МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
БЕРДЯНСЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ

Віталій ХОМЕНКО
Максим ПАВЛЕНКО

КОМП'ЮТЕРНІ МЕРЕЖІ

НАВЧАЛЬНИЙ ПОСІБНИК

Рекомендовано
Міністерством освіти і науки,
молоді та спорту України як
навчальний посібник для
студентів вищих навчальних
закладів

Донецьк
Видавництво
ЛАНДОН–ХХІ

2011

УДК 004.7(075.8)
ББК 32.973.202(073)
Х 76

Рекомендовано Міністерством освіти і науки, молоді та спорту України як навчальний посібник для студентів вищих навчальних закладів (Лист 1/11 –10307 від 08.11.2011 р.)

Рецензенти:
Лазарєв М.І. - доктор педагогічних наук, професор, проректор з наукової роботи Української інженерно-педагогічної академії;
Спірін О.М. – доктор педагогічних наук, доцент, заступник директора з наукової роботи Інституту інформаційних технологій і засобів навчання АПН України;
Богданов І.Т. – доктор педагогічних наук, проректор з наукової роботи Бердянського державного педагогічного університету.

Друкується за рішенням Вченої ради Бердянського державного педагогічного університету (протокол №1 від 31 серпня 2011 р.)

Хоменко В.Г., Павленко М.П.

Х 76 Комп'ютерні мережі : Навчальний посібник / В. Г. Хоменко, М. П. Павленко. – Донецьк : ЛАНДОН-ХХІ, 2011. – 316 с.

ISBN

У посібнику розглянуто основі технології комп'ютерних мереж, подано основи проектування, розробки, налагодження та використання комп'ютерних мереж, які застосовуються у діяльності сучасних підприємств та установ.

Посібник розрахований на студентів інженерно-педагогічних спеціальностей комп'ютерного профілю вищих навчальних закладів. Він буде корисним також слухачам курсів підготовки та перепідготовки фахівців у галузі комп'ютерних мереж, а також усім, хто має намір оволодіти сучасними мережевими технологіями.

УДК 004.7(075.8)
ББК 32.973.202(073)

ISBN

ЗМІСТ

ЕОМ	Електронна обчислювальна машина
КМ	Комп'ютерна мережа
ЛОМ	Локальна обчислювальна мережа
ATM	Asynchronous Transfer Mode – мережі з асинхронним режимом передавання
BNC	Bayonet Neill-Concelman – байонетний з'єднувач
CMS	Content Management System система керування змістом
DARPA	Defense Advanced Research Projects Agency – агентство передових оборонних дослідницьких проектів
DNS	Domain Name System – система доменних імен
ECTS	European credits transfer system – Європейська кредитно-трансферна система
FTP	File Transfer Protocol – протокол передавання файлів
GPL	General Public License – універсальна загальнодоступна ліцензія
HTML	Hypertext Markup Language – мова розмітки гіпертексту
HTTP	Hyper Text Transfer Protocol – протокол передавання гіпертексту
IRC	Internet Relay Chat – Інтернет-чат, що ретранслюється
ISO/OSI	Open Systems Interconnection Reference Model – модель взаємозв'язку відкритих систем
LDAP	Lightweight Directory Access Protocol – полегшений протокол доступу до каталогу
MAC	Media Access Control – управління доступом до носія
NNTP	Network News Transfer Protocol – мережений протокол передавання новин
PHP	Hypertext Preprocessor – процесор гіпертексту
POP3	Post Office Protocol Version 3 – протокол поштового відділення, версія 3
RFC	Request for Comments – запит коментарів
SCORM	Sharable Content Object Reference Model – загальний зміст об'єкту довідкової моделі для дистанційної освіти
SMTP	Simple Mail Transfer Protocol – простий протокол передавання пошти
SNMP	Simple Network Management Protocol – простий протокол

	керування мережею
SSL	Secure Sockets Layer – протокол захищених сокетів
STP	Shielded twisted pair – екранована кручена пара
TCP/IP	Transmission Control Protocol / Internet Protocol – протокол управління передачею / міжмережевий протокол
UDP	User Datagram Protocol – протокол передавання датаграм
URL	Uniform Resource Locator – єдиний визначник місця знаходження ресурсу
UTP	Unshielded twisted pair – неекранована кручена пара
VPN	Virtual Private Network – віртуальна приватна мережа
WWW	World Wide Web – всесвітня павутина

ПЕРЕДМОВА

Комп'ютер став невід'ємною частиною сучасного життя. У час швидкісних комунікацій комп'ютерні мережі надають можливість кожному подорожувати світом, дистанційно здобувати освіту, знаходити детальні відповіді на проблемні питання в різних сферах діяльності. Основним призначенням комп'ютерної мережі є забезпечення простого, зручного і надійного доступу користувача до спільних розподілених ресурсів мережі та організації їх колективного використання з надійним захистом від несанкціонованого доступу, а також забезпечення зручними і надійними засобами передачі даних між користувачами мережі. В епоху загальної інформатизації великі обсяги інформації зберігаються, обробляються і передаються в локальних та глобальних комп'ютерних мережах. У локальних мережах створюються спільні бази даних для роботи користувачів. У глобальних мережах здійснюється формування єдиного наукового, економічного, соціального і культурного інформаційного простору.

Комп'ютерна мережа – програмно-апаратний комплекс, що включає в себе комп'ютери, принтери, комунікаційне устаткування, кабельну систему і мережеві операційні системи, призначений для передачі інформації, ефективного використання обчислювальних і комунікаційних ресурсів устаткування і програмного забезпечення.

У навчальному посібнику подано орієнтовний зміст дисципліни "Комп'ютерні мережі", яка включена до навчального плану підготовки бакалавра (напрям *0101 Педагогічна освіта*, напрям підготовки *6.010104 Професійна освіта. Комп'ютерні системи та мережі* та *6.010104 Професійна освіта. Обробка та захист інформації в комп'ютерних системах та мережах*) і має на меті забезпечити фахову підготовку викладачів дисциплін професійної та практичної підготовки відповідно до галузевого стандарту вищої освіти.

Основу навчального посібника складають теоретичні та практичні аспекти організації та функціонування комп'ютерних мереж, мета яких – забезпечення якісної професійної підготовки студентів і розвитку їх творчих здібностей.

Побудова навчального посібника за блочно-модульною схемою спрямована на максимальну індивідуалізацію процесу навчання. Структура навчального посібника надає студентам можливість навчатися індивідуально та орієнтуватися на певні рівні вимог щодо

засвоєння навчального матеріалу.

За освітньо-професійною програмою підготовки бакалавра на вивчення дисципліни "Комп'ютерні мережі" відводиться 144/4 навчальних годин/кредитів в одному семестрі.

Працювати з посібником треба в такій послідовності: опрацювати лекційний матеріал, відповісти на питання для самоперевірки, підготуватися до лабораторної роботи, виконати індивідуальну та самостійну роботу, ознайомитися з поданим зразком тестових завдань до модульного контролю.

Цей навчальний посібник буде корисним не лише студентам інженерно-педагогічних спеціальностей, але й усім тим, хто цікавиться комп'ютерними мережами.

ОПИС НАВЧАЛЬНОГО КУРСУ

Курс: бакалавр (денна форма навчання)	**Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень**	**Характеристика навчального курсу**
Кількість кредитів, відповідних ECTS: *4 кредити* Змістових модулів: *8* Загальна кількість годин: *144* Тижневих годин: *4*	Шифр та назва галузі знань: *0101 Педагогічна освіта* Шифр та назва напряму підготовки: *6.010104 Професійна освіта. Комп'ютерні системи та мережі, Професійна освіта. Обробка та захист інформації в комп'ютерних системах та мережах* Освітньо-кваліфікаційний рівень: *бакалавр*	Обов'язковий рік підготовки: *II* Семестр: *3* Лекції: *32 год.* Лабораторні: *32 год.* Самостійна та індивідуальна робота: *80 годин*

Метою курсу є формування професійних компетентностей майбутніх інженерів-педагогів щодо використання засобів комп'ютерних мереж, установлення та обслуговування мережевого обладнання, проектування та розробки локальних мереж, ознайомлення з методиками розробки технологічних процесів обробки даних у комп'ютерних мережах, налагодження та використання засобів глобальних мереж та Інтернет.

Завданням курсу є теоретична і практична підготовка студентів з питань:

– віднаходження оптимальних показників працездатності локальної комп'ютерної мережі та конфігурації мережевого обладнання;

– розробка та планування заходів щодо проектування та впровадження локальних мереж організацій;

– використання технології об'єднання різнорідних комп'ютерних мереж на основі протоколів мережевого рівня;

– упровадження програмних та апаратних рішень для

поліпшення адміністрування комп'ютерних мереж;

– запровадження та використання прикладних протоколів комп'ютерних мереж.

Студент повинен ***оволодіти знаннями*** щодо:

– основних принципів побудови стеків протоколів TCP/IP та ISO/OSI;

– позитивні та негативні характеристики стеків протоколів ISO/OSI та TCP/IP;

– проектування фізичного середовища комп'ютерної мережі;

– архітектури локальних мереж, побудованих з використанням різних протоколів канального рівня у відповідності до моделі ISO/OSI;

– побудови комп'ютерних мереж за вимогами канального рівня моделі ISO/OSI;

– принципів об'єднання комп'ютерних мереж на основі мережевого рівня;

– основ функціонування протоколу IP та TCP;

– принципів функціонування протоколів транспортного рівня;

– функціонування протоколів маршрутизації в комп'ютерних мережах;

– загальних принципів функціонування прикладних мережевих протоколів;

– функціонування та налагодження протоколу передавання гіпертексту;

– функціонування та використання протоколу передавання файлів;

– функціонування та застосування мережевих поштових протоколів;

– функціонування та застосування протоколів Telnet та SSH.

Студент повинен ***уміти:***

– встановлювати мережеві пристрої та обладнання;

– діагностувати несправності в роботі мережі на фізичному рівні моделі ISO/OSI;

– проектувати локальні комп'ютерні мережі з використанням стандартів Fast Ethernet, Ethernet та вимог до канального рівня моделі ISO/OSI;

– розподіляти та керувати мережевими адресами різних

типів;

– налагоджувати маршрутизацію відповідно до типу комп'ютерної мережі;

– діагностувати працездатність стеку протоколів TCP/IP;

– керувати та експлуатувати протоколи прикладного рівня HTTP та FTP;

– використовувати мережі поштові протоколи;

– розробляти програмні засоби для роботи з прикладними протоколами комп'ютерних мереж;

– використовувати протоколи Telnet та SSH для потреб управління мережею.

Структуру навчального курсу "Комп'ютерні мережі" складають вісім змістових модулів.

У першому змістовому модулі розглядаються предмет і завдання дисципліни "Комп'ютерні мережі", основи мереж передавання даних.

Другий змістовний модуль розглядає питання технологій фізичного рівня комп'ютерних мереж, а саме: лінії зв'язку, кодування та мультиплексування даних, безпровідна їх передача.

У третьому змістовому модулі визначено положення технологій локальних мереж, дана характеристика протоколів локальних мереж з використанням розподілюваного середовища Ethernet.

Четвертий змістовний модуль розкриває принципи реалізації комутації в мережі Ethernet, висвітлює інтелектуальні функції комутаторів.

У п'ятому змістовому модулі розглянуто практичний аспект реалізації адресації в стеку протоколів TCP/IP та протокол міжмережевої взаємодії.

Матеріал шостого модуля визначає сутність базових протоколів TCP/IP та транспортні послуги і технології глобальних мереж

У сьомому змістовому модулі розкрито питання архітектури поширених прикладних протоколів.

У восьмому змістовому модулі з'ясовано особливості використання прикладних протоколів в адмініструванні комп'ютерних мереж.

З метою закріплення теоретичного матеріалу програмою

передбачено проведення низки лабораторних робіт. У процесі навчання можливе коригування програми та рекомендованих лабораторних робіт, викликане можливими змінами сучасної системи освіти в Україні.

У викладанні курсу "Комп'ютерні мережі" реалізуються міждисциплінарні зв'язки з такими навчальними предметами, як: "Архітектура ЕОМ", "Цифрова техніка", "Вища математика", "Фізика", "Філософія", "Програмні обчислювальні системи", "Теорія захисту даних в обчислювальних системах та мережах", "Забезпечення безпеки корпоративних ресурсів в Інтернет та локальних мережах", "Обладнання обчислювальних центрів в системі освіти", "Системне програмування".

ЗМІСТОВИЙ МОДУЛЬ 1

Тема 1.1. Основи комп'ютерних мереж.

Предмет і завдання дисципліни "Комп'ютерні мережі". Взаємозв'язок її із суміжними дисциплінами. Еволюція комп'ютерних мереж: перші комп'ютерні мережі, конвергенція мереж. Загальні принципи побудови мереж: проста мережа з двох комп'ютерів, мережеве програмне забезпечення, фізична передача даних лініями зв'язку, проблеми зв'язку декількох комп'ютерів, узагальнене завдання комутації. Комутація каналів і пакетів: порівняння мереж з комутацією пакетів і каналів, Ethernet – приклад стандартної технології з комутацією пакетів.

Тема 1.2. Мережеві характеристики та класифікація комп'ютерних мереж.

Класифікація комп'ютерних мереж, узагальнена структура телекомунікаційної мережі, мережі операторів зв'язку, корпоративні мережі, Інтернет. Мережеві характеристики: типи характеристик, продуктивність, надійність, характеристики втрат пакетів, характеристики мережі постачальника послуг.

ЗМІСТОВИЙ МОДУЛЬ 2

Тема 2.1. Архітектура і стандартизація мереж.

Архітектура і стандартизація мереж: декомпозиція завдань мережевої взаємодії, модель OSI, стандартизація мереж, інформаційні і транспортні послуги.

Тема 2.2. Технології фізичного рівня комп'ютерних мереж.

Лінії зв'язку: класифікація ліній зв'язку, їх характеристики, типи кабелів. Кодування та мультиплексування даних: модуляція, дискретизація аналогових сигналів, методи кодування, виявлення і корекція помилок, мультиплексування і комутація. Первинні мережі.

ЗМІСТОВИЙ МОДУЛЬ 3

Тема 3.1. Загальна характеристика протоколів локальних мереж з використанням розподілюваного середовища Ethernet.

Загальна характеристика протоколів локальних мереж з використанням розподілюваного середовища Ethernet із швидкістю 10 Мбіт/с: MAC-адреси, формати кадрів технології Ethernet, доступ

до середовища і передача даних, виникнення колізії, час обороту і розпізнавання колізій, специфікації фізичного середовища, максимальна продуктивність мережі Ethernet.

Тема 3.2. Високошвидкісні технології локальних мереж.

Технологія Ethernet зі швидкістю передачі 100 Мбіт/с. Гігабітові й 10-гігабітові технології Ethernet. Технології Token Ring і FDDI. Безпровідні локальні мережі IEEE 802.11. Персональні мережі.

ЗМІСТОВИЙ МОДУЛЬ 4

Тема 4.1. Комутовані мережі Ethernet.

Міст як попередник і функціональний аналог комутатора: логічна структуризація мереж і мости, алгоритм прозорого мосту IEEE 802.1D, топологічні обмеження при застосуванні мостів в локальних мережах.

Тема 4.2. Інтелектуальні функції комутаторів.

Комутатори. Архітектура комутаторів. Обмеження комутаторів. Агрегація ліній зв'язку в локальних мережах: транки і логічні канали, боротьба з "розмноженням" пакетів, вибір порту. Фільтрація трафіку.

ЗМІСТОВИЙ МОДУЛЬ 5

Тема 5.1. Протокол міжмережевої взаємодії. Адресація в стеку протоколів TCP/IP.

Протокол IP стеку протоколів TCP/IP. Формат IP-пакету. Типи адрес стеку TCP/IP: локальні адреси, мережеві IP-адреси, доменні імена. Формат IP-адреси: класи IP-адрес, особливі IP-адреса, використання масок при IP-адресації. Порядок призначення IP-адрес: призначення адрес автономній мережі, централізований розподіл адрес, адресація і технологія CIDR.

Тема 5.2. Особливості адресації в стеку протоколів TCP/IP.

Маршрутизація з використанням масок, структуризація мережі масками однакової довжини, перегляд таблиць маршрутизації з урахуванням масок, використання масок змінної довжини, перекриття адресних просторів, CIDR.

ЗМІСТОВИЙ МОДУЛЬ 6

Тема 6.1. Базові транспортні протоколи стеку TCP/IP.

Протоколи транспортного рівня TCP і UDP: порти і сокети, протокол UDP і UDP-дейтаграми, протокол TCP і TCP-сегменти,

логічні з'єднання – основа надійності TCP, повторна передача і ковзне вікно, реалізація методу ковзного вікна в протоколі TCP, управління потоком.

Тема 6.2. Загальні властивості і класифікація протоколів маршрутизації.

Загальні властивості і класифікація протоколів маршрутизації: протокол RIP, протокол OSPF, протокол BGP. Протокол ICMP: утиліта traceroute, утиліта ping. Трансляція мережевих адрес: причини підміни адрес, традиційна технологія NAT, базова трансляція мережевих адрес, трансляція мережевих адрес і портів. Типи публічних послуг мереж операторів зв'язку. Багатошарова мережа оператора зв'язку. Технологія Frame Relay. Технологія ATM. Віртуальні приватні мережі. IP в глобальних мережах.

ЗМІСТОВИЙ МОДУЛЬ 7

Тема 7.1. Електронна пошта та протокол передачі файлів.

Електронна пошта: електронні листи, протокол SMTP, безпосередня взаємодія клієнта і сервера, схема з виділеним поштовим сервером, схема з двома поштовими серверами-посередниками, протоколи POP3 і IMAP. Основні модулі служби FTP: керуючий сеанс і сеанс передачі даних, команди взаємодії FTP-клієнта з FTP-сервером.

Тема 7.2. Протокол передачі гіпертекстових повідомлень.

Веб-служба: веб- і HTML-сторінки, веб-клієнт і веб-сервер, протокол HTTP, формат HTTP-повідомлень, динамічні веб-сторінки.

ЗМІСТОВИЙ МОДУЛЬ 8

Тема 8.1, 8.2. Прикладні протоколи в адмініструванні комп'ютерних мереж.

Система DNS: плоскі символьні імена, ієрархічні символьні імена, схема роботи DNS, зворотна зона. Стандарти і програмні реалізації віддаленого доступу. Мережевий протокол для реалізації текстового інтерфейсу мережею: опції, принтер і клавіатура NVT, структура команд Telnet, безпека, Telnet і інші протоколи. Пірінговий (P2P) мережевий протокол для кооперативного обміну файлами через Інтернет.

ТЕМАТИЧНИЙ ПЛАН

Опрацювання курсу "Комп'ютерні мережі" передбачає аудиторну (лекції та лабораторні заняття), самостійну та індивідуальну роботу студентів, виконання завдань із самоперевірки, модульний контроль (табл. 1).

