Навчально-методичне видання

В. М. Базилевич, Д. Б. Мехед, Ю. М. Ткач

КОМП'ЮТЕРНІ МЕРЕЖІ

Протоколи, технології, обладнання

Навчальний посібник

В авторській редакції

Відповідальний за випуск – *Лук'яненко В.В.*

Підписано до друку 15.01.2019 р.
Формат 60х 84/16. Папір офсетний. Друк числовий.
Гарнітура Times New Roman. Обл.-вид. арк. 5,67.
Ум. друк. арк. 6,28. Тираж 300 прим.
Зам. № 559.

Віддруковано з оригінал-макету замовника

Видавець - ФОП Лук'яненко В.В. ТПК «Орхідея»

Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
серія ДК № 3020 від 02.11.2007 р.

16600, Чернігівська обл., м. Ніжин, вул. Небесної сотні, 13 а.
Тел.: 068 815 06 60
E-mail: holdingvv@ gmail.com

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

В. М. Базилевич, Д. Б. Мехед, Ю. М. Ткач

КОМП'ЮТЕРНІ МЕРЕЖІ

Протоколи, технології, обладнання

Навчальний посібник

Ніжин
2018

УДК 004.7

Б17

Рекомендовано до друку вченою радою Чернігівського національного технологічного університету (протокол № 7 від 2 липня 2018 року).

Рецензенти:

С. В. Казмірчук, д-р техн. наук, доцент;

С. В. Зайцев, д-р техн. наук, доцент.

Б-17 Комп'ютерні мережі. Протоколи, технології, обладнання : навч. посіб. для студ. спец. 125 «Кібербезпека» / В. М. Базилевич, Д. Б. Мехед, Ю. М. Ткач.– Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018.– 108 с. : іл.

ISBN 978-617-7609-20-8

У навчальному посібнику висвітлено теоретичні засади та практичні аспекти основ комп'ютерних мереж. Розглянуто базовий функціонал протоколів різних рівнів еталонної моделі OSI. Описано базове мережеве обладнання, фізику передачі сигналу та процес проектування комп'ютерних мереж. Також розглянуті поняття комутації пакетів в мережі та IP-адресації. Висвітлено передавальні середовища, описані переваги та недоліки кожного.

Навчальний посібник призначений для студентів спеціальності кібербезпека та інших технічних спеціальностей вищих навчальних закладів.

УДК 004.7

ISBN 978-617-7609-20-8

Рекомендована та використана література

1. CCNA R&S: Routing and Switching Essentials. URL: https://www.netacad.com/courses/networking/ccna-routing-switching-essentials.

2. OSI model. 2017. URL: https://en.wikipedia.org/wiki/OSI_model.

3. OSI Model Tutorial. 2011. URL: http://www.9tut.com/osi-model-tutorial.

4. RFC Editor. URL: https://www.rfc-editor.org.

5. Баженов В. А., Велигорський П. С. Інформатика. Комп'ютерна техніка. Комп'ютерні технології. Київ: Каравела, 2003. 464 с.

6. Грошев С. В., Коцюбинский А. О. Интернет: Быстро и обо всем: Экспресс- курс. Москва: Технолоджи, 2000. 256 с.

7. Дьяконов В. П. Краткий самоучитель пользователя INTERNET. Москва: СОЛОН-Р, 2011. 336 с.

8. Закер К. Компьютерные сети. Модернизация и поиск несправностей. Санкт-Петербург: БХВ-Петербург, 2012. 1008 с.

9. Комп'ютерні мережі. 2018. URL: http://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6.

10. Кулаков Ю. О., Луцький Г. М. Комп'ютерні мережі. Київ: Юніор, 2013. 395 с.

11. Левин М. Компьютерные сети: Устройство, подключение и использование. Москва: Оверлейн, 2011. 416 с.

12. Немет Э., Снайдер Г., Хейн Т., Уейн Б. Unix и Linux: Руководство системного администратора. 5-е изд. Москва: Вильямс, 2014. 1312 с.

13. Олифер В. Г., Олифер Н. А. Компьютерные сети: Принципы, технологии, протоколы. Санкт-Петербург: Питер, 2016. 958 с.

14. Олифер В. Г., Олифер Н. А. Сетевые операционные системы. Санкт-Петербург: Питер, 2012. 544 с.

15. Основы компьютерных сетей. Тема № 1. Основные сетевые термины и сетевые модели. 2016. Санкт-Петербург: https://habr.com/post/307252/.

16. Таненбаум Э. Компьютерные сети. Санкт-Петербург: Питер, 2012. 960 с.

Рядок / 26 - запозичення 2 біт формує 4 підмережі з підтримкою 62 вузлів в кожній

Рядок / 27 - запозичення 3 біт формує 8 підмереж з підтримкою 30 вузлів в кожній

Рядок / 28 - запозичення 4 біт формує 16 підмереж з підтримкою 14 вузлів в кожній

Рядок / 29 - запозичення 5 біт формує 32 підмереж з підтримкою 6 вузлів в кожній

Рядок / 30 - запозичення 6 біт формує 64 підмереж з підтримкою 2 вузлів в кожній

Для кожного біта, запозиченого в четвертому октеті, доступну кількість підмереж подвоюється зі скороченням числа адрес вузлів на підмережу.

Запитання для самоперевірки:

1. Опишіть базові характеристики протоколу IP.
2. Опишіть принципи розділення мережі на підмережі.
3. Запишіть діапазони локальних IP адрес. Які класи IP адрес Ви знаєте?
4. Що необхідно враховувати при плануванні адресної схеми мережі?

ЗМІСТ

534 вузла. Зверніть увагу, що перші два октету ідентифікують адресу мережевої частини, тоді як останні два октету визначають IP-адресу вузла.

В якості альтернативи, підприємство може виконати поділ на підмережі на кордоні октету / 24. Це дасть можливість підприємству визначити 65 536 підмереж, кожна з яких зможе зв'язати 254 вузли. Кордон октету / 24 дуже популярний при поділі на підмережі, тому що він дозволяє розмістити раціональне число вузлів і формує зручні для використання підмережі на кордоні октету.

Поділ на підмережі з безкласовою адресацією

У раніше наведених прикладах ми використовували біти вузлів із загальних префіксів мережі / 8, / 16 і / 24. Однак підмережа може запозичувати біти з будь-якої позиції біт у вузловий частини для створення інших масок.

Наприклад, адреса мережі / 24 зазвичай розбивається на підмережі за допомогою більш довгих префіксів, запозичуючи біти з четвертого октету. Завдяки цьому адміністратор може гнучко призначати мережеві адреси меншій кількості кінцевих пристроїв.

Довжина префікса	Маска підмережі	Маска підмережі в двійковій системі n - частина мережі; h - частина вузла.	Кількість підмереж	Кількість вузлів
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2

Рис.32 – Безкласові підмережі

Як показано на рисунку 32:

Рядок / 25 - запозичення 1 біта з четвертого октету формує 2 підмережі з підтримкою 126 вузлів в кожній

Кожен інтерфейс маршрутизатора підключається до однієї мережі. IPv4-адрес і маска підмережі, налаштовані на інтерфейсі маршрутизатора, ідентифікують певний широкомовний домен. Треба пам’ятати, що довжина префікса і маска підмережі – це різні способи представлення того самого - мережевої частини адреси.

Для створення IPv4-підмереж ми задіємо один або кілька біт із вузлової частини в ролі біта мережевої частини. Для цього ми розширюємо маску підмережі. Ми запозичуємо біти з вузловий частини адреси і створюємо додаткові біти для мережі. Чим більше запозичених біт із вузлової частини, тим більше підмереж можна створити.

Поділ мереж найпростіше виконати на кордонах октетів / 8, / 16 і / 24. Показана на Рис.31 таблиця визначає довжину цих префіксів, відповідні маски підмережі, біти мережевої й вузлової частин, а також кількість вузлів, які можна підключити в підмережі. Зверніть увагу, що збільшення довжини префікса скорочує кількість вузлів у кожній підмережі.

Довжина префікса	Маска підмережі	Маска підмережі в двійковій системі n - частина мережі; h - частина вузла.	Кількість вузлів
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

Рис.31. Зміна префіксу мережі

Поділ на підмережі на кордоні октетів

Розглянемо наступний приклад, щоб зрозуміти, як використовувати кордони октетів для поділу на підмережі. Припустимо, підприємство обрало приватну адресу 10.0.0.0/8 як адресу внутрішньої мережі. Ця мережева адреса може зв’язати 16 777 214 вузлів у один широкомовний домен. Однак це не кращий варіант.

Підприємство може далі розбити адресу 10.0.0.0/8 на підмережі на кордоні октету / 16. Це дасть можливість підприємству визначити 256 підмереж (тобто 10.0.0.0/16 - 10.255.0.0/16), кожна з яких зможе зв'язати 65

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

WAN - Wide Area Network

LAN - Local Area Network

ITU - International Telecommunication Union

ISO - International Organization for Standardization

IEEE - Institute of Electrical and Electronics Engineers

IAB - Internet Architecture Board

IETF - Internet Engineering Task Force

TIA - Telecommunications Industry Association

EIA - Electronic Industries Alliance

RFC - Request for comments

TCP - Transmission Control Protocol/ Internet Protocol

IP - Internet Protocol

ЕОМ - Електронна обчислювальна машина

ПЗ - Програмне забезпечення

ЕМП - Електромагнітні перешкоди

UTP - Unshielded Twisted Pair

STP - Shielded Twisted Pair

1. СТАНДАРТИЗАЦІЯ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

В епоху становлення комп'ютерних мереж проектувальникам, розробникам та адміністраторам доводилося витрачати чималі зусилля для створення якісного продукту.

Цікавим є той факт, що хронологічно глобальні мережі (WAN) з'явились раніше за локальні, задовольняючи потребу з'єднання комп'ютерів на великих відстанях. У 1969 році в США було розроблено й запущено першу глобальну комп'ютерну мережу під назвою ARPANET. Саме ця мережа стала відправною точкою для створення сучасної найбільшої мережі – Internet. Через те, що проведення нових кабелів на великі відстані коштувало дорого, перші глобальні мереж використовували в ролі передавального середовища вже наявні системи, такі як телефонна мережа. Багато технологічних особливостей передачі інформації також були запозичені з телефонних мереж. Серед нововведень варто відзначити хіба що відмову від комутації каналів, що використовувалась у телефонних мережах. Детальніше про методи комутації буде розглянуто в темі «Комутація та маршрутизація даних у мережі».

Що ж стосується локальних обчислювальних мереж (LAN), то в кожному конкретному випадку доводилось розробляти не лише програмне, але часто й апаратне забезпечення під потреби організації, підприємства тощо. Процес проектування, встановлення та налагодження мережі займав величезну кількість людино-годин та вимагав значних витрат ресурсів. Підтримка та адміністрування мережі переважно виконувалось тією ж організацією або особою, яка встановлювала мережу, що також викликало певні незручності.

Активний розвиток комп'ютерних мереж відбувся у 70-х роках, поштовхом якого стало створення великих інтегральних схем і, як результат, міні-комп'ютерів. Проте масове впровадження стало можливо лише після

мережа знайдена, по вузловій частині адреси можна визначити пристрій призначення.

Однак у міру зростання мережі в багатьох організаціях, коли до мережі підключаються сотні і навіть тисячі вузлів, дворівнева ієрархія стає неефективною.

При поділі мережі на підмережі в ієрархію мережі додається ще один рівень, і фактично створюється ієрархія з трьох рівнів: мережа, підмережа і вузол. При додаванні нового рівня ієрархії в IP-мережі створюються додаткові підгрупи. Це дозволяє прискорити доставку пакетів і забезпечити додаткову фільтрацію, сприяючи скороченню обсягу «локального» трафіку.

Причини для поділу на підмережі

Поділ на підмережі знижує загальний обсяг мережевого трафіку й підвищує продуктивність мережі. Крім того, це дає можливість адміністраторам застосовувати заходи безпеки. Наприклад, визначити підмережі, яким дозволено і яким не дозволено взаємодіяти один з одним.

Існує кілька способів використання підмереж для управління мережевими пристроями. Мережеві адміністратори можуть групувати пристрої в підмережі за такими принципами.

1. Місцезнаходження, наприклад по поверхах будівлі.
2. Підрозділ.
3. Тип пристрою.
4. Будь-який інший значущий для мережі принцип.

Розуміння принципу поділу мережі на підмережі – головний навик, яким повинен володіти кожен мережевий адміністратор. Розроблено різні методи, які допомагають зрозуміти сутність цього процесу. Ми розглянемо двійковий метод. На перший погляд поділ на мережі може здатися складним, але чим більше уваги приділяти деталям і чим більше практикуватися, тим цей процес ставатиме простіше і зрозуміліше.

Межі октетів

Live, TTL) пакета було змінено на 0. Якщо маршрутизатор отримує пакет і змінює значення в поле TTL IPv4-пакета на нуль, він відкидає пакет і відправляє на вузол джерела повідомлення про перевищення інтервалу очікування.

Протокол ICMPv6 також відправляє повідомлення про **перевищення інтервалу очікування**, в разі якщо маршрутизатор не може переслати IPv6-пакет через закінчення його терміну дії. У протоколі IPv6 поле TTL відсутнє; щоб з'ясувати, чи не минув термін дії пакета, використовується поле «межа переходів» (hop limit).

Запитання для самоперевірки:

1. Опишіть загальні принципи IP адресації.
2. Які версії протоколу IP Ви знаєте? Чим вони відрізняються?
3. Чому і коли з'явилась потреба в IPv6?
4. Які типи адрес Ви знаєте?
5. Опишіть відмінності групової та широкомовної адреси.
6. Для чого використовується маска підмережі.
7. У чому різниця локальних та глобальних IP адрес.

11.4 Поділ IP-мереж на підмережі

Проектування, впровадження й управління ефективним планом IP-адресації забезпечують надійність і ефективність роботи мереж. Це особливо актуально у випадках, коли збільшується кількість вузлів мережі. Розуміння ієрархічної структури IP-адреси і того, як змінити ієрархію для підвищення ефективності маршрутизації, є важливою частиною планування схеми IP-адресації.

У вихідній IPv4-адресі існує два рівні ієрархії: мережа і вузол. Ці два рівні адресації дають можливість створювати базові групування в мережі, які полегшують маршрутизацію пакетів у мережу призначення. Маршрутизатор пересилає пакети на підставі мережної частини IP-адреси. Після того, як

створення стандартів мережевих технологій, що були прийняті в середині 80-х років, зокрема: Arcnet, Token Ring, Token Bus та Ethernet.

Перед початком детального розгляду комп'ютерних мереж хотілося б зосередити увагу читача на одному з найважливіших аспектів, а саме на стандартизації. Справа в тому, що комп'ютерна мережа за своєю сутністю є способом з'єднання різноманітних пристроїв (вузлів мережі) в єдине ціле, тому проблема сумісності тут виникає сама собою. Стандарти в комп'ютерних мережах проявляються в різних аспектах: специфікації, класифікації, документації, стеки, відкрита система та ін. У цій темі будуть розглянуті деякі важливі поняття, а також джерела стандартів.

Стандартизація – це процес впровадження та розроблення технічних стандартів на основі консенсусу різних сторін, що включають підприємства, користувачів, організації стандартів та уряди.

Стандартизація може допомогти максимізувати сумісність, безпеку, повторюваність та якість.

Основними організаціями, які розробляють та сприяють впровадженню стандартів у галузі комп'ютерних мереж, є:

1. Міжнародний телекомунікаційний союз (**ITU** – International Telecommunication Union). Стандарти ITU поділяються на серії. Стандарти кожної серії присвячені одній тематиці й позначаються великою літерою латинського алфавіту. Після літери ставиться крапка і номер стандарту. Так, наприклад, літерою V позначаються стандарти щодо передавання даних телефонними каналами, літерою X – стандарти щодо мереж передавання даних, літерою Q – стандарти щодо телефонної комутації та сигналізації.

2. Технічний комітет **ISO** – комітет міжнародної організації зі стандартизації (ISO – International Standard Organization). Технічний комітет розробляє стандарти щодо опрацювання інформації за допомогою ЕОМ. Стандарти цієї організації позначаються чотиризначним числом та суфіксом ISO. Так, наприклад, стандарт, який стосується протокольного стеку TCP/IP, має позначення 7498 ISO

3. Інститут інженерів з електротехніки та електроніки (**IEEE**) – міжнародна організація інженерів у галузі електротехніки, радіоелектроніки

та радіоелектронної промисловості. Світовий лідер у галузі розроблення стандартів з електроніки та електротехніки, зокрема й комп'ютерних мереж.

4. Комісія з питань діяльності Internet (**IAB** – Internet Activities Board) – розробляє стандарти щодо діяльності Internet.

5. **EIA** (Electronic Industries Alliance) – Альянс галузей електронної промисловості. Розташована у США професійна організація, яка розробляє електричні та функціональні стандарти з ідентифікатором RS (Recommended Standards).

До жовтня 1997 р. називалася Electronic Industries Association.

EIA припинила свою діяльність 11 лютого 2011 року, але в колишніх секторах продовжують обслуговування стандартів.

6. The Telecommunications Industry Association (**TIA**) – це акредитована американським національним інститутом стандартів (ANSI) для розробки добровільних, консенсусних галузевих стандартів для широкого кола продуктів інформаційно-комунікаційних технологій (ІКТ), і нині налічує близько 400 компаній. У відділі стандартів і технології TIA діє дванадцять інженерних комітетів, які розробляють керівні принципи для приватного радіообладнання, стільникових веж, терміналів даних, супутників, термінального обладнання телефону, пристроїв VoIP, структурованих кабелів, центрів обробки даних, комунікацій мобільних пристроїв тощо.

Дотримання стандартів, які розроблені цими організаціями, обов'язкове під час проектування, створення та експлуатації будь-яких комп'ютерних мереж. Ці організації, звісно ж, не охоплюють весь діапазон стандартів, проте є найбільш важливими. Крім спеціальних міжнародних організацій, свої стандарти також можуть розробляти та впроваджувати окремі фірми, уряди країн тощо. Наприклад, в Україні діє державний стандарт ДСТУ 4708:2006 «Інформаційні технології. З'єднувачі інтерфейсу зв'язку, використовувані в локальних обчислювальних мережах».

Окремої згадки заслуговує організація **IETF** (Internet Engineering Task Force) – відкрите міжнародне співтовариство проектувальників, учених, мережевих операторів і провайдерів, що займається розробкою **RFC** (Request

Використовуються такі ICMP-повідомлення (однакові для ICMPv4 і ICMPv6).

– Підтвердження вузла.
– Вузол призначення або сервіс недоступні.
– Перевищено інтервал очікування.
– Переадресація маршруту.

Підтвердження вузла

Запит по протоколу ICMP можна використовувати, щоб визначити, чи функціонує вузол. Локальний вузол відправляє вузлу запит ICMP. Якщо вузол доступний, вузол призначення відправляє відповідь. Таке використання exo-запитів по протоколу ICMP лягло в основу утиліти ping.

Вузол призначення або сервіс недоступні

Коли вузол або шлюз отримує пакет, який не може доставити, він може використовувати ICMP-повідомлення «Вузол призначення недоступний» (Destination Unreachable), щоб повідомити джерела про те, що вузол призначення або сервіс для цього пакета недоступні. Таке повідомлення містить код, який визначає причину, через яку пакет не може бути доставлений.

Приклади деяких кодів повідомлень про недоступному вузлі призначення для ICMPv4:

0 – мережа недоступна.

1 – вузол недоступний.

2 – протокол недоступний.

3 – порт недоступний.

Примітка. Протокол ICMPv6 має практично такі ж коди повідомлень по недоступному вузлу призначення.

Перевищено інтервал очікування

Повідомлення ICMPv4 про перевищення інтервалу очікування (Time Exceeded) використовується маршрутизатором для вказівки на те, що пакет неможливо переслати, оскільки значення в полі «Час існування» (Time to

відмінності. Унікальні локальні адреси використовуються для локальної адресації в межах вузла або між обмеженою кількістю вузлів. Ці адреси не слід маршрутизувати в глобальному протоколі IPv6 і перетворювати в глобальні IPv6-адреси. Унікальні локальні адреси знаходяться в діапазоні від FC00 :: / 7 до FDFF :: 7.

У випадку з IPv4 приватні адреси об'єднані з перетворенням мережевих портів і адрес (NAT / PAT) для забезпечення перетворення адрес із приватних в публічні. Це пов’язано з обмеженим адресним простором IPv4. Багато сайтів використовують приватні адреси RFC 1918, щоб забезпечити безпеку або захистити мережу від потенційних загроз. Однак забезпечення безпеки ніколи не було метою технологій NAT / PAT, тому організація IETF завжди рекомендувала приймати відповідні запобіжні заходи при використанні маршрутизаторів в Інтернеті. Унікальні локальні адреси можуть використовуватися для пристроїв, яким ніколи не знадобиться використання інших мереж або отримання з них даних.

Повідомлення ICMPv4 і ICMPv6

Хоча протокол IP не дає гарантію доставки, набір протоколів TCP / IP забезпечує відправку повідомлень навіть в разі виникнення будь-яких помилок. Ці повідомлення відправляються за допомогою ICMP-сервісів. Призначення таких повідомлень - надавати зворотний зв'язок про проблеми, пов'язані з обробкою IP-пакетів у певних умовах, а не підвищувати надійність протоколу IP. З міркувань безпеки повідомлення ICMP не обов’язкові і часто навіть не дозволені в мережі.

ICMP може використовуватися як з IPv4, так і з IPv6. ICMPv4 - це протокол обміну повідомленнями для IPv4. Протокол ICMPv6 надає ті ж послуги для IPv6, але при цьому включає в себе додаткові функціональні можливості.

Існує безліч типів ICMP-повідомлень і причин їх відправки. Розглянемо деякі найбільш поширені повідомлення.

for comments) – набором документації, що містить технічні специфікації та стандарти.

Основні визначення

У процесі вивчення курсу будемо часто стикатись з новими термінами та поняттями. Нижче наведені лише деякі з них, які нам знадобляться вже зараз.

Канал – пристрій або програма, що передає дані між двома й більше вузлами.

Вузол мережі – пристрій або програма, здатна передавати або приймати дані від інших вузлів, користуючись каналом.

Мережа – сукупність вузлів мережі, зв‘язаних між собою каналами.

Протокол – набір правил, що визначають спосіб передачі даних по каналу.

Адреса – унікальний ідентифікатор вузла мережі.

Інтерфейс – пристрій або програма, що з’єднує вузол і мережу.

Інші визначення і поняття будуть розглянуті у відповідних темах.

Запитання для самоперевірки:

1. Що таке мережа? Класифікація комп’ютерних мереж.
2. Що ви знаєте про стандартизацію в комп’ютерних мережах.
3. Які організації займаються стандартизацією?
4. Що викликало необхідність створення стандартів у комп’ютерних мережах?

2. ТОПОЛОГІЇ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Під **топологією** (компонуванням, конфігурацією, структурою) комп'ютерної мережі зазвичай розуміється фізичне розташування комп'ютерів мережі один до одного та спосіб з'єднання їх лініями зв'язку.

