МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Г.Г. Киричек

Конспект лекцій з дисципліни
«Комп’ютерні мережі»
для студентів спеціальності
123 Комп'ютерна інженерія, усіх форм навчання

2024

Конспект лекцій з дисципліни «Комп’ютерні мережі» для студентів спеціальності 123 Комп'ютерна інженерія, усіх форм навчання / Укл. Г.Г Киричек. – Запоріжжя: Національний університет «Запорізька політехніка», 2024. – 58 с.

Укладачі: Г.Г. Киричек, доцент, к.т.н.

Рецензент: М.Ю. Тягунова, доцент, к.т.н.

Відповідальний за випуск: Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 5 від 18.12.2023

Затверджено
на засіданні НМК КНТ
Протокол № 5 від 25.12.2023

ЗМІСТ

1 ВСТУП ДО МЕРЕЖНИХ ТЕХНОЛОГІЙ

Мета – ознайомитись з моделями, які описують взаємодію відкритих систем та засвоїти загальні принципи роботи всіх рівнів моделі OSI (стеку TCP/IP) з метою підготовки до екзамену з дисципліни «Комп'ютерні мережі».

1.1 Модель OSI

У 1978 році Міжнародна Організація по Стандартизації (ISO - International Organization for Standardization) приступила до створення еталонної моделі OSI (Open System Interconnection) - створена універсальна загальноприйнята модель мережної взаємодії: модель, яка описує взаємодію відкритих систем.

Відкрита система - будь-яка система (ПК, мережа, ОС, пристрої, ПЗ), побудована відповідно до відкритих специфікацій.

Відкриті специфікації - опубліковані, загальнодоступні специфікації, які відповідають стандартам та прийняті в результаті досягнення згоди після обговорення зацікавленими сторонами. Використання при розробці систем відкритих специфікацій дозволяє фахівцям розробляти для них різні апаратні або програмні засоби розширення і модифікації, створювати програмно-апаратні комплекси з продуктів різних виробників.

Специфікація - формалізований опис апаратних або програмних компонентів, способів їх функціонування, взаємодії з іншими компонентами, умов експлуатації, обмежень і особливих характеристик. Не кожна специфікація - стандарт.

Для реальних систем повна відкритість - недосяжний ідеал. У відкритих системах цьому визначенню відповідають тільки частини, які підтримують зовнішні інтерфейси. Відкритість ОС Unix - в наявності стандартизованого програмного інтерфейсу між ядром і додатками, що дозволяє легко перенести додатки з середи однієї версії Unix в середу іншої версії.

Модель OSI стосується одного аспекту відкритості - відкритості засобів взаємодії пристроїв, які працюють в мережі. Тут під відкритою системою розуміється мережний пристрій, що взаємодіє з іншими мережними пристроями з використанням стандартних правил, які

визначають формат, зміст і значення повідомлень, що відправляються. Якщо мережі побудовані з дотриманням принципів відкритості - це надає наступні переваги:

– побудова мережі з апаратних засобів і ПЗ різних виробників;

– можливість простого з'єднання мереж між собою;

– проста заміна одних компонентів мережі іншими, простота обслуговування.

Приклад відкритої системи - мережа Internet.

Модель OSI включає сім рівнів.

Layer 7: Application Layer – Прикладний.

Layer 6: Presentation Layer – Представницький.

Layer 5: Session Layer – Сеансовий.

Layer 4: Transport Layer – Транспортний.

Layer 3: Network Layer – Мережний.

Layer 2: Data Link Layer – Канальний.

Layer 1: Physical Layer - Фізичний.

Фізичний рівень - забезпечує передачу потоку біт між об'єктами канального рівня через фізичні з'єднання. Визначає електричні та фізичні специфікації пристроїв і відповідає за передачу сигналів в лінії зв'язку, їх прийом і перетворення в біти даних. До цього рівня відносяться фізичні характеристики середовища передачі даних, способи перетворення біт даних в сигнали, визначаються електричні параметри сигналів, механічні та електричні вимоги до роз'ємів і т.д.

Канальний рівень - визначає спосіб доступу до лінії зв'язку, оформлення потоку байт в блоки даних для передачі, адресацію в лінії зв'язку, перевірку цілісності даних, шляхом додавання до блоку даних додатковою інформації. Забезпечує функціональні і процедурні засоби для передачі блоків даних канального рівня між об'єктами мережного рівня як в режимі без встановлення з'єднання (дейтаграмному), так і в режимі з встановленням з'єднання. З'єднання канального рівня може бути реалізовано з використанням одного або декількох фізичних з'єднань.

Висновок: створити працюючу мережу можна з використанням перших двох рівнів моделі, канального і фізичного.

Обмеження: не можна створити мережу довільного масштабу (адреси плоскі, неструктуровані). Для створення мереж довільного розміру потрібна робота верхніх рівнів OSI.

Мережний рівень - забезпечує процедурні і функціональні засоби для передачі даних між об'єктами транспортного рівня як в режимі без встановлення з'єднання, так і в режимі з встановленням з'єднання, забезпечуючи незалежність об'єктів транспортного рівня від способів і умов маршрутизації і доставки даних, дозволяє об'єднати невеликі мережі, побудовані з використанням фізичного і канального рівня в складну мережу довільного масштабу. Адреси мережного рівня на відміну від апаратних адрес є структурованими ієрархічними адресами. Ця властивість мережних адрес дозволяє адресувати не тільки окремі хости, а і мережі.

Транспортний рівень - забезпечує передачу даних між об'єктами сеансового рівня, звільняючи сеансовий рівень від проблем, пов'язаних з необхідністю досягнення надійної і ефективної передачі даних. Ніякої гарантії збереження будь-якого блоку даних при передачі немає - несправність або аварія приведуть до втрати даних, які перетинали пошкоджений сегмент мережі. Але відправник може повторювати їх відправку до тих пір, поки дані не потраплять до одержувача. Спосіб переконатися, що дані не загубилися в дорозі - доставка з повідомленням про вручення.

Рівні - над транспортним рівнем, називаються прикладними рівнями. Вони забезпечують роботу додатків на хостах.

Сеансовий рівень - надає засоби, які необхідні для організації взаємодії об'єктів рівня представлення, синхронізації їх діалогу та управління обміном даними. Забезпечує сервіс по встановленню сеансових з'єднань між двома об'єктами рівня уявлень, підтримки впорядкованого обміну даними і розриву сеансових з'єднань впорядкованим чином. Сеансовий рівень забезпечує управління діалогом. Функції сеансового рівня: визначення параметрів логічного з'єднання, встановлення логічного з'єднання, обслуговування логічного з'єднання, розрив логічного з'єднання.

Рівень представлення - забезпечує подання інформації, якою обмінюються об'єкти рівня додатків або на яку вони посилаються в процесі взаємодії. Звільняє об'єкти рівня додатків від необхідності вирішувати проблеми, пов'язані із загальним поданням інформації, надаючи синтаксичну незалежність.

Рівень додатків - забезпечує для прикладних процесів єдину можливість отримання доступу до середовища OSI для забезпечення взаємодії при вирішенні спільних завдань. Зв'язок між взаємодіючими

процесами додатків, узгодження контексту додатків, що визначає єдині для взаємодіючих об'єктів умови взаємозв'язку. Надає прикладним процесам мережеві сервіси загального призначення (електронна пошта, передача файлів, веб-браузер) - рівень, на якому програми не працюють, а взаємодіють.

У моделі OSI п'ять верхніх рівнів відносяться до рівнів, реалізованих програмно і вважається, що два нижніх рівні реалізовані апаратно. Термін «середовище OSI» є абстрактним представленням набору понять, елементів, функцій, протоколів, визначених у моделі OSI стандартами, які роблять можливим взаємодію між відкритими системами.

Процеси передачі інформації і взаємодії - регламентовані, описані правилами. Набори правил, що регламентують взаємодію є і в моделі OSI. Дамо визначення цих наборів правил:

Набір формальних правил і угод, які регламентують взаємодію між сусідніми рівнями однієї системи або мова взаємодії між сусідніми рівнями однієї системи є інтерфейсом. Набір формальних правил і угод, які регламентують взаємодію між однаковими рівнями різних систем чи мова взаємодії між однаковими рівнями різних систем є протоколом.

Процес додавання заголовків при передачі інформації називається інкапсуляція. Кожен заголовок має сенс тільки для відповідного рівня системи-одержувача, верхні рівні не потребують заголовків нижніх рівнів. Кожен рівень системи-одержувача, обробивши відповідний заголовок, відкидає його, і передає на верхній рівень дані вже без свого заголовка. Процес відкидання заголовків є декапсуляцією. ККД (коефіцієнт корисної дії) будь-якої мережевої технології завжди менше 100%. В мережі крім корисних даних будуть передаватися службові заголовки. Одиниці даних кожного рівня в рамках моделі називаються «протокольними одиницями даних» або PDU (Protocol Data Unit) відповідного рівня.

Блоки даних трьох верхніх рівнів не мають окремих назв, і називаються просто даними.

Блоки даних інших рівнів мають власні назви. Перерахуємо їх.

Блок даних транспортного рівня називається сегментом (segment), або дейтаграмою (datagram).

Блок даних мережного рівня називається пакетом (packet).

Блок даних канального рівня називається кадром (frame).

Одиниця даних фізичного рівня - біт (bit).

1.2 Класифікація мереж

За способом організації мережі поділяються на реальні і штучні:

– штучні мережі (псевдомережі) дозволяють пов'язувати комп'ютери разом через виту пару і не потребують додаткових пристроїв. Використовуються коли необхідно перекачати інформацію з одного комп'ютера на інший.

– реальні мережі дозволяють пов'язувати комп'ютери за допомогою спеціальних пристроїв комутації і фізичної середовища передачі даних.

У загальному випадку класифікація реальних комп'ютерних мереж ведеться по різного виду критеріям:

По територіальній поширеності:

– PAN - мережа, що належить одному користувачеві і використовується для взаємодії його пристроїв;

– LAN - локальні комп'ютерні мережі, характеризуються замкнутою інфраструктурою до рівня виходу на постачальника послуг зв'язку. До LAN відносяться невеликі офісні мережі з 5-10 комп'ютерів, так і мережі великих підприємств, що складаються з сотень пристроїв;

– MAN - міські мережі (регіональні), між установами. Об'єднують абонентські системи, розташовані в межах окремого регіону - міста, адміністративного району; функціонують в інтересах організацій і користувачів регіону і мають вихід в WAN;

– WAN - глобальні комп'ютерні мережі, що поширюються на великі географічні регіони і включають в себе LAN і безліч інших телекомунікаційних мереж і пристроїв. Інтернет відноситься до глобального виду мереж;

Об'єднання - дозволяє створювати складні багатомережні ієрархії. За відомчої приналежністю:

– відомчі (приватні) - належать одній організації і розташовуються на її території;

– державні мережі - мережі, використовувані в державних структурах.

За швидкістю передачі діляться на:

– низькошвидкісні (10 Мбіт / с),
– середньошвидкісні (від 100 Мбіт / с до 1000 Мбіт / с),
– високошвидкісні (понад 1000 Мбіт / с);

За типом середовища передачі:

– кабельні (телефонний, коаксіальний кабель, вита пара, волоконно-оптичний кабель);

– бездротові (передача інформації по радіохвилях в певному частотному діапазоні).

За функціональним призначенням:

– мережі зберігання даних;

– серверні ферми;

– мережі управління процесом;

– мережі SOHO (small / home), будинкові мережі.

За способом управління:

– мережі з централізованим управлінням - в мережі один або кілька керуючих пристроїв;

– мережі з децентралізованим управлінням - кожна абонентська система має засоби для управління мережею;

– мережі з змішаним керуванням - в певному поєднанні реалізовані принципи централізованого та децентралізованого управління.

За топологією комп'ютерних мереж поділяються на наступні види: шина; кільце; подвійне кільце; зірка; комірчаста; решітка; дерево та мережа fat tree (товсте дерево).

За способом адміністрування розрізняють 2 типи мереж - одноранговy і мережу на основі сервера. Обидва різновиди виконують поставлені завдання але роблять це по-різному.

Мережа на основі сервера найбільш керована і контрольована.

Під архітектурою розуміють специфікації зв'язку, розроблені для визначення функцій мережі і встановлення стандартів різних моделей обчислювальних систем, призначених для обміну та обробки даних.

Стандартизація - основа стандартизації багаторівневий підхід до розробки засобів мережевої взаємодії.

1.3 Стек TCP / IP

Стек протоколів TCP / IP. Transmission Control Protocol / Internet Protocol є промисловим стандартом стека протоколів, який розроблено для відкритих, глобальних мереж. Стандарти TCP / IP опубліковані в документах Request for Comment (RFC).

Стек TCP / IP є поширеним набором протоколів, протоколи стека використовуються для обміну даними між будь-якими пов'язаними мережами і однаково добре підходять для мереж будь-якого масштабу.

Внесок в розвиток стека TCP/IP додав університет Берклі, реалізувавши протоколи цього стека в ОС UNIX. Поширення UNIX привело і до поширення протоколу IP і інших протоколів стека. Протоколи стека TCP/IP є основою роботи Internet. Важлива роль стека TCP/IP пояснюється наступними його властивостями:

– найбільш завершений стандартний стек мережних протоколів;

– представляє собою набір відкритих стандартів, які можуть бути вільно використані будь-яким розробником;

– практично всі мережі передають основну частину свого трафіку за допомогою протоколу TCP/IP і це є методом отримання доступу до глобальної мережі Internet;

– всі сучасні операційні системи підтримують стек TCP/IP.

Стек TCP/IP розроблений до моделі OSI і має багаторівневу структуру але відповідність рівнів стека TCP/IP рівням моделі OSI досить умовна і в різних джерелах представлена по-різному.

Протоколи стеку TCP/IP поділяються на 4 рівня (рис.1.1):

– прикладний рівень (application);

– транспортний рівень (transport);

– міжмережевий рівень (internet);

– рівень мережних інтерфейсів (data link) або рівень доступу.

<table>
<tr><td>7
6
5</td><td>WWW, HTTP</td><td>SNMP</td><td>FTP, TFTP</td><td>telnet</td><td>SMTP, POP3</td><td>DNS, DHCP</td><td>IV</td></tr>
<tr><td>4</td><td colspan="6">TCP UDP</td><td>III</td></tr>
<tr><td>3</td><td colspan="2">IP</td><td>ICMP</td><td colspan="2">OSPF, RIP</td><td>ARP</td><td>II</td></tr>
<tr><td>2
1</td><td colspan="6">Ethernet, Token Ring, FDDI, X.25, SLIP, PPP,
Wi Fi, xDSL, ATM, Frame Relay ... ..</td><td>I</td></tr>
<tr><td>OSI</td><td colspan="6"></td><td>TCP / IP</td></tr>
</table>

Рисунок 1.1 - Протоколи стеку TCP/IP

Четвертий – відповідає фізичному і канальному рівням моделі OSI та в протоколах стеку TCP/IP не регламентується, підтримує стандарти фізичного і канального рівня або будь-яку БМТ (базову мережну технологію). З появою нової технології LAN або WAN включається в TCP/IP за рахунок розробки нового RFC, який визначає метод інкапсуляції пакетів IP в кадри, можна асоціювати з інтерфейсом між 2 і 3 рівнем OSI, чи єдиним стандартизованим інтерфейсом.

