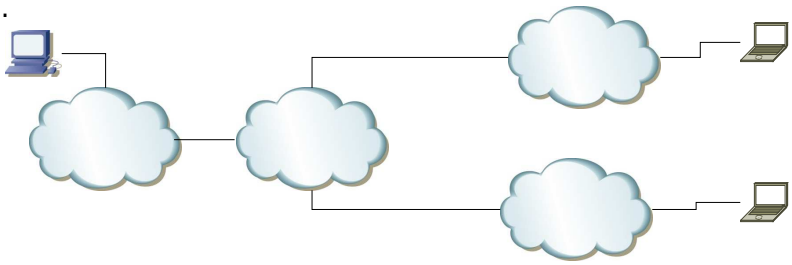
Mobile IP

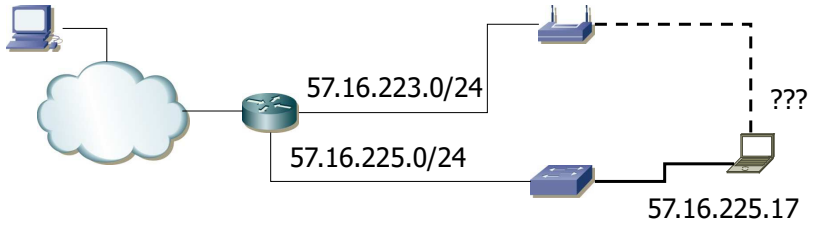
Problem

- Jak przenieść hosta z sieci do sieci?
- „Dodatkowe” wymagania:
  - komunikacja z przenoszonym hostem ma być cały czas możliwa -
    - *nomadic* != *mobile*
  - zmiany konfiguracyjne na urządzeniach (zarówno końcowych, jak i pośredniczących) mają być minimalne
  - przeniesienie nie może wymagać interwencji administratora
  - ...



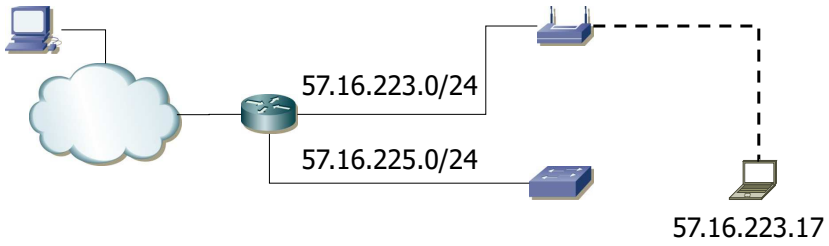
„Tradycyjny” Internet

- Adresy IP służą do dwóch celów:
  - identyfikacja hosta,
  - identyfikacja sieci, do której host jest połączony.
- Routing bazuje na prefiksach adresów IP przypisywanych hostom końcowym
- Zmiana miejsca podłączenia do sieci wymaga zmiany adresu IP na topologicznie poprawny lub dostosowania tablicy routingu



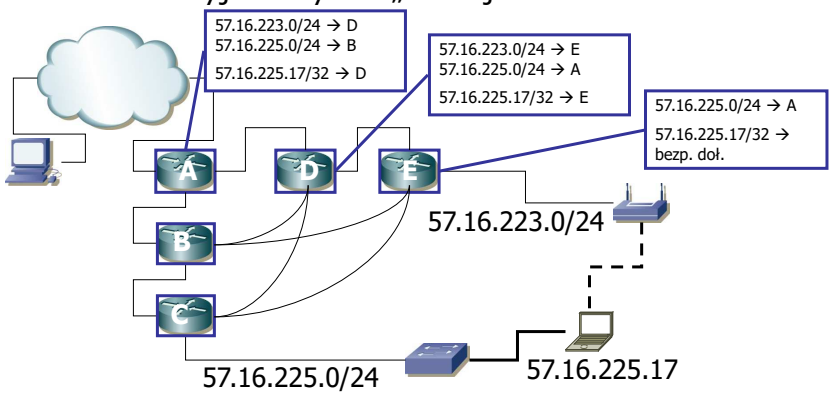
Zmiana adresu IP

- Wada: konieczność zerwania połączeń realizowanych np. przez TCP
- Problem ze znalezieniem przeniesionego hosta
  - można rejestrować się na nowo w DNS, ale to rozwiązanie jest zbyt wolne



Zmiana lub dodanie ścieżek

- Konieczność dodania ścieżki do hosta na routerach pośredniczących
- Konieczność uruchomienia mechanizmu *proxy ARP* na routerze wyjściowym z „nowej” sieci



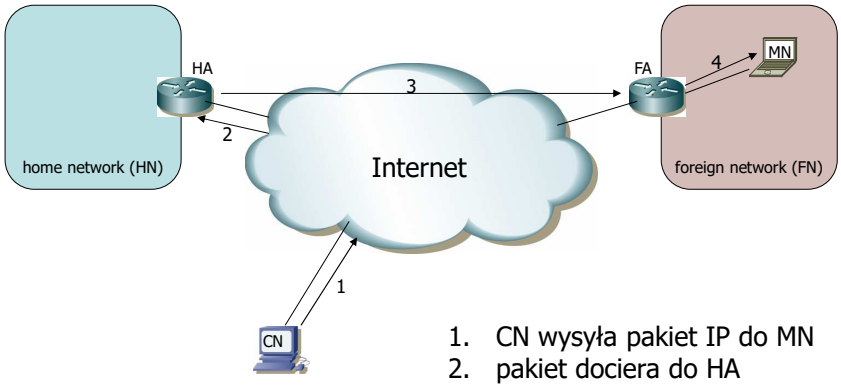
Wymagania stawiane Mobile IP
(RFC 2002 → RFC 3220 → RFC 3344)

- Kompatybilność:
  - współpraca ze wszystkimi protokołami warstwy 2, z którymi współpracuje „zwykłe” IP,
  - brak konieczności dokonywania zmian w istniejących hostach oraz routerach,
  - możliwość komunikacji systemów mobilnych z „tradycyjnymi”.
- Przezroczystość:
  - brak konieczności zmiany adresów IP na hostach mobilnych,
  - możliwość kontynuowania komunikacji po zmianie umiejscowienia hosta.
- Wydajność, skalowalność:
  - jak najmniej dodatkowych komunikatów,
  - możliwość obsługi na skalę ogólnoświatową.
- Bezpieczeństwo:
  - autentykacja komunikatów konfiguracyjnych.

Terminologia

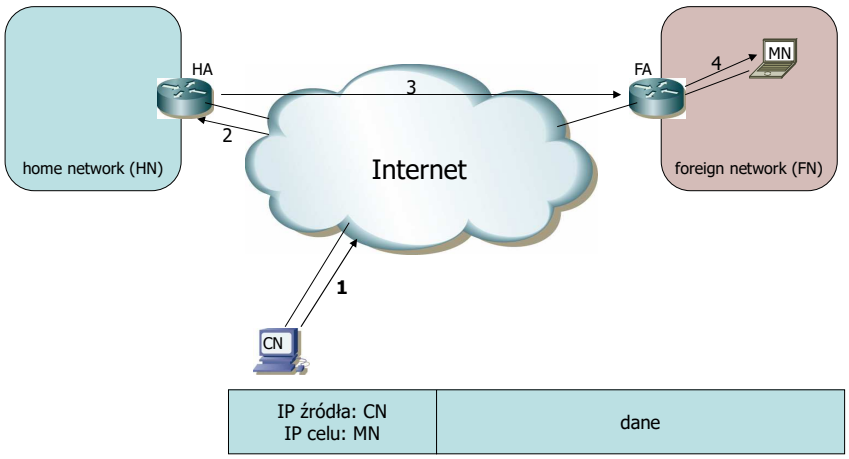
- Home Network (HN): sieć domowa mobilnego hosta
- Home Agent (HA): router w sieci domowej pełniący funkcję agenta Mobile IP
- Foreign Network (FN): sieć, do której mobilny host został przeniesiony
- Foreign Agent (FA): router w sieci FN pełniący funkcję agenta Mobile IP
- Mobile Node (MN): host mogący zmieniać miejsce podłączenia do sieci
- Corresponding Node (CN): host komunikujący się z MN (może także być mobilny)

