1. УВОД

У сваком од протекла три века доминирала је по једна технологија. Током XX века кључне технологије су биле сакупљање, процесирање и дистрибуирање информација. Кључни елементи развоја у том периоду су инсталација телефонске мреже широм света, проналазак радија и телевизије, рађање и посебан развој рачунарске индустрије и лансирање комуникационих сателита.

Мада је рачунарска индустрија млада у поређењу са осталим индустријским гранама, рачунари су веома напредовали у кратком временском периоду. У почетку су рачунарски системи били високо централизовани, обично у оквиру једне велике собе. Спајање рачунара и комуникација имала је велики утицај на начин на који су рачунарски системи организовани. Стари модел једног рачунара који опслужује све потребе организације замењен је великим бројем одвојених али повезаних рачунара који обављају посао. Ови системи се зову рачунарске мреже. Предмет овог дипломског рада је комуникација између више рачунарских мрежа и протоколу који игра велику улогу у том процесу – Интернет Протоколу.

2. ПРИНЦИПИ МЕЂУУМРЕЖАВАЊА

У овом дипломском раду проучавају се основне функције протокола међусобно повезаних мрежа. Ради погодности позваћемо се на Интернет Стандард IP, али треба напоменути да се овај рад односи на било који протокол без успоставе везе, као на пример IPv6.

2.1. ОСНОВНЕ ОПЕРАЦИЈЕ

IP обезбеђује сервис датаграма или сервис без успоставе везе између крајњих система. Постоје бројне предности оваквог приступа:

- Могућност интернета везана за не успостављање везе је флексибилна. Она може да подржи различите типове мрежа од којих су неке без успоставе везе. У суштини, IP захтева врло мало од саме мреже.
- Интернет сервис без успоставе везе може бити врло снажан. Ово је у основи исти аргумент направљен за датаграм мрежни сервис у поређењу са сервисом виртуелног кружења.
- Интернет сервис без успоставе везе је најпогоднији за транспортне протоколе без успоставе везе зато што не намеће непотребне додатке.

Слика 2.1 приказује типичан пример коришћења IP-а, у којем су два LAN-а међусобно повезана *frame relay* WAN-ом[1]. Слика описује операцију Интернет Протокола за размењивање података између хоста А из једног LAN-а и хоста В из другог LAN-а преко WAN-а. Слика показује архитектуру протокола и формат јединице података у свакој фази. Крајњи системи и рутери морају имати исти Интернет Протокол. Такође, крајњи системи морају имати исте протоколе изнад IP- а. *Посредни рутери треба само да се имплементирају кроз IP.*

IP код крајњег система А прима са виших слојева софтвера блок података који треба да се пошаљу до крајњег система Б. IP додаје заглавље блоку података (у тренутку t_1) које, између осталог, даје глобалну интернет адресу крајњег система Б. Та адреса се логички дели на два дела: идентификатор мреже и идентификатор крајњег система. Комбинација IP заглавља и података са вишег слоја се назива јединица података Интернет Протокола (Internet protocol data unit - PDU), или једноставније датаграм. Датаграм се затим енкапсулира са LAN протоколом (LLC заглавље у t_2; MAC заглавље и приколица у t_3) и затим шаље рутеру, који скида LAN поља како би прочитао IP заглавље (t_6). Рутер затим енкапсулира датаграм са пољима оквира преноса протокола (frame relay protocol fields) (t_8) и преноси их преко WAN-а до другог рутера. Овај рутер скида frame relay поља и враћа датаграм, који се онда умотава у LAN поља, која одговарају LAN-у 2 и шаље их крајњем систему Б.

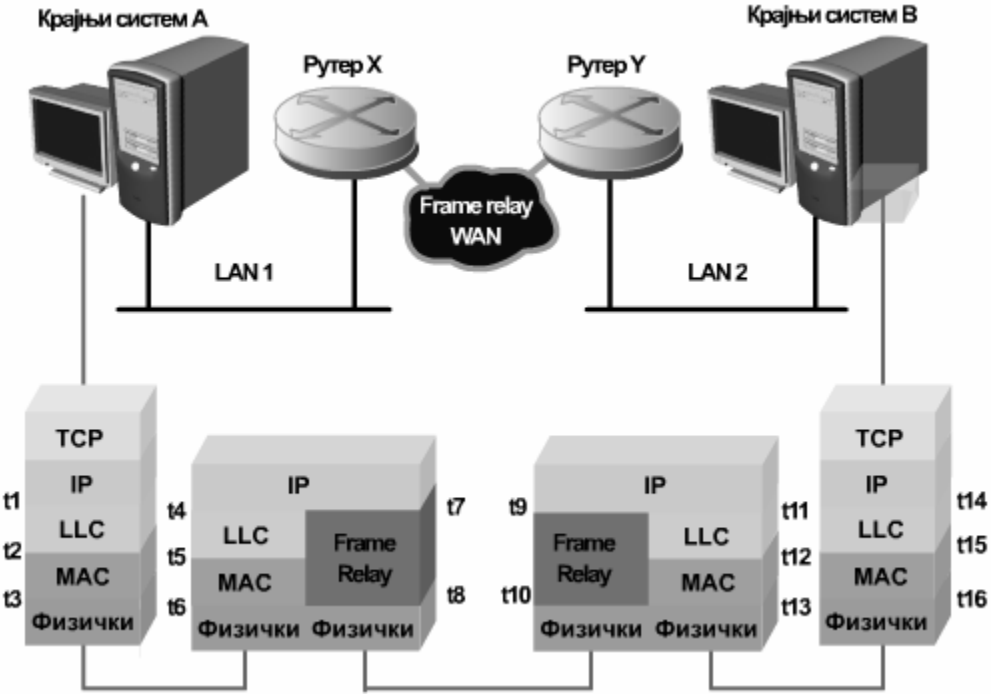
Погледајмо овај пример детаљније. Крајњи систем систем А има датаграм који треба да пренесе крајњем систему Б; датаграм има интернет адресу крајњег система Б. IP модул у крајњем систему А препознаје да је

[1] Архитектура протокола IEEE 802 се састоји од физичког слоја; слоја контроле везе (MAC) који се односи на адресирање и контролу грешака и слој контроле логичке везе (LLC), који се односи на логичке везе и идентификовање корисника LLC-а.

одредиште (Б) у другој мрежи. Тако да је први корак да пошаље податке рутеру, у овом случају рутеру X. Да би то урадио, IP преноси датаграм у следећи нижи ниво (у овом случају LLC) са инструкцијама да га пренесе рутеру X. LLC преноси ове информације MAC слоју, који убацује адресу MAC слоја рутера X у MAC заглавље. На тај начин, блок података који се преноси на LAN 1 укључује податке из слоја или слојева изнад TCP, плус TCP заглавље, IP заглавље, LLC заглавље, MAC заглавље и приколицу (тренутак t_3 на слици 2.1).

Даље, пакет путује кроз мрежу 1 до рутера X. Рутер уклања MAC и LLC поља и анализира IP заглавље да утврди коначно одредиште података, у овом случају Б. Рутер сад мора донети одлуку о рутирању. Постоје три могућности:

1. Одредишна станица Б је директно повезана са једном од мрежа за коју је рутер везан. Ако је тако, рутер шаље датаграм директно до одредишта.
2. Да би дошао до одредишта, мора ићи преко једног или више рутера. Ако је тако, мора се донети одлука о рутирању: До ког рутера треба послати датаграм? И у случају 1 и у случају 2, IP модул у рутеру шаље датаграм на нижи ниво са одредишном MAC адресом. Ради се о адреси нижег нивоа која је везана за ову мрежу.
3. Рутер не зна одредишну адресу. У овом случају рутер враћа поруку о грешци извориште датаграма.



Слика 2.1 Операције Интернет Протокола

У овом примеру, подаци се морају пренети преко рутера Y пре него што дођу до одредишта. Тако да рутер X конструише нови оквир повезујући *frame relay* заглавље и приколицу са јединицом података IP-а. *Frame relay* заглавље указује на логичну везу са рутером Y. Кад овај оквир стигне до рутера Y, заглавље оквира и приколица се отцепљују. Рутер одређује да ова IP јединица података потиче од хоста B, који је директно повезан са мрежом за коју је овај рутер везан. Рутер зато ствара оквир са *layer-2* одредишном адресом хоста B и шаље

је на LAN 2. Подаци коначно стижу до хоста B, где се LAN и IP заглавља отсецају.

Пре него што се подаци проследе, рутер ће можда морати да фрагментује јединицу података, да би је прилагодио мањој максималној величини пакета одредишне мреже. Јединица података је подељена у два или више делова, и сваки од њих постаје независна јединица података. Свака нова јединица података је умотана у пакет нижег нивоа и стављена у ред за пренос.

Рутер такође може ограничити листу чекања за сваку мрежу за коју је везан како би избегао да спорија мрежа успорава бржу. Када више нема места у реду, односно када дође до попуњавања лимита накнадно пристигли пакети се једноставно одбацују. Овај процес се понавља у онолико рутера колико је потребно да пакет стигне до дестинације. Као и рутер, дестинациони крајњи систем купи IP пакет са мреже. Ако је било фрагментације, IP модул у дестинационом систему зауставља пристигли податак док год се поново не скупи цео пакет. Овај блок података се онда прослеђује вишим нивоима крајњег система.

Овај сервис понуђен од стране IP-а је непоуздан зато што IP не гарантује да ће подаци стићи до одредишта или да ће подаци који стигну бити поређани одговарајућим редом. То је посао следећег вишег слоја (у овом случају TCP), који се бави обнављањем пакета у случају грешке при преносу. Овакав прилаз обезбеђује велику флексибилност.