Третій, рівень міжмережної взаємодії - передача пакетів з використанням різних технологій - відповідає мережному рівню OSI. Основним протоколом рівня є IP, або протокол передачі пакетів в складних мережах. До рівня міжмережної взаємодії відносяться протоколи маршрутизації (протоколи динамічної маршрутизації), наприклад: RIP, OSPF, BGP та протокол міжмережних керуючих повідомлень ICMP (Internet Control Message Protocol) застосовується для діагностики мережі та інформування про помилки.

Рівень 2 має назву - транспортний. На цьому рівні працюють: протокол управління передачею TCP (Transmission Control Protocol) і протокол призначених для користувача дейтаграм UDP (User Datagram Protocol). TCP забезпечує надійну передачу між прикладними процесами, а UDP – передачу прикладних пакетів дейтаграмним способом – функції сполучної ланки між мережним протоколом і прикладними процесами. У заголовку TCP – дані, завдяки яким відбуваються сеанси обміну даними між відправником і отримувачем, або функції сеансового рівня OSI. Асоціюють як з транспортним і сеансовим рівнями OSI, так із транспортним. Встановити чітку відповідність між двома моделями неможливо.

Верхній рівень - прикладний. В TCP/IP багато протоколів прикладного рівня - до них відносяться: протокол копіювання файлів FTP; отримання пошти SMTP; клієнтські поштові протоколи - POP3 і IMAP4; гіпертекстовий HTTP; динамічного конфігурування хостів DHCP; служби дозволу імен DNS; управління мережею SNMP і інші.

1.4 Фізичний рівень моделі OSI

Лінія зв'язку - шлях, який проходить сигнал від відправника до одержувача. Складається з фізичного середовища передачі даних, апаратури передачі даних (DCE), проміжного обладнання та пристроїв

(DTE), які передають одне одному інформацію у вигляді сигналу певної частоти і форми.

DTE, Data Terminal Equipment – пристрої, що формують дані для передачі в лінію зв'язку. Вони перетворюють призначену для користувача інформацію в дані і здійснюють зворотне перетворення.

DCE, Data Circuit Equipment – пристрої, що забезпечують фізичне з'єднання з мережею, формують сигнали, зрозумілі для протоколу фізичного рівня каналу зв'язку. DCE забезпечують подачу синхронізуючого сигналу, використовуваного для узгодження процесів обміну даними між DTE і DCE.

Фізичне середовище передачі даних та класифікація середовища передачі: провідні (або повітряні) лінії зв'язку; кабельні лінії зв'язку та бездротові лінії зв'язку (радіоканали).

Провідні лінії зв'язку – дроти без ізолюючих і екрануючих оболонок, прокладені між стовпами (в повітрі). Відсутність екрана позначається на якості і швидкості передачі даних. Тому сьогодні провідні лінії зв'язку практично повністю витіснені кабельними.

Кабельні лінії зв'язку використовують для з'єднання різні види кабелю. Кабель складається з провідників, електричної або механічної ізоляції і роз'ємів, для підключення до комунікаційного обладнання.

Кабелі мають два види:

– мідні кабелі, які використовують для передачі інформації, шляхом зміни струму в провіднику, це кабелі на основі витої пари (балансні кабелі) і коаксіальні кабелі;

– волоконно-оптичні кабелі, в яких сигнал переноситься за допомогою променю світла. Існує кілька різновидів.

У локальних мережах як фізичне середовище передачі даних частіше використовують мідні кабелі, рідше волоконно-оптичні.

Коаксіальний кабель складається з покритого ізоляцією твердого мідного дроту, розташованого в центрі кабелю. Поверх ізоляції натягнуто циліндричний провідник, у вигляді дрібної мідної сітки і покритий зовнішнім шаром ізоляції (пластиковою оболонкою).

Застосовуються зазвичай два типи коаксіального кабелю:

– 50 Ом - для передачі тільки цифрових даних;

– 75 Ом - для передачі аналогових сигналів.

Товщина тонкого коаксіального кабелю - приблизно 0,5 - 0,6 см, а товстого - 1 - 1,3 см.

Балансний кабель (вита пара) - найбільш вживаний вид кабелю, завдяки своїй дешевизні і простоті в експлуатації.

Кабелі на основі витої пари є симетричними - складаються з двох однакових в конструктивному відношенні, ізольованих мідних проводів, діаметром близько міліметра. Кабель вита пара може бути екранований за допомогою фольги або мідного обплетення, що збільшує його перешкодозахищеність, але це позначається на вартості. Кабель – екранована вита пара, STP (Shielded Twisted Pair). Кабель – неекранована вита пара, UTP (Unshielded Twisted Pair).

Кабель на основі неекранованої витої пари – ділиться в міжнародних стандартах на категорії (від 1 до 8).

Волоконно-оптичний кабель схожий за своєю структурою на коаксіальний, не має екрануючої сітки. Світлові імпульси передаються по сердечнику, товщиною від 8 до 60 мкм, в залежності від типу оптоволоконного кабелю. Сердечник укладений в скляну оболонку з більш низьким коефіцієнтом заломлення, що перешкоджає виходу світла за межі сердечника. Захистом для скляної частини служить пластикова оболонка. Якщо промінь світла з кутом падіння, більше критичного, відбивається від стінок волокна, то і безліч променів - відбивається під різними кутами. Кожен промінь має – моду (кут відбиття), а оптичне волокно, що володіє властивістю передавати відразу декілька променів – багатомодове. Якщо зменшити діаметр волокна до декількох довжин хвиль світла – волокно діє як хвилевід – світло рухається по прямій лінії, без відбитків від стінок волокна. Волокно одномодове коштує дорожче, але може використовуватися при передачі даних на великі відстані.

Бездротові лінії зв'язку – сигнал переноситься за допомогою передавача і приймача радіохвиль. Діляться на радіоканали, що відрізняються частотним діапазоном і дальністю каналу: Діапазони коротких, середніх і довгих хвиль (КХ, СХ і ДХ) - діапазони амплітудної модуляції (Amplitude Modulation, AM) за типом методу модуляції сигналу забезпечують далекий зв'язок при невисокій швидкості передачі даних. Діапазони ультракоротких хвиль (УКХ) - більш швидкісні канали і частотна модуляція (Frequency Modulation, FM). Діапазони надвисоких частот (НВЧ або microwaves).

У діапазоні СХЧ (понад 4ГГц) сигнали не відбиваються іоносферою Землі – для стійкого зв'язку потрібна наявність прямої

видимості між передавачем і приймачем. Використовують супутникові канали або радіорелейні канали.

2 КАНАЛЬНИЙ РІВЕНЬ. ТЕХНОЛОГІЯ ETHERNET

2.1 Порівняння базових мережевих технологій

Для порівняння мереж та їх технологій використовують такі основні параметри мереж, як:

- швидкість передачі інформації;
- метод доступу (або час доступу);
- можливі топології;
- необхідні проміжні мережеві пристрої;
- розміри мережі (або відстань між абонентами);
- вартість обладнання;
- рівень стандартизації;
- максимальна кількість абонентів;
- можливе середовище передачі;
- методи кодування, які використовуються при передачі;
- формати кадрів (розмір поля даних).

Протягом багатьох років існувало багато типів локальних мереж, але сьогоднішні мережі використовують два загальні типи локальних мереж: локальні мережі Ethernet і бездротові локальні мережі. У локальних мережах Ethernet для зв'язку між вузлами використовуються кабелі, найчастіше це балансний кабель (вита пара) та також використовують волоконно-оптичний кабель, він включає скловолоконне ядро, яке пристрої використовують для передачі даних за допомогою світла. На відміну від Ethernet, бездротові локальні мережі не використовують кабелі, натомість, для з'єднання між вузлами, вони використовують радіохвилі.

2.2 Види Ethernet

Найбільш поширеним на даний момент є стандарт IEEE 802.3 – це основний стандарт на технологію Ethernet – або на сімейство технологій пакетної передачі даних. Включає підстандарти або, для локальних мереж, наступні види Ethernet:

- IEEE 802.3 Ethernet;

– IEEE 802.3u Fast Ethernet;
– IEEE 802.3z, ab, ah GEthernet;
– IEEE 802.3ae 10GEthernet.

"Ethernet" (перекладається як "ефірна мережа") - все, що передається одним вузлом, одночасно приймається всіма іншими. Термін Ethernet відноситься до сімейства стандартів мереж, які разом визначають фізичний рівень і рівень каналу передачі даних найпопулярнішої у світі технології дротової локальної мережі. Стандарти, визначені Інститутом інженерів з електротехніки та електроніки (IEEE), визначають кабелі, роз'єми на кінцях кабелів, правила протоколу та все що необхідне для створення локальної мережі Ethernet. Сьогодні Ethernet містить багато стандартів для різних типів оптичних і мідних кабелів, а також для швидкості від 10 мегабіт на секунду (Мбіт/с) до 400 гігабіт на секунду (Гбіт/с). Стандарти також відрізняються за типами та довжиною кабелів.

Щоб бути готовим вибрати пристрої для побудови нової локальної мережі Ethernet, мережевий інженер повинен знати назви та особливості різних стандартів Ethernet. IEEE визначає стандарти фізичного рівня Ethernet, використовуючи спочатку ідентифікатор стандарту 802.3, за яким йдуть декілька суфіксів. І IEEE також використовує назви скорочень, які визначають швидкість, а також підказку про те, чи є це кабель UTP (використання суфіксів - T або TX) чи є кабель волокном (суфікс – F, FX або LX).

У таблиці 2.1, як приклад, надано достатню кількість стандартів фізичного рівня Ethernet, щоб ви могли зрозуміти ці правила.

Таблиця 2.1 - Стандарти фізичного рівня Ethernet

Speed	Common Name	Informal IEEE Standard Name	Formal IEEE Standard Name	Cable Type, Maximum Length
10 Mbps	Ethernet	10BASE-T	802.3	Copper, 100 m
100 Mbps	Fast Ethernet	100BASE-TX	802.3u	Copper, 100 m
1000 Mbps	Gigabit Ethernet	1000BASE-LX	802.3z	Fiber, 5000 m
1000 Mbps	Gigabit Ethernet	1000BASE-T	802.3ab	Copper, 100 m
10 Gbps	10 Gig Ethernet	10GBASE-T	802.3an	Copper, 100 m

2.3 Метод доступу CSMA/CD

Метод доступу до середовища передачі CSMA/CD (множинний доступ з контролем несучої і виявленням колізій).

Основні поняття:

– BT (Bit Time, бітовий інтервал) - тривалість передачі одного біта (10Мбіт - 100нс). Якщо 100Мбіт, то 10нс;

– IPG (Inter-Packet Gap, межпакетное щілину) - мінімальний інтервал між кадрами, IPG = 96 BT. (кадр не може починатися один після іншого (приймач не зможе розділити де закінчився один пакет і почався інший), тому стандартом встановлений інтервал 96 BT);

– PDV (Path Delay Value, затримка в дорозі) - подвійний час (подвійна затримка) проходження сигналу між абонентами мережі. (включає затримку по кабелю, в самих мережевих адаптерах (передавач - приймач) і проміжних пристроях);

– ST (Slot time, час каналу, квант часу) - максимально допустимий PDV (ST = 512 Вт (верхній допустима межа затримки)). (системний час в мережі - мінімальний часовий інтервал, для виникнення події, визначається мінімальною тривалістю пакета) (якщо дві події в мережі відбуваються з тимчасовим зрушенням <ніж часовий інтервал, то вони відбуваються одночасно);

– максимальний діаметр мережі - допустима довжина мережі (PDV = ST = 512 BT). (виходячи з ST (часу каналу) допустима довжина мережі, це десь виконується умова на максимальну затримку) більше цього розміру мережу бути не може;

– Jam (сигнал-пробка) - послідовність тривалістю 32 BT використовується для посилення колізії;

– Truncated binary exponential back off (усічена двоїчна експоненціальна відстрочка) - затримка перед повторною передачею пакета після колізії. (той часовий інтервал (тимчасова затримка) до початку повторної передачі).

Далі розглянемо як відбувається передача кадрів. Часовий інтервал між кадрами 96 Вт. Більше може бути, менше ні. Розглянемо докладніше алгоритм передачі. Перша частина - те, що відбувається на початку передачі, 2-а при передачі (рис.2.1, 2.2).

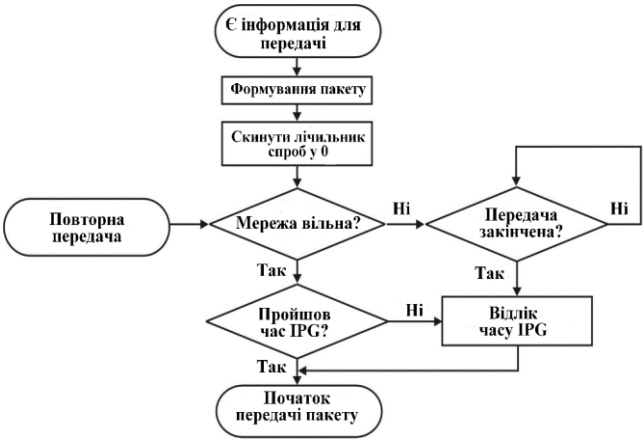

Рисунок 2.1 - Алгоритм початку передачі

Кількість повторів обмежено 16 спробами. Тому лічильник скидається в нуль. Якщо відбувається повторна передача. Ми переходимо на блок «Повторна передача».

Рисунок 2.2 - Алгоритм передачі пакету

Після передачі кожного біта перевіряємо є колізія чи ні. Якщо є то сигнал-пробка і перевірка лічильника спроб (16). Якщо менше 16, то повторна передача. Обчислення затримки повтору передачі. Затримка обчислюється по формулі:

$$RAND\ (0,\ 2\ min\ (N,\ 10)) \bullet ST, \qquad (2.1)$$

де N - значення лічильника спроб; RAND (a, b) ─ генератор випадкових нормально розподілених цілих чисел в діапазоні a ... b, включаючи крайні значення; ST ─ квант часу, рівний 512 BT; максимальна затримка дорівнює 1024 ST (524788 BT). (так як N до 10) (затримка обчислюється як випадкове число в діапазоні від 0 до 2^N, (з кожною наступною спробою діапазон затримок збільшується в 2 рази) і множиться на квант часу = 512 вт) (поки кількість спроб = 10).

