ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

МД	мережа доступу;
AIMD	(Additive-increase/multiplicative-decrease) алгоритм адитивного збільшення / мультиплікативного зменшення;
AS	(Autonomous Systems) автономна система;
ATM	(Asynchronous Transfer Mode) асинхронний спосіб передачі даних;
BGP	(Border Gateway Protocol) протокол граничних маршрутизаторів;
CAMEL	(Customised Applications for Mobile networks Enhanced Logic) набір стандартів, що реалізують інтелектуальні послуги;
CLNP	(Connection Less Network Protocol) мережевий протокол без встановлення з'єднання;
EGP	(Exterior Gateway Protocols) зовнішні протоколи маршрутизації;
FDDI	(Fiber Distributed Data Interface) волоконно-оптичний розподілений інтерфейс передачі даних;
FTP	(File Transfer Protocol) протокол передачі даних;
3GPP	(3-rd Generation Partnership Project) консорціум, який розробляє специфікації для мобільної телефонії;
HSS	(Home Subscriber Server) сервер абонентських даних;
ICMP	(Internet Control Message Protocol) протокол міжмережевих керуючих повідомлень;
IGP	(Interior GatewayProtocols) протоколи внутрішнього шлюзу;
IMS	(IP Multimedia Subsystem) специфікація передачі мультимедійного вмісту на основі протоколу IP;
INAP	(Intelligent Network Application Protocol) прикладна частина інтелектуальної мережі;
IP	(Internet Protocol) Інтернет протокол;
ISDN	(Integrated Services Digital Network) цифрова мережа з інтегрованими послугами;

IS-IS	(Intermediate System to Intermediate System) відкритий протокол маршрутизації;
ITU-T	(International Telecommunication Union — Telecommunication sector) підрозділ Міжнародного союзу електрозв'язку;
NGN	(Next Generation Networks) мережі наступного покоління;
OSI	(Open systems interconnection basic reference model) базова еталонна модель взаємодії відкритих систем;
OSPF	(Open Shortest Path First) протокол пошуку найкоротшого шляху;
PPP	(Point-to-Point Protocol) протокол точка-точка;
RIP	(Routing Information Protocol) протокол передачі маршрутної інформації;
RFC	(Request for Comment) документ із серії пронумерованих інформаційних документів Інтернету;
RTP	(Realtime Transport Protocol) протокол реального часу;
SIP	(Session Initiation Protocol) протокол встановлення сеансу;
SMTP	(Simple Mail Transfer Protocol) простий протокол пересилання пошти;
SNMP	(Simple Network Management Protocol) простий протокол керування мережею;
SLIP	(Serial Line Internet Protocol) мережевий протокол доступу до мереж стека TCP/IP;
Softwitch	програмний комутатор;
SYN	(Synchronize sequence numbers) синхронізація номерів послідовності;
TCP/IP	(Transmission Control Protocol / Internet Protocol) набір протоколів мережі Інтернет;
TDM	(Time Division Multiplexing) мультиплексування з поділом за часом;
UDP	(User Datagram Protocol, UDP) протокол дейтаграм користувача;
X.25.	сімейство протоколів канального рівня мережевої моделі OSI.

ВСТУП

Internet - найбільша глобальна комп'ютерна мережа, що зв'язує десятки мільйонів абонентів у більш як 150 країнах світу. Щомісяця її поширеність зростає на 7-10%. Такий шалений успіх, в першу чергу, обумовлений високою стійкістю сімейства протоколів TCP/IP до змін і його здатністю адаптуватися до основних мережних технологій.

Стрімкий розвиток Інтернету, мобільного зв'язку та зростаючі потреби користувачів в інфокомунікаційних послугах спонукали світове телекомунікаційне співтовариство висунути нову телекомунікаційну парадигму - мережі наступного покоління NGN, основою яких є пакетні технології передачі різних видів інформації.

NGN (Next Generation Network - мережа наступного покоління) - це мультисервісна мережа телекомунікацій, яка підтримує інтеграцію послуг передавання мови, даних і мультимедіа та базується на IP-мережі. Головна різниця між традиційною мережою та мережою наступного покоління полягає в поділу всієї цирклюючої в мережі інформації на дві слкладові – дані користувача та сигнальну інформацію. Безпосередньо дані коритувача містять корисну інформацію для абонента, наприкад відео, голос, дані. Сигнальна ж інформація забезпечує комутацію абонентів та надання послуг. Шляхи проходження даних користувача та сигнальних повідомлень можуть не збігатися.

Інфокомунікаційні послуги мають швидкий ріст розвитку, тому архітектура NGN, в межах єдиної інфраструктури, об'єднує ресурси мережі Інтернет, телефонні мережі загального користування (ТмЗК), мобільний зв'язок, телефонію по IP-протоколу. Відмінність концепції NGN, від раніше реалізованих мережних інфраструктур, полягає в переході до принципово іншої функціональної моделі. У стандартній ТмЗК головними функціональними компонентами були вузли комутації різного рівня і вузли доступу. При цьому обладнання вузла комутації могло одночасно виконувати декілька завдань: обробку виклику, комутацію потоків призначеної для користувача інформації і

надання послуг. Розвиток класичної ТФЗК, пов'язаний, перш за все, з появою технології ISDN, дозволивши розділити функції комутації потоків призначеної для користувача інформації і обробки сигналізації.

Щодо концепції NGN, то їй притаманний чіткий розподіл трьох рівнів з'єднання. Кожному з рівнів відповідає своє функціональне завдання. Так на транспортному рівні відбувається комутація і передача мовної інформації, на рівні сигналізації - передача інформації сигналізації, а рівень послуг призначений для надання послуг, відмінних від базових. При цьому між рівнями визначені інтерфейси, які є об'єктом стандартизації. Отримавши подібну незалежність один від одного, рівні надалі можуть розвиватися самостійно. Більш того, з точки зору адміністративного розподілу мережі може ставитися питання проте, аби послуги різних рівнів надавалися різними операторами.

TCP (Transmission Control Protocol) - основний протокол Інтернету. Він представляє собою набір синтаксичних і семантичних правил, які використовуються при обміні даними між двома комп’ютерами. З його допомогою, ми можемо описати процес обміну даними не прив’язуючись до якоїсь конкретної комп’ютерної платформи чи мережевому обладнанню конкретного виробника. Протокол TCP надає транспортні послуги, що відрізняються від послуг UDP. Замість ненадійної доставки датаграм без встановлення з'єднань, він забезпечує гарантовану доставку з встановленням з'єднань у вигляді байтових потоків. Він використовується в тих випадках, коли потрібна надійна доставка повідомлень.

Боротьба з перевантаженнями в мережі , коли виникають затори з пакетів – це одне із головних завдань протоколу TCP. Для контролю таких ситуацій здійснюється взаємне підстроювання швидкості відправки запитів. Попередньо встановивши з’єднання, механізм TCP надає потік даних, в разі втрати даних здійснює повторний запит даних і усуває дублювання при отриманні двох копій одного пакета. Таким чином TCP, на відміну від UDP, гарантує цілісність переданих даних і повідомлення відправника про результати передачі.

Суттєвим і важливим питанням для провайдера і оператора телекомунікацій є управління потоком в мережах NGN. TCP використовує протокол із змінним вікном (sliding window), тобто форму управління потоком даних, що дозволяє відправнику передати декілька пакетів, перед тим як він зупиниться і буде чекати підтвердження. А так як відправник не повинен чекати підтвердження кожного разу після відправки пакета, то дані передаються швидше. В данній роботі проводиться дослідження, пов’язані з ефективним управлінням потоком з застосуванням розподілених механізмів управління за протоколом TCP/IP.

З'єднання і взаємодія в рамках однієї потужної комп'ютерної мережі стало метою проектування і створення сімейства протоколів, названих надалі стеком протоколів TCP / IP. Головною ідеєю стека є створення механізму мережевого обміну.

TCP / IP - це загальна назва, присвоєна сімейству протоколів передачі даних, що використовуються для зв'язку комп'ютерів та іншого обладнання в мережі. Фактично TCP / IP являється стеком мережі NGN з іншими мережами і управляє всім потоком даних які передаються в мережі тому він такий важливий.

1 ВИЗНАЧЕННЯ Й ХАРАКТЕРИСТИКА ОСНОВНИХ МОЖЛИВОСТЕЙ МЕРЕЖ NGN

1.1 Фактори розвитку технології NGN

Спершу для передачі різних типів інформації будувалися окремі мережі зв'язку: телефонна мережа, телеграфна мережа, мережі передачі даних та ін. У другій половині XX століття виникла ідея об'єднати всі відомчі мережі зв'язку в одну. Таким чином була створена концепція мереж ISDN. ТмЗК стала мережею, що об'єднує ISDN-мережі.

В кінці XX століття відбулася інтеграція між телефонною мережею і мережею передачі даних, яка зумовила якісний стрибок у зміні концепції послуг зв’язку технології ISDN.

Сьогодні розвиток інфокомунікаційних послуг здійснюється, в основному, в рамках мережі Інтернет, де доступ до послуг виконується через традиційні мережі зв'язку. Мобільність та гнучкість мережі, гарантована якість послуг та незалежність від способів доступу мають задовольняти основні вимоги інфокомунікаційних послуг.

Нажаль, більшість послуг Інтернет не відповідають сучасним вимогам, що пред'являються до послуг інформаційного суспільства. У зв'язку з цим актуальною стає задача побудови універсальних мереж, які могли б так само ефективно надавати послуги різних типів. Прогрес у розвитку елементної бази та технологій передачі, поява нових можливостей, а також зростаючий потік користувачів в інтернет-телефонію – все це висунуло нові вимоги до мереж зв'язку і до організації бізнесу телекомунікаційними компаніями.

Беручи до уваги особливості інфокомунікаційних послуг, були висунуті наступні вимоги до перспективних мереж зв'язку:

– інтелектуальність, тобто можливість управління послугою, викликом і з'єднанням з боку користувача або постачальника послуг;

– широкосмуговість, тобто можливість гнучкої і динамічної зміни швидкості передачі інформації в широкому діапазоні залежно від поточних потреб користувача;

– мультисервісність, тобто незалежність технологій надання послуг від транспортних технологій;

– мультимедійність, тобто здатність мережі передавати багатокомпонентну інформацію (мова, дані, відео, аудіо) з необхідною синхронізацією цих компонентів у реальному часі і використанням складних конфігурацій з'єднань;

– інваріантність доступу, тобто можливість організації доступу до послуг незалежно від використовуваної технології;

– багатооператорність, тобто можливість участі декількох операторів в процесі надання послуги і розділення їх відповідальності відповідно до області діяльності.

Тому загальноприйнятою стала концепція мереж наступного покоління NGN. Перехід від цифрових мереж зв'язку до концепції NGN зробило революцію в сучасних послугах, оскільки третій вимір приніс передачу відеосигналів. На відміну від мереж ISDN, які базувалися на ТмЗК, мережі NGN опираються на передачу даних на базі IP-протоколу.

Впровадження NGN дозволяє виробляти модернізацію та розширення місцевих мереж зв'язку найбільш ефективним і економічним способом. За рахунок використання єдиної транспортної мережі IP і застосування нового принципу організації зв'язку, мережа NGN вимагає менших інвестицій при будівництві. Замість прийнятої в традиційних телефонних мережах канальної комутації, в NGN реалізується принцип організації віртуальних з'єднань, за якими здійснюється доставка сервісів кінцевому користувачеві в мережі IP.

Сутність мережі нового покоління полягає у переході від багатоплатформності до простої та ефективної мережі, розробленої спеціально

для того, щоб надавати всі види послуг. У результаті можна одержати мережі, що пристосовані до всіх видів послуг.

1.2 Структура NGN

Структура за концепцією ITU-T

Сектор стандартизації електрозв'язку ITU-T запропонував особливу модель NGN, яка полягає в функціональному розподілу на два рівні: послуг і транспортний (рис. 1.1). Це дозволяє розвивати сервіси управління послугами, транспортні і прикладні сервіси незалежно один від одного.

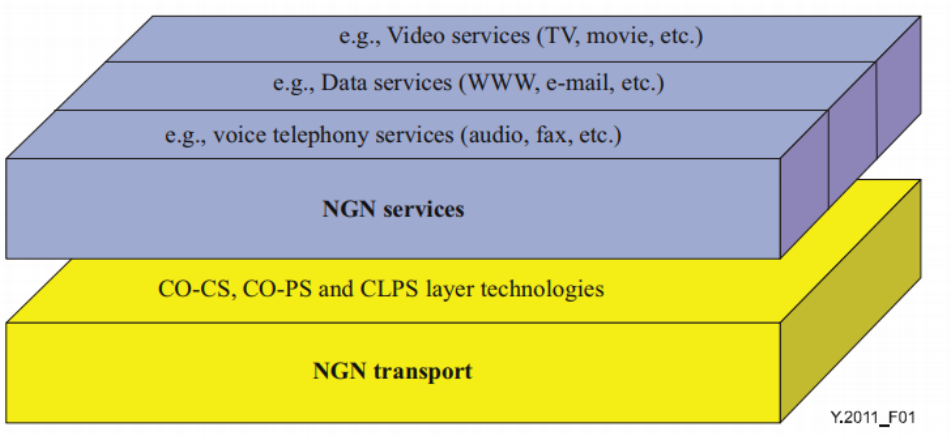

Рисунок 1.1. Розподіл функціональності послуг і транспорту

Транспортний рівень забезпечує виконання функції доставки інформації будь-якого типу між будь-якими двома географічно рознесеними терміналами. В транспортний рівень входять набори різних площин, які відносяться до трьох нижніх рівнів еталонної моделі взаємодії відкритих систем (OSI). Таким чином, транспортні функції надають можливість з'єднання двох мереж різної архітектури. У загальному випадку, згідно рекомендаціям МСЕ-Т G.805 і G.809, на транспортному рівні може використовуватися довільна технологія комутації пакетів , що включає передачу даних з комутацією пакетів (CO-PS), передачу даних з комутацією каналів (CO-CS) та пакетну передачу інформації без встановлення з'єднання (CLPS).

Однак ITU-T вважає, що технологія IP є кращою для організації транспорту в NGN, оскільки використання технологій IP/MPLS у середовищі Ethernet дозволяє підвищити масштабованість і якість обслуговування до рівня, необхідного для транспортних мереж.

Організація передачі мови, відеопослуги (включаючи перегляд фільмів і телевизійних програм), послуги з передачі даних (Web-послуги), або їхні комбінації (відеотелефонія або ігри) – всі ці прикладні функції реалізує рівень послуг. На рис. 1.1 наведено приклади послуг мереж наступного покоління.

З точки зору архітектури передбачається, що кожен шар містить один або кілька рівнів. Рівень складається з трьох площин:

- площина користувача;
- площина управління;
- площина менеджменту.

На рис. 1.2 наведена базова еталонна модель NGN за Рекомендацією ITU-T Y.2011.

Рисунок 1.2. Базова еталонна модель NGN

В функціональній моделі NGN ITU виділяє три категорії об'єктів: функції, сервіси та ресурси. Сервіси реалізуються різними функціями за допомогою доступних ресурсів. Один і той же сервіс може реалізовуватися різним набором функцій і навпаки, одна функція може використовуватися для реалізації різних сервісів. Для зручності всі ці функції було об’єднано в дві окремі площини. Так

в одну включили всі функції управління, а в іншу - всі функції менеджменту послуг. Групування функцій дозволяє визначити функціональні взаємозв'язки у межах даної групи, а також інформаційні потоки між функціями в даній групі. На рис. 1. 3 наведена узагальнена функціональна модель NGN.

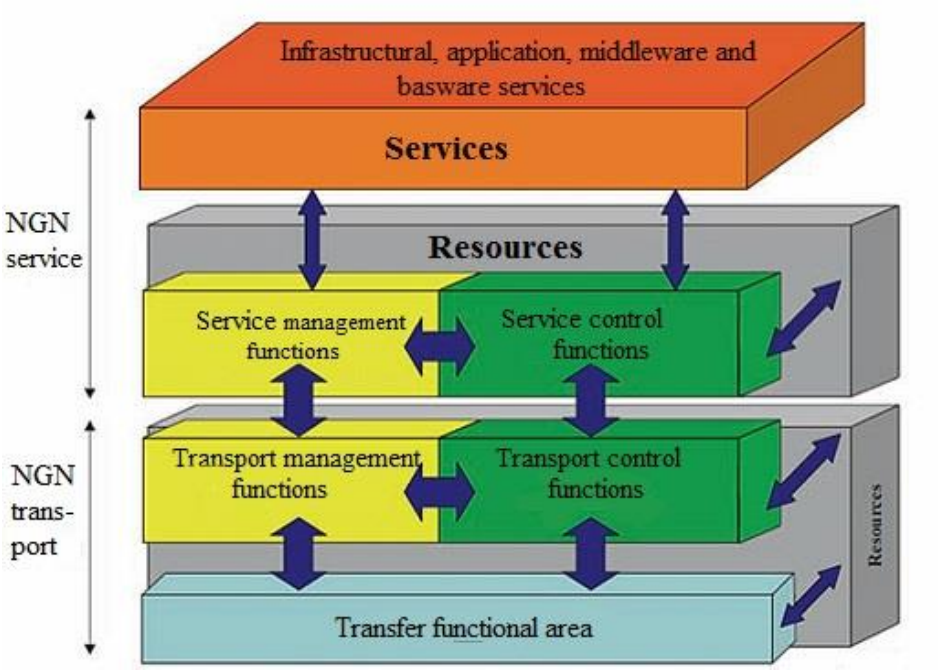

Рисунок 1.3. Узагальнена функціональна модель NGN

Ресурси повної моделі NGN повинні бути незалежні від функцій та послуг.

Функції транспорту повинні зберігати незалежність від відповіднихфункцій управління і менеджменту. Транспортна мережа повинна передавати як інформацію користувача, так і мережну інформацію.

Структура за чотирирівневою моделлю

Для підвищення ефективності операторської діяльності та надання відкритих інтерфейсів стороннім розробникам застосовується площинна архітектура мереж NGN. Незважаючи на рекомендації ITU-T, на практиці нині застосовується чотирирівнева архітектура NGN.

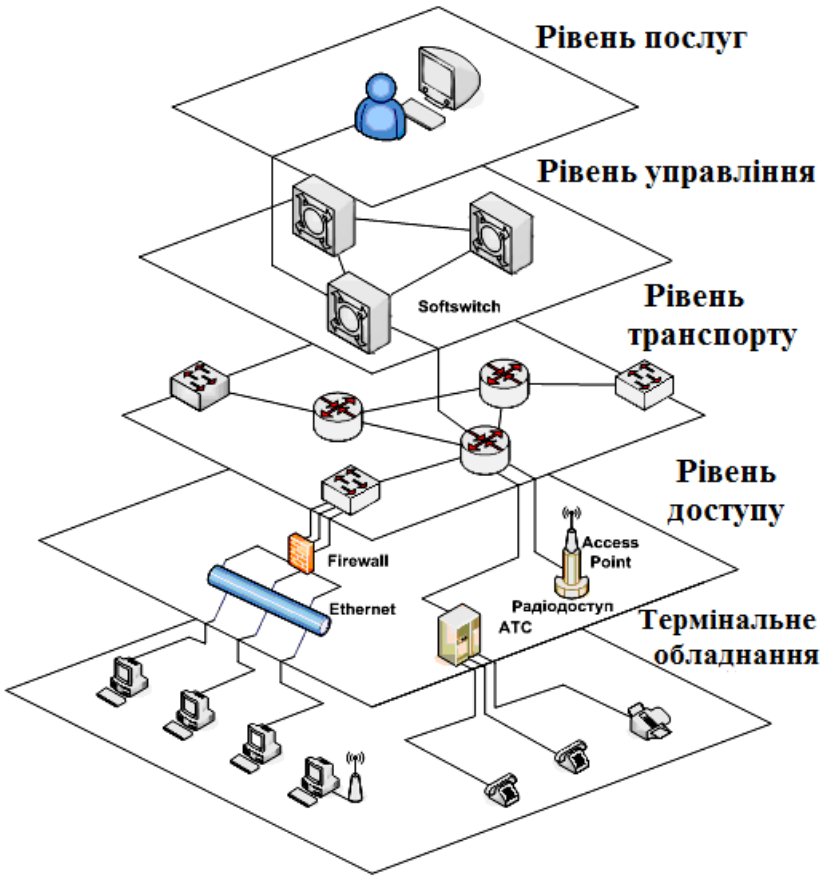

Рисунок 1.4. Чотирирівнева архітектура мережі наступного покоління

Рівень послуг і транспортний рівень еталонної моделі NGN в свою чергу поділилися на такі рівні:

- рівень доступу A (Access) - перший рівень;
- рівень транспорту T (Transport) – другий рівень;
- рівень управління C (Control) – третій рівень;
- рівень послуг S (Service) – четвертий рівень.

Рівень А забезпечує доступ користувачам до ресурсів мережі. До нього належать шлюзи, вузли агрегування доступу та мережі доступу (МД), тобто мережі електрозв'язку, які забезпечують підключення термінальних пристроїв користувачів до приграничного вузла транспортної мережі. Для організації рівня доступу можуть використовуватися різні середовища передачі. Це може бути мідна пара, коаксіальний кабель, волоконно-оптичний кабель, радіоканал, супутникові канали або будь-яка їхня комбінація.

Рівень T представляє собою основний ресурс мережі, який забезпечує передачу інформації від користувача до користувача шляхом її комутації та маршрутизації. ITU-T визначає такі вимоги до можливостей транспортного рівня:

- підтримка з'єднань у реальному часі й з'єднань, не чутливих до затримок;
- підтримка різних моделей з'єднань: «крапка — крапка», «крапка — багатокрапка», «багатокрапка — багатокрапка», «багатокрапка — крапка»;
- гарантовані рівні продуктивності, надійності, доступності, масштабованості.

Рівень C – це нова концепція комутації, яка заснована на використанні технології комп'ютерної телефонії та Softwitch. Він має забезпечувати обробку інформації сигналізації, маршрутизації викликів і управління потоками. Цей рівень підтримує логіку управління, яка необхідна для обробки й маршрутизації трафіка. Softswitch має здійснювати:

- обробку всіх видів сигналізації, які використовуються у його домені;
- зберігання й управління даними користувачів, що підключені до його домену безпосередньо або через обладнання шлюзів доступу;
- взаємодію із серверами аплікацій для надання розширеного списку послуг користувачам мережі.