Важливо відзначити, що поняття топології ставиться, насамперед, до локальних мереж, у яких структуру зв'язків можна легко простежити. У глобальних мережах структура зв'язків здебільшого схована від користувачів та не є занадто важливою, тому що кожний сеанс зв'язку може виконуватися по своєму власному шляху.

Топологія визначає вимоги до устаткування, тип використовуваного кабелю, можливі й найбільш зручні методи керування обміном, надійність роботи, можливості розширення мережі.

Існує три базових топології мережі:

- шина (bus), при якій усі комп'ютери паралельно підключаються до однієї лінії зв'язку й інформація від кожного комп'ютера одночасно передається всім іншим комп'ютерам (рис. 1.1);

- зірка (star), при якій до одного центрального комп'ютера приєднуються інші периферійні комп'ютери, причому кожний із них використовує свою окрему лінію зв'язку (рис. 1.2);

- кільце (ring), при якій кожний комп'ютер передає інформацію завжди тільки одному комп'ютеру, наступному в ланцюгу, а одержує інформацію тільки від попереднього комп'ютера в ланцюгу, і цей ланцюг замкнений у «кільце» (рис. 1.3).

Діапазон довжини префікса може становити від 0 до 128. Традиційна довжина IPv6-префікса для локальних (LAN) та інших типів мереж – / 64. Це означає, що довжина префікса, або мережева частина адреси, становить 64 біта, а 64 біта що залишилися використовуються для ідентифікатора інтерфейсу (вузлової частини) адреси.

Індивідуальні IPv6-адреси

Індивідуальна адреса служить для однозначного визначення інтерфейсу пристрою під керуванням протоколу IPv6. Пакет, який відправляється на таку адресу, буде отримано інтерфейсом, призначеним для цієї адреси. Як і у випадку з протоколом IPv4, IPv6-адреса має бути індивідуальною. IPv6-адреса призначення може бути як індивідуальною, так і груповою.

Найбільш поширеними типами індивідуальних IPv6-адрес є глобальні індивідуальні адреси (global unicast addresses, GUA) і локальні адреси каналу.

Глобальна індивідуальна адреса

Глобальна індивідуальна адреса аналогічна публічній IPv4-адресі. Ці адреси, до яких можна прокласти маршрут по Інтернету, є унікальними по всьому світу. Глобальні індивідуальні адреси можуть бути налаштовані статично або привласнені динамічно.

Локальна адреса каналу

Локальні адреси каналу використовуються для обміну даними з іншими пристроями по одному локальному каналу. У протоколі IPv6 термін «канал» означає підмережу. Локальні адреси каналів обмежені одним каналом. Вони повинні бути унікальні тільки в межах цього каналу, оскільки поза каналу до них не можна прокласти маршрут. Іншими словами, маршрутизатори не зможуть пересилати пакети, маючи локальну адресу каналу джерела або призначення.

Унікальна локальна адреса

Іншим типом індивідуальної адреси є унікальна локальна індивідуальна адреса. Унікальні локальні IPv6-адреси мають деякі спільні особливості з приватними адресами RFC 1918 для IPv4, але при цьому між ними є й істотні

Неправильна адреса:

2001: 0DB8 :: ABCD :: 1 234

Можливі розшифровки адрес, неоднозначно записаних в стислому форматі:

2001: 0DB8 :: ABCD: 0000: 0000: 1234

2001: 0DB8 :: ABCD: 0000: 0000: 0000: +1234

2001: 0DB8: 0000: ABCD :: тисячу двісті тридцять чотири

2001: 0DB8: 0000: 0000: ABCD :: 1234

Існує три типи IPv6-адрес.

Індивідуальний (або одноадресні розсилки, unicast): служить для однозначного визначення інтерфейсу на пристрої під управлінням протоколу IPv6.

Груповий (або під LGPL, multicast): використовується для відправки одного IPv6-пакета на кілька адрес призначення.

Довільний (або довільна розсилка, anycast): будь-яка індивідуальна IPv6-адреса, яка може бути призначена декільком пристроям. Пакет, що відправляється на адресу довільної розсилки, направляється до найближчого пристрою до цієї адреси.

На відміну від IPv4, IPv6 не використовує широкомовну адресу. Однак є групова IPv6-адреса для всіх вузлів, що дає аналогічний результат.

Довжина префікса IPv6-адреси

Як ви пам'ятаєте, префікс, або мережева частина адреси IPv4, може бути позначений маскою підмережі в десятковому форматі з розділовими точками або довжиною префікса (запис із похилою рискою). Наприклад, IPv4-адрес 192.168.1.10 з маскою підмережі в десятковому форматі з розділовими точками 255.255.255.0 еквівалентний запису 192.168.1.10/24.

Протокол IPv6 використовує довжину префікса для позначення префіксної частина адреси. IPv6 не використовує для маски підмережі десяткове подання з розділовими точками. Довжина префікса позначає мережну частину IPv6-адреси за допомогою адреси або довжини префікса IPv6.

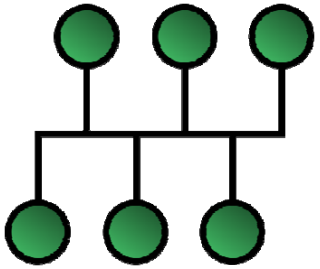

Рис.1. Мережева топологія «шина»

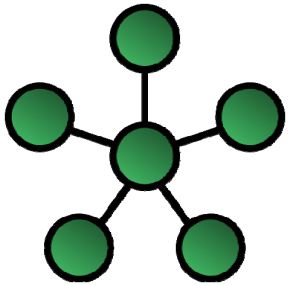

Рис.2. Мережева топологія «зірка»

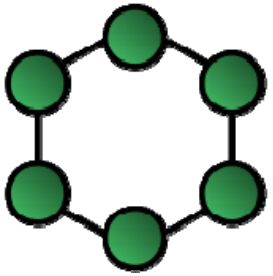

Рис.3. Мережева топологія «кільце»

На практиці нерідко використовують і комбінації базових топологій, але більшість мереж орієнтовані саме на ці три. Розглянемо тепер коротко особливості перерахованих мережних топологій.

Топологія «шина» самою своєю структурою припускає ідентичність мережного устаткування комп'ютерів, а також рівноправність усіх абонентів.

При такому з'єднанні комп'ютери можуть передавати тільки по черзі, тому що лінія зв'язку єдина. Інакше передана інформація буде спотворюватися в результаті накладення (конфлікту, колізії). Таким чином, у «шині» реалізується режим напівдуплексного (half duplex) обміну (в обох напрямках, але по черзі, а не одночасно).

У топології «шина» відсутній центральний абонент, через який передається вся інформація, що збільшує її надійність (адже в разі відмови будь-якого центру перестає функціонувати вся керована цим центром система). Додавання нових абонентів у «шину» досить просте й зазвичай можливе навіть під час роботи мережі. Здебільшого при використанні «шини» потрібна мінімальна кількість сполучного кабелю в порівнянні з іншими топологіями. Однак треба врахувати, що до кожного комп'ютера (крім двох кінцевих) підведено два кабелі, що не завжди зручно.

Оскільки розв'язок можливих конфліктів у цьому випадку лягає на мережеве устаткування кожного окремого абонента, апаратура мережевого адаптера при топології «шина» виходить складнішою, ніж при інших топологіях. Проте через широке поширення мереж із топологією «шина» (Ethernet, Arcnet) вартість мережевого устаткування виходить невисокою.

«Шині» не страшні відмови окремих комп'ютерів, тому що всі інші комп'ютери мережі можуть нормально продовжувати обмін. Може здатися, що «шині» не страшний і обрив кабелю, оскільки в цьому випадку ми одержимо дві цілком працездатні шини. Проте при розриві або ушкодженні кабелю порушується узгодження лінії зв'язку, і припиняється обмін навіть між тими комп'ютерами, які залишилися з'єднаними між собою. Коротке замикання в будь-якій точці кабелю шини виводить із ладу всю мережу. Будь-яку відмову мережного устаткування в «шині» дуже важко локалізувати, тому що всі адаптери включені паралельно, і зрозуміти, який із них вийшов із ладу, не є тривіальним завданням.

При проходженні по лінії зв'язку мережі з топологією «шина» інформаційні сигнали послабляються і ніяким чином не відновлюються, що

Переважний формат

Як показано на Рис.30, кращий формат запису IPv6-адреси: x: x: x: x: x: x: x: x, де кожен «x» складається з чотирьох шістнадцятирічних цифр. Октети – це термін, який використовується для позначення 8 біт IPv4-адреси. В IPv6-адреси сегмент з 16 біт або чотирьох шістнадцятирічних цифр неофіційно називають гекстетом. Кожен «x» – це 1 гекстет, 16 біт або 4 шістнадцяткові цифри.

Переважний формат означає, що IPv6-адреса записана за допомогою 32 шістнадцяткових цифр. Тим не менш, це не найоптимальніший спосіб представлення IPv6-адреси. Нижче наведено два правила, які допоможуть скоротити кількість цифр, необхідних для подання IPv6-адреси.

Правило 1. Пропуск початкових нулів

Перше правило для скорочення запису IPv6-адрес - пропуск усіх початкових 0 (нулів) в шістнадцятковій запису. наприклад:

01AB можна представити як 1AB

09F0 можна представити як 9F0

0A00 можна представити як A00

00AB можна представити як AB

Це правило застосовується тільки до початкових нулів, але НЕ до кінцевих, інакше адреса буде незрозумілою. Наприклад, гекстет «ABC» може бути представлений як «0ABC», або як «ABC0» (а це різні значення).

Правило 2. Пропуск всіх нульових сегментів

Друге правило для скорочення запису адрес IPv6 полягає в тому, що подвійна двокрапка (: :) може замінити будь-який єдиний, суміжний рядок одного або декількох 16-бітних сегментів (гекстетов), що складаються з нулів.

Подвійна двокрапка (: :) може використовуватися в адресі лише один раз, в іншому випадку в результаті може виникнути декілька адрес. Поєднання цього правила з методом пропуску нулів допомагає значно скоротити запис IPv6-адреси. Зазвичай це називається стиснутим форматом.

Подвійний стек: подвійний стек дозволяє протоколам IPv4 і IPv6 співіснувати в тому ж самому сегменті мережі. Пристрої з подвійним стеком одночасно працюють із протокольними стеками IPv4 і IPv6.

Тунелювання: це спосіб передачі пакета IPv6 через IPv4-мережу. IPv6-пакет інкапсулюється всередині IPv4-пакета, як і інші типи даних.

Перетворення: перетворення мережевих адрес 64 (NAT64) дозволяє пристроям під керуванням IPv6 обмінюватися даними з пристроями під керуванням IPv4 за допомогою методу перетворення, схожого на метод перетворення NAT для IPv4. IPv6-пакет перетворюється в пакет IPv4-пакет і навпаки.

Примітка. Тунелювання і перетворення використовуються тільки за необхідності. Кінцева мета – це природний обмін даними у форматі IPv6 між джерелом і призначенням.

Представлення IPv6-адрес

Довжина IPv6-адрес становить 128 біт, написаних у вигляді рядка шістнадцятирічних значень. Кожні 4 біта представлені однією шістнадцятковою цифрою, причому загальна кількість шістнадцяткових значень дорівнює 32. IPv6-адреси не чутливі до регістру, їх можна записувати як малими, так і великими літерами.

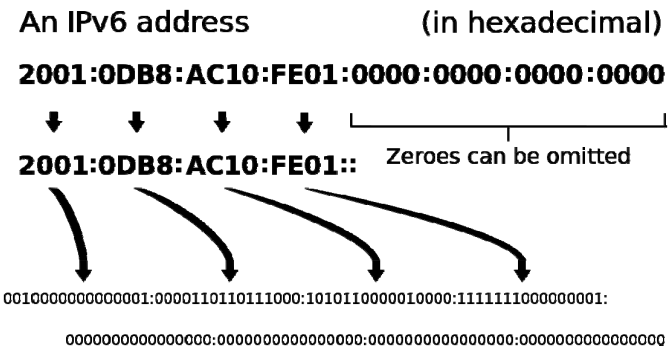

Рис.30. Структура IPv6 адреси

накладає тверді обмеження на сумарну довжину ліній зв'язку, крім того, кожний абонент може одержувати з мережі сигнали різного рівня залежно від відстані до передавального абонента. Це висуває додаткові вимоги до прийомних вузлів мережного устаткування. Для збільшення довжини мережі з топологією «шина» часто використовують кілька сегментів (кожний з яких являє собою шину), з'єднаних між собою за допомогою спеціальних підсилювачів сигналів – репітерів.

Однак таке нарощування довжини мережі не може тривати нескінченно, тому що існують ще й обмеження, пов'язані з кінцевою швидкістю поширення сигналів по лініях зв'язку.

Топологія «зірка» – це топологія з чітко виділеним центром, до якого підключаються всі інші абоненти. Весь обмін інформацією йде винятково через центральний комп'ютер, на який у такий спосіб лягає набагато більше навантаження. Зрозуміло, що мережеве устаткування центрального абонента повинне бути істотно більш складним, ніж устаткування периферійних абонентів. Про рівноправність абонентів у цьому випадку говорити не доводиться. Як правило, саме центральний комп'ютер є самим потужним, і саме на нього покладають усі функції з керування обміном. Ніякі конфлікти в мережі з топологією «зірка» фактично неможливі, тому що керування повністю централізоване, конфліктувати нема чому.

Якщо говорити про стійкість «зірки» до відмов комп'ютерів, то вихід із ладу периферійного комп'ютера ніяк не відбивається на функціонуванні частини мережі, що залишилася, проте будь-яка відмова центрального комп'ютера робить мережу повністю непрацездатною. Тому повинні прийматися спеціальні заходи щодо підвищення надійності центрального комп'ютера і його мережевої апаратури. Обрив будь-якого кабелю або коротке замикання в ньому при топології «зірка» порушує обмін тільки з одним комп'ютером, а всі інші комп'ютери можуть нормально продовжувати роботу.

На відміну від «шини», у «зірці» на кожній лінії зв'язку перебувають тільки два абоненти: центральний і один із периферійних. Найчастіше для їхнього з'єднання використовується дві лінії зв'язку, кожна з яких передає інформацію тільки в одному напрямку. Таким чином, на кожній лінії зв'язку є тільки один приймач і один передавач. Проблема загасання сигналів у лінії зв'язку також вирішується в «зірці» простіше, ніж у «шині», адже кожний приймач завжди одержує сигнал одного рівня. Серйозний недолік топології «зірка» полягає в жорсткому обмеженні кількості абонентів. Зазвичай центральний абонент може обслуговувати не більше 8-16 периферійних абонентів. Якщо в цих межах підключення нових абонентів досить просто, то при їхньому перевищенні воно просто неможливо. Іноді в «зірці» передбачається можливість нарощування, тобто підключення замість одного з периферійних абонентів ще одного центрального абонента (у результаті виходить топологія з декількох з'єднаних між собою «зірок»).

Велика **перевага «зірки»** полягає в тому, що всі точки підключення зібрані в одному місці. Це дає змогу легко контролювати роботу мережі, локалізувати несправності мережі шляхом простого відключення від центру тих або інших абонентів (що неможливо, наприклад, у випадку «шини»), а також обмежувати доступ сторонніх осіб. Загальним недоліком для всіх топологій типу «зірка» є значно більша, ніж при інших топологіях, витрата кабелю. Наприклад, якщо комп'ютери розташовані в одну лінію, то при виборі топології «зірка» знадобиться в кілька разів більше кабелю, ніж при топології «шина». Це може істотно вплинути на вартість усієї мережі загалом.

Топологія «кільце» – це топологія, у якій кожний комп'ютер з'єднаний лініями зв'язку тільки з двома іншими: від одного він тільки одержує інформацію, а іншому тільки передає. На кожній лінії зв'язку, як і у випадку «зірки», працює тільки один передавач і один приймач. Важлива особливість кільця полягає в тому, що кожний комп'ютер ретранслює (відновлює) сигнал, тобто виступає в ролі репітера, тому загасання сигналу в усьому кільці не має

темпам розвитку. У чотирьох з п'яти регіональних інтернет-реєстраторів (RIR) не залишилося вільних IPv4-адрес:

1. Північна Америка (ARIN): адреси IPv4 вичерпались в липні 2015 року.
2. Південна Америка (LACNIC): адреси IPv4 вичерпались у червні 2014 року.
3. Євразія (RIPE NCC): адреси IPv4 вичерпались у вересні 2012 року.
4. Австралія (APNIC): адреси IPv4 вичерпались у квітні 2011 року.
5. Африка (AfriNIC): адреси IPv4 орієнтовано закінчаться у 2019 році.

Теоретичне максимальну кількість IPv4-адрес – 4,3 мільярда. Приватні адреси разом із механізмом перетворення мережевих адрес (NAT) дозволяли якийсь час уповільнити процес виснаження адресного простору IPv4. Однак механізм перетворення мережевих адрес (NAT) має певні обмеження, які погіршують комунікації в тимчасовій мережі.

Всеохоплюючий Інтернет

Сучасний Інтернет істотно відрізняється від Інтернету останніх десятиліть. Сьогодні це не просто електронна пошта, веб-сторінки і передача файлів між комп'ютерами. У міру розвитку Інтернет стає Інтернетом речей. Скоро можна буде отримати доступ до Інтернету не тільки через комп'ютери, планшети і смартфони. Завтра практично всі пристрої – від автомобілів і біомедичного обладнання до побутової техніки та природної екосистеми – будуть оснащені сенсорами і підключені до Інтернету.

У зв'язку з поширенням Інтернету обмеженим адресним простором IPv4, проблемами з перетворенням мережевих адрес і проникненням Інтернету в наше життя прийшло час для переходу на протокол IPv6.

Спільне використання протоколів IPv4 та IPv6

Точної дати для переходу на протокол IPv6 немає. У найближчому майбутньому протоколи IPv4 і IPv6 будуть існувати спільно. Повний перехід може зайняти багато років. Фахівці IETF створили різні протоколи й інструменти, які дозволяють мережевим адміністраторам поступово переводити свої мережі на протокол IPv6. Методи переходу можна поділити на 3 категорії.

Шлюз за замовчуванням – локальний шлюз (тобто IPv4-адрес інтерфейсу локального маршрутизатора), який використовується для звернення до віддалених мереж.

При призначенні пристрою IPv4-адреси для визначення адреси мережі, до якої належить цей пристрій, використовується маска підмережі. Мережева адреса представляє всі пристрої в одній мережі.

Для ідентифікації мережевий і вузловий частини IPv4-адреси маска підмережі побітово порівнюється з IPv4-адресою зліва направо. Одиниці в масці підмережі визначають мережеву частину, а нулі – вузлову частину. Зверніть увагу, що маска підмережі насправді не містить мережевої або вузлової частини IPv4-адреси; вона лише вказує комп'ютеру, де шукати ці частини в конкретній IPv4-адресі.

Сам процес, який використовується для визначення мережевої і вузловий частин адреси, називається логічною операцією «І» (AND).

11.3 Мережеві адреси IPv6

Протокол IPv6 був розроблений як наступник протоколу IPv4. IPv6 має більший 128-бітовий адресний простір, що досить для 340 ундеціліонів адрес. (Це число 340, за яким 36 нулів.) Однак протокол IPv6 – це не тільки більша кількість адрес. Коли фахівці IETF почали розробку наступника IPv4, вони використовували цю можливість для усунення обмежень протоколу IPv4 і внесення додаткових поліпшень. Серед таких поліпшень – протокол керуючих повідомлень версії 6 (ICMPv6), який включає в себе дозвіл адрес і автоналаштування адрес, що було відсутнє в протоколі ICMP для IPv4 (ICMPv4).

Потреба в IPv6

Скорочення адресного простору протоколу IPv4 – основний стимулюючий чинник для переходу до використання IPv6. У міру того як Африка, Азія й інші регіони планети все більше потребують підключення до мережі Інтернет, залишається все менше IPv4-адрес, щоб відповідати таким

ніякого значення, важливо тільки загасання між сусідніми комп'ютерами кільця. Чітко виділеного центру в цьому випадку немає, всі комп'ютери можуть бути однаковими. Однак досить часто в «кільці» виділяється спеціальний абонент, що управляє обміном або контролює обмін. Безперечно, що наявність такого керуючого абонента знижує надійність мережі, тому що вихід його з ладу одразу ж паралізує весь обмін.

Таким чином, комп'ютери в «кільці» не є повністю рівноправними (на відміну, наприклад, від шинної топології). Одні з них обов'язково одержують інформацію від комп'ютера, що веде передачу в цей момент, раніше, а інші – пізніше. Саме на цій особливості топології й будуються методи керування обміном по мережі, спеціально розраховані на «кільце». У цих методах право на наступну передачу переходить послідовно до наступного по колу комп'ютеру.

Підключення нових абонентів у «кільце» зазвичай зовсім «безболісно», хоча й вимагає обов'язкової зупинки роботи всієї мережі на час підключення. Кільцева топологія зазвичай є найбільш стійкою до перевантажень, вона забезпечує впевнену роботу із найбільш великими потоками переданої по мережі інформації, тому що в ній переважно немає конфліктів (на відміну від «шини»), а також відсутній центральний абонент (на відміну від «зірки»).

Оскільки сигнал у «кільці» проходить через усі комп'ютери мережі, то вихід із ладу хоча б одного з них порушує роботу всієї мережі загалом. Так само будь-який обрив або коротке замикання в кожному з кабелів кільця робить роботу всієї мережі неможливою. Кільце найбільш уразливе до ушкоджень кабелю, тому в цій топології зазвичай передбачають прокладку двох (або більше) паралельних ліній зв'язку, одна з яких перебуває в резерві.

Водночас велика перевага «кільця» полягає в тому, що ретрансляція сигналів кожним абонентом дозволяє істотно збільшити розміри всієї мережі загалом (часом до декількох десятків кілометрів). Кільце щодо цього істотно перевершує будь-які інші топології.

Недоліком «кільця» (у порівнянні із зіркою) можна вважати те, що до кожного комп'ютера мережі необхідно підвести два кабелі.

Іноді топологія «кільце» виконується на основі двох кільцевих ліній зв'язку, що передають інформацію в протилежних напрямках. Мета подібного рішення – збільшення (в ідеалі удвічі) швидкості передачі інформації. До того ж у разі ушкодження одного з кабелів мережа може працювати з іншим кабелем (щоправда, гранична швидкість зменшиться).

Крім трьох розглянутих базових топологій, нерідко застосовується також мережева топологія **«дерево» (tree),** яку можна розглядати як комбінацію декількох «зірок». Як і у випадку «зірки», «дерево» (Рис.4) може бути активним, або справжнім, і пасивним. При активному дереві в центрах об'єднання декількох ліній зв'язку перебувають центральні комп'ютери, а при пасивному – концентратори (хаби).

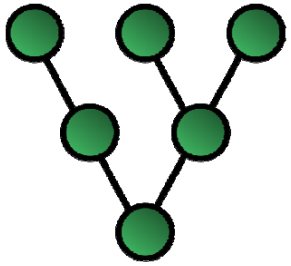

Рис.4. Топологія «дерево»

Застосовуються досить часто й комбіновані топології, наприклад зірково-шинна, зірково-кільцева.

