, subskrybent loguje się (SMS, karta kredytowa, etc.)
5. Portal aktualizuje AAA z MAC stacji
6. AAA zwraca *authentication success*
7. Ruch do Internetu może przepływać bezpośrednio. BNG może robić prosty policing
8. Zaawansowane polityki raczej wymagają przekierowania do PCEF rdzenia.

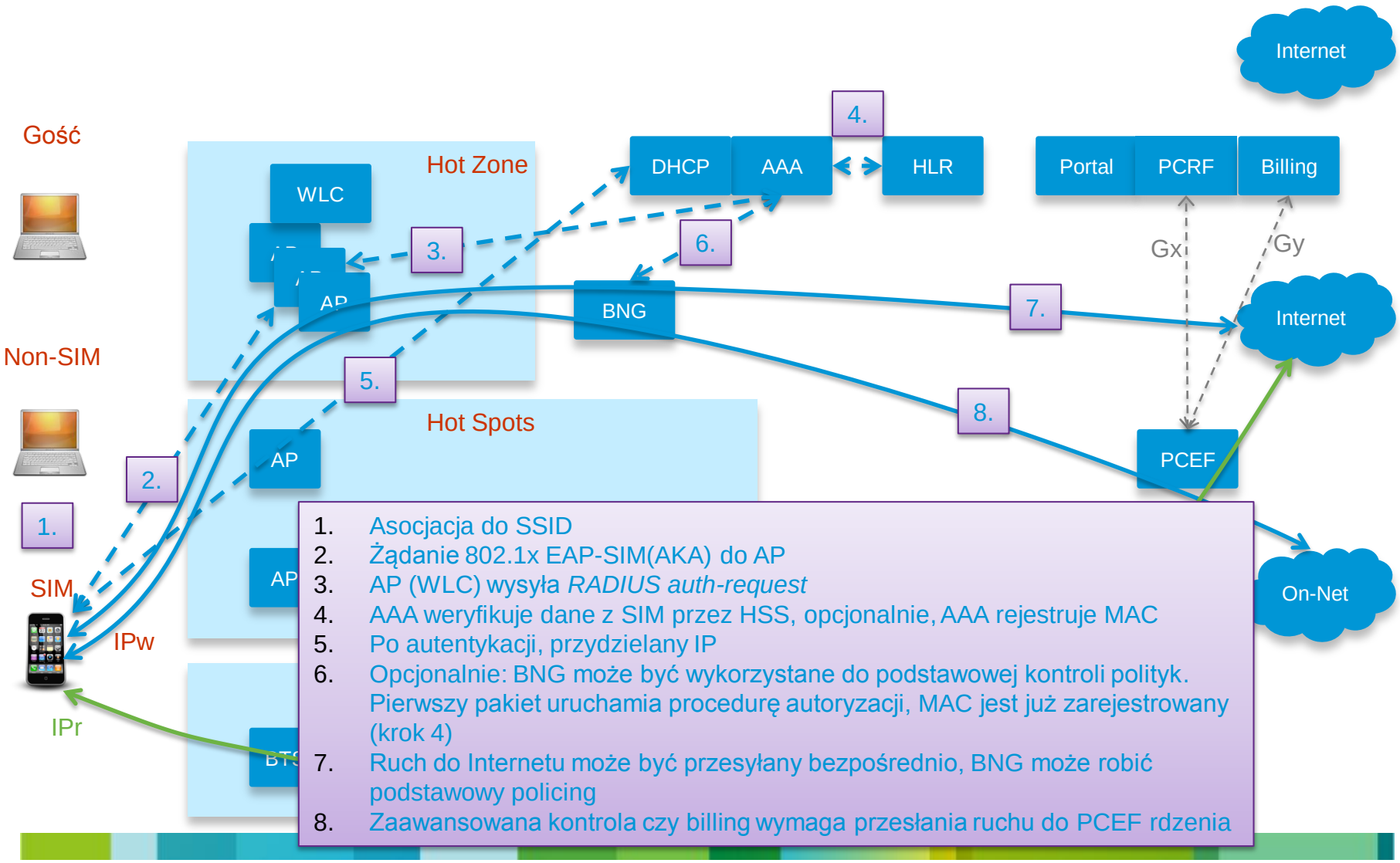
Transparent Auto Login

- **Interwencja subskrybenta**
  - Konieczny zakup usługi od operatora, dostęp do danych logowania
- **Konfiguracja usługi**
  - Konfiguracja/wybór SSID
  - Konfiguracja priorytetyzacji
  - Nowe dane logowania po wygaśnięciu starych
- **Polityki**
  - Podstawowe na BNG
  - Zaawansowane wymagają przesłania ruchu do PCEF
- **Mobilność**
  - Każde radio ma własny IP
  - Brak automatycznej mobilności
  - MIP lub I-WLAN może zostać zastosowany jako nakładka
- **Sieć strony 3ciej**
  - Możliwe porozumienia między operatorami
  - Subskrybent musi znać właściwe SSID