Са приступом Интернет Протокола, сваки део пакета се пребацује од рутера до рутера, све у намери да пакет стигне од изворишта до одредишта. Због немогућности гарантовања испоруке, не постоје одређени захтеви поузданости на било којој од мрежа. Према томе, протокол ће радити ма каква била комбинација типова мрежа. Пошто редослед испоруке није гарантован, успешни делови пакета могу да иду различитим путањама по интернету. Ово омогућава протоколу да утиче на ненагомилавање у интернету тако што ће променити руте.

2.2. ПРОБЛЕМИ ПРОЈЕКТОВАЊА

Са овим кратким приказом операција IP-контролисаног интернета, можемо да се вратимо и проучимо детаљније неке проблеме пројектовања:

- Рутирање
- Животни век датаграма
- Фрагментовање и поновно склапање
- Контрола грешке
- Контрола протока
- Адресирање

Рутирање

Циљ рутирања јесте да за сваки крајњи систем рутер конструише табелу рутирања која садржи путање до сваке одредишне мреже, до сваког рутера до кога би датаграм требало послати.

Табеле рутирања могу бити статичке или динамичке. Статичка табела, међутим, може да садржи алтернативне руте у случају да одређени рутер није доступан. Динамичка табела је флексибилнија у случајевима када дође до

нагомилавања или грешке. Узмимо за пример Интернет, наиме, ако један рутер прекине са радом сви његови суседи шаљу статусни извештај који онда омогућава рутерима и станицама да ажурирају своје табеле рутирања. Сличан план се може користити и за конторолу нагомилавања. Контрола нагомилавања је врло значајна због не слагања капацитета LAN-а и WAN-а.

Табеле рутирања се такође могу користити као помоћ оталим сервисима међусобно повезаних мрежа, као што су сигурност и приоритет. На пример, појединачне мреже могу служити за преузимање података до одређене сигурносне границе. Механизам рутирања мора уверити да ће подацима задатог сигурносног нивоа бити забрањено да пролазе кроз мреже које нису овлашћене да преузимају такве податке.

Још једна од техника рутирања је *изворишно рутирање*. Изворишна станица одређује руту тако што наводи доследан низ рутера у датаграму. Ова техника може бити корисна због захтева сигурности и приоритета.

Коначно, поменућемо сервис који је у сродству са рутирањем: записивање руте. Да би се обавило записивање руте, сваки рутер додаје своју интернет адресу у листу адреса у датаграму. Ова особина је корисна у намери тестирања или отклањања грешака (*debugging*).

Животни век датаграма

Ако се користи динамичко или алтернативно рутирање, постоји могућност да датаграм неодређено дуго кружи интернетом. Ово је недопустиво из два разлога. Прво, бескрајно дуго кружење датаграма троши средства. Друго, транспортни протокол може бити зависган од постаојања горње границе живота датаграма. Да би се избегли ови проблеми сваки датаграм може бити обележен са животним веком. Када животни век истекне, датаграм бива одбачен.

Најједноставнији начин да се имплементира животни век је коришћење бројача скокова. Сваки пут када датаграм прође кроз рутер, бројач се декрементира (умањује за један). Алтернативно, животни век може бити права временска величина. Ово затева од рутера да некако зна колико је времена прошло од када је датаграм или фрагмент последњи пут прошао кроз рутер, да би знао за колико да декрементира поље животнни век. Да би то било могуће потран је глобални временски механизам. Предност коришћења стварне временске величине је та што се може користити у алгоритму за поновно склапање пакета, што је објашњено следеће.

Фрагментовање и поновно склапање

Појединачне мреже у интернету могу назначити различите максималне величине пакета. Било би невешто и крајње незгодно диктирати исту величину пакета кроз различите мреже. Према томе, рутер мора да фрагментује пристигле пакете у мање целине, које се називају сегменти или фрагменти, пре него што их проследи следећој мрежи.

Ако датаграми могу бити фрагментовани (по могућству више од једнанут) у току путовања поставља се питање где ће се поново склопити. Најлакше решење је да се поновно спајање изврши само у одредишту. Главна неповољност овог приступа је та што фрагменти могу бити само мањи како се пакет креће по интернету. Ово може смањити ефикасност неких мрежа.

Међутим, ако је дозвољено поновно склапање у рутерима на међупутањи, може доћи до следећих неповољних околности:

1. Потребни су велики *бафери* у рутеру и постоји ризик да цео простор *бафера* буде потрошен у складиштењу дела датаграма.
2. Сви делови датаграма морају да прођу кроз исти рутер, што спречава коришћење динамичког рутирања.

У IP-у, фрагменти датаграма се склапају у одредишном систему. Техника IP фрагментовања користи следеће информације у IP заглављу:

- Идентификатор пакета (ID)
- Дужина Података
- Офсет
- Флег *More* (још)

ID служи да јединствено идентификује оригинални датаграм крајњег система. У IP-у се састоји од изворишне и одредишне адресе, броја који одговара слоју у коме се налази протокол који је генерисао податак (нпр. TCP), и идентификације набављене од стране слоја протокола. *Дужина Података* је дужина корисничких података, исказана у октетима (бајтовима), Офсет је позиција фрагмента корисничких података у пољу података у оригиналном датаграму, *повећано за 64 бита.*

Изворишни систем ствара датаграм са Дужином Података истом као цела дужина поља података, са Офсетом = 0 и флегом Још постављеним на 0 (false). Да би поделио дугачак датаграм у два дела, IP модул у рутеру извршава следеће:

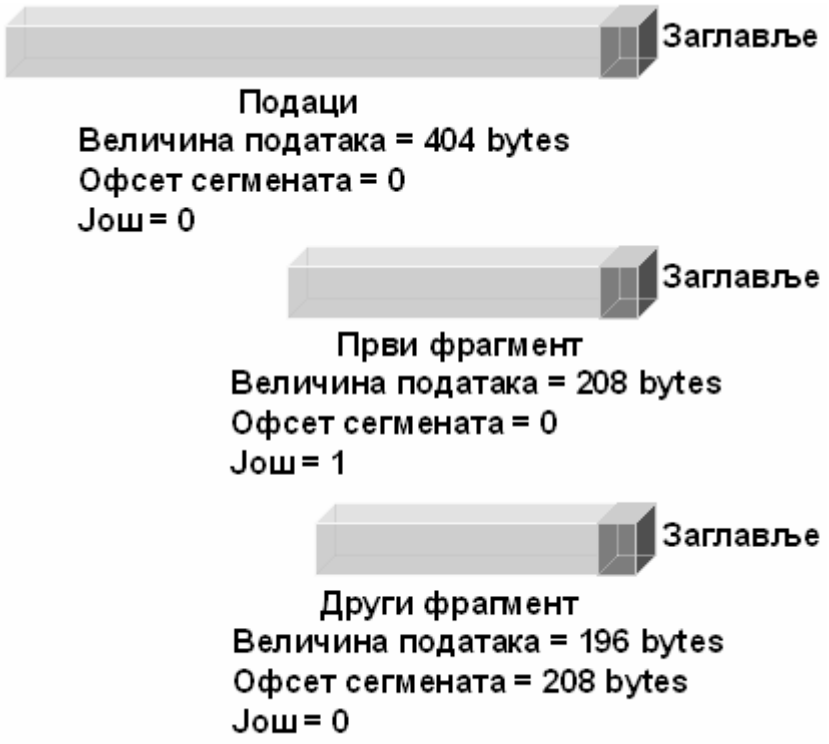
1. Прави два нова датаграма и копира заглавље оригиналног датаграма у оба.

2. Дели долазеће корисничке податке на два приближно једнака дела уз 64-битну границу, стављајући сваки део у нови датаграм, први део се мора повећати за 64 бита.

3. Поставља Дужину Података првог новог датаграма на дужину уметнутих података и поставља флег Још на 1 (true). Офсет поље оставља непромењено.

4. Поставља Дужину Података другог новог датаграма на дужину уметнутих података и додаје дужину првог дела података подељену са 8 у поље Офсет. Флег Још остаје исти (0, false).

Слика 2.2 описује претходно наведени пример. Процедура је лако уопштена на n-ту поделу.



Слика 2.2 Пример фрагментовања

Да би се поново склопио датаграм, мора да постоји довољно места у *баферу* на месту где се датаграм склапа. Како пристижу пакети са истим ID пољем, њихова поља са подацима се убацују у одговарајући део у *баферу* док се не склопи цело поље са подацима, што се постиже када група података почиње са Офсетом једнаким нула и завршава се подацима из фрагмента коме је флег Још био постављен на 0 (false).

Једна од могућности са којом се морамо суочити јесте да један или више фрагмената можда неће стићи до одредишта: IP сервис не гарантује испоруку. Потребна је метода којом би се одлучило када да се одустане од покушаја склапања података како би се ослободило место у *баферу*. Тренутно се користе два приступа. Први, треба доделити животни век склапању података првом фрагменту који пристигне. То је локални сат за склапање података, додељен од стране функције за склапање података, који се декрементира док се *баферују* фрагменти оригиналног датаграма. Ако време истекне пре него што се заврши склапање података, примљени фрагменти бивају одбачени. Други приступ је да се искористи животни век датаграма, који је део заглавља сваког пристиглог фрагмента. Наставља се са декрементирањем животног века од стране функције за склапање података; као и код првог приступа, ако животни век истекне пре него што се изврши склапање пакета, примљени фрагменти се одбацују.

Контрола грешке

Међуумрежавање не гарантује успешну испоруку сваког датаграма. Када рутер одбаци датаграм, он треба да врати неке информације извориште. Изворишни Интернет Протокол може да искористи ове информације да измени стратегију преноса и да обавести више слојеве. Да би пријавио да је неки датаграм био одбачен потребан је део идентификације датаграма.

Датаграм може бити одбачен из много разлога, укључујући истек животног века, загушења и грешке *чексуме*. У осталим случајевима, извештај није могућ зато што је поље са изворишном адресом можда оштећено.