Частковим випадком використання суміші декількох топологій є **«повнов'язна» (fully connected)** (Рис.5).

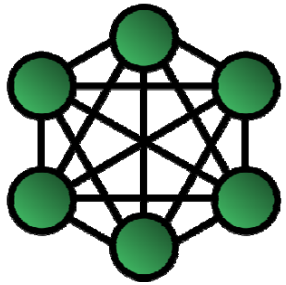

Рис.5. Топологія «повнов'язна»

Біти в мережевій частині адреси повинні бути однаковими в усіх пристроїв, що перебувають в одній мережі. Біти у вузловий частині адреси повинні бути унікальними для кожного вузла в мережі. Якщо два вузла мають одну бітову комбінацію в певній мережевій частини 32-бітного потоку, то ці два вузли перебувають в тій самій мережі.

Але як вузли визначають, яка з частин 32-бітного потоку є мережевою, а яка – вузловою? Для цього використовується маска підмережі.

11.2 Маска підмережі

Як показано на Рис.29, у процесі налаштування IPv4-конфігурації вузла необхідно задати три IPv4-адреси в десятковому форматі з точкою-роздільником.

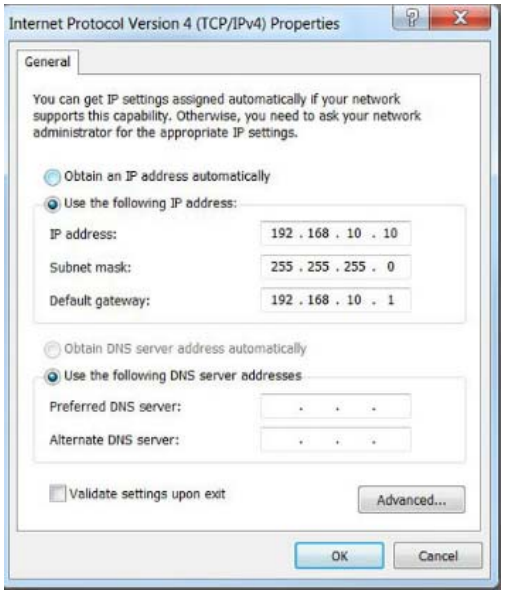

Рис.29. Налаштування IPv4

IPv4-адрес - унікальний IPv4-адрес вузла.

Маска підмережі використовується для визначення мережевої і вузловий частин IPv4-адреси.

11. IP АДРЕСАЦІЯ

Адресація є найважливішою функцією протоколів мережевого рівня. Адресація забезпечує обмін даними між вузлами – незалежно від того, чи перебувають вони в одній мережі або в різних мережах. Протоколи IPv4 iIPv6 здійснюють ієрархічну адресацію пакетів даних.

Проектування, впровадження й управління ефективним планом IP-адресації забезпечують надійність і ефективність роботи мереж.

11.1 Мережеві адреси IPv4

Структура IPv4

Мережева й вузлова частини

Розуміння двійковій системи числення необхідно, щоб встановити, чи перебувають два вузла в тій же самій мережі. IPv4-адреса є ієрархічною адресою, яка складається з двох частин: мережевої і вузлової. Визначаючи ту чи іншу частину, необхідно звертати увагу не на десяткове значення, а на 32-бітний потік. Як показано на рисунку 28, в 32-бітному потоці одна частина бітів визначає мережу, а інша – вузол.

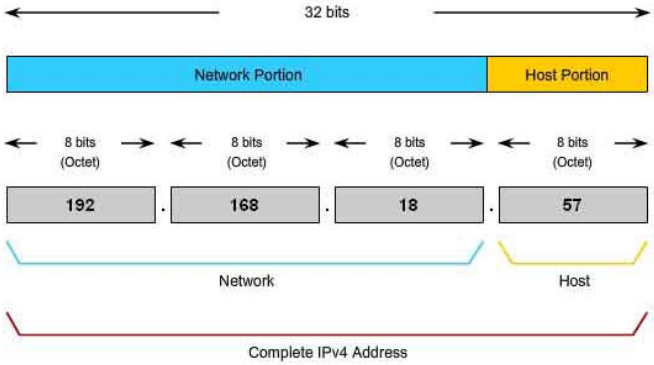

Рис.28. Структура IPv4-адреси

Багатозначність поняття топології

Топологія мережі визначає не тільки фізичне розташування комп'ютерів, але, що набагато важливіше, характер зв'язків між ними, особливості поширення сигналів по мережі. Саме характер зв'язків визначає ступінь відмовостійкості мережі, необхідну складність мережної апаратури, найбільш підходящий метод керування обміном, можливі типи середовищ передачі (каналів зв'язку), припустимий розмір мережі (довжина ліній зв'язку й кількість абонентів), необхідність електричного узгодження й багато чого іншого.

Коли в літературі згадується про топологію мережі, то можуть мати на увазі чотири зовсім різних поняття, що ставляться до різних рівнів мережної архітектури:

1. Фізична топологія (тобто схема розташування комп'ютерів і прокладки кабелів). У цьому змісті, наприклад, пасивна зірка нічим не відрізняється від активної зірки, тому її нерідко називають просто «зіркою».

2. Логічна топологія (тобто структура зв'язків, характер поширення сигналів по мережі). Це, напевно, найбільш правильне визначення топології.

3. Топологія керування обміном (тобто принцип і послідовність передачі права на захват мережі між окремими комп'ютерами).

4. Інформаційна топологія (тобто напрямок потоків інформації, переданої по мережі).

Наприклад, мережа з фізичною й логічною топологією «шина» може як метод керування використовувати естафетну передачу права захвату мережі (тобто бути в цьому змісті кільцем) і одночасно передавати всю інформацію через один виділений комп'ютер (бути в цьому змісті зіркою).

Запитання для самоперевірки:

1. Які топології комп'ютерних мереж ви знаєте?
2. Опишіть переваги та недоліки топології типу «зірка».
3. Опишіть переваги та недоліки топології типу «кільце».
4. Опишіть переваги та недоліки топології типу «дерево».
5. Опишіть переваги та недоліки топології типу «шина».
6. Опишіть переваги та недоліки топології типу «повнов'язна».
7. Що означає багатозначність поняття «топологія»?

3. МОДЕЛЬ OSI. РІВНІ ТА ЇХ ФУНКЦІЇ

Вище вже було розглянуто питання стандартизації та її важливість у проектуванні. Важливою подією з цього погляду було створення еталонної моделі взаємодії відкритих систем – Open System Interconnection (OSI). Наприкінці 70-х років XX ст. уже існувало декілька реалізацій наборів (стеків) протоколів різних фірм. Найбільш популярні з них: DECnet, TCP/IP та IBM SNA. Це призводило до несумісності мережевого обладнання та, як наслідок, до ускладнення процесу проектування. Одним із запропонованих рішень було створити єдиний стек протоколів, який би враховував та виправляв помилки та недоліки своїх «попередників». Цей процес почався зі створення моделі OSI у 1978 році.

Призначення моделі OSI полягає в узагальненому поданні засобів мережевої взаємодії. Вона розроблялася як свого роду універсальна мова мережевих фахівців, саме тому її називають довідкової моделлю.

Модель OSI визначає, по-перше, рівні взаємодії систем у мережах із комутацією пакетів, по-друге, стандартні назви рівнів, по-третє, функції, які повинен виконувати кожен рівень. Модель OSI не містить описів реалізацій конкретного набору протоколів.

У моделі OSI засоби взаємодії діляться на сім рівнів: прикладний, представлення, сеансовий, транспортний, мережевий, канальний і фізичний (Рис.6). Кожен рівень пов’язаний із певним, конкретним аспектом взаємодії мережевих пристроїв.

відправлені дані з прийнятими або визначаючи перевищення нормальної амплітуди сигналу в середовищі передачі даних. Дані, що передаються обома пристроями, будуть пошкоджені, через що буде потрібна їх повторна відправка.

10.2 Конкурентний доступ - CSMA/CA

Іншим видом доступу CSMA, використовуваним у бездротових локальних мережах IEEE 802.11, є множинний доступ із прослуховуванням несучої й уникненням колізій (Carrier Sense Multiple Access / Collision Avoidance; CSMA/CA). При доступі CMSA/CA для контролю звільнення середовища використовується метод, аналогічний CSMA/CD. У CMSA/CA також використовуються додаткові процедури. CMSA/CA не може виявити конфлікти, а намагається уникнути їх, чекаючи своєї черги для передачі. Кожний передавальний пристрій включає в передану інформацію відомості про час, необхідний йому для передачі. Усі інші бездротові пристрої приймають цю інформацію і знають, як довго середовище передачі даних буде зайняте. Після передачі бездротовим пристроєм кадру 802.11 приймач повертає підтвердження, інформуючи відправника про отримання кадру.

Незалежно від виду мережі (або локальна мережа Ethernet з концентраторами, або бездротова локальна мережа), системи з конкурентним доступом погано масштабуються при інтенсивному використанні засобів підключення. Слід зазначити, що в локальних мережах Ethernet з комутаторами конкурентний доступ не використовується, оскільки комутатор і мережева плата вузла працюють у повнодуплексному режимі.

Запитання для самоперевірки:

1. Опишіть відомі Вам методи керування доступом.
2. Опишіть загальний алгоритм конкурентного доступу.
3. Чим відрізняються методи конкурентного доступу CSMA/CD та CSMA/CA?

10.1 Конкурентний доступ - CSMA/CD

Як уже зазначалось, прикладами мереж з конкурентним доступом є бездротові локальні мережі (WLAN), локальні мережі Ethernet із концентраторами й застарілі мережі Ethernet із шинною топологією. Усі ці мережі працюють у напівдуплексному режимі. При цьому необхідний спеціальний протокол, що визначає, коли пристрій може здійснювати передачу, і що відбувається в разі одночасної передачі декількома пристроями.

У напівдуплексних мережах Ethernet використовується протокол множинного доступу з прослуховуванням несучої і виявленням колізій (Carrier Sense Multiple Access / Collision Detection; CSMA/CD).

Протокол CSMA працює за таким алгоритмом:

1. У PC1 є кадр Ethernet, який потрібно передати в PC3.

2. Мережева плата PC1 повинна визначити, чи здійснює хто-небудь передачу по середовищу. Якщо вона не виявляє сигнал несучої, іншими словами, не приймає дані від іншого пристрою, то робить висновок про те, що мережа вільна для передачі.

3. Мережева плата PC1 передає кадр Ethernet.

4. Концентратор Ethernet приймає кадр. Концентратор Ethernet також називають багатопортовим ретранслятором. Він здійснює регенерацію всіх бітів, прийнятих на вхідному порті, і їх розсилку через усі інші порти.

5. Якщо інший пристрій, наприклад PC2, хоче здійснити передачу, але в цей момент приймає кадр, він повинен дочекатися звільнення каналу.

6. Кадр буде доставлений усім пристроям, підключеним до концентратора. Але оскільки в кадрі була вказана адреса призначення цільового каналу даних, що відноситься до PC3, то тільки цей пристрій буде приймати і зберігати весь кадр. Мережеві плати всіх інших пристроїв ігнорують кадр.

Якщо два пристрої виконують передачу одночасно, виникає колізія (конфлікт). Обидва пристрої виявлять колізію в мережі. Це називається виявленням колізій (CD). Мережева плата розпізнає цю колізію, порівнюючи

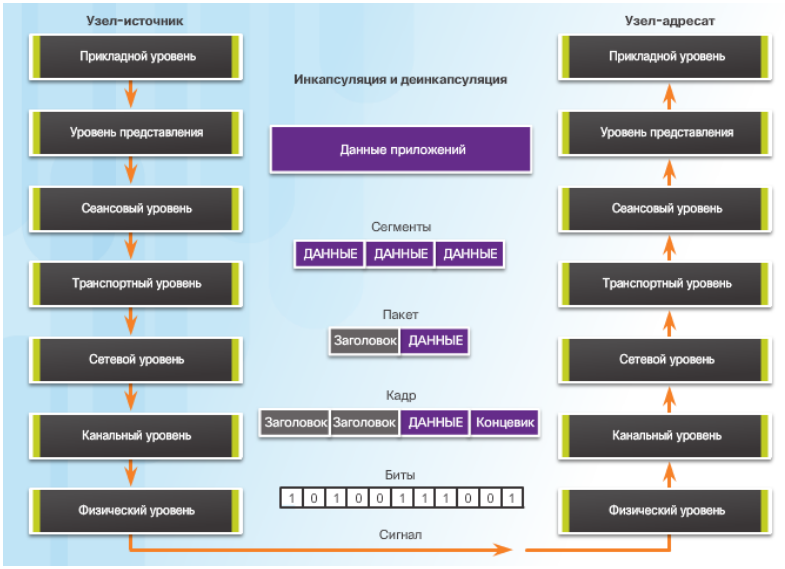

Рис.6. Модель OSI

Процес передачі повідомлень включає в себе додавання службової інформації (заголовку) протоколів на кожному з рівнів. Цей процес називається інкапсуляцією даних. Заголовки використовуються відповідними протоколами вузла-отримувача для коректної обробки повідомлення.

Як уже зазначалось, модель OSI складається із 7 рівнів і кожен рівень виконує певне, конкретне завдання. Коротко розглянемо, що робить кожен рівень, починаючи з найнижчого:

1. Фізичний рівень (Physical Layer): визначає метод передачі даних, яке середовище використовується (передача електричних сигналів, світлових імпульсів або радіоефір), рівень напруги, метод кодування двійкових сигналів.

2. Канальний рівень (Data Link Layer): він бере на себе задачу адресації в межах локальної мережі, виявляє помилки, перевіряє цілісність даних. Саме на цьому рівні «розташовуються» MAC-адреси та «Ethernet», які будуть розглянуті далі.

3. Мережевий рівень (Network Layer): цей рівень бере на себе об'єднання ділянок мережі і вибір оптимального шляху (тобто маршрутизацію). Кожен мережевий пристрій повинен мати унікальну мережеву адресу в мережі. Для цього використовуються протоколи IPv4 та IPv6, що працюють на цьому рівні. Докладніше ці протоколи та адресація в мережі будуть розглянуті у відповідній темі.

4. Транспортний рівень (Transport Layer): цей рівень бере на себе функцію транспорту. Наприклад, коли ви завантажуєте файл з Інтернету, файл у вигляді сегментів відправляється на Ваш комп'ютер. Також тут вводяться поняття портів, які потрібні для вказівки призначення конкретної служби. На цьому рівні працюють протоколи TCP (зі встановленням з'єднання) і UDP (без встановлення з'єднання).

5. Сеансовий рівень (Session Layer): роль цього рівня у встановленні, управлінні та розриві з'єднання між двома хостами. Наприклад, коли відкриваєте сторінку на веб-сервері, то Ви не єдиний відвідувач на ньому. І ось для того, щоб підтримувати сеанси з усіма користувачами, потрібен сеансовий рівень.

6. Рівень представлення (Presentation Layer): цей рівень структурує інформацію в «читабельний» вигляд для прикладного рівня. Наприклад, багато комп'ютерів використовують таблицю кодування ASCII для виведення текстової інформації або формат jpeg для виведення графічного зображення.

7. Прикладний рівень (Application Layer): напевно, це найзрозуміліший для всіх рівень. Саме на ньому працюють звичні для нас додатки – e-mail, браузери по протоколу http, https, ftp та ін.

Важливо також розуміти, що не можна перестрибувати з рівня на рівень (наприклад, з прикладного на канальний, або з фізичного на транспортний). Весь шлях повинен бути пройдений поступово з верхнього на нижній і з нижнього на верхній. Також варто згадати, що на кожному рівні передана інформація називається по-різному.

10. МЕТОДИ УПРАВЛІННЯ ДОСТУПОМ ДО СЕРЕДОВИЩА ПЕРЕДАЧІ

У деяких мережевих топологіях безліч вузлів використовують загальний засіб підключення. Такі мережі називаються мережами з множинним доступом. Прикладами таких мереж є локальні мережі Ethernet і бездротові локальні мережі (WLAN). У будь-який момент може виникнути ситуація, коли кілька пристроїв намагається відправити або отримати дані, використовуючи той же самий засіб підключення.

У деяких мережах із множинним доступом необхідні правила регулювання доступу пристроїв до загальної фізичної середовищі. Існує два основні методи управління доступом до загального середовища.

1. **Конкурентний доступ**: усі вузли, що працюють у напівдуплексному режимі, змагаються за використання середовища, але здійснювати передачу в кожен момент часу може лише один пристрій. Однак є спеціальний протокол, який визначає, що повинно відбуватися в разі одночасної передачі обома пристроями. Прикладами такого типу управління доступом є локальні мережі Ethernet з концентраторами й бездротові локальні мережі (WLAN).
2. **Керований доступ**: кожному вузлу відводиться власний час для використання середовища. Такі детерміновані типи мереж є неефективними через те, що пристрій має чекати своєї черги для доступу до середовища. Прикладами такого типу управління доступом є застарілі мережі Token Ring.

За замовчуванням комутатори Ethernet працюють у повнодуплексному режимі. Це дозволяє комутатору й підключеному до нього в повнодуплексному режимі пристрою здійснювати передачу і прийом одночасно.

частку службової інформації, тому що кожен пакет несе із собою заголовок фіксованої довжини, а кількість пакетів, на які розбиваються повідомлення, буде різко рости при зменшенні розміру пакета. Існує деяка золота середина, що забезпечує максимальну ефективність роботи мережі, однак її важко визначити точно, тому що вона залежить від багатьох факторів, деякі з них до того ж постійно змінюються в процесі роботи мережі. Тому розробники протоколів для мереж із комутацією пакетів вибирають межі, у яких може знаходитися довжина пакета, а точніше його поле даних, тому що заголовок, як правило, має фіксовану довжину. Здебільшого нижня межа поля даних вибирається рівним нулю, що дозволяє передавати службові пакети без даних користувача, а верхня межа не перевищує 4 кілобайт. Додатка при передачі даних намагаються зайняти максимальний розмір поля даних, щоб швидше виконати обмін даними, а невеликі пакети звичайно використовуються для квитанцій про доставку пакета.

Запитання для самоперевірки:

1. Що означає термін комутація?
2. Що означає термін маршрутизація?
3. Опишіть відмінності між комутацією пакетів та каналів.
4. Як відрізняється пропускна здатність при різних методах комутації?

На прикладному, рівні представлення та сеансовому, передана інформація позначається як PDU (Protocol Data Units). Українською, як правило, це звучить як блоки даних.

Інформацію транспортного рівня називають сегментами. Хоча поняття сегменти, може бути застосовано тільки для протоколу TCP. Для протоколу UDP використовується поняття – датаграмма. Але переважно цією відмінністю нехтують. На мережевому рівні передану інформацію називають IP пакети або просто пакети. На канальному рівні – кадри або фрейми (від англійського frame). На фізичному рівні інформація розглядається як біти.

Для наочності розглянемо процес інкапсуляції та деінкапсуляції повідомлення переданого від одного хоста іншому на прикладі передачі листа (Рис.7).

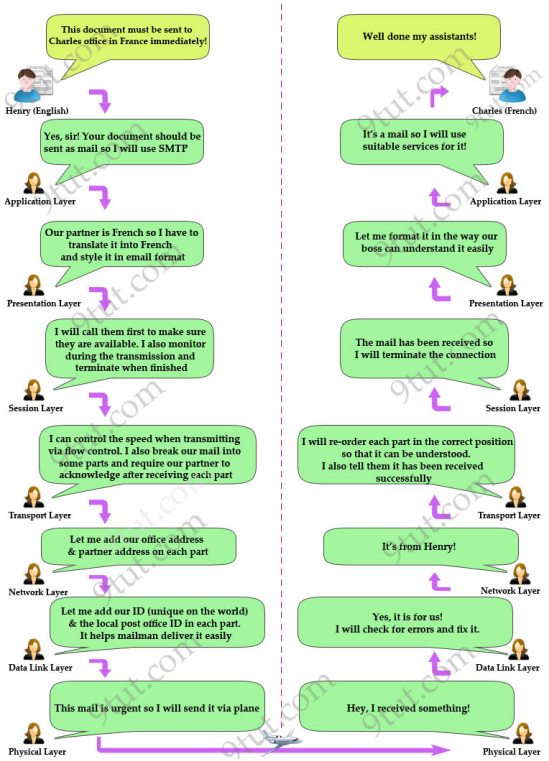

Рис.7. Абстрактний приклад передачі повідомлення в моделі OSI

Запитання для самоперевірки:

1. Опишіть модель взаємодії відкритих систем OSI, її особливості, переваги та недоліки.

2. Назвіть функції протоколів фізичного та канального рівнів. Наведіть приклади.

3. Назвіть функції протоколів мережевого та транспортного рівнів. Наведіть приклади.

4. Назвіть функції протоколів сеансового, представницького та прикладного рівнів. Наведіть приклади.

пропускна здатність мережі при передачі даних між кінцевими вузлами відома – це пропускна здатність каналу. Дані після затримки, пов'язаної зі встановленням каналу, починають передаватися на максимальній для каналу швидкості.

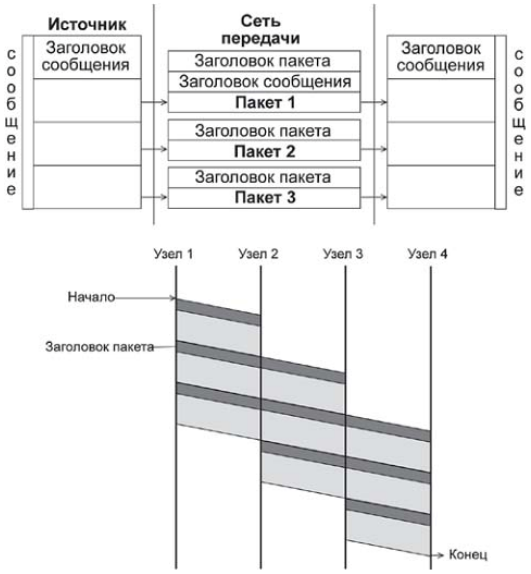

Рис.27. Розділення повідомлення на пакети (комутація пакетів)

Процедура встановлення з'єднання в цих мережах, якщо вона використовується, займає приблизно такий же час, як і в мережах із комутацією каналів, тому будемо порівнювати тільки час передачі даних.

Невизначена пропускна здатність мережі з комутацією пакетів – це плата за її загальну ефективність при деякому обмеженні інтересів окремих абонентів. Аналогічно, у мультипрограмній операційній системі час виконання додатка визначити заздалегідь неможливо, тому що він залежить від кількості інших додатків, з якими поділяє процесор цей додаток.

На ефективність роботи мережі істотно впливають розміри пакетів, що передає мережа. Занадто великі розміри пакетів наближають мережа з комутацією пакетів до мережі з комутацією каналів, тому ефективність мережі при цьому знижується. Занадто маленькі пакети помітно збільшують

інформаційні блоки. Комутатори мережі приймають пакети від кінцевих вузлів і на підставі адресної інформації передають їх один одному, а на при кінці – вузлу призначення.

