Universitatea Politehnica București
Facultatea de Electronică, Telecomunicații și Tehnologia Informației

MOBILE IPv6

Stundeți:
Bălănescu Diana
Vasile Ioana Iuliana
Grupa 442 A

Anul universitar 2011 – 2012

Cuprins

1. Introducere

de Vasile Ioana Iuliana

Mobilitatea este importantă şi incontestabilă la momentul actual, având în vedere noile dispozitive portabile care au acaparat piaţa şi necesitatea conectivităţii continue la Internet. Internetul este acum indinspensabil din viaţa de zi cu zi, iar cantităţile de informaţii care se transmit cresc. Astfel, conxiunile la internet sunt acum rapide, eficiente şi economice pentru un nod terminal. Este preferat în căutarea informaţiilor, în comunicaţii personale şi profesionale şi divertisment. Telefoanele inteligente, tablete, laptopuri de dimensiuni reduse au în comun mobilitatea, faptul ca pot fi folosite în orice locaţie, chiar în timp ce te mişti, iar performanţele hardware şi software cer conexiuni rapide la internet care să suporte transfer masiv ca *streaming*-ul. Momentan, conexiunea de reţea actuală este portabilă, nu mobilă, ceea ce înseamnă că reconectările nu sunt automate şi neinteractive, cum se doreşte a fi. Pentru acest tip se dezvolta reţeaua mobilă.

Mobile IP (*MIP*) este un protocol care aigură mobiliteatea unui nod în Internet. Aceasta însemnă că un nod terminal (*end terminal*) poate fi contactat chiar dacă îşi modifică locaţia. Dacă acest protocol nu ar exista, pachetele destinate acestui terminal mobil nu ar putea sa ajungă la destinaţie dacă terminalul se deplasează în altă locaţie decât cea iniţială (*home link*). Pentru a continua transferul chiar dacă nodul îşi modifică locaţia, acesta îşi poate schimba adresa IP, dar nu s-ar permite transfer continuu de pachete, mai ales dacă acestea sunt asociate între ele.

Astfel, protocolul MIP asigură posibilitatea nodului mobil să se mute de la un punct de legătură la altul fără să îşi schimbe „adresa de origine” (*home address*). Deci, pachetele pot fi rutate către nod folosind acestă adresă indiferent de punctul curent care îl leagă la Internet, permitând conexiuni transparente cu alte nodori (chiar dacă sunt staţionare, sau la rândul lor mobile).

Mobile IPv6 vine să înlocuiască cel destinat IPv4, folosindu-se de îmbunătăţirile aduse de protocolul IPv6. Necesitatea apariţiei IPv6 este dată de epuizarea adreselor din IPv4, algoritmi de rutare mai eficienţi, dezvoltarea reţelelor de viteze ridicate. Chiar IPv6 a fost ameliorat pentru a putea fi implementat MIPv6.

Perspectivele acestui protocol sunt sunt nemăsurabile: se poate face o comparaţie cu introducerea telefoniei mobile în telecomunicaţii, telefonul fix ar putea fi comparat cu sistemele desktop legate la Internet printr-o priză, iar telefoanele mobile pot fi comparate cu dispozitivle portabile legate la Internet folosind Mobile IP. Libertatea oferită de apariţia celularelor se formulează prin posibilitatea începerii unui apel telefonic într-o locaţie şi finalizarea lui în alta, utilizatorul putând fi contactat oricând oricând şi oriunde dacă este în posesiea telefonului mobil. Acelaşi lucru se poate prevede şi prin folosirea Mobile IP: transfer continuu de pachete prin Internet în timp ce ne deplasează fără să ne îngrijorăm de necesiteatea unei reconectări.

2. Utilizări

de Vasile Ioana Iuliana

După cum spuneam, MIPv6 este folositor pentru aplicaţiile în care schimbările de conexiune şi ale adresei IP creează probleme. Printre acesteasunt: VPN şi VoIP.

Un VPN (*Virtual Private Network*) este o reţea virtuală privată care foloseşte reţeaua Internet pentru furniza conexiuni securizate asemanătoare unor reţele private, folosite de obicei în cadrul diverselor tipuri companii sau organizaţii. Astfel, utilizatorii se pot conecta la reţeaua de bază, chiar dacă nu sunt conectaţi fizic la ea, ci prin intermediul Internetului. Sunt folosite atunci când se doreşte schimbul de informaţii între diverse sucursale ale companiilor sau când angajatul trebuie sa lucreze din altă locaţie decât biroul său.

VoIP (*Voice over Internet Protocol*) sau Voce peste Protocolul de Internet sau Telefonie IP este un proces de transmitere a conversaţiilor vocale prin legături IP prin reţelele care folosesc acest protocol. Cea mai cunoscută şi folosită aplicaţie VoIP este Skype. Avantajul acetui tip de telecomunicaţie este preţul scazut faţă de telefonia clasică, mai ales când e vorba de apeluri în alte ţări. În ultima vreme s-a dezoltat VoIP în cadrul companiilor pentru a scădea preţul convorbirilor din interior.

Utilizarea nativă a acestui protocol în mediile atât mobile, cât şi cele cu fir în care utilizatorii trebuie să îşi transporte dispozitivele protabile prin mai multe subreţele LAN. Un exemplu bun îl reprezintă roming-ul între diverse sisteme mobile care se suprapun: WLAN, WiMAX şi BWA.

WLAN (*Wireless Local Area Network*) leagă mai multe dispozitive folosind distribuţia fără fir a unei conexiuni la Internet. Majoirtatea WLAN sunt bazate pe Wi-Fi, iar de obicei, raza de acţiune nu este foarte mare.

WiMAX (*Worldwide Interoperability for Microwave Acces*) este o tehnologie fără fir pentru conexiuni de mare viteză la Internet pentru locaţii geografice extinse. Este parte din noua tehnologie de conectare la Internet, „generaţia 4G”.

Terminalele mobile pot fi telefoane inteligente, tablete, laptopuri, dar se pot extinde şi către încapsulare în alte sisteme precum automobilele, avioanele sau chiar nave sau bărci.

3. Principii de funcţionare

de Vasile Ioana Iuliana

Important este ca un terminal mobil să poate fi adresabil la aceaşi adresă de reşedinţă, indiferent dacă este conectat la punctul de legătură original (*home link*), sau la altul. Această adresă de reşedinţă (sau *home address*) este o adresă IP asignată nodului mobil care aparţine prefixului subreţelei punctului de legătura de reşedintă (*home link*). Când acesta este în raza de acţiune a legăturii de reşedinţă, pachetele sunt rutate către această adresă, în mod obişnuit. Adresa de reşedinţă este folosită din două motive: în primul rând, pentru a-i permite unui nod mobil să fie găsit având o stare stabilă în DNS (în felul acesta adresa IP nu se schimbă cu mişcarea nodului mobil), iar în al doilea rând pentru a ascunde nivelul de mobilitate IP nivelurilor superioare.

Când acesta este în raza unei legături externe sau străine (departe de legătura de reşedinţă), nodul mobil poate fi adresat la una sau mai multe adrese „de interes" (*care-of address – CoA*). O adresă de interes este o adresă IP asociată cu un nod mobil care aparţine prefixului subreţelei a unei legături externe specifice. Adresa IP poate fi obţinută prin modalităţi uzulate IPv6: autoconfigurare fără stare (*stateless*) sau cu stare (*stateful*). Cât timp terminalul stă în acoperirea aceluiaşi punct de legătură externă, el va primi pachete adresate acelei adrese de interes, dar poate să accepte pachetele de la mai multe adrese de interes, ca atunci când se terminalul se micşcă, dar poate fi încă accesibil la legătura precedentă.

Asocierea dintre adresa de bază a nodului mobil şi adresa de interes se numeste în termeni anglo-saxoni „*binding*" care se poate traduce ca asociere. Aceasta are o durată de viaţă fixată, necesară tocmai din pricina mobilităţii nodului terminal şi posibilităţilor de schimbare a agentului străin (de exemplu nodul pleacă din reţeaua străină pentru un timp, iar când se întoarce agentul nu mai are aceiaşi parametrii, posibil din cauza unei defectări).

Orice nod care comunică cu terminalul mobil se numeste nod de corespondenţă (*correspondent node*), şi acesta la rândului poate să fie un nod mobil sau poate să fie un nod staţionar.

Există două posibilităţi pentru comunicaţia dintre nodul mobil şi nodul corespondent. Cele două se alge în funcţie de tipul de comunicaţie care se stabilieste între nodul mobil şi nodul de corepsondenţă (de lungă durată sau de scurtă durată)..

Prima metodă se numeşte **tunelare bidirecţională** şi nu necesită suportul Mobile IPv6 de la nodul corespondent şi este disponibil chiar dacă nodul mobil nu şi-a înregistrat asocierea (*binding*) cu nodul de corespondenţă. Pachetele de la nodul corespondent sunt rutate către reprezentantul de reşedinţă (*home agent*) şi apoi tunelate către nodul mobil. Pachetele care sunt transmise nodului de corespondenţă sunt tunelate de la nodul mobil către reprezentantul de reşedinţă prin aşa—numita tunelare inversă, iar apoi sunt rutate normal de la reprezentantul de reşedintă către nodul corespondent. Astfel, reprezentantul de reşedinţă foloseşte descoperirea de vecini (*Neighbor Discovery*) pentru a intercepta orice pachete destinate adresei de reşedinţă. Fiecare pachet este tunetal cu adresa de interes primară pentru a fi primite de terminalul mobil. Tunelarea este făcută folosind încapsularea IPv6. Principiul de funcţionare este prezentat în figura 1. [1]

Pentru a se realiza încapsularea este necesără existenţa a trei mecanisme spearate:

- descoperirea adresei de interes
- înregistrarea adresei de interes
- tunelarea adresei de interes

Procesul de descoperire a adresei este bazat pe protocolul deja existent de anunţare a ruterului (*Router Advertisement*). Astfel, acesta nu modifică câmpurile deja existente în acest protocol, ci doar le extinde pentru a le asocia cu funcţionalităţile de mobilitate. Deci, o anunţare a ruterului transportă şi informaţii despre adresele de interes. Când această anunţare se exitende prin incluziunea şi adresei de interes necesară, se numeşte anunţare de agent. Totuşi, dacă un nod mobil doreşte să afle

adresa de interes, dar nu vrea să aştepte aunţarea periodică, atunci acesta va difuza un mesaj de solicitare, răspunzând toti agenţii străini sau de reşedinţă care-l primesc.