Контрола протока

Контрола протока у интернету дозвољава рутерима и/или одредишним станицама да ограниче норму примања података. За тип сервиса без успоставе везе који се овде описују, механизам контроле протока је ограничен. Најбољи приступ би био да се пошаље пакет који врши контролу протока другим рутерима и изворишним станицама који би захтевао смањење протока података. Овакав или сличан пример биће описан касније, када буде био описан ICMP (Internet Control Message Protocol).

Адресирање

Концепт адресирања у архитектури комуникације је скуп који покрива доста проблема, као што су:

- Ниво адресирања
- Област адресирања
- Начин адресирања

Ниво адресирања

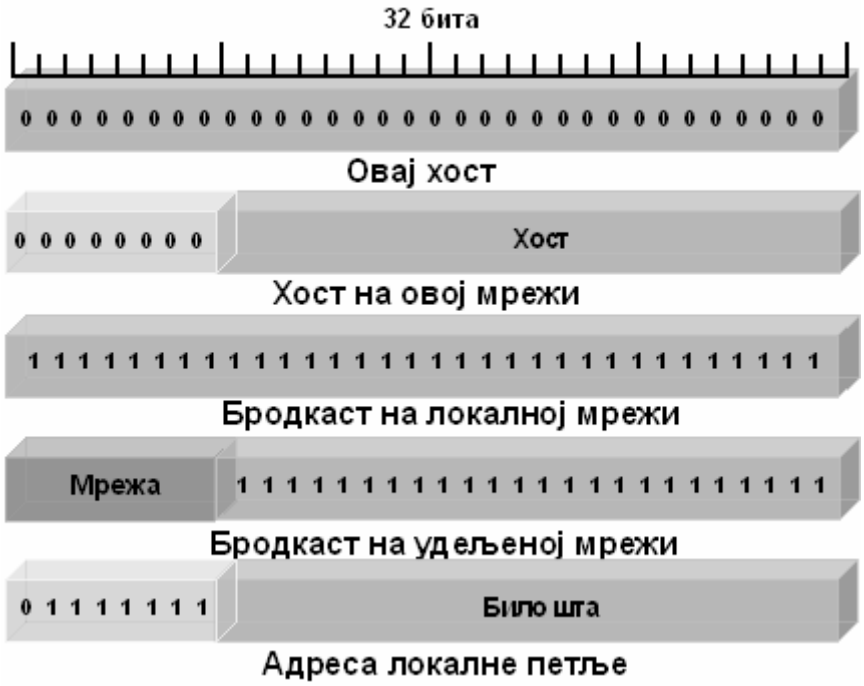
Односи се на ниво у архитектури комуникације у којој је именована суштина. Сваком крајњем и међу систему у конфигурацији додељује се јединствена адреса. У случају TCP/IP архитектуре, ово се односи на IP адресу или једноставно, интернет адресу. IP адреса се користи да би се рутирао PDU кроз мрежу или мреже до система на који указује IP адреса у PDU-у. Нижи ниво адресирања је потребан за било коју појединачну мрежу која има више привезаних система на себе, као што су *frame relay* или ATM мреже. У овом случају јединствена адреса се додељује сваком уређају привезаном на ову мрежу.

Када подаци стигну до одредишног система, они морају бити усмерени неком процесу или апликацији у систему. Систем ће подржавати више апликација и апликација може подржавати више корисника. Свакој апликацији и, можда, сваком заједничком кориснику апликације додељује се јединствени идентификатор, који се односи на порт у TCP/IP архитектури или као приступна тачка сервиса (Service Access Point – SAP) у OSI архитектури.

Још један проблем који се тиче адреса једног крајњег система или међу система је **област адресирања**. Интернет адреса је глобална адреса. Кључне карактеристике глобалних адреса су следеће:

- **Глобална недвосмисленост:** Глобална адреса идентификује јединствен систем. Синоними су дозвољени. Значи, систем може имати више од једне глобалне адресе.
- **Глобална употребљивост:** Могуће је на неком систему идентификовати било који други систем, на начин глобалне адресе другог система.

Због тога што је глобална адреса јединствена и глобално употребљива, интернету је омогућено да прослеђује податке са било ког система прикљученог на било коју мрежу ка било ком другом систему прикљученог на било коју другу мрежу.



Слика 2.3 Неке од могућих специјалних IP адреса

Још један од концепата адресирања је начин адресирања. Најопштије, једна адреса се односи на један систем или порт; у овом случају односи се на индивидуалну или **unicast** адресу. Такође је могуће да се једна адреса односи на више целина или портова. Као што је адреса која идентификује више симултаних појединаца. На пример, мрежни контролни центар жели да обавести све кориснике да мрежа пада. Адреса за више примаоца може бити **broadcast**, намењена за све целине одређеног домена, или **multicast**, намењена за одређену подмрежу или целину. Слика 2.3 приказује неке од могућности.

3. ИНТЕРНЕТ ПРОТОКОЛ

У овом делу бавимо се верзијом 4 IP-а, официјално дефинисаног у RFC-у 791. Ипак, намера је да ће IPv4 коначно бити замењен од стране IPv6, ово је стандардни IP који се користи у TCP/IP мрежама.

Интернет Протокол (IP) је део TCP/IP пакета и протокол међуумрежавања који се најшире користи. Као што је ствар са сваким протокол стандардом, тако је и IP описан из два дела:

- Интерфејс са вишим слојевима (нпр. TCP), описујући сервисе које IP обезбеђује.
- Формат и механизам протокола.

У овом одељку изучаваће се први IP сервиси, а онда и сам протокол. Онда ће се изучавати формати IP адреса. На крају се изучава Internet Control Message Protocol (ICMP), који је интегрисани део IP-а.

3.1. IP СЕРВИСИ

Сервиси који ће бити обезбеђени преко слојева протокола (нпр. између IP и TCP) су изражени у облику примитива и параметара. Примитива описује функцију која ће бити извршена, а параметри се користе у пропуштању података и контроли информација. Стварна форма примитива зависи од имплементације. Један од примера је позив подпрограма.

IP обезбеђује две сервисне примитиве интерфејса ка следећим слојевима. Send примитива се користи да би се затражила трансмисија податка. Deliver примитива се користи од стране IP-а да би се обавестио корисник да су подаци стигли. Параметри повезани са ове две примитиве су следећи:

- **Изворишна адреса:** Међумрежна адреса пошаљиоца.
- **Одредишна адреса:** Међумрежна адреса примаоца.
- **Протокол:** Протокол примаоца
- **Индикатор типа сервиса:** Користи се да специфицира третирање јединице података у току трансмисије кроз мреже.
- **Идентификација:** Користи се у комбинацији са изворишном и одредишном адресом и корисничким протоколом да би се јединствено идентификовала јединица података. Овај параметар је потребан због поновног склапања података и извештаја о грешци.
- **Идентификатор *Don't Fragment* (Немој Фрагментовати):** Указује да ли IP може да подели податак како би успешно обавио испоруку.
- **Идентификатор *Time To Live* (Време у Животу):** Исказује се у секундама.
- **Дужина података:** Дужина података која се преноси.
- **Опције података:** Опције које тражи IP корисник.
- **Подаци:** Кориснички подаци који се преносе.

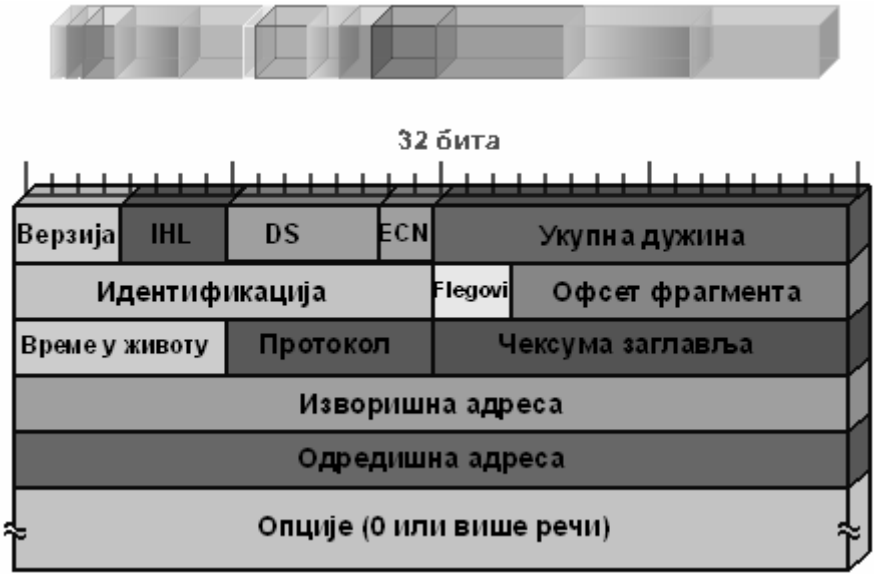
Параметри идентификација, идентификатор *Don't Fragment* (DF) и *Time To Live* (TTL) су присутни у Send примитиви али и у Deliver примитиви. Ова три параметра одређују иструкције IP-у које нису брига IP корисника који прима пакет.

Параметар назван опције података обезбеђује будуће проширење и позив параметара који се обично не позивају. Тренутно дефинисане опције су:

- **Сигурност:** Допушта да сигурносна ознака буде закачена на датаграм.
- **Изворишно рутирање:** Низ адреса рутера који специфицира руту коју треба следити. Рутирање може бити стриктно (само идентификовани рутери могу бити посећени) или незаобилазно (остали међу рутери могу бити посећени).
- **Запис руте:** Поље је постављено да би се записао низ рутера посећених од стране датаграма.
- **Идентификација тока:** Именује резервисана средства која се користе за сервис тока. Овај сервис омогућава специјално манипулисање за повремено густ саобраћај (нпр. глас).
- **Ознака времена:** Изворишни IP ентитет и неки од међу-рутера додају ознаку времена (у милисекундама) јединици података када пролази поред.