EAP

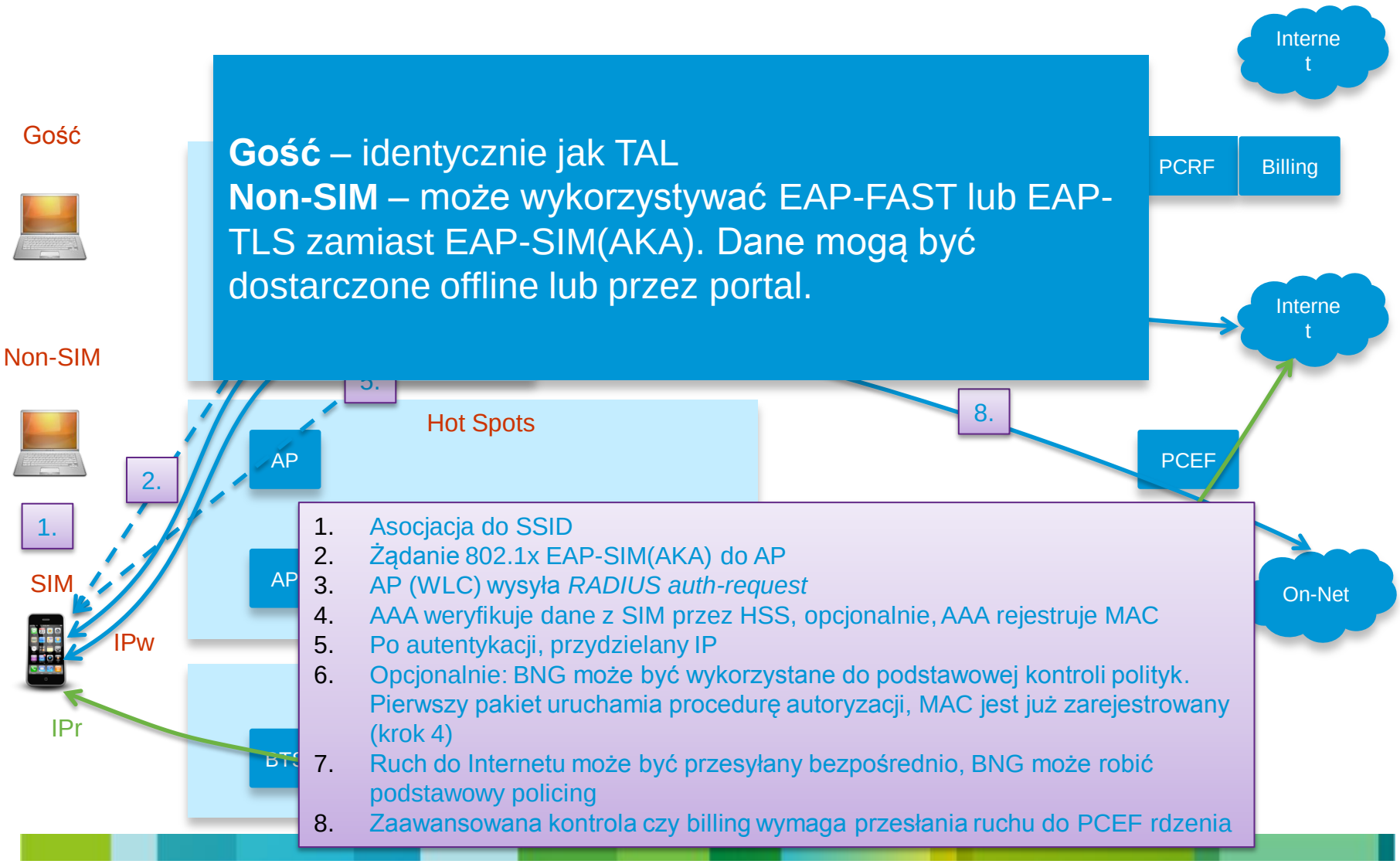


EAP



1. Asocjacja do SSID
2. Żądanie 802.1x EAP-SIM(AKA) do AP
3. AP (WLC) wysyła *RADIUS auth-request*
4. AAA weryfikuje dane z SIM przez HSS, opcjonalnie, AAA rejestruje MAC
5. Po autentykacji, przydzielany IP
6. Opcjonalnie: BNG może być wykorzystane do podstawowej kontroli polityk. Pierwszy pakiet uruchamia procedurę autoryzacji, MAC jest już zarejestrowany (krok 4)
7. Ruch do Internetu może być przesyłany bezpośrednio, BNG może robić podstawowy policing
8. Zaawansowana kontrola czy billing wymaga przesłania ruchu do PCEF rdzenia

EAP



Gość – identycznie jak TAL
Non-SIM – może wykorzystywać EAP-FAST lub EAP-TLS zamiast EAP-SIM(AKA). Dane mogą być dostarczone offline lub przez portal.

1. Asocjacja do SSID
2. Żądanie 802.1x EAP-SIM(AKA) do AP
3. AP (WLC) wysyła *RADIUS auth-request*
4. AAA weryfikuje dane z SIM przez HSS, opcjonalnie, AAA rejestruje MAC
5. Po autentykacji, przydzielany IP
6. Opcjonalnie: BNG może być wykorzystane do podstawowej kontroli polityk. Pierwszy pakiet uruchamia procedurę autoryzacji, MAC jest już zarejestrowany (krok 4)
7. Ruch do Internetu może być przesyłany bezpośrednio, BNG może robić podstawowy policing
8. Zaawansowana kontrola czy billing wymaga przesłania ruchu do PCEF rdzenia

EAP

- **Interwencja subskrybenta**
  - Non-SIM musi zakupić usługę i otrzymać dane do logowania
- **Konfiguracja usługi**
  - Konfiguracja SSID
  - Konfiguracja priorytetyzacji łącza
  - Jednorazowa konfiguracja EAP (często zautomatyzowana)
- **Polityki**
  - Podstawowe polityki na BNG
  - Zaawansowana kontrola wymaga przesłania ruchu do rdzenia
- **Mobilność**
  - Jak w TAL
- **Sieć strony 3ciej**
  - Możliwe porozumienia roamingowe
  - Możliwa kros-autentykacja
  - Subskrybent musi znać SSID

Problemy z wykryciem i wyborem sieci

- Terminal po włączeniu w środowisku miejskim po skanie środowiska znajdzie kilka[dziesiąt|naście] sieci Wi-Fi. Jak ma wybrać właściwą, nie drenując przy okazji baterii?
- Terminal nie rozpoznaje SSID, więc nie wie czy ma właściwe dane do logowania
- Terminal nie wie, która sieć daje dostęp do Internetu.
- Terminal asocjuje się do sieci, ale poczta się nie ściąga (Web-auth/WISPr, ale użytkownik nie uruchomił przeglądarki)
- Wybór sieci staje się zbyt skomplikowany dla nie-technicznych użytkowników

Polepszając odczucia użytkownika

Automatyzacja procesu wyboru metod dostępu

- przezroczysta autentykacja przy dostępie przez różne mechanizmy transmisyjne
- wybór mechanizmu dostępowego w oparciu o polityki
- kontrola operatora nad przesyłaniem ruchu
- możliwość zachowania sesji
- nowe usługi

NGHS vel HotSpot 2.0

- **Interwencja subskrybenta**
  - Non-SIM musi zakupić usługę i otrzymać dane do logowania
- **Konfiguracja usługi**
  - Konfiguracja SSID
  - Konfiguracja priorytetyzacji łącza
  - Jednorazowa konfiguracja EAP (często zautomatyzowana)
- **Polityki**
  - Podstawowe poli
  - Zaawansowana k
- **Mobilność**
  - Jak w TAL
- **Sieć strony 3ciej**
  - Możliwe poroz
  - Możliwa kros
  - Subskrybent r

Inicjatywa WBA *Hotspot 2.0* ma za celu uproszczenie interakcji ze strony subskrybentów przy dołączaniu się do WLAN przez zestandaryzowanie zestawu protokołów:

- 802.11u
  - wymiana/sygnalizowanie usług obsługiwanych przez AP
  - sygnalizacja które SSID umożliwia dostęp do usługi operatora „domowego”
- 802.1x
  - EAP-SIM
  - EAP-TLS
  - EAP-FAST
- Roaming – specyfikacja WRIX

HotSpot 2.0 – Next Generation

- WiFi równie łatwe w użytkowaniu jak sieci komórkowe
- Rozwiązanie problemu z roamingiem
  - w oparciu o standard IEEE 802.11u
- Rozwiązanie problemu z bezpieczeństwem
  - 802.11i
  - EAP (EAP-SIM/EAP-TLS/EAP-FAST)
- Interoperacyjność (certyfikacja WFA)
- Prace nad specyfikacją HS 2.0 Phase 1.0

HS 2.0 z perspektywy użytkownika

Przezroczysta autentykacja i roaming - Wireless Broadband Alliance

Mobile "concierge" service

Mobile Service Advertisement Protocol (MSAP)

IEEE 802.11u

- 802.11u – Interworking with External Networks
- Cel:

  Interworking with External Networks to kluczowy element umożliwiający urządzeniom IEEE 802.11 współpracę z sieciami innymi, w środowiskach typowych dla hotspotów, sieci publicznych, niezależnie czy usługa jest darmowa czy subskrypcyjna.

  Interworking Service wprowadza proces wykrycia i wyboru sieci, umożliwiając transfer informacji asocjacyjnych w sieciach zewnętrznych, a także usługi awaryjne. Udostępnia tą informację dla STA przed asocjacją.

- Funkcja:

  Network discovery and selection (NDS)

  - Generic Advertisement Service (GAS)
  - Access Network Query Protocol (ANQP)
  - Interworking Element

  Mało obciążający proces wyboru sieci

  GAS zapewnia wsparcie dla innych protokołów umożliwiających rozgłaszanie usług wyższych warstw.

- Status: IEEE 802.11u-2011 jest ratyfikowanym standardem IEEE

Proces asocjacyjny

- Radio Wi-Fi aktywuje się w określonych interwałach czasowych i skanuje
- Aktywny skan powoduje otrzymanie:
  - Internetworking element, identyfikujący AP jako obsługujący 802.11u
    - Network Type = {private | public-free | public-chargeable}
    - Internet Access available
    - ASRA bit — wskazuje konfigurację web-auth
  - Roaming consortium element zawierający właściciela hotspot'u (OI) + OI 2óch najważniejszych partnerów roamingowych
- Jeżeli urządzenie rozpoznaje OI, próbuje się zasocjować, używając danych logowania właściwych dla danego OI
  - 802.1x jeżeli otrzymało IE RSN
  - web-auth jeżeli nie otrzymało IE RSN oraz ASRA=1
  - Uwaga: Każdy operator musi zarejestrować się w IEEE w celu uzyskania OI. OI musi zostać skonfigurowane na urządzeniu końcowym.