У реальній мережі зазвичай 2-3 повтори, якщо мережа перевантажена (велика інтенсивність обміну) то може бути 4-5.

Як відрізнити, що кадри зіткнулися і пакет прийнятий неправильний. Маємо 3 ознаки. Ознаки спотвореного колізією кадру:

– кадр має довжину, меншу мінімально допустимого розміру 512 BT (карликовий кадр) - якщо колізія сталася до 480-го біта кадру;

– кадр має неправильну контрольну суму - якщо колізія сталася після 480-го біта кадру, то сигнал-пробка (32 біта) грає роль контрольної суми;

– кадр має довжину, не рівну цілому числу байт, - якщо колізія сталася в середині одного з переданих байтів. (саме довжина кадру тільки ціле число байт).

2.4 Область колізій. Розрахунок PDV

Приклад формування двох доменів колізій (рис.2.3).

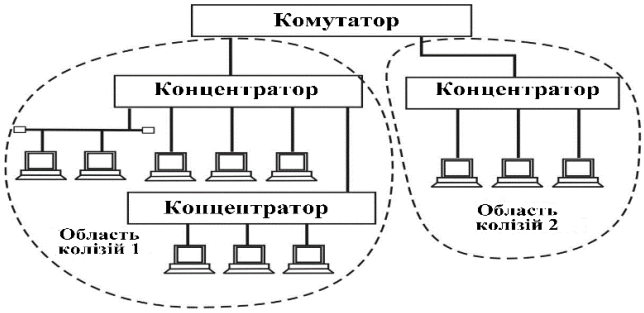

Рисунок 2.3 - Область колізії (Collision Domain)

Допустимі розміри мережі Ethernet визначаються:

– обмеження на довжину сегмента, пов'язані з загасанням і перекручуванням форми сигналу:10Base5 - 500 м і правило "5-4-3", 10Base2 - 185 м і "5-4-3", 10BaseT/100BaseTX/100BaseT4 - 100 м;

– обмеження на кількість вузлів в домені - не більше 1024;

– обмеження на кількість повторювачів між будь-якою парою вузлів: Ethernet - 4, Fast Ethernet - 1 або 2, Gigabit Ethernet – 1;

– обмеження на розмір домену колізій, пов'язані з часом поширення сигналу між кінцевими вузлами мережі: час подвійного обороту для Ethernet, Fast Ethernet і Gigabit Ethernet не повинно перевищувати 512 bt та для Gigabit Ethernet (якщо використовується одномодове волокно) - 2048 bt.

Для мереж на мідних кабелях - досить виконати перші три умови. Подвійна затримка поширення сигналу (PDV) по шляху максимальної довжини не повинна перевищувати 512 bt. У затримку входять: затримки в мережевих адаптерах, затримки в концентраторах, затримки в кабелях. Обмеження на довжину кабелів і кількість концентраторів.

Зменшення міжпакетної щілини (ΔIPG) для будь-якого шляху не повинно перевищувати 49 bt. IPG зменшується при проходженні пакетів через концентратори. Обмеження на кількість концентраторів. Обидва умови повинні виконуватися для всієї мережі. На рисунку 2.4 та в таблиці 2.2 (значення затримок) наведено приклад, який відображає метод знаходження шляху максимальної довжини Ethernet.

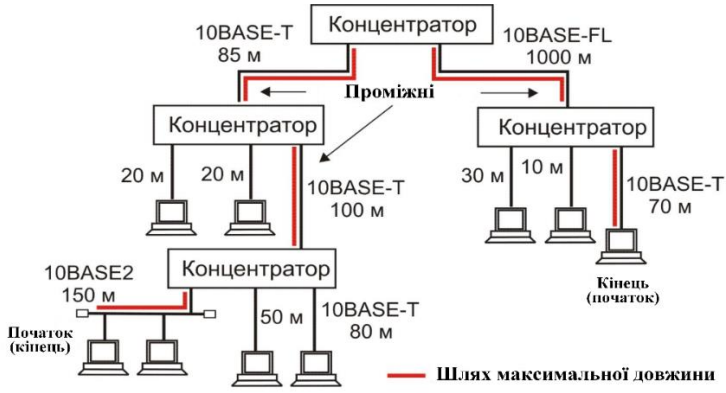

Рисунок 2.4 - Шлях максимальної довжини Ethernet

Таблиця 2.2 - Розрахунок PDV для мережі Ethernet (10 Мбит/с)

Тип сегменту	t_0 нач. сегм.	t_0 пром. сегм.	t_0 кінц. сегм.	t_1 на метр
10BASE5	11,8	46,5	169,5	0,087
10BASE2	11,8	46,5	169,5	0,103
10BASE-T	15,3	42,0	165,0	0,113
10BASE-F	12,3	33,5	156,5	0,100

При цьому PDV = Σ $PDV_S \leq$ 512 BT(bt), а $PDV_S = t_o + L \cdot t_l$, де L — довжина кабелю сегменту в метрах. Для прикладу наведеного на рисунку 2.4 отримаємо:

$PDV_1 = t_o + L \cdot t_l = 11,8 + 150 * 0,103 = 27,25$ BT(bt)

$PDV_2 = t_o + L \cdot t_l = 42 + 100 * 0,113 = 53,3$ BT

$PDV_3 = t_o + L \cdot t_l = 42 + 85 * 0,113 = 51,6$ BT

$PDV_4 = t_o + L \cdot t_l = 33,5 + 1000 * 0,1 = 133,5$ BT

$PDV_5 = t_o + L \cdot t_l = 165 + 70 * 0,113 = 172,9$ BT

PDV = Σ $PDV_S = 27,25 + 53,3 + 51,6 + 133,5 + 172,9 = 438,55$ BT ≤ 512 BT, що є підтвердженням працездатності мережі.

У випадку різних специфікацій на кінцях сегменту, розрахунок повторюємо у зворотному напрямку.

При проведенні розрахунку за іншим методом маємо наступну формулу $\Delta IPG = \Sigma \Delta IPG_S \leq 49$ BT(bt). Дані затримок на сегментах беремо з довідкової таблиці. Враховуються тільки початковий і проміжні сегменти шляху. Кінцевий сегмент не враховується.

Для перевірки на допустимість розміру домену колізій складають топологічний план мережі, на якому зазначають типи активного обладнання, типи і довжину кабельних сегментів. Далі визначають час подвійного обороту для пари вузлів, максимально віддалених один від одного (час поширення сигналу).

Якщо час вписується у обмеження - мережа працездатна. Якщо PDV виявиться більше допустимого, доведеться змінювати топологію чи розбивати мережу на сегменти (домени колізій) меншого розміру і пов'язувати їх мостами, комутаторами чи маршрутизаторами.

Для розрахунку допустимого розміру мережі Fast Ethernet скористаємось значеннями затримок для кабелів, адаптерів та концентраторів, які наведено в таблицях 2.3 – 2.5.

Таблиця 2.3 - Затримки, які вносяться кабелем

Тип кабелю	Подвоєна затримка бітових інтервалів на один метр	Подвоєна затримка на кабель максимальної довжини
UTP 3	1,14 BT	114BT на 100м
UTP 4	1,14 BT	114BT на 100м
UTP 5	1.112 BT	111.3 на 100м
STP	1.112 BT	111.3 на 100м
оптоволокно	1	412

Таблиця 2.4 - Затримки, які вносяться адаптерами

Тип мережевих адаптерів	Максимальна затримка при подвійному обороті
Два адаптера TX/FX	100 BT
Два адаптера T4	138 BT
Один адаптер TX/FX і другий T4	127 BT

Таблиця 2.5 - Затримки, які вносяться концентраторами

Тип концентраторів (повторювачів)	Максимальна затримка при подвійному обороті (BT)
Концентратор класу 1	140
Концентратор класу два з портами TX/FX	92
Концентратор 2 кл. порти T4	67

Розглянемо мережу 100BaseTX з двома повторювачами класу II. Підсумуємо наступні затримки:

– пара адаптерів TX – 100 BT;

– два кабельних сегмента по 100 м і шнур між повторювачами (5 м) - (100 + 100 + 5) x 1,112 BT = 227,96 BT;

– два повторювача TX класу II – 2 x 92 BT = 184 BT.

Разом: 100 BT + 227,96 BT + 184 BT = 511,96 BT < 512 BT - обмеження дотримується, хоча майже без запасу. Правда, для кабелю категорії 5 в таблиці наводиться погонне подвійна затримка 1,112 bt / м, що відповідає швидкості поширення сигналу 0,6c (c - швидкість світла у вакуумі), але багато кабелів мають швидкість поширення в межах 0,67- 0,75c.

Якщо в розрахунок брати кабель зі швидкістю поширення 0,7 с, то він в даному випадку вносить подвійну затримку на 32 bt менше, що і забезпечує необхідний запас. При використанні сегмента максимальної довжини для 100BaseFX (412 м) місця для повторювача вже немає - останні 100 bt "з'їдає" пара адаптерів.

2.5 Формат кадру Ethernet

Хоча Ethernet містить багато стандартів фізичного рівня, сам Ethernet працює як єдина технологія локальної мережі, оскільки використовує однаковий стандарт канального рівня для всіх типів фізичних каналів Ethernet. Цей стандарт визначає загальний заголовок і трейлер для кадру Ethernet. Незалежно від того, чи передаються дані через кабель UTP чи будь-який вид оптоволоконного кабелю, і незалежно від швидкості, заголовок і трейлер використовують однаковий формат.

Історично Ethernet визначає декілька альтернативних форматів для заголовка, причому сьогодні широко використовується формат кадру, показаний на рисунку 2.5.

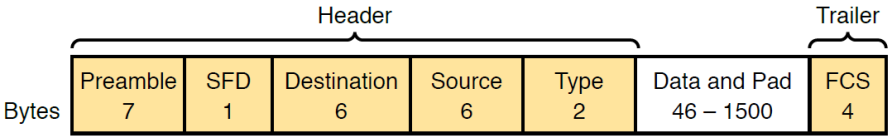

Рисунок 2.5 – Формат кадру Ethernet

Призначення полів кадру Ethernet:

– преамбула (синхронізація прийому) 8 байт: перші сім байт – це код синхронизації, зазвичай 10101010 …., восьмий байт – має 10101011 (є ознакою початку кадру);

– адреса одержувача та адреса відправника – 6-байтні стандартні MAC-адреси;

– поле управління (2 байти, L/T – Length/Type) – вказує або кількість байт у полі даних (до 1500) або тип пакету (більше 1500);

– поле даних – займає від 46 до 1500 байт даних. Якщо передається менше 46 байт – використовується поле заповнення;

– поле контрольної суми (трейлер) (FCS – Frame Check Sequence) – 32-розрядна циклічна контрольна сума (CRC);

– повна довжина кадру без преамбули – від 512 біт (64 байти) до 12144 біт (1518 байт).

Зверніть увагу на те, що кадр Ethernet не може бути без даних. Мінімальний розмір кадру Ethernet - 64 байти, максимальний - 1518 байт. Поле Преамбула не враховується під час підрахунку довжини кадру. Будь-який кадр довжиною менше ніж 64 байти вважається "фрагментом", який утворився в результаті колізії, його ще називають "карликовим кадром" і він автоматично відкидається. Кадри, довші за 1500 байтів вважаються "переповненими" або "гігантськими". Якщо розмір переданого кадру є меншим за мінімальний або більшим за максимальний, то приймаючий пристрій знищує кадр. Знищені кадри є результатом колізій або інших небажаних випадків передачі сигналу.

На рисунку 2.6 показано приклад процесу передачі кадру між мережами, які підтримують різні стандарти технології Ethernet. У цьому випадку ПК1 надсилає кадр Ethernet до ПК3. Кадр передається по каналу UTP до комутатора Ethernet SW1, потім по волоконно-оптичним лініям до комутаторів Ethernet SW2 і SW3 і, нарешті, через інший канал UTP до ПК3. Зверніть увагу, що в цьому прикладі біти фактично передаються з чотирма різними швидкостями: 10 Мбіт/с, 1 Гбіт/с, 10 Гбіт/с і 100 Мбіт/с відповідно.

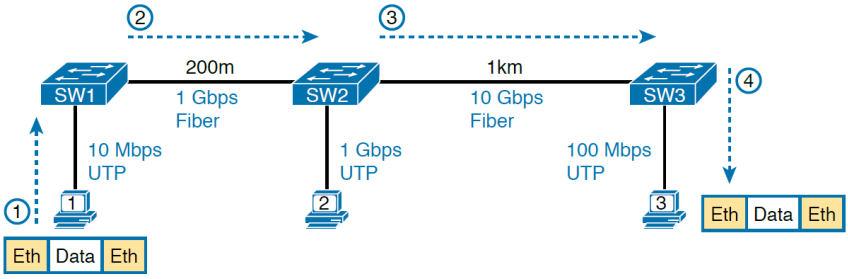

Рисунок 2.6 – Процес передачі кадру Ethernet

Ethernet є комбінацією пристроїв користувача, концентраторів і комутаторів локальної мережі із використанням різних видів кабелю

(фізичного середовища). Кожне з'єднання може використовувати різні типи кабелів із різною швидкістю.

2.6 Фізичні з'єднання

2.6.1 Ethernet та Fast Ethernet

Розглянемо три поширених стандарти Ethernet: 10BASE-T (Ethernet), 100BASE-T (Fast Ethernet або FE) і 1000BASE-T (Gigabit Ethernet або GE), та деталі надсилання даних в обох напрямках використовуючи кабель UTP із перевіркою конкретного з'єднання кабелів UTP, які використовуються для Ethernet 10 Мбіт/с, 100 Мбіт/с і 1000 Мбіт/с.

Термін зв'язок Ethernet стосується будь-якого фізичного кабелю між двома вузлами Ethernet. Щоб дізнатися, як працює UTP-з'єднання Ethernet, можна розбити фізичне з'єднання на основні частини, як показано на рисунку 2.7: сам кабель, роз'єми на кінцях кабелю та відповідні порти на пристрої, в які будуть вставлятися роз'єми.

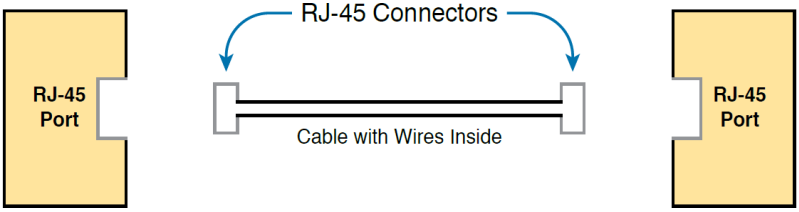

Рисунок 2.7 – UTP-з'єднання Ethernet

Кабель UTP містить декілька мідних проводів, згрупованих як виті пари. Для стандартів 10BASE-T і 100BASE-T потрібні дві пари проводів, а для стандарту 1000BASE-T – чотири пари.