Таблиця 1

Тематичний план навчального курсу

№ теми	Назва змістового модуля, теми	Усього годин	Лекції	Лабораторні заняття	Самостійна та індивідуальна робота
1	**2**	**3**	**4**	**5**	**6**
	ЗАЛІКОВИЙ КРЕДИТ I	***36***	***8***	***8***	***20***
	Змістовий модуль 1	***18***	***4***	***4***	***10***
1.1	Основи комп'ютерних мереж	9	2	2	5
1.2	Мережеві характеристики та класифікація комп'ютерних мереж	9	2	2	5
	Змістовий модуль 2	***18***	***4***	***4***	***10***
2.1	Архітектура і стандартизація мереж	9	2	2	5
2.2	Технології фізичного рівня комп'ютерних мереж	9	2	2	5
	ЗАЛІКОВИЙ КРЕДИТ II	***36***	***8***	***8***	***20***
	Змістовий модуль 3	***18***	***4***	***4***	***10***
3.1	Загальна характеристика протоколів локальних мереж з використанням розподілюваного середовища Ethernet	9	2	2	5
3.2	Високошвидкісні технології локальних мереж	9	2	2	5
	Змістовий модуль 4	***18***	***4***	***4***	***10***
4.1	Комутовані мережі Ethernet	9	2	2	5
4.2	Інтелектуальні функції комутаторів	9	2	2	5
	ЗАЛІКОВИЙ КРЕДИТ III	***36***	***8***	***8***	***20***
	Змістовий модуль 5	***18***	***4***	***4***	***10***
5.1	Протокол міжмережевої взаємодії. Адресація в стеку протоколів TCP/IP	9	2	2	5

1	2	3	4	5	6
5.2	Особливості адресації в стеку протоколів TCP/IP	9	2	2	5
	Змістовий модуль 6	***18***	***4***	***4***	***10***
6.1	Базові транспортні протоколи стеку TCP/IP	9	2	2	5
6.2	Загальні властивості і класифікація протоколів маршрутизації	9	2	2	5
	ЗАЛІКОВИЙ КРЕДИТ IV	***36***	***8***	***8***	***20***
	Змістовий модуль 7	***18***	***4***	***4***	***10***
7.1	Електронна пошта та протокол передачі файлів	9	2	2	5
7.2	Протокол передачі гіпертекстових повідомлень	9	2	2	5
	Змістовий модуль 8	***18***	***4***	***4***	***10***
8.1-8.2	Прикладні протоколи в адмініструванні комп'ютерних мереж	18	4	4	10
	Разом	***144***	***32***	***32***	***80***

ПРОЕКТУВАННЯ ДИДАКТИЧНОГО ПРОЦЕСУ З ВИДІВ НАВЧАЛЬНИХ ЗАНЯТЬ

1. Лекційні заняття, їх тематика та обсяг

Лекції з навчальних модулів відповідають конкретним темам курсу "Комп'ютерні мережі". За способом викладання лекції є інформаційними, оскільки передбачають передавання інформації шляхом послідовного розкриття наукових фактів, явищ, процесів. Обов'язковим елементом лекцій є подання теоретичного матеріалу у формі проблемного завдання, в умовах якого окреслюються певні суперечності, що потребують розв'язання.

Науковий і фактичний матеріал лекцій відображає ключові питання навчальної дисципліни (табл. 2).

Таблиця 2

Тематика лекційних занять

№ теми	Назва тем та анотований зміст	Кіль-кість годин
1	**2**	**3**
1.1	**Основи комп'ютерних мереж** Предмет і завдання дисципліни "Комп'ютерні мережі". Взаємозв'язок її із суміжними дисциплінами. Еволюція комп'ютерних мереж: перші комп'ютерні мережі, конвергенція мереж. Загальні принципи побудови мереж: проста мережа з двох комп'ютерів, мережеве програмне забезпечення, фізична передача даних лініями зв'язку, проблеми зв'язку декількох комп'ютерів, узагальнене завдання комутації. Комутація каналів і пакетів: порівняння мереж з комутацією пакетів і каналів, Ethernet – приклад стандартної технології з комутацією пакетів.	2
1.2	**Мережеві характеристики та класифікація комп'ютерних мереж** Класифікація комп'ютерних мереж, узагальнена структура телекомунікаційної мережі, мережі операторів зв'язку, корпоративні мережі, Інтернет. Мережеві характеристики: типи характеристик, продуктивність, надійність, характеристики втрат пакетів, характеристики мережі	2

	постачальника послуг.	
1	**2**	**3**
2.1	**Архітектура і стандартизація мереж** Архітектура і стандартизація мереж: декомпозиція завдань мережевої взаємодії, модель OSI, стандартизація мереж, інформаційні і транспортні послуги.	2
2.1	**Технології фізичного рівня комп'ютерних мереж** Лінії зв'язку: класифікація ліній зв'язку, типи кабелів, характеристики ліній зв'язку. Кодування і мультиплексування даних: модуляція, дискретизація аналогових сигналів, методи кодування, виявлення ікорекція помилок, мультиплексування і комутація. Первинні мережі.	2
3.1	**Загальна характеристика протоколів локальних мереж з використанням розподілюваного середовища Ethernet** Загальна характеристика протоколів локальних мереж з використанням розподілюваного середовища Ethernet із швидкістю 10 Мбіт/с: MAC-адреси, формати кадрів технології Ethernet, доступ до середовища і передача даних, виникнення колізії, час обороту і розпізнавання колізій, специфікації фізичного середовища, максимальна продуктивність мережі Ethernet.	2
3.2	**Високошвидкісні технології локальних мереж** Технологія Ethernet зі швидкістю передачі 100 Мбіт/с. Гігабітові й 10-гігабітові технології Ethernet. Технології Token Ring і FDDI. Безпровідні локальні мережі IEEE 802.11. Персональні мережі.	2
4.1	**Комутовані мережі Ethernet** Міст як попередник і функціональний аналог комутатора: логічна структуризація мереж і мости, алгоритм прозорого мосту IEEE 802.1D, топологічні обмеження при застосуванні мостів в локальних мережах.	2
4.2	**Інтелектуальні функції комутаторів** Комутатори. Архітектура комутаторів. Обмеження комутаторів. Агрегація ліній зв'язку в локальних мережах: транки і логічні канали, боротьба з "розмноженням" пакетів, вибір порту. Фільтрація трафіку.	2

5.1	**Протокол міжмережевої взаємодії. Адресація в стеку протоколів TCP/IP** Протокол IP стеку протоколів TCP/IP. Формат IP-пакету. Типи адрес стеку TCP/IP: локальні адреси, мережеві IP-адреси, доменні імена. Формат IP-адреси: класи I P-адрес, особливі IP-адреса, використання масок при IP-адресації. Порядок призначення IP-адрес: призначення адрес автономній мережі, централізований розподіл адрес, адресація і технологія CIDR.	2
1	**2**	**3**
5.2	**Особливості адресації в стеку протоколів TCP/IP** Маршрутизація з використанням масок, структуризація мережі масками однакової довжини, перегляд таблиць маршрутизації з урахуванням масок, використання масок змінної довжини, перекриття адресних просторів, CIDR.	2
6.1	**Базові транспортні протоколи стеку TCP/IP** Протоколи транспортного рівня TCP і UDP: порти і сокети, протокол UDP і UDP-дейтаграми, протокол TCP і TCP-сегменти, логічні з'єднання – основа надійності TCP, повторна передача і ковзне вікно, реалізація методу ковзного вікна в протоколі TCP, управління потоком.	2
6.2	**Загальні властивості і класифікація протоколів маршрутизації** Загальні властивості і класифікація протоколів маршрутизації: протокол RIP, протокол OSPF, протокол BGP. Протокол ICMP: утиліта traceroute, утиліта ping. Трансляція мережевих адрес: причини підміни адрес, традиційна технологія NAT, базова трансляція мережевих адрес, трансляція мережевих адрес і портів. Типи публічних послуг мереж операторів зв'язку. Багатошарова мережа оператора зв'язку. Технологія Frame Relay. Технологія ATM. Віртуальні приватні мережі. IP в глобальних мережах.	2
7.1	**Електронна пошта та протокол передачі файлів** Електронна пошта: електронні листи, протокол SMTP, безпосередня взаємодія клієнта і сервера, схема з виділеним поштовим сервером, схема з двома поштовими серверами-посередниками, протоколи POP3 і IMAP. Основні модулі служби FTP: керуючий сеанс і сеанс передачі даних, команди взаємодії FTP-клієнта з FTP-сервером.	2
7.2	**Протокол передачі гіпертекстових повідомлень** Веб-служба: веб- і HTML-сторінки, веб-клієнт і веб-сервер, протокол HTTP, формат HTTP-повідомлень, динамічні веб-сторінки.	2
8.1-8.2	**Прикладні протоколи в адмініструванні комп'ютерних мереж**	4

	Система DNS: плоскі символьні імена, ієрархічні символьні імена, схема роботи DNS, зворотна зона. Стандарти і програмні реалізації віддаленого доступу. Мережевий протокол для реалізації текстового інтерфейсу мережею: опції, принтер і клавіатура NVT, структура команд Telnet, безпека, Telnet і інші протоколи. Пірінговий (P2P) мережевий протокол для кооперативного обміну файлами через Інтернет.	
	Разом	**32**

2. Лабораторні заняття, їх тематика та обсяг

Лабораторні заняття з курсу "Комп'ютерні мережі" передбачають опрацювання студентами теоретичних положень, засвоєних на лекціях та в процесі самостійної роботи, обговорення реферативних повідомлень, виконання практичних завдань.

Таблиця 3

Тематика лабораторних занять

№ теми	Тема заняття	Кількість годин
1	**2**	**4**
1.1	Аналіз структури програмного та апаратного компонентів комп'ютерної мережі	2
1.2	Аналіз та визначення виду комп'ютерної мережі	2
2.1	Аналіз та співставлення стеків мережевих протоколів	2
2.2	Фізичне середовище передачі даних	2
3.1	Аналіз та перевірка дієздатності комп'ютерної мережі Ethernet	2
3.2	Побудова локальної мережі на основі стандартів 802.3	2
4.1	Концепції проектування комп'ютерної мережі на основі концентраторів і комутаторів	2
4.2	Інтелектуальні комутатори Ethernet	2
5.1	Керування IP-адресацією з використанням класів і масок	2
5.2	Управління адресами підмереж	2
6.1	Перевірка TCP/IP-з'єднання за допомогою команди ping	2
6.2.	Перевірка TCP/IP-з'єднання за допомогою команд ping і net view	2
7.1	Використання протоколу FTP	2
7.2	Дослідження роботи протоколу HTTP	2
8.1	Використання протоколів віддаленого адміністрування	4

	Разом	**32**

3. Самостійна робота студентів, її тематика та обсяг

Самостійна робота є основним засобом засвоєння студентами навчального матеріалу у вільний від аудиторних занять час.

Зміст самостійної роботи визначається навчальною програмою курсу "Комп'ютерні мережі", завданнями та рекомендаціями викладача.

Самостійна робота студентів передбачає вивчення окремих питань курсу, опрацювання теоретичних основ лекційного матеріалу, підготовку до лабораторної роботи, виконання індивідуальних завдань, систематизацію вивченого матеріалу курсу перед модульним контролем тощо. Засвоєний у процесі самостійної роботи навчальний матеріал виноситься на поточний контроль.

Таблиця 4

Тематика самостійної роботи

№ теми	**Зміст самостійної роботи**	**Кількість годин**
1	**2**	**3**
1.1	Топологія ієрархічної мережі	5
1.2	Функції та призначення ядра мережі	5
2.1	Рівень розподілення в реалізації ієрархічної комп'ютерної мережі	5
2.2	Рівень доступу як основа підключення абонентів в ієрархічній комп'ютерній мережі	5
3.1	Підключення до служб загального призначення при проектуванні ієрархічної мережі	5
3.2	Додавання мережевих адрес при проеуктуванні адресного простору в ієрархічній мережі	5
4.1	Стратегія адресації при проектуванні ієрархічної комп'ютерної мережі	5
4.2	Загальні принципи адресації	5
5.1	Мета та стратегія надлишковості в ієрархічних мережах	5
5.2	Надлишковість, що реалізується на рівні ядра ієрархічної мережі	5
6.1	Надлишковість, що реалізується на рівні розподілення ієрархічної мережі	5

6.2	Надлишковість, що реалізується на рівні доступу ієрархічної мережі	5
7.1	Реорганізація ієрархічної комп'ютерної мережі для стабілізації її роботи	5
7.2	Реорганізація адресації рівня розподілення та рівня доступу для стабілізації роботи ієрархічної мережі	5
8.1	Застосування принципів ієрархічного проектування мережі	10
	Разом	**80**

4. Індивідуальна робота студентів

Індивідуальна робота проводиться з окремими студентами з метою підвищення рівня їхньої підготовки та розвитку індивідуальних творчих здібностей.

Основним видом оформлення результатів індивідуальної роботи з навчальної дисципліни "Комп'ютерні мережі" є написання студентами реферату. За своєю формою реферат є кротким викладом основного змісту певної наукової роботи або узагальненням низки праць, які розкривають тему.

План реферату може бути простим або складним. Структуру реферату складають такі компоненти: *вступ*, у якому обґрунтовується актуальність теми, формулюються завдання реферативної роботи; *основна частина*, що містить стислий огляд і критичну оцінку наукових видань, їх порівняння, аргументацію найголовніших положень; *висновки,* які відображають наслідки сформульованих у вступі мети і завдань, можливість використання набутих знань у практичній роботі; *список використаних джерел.*

Таблиця 5

Проектування індивідуальної роботи

№ теми	**Тематика індивідуальних завдань**
1	**2**
1.1	Еволюція комп'ютерних мереж та напрямки їх розвитку
1.2	Сучасні підходи до реалізації комутації пакетів у глобальних мережах
2.1	Перспективи розвитку стеку мережевих протоколів TCP/IP
2.2	Тенденції використання ліній зв'язку та перспективи їх розвитку
3.1	Порівняльний аналіз стандартів локальних мереж та перспективи їх розвитку
3.2	Сучасні тенденції розвитку високошвидкісних локальних мереж
4.1	Порівняльний аналіз інтелектуальних комутаторів

4.2	Побудова корпоративних локальних мереж на основі інтелектуальних комутаторів
5.1	Сучасний стан розвитку протоколу IP
5.2	Динамічне виділення IP-адрес та протокол DHCP
6.1	Транспортні протоколи – особливості функціонування
6.2	Зв'язок прикладних протоколів з транспортним рівнем стеку TCP/IP
7.1	Засоби безпеки, що реалізуються в поштових протоколах
7.2	Встановлення та налагодження веб-сервера Apache
8.1	Використання протоколу SHH для віддаленого адміністрування серверів

5. Система оцінювання навчальних досягнень студентів

Рейтингова система оцінювання передбачає визначення якості виконання студентами всіх видів аудиторної та позааудиторної навчальної роботи, рівня набутих ними знань, умінь і навичок, ступеня досягнення кінцевих цілей професійної підготовки.

Оцінювання навчальних досягнень студентів здійснюється в балах з таким переведенням в оцінку за традиційною національною шкалою та шкалою ECTS (European Credit Transfer System).

Таблиця 6

Порівняння національної шкали оцінювання та шкали оцінювання ESTS

Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка за шкалою ECTS**	
		Оцінка	**Пояснення**
90 – 100	Відмінно	A	Відмінно (відмінне виконання лише з незначною кількістю помилок)
82 – 89	Добре	B	Дуже добре (вище середнього рівня з кількома помилками)
75 – 81		C	Добре (у цілому правильне виконання з певною кількістю суттєвих помилок)
67 – 74	Задовільно	D	Задовільно (непогано, але зі значною кількістю недоліків)
60 – 66		E	Достатньо (виконання задовольняє мінімальні критерії)
35 – 59	Незадовільно	FX	Незадовільно

			(з можливістю повторного складання)
1 – 34		F	Незадовільно (з обов'язковим повторним курсом)

Рейтингова система оцінювання передбачає використання поточного, проміжного та підсумкового контролю.

Поточна рейтингова оцінка складається з балів, які студент отримує за такі види навчальної діяльності із засвоєння змістового модуля:

– систематичність та активність роботи на семінарсько-практичних заняттях;

– виконання завдань для самостійного опрацювання;

– підготовка індивідуального завдання.

Проміжна рейтингова оцінка виставляється в балах за результатами засвоєння змістового модуля навчальної дисципліни та визначається як сума поточних і контрольних рейтингових оцінок. Проміжна рейтингова оцінка за окремий заліковий кредит становить не більше 59 балів.

Підсумкова рейтингова оцінка визначається в балах як сума середнього показника проміжних рейтингових оцінок та модульної контрольної рейтингової оцінки. Максимальна контрольна модульна рейтингова оцінка складає 41 бал.

Рейтингова система оцінювання передбачає використання поточного, проміжного та підсумкового контролю.

Таблиця 7

Види контролю

Заліковий кредит	Змістовий модуль	Поточна рейтингова оцінка			Контрольна рейтингова оцінка	Проміжна рейтингова оцінка			Контрольна модульна рейтингова оцінка	Підсумкова рейтингова оцінка
		Робота на практичному (на лабораторному) занятті	Самостійна робота	Індивідуальне завдання		За змістовий модуль	За заліковий кредит	Середній показник		
1	2	3	4	5	6	7	8	9	10	11

I	1	10	4	5	10	29	59	59	41	100
	2	10	5	5	10	30				
II	3	10	4	5	10	29	59			
	4	10	5	5	10	30				
III	5	10	4	5	10	29	59			
	6	10	5	5	10	30				
IV	7	10	4	5	10	29	59			
	8	10	5	5	10	30				

6. Засоби контролю

З метою забезпечення об'єктивного контролю формування компетенцій з курсу "Комп'ютерні мережі" студентам пропонується виконання контрольних робіт з кожного змістового модуля та модульної контрольної роботи.

Модульні контрольні роботи складаються із цілеспрямованих наборів тестових завдань.

Шкала оцінювання завдань контрольних робіт – бальна, побудована за принципом урахування типу завдання та особистих досягнень виконавця.

Тести закритої форми оцінюються 1 балом кожне, мають початковий ступінь складності, носять репродуктивний характер, дозволяють виявити ґрунтовність засвоєння теоретичних знань з мережевих технологій.

Критерієм визначення досягнень студентів-виконавців є правильність знань.

Оцінка "1 бал": відповідь правильна.

Оцінка "0 балів": відповідь неправильна, або відсутня.

У підсумковій модульній контрольній роботі, крім тестів закритої форми пропонуються завдання, які мають достатній ступінь складності, творчий характер і дають змогу виявити вміння студентів самостійно і творчо мислити, а також застосувати набуті знання з дисципліни "Комп'ютерні мережі" на практиці.

При визначенні досягнень студентів-виконавців об'єктом аналізу є такі орієнтири:

– характеристика відповіді: елементарна, фрагментарна, логічна, доказова, обґрунтована;

– якість знань: правильність, повнота, глибина, системність, узагальненість;

– рівень оволодіння розумовими операціями;

– досвід творчої діяльності: уміння виявляти проблеми, формулювати припущення, розв'язувати задачі;

– самостійність оціночних суджень.

Завдання оцінюється 3-ма балами, якщо відповідь правильна, повна, з достатнім теоретичним обґрунтуванням, позначена елементами творчості; є аргументація особистої позиції.

Оцінка "2 бали": у цілому завдання виконано правильно, повністю, проте є окремі неточності або розв'язання не містить належного теоретичного обґрунтування.

Оцінка "1 бал": відповідь елементарна, фрагментарна, що зумовлено нечітким уявленням про предмет питання.

Оцінка "0 балів": неправильна відповідь або її відсутність.

У процесі вивчення курсу "Комп'ютерні мережі" використовуємо такі види контролю:

– попередній – здійснюється в усній та письмовій формах роботи на початку вивчення курсу або перед вивченням нової теми з метою з'ясування рівня знань;

– поточний – проводить з метою діагностування рівня знань, умінь та навичок з теми лабораторного заняття, передбачає виконання тестових завдань та контрольних робіт; за змістом він включає два аспекти: якість засвоєння матеріалу, який охоплюється темою лабораторного заняття, та сумлінність студентів у лабораторній роботі;

– тематичний – проводиться після кожного розділу курсу в письмовій формі на основі питань, за допомогою яких перевіряється рівень оволодіння теоретичними знаннями та засвоєння практичних навичок; такий контроль здійснюється методом написання контрольних робіт, проведення індивідуальних консультацій, виконання тестових завдань тощо;

– підсумковий – здійснюється у формі диференційованого заліку в кінці семестру після вивчення всього курсу "Комп'ютерні мережі".

Оцінки детермінуються показниками контролю засвоєння лекцій і всього курсу в цілому.

7. Питання для самоконтролю

1. Еволюція комп'ютерних мереж: перші комп'ютерні мережі, конвергенція мереж.

2. Комутація каналів і пакетів: порівняння мереж з комутацією пакетів і каналів.

3. Класифікація комп'ютерних мереж, узагальнена структура телекомунікаційної мережі, мережі операторів зв'язку, корпоративні мережі, Інтернет.

4. Мережеві характеристики: типи характеристик, продуктивність, надійність, характеристики втрат пакетів, характеристики мережі постачальника послуг.

5. Архітектура і стандартизація мереж: декомпозиція завдань мережевої взаємодії, модель OSI, стандартизація мереж, інформаційні і транспортні послуги.

6. Лінії зв'язку: класифікація ліній зв'язку, характеристики ліній зв'язку, типи кабелів.

7. Кодування і мультиплексування даних: модуляція, дискретизація аналогових сигналів, методи кодування, виявлення і корекція помилок, мультиплексування і комутація. Первинні мережі.