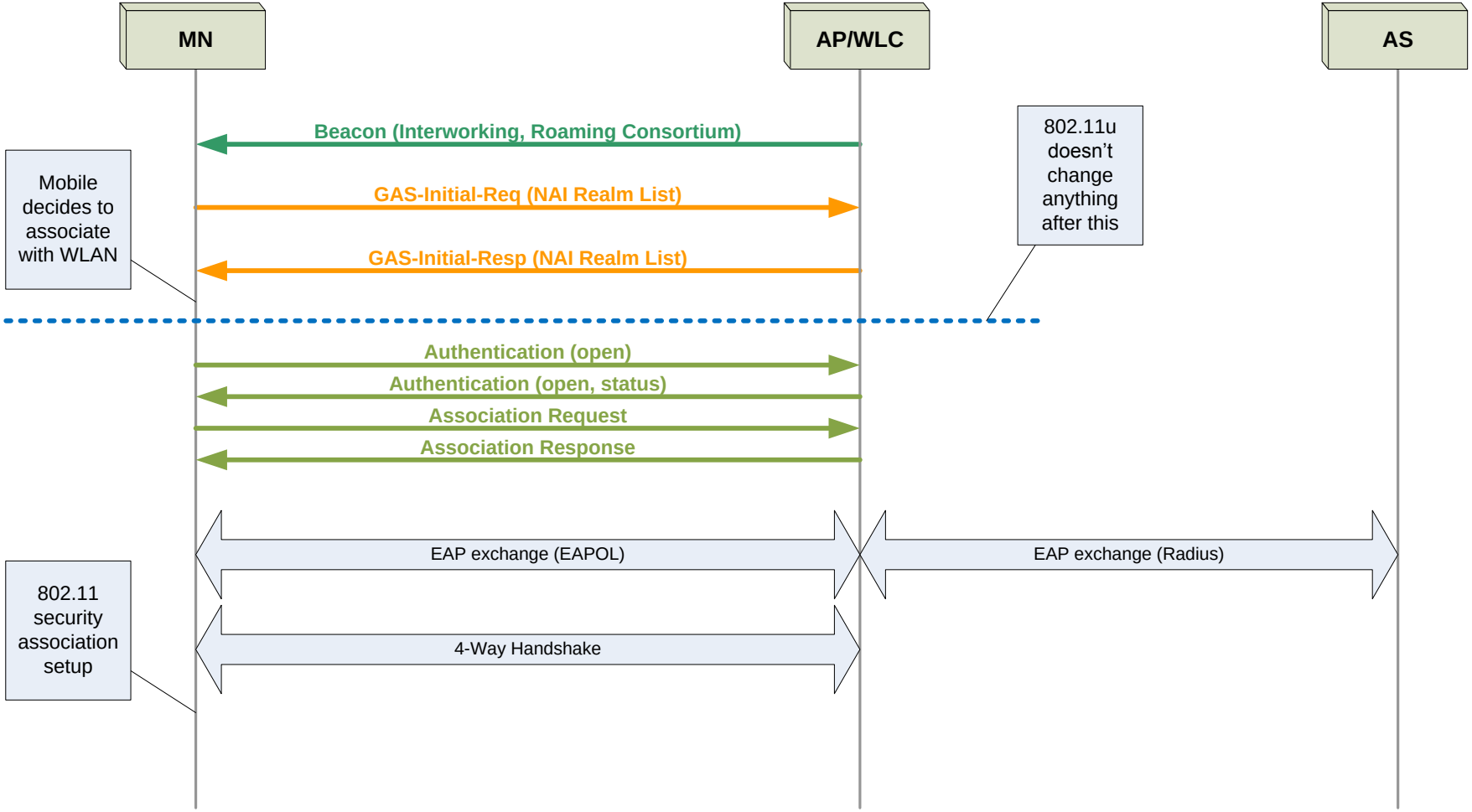
OI = organizational identifier
ASRA = Additional Step Required for Authentication

Proces asocjacyjny

- A jeżeli urządzenie nie rozpoznaje OI, to wysyła zapytanie GAS-ANQP i dostaje:
  - Roaming consortium list
  - NAI Realm List
    - Hotspot może zaakceptować dane do logowania dla tych kontekstów
    - Realm dotyczy operatora – właściciela hotspot'u lub jego parterów roamingowych
    - Lista zawiera obsługiwane typy EAP (np., EAP-SIM)
  - Jeżeli ASRA=1, GAS-ANQP jest wysyłane aby otrzymać Network Authentication Type (szczegóły do logowania web-auth)

NAI = Network Access Identifier (user@realm)
OI = Organizational Identifier
ASRA = Additional Step Required for Authentication