Багато кабелів Ethernet UTP використовують роз'єм RJ-45 на обох кінцях. Він має вісім фізичних точок, які є роз'ємами контактів і в них можна вставити вісім проводів кабелю, які мають контакт з електронікою всередині вузлів на кінці фізичного з'єднання.

Для завершення фізичного з'єднання кожному з вузлів потрібен порт Ethernet RJ-45, який відповідає роз'ємам RJ-45 на кабелі, щоб роз'єми на кінцях кабелю могли підключатися до вузла. Комп'ютери

часто включають цей порт Ethernet RJ-45 як частину мережевої інтерфейсної карти (NIC), яка може бути або платою розширення на ПК або вбудованою схемою в системі. Комутатори зазвичай мають багато портів RJ-45, які надають користувачам можливість підключатися до локальної мережі Ethernet.

На рисунку 2.8 показано чотири дроти, які розташовані в одному кабелі UTP, що з'єднує ПК і комутатор локальної мережі. У цьому прикладі ПК ліворуч передає за допомогою верхньої пари, а комутатор праворуч передає за допомогою нижньої пари.

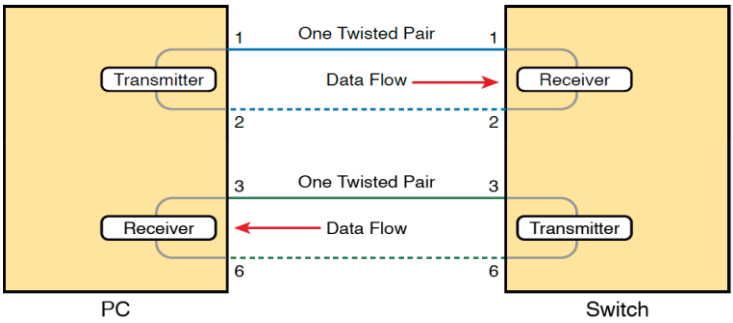

Рисунок 2.8 – Процес передачі через канал

Для правильної передачі через канал дроти UTP-кабелю мають бути під'єднані до правильних позицій контактів у роз'ємах RJ-45. Щоб зрозуміти підключення кабелю потрібно спочатку зрозуміти, як працюють мережеві карти та перемикачі. Як правило, передавачі Ethernet NIC використовують пару, підключену до контактів 1 і 2; а приймачі NIC пару проводів на контактах 3 і 6. Комутатори локальної мережі, знаючи, що роблять мережеві адаптери Ethernet, роблять навпаки: їхні приймачі використовують пару проводів на контактах 1 і 2, а їхні передавачі використовують пару проводів на контактах 3 і 6.

Щоб дозволити мережевій картці комп'ютера обмінюватися даними з комутатором, кабель UTP має використовувати розводку прямого кабелю. Термін «розпіновка» стосується того, провід якого кольору розміщено в кожному з восьми пронумерованих контактів роз'єму RJ-45. Прямий кабель Ethernet з'єднує провід на контакті 1 на одному кінці кабелю з контактом 1 на іншому кінці кабелю; провід на

контакті 2 потрібно підключити до контакту 2 на іншому кінці кабелю; контакт 3 на одному кінці з'єднується з контактом 3 на іншому і так далі. Крім того, він використовує дроти в одній парі проводів на контактах 1 і 2, а іншу пару на контактах 3 і 6 (рис.2.9).

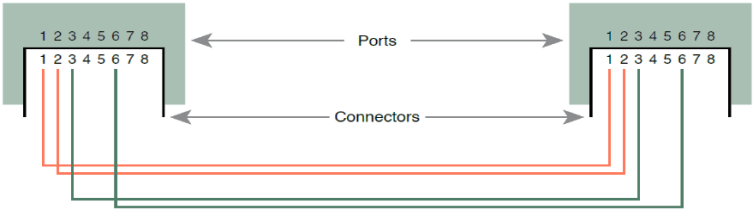

Рисунок 2.9 – Прямий кабель Ethernet

Прямий кабель працює правильно, коли вузли використовують протилежні пари для передачі даних. Однак, коли два схожі пристрої підключаються до каналу Ethernet, вони обидва передають дані на тих самих контактах. У цьому випадку вам знадобиться інший тип кабелю, який є перехресним кабелем. Розпіновка перехресного кабелю перетинає пару на контактах передачі на кожному пристрої з контактами прийому на протилежному пристрої.

На рисунку 2.10 показано, що відбувається при з'єднанні між двома комутаторами. Обидва передають на контактах 3 і 6, і приймають на контактах 1 і 2. Таким чином, кабель має з'єднати пару контактів 3 і 6 з одного боку із контактами 1 і 2 з іншого боку, з'єднуючись із логікою приймача іншого вузла. У верхній частині рисунка показано розпіновку, а в нижній половині – концептуальну схему.

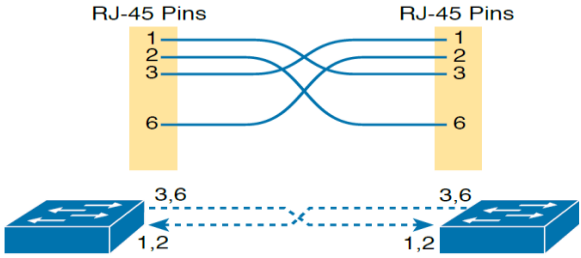

Рисунок 2.10 – Перехресний кабель

Щоб вибрати, який тип кабелю (прямий чи перехресний) потрібен у кожній частині мережі, потрібно знати, чи працює пристрій як мережева плата ПК (є пристроєм DTE), передаючи дані на контактах 1 і 2, чи як комутатор (DCE), передаючи дані на контактах 3 і 6.

2.6.2 Gigabit Ethernet

1000BASE-T (Gigabit Ethernet) відрізняється і від 10BASE-T і 100BASE-T кабельною розводкою та контактами. По-перше, для 1000BASE-T потрібні чотири пари проводів. По-друге, він використовує більш досконалу електроніку, яка дозволяє обом кінцям одночасно передавати та приймати по кожній парі проводів.

Однак схема проводки для 1000BASE-T працює майже ідентично попереднім стандартам, додаючи правила для додаткових двох пар. Прямий кабель для 1000BASE-T використовує чотири пари проводів для створення чотирьох ланцюгів. Він використовує ті самі контакти для двох пар, що й стандарти 10BASE-T і 100BASE-T, і додає пару на контакти 4 і 5 та пару на контакти 7 і 8, як показано на рисунку 2-11.

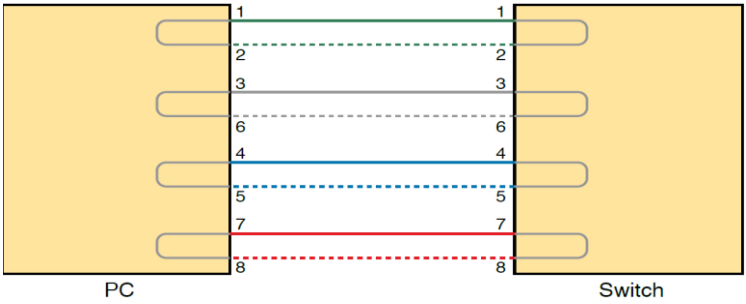

Рисунок 2.11 – Прямий кабель 1000BASE-T

Перехресний кабель Gigabit Ethernet перетинає ті самі двожильні пари, що й перехресний кабель для інших типів Ethernet (пари на контактах 1,2 і 3,6). Він також перетинає дві нові пари (пару на контактах 4,5 із парою на контактах 7,8).

Так як стандарти Ethernet на основі UTP використовують кабель довжиною до 100 метрів, то більшість з'єднань Ethernet на підприємстві найчастіше використовують виту пару, тому що відстань від

комутатора Ethernet до кожної кінцевої точки на поверхах будівлі, швидше за все, буде менше за 100 м. Однак у деяких випадках інженер може віддати перевагу використанню оптоволоконного кабелю для деяких з'єднань у локальній мережі Ethernet, звичайно спочатку з метою досягнення більших відстаней, а також можливо із інших причин. Щоб підключити оптоволокно до комутаторів Ethernet, потрібно використовувати комутатор із вбудованими портами, які підтримують певний оптичний стандарт Ethernet, або комутатор із модульними портами, які дозволяють змінювати стандарт Ethernet, який використовується на порту. Звернимося до рисунку 2.12 на якому зображено комутатор з двома портами SFP+, куди можна вставити будь-який із модулів SFP+.

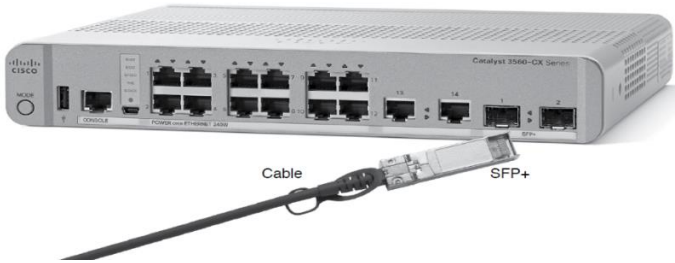

Рисунок 2.12 – Комутатор з двома портами SFP+

Ці порти SFP+ підтримують різні стандарти 10 Гбіт/с Ethernet. Щоб побудувати локальну мережу Ethernet в офісі, вам може знадобитися використання декількох багатомодових і одномодових оптоволоконних з'єднань. Фактично, у багатьох офісах уже можуть бути встановлені оптоволоконні кабелі для очікуваного, майбутнього використання орендарями будівель. Якби кожна будівля розташовувалась в межах декількох сотень метрів від принаймні однієї іншої будівлі, ви могли б використовувати багатомодове оптоволокно між будівлями та підключати комутатори для створення локальної мережі. Хоча відстань є першим критерієм, який слід враховувати, вибираючи використання UTP чи оптоволоконного кабелю, існує також інші критерії.

3 МЕРЕЖНИЙ РІВЕНЬ. АДРЕСАЦІЯ. МАРШРУТИЗАЦІЯ

3.1 Максимальна одиниця передачі MTU

MTU (Maximum Transmission Unit - максимальна одиниця передачі). MTU - максимальний розмір пакета даних, який може бути переданий за один фізичний кадр по стеку протоколів TCP/IP. При установці нового з'єднання два віддалених комп'ютера повинні узгодити між собою розмір кадру. Окрім того слідуючи до місця призначення, пакет долає цілий ряд проміжних серверів і маршрутизаторів, настройки MTU яких можуть бути абсолютно різними (рис.3.1). Тому занадто великий пакет в мережі фрагментується і заповнюється «повітрям», «баластом», що негативно позначається на ефективності зв'язку.

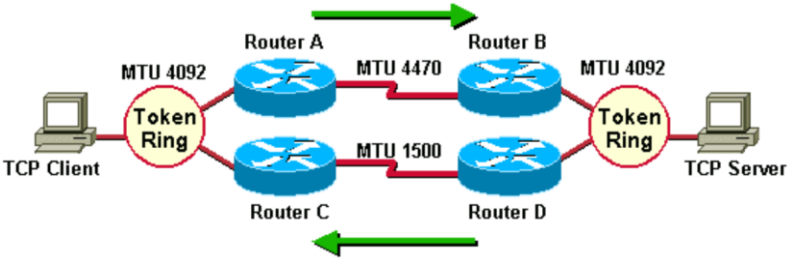

Рисунок 3.1 – Передача кадру між мережами з різним MTU

Якщо провайдер має установки MTU = 576, а у вас в Windows задано MTU = 1500, то кожний пакет розбивається на три по 576 байт: 576 + 576 + 576 = 1728 - тобто, 228 байт баласту додаються до кожного пакету. Але навіть якщо провайдер теж має MTU = 1500, то при зв'язку з віддаленим сервером цілком може бути задіяний маршрутизатор з меншим значенням MTU (рис.3.2) і пакети знову-таки фрагментуватимуться, сповільнюючи передачу даних. Цю ситуацію рятує включена в Windows, за замовчуванням, функція автоматичного визначення MTU - «PMTU Discovery» або «MTU Auto Discovery». Але процедура обчислення MTU для кожного з'єднання вимагає багато часу, що може затримувати роботу при передачі невеликих файлів. Окрім того, у разі неузгодження ваших параметрів з параметрами провайдера, ця функція навряд чи вам допоможе.

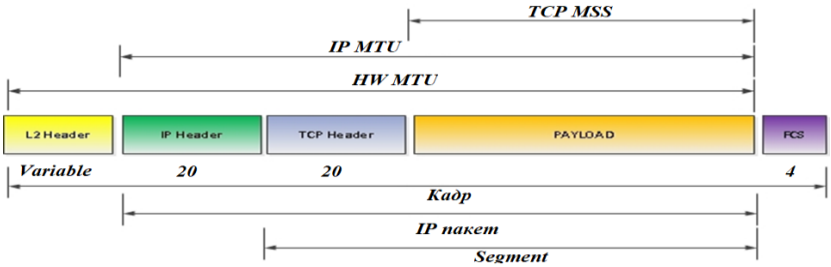

Рисунок 3.2 – Максимальний розмір пакету

Звичайно, існують загальноприйняті стандарти для даного параметра, так, наприклад, для Ethernet MTU = 1500 байт, для SLIP - 1006, для PPPoE -1492, для PPP, тобто модемного зв'язку з Інтернетом - 576. Для Ethernet MTU дорівнює 1500 байт - означає, що максимальний об'єм даних, що переноситься кадром, не може перевищувати 1500 байт (без урахування Eth-заголовка і CRC).

IP (Intrenet Protocol - міжмережевий протокол), описаний в RFC751. Важливою функцією IP – є підтримка інтерфейсу із базовими мережевими технологіями, які знаходяться і працюють на рівні моделі OCI, розташованому нижче (на канальному рівні) та підтримка інтерфейсу з протоколами вищого транспортного рівня.

Кожен пакет даних в дійсності складається з декількох сегментів - заголовка і фактичних даних. Формат стандартного заголовку IP-пакету (на прикладі протоколу IPv4) наведено на рисунку 3.3.

4 біта Номер версії	4 біта Довжина заголовку	8 біт Тип сервісу					16 біт Загальна довжина	
		PR	D	T	R			
16 біт Ідентифікатор пакету							3 біта флаги	13 біт Зсув фрагменту
							DF MF	
8 біт Час життя (TTL)		8 біт Протокол верхнього рівня					16 біт Контрольна сума	
32 біти IP-адреса джерела								
32 біти IP-адреса приймача								
Поле параметрів								

Рисунок 3.3 – Структура заголовку IP-пакету

Поле **номер версії** займає 4 біта і ідентифікує версію протоколу IP. Зараз використовується версія 4 (IPv4), але часто зустрічається і нова версія (IPv6).

Довжина заголовка IP-пакета займає 4 біта і вимірюється в 32-бітових словах. Зазвичай заголовок має довжину в 20 байт (п'ять 32-бітових слів). Найбільша довжина заголовка складає 60 байт.