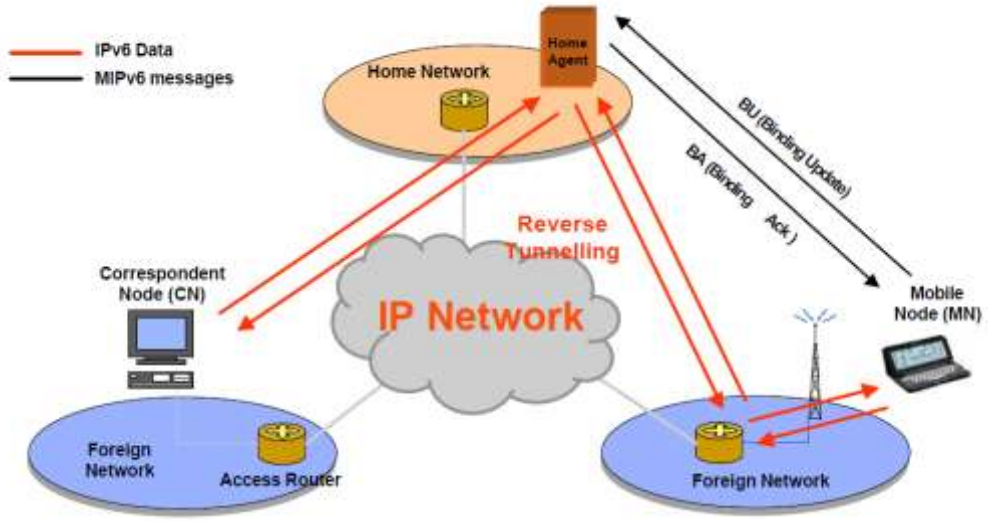
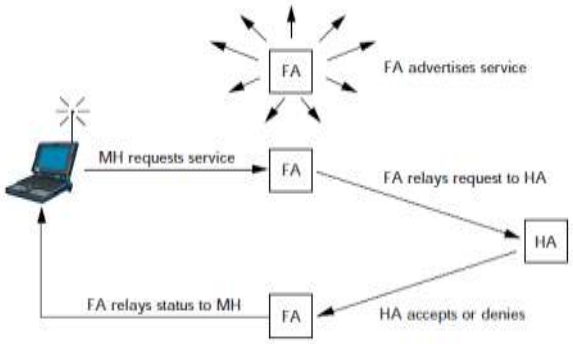


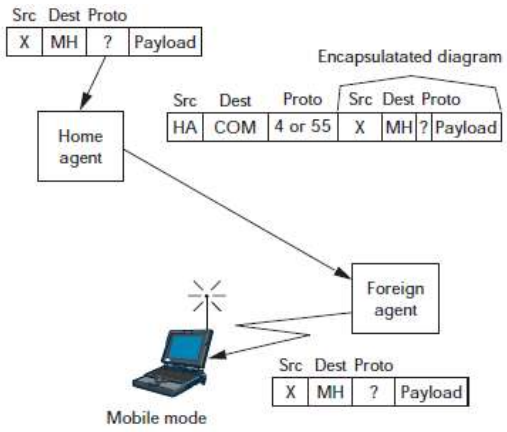
Figura 1 Procesul de tunelare bidirecţională

Agenţii de reşedinţă folosesc protocolul de anunţare de agent pentru a se face cunoscuţi, chiar dacă nu oferă nicio adresă de interes. Aşadar, anunţarea de agent permite detecţia agenţilor mobili, listarea a uneia sau mai multor adrese de interes, informarea nodului mobil de anumite funcţii speciale prevăzute de agenţii străini, lasă nodul mobil să determine reţeaua şi statusul legăturii la Internet, astfel putând şti dacă este vorba de un agent sătrin, de reşedinţă, sau chiar amandoi, rezultând în cunoaşterea reţelei în care se alfă.



Figură 2 Procesul de Înregistrare

În cele figura 2 [2] se evidenţiază inconvenientul acestei metode de tunelare a adresei de interes, pentru că agentul de reşedinţă (*HA*) trebuie să trateze fiecare înregistrare a unui noi agent străin (*FA*).



Figură 3 Încapsularea adresei de interes

Din figura 3 [3] se observă că încapsularea foloseşte principiul IP – în interiorul – IP. Astfel, agentul de reşedinţă, sursa tunetului, insereaza un nou antet IP înaintea antetului IP al oricărui pachet care este destinat adresei de reşedinţă. Noul antet va folosi ca adresa de destinaţie, sau destinaţia tunelului, adresa de interes. Pentru a se recupera pachetul original, agentul străin trebuie să elimine antetul de tunel şi să livrezul restul pachetului nodului mobil.

A doua metodă se numeşte **optimizarea rutării**. Prin ea se dorește ca dirijarea pachetelor dintre nodul mobil şi nodul corespondent să se facă prin cea mai scurta cale posibilă (cum se întâmplă de obicei în dirijarea normală a tragicului). În funcție de natura comunicației (de lungă durată sau de scurtă durată), nodul mobil poate să decidă daca ar trebui să încerce optimizarea rutării dintre el şi nodul corespondent. Astfel, cînd un nod mobil primește un pachet tunelat de la agentul de reședință, trebuie să decidă dacă optimizarea este necesară. În figura 4 [[4]] se poate observa cum nodul mobil poate comunica direct cu nodul corespondent, fără ca pachetele să mai treacă prin agenul de reședință, cum se întampla la tunelare (ilutrată în figura 1).

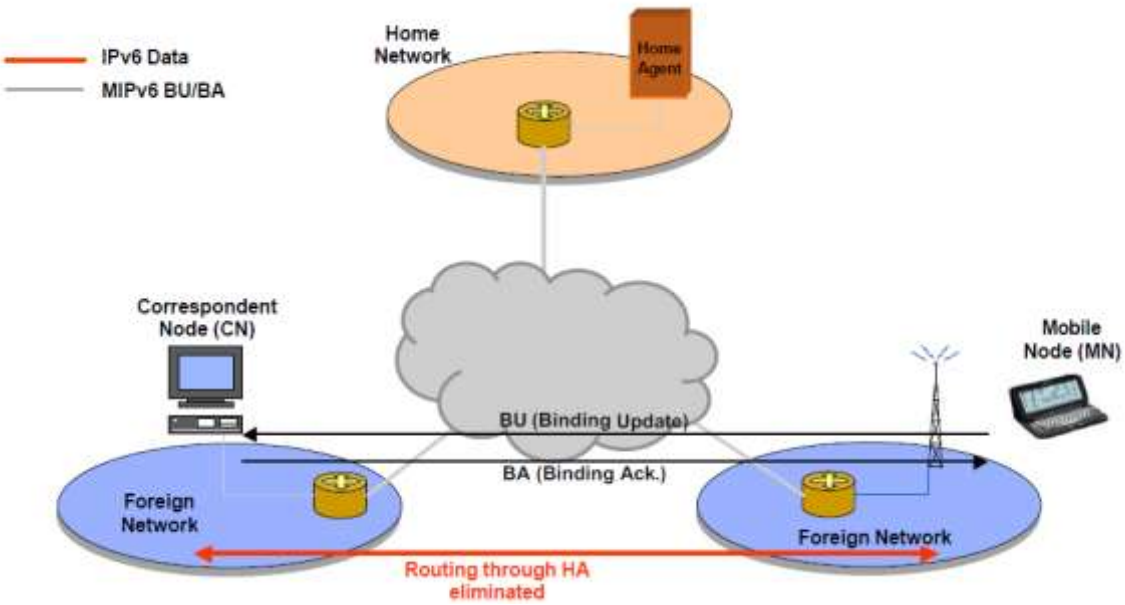
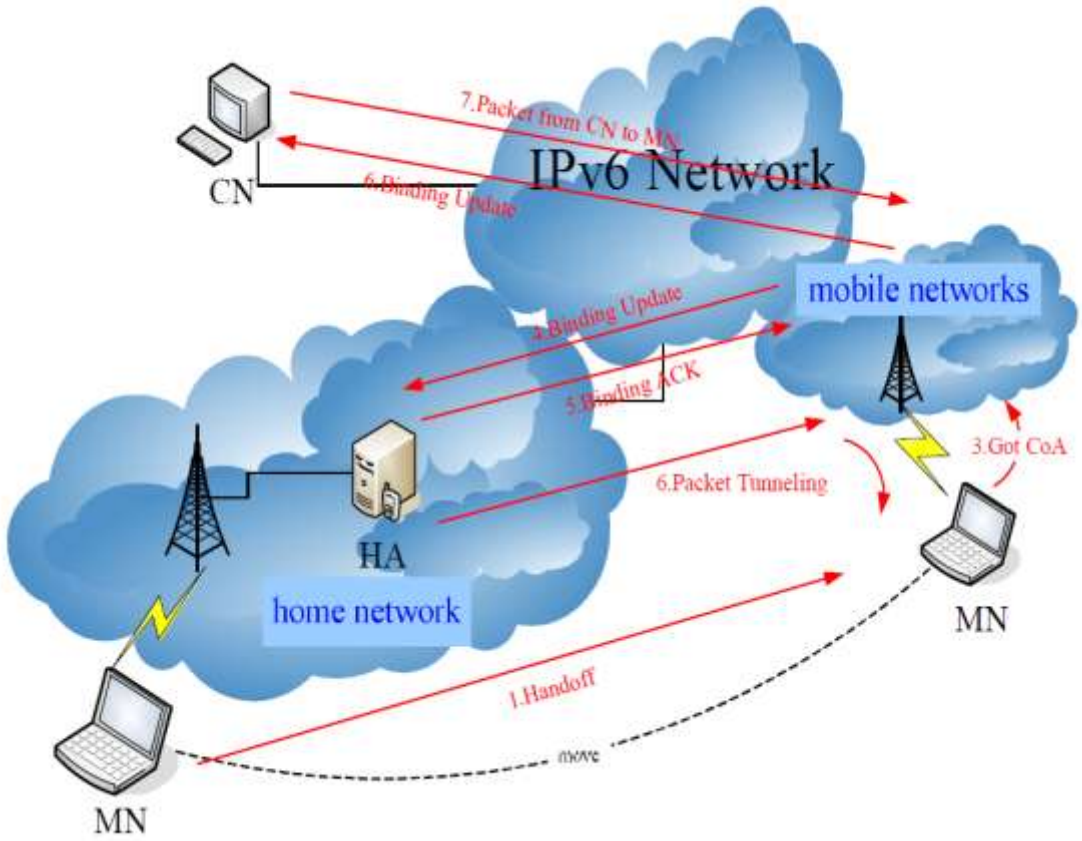


Figure 4 Rutare optimizată

Pentru opimizarea rutării este necesar ca nodul mobil să îşi înregistreze asocierea (*binding*) curentă cu nodul de corespondenţă. Scopurile acestor asocieri sunt: să ofere posibiltatea pachetelor să fie transmise direct între nodul mobil și nodul corespondent, fară a mai trece prin agentul de reşeidinţă, și să menţină conexiunea continuă în același timp permițând aplicațiilor să folosească în continuare adresa de reşedinţă ca sursă de adresa (în nodul mobil) și ca adresă de destinație (în nodul corespondent). Pachete de la nodul corespondent pot fi rutate direct la adresa de interes a terminalului mobil. Când se trimite un pachet către orice destinaţie în IPv6, nodul de corespondenţă verifică toate asocierile pentru adresa destinaţie din pachet. Dacă se găseşte o asociere, nodul foloseşte noul antet (*header*) de rutare IPv6 pentru a dirija pachetele către nodul mobil, care se numște dirijare inversă, iar antetul se numește *antetul de dirijare inversă* (*Reverse routing header – RRH*).

Această metodă este eficientă pentru că, spre deosebire de prima, elimină congestia la reprezentatul de reşedinţă şi a legăturii reşedinţă a nodului mobil cu aproximativ 50% (depinde de modelul traficului [5]– vezi chuck sellers), previne şi întreruperile cauzate de defecţiuni ce pot apărea la nivelul reprezentantului de reşedinţă, în acelaşi timp oferind drumul cel mai scurt către nodul mobil, reducând astfel latența, și, de asemenea, cu ajutorul dirijării inverse se folosește mai bine lărgimea de bandă.