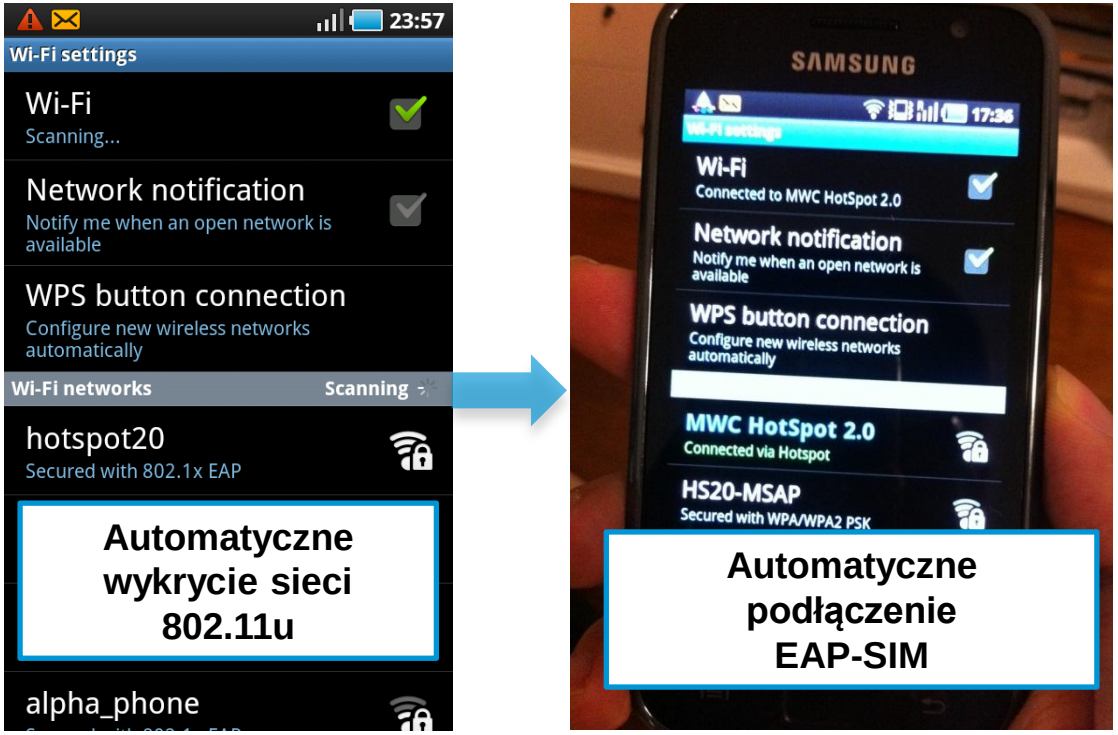
Proces asocjacji



EAPOL = EAP Over LANs

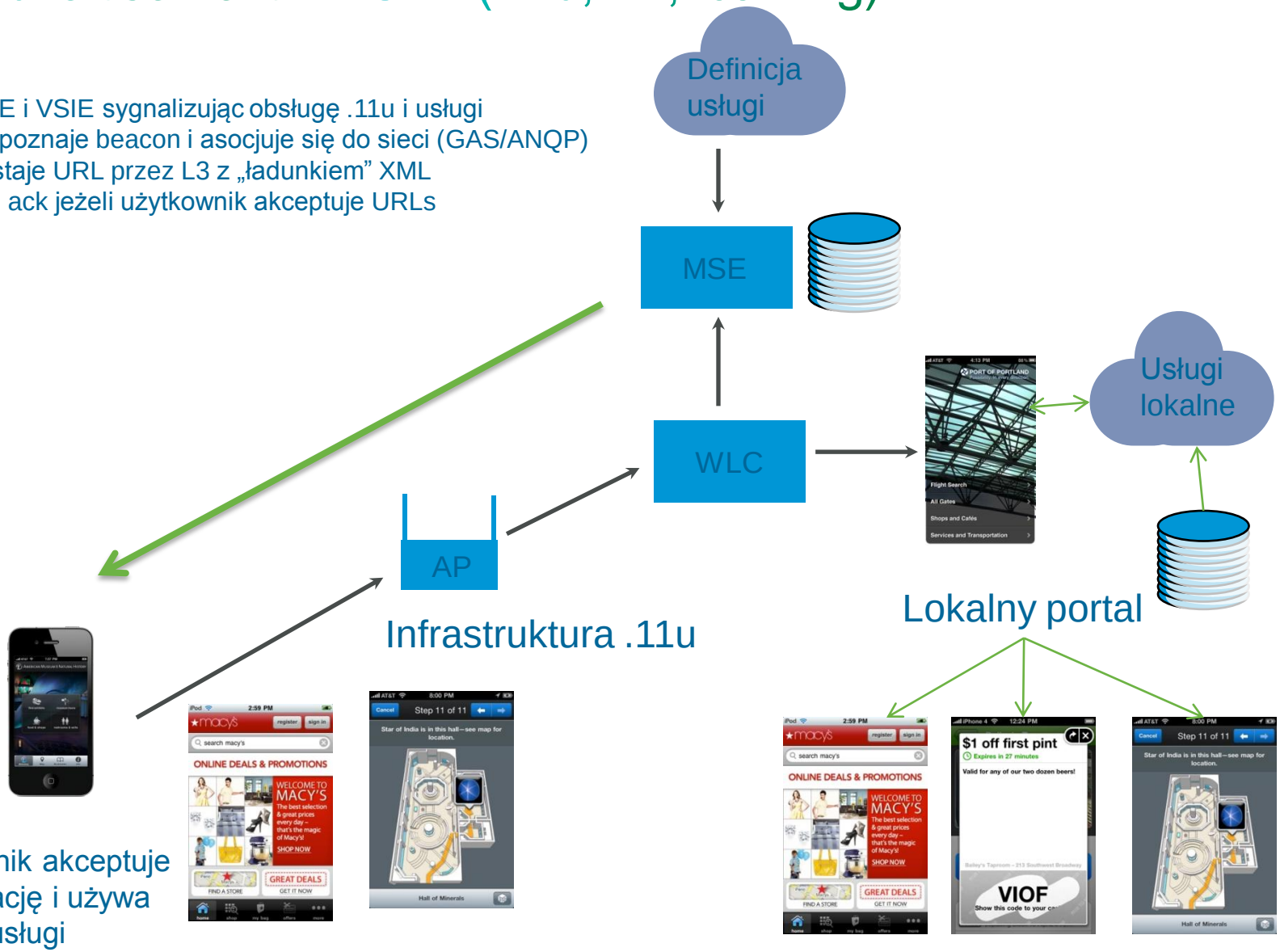
Z perspektywy użytkownika

- Klient ze wsparciem 802.11u nie wymaga konfiguracji dostępu
- Klient ma prekonfigurowaną listę dopuszczonych Realm names (operatorów)



Service Advertisement – MSAP (.11u, .1x, roaming)

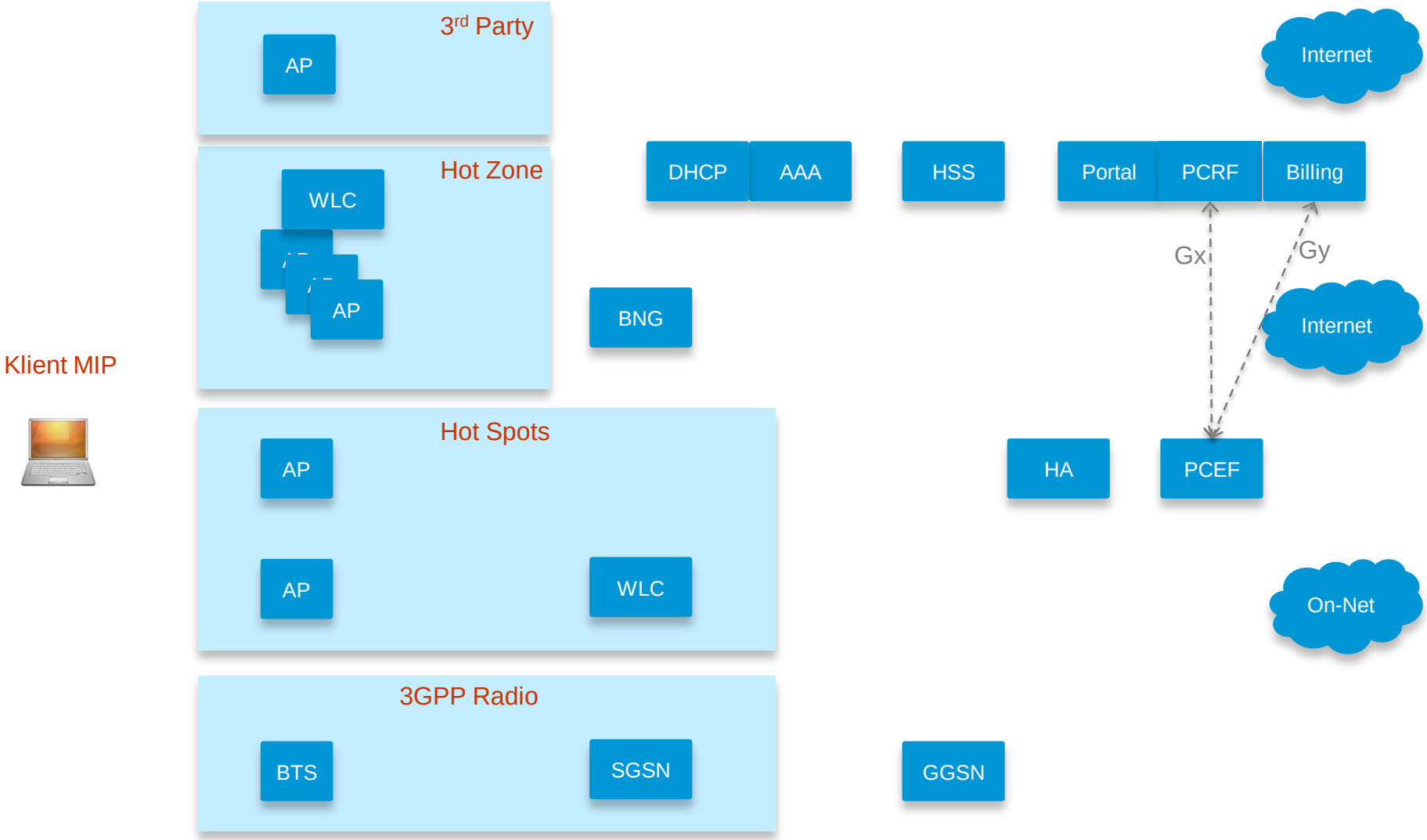
- AP rozgłasza IIE i VSIE sygnalizując obsługę .11u i usługi
- Urządzenie rozpoznaje beacon i asocjuje się do sieci (GAS/ANQP)
- Urządzenie dostaje URL przez L3 z „ładunkiem” XML
- MSE otrzymuje ack jeżeli użytkownik akceptuje URLs