Тип сервісу (Type of Service, ToS) - байт диференційованого обслуговування, або DS-байт. Зберігає ознаки, які відображають вимоги до якості обслуговування пакета. Перші три біти - значення пріоритету пакета: від найнижчого - 0 до найвищого - 7. Наступні три біта - критерій вибору маршруту. Якщо біт D (Delay - затримка) встановлений в 1, то маршрут вибирається з мінімізацією затримки доставки пакету, якщо встановлено в 1 біт T (Throughput - пропускна здатність) - для максимізації пропускної здатності, а біт R (Reliability - надійність) - для максимізації надійності доставки. Решта - два біти, мають нульове значення.

Поле загальної довжини займає 2 байти і характеризує загальну довжину пакета з урахуванням заголовка і поля даних. Максимальна довжина пакета обмежена розрядністю поля, яка визначає цю величину - 65535 байт. Залежить від максимальної довжини пакета протоколу нижнього рівня. Якщо це кадри Ethernet, то вибираються пакети з максимальною довжиною 1500 байт.

Ідентифікатор пакету займає 2 байти і використовується для розпізнавання пакетів, при фрагментації вихідного пакета. Всі фрагменти одного пакету повинні мати однакове значення цього поля.

Флаги займають 3 біта і містять ознаки, пов'язані з фрагментацією. Встановлений в 1 біт DF (Do not Fragment - не фрагментований) забороняє маршрутизатора 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, який залишився - зарезервований.

Поле зсуву фрагмента займає 13 біт і задає зсув у байтах поля даних цього фрагмента відносно початку поля даних вихідного не фрагментованого пакета. Використовується при складанні/розбиранні фрагментів пакетів. Зміщення повинно бути кратним 8 байтам.

Поле часу життя (Time To Live, TTL) - 1 байт, задає граничний термін, протягом якого пакет може переміщатися по мережі. Час життя пакету вимірюється в секундах і задається джерелом пакетів.

Поле протоколу верхнього рівня - один байт - ідентифікатор, який вказує, якому протоколу верхнього рівня належить інформація, яка розміщена в полі даних пакета. Значення ідентифікаторів для протоколів (RFC 1700), за адресою http://www.iana.org. 6 - в пакеті знаходиться повідомлення TCP, 17 - повідомлення UDP, 1 - повідомлення ICMP.

Контрольна сума заголовка -2 байти, розраховується тільки по заголовку.

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

Поле параметрів - необов'язково і використовується тільки при налагодженні мережі. Так як число підполів в полі параметрів може бути довільним, то в кінці заголовка має бути додано декілька нульових байтів для вирівнювання заголовка пакета по 32-бітній границі.

Та частина пакету, в якій містяться тільки фактичні дані, називається MSS (Maximum Segment Size) - це ще один параметр протоколу TCP, що визначає найбільший сегмент даних TCP, які можуть бути передані за один раз.

Тобто, MTU = MSS + заголовки TCP/IP. У реєстрі MSS задається так: **HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ VxD \ MSTCP "DefaultMSS" = "ваше число".**

Для заголовка теж є загальноприйнятий розмір - це 40 байт (20 байт IP і 20 байт TCP), зазвичай MSS = MTU - 40. З цієї причини у визначенні оптимального розміру MTU є деякі тонкощі.

Давайте на прикладі розглянемо передачу даних при різному розмірі MTU по широкосмугової лінії T1 (пропускна здатність T1 = 1544000 bits/sec), використовуючи наступну формулу: [(MSS + заголовок) * 8 бітів / байт] / [1544000 біт / sec] = затримка на один хоп (на кожен комп'ютер в мережі при передачі нашого пакета).

Використовуючи в цій формулі різні величини MTU, ми можемо обчислити затримку одного пакета. Якщо MTU = 1500, тоді: (1460 + 40) * 8/1544000 = 0.7772 ms. Якщо ж MTU = 576, то: (536 + 40) * 8/1544000 = 0.2924 ms. Припустимо, що при передачі пакету зустрічається 10 серверів (хопов), тоді при MTU = 1500 отримаємо затримку 7.772 ms, а при 576 - 2.924 ms - різниця досить помітна - очевидно, якщо пакети менші за розміром, то вони передаються швидше (через обмеження продуктивності лінії). Однак не все так просто.

Використовуючи ту ж формулу порахуємо, за який проміжок часу буде переданий файл розміром 1Mb за тією ж широкосмуговою

лінією T1. Один мегабайт дорівнює 1024 KB і дорівнює 1048576 байтам. Якщо MTU = 1500, то, як ми з'ясували, затримка на один хоп складе 0.7772 ms. Скільки при цьому знадобиться послати пакетів? 1 Mb / MSS = 1048576/1460 = 718.2, або всього потрібно 719 ефективних пакетів, щоб передати 1 мегабайт. Далі, множимо 719 пакетів на 0.7772 ms, отримуємо 558.8068 ms, або 5.588 секунд затримки на один хоп. Якщо ж ми передаємо свій файл через 10 хопів (ситуація зустрічаються частіше, ніж коли через один), то отримуємо 55.88 sec - час, який ми (вірніше, провайдер, який має лінію T1) витратили на передачу файлу в 1Mb при ідеальному зв'язку.

Якщо ж MTU = 576, тоді: 1 Mb / MSS = 1048576/536 = 1956.3, або потрібно 1957 пакетів, щоб передати 1 мегабайт. Далі, множимо кількість пакетів на затримку кожного з них: 1957 * 0,2924 = 572,2268 ms, або 5,722 секунди на один хоп. Ну і відповідно на 10 хопів доведеться витратити 57,22 секунд. Як бачимо, через те, що при використанні великих пакетів передається менше заголовків, реальна швидкість передачі файлу виходить вище.

Для того, щоб передати 1 мегабайт при використанні MTU = 1500, доводиться пересилати ще й «додаток» заголовків з 28760 байтів, тоді як при використанні MTU = 576 отримуємо аж 1957 * 40 = 78,280 байтів, тобто додаткові 49520 байт заголовків на кожен мегабайт корисної інформації.

Для нашої 10-хопової передачі це виливається в зайвих 1,34 секунди при передачі кожного мегабайту навіть при швидкому зв'язку. Ця різниця, можливо, буде ще трохи вище на практиці, оскільки сучасні реалізації TCP / IP використовують більші за розміром заголовки.

При підключенні до Інтернету в термінальному режимі – іноді, при здійсненні реєстрації користувачем, в одному з рядків з'являється рекомендоване значення MTU. Для ручного визначення MTU досить використовувати стандартну утиліту ping:

PING -f -l yyyy xxx.xxx.xxx.xxx -n 10,

де «xxx.xxx.xxx.xxx» - IP-адреса тестованого сервера, «-l» (англійська літера «ель», а не одиниця), yyyy - розмір буфера відправки (MTU) від 576 до 1492 байт (наприклад 1500 = 1472 + 28, де 1472 - розмір неподільного пакету, 28 = 20 байт заголовок IP + 8 байт ICMP. для Ethernet MTU = 1500 байт, для SLIP - 1006, для PPPoE -1492, для PPP (модемного зв'язку) - 576. Таким чином можна вручну підібрати найбільш відповідне значення MTU для вашого з'єднання. Припустимо

ми визначили, що для нас оптимальним є розмір буфера відправки рівний 1500. Додаємо необхідні дані до реєстру.

Значення MTU

HKEY_LOCAL_MACHINE\ System \ CurrentControlSet \ Services \ Class \ NetTrans \ 000x "MaxMTU" = "1500"

HKEY_LOCAL_MACHINE\ System \ CurrentControlSet \ Services \ VxD \ MSTCP

MSS (розмір корисних даних) = ab.1 & 6mb.co & m & ab.16mb.com MTU – 40 "DefaultMSS" = "1460"

HKEY_LOCAL_MACHINE\ System \ CurrentControlSet \ Services \ VxD \ MSTCP

Розмір буфера, в якому накопичується вміст області даних (MSS) декількох отриманих пакетів, перш ніж передається далі, наприклад, в браузер. Розмір RWIN обов'язково повинен бути кратний MSS і зазвичай для кращої ефективності модемного з'єднання рекомендується його встановлювати рівним 4-8 MSS.

Проте надмірно великий розмір буфера також небажаний, особливо на поганих лініях - при втраті всього одного пакета в разі збою на лінії буде повторно затребуваний не один втрачений пакет, а всі пакети з цього буфера, що займе деякий час - 1460 * 4 = 5840 "DefaultRcvWindow" = "5840".

Для того, щоб змінити MTU на маршрутизаторах під керуванням Cisco IOS використовується команда інтерфейс рівня:

R01(config)#interface gigabitEthernet 0/1

R01(config-if)#mtu 1532

R01(config-if)#exit

Перевірити:

R01#show interfaces gigabitEthernet 0/1

Але якщо доступ до Інтернету та передача даних працюють коректно, не варто експериментувати з параметром MTU, так як під час неправильних дій ви можете лише погіршити роботу мережі.

3.2 IP-адресація

IP-адреси являють собою основний тип адрес, на підставі яких мережний рівень передає пакети між мережами. Мережну адресу встановлює користувач (адміністратор) або вона призначається динамічно, протоколом DHCP з діапазону виділених адрес.

Мережна адреса має бути достатньо довгою (в IP-мережах версії IPv4 вона містить 32 біта (4 байти)), що дорівнює 2^{32} = 4294967296 та ієрархічною (на відміну від MAC-адрес інтерфейсів).

4-х байтова адреса може бути представлена у різних системах числення: десятковій, двійковій, шістнадцятковій:

175.100.220.14;

10101111 01100100 11011100 00001110;

A F 6 4 D C 0 E

Незважаючи на те, що в третьому випадку цифр менше, поширеним є десяткове подання, точніше точково-десяткове. Частина адреси (старші розряди) є номером мережі, а інша частина (молодші розряди) - номером вузла в мережі.

Виходячи з того, яка частина адреси відноситься до номера мережі, а яка - до номера вузла, адреси діляться на 5 класів: A, B, C, D та E. Для унікальної адресації вузлів використовуються тільки три перших класи адрес.

В адресі класу A старший байт задає адресу мережі, а три молодших байти - адресу вузла (host). 0.x.y.z - 127.x.y.z - мереж 2^7 - 2 (не може бути 0 і 127) = 126 мереж, вузлів 2^{24} = 16 млн.

В адресі класу B два старших байти задають адресу мережі, а два молодших байти - адресу вузла (host). 128.x.y.z - 191.x.y.z - мереж 2^{14} = 16 тис., Вузлів 2^{16} = 64 тис.

В адресі класу C три старших байти задають адресу мережі, а молодший байт - адресу вузла. 192.x.y.z - 223.x.y.z - мереж 2^{21} = 2 млн., Вузлів 2^8 = 256.

Існує також багатоадресний клас D і резервний клас E.

Номер вузла (адреса host) не може складатися тільки з одних одиниць або нулів. Якщо в поле адреси вузла всі нулі, це означає, що задається номер (адреса) мережі або підмережі.

Приватні адреси:

- 10.0.0.0 - 10.255.255.255 / 8;
- 172.16.0.0 - 172.31.255.255 / 12;
- 192.168.0.0 - 192.168.255.255 / 16.

Особливі адреси:

- IP-адреса 0.0.0.0;
- IP-адреси з нульовим номером мережі є поточною мережею;

– адреса, яка складається з усіх одиниць, забезпечує широкомовлення в межах поточної (зазвичай локальної) мережі - 255.255.255.255;

– адреси, в яких вказана мережа, але з усіма одиницями в поле номера хоста, забезпечують широкомовлення в межах віддаленої локальної мережі;

– адреси, які мають вид 127.x.y.z зарезервовані для тестування мережного програмного забезпечення методом зворотної передачі;

– 169.254.0.0/16 (169.254.0.1 - 169.254.255.255) - zeroconf.

Маски. У класовій адресації маємо недоцільність використання адресного простору для невеликих мереж, тому введене додаткове поле, що має назву - маска мережі.

Маска - 32 бітове число, яке використовується в парі з IP-адресою. Двійковий запис маски містить послідовність одиниць в тих розрядах, які повинні в IP-адресі інтерпретуватися як номер мережі. Оскільки номер мережі - цільна частина адреси, то одиниці в масці повинні представляти безперервну послідовність.

Додаючи кожній IP-адресі маску, можна відмовитися від понять класів адрес і зробити систему адресації більш гнучкою.

Нехай для IP-адреси 129.64.134.5 вказана маска 255.255.128.0. Якщо ігнорувати маску, то відповідно до системи класів 129.64.134.5 відноситься до класу B, тому номер мережі - перші два байти - 129.64.0.0, а номер вузла - 0.0.134.5.

Якщо ж використовувати для визначення границі номеру мережі маску, то 17 послідовних двійкових одиниць у масці 255.255.128.0, «накладені» на IP-адресу, ділять його на наступні дві частини: номер мережі 10000001. 01000000. 1 (129.64.128.0) і номер вузла 0000110. 00000101 (0.0.6.5). Маршрутизатор, отримавши пакет, з адресою призначення отримує адресу мережі, яку реалізує шляхом логічного множення мережної адреси вузла на маску.

Маски змінної довжини. Використовуючи маски різної довжини для створення підмереж, адміністратор може формувати підмережі різного розміру в межах однієї автономної системи. Таким чином, маски змінної довжини (Variable-Length Subnet Mask - VLSM) дозволяють створювати підмережі різного розміру, при цьому гнучко задаючи границі між полем адреси мережі і полем адреси вузла.

VLSM дають можливість задіяти більше ніж одну маску підмережі в межах виділеного адресного простору мережі.

3.3 Приклади вирішення завдань

Розглянемо **практичне завдання з визначення класу мережі та типу адреси**. Для наведених адрес маємо:

- 201.10.255.0 – клас C, адреса мережі;
- 190.195.0.255 – клас B, адреса вузла;
- 9.255.255.255 – клас A, широкомовна адреса;
- 10.10.255.0 – клас A, адреса вузла;
- 134.11.255.255 – клас B, широкомовна адреса;
- 252.250.0.255 – клас E, зарезервована адреса;
- 194.18.144.25 – клас C, адреса вузла;
- 129.77.0.0 – клас B, адреса мережі;
- 237.101.5.0 – клас D, групова адреса;
- 126.0.0.0 – клас A, адреса мережі.

Наведемо приклад **застосування маски для визначення номера мережі і діапазону вузлів** маючи IP-адресу і маску.

Нехай задана IP-адреса: 210.56.78.212. Віднесемо до неї маску 255.255.255.224 (префікс / 27) (в двійковому вигляді). Що тепер номер мережі, а що номер вузла?

Представимо у двійковому вигляді адресу, виконаємо логічне множення на маску, та отримаємо адресу мережі - 210.56.78.192.