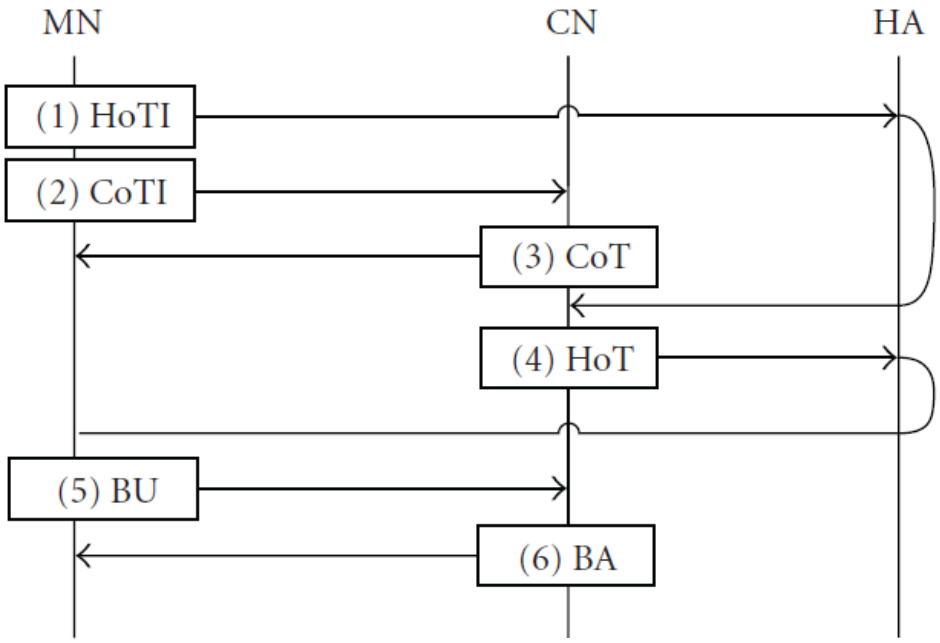


Figură 5 Mesajele schimbate în optimizarea rutării [6]

Când se dirijeaza pachete direct către nodul mobil, nodul corespondent setează adresa de destinaţie în antentul IPv6 ca adresă de interes a nodului mobil. Un nou tip de antet de rutare IPv6 este de asemenea adăugat pacheteului pentru a transporta adresa de bază dorită. În mod similar, nodul mobil setează ca adresă de destinaţie în antetul pachetului adresa de interes curent. Nodul mobil adaugă o nou opţiune IPv6 „adresă de reşedinţă" pentru a îşi transporta propria adresă de reşedinţă. Această incluziune a adresei în pachete face ca utilizarea unei adrese de interes să fie transparentă peste nivelul reţea.

Mobilitatea IPv6 asigură suport pentru mai mulţi agenţi de reşedinţă, şi un suport limitat pentru reconfigurarea reţelei de origine. În consecinţă, nodul mobil poate să nu stie adresa IP a agentului său de reşedinţă, iar prefixul adresei subreţelei poate chiar să se schimbe în timp. Un mecanism denumit "*descoperirea dinamică a adresei agentului de reşedinţă*" asigură ca un nod mobil să îşi descoperere dinamic adresa agentului de reşedinţă pe legătura sa de reşedinţă, chiar dacă nodul mobil este departe de ea. Terminalele mobile pot de asemenea să înveţe noi informaţii despre prefixul adresei de subreţea de reşedinţă prin mecanismul de "descoperire a prefixului mobil". De asemenea, descoperirea dinamică a adresei agentului de reşedinţă oferpa posibilitatea agenților de reședință să împartă încărcătura între ei, în cazul în care mai mulți agenți de reședință sunt localizați pe același link. Acest parametru este inclus în *opțiunea cu informații despre agentul de reşedinţă* din anunțarea rutelor trimisă de agenții de reședință.

Procedurile de dirijare inversă sunt folosite pentru a îi permite nodului de corespondeţă să obţină garantări rezonabile că nodul mobil este adresabil la adresa de interes şi la adresa de reşedinţă, oferind un fel de securitate. Doar cu aceste asigurări nodul de corespondenţă poate accepta actualizări de asociere (*Binding Updates*) de la nodul mobil. Apoi, se poate trece la actualizarea asocierii care presupune un schimb de mesaje de la nodul corespondent la nodul mobil. Modul de lucrul al acestei proceduri este ilustrat în figura 6 [7] și în figura 7 [[8]].



Figură 6 Schimbul de mesaje pentru asociere în rutarea optimizată

Nodul mobil trimite un mesaj de inițiere a testului de reședință (*Home Test Init - HoTI*) și un mesaj de inițializare a testului de interes (*Care-of Test Init - CoTI*) pentru a inițializa procesul de acualizarea asocierii. Aceste mesaje sunt trimise aproape simultan, dar pe două căi diferite; CoTI este trimis direct către nodul corespondent, pe când HoTI este trimis indirect via agentul de reședință.

Nodul corespondent trimite mesajele de test de reședință (*Home Test – HoT*) și testul de interes (*Care-of Test – CoT*) ca un răspuns la mesajele precedente. Acestea folosesc aceleași căi ca și mesajele de inițiere: CoT este trimis direct de la nodul corespondent către nodul mobil, pe când HoT este trimis către nodul mobil prin agentul de reședință. Nodul corespondent generează odată cu aceste mesaje niște jetoane care concatenate devin o cheie secretă pentru autentificare în mesajul de actualizarea asocierii. Securitatea dirijării inverse ține de folosirea corectă a acestor jetoane.

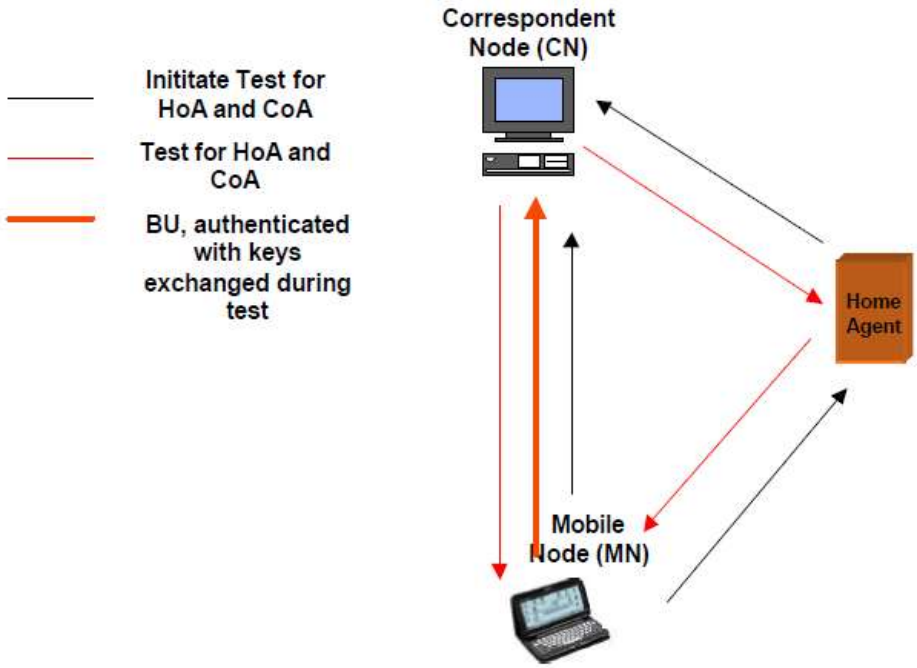


Figure 7 Dirijare inversă

Mesajul de actualizare (*BU*) a aocierii este trimist de la adresa de interes a nodului mobil către nodul corespondent. În acest mesaj sunt inlcuse: adresele de interes, de reședință și nodul corespondent, dar și o secvență, un timp de valitidate și cheia generată anterior. După ce se verifică autenticitatea, nodul corepsondent trimite nodului mobil un mesaje de confirmare a asocierii(*BA*).

Nodul mobil trebuie să stocheze o listă cu actualizările de asociere, în care sunt păstrate toate asocierile active (care nu au expriat) trimise atât către nodul de reşedinţă cât şi către nodurile corepsondente, dar şi cele care sunt în curs de completare. Această listă este folosită pentru a determina cum trebuie trimis un pachet.

Agentul de reşedinţă trebuie să păstreze o listă cu agenţii de reşedinţă şi memorie a asocierilor (*Bining Cache*). Lista cu agenţii de reşedinţă conţine informaţii despre fiecare ruter de pe aceaşi legătura care se comportă ca un agent de reşedinţă, aceasta este folosita de mecanismul dinamic de descoperire a adresei de reşedinţă.

Din punctul de vedere al securității, responsabilitatea nodului mobil este în două straturi. În primul rand, când nodul mobil actualizeaza adresa de interes temporară către nodul corepsondent, nodul mobil trebuie să confirme nodului corespodent că adresa sa de interes este o versiune temporară a adresei de reședință și ca ambele adrese sunt deținute de nodul mobil. Adresa de reședintă staționară servește ca identificator al nodului mobil. În al doilea rând, din presectiva nodului corespondent, mai bine decât să fie informat de nodul mobil că adresa acestuia s-a schimbat la noua adresp de itneres, se consideră mai sigur ca nodul corespondent sp participe acitv în procedura de actualizarea a asocierii prin confirmarea existenței și dirijabilității adresei de interes a nodului mobil. Aceasta este importantă pentru că un nod mobil „necinsit" ar putea anunța o adresă de interes falsă.

Chiar dacă s-au înlăturat anumite probleme de securitate, totuşi mai există unele:

- cea mai mare vulnerabilitate o prezintă autorizaţia din cadrul acutalizării asocierii;
- mobilitatea nu este compatibilă cu utilizarea unui firewall;
- probleme legate de securizarea descoperii de vecini;
- apar incompatibilităţi când se face roaming între arhitecturi diferite de Mobile IPv4 şi Mobile IPv6.

4. Schimbări IPv6 pentru integrarea Mobile IPv6

de Vasile Ioana Iuliana

Pentru a se integra noile idei despre mobilitate, s-au făcut schimbări şi în cadrul noului protocol IPv6 care se doreşte a înlocui complet versiunea actuală, IPv4. Acestea sunt: un nou set de opţiuni de mobilitate incluse în mesajele de mobilitate, o nouă opţiune de „adresă de reşedinţă" pentru antetul cu opţiunile pentru destinaţie (*Destination Option*), un nou antet pentru rutare de tip 2, un noi mesaje de tip ICMPv6 pentru descoperirea agenţilor de reşedinţă şi pentru a obţine prefixul subreţelei a legăturii de reşedinţă, opţiuni pentru descoperirea vecinilor.

