

Лабораторна робота №2

Основи побудови комп'ютерної мережі

Мета лабораторної роботи – ознайомитися з основними поняттями комп'ютерних мереж, з видами топологій, класифікацією по області дії, за призначенням, типом комп'ютерів, які входять до складу комп'ютерної мережі, за територіальним розташуванням, за типом функціональної взаємодії та набуття навиків у побудові мережі та її налаштуванні.

Основні питання які розглядаються у лабораторній роботі:

1. Фізичне підключення комп'ютерів до мережі

1.1. Топологія мереж.

1.2. Використовувані кабелі.

1.3. Мережеве обладнання і адаптери.

1.4. Схеми розводки патч-кабелю (комутаційний шнур, комутаційний кабель) для мереж 10/100 Мбіт/с і 1000 Мбіт/с.

2. Адресація комп'ютерів в мережі

2.1. Поняття про стек протоколів TCP/IP.

2.2. Три основні класи IP – адрес.

2.3. Номер мережі і номер вузла в IP–мережі.

1. Теоретичні відомості

Топологія мережі

Існує кілька основних топологій мережі, тобто фізичного розміщення комп'ютерів, кабелів та інших компонентів:

Шина (*bus*) – комп'ютери підключені уздовж одного кабелю (було розглянуто в лекції).

Зірка (*star*) – комп'ютери підключені до сегментів кабелю, що виходять з однієї точки, або концентратора (*hub*) (рис. 1).

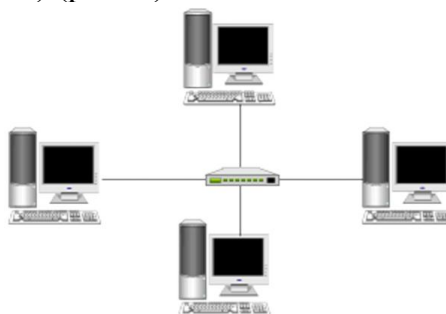


Рис. 1 – Топологія типу зірка

Кільце (*ring*) – комп'ютери підключені до кабелю, замкнутому в кільце (рис. 2). В даний час часто використовуються комбіновані топології.



Рис. 2 – Фізична топологія кільце

Перераховані топології є базовими. Більшість локальних обчислювальних мереж, що створюються в різних організаціях, мають більш складну структуру і є різними варіантами комбінування вищезазначених топологій.

Мережеві адаптери

Комп'ютери підключається до мережі за допомогою мережевої карти, яка встановлюється в один з вільних слотів материнської плати. Мережеві карти є посередниками між комп'ютером і мережею і передають дані по системі шин до CPU і RAM сервера або робочої станції. Більшість мережевих карт мають гніздо для установки мікросхеми постійно запам'ятовуючих пристроїв віддаленого завантаження (Remote Boot ROM), що необхідно для бездисккових станцій. Випускалися і випускаються 16- і 32-розрядні мережеві карти для різних комп'ютерних архітектур: ISA, EISA, PCI, MCA.

На зовнішній стороні карти є роз'єми для підключення кабелів:

BNC – роз'єм для підключення тонкого коаксіального кабелю Ethernet (RG-58) (мережеве середовище 10Base2);

AUI – роз'єм для підключення товстого кабелю Ethernet (мережеве середовище 10Base5);

RJ-45 (UTP) – роз'єм для підключення крученої пари (мережеве середовище 10BaseT, 100BaseTX);

ST – роз'єм для підключення оптоволоконного кабелю (мережеве середовище 10BaseFX, 100BaseFX).

Кабелі

У мережі дані передаються по кабелях, що з'єднує окремі комп'ютери по-різному в залежності від топології і виду мережі (Ethernet, Arcnet, Token Ring).

Вита пара це два ізольованих мідних дроти, скручених між собою. Для Ethernet використовується 8-жильний кабель, тобто що складається фізично з 4-х кручених пар. При цьому розрізняють неекранований (UTP) і екранований (STP) кабелі. Роз'єм відповідає стандарту RJ-45.

Коаксіальний кабель складається з центрального провідника (одножильного або багатожильного) і зовнішньої екранує обплетення. Для Ethernet застосовують кабель з хвильовим опором 50 Ом і рекомендується використовувати кабель RG-58.

Максимальна довжина сегменту кабелю

Вита пара – 100 м.

Тонкий коаксіальний кабель – 185 м (максимальна довжина кабелів всієї мережі при використанні додаткового обладнання може досягати 925 м).