Рівень S визначає склад інформаційного наповнення мережі. Тут знаходиться корисне навантаження мережі в якості послуг по доступу користувачів до інформації. Він забезпечує:

- надання (підтримку) інфокомунікаційних послуг;
- безпосередньо управління послугами;
- створення й упровадження нових послуг;
- взаємодію різних послуг.

Цей рівень має реалізувати специфіку послуг і застосовувати одну й ту саму програму логіки послуг незалежно від типу транспортної мережі й способу

доступу. Наявність цього рівня забезпечить також можливість введення на транспортній мережі нових послуг без втручання у функціонування інших рівнів.

Термінальне обладнання включає різні типи кінцевих (термінальних) вузлів, мережі терміналів — обладнання, встановленого у користувачів, за допомогою яких користувач використовує через мережі доступу ресурс транспортного рівня. У комп'ютерній мережі кінцевими вузлами є комп'ютери, телефонній — телефонні апарати, а телевізійній або радіомережі — відповідні теле- і радіоприймачі.

Структура за концепцією 3GPP

Залежність мережної інфраструктури від нових послуг NGS знайшла відображення в роботах Форуму 3GPP (3-rd Generation Partnership Project), у яких запропонована концепція IMS (IP Multimedia Subsystem). На думку фахівців, платформа IMS стане центром мереж майбутнього, навколо якого формуватимуться інші рівні функціональної моделі мережі NGN. Концепцію IMS регламентує частина необхідних стандартів і створює базу для трансформації NGN з мереж з пакетною передачею мовлення в реальні мультисервісні мережі, які конвергуються з будь-якими іншими мережами.

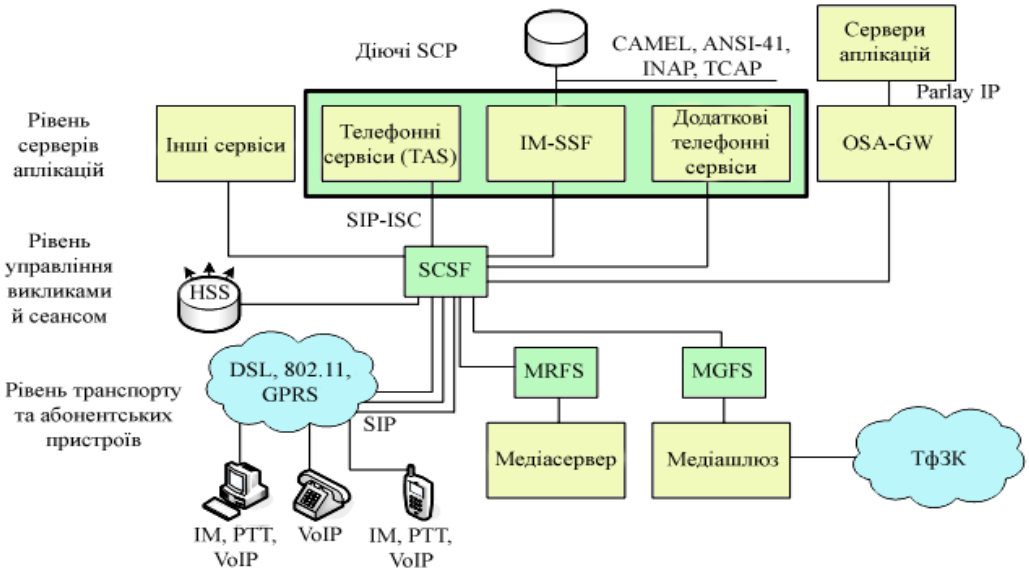

Рисунок 1.5. Спрощена структура IMS

За допомогою цієї архітектури можна надавати послуги користувачам через будь-які технології доступу до мережі.

Архітектуа IMS – це представник архітектур, заснованих на розповсюджених протоколах сімейства TCP/IP. Дана технологія призначена для надання послуг і забезпечення управління сеансами зв'язку, і доставку в рамках цих сеансів будь-яких типів інформації — мови, даних, відео, мультимедіа. Принципово важливим є те, що в системах, що відповідають концепції IMS, послуги можуть надаватися різними сервіс–провайдерами і доставлятися до користувачів по різним (дротовим і бездротовим) мережам доступу.

На рівні транспорту та абонентських пристроїв ініціюється й здійснюється сигналізація SIP, необхідна для встановлення сеансів і надання базових послуг, таких як перетворення мови з аналогової або цифрової форми в IP-пакети з використанням протоколу RTP (Realtime Transport Protocol).

Рівень управління викликами й сеансами реалізує функцію управління викликами й сеансами CSCF (Call Session Control Function), яка реєструє абонентські пристрої й направляє сигнальні повідомлення протоколу SIP до відповідних серверів аплікацій. Цей рівень включає сервер абонентських даних HSS (Home Subscriber Server), де централізовано зберігаються унікальні сервісні профілі всіх абонентів. Профіль містить поточну реєстраційну інформацію (наприклад, IP-адресу), дані роумінгу, дані щодо телефонних послуг, дані щодо обміну миттєвими повідомленнями, параметри голосової пошти тощо. На даному рівні також реалізується функція управління медіашлюзами MGCF (Media Gateway Control Function), які забезпечують взаємодію сигналізації SIP із сигналізацією інших медіашлюзів.

2 СТЕК ПРОТОКОЛУ TCP/IP

2.1 Поняття та модель стека TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) – це промисловий стандарт стека протоколів, розроблений групою Internet Engineering Task Force (IETF) для глобальних мереж. Стандарти TCP / IP опубліковані в серії документів, названих Request for Comment (RFC). Документи RFC описують внутрішню роботу мережі Internet.

Протоколи, що взаємодіють між собою, об'єднуються в стеки. Порядок виконання протоколів стека визначається операційною системою. На пристрої-відправнику протоколи стека виконуються зверху вниз, тобто від протоколів верхніх рівнів до протоколів нижніх рівнів. На пристрої - одержувачі (комп'ютері) протоколи стека виконуються від низу до верху.

Основними перевагами стека протоколів TCP / IP є:

• Незалежність від мережевої технології. Стек не залежить від устаткування кінцевих користувачів.

• Загальна зв'язаність. Стек дозволяє будь-якій парі комп'ютерів, які його підтримують, взаємодіяти один з одним.

• Міжкінцеве підтвердження. Протоколи стека TCP / IP забезпечують підтвердження правильності проходження інформації при обміні між відправником і отримувачем.

Відповідність рівнів стека TCP/IP рівням моделі OSI має досить умовний характер, оскільки стек був розроблений до появи моделі взаємодії відкритих систем, хоча він також має багаторівневу структуру. Відповідність еталонних моделей OSI та TCP/IP показана на рис. 2.1.

Рисунок 2.1. Відповідність еталонних моделей OSI та TCP/IP

Структуру стека протоколів TCP / IP можна розділити на чотири рівні. На рис. 2.2 видно, що кожен рівень несе власне функціональне навантаження.

1. Рівень додатків (application layer) є вищим рівнем моделі TCP / IP. На цьому рівні реалізується доступ додатків до комп'ютерної мережі. Стек протоколів TCP / IP включає до свого складу велику кількість протоколів прикладного рівня. До них відносяться протокол передачі файлів FTP (забезпечує переміщення файлів між комп'ютерними системами), поштовий протокол SMTP (забезпечує механізм передачі електронної пошти), гіпертекстові сервіси доступу до вилученої інформації, такі як WWW, протокол керування мережею SNMP (повідомляють про аномальні умовах в мережі і встановлення значень допустимих порогів в мережі).

2. Транспортний рівень (transport layer) називається основним. На цьому рівні функціонує протокол управління передачею даних TCP (Transmission Control Protocol) і протокол передачі прикладних пакетів дейтаграмним методом UDP (User Datagram Protocol). Протокол TCP забезпечує гарантовану доставку даних за рахунок утворення логічних з'єднань між віддаленими прикладними процесами. Робота протоколу UDP аналогічна роботі протоколу IP, але основним його завданням є виконання функцій сполучної ланки між мережним протоколом і різними додатками.

3. Мережний рівень (network layer) - це рівень міжмережевої взаємодії. В якості основного протоколу мережевого рівня в стеці TCP / IP використовується

протокол IP, який і створювався з метою передачі інформації в розподілених мережах. Перевагою протоколу IP є можливість його ефективної роботи в мережах зі складною топологією. В основі протоколу IP закладений дейтаграммний метод, який не гарантує доставку пакета, але спрямований на її здійснення. До цього рівня відносяться всі протоколи, які створюють, підтримують і оновлюють таблиці маршрутизації.

4. Рівень підмереж (link layer) - відповідає фізичному і канальному рівням моделі OSI. Рівень мережевого інтерфейсу відповідає за прийом дейтаграм і передачу їх по конкретної мережі. Він підтримує стандарти фізичного і канального рівня популярних локальних мереж: Ethernet, Token Ring, FDDI і т.д. Для розподілених мереж підтримуються проколи з'єднань PPP і SLIP, а для глобальних мереж - протокол X.25. Передбачена підтримка використання технології, що розвивається комутації комірок - ATM. Звичайною практикою стало включення в стек протоколів TCP/IP нових технологій локальних або розподілених мереж і регламентація їх новими документами RFC.

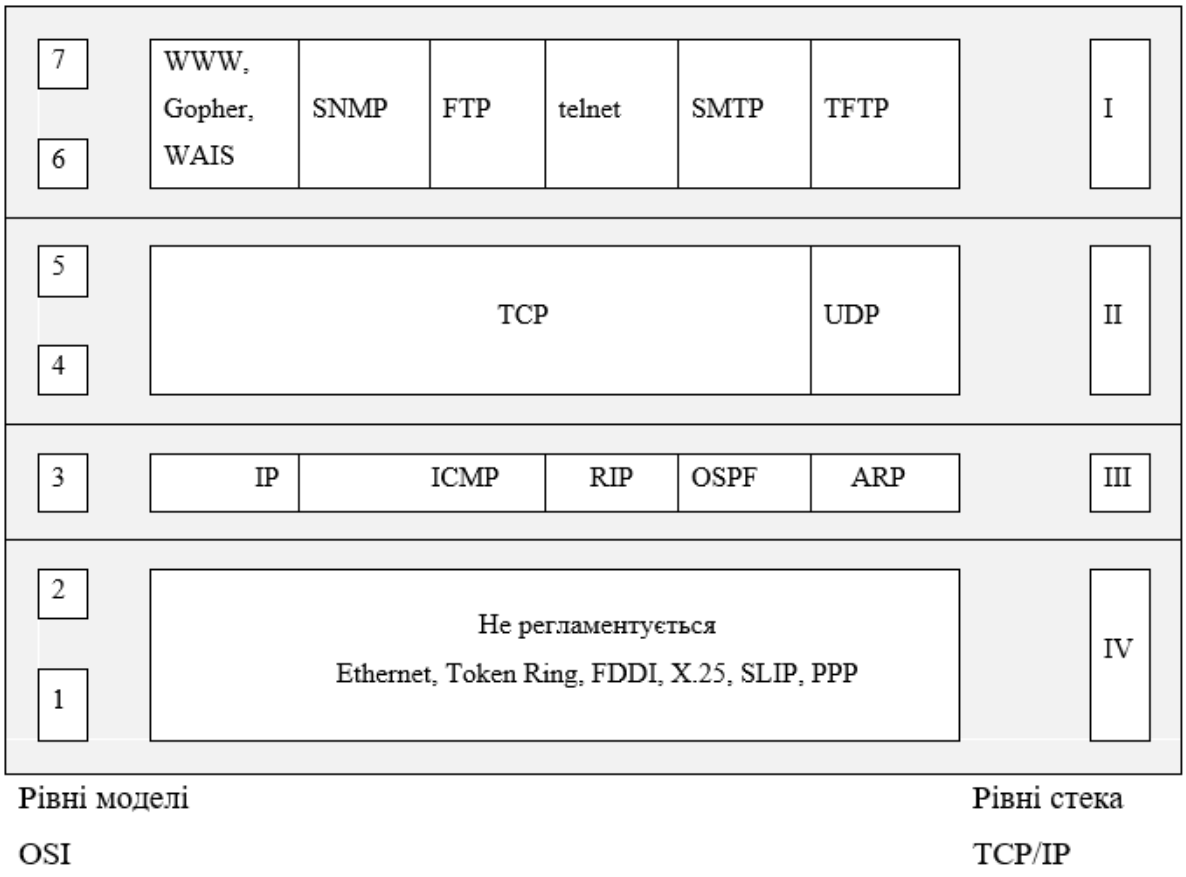

Рисунок 2.2. Функціональне навантаження кожного рівня

2.2 Особливості TCP протоколу та TCP-сесії

TCP протокол - один з основних протоколів передачі даних Internet. У стеку протоколів TCP/IP, TCP виконує функції протоколу транспортного рівня моделі OSI.

TCP забезпечує свою надійність завдяки:

- Гарантованій доставці з встановленням з'єднань у вигляді байтових потоків. Блок інформації, який передається від TCP в IP, називається сегментом.
- Коли TCP посилає сегмент, він встановлює таймер, чекаючи, що з віддаленого кінця прийде підтвердження на цей сегмент. Якщо підтвердження не отримане після закінчення часу, сегмент передається повторно.
- Коли TCP приймає дані від віддаленої сторони з'єднання, він відправляє підтвердження. Це підтвердження не вирушає негайно, а зазвичай затримується на долі секунди.
- TCP здійснює розрахунок контрольної суми для свого заголовка і даних, метою якої є виявити будь-яку зміну даних в процесі передачі. Якщо сегмент прибуває з невірною контрольною сумою, TCP відкидає його і підтвердження не генерується. При цьому, очікується, що відправник відпрацює тайм-аут і здійснить повторну передачу.
- Оскільки TCP сегменти передаються у вигляді IP - дейтаграм, а IP - дейтаграми можуть прибувати хаотично, також хаотично (без дотримання черги) можуть прибувати і TCP сегменти. Після отримання даних TCP може за необхідністю змінити їх послідовність, в результаті чого застосування отримує дані в правильному порядку.
- Оскільки IP - дейтаграма може бути продубльована, приймаючий TCP повинен відкидати продубльовані дані.

TCP здійснює контроль потоку даних. Кожна сторона TCP з'єднання має буфер певного розміру. TCP на приймаючій стороні дозволяє віддаленій стороні посилати дані лише в тому випадку, якщо одержувач може помістити їх в буфер.

Це запобігає від переповнювання буферів хостів з невисокою продуктивністю швидкими хостами.

Заголовок TCP-сегмента містить значно більше полів, ніж заголовок UDP, що відображає більш розвинені можливості протоколу TCP (рис. 2.3)

Біт	0-3	4-9	10-15	16-31
0	Порт джерела, **Source Port**			Порт призначення, **Destination Port**
32	Порядковий номер, **Sequence Number (SN)**			
64	Номер підтвердження, **Acknowledgment Number (ACK SN)**			
96	Довжина заголовка	Зарезервовано	Прапори	Розмір вікна
128	Контрольна сума			Показник важливості
160	Опції			
160/192+	Дані			

Рисунок 2.3. Структура заголовка TCP-сегмента

Порт джерела: 16 бітний номер, який ідентифікує номер вихідного порту (TCP-порт відправника комп'ютера).

Порт призначення: 16 бітний номер, який визначає номер кінцевого порту (приймальний порт).

Порядковий номер: 32 бітовий номер, що використовується для нумерації байтів сегментів TCP. Порядковий номер виконує два завдання:

- якщо встановлено прапор SYN, то це початковий порядковий номер - ISN, і перший байт даних, які будуть передані в наступному пакеті, буде мати номер ISN + 1.
- якщо SYN не встановлений, перший байт даних, який передається в даному пакеті, має цей порядковий номер.

Номер підтвердження: поле з 32 бітовим числом, яке вказує наступний послідовний номер, який відправник очікує від іншого пристрою.

Довжина заголовка: поле 4 бітів, яке показує кількість 32 бітових слів у заголовку. Також відомий як поле зсуву даних. Мінімальний розмір заголовку

становить 20 байт (п'ять 32-бітових слів), а максимальний - 60 байт (п'ятнадцять 32-бітових слів).

Поле зарезервовано складається з 6 бітів, для майбутнього використання і завжди встановлюється значення 0.

Наступне поле містить 6 бітових прапорів:

- URG - поле «Показник важливості»;
- ACK - поле «Номер підтвердження»;
- PSH - інструктує отримувача проштовхнути дані, накопичені в приймальному буфері, в додаток користувача;
- RST - обірвати з'єднання, скинути буфер (очищення буфера);
- SYN- синхронізація номерів послідовності;
- FIN - прапор, будучи встановлений, вказує на завершення з'єднання та припинення зв'язку.

Поле розмір вікна - вказує розмір вікна прийому. Кількість байт даних починаючи з останнього номера підтвердження, які може прийняти відправник даного пакета. Інакше кажучи, відправник пакета має для прийому даних буфером довжиною "розмір вікна" байт.

Контрольна сума: поле для 16-бітної контрольної суми використовується для перевірки помилок заголовка та даних.

Показник важливості - це 16-бітове значення позитивного зсуву від порядкового номера. Це поле вказує порядковий номер октету, яким закінчуються важливі (urgent) дані. Поле береться до уваги тільки для пакетів з встановленим прапором URG.

Опції - можуть застосовуватися в деяких випадках для розширення протоколу. Іноді використовуються для тестування.

На відміну від традиційної альтернативи - UDP, який може відразу ж почати передачу пакетів, TCP встановлює з'єднання, які повинні бути створені перед передачею даних. TCP з'єднання можна розділити на 3 стадії:

- Установка з'єднання;
- Передача даних;

- Від'єднання;

Встановлення зв'язку клієнт-сервер здійснюється в три етапи (триступінчате рукостискання - three way handshake). При встановленні сесії використовується поле прапорів. Технологія тристороннього руху TCP часто називається SYN-SYN-ACK (рис. 2.4).

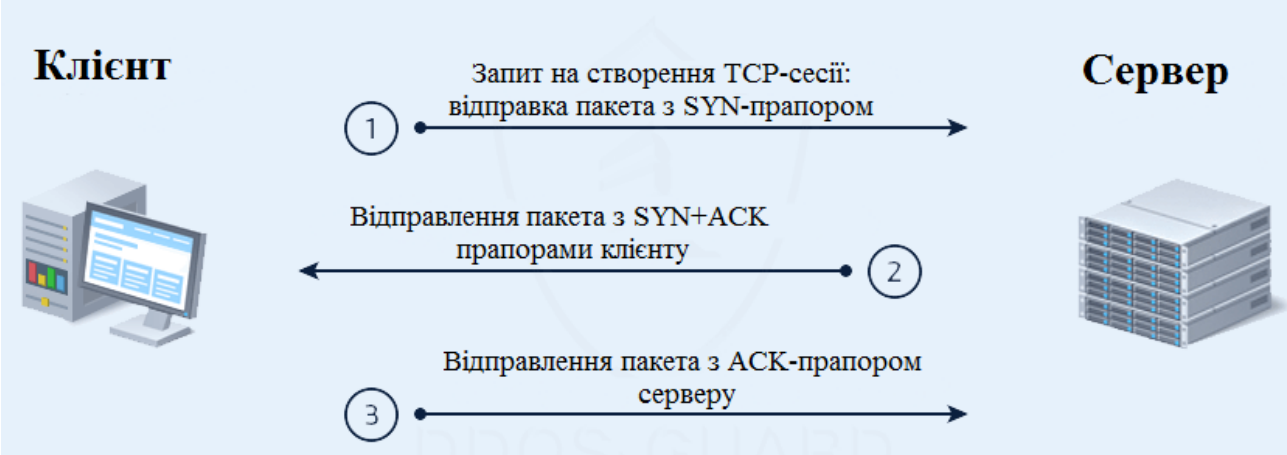

Рисунок 2.4. Триступінчате рукостискання

1) Режим активного доступу (Active Open). Відправник відправляє запит на встановлення з'єднання - повідомлення SYN. Також в сегмент включається порядковий номер байту, що передається.

Подальший алгоритм:

- Сервер отримує сегмент, запам'ятовує номер послідовності і намагається створити сокет (буфери і керуючі структури пам'яті) для обслуговування нового клієнта;
- У разі успіху сервер посилає клієнтові сегмент з номером послідовності і прапорами SYN і ACK, і переходить в стан SYN-RECEIVED (SYN- отримано);
- У разі невдачі сервер посилає клієнтові сегмент з прапором RST.

2) Режим пасивного доступу (Passive Open). Якщо клієнт отримує сегмент з прапором SYN, то він запам'ятовує номер послідовності і посилає сегмент з прапором ACK та порядковий номер байту, на який він чекає.

Подальший алгоритм:

- Якщо клієнт отримує прапор ACK (що зазвичай і відбувається), то він переходить в стан ESTABLISHED, тобто встановлено;
- Якщо клієнт отримує сегмент з прапором RST, то він припиняє спроби з'єднатися;
- Якщо клієнт не отримує відповіді протягом 10 секунд, то він повторює процес з'єднання .

3) Завершення рукостискання. На цьому етапі пересилаються підтвердження отримання попереднього запиту на встановлення з’єднання номер наступного очікуваного байту , а також номер байту повідомлення.

2.3 Функції управління потоком за протоколом TCP/IP

Метод ковзаючого вікна

В рамках встановленого з'єднання правильність передачі кожного сегмента повинна підтверджуватися квитанцією одержувача, що являється основою метода ковзаючого вікна.

Квитування - це один з традиційних методів забезпечення надійного зв'язку. У протоколі TCP використовується окремий випадок квитування - алгоритм ковзаючого вікна. Алгоритм ковзаючого вікна в протоколі TCP має деякі суттєві особливості. Зокрема, в узагальненому алгоритмі одиницею переданих даних є кадр.

Для підвищення коефіцієнта використання лінії, джерелу дозволяється передавати деяку кількість пакетів в непрепивному режимі, тобто в максимально можливому для джерела темпі, без отримання на ці пакети відповідних квітанцій. Кількість пакетів, які дозволяються передавати таким чином, називається «розміром вікна». Рисунок 2.5. ілюструє даний метод для розміра вікна в 8 пакетів.