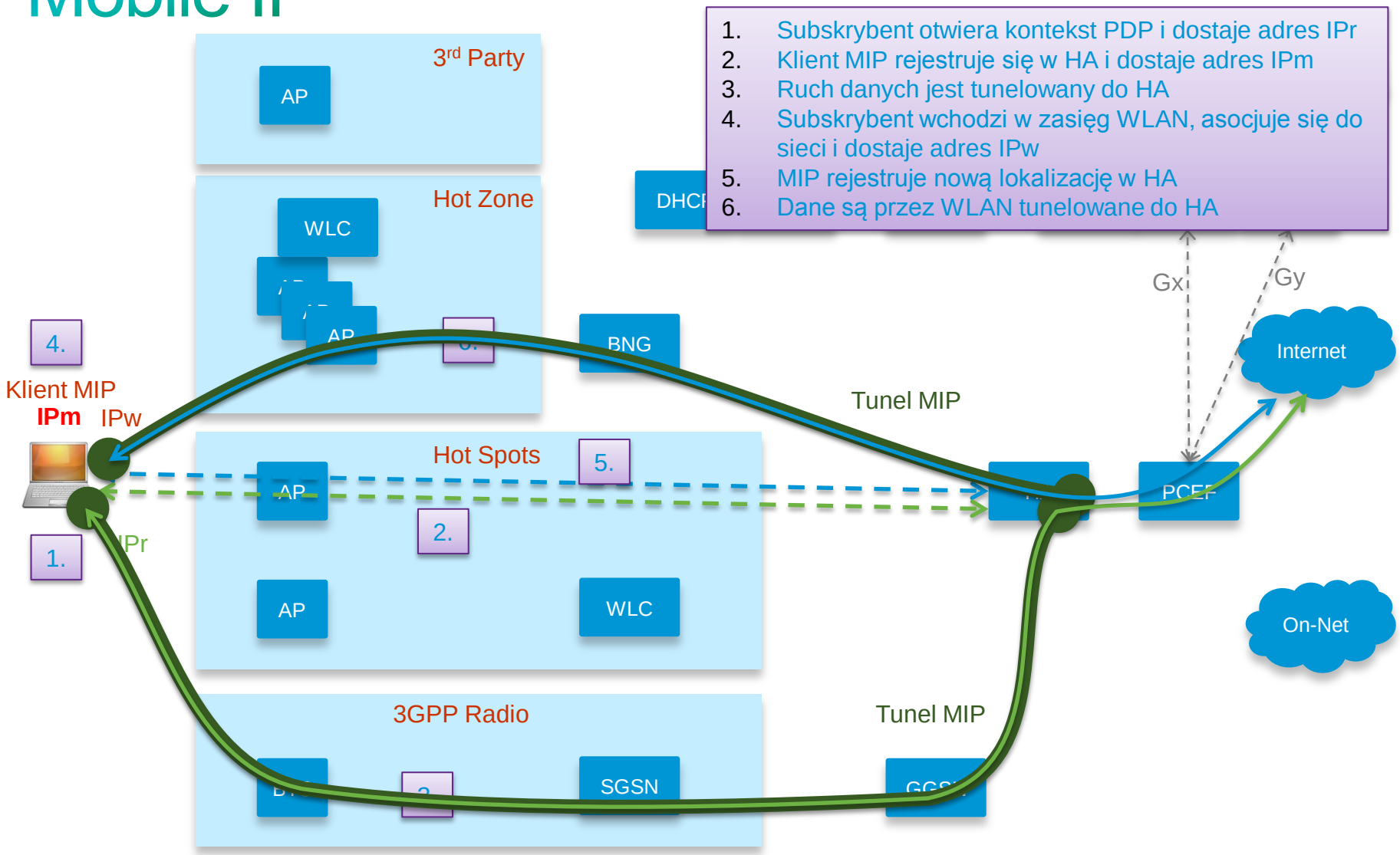
Mobilność

- Charakterytyka
  - UE ma dwa radia, dwa adresy IP
  - Brak komunikacji pomiędzy kontrolerami RAN (RNC/WLC) dwóch sieci
  - Każdy RAN zapewnia wewnętrznie mobilność
  - WLAN RAN może należeć do operatora lub strony 3ciej
  - Różne metody autentykacji dla WLAN i 3GPP
- Konsekwencje
  - UE decyduje o wyborze radia – konieczny klient
  - Konieczy punkt zaczepienia (Home Agent / Local Mobility Agent) dla zapewnienia ciągłości usług
- Mobilność jest niezależna od architektury dostępowej (TAL, EAP etc.). Dostęp musi być zautentykowany zanim zestawiony będzie tunel.