Рис. 3 – Ethernet за допомогою коаксіального кабелю

Поняття про стек протоколів TCP

Так як стек TCP/IP був розроблений до появи моделі взаємодії відкритих систем ISO TC/ OSI, він також має багаторівневу структуру, відповідність рівнів стека моделі OSI досить умовно.

Структура протоколів TCP/IP приведена на рис. 4. Протоколи TCP/IP поділяються на 4 рівня.

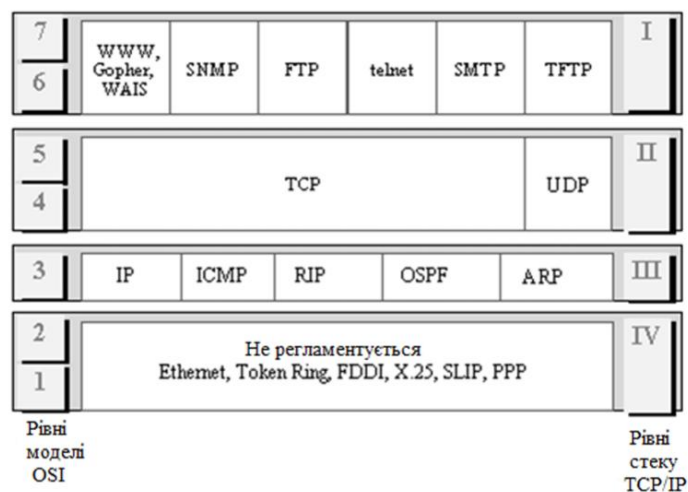


Рис. 4 – Структура протоколів TCP/IP

Найнижчий (рівень IV) відповідає фізичному і каналному рівням моделі OSI. Цей рівень в протоколах TCP/IP не регламентується, але підтримує всі популярні стандарти фізичного і каналного рівня: для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, для глобальних мереж – протоколи з'єднань "точка-точка" SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X.25, *frame relay* (протокол каналного рівня мережевої моделі OSI). Розроблено також спеціальна специфікація, що визначає використання технології ATM як транспорт каналного рівня. Звичайно при появі нової технології локальних або глобальних мереж вона швидко включається в стек TCP/IP за рахунок розробки відповідного RFC (*Request for*

Comments – документ із серії пронумерованих інформаційних документів Інтернету, що містить технічні специфікації), що визначає метод інкапсуляції пакетів IP у її кадри.

Наступний рівень (рівень III) – це рівень міжмережевої взаємодії, який займається передачею пакетів з використанням різних транспортних технологій локальних мереж, територіальних мереж, ліній спеціального зв'язку і т. п. В якості основного протоколу мережевого рівня (в термінах моделі OSI) в стеку використовується протокол IP, який спочатку проектувався як протокол передачі пакетів в складових 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 ощадливо витрачаючи пропускну здатність низькошвидкісних ліній зв'язку. Протокол IP є дейтаграмним протоколом, тобто він не гарантує доставку пакетів до вузла призначення, але намагається це зробити. 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 міжмережових керуючих повідомлень ICMP (Internet Control Message Protocol). Останній протокол призначений для обміну інформацією про помилки між маршрутизаторами мережі і вузлом – джерелом пакета. За допомогою спеціальних пакетів ICMP повідомляється про неможливість доставки пакета, про перевищення часу життя або тривалості зборки пакета з фрагментів, про аномальні величини параметрів, про зміну маршруту пересилання і типу обслуговування, про стан системи і т.п.

Наступний рівень (рівень II) називається основним. На цьому рівні функціонують протокол управління передачею TCP (*Transmission Control Protocol*) і протокол дейтаграм користувача UDP (*User Datagram Protocol*).

Протокол TCP забезпечує надійну передачу повідомлень між віддаленими прикладними процесами за рахунок утворення віртуальних з'єднань. Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним способом, як і IP, і виконує тільки функції сполучної ланки між мережним протоколом і численними прикладними процесами.

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, гіпертекстові сервіси доступу до вилученої інформації, такі як WWW і багато інших.

Протокол пересилки файлів FTP (File Transfer Protocol) реалізує віддалений доступ до файлу. Для того, щоб забезпечити надійну передачу, FTP використовує в якості транспорту протокол з встановленням з'єднань – TCP. Крім пересилки файлів протокол FTP пропонує й інші послуги. Так, користувачеві надається можливість інтерактивної роботи з віддаленою машиною, наприклад, він може роздрукувати вміст її каталогів. Нарешті, FTP виконує аутентифікацію користувачів. Перш, ніж

отримати доступ до файлу, відповідно до протоколу користувачі повинні повідомити своє ім'я і пароль. Для доступу до публічних каталогів FTP-архівів Internet пароліна аутентифікації не потрібно, і її обходять за рахунок використання для такого доступу обумовленого імені користувача *Anonymous*.