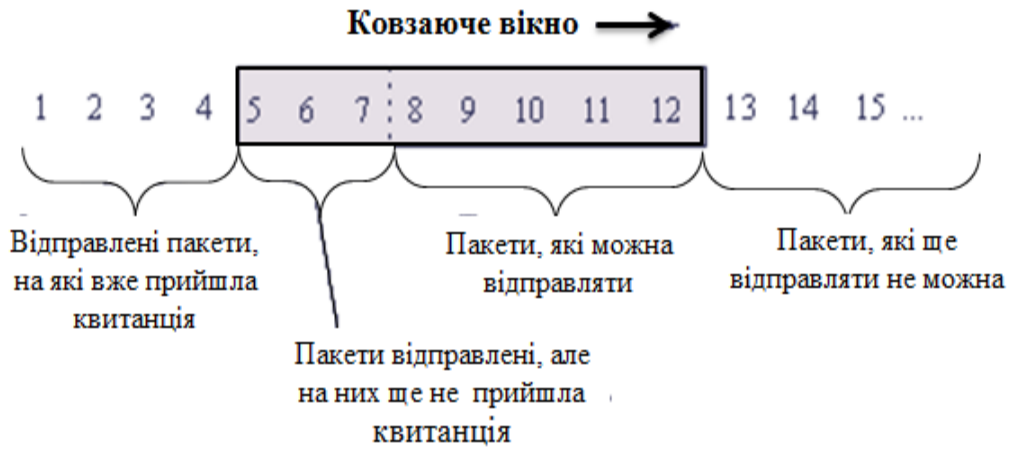

Рисунок 2.5. Метод ковзаючого вікна

На рис. 2.6 більш розгорнуто показаний принцип методу ковзаючого вікна. При кожному отриманні квитанції вікно переміщається (ковзає), захоплюючи нові дані, які дозволяється передавати без підтвердження. В якості квитанції, одержувач сегмента у відповідь відсилає повідомлення (сегмент), в яке вміщує число, що на одиницю перевищує максимальний номер байта в отриманному повідомленні. Якщо розмір вікна дорівнює W, а остання квитанція містила значення N, то відправник може відправляти нові сегменти доти, поки в черговий сегмент не потрапить байт з номером N + W. Цей сегмент виходить за рамки вікна, і передавачу в такому випадку необхідно припинити до приходу наступної квитанції. Коли протокол TCP передає сегмент з даними, він поміщає його копію в чергу повторної передачі і запускає таймер. Коли приходить підтвердження для цих даних, відповідний сегмент видаляється з черги. Якщо підтвердження не спадає до закінчення терміну, то сегмент посилається повторно.

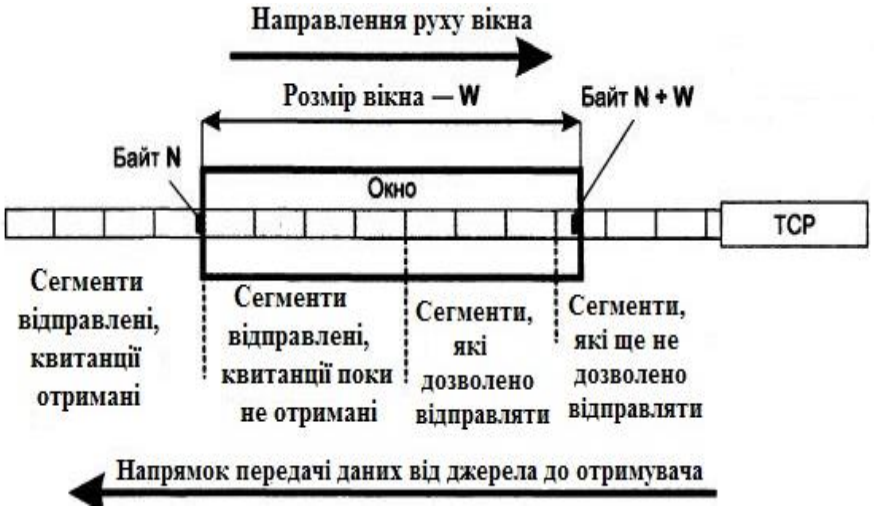

Рисунок 2.6. Особливості алгоритму ковзаючого вікна в протоколі TCP

Вибір часу очікування (тайм-ауту) чергової квитанції є важливим завданням, результат рішення якої впливає на продуктивність протоколу TCP. Тайм-аут не повинен бути занадто коротким, щоб по можливості виключити надлишкові повторні передачі, які знижують корисну пропускну здатність системи. Але він не повинен бути і занадто великим, щоб уникнути тривалих простоїв, пов'язаних з очікуванням неіснуючої або «заблукала» квитанції.

У протоколі TCP тайм-аут визначається за допомогою досить складного адаптивного алгоритму, ідея якого полягає в наступному. При кожній передачі засікається час від моменту відправки сегменту до приходу квитанції про його прийом (час обороту). Отримувані значення часу обороту усереднюються з ваговими коефіцієнтами, що зростають від попереднього виміру до чого. Це робиться для того, щоб посилити вплив останніх вимірів. Як тайм-аут вибирається середній час обороту, помножене на деякий коефіцієнт. Практика показує, що значення цього коефіцієнта повинно перевищувати 2.

Механізм повільного старту

Механізм повільного старту використовується для оцінки пропускної здатності, доступної для потоку TCP в даний момент часу. Головна ідея, що лежить в основі цього алгоритму, полягає в тому, що на початковій стадії передачі сегменти повинні відправлятися зі швидкістю, пропорційною

швидкості отримання підтверджень. Реалізація цього алгоритму передбачає використання додаткового вікна відправника - вікна перевантаження (congestion window, CWnd). Перевантажувальне вікно починається з розміру в 1 сегмент. Для кожного сегмента з успішно отриманим ACK розмір перевантажувального вікна збільшується на 1 сегмент. Хоча алгоритм і називається «повільний старт», розмір його вікна перевантаження зростає досить енергійно.

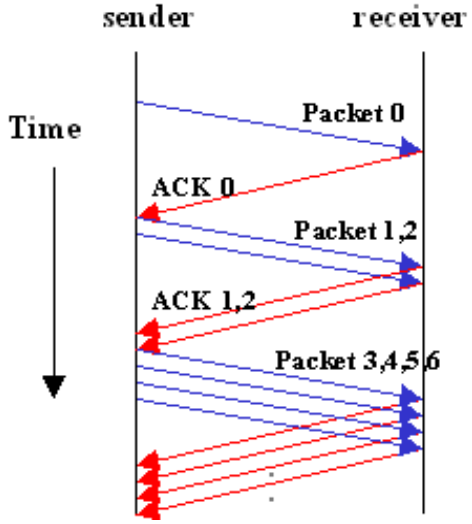

Рисунок 2.7. Механізм повільного старту

Основна ідея «повільного старту» - відправити пакети стільки, скільки може прийняти мережа. Він починає передавати 1 пакет, і якщо цей пакет успішно передається і отримує ACK (Номер підтвердження), він збільшує його розмір вікна до 2, і після отримання 2 ACK він збільшує розмір вікна до 4, а потім 8 і т. д.

Різниця між «ковзаючим вікном» і «повільним стартом» полягає в тому, що «повільний старт» дозволяє використовувати різні розміри вікна, в той час як «ковзаюче вікно» має фіксований розмір вікна.

Алгоритм управління перевантаження AIMD

Алгоритм адитивного збільшення / мультиплікативного зменшення (AIMD) являє собою алгоритм управління зі зворотним зв'язком.

Основною ідеєю механізму контролю перевантаження протоколу TCP є зниження швидкості передачі джерела шляхом зменшення розміру його вікна

перевантажень при втраті пакету. Цілком ймовірно, що у всіх TCP-з'єднаннях, що обслуговуються перевантаженим маршрутизатором, спостерігаються втрати пакетів, що призводить до одночасного зменшення вікон перевантажень усіма цими сполуками. Кінцевий ефект полягає в зниженні трафіку, що проходить через перевантажений маршрутизатор і, як наслідок, в ослабленні перевантаження.

Однак все ще залишається відкритим питання про те, наскільки істотним повинно бути зниження швидкості передачі при втраті пакету. У протоколі TCP використовується так зване «мультиплікативне зменшення», що означає подвійне зменшення розміру вікна перевантаження при втраті пакету. Якщо втрата пакета сталася при значенні CongWin, рівному 20 Кбайт, то останнє буде «урізано» до 10 Кбайт. У разі втрати ще одного пакета значення CongWin стане рівним 5 Кбайт. Зменшення розміру вікна перевантаження може відбуватися багато разів, однак значення CongWin, менше ніж максимального розміру сегмента (MSS), не допускаються. При втраті пакету значення CongWin спочатку стає рівним MSS і лише потім досягає половини початкового значення.

Рисунок 2.8. Алгоритм адитивного збільшення / мультиплікативного зменшення

Повільний старт - це спосіб спочатку встановити потік даних по з'єднанню. Проте, в цей же самий час ми досягнемо межі в проміжного маршрутизатора, при якому пакети відкидатимуться. Запобігання перевантаженню це спосіб, що дозволяє запобігти втраті пакетів.

Запобігання перевантаження і повільний старт це незалежні один від одного алгоритми, більш того, працюють з різними об'єктами. Проте, коли виникає перевантаження, необхідно уповільнити швидкість передачі пакетів по мережі, а потім використовувати повільний старт, аби почати все з початку. На практиці ці алгоритми використовуються разом.

Алгоритми управління потоком за протоколом TCP

Останнім часом Інтернет еволюціонує від гомогенного контролю перевантаження до гетерогенного контролю перевантаження. Кілька років тому інтернет-трафік в основному контролювався традиційним алгоритмом AIMD, в той час як інтернет-трафік тепер контролюється багатьма різними алгоритмами TCP, такими як AIMD, BIC, CUBIC і CTCP.

TCP Congestion Avoidance Algorithm - це алгоритми, які намагаються зробити все можливе, щоб забезпечити найбільш швидку швидкість передачі даних між двома вузлами, які передають дані через TCP. Вони управляють розміром TCP-вікна і можуть орієнтуватися на RTT (Round Trip Time - час від відправки запиту до отримання відповіді), втрату пакетів, час очікування відправки пакета з черги і т.д. Кожен алгоритм по різному веде себе в тій чи іншій ситуації і немає якогось універсального.

Основні алгоритми:

1. TCP Reno - розмір вікна змінюється циклічно. Він збільшується при кожному циклі до втрати пакета. Коли відбувається втрата пакета, TCP Reno зменшує розмір вікна до половини поточного розміру. Це називається – аддитивним збільшенням і мультиплікативний зменшенням

2. TCP NewReno (RFC-6582) - являється одним з найбільш поширених TCP-алгоритмів. Він заснований на алгоритмі Fast Retransmit & Fast Recovery (швидка повторна пересилання і швидке відновлення)

3. TCP Vegas - використовує різницю між очікуваною і фактичною швидкістю потоків для оцінки пропускної здатності мережі. Основна ідея полягає в тому, що коли мережа не перевантажена, фактична швидкість потоку

буде близька до очікуваної. В іншому випадку фактична швидкість потоку буде менше, ніж очікувана швидкість потоку. За допомогою різниці швидкостей, TCP Vegas оцінює рівень заторів у мережі і відповідним чином оновлює розмір вікна.

4. TCP Compound - алгоритм, розроблений Microsoft 2008 р. для агресивного збільшення TCP вікна для оптимізації TCP швидкості передачі даних при великій затримці з мінімальними відхиленнями від стандарту.

5. TCP Tahoe - використовує алгоритм швидкої повторної передачі, за допомогою якого він швидше реагує на помилки пакетів.

6. TCP Westwood - дозволяє досягти більшої ефективності використання каналу, використовуючи новий алгоритм управління вікном перевантаження, заснований на оцінці потоку даних (RE - Rate Estimation) і поточного значення смуги пропускання.

7. TCP Hybla - розроблена для широких каналів з високим RTT. Максимальної утилізації каналу вдається досягти завдяки аналітичній оцінці динаміки вікна перевантаження.

8. BIC-TCP - двійковий контроль зменшення перевантаження, забезпечує досить велику масштабованість для швидкісних мереж передачі даних та стабільність, не дивлячись на низький рівень осциляції розміру його вікна.

9. CUBIC-TCP – розмір «вікна» визначається кубічної функцією, що залежить від часу, що пройшов після останньої втрати пакету, і зміною розміру «вікна», при якому сталася втрата. CUBIC не залежить від прийому підтверджень (ACK) для збільшення розміру «вікна». Розмір «вікна» CUBIC залежить тільки від останнього затору.

10. TCP RED – один з алгоритмів AQM для управління переповненням черг маршрутизаторів. RED відстежує середній розмір черги і відкидаються пакетів, грунтуючись на статистичну вірогідність. RED стає набагато ефективніше інших алгоритмів в разі малих розмірів черг, а також при «вибуховий» характер трафіку.

11. TCP WRED - поєднує в собі можливості алгоритму RED і IP-пріоритети. Це поєднання забезпечує можливість привілейованої обробки

пакетів з високим пріоритетом. Використання WRED уможливлює поділ за класами якості обслуговування (QoS).

Основним завданням TCP-алгоритмів запобігання перевантажень є підтримка значення потоку даних, що передаються по мережі, нижче рівня, при якому пропускна здатність мережі починає різко падати, обмежуючи потоки вхідного і вихідного трафіку.

2.3 Протокол IP

Протокол IP є протоколом мережного (3-го) рівня, який містить інформацію про адресацію і управляючу інформацію для маршрутизації пакетів. Протокол IP описаний в RFC 791. Разом з протоколом управління передачею (TCP) протокол IP утворює основу протоколів Internet. Протокол IP має дві основні функції: забезпечення передачі дейтаграм по об'єднаній мережі методом негарантованої доставки без підтвердження з'єднання і забезпечення фрагментації повторної збірки дейтаграм для підтримки каналів передачі даних з різними розмірами максимального передаваємого модуля даних (MTU).

Протокол відповідає за адресацію пакетів, але не відповідає за встановлення з'єднань, не є надійним і дозволяє реалізувати тільки негарантовану доставку даних. Проте IP надає певний сервіс обробки деяких подій. Коли що-небудь йде не так як хотілося б, як наприклад, тимчасове переповнювання буфера маршрутизатора, IP застосовує простий алгоритм обробки помилок: він відкидає дейтаграму і прагне послати ICMP повідомлення відправнику. Будь-яка необхідна надійність має бути забезпечена верхніми рівнями (наприклад, TCP).

Термін «протокол без встановлення з'єднань» (connectionless) означає, що протокол для взаємодії не потребує виділеного каналу, як це відбувається під час телефонної розмови і не існує процедури виклику перед початком передачі даних між мережевими вузлами. IP не містить жодної інформації про

просування дейтаграм. Кожна дейтаграма обробляється незалежно від інших. Це також означає, що може бути доставлена зіпсована дейтаграма. Якщо джерело відправляє дві послідовні дейтаграмы (перша А, потім В) в один і той же пункт призначення, кожна з них маршрутизується незалежно і може пройти за різними маршрутами, тобто дейтаграма В може прибути раніше чим А.

Архітектура IP-пакету

IP-пакети складаються з даних верхнього рівня та IP-заголовку. За специфікацією протоколу, пакет має бути не більший за 65535 бітів (з заголовком та даними включно). Заголовок зазвичай має довжину 20 байт = 160 біт. Розглянемо його структуру (рис. 2.9).

Поле номера версії займає 4 біта і ідентифікує версію протоколу IP. Існує дві версії IPv4 та IPv6.

Значення довжини заголовка IP-пакета також займає 4 біта і вимірюється в 32-бітових словах. Зазвичай заголовок має довжину в 20 байт (п'ять 32-бітових слів), але при додаванні деякої службової інформації це значення може бути збільшено за рахунок додаткових байтів в поле параметрів. Найбільша довжина заголовка складає 60 байт.

Рисунок 2.9. Структура заголовка IP-пакета

Поле типу сервісу має й іншу, більш сучасну назву - байт диференційованого обслуговування, або DS-байт. Поле складається з декількох підполів. Спочатку йде підполе пріоритету (Precedence) пакету (довжина 3 біта). Пріоритет може мати значення від найнижчого - 0 (звичайний пакет) до найвищого - 7 (пакет управляючої інформації). Важливіші пакети обробляються в першу чергу. Далі слідують чотири біти D, T, R, C, які визначають бажаний тип маршрутизації: D (Delay) - вибір маршруту з мінімальною затримкою, T (Throughput) - вибір маршруту з максимальною пропускною здатністю, R (Reliability) - вибір маршруту з максимальною надійністю, C (Cost) - вибір маршруту з мінімальною вартістю. У дейтаграми може бути встановлений тільки один з бітів D, T, R, C.

Поле Загальна довжина (довжина 16 біт) описує загальний розмір пакету в байтах з врахуванням заголовка і поля даних. Максимальна довжина пакету обмежена розрядністю цього поля і складає 65535 байт. Завдяки цьому полю і полю довжини заголовка, ми знаємо, з якого місця починаються дані в IP дейтаграмі і їх довжину.

Ідентифікатор пакету займає 2 байта і використовується для розпізнавання пакетів, що утворилися шляхом паділу (фрагментації) вихідного пакета. Всі фрагменти одного пакета повинні мати однакове значення цього поля.

Прапори займають 3 біта і містять ознаки, пов'язані з фрагментацією. Встановлений в 1 біт DF (Do not Fragment - НЕ фрагментувати) забороняє маршрутизатору фрагментувати даний пакет, а встановлений в 1 біт MF (More Fragments - більше фрагментів) говорить про те, що даний пакет є проміжним (не останнім) фрагментом. Біт, що залишився є зарезервований.

Поле зсуву фрагмента займає 13 біт і задає зміщення в байтах поля даних цього фрагмента щодо початку поля даних вихідного (нефрагментовані) пакета. Використовується при складанні / розбиранні фрагментів пакетів. Зсув повиннен бути кратним 8 байт.

Поле часу життя займає один байт і використовується для задання граничного терміну, протягом якого пакет може пересуватися по мережі. Час життя пакету вимірюється в секундах і задається джерелом. Після закінчення кожної секунди перебування на кожному з маршрутизаторів, через які проходить пакет під час свого «подорожі» по мережі, з його поточного часу життя віднімається одиниця; одиниця віднімається і в тому випадку, якщо час перебування було менше секунди. Якщо значення поля часу життя стає нульовим до того, як пакет досягає одержувача, пакет знищується. Таким чином, час життя є свого роду годинниковим механізмом самознищення пакета.

Поле протоколу верхнього рівня займає один байт і містить ідентифікатор, який вказує, якому протоколу верхнього рівня належить інформація, розміщена в полі даних пакета. Значення ідентифікаторів для різних протоколів наводяться в документі RFC 1700. Наприклад, 6 означає, що в пакеті знаходиться повідомлення протоколу TCP, 17 - протоколу UDP, 1 - протоколу ICMP.

Контрольна сума заголовка займає 2 байта (16 біт) і розраховується тільки по заголовку. Оскільки деякі поля заголовка міняють своє значення в процесі передачі пакета по мережі (наприклад, поле часу життя), контрольна сума перевіряється і повторно розраховується на кожному маршрутизаторі і

кінцевому вузлі як доповнення до суми всіх 16-бітних слів заголовка. При обчисленні контрольної суми значення самого поля контрольної суми встановлюється в нуль. Якщо контрольна сума невірна, то пакет відкидається, як тільки знаходять помилку.

Поля IP-адрес джерела і приймача мають однакову довжину - 32 біта.

Поле параметрів є необов'язковим і використовується зазвичай тільки при налагодженні мережі. У ньому можна вказувати точний маршрут, реєструвати прохідні пакетом маршрутизатори, поміщати дані системи безпеки або тимчасові позначки.

Принцип IP-маршрутизації

IP-маршрутизація - процес вибору шляху для передачі пакета в мережі. Під шляхом (маршрутом) розуміється послідовність маршрутизаторів, через які проходить пакет по шляху до вузла-призначення.

Основні компоненти маршрутизації: виявлення оптимальних трактів та транспортування пакетів через об’єднану мережу. Процес маршрутизації починається з моменту потрапляння пакета в глобальну мережу та продовжується до момента його виходу за рамки мережі.

IP-маршрутизація складається з наступних складових:

- розрахунок таблиці маршрутизації;
- аналіз IP-адреси одержувача в заголовку пакета;
- визначення найкоротшого шляху до вузла одержувача по таблиці маршрутизації;
- відсилання пакета на наступний вузол.

Для визначення маршрута використовуються таблиці маршрутизації. В ній містяться IP-адреси мереж (<мережа, 0>) і IP-адреси хостів (<ця мережа, хост>). Адреси мереж дозволяють отримувати доступ до віддалених мереж, а адреси хостів - звертатися до локальних хостів. З кожною таблицею пов'язаний

мережевий інтерфейс, що застосовується для отримання доступу до пункту призначення, а також інша інформація.

Коли IP-пакет прибуває на маршрутизатор, адреса одержувача, зазначена в пакеті, шукається в таблиці маршрутизації. Якщо пакет направляється в віддалену мережу, він пересилається наступному маршрутизатору по інтерфейсу, вказаному в таблиці. Якщо пакет призначений хосту - він пересилається безпосередньо адресату. Якщо номери мережі, в яку посилається пакет, в таблиці маршрутизатора немає, пакет посилається маршрутизатору за замовчуванням, з більш докладними таблицями.

Існує пряма та непряма доставка датаграм.

На рис. 2.10 показана невелика IP-мережа, що складається з 4 машин: A, B, C і D. Кожна машина має такий же стек протоколів TCP / IP. Кожен мережевий адаптер цих машин має свою Ethernet-адресу та унікальний IP-адресу.

Пряма маршрутизація - пакети йдуть від відправника до одержувача безпоередньо, тобто вони знаходяться в межах однієї підмережі (наприклад, мережі Ethernet).