8. Загальна характеристика протоколів локальних мереж з використанням розподілюваного середовища Ethernet із швидкістю 10 Мбіт/с:

9. Технологія Ethernet зі швидкістю передачі 100 Мбіт/с. Гігабітові й 10-гігабітові технології Ethernet.

10. Технології Token Ring і FDDI.

11. Безпровідні локальні мережі IEEE 802.11.

12. Персональні мережі.

13. Міст як попередник і функціональний аналог комутатора: логічна структуризація мереж і мости, алгоритм прозорого мосту IEEE 802.1D.

14. Топологічні обмеження при застосуванні мостів в локальних мережах.

15. Комутатори. Архітектура комутаторів.

16. Обмеження комутаторів.

17. Агрегація ліній зв'язку в локальних мережах: транки і логічні канали, боротьба з "розмноженням" пакетів, вибір порту.

18. Фільтрація трафіку.

19. Протокол IP стеку протоколів TCP/IP.

20. Формат IP-пакету.

21. Типи адрес стеку TCP/IP: локальні адреси, мережеві IP-адреси, доменні імена.

22. Формат IP-адреси: класи IP-адрес, особливі IP-адреса, використання масок при IP-адресації.

23. Порядок призначення IP-адрес.

24. Централізований розподіл адрес.
25. Адресація і технологія CIDR.
26. Маршрутизація з використанням масок.
27. Структуризація мережі масками однакової довжини.
28. Перегляд таблиць маршрутизації з урахуванням масок.
29. Використання масок змінної довжини, перекриття адресних просторів, CIDR.
30. Протоколи транспортного рівня TCP і UDP: порти і сокети, протокол UDP і UDP-дейтаграми.
31. Протокол TCP і TCP-сегменти.
32. Логічні з'єднання – основа надійності TCP.
33. Повторна передача і ковзне вікно, реалізація методу ковзного вікна в протоколі TCP, управління потоком.
34. Загальні властивості і класифікація протоколів маршрутизації.
35. Протокол RIP.
36. Протокол OSPF.
37. Протокол BGP.
38. Протокол ICMP.
39. Утиліта traceroute.
40. Утиліта ping.
41. Трансляція мережевих адрес: причини підміни адрес, традиційна технологія NAT, базова трансляція мережевих адрес, трансляція мережевих адрес і портів.
42. Типи публічних послуг мереж операторів зв'язку.
43. Багатошарова мережа оператора зв'язку.
44. Технологія Frame Relay.
45. Технологія ATM.
46. Віртуальні приватні мережі.
47. IP в глобальних мережах.
48. Електронна пошта: електронні листи, протокол SMTP.
49. Безпосередня взаємодія клієнта і сервера, схема з виділеним поштовим сервером, схема з двома поштовими серверами-посередниками, протоколи POP3 і IMAP.
50. Основні модулі служби FTP: керуючий сеанс і сеанс передачі даних.
51. Команди взаємодії FTP-клієнта з FTP-сервером.
52. Веб-служба: веб- і HTML-сторінки.
53. Веб-клієнт і веб-сервер.

54. Протокол HTTP, формат HTTP-повідомлень, динамічні вебсторінки.

55. Система DNS: плоскі символьні імена, ієрархічні символьні імена, схема роботи DNS, зворотна зона.

56. Стандарти і програмні реалізації віддаленого доступу. Мережевий протокол для реалізації текстового інтерфейсу мережею: опції, принтер і клавіатура NVT, структура команд Telnet, безпека, Telnet і інші протоколи.

57. Пірінговий (P2P) мережевий протокол для кооперативного обміну файлами через Інтернет.

Література

Основна

1. *Антонов В. М.* Сучасні комп'ютерні мережі / Валерій Миколайович Антонов. – К. : МК-Прес, 2005. – 480 с.

2. *Бройдо В. Л.* Вычислительные системы, сети и телекоммуникации: учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Прикладная информатика" и "Информационные системы в экономике" / В. Л. Бройдо, О. П. Ильина. – 3-е изд. – Москва [и др.]: Питер, 2008. – 765 с.: ил., табл.; 24 см.

3. *Валецька Т. М.* Комп'ютерні мережі. Апаратні засоби: навч. посіб. для студ. вищ. навч. закл. / Тетяна Михайлівна Валецька. – К. : Центр навчальної літератури, 2004. – 208 с.

4. *Гук М.* Аппаратные средства локальных сетей. Энциклопедия : [Наиболее полн. и подроб. рук.] / Михаил Гук. – СПб. : Питер, 2000.– 572 с.

5. *Жуков І. А.* Комп'ютерні мережі та технології: навч. посіб. для студ. вищих навч. закл. / Жуков І. А., Гуменюк В. О., Альтман І. Є.. – К. : НАУ, 2004. – 276 с. – (Комп'ютерні технології).

6. *Компьютеры*, сети, Интернет: Энциклопедия: Наиболее полн. и подроб. рук. / Ю. Новиков, Д. Новиков, А. Черепанов, В. Чуркин; Под общ. ред. Ю. Новикова. – 2. изд. – М. [и др.]: Питер, 2003 (СПб.: ГПП Печ. Двор им. А.М. Горького). – 831 с.: ил.; 24 см.

7. *Новиков Ю. В.* Локальные сети: Архитектура, алгоритмы, проектирование / Новиков Ю. В., Кондратенко С. В. – М.: ЭКОМ, 2002. – 311 с.: ил.; 23 см. – (Современные компьютерные технологии).

8. *Оглтри Т. В.* Модернизация и ремонт сетей / Терри

Оглтри ; [пер. с англ. И. В. Берштейна и др.]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (ГПП Печ. Двор). – 1321 с.: ил.; 24 см. – (Библиотека Скотта Мюллера).

9. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

10. *Олифер В. Г.* Новые технологии и оборудование IP-сетей / Виктор Олифер, Наталья Олифер. – СПб. и др.: BHV, 2000. – 512 с.: ил., табл.; 24 см. – (Мастер) (Современные сетевые технологии).

11. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. – 4-е изд. – М. [и др.]: Питер, 2005. – 991 с.: ил., табл.; 24 см. – (Классика computer science).

12. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

13. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

14. *Уилсон Э.* Мониторинг и анализ сетей. Методы выявления неисправностей / Эд Уилсон; [Пер. с англ. О. Труфанова]. – М.: ЛОРИ, [2002]. – 350 с.: ил., табл.; 24 см.

Додаткова

1. *Администрирование* сети на основе Microsoft Windows 2000 : учеб. курс MCSA/MCSE : Сертификац. экзамен 70216 : пер. с англ. – [2. изд.]. – М. : Рус. ред., 2003 (ОАО Тип. Новости). – 462 с. – (Официальное учебное пособие для самоподготовки).

2. *Бабій М. С.* Локальні мережі ЕОМ: [навч. посіб. для студ. спец. "Прикладна математика"] / Михайло Семенович Бабій. –

Суми : Видавництво СумДУ, 2003. – 64 с.

3. *Башмаков А. И.* Интеллектуальные информационные технологии: учеб. пособие для студ. вузов, обуч. по направлению подгот. дипломированных спец. "Информатика и вычислительная техника" / А. И. Башмаков, И. А. Башмаков – М. : МГТУ им.Н.Э.Баумана, 2005. – 302 с.

4. *Білоус Л. Ф.* Інформаційні мережі : навч. посібник / Білоус Л. Ф. – К. : Логос, 2005. – 140 с.

5. *Бортник Г. Г.* Мережі доступу: навч. посібник для студ. напряму підготовки 0924 – "Телекомунікації" всіх спец. / Бортник Г. Г., Стальченко О. В., Яблонський В. Ф. – Вінниця : ВНТУ, 2006. – 139 с.

6. *Буров Є.* Комп'ютерні мережі / Євген Буров [ред. В. Пасічник]. – Л. : БаК, 1999. – 467 с.

7. *Вишневский А.* Сетевые технологии Windows 2000 / Алексей Вишневский. – СПб. и др.: Питер, 2000. – 591 с.: ил., табл.; 24 см. – (Для профессионалов).

8. *Грир Т.* Сети Интернет: Пер. с англ. – М.: ИТД "Русская редакция", 2000. – 368 с.

9. *Джонс А.* Руководство системного администратора Windows: Windows 98. Windows NT. Windows 2000 / Аллен Джонс; [Пер. с англ. А. Файзрахманов]. – СПб.: Питер, 2000. – 367 с.: ил.; 24 см. – (Для профессионалов).

10. *Єфіменко А. А.* Комп'ютерні мережі: метод. вказівки до викон. курсової роботи для студ. спец. 7.080402 – інформаційні технології проектування / А. А. Єфіменко; Одеський національний політехнічний ун-т. – Одеса : Наука і техніка, 2007. – 12 с.

11. *Жалдак М. І.* Вивчення основ комп'ютерних мереж / М. І. Жалдак, Н. В. Морзе, О. В. Козачук // Комп'ютер у школі та сім'ї. – 2000. – №2(10). – С. 14–18.

12. *Зайченко Ю. П.* Комп'ютерні мережі: навч. посіб. для студ. вищ. навч. закл. [Intertational Science and Technology University] / Ю. П. Зайченко. – К. : Слово, 2003. – 284 с. – (До 10-річчя Міжнародного науково-технічного ун-ту).

13. *Ибе О.* Сети и удаленный доступ: Протоколы, проблемы, решения / Оливер Ибе. – М.: ДМК Пресс, 2002. – 332 с.: ил.; 23 см. – (Серия "Защита и администрирование").

14. *Интеллектуальные* сети связи / Б.Я. Лихтциндер, М.А. Кузякин, А.В. Росляков, С.М. Фомичев. – 2. изд. – М.: Эко-Трендз, 2002. – 205 с.: ил., табл.; 24 см. – (Инженерная энциклопедия)

(Технологии электронных коммуникаций: ТЭК).

15. *Калита Д. М.* Комп'ютерні мережі. Апаратні засоби та протоколи передачі даних : навч. посіб. для студ. вищих закл. освіти / Калита Д. М.; [ред. Третяк О. В.]. – К. : ВПЦ "Київський ун-т", 2003. – 326 с. – (Автоматизація наукових досліджень).

16. *Камер Д.Э.* Компьютерные сети и Internet: Разработка приложений для Internet (пер. с англ. Птицына К.А.) Изд. 3-е + CD-Rom – 640 с.

17. *Карташевский В.Г.* Сети подвижной связи / В.Г. Карташевский, С.Н. Семенов, Т.В. Фирстова. – М.: Эко-Трендз, 2001. – 299 с.: ил.; 24 см. – (Инженерная энциклопедия. Технологии электронных коммуникаций (ТЭК)).

18. *Коваленко А. Є.* Корпоративні комп'ютерні мережі та телекомунікації : конспект лекцій для студ. спец. 7.080401 "Інформаційні управляючі системи та технології" ден. форми навч. / Анатолій Єпіфанович Коваленко. – К. : НУХТ, 2004. – 27 с.

19. *Комп'ютерні* мережі : метод. вказівки та контрольні завдання для студ. Ін-ту заоч. та дистанційного навчання спец. 8.091401 "Системи управління і автоматики" / [Уклад. В. О. Поліщук, А. І. Волевач]. – К. : НАУ, 2003. – 31 с.

20. *Комп'ютерні* мережі. Практикум : для студ. комп'ютерних спец. денної і заоч. форм навч. / [уклад. В. В. Швидкий]. – Черкаси : ЧДТУ, 2002. – 56 с.

21. *Контроль* та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології : навчальний посібник / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. – Х. : "Компанія СМІТ", 2004. – 544 с.

22. *Кулаков Ю. А.* Компьютерные сети / Ю. А. Кулаков, Г. М. Луцкий. – К. : Юниор, 1998. – 384 с.

23. *Кулаков Ю. А.* Локальные сети / Ю. А. Кулаков, Г. М. Луцкий. – К. : Юниор, 1998. – 336 с.

24. *Кульгин М.В.* Практика построения компьютерных сетей: Для профессионалов / Максим Кульгин. – СПб. [и др.]: Питер, 2001. – 318 с.: ил., табл.; 24 см. – (Серия для профессионалов).

25. *Кульгин М.В.* Технологии корпоративных сетей / Максим Кульгин. – СПб. и др.: Питер, 1999. – 699 с.: ил.; 24 см. – (Серия Энциклопедия).

26. *Лозікова Г.М.* Комп'ютерні мережі: Навч. посібник / Г.М. Лозікова . – К.: Центр навчальної літератури, 2004 . – 128 с.

27. *Мережі* ЕОМ. Лабораторний практикум / А. М. Пєтух, В. В. Войтко, С. В. Бевз, С. А. Яремко. – Вінниця : ВНТУ, 2003. – 125 с.

28. *Методические* рекомендации к выполнению лабораторных работ по курсу "Internet-технологии и язык Java": для студ. спец. 7.080401, 7.080407 всех форм обучения / Харьковский гос. экономический ун-т / Сост. С. В. Минухин, С. В. Знахур. – Х. : ХГЭУ, 2004. – 103с.

29. *Методичні* вказівки для виконання контрольних робіт з дисципліни "Мережі ЕОМ" для студентів заочної форми навчання спеціальності 7.091501 "Комп'ютерні системи і мережі" / Уклад. С. М. Захарченко. – Вінниця : ВДТУ, 2003. – 20 с.

30. *Методичні* вказівки до виконання лабораторних робіт з дисципліни "Мережі ЕОМ" для студентів спеціальності 7.0911501 "Комп'ютерні системи та мережі" / Черкаський держ. технологічний ун-т / Уклад. В. А. Тазетдінов – Черкаси : ЧДТУ, 2002. – 52 с. – (Користувачу сучасних інформаційних систем).

31. *Науман Ш.,* Вер Х. Компьютерные сети. – М. : ДМК, 2000. – 336 с.

32. *Олексюк В. П.* Організація комп'ютерної локальної мережі : [посіб.] / Олексюк В. П., Балик Н. Р., Балик А. В. – Тернопіль. : Підручники і посібники, 2006. – 80 с.

33. *Олифер В. Г.* Сетевые операционные системы : [учеб. для студентов, аспирантов и препод. вузов] / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2001. – 538 с.

34. *Основи* роботи та адміністрування мережних операційних систем : [навч. посіб. для студ. спец. "Комп'ютерні системи та мережі" денної та заоч. форми навч.] / [Азаров О. Д., Захарченко С. М., Яремчук Є. В., Дубінін В. М.]. – Вінниця : ВДТУ, 2001. – 145 с.

35. *Рамський Ю. С.* Вивчення інформаційно-пошукових систем мережі Інтернет: навч.-метод. посіб. / Ю. С. Рамський, О. В. Рєзіна. – К. : РННЦ "ДІНІТ", 2004. – 60 с.

36. *Толковый* словарь сетевых терминов и аббревиатур: Офиц. изд. Cisco systems, inc.: Янв. 2001: [Пер. с англ.]. – М. [др.]: Вильямс, 2002. – 366 с.; 24 см.

37. *Хошаба О. М.* Протоколи основних служб міжнародної комп'ютерної мережі Internet. Лабораторний практикум: навч. посіб. для студ. спец. "Інтелектуальні системи прийняття рішень" / Хошаба О. М.– Вінниця: ВДТУ, 2001. – 96 с.

38. *Шниер М.* Толковый словарь компьютерных технологий: [Сетевые технологии. Аппарат. средства. Интернет: Пер. с англ.] / Митчелл Шниер. – Киев: DiaSoft, Cop. 2000. – 720 с.: ил., табл.; 24 см. – (Библиотека Скотта Мюллера).

39. *Щербо В.К.* Стандарты вычислительных сетей. Взаимосвязи сетей: Справочник / В.К. Щербо. – М.: Кудиц-образ, 2000. – 268 с.: ил.; 29 см.

ЗМІСТОВИЙ МОДУЛЬ 1

ПРЕДМЕТ І ЗАВДАННЯ ДИСЦИПЛІНИ "КОМП'ЮТЕРНІ МЕРЕЖІ". ОСНОВИ МЕРЕЖ ПЕРЕДАВАННЯ ДАНИХ

Таблиця 8

Тематичний план змістового модуля

№ теми	Назва змістового модуля, теми	Усього годин	Лекції	Лабораторні заняття	Самостійна та індивідуальна робота
1.1	Основи комп'ютерних мереж	9	2	2	5
1.2	Мережеві характеристики та класифікація комп'ютерних мереж	9	2	2	5
	Разом	***18***	***4***	***4***	***10***

Навчальні цілі: сприяти засвоєнню студентами знань щодо сучасного стану та тенденцій теорії і практики розвитку мережевих технологій як складової сучасного інформаційного суспільства; ознайомити з напрямками розвитку комп'ютерних мереж; забезпечити засвоєння студентами знань понятійного апарату.

Основні поняття: комп'ютерна мережа, конвергенція мереж, мережеве програмне забезпечення, комутація, комутація каналів, комутація пакетів, фізична передача даних, класифікація мереж, продуктивність мережі, узагальнена структура телекомунікаційної мережі.

Методичні рекомендації щодо роботи з модулем: робота з модулем передбачає засвоєння лекційного матеріалу, участь у лабораторних заняттях, написання реферату (окремими студентами), самостійну роботу над визначеними питаннями теми, модульний контроль у формі тестування.

Після опрацювання цих тем студент може отримати бали, наведені в табл. 9.

Таблиця 9

Оцінювання навчальних досягнень студентів

Поточний контроль					**Контрольна рейтингова оцінка**	**Проміжна рейтингова оцінка**
Робота на лабораторному занятті		**Самостійна робота**		**Індивідуальне завдання**		
Тема №1.1	**Тема №1.2**	**Тема №1.1**	**Тема №1.2**			
5	5	2	2	5	10	29

ТЕМА 1.1. ОСНОВИ КОМП'ЮТЕРНИХ МЕРЕЖ

Лекція

План

1. Призначення комп'ютерних мереж.
2. Архітектура "клієнт-сервер".

Література

Основна

1. *Жуков І. А.* Комп'ютерні мережі та технології: навч. посіб. для студ. вищих навч. закл. / Жуков І. А., Гуменюк В. О., Альтман І. Є.. – К. : НАУ, 2004. – 276 с. – (Комп'ютерні технології).

2. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

3. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. – 4-е изд. – М. [и др.]: Питер, 2005. – 991 с.: ил., табл.; 24 см. – (Классика computer science).

4. *Бройдо В. Л.* Вычислительные системы, сети и телекоммуникации: учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Прикладная информатика" и "Информационные системы в экономике" / В. Л. Бройдо, О. П. Ильина. – 3-е изд. – Москва [и др.]: Питер, 2008. – 765 с.: ил., табл.; 24 см.

Додаткова

1. *Бабій М. С.* Локальні мережі ЕОМ: [навч. посіб. для студ. спец. "Прикладна математика"] / Михайло Семенович Бабій. – Суми : Видавництво СумДУ, 2003. – 64 с.

2. *Білоус Л. Ф.* Інформаційні мережі : навч. посібник / Білоус Л. Ф. – К. : Логос, 2005. – 140 с.

3. *Буров Є.* Комп'ютерні мережі / Євген Буров [ред. В. Пасічник]. – Л. : БаК, 1999. – 467 с.

4. *Камер Д.Э.* Компьютерные сети и Internet: Разработка приложений для Internet (пер. с англ. Птицына К.А.) Изд. 3-е + CD-Rom – 640 с.

5. *Коваленко А. Є.* Корпоративні комп'ютерні мережі та телекомунікації : конспект лекцій для студ. спец. 7.080401 "Інформаційні управляючі системи та технології" ден. форми навч. / Анатолій Єпіфанович Коваленко. – К. : НУХТ, 2004. – 27 с.

6. *Комп'ютерні* мережі. Практикум : для студ. комп'ютерних спец. денної і заоч. форм навч. / [уклад. В. В. Швидкий]. – Черкаси : ЧДТУ, 2002. – 56 с.

7. *Кульгин М.В.* Технологии корпоративных сетей / Максим Кульгин. – СПб. и др.: Питер, 1999. – 699 с.: ил.; 24 см. – (Серия Энциклопедия).

8. *Лозікова Г.М.* Комп'ютерні мережі: Навч. посібник / Г.М. Лозікова . – К.: Центр навчальної літератури, 2004 . – 128 с.