У стеці TCP/IP протокол FTP пропонує найбільш широкий набір послуг для роботи з файлами, проте він є і найскладнішим для програмування. Додатки, яким не потрібні всі можливості FTP, можуть використовувати інший, більш економічний протокол – найпростіший протокол пересилки файлів TFTP (*Trivial File Transfer Protocol*). Цей протокол реалізує тільки передачу файлів, причому як транспорт використовується більш простий, ніж TCP, протокол без встановлення з'єднання – UDP.

Протокол **telnet** забезпечує передачу потоку байтів між процесами, а також між процесом і терміналом. Найбільш часто цей протокол використовується для емуляції терміналу віддаленого комп'ютера. При використанні сервісу **telnet** користувач фактично керує віддаленим комп'ютером так само, як і локальний користувач, тому такий вид доступу вимагає гарного захисту. Тому сервери **telnet** завжди використовують як мінімум аутентифікацію за паролем, а іноді і більш потужні засоби захисту, наприклад, систему Kerberos.

Протокол SNMP (*Simple Network Management Protocol*) використовується для організації мережевого управління

Форми запису IP-адреси

IP-адреса має довжину 4 байта (32 біта) і складається з двох логічних частин – номера мережі і номера вузла в мережі наприклад: 128.10.2.30 IP-адреса може бути представлена в двійковому форматі: 10000000 00001010 00000010 00011110 .

А також в шістнадцятковому форматі: 80.0A.92.10.

Запис адреси не передбачає спеціального розмежувального знаку між номером мережі і номером вузла. Один з підходів розмежування номера мережі і вузла заснований на використанні маски.

В даному випадку маска – це число, яке використовується в парі з IP-адресою; двійковий запис маски містить послідовність одиниць в тих розрядах, які повинні в IP-адресу інтерпретуватися як номер мережі. Оскільки номер мережі є цілісною частиною адреси, одиниці в масці також повинні представляти безперервну послідовність. Границя між послідовністю одиниць і послідовністю нулів в масці відповідає границі між номером мережі і номером вузла в IP-адресу. При такому підході адресний простір можна уявити як сукупність безлічі мереж різного розміру.

Приклад:

	№ мережі	№ вузлу
IP-адрес 129.64.134.5	10000001. 01000000. 1	0000110. 00000101
Маска 255.255.128.0	11111111. 11111111. 1	0000000. 0000000

Номер мережі 129.64.128.0, номер вузла 0.0.6.5

Традиційний спосіб розмежування номера мережі і вузла полягає в використанні класів. Цей спосіб є компроміс по відношенню до двох вище описаних: розміри

мереж хоча і не є довільними, як при використанні масок, але і не є однаковими, як при встановленні фіксованих меж. Вводиться кілька класів мереж, і для кожного класу визначені свої розміри.

Класи IP-адрес

Традиційна схема ділення IP-адреси на номер мережі і номер вузла заснована на понятті класу, який визначається значеннями декількох перших бітів адреси. Саме тому, що перший байт адреси 185.23.44.206 потрапляє в діапазон 128 191, ми можемо сказати, що ця адреса відноситься до класу **В**, а значить, номером мережі є перші два байту IP-адреси, доповнені двома нульовими байтами – 185.23.0.0, а номером вузла – два молодші байти, доповнені з початку двома нульовими байтами – 0.0.44.206.

Приналежність адреси до класу визначається значеннями перших бітів адреси. різних класів. На рис.5 показана структура IP-адрес різних класів.



Рис. 5 Структура IP-адреси

Якщо адреса починається з 0, то ця адреса відноситься до класу **А**, в якому під номер мережі відводиться один байт, а решта три байти інтерпретуються як номер вузла в мережі. Мережі, які мають номери в діапазоні від 1 (00000001) до 126 (01111110), називаються мережами класу **А**. (Номер 0 не використовується, а номер 127 зарезервований для спеціальних цілей). Мереж класу **А** небагато, зате кількість вузлів в них може досягати 2^{24} , тобто 16 777 216 вузлів.