3.2. ИНТЕРНЕТ ПРОТОКОЛ

Протокол између IP ентитета најбоље се може описати позивањем на формат IP датаграма који је приказан на слици 3.1 . Поља иду следећим редоследом:



Слика 3.1 IPv4 Заглавље

- **Верзија (4 бита):** Приказује износ верзије како би се могао дозволити развој протокола. Вредност поља је 4.
- **Дужина Интернет Заглавља (IHL) (4 бита):** Дужина заглавља у 32-битној речи. Минимална вредност је пет за минималну дужину заглавља од 20 бајта.
- **DS/ECN (8 бита):** У претходном опису сервиса, ово поље се односило на поље **Тип Сервиса** и одређивало је поузданост, предност, одлагање и параметре пропусне моћи. Оваква итерпретација је сада замењена. Првих 6 бита поља Типа Сервиса сада припада пољу DS (Differentiated

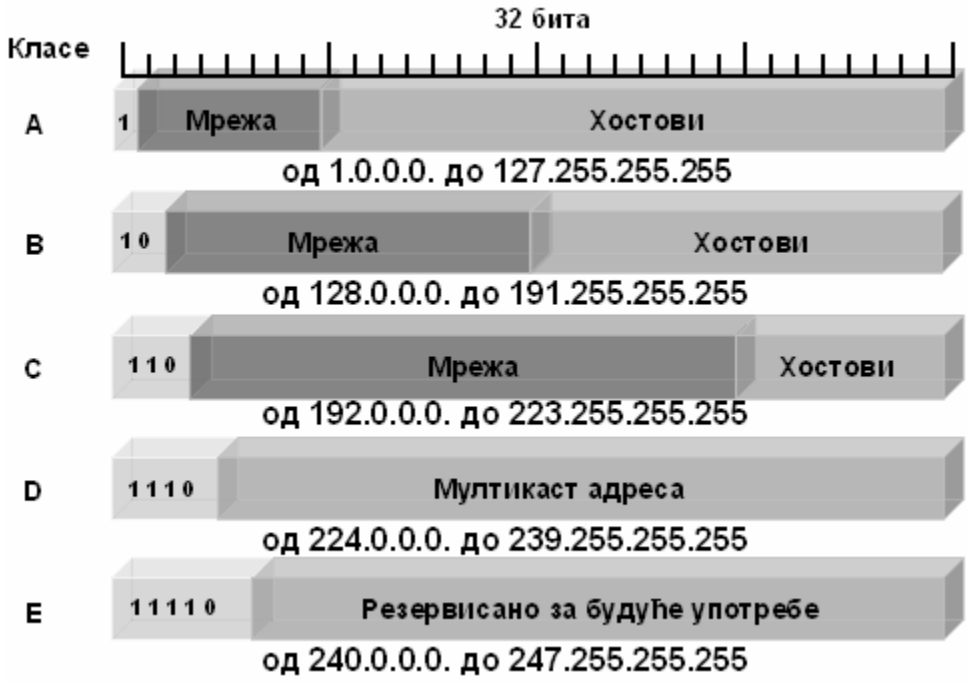
Services), а остала 2 бита резервисана су за поље ECN (Explicit Congestion Notification).

- **Укупна дужина (16 бита):** Укупна дужина датаграма, укључујући заглавље и податке, изражено је у бајтовима (октетима).
- **Идентификација (16 бита):** Низ бројева, који заједно са изворишном адресом, одредишном адресом и корисничким протоколом намерава да јединствено идентификује датаграм. Према томе, овај број би требао да буде јединствен за изворишну адресу, одредишну адресу и кориснички протокол датаграма док год је он у интернету.
- **Флегови (3 бита):** Само два од ових бита су тренутно дефинисана. *More* се користи за фрагментацију и поновно склапање, као што је малопре објашњено. Бит DF забрањује фрагментацију када се то тражи. Овај бит може бити од велике користи када се зна да дестинација нема капацитета да склопи фрагменте. Ипак, ако је овај бит постављен, датаграм ће бити одбачен ако премаши максималну величину мреже на некој рути. Да се ово не би десило, било би паметно користити изворишно рутирање да би се заобишле мреже које имају дефинисану малу максималну величину пакета.
- **Офсет фрагмената (13 бита):** Показује где је у оригиналном датаграму место овом фрагменту, исказано у 64 бита. То значи да фрагменти који нису последњи фрагмент морају да садрже поље података које је дељиво са 64 бита у дужини.
- **Време у животу (8 бита):** Показује колико дуго, у секундама, је дозвољено датаграму да буде у интернету. Сваки рутер који процесира датаграм мора да смањи TTL за најмање један, тако да је TTL донекле сличан бројачу скокова.
- **Протокол (8 бита):** Показује протокол следећег-вишег-нивоа који треба да прими поље са подацима у дестинацији; према томе, ово поље идентификује тип следећег заглавља у пакету које је после IP заглавља.
- **Чексума заглавља (16 бита):** Код за детектовање грешке који је привезан само заглављу. Због мењања неких поља током пута (нпр. време у животу, фрагментациона поља), ово поље се реверификује и процењује у сваком рутеру. Поље се формира тако што се узму јединице из 16 бита и додају се све јединице из свих 16-битних речи у заглављу. Због рачунања, поља чексуме су иницијализована на вредност нула.
- **Изворишна адреса (32 бита):** Кодирано да би се дозволиле различите комбинације бита за специфицирање мреже или система прикаченог на мрежу.
- **Одредишна адреса (32 бита):** Исте катактеристике као изворишна адреса.
- **Опције (променљиво):** Кодира опције тражене од стране пошиљаоца.
- **Повећавање (променљиво):** Користи се да би се могло гарантовати да је заглавље датаграма спој 32-битних дужина.
- **Подаци (променљиво):** Ово поље мора бити спој 8-битних дужина целих бројева. Максимална дужина датаграма (поља података + заглавља) је 65,535 бајтова.

Сада је јасно да се IP сервиси, објашњени у Send и Deliver примитивама, поклапају са пољима IP датаграма.

3.3. IP АДРЕСЕ

Свако од поља изворишне и одредишне адресе у IP заглављу садржи 32-битну глобалну интернет адресу, која се генерално састоји од идентификатора мреже и идентификатора хоста.



Слика 3.2 Класе IP адреса

Класе мрежа

Адреса је кодирана да би се дозволиле различите комбинације бита за специфицирање мреже или хоста, као што се види на слици 3.2. Енкодовање обезбеђује флексибилност у додељивању адреса хостовима и дозвољава различите величине мрежа у интернету. Постоје три главне класе мрежа за које је најбољи пример следећи:

- **Класа А:** Мало мрежа, свака има мало хостова.
- **Класа В:** Средњи број мрежа, свака са средњим бројем хостова.
- **Класа С:** Много мрежа, свака са мало хостова.

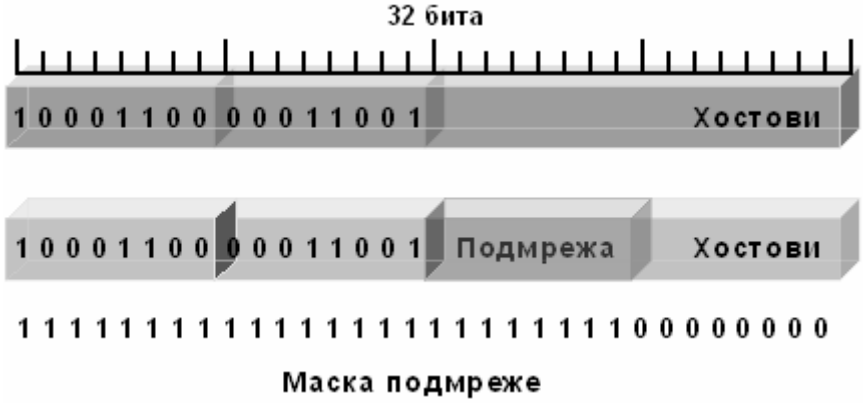
У одвојеном окружењу би било најбоље користити адресе из само једне класе. На пример, заједничка међумрежа која се састоји од великог броја локалних рачунарских мрежа би требало да користи адресе из класе С. Ипак, формат адресе је такав да је могуће мешати све три класе адреса на истој међумрежи, што се ради на самом Интернету. Мешање класа је својствено за међумрежу која се састоји од неколико великих мрежа, пуно малих мрежа и средњег броја средњих мрежа.

IP адресе се обично записују у, како се то каже, децималама одвојеним тачкама, где свака децимала означава сваки од октета 32-битне адресе. На пример, IP адреса 11000000 11100100 00010001 00111001 је написана као 192.228.17.57.

Приметите, да свака од адреса из класе А почиње са бинарно 0. Мрежне адресе са првим октетом 0 (бинарно 00000000) и 127 (бинарно 01111111) су резервисане, тако да постоји 126 потенцијалних мрежа из класе А, које имају прву децималу од 1 до 126. Мрежне адресе из класе В почињу са бинарно 10, стога је опсег адреса мреже у децималном облику од 128 до 191 (бинарно 10000000 до 10111111). Други октет је такође део адреса мрежа класе В, тако да постоји 2^{14} = 16 384 мрежних адреса из класе В. Мрежне адресе из класе С почињу са бинарно 110, тако да за мрежне адресе из класе С опсег адреса у децималном облику иде од 192 до 223 (бинарно 11000000 до 11011111). Укупан број мрежних адреса из класе С је 2^{21} = 2 097 152.