9. *Щербо В.К.* Стандарты вычислительных сетей. Взаимосвязи сетей: Справочник / В.К. Щербо. – М.: Кудиц-образ, 2000. – 268 с.: ил.; 29 см.

10. *Основи* роботи та адміністрування мережних операційних систем : [навч. посіб. для студ. спец. "Комп'ютерні системи та мережі" денної та заоч. форми навч.] / [Азаров О. Д., Захарченко С. М., Яремчук Є. В., Дубінін В. М.]. – Вінниця : ВДТУ, 2001. – 145 с.

1.1.1. Призначення комп'ютерних мереж

Комп'ютерні мережі (КМ) виникли давно. Ще на зорі появи комп'ютерів існували величезні системи, відомі як системи поділу

часу. Вони дозволяли використовувати центральну ЕОМ за допомогою віддалених терміналів. Такий термінал складався з дисплея й клавіатури. Зовні виглядав як звичайний персональний комп'ютер, але не мав власного процесорного блоку. Користуючись такими терміналами, сотні, а іноді тисячі співробітників мали доступ до центрального ЕОМ.

Такий режим забезпечувався завдяки тому, що система поділу часу розбивала час роботи центральної ЕОМ на короткі інтервали, розподіляючи їх між користувачами. При цьому створювалася ілюзія одночасного використання центральної ЕОМ багатьма співробітниками.

У 70-х роках великі ЕОМ поступилися місцем мінікомп'ютерним системам, що використовують той же режим розподілу часу. Технологія розвивалася, і з кінця 70-х років на робочих місцях з'явилися персональні комп'ютери. Однак, персональні комп'ютери, що автономно працюють не дають безпосереднього доступу до даних усієї організації й не дозволяють спільно використовувати програми й устаткування.

Із цього моменту починається сучасний розвиток комп'ютерних мереж.

Комп'ютерною мережею називається система, що складається із двох або більше віддалених ЕОМ, з'єднаних за допомогою спеціальної апаратури, взаємодіють між собою по каналах передачі даних.

Найпростіша *мережа (network)* складається з декількох персональних комп'ютерів, з'єднаних між собою мережевим кабелем (рис. 1). При цьому в кожному комп'ютері встановлюється спеціальна плата мережевого адаптера (NIC), що здійснює зв'язок між системною шиною комп'ютера й мережевим кабелем.

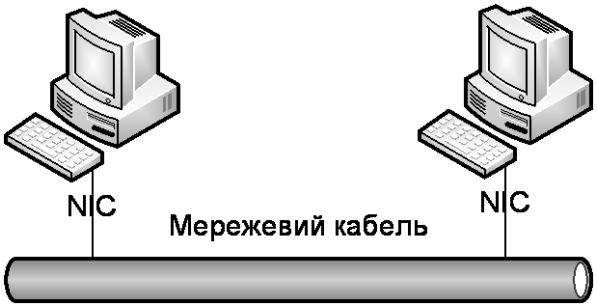


Рис. 1. Структура найпростішої обчислювальної мережі

Крім цього, усі комп'ютерні мережі працюють під керуванням спеціальної мережевої операційної системи (NOS – Network Operation Sistem). Основне призначення комп'ютерних мереж – спільне використання ресурсів і здійснення інтерактивного зв'язку як усередині однієї фірми, так і за її межами (рис. 2).

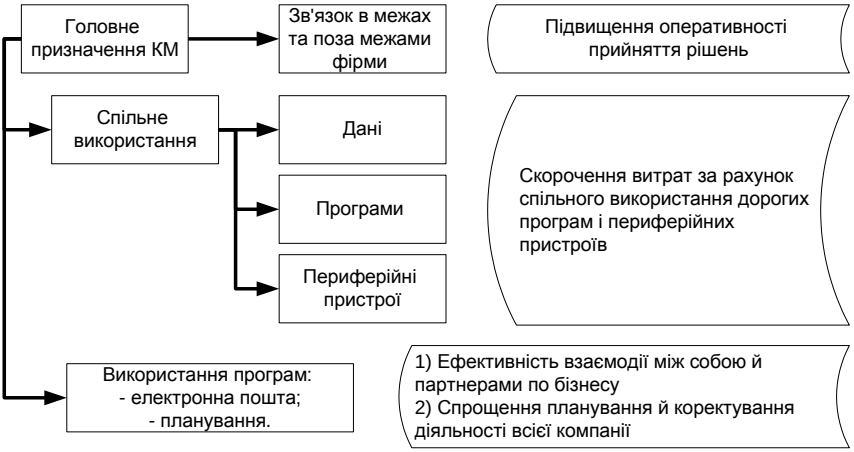


Рис. 2. Призначення комп'ютерної мережі

Ресурси являють собою дані (у тому числі корпоративні бази даних і знань), додатки (у тому числі різні мережні програми), а також периферійні пристрої, зокрема принтер, сканер, модем і т.д.

До об'єднання персонального комп'ютера в мережу кожний користувач повинен мати свій принтер, плотер та інші периферійні пристрої, а також на кожному з комп'ютерів повинні бути встановлені ті ж програмні засоби, що і у інших користувачів.

Перевагою мережі є також наявність програм електронної пошти й планування робочого дня. Завдяки їм співробітники ефективно взаємодіють між собою й партнерами по бізнесу, а планування й коректування діяльності всієї компанії здійснюється значно простіше. Використання комп'ютерних мереж дозволяє: а) підвищити ефективність роботи персоналу підприємства; б) знизити витрати за рахунок спільного використання даних, дорогих периферійних пристроїв і програмних засобів.

Основними характеристиками комп'ютерної мережі є:

– операційні можливості мережі;
– часові характеристики;
– надійність;
– продуктивність;
– вартість.

Операційні можливості мережі характеризуються такими умовами, як:

– надання доступу до прикладних програмних засобів, БД, БЗ, і т.д.;
– віддалене введення завдань;
– передача файлів між вузлами мережі;
– доступ до віддалених файлів;
– видача довідок про інформаційні й програмні ресурси;
– розподілена обробка даних на декількох ЕОМ і т.д.

Часові характеристики мережі визначають тривалість обслуговування запитів користувачів:

- середній час доступу, що залежить від розмірів мережі, завантаження й пропускної здатності каналів зв'язку й т.д.;
- середній час обслуговування.

Пакет як основна одиниця інформації в обчислювальних мережах. При обміні даними між персональними комп'ютерами будь-яке інформаційне повідомлення розбивається програмами передачі даних на невеликі блоки, які називаються пакетами (рис. 3).

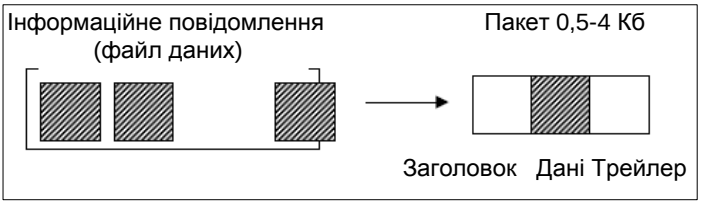


Рис. 3. Інформаційне повідомлення

Зв'язано це з тим, що дані звичайно містяться у великих за розміром файлах, і якщо передавальний комп'ютер відправить його повністю, то він надовго заповнить канал зв'язку і "зв'яже" роботу всієї мережі, тобто буде перешкоджати взаємодії інших учасників мережі. Крім цього, виникнення помилок при передачі великих блоків призведе до більших витрат часу, ніж на його повторну передачу.

Пакет – основна одиниця інформації в комп'ютерних мережах. При розподілі даних на пакети швидкість їхньої передачі зростає на стільки, що кожний комп'ютер мережі одержує можливість приймати й передавати дані практично одночасно з іншими ПК.

При розподілі даних на пакети мережева операційна система до власних переданих даних додає спеціальну інформацію, що містить:

– *заголовок*, у якому вказується адреса відправника, а також інформація зі збору блоків даних у вихідне інформаційне повідомлення при їхньому прийомі одержувачем;

– *трейлер*, у якому утримується інформація для перевірки безпомилковості в передачі пакета. При виявленні помилки передача пакета повинна повторитися.

Способи організації передачі даних між персональними комп'ютерами. Передача даних між комп'ютерами й іншими пристроями відбувається паралельно або послідовно.

Більшість персональних комп'ютерів користується паралельним портом для роботи із принтером. Термін "паралельно" означає, що дані передаються одночасно по кількох проводах.

Щоб послати байт даних по паралельному з'єднанню, комп'ютер одночасно встановлює весь байт на восьми проводах. Схему паралельного з'єднання проілюстровано на рис. 4.

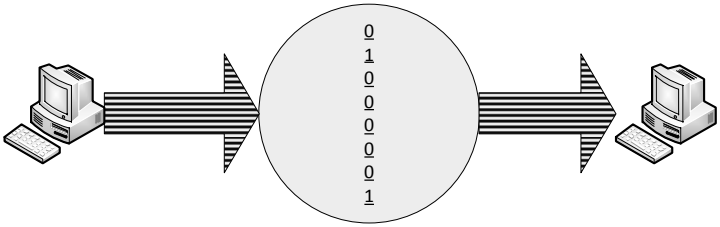


Рис. 4. Паралельне з'єднання

Як видно з малюнка, паралельне з'єднання по восьми проводах дозволяє передати байт даних одночасно.

Навпаки, послідовне з'єднання організує передачу даних по черзі, біт за бітом. У мережах найчастіше використовується саме такий спосіб роботи, коли біти вишиковуються один за одним і послідовно передаються (і приймаються теж), що ілюструє рис. 5.

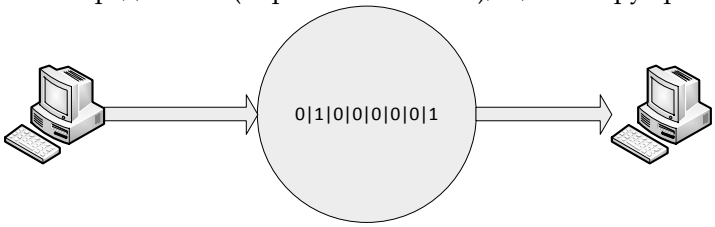


Рис. 5. Послідовне з'єднання

При з'єднанні по мережевих каналах використовують три різних методи. З'єднання буває симплексне, напівдуплексне й дуплексне.

Про *симплексне* з'єднання говорять, коли дані переміщаються тільки в одному напрямку (рис. 6). *Напівдуплексне* з'єднання дозволяє даним переміщатися в обох напрямках, але в різний час.

І, нарешті, *дуплексне* з'єднання дозволяє даним переміщатися в обох напрямках одночасно.

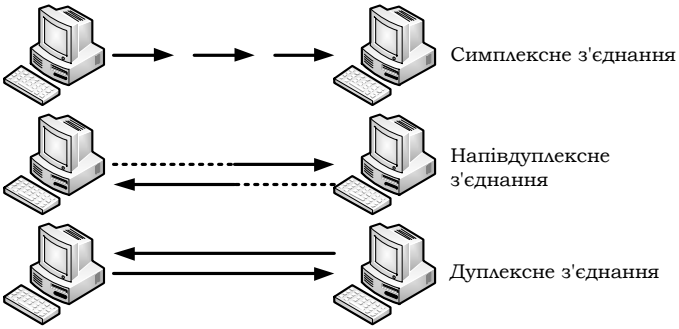


Рис. 6. Типи з'єднань

1.1.2. Архітектура "клієнт-сервер"

Комп'ютерна мережа (КМ) – це сукупність комп'ютерів і терміналів, з'єднаних за допомогою каналів зв'язку в єдину систему, що задовольняє вимогам розподіленої обробки даних, спільного використання загальних інформаційних і обчислювальних ресурсів.

Часто виникає плутанина між розподіленими системами й КМ. Працюючи з розподіленою системою, користувач може не мати ні найменшого уявлення про те, на яких процесорах, де, з використанням конкретно яких фізичних ресурсів буде виконуватися його програма. У мережі, оскільки всі машини там автономні, користувач повинен робити все явно. Основна відмінність між цими системами полягає в організації їхнього програмного забезпечення. І там, і там відбувається передача даних. У мережі – користувач, у розподіленій системі – система.

Розподілені обчислення в комп'ютерних мережах засновані на архітектурі "клієнт-сервер", що став основним способом обробки даних. Терміни "клієнт" і "сервер" позначають ролі, які відіграють різні компоненти в розподіленому середовищі обчислень. Компоненти "клієнт" і " сервер" не обов'язково повинні працювати на різних машинах, хоча звичайно це так і є – клієнт-додаток перебуває на робочій станції користувача, а сервер – на спеціальній виділеній машині. Найпоширеніші такі види серверів: файли-сервери, сервери баз даних, сервери друку, сервери електронної пошти, Web-сервер та інші. Останнім часом інтенсивно впроваджуються багатофункціональні сервери додатків.

Клієнт формує запит на сервер для виконання відповідних

функцій. Наприклад, файл-сервер забезпечує зберігання даних загального користування, організує доступ до них і передає дані клієнту. Обробка даних розподіляється в тому або іншому співвідношенні між сервером і клієнтом. Останнім часом частку обробки, що припадає на клієнта, почали називати "товщиною" клієнта.

Розвиток архітектури "клієнт-сервер" відбувається по спіралі й у цей час є тенденція централізації обчислень, тобто заміни "товстих" клієнтів – робочих станцій на основі високопродуктивних ПЭВМ, оснащених потужним програмним забезпеченням для підтримки прикладних програм, мультимедійних засобів, навігаційного й графічного інтерфейсу – "тонкими" клієнтами. Характерний приклад "тонкого" клієнта – архітектура Sun Ray Hot Desk, запропонована компанією Sun Microsystems.

Архітектура Sun Ray Hot Desk припускає використання настільних систем типу графічних терміналів Sun Ray 1, що мають мінімум програмних і апаратних засобів, які володіють широкими можливостями, з додатками відповідно до основної ідеї "тонких" клієнтів – винести на сервер усе, аж до віртуальних драйверів пристроїв, включаючи драйвер монітора. Історичними попередниками "тонких" клієнтів були алфавітно-цифрові термінали, що підключалися до головних ЕОМ або мейнфреймів (mainframe) через спеціалізовані інтерфейси або універсальні послідовні порти.

Мейнфрейми – класичний приклад централізації обчислень, оскільки в єдиному комплексі були сконцентровані всі обчислювальні ресурси, зберігання й обробка великих масивів даних. Основні переваги централізованої архітектури – простота адміністрування й захисту інформації. Усі термінали були однотипними, отже, пристрої на робочих місцях користувачів поводилися передбачувано й у будь-який момент могли б бути замінені, витрати на обслуговування терміналів і ліній зв'язку також легко прогнозувалися.

Революція, викликана появою персональних комп'ютерів, дала змогу мати обчислювальні й інформаційні ресурси на робочому столі користувача й управляти ними на власний розсуд за допомогою кольорового віконного графічного інтерфейсу. Підвищення продуктивності ПК дозволило перенести частини системи (інтерфейс із користувачем, прикладну логіку) для

виконання на персональному комп'ютері безпосередньо на робочому місці, а функції обробки даних залишити на центральному комп'ютері. Система стала розподіленою – одна частина функцій виконується на центральному комп'ютері, інша – на персональному, пов'язаному із центральним за допомогою комунікаційної мережі. Таким чином, з'явилася клієнт-серверна модель взаємодії комп'ютерів і програм у мережі й на цій основі стали розвиватися засоби розробки додатків для реалізації інформаційних систем.

Однак дворівнева архітектура "клієнт-сервер" має такі істотні недоліки, як складність адміністрування й низька інформаційна безпека, особливо помітні при порівнянні її з централізованою архітектурою мейнфреймів (табл. 10).

Таблиця 10

Порівняння централізованої архітектури мейнфреймів і дворівневої архітектури "клієнт-сервер"

Централізована архітектура мейнфреймів	**Дворівнева архітектура "клієнт-сервер"**
Уся інформаційна система на центральному комп'ютері	Систему, що складається з великої кількості різнотипних комп'ютерів, на яких працюють різнорідні додатки, важко адмініструвати
1	**2**
На робочих місцях прості пристрої доступу, що дають можливість користувачу управляти процесами в інформаційній системі	Комп'ютери складні в конфігуруванні й пошуку несправностей, вартість обслуговування досить велика
Пристрій доступу спілкується із центральним комп'ютером за допомогою простого, апаратно реалізованого протоколу	Комп'ютер досить уразливий для вірусів і несанкціонованого доступу

Лабораторна робота №1 (2 год.)

Тема: Аналіз структури програмного та апаратного компонентів комп'ютерної мережі

Мета: розвивати у студентів аналітичні вміння з питання виокремлення програмного та апаратного компонентів комп'ютерної мережі;

виховувати ціннісне ставлення студентів до майбутньої професійної діяльності.

Студент повинен знати: загальні принципи побудови простої комп'ютерної мережі, мережеве програмне забезпечення, фізичні основи передачі даних лініями зв'язку.

Студент повинен уміти: аналізувати апаратні та програмні компоненти локальної мережі.

Обладнання: комп'ютерний клас з локальною мережею на основі стандарту Fast Ethernet, картки зі схемами локальних мереж з позначенням апаратного та програмного компонентів мереж.

Інструктаж

1. Скласти переліки апаратних та програмних компонентів для локальної мережі комп'ютерного класу.
2. Обговорити особливості реалізації кожної з компонентів локальної мережі комп'ютерного класу.

Завдання для письмового звіту та спостережень:

– письмовий аналіз апаратного та програмного компонентів локальних мереж відповідно до запропонованої схеми;

– порівняння та аналіз компонентів локальних мереж навчального класу та запропонованої схеми.

Самостійна робота
Тема: Топологія ієрархічної мережі

Мета: розвивати аналітичні вміння студентів з питання проектування топології ієрархічної мережі.

Студент повинен знати: принципи проектування та особливості реалізації топології в ієрархічних комп'ютерних мережах.

Студент повинен уміти: обирати топологію для ієрархічної мережі .

Хід роботи

Теоретична частина

1. Чому топологія мережі має таке велике значення?
2. Чи є топологія мережі та логічна структура мережі взаємозамінними поняттями?
3. Чому ієрархічні мережі складаються з декількох "рівнів"?

Практична частина

Завдання

Законспектуйте основні положення щодо типів топологій в ієрархічних мережах.

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Еволюція комп'ютерних мереж та напрямки їх розвитку".

ТЕМА 1.2. МЕРЕЖЕВІ ХАРАКТЕРИСТИКИ ТА КЛАСИФІКАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Лекція

План

1. Класифікація комп'ютерних мереж.
2. Мережеві топології й методи доступу до середовища передачі даних.

Література

Основна

1. *Антонов В. М.* Сучасні комп'ютерні мережі / Валерій Миколайович Антонов. – К. : МК-Прес, 2005. – 480 с.

2. *Новиков Ю. В.* Локальные сети: Архитектура, алгоритмы, проектирование / Новиков Ю. В., Кондратенко С. В. – М.: ЭКОМ, 2002. – 311 с.: ил.; 23 см. – (Современные компьютерные технологии).

3. *Компьютеры*, сети, Интернет: Энциклопедия: Наиболее

полн. и подроб. рук. / Ю. Новиков, Д. Новиков, А. Черепанов, В. Чуркин; Под общ. ред. Ю. Новикова. – 2. изд. – М. [и др.]: Питер, 2003 (СПб.: ГПП Печ. Двор им. А.М. Горького). – 831 с.: ил.; 24 см.

4. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. – 4-е изд. – М. [и др.]: Питер, 2005. – 991 с.: ил., табл.; 24 см. – (Классика computer science).

Додаткова

1. *Білоус Л. Ф.* Інформаційні мережі : навч. посібник / Білоус Л. Ф. – К. : Логос, 2005. – 140 с.

2. *Буров Є.* Комп'ютерні мережі / Євген Буров [ред. В. Пасічник]. – Л. : БаК, 1999. – 467 с.

3. *Ибе О.* Сети и удаленный доступ: Протоколы, проблемы, решения / Оливер Ибе. – М.: ДМК Пресс, 2002. – 332 с.: ил.; 23 см. – (Серия "Защита и администрирование").

4. *Калита Д. М.* Комп'ютерні мережі. Апаратні засоби та протоколи передачі даних : навч. посіб. для студ. вищих закл. освіти / Калита Д. М.; [ред. Третяк О. В.]. – К. : ВПЦ "Київський ун-т", 2003. – 326 с. – (Автоматизація наукових досліджень).