Якщо перші два біти адреси рівні 10, то адреса належить до класу **В**. В адресах класу **В** під номер мережі і під номер вузла відводиться по два байту. Мережі, які мають номери в діапазоні від 128.0 (1000000000000000) до 191.255 (10111111 11111111), називаються мережами класу **В**.

Таким чином, мереж класу **В** більше, ніж мереж класу **А**, але розміри їх менше, максимальна кількість вузлів в них випадках становить 2^{16} (65 536).

Якщо адреса починається з послідовності бітів 110, то це адреса класу **С**. У цьому випадку під номер мережі відводиться 24 біти, а під номер вузла – 8 біт. Мережі класу **С** найбільш поширені, але число вузлів в них обмежене значенням 2^8 (256) вузлів. Ще два класи адрес **Д** і **Е** не пов'язані безпосередньо з мережами. Характеристики адрес різного класу наведено в таблиці.

Клас	Перші біти	Найменший номер мережі	Найбільший номер мережі	Максимальна кількість вузлів в мережі
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^8
D	1110	224.0.0.0	239.255.255.255	<i>Multicast</i>
E	11110	240.0.0.0	247.255.255.255	<i>Зарезервовано</i>

Великі мережі отримують адреси класу А, середні – класу В, а невеликі – класу С.

Особливі IP-адреси

У протоколі IP існує кілька угод про особливу інтерпретацію IP-адрес.

1. Якщо весь *IP-адреса* складається тільки з двійкових нулів, то він позначає адресу того вузла, який згенерував цей пакет (цей режим використовується тільки в деяких повідомленнях ICMP).

2. Якщо в полі номеру мережі розміщено тільки нулі, то за замовчуванням вважається, що вузол призначення належить тій же самій мережі, що і вузол, який відправив пакет.

3. Якщо всі двійкові розряди *IP-адреси* рівні 1, то пакет з такою адресою призначення повинен розсилатися всім вузлам, що знаходяться в тій же мережі, що й джерело цього пакета. Така розсилка називається обмеженим широкомовним повідомленням (*limited broadcast*). Обмеженість в даному випадку означає, що пакет не вийде за межі маршрутизатора ні за яких умов.

4. Якщо в полі номера вузла призначення стоять тільки одиниці, то пакет, що має таку адресу, розсилається всім вузлам мережі із заданим номером мережі.

Наприклад, пакет з адресою 192.190.21.255 доставляється всім вузлам мережі 192.190.21.0. Така розсилка називається широкомовним повідомленням (*broadcast*).

Спеціальні адреси, що складаються з послідовностей нулів, можуть бути використані тільки в якості адреси відправника, а адреси, що складаються з послідовностей одиниць, – тільки в якості адреси одержувача. При призначенні адрес кінцевим вузлам і маршрутизаторам необхідно враховувати ті обмеження, які вносяться особливим призначенням деяких IP-адрес.

Так, ні номер мережі, ні номер вузла не може складатися тільки з одних двійкових одиниць або тільки з одних двійкових нулів. Звідси випливає, що максимальна кількість вузлів, наведена в таблиці для мереж кожного класу, на практиці має бути зменшена на 2. Наприклад, в адресах класу **C** під номер вузла відводиться 8 біт, які дозволяють задати 256 номерів: від 0 до 255. Однак на практиці максимальне число вузлів в мережі класу **C** не може перевищувати 254, так як адреси 0 і 255 мають спеціальне призначення. З цих же міркувань

слідуює, що кінцевий вузол не може мати адресу типу 98.255.255.255, оскільки номер вузла в цій адресі класу *A* складається з одних двійкових одиниць.

Особливий сенс має IP-адреса, перший байт якої дорівнює 127. Він використовується для тестування програм і взаємодії процесів в межах однієї машини. Коли програма посилає дані за IP-адресою 127.0.0.1, то утворюється “петля”. Дані не передаються по мережі, а повертаються модулям верхнього рівня, як тільки що прийняті. Тому в IP-мережі забороняється привласнювати мережним інтерфейсам IP-адреси, що починаються з числа 127. Ця електронна адреса має назву *loopback*. Можна віднести адресу 127.0.0.0 до внутрішньої мережі модуля маршрутизації вузла, а адресу 127.0.0.1 – до адреси цього модуля на внутрішній мережі. Насправді будь-яка адреса мережі 127.0.0.0 слугить для позначення свого модуля маршрутизації, а не тільки 127.0.0.1, наприклад 127.0.0.3.