Jak to „z grubsza” działa

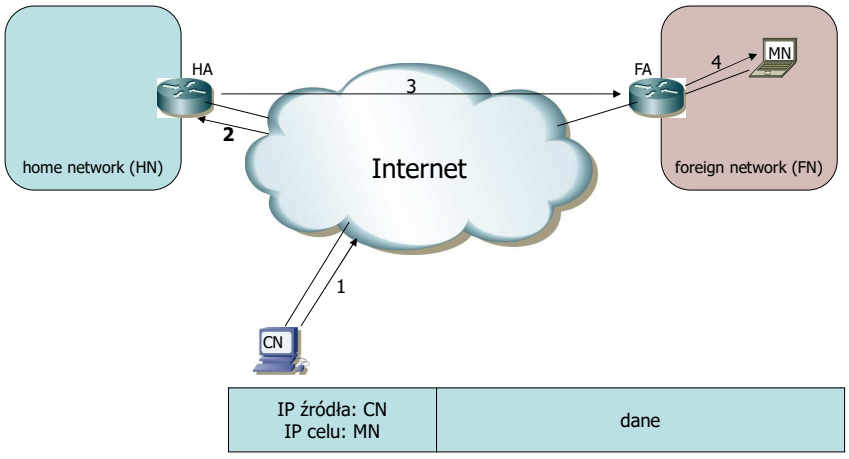


1. CN wysyła pakiet IP do MN
2. pakiet dociera do HA
3. HA przesyła pakiet do FA
4. FA przesyła pakiet do MN

1. CN wysyła pakiet IP do MN

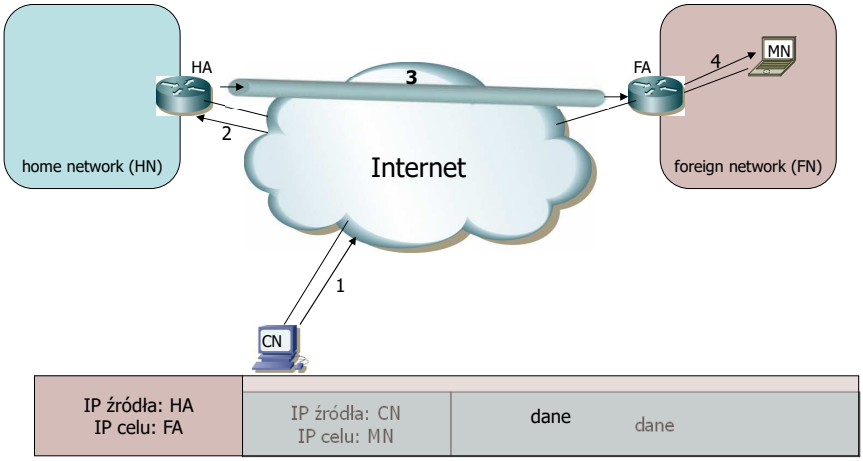


2. Pakiet dociera do HA



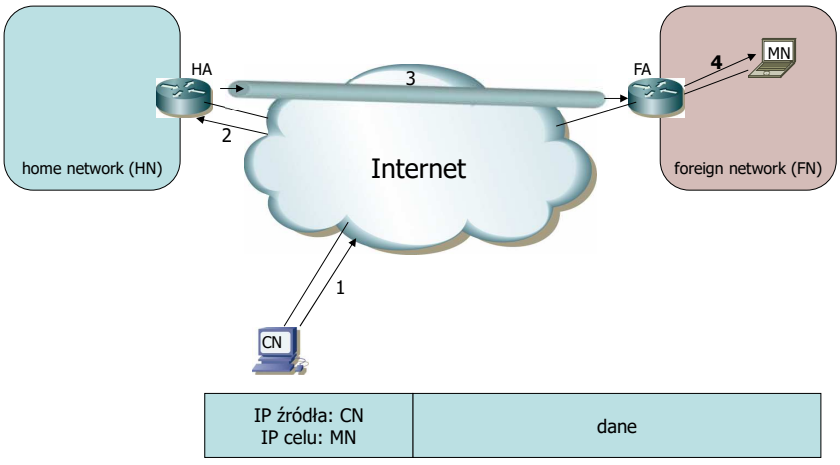
HA „przechwytuje” pakiet

3. HA przesyła pakiet do FA



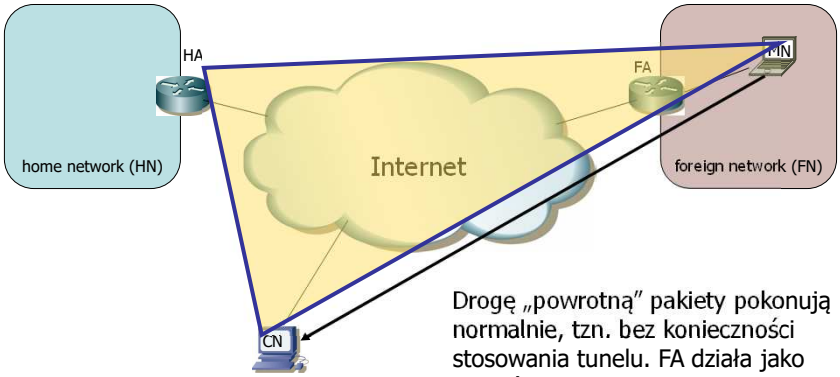
Aby pakiet trafił do FA, zostaje przesłany za pomocą tunelu.

4. FA przesyła pakiet do MN



FA „odpakowuje” pakiet z tunelu i przesyła go do hosta docelowego.

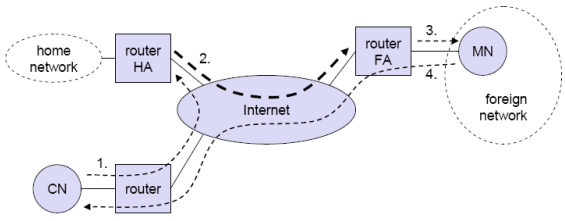
Ścieżka MN -> CN



Drogę „powrotną" pakiety pokonują normalnie, tzn. bez konieczności stosowania tunelu. FA działa jako domyślny router dla MN.
Opisane podejście nazywane jest „routingiem w trójkącie" (ang. *triangle routing*).

Jak realizuje się Mobile IP?

- Skąd CN wie, że ma przesłać pakiet w stronę HA?
- Skąd HA wie, że ma przechwycić pakiet kierowany do MN?
- Skąd HA wie, do kogo ma przekazać przechwycony pakiet?
- Skąd FA wie, że dany MN jest do niego podłączony?
- Skąd MN wie o istnieniu HA i FA?



Jak realizuje się Mobile IP?