5. *Контроль* та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології : навчальний посібник / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. – Х. : "Компанія СМІТ", 2004. – 544 с.

6. *Шниер М.* Толковый словарь компьютерных технологий: [Сетевые технологии. Аппарат. средства. Интернет: Пер. с англ.] / Митчелл Шниер. – Киев: DiaSoft, Cop. 2000. – 720 с.: ил., табл.; 24 см. – (Библиотека Скотта Мюллера).

7. *Щербо В.К.* Стандарты вычислительных сетей. Взаимосвязи сетей: Справочник / В.К. Щербо. – М.: Кудиц-образ, 2000. – 268 с.: ил.; 29 см.

1.2.1. Класифікація комп'ютерних мереж

На сьогодні немає загальновизнаної класифікації мереж. Є два фактори для їх розрізнення: технологія передачі й масштаб.

Є два основних *типи технологій передачі*, що використовуються в мережах:

- широкомовна (від одного до багатьох);
- точка-тока.

Мережі широкомовного типу мають єдиний канал передачі

даних, що використовують усі машини мережі. Пакет, відправлений якоюсь машиною, одержують усі інші машини мережі. У певному полі пакета зазначена адреса одержувача. Кожна машина перевіряє це поле, і якщо вона виявляє в ньому адресу, приступає до обробки цього пакета; якщо в цьому полі не її адреса, то вона просто ігнорує цей пакет.

Мережі широкомовного типу, як правило, мають режим, коли один пакет адресується всім машинам у мережі. Це, так званий, широкомовний режим роботи. Є в таких мережах режим групового віщання – той самий пакет одержують машини приналежні до певної групи в мережі.

Мережі точка-точка з'єднують кожну пару машин індивідуальним каналом. Тому, перш ніж пакет досягне адресата, він проходить через кілька проміжних машин. У цих мережах виникає потреба в маршрутизації. Від її ефективності залежить швидкість доставки повідомлень, розподіл навантаження в мережі.

Мережі широкомовного типу, як правило, використовуються на географічно невеликих територіях. Мережі точка-точка – для побудови великих мереж, що охоплюють великі регіони.

Масштаб мережі – інший критерій для класифікації мереж. Довжина зв'язку, що забезпечує комп'ютерна мережа, може бути різною: у межах одного приміщення, будинку, підприємства, регіону, континенту або всього світу.

До *локальних мереж – Local Area Networks (LAN)* – відносять мережі комп'ютерів, зосереджені на невеликій території (звичайно в радіусі не більше 2,5 км). Зазвичай локальна мережа є комунікаційною систему, що належить одній організації. Через короткі відстані в локальних мережах є можливість використання дорогих високоякісних ліній зв'язку, які дозволяють, застосовуючи прості методи передачі даних, досягати високих швидкостей обміну даними порядку 100 Мбіт/с. У зв'язку із цим послуги, надавані локальними мережами, відрізняються широкою розмаїтістю й звичайно передбачають реалізацію в режимі on-line.

Глобальні мережі – Wide Area Networks (WAN) – поєднують територіально розосереджені комп'ютери, які можуть перебувати в різних містах і країнах. Оскільки прокладка високоякісних ліній зв'язку на великі відстані обходиться дуже дорого, у глобальних мережах часто використовуються вже наявні лінії зв'язку, призначені зовсім для інших цілей. Наприклад, багато глобальних мереж

будуються на основі телефонних і телеграфних каналів загального призначення. Через низькі швидкості таких ліній зв'язку в глобальних мережах надавані послуги зазвичай обмежують передачею файлів. Для стійкої передачі дискретних даних по неякісних лініях зв'язку застосовуються методи й устаткування, що істотно відрізняються від методів і устаткування, характерних для локальних мереж. Як правило, тут застосовуються складні процедури контролю й відновлення даних, тому що найбільш типовий режим передачі даних по територіальному каналі зв'язку зв'язаний зі значними перекручуваннями сигналів.

Міські мережі (або мережі мегаполісів) – Metropolitan Area Networks (MAN) – є менш розповсюдженим типом мереж. Вони з'явилися порівняно недавно, й призначені для обслуговування території великого міста – мегаполіса. Тим часом як локальні мережі щонайкраще підходять для поділу ресурсів на коротких відстанях і широкомовних передачах, а глобальні мережі забезпечують роботу на великих відстанях, але з обмеженою швидкістю й небагатим набором послуг, мережі мегаполісів займають деяке проміжне положення. Вони використовують цифрові магістральні лінії зв'язку, часто оптичні, зі швидкостями від 45 Мбіт/с, і призначені для зв'язку локальних мереж у масштабах міста й з'єднання локальних мереж із глобальними. Ці мережі спочатку були розроблені для передачі даних, але також вони підтримують і такі послуги, як відеоконференції й інтегральну передачу голосу й тексту. Розвиток технології мереж мегаполісів здійснювався місцевими телефонними компаніями.

Локальні обчислювальні мережі (ЛОМ) стали сьогодні поширеним через невелику складність і невисоку вартість. Вони використовуються при автоматизації комерційної, банківської діяльності, а також для створення розподілених, керуючих і інформаційно-довідкових систем. ЛОМ мають модульну організацію (рис. 7).

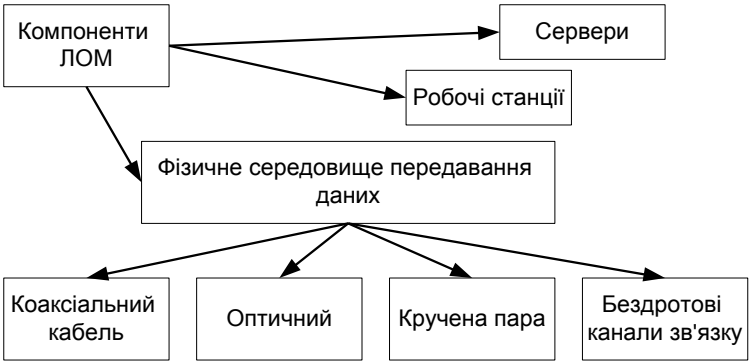


Рис. 7. Компоненти ЛОМ

Їхні основні компоненти:

– сервери – це апаратно-програмні комплекси, які виконують функції керування розподілом мережних ресурсів загального доступу;

– робочі станції – це комп'ютери, що здійснюють доступ до мережних ресурсів, надаваним сервером;

– фізичне середовище передачі даних (мережевий кабель) - це коаксіальні й оптичні кабелі, кручені пари проводів, а також бездротові канали зв'язку (інфрачервоне випромінювання, лазери, радіопередача).

Виділяється два основних типи локальних обчислювальних мереж: однорангові й на основі сервера. Різниця між ними має принципове значення, тому що визначає їхні можливості.

Однорангові мережі. У цих мережах усі комп'ютери рівноправні: немає ієрархії, виділеного сервера. Як правило, кожний ПК функціонує і як робоча станція (РС), і як сервер, тобто немає ПК, відповідального за адміністрування всієї мережі. Усі користувачі вирішують самі, які дані й ресурси на своєму комп'ютері зробити загальнодоступними по мережі.

Робоча група – це невеликий колектив, об'єднаний загальною метою й інтересами. Тому в однорангових мережах найчастіше не більше 10 комп'ютерів. Ці мережі відносно прості, тому що кожний ПК є одночасно й РС, і сервер. Немає необхідності в потужному центральному сервері або в інших компонентах, обов'язкових для більш складних мереж.

Щоб установити однорангову мережу, додаткового

програмного забезпечення не потрібно, а для об'єднання комп'ютерів застосовується проста кабельна система.

Незважаючи на те, що однорангові мережі цілком задовольняють потреби невеликих фірм, виникають ситуації, коли їхнє використання є недоречним. У цих мережах захист передбачає установку пароля на поділюваний ресурс (наприклад, каталог). Централізовано управляти захистом в одноранговій мережі дуже складно, тому що:

– користувач установлює її самостійно;

– "загальні" ресурси можуть перебувати на всіх ПК, а не тільки на центральному сервері.

Така ситуація – загроза для всієї мережі; крім того, деякі користувачі можуть взагалі не встановити захист. Якщо питання конфіденційності є для фірми принциповими, то такі мережі застосовувати не рекомендується. Крім того, оскільки в цих ЛОМ кожний ПК працює і як РС, і як сервер, користувачі повинні мати достатній рівень знань, щоб працювати і як користувачі, і як адміністратори свого комп'ютера.

Клієнт-серверні мережі. При підключенні більше 10 користувачів однорангова мережа може виявитися недостатньо продуктивною. Тому більшість мереж використовує виділені сервери. Виділеними називаються такі сервери, які функціонують тільки як сервер (крім функції РС або клієнта). Вони спеціально оптимізовані для швидкої обробки запитів від мережних клієнтів і для керування захистом файлів і каталогів.

Завдання, які виконують сервери, різноманітні й складні. Щоб пристосуватися до зростаючих потреб користувачів, сервери в ЛОМ спеціалізовані. Так, наприклад, в операційній системі Windows Server існують різні типи серверів:

– файли-сервери й принт-сервери; вони управляють доступом користувачів до файлів і принтерів;

– сервери додатків (у тому числі сервер баз даних, Web-сервер), на них виконуються прикладні частини клієнт-серверних додатків (програм);

– поштові сервери керують передачею електронних повідомлень між користувачами мережі;

– факс-сервери керують потоком вхідних і вихідних факсимільних повідомлень через один або кілька факсів-модемів;

– комунікаційні сервери – керують потоком даних і поштових

повідомлень між даною ЛОМ та іншими мережами або віддаленими користувачами через модем і телефонну лінію; вони ж забезпечують доступ до Інтернету;

– сервер служб каталогів призначений для пошуку, зберігання й захисту інформації в мережі, Windows Server поєднує PC у логічні групи-домени, система захисту яких наділяє користувачів різними правами доступу до будь-якого мережного ресурсу.

Мережі відділів, кампусів, корпоративні мережі. Ще одним популярним способом класифікації мереж є їхній розподіл за масштабом виробничого підрозділу, у межах якого діє мережа. Розрізняють мережі відділів, мережі кампусів і корпоративні мережі.

Мережі відділів – це мережі, які використовуються порівняно невеликою групою співробітників, що працюють в одному відділі підприємства. Ці співробітники вирішують деякі загальні завдання, наприклад, ведуть бухгалтерський облік або займаються маркетингом. Вважається, що відділ може нараховувати до 100-150 співробітників.

Головною метою мережі відділу є поділ локальних ресурсів, зокрема додатків, даних, принтерів й модемів. Звичайно мережі відділів мають один або два файлових сервери й не більше тридцяти користувачів. Мережі відділів не поділяються на підмережі. У цих мережах локалізується більша частина трафіку підприємства. Мережі відділів зазвичай створюються на основі якої-небудь однієї мережної технології – Ethernet, Token Ring.

Завдання керування мережею на рівні відділу відносно просте: додавання нових користувачів, усунення простих відмов, інсталяція нових вузлів і установка нових версій програмного забезпечення. Такою мережею може керувати співробітник, що присвячує обов'язкам адміністратора тільки частину свого часу. Найчастіше адміністратор мережі відділу не має спеціальної підготовки, але є тою людиною у відділі, що краще всіх розбирається в комп'ютерах, і саме собою виходить так, що він займається адмініструванням мережі (рис. 8).

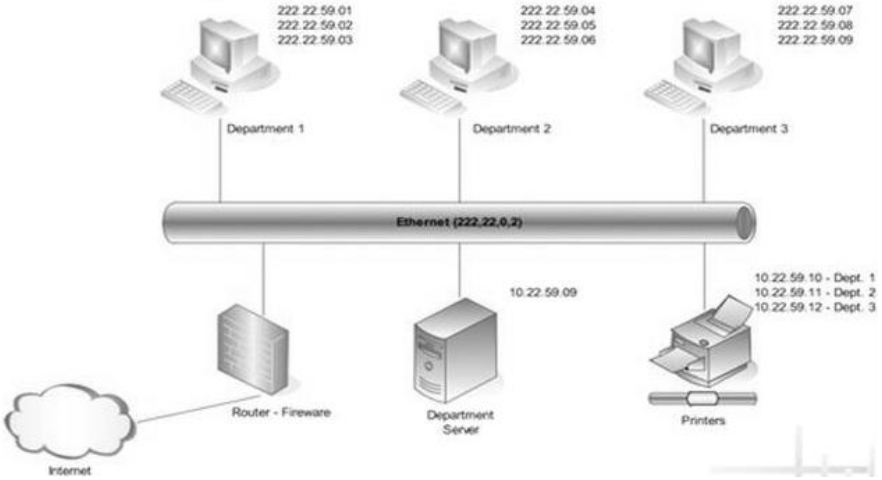


Рис. 8. Приклад мережі масштабу відділу

Існує й інший тип мереж, близький до мереж відділів, – *мережі робочих груп*. До них відносять зовсім невеликі мережі, що включають до 10-20 комп'ютерів. Характеристики мереж робочих груп практично не відрізняються від описаних вище характеристик мереж відділів. Такі властивості, як простота мережі й однорідність, тут проявляються найбільшою мірою, тим часом як мережі відділів можуть наближатися в деяких випадках до наступного за масштабом типу мереж – мереж кампусів.

Мережі кампусів одержали свою назву від англійського слова campus – студентське містечко. Саме на території університетських містечок часто виникала необхідність об'єднання декількох дрібних мереж в одну більшу мережу. Зараз цю назву не пов'язують зі студентськими містечками, а використовують для позначення мереж будь-яких підприємств і організацій.

Головними особливостями мереж кампусів є такі. Мережі цього типу поєднують безліч мереж різних відділів одного підприємства в межах окремого будинку або однієї території, що покриває площу в кілька квадратних кілометрів. При цьому глобальні з'єднання в мережах кампусів не використовуються. Служби такої мережі включають взаємодію між мережами відділів, доступ до загальних баз даних підприємства, факсів-серверів, високошвидкісних модемів і високошвидкісних принтерів. У результаті співробітники кожного

відділу підприємства одержують доступ до файлів і ресурсів мереж інших відділів. Важливою службою мереж кампусів став доступ до корпоративних баз даних незалежно від того, на яких типах комп'ютерів вони розташовуються.

Саме на рівні мережі кампусу виникають проблеми інтеграції неоднорідного апаратного й програмного забезпечення. Типи комп'ютерів, мережевих операційних систем, мережевого апаратного забезпечення можуть відрізнятися в кожному відділі. Звідси випливають складності керування мережами кампусів. Адміністратори повинні бути в такому разі більш кваліфікованими, а засоби оперативного керування мережею – більш досконалими (рис. 9).

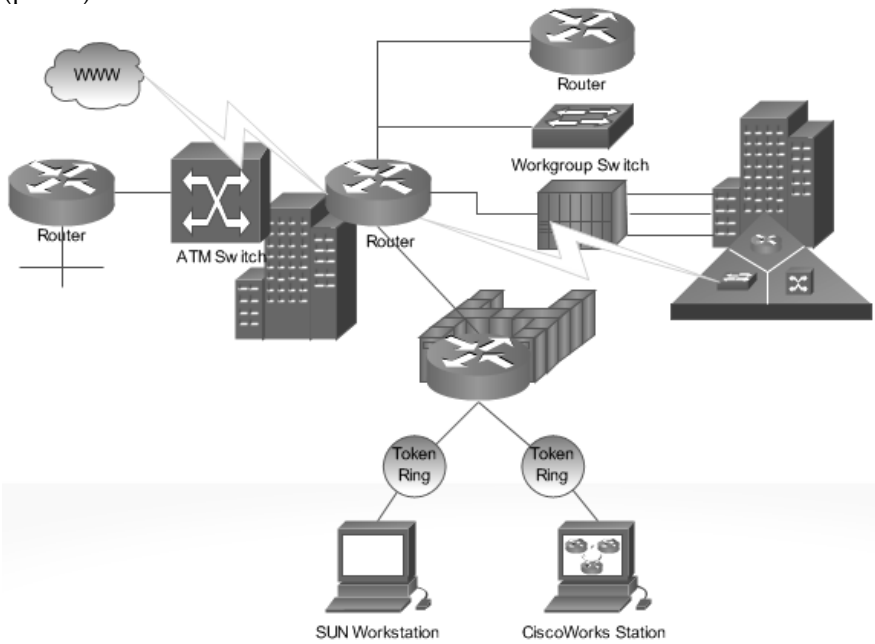


Рис. 9. Приклад мережі кампусу

Корпоративні мережі називають також мережами масштабу підприємства. Вони поєднують велику кількість комп'ютерів на всіх територіях окремого підприємства, можуть бути складно зв'язані й покривати місто, регіон або навіть континент. Число користувачів і комп'ютерів може вимірятися тисячами, а число серверів – сотнями, відстані між мережами окремих територій можуть виявитися такими,

що стає необхідним використання глобальних зв'язків. Для з'єднання віддалених локальних мереж і окремих комп'ютерів у корпоративній мережі застосовуються різноманітні телекомунікаційні засоби, у тому числі телефонні канали, радіоканали, супутниковий зв'язок. Корпоративну мережу можна представити у вигляді "острівців локальних мереж", що плавають у телекомунікаційному середовищі.

У корпоративній мережі обов'язково будуть використовуватися різні типи комп'ютерів – від мейнфреймів до ПК, кілька типів операційних систем і безліч різних додатків. Неоднорідні частини корпоративної мережі повинні працювати як єдине ціле, надаючи користувачам по можливості прозорий доступ до всіх необхідних ресурсів.

При об'єднанні окремих мереж великого підприємства, що має філії в різних містах і навіть країнах, у єдину мережу багато кількісних характеристик об'єднаної мережі перевищують деякий критичний поріг, за яким починається нова якість (рис. 10).

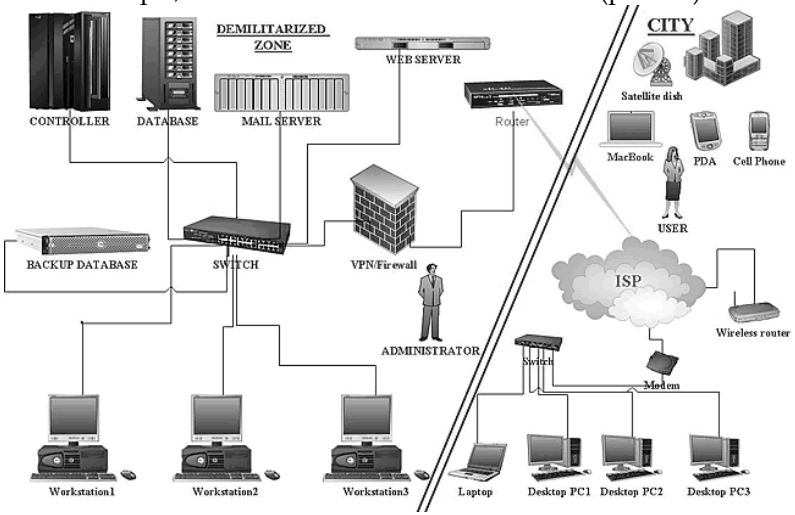


Рис. 10. Приклад корпоративної мережі

Най простіший спосіб її розв'язання – переміщення облікових даних кожного користувача в локальну базу облікових даних кожного комп'ютера, до ресурсів якого користувач повинен мати доступ. При спробі доступу ці дані витягають із локальної облікової бази й на їхній основі доступ надається або не надається. Для невеликої мережі, що складається з 5-10 комп'ютерів і приблизно

такої ж кількості користувачів, такий спосіб є придатним. Але якщо в мережі налічується кілька тисяч користувачів, кожному з яких потрібний доступ до декількох десятків серверів, то це рішення стає вкрай неефективним. Адміністратор повинен повторити кілька десятків разів операцію занесення облікових даних користувача. Сам користувач також змушений повторювати процедуру логічного входу щораз, коли йому потрібний доступ до ресурсів нового сервера. Розв'язання цієї проблеми для великої мережі – використання централізованої довідкової служби, у базі даних якої зберігаються облікові записи всіх користувачів мережі. Адміністратор один раз виконує операцію занесення даних користувача в цю базу, а користувач один раз виконує процедуру логічного входу, причому не в окремий сервер, а в мережу в цілому.