2. Завдання

1. Побудувати мережу за допомогою даних таблиці

№ з/п	Кількість робочих станцій (PC0.....PCN)	Кількість мережних пристроїв	Топологія мережі	Клас мережі
1	8	1	Шина	A
2	9	2	Шина	B
3	7	2	Шина	A
4	8	1	Зірка	B
5	9	2	Зірка	C
6	16	2	Шина	C
7	15	1	Зірка	A
8	11	1	Шина	B
9	5	2	Зірка	C
10	15	3	Шина	B
11	6	1	Зірка	C
12	12	3	Зірка	C
13	12	2	Шина	B
14	5	3	Зірка	C
15	15	3	Шина	B
16	6	2	Зірка	C
17	12	4	Зірка	C
18	13	3	Шина	B
19	7	2	Зірка	C
20	10	3	Шина	C
21	6	2	Шина	A
22	7	2	Зірка	B

Примітка.

IP – адреса шлюзу вибирати виходячи з першої адреси вузла обраної мережі.

IP – адрес DNS сервера 172.20.0.149

Пояснення Маска 255.255.255.240 відповідає підмережі з 16 адресами. Перша адреса – номер мережі, остання – широкомовна. Приклад 192.168.100.0 і 192.168.100.15 і 192.168.100.1-192.168.100.14. Або може бути мережа 192.168.100.64-192.168.100.79. Перша і остання – спеціальна адреса, проміжна – адреса комп'ютерів.

Маска 255.255.255.248 відповідає 8 адресам.

255.255.255.224 – 32 адреси.

DNS – визначає відповідність між іменами комп'ютерів і їх IP-адресами.

Шлюз – мережеве пристрій (комп'ютер) до якого надсилаються пакети з адресами призначення, які не належать даній мережі.

2. Присвоїти IP– адресу усім комп'ютерам мережі із врахуванням класу мережі у відповідності до таблиці: IP – адресу, маску мережі, адресу шлюзу, DNS сервера мережі відобразити на схемі мережі.

3. У відповідності до побудованої мережі представити наступні теоретичні матеріали

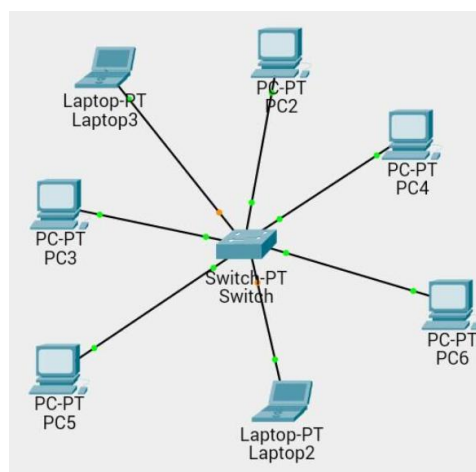
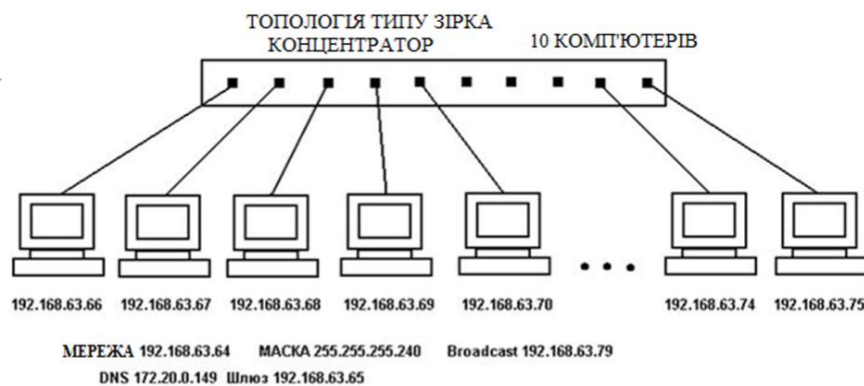
3.1. Характеристику використаної кабельної системи.

3.2. Описати переваги і недоліки використаної топології мережі.

3.3. Пояснити поняття класів IP – адрес (A, B, C)

3.4. Призначення маски мережі і розрахунок з її допомогою кількості вузлів проводити за умови дефіциту IP – адрес.

Приклади побудови мережі



4. Замість висновку відповісти на теоретичні питання.

1. Описати основні положення LAN, PAN, WAN?
2. Які ви знаєте види комп'ютерних мереж? Поясніть, чим вони різняться.
3. Назвіть характеристики каналів зв'язку.
4. Поясніть різницю між повторювачем та концентратором.