Mobile IP



Mobile IP

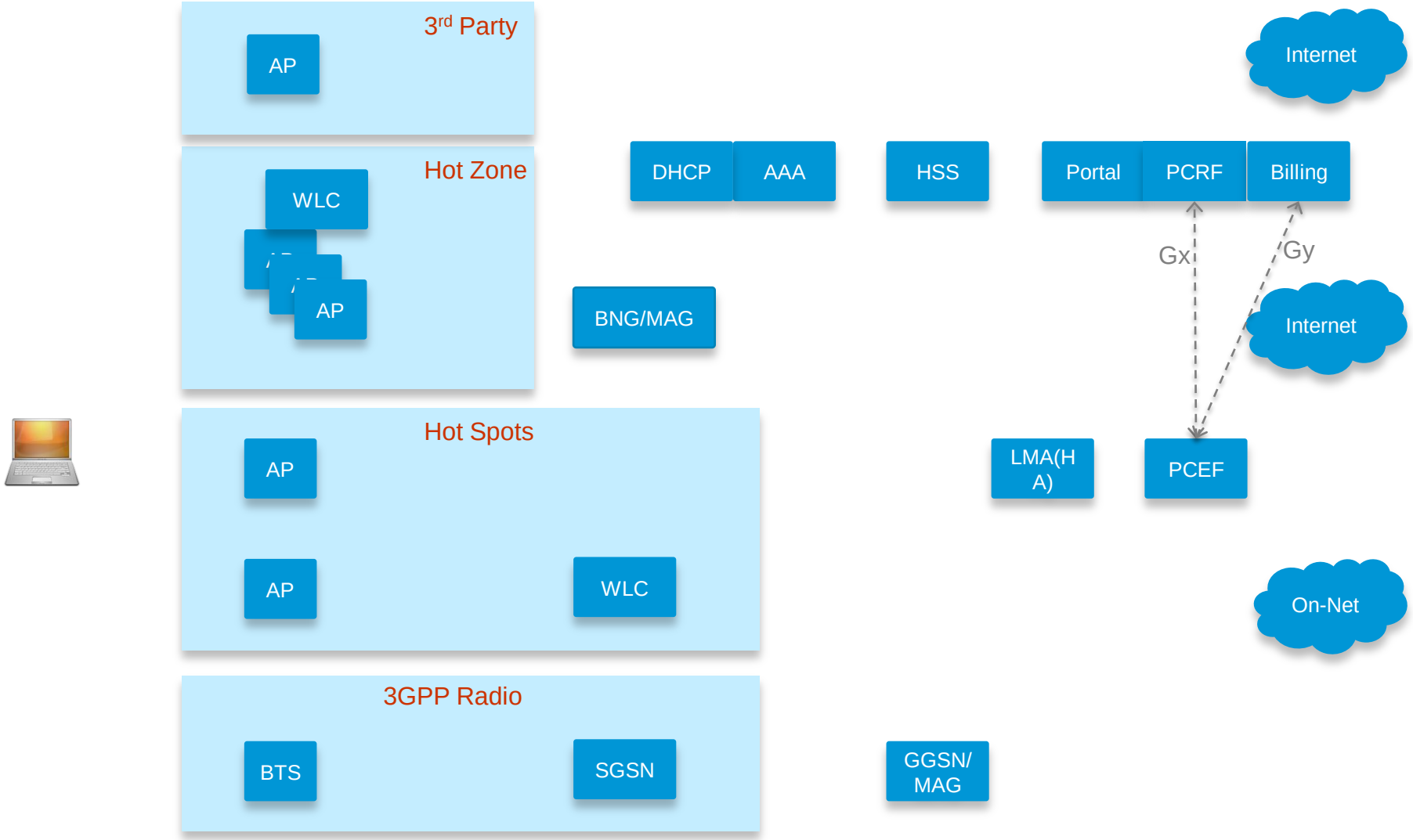


Mobile IP

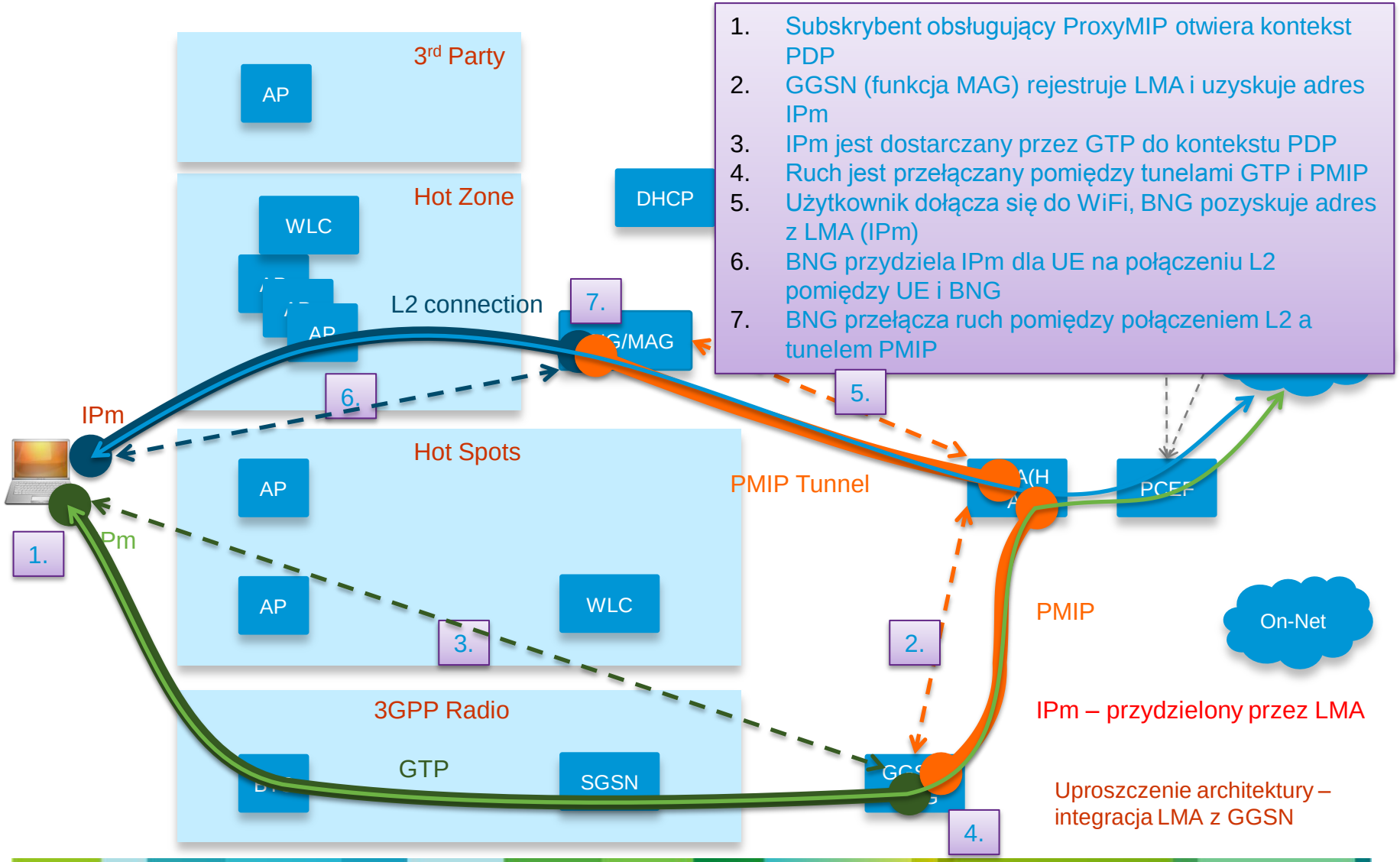
1. Subscriber opens PDP context and gets IPr assigned

- **Interwencja subskrybenta**
  - Instalacja klienta MIP
- **Konfiguracja usługi**
  - Zależnie od WLAN
- **Polityki**
  - Całość ruchu tunelowana do HA
  - PCEF z reguły zintegrowana z HA, całość ruchu może być objęta wymuszeniem polityk
- **Mobilność**
  - Przezroczysta
  - Oprogramowanie klienta decyduje o przełączeniu
  - Całość ruchu do klienta idzie na IPm
  - Dane przesyłane przez WLAN mogą nie być szyfrowane
- **Sieć strony 3ciej**
  - Możliwe umowy partnerskie
  - Działa, może nie być chronione