Комутатори пакетної мережі відрізняються від комутаторів каналів тим, що вони мають внутрішню буферну пам’ять для тимчасового збереження пакетів, якщо вихідний порт комутатора в момент прийняття пакета зайнятий передачею іншого пакета. У цьому випадку пакет перебуває якийсь час у черзі пакетів у буферній пам’яті вихідного порту, а коли до нього дійде черга, то він передається наступному комутатору. Така схема передачі даних дозволяє згладжувати пульсації трафіку на магістральних зв’язках між комутаторами і тим самим використовувати їх найбільш ефективним чином для підвищення пропускної здатності мережі загалом.

Дійсно, для пари абонентів найбільш ефективним було б надання їм в одноособове користування скомутованного каналу зв'язку, як це робиться в мережах із комутацією каналів. При цьому способі час взаємодії цієї пари абонентів був би мінімальним, тому що дані без затримок передавалися б від одного абонента іншому. Простої каналу під час пауз передачі абонентів не цікавлять, для них важливо швидше вирішити свою власну задачу. Мережа з комутацією пакетів сповільнює процес взаємодії конкретної пари абонентів, тому що їхні пакети можуть очікувати в комутаторах, поки по магістральних зв’язках передаються інші пакети, що прийшли в комутатор раніше.

Проте загальний обсяг переданих мережею комп'ютерних даних в одиницю часу при техніці комутації пакетів буде вище, ніж при техніці комутації каналів. Це відбувається тому, що пульсації окремих абонентів відповідно до закону великих чисел розподіляються в часі. Тому комутатори постійно і досить рівномірно завантажені роботою, якщо число абонентів, що обслуговуються ними, дійсно велике.

Пропускна здатність мереж із комутацією пакетів

Однією з відмінностей методу комутації пакетів від методу комутації каналів є невизначеність пропускної здатності з'єднання між двома абонентами. У методі комутації каналів після утворення складеного каналу

4. ФІЗИКА ПЕРЕДАЧІ ДАНИХ

Питання передачі даних на фізичному рівні є базовим для розуміння комп’ютерних мереж, адже включає в себе велику кількість проблем, які можуть виникнути у процесі роботи мережі ще до початку налагодження мережевого обладнання, встановлення програмного забезпечення тощо.

4.1 Кодування

Як відомо, для представлення даних у обчислювальній техніці використовується двійкова система числення (бінарний код). Всередині комп’ютера одиницям та нулям відповідають дискретні сигнали.

Процес перетворення даних у електричні або оптичні сигнали, цей процес називається **кодуванням**.

Існують різні способи кодування, наприклад потенційне кодування, коли одиниці відповідає один рівень напруги, а нулю – інший, або імпульсне кодування, при якому для представлення цифр використовуються імпульси різної полярності.

Аналогічні методи кодування даних використовуються також і в комп’ютерних мережах. Однак ці лінії зв’язку відрізняються за своїми характеристиками від ліній всередині комп'ютера. Головні відмінності зовнішніх ліній зв’язку від внутрішніх виражаються в тому, що їхня протяжність значно більша, а також у тому, що вони проходять поза екрануючого корпусу по просторах, часто під впливом дії сильних електромагнітних перешкод. Усе це призводить до істотно більших розбіжностей прямокутних імпульсів (наприклад, «завалювання» фронтів), ніж усередині комп’ютера. Тому для надійного розпізнавання імпульсів на приймальному кінці лінії зв’язку при передачі даних усередині та за межами комп’ютера не завжди можна використовувати ті ж самі швидкості та способи кодування. Наприклад, повільне нарощування фронту імпульсу через високу ємність навантаження лінії вимагає, щоб імпульси передавалися з меншою швидкістю (щоб передні та задні фронти сусідніх імпульсів не перекривалися й імпульс встиг «збільшитись» до потрібного рівня).

У комп'ютерних мережах застосовуються як потенційне, так і імпульсне кодування дискретних даних (Рис.8), а також специфічний спосіб подання даних, який ніколи не використовується в комп'ютері, – модуляція (рис 1.9). При модуляції дискретна інформація являє собою синусоїдальний сигнал тієї частоти, який ефективно передає наявна лінія зв'язку.

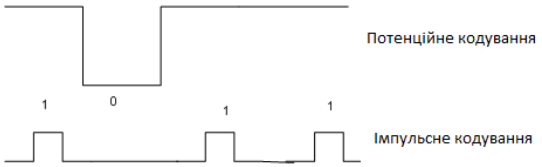

Рис.8. Методи кодування сигналів (потенційний та імпульсний)

Потенційне та імпульсне кодування застосовується на каналах високої якості, але коли канал вносить сильні розбіжності в сигнали, що передаються, переважно застосовується модуляція на основі синусоїдальних сигналів. Наприклад, модуляція використовується в глобальних мережах при передачі даних через аналогові телефонні канали зв'язку, які були розроблені для передачі голосу в аналоговій формі й тому погано підходять для безпосередньої передачі імпульсів.

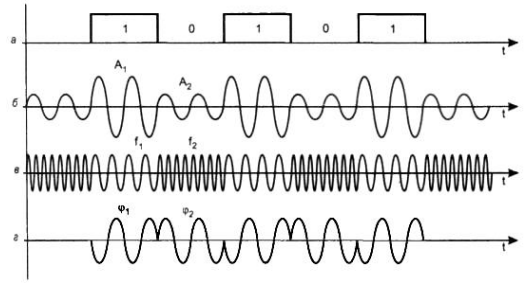

Рис.9. Модуляція сигналу:

а – цифровий код вихідного сигналу; *б* – амплітудна (АМ);

в – частотна (FM); *г* – фазова (РМ)

9. КОМУТАЦІЯ ТА МАРШРУТИЗАЦІЯ ДАНИХ У МЕРЕЖІ

З'єднання кінцевих вузлів у комп'ютерних мережах через вузли-посередники називається **комутацією**.

Комутація є необхідним елементом зв'язку вузлів між собою, що дозволяє скоротити кількість необхідних ліній зв'язку й підвищити завантаження каналів зв'язку. Практично неможливо надати кожній парі вузлів виділену лінію зв'язку, тому в мережах завжди застосовується той або інший спосіб комутації абонентів, що використовує існуючі лінії зв'язку для передачі даних різних вузлів.

Існує два типи комутації: **комутація каналів** (circuit switching) та **комутація пакетів** (packet switching).

Комутація каналів – при комутації каналів комутаційна мережа утворює між кінцевими вузлами безперервний складовою фізичний канал із послідовно з'єднаних комутаторами проміжних канальних ділянок. Умовою того, що кілька фізичних каналів при послідовному з'єднанні утворюють єдиний фізичний канал, є рівність швидкостей передачі даних у кожному зі складових фізичних каналів. Рівність швидкостей означає, що комутатори такої мережі не повинні буферизувати передані дані.

Комутація пакетів – це техніка комутації абонентів, яка була спеціально розроблена для ефективної передачі комп'ютерного трафіка при комутації пакетів всі передані користувачем мережі повідомлення розбиваються у вихідному вузлі на порівняно невеликі частини, які називаються *пакетами*. Повідомлення можуть мати довільну довжину, від декількох байт до багатьох мегабайт. З іншого боку, пакети зазичай теж можуть мати перемінну довжину, але у вузьких межах, наприклад від 46 до 1500 байт. Кожен пакет забезпечується заголовком, у якому вказується адресна інформація, необхідна для доставки пакета вузлу призначення, а також номер пакета, що буде використовуватися вузлом призначення для зборки повідомлення. Пакети транспортуються в мережі як незалежні

процесор. Прикладом мережевого адаптера четвертого покоління може служити адаптер компанії 3Com Fast EtherLink XL 10/100.

Запитання для самоперевірки:

1. Яким чином відбувається відбір даних за MAC адресою?

2. Яким чином відбувається пересилка даних через концентратор?

3. Назвіть основні особливості маршрутизатора? На якому рівні він працює?

4. Опишіть основні функції мережевого адаптера.

4.2 Характеристики фізичних каналів

Основними характеристиками передачі даних є пропускна здатність (bandwidth) і продуктивність (throughput).

Пропускна здатність (bandwidth) – це кількісна характеристика, відображення можливостей передачі даних за конкретним способом зв'язку.

У цифрових мережах під пропускною здатністю розуміється об'єм даних, який можна передавати з однієї точки в іншу за певний час. Зазвичай пропускна здатність вимірюється в кілобітах за секунду (Кбіт/с), мегабітах за секунду (Мбіт/с) або гігабітах за секунду (Гбіт/с). Інколи під пропускною здатністю розуміють швидкість доставки бітів, хоча це не зовсім правильно. Наприклад, як у мережі Ethernet 10 Мбіт/с, так і в мережі Ethernet 100 Мбіт/с біти передаються зі швидкістю розповсюдження електричного сигналу. Різниця полягає в кількості бітів, що передаються за секунду.

Фактична пропускна здатність мережі визначається сукупністю таких факторів:

– властивості фізичних засобів підключення;

– технології передачі та виявлення сигналів у мережі.

На реальну пропускну здатність впливають властивості фізичних засобів зв'язку, використовувані технології та закони фізики.

Продуктивність (throughput) – це кількість бітів, переданих за допомогою засобів зв'язку за певний проміжок часу.

Через велику кількість факторів продуктивність (throughput) зазвичай не відповідає заявленій пропускній здатності (bandwidth) у реалізаціях на фізичному рівні. На продуктивність впливає багато факторів, у тому числі такі:

– об'єм трафіку;

– тип трафіку;

– сумарна затримка, залежно від кількості мережевих пристроїв між джерелом і пунктом призначення;

Затримки в мережі надають вплив на остаточний час, необхідний для доставки даних з однієї точки в іншу.

Виробнича мережа, що складається з декількох мереж або декількох сегментів, не може перевищувати швидкість найповільнішого з'єднання між джерелом і адресатом. Навіть якщо всі або більшість сегментів мають високу пропускну здатність, єдиний сегмент із низькою продуктивністю створює вузьке місце і продуктивність усієї мережі знизиться.

Існує також третій параметр, що характеризує передачу корисних даних, який називається корисною пропускною здатністю (goodput). Корисна пропускна здатність – це обсяг корисних даних, переданих за певний період. Корисна пропускна здатність дорівнює продуктивності (throughput) із вирахуванням службового трафіку, необхідного для створення сеансів, підтверджень та інкапсуляції.

4.3 Симплексний та дуплексний канали передачі

Фізичні канали зв'язку плділяються на кілька типів залежно від того, можуть вони передавати інформацію в обох напрямках чи ні.

Дуплексний (duplex) канал забезпечує одночасну передачу інформації в обох напрямках. Дуплексний канал може складатися з двох фізичних середовищ, кожне з яких використовується для передачі інформації тільки в одному напрямку. Можливий варіант, коли одне середовище служить для одночасної передачі зустрічних потоків, в цьому випадку застосовують додаткові методи виділення кожного потоку із сумарного сигналу.

Напівдуплексний (half-duplex) канал також забезпечує передачу інформації в обох напрямках, але не одночасно, а по черзі. Тобто протягом певного періоду часу інформація передається в одному напрямку, а протягом наступного періоду – у зворотному.

Симплексний (simplex) канал дозволяє передавати інформацію тільки в одному напрямку.

часі. Таким чином, після прийому декількох перших байт кадру починається їхня передача. Це істотно (на 25-55 %) підвищує продуктивність ланцюга оперативна пам'ять – адаптер – фізичний канал – адаптер – оперативна пам'ять. Така схема дуже чутлива до порога початку передачі, тобто до кількості байт кадру, що завантажується в буфер адаптера перед початком передачі в мережу. Мережевий адаптер третього покоління здійснює самонастроювання цього параметра шляхом аналізу робочого середовища, а також методом розрахунку, без участі адміністратора мережі. Самонастроювання забезпечує максимально можливу продуктивність для конкретного сполучення продуктивності внутрішньої шини комп'ютера, його системи переривань і системи прямого доступу до пам'яті.

Адаптери третього покоління базуються на спеціалізованих інтегральних схемах (ASIC), що підвищує продуктивність і надійність адаптера при одночасному зниженні його вартості. Компанія 3Com назвала свою технологію конвеєрною обробкою кадрів Parallel Tasking, інші компанії також реалізували схожі схеми у своїх адаптерах. Підвищення продуктивності каналу «адаптер-пам'ять» дуже важливо для підвищення продуктивності мережі загалом, тому що продуктивність складного маршруту обробки кадрів, що включає, наприклад, концентратори, комутатори, маршрутизатори, глобальні канали зв'язку тощо, завжди визначається продуктивністю самого повільного елемента цього маршруту. Отже, якщо мережевий адаптер сервера або клієнтського комп'ютера працює повільно, ніякі швидкі комутатори не зможуть підвищити швидкість роботи мережі.

Мережеві адаптери, що випускають сьогодні, можна віднести до четвертого покоління. У ці адаптери обов'язково входить ASIC, що виконує функції мас-рівня, а також велика кількість високорівневих функцій. У набір таких функцій може входити підтримка агента вилученого моніторингу RMON, схема пріоритезації кадрів, функції дистанційного керування комп'ютером і т. ін. У серверних варіантах адаптерів майже обов'язкова наявність потужного процесора, що розвантажує центральний

Класифікація мережевих адаптерів

Як приклад класифікації адаптерів, використаємо підхід фірми 3Com, що має репутацію лідера у сфері адаптерів Ethernet. Фірма 3Com вважає, що мережеві адаптери Ethernet пройшли у своєму розвитку три покоління.

Адаптери першого покоління були виконані на дискретних логічних мікросхемах, у результаті чого мали низьку надійність. Вони мали буферну пам'ять тільки на один кадр, що приводило до низької продуктивності адаптера, тому що всі кадри передавалися з комп'ютера в мережу або з мережі в комп’ютер послідовно. Крім цього, завдання конфігурації адаптера першого покоління відбувалося вручну, за допомогою перемичок. Для кожного типу адаптерів використався свій драйвер, причому інтерфейс між драйвером і мережевою операційною системою не був стандартизований.

У мережевих адаптерах другого покоління для підвищення продуктивності стали застосовувати метод багатокадрової буферизації. При цьому наступний кадр завантажується з пам'яті комп'ютера в буфер адаптера одночасно з передачею попереднього кадру в мережу. У режимі прийому, після того як адаптер повністю прийняв один кадр, він може почати передавати цей кадр із буфера на згадку комп’ютера одночасно із прийомом іншого кадру з мережі.

У мережевих адаптерах другого покоління широко використовуються мікросхеми з високим ступенем інтеграції, що підвищує надійність адаптерів. Крім того, драйвери цих адаптерів засновані на стандартних специфікаціях. Адаптери другого покоління зазвичай поставляються з драйверами, що працюють як у стандарті NDIS (специфікація інтерфейсу мережевого драйвера), розробленого фірмами 3Com й Microsoft і схваленого IBM, так й у стандарті ODI (інтерфейс відкритого драйвера), розробленого фірмою Novell.

У мережевих адаптерах третього покоління (до них фірма 3Com відносить свої адаптери сімейства EtherLink III) здійснюється конвеєрна схема обробки кадрів. Вона полягає в тому, що процеси прийому кадру з оперативної пам’яті комп’ютера й передачі його в мережу сполучаються в

Запитання для самоперевірки:

1. Опишіть процес кодування.
2. У чому різниця потенційного та імпульсного кодування?
3. Опишіть основні характеристики фізичних каналів зв’язку.
4. Опишіть відмінності між симплексним та дуплексним каналом.
5. Що означає термін «напівдуплексний канал»?

5. СТЕК ПРОТОКОЛІВ TCP/IP

Конкретна реалізація набору протоколів називається **протокольним стеком**.

Цей набір підтримують усі рівні взаємодії відкритих систем. Найбільш поширений протокольний стек – TCP/IP.

Історія створення протоколів TCP/IP веде свій початок зі створення мережі ARPANET, для якої його було розроблено в 1970-1973 рр. Експеримент із використання TCP/IP у цій мережі закінчився успішно. У результаті стек TCP/IP було здано до промислової експлуатації. Пізніше він адаптувався для використання в ЛОМ. На початку 1980 р. протокол став складовою ОС Berkeley, UNIX v 4.2. Після розпаду ARPANET на Military Net та NSFNET (Internet) у 1983 р. було прийняте рішення про його використання в мережі Internet.

Важливою частиною технології TCP / IP є завдання адресації, до числа яких відносяться наведені нижче.

1. Узгоджене використання адрес різного типу. Це завдання включає відображення адрес різних типів один на одного, наприклад мережевої IP-адреси на локальну, доменного імені – на 1Р-адресу тощо.

2. Забезпечення унікальності адрес. Залежно від типу адреси потрібно забезпечувати однозначність адресації в межах комп'ютера, підмережі, корпоративної мережі або Інтернету.

3. Конфігурація мережевих інтерфейсів і мережевих додатків.

Стек TCP/IP надає користувачам дві основні служби, які використовують прикладні програми.

Дейтаграмний метод доставки пакетів. Це означає, що протоколи стеку визначають маршрут передачі повідомлення, спираючись тільки на адресну інформацію, яка міститься в цьому повідомленні. Доставка відбувається без встановлення логічного з’єднання.

В адаптерах для клієнтських комп’ютерів значна частина роботи перекладається на драйвер, тим самим адаптер виявляється простіше й дешевше. Недоліком такого підходу є високий ступінь завантаження центрального процесора комп’ютера рутинними роботами по передачі кадрів з оперативної пам’яті комп’ютера в мережу. Центральний процесор змушений займатися цією роботою замість виконання прикладних завдань користувача.

Тому адаптери, призначені для серверів, здебільшого забезпечуються власними процесорами, які самостійно виконують більшу частину роботи з передачі кадрів з оперативної пам’яті в мережу й у зворотному напрямку. Прикладом такого адаптера може служити мережевий адаптер SMS Ether Power з вбудованим процесором Intel i960.

Залежно від того, який протокол реалізує адаптер, адаптери діляться на Ethernet-адаптери, Token Ring-адаптери, FDDI-адаптери й т.д. Тому що протокол Fast Ethernet дозволяє за рахунок процедури автопереговорів автоматично вибрати швидкість роботи мережевого адаптера залежно від можливостей концентратора, тому багато адаптерів Ethernet сьогодні підтримують дві швидкості роботи й мають у своїй назві приставку 10/100. Цю властивість деякі виробники називають авточуттєвістю.

Мережевий адаптер перед установкою в комп’ютер необхідно конфігурувати. При конфігуруванні адаптера задаються номер переривання IRQ, використовуваного адаптером, номер каналу прямого доступу до пам’яті DMA (якщо адаптер підтримує режим DMA) і базова адреса портів введення/виведення. Якщо мережний адаптер, апаратури комп’ютера й операційна система підтримують стандарт Plug-and-Play, то конфігурування адаптера і його драйвера здійснюється автоматично. Інакше потрібно спочатку сконфігурувати мережевий адаптер, а потім повторити параметри його конфігурації для драйвера. У загальному випадку, деталі процедури конфігурування мережевого адаптера і його драйвера багато в чому залежать від виробника адаптера, а також від можливостей шини, для якої розроблений адаптер.

й повинне бути згідно з моделлю стека протоколів IEEE 802.x Наприклад, у ОС Windows NT рівень LLC реалізується в модулі NDIS, загальному для всіх драйверів мережевих адаптерів, незалежно від того, яку технологію підтримує драйвер.

Мережевий адаптер разом із драйвером виконують дві операції: передачу й прийом кадру. Передача кадру з комп'ютера в кабель складається з перерахованих нижче етапів (деякі можуть бути відсутні, залежно від прийнятих методів кодування). Прийом кадру даних LLC через міжрівневий інтерфейс разом з адресною інформацією MAC-підрівень. Взаємодія між протоколами всередині комп'ютера відбувається через буфери, розташовані в оперативній пам'яті. Дані для передачі в мережу містяться в цьому буфері протоколами верхніх рівнів, які витягають їх з дискової пам'яті або з файлового кеша за допомогою підсистеми ведення/виведення операційної системи.

Оформлення кадру даних MAC-підрівня, у який інкапсулюються кадр LLC (з відкинутими прапорами 01111110). Заповнення адрес призначення й джерела, обчислення контрольної суми.

Прийом із кабелю сигналів, що кодують бітовий потік.

Виділення сигналів на тлі шуму. Цю операцію можуть виконувати різні спеціалізовані мікросхеми або сигнальні процесори DSP. У результаті в приймачі адаптера утвориться деяка бітова послідовність, яка з великим ступенем імовірності збігається з тієї, що була послана передавачем.

Перевірка контрольної суми кадру. Якщо вона неправильна, то кадр відкидається, а через міжрівневий інтерфейс наверх, протоколу LLC передається відповідний код помилки. Якщо контрольна сума правильна, то з MAC-кадру витягається кадр LLC і передається через міжрівневий інтерфейс наверх, протоколу LLC. Кадр LLC міститься в буфері оперативної пам'яті.

Розподіл обов'язків між мережевим адаптером і його драйвером стандартами не визначається, тому кожен виробник вирішує це питання самостійно. Завичай мережеві адаптери поділяються на адаптери для клієнтських комп'ютерів і адаптери для серверів.

Надійний потоковий транспортний засіб. Більшість прикладних програм потребують від комунікаційного ПЗ автоматичного відновлення при помилках передавання, втраті пакетів або при збоях у проміжних маршрутизаторах. Надійний транспортний засіб дає змогу встановлювати логічне з'єднання між прикладними програмами, після чого відсилати великі об'єми даних через це з'єднання.

Основні переваги стеку протоколів TCP/IP

Незалежність від мережевої технології. TCP/IP не залежить від обладнання, оскільки він визначає елемент передачі – дейтаграму та описує спосіб її руху мережею.

Загальна зв'язаність. Стек дозволяє будь-якій парі комп'ютерів, що його підтримують, взаємодіяти один з одним. Кожному комп'ютеру надається логічна адреса, а кожна дейтаграма, що передається, містить логічні адреси відправника та одержувача.

Підтвердження. Протоколи стеку TCP/IP забезпечують підтвердження правильності проходження при обміні між відправником та одержувачем.

Стандартні прикладні програми. Протокол TCP/IP містить засоби підтримки основних прикладних програм, таких як, електронна пошта, передача файлів, віддалений доступ тощо.

Окремі протоколи реалізовані на різних рівнях відповідно до моделі TCP/IP: на прикладному, транспортному, мережевому рівнях і рівні доступу до мережі. Протоколи TCP/IP працюють на прикладному, транспортному, мережевому рівнях. Протоколи рівня мережевого доступу забезпечують доставку IP-пакетів із фізичного засобу підключення. Ці протоколи нижчих мережевих рівнів розроблені організаціями зі стандартизації.

Набір протоколів TCP/IP реалізований у вигляді стека TCP/IP, який працює як на відправному, так і на приймаючому вузлах для забезпечення наскрізної доставки даних по мережі. Протоколи Ethernet використовуються для передачі IP-пакетів по засобу підключення, використовуваному мережею LAN.