Noul antet pentru mobilitate şi opţiunile sale

Antetul pentru mobilitate este o extensie a antetului utilizat de nodurile mobile, nodurile corepsondente şi agenţii de reşedinţă în toate mesajele legate de crearea şi administarea asocierilor (*bingings*). Astfel, el este folosit pentru a trnasporta următoarele informaţii:

- *home test init, home test, care-of test init, care-of test* sunt folosite pentru procedura de rutare inversă;

- Actualizarea asocierii (*Binding update*) este folosită pentru ca un nod mobil să informeze nodul de corespondenţă sau agentul de reşedinţă acestuia de asocierile curente;

- Înregistrarea reşedinţei (*Home registration*) reprezintă o acutalizare a legăturii trimisă de agentul de reşedinţă nodului mobil pentru a înregistra adresa de interes primară;

- Confirmarea asocierii (*Binding Acknowledgment*) este folosită pentru confirmarea recepţiei unei actualizări de asociere, dacă aceasta a fost cerută sau dacă a apărut o eroare;

- Cererea de reacualizare a asocierii (*Binding Refresh Request*) este folosită de un nod de corespondenţă pentru a cere ca un nod mobil să refacă asocierea cu acesta;

- Eroarea de asociere (*Binding error*) este folosită de nodul corepondent pentru a semnala o eroare legată de mobilitate.

Antetul de mobilitate este identificat de valoarea 135 din câmpul Antet Următor (*Next Header*) din structura unui pachet IPv6.

Are următorul format:

Payload Protocol	Header length	MH Type	Reserved
Checksum		Message data	

Protocolul de sarcină utilă (*Payload Protocol*) este un selector pe 8 biţi, identificând tipul antetului ce urmează imediat după antetul de mobilitate.

Lungimea antetului (*Header Length*) este un câmp pe 8 biţi care ia valori întregi pozitive (*unsigned integer*) şi reprezintă lungimea antetului de mobilitate în unităţi de 8 octeţi, excluzând primii 8 octeţi.

Tipul nodului mobil (*MH Type*) este un selector pe 8 biţi, identificând mesajele de mobilitate specificate de antet.

Reserved este un câmp de 8 biţi rezervaţi pentru utilizări ulterioare, el trebuie iniţializat cu zero de către expeditor şi ignorat de destinatar.

Suma de verificare (*Checksum*) este un câmp de 16 biţi de tip întreg pozitiv care conţine suma de verificare a antetului de mobilitate.

Mesajul de date (*Message data*) este un câmp variabil care conţine datele specifice acestui antet.

Opţiunile de mobilitate sunt codate în spaţiul care mai rămâne din câmpul mesaj de date din antet după cum urmează:

Option Type	Option Length	Option Data

Tipul opţiunii *(option type)* este un identificator pe 8 biţi a tipului opţiunii de mobilitate;

Lungimea opţiunii (*option length*) este un întreg pozitiv pe 8 biţi care reprezintă lungimea în octeţi a opţiunii, fără să includă câmpurile de tip şi de lungime a opţiunii;

Datele opţiunii (*option data*) este un câmp cu dimensiune variabilă care conţine datele specifice opţiunilor.

Printre opţiunile de mobilitate noi, au apărut:

- *Pad1* este folosit pentru a insera un octet de umplutură *(padding)* în locul de opţiune de mobilitate ai antetului de mobilitate;
- Îndrumarea actualizării asocierii (*Binding Refresh Advice*) este validă doar în confirmarea asocierii şi doar pe cele trimise de la agentul de reşedinţă a nodului mobil ca un răspuns la înregistrea reşedinţei;
- Adresa de interes alternativă (*Alternate Care-of Address*) este prevăzută pentru cazurile în care adresa de interes solicitată în aculaizarea asocierii nu este validă;
- Datele de autorizaţie a asocierii (*Binding Authorization Data*) este validă în actualizarea asocierii şi în confirmarea asocierii conţinând autentificator pentru securitate.

Noile mesaje ICMPv6

MIPv6 introduce de asemenea patru tipuri noi de mesaje ICMP, două dintre acestea fiind folosite în mecanismul de descoperire dinamică a adresei agentului de reşedinţă, iar celelalte două fiind folosite pentru mecanismenele de renumerotare şi configurare mobila.

Cele două mesaje pentru mecanismul de descoperire dinamica a adresei agentului de reşedinţă: *Home agent address discovery request* (cererea de descoperire a adresei agentului de reşedinţă) şi *Home agent address discovery reply* (răspunsul primit de la cererea de descoperire a adresei agentului de reşedinţă)

Cele două mesaje folosite pentru renumerotarea rețelei şi pentru configurarea adresei pe nodul mobil: *Mobile prefix Solicitation* (solictarea prefixului mobil) şi *Mobile prefix Advertisment* (anuntarea prefixului mobil).

Opţiunea pentru Adresa de Reşedinţă

Aceasta este transportată de extensia de antet a opţiunii de destinaţie (valoarea 60 în câmpul antet următor). Este folosit în pachetele trimise de nodul mobil când e departe de reşedinţă, pentru a informa destinatarul de adresei de reşedinţă a nodului mobil.

Opţiunea de Adresă de Reşedinţă are următoarul format:

	Option Type	Option Length
Home Address		

Tipul opţiunii este setat cu valoarea 201 (0xC9);

Lungimea opţiunii este un întreg pozitiv de 8 biţi are reprezintă lungimea în octeţi a opţiunii, fără să includă câmpurile de tip şi de lungime a opţiunii. Acest câmp trebuie setat cu valoarea 16;

Adresa de reşedinţă a nodului mobil care trimite pachetul.

Această opţiune trebuie plasată astfel: după antetul de rutare (dacă este prezent), înainte de antetul de fragmentare (dacă este prezent), înainte de antetul AH sau antetul ESP (dacă acestea sunt prezente). De asemenea, acestă opţiune nu trebuie să apară decât o singură dată.

Antetul pentru rutare de tip 2

Acest antet este folosit pentru a se permite dirijarea directă de la un nod corespondet către adresa de interes a nodului mobil. Adresa de inters a nodului mobile trbuie inserată în câmpul de Adresă de Destinţie Ipv6. Când pachetul ajunge la adresa de interes, nodul mobil îşi recuperează adresa de reşedinţă din antetul de rutare şi apoi aceasta este folosită pentru adresa de destinaţie finala pentru pachet. Noul antet de rutare permite firewall-urilor să aplice alte reguli la sursa pachetelor rutate. Acesta este restricţionat să transmită numai adrese IPv6.

Formatul antetului:

Next Header	Hdr Ext Len=2	Routing Type=2	Segments left=1
Reserved			
Adresa de reşedinţă			

Antetul următor (*Next Header*) este un selector pe 8 biţi care identifică tipul antetului imediat următor.

Lungimea antetului (*Hdr Ext Len*) reprezintă lungimea antetului de rutare in unităţi de 8 octeţi, fără a include primii 8 octeţi, ea este setată la valoarea 2.

Tipul rutării (*Routing Type*) are valoarea 2.

Numărul de segemente rămase (*segments left*) este setat la 1 şi descrie numărul de segmente de rutare rămase de vizitat până la destinaţia finală.

Câmpul rezervat (*reserved*) are 32 de biţi şi trebuie să fie iniţializat cu zero de expeditor şi ignorat de destinatar.

Adresa de reşedinţă (*Home Address*) reprezintă adresa destinatarului mobil.

5. Comparaţie intre Mobile IPv4 si Mobile IPv6

de Bălănescu Diana

Protocolul de mobilitate MIPv4

Mobile Ipv4 este un protocol de mobilitate folosit în mod curent în reţele Ipv4. Odată cu evoluţia noii generaţii Internet Ipv6 a fost dezvoltat şi protocolul mobil Ipv6 în scopul de a se ocupa de mobilitate şi de a rezolva problemele predecesorului său. Cu toate că MIPv6 are în comun multe din caracteristicile protocolului MIPv4, există şi diferenţe.

Caracteristica cheie a conceptului Mobile IP este accesa că toate funcţionalităţile necesare procesării şi administrării mobilitaţii sunt încorporate în entităţi foarte bine definite: Agentul de Reşedinţă (HA), Agentul Străin (FA) şi Nodul Mobil (MN). MIPv4 este o protocol complet transparent la nivelul Transport şi la nivelurile OSI superioare. Acesta nu necesită schimbări la nivelul de Internet host si router, permiţând nodurilor mobile să le reţină adresele IP indiferent de punctul de ataşament la reţea. Acest lucru este posibil prin alocarea a două adrese IP, una pentru identificare (adresa de reşedinţă), iar cealalta pentru rutare (adresa de interes). Adresa de reşedinţă este statică şi este folosită în principal pentru identificarea conexiunilor de nivel înalt (ex. TCP). Adresa de interes (Care-of Address) este cea asignată nodului mobil în timpul procesului de roaming (mutare dintr-o reţea în alta). Atunci când un nod mobil se mută în alta reţea adresa de interes are rolul de a identifica noul punct de ataşament respectând topologia reţelei. In cadrul Mobile IPv4 managementul adresei de interes este realizat de entitatea numită Agent străin (Foreign Agent).

Modul de functionare al MIPv4 este următorul: Agenţii de mobiltate (routere) trimit mesaje pentru a anunţa nodul mobil de reţeaua la care este conectat. Cand un nod mobil este conectat la o retea străină, acesta va obţine o adresă de interes pe care o va inregistra la routerul său de reşedinţă. Agentul din reţeaua de reşedinţă prin mecanismul de tunelare permite livrarea de datagrame IP către nodul mobil, atunci când acesta nu se găseşte în reţeaua locală. Tunelarea adresei de interes este realizată folosind mecanisme de încapsulare. Fiecare agent de Mobilitate ce foloseşte MIPv4 este capabil de a folosi un mecanism de încapsulare default inclus in adresa IP [RFC2003]. Acest presupune ca sursa tunelului să insereze un antet IP tunnel în faţa antetului din cadrul pachetului IP original. Agentul din reţeaua străină AS (Agent Străin) oferă servicii de rutare atâta timp cât nodul mobil este înregistrat la el. Se execută operaţiile de detunelare şi livrare a datagramelor IP iniţial încapsulate de către Agentul de reşedinţă al nodului respectiv.

Protocolul MIPv4 poate asigura suport pentru mobilitatea dispozitivelor portabile însă exstă e serie de probleme pe care acest protocol nu le poate depăşi. Exemple de astfel de probleme sunt următoarele:

- Rutarea în triunghi
- Rutare directă ineficientă
- Mecanism ineficient de notificare al Agentului de Reşedinţă.
- Securitate scăzută.

- Procesul de reîncapsulare pentru tunelare adaugă un overhead (suprasarcină) destul de mare în reţea.

Mai există şi altele.

Optimizări aduse de protocolul Mobile IPv6

Pachetele trimise către un nod mobil atunci când acesta nu se află în reţeaua locală sunt tunelate in cazul MIPv6 folosind un antet Ipv6 în locul încapsulării IP. Protocolul Ipv4 mobil trebuie sa folosească încapsularea pentru toate pachetele. Acest lucru implică o încărcare inutilă a reţelei. Prin urmare din prisma suprasarcinii MIpv6 împovărează mult mai puţin reţeaua.

Mipv6 nu mai foloseşte routere speciale cu funcţii de agenţi străini. Nodurile mobile in acest caz se folosesc de caracteristici ale Ipv6 precum: descoperirea în mod automat a vecinilor şi auto-configurarea adresei.