Proxy Mobile IP

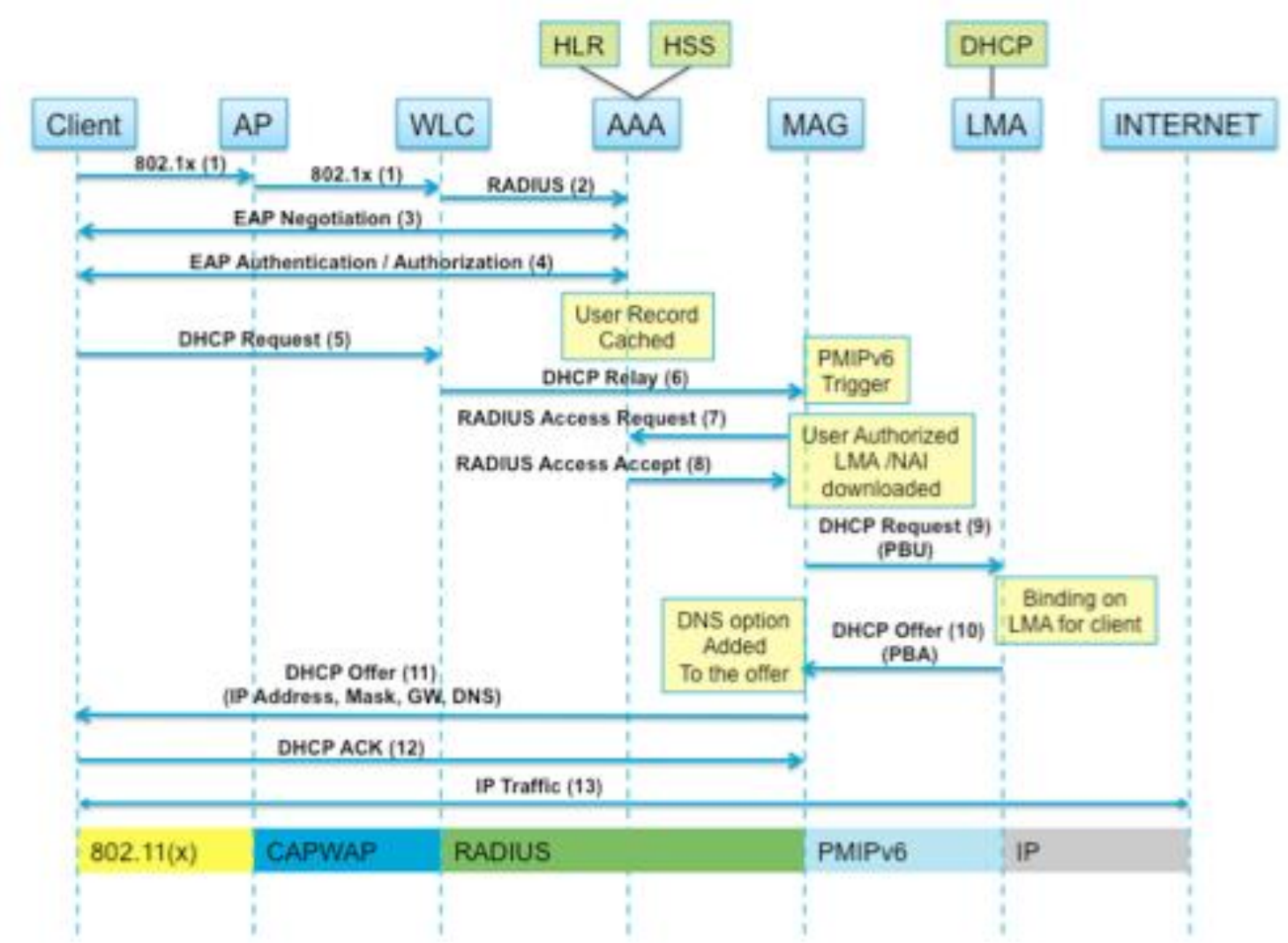


Proxy Mobile IP



1. Subskrybent obsługujący ProxyMIP otwiera kontekst PDP
2. GGSN (funkcja MAG) rejestruje LMA i uzyskuje adres IPm
3. IPm jest dostarczany przez GTP do kontekstu PDP
4. Ruch jest przełączany pomiędzy tunelami GTP i PMIP
5. Użytkownik dołącza się do WiFi, BNG pozyskuje adres z LMA (IPm)
6. BNG przydziela IPm dla UE na połączeniu L2 pomiędzy UE i BNG
7. BNG przełącza ruch pomiędzy połączeniem L2 a tunelem PMIP

PMIPv6 WLAN - przepływ

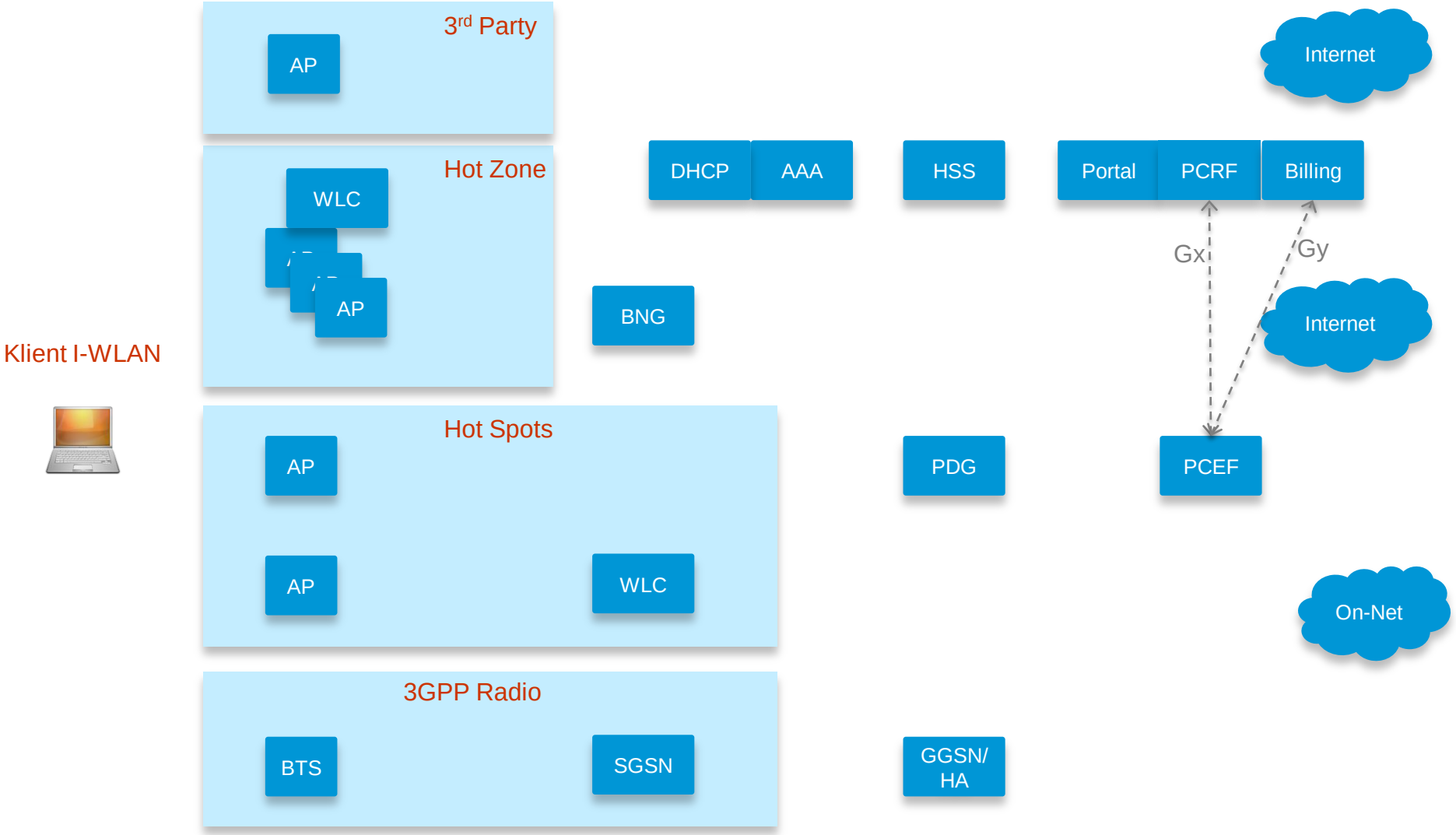


Proxy Mobile IP

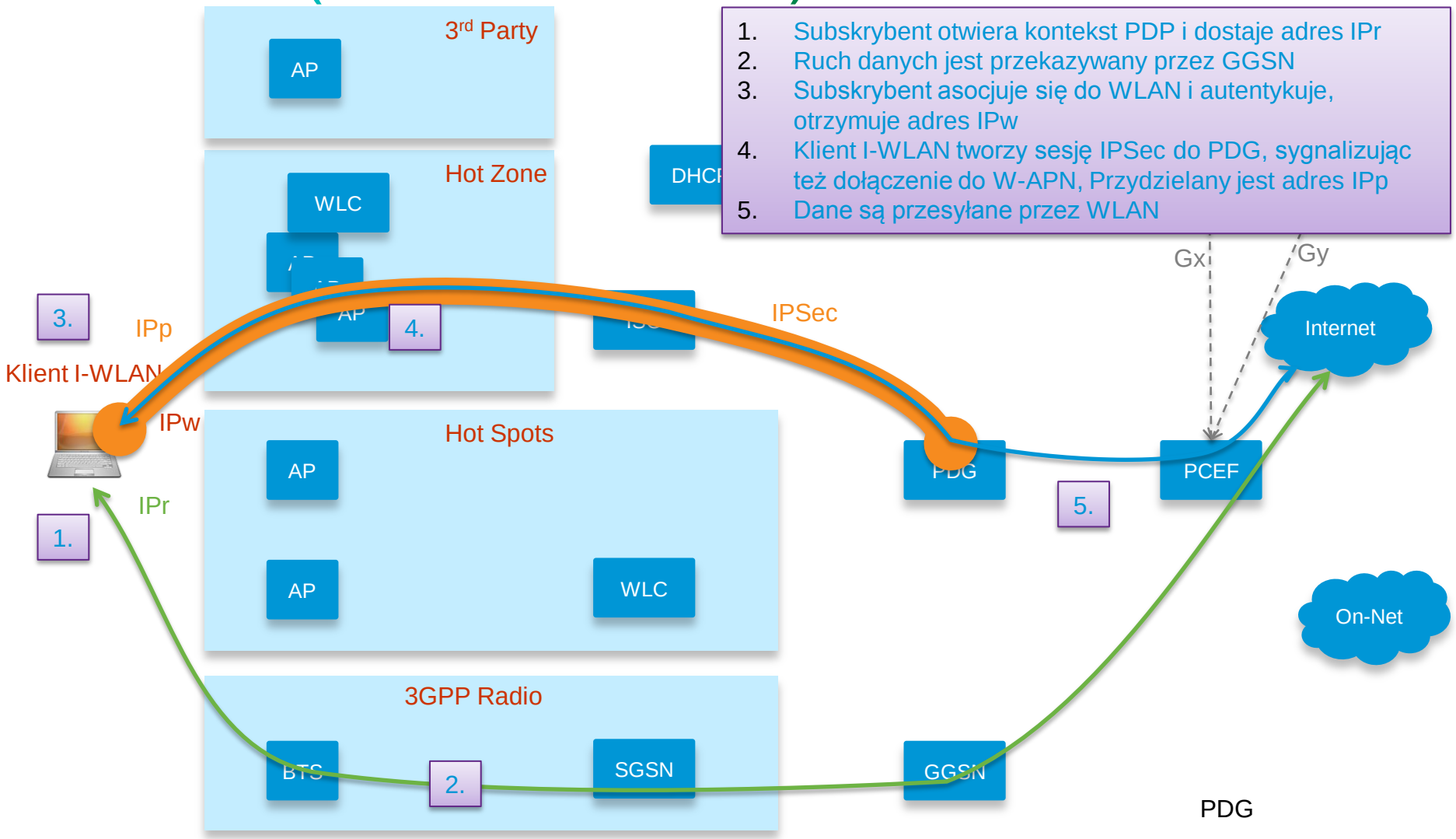
1. ProxyMIP enabled subscriber opens PDP context