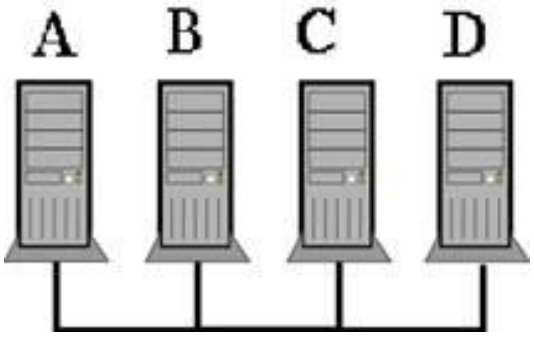

Рисунок. 2.10. Звичайна IP-мережа

Коли машина A посилає IP-пакет машині B, то заголовок IP-пакета містить в полі відправника IP-адресу вузла A, а заголовок Ethernet-кадру містить в полі відправника Ethernet-адресу A. Крім цього, IP-заголовок містить у полі отримувача IP-адреса вузла B, а Ethernet-заголовок містить у полі отримувача Ethernet-адреса B. Відобразимо це в таблиці 2.1.

Таблиця 2.1.

Відповідність IP та Ethernet – заголовків відправника та отримувача при прямій маршрутизації

Адреса:	відправника	отримувача
IP-заголовок:	A	B
Ethernet-заголовок:	A	B

Коли в машині B модуль IP отримує IP-пакет від машини A, він зіставляє IP-адреса місця призначення зі своїм і, якщо адреси співпадають, то передає датаграмму протоколу верхнього рівня.

Непряма маршрутизація здійсньється коли пакети йдуть через шлюз, тобто відправник та отримувач належать до різних підмереж.

На рис. 2.11 представлена більш реалістична картина мережі. В даному випадку мережа складається з двох мереж Ethernet, на базі яких працюють дві IP-мережі, об'єднані шлюзом G. Кожна IP-мережа включає чотири машини; кожна машина має свої власні IP- і Ethernet адреси.

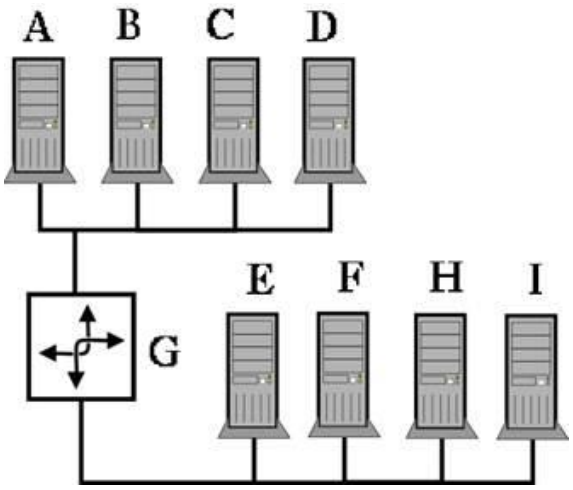

Рисунок 2.11. Мережа з двома IP-мережами

Шлюз G з'єднує обидві мережі і, отже, має 2 IP-адреси і 2 Ethernet-адреси.

Коли машина A посилає IP-пакет машині B, то процес передачі йде в межах однієї мережі. Коли машина G взаємодіє з машиною A, то це пряме взаємодія. Коли машина G взаємодіє з машиною E, то це пряме взаємодія. Це так, оскільки кожна пара цих машин підключена до однієї IP-мережі.

Однак, якщо машина A посилає машині E IP-пакет, то IP-адреса і Ethernet-адреса відправника відповідають адресами A (таблиця 2.2). IP-адреса місця призначення є адресою E, але оскільки модуль IP в A посилає IP-пакет через G, Ethernet-адреса місця призначення є адресою G.

Таблиця 2.2.

Відповідність IP та Ethernet – заголовків відправника та отримувача при непрямій маршрутизації

Адреса:	відправника	отримувача
IP-заголовок:	A	E
Ethernet-заголовок:	A	G

Модуль IP в машині G отримує IP-пакет і перевіряє IP-адреса місця призначення (таблиця 2.3). Визначивши, що це не його IP-адреса, шлюз G посилає цей IP-пакет прямо до E.

Таблиця 2.3.

Перевірка IP-адреси місця призначення машиною G при непрямій маршрутизації

Адреса:	відправника	отримувача
IP-заголовок:	A	E
Ethernet-заголовок:	G	E

Отже, при прямій маршрутизації IP- і Ethernet-адреси відправника відповідають адресами того вузла, який послав IP-пакет, а IP- і Ethernet-адреси місця призначення відповідають адресами отримувача. При непрямій маршрутизації IP- і Ethernet-адреси не утворюють таких пар.

Адресація протоколу IPv4 та IPv6

У мережі IP всі пристрої мають унікальний адрес (IP-адрес). IP-адрес характеризує не сам пристрій, а з'єднання пристрою з мережею (наприклад, пристрій з двома мережними інтерфейсами матиме як мінімум два IP- адреси). Схема адресації протоколу IPv4 описана в документах RFC 990, RFC 997.

IP-адрес має довжину 32 біта. Для зручності прийнято записувати IP-адрес у вигляді двійково-десяткового числа: кожен байт (октет) записується у вигляді десяткового числа в діапазоні від 0 до 255; октети розділені крапками (наприклад, 192.168.0.1). Така форма запису носить назву десятково-точкової нотації.

IP-адреса розділяються на 5 класів: A, B, C, D, E. Адреси класів A, B і C діляться на дві логічні частини: номер мережі і номер вузла (рис. 2.8).

Адреса класу A призначена для дуже великих мереж. В ній використовується тільки перший октет як ідентифікатор мережі. Три октети, що залишились, ідентифікують адресу вузлів. Перший біт в адресі класу A завжди нульовий. Довжина мережного префікса - 8 біт. Для номера вузла виділяється 24 біта.

Адреса класу B використовується для мереж середнього та великого розмірів. В IP-адресі класу B два перших октети використовується для мережевої адреси, а два других являють собою адресу вузла. Перші два біти першого октета завжди приймають значення „1” і „0”, шість бітів, що залишились, можуть містити будь-які комбінації нулів та одиниць. Довжина мережного префікса - 16 біт. Поле номера вузла теж має довжину 16 біт.

Адреси класу C – це найчастіше використовувані адреси, призначені для використання в малих мережах. Адреса даного класу починається з двійкової комбінації 110. Префікс мережі має довжину 24 біта, номер вузла - 8 біт.

Два класи, що залишилися, мають іншу структуру адресу.

Адреси класу D були створені для реалізації в IP-адресах механізму багатоадресної розсилки. Багатоадресною або груповою адресою (multicast address) називається унікальна мережева адреса, що використовується для відправлення пакетів певним групам мережевих пристроїв. Таким чином, одна мережева станція може передавати один потік даних декільком отримувачам.

Діапазон адрес класу D, які називають багатоадресними IP-адресами також певним чином обмежений. Перші чотири біти такої адреси є 1110

Перші чотири біти адрес класу E завжди одиничні. Клас E зарезервований для експериментального використання.

Рисунок 2.12. Класи мереж IPv4

Розглянемо поняття "маска підмережі (мережі)". Маскою підмережі або маскою мережі називається бітова маска, що визначає, яка частина IP-адреса вузла мережі відноситься до адресу мережі, а яка - до адресу самого вузла в цій мережі.

Поля номерів мережі і підмережі утворюють розширений мережний префікс. Для виділення розширеного мережного префікса використовується маска підмережі (Subnet Mask) - 32-розрядне двійкове число (по довжині IP-адреса), в розрядах розширеного префікса що містить одиницю, а в останніх розрядах - нуль, інакше кажучи маска містить біти, встановлені в одиницю для ідентифікатора мережі і ідентифікатора підмережі, і біти, встановлені в 0 для ідентифікатора хоста.

Розширений мережний префікс виходить побітовим порозрядним множенням (логічне "I") IP-адреса і маски підмережі. При такій побудові вочевидь, що число підмереж є мірою двійки – 2^n, де n - довжина поля номера підмережі. Таким чином, характеристики IP-адреса повністю задаються власне IP-адресом і маскою підмережі.

Для спрощення запису застосовують наступну нотацію (так звана CIDR - нотація): IP-адрес/довжина_ розширеного_мережного_префікса.

Число після слеша означає кількість одиничних розрядів, що містяться в масці підмережі.

Наприклад, адрес 192.168.0.1 з маскою 255.255.255.0 в даній нотації виглядатиме як /24 (тобто кількість одиниць в масці дорівнює 24).

Для стандартних класів мереж можна записати наступні значення масок підмереж (у десятково-точковій нотації):

- 255.0.0.0 - маска для мережі класу A; довжина розширеного мережного префікса - 8;
- 255.255.0.0 - маска для мережі класу B; довжина розширеного мережного префікса - 16;
- 255.255.255.0 - маска для мережі класу C; довжина розширеного мережного префікса - 24.

Шоста версія протоколу IPv6 внесла істотні зміни в систему адресації IP-мереж. RFC-2460 - нормативний документ протоколу IPv6.

Адреса IPv6 складається з 128 біт або 16 байт. Це дає можливість пронумерувати величезна кількість вузлів: Обрана довжина IP-адреси повинна надовго зняти проблему дефіциту IP-адрес.

Адреса протоколу IPv6 складається з 128 біт, тобто, він в 4 рази довше 32-бітного IPv4 адресу. Подібно IPv4, в цьому адресі можна виділити дві частини: мережа і хост.

На відміну від попередньої версії протоколу, в IPv6 не застосовуються маски підмережі, так як вони вийшли б дуже довгими, замість цього використовується префікс. який записується так само через слеш після адреси. Наприклад, префікс / 64 означає, що з 128 біт, перші 64 - це мережа, а частина, що залишилася (в даному випадку другі 64) - це хост. Префікс описує, скільки біт в адресі використовується під зберігання інформації про мережу.

Однак структура префікса мережі складніше, ніж в попередній версії. Замість колишніх двох рівнів ієрархії адреси (номер мережі і номер вузла) в IPv6 пропонується використовувати чотири рівні, включаючи трирівневу ідентифікацію мереж, і один рівень для идентифікації вузлів мережі. За рахунок збільшення числа рівнів ієрархії в адресі новий протокол ефективно підтримує технологію агрегування адрес (CIDR).

Тобто, не всі біти в адресі мають однакове значення. Частина бітів зліва (скільки саме залежить від префікса) позначають мережу, інші біти праворуч - ідентифікують пристрій всередині мережі. Частина, відповідальна за зберігання інформації про вузол називається ідентифікатор інтерфейсу (interface id). Сам адрес записують не в десятковому, а в шістнадцятирічному вигляді - так коротше. Адреса розбивається на групи по 16 біт (хекстети) і кожна група представляється чотирма шістнадцятирічними цифрами. Хекстети відокремлюються один від одного знаком двокрапки. Таким чином, адрес складається з 8 хекстетов ([8 хекстетов] * [16 біт в хекстете] = [128 біт] - загальна довжина адресу).

Адреси в IPv6 настільки довгі, що їх запис у звичній десятичній нотації стає вельми незручним (128 біт = 16 байт). Тому їх записують в шістнадцятирічному форматі, причому кожні чотири шістнадцятирічні цифри відокремлюються одна від одної двокрапкою, наприклад:

FEDC:0A98:0000:0000:0000:0000:7654:3210.

Але навіть і в цьому випадку адреси виявляються занадто довгими, тому придумані деякі способи скорочення запису.

Існує також скорочена форма запису, яку можна отримати, використовуючи такі угоди:

1) У кожному хекстеті (групі з 4-х цифр) провідні нулі видаляються. Наприклад, в в хекстеті 0DB0 замінюється на DB0. Тобто нуль зліва видаляється, нуль справа ми не чіпаємо. Якщо хекстет складається з одних нулів, то він замінюється на один нуль.

Таким чином адрес 2001:0DB0:0000:123A:0000:0000:0000:0030 перетворюється в 2001:DB0:0:123A:0:0:0:30.

А адрес FEDC:0A98:0000:0000:0000:0000:7654:3210 можна записати як FEDC:A98:0:0:0:0:7654:3210

Наприклад, адрес loopback (127.0.0.1 в IPv4) в шостої версії протоколу 0000:0000:0000:0000:0000:0000:0000:0001 замінюється на 0:0:0:0:0:0:0:1

2) Якщо в адресі є довга послідовність нулів, то запис адреси можна скоротити. Наприклад, наведений вище адресу можна записати таким чином:

FEDC:A98::7654:3210.

Скорочення «::» може використовуватися в адресі тільки один раз. Крім того, не можна замінювати одну групу з: 0: на ::, правило два застосовується лише якщо є більше однієї нульової групи.

3) Для мереж, що підтримують обидві версії протоколу IPv4 і IPv6, дозволяється використовувати для молодших 4 байт традиційний для IPv4 десятичний запис, а для старших 12 байт - зручній для IPv6 шістнадцятирічну форму: замість 0:0:0:0:0:FCDE:81C0:0C05 або ::FCDE:81C0:C05 можна записати::FCDE:129.192.12.5.

3 ПРОТОКОЛИ МАРШРУТИЗАЦІЇ

3.1 Поділ мережі на автономні системи

Мережі NGN можна розглядати в якості мережевих рішень, які об'єднують фрагменти різних існуючих мереж із застосуванням властивих цим мережам технологій. Відповідно, в NGN застосовуються як протоколи Інтернет, так і протоколи ТМЗК. Крім того, деякі протоколи NGN є перспективними, прямо або побічно зачіпаючи принципи взаємодії мереж Інтернет і Топ в рамках створення мультисервісної мережі.

Протоколи NGN з деякою часткою умовностю можна класифікувати наступним чином:

• базові протоколи мережі Інтернет: IP, ICMP, TCP, UDP;

• транспортні протоколи: RTP, RTCP;

• сигнальні протоколи: SIP, H.323, SIGTRAN, MEGACO / H.248, MGCP, RSVP, SCTP, ISUP, BICC, SCCP, INAP;

• протоколи маршрутизації: RIP, IGRP, OSPF, IS-IS, EGP, BGP, IDRP, TRIP;

• протоколи інформаційних служб і управління: SLP, OSP, LDAP, SNMP;

• протоколи послуг: FTP, SMTP, HTTP, кодекси G. xxx, H. xxx, факс т.37, T.38, IRP, NNTP.

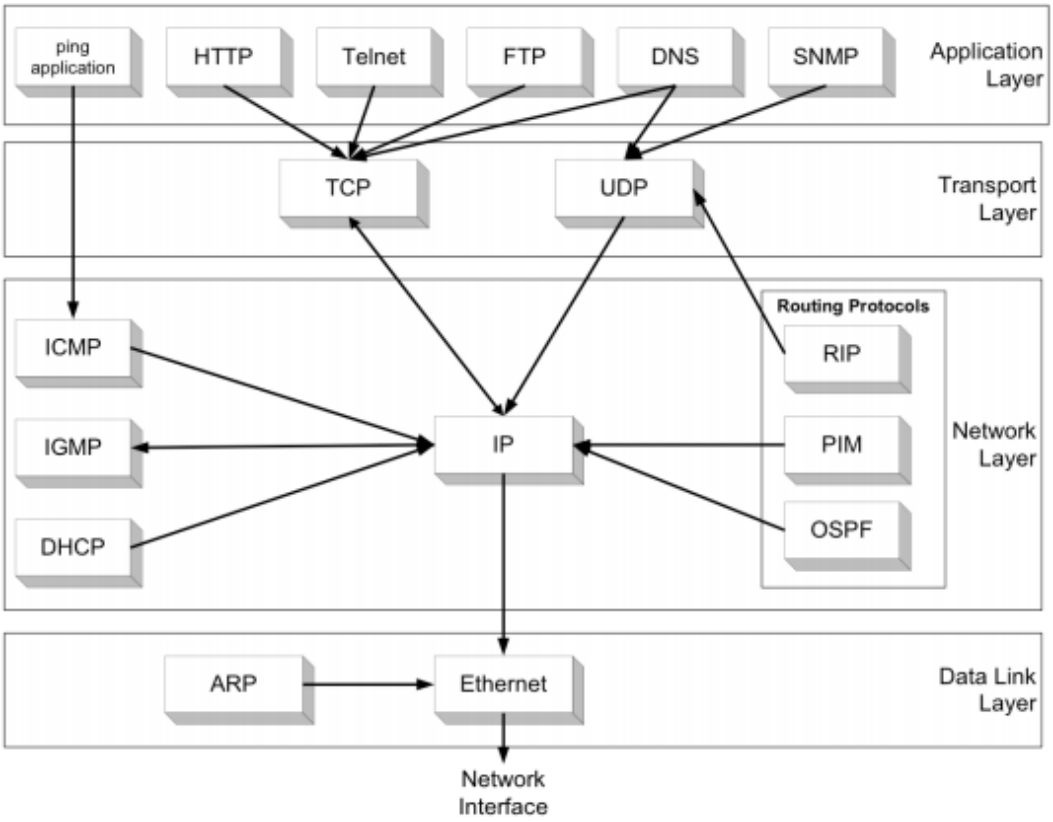

Рисунок 3.1. Основні протоколи мережного та транспортного рівнів

Розглянемо більш докладно протоколи мережного і транспортного рівнів.

Великі об'єднані комп'ютерні мережі складаються з безлічі фізичних мереж, які зв'язуються між собою за допомогою маршрутизаторів. Автономною системою AS (Autonomous Systems) називають групу мереж і маршрутизаторів R, об'єднаних спільною політикою маршрутизації (рис. 3.2.).

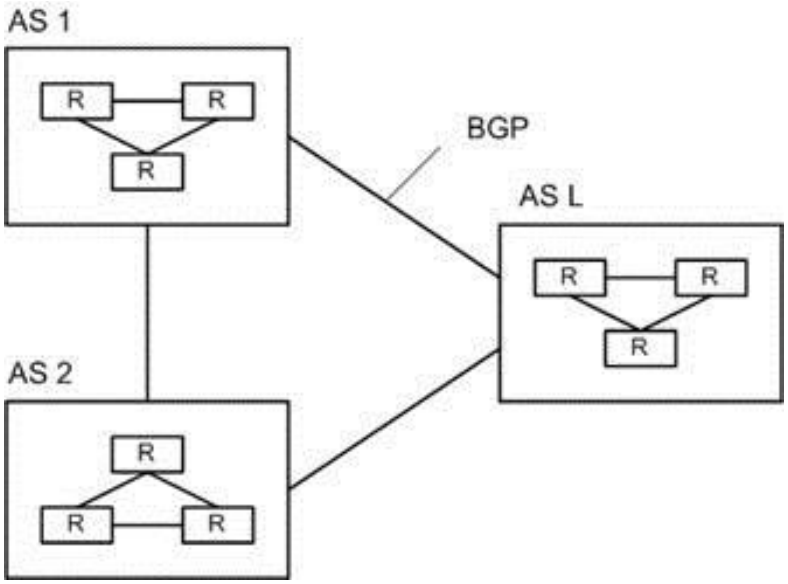

Рисунок 3.2. Автономні системи AS

Якщо AS може передавати транзитний трафік інших мереж, вона називається транзитної.

Для визначення маршруту всередині AS застосовують внутрішні протоколи маршрутизації IGP (Interior GatewayProtocols, протоколи внутрішнього шлюзу) (рис.3.3). До протоколів такого типу відносяться будь-які протоколи маршрутизації, які використовуються виключно всередині автономної системи. Найбільш поширеними протоколами внутрішньої маршрутизації є протоколи RIP (Routing Information Protocol), OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol), розроблений компанією CISCO, як альтернативний RIP, а потім і його покращений варіант EIGRP (Enhanced Interior Gateway Routing Protocol) і IS-IS (Intermediate System - Intermediate System)

Автономні системи об'єднуються між собою за допомогою зовнішніх або прикордонних (Border) маршрутизаторів. Зовнішні протоколи маршрутизації EGP (Exterior Gateway Protocol, протоколи зовнішнього шлюзу) - це протоколи маршрутизації, що забезпечують маршрутизацію між різними автономними системами. Протоколи EGP забезпечують з'єднання окремих автономних систем і транзит переданих даних між ними (рис. 3.3). Єдиним зовнішнім протоколом маршрутизації в даний час є протокол прикордонного шлюзу BGP {Border Gateway Protocol).

Рисунок 3.3. Внутрішні та зовнішні протоколи маршрутизації

Два сусідніх маршрутизаторів, які обмінюються інформацією всередині AS, називаються внутрішнім і зовнішнім, якщо вони обмінюються інформацією, що належить різним системам. Зв'язок між різними автономними системами

здійснюється за допомогою високошвидкісної магістральної або опорної мережі (Backbone).

Протокол IP є маршрутизованим, для його маршрутизації потрібна маршрутна інформація. Маршрутна інформація, може бути:

- Статичної (маршрутні таблиці прописуються вручну)
- Динамічної (маршрутну інформацію поширюють спеціальні протоколи)

Протоколи динамічної маршрутизації:

- RIP (Routing Information Protocol) - протокол передачі маршрутної інформації, маршрутизатори динамічно створюють маршрутні таблиці.
- OSPF (Open Shortest Path First) - протокол "Відкрий найкоротший шлях першим", є внутрішнім протоколом маршрутизації.
- IGP (Interior Gateway Protocols) - внутрішні протоколи маршрутизації, поширює маршрутну інформацію всередині однієї автономної системи.
- EGP (Exterior Gateway Protocols) - зовнішні протоколи маршрутизації, поширює маршрутну інформацію між автономними системами.
- BGP (Border Gateway Protocol) - протокол граничних маршрутизаторів.
- ICMP (Internet Control Message Protocol) - розширення протоколу IP, дозволяє передавати повідомлення про помилку або перевірочні повідомлення.