Procedura de optimizare a rutării este construită ca parte fundamentală a MIPv6. Pentru MIPv4 acestă procedură este opţională si nu este suportată de către toate nodurile mobile. Optimizarea rutării permite rutarea directă dintre orice nod corespondent şi orice nod mobil, fără a mai trece prin reţeaua de reşedinţă a nodului, eliminând astfel fenomenul „rutării in trunghi" prezent la protocolul IPv4 mobil care este ineficient şi creşte prea mult traficul.

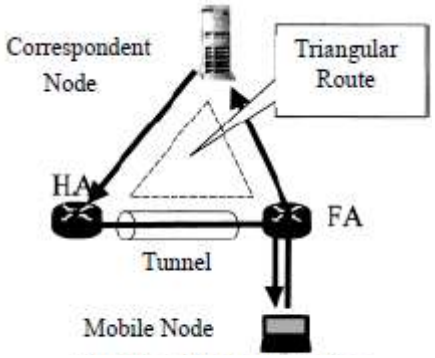


Figura 8 : Rutare în Triunghi

Figura 8 [9] înfăţişează procesul de rutare în triunghi. Notaţiile HA, FA reprezintă:

HA = Home Agent, Routerul din reţeaua reşedinţa

FA = Foreign Agent, Routerul din reţeaua vizitată;

Atâta timp cât un nod mobil nu se află in reţeua reşedinţă, agentul reşedinţă interceptează orice pachet pentru acel nod folosind însă procedeul de descoperire a vecinilor în loc de ARP (Address Resolution Protocol, Protocol de Rezolvare a Adreselor), protocol folosit de MIPv4.

Traficul de control al protocolului Ipv6 mobil este alăturat oricăror pachete Ipv6 existente, pe când la protocolul MIpv4 pentru fiecare mesaj de control sunt necesare pachete UDP separate.

Pentru toate cerinţele de securitate (autentificare, protecţia integrităţii datelor etc) MIPv6 foloseşte IPsec (IP Security). MIPv6 se bazează pe propiile mecanisme de securitate bazate pe configurarea statică a asocierilor de mobilitate securizată.

În concluzie îmbunătăţirile pe care protocolul Ipv6 mobil le aduce, fac din acest protocol un o tehnologie mult mai efiecientă de asigurare a mobilităţii utilizatorilor faţă de ce a înaintaşului său. Carcteristicile suplimentare implementate la MIPv6 sunt: optimizarea rutării, sporirea securităţii, împovărare redusă a reţelei prin folosirea antetului Ipv6 in procesul de rutare, lipsa necesităţii unui agent străin şi altele. Un lucru interesant este acela că anumite routere Ipv6 suportă mobilitatea unei reţele întregi.

6. Dezvoltări

de Bălănescu Diana

Având în vedere importanţa pe care suportul pentru mobilitate o are asupra viitoului Internetului, în ultimii ani, s-au dezvoltat o serie de propuneri pentru protocoale sau scheme. Printre ele, protocolul de nivel Reţea, IPv6 mobil, reprezintă soluţia cea mai renumită. Acesta defineşte un identificator constant (adresa de reşedinţă) pentru protocoalele de nivel Transport şi deasemenea utilizează o entitate centralizată pentru transferul de pachete şi determinarea locului de înmagazinare a informaţiei (agentul reşedinţă). Arhitectura mobilităţii centralizate are lipsuri importante: nu numai că îi lipseşte flexibilitatea în dezvoltare, dar limitează eficienţa transferului şi introduce instabilitate in sistemele de reţea prin supraîncărcarea agentului de reşedinţă. Aceste caracteristici referitoare la mobiltate centralizată vor introduce, din păcate, probleme de scalabilitate şi performanţă în momentul în care marea majoritate a nodurilor din Internet vor deveni mobile. Din acest motiv este necesară gasirea unei arhitecturi alternative pentru managementul mobilităţii Internet. Astfel s-au încercat şi se încercă dezvoltarea unor soluţii pentru planificarea în avans a evoluţiei pe termen lung a comunităţii Internet. În continuare vor fi prezentate trei dintre aceste dezvoltari.

a. Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6) reprezintă unule din protocoalele de mobiltate de nivel Reţea care poate evita supraîncărcarea prin tuneleare cât şi implicarea utilizatorilor în managementul mobilităţii. PMIPv6 se concentrează pe extinderea protocoluilui MIPv6 din două motive. Primul este acela că MIPv6 este un protocol de mobilitate foarte matur. În prezent există e serie impotantă de implementări şi evenimente de interoperatibilitate în cadrul cărora MIPv6 a fost extensiv testat. Arihitectura PMIPv6 consideră refolosirea acestor mecanisme mature pentru rezolvarea problemei reale de implementare. În al doilea rând, PMIPv6 permite reutilizarea agenţilor din reţeaua de reşedinţa folosiţi la MIPV6 pentru a asigura mobilitate nodurilor gazdă fără a necesita un protocol de mobilitate adiţional.

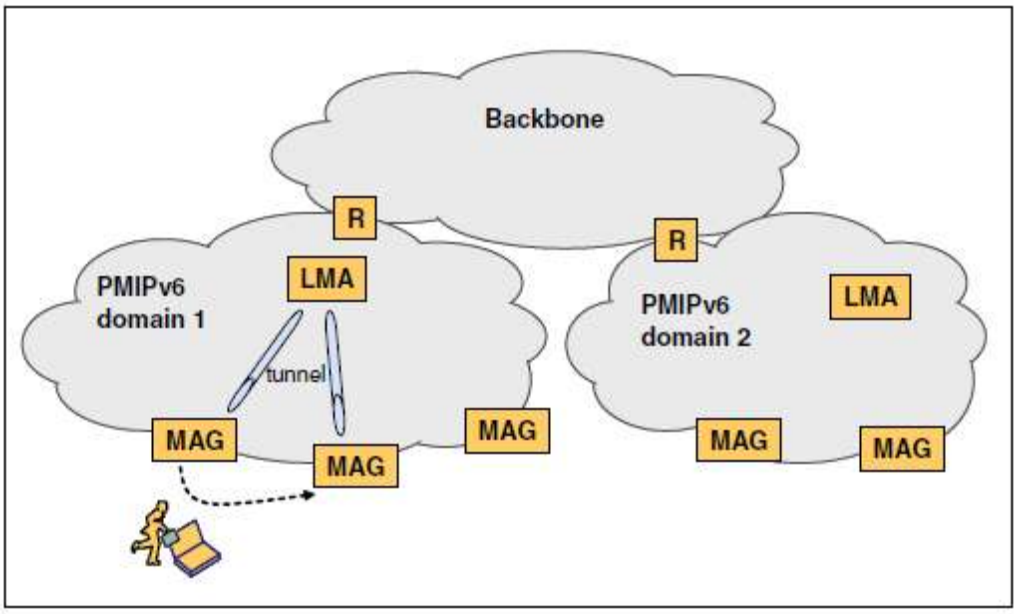


Figura 9: Arhitectura Proxy Mobile Ipv6

Figura 9 [10] oferă o scurtă privire de ansamblu a arhitecturii PMIPv6. În domeniul PMIPv6, o nouă entitate – Poarta de Acces Mobil (Mobile Access Gateway sau MAG) – este introdusă. Aceasta are în principal următoarele trei roluri:

(1) detectarea momentului în care nodul mobil se deplasează şi semnalizarea LMA-ului (Local Mobility Anchor – Ancora locala de mobilitate) pentru ca acesta să actualizeze ruta către adresa de reşedinţă a nodului.

(2) aranjarea căii de date care asigură că nodul mobil poate comunica prin intermediul adresei de reşedinţă cu punctul de acces la Internet.

(3) simularea legăturii cu reţeaua de reşedinţă a nodului mobil în punctul de access.

Ancora locală de mobilitate este entitatea care menţine asocierea dintre prefixul asignat nodului mobil si adresa proxy de interes. Aşadar LMA are capabilităţile funcţionale ale Agentului de Reşedinţă definit în specificaţiile de bază ale protocolului MIPv6 plus caracteristici adiţionale necesare pentru suportul protocolului PMIPv6. Din perspectiva LMA-ului, Poarta de Acces Mobil este acea entitate care transmite mesaje de semnalizare din partea nodului mobil. De fiecare dată când nodul se mută de la o poartă de acces la alta, LMA-ul trebuie sa actualizeze locaţia curentă a acestuia. Pentru procesul de actualizare a locaţiei, Poarta de Acces va trimite un mesaj de tipul PBU (Proxy Binding Update - Update pentru Asocierea Proxy) routerului ancora. La recepţionarea mesajului, routerul LMA va răspunde cu un mesaj de tipul PBA (Proxy Binding Acknowledgment – Confirmare a Asocierii Proxy). Dupa ce poarta de acces recepţionează la rândul său mesajul PBA, va întemeia un tunel către Poarta de Acces Mobil şi va adăuga o ruta implicită spre aceasta. Apoi, LMA va trimite orice pachet primit de la oricare nod corespunzător către nodul mobil prin intermediul MAG-ului curent. Aşadar, PMIPv6 poate fi deasemenea privit ca un protocol de mobilitate centralizată.

b. Mobile IPv6 Ierarhic (Hierarchical Mobile IPv6 (HMIPv6))

Protocolul IPv6 mobil manevrează mobilitate locala a unui nod gazdă (mobilitatea în reţeaua locală) în acelaşi mod în care manevrează mobilitatea globală (inter-reţea). Prin urmare, în cadrul domeniului MIPv6 nodul mobil va trimite actualizări de asociere routerului reşedinţă şi nodurilor corespondente de fiecare dată când îşi schimbă punctul de ataşament indiferent de localizarea sau amplitudinea mutării. În consecinţă, acelaşi nivel de încarcare a reţelelor este introdus în Internet independet de tiparul de mobilitate al utilizatorului. Această abordare nu este scalabilă deoarece gradul de încarcare a reţelei poate deveni copleşitor atunci când numarul de noduri gazdă creşte. Se consideră o schemă ierarhizată care diferenţiază mobilitatea locală de cea globală mai ca fiind apropiată de cerinţele Internet. O astfel de abordare are cel puţin două avantaje. Mai înâi, îmbunătăţeşte performanţele locale, deorece procesul de mutare de la un punct de acces la altul a nodului se excută local şi deci creşte viteza şi se minimizează probabilitatea de pierdere a pachetelor din timpul tranziţiilor. Apoi, se reduce semnificativ povara pe care mesajele de semnalare a mobilităţii o introduceau în Internet, deoarece aceste mesaje se transmit doar în interiorul reţelei. Mai mult, ierarhia este motivată de tiparul de mobiltate a utilizatorilor care de regulă nu tranzitează zone geografice semnificative. Conform unui studiu, 69% din utilizatori mobili nu depăşesc limitele reţelei locale, ci rămân în aceeaşi zonă (clădire, campus). Aşadar este importantă conceperea unei arhitecturi care optimizează mobilitatea locală.

HMIPv6 diferenţiază mobilitatea intra-reţea de mobilitatea inter-reţea. Un calculator-gazdă care comunică cu un dispozitiv gazdă mobil este conştient de mobilitatea acestuia doar în momentul în care acesta se mută din reţeaua locală (mobilitate inter-reţea), mobilitatea intra-reţea fiind un proces complet ascuns. O reţea reprezintă nivelul superior în arhitectura ierarhică. Aceasta poate fi o reţea a unui ISP (Internet Sevice Provider – Furnizor de servicii Internet), reţeaua din cadrul unui campus, reţeaua unei companii, un set de Lan-uri sau un chiar un singur LAN (Local Area Network – Reţea din Aria Locală). O astfel de reţea se conectează la Internet prin intermediul a unuia sau mai multor routere de interconectare numite Routere de Graniţă (Border Routers (BR)).