Подмреже и маске подмрежа

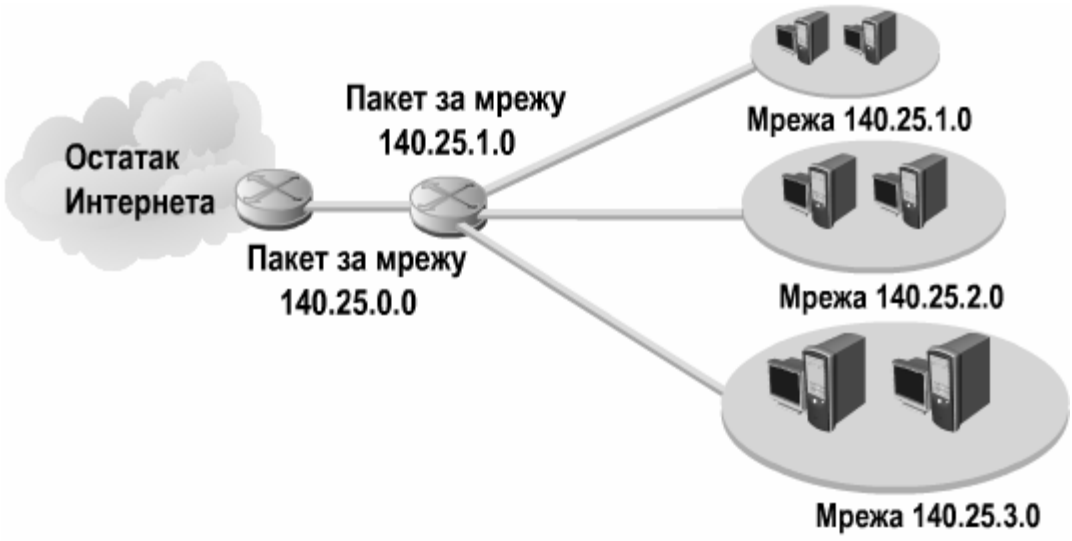
Концепт подмреже је уведен због следећих захтева. Замислите једну велику мрежу која укључује један или више WAN-ова и велики број тачака, од којих се свака састоји од великог броја LAN-ова. Желели бисмо да дозволимо самовољну сложеност међуповезаних LAN структура унутар једне организације док изолујемо целокупан интернет против експлозивног раста мрежних бројева и комплексности рутирања. Један од начина да се превазиђе овај проблем је да се додели један број за све LAN-ове у једној тачки који би поједноставио адресирање и рутирање. Да би се дозволило рутерима у оквиру једне тачке да функционишу како треба, сваком LAN-у се додељује број подмреже. Део адресе резервисан за хостове бива подељен на број подмреже и број хоста да би се прилагодио овом новом начину адресирања.



Слика 3.3 Подмрежа и маска подмреже

Унутар подељене мреже, локални рутери морају рутирати по бази проширеног мрежног броја који се састоји од мрежног дела IP адресе и броја подмреже. Да би се одредила позиција битова у оваквом проширеном мрежном броју користи се маска подмреже. Коришћење маске подмреже помаже хосту да утврди да ли је одлазећи датаграм намењен хосту на истом LAN-у (шаље директно) или на другом LAN-у (шаље датаграм рутеру). Усвојено је да се неки други начини (нпр. мануелна конфигурација) користе да би се маска подмреже направила и да би била позната локалним рутерима. Слика 3.3 показује принцип прављења подмреже и маске подмреже. Ефекат маске подмреже јесте да обрише поделу између поља са хостовима која се односе на стварни хост на подмрежи. Оно што остаје су број мреже и број подмреже. Слика 3.4 показује

пример коришћења подмрежавања. Слика приказује локални комплекс који се састоји од три LAN-а и два рутера. Остатак Интернета овај комплекс види само као мрежу класе B са мрежном адресом 140.25.x.x, где су лева два октета број мреже, а десна два број хоста. Рутер који дели мрежу на подмреже је конфигурисан маском подмреже која има вредност 255.255.255.0. На пример, ако датаграм са одредишном адресом 140.25.2.1 стигне у рутер Y са остатка Интернета, рутер користи маску подмреже да би утврдио да се ова адреса односи на подмрежу 1 и онда прослеђује датаграм том LAN-у где нови рутер мора да утврди ком хосту са тог LAN-а је намењем пакет. Када је утврдио коме је намењен пакет, рутер коначно прослеђује пакет хосту.

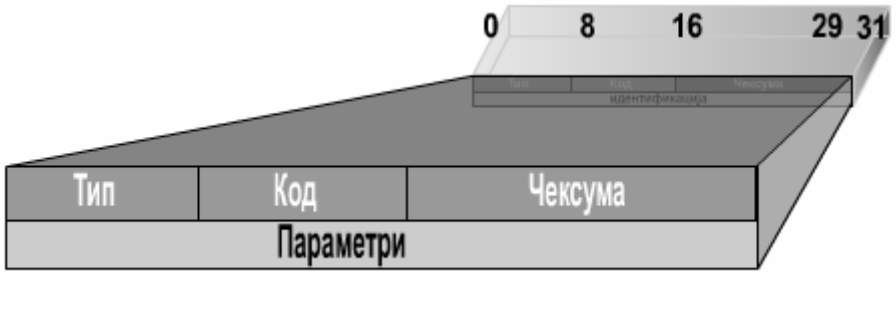


Слика 3.4 Пример коришћења подмреже

3.4. INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

IP стандард наводи да имплементација протокола мора да садржи и ICMP (RFC 792). ICMP обезбеђује средство за трансмисију порука од рутера и осталих хостова до хостова. У суштини, ICMP обезбеђује повратну спрегу у вези проблема у комуникацији у окружењу. Пример употребе ICMP-а је када датаграм не може да стигне до одредишта, када рутер нема довољну величину *бафера* да би проследио датаграм и када рутер може да упути станицу да шаље пакете краћом рутом. У већини случајева, ICMP порука се шаље као одговор на датаграм, било од стране рутера који се налази на путу датаграма или од стране хоста који је одредиште датаграма.

Иако је ICMP на истом слоју као и IP у TCP/P архитектури, он је уствари корисник IP-а. ICMP порука се прво направи па се онда предаје IP-у који спаја поруку са IP заглављем и онда преноси резултујући датаграм на већ уобичајени начин. Из разлога што се ICMP поруке шаљу као IP датаграми, њихова испорука није гарантована нити њихово коришћење поуздано.



Слика 3.5 Формат ICMP поруке

Слика 3.5 приказује ICMP поруке. Једна ICMP порука почиње са 64-битним заглављем које се састоји од следећих поља:

- **Тип (8 bita):** Означава тип ICMP поруке.
- **Kod (8 bita):** Користи се да би се специфицирали параметари поруке која се може кодовати са једним или више бита.
- **Чексума (16 бита):** Чексума ICMP поруке. Исти алгоритам се користи и у чексуми IP-а.
- **Параметри (32 бита):** Служи да би се назначили параметри који следе.

Ова поља су углавном праћена допунским информацијоним пољима која даље описују садржај поруке.

У оним случајевима у којима се ICMP порука одности на претходни датаграм, информациона поља садрже цело IP заглавље плус првих 64 бита поља података оригиналног датаграма. Ово омогућава изворишном хосту да упореди долазећу ICMP поруку са претходним датаграмом. Разлог за укључивање првих 64 бита поља података је тај што ће ово омогућити IP модулу у хосту да одреди који протокол или протоколи вишег слоја су били укључени. Првих 64 бита би укључило део TCP заглавља или заглавља неког другог протокола транспортног слоја.

Одредиште недоступно

Порука покрива бројне случајеве. Рутер може да врати ову поруку ако не зна како да дође до одредишне мреже. У неким мрежама рутер може да процени да је неки хост недоступан и онда врати поруку о томе. Одредишни хост такође може да врати ову поруку ако је кориснички протокол или нека од приступних тачака сервиса виших слојева недоступана. Ово може да се деси ако је одговарајуће поље у IP заглављу неправилно подешено. Ако је у датаграму наведено изворишно рутирање које се не користи, порука ће бити враћена. На крају, када рутер треба да фрагментује датаграм, а флег Немој Фрагментовати је постављен, рутер одбацује датаграм, а изворишном хосту се шаље порука.

Рутер ће вратити **поруку о истеку времена** ако животни век датаграма истекне. Хост ће послати ову поруку не заврши склапање датаграма у року.

Синтаксичке или семантичке грешке у IP заглављу проузроковале би поруку о грашкама у параметрима која би била враћена од стране рутера или хоста. На пример, неправилни аргументи могу бити дати од стране поља опција. Поље параметара садржи показивач на октет у оригиналном датаграму у коме је детектована грешка.

Порука о стишавању протока из изворишта (source quench)

Обезбеђује основну форму о контроли протока. Рутери или одредиште шаљу ову поруку изворишном хосту, тражећи да смањи брзину слања пакета према одредишту. Када се прими порука о стишавању протока, изворишни хост би требало да смањи брзину којом шаље пакете ка одређеној дестинацији док не престане да добија поруке о стишавању протока. Ова порука може бити коришћена од стане рутера или хоста који мора да одбаци пакете због пуног бафера. У том случају ће рутер или хост објављивати поруку о смањењу протока за сваки датаграм који је одбачен. Систем ће упозорити да је дошло до нагомилавања овом поруком када се бафер приближи горњој граници капацитета. У том сличају, датаграм који припада поруци о стишавању протока ће бити успешно испоручен. Ипак, пријем поруке о стишавању протока не говори ништа о испоруци или неиспоруци одговарајућег датаграма.

Рутер шаље **поруку редирекције** хосту који је прикачен на директно повезан рутер да би обавестио хост о бољој рути ка одређемом одредишту.

Ехо поруке и **ехо одзив поруке**

Обезбеђују механизам за тестирање да ли је могућа комуникација између два ентитета. Прималац ехо поруке је обавезан да врати поруку у облику поруке о ехо одзиву. Идентификатор и низ бројева се придружују ехо поруци да би се прилагодила поруци са ехо одзивом. Идентификатор се може користити као приступна тачка сервиса да би се идентификовала одређена сеанса, низ бројева се може инкрементирати сваки пут када се пошаље ехо захтев.