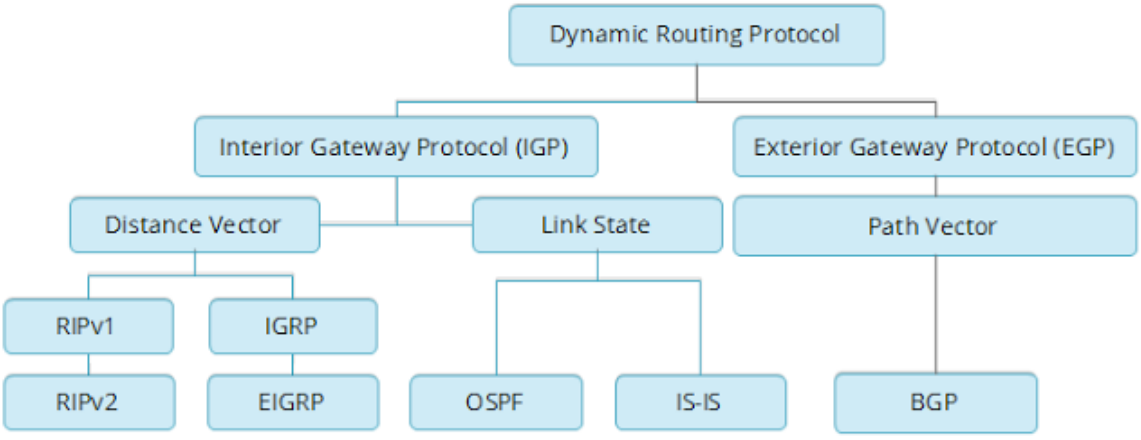

Рисунок 3.4. Протоколи динамічної маршрутизації

Всі протоколи обміну маршрутною інформацією стека TCP / IP відносяться до класу адаптивних протоколів, які в свою чергу діляться на дві групи, кожна з яких пов'язана з одним з наступних типів алгоритмів:

- дистанційно-векторний алгоритм (Distance Vector Algorithms, DVA)
- алгоритм стану зв'язків (Link State Algorithms, LSA).

В алгоритмах дистанційно-векторного типу кожен маршрутизатор періодично і широкомовно розсилає по мережі вектор відстаней від себе до всіх відомих йому мереж. Під відстанню зазвичай розуміється число проміжних маршрутизаторів через які пакет повинен пройти перш, ніж потрапить у відповідну мережу. Може використовуватися і інша метрика, що враховує не тільки число перевалочних пунктів, але і час проходження пакетів по зв'язку між сусідніми маршрутизаторами. Отримавши вектор від сусіднього маршрутизатора, кожен маршрутизатор додає до нього інформацію про відомі йому інші мережі, про які він дізнався безпосередньо (якщо вони підключені до його портів) або з аналогічних оголошень інших маршрутизаторів, а потім знову розсилає нове значення вектора по мережі. В кінці-кінців, кожен маршрутизатор дізнається інформацію про наявні в інтермережі мережах і про відстань до них через сусідні маршрутизатори.

Дистанційно-векторні алгоритми добре працюють тільки в невеликих мережах. У великих мережах вони засмічують лінії зв'язку інтенсивним широкомовним трафіком, до того ж зміни конфігурації можуть відпрацьовуватися за цим алгоритмом не завжди коректно, так як маршрутизатори не мають точного уявлення про топологію зв'язків в мережі, а мають у своєму розпорядженні тільки узагальнену інформацію - вектором дистанцій, до того ж отриманої через посередників.

Найбільш поширеним протоколом, заснованим на дистанційно-векторному алгоритмі, є протокол RIP.

3.2 Протокол RIP

Протокол RIP (Routing Information Protocol) відноситься до класу IGP. Протокол RIP був спочатку визначений у документі RFC 1058 в 1982 році як частина стека протоколів TCP / IP. Став стандартним протоколом маршрутизації всередині автономної системи.

Рисунок 3.5. Взаємодія протоколів машрутизації

Його основні характеристики:

• В якості метрики протоколом RIP використовується кількість переходів (хопів) між маршрутизаторами, необхідне для досягнення мережі-одержувача.

• Якщо кількість переходів стає довше 15 - пакет відкидається;

• Кожен RIP-маршрутизатор за замовчуванням віщає в мережу свою повну таблицю маршрутизації раз в 30 секунд, досить сильно навантажуючи низькошвидкісні лінії зв'язку;

• RIP працює на 4 рівні (рівень додатки) стека TCP / IP, використовуючи UDP порт 520.

Цей протокол маршрутизації призначений для порівняно невеликих і відносно однорідних мереж. В якості метрики використовується кількість переходів (тобто число маршрутизаторів, які повинна пройти дейтаграма, перш ніж досягне одержувача). Маршрутизатори, що підтримують протокол RIP, завжди вибирають шлях з найменшим числом переходів і записують його в таблицю маршрутизації.

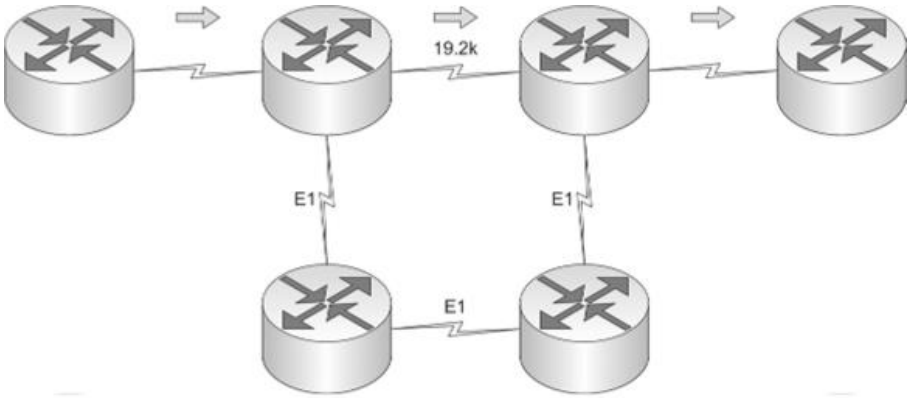

Рисунок 3.6. Метрика маршрута в протоколе RIP

На рис. 3.6. маршрут з пропускною здатністю, що дорівнює 19,2 кбіт/с, включає в себе три переходи. Нижній альтернативний маршрут по каналах зв'язку E1 включає п'ять переходів. Оскільки вибір маршруту в протоколі RIP грунтується виключно на кількості переходів, то в даному випадку в таблицю маршрутизації буде записаний маршрут з пропускною спроможністю 19,2 Кбіт/с замість більш швидких каналів E1.

Принцип функціонування протоколу:

Етап 1 - створення мінімальної таблиці. У початковому стані на кожному маршрутизаторі програмним забезпеченням стека TCP/IP автоматично створюється мінімальна таблиця маршрутизації, в якій враховуються тільки безпосередньо приєднані мережі. Таблиця маршрутизації RIP містить по запису на кожен маршрут. Запис повинен включати в себе:

- IP-адреса місця призначення.

- Метрика маршруту (від 1 до 15, а число кроків до місця призначення).
- IP-адреса найближчого маршрутизатора (gateway) по дорозі до місця призначення.
- Таймери маршруту

Етап 2 - розсилка мінімальної таблиці сусідам. Після створення своїх мінімальних таблиць, маршрутизатор починає розсилати своїм сусідам повідомлення протоколу RIP. Повідомлення, які передаються в дейтаграммах UDP, включають в себе інформацію про кожну мережі: її IP-адреса і відстань до неї від передавального маршрутизатора.

Етап 3 - отримання RIP-повідомлень від сусідів і обробка отриманої інформації. Наш маршрутизатор, після отримання повідомлень від сусідніх маршрутизаторів, збільшує кожне поле метрики на 1 і запам'ятовує, через який порт і від якого маршрутизатора отримана інформація, після порівнює значення зі своєю таблицею.

Етап 4 - розсилка нової таблиці сусідам. Сконфігуровану таблицю маршрутизатор знову відправляє всім своїм сусідам. У ній зберігається інформація не тільки про мережі, до яких маршрутизатор підключений безпосередньо, а й про віддалених, про які він дізнався від сусідніх маршрутизаторів на другому етапі. Тут починає ставати зрозуміло, чому протокол RIP використовується в основному в невеликих мережах.

Етап 5 - отримання таблиць і обробка отриманої інформації. Тут все, як на 3 етапі - маршрутизатор отримує таблицю і порівнює зі своєю, вносячи зміни.

Періодично (раз в 30 сек) кожен маршрутизатор посилає широкомовно копію своєї маршрутної таблиці всім сусідам-маршрутизаторів, з якими безпосередньо пов'язаний. Маршрутизатор-одержувач переглядає таблицю. Якщо в таблиці присутній новий шлях або повідомлення про більш короткий маршрут, або відбулися зміни довжин шляху, ці зміни фіксуються одержувачем у своїй маршрутній таблиці.

Протокол RIP повинен бути здатний обробляти три типи помилок:

- Циклічні маршрути.
- Для придушення нестабільності RIP повинен використовувати мале значення максимально можливого числа кроків (не більше 16).
- Повільне поширення маршрутної інформації по мережі створює проблеми при динамічній зміні маршрутної ситуації (система не встигає за змінами). Мале граничне значення метрики покращує збіжність, але не усуває проблему.

Невідповідність маршрутної таблиці реальної ситуації характерно не тільки для RIP, але характерно для всіх протоколів, що базуються на векторі відстані, де інформаційні повідомлення актуалізації несуть в собі тільки пари кодів: адреса місця призначення і відстань до нього.

Основна перевага алгоритму вектора відстаней - його простота. Дійсно, в процесі роботи маршрутизатор спілкується тільки з сусідами, періодично обмінюючись з ними копіями своїх таблиць маршрутизації. Отримавши інформацію про можливі маршрути від всіх сусідніх вузлів, маршрутизатор вибирає шлях з найменшою вартістю і вносить його в свою таблицю.

Кожному маршруту ставиться у відповідність таймер тайм-ауту і "збирача сміття". Тайм-аут-таймер скидається кожен раз, коли маршрут ініціалізується або коригується. Якщо з часу останньої корекції пройшло 3 хвилини або отримано повідомлення про те, що вектор відстані дорівнює 16, маршрут вважається закритим. Але запис про нього не стирається, поки не закінчиться час "прибирання сміття" (2хв). При появі еквівалентного маршруту перемикання на нього не відбувається, таким чином, блокується можливість осциляції між двома або більше рівноцінними маршрутами.

Повідомлення протоколу складаються із заголовка та маршрутних записів (Route Entries, RTE) рис. Зазвичай, в повідомлені протоколу міститься не більше 25 маршрутних записів. Формат повідомлення протоколу RIP має вигляд:

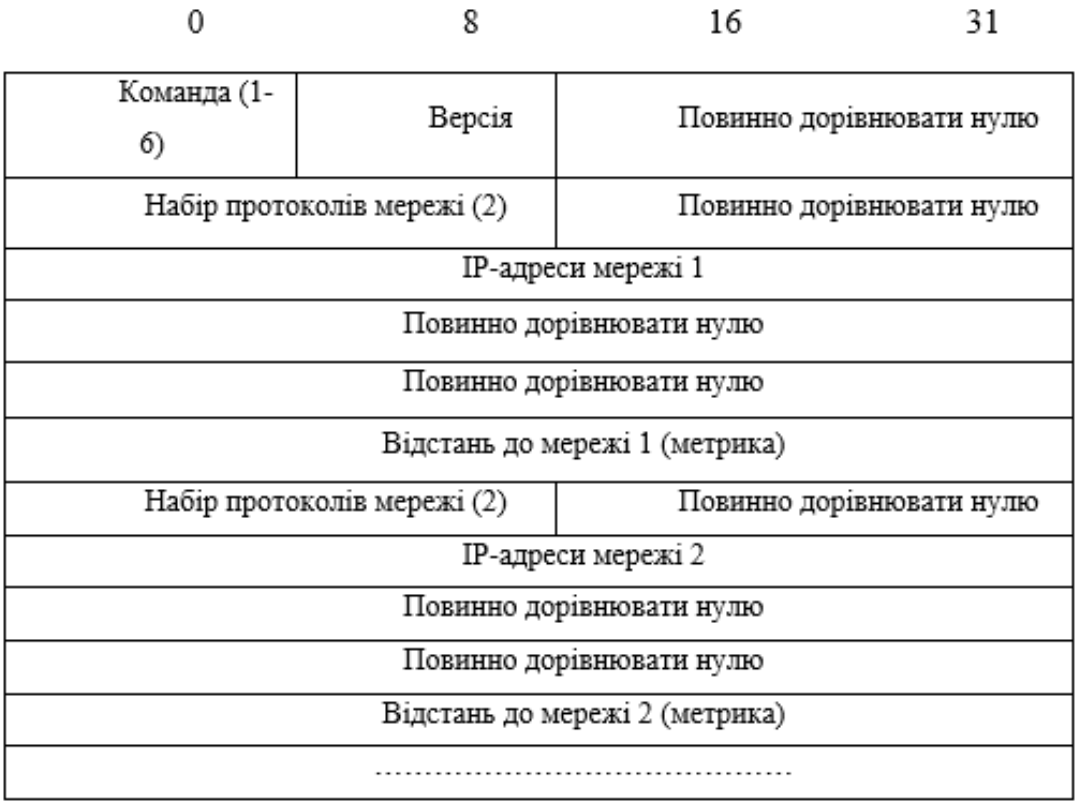

Рисунок 3.7. Формат повідомлення протоколу RIP

Поле команда може приймати наступні значення:

1. Запит на отримання часткової чи повної маршрутної інформації;

2. Відгук, що містить інформацію про відстані з маршрутної таблиці відправника;

3. Включення режиму трасування;

4. Вимкнення режиму трасування;

5-6. Зарезервовані для внутрішніх цілей SUN Microsystem.

Поле версія - вказує версію протоколу RIP (1чи 2).

Поле набір протоколів мережі – вказує ціле число кроків до даної мережі (від 1 до 15)

Поле відстань до мережі - містить ціле число кроків (від 1 до 15) до даної мережі.

При реалізації RIP можна виділити наступні режими:

- Ініціалізація, визначення всіх "живих" інтерфейсів шляхом посилки запитів, отримання таблиць маршрутизації від інших маршрутизаторів. Часто використовуються широкомовні запити.
- Отримано запит. Залежно від типу запиту надсилається адресату повна таблиця маршрутизації, або проводиться індивідуальна обробка.
- Отриманий відгук. Проводиться корекція таблиці маршрутизації (видалення, виправлення, додавання).
- Регулярні корекції. Кожні 30 секунд вся або частина таблиці маршрутизації надсилається всім сусіднім маршрутизаторам. Можуть посилатися і спеціальні запити при локальній зміні таблиці.

Недоліки RIP:

- RIP не працює з адресами підмереж;
- RIP вимагає багато часу для відновлення зв'язку після збою в маршрутизаторі (хвилини). В процесі встановлення режиму можливі цикли;
- Число кроків важливий, але не єдиний параметр маршруту, та й 15 кроків не межа для сучасних мереж.
- Оскільки в якості транспортного протоколу використовується протокол негарантованої доставки UDP, протокол RIP не має можливості виробляти гарантовану передачу маршрутних оновлень

RIP v.1 не підтримує маски, він поширює між маршрутизаторами інформацію тільки про номерах мереж і відстанях до них, але не про масках цих мереж, вважаючи, що всі адреси належать до стандартних класів A, B або C. RIP v .2 передає дані про масках мереж, тому він більшою мірою відповідає сучасним вимогам.

Протокол RIPv2 – є розширенням протоколу RIP v.1. Він не вніс глобальних змін в механізм чи повідомлення, а лише додав можливість передачі додаткової інформації. Зміна формату заголовка пакету RIPv2 торкнулися лише поля «Версія» та тих полей, які раніше не використовувалися.

Так, в новій версії протоколу з'явилася можливість аутентифікації передаваємих повідомлень, для чого і використовується перший маршрутний запис у заголовку пакета. Крім того, стало можливим розрізняти внутрішні маршрути (отримані через RIP) від зовнішніх (отриманих від інших протоколів маршрутизації, таких як EGP, BGP). В новій версії RIP стало можливим за допомогою поля Маски підмережі розрізнити не тільки мережі, але й підмережі. В цілях зменшення полоси пропускання мережі протокол RIPv2 замість адреса broadcast використовує multicast-адрес – 224.0.0.9.

3.3 Протокол IGRP

Протокол IGRP - протокол маршрутизації, розроблений компанією Cisco, для своїх багатопротокольних маршрутизаторів в середині 80-х років для маршрутизації в межах автономної системи (AS), що має складну топологію і різні характеристики смуги пропускання і затримки. IGRP є протоколом внутрішніх роутерів (IGP) з вектором відстані.

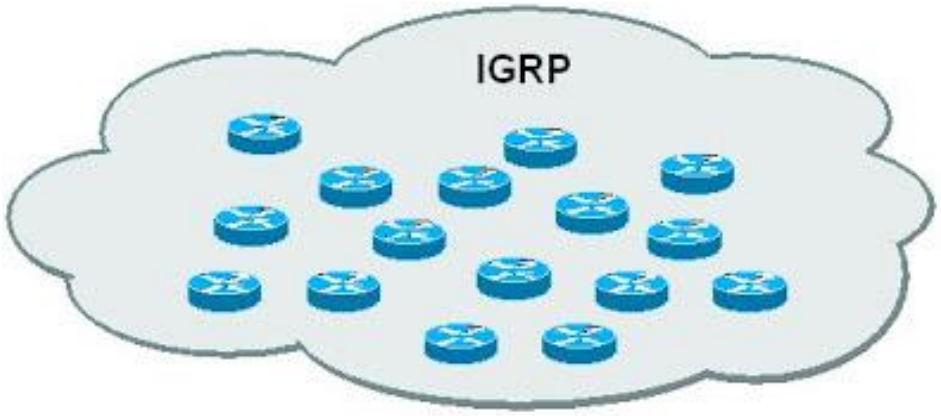

Рисунок 3.8. Протокол IGRP

Використання протоколу маршрутизації IGRP дозволяє визначати і обслуговувати кілька паралельних маршрутів, які пов'язують одну пару джерело - приймач. Суттєвою особливістю даного протоколу маршрутизації є те, що ці маршрути не обов'язково повинні мати однакову метрику для того, щоб бути використаними в якості компонентів єдиного інтегрального каналу.

Для забезпечення мінімального часу реагування протоколу на зміни, які відбуваються в системі, і запобігання утворенню циклів маршрутизації, в протоколі IGRP використані наступні рішення:

- Flash updates - керовані оновлення передаються в момент виникнення змін в мережі
- Hold down timers - спеціальні таймери використовуються для того, щоб через різницю в часі проходження керованих оновлень по мережі в ній не виникли петлі маршрутизації. «Свіжі» маршрути не використовуються для передачі пакетів до закінчення інтервалу часу, величина якого визначається даним таймером.
- Split horizon - для запобігання виникненню циклів оновлення для маршрутів, які були отримані з певного напряму не повинні передаватися в цьому напрямку.
- Poison reverse - зростання метрики маршруту зазвичай є наслідком існування петлі маршрутизації. Для блокування маршрутів, метрика яких починає неухильно зростати, їм зазвичай присвоюється значення метрики, яке відповідає нескінченності.

Найбільш істотною відмінністю протоколу IGRP від першої версії протоколу RIP була наявність комплексного критерію оцінки якості маршруту - метрики. У протоколі RIP, в якості метрики, виступала кількість проміжних вузлів (маршрутизаторів) до мережі призначення. У протоколі IGRP використовується композитна метрика, що обчислюється на основі:

- ширини смуги пропускання – швидкість каналу, яка вимірюється кількістю переданих біт в секунду.
- часу затримки - час доставки трафіку до одержувача в незавантаженої мережі.
- рівня завантаження каналу - показує, яка частина пропускної здатності зайнята зараз.
- надійності каналу - визначається кількістю помилок при передачі.

Зазвичай використовуються тільки перші дві, а рівень завантаження і надійність відкидаються. Значення всіх цих параметрів статично задаються в конфігурації маршрутизатора, і не змінюються динамічно в процесі його роботи.

Протокол IGRP передбачає широкий діапазон значень метрик. Наприклад, надійність і завантаженість каналу зв'язку можуть приймати будь-яке значення в інтервалі від 1 до 255. Пропускна здатність каналу може лежати в інтервалі від 1200 біт / с до 10 Гбіт / с. Час затримки задається позитивним цілим числом, що не перевищує 2^{24}. Такі широкі діапазони метрик дозволяють виробляти дуже точне їх регулювання у великій мережі з мінливою продуктивністю. При цьому адміністратор сам визначає необхідний набір метрик.

У порівнянні з протоколами RIP, протокол IGRP має такі переваги:

- при розрахунку метрики враховує пропускну здатність каналів зв'язку
- є більш масштабованим і гнучким, що дозволяє застосовувати його у великих мережах зі складною топологією.

3.3 Протокол EIGRP

Фірма Cisco розробила протокол EIGRP (Enhanced Interior Gateway Routing Protocol, покращений IGRP). Він об'єднує в собі переваги алгоритмів вектора відстані і стану каналу.

До його переваг відносяться: невеликий службовий трафік, швидке відновлення після змін в мережевій топології (фірма стверджує, що час збіжності, навіть у великих мережах, становить кілька секунд) і можливість використання маски підмережі в мережах IP.

Протокол EIGRP є першою реалізацією алгоритму DUAL (Distributed Update Algorithm, алгоритм розподіленого оновлення), який дозволяє маршрутизатору відновлювати свою працездатність відразу ж після зміни в мережевий топології, що значно збільшує надійність розподіленої мережі. У

більшості випадків маршрутизатори, що працюють по протоколу EIGRP, перебудовуються відповідно до нової топологією менше, ніж за одну секунду.

Таким чином, хоча протокол EIGRP і перейняв алгоритм вектора відстані від протоколу IGRP, він має можливості протоколів, що працюють за алгоритмом стану каналу, таких як IS-IS і OSPF. Протокол підтримує маски підмереж змінної довжини, що дозволяє організації більш ефективно використовувати виділений їй адресний простір. Протоколи маршрутизації RIP і IGRP не підтримують передачу інформації про маски підмережі, тому для коректної роботи таких маршрутизаторів в мережі повинні бути однакові маски підмереж.