При переході від більш простого типу мереж до більш складного – від мереж відділу до корпоративної мережі – мережа повинна бути усе більш надійною, при цьому вимоги до її продуктивності також істотно зростають. У міру збільшення масштабів мережі збільшуються і її функціональні можливості. Мережею циркулюють дані, кількість яких збільшується і мережа повинна забезпечувати їх безпеку й захищеність поряд з доступністю. З'єднання, що забезпечують взаємодію, повинні бути більше прозорими. При переході на наступний рівень складності комп'ютерне обладнання мережі стає усе більш різноманітним, а географічні відстані збільшуються, роблячи досягнення цілей більше складним; проблемним, а керування такими з'єднаннями стає дорогим.

1.2.2. Мережеві топології й методи доступу до середовища передачі даних

Топологія мережі характеризує взаємозв'язки й просторове розташування компонентів мережі – мережних комп'ютерів (хостів), робочих станцій, кабелів та інших активних і пасивних пристроїв. Топологія впливає на:

– склад і характеристики устаткування мережі;
– можливості розширення мережі;
– спосіб керування мережею.

Усі мережі будуються на основі трьох базових топологій:

– шина (bus);

– зірка (star);
– кільце (ring).

Метод доступу до середовища передачі даних визначає, як поділяється ресурс – мережевий кабель – надається вузлам мережі для здійснення передачі даних. Основні методи доступу до середовища передачі даних:

– множинний доступ з контролем несучої й виявленням колізій – CSMA/CD;
– з передачею маркера;
– за пріоритетом запиту.

Шинна топологія. За допомогою кабелю кожна робоча станція з'єднується з іншими робочими станціями й з файловим сервером. Кабель проходить від вузла до вузла, послідовно з'єднуючи всі станції та файлові сервери. На кожному кінці кабелю підключається термінатор для запобігання відбиттю сигналу (рис. 11).

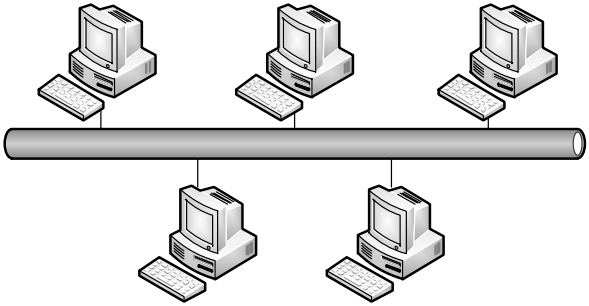


Рис. 11. Шинна топологія

Шинна топологія використовує метод доступу CSMA/CD. Це означає, що інформацію приймає тільки той комп'ютер, адреса якого відповідає адресі одержувача, зашифрованій у переданих сигналах. Інші комп'ютери відкидають повідомлення. Перед передачею даних комп'ютер повинен очікувати звільнення шини. У кожний момент часу відправляти повідомлення може тільки один комп'ютер, тому число підключених до мережі машин значно впливає на її швидкодію.

Переваги шинної топології:

– надійно працює в невеликих мережах, проста у використанні;
– вимагає менше кабелю для з'єднання комп'ютерів і тому

дешевше, ніж інші схеми з'єднання;

– легко розширюється за рахунок стикування кабельних сегментів за допомогою з'єднувача BNC і використання повторювачів.

Недоліки шинної топології:

– інтенсивний мережевий трафік знижує продуктивність мережі; при великій кількості комп'ютерів у мережі станції часто переривають один одного, і чимала частина смуги пропущення губиться; при додаванні комп'ютерів до мережі різко падає продуктивність;

– циліндричні з'єднувачі послабляють електричний сигнал, і велика їх кількість викликає порушення в передачі інформації із шини;

– розрив кабелю або неправильне функціонування однієї зі станцій може привести до порушення працездатності всієї мережі. Мережу важко діагностувати.

Зіркоподібна топологія. Кожний комп'ютер у мережі з топологією типу "зірка" ("star") взаємодіє із центральним концентратором (*hub* – пристрій для повторення мережевих сигналів) (рис. 12).

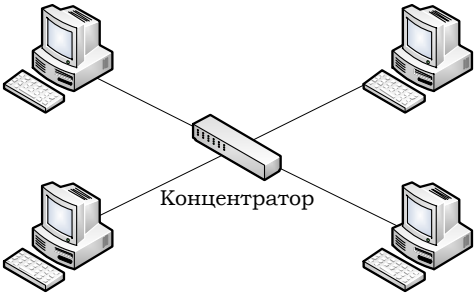


Рис. 12. Топологія "зірка"

Hub – пристрій множинного доступу, що виконує роль центральної точки з'єднання в топології "фізична зірка". Поряд із традиційною назвою "концентратор" у літературі трапляється також термін "хаб".

У зіркоподібній мережі використовується метод доступу CSMA/CD до середовища – концентратор (хаб) передає повідомлення всім комп'ютерам. У зіркоподібній мережі з комутацією комутатор передає повідомлення тільки комп'ютеру-

адресатові.

Активний концентратор регенерує електричний сигнал і посилає його всім підключеним комп'ютерам. Такий тип концентратора часто називають multiport repeater. Для роботи активних концентраторів і комутаторів потрібне живлення від мережі. Пасивні концентратори, наприклад, комутаційна кабельна панель або комутаційний блок, діють як точка з'єднання, не підсилюючи й не регенеруючи сигнал. Електроживлення пасивні концентратори не вимагають.

Гібридний концентратор дозволяє використовувати в одній зіркоподібній мережі різні типи кабелів. Розширити зіркоподібну мережу можна шляхом підключення замість одного з комп'ютерів ще одного концентратора й приєднання до нього додаткових станцій, у результаті чого виходить гибридно-зіркоподібна мережа (рис. 13).

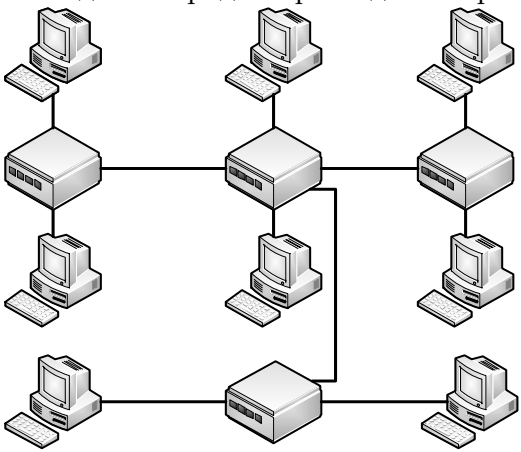


Рис. 13. Гибридно-зіркоподібна топологія

Переваги топології "зірка "(Ethernet 10Base, 100Base). Центральний концентратор зіркоподібної мережі зручно використовувати для діагностики.

Інтелектуальні концентратори (пристрої з мікропроцесорами, доданими для повторення мережних сигналів) забезпечують також вимір параметрів (моніторинг) і керування мережею. Відмова одного комп'ютера не обов'язково приводить до зупинки всієї мережі. Концентратор здатний виявляти відмови й ізолювати таку машину або мережевий кабель, що дозволяє мережі продовжувати роботу. В

одній мережі допускається застосування декількох типів кабелів (якщо їх дозволяє використати концентратор).

Недоліки мережі із зіркоподібною топологією:

– при відмові центрального концентратора вся мережа стає непрацездатною;

– усі комп'ютери повинні з'єднуватися із центральною точкою, це збільшує витрату кабелю, отже, такі мережі обходяться дорожче, ніж мережі з іншою топологією.

Кільцева топологія. На рис. 14 наведений приклад топології ЛОМ, у якій кожна робоча станція з'єднана із двома іншими робочими станціями. Така топологія називається кільцем (ring).

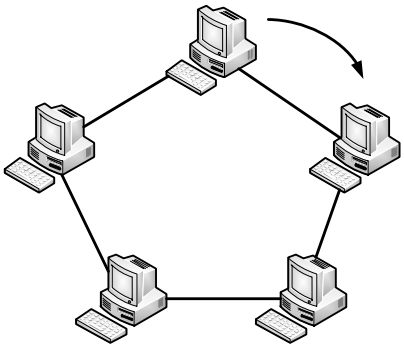


Рис. 14. Кільцева топологія

Кільцева топологія застосовується переважно в США для мереж, що вимагають виділення певної частини смуги пропущення для критичних за часом засобів (наприклад, для передачі відео й аудіо), у високопродуктивних мережах, а також при великій кількості клієнтів, що звертаються до мережі (що вимагає її високої пропускної здатності). У мережі з кільцевою топологією кожний комп'ютер з'єднується з наступним комп'ютером, що ретранслює ту інформацію, яку він одержує від першої машини. Завдяки такій ретрансляції мережа є активною, і в ній не виникають проблеми втрати сигналу, як у мережах із шинною топологією. Крім того, оскільки "кінця" у кільцевій мережі немає, ніяких кінцевих навантажень не потрібно.

Деякі мережі з кільцевою топологією використовують метод доступу до середовища на основі маркера (метод естафетної передачі). Спеціальне коротке повідомлення-маркер циркулює по

кільцю поки комп'ютер не захоче передати інформацію іншому вузлу. Він модифікує маркер, додає адресу й дані, а потім відправляє його по кільцю. Кожний з комп'ютерів послідовно одержує даний маркер з доданою інформацією й передає його сусідній машині, поки електронна адреса не збіжиться з адресою комп'ютера-одержувача або маркер не повернеться до відправника. Комп'ютер, що одержав повідомлення, повертає відправникові відповідь, яка підтверджує, що послання прийняте. Тоді відправник створює ще один маркер і відправляє його в мережу, що дозволяє іншій станції перехопити маркер і почати передачу. Маркер циркулює по кільцю, поки яка-небудь зі станцій не буде готова до передачі й не захопить його.

Усі ці події відбуваються дуже часто: маркер може пройти кільце з діаметром в 200 м приблизно 10000 разів у секунду. У деяких ще більш швидких мережах циркулює відразу кілька маркерів. В інших мережних середовищах застосовуються два кільця із циркуляцією маркерів у протилежних напрямках. Така структура сприяє відновленню мережі в разі виникнення відмов.

Переваги мережі з кільцевою топологією:

– оскільки всім комп'ютерам надається однаковий до маркера, ніхто з них не зможе монополізувати мережу;

– справедливе спільне використання мережі забезпечує поступове зниження її продуктивності в разі збільшення числа користувачів і перевантаження (краще, якщо мережа буде продовжувати функціонувати, хоча й повільно, чим відразу відмовить при перевищенні пропускної здатності).

Недоліки мережі з кільцевою топологією:

– відмова одного комп'ютера в мережі може вплинути на працездатність усієї мережі;

– кільцеву мережу важко діагностувати;

– додавання або видалення комп'ютера змушує розривати мережу.

Змішані топології. На основі трьох базових топологій можна створювати так звані гібридні або змішані топології. До цих топологій належать:

– шинно-зіркоподібна;

– зіркоподібна-кільцева.

Шинно-зіркоподібна топологія комбінує мережі типу "зірка" і

"шина", зв'язуючи кілька концентраторів шинними магістралями (рис. 15).

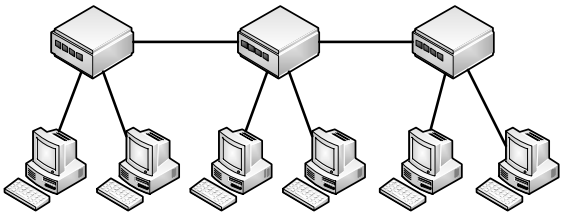


Рис. 15. Шинно-зіркоподібна топологія

Якщо один з комп'ютерів відмовляє, концентратор може виявити комп'ютер, що відмовив, і ізолювати несправну машину. При відмові концентратора з'єднані з ним комп'ютери не зможуть взаємодіяти з мережею, а шина розімкнеться на два не зв'язаних один з одним сегменти.

У зіркоподібній-кільцевій топології (яку називають також кільцем із з'єднанням типу "зірка") мережеві кабелі прокладаються аналогічно зіркоподібної мережі, але в центральному концентраторі реалізується кільце (рис. 16).

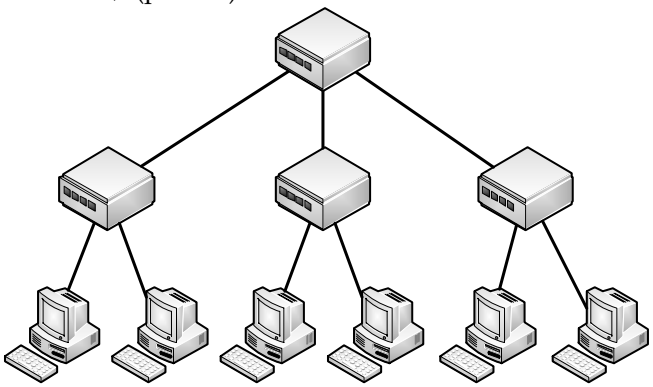


Рис. 16. Зіркоподібна-кільцева топологія

Із внутрішнім концентратором можна з'єднати зовнішні, тим самим, розширивши петлю внутрішнього кільця.

Лабораторна робота №2 (2 год.)
Тема: Аналіз та визначення виду комп'ютерної мережі

Мета: розвивати у студентів аналітичні вміння з визначення виду комп'ютерної мережі;

виховувати ціннісне ставлення студентів до навчальної діяльності.

Студент повинен знати: класифікацію комп'ютерних мереж; мережеві характеристики, що впливають на вибір виду комп'ютерної мережі.

Студент повинен уміти: аналізувати характеристики комп'ютерної мережі та визначати її вид відповідно до класифікації.

Обладнання: комп'ютерний клас з мережею стандарту Fast Ethernet, приклади комп'ютерних мереж відповідно до класифікації.

Інструктаж

1. Розглянути приклади комп'ютерних мереж відповідно до класифікації.
2. Визначити основні характеристики запропонованих прикладів комп'ютерних мереж.
3. Проаналізувати відмінності прикладів комп'ютерних мереж
4. Дати оцінку видам комп'ютерних мереж, поданих у прикладах.

Практична частина

Проаналізуйте вид комп'ютерної мережі за вказаною схемою.

1. Розмір мережі.
2. Апаратне устаткування мережі.
3. Програмний компонент мережі.
4. Призначення та використання мережі.

Самостійна робота №2

Тема: Функції та призначення ядра мережі

Мета: розвивати у студентів уміння аналізувати та визначати функції ядра комп'ютерної мережі.

Студент повинен знати: функції та призначення видів ядра комп'ютерної мережі.

Студент повинен уміти: визначати вид ядра комп'ютерної мережі в залежності від виконуваних ним функцій.

Хід роботи

Теоретична частина

1. Яка первинна мета ядра мережі? Які стратегії використовуються для досягнення цієї мети?

2. Обґрунтуйте виняткову важливість оптимальної маршрутизації в ядрі мережі?

3. Назвіть два фактори, від яких залежить час, необхідний протоколу маршрутизації для завершення процесу збіжності.

Практична робота

Проаналізуйте літературу та обґрунтуйте правильність тези: "Існують дві основні стратегії, що дозволяють домогтися максимальної продуктивності ядра мережі:

– у ядрі не повинні реалізовуватися мережні правила;

– кожен пристрій ядра повинен мати можливість доступу до кожного пункту призначення мережі."

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Сучасні підходи до реалізації комутації пакетів у глобальних мережах".

МОДУЛЬНА КОНТРОЛЬНА РОБОТА №1

Оберіть номер правильної відповіді:

1. Із чого складається найпростіша мережа?

а) з декількох персональних комп'ютерів, з'єднаних між собою мережевим кабелем;

б) з 2 персональних комп'ютерів, з'єднаних між собою

0-модемним кабелем;

в) з декількох ЕОМ, один із яких обов'язково наділяється правами сервера.

1 б.

2. *Що означає паралельна передача даних?*

а) дані передаються одночасно по декількох проводах;

б) дані передаються по черзі біт за бітом.

1 б.

3. *Принцип архітектури "клієнт-сервер":*

а) існує виділений сервер, що надає всілякі сервіси, і безліч клієнтських ПК, що використовують їх у своїх цілях;

б) кожний ПК є як сервером, так і клієнтом;

в) жоден із ПК не має повноваження сервера.

1 б.

4. *Однорангові мережі – це:*

а) мережі з одним виділеним сервером;

б) мережі з одним і більше виділеними серверами;

в) мережі, де всі комп'ютери рівноправні.

1 б.

5. *Дуплексний зв'язок використовується для …*

а) одночасного прийому і передачі даних на комп'ютері;

б) зв'язку клієнта та сервера;

в) визначення повноваження сервера.

1 б.

6. *Мережі відділів – це:*

а) локальні мережі, що мають вихід у глобальну мережу Internet;

б) мережі, які використовуються порівняно невеликою групою співробітників, що працюють в одному відділі підприємства.

в) локальні мережі, що не мають вихід у глобальну мережу Internet і функціонують без виділеного сервера.

1 б.

7. *Мережі кампусів – це:*

а) мережі, що поєднують множину мереж різних відділів одного підприємства в межах окремого будинку або в межах однієї території:

б) підмережі мереж відділів;

в) локальні мережі, що не мають вихід у глобальну мережу Internet і функціонують без виділеного сервера.

1 б.

8. Яка з топологій використовує метод доступу до середовища на основі маркера:

а) зірка;

б) шина;

в) кільце.

1 б.

9. Яка з топологій не належить до змішаних?

а) шинно-зіркоподібна;

б) зіркоподібна-кільцева;

в) шинно-кільцева.

1 б.

10. Технологія передачі даних, що використовуються в мережах:

а) бітова;

б) символьна;

в) широкомовна (від одного до багатьох).

1 б.

Усього: 10 балів.

Правильні відповіді

Питання	1	2	3	4	5	6	7	8	9	10
Відповідь	б	а	а	в	а	б	а	в	в	в

ЗМІСТОВИЙ МОДУЛЬ 2

АРХІТЕКТУРА І СТАНДАРТИЗАЦІЯ МЕРЕЖ.

ТЕХНОЛОГІЇ ФІЗИЧНОГО РІВНЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Таблиця 11

Тематичний план змістового модуля

№ теми	Назва змістового модуля, теми	Усього годин	Лекції	Лабораторні заняття	Самостійна та індивідуальна робота
2.1	Архітектура і стандартизація мереж	9	2	2	5
2.2	Технології фізичного рівня комп'ютерних мереж	9	2	2	5
	Разом	***18***	***4***	***4***	***10***

Навчальні цілі: сприяти засвоєнню студентами знань щодо архітектури і стандартизації мереж, ліній зв'язку та їх характеристик; ознайомити з напрямками розвитку стандартизації комп'ютерних мереж, зокрема моделлю OSI.

Основні поняття: мережева взаємодія, модель OSI, інформаційні послуги, транспортні послуги, типи кабелів, мультиплексування, комутація, корекція помилок.

Методичні рекомендації щодо роботи з модулем: робота з модулем передбачає засвоєння лекційного матеріалу, участь у лабораторних заняттях, написання реферату (окремими студентами), самостійну роботу над визначеними питаннями теми, модульний контроль у формі тестування.

Після опрацювання цих тем студент може отримати бали,

наведені в табл. 12.

Таблиця 12

Оцінювання навчальних досягнень студентів

Поточний контроль					**Контрольна рейтингова оцінка**	**Проміжна рейтингова оцінка**
Робота на лабораторному занятті		**Самостійна робота**		**Індивідуальне завдання**		
Тема №2.1	**Тема №2.2**	**Тема №2.1**	**Тема №2.2**			
5	5	2	3	5	10	30

ТЕМА 2.1. АРХІТЕКТУРА І СТАНДАРТИЗАЦІЯ МЕРЕЖ

Лекція

План

1. Еталонна модель OSI
2. Характеристика стеків комунікаційних протоколів

Література

Основна

1. *Жуков І. А.* Комп'ютерні мережі та технології: навч. посіб. для студ. вищих навч. закл. / Жуков І. А., Гуменюк В. О., Альтман І. Є.. – К. : НАУ, 2004. – 276 с. – (Комп'ютерні технології).

2. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

3. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. – 4-е изд. – М. [и др.]: Питер, 2005. – 991 с.: ил., табл.; 24 см. – (Классика computer science).

Додаткова

1. *Бабій М. С.* Локальні мережі ЕОМ: [навч. посіб. для студ. спец. "Прикладна математика"] / Михайло Семенович Бабій. –

Суми : Видавництво СумДУ, 2003. – 64 с.