Порука са ознаком времена и **порука са одговором са ознаком времена**

Обезбеђују механизам за одмеравање карактеристике кашњења интернета. Пошиљалац поруке са ознаком времена може да укључи и идентификатор и низ бројева у параметарским пољима и укључи време слања поруке (почетак ознаке времена). Прималац бележи време када је примио поруку и време када је послао поруку са одговором у поруци са одговором са ознаком времена. Ако је порука са ознаком времена послата коришћењем стриктног изворишног рутирања, онда могу бити мерене и карактеристике кашњења одређене руте.

Поруке са захтевом адресне маске и **поруке са одговором са адресном маском**

Корисне су у окружењу са подмрежама. Поруке са захтевом адресне маске и поруке са одговором омогућавају хосту да научи адресну маску за LAN за који је везан. Хост шаље *broadcast* са поруком са захтевом адресне маске на LAN. Рутер на LAN-у одговара са поруком са одговором са адресном маском која садржи адресну маску.

4. ВЕРЗИЈА 6 ИНТЕРНЕТ ПРОТОКОЛА

Интернет протокол (IP) је био темељ Интернета свих међусобно повезаних мрежа. Овај протокол је стигао до краја свог корисног живота, а нови протокол познат као IPv6 (IP верзија 6), дефинисан је како би коначно заменио IP.

У овом раду ће се прво испитати разлог због ког је дошло до развоја нове верзије IP-а, а онда ће бити описани неки његови детаљи.

4.1. НОВА ГЕНЕРАЦИЈА IP-А

Главни разлог за прихватање нове верзије протокола је граница коју је стварала адреса састављена од 32 бита у IPv4. Са 32-битном адресом, по правилу би могло да се додели 2^{32} различитих адреса, што је више од 4 милиона могућих адреса. На први поглед рекло би се да је овај број адреса више него довољан да задовољи потребе адресирања Интернета. Ипак, у касним 80-им назирало се да ће да наступи проблем, и овај проблем је почео да се манифестује у касним 90-им. Разлог због којих је неадекватна 32-битна адреса су следећи:

- Двослојна структура IP адреса (мрежни број и број хоста) је згодна ствар, али исто тако и расипно трошење адресног простора. Када се мрежни број једном додели мрежи, сви бројеви хостова на тој мрежи су аутоматски додељени. Адресни простор за ту мрежу може бити ретко коришћен, али док год се гледају корисне IP адресе, ако се користи мрежни број, онда су искоришћене све адресе у тој мрежи.
- Модел IP адресирања генерално захтева да јединствен мрежни број буде додељен свакој IP мрежи било да је она тренутно везана за Интернет или не.
- Број мрежа расте великом брзином. Многе организације се хвале са више LAN-ова, а не само једним LAN системом. Бежичне мреже веома брзо преузимају велику улогу. Сам интернет је много порастао у претходних неколико година.
- Пораст коришћења TCP/IP у новим областима ће резултирати брзим растом захтева за јединственим IP адресама. Примери укључују коришћење TCP/IP-а за међусобно повезивање терминала тачака-за-продају и за кориснике кабловске телевизије.
- Сваком хосту се додељује по једна IP адреса. Флексибилнији распоред ће дозволити више IP адреса по хосту. Ово, наравно, повећава потребу за IP адресама.

Тако да је потреба за певећаним адресним простором захтевала нову верзију IP-а. Такође IP је веома стар протокол, а нови захтеви у пољима конфигурације адреса, флексибилности рутирања и помоћи у саобраћају су дефинисани.

У одговору на ове потребе, Снага за Послове у Интернет Инжењерингу (The Internet Engineering Tast Force, IETF) тражила је понуде за нову генерацију IP-а (IPng) у јулу 1992. Велики број понуда је био примљен да би 1994. испливао финални нацрт за IPng. Главна *прекретница* је уследила објављивањем RFC

1752, “The Recommendation for the IP Next Generation Protocol”, избаченог у Јануару 1995. RFC 1752 описује захтеве за IPng, даје формат PDU-а и ставља у први план приступ IPng-а према областима адресирања, рутирања и сигурности. Многи други Интернет документи дефинишу детаље протокола, који се сада званично зове IPv6. Ово наравно укључује и крајњу спецификацију IPv6 (RFC 2460), RFC-а који се брине о структури адресирања IPv6 (RFC 2373) и многи други.

IPv6 укључује следећа унапређења у односу на IPv4:

- **Проширен адресни простор:** IPv6 користи 128-битне адресе уместо 32-битних адреса које је користио IPv4. Ово је повећање адресног простора за 2^{96}. Израчунато је да ово омогућава 6 x 10^{23} јединствених адреса по квадратном метру на површини Земље. Чак и ако се адресе невешто додељују, овај адресни простор делује безбедно.
- **Унапређен механизам опција:** Опције IPv6 су смештене у засебна факултативна заглавља која се налазе између IPv6 заглавља и заглавља транспортног слоја. Већина од ових необавезних заглавља не бивају испитана или обрађена од стране рутера на путу пакета. Ово поједностављује и убрзава рутерску обраду IPv6 пакета у односу на IPv4 датаграме. Ово,такође, додатно упрошћава поступак додавања додатних опција.
- **Повећана флексибилност адресирања:** IPv6 укључује концепт *anycast* адресе, до које се пакет испоручује само једним путем. Скалабилност *multicast* рутирања је унапређена тако што је додат опсег поље за *multicast* адресе.
- **Помоћ за додељивања средстава:** IPv6 омогућава означавање пакета за спорији проток ако пошиљалац тражи посебан поступак. Ово укључује помоћ за специјални саобраћај као што је real-time video.

4.2. IPv6 СТРУКТУРА

Један IPv6 пакет има следећу општу форму:

Једино потребно заглавље се односи на IPv6 заглавље. Ово је фиксна величина са дужином од 40 бајтова, у поређењу са 20 бајтова помоћног дела IPv4. Следећа продужена заглавља су дефинисана:

- **Заглавље Hop-by-Hop опција:** Дефинишу специјалне опције које захтевају hop-by-hop процесирање.
- **Заглавље рутирања:** Обезбеђује проширено рутирање, слично изворишном рутирању у IPv4.
- **Заглавље фрагмената:** Садржи информације о фрагментацији и поновном склапању.

- **Заглавље аутентичности:** Овезбеђује интегритет и аутентичност сваког пакета.
- **Заглавље енкапсулације сигурности података:** Обезбеђује приватност.
- **Заглавље одредишних опција:** Садржи факултативне информације које ће испитати одредишни чвор.

У случају када се користи више продужених заглавља, IPv6 препоручује да се редослед заглавља појави у следећем редоследу:

1. IPv6 заглавље: Обавезно, мора увек да буде прво.
2. Заглавље Hop-by-Hop опција
3. Заглавље Дестинационих Опција: За опције које ће бити обрађене од стране првог одредишта које се појављује у пољу IPv6 Одредишне Адресе плус накнадних одредишта која су набројана у заглављу рутирања.
4. Заглавље рутирања
5. Заглавље фрагмената
6. Заглавље аутентичности
7. Заглавље енкапсулације сигурности податка
8. Заглавље одредишних опција: За опције које ће бити обрађене само у крајњем одредишту пакета.

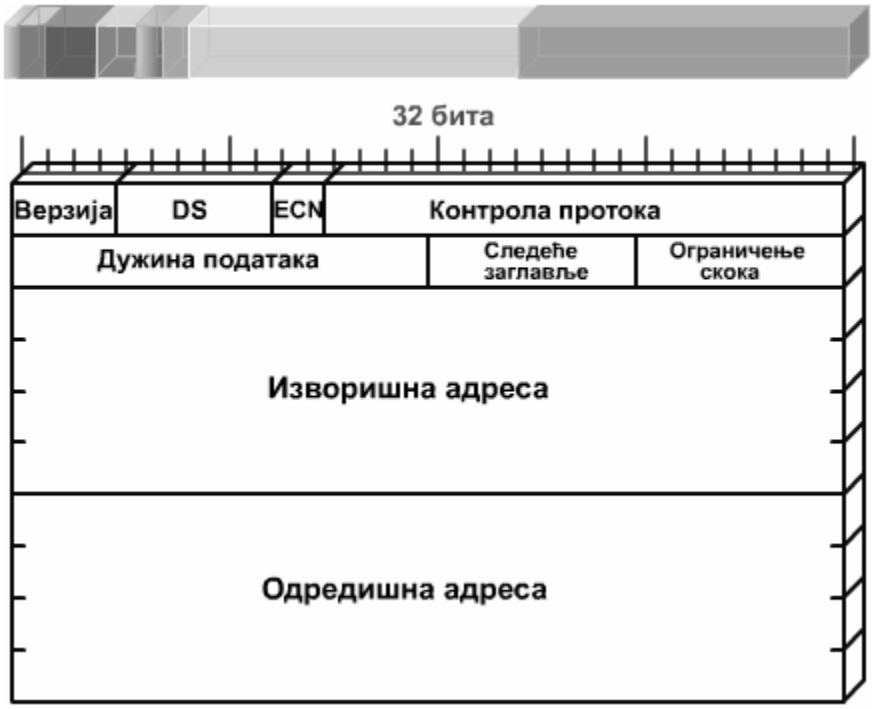
Слика 4.1 IPv6 пакет са продуженим заглављима

Слика 4.1 приказује пример пример једног IPv6 пакета који укључује део сваког заглавља осим оних која су повезана са сигурношћу. IPv6 заглавље и свако продужено заглавље садрже поље Следеће Заглавље. Ово поље идентификује тип следећег заглавља. Ако је следеће заглавље једно од продужених заглавља, онда ово поље садржи идентификатор типа тог заглавља. У противном, ово поље садржи идентификатор протокола за

протокол вишег слоја који користи IPv6 (обично протокол транспортног слоја), користе се исте величине као и поља IPv4 протокола. На слици 4.1, протокол вишег слоја је TCP, тако да се подаци виших слојева које носи IPv6 пакет садрже од заглавља TCP-а које прати блок апликационих података.