Протокол маршрутизації EIGRP має чотири базових складових:

- виявлення сусіда - маршрутизатори динамічно отримують інформацію про інші маршрутизатори, що знаходяться в мережах, підключених до них безпосередньо. Маршрутизатори також повинні вміти визначати, що їх сусіди недосяжні. Цей процес виконується при низькому завантаженні мережі за допомогою періодичної посилки невеликих пакетів Hello. Після того як пакет отриманий, маршрутизатор вважає, що його сусід функціонує нормально. Потім сусідні маршрутизатори обмінюються маршрутною інформацією.
- надійний транспортний протокол (Reliable Transport Protocol, RTP) - відповідає за гарантовану доставку повідомлень протоколу EIGRP всім сусідам. Даний процес підтримує як одиничну, так і групову адресацію. Однак надійність не є неодмінною умовою доставки. Деякі повідомлення можуть передаватися з гарантією доставки, а деякі - ні. Наприклад, в мережі з підтримкою пакетного передавання даних (Ethernet) немає необхідності надсилати повідомлення Hello всім сусідам з гарантією доставки. Замість цього маршрутизатор може послати одне повідомлення групі сусідів із зазначенням, що отримання даного повідомлення можна й не підтверджувати. Це прискорює процес обміну і гарантує, що час збіжності буде малим, навіть в разі використання каналів зв'язку з різними швидкостями. Інші повідомлення, наприклад, про відновлення маршрутизації, вимагають підтвердження; це вказується в самому повідомленні.

- алгоритм DUAL - визначає шлях передачі трафіку. Він відстежує інформацію про маршрути, що отримується від всіх сусідів, і потім вибирає маршрут до так званого «можливого спадкоємця». Спадкоємець - це сусідній маршрутизатор, який має найменшу метрику до одержувача і який гарантовано не є частиною петлі маршрутизації.
- модуль, що залежить від протоколу - відповідає за взаємодію з певним протоколом мережевого рівня. Наприклад, при використанні протоколу IP даний модуль відповідає за інкапсуляцію повідомлень EIGRP в IP-дейтаграми.

Переваги EIGRP в порівнянні з IGRP:

- Швидка збіжність
- Підтримка CIDR (безкласова адресація) і VLSM (маска підмережі змінної довжини)
- Використовує досконаліший алгоритм DUAL (Diffusing Update Algorithm), для визначення якості того чи іншого маршруту.
- Може використовувати маршрути інших протоколів маршрутизації.

При побудові розподіленої мережі на базі протоколів маршрутизації IGRP або EIGRP необхідно враховувати, що їх підтримка реалізована, в основному, тільки в маршрутизаторах фірми Cisco. Протокол EIGRP може забезпечити менший час збіжності, ніж протокол IGRP, але налаштовувати його складніше. Крім того, для отримання максимального ефекту від цього протоколу потрібно продуктивний маршрутизатор з великим об'ємом оперативної пам'яті.

3.4 Алгоритми стану зв'язків. Протокол OSPF

Існує два класи протоколів маршрутизації всередині автономних систем: Distance Vector, до якого відносяться RIP, EIGRP і Link State, до якого відносяться OSPF і IS-IS.

Ідеологія Link State має на увазі, що кожен маршрутизатор повинен не просто знати найкращі маршрути в усі вилучені мережі, але і мати в пам'яті

повну карту мережі з усіма існуючими зв'язками між іншими маршрутизаторами в тому числі. OSPF - найбільш поширений протокол маршрутизації.

Відкритий протокол, який базується на алгоритмі пошуку найкоротшого шляху (Open shartest Path First - OSPF) є протоколом маршрутизації, розробленим для мереж IP робочою групою Internet Engineering Task Force (IETF), що займається розробкою протоколів для внутрішньо-системних роутерів (IGP).

Як видно з його назви, OSPF має дві основні характеристики. Перша з них - це те, що протокол є відкритим, тобто його специфікація є суспільним надбанням. Специфікація OSPF опублікована в форумі Запиту для Коментаря (RFC) 1247. Друга – протокол базується на алгоритмі SPF.

OSPF є протоколом маршрутизації з оголошенням стану про канал (Link-state). Це означає, що він вимагає відправки оголошень про стан каналу (Link-state advertisement - LSA). В оголошення LSA протоколу OSPF включається інформація про підключені інтерфейси, про використаних показників і про інших змінних. У міру накопичення роутерами OSPF інформації про стан каналу, вони використовують алгоритм SPF для розрахунку найкоротшого шляху до кожного вузла.

Будучи алгоритмом з оголошенням стану каналу, OSPF відрізняється від RIP і IGRP, які є протоколами маршрутизації з вектором відстані. Роутери, що використовують алгоритм вектора відстані, відправляють всю або частину своєї таблиці маршрутизації в повідомлення про коректування маршрутизації, але тільки своїм сусідам. На відміну від RIP, OSPF може працювати в межах деякої ієрархічної системи. Найбільшим об'єктом в цій ієрархії є - автономна система (AS). OSPF є протоколом маршрутизації всередині AS, хоча він і здатний приймати маршрути з інших AS і відправляти маршрути в інші AS.

Будь-яка AS може бути розділена на ряд областей (area). Область - це група суміжних мереж і підключених до них хостів. Роутери, що мають кілька інтерфейсів, можуть брати участь в декількох областях. Роутери однієї зони не

знають топологію мережі іншої зони, тобто не отримують оновлення з іншої зони і таким чином зменшується навантаження на маршрутизатор.

Слід виділити спеціальні маршрутизатори, які відіграють певну роль при поділі на зони:

• У OSPF зона 0 (Area 0) завжди є магістральною (Backbone router, BR), до якої підключаються інші зони. Зв'язок між зонами завжди здійснюється тільки через магістральну зону.

• Прикордонний маршрутизатор (Area Border Router, ABR) - включається на стику 2-х і більше зон.

• Внутрішній маршрутизатор (Internal Router) - звичайний внутрізонний маршрутизатор.

• Прикордонний маршрутизатор автономної мережі (AS Boundary router, ASBR) - підключається на стику різних автономних систем.

На рис. 3.9. показаний приклад поділу мережі на області в разі використання протоколу OSPF:

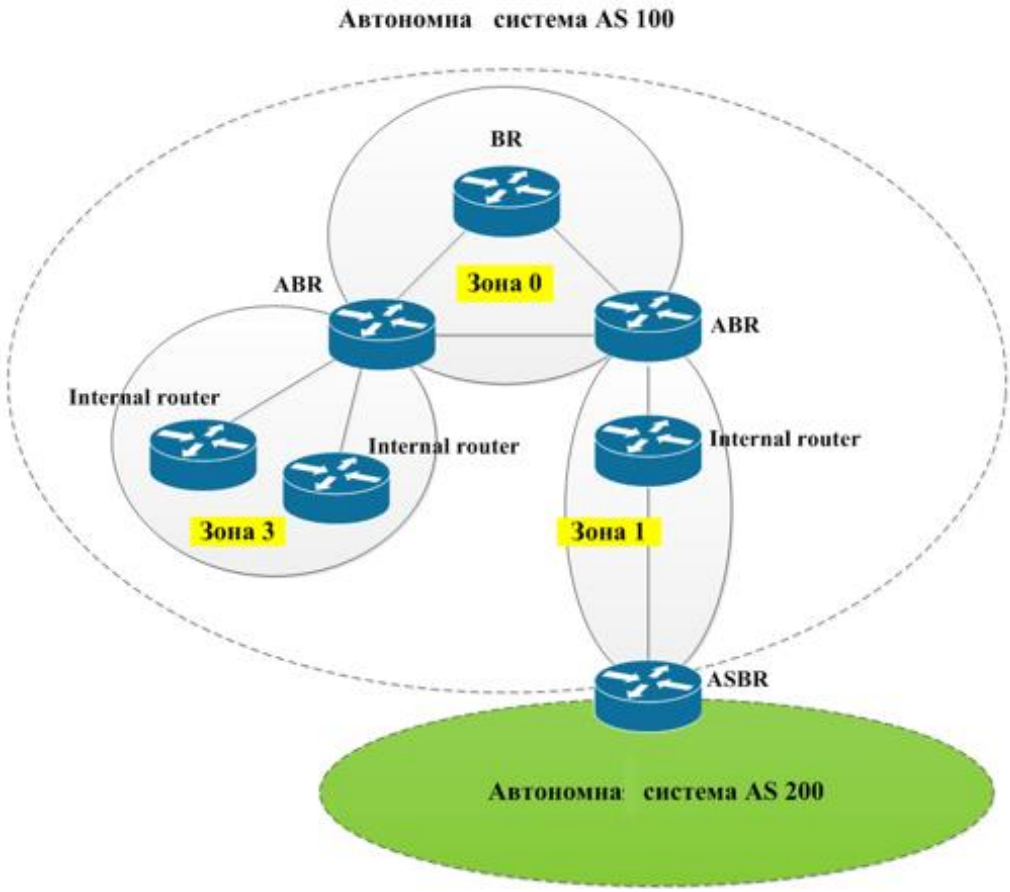

Рисунок 3.9. Поділ мережі на області з використанням протоколу OSPF

Топологічна база даних фактично являє собою загальну картину мережі по відношенню до роутера. Топологічна база даних містить набір LSA, отриманих від усіх роутерів, які перебувають в одній області. Оскільки роутери однієї області колективно користуються однією і тією ж інформацією, вони мають ідентичні топологічні бази даних.

Термін «домен» використовується для опису частини мережі, в якій всі роутери мають ідентичну топологічну базу даних. Термін «домен» часто використовується замість AS.

Топологія області є невидимою для об'єктів, що перебувають поза цією областю. Шляхом зберігання топологією областей окремо, OSPF домагається меншого трафіку маршрутизації, ніж трафік для випадку, коли AS відділена на області.

При роботі протоколу OSPF в кожному маршрутизаторі створюються 3 таблиці, необхідні для нормальної роботи мереж:

- Таблиця суміжності або таблиця сусідів (Adjacency table) - містить всіх безпосередньо підключених сусідів;
- Топологічна таблиця (Link State Data Base, LSDB) - містить інформацію про всі маршрутизатори своєї зони і активних інтерфейсів цих маршрутизаторів. Всі маршрутизатори однієї зони мають однакову таблицю;
- Таблиця маршрутизації (Route table) - обчислюється алгоритмом SPF на основі інформації з топологічної таблиці

Поділ на області призводить до утворення двох різних типів маршрутизації (внутрішня і між областями) OSPF, які залежать від того, чи знаходяться джерело і пункт призначення в одній і тій же або різних областях.

Магістральна або стрижнева зона OSPF (backbone) відповідає за розподіл маршрутної інформації між областями. Вона включає в себе всі роутери границі області, мережі, які не належать повністю до будь-якої з областей, і підключені до них роутери.

Граничні роутери AS, що використовують OSPF, дізнаються про зовнішні роутери через протоколи зовнішніх роутерів, таких як (EGP) або (BGP), або через інформацію про конфігурацію.

Принцип роботи OSPF:

- Маршрутизатор, підключений до джерела живлення, ініціалізує свої структури даних про протоколи маршрутизації, а потім очікує індикації від протоколів нижчого рівня про те, що його інтерфейси працездатні;
- Після отримання підтвердження маршрутизатори кожні 10 обмінюються маленькими HELLO-пакетами;
- Обмінявшись пакетами, вони встановлюють сусідські відносини, додаючи кожен один одного в свою локальну таблицю сусідів;
- Маршрутизатори збирають стан всіх своїх лінків (зв'язків з сусідами), що включають в себе id Маршрутизатора, id сусіда, мережу, тип мережі, метрику і формують пакет, званий LSA (Link State Advertisement).
- Маршрутизатор розсилає LSA своїм сусідам, ті поширюють LSA далі.
- Кожен маршрутизатор, який отримав LSA додає в свою локальну табличку LSDB (Link State Database) інформацію з LSA.
- У LSDB накопичується інформація, про всі пари з'єднаних в мережі маршрутизаторів, тобто кожен рядок таблиці - це інформація виду: «Маршрутизатор А має з'єднання зі своїм сусідом маршрутизатором В, між ними мережа така-то з такими-то властивостями».
- Після обміну LSA, кожен маршрутизатор знає про всі лінки, на підставі пар будується повна карта мережі, що включає всі маршрутизатори та всі зв'язки між ними.
- На підставі цієї карти кожен маршрутизатор індивідуально шукає найкоротші з точки зору метрики маршрути в усі мережі та додає їх в таблицю маршрутизації.

OSPF пакет поміщається в IP пакет, у якого адреса відправника – це адреса відправника пакету маршрутизатора, а адреса одержувача, як правило,

мультикастового. Пакет поміщається у відповідний мультикастовий фрейм, наприклад, Ethernet. Слід звернути увагу, що OSPF безпосередньо інкапсулюється в IP з номером протоколу 89, а не в TCP або UDP.

Octet	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
00	Version #								Type								Packet Length															
04	Router ID																															
08	Area ID																															
12	Checksum																AuthType															
16	Authentication																															
20	Authentication																															
24	Data																															

Рисунок 3.10. Формат заголовку пакету OSPF

1. Версія протоколу – версія OSPF. Поточна версія для IPv4 = 2

2. Тип пакету – який тип пакету відправляється. Всього існує п'ять типів OSPF повідомлень:

- Hello - відправляються регулярно для пошуку сусідів і установки сусідських відносин;
- Database Description (DBD) - використовуються для перевірки синхронізації LSDB у сусідніх маршрутизаторів
- Link state request (LSR) - примусовий запит у якогось маршрутизатора його LSA. Може використовуватися, наприклад, коли маршрутизатор тільки включився і йому треба дізнатися поточні зв'язку в мережі, або, коли у маршрутизатора пропала мережа, і він хоче дізнатися чи немає у інших маршрутизаторів альтернативних маршрутів до неї.
- Link state update (LSU) - містить стани зв'язків маршрутизатора.
- Link State Acknowledgment (LSAck) - пакет-підтвердження, надсилається у відповідь на інші типи пакетів. Це пов'язано з тим, що OSPF не використовує протокол TCP і для надійної доставки потрібен свій власний механізм підтверджень.

3. Довжина пакету (Packet lenght) – в байтах, яка включає в себе і заголовок;

4. Ідентифікатор маршрутизатора (Router ID) – визначає який маршрутизатор відправив пакет;

5. Ідентифікатор зони (Area ID) – визначає в якій зоні згенерований пакет;

6. Контрольна сума (Checksum) – використовується для перевірки цілісності пакету OSPF, для виявлення помилок при передачі;

7. Тип аутентифікації (Authentication type) – тип аутентифікації, який використовується між маршрутизаторами:

- 0 – аутентифікація не використовується,
- 1 – аутентифікація відкритим текстом,
- 2 – MD5-аутентифікація.

8. Дані аутентифікації (Authentication) – використовується при аутентифікації маршрутизаторів.

9. Поле Дані відрізняється для різних типів пакетів OSPF:

- Hello – список відомих сусідів;
- DBD – містить сумарну інформацію бази даних станів каналів, яка включає в себе всі відомі ідентифікатори маршрутизаторів та її останні номера послідовностей (sequence number) та іншу інформацію.
- LSR – містить тип необхідного LSU та ідентифікатор маршрутизатора, у якого є цей LSU.
- LSU – містить повні записи оголошення про стан каналу. Декілька LSA можуть передаватися в одному пакеті оновлень.
- LSAck – поле даних пусте.

У порівнянні з протоколом RIP протокол маршрутизації OSPF має наступні переваги:

• алгоритм, що лежить в основі протоколу OSPF, дозволяє уникнути петель маршрутизації;

• в процесі свого функціонування протокол OSPF генерує значно менший мережевий трафік, ніж протокол RIP. Як наслідок, перехід з RIP на OSPF дозволить знизити навантаження на мережу;

• протокол OSPF для розсилки службових повідомлень використовує тільки групове мовлення (на відміну від протоколу R1P версії 1);

• протокол OSPF передбачає можливість розбиття корпоративної мережі на області. Області можуть, з одного боку, розглядатися як домени маршрутизації, з іншого боку, полегшують процес адміністрування підсистеми маршрутизації;

• протокол OSPF не має обмежень на кількість переходів між маршрутизаторами, що дозволяє його використовувати в корпоративних мережах будь-якого масштабу;

• реконфігурація таблиць маршрутизації, викликана змінами в структурі мережі, відбувається за дуже короткий період (значно швидше, ніж у випадку використання протоколу RIP).

OSPF завоював популярність не дивлячись на деякі його недоліки в порівнянні з EIGRP: меншу гнучкість, відсутність чіткого опису механізму підрахунку метрики, підвищені вимоги до ресурсів маршрутизатора. У той же час, у OSPF є і безліч переваг: ієрархічний дизайн мережі (реалізується за допомогою зон), зручність при налагодженні (так як можна бачити карту мережі).

3.5 Протокол IS-IS

Протокол IS-IS *(*Intermediate System to Intermediate System) або проміжна система до проміжної системі, є відкритим стандартним протоколом маршрутизації. *ISO* опублікувала стандарт як спосіб маршрутизації дейтаграм як частини їх стека OSI. Пізніше IETF перевидав стандарт і додав підтримку IP-маршрутів.

Між IS-IS і OSPF багато спільного. З одного боку, обидва є протоколами маршрутизації стану каналу, що означає, що вони обидва створюють «карту» мережі. Вони обидва заповнюють дані стану каналу через мережу і створюють базу даних стану каналу (LSDB). Крім того, вони обидва запускають алгоритм

Дейкстри, зазвичай згадується як алгоритм переваги найкоротшого шляху (SPF), на LSDB для обчислення найкоротших шляхів.

Але є дві масивні сили IS-IS. Перше - це масштабованість. Набагато простіше будувати великі мережі з IS-IS, ніж це з OSPF. Це робить його загальним вибором з постачальниками послуг щодо їх інфраструктури. Друга сила - це незалежний підхід до даних, які він несе. IS-IS несе корисне навантаження даних про досяжності, але здебільшого його не хвилює, що знаходиться в корисному навантаженню. Це те, що робить його корисним для таких протоколів, як FabricPath. На відміну від цього, OSPF здійснює лише маршрути IP. Коли з'явився IPv6, йому була потрібна цілком нова версія OSPF (OSPFv3) для перенесення маршрутів IPv6. У IS-IS такої проблеми немає.

IS - це проміжна система. Це зв'язок між проміжними системами або маршрутизаторами.

ES - це кінцева система. Це пристрій в мережі, такий як сервер або робоча станція. В оригінальній специфікації ES братиме участь в IS-IS. У нього не буде необхідності в DHCP або FHRP, так як у нього вже буде локальна таблиця маршрутизації.

CLNS (Мережева служба без встановлення з'єднань) - це мережева служба в стеці OSI. CLNP (мережевий протокол без встановлення з'єднання) - це протокол, який реалізує CLNS.

NSAP - це точка доступу до мережевого сервісу. Це адреса рівня 3 для пакетів CLNS. Це схоже на IP-адресу в стек TCP / IP. IS-IS використовує для зв'язку адреси NSAP, а не IP-адреси.

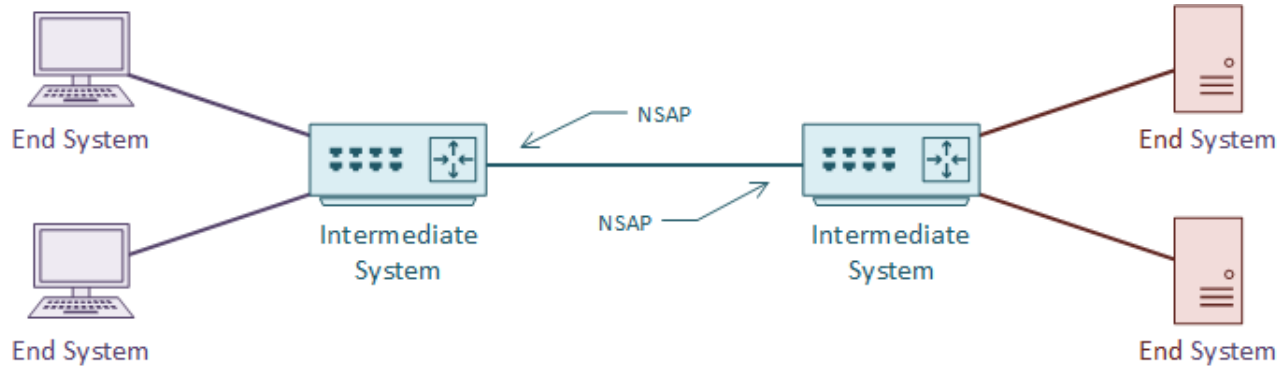

Рисунок 3.11. Модель роботи протоколу IS-IS

TLV, або Type Length Value, є полями корисного навантаження в IS-IS. Поля TLV містять інформацію про маршрут. IS-IS не дбає про те, що відбувається в цих областях, що робить його незалежним від протоколу.

IS-IS використовує CLNS для транспорту. Кожен маршрутизатор має адресу NSAP для відправки та отримання інформації про стан каналу. Інформація про стан каналу може містити кілька полів TLV.

Як і OSPF, IS-IS використовує вартість як метрику. У специфікації зазначено, що це може бути або широким, або вузьким значенням. Маршрутизатори Cisco підтримують лише широку метрику, яка використовує 24 біта для метрики посилання та 32 біта для метрики шляху.

Усі посилання за замовчуванням мають вартість 10. Це означає, що в реалізації за замовчуванням підрахунок хопу утворює метрику. Менеджер мережі повинен вибрати найбільш підходящу схему витрат.

Однією із спільних рис OSPF з IS-IS є використовує області. Області можуть бути або області магістралі, або нормальні області. Для підтримки цих концепцій маршрутизатор може бути одним із наступних типів:

- Уровень 1 - Маршрутизатор в нормальній області, який не підключається до іншої області
- Уровень 1-2 - Маршрутизатор в нормальній або магістральній області, який з'єднує різні області
- Уровень 2 - магістральний маршрутизатор, який не підключається до інших областей.

У наведеній нижче топології показаний приклад мережі з декількома областями (рис. 3.12.).