2. *Бортник Г. Г.* Мережі доступу: навч. посібник для студ. напряму підготовки 0924 – "Телекомунікації" всіх спец. / Бортник Г. Г., Стальченко О. В., Яблонський В. Ф. – Вінниця : ВНТУ, 2006. – 139 с.

3. *Коваленко А. Є.* Корпоративні комп'ютерні мережі та телекомунікації : конспект лекцій для студ. спец. 7.080401 "Інформаційні управляючі системи та технології" ден. форми навч. / Анатолій Єпіфанович Коваленко. – К. : НУХТ, 2004. – 27 с.

2.1.1. Еталонна модель OSI

Обмін інформацією між комп'ютерами, об'єднаними в мережу, дуже складне завдання. Це пов'язане з тим, що існує багато виробників апаратних і програмних засобів обчислювальних систем. Єдиний вихід – уніфікувати засоби сполучення систем, а саме використати відкриті системи. Відкрита система взаємодіє з іншими системами відповідно до прийнятих стандартів.

У 1984р. Міжнародна Організація зі Стандартизації (ISO) випустила стандарт – *еталонна модель взаємодії відкритих систем (Seven-layer Open System Interconnection Reference Model – OSI)*, щоб допомогти постачальникам створювати сумісні мережеві апаратні й програмні засоби. Модель OSI являє собою універсальний стандарт на взаємодію двох систем (комп'ютерів) через обчислювальну мережу.

Ця модель описує функції семи ієрархічних рівнів і інтерфейси взаємодії між рівнями. Кожний рівень визначається сервісом, який він надає рівню, що стоїть вище, і протоколом – набором правил і форматів даних для взаємодії між собою об'єктів одного рівня, котрі працюють на різних комп'ютерах.

Кожний рівень підтримує інтерфейси з вищим і нижчим рівнями.

Нижче перераховані (у напрямку зверху вниз) рівні моделі OSI і зазначені їхні загальні функції.

Прикладний рівень (Application) – інтерфейс із прикладними процесами.

Рівень подання (Presentation) – узгодження подання (форматів, кодувань) даних прикладних процесів.

Сеансовий рівень (Session) – установлення, підтримка й закриття

логічного сеансу зв'язку між віддаленими процесами.

Транспортний рівень (Transport) – забезпечення безпомилкового наскрізного обміну потоками даних між процесами під час сеансу.

Мережевий рівень (Network) – фрагментація й збірка переданих транспортним рівнем даних, маршрутизація й просування їх по мережі від комп'ютера-відправника до комп'ютера-одержувача.

Канальний рівень (Data Link) – керування каналом передачі даних, доступом до середовища передачі, передача даних по каналу, виявлення помилок у каналі та їх корекція.

Фізичний рівень (Physical) – фізичний інтерфейс із каналом передачі даних, подання даних у вигляді фізичних сигналів і їх кодування.

Принципи виділення цих рівнів такі: кожний рівень відбиває належний рівень абстракції, має певну функцію. Ця функція вибиралася, насамперед, так, щоб можна було визначити міжнародний стандарт. Границі рівнів вибиралися так, щоб мінімізувати потік інформації через інтерфейси.

Два най нижчих рівні – фізичний і канальний – реалізуються апаратними й програмними засобами, інші п'ять, більш високих рівнів, реалізуються, як правило, програмними засобами (рис. 17).

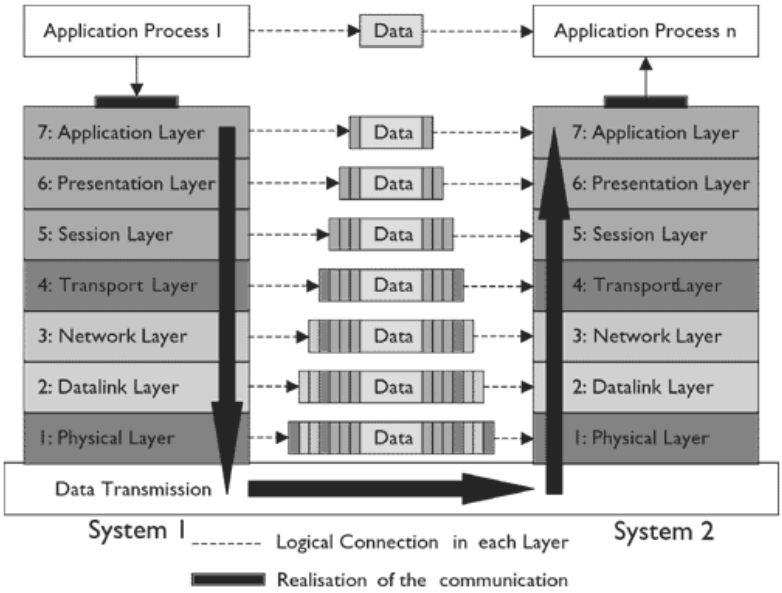


Рис. 17. Модель взаємодії відкритих систем ISO/OSI

При просуванні пакета даних по рівнях зверху вниз кожний новий рівень додає до пакета свою службову інформацію у вигляді заголовка й, можливо, трейлера (інформації, що поміщає в кінець повідомлення). Ця операція називається інкапсуляцією даних верхнього рівня в пакеті нижнього рівня. Службова інформація призначається для об'єкта того ж рівня на віддаленому комп'ютері, її формат і інтерпретація визначаються протоколом даного рівня.

Коли повідомлення по мережі надходить на іншу машину, воно послідовно переміщається нагору з рівня на рівень. Кожний рівень аналізує, обробляє й видаляє заголовок свого рівня, виконує відповідному даному рівню функції й передає повідомлення наступному рівню. Той у свою чергу розглядає ці дані як пакет зі своєю службовою інформацією й даними для більш верхнього рівня, і процедура повторюється, поки дані користувача, очищені від усієї службової інформації, не досягнуть прикладного процесу.

Крім терміна "повідомлення" (message), існують інші назви, використовувані мережними фахівцями для позначення одиниці обміну даними. У стандартах ISO для протоколів будь-якого рівня використовується такий термін як "*протокольний блок даних*" – *Protocol Data Unit (PDU)*. Крім цього, часто послуговуються назвами *кадр (frame)*, *пакет (packet)*, *дейтаграма (datagram)*.

Тепер розглянемо кожний рівень цієї моделі. Зазначимо, що це модель, а не архітектура мережі. Вона не визначає протоколів і сервіс кожного рівня, а лише говорить, що він повинен робити.

Фізичний рівень. Цей рівень має справу з передачею біт по фізичних каналах, таким, наприклад, як коаксіальний кабель, кручена пара або оптичний кабель. До цього рівня мають відношення характеристики фізичних середовищ передачі даних, зокрема смуга пропущення, перешкодозахищеність, хвильовий опір та інші. На цьому ж рівні визначаються характеристики електричних сигналів: вимоги до фронтів імпульсів, рівня напруги або струму переданого сигналу, тип кодування, швидкість передачі сигналів. Крім цього, тут стандартизуються типи з'єднувачів і призначення кожного контакту.

Цей рівень відповідає за передачу послідовності біт через канал зв'язку. Основна проблема: не можна гарантувати, що якщо на одному кінці послали 1, то на іншому одержали 1, а не 0. На цьому

рівні вирішують такі питання, якою напругою треба представляти 1, а якою – 0; скільки мікросекунд витрачатися на передачу одного біта; чи варто підтримувати передачу даних в обох напрямках одночасно; як установлюється початкове з'єднання і як воно розривається; яка кількість контактів на мережевому з'єднувачі, для чого використовується кожний контакт. Тут в основному питання механіки, електрики.

Функції фізичного рівня реалізуються в усіх пристроях, підключених до мережі. З боку комп'ютера функції фізичного рівня виконуються мережним адаптером або послідовним портом.

Прикладом протоколу фізичного рівня може служити специфікація 10Base-T технології Ethernet.

Канальний рівень. Основним завданням рівня каналу даних – перетворити недосконале середовище передачі в надійний канал, вільний від помилок передачі. Іншим завданням канального рівня є реалізація механізмів виявлення й корекції помилок. Це завдання розв'язується поділом даних відправника на фрейми (зазвичай від декількох сотень до декількох тисяч байтів), передачею фреймів послідовно й обробкою фреймів повідомлення, що надходять від одержувача. Оскільки фізичний рівень не розпізнає структури в переданих даних, завданням каналу даних є визначення границь фрейму. Це завдання вирішується введенням спеціальної послідовності біт, що додається в початок і в кінець фрейму й завжди інтерпретуються як границі фрейму.

Перешкоди на лінії можуть зруйнувати фрейм. У такому разі він повинен бути переданий повторно. Він буде повторений також і тоді, коли фрейм повідомлення буде загублений. І рівень має боротися з дублікатами того самого фрейму, втратами або перекручуваннями фреймів. Рівень каналу даних може підтримувати сервіс різних класів для мережного рівня, різної якості й вартості.

У протоколах канального рівня, використовуваних у локальних мережах, закладена певна структура зв'язків між комп'ютерами й способи їхньої адресації. Хоча канальний рівень і забезпечує доставку кадру між будь-якими двома вузлами локальної мережі, він це робить тільки в мережі з певною топологією зв'язків, саме тією топологією, для якої він був розроблений. До таким типових топологій, що підтримуються протоколами канального

рівня локальних мереж, відносяться загальна шина, кільце й зірка.

На фізичному рівні просто пересилаються біти. При цьому не враховується, що в деяких мережах, де лінії зв'язку використовуються (розділяються) попеременно декількома парами комп'ютерів, що взаємодіють, фізичне середовище передачі може бути зайнятим. Тому одним із завдань канального рівня є перевірка доступності середовища передачі. У локальних мережах протоколи канального рівня використовуються комп'ютерами, мостами, комутаторами й маршрутизаторами. У комп'ютерах функції канального рівня реалізуються спільними зусиллями мережних адаптерів та їхніх драйверів.

Прикладами протоколів "точка-точка" (як часто називають такі протоколи) можуть служити широко розповсюджені протоколи PPP і LAP-B, Ethernet, Token Ring, FDDI.

Мережевий рівень. Цей рівень забезпечує можливість з'єднання й вибір маршруту між двома кінцевими системами, підключеними до різних підмереж. Маршрути можуть бути визначені заздалегідь і прописані в статичній таблиці, що не змінюється. Вони можуть визначатися в момент установлення з'єднання. Нарешті, вони можуть будуватися динамічно залежно від завантаження мережі.

Якщо в підмережі циркулює занадто багато пакетів, то вони можуть використати ті самі маршрути, що спричинятиме затори. Ця проблема так само розв'язується на мережевому рівні.

Оскільки за використання підмережі, як правило, передбачається оплата, то на цьому рівні також присутні функції обліку: як багато байт, символів послав або одержав абонент мережі. Якщо абоненти розташовані в різних країнах, де різні тарифи, то треба належним чином скорегувати ціну послуги.

Мережевий рівень служить для створення єдиної транспортної системи, що поєднує кілька мереж з різними принципами передачі інформації між кінцевими вузлами.

Усередині мережі доставка даних регулюється канальним рівнем, а от доставкою даних між мережами займається мережевий рівень.

Повідомлення мережного рівня прийнято називати *пакетами (packets)*. При організації доставки пакетів на мережному рівні використовується поняття "номер мережі". У цьому випадку адреса одержувача складається з номера мережі й номера комп'ютера в цій

мережі.

На мережному рівні визначається два види протоколів. Перший вид відноситься до визначення правил передачі пакетів з даними кінцевих вузлів від вузла до маршрутизатора й між маршрутизаторами. Саме про ці протоколи звичайно йдеться, коли говорять про протоколи мережевого рівня. До мережевого рівня відносять і інший вид протоколів, називаних протоколами обміну маршрутною інформацією. За допомогою цих протоколів маршрутизатори збирають інформацію про топологію міжмережевих з'єднань.

Прикладами протоколів мережевого рівня є протокол міжмережевої взаємодії IP стека TCP/IP і протокол міжмережевого обміну пакетами IPX стека Novell.

Транспортний рівень. Транспортний рівень забезпечує інтерфейс між процесами й мережею, встановлює логічні канали між процесами й забезпечує передачу по цих каналах інформаційних блоків. Ці логічні канали називаються транспортними.

Основна функція транспортного рівня – прийняти дані з рівня сесії, розділити, якщо треба, на більш дрібні одиниці, передати на мережевий рівень і подбати, щоб усі вони дійшли повністю до адресата. Усе це має бути зроблене ефективно й так, щоб сховати від вищого рівня непринципові зміни на нижніх рівнях.

Транспортний рівень визначає, який тип сервісу надати вищим рівням і користувачам мережі. Часто використовуваним сервісом є канал точка-точка без помилок, що забезпечує доставку повідомлень або байтів у тій послідовності, у якій вони були відправлені. Інший вид сервісу – доставка окремих повідомлень без гарантії збереження їхньої послідовності, розсилання одного повідомлення багатьом у режимі віщання. Тип сервісу визначається при встановленні транспортного з'єднання.

Транспортний рівень також відповідає за встановлення й розрив транспортного з'єднання в мережі. Це передбачає наявність механізму іменування, тобто процес на одній машині повинен уміти вказати, з ким у мережі йому треба обмінятися інформацією. Транспортний рівень також повинен запобігати "перевантаженню" одержувача в разі дуже "швидко" відправника. Механізм для цього називається управління потоком. Він є й на інших рівнях. Однак керування потоком між хостами відрізняється від керування потоком

між маршрутизаторами, хоча в них є загальні принципи.

Як правило, усі протоколи, починаючи із транспортного рівня й вище, реалізуються програмними засобами кінцевих вузлів мережі – компонентами їх мережевих операційних систем. Як приклад транспортних протоколів можна привести протоколи TCP і UDP стека TCP/IP і протокол SPX стека Novell.

Сеансовий рівень. Рівень сесії дозволяє користувачам на різних машинах (нагадаємо, що користувачем може бути програма) установлювати сесії. Сесія дозволяє передавати дані, як це може робити транспортний рівень, але, крім того, цей рівень має більш складний сервіс, корисний у деяких додатках. Наприклад, вхід у віддалену систему, передача файлів між двома додатками.

Одна з послуг цього рівня – керування діалогом. Потоки даних можуть бути санкціоновані в обох напрямках одночасно або по черзі в одному напрямку. Сервіс на рівні сесії буде керувати напрямком передачі.

Інший вид сервісу – керування маркером. Для деяких протоколів неприпустиме виконання однієї й тієї ж операції на обох кінцях з'єднання одночасно. Для цього рівень сесії виділяє активний бік маркера. Операцію може виконувати той, хто володіє маркером.

Іншою послугою рівня сесії є синхронізація. Нехай нам треба передати файл такий, що його пересилання займе дві години, між машинами, час роботи на відмову, у яких одна година. Передавання такого файлу засобами транспортного рівня не можливе. Рівень сесії дозволяє розставляти контрольні точки. У разі відмови однієї з машин передача відновиться з останньої контрольної точки.

Сеансовий рівень забезпечує керування діалогом для того, щоб фіксувати, яка зі сторін є активною в цей момент, а також надає засоби синхронізації. Останні дозволяють вставляти контрольні точки в довгі передачі, щоб у разі відмови можна було повернутися назад до останньої контрольної точки, замість того, щоб починати все з початку. На практиці додатки рідко використовують сеансовий рівень, і він рідко реалізується.

Рівень подання. Рівень подання визначає синтаксис, формати й структури подання переданих даних (але не торкається семантики, значення даних). Для того щоб інформація, що посилає із прикладного рівня однієї системи, була іншою системою прочитана на прикладному рівні, представницький рівень здійснює трансляцію

між відомими форматами подання інформації за рахунок використання загального формату. Цей рівень має справу з інформацією, а не з потоком біт.

Типовим прикладом послуги на цьому рівні – уніфіковане кодування даних. Річ у тому, що на різних машинах використовуються різні способи кодування ASCII, Unicode і т.п. для символів, різні способи подання цілих – у прямому, зворотному або додатковому коді, нумерація біт у байті ліворуч, праворуч або навпаки й т.п. Користувачі, як правило, використовують структури даних, а не випадковий набір байт. Для того, щоб машини з різним кодуванням і поданням даних могли взаємодіяти, передані структури даних визначаються спеціальним абстрактним способом, що не залежить від кодування, використовуваного при передачі. Рівень подання працює зі структурами даних в абстрактній формі, перетворює це подання у внутрішнє для конкретної машини й із внутрішнього, машинного, подання в подання для передачі мережею.

На цьому рівні може виконуватися шифрування й дешифрування даних, завдяки якому таємність обміну даними забезпечується відразу для всіх прикладних сервісів.

Прикладний рівень. На відміну від інших рівнів, прикладний рівень – найближчий до користувача рівень OSI – не надає послуги іншим рівням OSI, однак він забезпечує прикладні процеси, що лежать за межами масштабу моделі OSI.

Прикладний рівень забезпечує безпосередню підтримку прикладних процесів і програм кінцевого користувача і керування взаємодією цих програм з мережею передачі даних.

Прикладний рівень – це просто набір різноманітних протоколів, за допомогою яких користувачі мережі одержують доступ до поділюваних ресурсів, зокрема файлів, принтерів або гіпертекстових Web-сторінок, а також організують свою спільну роботу, наприклад, за допомогою протоколу електронної пошти. Одиниця даних, якою оперує прикладний рівень, зазвичай називається повідомленням (message). Існує велике розмаїття протоколів прикладного рівня.

Модель OSI представляє хоча й дуже важливу, але тільки одну з багатьох моделей комунікацій. Ці моделі й пов'язані з ними стеки протоколів можуть відрізнятися кількістю рівнів, їхніми функціями, форматами повідомлень, сервісами, надаваними на верхніх рівнях і

інших параметрах.

Тому модель OSI варто розглядати, в основному, як опорну базу для класифікації й зіставлення протокольних стеків.

2.1.2. Характеристика стеків комунікаційних протоколів

Головна мета, що переслідується при з'єднанні комп'ютерів у мережу, – це можливість використання ресурсів кожного комп'ютера всіма користувачами мережі. Для того, щоб реалізувати цю можливість, комп'ютери, приєднані до мережі, повинні мати необхідні для цього засоби взаємодії з іншими комп'ютерами мережі. Завдання поділу мережних ресурсів є складним.

Звичайним підходом при розв'язанні складної проблеми є її декомпозиція на кілька окремих проблем – підзавдань. Для розв'язання кожного підзавдання призначається деякий модуль. При цьому чітко визначаються функції кожного модуля й правила їхньої взаємодії.

Прикладом декомпозиції завдання є багаторівневе представлення, при якому всі модулі, що вирішують підзавдання, розбиваються на ієрархічно впорядковані групи – рівні. Для кожного з них визначаються функції-запити, з якими до модулів цього рівня можуть звертатися модулі вищого рівня для розв'язання своїх завдань. Такі формально визначені функції, виконувані певним рівнем для вищого рівня, а також формати повідомлень, якими обмінюються два сусідніх рівні в процесі своєї взаємодії, називається *інтерфейсом*.

Інтерфейс визначає сукупний сервіс, що надається певним рівнем вищому рівню.

При взаємодії комп'ютерів у мережі кожний рівень веде "переговори" з відповідним рівнем іншого комп'ютера. При передачі повідомлень обидва учасники мережевого обміну повинні прийняти угоди. Угоди повинні бути прийняті для всіх рівнів, починаючи від найнижчого рівня передачі біт, до найвищого рівня, що деталізує, як інформація повинна бути інтерпретована.

Правила взаємодії двох машин можуть бути описані у вигляді процедур для кожного з рівнів. Такі формалізовані правила, що визначають послідовність і формат повідомлень, якими обмінюються мережеві компоненти, що лежать на одному рівні, але в різних вузлах, називаються *протоколами*.

Протоколи реалізуються не тільки програмно-апаратними

засобами комп'ютерів, але й комунікаційними пристроями. Загалом зв'язок комп'ютерів у мережі здійснюється не прямо – "комп'ютер-комп'ютер", а через різні комунікаційні пристрої, такі, наприклад, як концентратори, комутатори або маршрутизатори. Залежно від типу пристрою, у ньому повинні бути вбудовані засоби, що реалізують деякий набір мережевих протоколів.