Кількість вузлів маємо 2^5 (кількість нулів у масці = 5) = 32 - 2 (адреса мережі і широкомовна адреса) = 30.

Отримаємо діапазон адрес даної мережі:

- адреса першого вузла - 210.56.78.193;
- адреса останнього вузла - 210.56.78.222;
- широкомовна адреса - 210.56.78.223.

У ряді випадків для зручності управління адміністратор може самостійно формувати підмережі всередині виділеного діапазону.

Розглянемо **практичне завдання з формування підмереж із однаковою кількістю вузлів**. Почнемо з формування мереж класу C.

Маємо адресу мережі - 212.24.222.0 / 24.

Розділимо її на 2 підмережі, для цього використовуємо 1 біт маски. Маска збільшиться на 1.

212.24.222.0 | 0000000 / 25 (255.255.255.128)

255.255.255.1 |

Перша підмережа 212.24.222.0 / 25.

Діапазон адрес - 212.24.222.1 - 212.24.222.126, 212.24.222.127 - широкомовна адреса.

Друга підмережа 212.24.222.128 / 25.

Діапазон адрес - 212.24.222.129 - 212.24.222.254, 212.24.222.255 - широкомовна адреса.

Маючи маску 255.255.255.224 (/27) можемо отримати 2^3 підмереж і 2^5-2 вузлів.

Якщо адміністратору виділена адреса мережі класу С (дорівнює 198.11.163.0) і йому необхідно створити 10 комп'ютерних підмереж по 14 вузлів, то для адресації 10 підмереж потрібно 4 розряди адреси (4 біта). У цьому випадку максимально можна бути задати 16 підмереж по 14 вузлів у кожній. З 16 підмереж адміністратор використовує 10, а решта 6 використовуватися не будуть (резервні). У практичних випадках мережі формуються з різною кількістю вузлів в мережі.

Розглянемо **практичне завдання з формування підмереж з використанням масок змінної довжини**.

Дана адреса мережі **200.33.224.0/24** і маска, необхідно сформувати **9** підмереж: 3 підмережі на 50 вузлів; 3 підмережі на 10 вузлів; 1 підмережа на 4 вузла; 2 підмережі на 2 вузли.

Після збільшення маски на 2 біти (**200.33.224. |00| 000000**) маємо наступні підмережі:

- **200.33.224.0/26** – перша на 62 вузли (виділяємо на 50 вузлів);
- 200.33.224.1-200.33.224.62 – діапазон;
- 200.33.224.63 – широкомовна адреса;
- **200.33.224.64/26** – друга на 62 вузли (виділяємо на 50 вузлів);
- 200.33.224.65-200.33.224.126 – діапазон;
- 200.33.224.127 – широкомовна адреса;
- **200.33.224.128/26** – третя на 62 вузли (виділяємо на 50 вузлів);
- 200.33.224.129-200.33.224.190 – діапазон;
- 200.33.224.191 – широкомовна адреса;
- **200.33.224.192/26** – підмережа на 62 вузли (цю ділимо далі по 10 вузлів).

Після збільшення маски на 2 біти (**200.33.224. 11 |00| 0000**) маємо наступні підмережі:

– **200.33.224.192/28** – четверта на 14 вузлів (на 10 вузлів);
– 200.33.224.193-200.33.224.206 – діапазон;
– 200.33.224.207– широкомовна адреса;
– **200.33.224.208/28** – п’ята на 14 вузлів (на 10 вузлів);
– 200.33.224.209-200.33.224.222 – діапазон;
– 200.33.224.223 – широкомовна адреса;
– **200.33.224.224/28** – шоста на 14 вузлів (на 10 вузлів);
– 200.33.224.225-200.33.224.238 – діапазон;
– 200.33.224.239 – широкомовна адреса;
– **200.33.224.240/28 -** підмережа на 14 вузлів (цю ділимо далі по 4 вузли).

Після збільшення маски на 1 біт (**200.33.224. 1111 |0| 000**) маємо наступні підмережі:

– **200.33.224.240/29** – сьома на 6 вузлів (виділяємо на 4 вузли);
– 200.33.224.241-200.33.224.246 – діапазон;
– 200.33.224.247 – широкомовна адреса;
– **200.33.224.248/29 -** підмережа на 6 вузлів (цю ділимо далі по 2 вузли).

Після збільшення маски на 1 біт (**200.33.224. 11111 |0| 00**) маємо наступні підмережі:

– **200.33.224.248/30** – восьма на 2 вузли;
– 200.33.224.249-200.33.224.250 – діапазон;
– 200.33.224.251 – широкомовна адреса;
– **200.33.224.252/30** – дев’ята на 2 вузли;
– 200.33.224.253-200.33.224.254 – діапазон;
– 200.33.224.255 – широкомовна адреса.

Таким чином отримали 9 підмереж із різною кількістю вузлів.

3.4 Маршрутизація

Маршрутизація – дія з передачі пакета з однієї логічної мережі (або підмережі) до іншої. Маршрутизатор – проміжний пристрій у складній (розподіленій) мережі, який виконує цю дію.

Маршрутизатори – пристрої мережевого рівня з двома або декількома мережевими інтерфейсами (або портами). Кожен інтерфейс маршрутизатора є окремим кінцевим вузлом мережі та має мережеву

адресу у тій мережі, яка до нього підключена. Пакети в мережі передаються маршрутизатором на підставі прокладених маршрутів за певними критеріями.

При цьому завдання вибору маршруту, з декількох можливих, вирішують як маршрутизатори, так і кінцеві вузли. Маршрут вибирається на підставі інформації про поточну конфігурацію мережі, та на підставі критерію вибору маршруту. Як критерій можуть вибиратися: затримка проходження маршруту окремим пакетом; середня пропускна спроможність маршруту для послідовності пакетів; або кількість пройдених проміжних маршрутизаторів. Вся, отримана під час аналізу інформація про маршрути, заноситься до таблиць маршрутизації. Типи маршрутизації - без таблиць і на основі таблиць.

Маршрутизація без таблиць:

– лавинна - кожен маршрутизатор передає пакет всім своїм сусідам по всім активним інтерфейсів, крім того, від якого його отримав;

– маршрутизація, керована подіями - пакет до певної мережі призначення надсилається за маршрутом, вже наводив раніше до успіху (для даної адреси призначення);

– маршрутизація від джерела - відправник поміщає в пакет інформацію, які хопи повинен пройти пакет до мережі призначення.

Маршрутизація на основі таблиць:

– статична «фіксована» - таблиці вводяться в пам'ять кожного маршрутизатора вручну адміністратором мережі. Всі записи в таблиці мають статус статичних з нескінченний терміном життя; таблиця має, як мінімум п'ять стовпців: адреса мережі - мережа або окремий ір-адреса, куди повинен бути доставлений пакет. Маска мережі - щоб однозначно ідентифікувати сіть. Шлюз - для передачі пакетів з різними адресами призначення. Інтерфейс (номер порту) - ініціалізує інтерфейс, з якого буде відправлений пакет. Метрика - число, що характеризує канал зв'язку;

– адаптивна (динамічна) - всі зміни конфігурації мережі автоматично вносяться в таблиці маршрутизаторів протоколами маршрутизації. У таких таблицях є запис ttl маршруту (час життя в секундах). Якщо після закінчення часу існування маршруту не підтверджується протоколом маршрутизації, то він вважається неробочим.

Для маршрутизації в IP-мережах застосовуються протоколи, в яких маршрут вибирається за різними варіантами критеріїв, пов'язаних зі зменшенням часу проходження пакету і якістю маршруту (критерії: найкоротша відстань (кількості маршрутизаторів на шляху пакета - хопів), пропускна здатність каналів між маршрутизаторами, надійність каналів, латентність (затримка (доставки даних) - збільшує час відгуку)).

Основою протоколу маршрутизації є алгоритми маршрутизації, які застосовуються для визначення найкращого шляху пакетів від відправника до отримувача (рис.3.4).

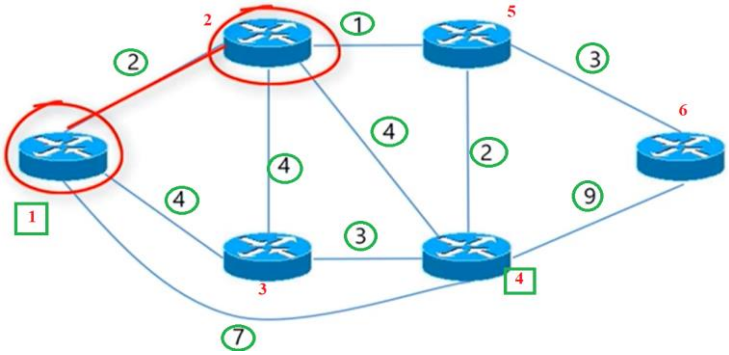

Рисунок 3.4 – Граф мережі

Для подання роботи алгоритмів маршрутизації мережа представляється графом. Вузлами графа є маршрутизатори, а ребрами - фізичні лінії зв'язку між ними. Кожній грані відповідає певне число - вартість, що залежить від довжини лінії зв'язку, швидкості передачі даних або фінансової вартості лінії.

Протокол маршрутизації формує в маршрутизаторах узгоджені один з одним таблиці маршрутизації, які забезпечують доставку пакета від вихідної мережі в мережу призначення за кінцеве число кроків. Таблиця може бути статична, або динамічна.

Який шлях оптимальний - визначається метрикою - умовна вартість передачі по мережі. Повна вартість маршруту дорівнює сумі метрик мереж, по маршруту. Маршрутизатор вибирає маршрут з найменшою метрикою.

Алгоритми маршрутизації діляться на 2 групи:

– дистанційно-векторні алгоритми (distance vector). Кожен маршрутизатор періодично широкомовно розсилає по мережі вектор відстаней від себе до всіх відомих йому мереж. Дистанційно-векторні алгоритми добре працюють тільки в невеликих мережах. Приклад - протокол RIP;

– алгоритми стану зв'язків (link state) забезпечують кожен маршрутизатор інформацією для побудови точного графа зв'язків мережі. Всі маршрутизатори працюють на підставі одного й того ж графа. Приклад - протокол OSPF.

Протокол RIP (routing information protocol) - протокол маршрутної інформації. Алгоритм роботи протоколу:

– крок 1 - створення мінімальної таблиці. У початковому стані в кожному маршрутизаторе програмним забезпеченням стека TCP / IP автоматично створюється мінімальна таблиця маршрутизації, в якій враховуються тільки безпосередньо приєднані мережі;

– крок 2 - розсилка мінімальної таблиці сусідам. Після ініціалізації кожен маршрутизатор починає посилати своїм сусідам повідомлення протоколу RIP, в яких міститься його мінімальна таблиця;

– крок 3 - отримання RIP-повідомлень від сусідів і обробка отриманої інформації. Після отримання повідомлень від сусідів маршрутизатор нарощує кожне отримане поле метрики на одиницю і запам'ятовує, через який порт і від якого маршрутизатора отримана нова інформація. Потім маршрутизатор порівнює нову інформацію з тієї, яка зберігається в таблиці маршрутизації;

– крок 4 - розсилка нової таблиці сусідам. Далі - до кроку 3.

Щоб отримувати попередження - маршрут недійсний, RIP використовує два механізми:

– закінчення TTL маршруту. У протоколі RIP період розсилки - 30 секунд, а TTL маршруту - 180 секунд;

– вказівка нескінченного відстані до недоступної мережі. В RIP нескінченним умовно вважається відстань 16 хопов.

Протокол OSPF (open shortest path first) - вибір найкоротшого шляху першим. Алгоритм роботи протоколу:

– крок 1 - кожен маршрутизатор будує граф зв'язків мережі, в якому вершинами є маршрутизатори і IP-мережі, а ребрами -

інтерфейси маршрутизаторів. Всі маршрутизатори обмінюються зі своїми сусідами тією інформацією про графа мережі, якою вони володіють до даного моменту. Повідомлення, за допомогою яких поширюється топологічна інформація, називаються оголошеннями про стан зв'язків мережі (link state advertisements, LSA);

– крок 2 - знаходження оптимальних маршрутів за допомогою отриманого графа. Завдання вирішується за допомогою алгоритму Дейкстри. Алгоритм Дейкстри обчислює найкоротший шлях між двома точками в мережі, використовуючи граф за методом вузлів і кордонів. При цьому кожен маршрутизатор вважає себе центром мережі і шукає оптимальний маршрут до кожної відомої йому мережі.

Всі протоколи маршрутизації можна розділити на дві великі групи: зовнішні (EGP - Exterior Gateway Protocol) і внутрішні (IGP - Interior Gateway Protocol). Щоб пояснити відмінності між ними - потрібно термін "автономна система".

Маршрутизація Інтернет функціонує в межах автономних систем. АС (домен маршрутизації) - сукупність мереж (група маршрутизаторів) під єдиним адміністративним керуванням, що забезпечує загальну політику маршрутизації.

Автономні системи з'єднуються зовнішніми шлюзами. Реєстрація АС відбувається централізовано.

Номер АС - 16 розрядів (65535). Інтернет - набір взаємопов'язаних АС, що забезпечує багаторівневий підхід до маршрутизації: маршрут визначається як послідовність АС, потім - як послідовність мереж, а потім - веде до кінцевого вузла.

АС може належати до наступних категорій: обмежена (stub) AS; многоінтерфейсная (multihomed) AS; транзитна (transit) AS.

Загальна топологія Internet складається з транзитних, многоінтерфейсних і обмежених автономних систем.

Протокол граничної маршрутизації (BGP - Border Gateway Protocol) - це протокол маршрутизації між автономними системами. Він заснований на методах маршрутизації, які називаються "маршрутизація вектором шляху".

Маршрутизація з використанням вектору шляхів відрізняється і від маршрутизації з використанням вектору довжини маршруту, і від маршрутизації станом лінії. Кожен вхід в таблицю маршрутизації містить мережу пункту призначення, наступний маршрутизатор і шлях до пункту призначення. Шлях зазвичай визначається як впорядкований

список автономної системи, який повинен пройти пакет для досягнення пункту призначення.

Автономний граничний маршрутизатор - бере участь в маршрутизації з використанням вектору шляхів, сповіщає про досяжності мереж в їх власній автономній системі для сусідніх автономних прикордонних маршрутизаторів. Концепція оточення тут та ж сама, як у вже розглянутих протоколах RIP і OSPF.

Граничний маршрутизатор автономної системи отримує свою інформацію від внутрішнього алгоритму маршрутизації, такого як RIP і OSPF. Кожен маршрутизатор, який отримує вектор шляху, перевіряє, що запропонований шлях узгоджений з його політикою. Якщо політика маршрутизації відповідає записаної в програмі, маршрутизатор оновлює таблиці маршрутизації і модифікує повідомлення, перш ніж послати його до наступного сусідові.

Маршрутизатор взаємодіє з іншими маршрутизаторами по протоколу BGP тільки в тому випадку, якщо адміністратор явно вказує, що ці маршрутизатори є його сусідами.