Прво ћемо се позабавити главним IPv6 заглављем, а онда ћемо испитати сваки од продужених заглавља по реду.

4.3. IPv6 ЗАГЛАВЉЕ



Слика 4.2 Формат IPv6 заглавља

IPv6 заглавље има фиксну дужину од 40 бајтова (окета), а састоји се од следећих поља (слика 4.2):

- **Верзија (4 бита):** Верзија интернет протокола, вредност је 6.
- **DS/ECN (8 бита):** У претходном опису сервиса, ово поље се односило на поље ***Traffic Class*** и било је резервисано за употребу од стране почетних чворова и/или прослеђујућих рутера да би се идентификовало и разликовало између различитих класа приоритета IPv6 пакета. Првих шест бита поља Класа Саобраћаја сада се односне на поље DS (differentiated services), а осталих 2 бита су резервисана за поље ECN (explicit congestion notification).
- **Ознака тока (20 бита):** Може бити коришћено од стране хоста да обележи оне пакете са којима рутери треба да посебно поступају у оквиру мреже.
- **Дужина података (16 бита):** Дужина остатка IPv6 пакета који прати заглавље, у октетима. Другим речима, ово је комплетна дужина свих продужених заглавља плус дужина PDU-а транспортног нивоа.
- **Следеће заглавље (8 бита):** Идентификује тип заглавља које прати IPv6 заглавље. Ово може бити и IPv6 продужено заглавље или заглавље вишег слоја, као што је TCP или UDP.

- **Ограничење скоко (8 бита):** Преостали број дозвољених скокова за овај пакет. Ограничење скокова је постављено на жељену максималну величину од стране изворишта и декрементира се од стране сваке тачке која прослеђује пакет. Пакет се одбацује када вредност овог поља постане нула. Ово је поједностављен поступак у односу на поступак који треба да се обави са пољем дужине живота код IPv4. Сагласност је била да додатни напор у обрачуну временских интервала у IPv4 није донео никакву значајну вредност протоколу. У ствари, IPv4 рутери, као главно правило, третирали су TTL поље као поље ограничења скока.
- **Изворишна адреса (128 бита):** Адреса творца пакета.
- **Одредишна адреса (128 бита):** Адреса одређеног примаоца пакета. Ово не мора, у суштини, да буде крајња одредишна адреса ако је присутно заглавље рутирања.

Иако је IPv6 заглавље дуже него обавезно IPv4 заглавље (40 октета према 20 октета), оно садржи мање поља (8 према 12). Према томе, рутери имају да одраде мање посла при заглављу, што убрзава рутирање.

Ознака тока

IPv6 стандард дефинише ток као последицу слања пакета са одређеног изворишта ка одређеном одредишту (unicast или multicast) при коме изворište тражи да интервентни рутери са пакетом посебно поступају. Ток је јединствено дефинисан тако што се комбинују изворишна и одредишна адреса са 20-битном ознаком протока која није нула. Стога, изворište додељује исту ознаку тока свим пакетима који су део истог тока.

Гледано из угла изворишта, ток је, у суштини, низ пакета које је генерисао један део апликације у изворишту, а која има исте захтеве транспортног сервиса. Ток може обухватати једну TCP конекцију или чак више TCP конекција. Једна апликација може да генерише један ток или више токова. Пример два тока је мултимедијални састанак, који може да има један ток за звук и други за графику, сваки са другачијим зехтевима трансфера у погледу преноса података, кашњења или одступања од кашњења.

Ако се погледа из угла рутера, ток је низ пакета који деле атрибуте који утичу на то како ће се рутер понашати према овим пакетима. То убраја пут, додељивање средстава, захтеве одбацивања, обрачун и атрибуте сигурности. Рутер може другачије да се понаша према пакетима који нису са истог тока, укључујући додељивање другачијег простора у баферу, давањем другачијег првенства у случају прослеђивања и захтевом за другачијим квалитетом услуге од стране мрежа.

Не постоји посебан значај било које ознаке тока. Уместо тога, да би се обезбедио специјални поступак ток се мора објавити на неки други начин. На пример, изворište може да преговара са рутером или затражи од рутера специјали поступак испред времена на помоћу контролног протокола или у току трансмисије тако што ће поставити информацију у једно од продужених заглавља у пакету, као што је рецимо заглавље Hop-by-Hop опција. Примери специјалног поступка који могу бити затражени укључују неку врсту не стандардног квалитета сервиса и неку врсту сервиса у реалном времену.

У начелу, сви кориснички захтеви за одређеним током могу бити дефинисани у продуженом заглављу и укључени у сваки пакет. Ако желимо да

оставимо концепт тока отворен да би се укључило мноштво захтева, овај план приступа могао би резултирати у веома великим заглављима пакета. Алтернатива, усвојена за IPv6, је ознака тока, у којој су захтеви тока дефинисани пре почетка тока и јединствена ознака тока је додељена току. У овом случају рутер мора да сачува информације захтева тока о сваком току.

Следећа правила важе за ознаке тока:

1. Хостови или рутери који не подржавају поље Ознаке Тока морају да поставе поље на нулу када праве пакет, спроведу поља непромењена при прослеђивању пакета и игноришу поља када приме пакет.
2. Сви пакети који су произведени у датом изворишту са истом ненултом Ознаком Тока морају да имају исту Одредишну Адресу, Изворишну Адресу, садржину заглавља Hop-by-Hop опција (ако је заглавље присутно) и садржај заглавља Рутирања (ако је ово заглавље присутно). Сврха је та да рутер може да обради пакет тако што ће једноставно погледати ознаку тока у табели без испитивања осталих заглавља.
3. Изворište додељује току ознаку тока. Нова ознака тока мора бити изабрана (привидно) случајно и уједначено у опсегу од 1 до 2^{20}-1, под условом да изворište не искористи поново ознаку тока за нови ток док је постојећи ток у животу. Нула Ознака Тока је резервисана да назначи да се не користи ни једна ознака тока.

Ова последња тачка захтева мало разраде. Рутер мора да пружи неке информације о карактеристикама сваког активног тока који пролази кроз њега, вероватно у некој врсти табеле. Да би успешније и брже проследио пакет, поглед на табелу мора бити бржи. Једна алтернатива је да има табелу са 2^{20} (око милион) тачака, једна за сваку могућу ознаку тока што намеће непотребни меморијски терет рутеру. Још једна алтернатива је имати једну тачку у табели по активном току, укључити ознаку тока у сваку тачку, и тражити од рутера да претражује табелу сваки пут када наиђе пакет. Ово рутеру намеће непотребни терет при обради. Уместо тога, многи рутери користе неку врсту мешане табеле. Са оваквим приступом користе се табеле умерене величине и сваки ток се уврштава у табелу користећи функцику за меланзирање над ознакаам токова. Меланзна функција може једноставно бити неколико најмање значајних бита (рецимо 8. или 10.) ознаке тока или једноставно рачунање над 20 бита ознака токова које су уједначено дељене на њихове могуће опсеге. Одавде захтев број 3 у претходној листи.

4.4. IPv6 АДРЕСЕ

IPv6 адресе су дугачке 128 бита. Адресе се додељују појединачним интерфејсима на чворовима, а не чворовима лично. Појединачни интерфејс може да има вишеструку unicast адресу. Било која од unicast адреса повезана са чворним интерфејсом може бити искоришћена како би јединствено представила тај чвор.

Комбинација дугих адреса и вишеструких адреса по интерфејсу омогућава ефикасније рутирање у односу на IPv4. У IPv4, адреса генерално нема конструкцију која помаже рутирању и због тога рутер мора да води велику табелу путања рутирања. Дуже интернет адресе дозвољавају велики број адреса од стране хијерархија мрежа, добављача приступа, географије,

предузећа итд. Такав број би требало да учини да табеле рутирања буду мање, а преглед табела бржи. Допуштање вишеструких адреса по интерфејсу би тренало да обезбеди претплатнику који користи вишеструке добављаче приступа по истом интерфејсу да има одвојену адресну гомилу код сваког добављача.

IPv6 дозвољава три типа адреса:

- **Unicast:** Идентификатор за један интерфејс. Пакет послат unicast адреси се испоручује интерфејсу који је идентификован том адресом.
- **Anycast:** Идентификатор за сет интерфејса (који припадају различитим чворовима). Пакет послат anycast адреси се испоручује неком од интерфејса који је идентификован том адресом (најближем, гледајући по протоколу рутирања).
- **Multicast:** Идентификатор за сет интерфејса (који припадају различитим чворовима). Пакет послат multicast адреси се испоручује свим интерфејсима који су идентификовани том адресом.

4.5. ЗАГЛАВЉЕ HOP-BY-HOP ОПЦИЈА

Заглавље Hop-by-Hop опција носи факултативне информације које, уколико је ово поље присутно, морају бити испитане од стране сваког рутера који се налази на путањи. Ово поље се састоји од следећих поља (слика 4.3):

- **Следеће Заглавље (8 бита):** Идентификује тип заглавља које иде одмах иза овог заглавља.
- **Дужина продужености заглавља (8 бита):** Дужина овог заглавља исказана у јединицама од 64 бита, не укључујући првих 64 бита.
- **Опције:** Поље променљиве дужине које се састоји од једне или више дефиниција опција. Свака дефиниција је састављена од три подпоља: Тип Опције (8 бита), које идентификује опцију; Дужина (8 бита), које одређује дужину поља Опције Података у бајтовим; и Опције Података, које је спецификација опција променљиве дужине.