- Skąd CN wie, że ma przesłać pakiet w stronę HA?
  - CN tego nie wie, wiedzą to routery
  - routery wiedzą, gdzie jest HN hosta MN
  - do przesłania pakietu w stronę HN zawierającej HA stosowany jest „zwykły” routing
- Skąd HA wie, że ma przechwycić pakiet kierowany do MN?
  - HA jest o tym informowany przez MN w procesie **rejestracji**
- Skąd HA wie, do kogo ma przekazać przechwycony pakiet?
  - HA jest o tym informowany przez FA w procesie **rejestracji**
- Skąd FA wie, że dany MN jest do niego podłączony?
  - FA jest o tym informowany przez MN w procesie **rejestracji**
- Skąd MN wie o istnieniu HA i FA?
  - dowiaduje się o tym za pomocą procedury **wykrywania agenta**

Wykrywanie agenta

Procedura wykrywania agenta

- Agent Mobile IP periodycznie wysyła ogłoszenia o swoim istnieniu
- MN nasłuchuje na te ogłoszenia i wnioskuje, czy jest w HN, czy w (jakiejś) FN
- MN czyta **COA** (*care-of address*) z ogłoszenia agenta
  - COA jest adresem IP, na którym kończy się tunel (po stronie FN)
- MN może „przyspieszyć" ogłoszenie agenta przez rozgłoszenie odpowiedniego komunikatu

Ogłoszenie o istnieniu agenta

- Realizowane jako rozszerzenie IRDP (ICMP Router Discovery)

version (4)	header len	type of service	total length
identification		flags	fragment offset
time to live = **1**	protocol = ICMP	header checksum	
source address (**adres agenta**)			
destination address (**255.255.255.255** lub **224.0.0.1**)			

type (9)	code	checksum
number of addresses	address entry size	advertisement lifetime
router address 1		
preference level 1		
router address 2		
preference level 2		
...		

type (16)	length = 6+4N	sequence number	
maximum registration lifetime		flags: R,B,H,F,M,G,V	reserved
care-of address 1			
care-of address 2			
...			

type (19)	length	prefix length 1	prefix length 2
...			

Ogłoszenie o istnieniu agenta

- Realizowane jako rozszerzenie IRDP

version (4)	header len	type of service	**total length**
identification		flags	fragment offset
time to live = **1**	protocol = ICMP	header checksum	
source address (**adres agenta**)			
destination address (**255.255.255.255** lub **224.0.0.1**)			

type (9)	**code**	checksum
number of addresses	**address entry size**	advertisement lifetime
router address 1		
preference level 1		
router address 2		
preference level 2		
...		

type (16)	length = 6+4N	sequence number	
maximum registration lifetime		flags: R,B,H,F,M,G,V	reserved
care-of address 1			
care-of address 2			
...			

type (19)	length	prefix length 1	prefix length 2
...			

Ogłoszenie o istnieniu agenta

- Realizowane jako rozszerzenie IRDP

version (4)	header len	type of service	total length
identification		flags	fragment offset
time to live = **1**	protocol = ICMP	header checksum	
source address (**adres agenta**)			
destination address (**255.255.255.255** lub **224.0.0.1**)			

type (9)	**code**	checksum
number of addresses	**address entry size**	advertisement lifetime
router address 1		
preference level 1		
router address 2		
preference level 2		
...		

type (16)	length = 6+4N	sequence number	
maximum registration lifetime		flags: R,B,H,F,M,G,V	reserved
care-of address 1			
care-of address 2			
...			

type (19)	length	prefix length 1	prefix length 2
...			

Ogłoszenie o istnieniu agenta

- Realizowane jako rozszerzenie IRDP

version (4)	header len	type of service	**total length**
identification		flags	fragment offset
time to live = **1**	protocol = ICMP	header checksum	
source address (**adres agenta**)			
destination address (**255.255.255.255** lub **224.0.0.1**)			

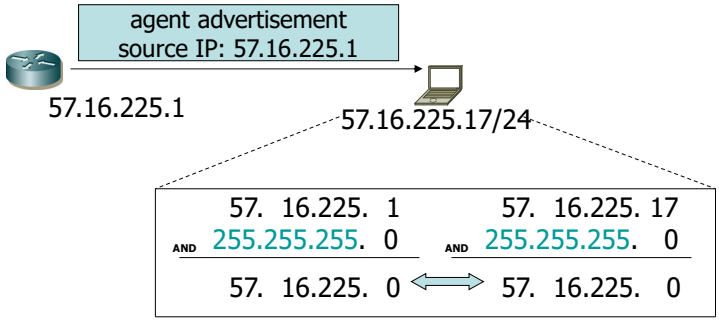
type (9)	**code**	checksum	
number of addresses	**address entry size**	advertisement lifetime	
router address 1			
preference level 1			
router address 2			
preference level 2			
...			

type (16)	length = 6+4N	sequence number	
maximum registration lifetime		flags: R,B,H,F,M,G,V	reserved
care-of address 1			
care-of address 2			
...			

type (19)	length	**prefix length 1**	**prefix length 2**
...			

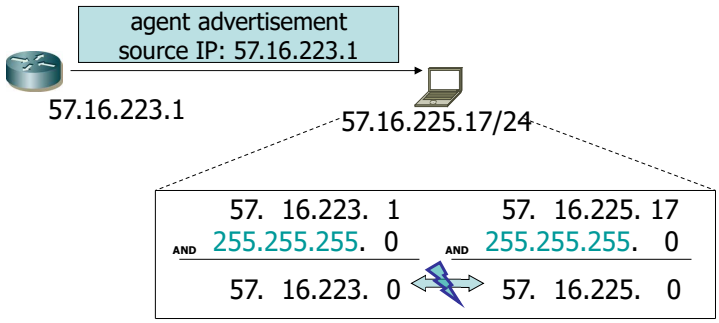
Procedura wykrywania agenta

- Jeżeli adres źródłowy pakietu zawierającego ogłoszenie agenta pokrywa się z adresem HA danego MN lub (bardziej ogólnie) prefiks adresu źródłowego odpowiada prefiksowi adresu MN, to MN znajduje się w HN
  - jeśli powrócił do sieci domowej, to zwalnia dotychczasowe powiązania (ang. *bindings*)



Procedura wykrywania agenta

- Jeżeli prefiks ogłaszanego adresu agenta nie zgadza się
  z prefiksem adresu MN, to MN przyjmuje, że jest w FN i przechodzi do procedury rejestracji



Procedura wykrywania agenta

- Jeżeli MN przestaje odbierać ogłoszenia agentów (upłynie czas *lifetime* ostatniego ogłoszenia), może spróbować wysłania komunikatu *Agent Solicitation*
- Jeżeli wysyłanie komunikatów *Agent Solicitation* nie pomaga, to:
  - MN sprawdza, czy jest w HN poprzez wysłanie *ICMP echo request* do routera domyślnego w HN
    - odpowiedź routera oznacza, że jesteśmy w HN; możliwe, że HA został wyłączony lub uległ awarii
  - jeśli router nie odpowiada, MN zakłada, że jest w FN i próbuje uzyskać *care-of address* (koniec tunelu, COA) do wykorzystania w procedurze rejestracji
    - przez DHCP,
    - z wprowadzonej „ręcznie” konfiguracji.
  - w tym przypadku koniec tunelu znajduje się na MN

Procedura wykrywania agenta

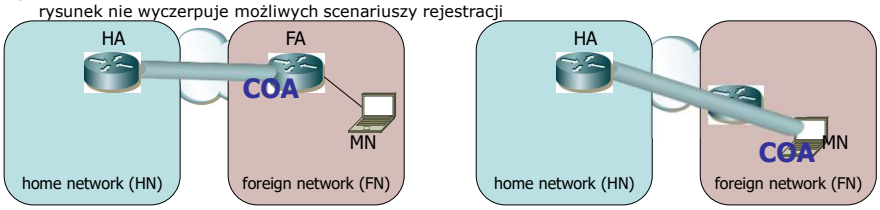
- Problem: w jaki sposób MN może wykryć przeniesienie pomiędzy „bezagentowymi” FN?
  - rozwiązanie 1: Śledzenie transmisji na warstwie 4
    - „urwanie” wszystkich transferów oznacza konieczność uzyskania nowego COA itd.
  - rozwiązanie 2: Przełączenie karty sieciowej w tryb promiscuous i śledzenie pakietów IP pojawiających się na łączu
    - jeśli nie pojawiają się adresy źródłowe z sieci COA, to trzeba go wymienić
- Problem: w jaki sposób MN ma znaleźć domyślny router w „bezagentowej” FN?
  - brak wiadomości router/agent advertisement,
  - brak informacji z DHCP,
  - zakaz wysyłania zapytań ARP z domowym adresem IP,
  - rozwiązanie: w przypadku posiadania co-located COA można wysłać zapytanie ARP z COA jako adresem źródłowym