Таким чином, адміністратор може вирішувати, з якими автономними системами він буде обмінюватися трафіком, а з якими ні. Одночасно протоколи RIP і OSPF обмінюються маршрутною інформацією з усіма маршрутизаторами, що знаходяться в межах їх безпосередньої досяжності. BGP відрізняється від RIP або OSPF тим, що BGP використовує TCP в якості транспортного протоколу.

Проектувальнику треба чітко розуміти до якої мережі належить кожний конкретний мережевий адаптер маршрутизатора. Перевірити правильність налаштувань можна відомою вже вам командою (ping).

При цьому важливо звертати увагу не тільки на адреси але й на правильне визначення маски мережі. Переплутані при налаштуванні інтерфейси маршрутизатора, або неправильне визначення маски мережі призводять до неробочого стану мережі, та складнощів при налаштуванні маршрутизації. Зверніть увагу на те, що у таких схемах, при підключенні мережі до маршрутизатора, підключення частіше відбувається за допомогою комутатора. Але є ситуації, коли застосовується пряме підключення маршрутизатора до маршрутизатора.

При такому підключенні та використанні між маршрутизаторами з’єднання serial портів – застосовується поняття clock rate (реальна

швидкість каналу) та розрізняють мережеві адаптери цих двох пристроїв, як пристрої DTE або DCE.

Перевірити таке налаштування можна наведеною командою:

R2#show controllers вказавши ідентифікатор інтерфейса, наприклад serial 0/1/0

При цьому буде надана інформація про статус цього інтерфейсу

Interface Serial0/1/0

Hardware is PowerQUICC MPC860

або DTE V.35 TX і RX clocks detected

(або DCE V.35, clock rate 6400)

idb at 0x81081AC4, driver data structure at 0x81084AC0

швидкість роботи каналу clock rate задаємо (перевіряємо) на пристрої DCE.

4 МЕРЕЖНІ СЛУЖБИ DHCP ТА DNS

4.1 Протокол динамічної конфігурації хостів

Протокол динамічної конфігурації хостів (Dynamic Host Configuration Protocol, DHCP) автоматизує процес конфігурації мережних інтерфейсів, гарантуючи від дублювання адрес за рахунок централізованого управління їх розподілом. DHCP побудований за схемою клієнт сервер, де DHCP-сервер виділяє мережні адреси і доставляє конфігураційні параметри ПК, які динамічно конфігуруються.

Клієнт і сервер можуть погоджувати список необхідних параметрів. ПК не повинна діяти як DHCP-сервер, якщо вона спеціально не налаштована системним адміністратором.

DHCP не може використовуватися для конфігурації маршрутизаторів. Список основних завдань DHCP:

– DHCP є механізм, а не політика і управляється системними адміністраторами, шляхом завдання конфігураційних параметрів;

– клієнти не повинні вимагати ручної конфігурації і повинні читати локальні конфігураційні параметри;

– мережі не вимагають ручної конфігурації для окремих клієнтів. Адміністратор не вводить індивідуальні параметри клієнта;

– DHCP не вимагає окремого сервера для кожної підмережі;

– клієнт DHCP може отримати кілька відгуків на запит конфігураційних параметрів. Для підвищення надійності та швидкодії використовують декілька серверів для перекриття областей мережі;

– DHCP повинен співіснувати з ПК, які сконфігуровані вручну.

DHCP повинен також:

– гарантувати, що будь-яка мережна адреса не буде використовуватися більш ніж одним клієнтом одночасно;

– підтримувати DHCP конфігурацію клієнта при стартовому перезавантаженні DHCP-клієнта - при кожному запиті по мірі можливості, присвоюється один і той же набір конфігураційних параметрів (мережна адреса);

– підтримувати конфігурацію DHCP-клієнта при перезавантаженні сервера (той же набір конфігураційних параметрів);

– дозволяти автоматично отримувати конфігураційні параметри новим клієнтам, щоб уникнути ручної конфігурації;

– підтримувати фіксоване або постійне присвоєння конфігураційних параметрів для заданого клієнта.

Модель DHCP пам'яті характеризується записами ключ-значення для кожного клієнта, де ключ це деякий унікальний ідентифікатор (номер IP-мережі і унікальний ідентифікатор в межах мережі), а значення містить набір конфігураційних параметрів клієнта. Ключ може являти собою пару номер IP-мережі, апаратну адресу.

Повідомлення	**Використання**
DHCPDISCOVER	Клієнт посилає повідомлення широкомовно, щоб виявити доступний сервер
DHCPOFFER	Надсилається сервером клієнтові у відповідь на DHCPDISCOVER і містить пропозицію по конфігураційним параметрам
DHCPREQUEST	Повідомлення клієнта серверу. Робить запит параметрів від одного сервера і відкидає пропозиції інших серверів, підтверджує коректність раніш присвоєної адреси після перезавантаження системи
DHCPACK	Надсилається сервером клієнтові і містить конфігураційні параметри, включаючи присвоєну мережну адресу

DHCPNAK	Надсилається сервером клієнтові, повідомляючи про те, що мережна адреса не коректна (клієнт перемістився в нову підмережу) або час використання адреси клієнтом минув
DHCPDECLINE	Клієнт і сервер виявили, що мережна адреса вже використовується
DHCPRELEASE	Надсилається клієнтом серверу з метою відмови від мережної адреси і анулює час дії адреси
DHCPINFORM	Надсилається клієнтом серверу з проханням про локальні параметри

DHCP може працювати в різних режимах, включаючи:

– ручне призначення статичних адрес - адміністратор, з пулом доступних адрес, постачає DHCP-сервер інформацією про жорстку відповідність IP-адрес фізичним адресам або іншим ідентифікаторам клієнтських вузлів;

– автоматичне призначення статичних адрес - DHCP-сервер самостійно без втручання адміністратора довільним чином вибирає клієнтові IP-адресу з пулу IP-адрес. Адреса дається клієнту з пулу в постійне користування. При наступних запитах сервер повертає клієнтові ту же IP-адресу;

– автоматичний розподіл динамічних адрес - DHCP-сервер видає клієнту адресу та набір конфігураційних параметрів на обмежений час, термін оренди. Коли DHCP-клієнт видаляється з мережі, IP-адреса автоматично звільняється. У всіх режимах роботи адміністратор при конфігуруванні DHCP-сервера повідомляє йому один або декілька діапазонів IP-адрес - все адреси належать до однієї мережі - мають одне і те ж значення в поле номера мережі.

4.2 Централізована служба DNS

Централізована служба DNS (Domain Name System - система доменних імен), заснована на розподіленої базі відображень «доменне ім'я - IP-адреса». DNS являє собою, з одного боку, базу даних, розподілену між ієрархічно структурованими серверами імен, з іншого боку, протокол прикладного рівня, який організовує взаємодію між хостами і серверами імен для виконання операцій перетворення.

Протоколу DNS призначено порт з номером 53 і працює він поверх протоколу UDP транспортного рівня. Основні специфікації DNS містяться в документах RFC 1034 і RFC 1035. Служба DNS використовує в своїй роботі DNS-сервери і DNS-клієнти. DNS-сервери підтримують розподілену базу відображень, а DNS-клієнти звертаються до серверів із запитами про перетворення доменного імені в IP-адресу. DNS має ієрархічну деревоподібну структуру, яка допускає наявність в імені довільної кількості складових частин (рис.4.1).

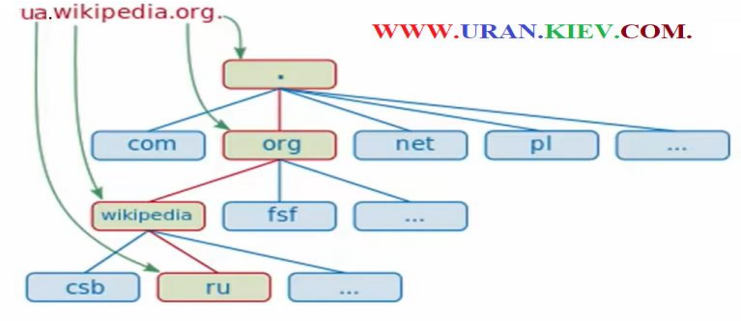

Рисунок 4.1 – Структура DNS

Ієрархія доменних імен аналогічна ієрархії імен файлів, прийнятої в файлових системах. Дерево імен починається з кореня, що позначається крапкою (.). Потім слідує старша символьна частина імені, друга за старшинством символьна частина імені і т.ін.

У доменній системі імен розрізняють короткі імена, відносні імена і повні доменні імена. Коротке ім'я - ім'я кінцевого вузла мережі: хоста або порту маршрутизатора. Коротке ім'я - це лист дерева імен. Відносне ім'я - ім'я, яке починається з деякого рівня ієрархії, але не з самого верхнього. www1.zil - це відносне ім'я. Повне доменне ім'я (Fully Qualified Domain Name, FQDN) включає складові всіх рівнів ієрархії.

Кореневий домен управляється центральними органами Інтернету IANA і InterNIC. Домени верхнього рівня призначаються для кожної країни, а також для різних типів організацій. Імена цих доменів повинні слідувати міжнародному стандарту ISO 3166. Для позначення країн використовуються три або дволітерні абревіатури, наприклад ru (Росія), uk (Велика Британія), fi (Фінляндія), us (США), а для різних

типів організацій: com - комерційні організації (microsoft.com); edu - освітні організації (mit.edu); gov - урядові організації (nsf.gov); org - некомерційні організації (fidonet.org); net - мережеві організації (nsf.net). Кожен домен адмініструє конкретна організація, яка зазвичай розбиває свій домен на піддомени і передає функції адміністрування цих піддоменів іншим організаціям. Процедура дозволу DNS-імені аналогічна процедурі пошуку файлової системою адреси файлу по його символьному імені. Істотною відмінністю файлової системи від служби DNS є те, що перша розташована на одному комп'ютері, а друга є розподіленою. Жоден сервер не знає про весь простір імен. Він знає тільки про імена у домені за який він відповідає. Коли клієнт звертається до сайту (www.udemy.com) - запит відправляється на DNS сервер зазначений у налаштуваннях даного клієнта (рис.4.2).

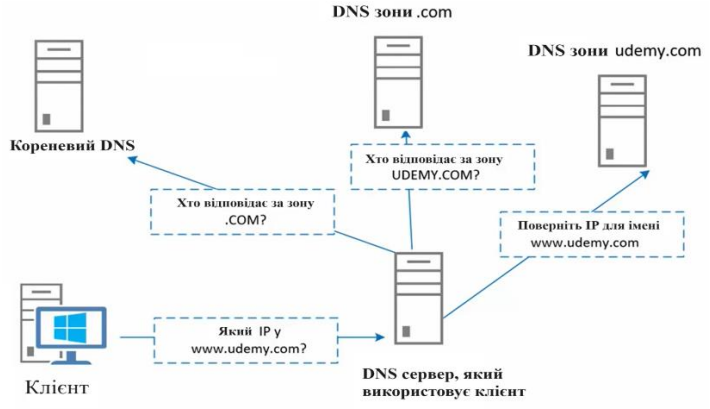

Рисунок 4.2 – Процедура дозволу DNS-імені

Так як цей сервер не обслуговує домен udemy.com, то він не знає яка IP адреса у www. І тому він не може відповісти на цей запит використовуючи власну інформацію, але він може отримати цю інформацію через звернення до інших DNS серверів.

При цьому на кожному DNS сервері є список кореневих DNS серверів (які відповідають за зону з точкою) тому перший запит буде такий «Надай мені інформацію який DNS сервер відповідає за зону .com» (ім'я яке запросив клієнт знаходиться в домені .com).

Отримавши інформацію про імена DNS серверів які обслуговують зону .com, наш сервер звертається до них за інформацію про сервери, які відповідають за домен .udemy.com.

Далі він звертається до серверів, які відповідають за домен .udemy.com. із запитом «Надайте інформацію яка IP адреса у www.udemy.com.». Ці сервера дозволяють даний запис в IP-адресу і пересилають її серверу клієнта, який надає остаточну відповідь.

Існує дві основні схеми дозволу DNS-імен. У першому варіанті роботу з пошуку IP-адреси координує DNS-клієнт. DNS-клієнт звертається до кореневого DNS-сервера із зазначенням повного доменного імені. DNS-сервер відповідає клієнту, вказуючи адресу наступного DNS-сервера, який обслуговує домен верхнього рівня, заданий в наступній старшій частині імені, яке запитується. DNS-клієнт робить запит наступного DNS-сервера, який відсилає його до DNS-сервера потрібного піддомену і т.п., Поки не буде знайдений DNS-сервер, в якому зберігається відповідність імені, яке запитується IP-адресі. Цей сервер і дає остаточну відповідь клієнту.

Така процедура дозволу імені називається нерекурсивною, коли клієнт сам ітеративно виконує послідовність запитів до різних серверів імен. Це завантажує клієнта складною роботою тому застосовується рідко. У другому варіанті реалізується рекурсивна процедура. DNS-клієнт запитує локальний DNS-сервер - сервер, який обслуговує піддомен, якому належить ім'я клієнта. Далі можливі два варіанти дій:

– локальний DNS-сервер знає відповідь і відразу повертає значення клієнту (коли ви запросили ім'я входить в той же піддомен, що і ім'я клієнта або, коли сервер визначав відповідність для іншого клієнта і зберіг його в кеші);

– локальний сервер не знає відповідь і виконує ітеративні запити до кореневого сервера так само, як це робив клієнт в попередньому варіанті, а отримавши відповідь, передає її клієнту, який чекає її від свого локального DNS-сервера.

Записи DNS або ресурсні записи (Resource Records, RR) - одиниці зберігання і передачі інформації в DNS. Кожна запис складається з наступних полів:

– ім'я (NAME) - доменне ім'я, до якого прив'язана або якому «належить» дана ресурсна запис;

– TTL (Time To Live) - допустимий час зберігання даної ресурсної записи в кеші невідповідального DNS-сервера;

– тип (TYPE) ресурсної записи - визначає формат і призначення даної ресурсної записи;

– клас (CLASS) ресурсної записи; теоретично вважається, що DNS може використовуватися не тільки з TCP / IP, але і з іншими типами мереж, код в поле клас визначає тип мережі;

– довжина поля даних (RDLEN);

– поле даних (RDATA) формат і зміст залежать від типу запису;

Найбільш важливі типи DNS-записів:

– запис A (address record) або запис адреси пов'язує ім'я хоста з IP-адресою. Наприклад, запит A-записи на ім'я referrals.icann.org поверне його IP адресу - 192.0.34.164;

– запис AAAA (IPv6 address record) пов'язує ім'я хоста з адресою протоколу IPv6. Наприклад, запит AAAA-запису на ім'я K.ROOT-SERVERS.NET поверне його IPv6 адресу - 2001: 7fd :: 1;

– запис CNAME (canonical name record) або канонічний запис імені (псевдонім) використовується для перенаправлення на інше ім'я;

– запис MX (mail exchange) або поштовий обмінник вказує сервер (и) обміну поштою для даного домену;

– запис NS (name server) вказує на DNS-сервер для домену;

– запис SOA (Start of Authority) або початковий запис зони вказує, на якому сервері зберігається еталонна інформація про домен, містить контактну інформацію особи, відповідальної за дану зону;

– запис PTR (pointer) або запис покажчика пов'язує IP хоста з його канонічним ім'ям. Запит в домені in-addr.arpa на IP хоста в reverse формі поверне ім'я (FQDN) даного хоста (див. Зворотний DNS-запит). Наприклад для IP адреси 192.0.34.164: запит записи PTR 164.34.0.192.in-addr.arpa поверне його канонічне ім'я referrals.icann.org.

in-addr.arpa

DNS-запис in-addr.arpa виглядає так:

56.34.12.10.in-addr.arpa. IN PTR host1.example.net.