Оскільки стек протоколів TCP/IP було розроблено до появи еталонної моделі OSI, то відповідність його рівнів рівням OSI дуже умовна. В таблиці 1.1 показана структура стеку протоколів TCP/IP і відповідність його рівням OSI.

Таблиця 1 – Взаємозв'язок між моделлю OSI і стеком протоколів TCP/IP

	Рівні моделі OSI	Рівні моделі TCP/IP	Протоколи
7	Прикладний	Рівень I: прикладний	HTTP, FTP, SMTP, DNS, SNMP, POP, DHCP, RPC
6	Представницький		
5	Сеансовий		
4	Транспортний	Рівень II: транспортний	TCP, UDP
3	Мережний	Рівень III: мережевий	IP, ICMP, NAT, IGMP, OSPF
2	Канальний	Рівень IV: мережевого інтерфейсу	ARP, Ethernet, FDDI, Token ring, PPP
1	Фізичний		

Кожен рівень стеку, аналогічно з моделлю OSI, має свої конкретні функції. Реалізуються ці функції через відповідні протоколи.

Найнижчий рівень (*рівень IV*) – рівень мережевого інтерфейсу – відповідає фізичному і канальному рівням моделі OSI. Цей рівень у протоколах TCP/IP не регламентується, але підтримує всі популярні стандарти фізичного й канального рівня: для локальних каналів – це Ethernet, Token Ring, FDDI, для глобальних каналів – власні протоколи роботи на аналогових комутованих і виділених лініях SLIP/PPP, які встановлюють з'єднання типу «точка-точка» через послідовні канали глобальних мереж, і протоколи територіальних мереж X.25 і ISDN. Розроблена також спеціальна специфікація, що визначає використання технології ATM як транспорт канального рівня.

Наступний рівень (*рівень III*) – це рівень міжмережевої взаємодії(мережевий), який займається передачею дейтаграм із використанням різних локальних мереж, територіальних мереж X.25, ліній спеціального зв'язку тощо. Як основний протокол мережевого рівня (в термінах моделі OSI), у стеку використовується протокол IP, який спочатку

Алгоритми маршрутизації можуть працювати в мережах з однорівневою чи ієрархічної архітектурою. В однорівневій мережі її фрагменти мають однаковий пріоритет, що переважно зумовлено схожістю їхнього функціонального призначення. Ієрархічна мережа містить підмережі (фрагменти мережі). Маршрутизатори нижнього рівня служать для зв'язку фрагментів мережі. Маршрутизатори верхнього рівня утворюють особливу частину мережі, звану магістраллю (опорна частина). Маршрутизатори магістральної мережі передають пакети між мережами нижнього рівня.

Ієрархічна структура у великих і складних мережах дозволяє значно спростити процес управління мережею, полегшує ізоляцію сегментів мережі.

Деякі алгоритми маршрутизації діють у межах своїх доменів (внутрішня маршрутизація), інші – як у межах своїх доменів, і у суміжних із ними (міждоменна маршрутизація). У цьому випадку домен означає область маршрутизації, у якому працює один чи кілька протоколів. У різних доменах працюють різні протоколи. Якщо необхідний зв'язок доменів, використовується міждоменна маршрутизація.

Одноадресні алгоритми маршрутизації призначені для передачі конкретної інформації лише одному одержувачу. Багатоадресні (чи групові) алгоритми здатні передавати інформацію багатьом одержувачам одночасно.

Коли маршрутизатор отримує пакет, він зчитує адресу призначення, яка визначає, з якого маршруту відправлено пакет. Зазвичай маршрутизатори зберігають дані про кілька можливих маршрутів.

8.4 Мережеві адаптери

Функції й характеристики мережевих адаптерів

Мережевий адаптер (Network Interface Card, NIC) разом зі своїм драйвером реалізує другий, канальний рівень моделі відкритих систем у кінцевому вузлі мережі – комп'ютері. Більш точно в мережній операційній системі пара адаптер і драйвер виконує тільки функції фізичного й MAC-підрівня, у той час як LLC-рівень зазвичай реалізується модулем операційної системи, єдиним для всіх драйверів і мережевих адаптерів. Властиво так воно

маршрутизатори розсилають повідомлення один одному про зміни в мережі. Після отримання цих повідомлень маршрутизатори роблять повторне призначення оптимальних маршрутів, що може викликати новий потік повідомлень. Цей процес повинен швидко завершуватись, інакше у мережевий топології можуть з’явитися петлі, чи мережа загалом перестане функціонувати.

Алгоритми маршрутизації повинні швидко враховувати зміни у стані мережі (наприклад, відмова вузла чи сегмента мережі, додавання нового обладнання тощо).

Алгоритми маршрутизації можуть бути: статичними чи динамічними; одномаршрутними чи багатомаршрутними; однорівневими чи багаторівневими; внутрішніми чи міждоменними; одноадресними чи груповими.

Для статичних (неадаптивних) алгоритмів маршрути вибираються заздалегідь і заносяться вручну в таблицю маршрутизації, де зберігається інформація про те, на який порт відправити пакет з певною адресою. Протоколи, розроблені з урахуванням статичних алгоритмів, називають немаршрутизованими. Прикладом немаршрутизованих протоколів можуть бути LAT (LocalAreaTransport, транспортний протокол для канальних областей) фірми DEC, протокол підключення термінала та NetBIOS. Зазвичай разом із цими протоколами працюють мости.

З використанням динамічних алгоритмів таблиця маршрутизації автоматично оновлюється відповідно до топології мережі або трафіка в ній. Динамічні алгоритми відрізняються за способом отримання інформації про стан мережі, за часом зміни маршрутів і іншими показниками оцінки маршруту.

Одномаршрутні протоколи визначають лише один маршрут. Він завжди виявляється оптимальним. Багатомаршрутні алгоритми пропонують кілька маршрутів до одержувача. Такі алгоритми дозволяють передавати інформацію по кількох каналах одночасно, що означає підвищення пропускної здатності мережі.

проектувався як протокол передачі пакетів у складених мережах, що складаються з великої кількості локальних мереж, об’єднаних як локальними, так і глобальними зв’язками. Тому протокол IP добре працює в мережах зі складною топологією, раціонально використовуючи наявність у них підсистем і ефективно використовуючи пропускну спроможність низько швидкісних ліній зв’язку. Протокол IP є дейтаграмним протоколом.

До рівня міжмережевої взаємодії відносяться і всі протоколи, пов’язані зі складанням і модифікацією таблиць маршрутизації, такі як протоколи збору маршрутної інформації RIP (Routing Internet Protocol) і OSPF (Open Shortest Path First)а також протокол міжмережевих керівників повідомлень ICMP (Internet Control Message Protocol). Останній протокол призначений для обміну інформацією про помилки між маршрутизатором і шлюзом, системою-джерелом і системою-приймачем, тобто для організації зворотного зв'язку. За допомогою спеціальних пакетів ICMP повідомляється про неможливість доставки пакета, про перевищення часу життя або тривалості збірки пакета з фрагментів, про аномальні величини параметрів, про зміну маршруту пересилки і типу обслуговування, про стан системи і т. ін.

Наступний рівень (рівень II) називається транспортним. На цьому рівні функціонують протокол управління передачею TCP (Transmission Control Protocol) і протокол дейтаграм користувача UDP (User Datagram Protocol). Протокол TCP забезпечує стійке віртуальне з'єднання між видаленими прикладними процесами. Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним методом, тобто без встановлення віртуального з’єднання, і тому вимагає менших накладних витрат, ніж TCP. Він забезпечує з’єднання між двома хостами, при якому не гарантується доставка пакетів.

Верхній рівень (рівень I) називається прикладним. За довгі роки використання в мережах різних країн і організацій стек TCP/IP накопичив велику кількість протоколів і сервісів прикладного рівня. До них відносяться такі широко використовувані протоколи, як протокол копіювання файлів FTP, протокол емуляції терміналу telnet, поштовий протокол SMTP,

використовуваний в електронній пошті мережі Internet і її російської гілки РЕЛКОМ, гіпертекстові сервіси доступу до видаленої інформації, такі як WWW і багато інших. Зупинимося дещо докладніше на деяких з них, найбільш тісно пов’язаних із темою цього курсу.

Протокол SNMP (Simple Network Management Protocol) використовується для організації мережевого управління. Проблема управління поділяється на два завдання. Перше завдання пов’язане з передачею інформації. Протоколи передачі інформації, що управляє, визначають процедуру взаємодії сервера з програмою-клієнтом, що працює на хості адміністратора. Вони визначають формати повідомлень, якими обмінюються клієнти і сервери, а також формати імен і адрес. Друге завдання пов’язане з контрольованими даними. Стандарти регламентують, які дані повинні зберігатися й накопичуватися у шлюзах, імена цих даних і синтаксис цих імен. У стандарті SNMP визначена специфікація інформаційної бази даних управління мережею. Ця специфікація, відома як база даних MIB (Management Information Base), визначає ті елементи даних, які хост або шлюз повинен зберігати, і допустимі операції над ними.

Протокол пересилки файлів FTP (File Transfer Protocol) реалізує віддалений доступ до файлу. Для того, щоб забезпечити надійну передачу, FTP використовує як транспорт протокол із встановленням з’єднань – TCP. Крім пересилки файлів, протокол FTP пропонує й інші послуги. Так користувачу надається можливість інтерактивної роботи з віддаленою машиною, наприклад, він може роздрукувати вміст її каталогів, FTP дозволяє користувачу вказувати тип і формат даних, що запам’ятовуються. Нарешті, FTP виконує аутентифікацію користувачів. Перш ніж дістати доступ до файла, відповідно до протоколу користувачі повинні повідомити своє ім’я і пароль.

У стеку TCP/IP протокол FTP пропонує найбільш широкий набір послуг для роботи з файлами, проте він є і найскладнішим для програмування. Застосування, яким не потрібні всі можливості FTP, можуть використовувати інший, більш економічний протокол – простий протокол пересилки файлів

Визначення маршруту передачі відбувається програмно. Відповідні програмні ресурси носять назви протоколів маршрутизації. Логіка їхньої роботи полягає в алгоритмі маршрутизації, який обчислює вартість доставки й обирають шлях із меншою вартістю. Найпростіші алгоритми маршрутизації визначають маршрут, зважаючи на найменшу кількість проміжних (транзитних) вузлів шляху до адресата. Більш складні алгоритми в поняття «вартість» закладають кілька показників, наприклад, затримку під час передачі пакетів, пропускну спроможність каналів зв'язку і т. ін. Основним результатом роботи алгоритму маршрутизації є створення умов та підтримка таблиці маршрутизації, у якій записується вся маршрутна інформація. Зміст таблиці маршрутизації залежить від використовуваного протоколу маршрутизації. Наприклад, таблиця маршрутизації може містити таку інформацію:

- справжні адреси пристроїв у мережі;
- службову інформацію протоколу маршрутизації;
- адреси найближчих маршрутизаторів.

Основними вимогами, що висуваються до алгоритму маршрутизації є:

- оптимальность вибору маршруту;
- простота реалізації;
- стійкість;
- швидка відповідність;
- гнучкість реалізації.

Оптимальність вибору маршруту є основним параметром алгоритму.

Алгоритми маршрутизації мають бути простими в реалізації й використовувати якнайменше ресурсів.

Алгоритми мають бути стійкими до відмов устаткування, високих навантажень і помилок у фізичному середовищі мережі.

Збіжність – це процес узгодження між маршрутизаторами інформації про топології мережі. Якщо певні події мережі призводять до того, що деякі маршрути стають недоступними чи з’являються нові маршрути,

Маршрутизатор базової мережі складається з таких основних компонентів:

– мережеві адаптери, які з'єднують маршрутизатор через відповідні інтерфейси з локальними і глобальними мережами;

– управляючий процесор, який визначає маршрут і оновлює інформацію про топології;

– основна магістраль, яка після вступу пакета на інтерфейсний модуль аналізує адресу призначення та приймає команди управляючого процесора для визначення вихідного порту. Потім пакет по основний магістралі маршрутизатора передається в інтерфейсний модуль, який слугує для зв'язку із сегментом локальної чи глобальної мережі, на який пакет було адресовано.

У ролі маршрутизатора може виступати також робоча станція чи сервер, що мають кілька мережевих інтерфейсів і забезпечені спеціальним програмним забезпеченням. Маршрутизатори верхнього класу – це, зазвичай, спеціалізовані пристрої, які об'єднують в окремому корпусі безліч маршрутизуючих модулів.

За визначенням, основне призначення маршрутизаторів – це маршрутизація трафіку мережі. Процес маршрутизації можна поділити на два ієрархічно пов'язаних рівні:

1. Рівень маршрутизації. На цьому рівні здійснюється робота з таблицею маршрутизації. Таблиця маршрутизації служить для визначення адреси (мережевого рівня) наступного маршрутизатора чи одержувача за наявною адресою (мережного рівня), після визначення адреси передачі вибирається певний вихідний фізичний порт маршрутизатора. Цей процес називається визначенням маршруту переміщення пакета. Налаштування таблиці маршрутизації ведеться протоколами маршрутизації. Також на цьому рівні визначається перелік необхідних наданих сервісів;

2. Рівень передачі пакетів. Перш ніж передати пакет, необхідно: перевірити контрольну суму заголовка пакета, визначити адресу канального рівня одержувача пакета і зробити безпосередньо відправку пакета з урахуванням черги, фрагментації, фільтрації тощо. Ці дії виконуються виходячи з команд, що надходять з рівня маршрутизації.

TFTP (Trivial File Transfer Protocol). Цей протокол реалізує тільки передачу файлів, причому як транспорт використовує простіший, ніж TCP, протокол без встановлення з'єднання – UDP.

Протокол telnet забезпечує передачу потоку байтів між процесами, а також між процесом і терміналом. Найчастіше цей протокол використовується для емуляції терміналу віддаленої ЕОМ. Детальніше деякі протоколи стеку та їх функції розглянуті в наступних темах.

5.1 Протоколи фізичного та канального рівнів

Протоколи фізичного рівня призначені для сполучення систем із фізичним середовищем. Вони визначають механічні, електричні, функційні, процедурні характеристики, які описують доступ до фізичних сполучень. Фізичне сполучення забезпечує прозорість, тобто передавання довільної послідовності бітів.

Є два типи фізичних сполучень для передавання даних:

Двопунктове (point-to-point connection) – це сполучення між двома станціями, наприклад IrDA (Infrared Data Association).

Багатопунктове (multipoint connection) – між трьома і більше станціями, наприклад Wi-Fi.

До типових функцій (сервісів) протоколів фізичного рівня відносять:

1. Передавання даних.

2. Індикація спотворень під час передавання. Спотворення можуть виникнути, коли дві або більше станцій передають інформацію одночасно.

3. Контроль часу передавання кадру. Виконують для усунення збоїв, спричинених появою необмеженої послідовності бітів. Для цього фізичний рівень перериває передавання, якщо воно триває понад 150 мс.

4. Автоузгодження швидкості передавання. Сервіс автоузгодження швидкості передавання на фізичному рівні дає змогу партнерам зв'язку обмінятися інформацією про технології та швидкості передавання, які вони підтримують, та вибрати прийнятний варіант передавання.

У сучасних локальних мережах архітектуру фізичного рівня поділяють на підрівні, кожен із яких виконує визначений набір функцій. Наприклад, для мережі побудованої за стандартом 10 Gigabit Ethernet є такі підрівні та інтерфейси (Рис.10):

Інтерфейс 10GMII (10G Media Independent Interface) – стандартний інтерфейс між канальним та фізичним рівнем, який унезалежнює реалізацію обох рівнів.

PCS (Physical Coding Sublayer) – виконує кодування та декодування.

PMA (Physical Medium Attachment) – приєднує до фізичного середовища, перетворює паралельне передавання у послідовне та навпаки, забезпечує синхронізацію передавання.

PMD (Physical Medium Dependent) – передає сигнали у фізичному середовищі, відповідає за характеристики сигналів (такі як амплітуда, частота, форма імпульсів, тощо), виконує підсилення та модуляцію сигналів.

MDI (Media Dependent Interface) – інтерфейс, залежний від середовища, визначає конектори для приєднання до фізичного середовища та їхні характеристики.

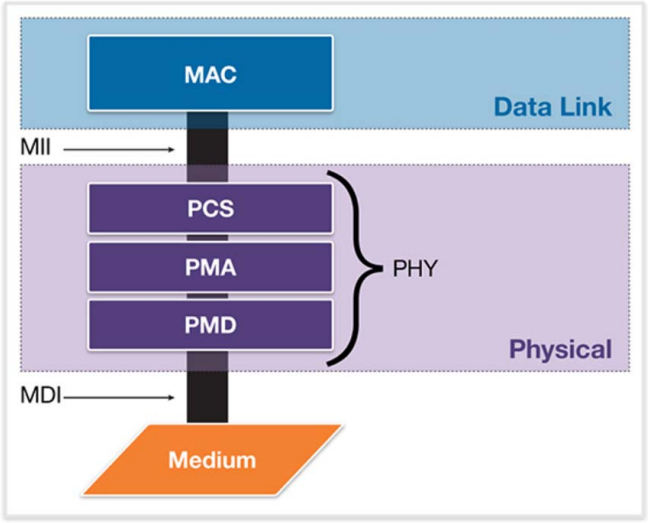

Рис.10. Архітектура протоколів фізичного та канального рівнів

Буферизація спільно використовуваної пам'яті

При буферизації спільно використовуваної пам’яті всі кадри поміщаються в буфер, який є загальним для всіх портів комутатора. Обсяг буферної пам’яті, який потрібно кожному порту, виділяється динамічно. Кадри в буфері динамічно зв’язуються з портом призначення. Це дозволяє отримувати пакет на один порт і потім пересилати його на інший порт без переміщення в іншу чергу.

Комутатор зберігає зіставлення кадру зі зв’язаними портами, на які необхідно переслати пакет. Збережене зіставлення видаляється після успішної передачі кадру. Кількість кадрів, збережених у буфері, обмежена розміром всього буфера пам’яті й не обмежується буфером одного порту. Це дозволяє передавати кадри більшого обсягу, при цьому кількість скинутих кадрів буде менше. Це особливо важливо для асиметричної комутації. Асиметрична комутація дозволяє використовувати різні швидкості передачі даних на різних портах. Це забезпечує виділення більшої смуги пропускання деяких портів, наприклад, порту, підключеному до сервера.

8.3 Маршрутизатори (Routers)

Маршрутизатор – це прилад мережевого рівня еталонною моделі OSI, що використовує одну чи більше метрик визначення оптимального шляху передачі мережного трафіку, з огляду на інформацію мережевого рівня.

З цього визначення випливає, що маршрутизатор передусім необхідний для визначення подальшого шляху даних, посланих на велику й складну мережу. Користувач такої мережі відправляє дані до мережі та вказує адресу свого абонента. Дані проходять через мережу й у точках із розгалуженням маршрутів надходять на маршрутизатори. Маршрутизатор вибирає подальший найкращий шлях. Те, який шлях краще, визначається кількісними показниками, які називаються метриками. Кращий шлях – це шлях із найменшої метрикою. У метриці може враховуватися кілька показників, наприклад, довжина шляху, час перебігу, завантаженість мережі тощо.

Якщо MAC-адреса джерела вже існує, комутатор оновлює таймер поновлення для цього запису. За замовчуванням у більшості комутаторів Ethernet дані в таблиці зберігаються протягом 5 хвилин.

Примітка. Якщо MAC-адреса джерела вказана в таблиці, але з іншим портом, комутатор вважає цей запис новим. Запис замінюється на тій самій MAC-адресі, але з більш актуальним номером порту.

Пересилання: перевірка MAC-адреси призначення

Якщо MAC-адреса призначення є адресою одноадресної розсилки, комутатор шукає збіг між MAC-адресою призначення в кадрі й записом у таблиці MAC-адрес.

Якщо MAC-адресу призначення є в таблиці, комутатор пересилає кадр через вказаний порт.

Якщо MAC-адреси призначення немає в таблиці, комутатор пересилає кадр через всі порти, крім вхідного порту. Цей процес називається одноадресною розсилкою без адреси.

Буферизація пам'яті на комутаторах

Комутатор Ethernet може використовувати метод буферизації для зберігання кадрів до їх пересилання. Крім того, буферизацію можна використовувати в тому випадку, якщо порт призначення зайнятий через його перевантаження, і комутатор зберігає кадр доти, поки не з’явиться можливість його передачі.

Існують два методи буферизації пам’яті: буферизація на базі портів і буферизація спільно використовуваної пам’яті.

Буферизація пам'яті на базі портів

У процесі буферизації пам'яті на базі портів кадри зберігаються в чергах, пов’язаних із певними вхідними та вихідними портами. Кадр пересилається на вихідний порт тільки в тому випадку, якщо всі кадри, що знаходяться в черзі перед ним, були успішно відправлені. Один кадр може стати причиною затримки передачі всіх кадрів у пам’яті через зайнятість порту призначення. Така затримка виникає і в тому випадку, якщо інші кадри можна передати на відкриті порти призначення.

За порядком організації передавання на фізичному рівні в комп’ютерних мережах визначають моноканали та мережі з ретрансляцією.

Моноканал – це така мережа, у якій фізичне середовище забезпечує одночасне (з точністю до часу поширення сигналу) передавання блоків даних усім приєднаним абонентам.

На відміну від моноканалу, у мережах з ретрансляцією блоки даних приймаються в проміжних вузлах, а потім знову передаються.

Протоколи канального рівня (Рис.11) призначені для передавання блоків даних через одне фізичне сполучення. Протокольні блоки даних канального рівня називають кадрами (frames).

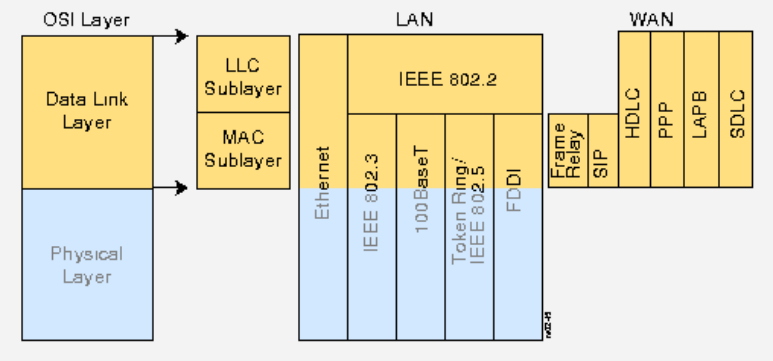

Рис.11. Структура канального рівня

На сучасному етапі канальний рівень протоколу розділяють на два підрівні (Рис.11): керування логічним каналом (Logical Link Control(LLC)) та керування доступом до середовища (Media Access Control(MAC)). Перший забезпечує керування логічним каналом і не залежить від фізичного середовища, а другий – доступ до фізичних з’єднань і залежить від них.

Протоколи MAC часто регламентує організацію передавання в локальних мережах, в яких єдине передавальне середовище розподіляється між багатьма абонентськими системами. Тому головною функцією MAC-підрівня є забезпечення доступу окремих абонентів до передавального середовища так, щоб пропускна здатність каналу зв’язку була використана ефективно.