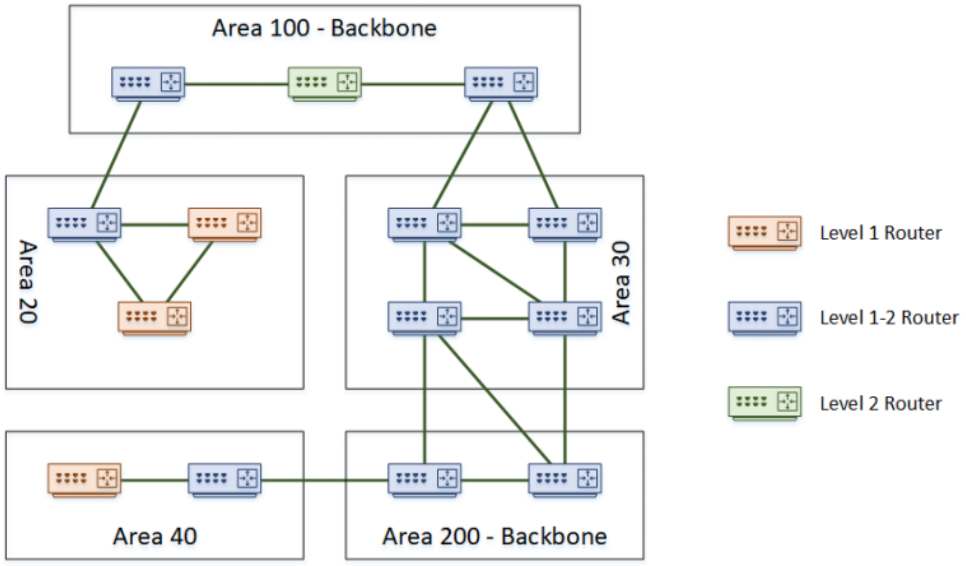

Рисунок 3.12. Області мережі з використанням протоколу IS-IS

У цій топології магістральна область не обмежена тим, щоб бути «областю 0», як в OSPF. У IS-IS будь-який номер області може бути основою. Також є можливість розбити магістраль. У цій топології як область 100, так і область 200 є основою. Ще одним цікавим моментом є те, що кордони області не перебувають на самих маршрутизаторах. Скоріше, межі області знаходяться між маршрутизаторами. Це відрізняється від OSPF, де маршрутизатор ABR або ASBR є кордоном.

3.6 Протокол EGP

EGP - Протокол зовнішніх роутерів (Exterior Gateway Protocol) є протоколом міждоменної досяжності, який застосовується в Internet. EGP документально оформлений в RFC 904, опублікованих в 1984 р.

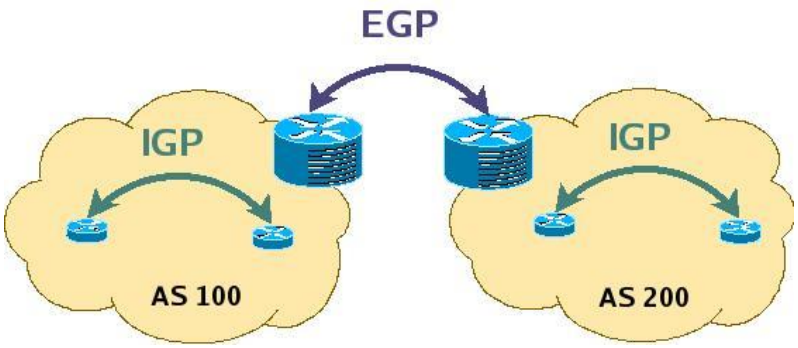

Рисунок 3.13 Протокол зовнішніх роутерів

Незважаючи на те, що EGP є динамічним протоколом маршрутизації, схема його роботи дуже проста. Він не може приймати інтелектуальних рішень про маршрутизації. Коригування маршрутизації EGP містять інформацію тільки про досяжності мереж. Іншими словами, вони вказують, що в певні мережі інформаційні пакети потрапляють через певні роутери.

EGP виконує три основні функції:

- Встановлення сусідських відносин,
- Підтвердження досяжності сусіда,
- Оновлення маршрутної інформації.

Для реалізації цих функцій протокол використовує систему наступних повідомлень:

- *Придбання сусіда (Neighbor acquisition).* Перш ніж почати отримувати інформацію від зовнішніх маршрутизаторів, необхідно встановити, який маршрутизатор є сусіднім. Ця операція складається з обміну повідомленнями типу «придбання сусіда» (відповідно запит / відповідь / відмова та ін.) Через стандартний механізм трьохходового квитування. Маршрутизатор передбачуваного сусіда також повинен підтримувати механізм повідомлень типу «придбання сусіда». Дане повідомлення включає в себе поле інтервалу вітання (hello interval) і поле інтервалу опитування (poll interval). Поле інтервалу вітання визначає період інтервалу перевірки працездатності сусідів. Поле інтервалу опитування визначає частоту коригування маршрутизації.

- *Досяжність сусіда (Neighbor reachability).* Для маршрутизаторів, що виконують функції зв'язку різних доменів мереж, важливо розташовувати останній інформацією про роботу своїх сусідів. Якщо маршрутизатор виявляє, що будь-якої шлюз не функціонує, йому необхідно негайно припинити потік даних до цього шлюзу. Для цих цілей і використовується даний вид повідомлень.

- *Опитування (Poll).* Для забезпечення правильної маршрутизації між AS, EGP повинен мати інформацію про відносне розташування віддалених хостів. Дані повідомлення дозволяють маршрутизаторам EGP отримувати інформацію про досяжності мереж, в яких знаходяться ці машини. Такі повідомлення мають, крім звичайного заголовка, тільки одне поле - поле мережі джерела IP (source network). Це поле визначає мережу, яка повинна використовуватися в якості контрольної точки опитування.

Будь-яка частина EGP-мережі Internet повинна являти собою структуру дерева, у якій стрижневий маршрутизатор є коренем, і в межах якого відсутні петлі між іншими AS (рис. 3.14). Це обмеження є основним обмеженням EGP. Воно стало причиною його поступового витіснення іншими, більш досконалими протоколами маршрутизації.

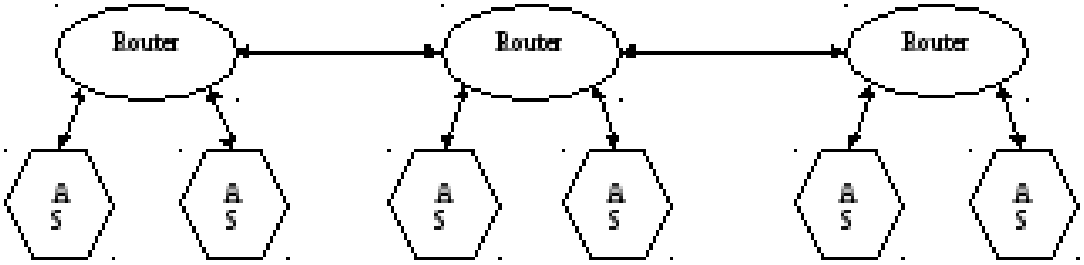

Рисунок 3.14. Структура мереж під управлінням EGP

Будь-яка частина EGP-мережі Internet повинна являти собою структуру дерева, у якій стрижневою маршрутизатор є коренем, і в межах якого відсутні петлі між іншими AS. Це обмеження є основним обмеженням EGP. Воно стало причиною його поступового витіснення іншими, більш досконалими протоколами маршрутизації.

Offset	0	7	8	15	16	31
0	EGP Version		Type		Code	Status
4	Checksum				Autonomous System	
8	Sequence				Data …	

Рисунок 3.15. Формат заголовка EGP-пакета

Номер версії EGP (EGP Version) - 8 біт - позначає поточну версію EGP і перевіряється прийомними пристроями для визначення відповідності між номерами версій відправника і одержувача.

Тип (Type) - 8 біт - позначає один з 5 типів повідомлень EGP.

Код (Code) - 8 біт - визначає відмінність між підтипами повідомлень.

Статус (Status) - 8 біт - містить інформацію про стан, що залежить від повідомлення. У число кодів стану входять коди нестачі ресурсів (insufficient resources), несправних параметрів (parameter problem), порушень протоколу (protocol violation) і ін.

Контрольна сума (Checksum) - 16 біт - використовується для виявлення можливих проблем, які могли з'явитися в пакеті в результаті його транспортування.

Номер автономної системи (Autonomous System Number) - 16 біт - позначає AS, до якої належить шлюз відправник.

Номер послідовності (Sequence Number) - 16 біт - дозволяє двом маршрутизаторам EGP, які обмінюються повідомленнями, співвідносити повідомлення запитів з повідомленнями відповідей. Коли визначено який-небудь новий сусід, номер послідовності встановлюється в вихідний нульовий значення і збільшується на одиницю з кожним новим транзакцією запит-відповідь.

Будучи першим протоколом зовнішніх роутерів, який отримав широке визнання в Internet, EGP зіграв важливу роль. На жаль, недоліки EGP стали більш очевидними після того, як Internet став більшою і досконалою мережею. Тому EGP в даний час не відповідає всім вимогам Internet та замінюється іншими протоколами зовнішніх роутерів, такими, як Протокол граничних роутерів (Border Gateway Protocol - BGP) і Протокол міждоменної маршрутизації (Inter-Domain Routing Protocol - IDRP)

3.7 Протокол BGP

Прикордонний (зовнішній) шлюзовий протокол (Border Gateway Protocol, BGP) версії 4 є сьогодні основним протоколом обміну маршрутною інформацією між автономними системами Інтернету. Він прийшов на зміну протоколу EGP1, що використовувався в той початковий період, коли Інтернет мав єдину магістраль. Ця магістраль була центральною автономною системою, до якої приєднувалися відповідно по деревовидній топологією всі інші автономні системи. Так як між автономними системами, при такій структурі, петлі виключалися, протокол EGP не робив ніяких заходів для того, щоб виключити зациклення маршрутів.

Отже, BGP - це протокол зовнішньої маршрутизації, що використовується для з'єднання двох AS. Схема виглядає приблизно так:

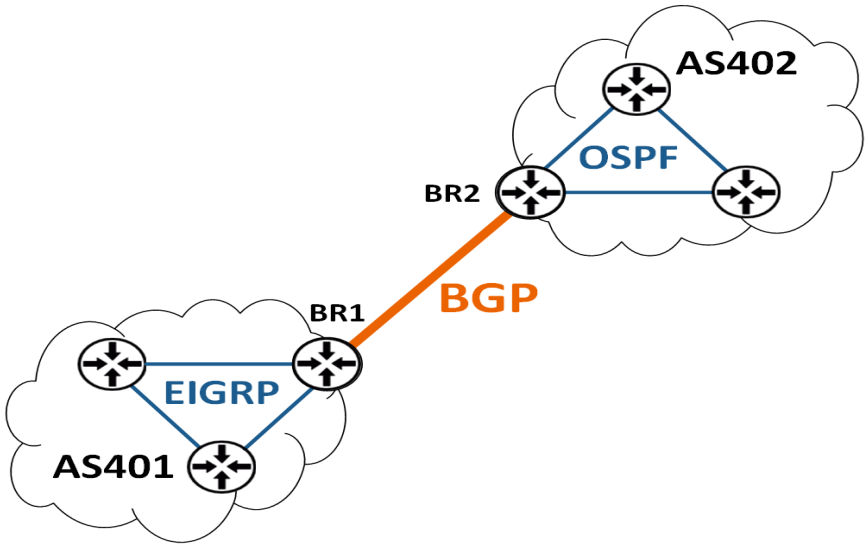

Рисунок 3.16. Протокол BGP

Так як BGP з'єднує автономні систем у всьому Інтернеті, то він повинен бути дуже надійним. Для ЦИХ цілей, на самому початку роботи, BGP-маршрутизатор ініціює встановлення TCP сесії на 179 порт до свого сусіда, відбувається стандартних обмін SYN і ACK.

Коли вказується сусід локального маршрутизатора, обов'язково вказується автономна система сусіда. За цією інформацією BGP визначає тип сусіда (рис. 3.17):

- Внутрішній BGP сусід (iBGP-сусід) - сусід, який знаходиться в тій же автономній системі, що і локальний маршрутизатор. iBGP-сусіди не обов'язково повинні бути безпосередньо пов'язані.
- Зовнішній BGP сусід (eBGP-сусід) - сусід, який знаходиться в автономній системі відмінній від локального маршрутизатора. За замовчуванням, eBGP-сусіди повинні бути безпосередньо пов'язані.

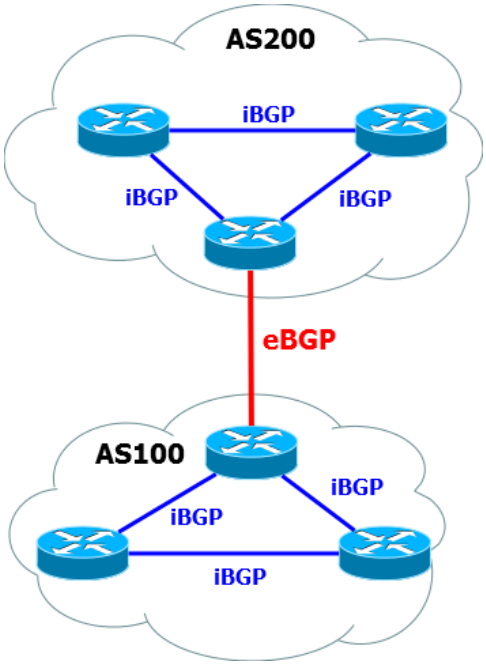

Рисунок 3.17. Тип сусіда за протоколом BGP

Тип сусіда мало впливає на установку відносин сусідства. Більш суттєві відмінності між різними типами сусідів проявляються в процесі відправки оновлень BGP і додаванні маршрутів в таблицю маршрутизації.

Процес встановлення відносин сусідства відбувається наступним чином:

1. Початковий стан BGP-сусідства - IDLE. Нічого не відбувається. BGP знаходиться в стані IDLE, якщо немає маршруту до BGP-сусідові;

2. BGP-маршрутизатор (їх також називають BGP-спікерами / speaker або BGP-ораторами) слухає і посилає пакети на 179-й TCP порт. Коли слухає - це стан CONNECT (в такому стані BGP знаходиться дуже недовго). Коли відправив і чекає відповіді від сусіда - це стан ACTIVE.

3. Маршрутизатор повинен отримати запит на TCP-з'єднання з адресою відправника. Для маршрутизатор відправника направляє TCP SYN на порт 179

сусіда, ініціюючи TCP-сесію. Інший маршрутизатор повертає TCP ACK, мовляв, все отримав, згоден і свій TCP SYN. Відправник теж звітує, що отримав SYN від сусіда. Після цього TCP-сесія встановлена.

4. Після того, як TCP-сесія встановлена, BGP-оратори починають обмін повідомленнями OPEN. У ньому передаються версія протоколу, номер AS, Hold Timer і Router ID. Hold timer - це час, протягом якого буде підтримуватися TCP-сесія.

5. Щоб BGP-сесія піднялася, повинні дотримуватися такі умови:

- Версії протоколу повинна бути однаковою.
- Номери AS в повідомленні OPEN повинні збігатися з настройками на віддаленій стороні.
- Ідентифікатори маршрутизаторів (Router ID) повинні відрізнятися

6. Якщо умови, перераховані раніше, не дотримуються, наприклад, не збігається інформація про номер AS, то повідомленням NOTIFICATION маршрутизатор, який отримав невірний ASN, повідомить про це свого сусіда і скине TCP-сесію.

7. Якщо ж всі умови дотримуються, то маршрутизатори, з певним інтервалом, починають висилати один одному повідомлення KEEPALIVE, що означають підтвердження параметрів, прийнятих в OPEN і повідомлення "я ще живий".

8. Нарешті, маршрутизатори можуть приступати до обміну маршрутної інформацією по засобам комунікації UPDATE. Структура даного повідомлення ділиться на дві частини:

- Path Attributes (Атрибути шляху). Тут вказується з якої AS надійшов маршрут, його походження і Next Hop для даного шляху.
- NRLI (Network Layer Reachability Information). Тут вказує інформація безпосередньо про мережах, які підлягають додаванню в таблицю маршрутизації, тобто IP-адреса мережі та її маска.

Повідомлення UPDATE передаватиметься кожен раз, коли один з маршрутизаторів отримає інформацію про нові мережах, а повідомлення KEEPALIVE протягом усього TCP-сесії.

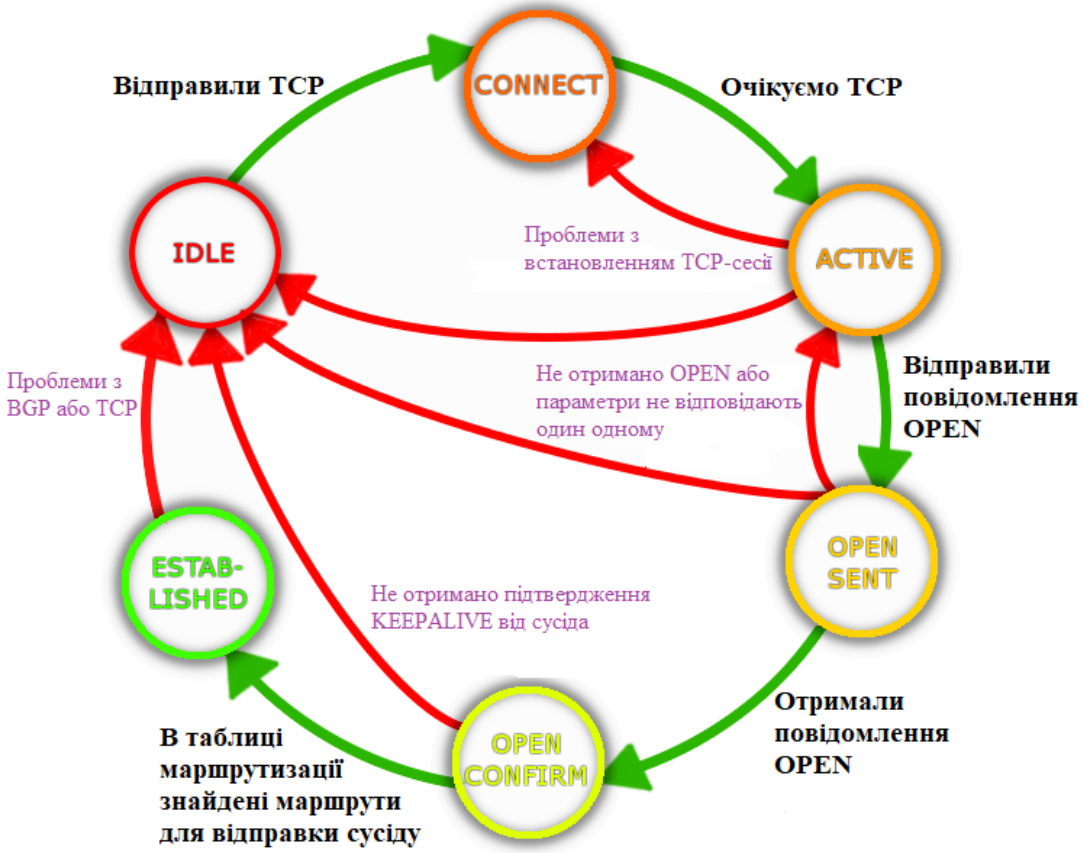

Рисунок 3.18. Процес встановлення відносин сусідства

Форматом заголовка повідомлення в BGP є поле маркера завдовжки 16 байт, за яким слідує поле довжини (2 байта) і поле типу (1 байт). На рис. 3.19 представлений формат заголовка повідомлення протоколу BGP:

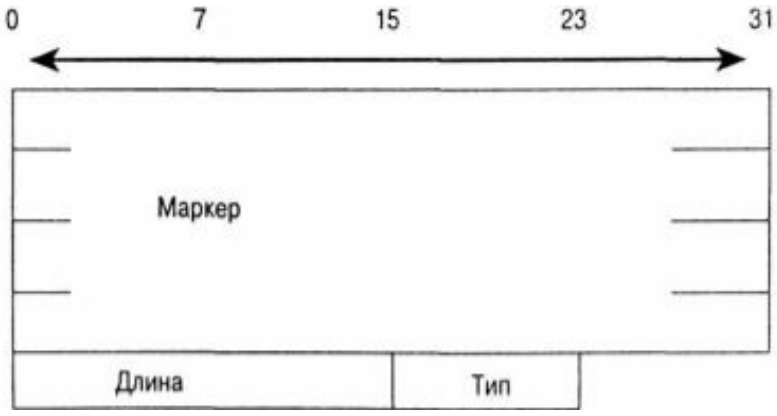

Рисунок 3.19. Формат заголовка повідомлення BGP

Поле маркера завдовжки 16 байт використовується для аутентифікації вхідних повідомлень BGP або для детектування втрати синхронізації між двома взаємодіючими по BGP маршрутизаторами. Поле маркера буває двох форматів:

- Якщо послано повідомлення типу OPEN або в ньому відсутня інформація про аутентифікації, то в полі маркера всі позиції виставляються в 1.
- В іншому випадку значення поля маркера обчислюється відповідно до використовуваним механізмом аутентифікації.

Поле довжини розміром 2 байти використовується для відображення повної довжини повідомлення BGP, включаючи заголовок. Найменша довжина повідомлення BGP становить 19 байт (16 + 2 + 1), а найбільша - 4096 байт.

Поле типу розміром 1 байт визначає тип повідомлення. Можливі такі значення:

- OPEN (Відкриття з'єднання)
- UPDATE (Оновлення маршрутної інформації)
- NOTIFICATION (Повідомлення про помилку)
- KEEPALIVE (Перевірка стану з'єднання)

Саме таким чином і працює маршрутизація в усьому Інтернеті. Історії відомо безліч інцидентів, коли неправильна робота протоколу BGP приводила до збоїв великих частин глобальної мережі, тому недооцінювати його важливість категорично не можна.

4 РОЗРАХУНОК ЗАТРИМКИ ЧАСУ В МЕРЕЖАХ NGN

4.1 Розрахунок часу затримки на основі моделі масового обслуговування для вузлів різного призначення

При обслуговуванні користувачів часто виникає необхідність у наданні певним категоріям системи послуг за пріоритетами. Цей фактор найбільш важливий при проектуванні інфокомунікаційних мереж. Класи пріоритетів вводяться для різних послуг і різних категорій абонентів. Необхідність вищих пріоритетів - це забезпечення команд і службових повідомлень, що застосовуються для управління процесами взаємодії елементів мережі, а також при управлінні мережею.

Розглянемо як приклад мережу каналів передачі даних зі швидкістю 9600біт/с. Будемо відмічати пакети даних індексом - *2*, а управляючі пакети (як правило меншої довжини) індексом - *1*.