Principalele operaţii ale protocolului propus sunt următoarele:
- Mobilitatea Inter-reţea
- Mobilitatea Intra-reţea

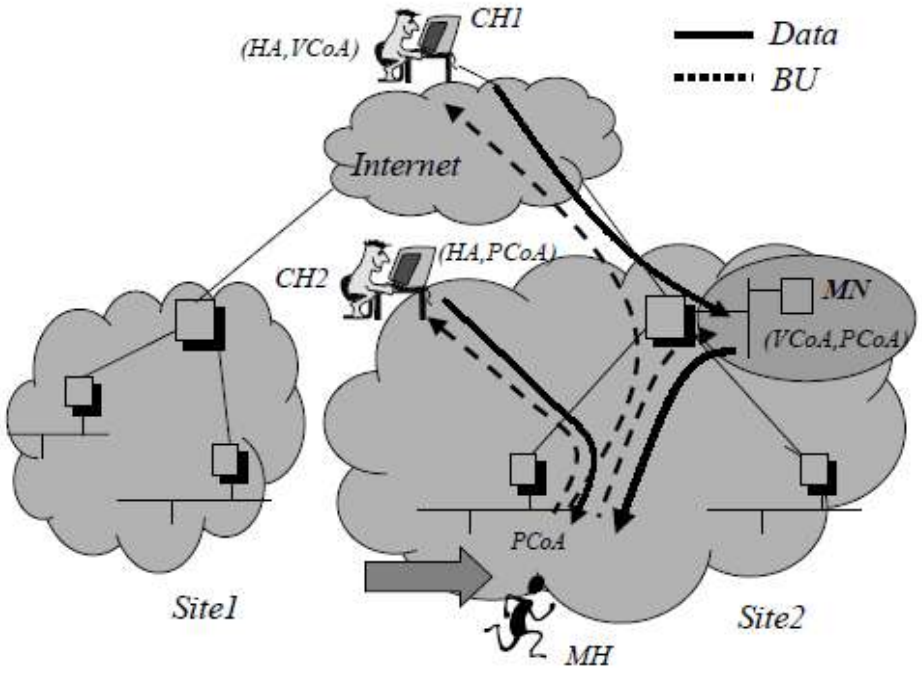


Figura 10: Mobilitate Inter-Reţea [11]

Mobilitatea Inter-reţea: În momentul în care o gazdă mobilă accesează o reţea nouă va primi două adrese De interes: una privată, fizică (PCoA) ce reprezintă adresa puctului de legătură la care s-a conectat, iar cealalta, o adresă virtuală (VCoA), ce reprezintă o adresă din reţeaua mobilă accesată. (A se remarca faptul că în cadrul protocolului MIPv6 este nevoie doar de adresa PCoA).

Nodul mobil va trimite apoi urmatoarele mesaje de actualizare a asocierii (BU – Binding Updates):

- Un mesaj de actualizare a asocierii în cadrul căruia se specifică asocierea între adresa de interes virtuală şi cea fizică, către MA (Agentul de Mobilitate). La recepţie, Agentul de Mobilitate efectuează controlul de admisiune cum ar fi autentificarea. Dacă se acceptă cererea, un mesaj de confirmare este transmis nodului mobil (MN).
- Un mesaj de actualizare a asocierii în cadrul căruia se specifică asocierea între adresa de reşedinţă şi adresa de interes virtuală, către nodul mobil şi către fiecare nod gazdă extern corespondent (CH) (în afara reţelei).
- Un mesaj de actualizare a asocierii în cadrul căruia se specifică asocierea între adresa de reşedinţă şi adresa de interes fizică către fiecare nod gazdă corespondent (în interiorul reţelei (site))

Ca rezultat:

- Un dispozitiv gazdă extern trimite pachete catre nodul mobil folosind adresa VCoA. Pachetele sunt apoi rutate către Reţeaua de Mobilitate a reţelei vizitate, interceptate de agentul de mobilitate şi tunelate către adresa fizică curentă a nodului mobil.

- Un dispozitiv gazdă local care trimite pachete către nodul mobil va folosi *PCoA*. Pachetele sunt apoi, expediate direct nodului mobil.

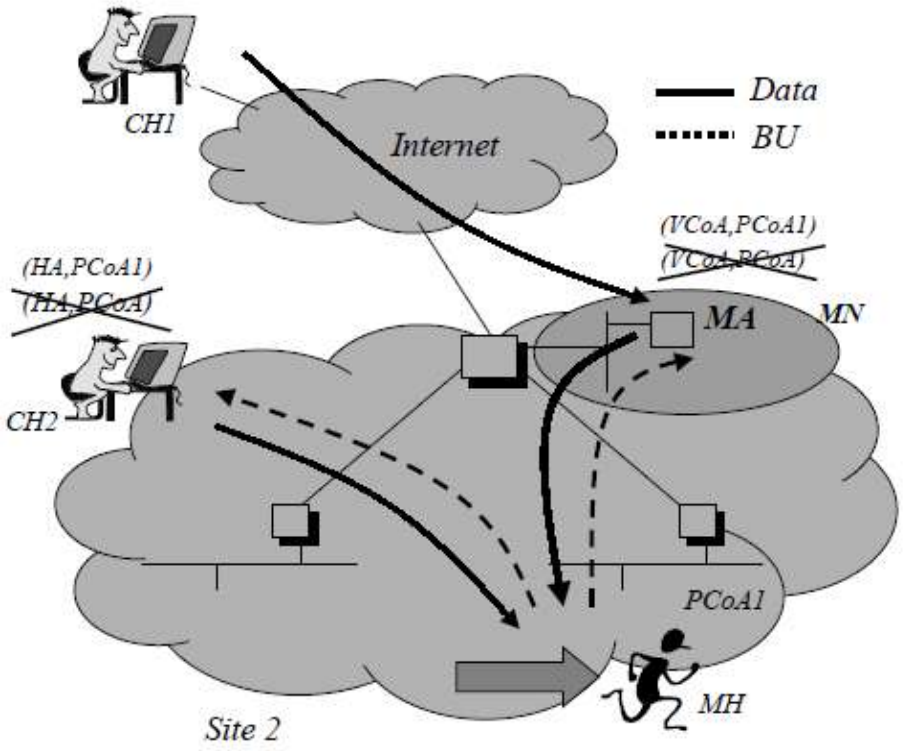


Figura 11: Mobilitate Intra-Reţea[12]

***Mobilitatea Intra-reţea*:** Atunci când un nod mobil (MN) se mişcă în cadrul reţelei, acesta va primi o adresa PCoA în punctul de ataşsament. Adresa virtuala VCoA rămâne constantă cât timp nodul mobil tranzitează local.

Dupa primirea adresei nodul mobil trimite următoarele mesaje de actualizare a asocierii (BU)

- Un mesaj de actualizare a asocierii în cadrul căruia se specifică asocierea între adresa de reşedinţă şi noua adresa PC0A către fiecare nod corespondent local (CH).
- Un mesaj de actualizare a asocierii în cadrul căruia se specifică asocierea între adresa VCoA şi noua adresă PCoA către Agentul de Mobilitate al reţelei.

Se observă că în timpul mobilităţii intra-reţea nici un mesaj de actualizare/semanlizare nu este transmis către Internet, tranziţiile fiind efectuate local.

Conceptul HMIPv6 este în esenţă o extensie a Protocolului Internet Mobil versiunea 6 (HMIpv6) ce are drept scop reducerea cantităţii de mesaje de semnalare şi sporirea vitezei conexiunilor mobile. Prin separarea mobilităţii globale de cea locală, acest protocol îşi îndeplineşte cu brio roulul.

c. Arhitectura de mobilitate descentralizată (Decentralized Mobility Architecture)

Pentru a rezolva deficienţele protocolului MIPv6 a fost propus pentru reţelele Ipv6 un nou tip de arhitectură: "Serviciul de Management Descentralizat al Mobilităţii" (DMMS) . Această propunere are avantajul că nu necesită un proces centralizat de înregistrare în reţeaua de reşedinţă şi că nu este necesara întreţinearea adreselor dedicate de reşedinţă. În afară de acestea , datorită particularităţii descentralizate, arhitectura DMMS îmbunătăţeşte stabilitatea şi eficienţa managementului mobilităţii şi este mai flexibilă din punctul de vedere al implementării. Configuraţia rezultată este ilustrată în Figura 12 [13] .

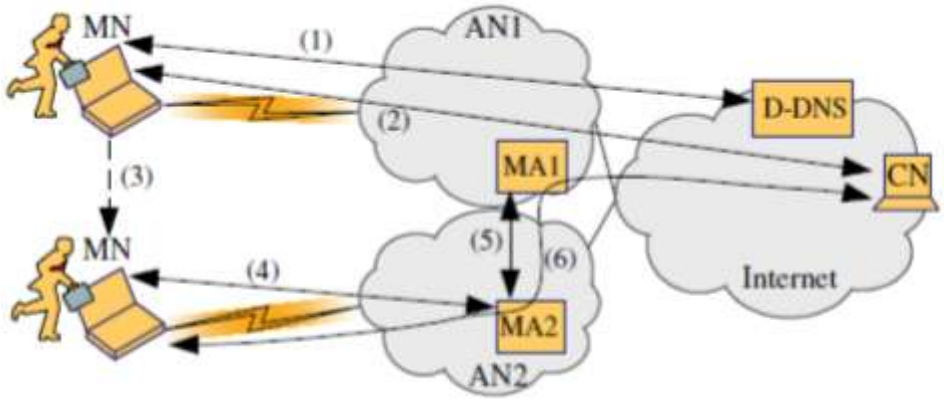


Figura 12: Serviciul de Management Descentralizat al Mobilităţii (DMMS)

Din figură se observă paşii propuşi de arhitectura DMMS:

(1)Actualizarea locaţiei
(2)Iniţierea unei noi comunicaţii
(3)Detectarea mişcării
(4)Configurarea noii adrese Ip
(5)Stabilirea contextului SHIM6
(6)Redirectarea Traficului de date

Adresa IP Descentralizată

În cadrul arhitecturii DMMS nodului mobil, dintr-o reţea de acces, îi este alocată o singură adresa IP. Aceasta prezintă următoarele caracteristici: (1) este o adresa unica, globală şi rutabilăş; (2) este alocată dinamic nodului mobil; (3) depinde de locaţia curentă a reţelei de acces de care nodul mobil este ataşat. Prin urmare, adresa poartă numele de adresă descentralizată. De fiecare dată când nodul mobil obţine o adresă IP descentralizată, adresa va fi semnalată severului DNS Dinamic şi actualizată, aşa încât nodul mobil să poată stabili o comunicaţie nouă cu celelate noduri folosind noua adresă IP. Noua adresă IP descentralizată este utilizată atât ca adresă de rutare cât şi ca identificator al conexiunii la nivel transport.