Завданням протоколу LLC-підрівня є забезпечення правильного передавання даних між двома станціями (відправником інформації та її одержувачем) для довільного фізичного середовища передавання. У цьому випадку між об'єктами канального рівня налагоджується «логічний канал». Весь сервіс передавання забезпечує MAC-підрівень.

Для реалізації свого завдання LLC-протокол може нумерувати кадри та слідкувати за отриманням кадрів у порядку номерів, вимагати повторення передавання спотворених або втрачених кадрів.

Рівень LLC відповідає за передачу кадрів даних між вузлами з різним ступенем надійності, а також реалізує функції інтерфейсу з прилягаючим до нього мережним рівнем. Саме через рівень LLC мережевий протокол запитує в канального рівня потрібну йому транспортну операцію з потрібною якістю. На рівні LLC існує кілька режимів роботи, що відрізняються наявністю чи відсутністю на цьому рівні процедур відновлення кадрів у випадку їхньої втрати чи перекручування, тобто транспортних послуг, що відрізняються якістю, цього рівня.

Згідно зі стандартом 802.2 рівень керування логічним каналом LLC надає верхнім рівням три типи процедур:

LLC1 – процедура без встановлення з'єднання і без підтвердження;

LLC2 – процедура зі встановленням з'єднання і з підтвердженням;

LLC3 – процедура без встановлення з'єднання, але з підтвердженням.

Цей набір процедур є загальним для всіх методів доступу до середовища, визначених стандартами 802.3 - 802.5

Одним із найбільш поширених протоколів канального рівня є протокол Ethernet.

Ethernet – базова технологія локальних обчислювальних (комп'ютерних) мереж із комутацією пакетів. Цей протокол дає змогу в кожний момент часу лише один сеанс передачі в логічному сегменті мережі. При появі двох і більше сеансів передачі одночасно виникає колізія, яка фіксується станцією, що ініціює передачу. Станція аварійно зупиняє процес і очікує закінчення поточного сеансу передачі, а потім знову намагається повторити передачу.

(Рис.26), або коли порт, куди має бути спрямований пакет, зайнятий, в інших випадках він комутирує пакети «на льоту». Комутатор лише аналізує адресу призначення із заголовка пакета і, звірившись з адресною таблицею, одразу (час затримки близько 30-40 мікросекунд) спрямовує цей пакет у відповідний порт. Отже, коли пакет ще повністю не увійшов на вхідний порт, його заголовок вже передається через вихідний.

Комутатори підтримують повно дуплексний режим. У цьому режимі дані передаються та приймаються одночасно, що організувати неможливо у звичайних мережах Ethernet. У цьому випадку швидкість передачі зростає у двічі.

MAC	Порт
C8-5B-76-96-2E-B7	1
C8-5B-76-96-2E-B8	3
C8-5B-76-96-2E-B9	4
C8-5B-76-96-2E-BA	2

Рис.26. Таблиця MAC-адрес

Отримання інформації про MAC-адреси

Комутатор створює таблицю MAC-адрес динамічно, перевіряючи MAC-адресу джерела в кадрах, прийнятих портом. Він пересилає кадри на основі збігу між MAC-адресою призначення в кадрі й записом у таблиці MAC-адрес.

При кожному надходженні кадру Ethernet у комутатор виконується наступний процес.

Отримання інформації: перевірка MAC-адреси джерела

При кожному надходженні кадру в комутатор виконується перевірка на наявність нової інформації. Перевіряється MAC-адреса джерела, зазначена в кадрі, і номер порту, по якому кадр надходить у комутатор.

Якщо MAC-адреса джерела відсутня, вона додається в таблицю разом із номером вхідного порту.

8.2 Комутатори (Switches)

Коли з'явилися перші пристрої, що дозволяють роз'єднувати мережу на кілька доменів (власне фрагменти мереж, побудовані на концентраторах), вони були двох портовими й одержали назва мостів (bridges). З розвитком такого типу устаткування вони стали багатопортовими й одержали назву комутаторів (switches).

У загальному випадку комутатор і міст аналогічні за функціональністю; різниця полягає у внутрішньому устрої: мости обробляють трафік, використовуючи центральний процесор, комутатор використовує комутаційну матрицю (апаратну схему для комутації пакетів). Нині мости практично не використовуються (оскільки для роботи вимагають продуктивний процесор), за винятком ситуацій, коли зв'язуються сегменти мережі з різною організацією першого рівня, наприклад, між xDSL сполуками, оптикою, Ethernet.

Зазвичай проектувальники мереж за допомогою комутаторів з'єднують кілька доменів локальної мережі між собою. У реальному житті у ролі доменів виступають здебільшого поверхи будинку, у якому створюється мережа. Їх зазвичай більше двох, тому в результаті забезпечується значно ефективніше керівництво трафіком, ніж у прародича комутатора – моста.

Завдяки тому, що комутатори керують трафіком з урахуванням протоколу канального рівня моделі OSI, вони можуть контролювати MAC адреси підключених до нього пристроїв і навіть координувати організацію трансляції пакетів зі стандарту в стандарт (наприклад, Ethernet в FDDI і навпаки). Особливо вдало результати такої можливості представлені в комутаторах мережевого рівня, тобто в пристроях, можливості яких наближаються до можливостей маршрутизаторів.

Комутатор дозволяє пересилати пакети між кількома сегментами мережі. На відміну від мостів, деякі комутатори не заносять всі пакети, які надходять у буфер. Це відбувається лише тоді, коли треба узгодити швидкості передачі, чи адреси призначення немає в таблиці MAC-адрес

Ethernet-мережі функціонують на швидкостях 10 Мбіт/с, Fast Ethernet – на швидкостях 100 Мбіт/с, Gigabit Ethernet – на швидкостях 1000 Мбіт/с, 10 Gigabit Ethernet – на швидкостях 10 Гбіт/с. У червні 2010 року було остаточно прийняті стандарти з досягненням швидкості 100 Гбіт/с (100 Gigabit Ethernet).

Найпоширеніший формат кадру Ethernet (Рис.12):

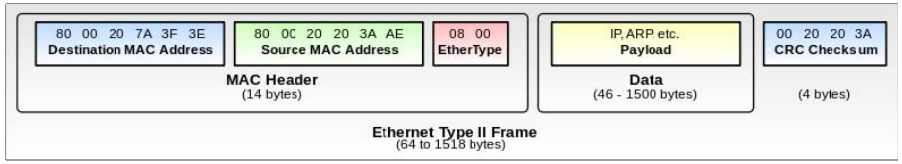

Рис.12. Формат кадру Ethernet

5.2 Протоколи мережевого та транспортного рівнів

Треба розрізняти два схожі за назвою, але діаметрально протилежні за властивостями терміни – маршрутизований протокол та протокол маршрутизації. Ще більша плутанина виникає з оригінальною назвою – routed & routing protocols.

Маршрутизований протокол – це будь-який мережевий протокол, адреса мережевого рівня якого надає достатньо інформації для доставки пакета від одного вузла мережі до іншого на основі використовуваної схеми адресації. Такий протокол задає формати полів *усередині* пакета. Пакети зазвичай передаються від однієї кінцевої системи до іншої. Маршрутизований протокол використовує таблицю маршрутизації для пересилки пакетів.

Приклади маршрутизованих протоколів – Internet-протокол (IP), протокол міжмережевого пакетного обміну IPX тощо. Набагато легше зрозуміти, що таке маршрутизовані протоколи, якщо пам'ятати, що це – протоколи передачі даних.

Протокол маршрутизації – такий протокол, який підтримує маршрутизовані протоколи й надає механізми обміну маршрутною інформацією. Повідомлення протоколу маршрутизації передаються між

маршрутизаторами (роутерами). Протокол маршрутизації дозволяє роутерам обмінюватись інформацією між собою для оновлення записів і підтримки таблиці маршрутизації. Приклади протоколів маршрутизації: RIP (Routing Information Protocol), IGRP, EIGRP, OSPF. Легше зрозуміти, що таке протоколи маршрутизації, якщо пам'ятати, що це – протоколи обміну маршрутною інформацією.

Для того щоб протокол був маршрутизованим, він має включати механізми призначення як номера мережі, так і номера вузла для кожного пристрою в мережі. У деяких протоколах, як, наприклад, IPX необхідно визначати лише адресу мережі, оскільки як адресу пристрою ця технологія використовує фізичну адресу (MAC-адресу) пристрою. Інші протоколи, такі як IP-протокол, вимагають явного задання повної адреси й маски підмережі.

IP-протокол (rfc -791) (англ. IP — Internet protocol) – найбільш розповсюджена реалізація ієрархічної схеми мережної адресації. Використовуваний у мережі Інтернет протокол відповідає за адресацію пакетів, але не відповідає за встановлення з'єднань, не є надійним і дозволяє реалізувати тільки негарантовану доставку даних. Протокол IP вибирає найефективніший шлях із числа доступних на основі рішень, прийнятих протоколом маршрутизації. Відсутність надійності й негарантована доставка не означає, що система працює погано або ненадійно, а вказує лиш на те, що протокол IP не докладає ніяких зусиль, щоб перевірити, чи був пакет доставлений за призначенням. Ці функції делеговані протоколам транспортного та вищих рівнів. Транспортний рівень також відповідає за збірку пакетів у повідомлення в потрібній послідовності.

Структура пакета IP зображена на Рис.13.

в «ефірі», що веде до зростання колізій (накладання пакетів один на один) і, відповідно, до уповільнення роботи мережі загалом. Багатосегментні концентратори допомагають усунути «вузькі місця», роз'єднуючи мережу на сегменти.

Робочі станції у межах одного сегмента конкурують між собою за загальне середовище передачі даних, незважаючи станціям в іншому сегменті. Таким чином, загальна пропускна спроможність мережі збільшується практично кратно кількості сегментів.

Оскільки кожний сегмент у багатосегментному концентраторі є незалежним, то для їхньої спільної роботи вимагається міст, комутатор або маршрутизатор для передачі пакетів з одного сегмента в інший, що, у свою чергу, призводить до зростання накладних витрат – збільшує вартість підключення і час передачі пакета між сегментами.

Конструктивно концентратор може бути виконаний у вигляді окремого пристрою зі своїм блоком живлення або у вигляді плати, яка встановлюється у слот розширення материнської плати комп'ютера.

Концентратор у вигляді окремого пристрою дорожчий, однак має ту перевагу, що до нього можна приєднувати сегменти, виконані як на тонкому, так і на товстому коаксіальному кабелі, а також на витій парі.

Концентратор у вигляді електронної плати з'єднує тільки сегменти на тонкому коаксіальному кабелі, недоліком також є те, що для забезпечення цілодобової роботи разом з концентратором повинна працювати робоча станція.

Існують також гібридні концентратори, до яких можна підключати кабелі різних типів.

Можна сказати, що концентратори підвищують надійність роботи мережі, тому що відмова в роботі одного сегмента не впливає на роботу всієї мережі.

Усі мережі, за винятком найменших, складаються з більш ніж одного сегмента. Робиться це або для досягнення більшої віддаленості між кінцевими станціями, або для збільшення пропускної спроможності мережі. Щоб комп'ютери могли обмінюватися повідомленнями так, ніби з'єднані одним кабелем, сегменти, в яких знаходяться комп'ютери, з'єднуються один з одним через мости або маршрутизатори.

Каскадні використовуються у мережах, які розширюються, їх можна об’єднувати в стеки (створювати каскади), де вони працюють як єдиний пристрій. Кожен із них має окремий блок живлення. Об’єднання в стек виконується кабелями.

Модульні (подібно до каскадних) об’єднуються один з одним, але використовуються в мережах зі змішаними технологіями Ethernet та Token Ring.

Назва «модульні» походить від конструктивних особливостей приладів – концентратори у вигляді електронних плат із портами встановлюються в плату об’єднання модулів та мають загальний блок живлення. Тобто в модульний концентратор можуть підключатися модулі для різних типів мереж.

Існує три основних типи концентраторів за функціональним призначенням:

– пасивні (passive);

– активні (active);

– інтелектуальні (intelligent).

Пасивні концентратори не потребують живлення і діють просто як фізична точка з’єднання, нічого не додаючи до сигналу, що проходить.

Активні концентратори потребують живлення, яке вони використовують для відновлення та підсилення сигналу, що проходить через них.

Інтелектуальні можуть надавати можливість переключення пакетів та перенаправлення трафіку.

Деякі концентратори дозволяють програмним шляхом розділяти порти пристрою на сегменти. Така можливість називається переключенням портів. Концентратор може містити декілька сегментів Ethernet, що організовуються внутрішніми засобами пристрою. Переключення портів забезпечує гнучкість організації сегментів. Забезпечується можливість переносу портів з одного сегмента в інший. Навантаження мережі розподіляється між сегментами, тим самим знижуються витрати на подібні операції.

Концентратори не вирішують проблему збільшення смуги пропускання мережі – зі зростанням кількості комп’ютерів збільшується і кількість пакетів

Біти 0-3	4-7	8-15	16-18	19-23	24-31
Версія	HLEN	Тип обслуговування	Загальна довжина		
Ідентифікація			Флаги	Зміщення фрагментації	
Час життя		Протокол	Контрольна сума заголовку		
IP-адреса відправника					
IP-адреса отримувача					
Опції					Додаток
Дані (65535 мінус заголовок)					
...					

Рисунок 13. Структура пакету IP

Версія (Version) – 4-бітове поле, що описує використовувану версію протоколу IP. Усі пристрої зобов’язані використовувати протокол IP однієї версії, пристрій, що використовує іншу версію буде відкидати пакети.

Довжина IP-заголовка (IP header Length – HLEN) – 4-бітове поле, що описує довжину заголовка пакета в 32-бітових блоках. Це значення – повна довжина заголовка з урахуванням двох полів змінної довжини.

Тип обслуговування (Type of Service – TOS) – 8-бітове поле, що вказує на ступінь важливості інформації, яка присвоєна протоколом верхнього рівня.

Загальна довжина (Total Length) – 16-бітове поле, що описує довжину пакета в байтах, із заголовком і даними включно. Для того щоб вирахувати довжину блока даних, потрібно від повної довжини відняти значення поля HLEN.

Ідентифікація (Identification) – 16-бітове поле, що зберігає ціле число, яке описує даний пакет. Це число являє собою послідовний номер.

Флаги (Flags) – 3-бітове поле, в якому два молодших біти контролюють фрагментацію пакетів. Перший біт визначає, чи був пакет фрагментовано, а другий – чи є цей пакет останнім фрагментом у серії фрагментів.

Зміщення фрагментації (Fragment Offset) – 13-бітове поле, що допомагає зібрати разом фрагменти пакетів. Це поле дозволяє використовувати 16 бітів у сумі для флагів фрагментації.

Час життя (Time-to-Live – TTL) – 8-бітове поле-лічильник, в якому зберігаються послідовно зменшуване значення кількості пройдених вузлів (роутерів, що їх ще іноді в цьому випадку називають хопами (hops)) на шляху

до місця призначення. У випадку коли лічильник пройдених хопів дорівнюватиме нулю – пакет буде відкинуто, таким чином попереджується нескінченна циклічна пересилка пакетів.

Протокол (Protocol) – 8-бітове поле, що вказує на те, який протокол верхнього рівня отримає пакет після завершення обробки IP-протоколом. Наприклад, TCP або UDP.

Контрольна сума заголовку (Header Checksum) – 16-бітове поле, що допомагає перевірити цілісність заголовка пакета.

IP-адреса відправника (Source IP address) (адресант, сорс, відправник) – 32-бітове поле, що зберігає IP-адресу вузла-відправника.

IP-адреса отримувача (Destination IP adress) (адресат, дест, отримувач) – 32-бітове поле, що зберігає адресу вузла призначення (отримувача).

Опції (Options) – поле змінної довжини, що дозволяє протоколу IP реалізувати підтримку різних опцій, зокрема засобів безпеки.

Підкладка (Padding) – поле, що використовується для вставки додаткових нулів для гарантування кратності IP-заголовка 32 бітам.

Дані (Data) – поле змінної довжини (64 Кбіт макс.), що зберігає інформації для верхніх рівнів.

Routing Information Protocol,(RIP) – один із найпоширеніших протоколів маршрутизації в невеликих комп'ютерних мережах, який дозволяє маршрутизаторам динамічно оновлювати маршрутну інформацію (напрямок і дальність в хопах).

Transmission Control Protocol(rfc-793), TCP (укр. *Прото́кол керува́ння переда́чею*) – один з основних мережевих протоколів Інтернету, призначений для управління передачею даних у мережах і підмережах TCP/IP (рис. 14).

Інформацію, яку потрібно передати, TCP розбиває на порції-сегменти. Кожна порція нумерується, щоб можна було перевірити, чи вся інформація отримана, і розташувати інформацію в правильному порядку. Для передачі цього порядкового номера по мережі в протоколі є свій власний сегмент даних, в якому, зокрема, написана службова необхідна інформація. Порція ваших даних розміщується в сегмент TCP. Сегмент TCP, у свою чергу, розміщується в сегменті IP і передається в мережу.

При цьому слід враховувати кількість портів концентраторів. Зазвичай це 8-, 16-, 24-портові прилади.

Кількість портів концентратора пов'язують із кількістю робочих станцій, які необхідно з'єднати в мережі. Приклад 16-портового концентратора наведено на Рис.25.

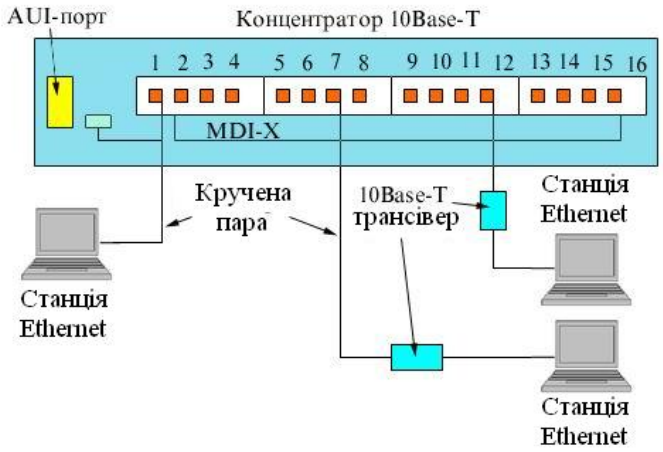

Рис.25. 16-портовий концентратор

Кожен порт використовується для підключення одного комп'ютера до мережі. Завдяки тому, що він працює на фізичному рівні, в ньому не виконуються операції по адресації або створенню кадрів. Він тільки приймає дані від одного порту та пересилає їх іншим портам, тому кожен комп'ютер може прийняти ці дані.

За конструктивними особливостями концентратори класифікують так:

– автономні;

– каскадні;

– модульні.

Автономні у вигляді невеликих пристроїв використовують для побудови локальних обчислювальних мереж робочої групи. Кількість портів невелика – від 2 до 10.

концентратори й мережеві адаптери дозволяють будувати невеликі базові фрагменти мереж, які потім повинні поєднуватися один з одним за допомогою мостів, комутаторів і маршрутизаторів.

Як вже зазначалось, цей мережевий пристрій діє на фізичному рівні моделі OSI та використовується як центральна точка з'єднання при топології «зірка». На принциповій схемі концентратор розташовують в центрі «зірки». До нього під'єднуються робочі станції так, ніби концентруються всі в одному місці. Звідси й походить назва приладу.

На Рис.23 показано просту мережу з використанням одного концентратора.

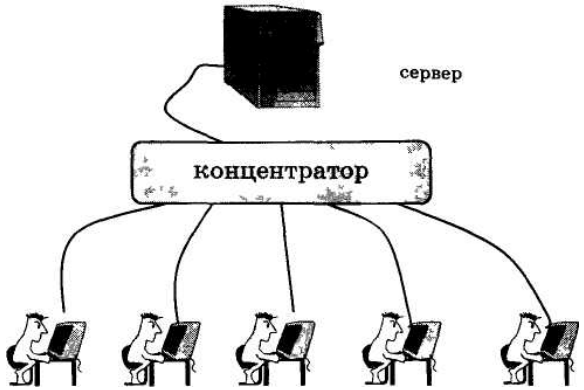

Рис.23. Мережа з одним концентратором

При збільшенні кількості робочих станцій мережі можна йти шляхом збільшення кількості концентраторів (Рис.24).

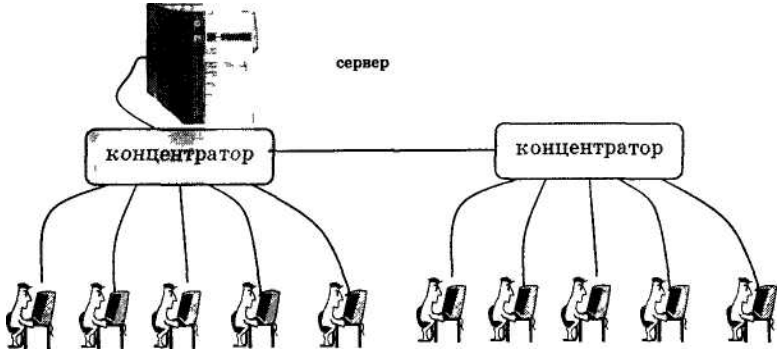

Рис.24 – Мережа з двома концентраторами.

На приймаючій стороні програмне забезпечення протоколу TCP збирає сегменти, витягує з них дані й розташовує їх у правильному порядку. Коли якихось сегментів немає, програма просить відправника передати їх ще раз. Після розміщення всієї інформації в правильному порядку ці дані передаються тій програмі, яка використовує послуги TCP.

Біт	0 — 3	4 — 9	10 — 15	16 — 31
0	Порт джерела			Порт призначення
32	Номер послідовності			
64	Номер підтвердження			
96	Зсув даних	Зарезервовано	Прапорці	Вікно
128	Контрольна сума			Вказівник важливості
160	Опції (необов'язково)			
160/192+	Дані			

Рисунок 14. Формат сегменту TCP

Порт джерела ідентифікує порт, з якого відправлений пакет.

Порт призначення ідентифікує порт, на який відправлений пакет.

Номер послідовності виконує два завдання:

Якщо встановлений прапор SYN, то це початкове значення номера послідовності й перший байт даних – це номер послідовності плюс 1.

Інакше, якщо SYN не встановлений, перший байт даних – номер послідовності.

Номер підтвердження. Якщо встановлений прапор ACK, то це поле містить номер послідовності, очікуваний відправником наступного разу. Позначає цей пакет як підтвердження отримання.

Зсув даних. Це поле визначає розмір заголовка пакету TCP в 32-бітових словах. Мінімальний розмір становить 5 слів, а максимальний – 15, що становить 20 і 60 байт відповідно. Зсув рахується від початку заголовка TCP.

Зарезервовано. 4 біта зарезервовано для майбутнього використання й повинні встановлюватися в нуль.