Rejestracja

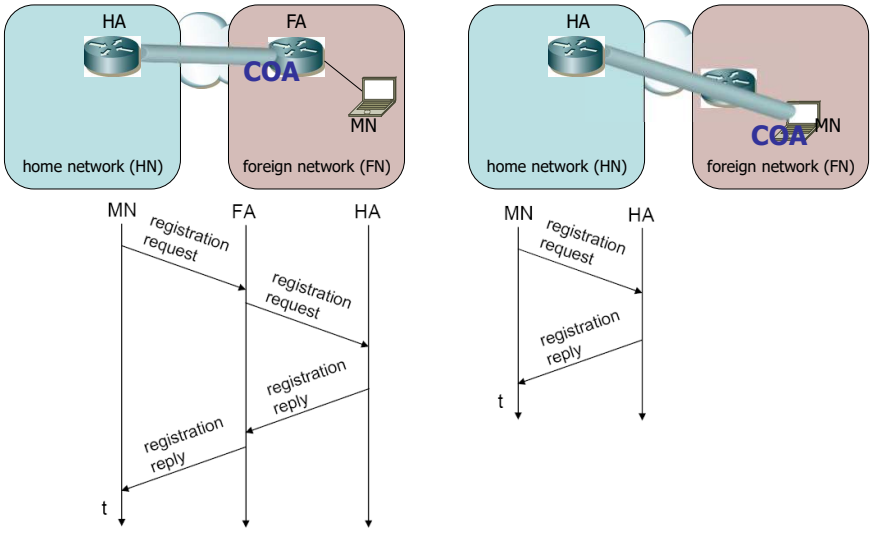
Procedura rejestracji

- Inicjowana jest przez MN każdorazowo po wykryciu przeniesienia do innej FN (lub z powrotem do HN)
- Podstawowy cel: poinformowanie HA o dostępności MN
- Przebieg procedury rejestracji zależy od tego, gdzie ma się kończyć tunel pomiędzy HA a FN*
  - MN rejestruje się w HA bądź to za pośrednictwem FA, bądź bezpośrednio (korzysta z *co-located care-of address*)

* rysunek nie wyczerpuje możliwych scenariuszy rejestracji

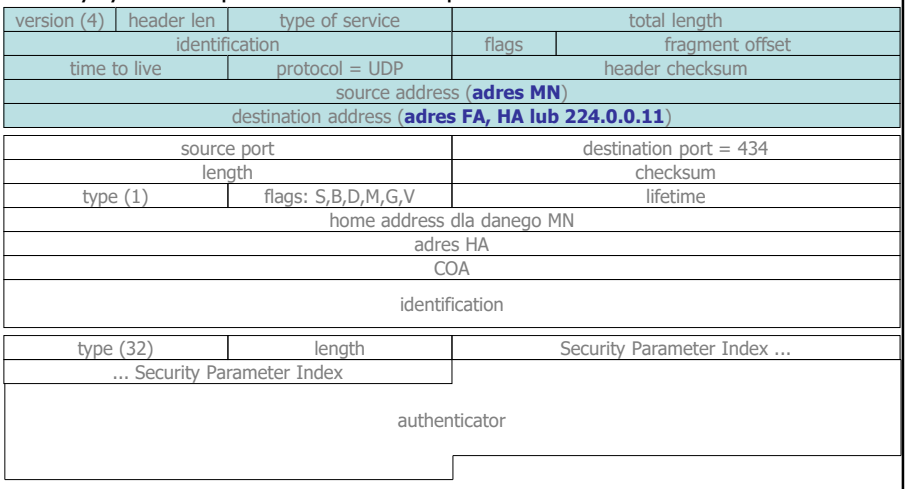


Procedura rejestracji



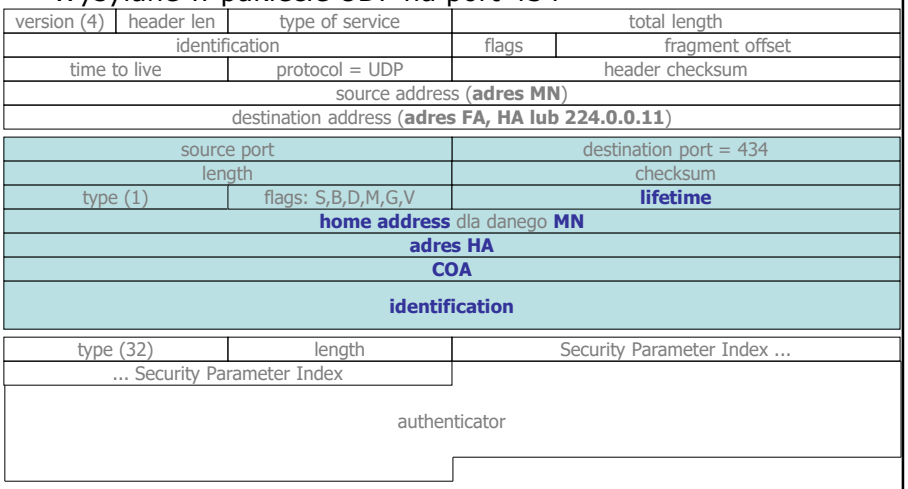
Żądanie rejestracji

- Wysyłane w pakiecie UDP na port 434



Żądanie rejestracji

- Wysyłane w pakiecie UDP na port 434



Żądanie rejestracji

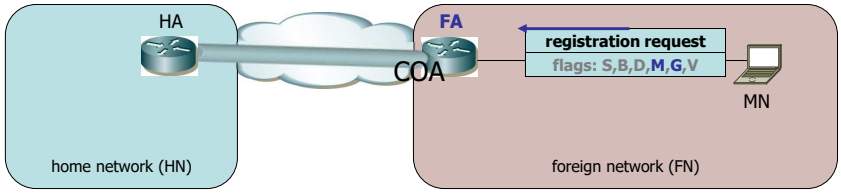
- Wysyłane w pakiecie UDP na port 434

version (4)	header len	type of service	total length	
identification			flags	fragment offset
time to live		protocol = UDP	header checksum	
source address (**adres MN**)				
destination address (**adres FA, HA lub 224.0.0.11**)				

source port		destination port = 434
length		checksum
type (1)	flags: S,B,D,M,G,V	**lifetime**
home address dla danego **MN**		
adres HA		
COA		
identification		

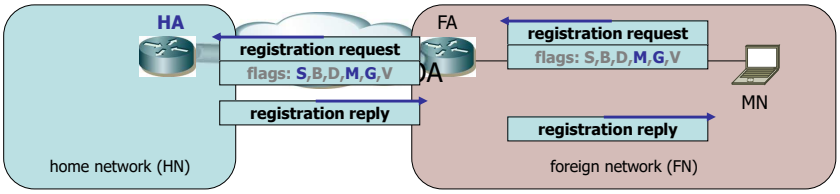
type (32)	length	**S**ecurity **P**arameter **I**ndex ...
... **S**ecurity **P**arameter **I**ndex		
authenticator		

Przetwarzanie żądania rejestracji



- **FA** po odebraniu żądania rejestracji od MN:
  - sprawdza, czy żądanie rejestracji jest poprawne i uprawnione
    - jeśli nie, to je odrzuca i wysyła registration reply z kodem błędu:
      - authentication failed
      - maximum lifetime exceeded
      - requested tunelling mode not supported
      - insufficient resources
      - ...
  - zapamiętuje niektóre dane z żądania w celu przekazania odpowiedzi
  - przekazuje zmodyfikowane żądanie do HA
    - zmieniają się adresy warstwy 3, dane (pola Mobile IP) pozostają

Przetwarzanie żądania rejestracji



- **HA** po odebraniu żądania rejestracji przekazanego przez FA:
  - sprawdza, czy żądanie rejestracji jest poprawne i uprawnione
    - jeśli nie, to je odrzuca i wysyła registration reply z odpowiednim kodem błędu
  - uaktualnia powiązania
  - tworzy lub zamyka tunel
  - generuje odpowiedź (registration reply) i wysyła ją do FA
- FA sprawdza poprawność odpowiedzi, modyfikuje ją i przekazuje do MN
- w razie odrzucenia żądania MN może próbować „poprawić" błąd
  - np. wysyła nowe żądanie z mniejszym lifetime

Jak MN może „zdalnie" poznać HA?