Це означає, що IP-адреса 10.12.34.56 відповідає імені хоста host1.example.net. DNS-запис ip6.arpa виглядає так:

5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa. IN PTR host1.example.net. Це означає, що IPv6-адреса 2001: 0db8 :: 1: 2345 відповідає імені хоста host1.example.net.

4.3 Протоколи дозволу адрес

В мережі, для визначення локальної (фізичної, MAC) адреси за відомою IP-адресою, використовується протокол дозволу адрес (Address Resolution Protocol, ARP). Він реалізується по-різному, в залежності від того, який протокол (чи технологія) локальної мережі (Ethernet, Token Ring, FDDI) використовується.

Коли пакет відправляється на канальний рівень для інкапсуляції в кадрі Ethernet, пристрій звертається до таблиці у своїй пам'яті, щоб знайти MAC-адресу, яка відповідає пристрою із IPv4-адресою. Ця таблиця називається таблицею ARP чи кешем ARP. Таблиця ARP зберігається в оперативній пам'яті пристрою.

Пристрій, який планує почати передачу в мережі, починає шукати у своїй ARP таблиці IPv4-адресу призначення та відповідну MAC-адресу. Якщо IPv4-адреса призначення пакета знаходиться в тій же мережі, що й IPv4-адреса відправника, то пристрій шукає в таблиці ARP IPv4-адресу призначення. Далі наведено простий приклад, коли відправник та отримувач знаходяться в одній логічній мережі (рис.4.3).

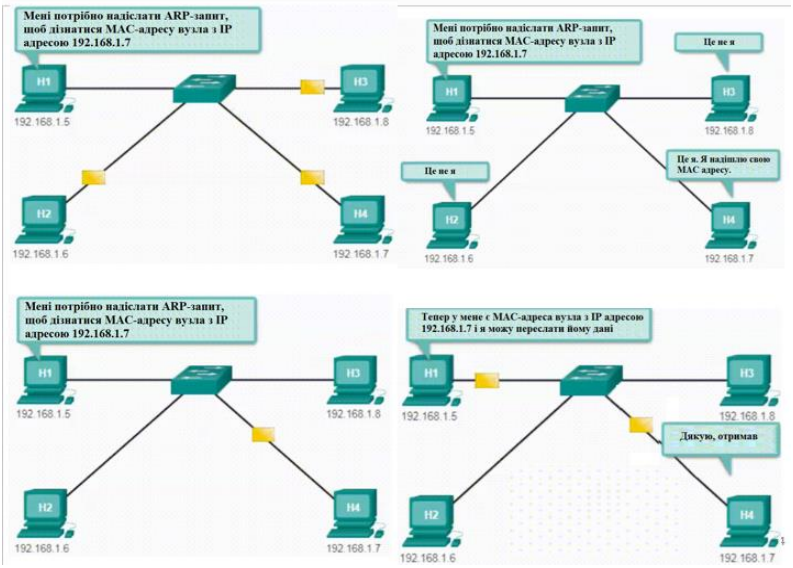

Рисунок 4.3 – Приклад

Відправнику потрібно переслати пакети пристрою із IP-адресою 192.168.1.7 і він починає шукати MAC-адресу цього пристрою. Чому? Для чого? А для того щоб сформувати кадр, бо технології канального рівня не працюють з пакетами, а працюють з кадрами. Тому буде сформовано широкомовний запит та відправлено його всім пристроям мережі. І далі відповість тільки той, який впізнає свій IP-адрес.

Якщо IPv4-адреса призначення пакета знаходиться не в тій же мережі, що IPv4-адреса джерела, пристрій шукає в таблиці ARP IPv4-адресу шлюзу за замовчанням. В обох випадках необхідно знайти IPv4-адресу та відповідну MAC-адресу пристрою.

Для того, щоб зменшити число ARP-звернень в мережі, відповідність між IP-адресою і MAC-адресою зберігається в ARP-таблиці інтерфейсу.

Даний запис в ARP-таблиці з'являється автоматично, через декілька мілісекунд після того, як модуль ARP проаналізує ARP-відповідь. Якщо потрібно надіслати пакет за певною адресою - протокол IP, перш ніж посилати широкомовний запит, перевірить, чи немає вже такої адреси в ARP-таблиці (рис.4.4).

IP-адрес	MAC-адрес	Тип
172.16.10.253	00:1C:C5:34:B3:01	Динамічний
172.16.10.88	1C:75:08:D2:49:45	Статичний

Рисунок 4.4 – ARP-таблиця

ARP-таблиця поповнюється не тільки за рахунок ARP-відповідей, які надходять, а й в результаті отримання інформації із широкомовних ARP-запитів.

У ARP-таблицях існує два типи записів: динамічні і статичні. Статичні записи створюються вручну за допомогою утиліти ARP і не мають терміну старіння, існують, поки комп'ютер або маршрутизатор залишається включеним. Динамічні записи повинні підлягати періодичному оновленню.

Вміст таблиці можна подивитись наведеною командою arp – a – команда для перегляду таблиці.

Утиліта командного рядка ARP.EXE використовується для відображення змін у таблиці перетворення IP-адрес в фізичні (MAC - адреси), які використовуються протоколом дозволу адрес (Address Resolution Protocol - ARP).

ARP -a [inet_addr] [-N if_addr] [-v]

ARP -d inet_addr [if_addr]

ARP -s inet_addr eth_addr [if_addr]

Ключ -a показує поточні ARP-запису, опитуючи поточні дані протоколу. Якщо заданий inet_addr, то будуть відображені IP і фізичні адреси тільки для заданого кінцевого пристрою. Якщо ARP використовує більше одного мережевого інтерфейсу, то будуть відображатися записи для кожної таблиці (рис.4.5).

```
C:\Users\sem>arp -a

Интерфейс: 192.168.0.77 --- 0x3
  адрес в Интернете      Физический адрес      Тип
  192.168.0.1           e0-88-5d-8c-fc-6f     динамический
  192.168.0.10          00-10-95-de-ad-07     динамический
  192.168.0.255         ff-ff-ff-ff-ff-ff     статический
  224.0.0.2             01-00-5e-00-00-02     статический
  224.0.0.22            01-00-5e-00-00-16     статический
  224.0.0.251           01-00-5e-00-00-fb     статический
  224.0.0.252           01-00-5e-00-00-fc     статический
  239.255.255.250       01-00-5e-7f-ff-fa     статический
  255.255.255.255       ff-ff-ff-ff-ff-ff     статический

Интерфейс: 192.168.228.1 --- 0x16
  адрес в Интернете      Физический адрес      Тип
  192.168.228.255       ff-ff-ff-ff-ff-ff     статический
  224.0.0.2             01-00-5e-00-00-02     статический
  224.0.0.22            01-00-5e-00-00-16     статический
  224.0.0.252           01-00-5e-00-00-fc     статический
  239.255.255.250       01-00-5e-7f-ff-fa     статический

Интерфейс: 192.168.145.1 --- 0x17
  адрес в Интернете      Физический адрес      Тип
  192.168.145.255       ff-ff-ff-ff-ff-ff     статический
  224.0.0.2             01-00-5e-00-00-02     статический
  224.0.0.22            01-00-5e-00-00-16     статический
  224.0.0.252           01-00-5e-00-00-fc     статический
  239.255.255.250       01-00-5e-7f-ff-fa     статический

C:\Users\sem>
```

Рисунок 4.5 – ARP-таблиця

inet_addr визначає IP-адресу.

Ключ -N if_addr відображає ARP-записи для заданого в if_addr мережевого інтерфейсу.

Ключ -d видаляє вузол, який задається inet_addr. Параметр inet_addr може містити знак шаблону * для видалення всіх вузлів.

Ключ -s додає вузол і пов`язує адреси в Інтернет та inet_addr с фізичною адресою eth_addr - фізична адреса задається 6 байтами (в шістнадцятковому вигляді), розділених дефісом.

Якщо запис не оновлювався протягом якогось часу - він видаляється з таблиці. У ARP-таблиці містяться записи тільки про ті вузли у мережі, які активно беруть участь в мережевих операціях. Спосіб зберігання записів має назву - кешування, а ARP-таблиці - називають ARP-кешем.

Після додавання запису до таблиці їй надається таймер кешу ARP, який видаляє записи з таблиці ARP, які не використовуються. При цьому якщо запис не використовується перші 2 хвилини, то видаляється, а якщо використовується, то час його життя продовжується ще на 2 хвилини. Цей період може бути різним, залежно від операційної системи пристрою - при цьому максимально - 10 хвилин для Windows і Linux (FreeBSD - 20 хвилин, Cisco IOS - 4 години). Після чого проводиться новий широкомовний ARP-запит.

Головною перевагою протоколу ARP є його простота, яка породжує в собі і головний його недолік - абсолютну незахищеність, тому що протокол не перевіряє справжність пакетів, і, в результаті, можна здійснити заміну записів в ARP-таблиці, вклинившись між відправником та одержувачем.

4.4 Трансляція адрес

NAT (Network Address Translation) забезпечує перетворення приватних адрес в відкриті адреси – у цьому випадку, пристрій з приватною адресою, отримує доступ до ресурсів мережі Інтернет, одночасно вирішуючи питання економії публічних адрес IPv4.

Маршрутизатори NAT мають таку функцію, яка дозволяє їм працювати як апаратний брандмауер у мережі, і вони захищають мережу LAN від будь-якого небажаного та незвичного трафіку, який може завдати шкоди мережі. Таким чином, він діє як фільтр між Інтернетом та приватною LAN і дозволяє проходити в мережу лише дозволеному трафіку.

Для маршрутизатора з підтримкою NAT налаштовують один або декілька відкритих IPv4-адрес - пул адрес NAT. Зовнішні пристрої

сприймають весь трафік, який входить в мережу і виходить з неї, згідно IPv4-адреси з пулу виділених адрес.

Крім того, NAT виконує перетворення номерів портів, тобто маскує номер порту хоста іншим номером порту в пакеті, який буде направлений до пункту призначення. При цьому NAT не тільки зберігає пул загальнодоступних IP-адрес, а й приховує схему адресації вашої мережі. Потім він вносить відповідні записи IP-адреси і номера порту в таблицю NAT.

Алгоритм роботи технології полягає в тому, що коли клієнт в мережі відправляє якийсь запит в Інтернет, маршрутизатор пересилає запит спеціальному пристрою NAT, далі він перетворює адресу відправника в загальнодоступну IP-адресу пристрою перед пересиланням запиту в Інтернет і для подальшого отримання інформації з сервера.

Коли відповідь отримана від зовнішнього джерела, NAT перетворює загальнодоступну IP-адресу в приватну IP-адресу перед самим пересиланням пакету клієнту. Для цього NAT створює зіставлення між парою PrivateSrcIP, PrivateSrcPort і парою PublicSrcIP, PublicSrcPort, щоб знати напевно, як перетворити IP-адресу і номер порту призначення.

Маршрутизатор NAT зазвичай працює на межі тупикової мережі. Тупикова - це мережа, у якій є тільки один шлях до сусідньої мережі, один вхідний і один вихідний маршрут.

Пакети з мережі пересилаються граничному маршрутизатору, який виконує процес NAT перетворення. У NAT - «внутрішня мережа» - це набір мереж, адреси яких транслюються. «Зовнішня мережа» - всі інші мережі.

У NAT є 4 типи адрес:

- внутрішня локальна адреса;
- внутрішня глобальна адреса;
- зовнішня локальна адреса;
- зовнішня глобальна адреса.

При визначенні типу адреси пам'ятаємо, що термінологія застосовується з точки зору пристрою, адреса якого транслюється.

Внутрішня (inside) – це адреса пристрою, яка перетворюється механізмом NAT. Зовнішня (ouside) – це адреса пристрою призначення.

Ще у NAT до адрес використовується поняття локальна або глобальна. Локальна – це будь-яка адреса у внутрішній частині мережі. Глобальна - будь-яка адреса в зовнішній частині мережі.

Існують три механізми перетворення.

1. Статичне перетворення (статичний NAT) - взаємно-однозначна відповідність між локальною і глобальною адресами.

2. Динамічне перетворення (динамічний NAT) – зіставлення (сопоставление) адрес за схемою «багато до багатьох» між локальними і глобальними адресами.

3. Перетворення адреси і номера порту (PAT) - зіставлення адрес за схемою «багато до одного» між локальними та глобальними адресами. Даний метод також називається перевантаженням (NAT з перевантаженням).

Статичне перетворення NAT - використовує відповідність локальних і глобальних адрес за схемою «один в один» - задає цю відповідність адміністратор мережі і вона залишається незмінною.

При динамічному перетворенні NAT – надається пул публічних адрес, які призначаються в порядку черги - схема «багато до багатьох» («першим прийшов - першим обслужили»). Коли внутрішній пристрій запитує доступ до зовнішньої мережі, динамічне перетворення NAT призначає доступний публічний з пулу IPv4-адрес.

Перетворення адреси і номера порту (PAT) - NAT з перевантаженням, ставить у відповідність безліч приватних IPv4-адрес однієї або декільком публічним IPv4-адресам (схема «багато до одного») – Ця схема реалізується, як на великих підприємствах так і в домашніх маршрутизаторах – наприклад, одна адреса для декількох членів сім'ї – забезпечує усім доступ до Інтернет.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Odom, W. CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. 2019.

2. Odom, W. CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press. 2019.

3. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 1. Навчальний посібник. 2020.

4. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 2. Навчальний посібник. 2020.

5. Блозва А.І. Комп'ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька. К.: Компрінт, 2017.

6. Odom, W. Cisco CCENT/CCNA ICND1 100-101. Indianapolis: Cisco Press. 2013.

7. Odom, W. CCNA Routing and Switching ICND2 200-101 Official Cert Guide. Cisco Press. 2013.

8. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. 2nd Edition. USA: Cisco Press, 2015. 578 p.