Прапорці (управляючі біти). Це поле містить 8 бітових прапорців:

CWR – Поле встановлюється відправником, щоб показати, що TCP-сегмент був отриманий зі встановленим полем ECE (додано до заголовку в RFC 3168); ECE – Поле показує, що відправник підтримує ECN (Explicit Congestion Notification); URG – Поле «Покажчик важливості» задіяно (англ. Urgent pointer field is significant); ACK – Поле «Номер підтвердження» (англ. Acknowledgement field is significant); PSH (англ. Push function) інструктує отримувача передати дані з прийомного буфера до програми, якій ці дані призначені; RST – Обірвати з'єднання, скинути буфер (очищення буфера) (англ. Reset the connection); SYN – Синхронізація номерів послідовності (англ. Synchronize sequence numbers); FIN (англ. final) – прапорець, якщо встановлений, указує на завершення з'єднання (англ. FIN bit used for connection termination).

Контрольна сума. Поле контрольної суми – це 16-бітове доповнення суми всіх 16-бітових слів заголовка і тексту. Якщо сегмент містить непарне число октетів в заголовку /або тексті, останні октети доповнюються праворуч 8 нулями для вирівнювання по 16-бітовій межі. Біти заповнення (0) не передаються в сегменті і служать тільки для розрахунку контрольної суми. При розрахунку контрольної суми значення самого поля контрольної суми приймається рівним 0.

Покажчик важливості. 16-бітове значення позитивного зсуву від порядкового номера в цьому сегменті. Це поле вказує порядковий номер октету, з якого починаються важливі (urgent) дані. Поле береться до уваги тільки для пакетів зі встановленим прапором U.

User Datagram Protocol, UDP(rfc-768) (рис. 15) (укр. *Протокол дейтаграм користувача*) – один із протоколів у стеку TCP/IP. Від протоколу TCP він відрізняється тим, що працює без встановлення з'єднання. UDP – це один із найпростіших протоколів транспортного рівня моделі OSI, що виконує обмін дейтаграмами без підтвердження та гарантії доставки. UDP є ефективним для серверів, що надсилають невеликі відповіді великій кількості клієнтів.

8. ПАСИВНЕ ТА АКТИВНЕ ОБЛАДНАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Пасивне апаратне забезпечення – обладнання, що повторює електричний сигнал для збільшення відстані з'єднання або топологічного розгалуження і нічого «інтелектуального» собою не являє (повторювач (repeater), розетка, кабелі, концентратори (hub) тощо).

Активне апаратне забезпечення – це устаткування, що має певні «інтелектуальні» можливості. Тобто маршрутизатор, комутатор (switch) і т. ін. є активним мережним устаткуванням.

Керовані комутатори відносяться до активного мережного обладнання, оскільки можуть бути наділені певними «інтелектуальними властивостями».

Нижче наведено опис деякого найпопулярнішого мережевого обладнання.

8.1 Концентратори (Hubs)

Концентратори (hubs), які прийшли на зміну загальному кабелю, створили значно гнучкішу та зручнішу основу для побудови локальних мереж.

Концентратор працює як повторювач (перший рівень OSI-моделі), передаючи сигнал, що надійшов на один із портів, без зміни на інші порти.

Отже, кожний комп'ютер «чує» весь трафік у мережі так, як ніби це була б «широкомовна» мережа із загальним кабелем. Усі роз'ємні сполучення виявляються зосередженими в одному місці, спрощуючи завдяки цьому підключення додаткових робочих місць у мережу.

Концентратори разом із мережевими адаптерами, а також кабельною системою становлять той мінімум обладнання, за допомогою якого можна створити локальну мережу. Така мережа буде являти собою загальне поділюване середовище. Зрозуміло, що мережа не може бути занадто великою, тому що при великій кількості вузлів загальне середовище передачі даних швидко стає вузьким місцем, що знижує продуктивність мережі. Тому

Запитання для самоперевірки:

1. Опишіть особливості, переваги та недоліки витої пари.
2. Опишіть особливості, переваги та недоліки коаксіального кабелю.
3. Опишіть особливості, переваги та недоліки волоконно-оптичного кабелю.
4. Опишіть особливості, переваги та недоліки бездротової передачі даних.
5. Які категорії та види витої пари Ви знаєте? Опишіть їх.

Біти	0-15	16-31
0	Початковий Номер Порту	Номер Порту Призначення
32	Довжина	Контрольна сума
64+	Дата	

Рисунок 15. Формат сегмента UDP

Запитання для самоперевірки:

1. Порівняйте стек протоколів TCP/IP та модель OSI.
2. Опишіть реалізації протоколів різних рівнів:
    a) протоколи SMTP та ICMP;
    b) протоколи IGMP та IP;
    c) протоколи TCP та UDP.
3. Опишіть архітектуру протоколів фізичного та канального рівнів.
4. Опишіть структуру канального рівня.
5. Які функції виконує LLC підрівень канального рівня?
6. Які функції виконує MAC підрівень канального рівня?
7. Опишіть структуру та призначення полів кадру Ethernet.

6. ТЕХНОЛОГІЇ СІМЕЙСТВА ETHERNET

Ethernet – сімейство стандартизованих технологій пакетної передачі даних для комп'ютерних мереж (започаткований в 70-х, перший стандарт у 1980).

Протоколи Ethernet визначають:

Фізичний рівень: середовище передачі, топологія, бітові швидкості, способи підключення, довжини кабелів, способи кодування бітів.

Канальний рівень: порядок доступу до середовища, правила формування та розмежування кадрів, доставка даних за призначенням, перевірка цілісності кадрів.

Технологія Ethernet стандартизована в IEEE 802.2/ 802.3, однак є певні відмінності з Ethernet II (рис. 16).

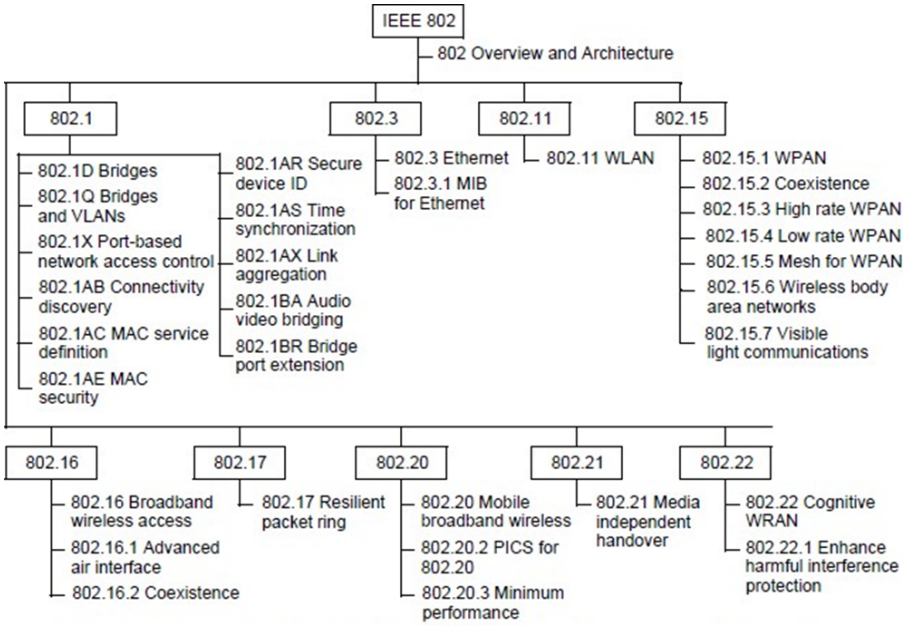

Рис.16. Структура сімейства стандартів IEEE 802.x

Як вже зазначалось раніше, фізичний рівень OSI забезпечує засоби транспортування бітів, що утворюють кадр даних канального рівня, по засобу мережевого підключення.

- кодування даних за допомогою радіосигналів;
- частота і потужність передачі;
- вимоги до прийому і декодування сигналів;
- проектування і будівництво антен;

Примітка. Wi-Fi є товарним знаком Wi-Fi Alliance. Wi-Fi використовується із сертифікованими продуктами, які відносяться до пристроїв бездротової локальної мережі (WLAN) і підтримують стандарти IEEE 802.11.

7.5 Бездротова локальна мережа

Найчастіше бездротова передача даних використовується для бездротового зв'язку пристроїв через локальну мережу (LAN). Здебільшого для створення бездротової LAN потрібні такі мережеві пристрої.

Бездротова точка доступу (AP): концентрує бездротові сигнали від користувачів. Підключається до мережевої інфраструктури на основі мідних кабелів, наприклад Ethernet. Бездротові маршрутизатори для дому та невеликих підприємств в одному пристрої поєднують функції маршрутизатора, комутатора й точки доступу.

Бездротові мережеві плати: забезпечують можливість бездротового підключення для кожного вузла в мережі.

У міру розвитку технології був створений багато стандартів бездротової локальної мережі (WLAN) на основі Ethernet. Тому, купуючи бездротові пристрої, слід звертати особливу увагу на їх сумісність.

Переваги бездротових технологій передачі даних очевидні, особливо в плані економії витрат на прокладку дорогих кабелів у приміщеннях і зручностей за рахунок мобільності мережевих пристроїв. Мережеві адміністратори повинні розробляти й застосовувати суворі правила і протоколи безпеки для захисту бездротових локальних мереж від несанкціонованого доступу і потенційного збитку.

Хоча популярність бездротового підключення настільних комп'ютерів до мережі зростає, найбільш популярним засобом мережевого підключення на фізичному рівні залишаються мідні й оптоволоконні кабелі.

Типи засобів бездротового підключення

Стандарти IEEE і телекомунікаційні галузеві стандарти бездротової передачі даних охоплюють як канальний, так і фізичний рівні. Нижче наведені деякі найпопулярніші стандарти бездротових мереж. Детальніше ці та інші технології будуть розглянуті у відповідній темі.

Стандарт IEEE 802.11. Wi-Fi

Технологія бездротового LAN (WLAN), яку зазвичай називають Wi-Fi. У WLAN застосовується конкурентний доступ до середовища, відомий як множинний доступ із контролем несучої і запобіганням колізій (CSMA/CA). Мережева інтерфейсна плата перед передачею даних повинна перевірити, чи вільний радіоканал. Якщо інший пристрій передає дані, мережева інтерфейсна плата повинна чекати звільнення каналу. Детальніше різні методи доступу будуть розглянуті у відповідній темі.

Стандарт IEEE 802.15. Bluetooth

Стандарт бездротових особистих мереж (WPAN), широко відомий як Bluetooth, для передачі даних на відстані від 1 до 100 метрів використовує процес сполучення пристроїв.

Стандарт IEEE 802.16. WiMAX

Більш відомий як протокол широкосмугового радіозв'язку (WiMAX); використовує топологію «точка – багато точок» для забезпечення бездротового широкосмугового доступу.

Примітка. Для створення мереж передачі даних можуть використовуватися й інші бездротові технології, наприклад, стільниковий або супутниковий зв'язок. Однак у цій темі ці бездротові технології не розглядаються.

У кожному зі згаданих стандартів специфікації фізичного рівня застосовуються до наступних характеристик:

Нині Ethernet є основною технологією для локальних мереж (LAN) у всьому світі. Ethernet функціонує на канальному і фізичному рівнях. Стандарти протоколів Ethernet визначають багато аспектів мережевого обміну даними, включаючи формат і розмір кадру, інтервал відправки і кодування. При пересиланні повідомлень між вузлами в мережі Ethernet, вузли форматують їх відповідно до стандартів макета кадру.

Оскільки технологія Ethernet складається з стандартів на цих нижчих рівнях, принцип її роботи можна найкраще зрозуміти на прикладі моделі OSI. Модель OSI відокремлює функціональні можливості адресації канального рівня, формування кадрів і доступу до середовища передачі даних від стандартів фізичного рівня такого середовища. Стандарти Ethernet регламентують як протоколи рівня 2, так і технології рівня 1. Незважаючи на те, що технічні вимоги Ethernet підтримують різні середовища передачі даних, смуги пропускання та інші варіанти рівнів 1 і 2, основний формат кадру і схема адреси будуть однаковими для всіх різновидів Ethernet (див. Рис.12).

Зазвичай стандарти сімейства Ethernet відрізняються середовищем передачі сигналу, швидкістю та режимом роботи.

Варіанти технологій (**X**Base**Y**):

1. Середовище передачі та способи підключення (**Y**):

– товстий коаксіальний кабель, підключення «зуб вампіра» (застарів);

– тонкий коаксіальний кабель , підключення BNC (застарів);

– екранована/неекранована вита пара (декілька пар), підключення RJ45;

– оптоволокно;

– радіосигнал (група 802.11).

2. Швидкість(**X**): 10 Мбіт/с, 100 Мбіт/с (FAST), 1 Гбіт/с (Gigabit), 10 Гбіт/с (10G), 40 Гбіт/с (40G), 100 Гбіт/с (100G).

3. Режими роботи за напрямком:

– дуплекс;

– напівдуплекс.

Таблиця 2 – Характеристики стандартів сімейства Ethernet

Стандарт	Тип стандарту	Тип кабелю	Топологія	Довжина зв'язку/ променя	Інтерфейс конекторів, коментар
10Base5	Ethernet 10Мбіт/с IEEE 802.3	товстий коаксіальний	Ш	500м	AUI
10Base2		тонкий коаксіальний	Ш	185м	BNC
10BaseT		UTP категорія 3 та вище (2 пари проводів)	З	100м	RJ-45
10BaseF		оптоволокно	З	1 - 10 км	AUI
100BaseTX	Fast Ethernet 100Мбіт/с IEEE 802.3u	UTP кат. 5 та вище (2 пари проводів)	З	100 м	RJ-45
100BaseT4		UTP категорія 3 та вище (4 пари проводів)	З	100м	RJ-45
100BaseFX		оптоволокно одномодове	З	10 км	ST, SC, MT-RJ…
100BaseSX		оптоволокно багатомодлве	З	300 м	сумісний з 10BaseF,
1000BaseCX	Gigabit Ethernet 802.3z, 802.3ab	STP (2 пари проводів)	З	25 м	RJ-45
1000BaseT		UTP категорія 5 та вище (4 пари проводів)	З	100 м	RJ-45
1000BaseSX		Оптоволокно багатомодове	З	200-500 м	ST, SC, MT-RJ…
1000BaseLX		оптоволокно одномодове	З	10 км	ST, SC, MT-RJ…
…					
10GBASE-…	10Gae				
100GBASE-…	100Gba				
40GBASE-…	40Gba				

Технологія Token Ring

Мережі Token Ring, так само як і мережі Ethernet, характеризує поділюване середовище передачі даних, що у цьому випадку складається з відрізків кабелю, що з'єднують усі станції мережі в кільце.

Кільце розглядається як загальний поділюваний ресурс, і для доступу до нього потрібно не випадковий алгоритм, як у мережах Ethernet, а детермінований, заснований на передачі станціям права на використання кільця у визначеному порядку. Це право передається за допомогою кадру спеціального формату, який називається *маркером* чи *токеном* (*token*).

Технологія Token Ring була розроблена компанією IBM у 1984 році, а потім передана як проект стандарту в комітет IEEE 802, який на її основі

7.4 Властивості засобів бездротового підключення

Засоби бездротового підключення забезпечують передачу двійкових розрядів даних у вигляді електромагнітних сигналів радіочастотного або мікрохвильового діапазону.

Засоби бездротового підключення забезпечують найбільший рівень мобільності в порівнянні з будь-якими іншими засобами, тому число пристроїв, що підтримують бездротове підключення, зростає з кожним днем. У міру збільшення пропускної здатності бездротове підключення завойовує все більшу популярність у корпоративних мережах.

Бездротове середовище має описані нижче особливості, які необхідно враховувати.

1. Зона покриття. Бездротові технології передачі даних добре працюють на відкритих просторах. Однак деякі будівельні матеріали, що використовуються при зведенні будівель і споруд, а також умови місцевості можуть обмежувати зону покриття.

2. Перешкоди. Якість бездротових з'єднань вразливе до перешкод і може погіршуватися при роботі таких звичайних пристроїв, як бездротові телефони, деякі типи флуоресцентних ламп, мікрохвильові печі, а також під впливом інших бездротових комунікацій.

3. Безпека. Для доступу до середовища бездротового підключення не потрібно підключатися до фізичних кабелів. Тому доступ до цього середовища можуть отримувати несанкціоновані користувачі та пристрої. Отже, головним аспектом адміністрування бездротової мережі є безпека.

4. Спільний доступ до засобу підключення. Мережі WLAN працюють у напівдуплексному режимі, що означає, що в кожен момент часу передачу або прийом може здійснювати тільки один пристрій. Засоби бездротового підключення спільно використовують усі бездротові користувачі. Чим більше користувачів одночасно підключаються до WLAN, тим менша пропускна здатність доводиться на кожного з них.

Багатомодовий оптоволоконний кабель (МОК). Має сердечник більшого діаметра. Для передачі світлових імпульсів використовуються світлодіодні випромінювачі. Світло, що випромінюється світлодіодом, входить у багатомодове волокно під різними кутами. Такі кабелі популярні в локальних мережах, оскільки дозволяють використовувати для роботи недорогі світлодіоди. Багатомодовий кабель забезпечує пропускну здатність до 10 Гбіт/с на відстані до 550 метрів.

Одне з основних відмінностей між МОК і ООК – рівень дисперсії. Під дисперсією в цьому контексті мається на увазі розширення світлового імпульсу в міру його руху через оптичне волокно. Чим вище дисперсія, тим більше втрати сигналу.

7.3 Оптоволоконні кабелі й мідні кабелі: порівняння

Оптоволоконні кабелі мають безліч переваг перед мідними.

Оскільки волокна, використовувані в оптоволоконних кабелях, не є провідниками, цей тип засобів підключення не схильний до електромагнітних перешкод і не проводить небажані електричні струми в разі проблем із заземленням. Оскільки оптичні волокна мають малу товщину й відрізняються порівняно малими втратами сигналу, вони дозволяють передавати інформацію на набагато більші відстані в порівнянні з мідними кабелями. Деякі специфікації фізичного рівня для оптоволоконних засобів підключення допускають використання оптичних кабелів довжиною до кількох кілометрів.

Нині більшості корпоративних мереж оптоволоконні кабелі в основному використовуються як магістральні для організації високошвидкісних з'єднань «точка-точка» між пристроями розподілу даних, а також для зв'язку між будівлями в комплексах будинків. Оскільки оптичне волокно не проводить електрику й відрізняється малими втратами сигналу, воно оптимально підходить для цих цілей.

прийняв у 1985 році стандарт 802.5. Компанія IBM використовує технологію Token Ring як своєю основну мережеву технологію для побудови локальних мереж на основі комп'ютерів різних класів – мэйнфреймів, міні-комп'ютерів і персональних комп'ютерів.

Технологія Token Ring є більш складною технологією, ніж Ethernet. Вона має властивості відмовостійкості. У мережі Token Ring визначені процедури контролю роботи мережі, що використовують зворотний зв'язок кільцеподібної структури – посланий кадр завжди повертається в станцію-відправник. У деяких випадках виявлені помилки в роботі мережі усуваються автоматично, наприклад, може бути відновлений загублений маркер. В інших випадках помилки тільки фіксуються, а їхнє усунення виконується вручну обслуговуючим персоналом.

Для контролю мережі одна зі станцій виконує роль так названого *активного монітора*. Активний монітор вибирається під час ініціалізації кільця як станція з максимальним значенням Mac-адреси. Якщо активний монітор виходить із ладу, процедура ініціалізації кільця повторюється й вибирається новий активний монітор. Щоб мережа могла знайти відмовлення активного монітора, останній у працездатному стані кожні 3 секунди генерує спеціальний кадр своєї присутності. Якщо цей кадр не з'являється в мережі більш 7 секунд, то інші станції мережі починають процедуру вибору нового активного монітора.

Маркерний метод доступу до середовища

У мережах з маркерним методом доступу (а до них, крім мереж Token Ring, відносяться мережі FDDI, а також мережі, близькі до стандарту 802.4, – ArcNet, мережі виробничого призначення MAP) право на доступ до середовища передається циклічно від станції до станції по логічному кільцю.

У мережі Token Ring кільце утворюється відрізками кабелю, що з'єднують сусідні станції. Таким чином, кожна станція зв'язана зі своєю попередньою і наступною станцією й може безпосередньо обмінюватися даними тільки з ними. Для забезпечення доступу станцій до фізичного

середовища по кільцю циркулює кадр спеціального формату і призначення – *маркер*. У мережі Token Ring будь-яка станція завжди безпосередньо одержує дані тільки від однієї станції – тієї, яка є попередньою в кільці. Така станція називається *найближчим активним сусідом, розташованим вище по потоку* (даних) – *Nearest Active Upstream Neighbor*, *NAUN*. Передачу ж даних станція завжди здійснює своєму найближчому сусіду вниз по потоку даних.

Одержавши маркер, станція аналізує його і у разі відсутності в неї даних для передачі забезпечує його просування до наступного станції. Станція, що має дані для передачі, одержавши маркер, вилучає його з кільця, що дає їй право доступу до фізичного середовища і передачі своїх даних. Потім ця станція видає в кільце кадр даних встановленого формату послідовно по бітах. Дані, що передаються, проходять по кільцю завжди в одному напрямку від однієї станції до іншої. Кадр містить адресу призначення й адресу джерела.

Усі станції кільця ретранслюють кадр побітно, як повторювачі. Якщо кадр проходить через станцію призначення, то, розпізнавши свою адресу, ця станція копіює кадр у свій внутрішній буфер і вставляє в кадр ознаку підтвердження прийому. Станція, що видала кадр даних у кільце, при зворотному його одержанні з підтвердженням прийому вилучає цей кадр із кільця і передає в мережу новий маркер для забезпечення можливості іншим станціям мережі передавати дані. Такий алгоритм доступу застосовується в мережах Token Ring зі швидкістю роботи 4 Мбіт/с, описаний у стандарті 802.5.

На Рис.17 описаний алгоритм доступу до середовища ілюструється тимчасовою діаграмою. Тут показана передача пакета А в кільці, що складається з 6 станцій, від станції 1 до станції 3. Після проходження станції призначення 3 у пакеті А встановлюються дві ознаки – ознака розпізнавання адреси й ознака копіювання пакета в буфер. Після повернення пакета в станцію 1 відправник розпізнає свій пакет за адресою джерела і видаляє пакет з кільця. Встановлені станцією 3 ознаки говорять станції-відправнику про те, що пакет дійшов до адресата й був успішно скопійований їм у свій буфер.

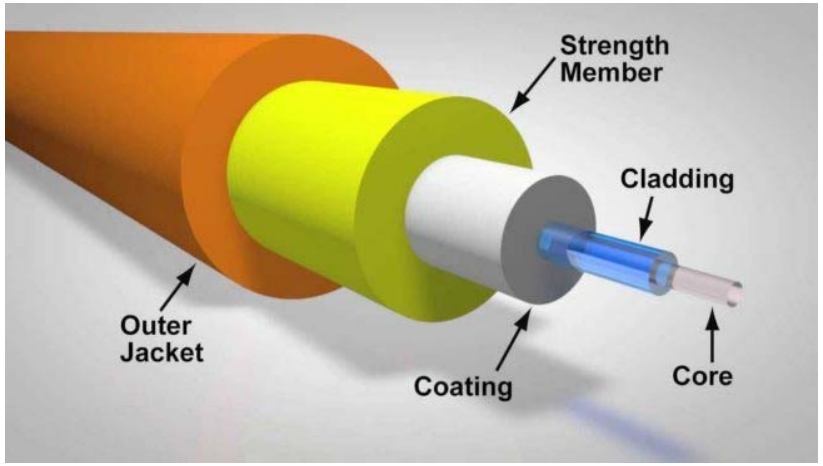

Рис.22. Структура оптоволоконного кабелю

Хоча оптичне волокно дуже тонке і може легко гнутися, але завдяки властивостям сердечника й оболонки воно дуже міцне. Завдяки своїй міцності оптичне волокно може використовуватися в найважчих умовах експлуатації.