- **Interwencja subskrybenta**
  - Brak (potencjalnie)
- **Konfiguracja usługi**
  - Profil autentykacji
- **Polityki**
  - Całość ruchu przechodzi przez GGSN/HA
  - Całość ruchu może być poddana wymuszeniu polityk
- **Mobilność**
  - Zachowanie IP
  - Nie całkiem transparentna. Czas przełączenia zależy od OS, sterowników itp. Klient musi poradzić sobie z obsługą jednego adresu na kilku aktywnych interfejsach.
  - Konieczne oprogramowanie po stronie klienta aby zapewnić transparencję
- **Sieć strony 3ciej**
  - Podobnie jak MIP

I-WLAN

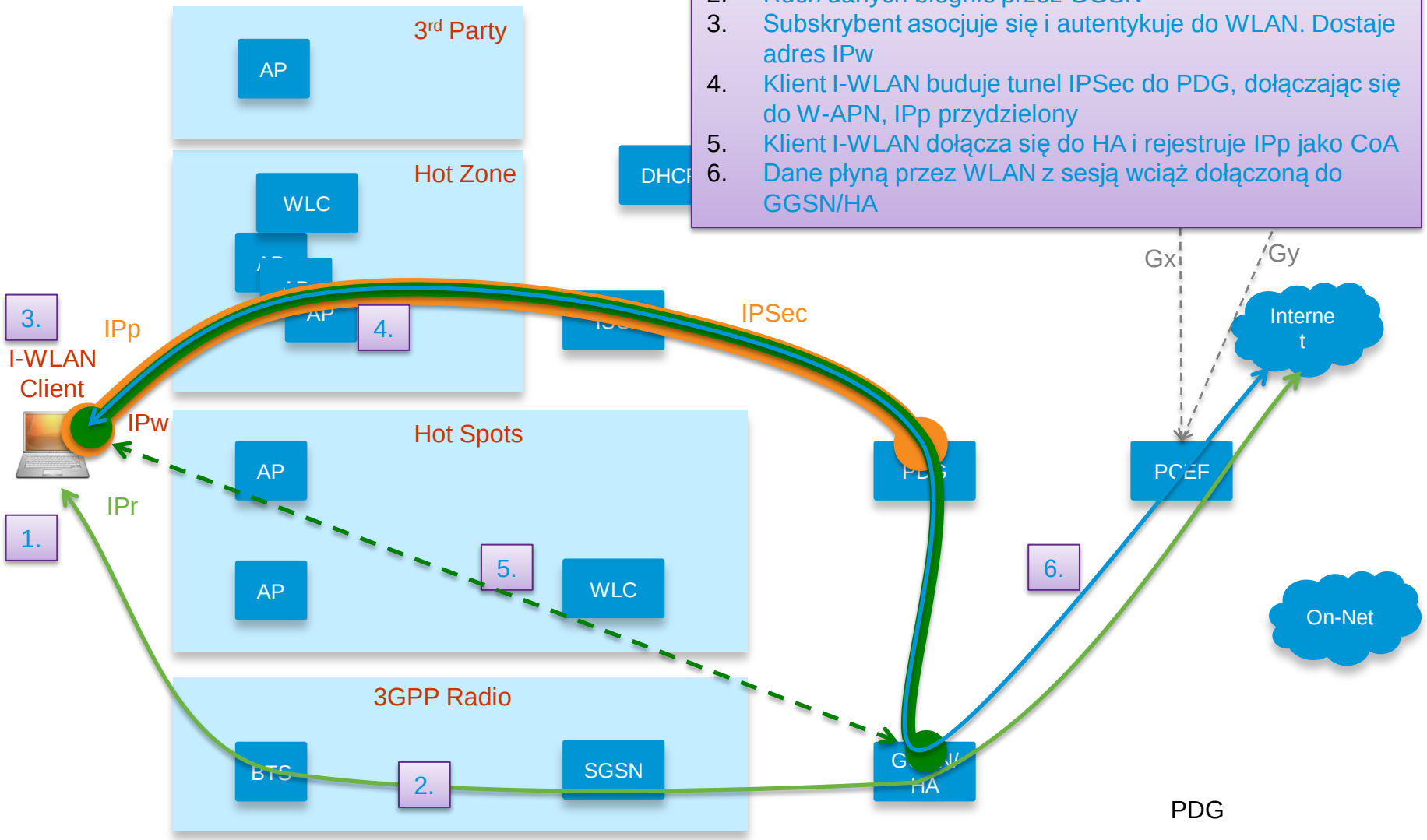


I-WLAN (bez mobilności)



I-WLAN

1. Subskrybent otwiera kontekst PDP, otrzymuje adres Ipr. Powinien być jednoznaczny z adresem „domowym”
2. Ruch danych biegnie przez GGSN
3. Subskrybent asocjuje się i autentykuje do WLAN. Dostaje adres IPw
4. Klient I-WLAN buduje tunel IPSec do PDG, dołączając się do W-APN, IPp przydzielony
5. Klient I-WLAN dołącza się do HA i rejestruje IPp jako CoA
6. Dane płyną przez WLAN z sesją wciąż dołączoną do GGSN/HA



I-WLAN

1. Subscriber opens PDP context and gets IPr assigned

- **Interwencja subskrybenta**
  - Klient I-WLAN
- **Konfiguracja usługi**
  - Zależy od metod uwierzytelnienia WLAN
- **Polityki**
  - Całość ruchu przepływa przez GGSN, PCEF z reguły blisko zintegrowana.
- **Mobilność**
  - Transparentna
  - Oprogramowanie klienckie decyduje o przełączeniu
  - Całość danych do UE kierowana na IPr
- **Sieć strony 3ciej**
  - Możliwe porozumienia między operatorami

Podsumowując

Architektury Offload

Architektura	Interwencja subskrybenta	Konfiguracja klienta	Polityki	Mobilność	Sieci stron 3cich
Ręczna kontrola	Autentykacja				
TAL					
EAP					
NGHS					
MIP	Mobilność				
I-WLAN					

Architektury Offload

Architektura	Interwencja subskrybenta	Konfiguracja klienta *	Polityki	Mobilność	Sieci stron 3cich
Ręczna kontrola	Tak	Tak	Nie	Nie	Tak
TAL	Tak	Tak	Przy przełączeniu do rdzenia	Do zrobienia	Dostępne
EAP	Non SIM	Minimalna	Przy przełączeniu do rdzenia	Do zrobienia	Dostępne
NGHS	Non SIM	Tak	Przy przełączeniu do rdzenia	Do zrobienia	Dostępne
MIP	Klient	Nie	Tak	Tak	Tak, nie szyfrowane
I-WLAN	Klient	Nie	Tak	Tak	Tak, szyfrowane

Dziękuję.