Слика 4.3 Hop-by-Hop опције

У ствари користе се најнижих пет битова да би се описала нека одређена опција. Највиша два бита указују на то која ће се акција применити од стране чвора који који не препознаје овај тип опција, то су следеће акције:

- 00 – Прескочи ову опцију и настави са обрадом заглавља.
- 01 – Одбаци пакет.
- 10 – Одбаци пакет и пошаљи ICMP поруку о проблему са параметима пекетовој изворишној адреси, показујући на не препознавање типа опција.
- 11 – Одбаци пакет и само ако одредишна адреса није multicast адреса, пошаљи ICMP поруку о проблему са параметрима изворишној адреси пакета, показујући на непрепознатљив тип опција.

Трећи највиши бит специфицира да ли се поље Опција Података не мења (0) или се може мењати (1) на рути од извориштa до одредиштa. Подаци који се могу мењати морају бити искључени из рачунања аутентичности.

Договор за Тип Опција се односи и на заглавље Дестинационих Опција.

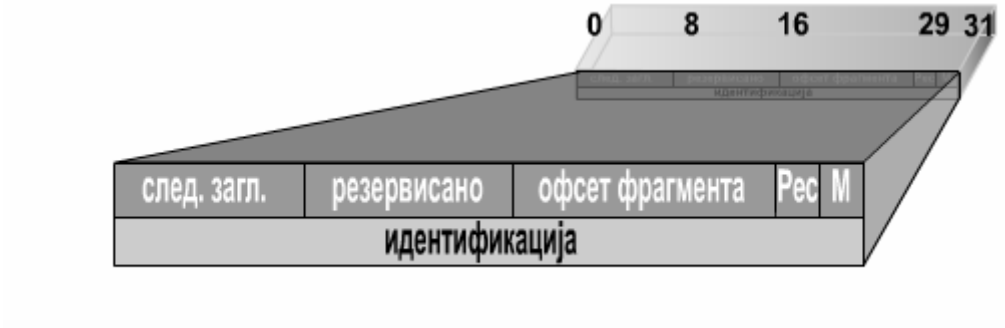
Четири hop-by-hop опција је тренутно одређено:

- **Подметач 1:** Користи се да би се предео заглавља са Опцијама напунио са једним бајтом.
- **Подметач N:** Користи се да би се предео са Опцијама напунио са N ($N \geq 2$) бајтова. Два пуњења уверавају да заглавље има више од 8 бајтова дужине.
- **Огроман Користан Терет:** Користи се да би се послао IPv6 пакет са теретом који је дужи од 65 535 октета. Поље Опција Података ове опције је дугачко 32 бита и даје дужину пакета у октетима, укључујући IPv6 заглавље. За такве пакете, поље Дужина Података у IPv6 заглављу мора бити постављено на нулу и не сме бити присутно заглавље фрагмената. Са овом опцијом, IPv6 подржава величине пакета до 4 милиона бајта. Ово олакшава пренос великих видео пакета и омогућава IPv6 да најбоље искористи постојећи капацитет транмисионог медијума.
- **Упозоравање рутера:** Информише рутер да је садржај пакета користан за рутер и да треба руковати било којом контролом података на тај начин. Изостанак ове опције у IPv6 датаграму информише рутер да пакет не садржи информације које требају рутеру, па стога пакет може бити безбедно рутиран без даљег рашчлањивања пакета. Хостови који производе IPv6 пакете треба да укључе ову опцију под одређеним условима. Циљ ове опције је да обезбеди ефикасну помоћ протоколима као што су RSVP, који производе пакете који треба да буду испитани од стране успутних рутера за сврху контроле саобраћаја. Уместо да се зехтева од међу-рутера да гледају детаље продужених заглавља пакета, ова опција говори рутерима када је тако нешто потребно.

4.6. ЗАГЛАВЉЕ ФРАГМЕНТА

У IPv6, фрагментацију могу одрадити само изворишне тачке, а не рутери који се налазе на путу пакета. Да би искористила комплетне предности међуумрежавања, изворишна тачка мора применити алгоритам за откривање пута, који јој омогућава да сазна која је најмања максимална трансмисиона јединица (Maximum Transmission Unit – MTU), коју подржава нека од мрежа на

путу пакета. Знајући која је најмања MTU изворишна тачка ће фрагментовати, као што се од ње тражи, за сваку дату одредишну мрежу. У супротном, изворište мора да ограничи све пакете на 1280 бајтова, који је максимални MTU који мора да подржи свака мрежа.



Слика 4.4 Заглавље фрагмената

Заглавље фрагмента се састоји од следећих поља (слика 4.4):

- **Следеће Заглавље (8 бита):** Идентификује тип заглавља које је одмах после овог залавља.
- **Резервисано (8 бита):** За будућу употребу.
- **Офсет Фрагмената (13 бита):** Показује где у оригиналном пакету је место корисном делу овог фрагмента. Мери се у јединицама од 64 бита. Ово значи да фрагмент (другачији од претходног фрагмента) мора да садржи поље података које је дуже од 64 бита.
- **Рес (2 бита):** Резервисано за будућу уптребу.
- **М флег (1 бит):** 1 = још фрагмената; 0 = последњи фрагмент.
- **Идентификација (32 бита):** Служи да јединствено идентификује оригинални пакет. Идентификатор мора бити јединствен за изворишну и одредишну адресу пакета за време док је пакет у инетрнету. Сви фрагменти са истим идентификатором, изворишном адресом и одредишном адресом се поново склапају како би се направио оригинални пакет.

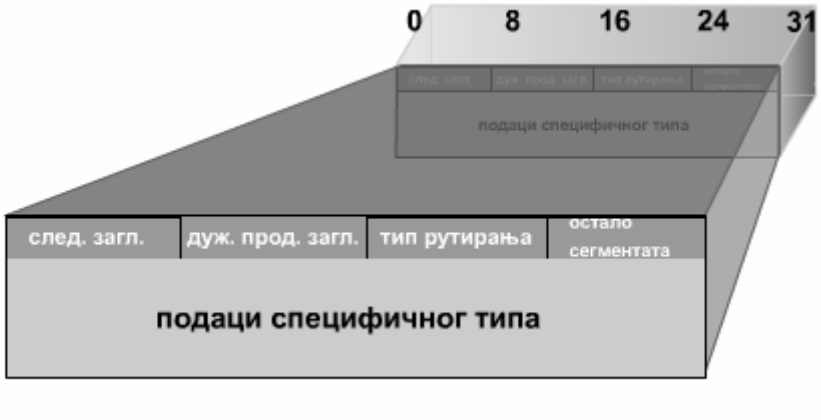
Алгоритам фрагментације је исти као што је описано раније.

4.7. ЗАГЛАВЉЕ РУТИРАЊА

Заглавље рутирања садржи листу једног или више успутних чворова које треба посетити на путу до одредишта пакета. Сва заглавља рутирања почињу 32-битним блоком који се састоји од четири 8-битних поља, праћена од стране података рутирања који су специфични за одређени тип рутирања (слика 4.5). Четири 8-битна поља су следећа:

- **Следеће Заглавље:** Идентификује тип заглавља одмах после овог залавља.
- **Дужина продужености заглавља:** Дужина овог заглавља исказана у јединицама од 64 бита, не укључујући првих 64 бита.
- **Тип Рутирања:** Идентификује одређену варијанту заглавља рутирања. Ако рутер не препозна вредност типа рутирања, он мора да одбаци пакет.

- **Остало Сегмената:** Број преосталих сегмената рутирања; то је број јасно набројаних међу-чворова које јпакет мора да посети пре доласка до одредишта.



Слика 4.5 Заглавље рутирања

Једино специфично заглавље рутирања које је дефинисано RFC-ом 2460 је заглавље рутирања Тип 0. Када се користи Тип 0 заглавља рутирања, изворишна тачка не поставља крајњу одредишну адресу у IPv6 заглавље. Уместо тога, адреса је она која је последња у листи адреса у заглављу рутирања, а IPv6 заглавље садржи адресу првог жељеног рутера на траси. Заглавље рутирања неће бити испитивано док пакет не дође до тачке коју је наведена од стране IPv6 заглавља. У тачки, садржаји заглавља рутирања и IPv6 заглавља се ажурирају и пакет се прослеђује даље. Ажурирање се састоји од постављања следеће адресе коју треба посетити у IPv6 заглавље и декрементирању поља Остало Сегмената у заглављу рутирања.

4.8. ЗАГЛАВЉЕ ОДРЕДИШНИХ ОПЦИЈА

Заглавље Одредишних Опција, носи факултативне информације које, уколико је заглавље присутно, испитује само одредишна тачка пакета. Формат овог заглавља је исти као и формат заглавља Hop-by-Hop опција. (слика 4.3).

5. ЗАКЉУЧАК

На основу свега до сада изложеног, може се закључити да Интернет Протокол омогућава и олакшава комуникацију између разноврсних мрежа што га чини ослонцем целог Интернета. Интернет протокол (IP) је био темељ Интернета и свих међусобно повезаних мрежа дуги низ година. Овај протокол је стигао до краја свог корисног живота, а нови протокол познат као IPv6 (IP верзија 6), дефинисан је како би коначно заменио IP. По свему судећи нови протокол ће наћи велику примену у систему међусобно повезаних мрежа због својих револуционарних решења за проблеме које је иза себе оставио IP. У те проблеме као прво спада недостатак адресног простора, а затим и спорост у преносу података.

Сада само остаје да се сачека долазак и глобална имплементација протокола како би се уверили у његове могућности.

6. ИНДЕКС ПОЈМОВА

WAN Wide Area Network

LAN Local Area Network

IP Internet Protocol

PDU Protocol Data Unit

MAC Medium Access Control

LLC Logical Link Control

TCP Transport Control Protocol

ICMP Internet Control Message Protocol

SAP Service Access Point

UDP User Datagram Protocol

7. ЛИТЕРАТУРА

1. Computer Networks, Andrew S. Tanenbaum, 1996
2. Computer Networking & Internet Protocols, William Stallings,1996
3. **http://www.cisco.com**
4. **http://www.rfc-editor.org**
5. **http://www.iana.org**