Componenta DNS Dinamic

Aşa cum a fost descris mai sus, nodul mobil din interiorul unei reţele de acces locale va fi configurat dinamic cu o adresă IP temporară. Pentru a permite altor noduri să iniţieze comunicaţia cu nodul mobil, este necesară publicarea dinamică a adresei IP prin serverul D-DNS

Pentru a implementa un server Nume de Domeniu în mod dinamic, este necesară setarea timpului maxim de fixare a domeniului la o valoare neobişnuit de mică. Acest lucru previne reţinerea adresei vechi a nodului mobil în memoria cache a DNS-ului altor noduri.

Agentul de Mobilitate

Atunci când un nod mobil, aflat intr-o nouă reţea, trimite un pachet ce conţine drept adresă sursă o adresă IP externă, pachetul este interceptat de noul Agent de Mobilitate (MA). Noul Agent de mobilitate (nMA) va stabili un context SHIM6 cu vechiul Agent de Mobilitate (oMA). SHIM6 stabileşte un context pentru fiecare conexiune cu un protocol de nivel înalt folosind mesaje de semnalizare. Odată ce contextul SHIM6 a fost realizat, pachetele sunt translatate iar adresele locale asociate contextului sunt incluse în câmpurile de adresă ale pachetului.

Detalii despre Modul de Funcţionare

Modul în care arhitectura descentralizată schimbă mesaje este ilustrat în Figura 5. Se poate observa, din figură, că shema de management al mobilităţii este atinsă prin urmărirea celor 6 paşi.

1. Actualizarea locaţiei

În cadrul arhitecturii DMMS, fiecare adresă IP asociată unui nod mobil este descentralizată. De fiecare dată când un nod mobil se ataşează la o reţea străină, serverul dinamic DNS va trebui să fie actualizat pentru a face accesibilă mobilitatea nodului. În acest scop, nodul mobil îşi va întregistra, prin mesaje de actualizare, noua adresa IP serverului D-DNS. În contrast cu MIPv6 sau cu Proxy MIPv6 în cadrul cărora informaţia despre locaţia curentă a nodului mobil era stocată intr-o entitate specifică (Agentul de Reşedinţă, respectiv Ancora Locală de Mobilitate), arhitectura descentralizată permite stocarea informaţiei referitoare la nodul mobil intr-in tip de server DNS. Cum DNS reprezintă un standard matur şi omniprezent în Internet, metoda propusă are avantajul de a evita utilizarea unei entităţi adiţionale pentru administrarea locaţiei, fără nici un impact asupra infrastructurii Internetului.

2. Iniţierea unei noi comunicaţii

Când un nod mobil se ataşeaza la o reţea de acces (ex. AN1 – figura 12) şi îi este asignată o adresă IP, nodul mobil foloseşte adresa drept identificator al conexiunii şi totodată drept indentificator de poziţie, iar fluxul de pachete destinat nodul va trece prin reţea. Datagramele schimbate de nodul mobil si peer-ul (ex: CN) său vor fi rutate în mod standard. În comparaţie cu protocolul IPV6 mobil, unde fiecare comunicaţie trebuia iniţiată prin intermediul unei entităţi intermediare (Agentul de Reşedinţă), abordarea descentralizată permite iniţierea directă a comunicaţiei cu nodul mobil la

locaţia curentă a acestuia. Adevăratul avantaj al acestei abordări este optimizarea comunicaţiei din punctul de vedere al rutării.

3. Detectarea mişcării

Mişcarea unui nod mobil din o locaţie în alta implică procesul de detectare a noii locaţii. În reţelele IPv6, un nod mobil işi poate determina locaţia curentă prin verificarea mesajelor primite de la router şi compararea prefixului adresei sursă a mesajului cu prefixul identificatorului său de locaţie. Daca prefixul de reţea al adresei routerului este egal cu prefixul reţelei identificatorului nodului mobil atunci locaţia nodului mobil nu se schimbă. Almiteri, nodul mobil se mută în altă reţea. La fel ca la MIPv6, respectiv PMIPv6, arhitectura descentralizată mosteneşte de la Ipv6 mecanismul de descoperire a vecinilor.

4. Configurarea noii adrese IP

În momentul ataşării unui nod mobil la o reţea de acces nouă, acesta va trebui sa obţină o adresa IP nouă. Pnetru obţinerea adresei, va trebuie ca nodul mobil să aleagă una din metodele de auto-configurare a adresei: dinamcă sau statică. În primul caz, nodul mobil obţine adresa IP prin serverul DHCPv6 (Dynamic Host Configuration Protocol for IPv6 – Protocolul de Configurarea Dinamica a adresei Gazdă pentru Ipv6). În cel de-al doilea caz, prin utilizarea protocolului de descoperire a vecinilor, nodul mobil este capabil de a-şi găsi un prefix de reţea în orice punct de ataşament la care se leagă şi de a-şi adăuga apoi un indentificator unic de interfaţă pentru a forma o nouă adresă IP.

5. Stabilirea contextului SHIM6

Odată ce Agentul de Mobilitate devine conştient de prezenţa unui nod mobil, va iniţia aşa numitul proces 4-way handshake (proces în cadrul căruia se stabileşte o conexiune prin schimbul de mesaje; traducerea în limba română ar fi: strângere de mână în 4 etape) pentru a crea contextul SHIM6. În cadrul contextului, perechea de idendificatori de nivel superior (nivel transport) vor reprezenta vechea adresă IP a nodului mobil respectiv adresa nodului corespondent, iar perechea de identificatori activi ai locaţiei vor fi adresele IP ale Agentului de Mobilitate. Odată ce contextul SHIM6 a fost stabilit, acesta va fi folosit pentru a procesa pachete. Comparând cu MIPv6, ce necesită înregistrarea constantă a informaţiei referitoare la locaţia curentă, contextul SHIM6 este propunerea arhitecturii descentralizate pentru acordarea permisiunii folosirii identificatorului de locaţie drept indentificator de conexiune transport. Acest lucru îngăduie funcţiei de management a mobilităţii sa fie îndeplinită în cadrul reţelei locale de acces şi nu într-o reţea centralizată. Aşadar arhitectura descentralizată reprezintă o metodă mai flexibilă şi aduce îmbunătăţiri asupra fiabilităţii sistemelor de reţea.

6. Redirectarea Traficului de Date

În final, după stabilirea contextului SHIM6, conexiunile în curs de desfăşurare create în reţeaua anterioară pot transfera în continuare datagrame. Aceast lucru este săvârşit prin schimbul de datagrame între vechiul Agent de Mobilitate şi noul Agent de Mobilitate cu ajutorul contextului SHIM6. Protocolul IPv6 mobil foloseşte tunelarea traficului de date, însă schema descentralizată câştigă prin metoda abordată mai multa eficienţă in transport, adică reţeaua va fi mai puţin împovărată.

7. Performanţă

de Bălănescu Diana

Protocolul IPv6 mobil formează coloana vertebrală a urmatoarei generaţii de tehnologie Wireless pentru servicii Internet neîntrerupte în timpul deplasării. Conceput pentru a sprijini computerele mobile ce operează în reţele de calculatoare convenţionale, acest protocol permite dispozitivului mobil deplasarea în diverse reţele, păstrând conexiunile cu alte calculatoare active. Performanţa protocolului IPv6 mobil este dată, prin urmare, de capacitatea sa de a-şi îndeplini funcţia în orice condiţii. La ora actuală un mare minus în performanţa acestui protocol este acela că în timpul tranziţiei din o reţea în alta există o mare posibilitate de întrerupere a comunicaţiilor cu alte noduri datorită pierderilor de pachete. Rezultatul este acela că pentru tranziţii frcvente, calitatea comunicaţiilor va scădea în mod semnificativ.

Performanţa protocolului IPv6 mobil a fost evaluată prin diverse simulări. În plus au fost analizate şi performanţele acelor protocoale sau scheme ce completează lipsurile MIPv6: HMIPv6 şi Arhitectura Descentralizată. După diverse scenarii în care s-a considerat simularea unor reţele de acces cu noduri mobile ce comunică conform standardului WLAN IEEE 802.11, şi pentru care observaţiile au fost luate privind următoarele aspecte: întarzieri punct-la-punct, latenţa tranzitiilor, pierderi de pachete în momentul tranziţiilor, gradul de utilizare a canalului, gradul de solicitare al reţelei, lărgimea de bandă aferantă fiecărei staţii şi de asemenea cum diferite tipuri de trafic precum UDP, VoIP şi TCP sunt afectate, s-a ajuns la următoarele concluzii:

Trecerea de la o reţea de acces la alta şi obţinerea unei noi adrese în cadrul abordării actuale a protocolului MIPv6 implică întârzieri semnificative în comunicaţia dintre nodul mobil si nodurile corespondente. Aceste întârzieri excesive sunt datorate, în mod fundamental, procesului de înregistrare cu noul punct de ataşament. Ideal acest proces ar trebui sa fie transparent comunicaţiei, insă, în realitate produce întârzieiri semnificative. Prin urmare forma curentă a protocolului nu este sufucientă pentru a susţine aplicatiţii Ipv6 interactive sau aplicaţii în timp real.

Pentru scenarii in care nu există mult trafic, utilizatorii trimit pachete de dimensiuni mici reţeaua mobila funcţionează bine, nu este supraîncărcată, ba chiar aplicarea protocolului MIPV6 conduce la rezultate mai bune decât în cazul protocoalelor dezvoltate pentru sporirea performanţei acestuia.

Numărul staţiilor mobile are deasemenea un impact asupra performanţei protocolului în cauză. Pentru un număr mic de staţii (10-20) protocolul HMIPv6 se arată mai performat decât MIPv6 din punctul de vedere al latenţei. ÎInsă pentru cazul în care numărul staţiilor creşte, acesta (HMIPv6) işi atinge pragul de saturaţie, reţeaua va fi mult mai încărcată faţă de situaţia în care pentru gestiunea ei s-ar folosi protocolul Ipv6 mobil.

Avantajul pentru care protocoale precum HMIPv6 au fost create, si anume acela de nu transmite inutil mesaje de semnalizare sau anunţuri de rutare în Internet, reprezintă un plus în performanţa acestui protocol, şi un mare minus în perfoemanţa protocolului MIPv6. În cazul acestuia, se introduce în Internet o abundenţă inutilă de mesaje care scad per ansamblu perfomanţa reţelei .

În termeni de eficienţă şi stabilitate protocolul MIPv6 are o slăbiciune şi anume faptul că tot traficul este dirijat de Agentul de Reşedinţă (Arhitectură Centralizată). Pentru a rezolva această problemă a fost propus Serviciul de Management Descentralizat al Mobilităţii. În acest caz, dacă un Agent de Mobilitate eşuează, impactul asupra reţelei este minim şi se referă doar la conexiunile deja stabilite prin acel agent. Conexiunile ce urmează a fi stabilite nu vor întâmpina probleme deoarece nodurile mobile pot obţine noi adrese IP de la serverul DHCP dinamic.