- Założenie: MN zna swój adres domowy i długość prefiksu HN
- Jeżeli MN nie ma skonfigurowanego adresu HA, może wysłać żądanie rejestracji wstawiając w miejsce adresu HA skierowany broadcast do HN
- Żądanie takie dotrze do wszystkich agentów obecnych w HN i zostanie odrzucone
- Odpowiedź odrzucająca żądanie rejestracji zawiera adres źródłowy odrzucającego agenta
- FA przekazuje do MN informację o odrzuceniu żądania
- MN pobiera adres agenta z przekazanej odpowiedzi i formułuje nowe żądanie z unicastowym adresem HA

Przetwarzanie żądania rejestracji

- Flaga „S” oznacza „save existing bindings”; dokładniejsza interpretacja jest dokonywana w połączeniu z innymi polami:

COA	lifetime	S	Znaczenie
!= home addr.	>0	0	nadpisz dotychczasowe powiązania
!= home addr.	>0	1	dodaj nowe powiązanie
!= home addr.	0	1	usuń wyspecyfikowane powiązanie
== home addr.	0	*	usuń wszystkie powiązania
== home addr.	>0	*	MN jest uszkodzony

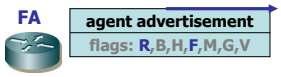
- Flaga „B” oznacza, że do zarejestrowanego urządzenia mają być przekazywane pakiety broadcastowe pojawiające się w HN

Przetwarzanie żądania rejestracji

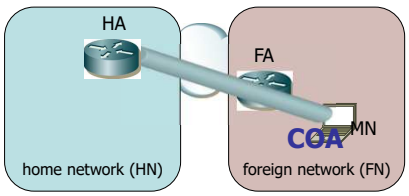
- Flaga „D” oznacza, że MN sam dokonuje dekapsulacji, czyli jest końcem tunelu, a więc korzysta z co-located COA
  - ma to znaczenie szczególnie w przypadku przekazywania broadcastów.
- Flaga „M” oznacza, że MN oczekuje, że skonstruowany tunel będzie korzystał z tzw. „minimal encapsulation”; flaga „G” oznacza żądanie enkapsulacji GRE (Generic Routing Encapsulation)
- Flaga „V” oznacza żądanie kompresji nagłówków TCP (van Jacobson)

Wymuszanie rejestracji

- Flaga „F” oznacza, że ogłaszający się agent pełni funkcję FA dla danej sieci



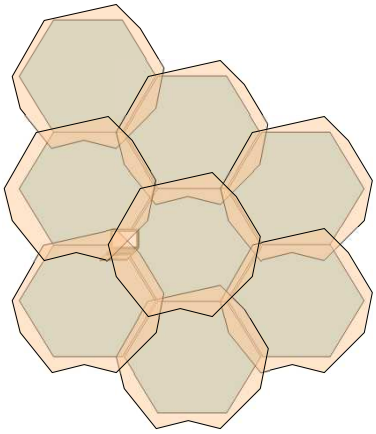
- Flaga „R” informuje hosty, że muszą rejestrować się za pośrednictwem FA
  - to nie znaczy, że nie mogą korzystać z co-located COA – tyle że FA musi brać udział w rejestracji
    - w takim wypadku po rejestracji FA pełni funkcję „zwykłego” routera; nie kończy tunelu
  - cel: np. billing – ISP sprawdza, czy dany MN jest jego klientem
  - funkcjonalność ta ma sens, jeśli ISP jest w stanie blokować pakiety, które wyszły z MN zarejestrowanego bez pośrednictwa FA



Optymalizacja

Jak zapobiec częstym zmianom powiązań przez MN?

- Problem: MN znajduje się np. na styku kilku komórek sieci bezprzewodowej

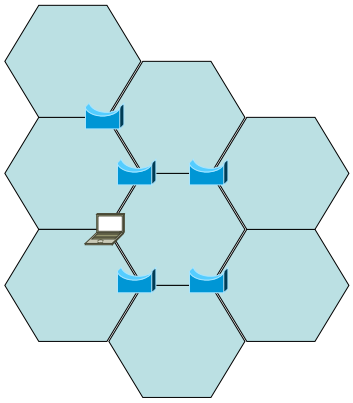


- rzeczywisty zasięg przekaźników kształtem nie odpowiada sześciokątom
- zasięg przekaźników może nawet zmieniać się w czasie

- MN może zmieniać punkty przyłączenia do sieci nawet nie ruszając się z miejsca

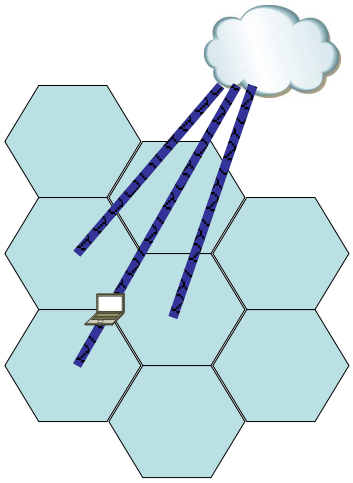
- MN po zmianie punktu przyłączenia na nowo się rejestruje

Jak zapobiec częstym zmianom powiązań przez MN?



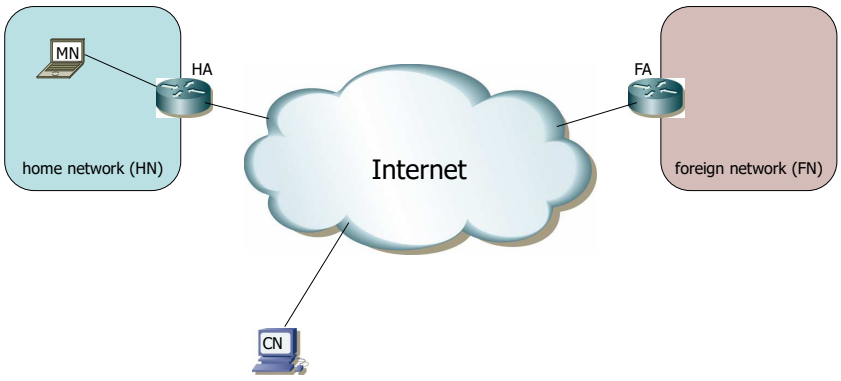
- Rozwiązanie „spoza Mobile IP”: połączyć sąsiednie komórki na warstwie 2 (za pomocą mostków)
  - komórki organizowane są w tzw. konfederacje
  - wewnątrz konfederacji realizowany jest *handover* na warstwie 2
  - osobne konfederacje wykorzystują inne pasma, co utrudnia MN komunikowanie się jednocześnie przez dwie konfederacje
  - MN mimo zmiany komórki nie zmienia FN, więc nie przechodzi ponownej rejestracji
- często stosowane rozwiązanie

Jak zapobiec częstym zmianom powiązań przez MN?