Типи оптоволоконних кабелів

Світлові імпульси, за допомогою яких біти даних кодуються для передачі, можуть генеруватися такими джерелами:

- лазери;
- світловипромінюючі діоди (LED).

На стороні прийому напівпровідникові пристрої, які називаються фотодіодами, приймають світлові імпульси і перетворюють їх у напруги. Передане по оптоволоконному кабелю лазерне випромінювання небезпечно для очей. Тому при роботі з активним оптоволоконним кабелем необхідно дотримуватися запобіжних заходів.

Оптоволоконні кабелі поділяються на два основних типи.

Одномодовий оптоволоконний кабель (ООК). Має сердечник дуже малого діаметра. Для передачі променя світла потрібна дорога лазерна технологія. Широко використовується для організації ліній зв’язку довжиною кілька сотень кілометрів, наприклад для далекої телефонії і кабельного телебачення.

Для аналогії уявіть собі порожній сердечник від рулону паперових рушників, внутрішні стінки якого вкриті матеріалом, який дзеркально відображає промені. Його довжина становить тисячу метрів. За допомогою невеликої лазерної указки через нього зі швидкістю світла передаються сигнали азбуки Морзе. По суті, саме так функціонує оптоволоконний кабель, тільки він має набагато менший діаметр і створений із застосуванням найсучасніших оптичних технологій.

На сьогодні оптоволоконні кабелі використовуються в таких чотирьох сферах.

Корпоративні мережі. Оптоволоконні кабелі використовуються як магістральні кабелі та для з'єднань між пристроями мережної інфраструктури.

Технологія «оптоволокно до квартири» (FTTH). Оптоволоконні кабелі використовуються для постійного широкосмугового доступу індивідуальних користувачів і невеликих підприємств до мережі.

Мережі телекомунікації. Оптоволоконні кабелі використовуються провайдерами послуг для міжнародного та міжміського зв'язку.

Підводні кабельні мережі. Оптоволоконні кабелі використовуються для будівництва надійних високошвидкісних ліній зв'язку, здатних працювати у важких умовах великих глибин і забезпечувати зв'язок на великих відстанях, аж до трансокеанських.

Конструкція оптоволоконного кабелю

Оптичне волокно складається з двох видів скляних компонентів (сердечника і внутрішньої оболонки) і захисної зовнішньої оболонки (Рис.22).

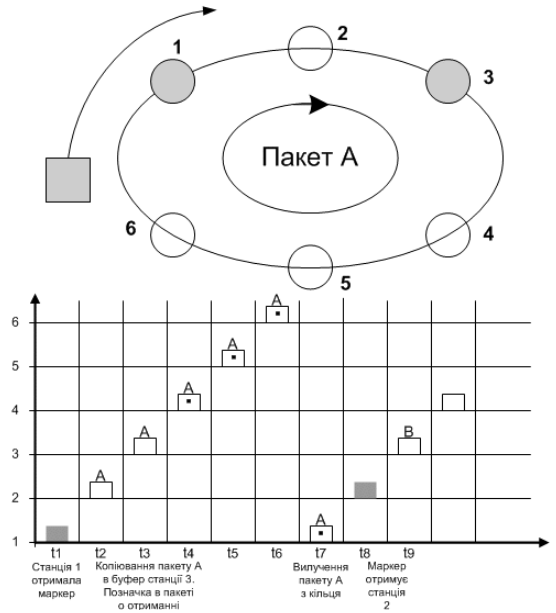

Рис.17. Принцип маркерного доступу

Час володіння поділюваним середовищем у мережі Token Ring обмежується *часом утримання маркера* (*token holding time*), після закінчення якого станція зобов'язана припинити передачу власних даних (поточний кадр дозволяється завершити) і передати маркер далі по кільцю. Станція може встигнути передати за час утримання маркера один чи кілька кадрів залежно від розміру кадрів і величини часу утримання маркера. Звичайний час утримання маркера за замовчуванням дорівнює 10 мс, а максимальний розмір кадру в стандарті 802.5 не визначений. Для мереж 4 Мбіт/с він зазвичай дорівнює 4 Кбайт, а для мереж 16 Мбіт/с – 16 Кбайт. Це пов'язано з тим, що за час утримання маркера станція повинна встигнути передати хоча б один кадр. При швидкості 4 Мбіт/с за час 10 мс можна передати 5000 байт, а при швидкості 16 Мбіт/с – відповідно 20 000 байт. Максимальні розміри кадру обрані з деяким запасом.

У мережах Token Ring 16 Мбіт/с використовується також трохи інший алгоритм доступу до кільця, який називається алгоритмом *раннього звільнення маркера* (*Early Token Release*). Відповідно до нього станція

передає маркер доступу наступної станції одразу ж після закінчення передачі останнього біта кадру, не чекаючи повернення по кільцю цього кадру з бітом підтвердження прийому. У цьому випадку пропускна здатність кільця використовується більш ефективно, тому що по кільцю одночасно просуваються кадри декількох станцій. Проте свої кадри в кожен момент часу може генерувати тільки одна станція — та, котра в даний момент володіє маркером доступу. Інші станції в цей час тільки повторюють чужі кадри, так що принцип поділу кільця в часі зберігається, прискорюється тільки процедура передачі володіння кільцем.

Для різних видів повідомлень, переданим кадрам, можуть призначатися різні *пріоритети*: від **0 (нижчий)** до **7 (вищий)**. Рішення про пріоритет конкретного кадру приймає передавальна станція (протокол Token Ring одержує цей параметр через міжрівневі інтерфейси від протоколів верхнього рівня, наприклад прикладного). Маркер також завжди має деякий рівень поточного пріоритету. Станція має право захопити переданий їй маркер тільки в тому випадку, якщо пріоритет кадру, що вона хоче передати, вище (чи дорівнює) пріоритету маркера. Інакше станція зобов'язана передати маркер наступної по кільцю станції.

За наявність у мережі маркера, причому єдиної його копії, відповідає активний монітор. Якщо активний монітор не одержує маркер протягом тривалого часу (наприклад, 2,6 с), то він породжує новий маркер.

Запитання для самоперевірки:

1. Сімейство стандартів Ethernet. Історія, особливості, характеристики.

2. Методи доступу в комп'ютерних мережах. Метод передачі маркера (токену).

3. За якими характеристиками зазвичай відрізняються стандарти сімейства Ethernet?

4. Які рівні еталонної моделі OSI визначають протоколи Ethernet?

Прямий кабель Ethernet: найбільш поширений тип мережевого кабелю; здебільшого використовується для підключення вузла до комутатора й комутатора до маршрутизатора.

Перехресний кабель (Crossover) Ethernet: використовується для з'єднання однотипних пристроїв, наприклад для підключення комутатора до комутатора, комп'ютера до комп'ютера або маршрутизатора до маршрутизатора.

Консольний кабель (Rollover): фірмовий кабель Cisco; використовується для підключення робочої станції до консольного порту маршрутизатора або комутатора.

Неправильне використання перехресного або прямого кабелю між пристроями не зашкодить їм, але зв'язок і взаємодія між ними будуть неможливі. Подібна помилка часто відбувається в ході практичних занять. Тому за відсутності зв'язку між пристроями передусім потрібно перевірити правильність підключення.

7.2 Властивості оптоволоконних кабелів

Оптоволоконні кабелі дозволяють передавати дані на великі відстані й з більш високою пропускною здатністю, ніж інші засоби мережевого підключення. На відміну від мідних проводів оптоволоконний кабель дозволяє передавати сигнали з більш низьким загасанням. Такий кабель також абсолютно несприйнятливий до впливу електромагнітних і радіочастотних перешкод. Оптичні кабелі зазвичай використовуються для з'єднання мережевих пристроїв один з одним.

Оптичне волокно – це гнучка, дуже тонка і прозора нитка з хімічно чистого скла товщиною трохи більше за людську волосину. Для передачі по оптоволоконному кабелю біти кодуються за допомогою світлових імпульсів. Оптоволоконний кабель діє як світловод, що забезпечує передачу світлового сигналу між двома кінцями кабелю з мінімальними втратами.

технічні вимоги до прокладання кабелю в локальних мережах. Це найбільш часто вживаний у цій сфері стандарт. У ньому, зокрема, визначено такі елементи:

- типи кабелів;
- довжина кабелів;
- роз'єми;
- роз'єми кабелів;
- методи тестування кабелів.

Електричні характеристики мідних кабелів визначаються Інститутом інженерів із електротехніки та електроніки (IEEE). IEEE класифікує кабелі UTP згідно з їхніми характеристиками. Кабелі поділяються на категорії відповідно до можливої швидкістю передачі даних по ним. Наприклад, кабель категорії 5 (Cat5) зазвичай використовується в мережах Fast Ethernet 100BASE-TX. До інших категорій кабелів відносяться: розширена категорія 5 (Cat 5e), категорія 6 (Cat6) і категорія 6a.

Кабелі більш високих категорій призначені для передачі даних на більш високій швидкості. У результаті розробки і впровадження нових технологій Ethernet для гігабітних швидкостей передачі даних нині мінімально допустимим типом кабелів є Cat5e, а для прокладки нових мереж рекомендується Cat6.

Деякі виробники випускають кабелі з характеристиками вище, ніж у кабелів категорії 6a TIA / EIA, і позиціонують їх як кабелі категорії 7.

Типи кабелів UTP

У різних ситуаціях можуть застосовуватися різні схеми підключення проводів кабелів UTP до роз'ємів. Іншими словами, окремі дроти кабелю можуть підключатися до різних груп контактів роз'єму RJ-45 в різному порядку.

Нижче описані основні типи кабелів, які можна отримати, застосовуючи різний порядок підключення проводів.

7. СЕРЕДОВИЩА ПЕРЕДАЧІ ДАНИХ

7.1 Мідний кабель

Характеристики мідних кабелів

Основні причини використання мідних кабелів у мережах – їх невисока вартість, простота монтажу та низький електричний опір. Однак при передачі сигналів по мідних кабелях можуть бути встановлені обмеження по дальності передачі й завадостійкості.

Дані по мідних кабелях передаються у вигляді електричних імпульсів. Приймач у мережевому інтерфейсі цільового пристрою повинен отримати такий сигнал, який можна легко декодувати для відновлення відправленого сигналу. Однак чим більше дальність передачі сигналу, тим сильніше він спотворюється. Це називається загасанням сигналів. Тому для всіх засобів підключення на основі мідних кабелів у стандартах встановлені суворі обмеження на дальність передачі.

Тимчасові характеристики і значення напруги електричних імпульсів також схильні до впливу джерел перешкод, що наведені нижче.

Електромагнітні перешкоди (ЕМП) або радіочастотні перешкоди (РЧП). Сигнали ЕМП і РЧП можуть спотворювати і пошкоджувати сигнали даних, що передаються по мідному кабелю. Потенційними джерелами ЕМП та РЧП є джерела радіочастотного випромінювання та електромагнітні пристрої, наприклад флуоресцентні лампи або електродвигуни (Рис.18).

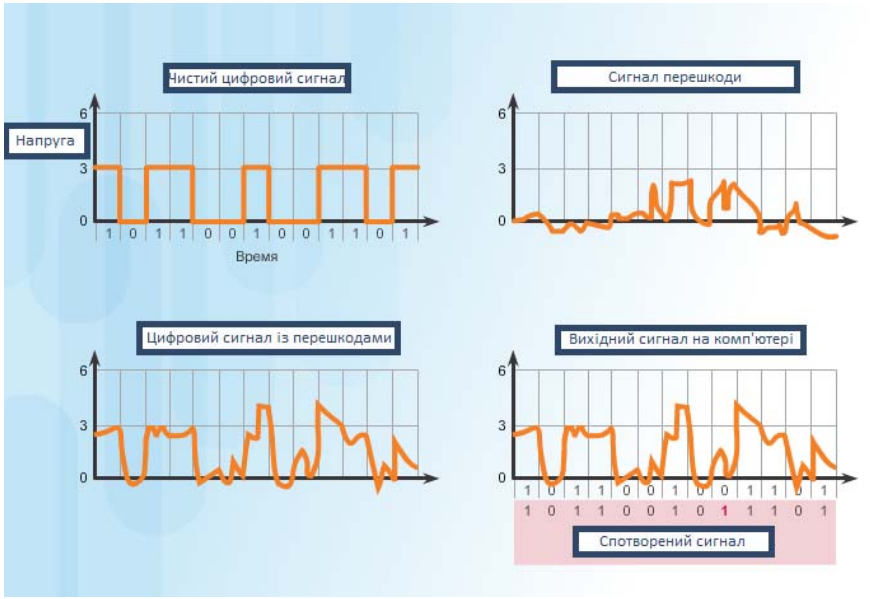

Рис.18. Вплив ЕМП на передавання сигналу

Перехідні перешкоди. Це перешкоди, викликані впливом електричних або магнітних полів сигналу одного кабелю на сигнал сусіднього кабелю. У телефонних каналах перехідні перешкоди можуть призвести до часткової чутності сторонньої розмови по сусідньому каналу. Причина цього в тому, що при проходженні електричного струму по дроту навколо нього створюється слабке кругове магнітне поле, яке може впливати на сусідній провід.

Для захисту від шкідливого впливу ЕМП та РЧП деякі типи мідних кабелів обгорнуті металевою екранною оболонкою. Такі кабелі вимагають належного заземлення.

У деяких типах мідних кабелів дроти кожної пари скручені між собою, що забезпечує ефективне «придушення» перехідних перешкод.

Захищеність мідного кабелю від електронних перешкод можна також підвищити за рахунок заходів, описаних нижче.

1. Вибір типу і категорії кабелю, найбільш придатних для цього мережевого оточення.

У кабелях UTP не передбачено екранування для захисту від ЕМП і РЧП. Замість цього для обмеження негативного впливу перехідних перешкод застосовуються такі рішення, свого часу знайдені проектувальниками кабелів:

Взаємокомпенсування. Проектувальники об'єднують дроти одного електричного кола в пару. При розміщенні двох проводів одного електричного кола в безпосередній близькості один до одного магнітні поля навколо них протилежні одна одній. Тому два магнітних поля взаємно компенсуються, а також забезпечується компенсація впливу зовнішніх ЕМП і РЧП.

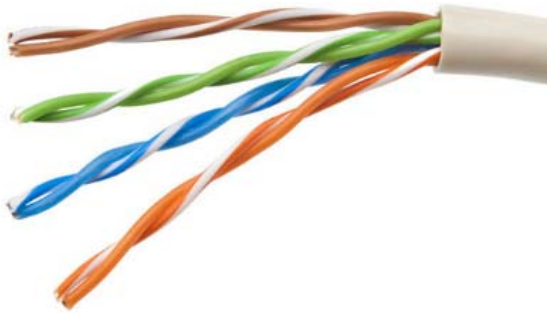

Рис.21. Кабель UTP

Різний крок витків у парах. Для підвищення ефекту придушення перешкод проектувальники використовують різний крок витків у сусідніх парах одного кабелю. Кабелі UTP повинні точно відповідати специфікаціям, який регламентує допустиму кількість витків на 1 метр кабелю. Зверніть увагу, що на Рис.21 помаранчевий і біло-помаранчевий дроти скручені рідше, ніж синій і біло-синій. Пари різних кольорів скручені з різним кроком скрутки.

У кабелях UTP захист від спотворень сигналу й ефективне самоекранування пар проводів здійснюються виключно завдяки ефекту придушення перешкод, що досягається скручуванням дротів у пари.

Стандарти прокладки кабелів UTP

Кабелі UTP відповідають вимогам стандартів, спільно вироблених організаціями TIA і EIA. Зокрема, у стандарті TIA / EIA-568A описуються

7.1.4 Безпека мідних кабелів

При роботі з мідними кабелями всіх трьох типів необхідно враховувати їхню потенційну пожежонебезпеку та електронебезпеку.

Їх пожежонебезпека зумовлена можливим загорянням ізоляції та оболонок або токсичністю, що виділяється під час їх нагрівання або горіння. Служби або організації технічного нагляду за будівництвом можуть встановлювати відповідні стандарти безпеки для прокладки кабелів і підключення обладнання.

Електронебезпека мідних кабелів зумовлена їхньою здатністю проводити електричні струми в непередбачених випадках. При цьому персонал і обладнання піддаються різним небезпекам. Наприклад, струм від несправного мережевого пристрою може надходити на корпуси інших мережевих пристроїв. Крім того, при з'єднанні пристроїв, джерела живлення яких мають різні електричні потенціали, на мережевих кабелях можуть створюватися небажані рівні напруги. Такі ситуації можливі у разі використання мідних кабелів для з'єднання мереж у різних будівлях або на різних поверхах будівлі, що мають незалежні джерела електропостачання. Крім того, мідні кабелі можуть проводити напруги, викликані потраплянням блискавок у мережеві пристрої.

Ці небажані напруги та струми можуть пошкоджувати мережеві пристрої й підключені до них комп'ютери, а також травмувати персонал. Тому, щоб уникнути нещасних випадків і пошкодження обладнання при монтажі мідних кабелів, необхідно суворо дотримуватись будівельних норм і правил.

Властивості кабелів UTP

Кабель на основі неекранованої кручений пари (UTP), який використовується як засіб мережевого підключення, складається з чотирьох скручених пар мідних провідників із кольоровим маркуванням, укладених у загальну гнучку пластикову оболонку. Завдяки невеликому діаметру кабелю його зручно монтувати.

2. Проектування кабельної інфраструктури будівлі з обходом відомих і можливих джерел електромагнітних полів.
3. Дотримання правил прокладки і підключення кабелів при монтажі.

7.1.1 Типи мідних кабелів

Для побудови мереж використовується три основних типи мідних кабелів (Рис.19):

- неекранована кручена(вита) пара (UTP);
- екранована кручена(вита) пара (STP);
- коаксіальні кабелі;

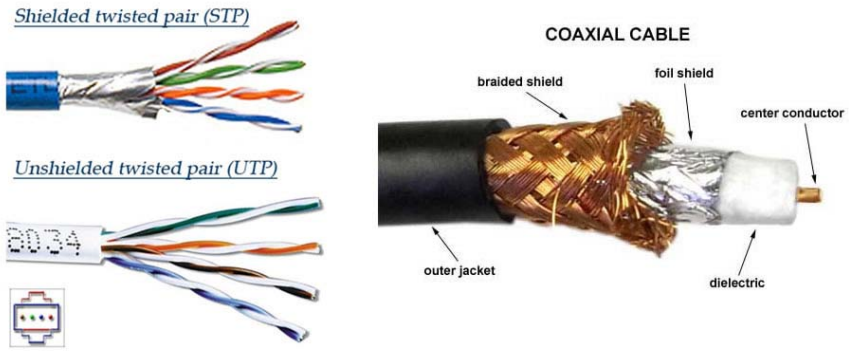

Рис.19. Типи мідних кабелів

Ці кабелі використовуються для з'єднання вузлів локальної мережі і підключення пристроїв мережевої інфраструктури, таких як комутатори, маршрутизатори й бездротові точки доступу. У стандартах фізичного рівня описані вимоги до кабелів для кожного з типів з'єднання і відповідних ним пристроїв.

Різні стандарти фізичного рівня вимагають використання різних роз'ємів. Ці стандарти визначають фізичні розміри й допустимі електричні характеристики кожного типу роз'ємів. У засобах мережевого підключення для забезпечення простого підключення і відключення використовуються модульні гнізда і штекери. При цьому фізичні роз'єми одного типу можуть

використовуватися для декількох типів підключень. Наприклад, роз'єм RJ-45 широко використовується в локальних мережах (LAN) з одним типом засобів підключення, а в деяких глобальних мережах (WAN) – з іншим типом.

7.1.2 Вита пара

Кабель на основі неекранованої крученої пари

Кабелі на основі неекранованої крученої пари (UTP) є найпоширенішим засобом підключення. Кабелі UTP з роз'ємами RJ-45 використовуються для з'єднання вузлів із проміжними мережевими пристроями, такими як комутатори і маршрутизатори.

Кабель UTP для локальних мереж складається з чотирьох скручених пар провідників з кольоровим маркуванням, які укладені в загальну гнучку пластикову оболонку, що захищає кабель від незначних пошкоджень. Скручування провідників знижує вплив перешкод від інших провідників.

Кабель на основі екранованої кручений пари

Кабелі на основі екранованої крученої пари (STP) краще захищені від перешкод, ніж кабелі UTP. Але при цьому вони значно дорожчі, і їх складніше монтувати. Як і для кабелів типу UTP, для кабелів STP використовується роз'єм RJ-45.

У кабелях STP застосовується екранування для захисту від ЕМП і РЧП та скручування провідників для захисту від перехідних перешкод. Для отримання найбільш повного ефекту від екранування кабелі STP оснащуються спеціальними екранованими роз'ємами для ліній передачі даних STP. Якщо такий кабель не заземлити належним чином, то екран може діяти як антена і приймати небажані сигнали.

7.1.3 Коаксіальний кабель

Коаксіальний кабель називається так тому, що він містить два співвісних провідника (Рис.20).

Рис.20. Структура коаксіального кабелю

Як показано на рисунку 1.20, коаксіальний кабель складається з таких елементів.

1. Мідний провідник, який використовується для передачі електричних сигналів.

2. Шар гнучкої пластикової ізоляції навколо мідного провідника.

3. Мідна оплітка або металева фольга, що розташовується навколо шару ізолюючого матеріалу й виступає другим проводом у ланцюзі, а також екраном для внутрішнього провідника. Цей другий шар, названий екраном, також знижує рівень зовнішніх електромагнітних завад.

4. Зовні кабель покритий кабельної оболонкою для захисту від незначних фізичних ушкоджень.

Хоча в сучасних мережах Ethernet коаксіальні кабелі фактично поступилися місцем кабелям UTP, кабелі коаксіальної структури все ще використовуються в деяких сферах.

Устаткування бездротових мереж. Коаксіальні кабелі використовуються для підключення антен до пристроїв бездротового зв'язку. Коаксіальний кабель забезпечує передачу енергії радіочастотних сигналів між антенами й радіоустаткуванням.

Мережі кабельного телебачення з доступом в Інтернет. Оператори кабельних мереж пропонують своїм клієнтам доступ в Інтернет, частково замінюючи коаксіальні кабелі й відповідні підсилювальні елементи на оптоволоконні кабелі. Однак з'єднання в приміщеннях клієнтів, як і раніше, виконуються коаксіальними кабелями.