Середня довжина пакетів даних 960 біт, тобто $1/\mu_2 = 0{,}1c$, а дисперсія $\sigma_2^2 = 2(1/\mu_2)^2$, або $E(\tau^2) = 3(1/\mu_2)^2$. З іншого боку всі керуючі пакети мають довжину 48 біт, отже, $1/\mu_1 = 5мс$. У прикладі з фіксованою довжиною пакетів $\sigma^2_1 = 0$, розглянемо систему обслуговування в порядку надходження з однією чергою, яка представляє початковий канал передачі даних.

Нехай *20%* загального навантаження створюється короткими управляючими пакетами, а *80%* - набагато довшими пакетами даних. Таким чином, маємо $\lambda_1 = 0{,}2\lambda$ та $\lambda_2 = 0{,}8\lambda$, де λ - загальна швидкість надходжень вхідного потоку в пакетах/секунду. Очевидно, що без пріоритетів робота системи обслуговування з комбінованим вхідним потоком може бути описана моделлю *M/G/1*. Інтенсивність комбінованого навантаження - $\rho = \rho_1 + \rho_2$. Оскільки пакети обох класів поступають випадково з інтенсивністю відповідно λ_1 і λ_2, другий момент комбінованого потоку зваженою сумою других моментів:

$$E(\tau^2) = \frac{\lambda_1}{\lambda} E(\tau_1^2) + \frac{\lambda_2}{\lambda} E(\tau_2^2), \qquad (4.1)$$

Нехай для визначеності ефективне значення ρ дорівнює *0,2.* Тоді загальна інтенсивність надходжень становить λ = *6,17* пакетів/секунду, і досить просто визначається середній час очікування для пакету будь-якого типу - *148* мс. Управляючі пакети довжиною *48* біт, які потребують для передачі *5* мс, часто можуть виявитися в черзі набагато довшими за довжиною *100*-мілісекундними інформаційними пакетами і повинні чекати передачі, в середньому *148* мс. Очевидним рішенням є надання управляючим пакетам вищого пріоритету, що дозволяє їм обійти при надходженні інформаційні пакети більш низького пріоритету і безпосередньо бути першими в черзі. Звичайно використовуються два типи пріоритетів: відносний і абсолютний. У першому випадку користувачі (пакети або виклики послуг) вищого пріоритету стають попереду користувачів (пакетів) нижчого пріоритету в черзі, але не витісняють їх. У разі абсолютного пріоритету, обслуговування користувачів з нижчим пріоритетом припиняється і продовжується лише після того, коли всі користувачі, що надійшли з вищим пріоритетом будуть обслужені. В даному випадку розглядається тільки відносні пріоритети. Покажемо, що надання відносного пріоритету управляючим пакетам в середньому скорочує їх час очікування вдвічі до *47,5* мс, збільшуючи при цьому час очікування інформаційних пакетів на незначну величину. Якщо це зменшення в реальних випадках виявиться недостатнім, може бути використаний абсолютний пріоритет. Проте, необхідно зазначити, що користувачі, обслуговування яких було перерване, повинні бути позначеними. Це викликає необхідність додаткової обробки, яка може привести до зменшення теоретичної ефективності, очікуваного від введення пріоритету. Для більшого узагальнення передбачимо, що в черзі чекають обслуговування *2r* класи користувачів. Інтенсивність потоків, що створюються ними - λ_1, λ_2, ..., λ_r, причому кожний з цих потоків - пуассонівський. Середній час обслуговування для *k*-того класу, *k = 1,2,..., r*, дорівнює *1/мk* .

Будемо вважати, що вищим пріоритетом володіє клас *1*, нижчим - клас *r* зі спаданням пріоритетів у послідовності зростання номера. Представимо розрахунок середнього часу очікування для будь-якого класу в припущенні, що пріоритети є відносними. Візьмемо для прикладу клас $\rho(1 \le \rho \le k)$. Нехай типовий користувач цього класу поступає в довільний момент часу t_0. Його випадковий час очікування W_p, що вимірюється від моменту надходження до початку обслуговування, залежить від трьох параметрів. Користувач, який поступив повинен чекати протягом випадкового проміжку часу T_0, поки закінчитися поточний час обслуговування користувача. Крім того, він повинен чекати випадкове число $T_к$ одиниць часу, поки закінчитися обслуговування всіх користувачів класу *k*, вищого або рівного класу *p*, які вже знаходилися в черзі в момент часу t_0. Нарешті, він повинен чекати випадковий час $T_к$ обслуговування користувачів кожного класу *k*, який вищій за клас *p* і надійшли протягом часу очікування W_p.

Об'єднуючи разом ці параметри, отримаємо:

$$Wp = T_0 + \sum_{k=1}^{P} T_k + \sum_{k=1}^{p-1} T'k \,. \tag{4.2}$$

Для визначення середнього часу очікування:

$$E(Wp) = E(T_0) + \sum_{k=1}^{p} E(T_k) + \sum_{k=1}^{p-1} E(T'k) \,. \tag{4.3}$$

Для того, щоб знайти три середніх значення часу в рівності (4.3) зазначимо, що $E(T_k)$ виникає за рахунок середнього числа $E(mk)$ користувачів класу *k*, котрі очекують в системі. Кожний з них потребує, в середньому, $1/\mu k$ одиниць часу, тому безпосередньо одержимо:

$$E(T_k) = E(mk)/\mu k \,. \tag{4.4}$$

Але на основі формули Літтла величина $E(mk)$ пов'язана з середнім очікуванням $E(Wk)$, а саме

$$\mathrm{E(mk)} = \lambda_\mathrm{k} \mathrm{E(Wk)} \,. \tag{4.5}$$

Об'єднуючи рівняння (4.4) і (4.5), отримаємо:

$$E(T_k) = \rho_k E(Wk), \quad \rho_k \equiv \lambda_k / \mu_k . \tag{4.6}$$

Розглянемо тепер параметр $E(T_k)$, який одержали за рахунок надходження, в середньому $E(mk)$ користувачів класу k протягом проміжку часу $E(Wp)$.

Оскільки інтенсивність надходжень рівна λk і кожний користувач потребує в середньому $1/\lambda k$ одиниць часу обслуговування, безпосередньо отримаємо:

$$E(T_k) = \lambda k E(Wp) / \mu k = \rho k E(Wp) . \tag{4.7}$$

Отже, що $E(T_0)$ - це залишковий час обслуговування користувача, який знаходиться на обслуговуючій лінії.

Для системи обслуговування з відносними пріоритетами, які зберігають функціонування (тобто, коли обслуговуюча лінія знаходиться в режимі нормальної роботи, а користувач чекає обслуговування), вказаний час не залежить від дисципліни обслуговування. Воно повинне бути одним і тим же, якщо користувачі всіх k класів обслуговуються з однаковим пріоритетом за надходженням. Для середнього часу очікування в системі $M/G/1$, знаходимо:

$$\mathrm{E}(\mathrm{T}_0) = \lambda \mathrm{E}(\tau^2) / 2 = \sum_{k=1}^{r} \lambda_k \mathrm{E}(\tau_k^2) / 2 . \tag{4.8}$$

Це узагальнює описаний вище приклад з двома пріоритетними класами.

Зазначимо особливість систем з пріоритетами, яка полягає в тому, що деякі класи пріоритетів (високі) поліпшують характеристики, інші - навпаки. Цікаво, що тут має місце закон збереження. Можна показати, що зважена сума часів очікування завжди зберігає своє значення.

Зокрема:

$$\sum_{k=1}^{r} \rho_k \mathrm{E}(\mathrm{Wk}) = \rho \mathrm{E}(\mathrm{W}), \tag{4.9}$$

де $E(W)$ - час очікування в системі $M/G/1($ обслуговуючій чергу за надходженням).

При зменшенні деяких часів очікування інші в порядку компенсації повинні збільшитися. Цей закон збереження є окремим випадком більш

загального закону для систем із збереженням функціонування, який уперше був відкритий Клейнроком.

Скориставшись результатами теорії масового обслуговування і теоремою Літтла, можна обчислити середню затримку проходження інформації в мережі.

Наприклад, середня затримка виклику в системі:

$$T = \frac{1}{\mu} + \frac{P_Q}{m\mu - \lambda}, \tag{4.10}$$

де μ - швидкість обслуговування (даний параметр показує з якою швидкістю працює обслуговуючий прилад, тобто число викликів, що обслуговуються в одиницю часу, коли він зайнятий); P_Q - імовірність події: вимога, яка надійшла, визначає, що в системі всі обслуговуючі прилади зайняті, і буде поставлена у чергу для очікування (визначається за формулою Ерланга);

m – кількість обслуговуючих пристроїв.

Застосовуючи теорему Літтла, знаходимо середнє число вимог у системі:

$$N = T\lambda = \frac{\lambda}{\mu} + \frac{\lambda P_Q}{m\mu - \lambda} \ . \tag{4.11 }$$

Аналогічно за допомогою відомих співвідношень у теорії масового обслуговування визначається середній час проходження управляючої інформації телекомунікаційною мережею в залежності від різних умов.

4.2 Розрахунок затримки інформації з врахуванням структури інфокомунікаційної мережі

Розрахунок затримки інформації управління в вузлах ІКМ дозволяє кількісно оцінити якість структурної схеми, визначити оптимальну структуру мережі передачі інформації для різної кількості абонентів та спектра послуг, які надаються.

Розроблене програмне забезпечення призначено для отримання даних щодо часу затримки інформації управління в різних умовах і надає можливість зробити висновки про оптимальність структури інфокомунікаційной мережі.

Залежність затримки від інтенсивності надходження команд управління (вимог) представлена на рис. 4.1.

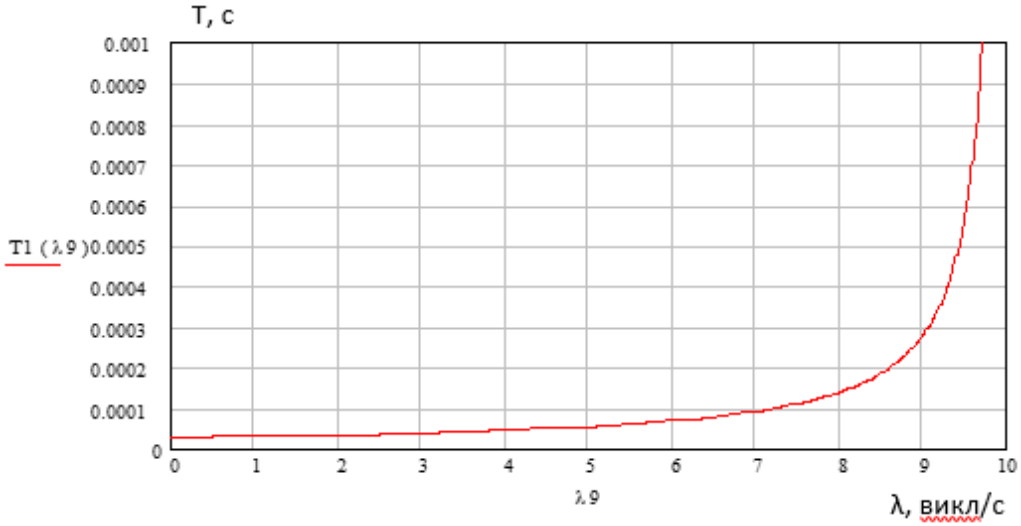

Рисунок 4.1. Залежність затримки від інтенсивності надходжень вимог

Як і передбачалось, на рисунку видно, що затримка збільшується пропорційно інтенсивності. Як наслідок, для забезпечення її величини ,яка не перевищує заданої, необхідно при збільшенні інтенсивності команд інфокомунікаційной мережі збільшити продуктивність комутаційних вузлів.

На рис. 4.2 представлено залежність затримки інформації від продуктивності вузла комутації при різній інтенсивності надходження вимог.

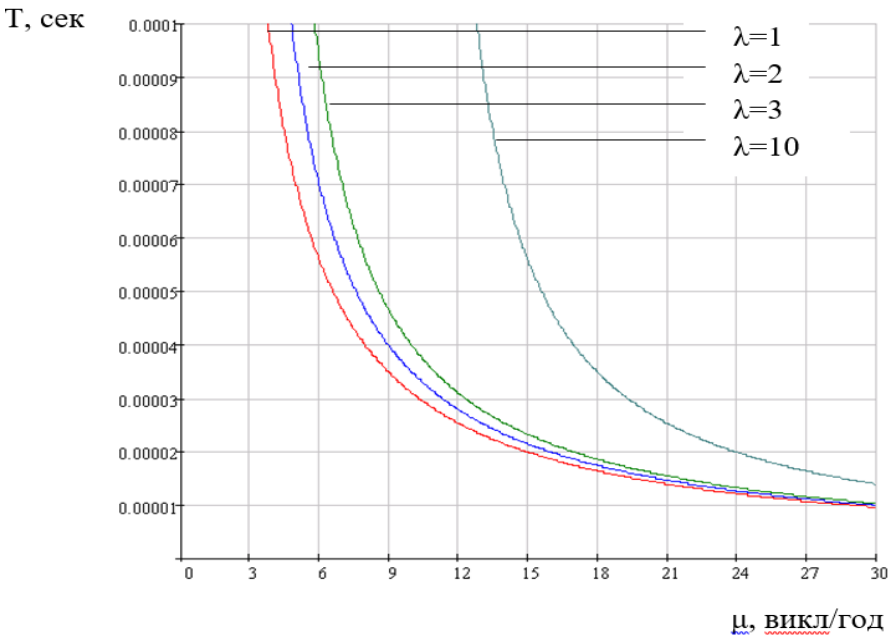

Рисунок 4.3. Залежність затримки інформації від продуктивності вузла комутації, модель M/M/1

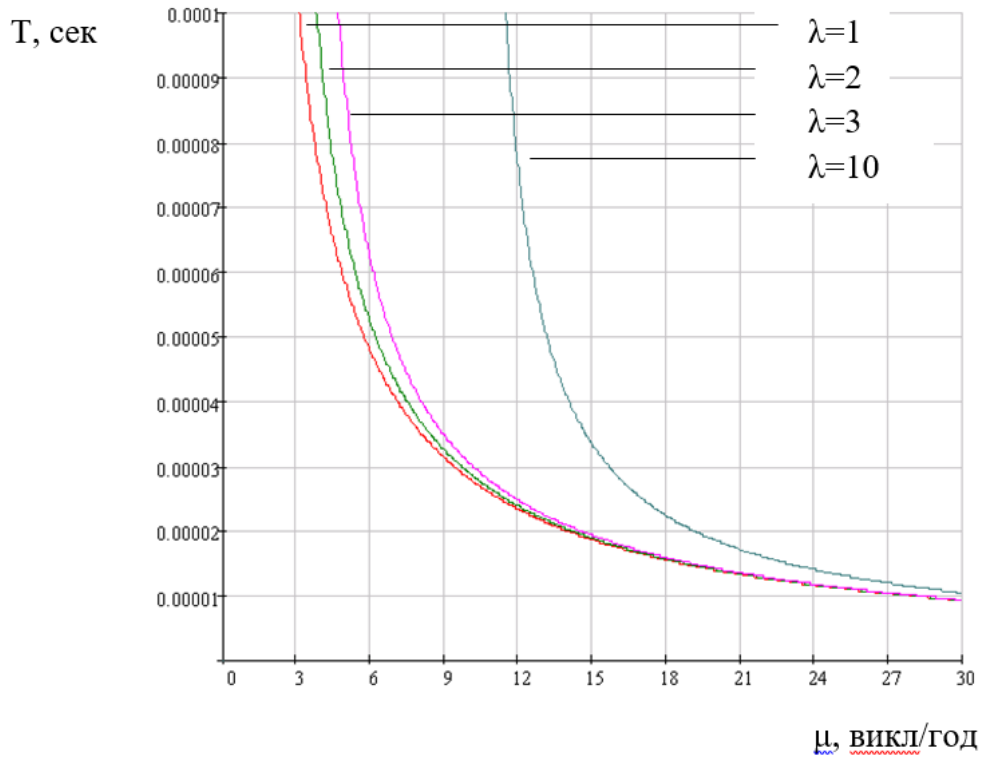

Рисунок. 4.4 Залежність затримки інформації від продуктивності вузла комутації, модель M/M/2

Можна зробити висновок, що при проектуванні ІКМ необхідно враховувати фактор, що при підвищенні продуктивності вузла комутації до певного рівня затримка несуттєво залежить від інтенсивності надходження пакетів. Тому найефективнішим способом зменшення затримки є підвищення продуктивності комутаційних вузлів, а не зниження навантаження на комутаційний вузол.

На основі розрахунку отримано залежності затримки одержання інформації від інтенсивності надходження вимог, від швидкості, а також від методу обслуговування. Ці дані дозволяють мінімізувати затримку при різних умовах.

Представлені методи доцільно впроваджувати в інфокомунікаційних мережах України, вони охоплюють новітні технологічні рішення. Це дозволяє на базі традиційного устаткування здійснювати більш ефективне та досконале управління

ВИСНОВКИ

На основі проведеного аналізу можна зробити висновок що для управління потоком в мережах NGN протокол TCP/IP є більш зручним механізмом. Так як протокол TCP є ефективним засобом управління потоками даних, мережі збалансованого навантаження, боротьби з перевантаженнями, забезпечення наскрізних показників якості та ін.. Простота, надійність та якість протоколу TCP/IP відповідає критеріям, які висувають оператори та провайдери телекомунікаційних мереж.

Для управління потоком в мережах NGN є три ключові механізми управління потоком за протоколом TCP/IP:

1. Механізм ковзаючого вікна. Дозволяє відправникові посилати черговий сегмент не чекаючи підтвердження, поки він залишається в межах оголошеного вікна.

2. Механізм повільного старту. Дозволяє визначити швидкість відправки сегментів, яка була б пропорційна швидкості отримання підтверджень.

3. Алгоритм запобігання перевантаження. На основі механізму ковзаючого вікна для запуску використовує повільний старт, для визначення розміру вікна та порогу передачі даних, далі збільшується лінійно щоб не допустити великої кількості втрачених даних та не затопити мережу, далі управління відбувається за принципом AIMD.

Механізми протоколу TCP гарантують забезпечення доставки даних, цілісність переданих даних і повідомлення відправника про результати передачі.

Представлені дослідження охоплюють новітні технологічні рішення, дозволяють покращити показники якості мереж і доцільні до впровадження на сучасних системах телекомунікацій.

ПЕРЕЛІК ПОСИЛАНЬ

1. А.В. Росляков. / Сети следующего поколения NGN / Под ред. А.В. Рослякова. – М: Эко-Трендз, 2008. – 400 с.

2. Семенов Ю.В. / Проектирование сетей связи следующего поколения / Ю.В. Семенов. – СПб.: Наука и Техника, 2005. – 240 с.

3. Дуглас Камер. / Сети TCP/IP, том 1. Принципы, протоколы и структура / М.: «Вильямс», 2003. – 417с.

4. Стеклов В.К., Беркман Л.Н. Проектування телекомунікаційних мереж: Підруч. для студ. вищ. навч. закл. за напрямком “Телекомунікації”/ За ред. В.К. Стеклова. – К.:Техніка,2002. – 792 с.

5. Поповський В.В, Лемешко О.В.; / Телекомунікаційні системи та мережі. Структура й основні функції. Том 1 / [Електронний ресурс] // URL: http://www.znanius.com/3577.html (дата звернення 12.12.2019)

6. Срібна І.М., Кирпач Л.А. / Методичний посібник з дисципліни „Проектування цифрових систем зв’язку” / [Електронний ресурс] // URL: http://www.dut.edu.ua/uploads/l_1097_96748351.pdf// (дата звернення 12.12.2019)

7. В.В. Правило / Дослідження методів управління телекомунікаційними мережами в умовах перевантаження / Правило В.В. / - І-а НТК Харківського університету повітряних сил. 17.02.05 – 16с.

8. TCP Congestion Control или Почему скорость прыгает / [Електронний ресурс] // URL: https://habr.com/ru/post/168407/ (дата звернення 12.12.2019)

9. Варфоломеєва О. Г., Мороз О.О. / Дослідження методів управління потоком в мережах NGN за протоколом TCP/IP / «Телекомунікаційні та інформаційні технології, – 2016, – №4»

10. Б. Кришнамурти, Дж. Рексфорд. / Web-протоколы. Теория и практика. — М.: ЗАО «Издательство БИНОМ», 2002 г. – 592с.

11. Протокол маршрутизации OSPF / [Електронний ресурс] // URL: http://ciscotips.ru/ospf (дата звернення 03.12.2019)

12. Introduction to IS-IS/ [Електронний ресурс] // URL: https://networkdirection.net/articles/routingandswitching/introductiontois-is/ (дата звернення 04.12. 2019)

13. Хелеби, Сэм, Мак-Ферсон, Денни / Принципы маршрутизации в Internet, 2-е издание / [Електронний ресурс] // URL: https://studfile.net/preview/1095675/page:12/ (дата звернення 05.12.2019)

14. Сети для самых маленьких. Часть восьмая. BGP и IP SLA / [Електронний ресурс] // URL: https://habr.com/ru/post/184350/ (дата звернення 05.12.2019)

К. Самуйлов, В. Василевский, А. Королькова, И. Шалимов, Н. Васин, Д. Кулябов / Сети и телекоммуникации. Учебник и практикум для СПО Сети и телекоммуникации. Учебник и практикум для СПО / [Електронний ресурс] // URL: https://books.google.com.ua/books?id=4ZN9DwAAQBAJ&pg=PA172&lpg=PA172&dq=Формат+сообщения+RIP&source=bl&ots=Sjd40xqurQ&sig=ACfU3U1tnA1T9eK1CYvpJu7FEWhPkPSgzQ&hl=ru&sa=X&ved=2ahUKEwjhuIOc1JfmAhWF-ioKHVJ0DtgQ6AEwD3oECAkQAQ#v=onepage&q=Формат%20сообщения%20RIP&f=false (дата звернення 12.12.2019)

19. В.И. Гостев, Т.П. Довженко/ Исследование сети TCP/IP с применением основных TCP-алгоритмов предотвращения перезагрузок /Системи управління, навігації та зв'язку, - 2014, - 3 (31)»

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