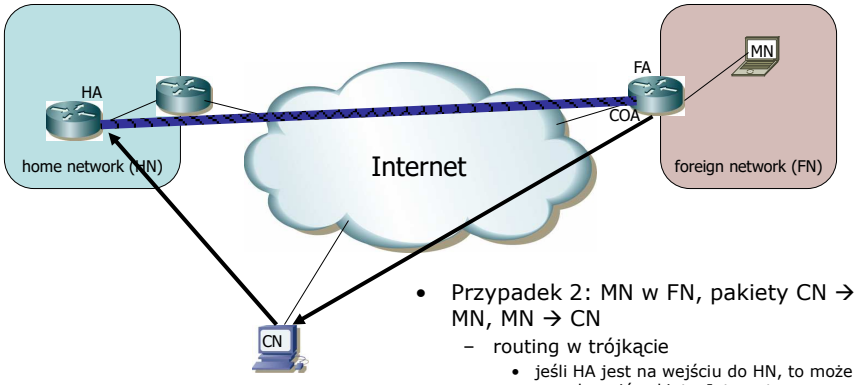
- Rozwiązanie z Mobile IP: przechowywanie wielu powiązań przez HA
  - MN tworzy powiązanie dla każdej komórki
  - pakiety IP przeznaczone dla MN są przez HA przekazywane osobno dla każdego powiązania
    - może się zdarzyć, że do MN dotrze więcej, niż jedna kopia pakietu; z tym ma sobie radzić warstwa 4
  - wada: implementacja tej funkcjonalności jest opcjonalna (HA może, ale nie musi obsługiwać wielokrotnych powiązań)
    - jeśli nie obsługuje, to nadpisuje ostatnie
- Rzadko stosowane, przydatność problematyczna

Jak działa routing do/z MN?



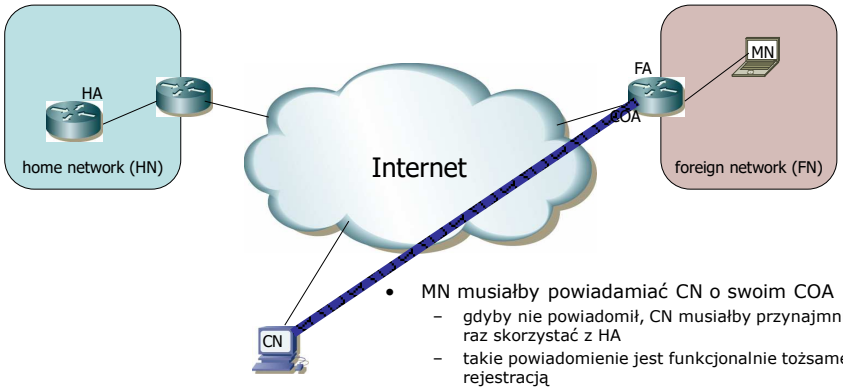
- Przypadek 1: MN w HN, pakiety CN → MN, MN → CN
  - prosta sytuacja: zwykły routing IP

Jak działa routing do/z MN?



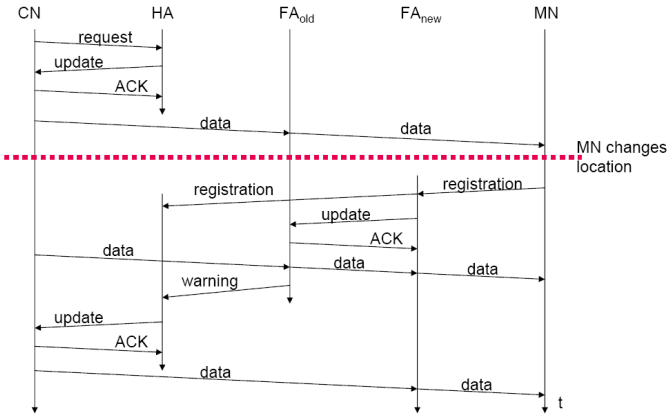
- Przypadek 2: MN w FN, pakiety CN → MN, MN → CN
  - routing w trójkącie
    - jeśli HA jest na wejściu do HN, to może przechwycić pakiet z Internetu
    - jeśli nie, odpowiada na zapytania ARP o MN pojawiające się w HN, po czym przesyła je tunelem na COA odpowiadający(-e) MN
    - MN odpowiada „wprost" do CN

Dlaczego nie tak?



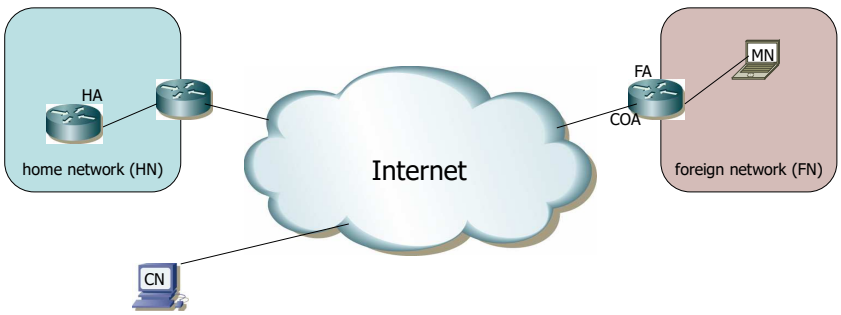
- MN musiałby powiadamiać CN o swoim COA
  - gdyby nie powiadomił, CN musiałby przynajmniej raz skorzystać z HA
  - takie powiadomienie jest funkcjonalnie tożsame z rejestracją
    - w procesie rejestracji musi zachodzić autentykacja hostów
    - jak dystrybuować klucze?
- Taka optymalizacja Mobile IP przynosi realne korzyści tylko wtedy, gdy CN i MN znajdują się geograficznie blisko siebie

Optymalizacja zmiany FA



- Cel: zapobieganie utracie pakietów przy zmianie FA
- Przy okazji „stary” FA jest informowany, kiedy może zwolnić zasoby

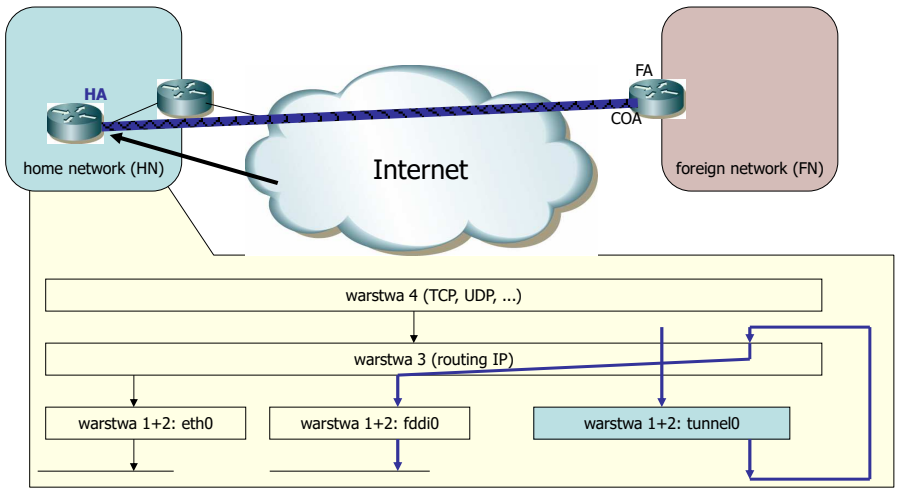
Dlaczego nie source routing?