În lucrarea „**A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their Combination”** scrisă de Xavier P´erez-Costa, Marc Torrent-Moreno, Hannes Hartenstein, Network Laboratories de la NEC Europe Ltd., Heidelberg, Germany perfomanţele protocolului MIPv6 au fost comparate cu cele al protocolului HMIPv6. Scenariul simulării este alcătuit din 4 routere de access şi până la 50 de noduri mobile care comunică conform standardului IEEE802.11. Studiul s-a bazat pe aspecte precum aspecte întarzieri punct-la-punct, latenţa , pierderi de pachete, gradul de utilizare şi desolicitare a reţelei.

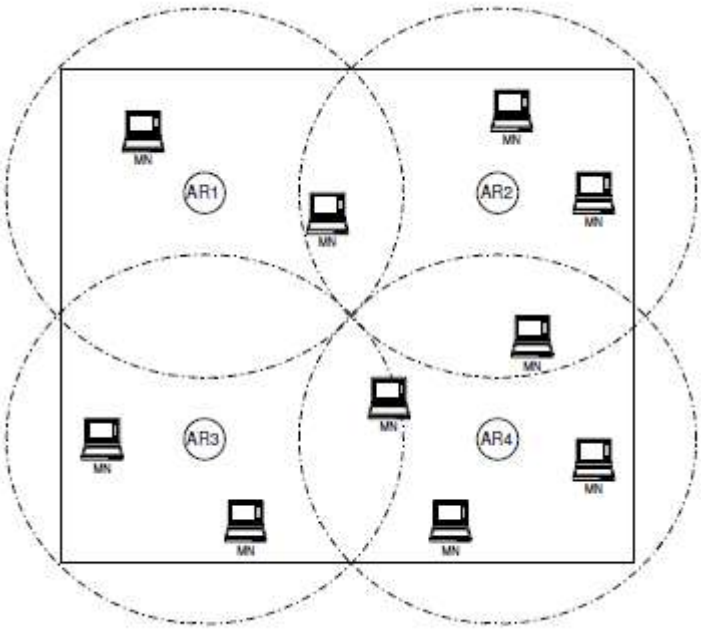


Figura 12: Scenariul simulării [14]

Un rezultat interesant din acestă lucrare este studiul impactului numarului de staţii mobile prezente în reţea asupra latenţei în comunicare. Din punct de vedere al impactului numărului de staţii asupra reţelei a reieşit următorul grafic [15]:

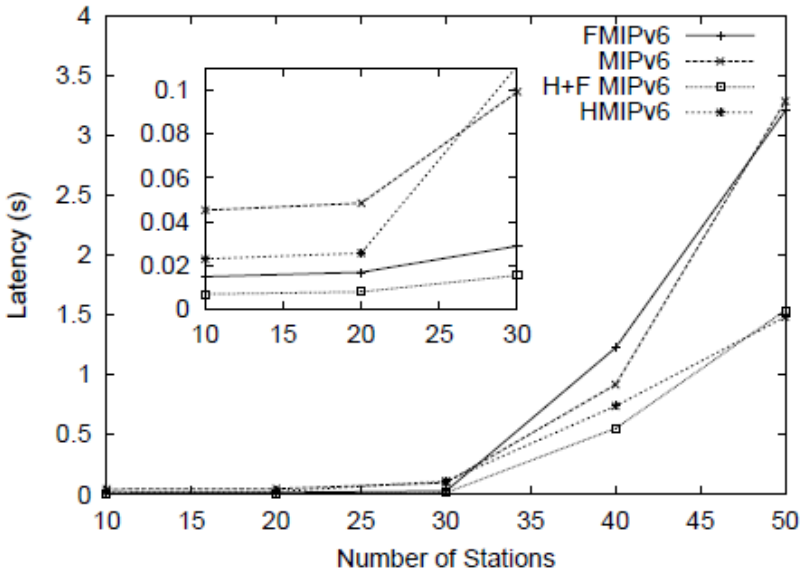


Figura 13: Impactul Numarului de staţii asupra reţelei.

Se observă că pentru un număr mic de staţii latenţa protocolului MIPv6 este mult mai mare decât cea a protocolui HMIPv6. După pragul de 20 de staţii latenţa HMIPv6 incepe sa crească din ce in ce mai mult. Pentru un numar de 27 de staţii aceasta devedind aceeaşi pentru ambele protocoale. După acest număr, protocolul HMIpv6 işi pierde din eficienţă având o latenţă mult mai mare ce va continua să crească odată cu numarul staţiilor. Tot din acest grafic se poate observa că versiunea imbunătăţită a lui MIPv6 -FMIPv6- (Fast Handovers for Mobile IPv6) are o latenţă foarte bună. Prin urmare există loc de îmbunătăţiri la protocolul de mobilitate IPv6 şi cu siguranţa cu trecerea timpului acesta va deveni un protocol mai performant şi mai stabil.

8. Concluzii

de Bălănescu Diana

Evoluţia rapidă a Internetului împreună cu creşterea enormă a numărului de utilizatori ai tehnologiei wireless au condus la tendinţa de folosire a protocolului IP drept protocol de reţea comun atât reţelelor fixe cât şi celor mobile. Viitoarele reţele vor permite utilizatorilor servicii de Internet continue atunci când aceştia trec prin sisteme wireless diferite. Protocoalele propuse de IETF pentru a suporta mobiltatea IP sunt Protocolul Ipv4 mobil si Protocolul Ipv6 Mobil.

Protocolulul Ipv6 mobil a fost creat pentru a permite accesibilitatea nodurilor mobile şi pentru a menţine neîntreruptă conexiunea cu un peer atunci când nodul mobil îşi schimbă locaţia în cadrul topologiei. Necesitatea apariţiei protocolului IPv6 este dată atât de epuizarea adreselor din IPv4, cât şi de avantajele pe care acesta le aduce serviciilor de mobilitate: algoritmi de rutare mai eficienţi, dezvoltarea reţelelor de viteze ridicate, descoperirea în mod automat a vecinilor şi auto-configurarea adresei.

În practică protocolul de mobiltate Ipv6 este întâlnit în sisteme mobile precum WLAN, WiMAX şi BWA şi este utilizat atât în aplicaţiile VoIP cât şi în reţelele VPN.

Ideea de bază în funcţionarea acestui prtococol este aceea că un terminal mobil poate fi adresabil la aceaşi adresă de reşedinţă, indiferent dacă este conectat la punctul de legătură original (*home link*), sau la altul. Permanenta conectivitate reprezintă un criteriu de perfomanţă deosebit de important. Din păcate trecerea de la o reţea de acces la alta şi obţinerea unei noi adrese în cadrul abordării actuale a protocolului MIPv6 implică întârzieri semnificative şi poate duce la o pierdere provizorie a conexiunii. De asemenea funcţionarea protocolului se bazează pe o arhitectură centralizată care nu este flexibilă la o eventuală evoluţie a reţelelor mobile.

Pentru a aduce îmbunătăţiri protocolului MIPv6 s-au dezvoltat o serie de protocoale şi scheme, printre care am amintit de PMIPv6 (Proxy Mobile Ipv6), HMIPv6 (Hierarchical Mobile IPv6) şi Arhitectura Descentralizată.

Deşi în momentul de faţă, protocolul IPv6 Mobil are o serie de deficienţe, testele de performanţă denotă că acesta prezintă un poteţial bun şi pe viitor va evolua intr-un protocol de mobiltate net superior.

Mobilitatea reprezintă un domeniu de actualitate, un domeniu ce va fi larg tratat şi utilizat în viitor, din acest motiv MIPv6 va asigura utilizatorilor interactivitate şi lejeritate.

Bibliografie

Capitolele 1 – 4:

1. **Charles E. Perkins, „***Mobile networking through MOBILE IP***”,** în IEEE Internet Computing, nr Ianuarie – Februarie 1998

2. **Request for Comments 6275**, „*Mobility Support in IPv6*”, Internet Engineering Task Force

3. **Sehwa Song, Hyoung-Kee Choi, and Jung-Yoon Kim, „***A Secure and Lightweight Approach for Routing Optimization inMobile IPv6***”,** în EURASIP Journal onWireless Communications and Networking, Volume 2009

4. **Hesham Soliman** , „*Mobile IPv6: Mobility In A Wireless Internet*” , editura Addison – Wessley, 2004

5. http://en.wikipedia.org/wiki/Mobile_IP accesat 12.12.2011

Capitolele 5 – 8:

1. **“Performance Analysis of Mobile IPv4 and Mobile IPv6”,** Fayza Nada, Faculty of Computers and information, Suez Canal University, Egypt

2. **“A New Decentralized Mobility Management ServiceArchitecture For IPV6-Based Networks” Autori:** Deguang Le, Jun Lei and Xiaoming Fu, Computer Networks Group, University of Goettingen, Germany

3. ***“A Hierarchical Mobile IPv6 Proposal”,*** Claude Castelluccia, Institut National De Recherche En Informatique Et En Automatique.

4. **“A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their Combination”,** Xavier P´erez-Costa, Marc Torrent-Moreno, Hannes Hartenstein, Network Laboratories, NEC Europe Ltd., Heidelberg, Germany.

5. http://en.wikipedia.org/wiki/Mobile_IP accesat 21.12.2011

Referințe

1 Karim El Malki, „*Mobile IPv6 Tutorial*”, North American IPv6 Summit, 23 Iunie 2003, figura 3

2 Charles E. Perkins, „*Mobile networking through MOBILE IP*”, figura 1

3 Charles E. Perkins, „*Mobile networking through MOBILE IP*”, figura 2

4 Karim El Malki, „*Mobile IPv6 Tutorial*”, North American IPv6 Summit, 23 Iunie 2003, figura 4

5 Charles Sellers, „*Introduction to Mobile IPv6*”, RMv6TF/NTT America, 9 Aprilie, 2008

6 Zhou Yi, Zheng Xuefend, Jia Jia, „Mobile IPv6 Protocol Research And Development”, figura 2

7 Sehwa Song, Hyoung-Kee Choi, and Jung-Yoon Kim, „*A Secure and Lightweight Approach for Routing Optimization inMobile IPv6*”, figura 1

8 Karim El Malki, „*Mobile IPv6 Tutorial*”, North American IPv6 Summit, 23 Iunie 2003, figura 7

9 **“***Performance Analysis of Mobile IPv4 and Mobile IPv6***”,** Fayza Nada, Faculty of Computers and information, Suez Canal University, Egypt

10 **“***A New Decentralized Mobility Management ServiceArchitecture For IPV6-Based Networks***”,** Deguang Le, Jun Lei and Xiaoming Fu, Computer Networks Group, University of Goettingen, Germany

11 *“A Hierarchical Mobile IPv6 Proposal”,* Claude Castelluccia, Institut National De Recherche En Informatique Et En Automatique.

12 *“A Hierarchical Mobile IPv6 Proposal”,* Claude Castelluccia, Institut National De Recherche En Informatique Et En Automatique.

13 **“***A New Decentralized Mobility Management ServiceArchitecture For IPV6-Based Networks***”,** Deguang Le, Jun Lei and Xiaoming Fu, Computer Networks Group, University of Goettingen, Germany

14 *A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their Combination***”**, Xavier P´erez-Costa, Marc Torrent-Moreno, Hannes Hartenstein, Network Laboratories de la NEC Europe Ltd., Heidelberg, Germany

15 „*A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their Combination***”**, Xavier P´erez-Costa, Marc Torrent-Moreno, Hannes Hartenstein, Network Laboratories de la NEC Europe Ltd., Heidelberg, Germany