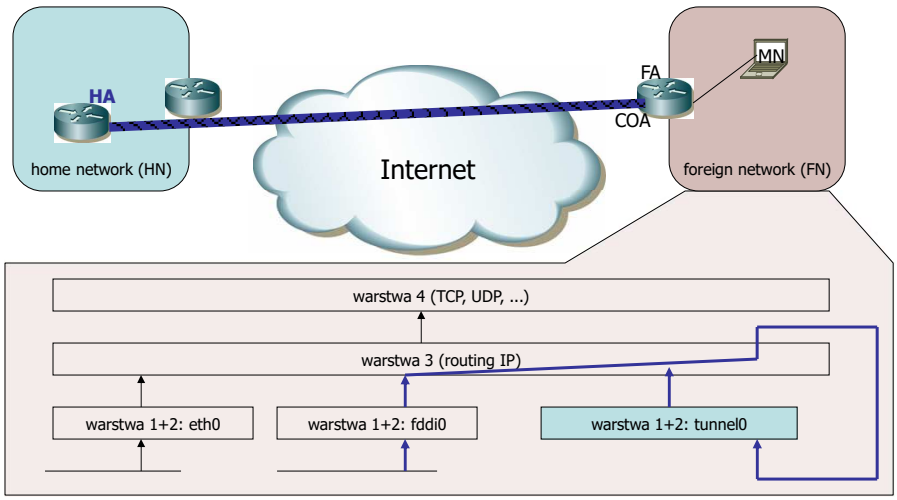
- Mogłoby być tak:
  - MN w pakietach do CN stosowałby opcje Record Route oraz Loose Source Route
  - CN odwracałby kolejność routerów w liście i odpowiadał z wykorzystaniem lepszej ścieżki
- A jest...
  - wiele implementacji IP nie stosuje się do wymagania odnośnie odwracania ścieżki
  - pakiety IP z opcjami są przez routery przetwarzane znacznie mniej efektywnie (nawet 10:1)
  - takie podejście jest wystawione na ataki przez podszycie
    - łatwo jest sfabrykować pakiet IP z jakimś COA i fałszywą listą adresów

Routing – trochę dokładniej

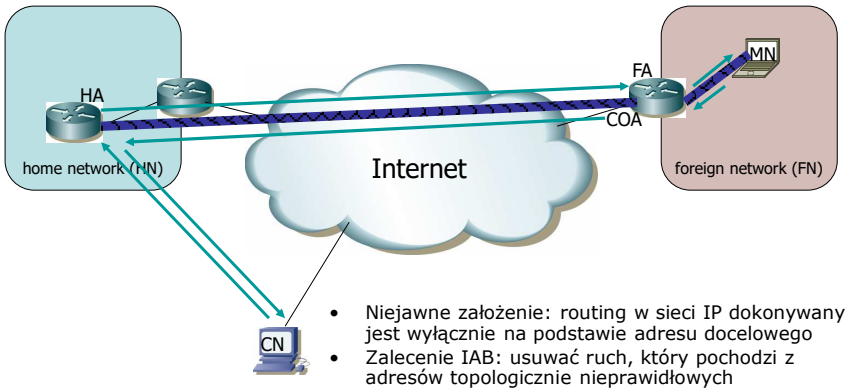
Co „siedzi” w tablicy routingu HA?



Co „siedzi” w tablicy routingu FA?



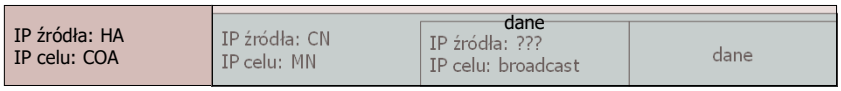
Reverse tunneling



- Niejawne założenie: routing w sieci IP dokonywany jest wyłącznie na podstawie adresu docelowego
- Zalecenie IAB: usuwać ruch, który pochodzi z adresów topologicznie nieprawidłowych
- Rozwiązanie: tunelowanie ruchu z powrotem do HA, który przekazuje go do CN
- Czasami musi istnieć dodatkowy tunel pomiędzy MN a FA

Odbieranie broadcastów przez MN

- MN z co-located COA:
  - broadcasty są powtarzane jeśli MN ustawił bit B w żądaniu rejestracji
  - pakiety takie są tunelowane tak, jak unicastowe
- MN z COA na FA:
  - konieczny jest dodatkowy etap enkapsulacji
    - HA opakowuje broadcast w pakiet IP(HA)→IP(MN)
    - tak opakowany broadcast przesyła tunelem



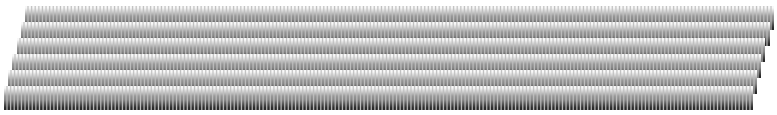
Wysyłanie broadcastów przez MN

- Broadcasty **lokalne** przeznaczone dla FN są po prostu rozgłaszane
- Broadcasty **lokalne** przeznaczone dla HN są tunelowane do HA (przez MN bądź przez FA)
- Broadcasty **skierowane** do sieci HN mogą być tunelowane lub przesyłane „normalnie”
  - UWAGA: broadcasty skierowane są często usuwane przez routery znajdujące się na trasie do sieci docelowej

Wysyłanie i odbieranie multicastów przez MN

- Wysyłanie może być realizowane tak, jak w przypadku broadcastów (tunel do HA) lub bezpośrednio do FN
  z wykorzystaniem co-located COA
- Odbieranie wymaga periodycznego wysyłania pakietów IGMP
  - pakiety te mogą być:
    - tunelowane do HA,
    - wysyłane do routerów w FN z co-located COA,
    - wysyłane do routerów w FN z wykorzystaniem adresu domowego.

Tunelowanie



Tunelowanie

- Datagram IP przeznaczony dla MN jest opakowywany w inny datagram
- Tunel jest z punktu widzenia „wewnętrznego” datagramu pojedynczym łączem
  - „wewnętrzny” TTL jest zmniejszany o 1,
  - „zewnętrzny” TTL jest niezależny od „wewnętrznego”
    - problem: pętla routingu zawierająca tunel „zneutralizuje” mechanizm usuwania krążących pakietów i dodatkowo spowoduje „pakowanie w nieskończoność”

Opcje enkapsulacji w tunelu Mobile IP

- IPinIP – zapakowanie datagramu w nowy datagram
- Minimal encapsulation – dodanie nowego nagłówka pomiędzy oryginalny nagłówek IP i pole danych
- Generic Routing Encapsulation (GRE) – wykorzystanie wieloprotokołowego mechanizmu tunelowania

IPinIP

version (4)	header len	type of service	total length	
identification			flags	fragment offset
time to live		protocol = **IPinIP** (4)	header checksum	
source address (**HA**)				
destination address (**COA**)				

version (4)	header len	type of service	total length	
identification			flags	fragment offset
time to live		protocol	header checksum	
source address (**CN**)				
destination address (**MN home address**)				

dane

- IPinIP – zapakowanie całego datagramu w nowy datagram
  - wewnętrzny pakiet niezmieniony (z wyj. TTL)
  - dodany zewnętrzny nagłówek
  - ze starego nagłówka kopiowane tylko ToS
- Obsługa tunelowania IPinIP przez agentów jest wymagana
- Eliminacja prostych pętli jest możliwa
  - jeśli adres źródłowy pakietu jest równy adresowi „wejściowemu" tunelu lub adresowi „wyjściowemu" tunelu, to pakiet nie jest dodatkowo pakowany

Minimal Encapsulation

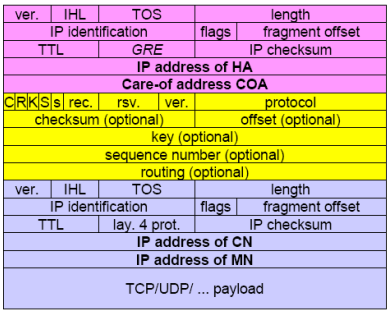
version (4)	header len	type of service	**total length**	
identification			flags	fragment offset
time to live		protocol = **55**	**header checksum**	
source address (**HA**)				
destination address (**COA**)				

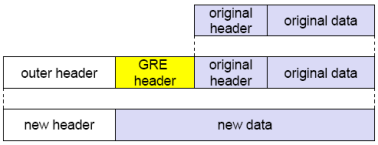
protocol	S	reserved	header checksum
destination address (**MN home address**)			
source address (**CN**)			

dane

- Minimal encapsulation – dodanie nowego nagłówka pomiędzy oryginalny nagłówek IP i pole danych
  - wiąże się to także z modyfikacją nagłówka
    - total length,
    - Protocol,
    - Adresy.
  - dodatkowy nagłówek przenosi informacje wymagane do odtworzenia oryginalnego nagłówka po drugiej stronie tunelu
- Eliminacja prostych pętli – jak w przypadku IPinIP

GRE





- Polega na dodaniu zewnętrznego nagłówka oraz dodatkowego nagłówka GRE
  - pakiety „rosną” sporo,
  - obsługuje nie tylko IP,
  - posiada mechanizm eliminacji rekursywnego tunelowania (pętli routingu zawierających tunel).

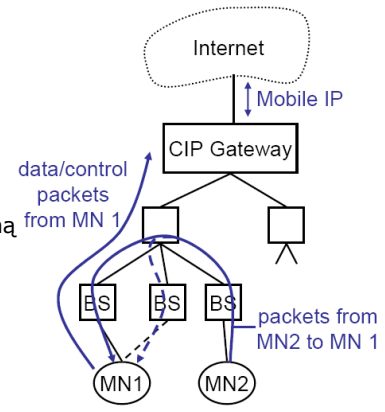
Optymalizacja – c.d.

Micro-mobility

- Istnieje szereg mechanizmów pozwalających na przekazywanie MN (*handover*) wewnątrz domeny
  (tzw. *foreign domain*) bez konieczności przesyłania komunikatów kontrolnych „na drugą stronę Internetu”
  - Cellular IP,
  - HAWAII,
  - Hierarchical Mobile IP (HMIP).

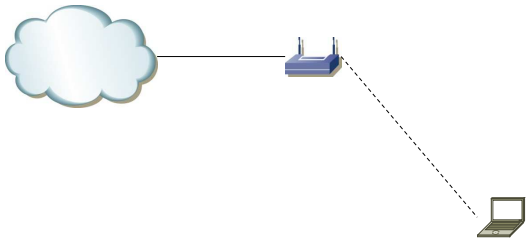
Cellular IP

- Tunele kończą się na Cellular IP Gateway
- Zalety:
  - ruch wewnątrzdomenowy realizowany jest lokalnie
  - nie ma wymagania, by wewnątrz domeny hosty mogły się komunikować na warstwie 2
  - prostota i elegancja
  - możliwość integracji z adr. prywatną
- Problemy:
  - nieustandaryzowane metody autentykacji,
  - autentykacja MN na podstawie znajomości *network key*
  - brak mechanizmu automatycznej wymiany klucza
  - szyfrowanie z kluczem publicznym może być za trudne dla MN



Mobile IP Proxy

- Problem: obsługa Mobile IP wymaga od MN posiadania odpowiedniego oprogramowania
- Rozwiązanie: wiele hostów MN reprezentowane przez proxy
- Zaleta: brak konieczności instalowania dodatkowych pakietów na hostach końcowych
- Wada: bardziej złożona autentykacja



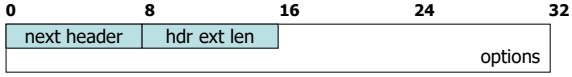
Mobile IPv6

Routing Header

- Identyfikowany przez wartość 43 w poprzedzającym nagłówku
- Funkcjonalnie podobny do opcji Loose Source Routing oraz Record Route w IPv4
- Składa się z następujących pól:
  - next header – oznaczenie następnego nagłówka
    - wykorzystuje także wartości oznaczające protokół warstwy 4 w IPv4 (RFC 1700)
  - hdr ext len – zawiera długość nagłówka w jednostkach 8-oktetowych, bez pierwszych 8 oktetów
  - routing type – identyfikator wariantu
  - segments left – ilość punktów pośrednich, przez jakie pakiet musi przejść
  - type-specific data – pole o zmiennej długości; format zdeterminowany jest przez pole routing type
    - cały nagłówek musi mieć długość N*8 oktetów

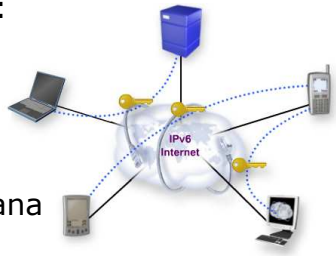
Destination Options Header

- Identyfikowany przez wartość 60 w poprzedzającym nagłówku
  - jeśli występuje, musi być pierwszy
- Składa się z następujących pól:
  - next header – oznaczenie następnego nagłówka
    - wykorzystuje także wartości oznaczające protokół warstwy 4 w IPv4 (RFC 1700)
  - hdr ext len – zawiera długość nagłówka w jednostkach 8-oktetowych, bez pierwszych 8 oktetów
  - options – pole o długości N*8-2 oktetów
    - cały nagłówek musi mieć długość N*8 oktetów



IPSec

- Standard IETF dotyczący zabezpieczenia sieci IPv4 oraz IPv6
  - definiuje dwa protokoły (dla IPv4):
    - ESP (encapsulating security payload):
      - szyfrowanie zawartości pakietu
      - autentykacja
    - AH (authentication header)
      - autentykacja
  - w IPv6 obsługa IPSec jest wymagana
    - nagłówek Authentication,
    - nagłówek Encapsulating Security Payload.
- Problem: dystrybucja kluczy

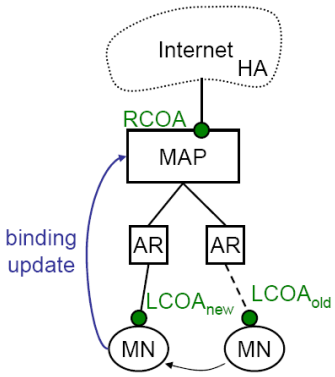


Co wnosi IPv6?

- Dużo adresów
  - Mobile IPv6 działa tylko na co-located COA uzyskiwanym za pomocą autokonfiguracji
- Mniejsze wymagania w stosunku do przetwarzania opcji
  - w szczególności Routing Header musi być przetwarzany tylko przez „zainteresowane" routery (wyznaczone przez adres docelowy)
  - host, który odebrał pakiet z nagłówkiem Routing Header nie musi wysyłać odpowiedzi z analogicznym nagłówkiem
- Authentication Header
  - na razie nie na wiele się przydaje (brakuje standardowego mechanizmu dystrybucji kluczy), ale wymaganie obsługi AH pozwoli na przejście do optymalizowanego routingu, gdy taki mechanizm powstanie
- Ogłaszanie zmian COA (binding update)
  - przesyłane do HA i niektórych CN
    - taki CN musi przechowywać wszystkie dane potrzebne do utworzenia tunelu (tzw. *Security Association*)
  - komunikat *binding update* jest przesyłany wewnątrz nagłówka Destination Options
    - podobnie *binding request* oraz *binding acknowledge*

HMIPv6

- MAP: mobility anchor point
  - odwzorowuje RCOA na LCOA
- RCOA: *regional care-of address*
- LCOA: *link care-of address*
- Przy zmianie łącza MN informuje o tym wyłącznie MAP
  - HA jest informowany o zmianie MAP
- Zalety:
  - LCOA może być ukryty
  - możliwy jest bezpośredni routing pomiędzy hostami na tym samym łączu
  - mała ilość zmian przy zmianie łącza
  - można korzystać z adresacji prywatnej
- Problemy:
  - decentralizacja zabezpieczeń (różne MAPy realizują autentykację)
  - MN wpływają na zawartość tablic routingu
  - MN musi mieć „świadomość" korzystania z HMI.
  - przesyłanie komunikatów służących do zmiany tablic routingu przez łącza bezprzewodowe



Źródła

- J. D. Solomon, *Mobile IP: The Internet Unplugged*, Prentice Hall 1998
- J. Schiller, *Mobile Communications*, Addison-Wesley 2000
- R. Wattenhofer, *Mobile Computing*
- RFC 3344: IP Mobility Support for IPv4
- RFC 3753: Mobility Related Terminology
- RFC 3775: Mobility Support in IPv6
- RFC 2003: IP Encapsulation within IP
- RFC 2004: Minimal Encapsulation within IP
- RFC 4140: Hierarchical Mobile IP Version 6

KONIEC