При організації взаємодії можуть бути використані два основних типи протоколів. У протоколах *зі встановленням з'єднання (connection-oriented network service, CONS)* перед обміном даними відправник і одержувач повинні спочатку встановити логічне з'єднання, тобто домовитися про параметри процедури обміну, які будуть діяти тільки в рамках певного з'єднання. Після завершення діалогу вони повинні розірвати це з'єднання. Коли встановлюється нове з'єднання, переговірна процедура виконується заново. Телефон – це приклад взаємодії, заснованого на встановленні з'єднання.

Друга група протоколів – протоколи *без попереднього встановлення з'єднання (connectionless network service, CLNS)*. Вони називаються також дейтаграмними протоколами. Відправник просто передає повідомлення, коли воно готове. Опускання листа в поштову скриньку – це приклад зв'язку без установлення з'єднання.

Погоджений набір протоколів різних рівнів, достатній для організації міжмережевої взаємодії, називається *стеком протоколів*.

Існує досить багато стеків протоколів, широко застосовуваних у мережах. Це й стеки, що є міжнародними й національними стандартами, і фірмові стеки, що одержали поширення завдяки поширеності устаткування тієї або іншої фірми. Прикладами популярних стеків протоколів можуть служити стек IPX/SPX фірми Novell, стек TCP/IP, використовуваний у мережі Internet і в багатьох мережах на основі операційної системи UNIX, стек OSI міжнародної організації зі стандартизації, стек DECnet корпорації Digital Equipment і деякі інші.

Стек OSI

Варто розрізняти стек протоколів OSI і модель OSI. Тим часом як модель OSI концептуально визначає процедуру взаємодії відкритих систем, стек OSI – це набір цілком конкретних специфікацій протоколів, що утворять погоджений стек протоколів. Це міжнародний, незалежний від виробників стандарт. З цілком очевидних причин стек OSI, на відміну від інших стандартних стеків,

повністю відповідає моделі взаємодії OSI, оскільки включає специфікації для всіх семи рівнів моделі взаємодії відкритих систем (рис. 18).

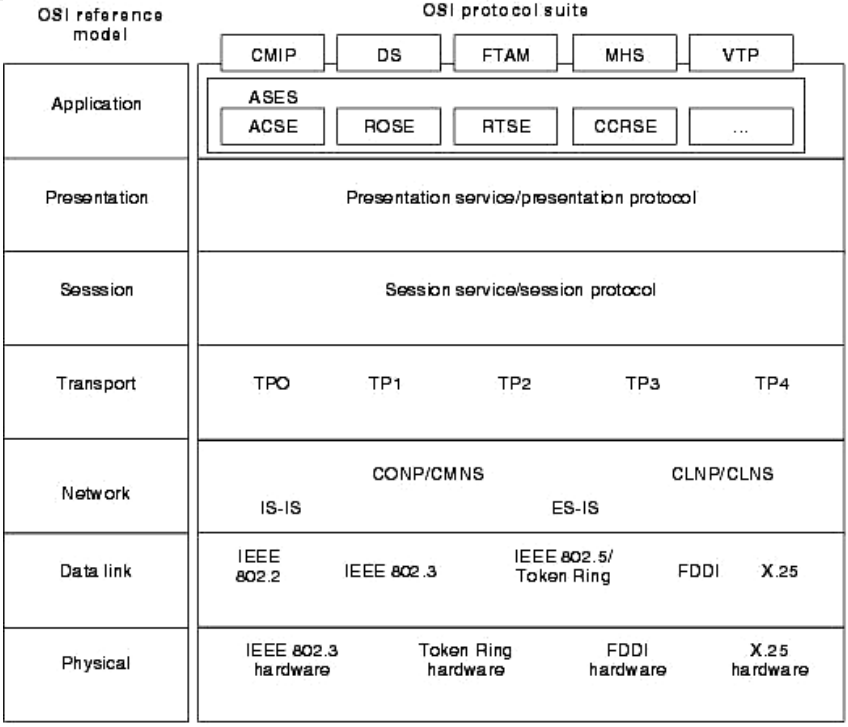


Рис. 18. Стек OSI

На фізичному й канальному рівнях стек OSI підтримує протоколи Ethernet, Token Ring, FDDI, а також протоколи LLC, X.25 і ISDN.

На мережевому рівні реалізовані протоколи як без установлення з'єднань, так і їх установленням. Транспортний протокол стека OSI відповідно до функцій, визначених для нього в моделі OSI, приховує відмінність між мережевими сервісами з установленням з'єднання й без установлення з'єднання, так що користувачі одержують потрібну якість обслуговування незалежно від нижнього мережевого рівня. Щоб забезпечити це, транспортний рівень вимагає, аби користувач задав потрібну якість

обслуговування. Визначені 5 класів транспортного сервісу, від нижчого класу 0 до вищого класу 4, відрізняються ступенем стійкості до помилок і вимогами до відновлення даних після помилок.

Сервіси прикладного рівня включають передачу файлів, емуляцію термінала, службу каталогів і пошту. З них найбільш перспективними є служба каталогів (стандарт X.500), електронна пошта (X.400), протокол віртуального термінала (VT), протокол передачі, доступу й керування файлами (FTAM), протокол пересилання й керування роботами (JTM). Останнім часом ISO сконцентрувала свої зусилля саме на сервісах верхнього рівня.

X.400 – описують модель системи обміну повідомленнями, протоколи взаємодії між всіма компонентами цієї системи, а також безліч видів повідомлень і можливості, якими володіє відправник з кожного виду повідомлень, що відправляють.

Метою рекомендацій X.500 є вироблення стандартів глобальної довідкової служби. Процес доставки повідомлення вимагає знання адреси одержувача, що при більших розмірах мереж являє собою проблему, тому необхідно мати довідкову службу, що допомагає одержувати адреси відправників і одержувачів. У загальному виді служба X.500 являє собою розподілену базу даних імен і адрес. Усі користувачі потенційно мають право ввійти в цю базу даних, використовуючи певний набір атрибутів.

Над базою даних імен і адрес визначені такі операції: читання (одержання адреси за відомим ім'ям), запит (одержання імені за відомими атрибутами адреси), модифікація, що включає видалення й додавання записів у базу даних.

Облік рекомендацій X.400 і X.500 при проектуванні систем електронної пошти робить принципово можливе й концептуально просте стикування поштових систем різних виробників.

Протокол VT розв'язує проблему несумісності різних протоколів емуляції терміналів. Зараз користувачу персонального комп'ютера, сумісного з IBM PC, для одночасної роботи з комп'ютерами VAX, IBM 3090 і HP9000 потрібно придбати три різні програми для емуляції терміналів різних типів і різних протоколів, що використовують. Якби кожний хост-комп'ютер мав би у своєму складі програмне забезпечення протоколу емуляції термінала ISO, то й користувачеві б знадобилася тільки одна програма, що підтримує протокол VT.

Передача файлів – це найпоширеніший комп'ютерний сервіс.

ISO передбачає такий сервіс у протоколі FTAM, що включає засоби для локалізації й доступу до вмісту файлу й набір директив для вставки, заміни, розширення й очищення вмісту файлу. FTAM також передбачає засоби для маніпулювання файлом як єдиним цілим, включаючи створення, видалення, читання, відкриття, закриття файлу й вибір його атрибутів.

Протокол пересилання й керування роботами JTM дозволяє користувачам пересилати роботи, які повинні бути виконані на хост-комп'ютері. Мова керування завданнями, що забезпечує передачу робіт, указує хост-комп'ютеру, які дії та з якими програмами і файлами повинні бути виконані. Протокол JTM підтримує традиційну пакетну обробку, обробку транзакцій, уведення віддалених завдань і доступ до розподілених баз даних.

Стек TCP/IP

Розглянемо функції кожного рівня й приклади протоколів для стеку TCP/IP (рис. 19).

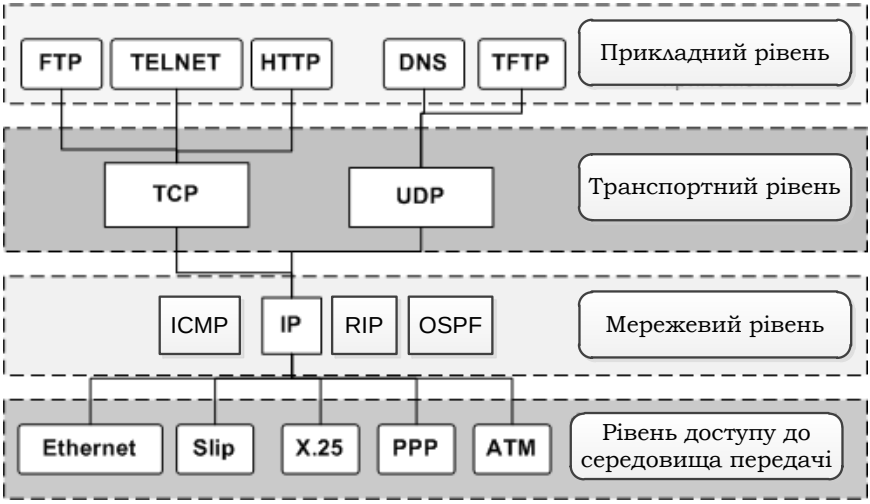


Рис. 19. Стек TCP/IP

Найнижчій (рівень IV) – *рівень доступу до середовища передачі* – відповідає фізичному й канальному рівням моделі OSI. Він у протоколах TCP/IP не регламентується, але підтримує всі популярні стандарти фізичного й канального рівнів: для локальних каналів це Ethernet, Token Ring, FDDI, для глобальних каналів – власні

протоколи роботи на аналогових 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 для транспорту на канальному рівні.

Наступний рівень (рівень III) – це *рівень міжмережевої взаємодії*, що займається передачею дейтаграм із використанням різних локальних мереж, територіальних мереж X.25, ліній спеціального зв'язку й т.п. Як основний протокол мережного рівня, у стеку використовується протокол IP, що проектувався як протокол передачі пакетів у 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 ліній зв'язку.

До рівня міжмережевої взаємодії відносяться й усі протоколи, пов'язані зі складанням і модифікацією таблиць маршрутизації, зокрема протоколи збору маршрутної інформації RIP (Routing Internet Protocol) і OSPF (Open Shortest Path First), а також протокол міжмережевих керуючих 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, перевищення часу життя або тривалості збору пакета із фрагментів, аномальні величини параметрів, зміну маршруту пересилання й типу обслуговування, стан системи й т.п.

Наступний рівень (рівень II) називається *транспортним*. Протоколи транспортного рівня забезпечують прозору (наскрізну) доставку даних (*end-to-end delivery service*) між двома прикладними процесами. Процес, що одержує або відправляє дані за допомогою транспортного рівня, ідентифікується на цьому рівні номером, що називається номером порту. Таким чином, роль адреси відправника й одержувача на транспортному рівні виконує номер порту (або простіше – *порт*).

Аналізуючи заголовок свого пакета, отриманого від міжмережевого рівня, транспортний модуль визначає по номеру

порту одержувача, якому із прикладних процесів спрямовані дані, і передає ці дані відповідному прикладному процесу (можливо, після перевірки їх на наявність помилок і т.п.). Номери портів одержувача й відправника записуються в заголовок транспортним модулем, що відправляє дані; заголовок транспортного рівня містить також іншу службову інформацію; формат заголовка залежить від використовуваного транспортного протоколу.

На транспортному рівні працюють два основних протоколи: UDP(User Datagram Protocol) і TCP (Transmission Control Protocol).

TCP (Transmission Control Protocol – протокол контролю передачі) – надійний протокол із установленням з'єднання: він керує логічним сеансом зв'язку (установлює, підтримує й закриває з'єднання) між процесами й забезпечує надійну (безпомилкову й гарантовану) доставку прикладних даних від процесу до процесу.

Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним методом, тобто без установлення віртуального з'єднання, і тому вимагає менших накладних витрат, ніж TCP.

Верхній рівень (рівень I) називається *прикладним* рівнем. За довгі роки використання в мережах різних країн і організацій стек TCP/IP нагромадив велику кількість протоколів і сервісів прикладного рівня. Для пересилання даних іншому додатку, додаток звертається до того або іншого модуля транспортного рівня.

Протокол SNMP (Simple Network Management Protocol) використовується для організації мережного керування. Перше завдання такого керування пов'язане з передачею інформації. Протоколи передачі керуючої інформації визначають процедуру взаємодії сервера з програмою-клієнтом, що працює на хості адміністратора. Вони визначають формати повідомлень, якими обмінюються клієнти й сервери, а також формати імен і адрес. Друге завдання пов'язане з контрольованими даними. Стандарти регламентують, які дані повинні зберігатися й накопичуватися в шлюзах, імена цих даних і синтаксис цих імен.

Протокол пересилання файлів FTP (File Transfer Protocol) реалізує віддалений доступ до файлу. Для того, щоб забезпечити надійну передачу, FTP використовує як транспорт протокол з установленням з'єднань – TCP. Крім пересилання 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 одержати доступ до файлу, відповідно до протоколу користувачі повинні повідомити своє ім'я та пароль.

Програми, яким не потрібні всі можливості FTP, можуть використати інший, більш економічний протокол – найпростіший протокол пересилання файлів TFTP (Trivial File Transfer Protocol). Він реалізує тільки передачу файлів, причому як транспорт використовується більш простий, ніж TCP, протокол без установлення з'єднання – UDP.

Протокол telnet забезпечує передачу потоку байтів між процесами, а також між процесом і терміналом. Найчастіше цей протокол використовується для емуляції термінала віддаленої ЕОМ. При використанні сервісу telnet користувач фактично управляє віддаленим комп'ютером так само, як і локальний користувач, тому такий вид доступу вимагає гарного захисту.

Лабораторна робота №3 (2 год.)
Тема: Аналіз та зіставлення стеків мережевих протоколів

Мета: розвивати у студентів аналітичні вміння з визначення властивостей та особливостей реалізації стеків мережевих протоколів;

виховувати ціннісне ставлення студентів до навчальної діяльності.

Студент повинен знати: специфікацію стеків мережевих протоколів (OSI, TCP/IP); відмінності у функціях та реалізації відповідних мережевих протоколів у стеках (OSI, TCP/IP).

Студент повинен уміти: аналізувати характеристики комп'ютерної мережі та визначати її вид відповідно до класифікації.

Хід роботи

Інструктаж

1. Розглянути структури стеків протоколів TCP/IP та OSI.
2. Визначити основні відмінності у реалізації стеків протоколів TCP/IP та OSI.
3. Заповнити порівняльну таблицю стеків протоколів, у якій відобразити відповідні та розбіжні функції в реалізації мережевих

рівнів.

Самостійна робота №3

Тема: Рівень розподілення в реалізації ієрархічної комп'ютерної мережі

Мета: розвивати у студентів уміння аналізувати та визначати функції рівня розподілення в реалізації ієрархічної комп'ютерної мережі.

Студент повинен знати: функції та призначення рівня розподілення ієрархічної комп'ютерної мережі .

Студент повинен уміти: визначати завдання рівня розподілення та формулювати стратегії їх реалізації.

Хід роботи

Теоретична частина

1. Назвіть первинні цілі рівня розподілення мережі.
2. Які стратегії використовуються на рівні розподілення мережі для досягнення первинних цілей цього рівня?

Практична робота

Використавши запропоновану літературу, доведіть правильність твердження: "Агрегація досягається за рахунок об'єднання трафіку, що надходить за багатьма низькошвидкісними каналами передачі інформації, які зв'язують рівень розподілу з пристроями рівня доступу, у малу кількість широкополосних каналів, котрі зв'язують рівень розподілу з ядром мережі. Подібна стратегія породжує в мережі ефективні точки підсумовування і зменшує кількість маршрутів, що повинні брати до уваги маршрутизатори ядра при ухваленні рішення про комутації пакетів."

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол.

справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Перспективи розвитку стеку мережевих протоколів TCP/IP".

ТЕМА 2.2. ТЕХНОЛОГІЇ ФІЗИЧНОГО РІВНЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Лекція

План

1. Основні типи кабельних середовищ передачі даних
2. Оптоволоконні кабелі

Література

Основна

1. *Жуков І. А.* Комп'ютерні мережі та технології: навч. посіб. для студ. вищих навч. закл. / Жуков І. А., Гуменюк В. О., Альтман І. Є.. – К. : НАУ, 2004. – 276 с. – (Комп'ютерні технології).

2. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, *обучающихся* по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

3. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. – 4-е изд. – М. [и др.]: Питер, 2005. – 991 с.: ил., табл.; 24 см. – (Классика computer science).

Додаткова

1. *Калита Д. М.* Комп'ютерні мережі. Апаратні засоби та протоколи передачі даних : навч. посіб. для студ. вищих закл. освіти / Калита Д. М.; [ред. Третяк О. В.]. – К. : ВПЦ "Київський ун-т", 2003. – 326 с. – (Автоматизація наукових досліджень).

2. *Контроль* та керування корпоративними комп'ютерними

мережами: інструментальні засоби та технології : навчальний посібник / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. – Х. : "Компанія СМІТ", 2004. – 544 с.

3. *Кулаков Ю. А.* Локальные сети / Ю. А. Кулаков, Г. М. Луцкий. – К. : Юниор, 1998. – 336 с.

4. *Лозікова Г.М.* Комп'ютерні мережі: Навч. посібник / Г.М. Лозікова . – К.: Центр навчальної літератури, 2004 . – 128 с.

5. *Науман Ш.,* Вер Х. Компьютерные сети. – М.: ДМК, 2000. – 336 с.

6. *Щербо В.К.* Стандарты вычислительных сетей. Взаимосвязи сетей: Справочник / В.К. Щербо. – М.: Кудиц-образ, 2000. – 268 с.: ил.; 29 см.

2.2.1. Основні типи кабельних середовищ передачі даних

На сьогодні більша частина комп'ютерних мереж використовує з'єднання кабелів. Вони виступають як середовище передачі сигналів між комп'ютерами. Найпоширеніші: коаксіальний кабель, кручена пара, оптичний кабель (табл. 13).

Таблиця 13

Мережеві кабелі

Характеристика	Тонкий коаксіальний кабель	Товстий коаксіальний кабель	Кручена пара	Оптичний кабель
Ефективна довжина кабелю	185 м	500м	100м	2 км
Швидкість передачі	10 Мбіт/с	10 Мбіт/с	> 10 Мбіт/с	> 10 Мбіт/с
Гнучкість	Досить гнучкий	Менш гнучкий	Самий гнучкий	Не гнучкий
Захищеність	Добре захищений	Добре захищений	Підданий перешкодам	Не підданий перешкодам

Однак поступово в наше життя входить бездротове середовище передачі даних. Для бездротової передачі даних використовують інфрачервоне й лазерне випромінювання, радіопередачу й телефонію. Ці способи передачі даних у комп'ютерних мережах, як локальних, так і глобальних, привабливі тим, що гарантують певний

рівень мобільності, дозволяють зняти обмеження на довжину мережі, а використання радіохвиль і супутникового зв'язку роблять доступ до мережі фактично необмеженим.

У табл. 13 наведені основні типи кабелів, використовуваних у ЛОМ. Для високопродуктивного обміну, на обмеженій відстані, розвивалося кілька напрямків реалізації локальних мереж – Ethernet, ARCnet, TokenRing, адаптери яких широко використовуються в персональних комп'ютерах (ПК).

Коаксіальний кабель. Донедавна найпоширенішим середовищем передачі даних був коаксіальний кабель: недорогий, легкий і гнучкий, безпечний і простий в установці. На рис. 20 наведена конструкція коаксіального кабелю.

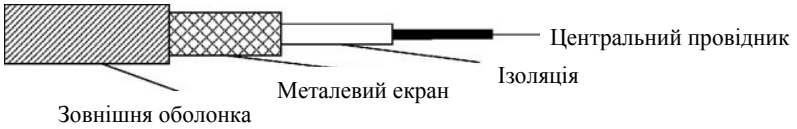


Рис. 20. Конструкція коаксіального кабелю

Електричні сигнали, що кодують дані, передаються по жилі. Вона ізоляцією відділяється від металевої оплітки, що відіграє роль заземлення й захищає передані по жилі сигнали від:

– зовнішніх електромагнітних шумів (атмосферних, промислових);

– перехресних перешкод – електричних наведень, викликаних сигналами в сусідніх проводах.

Використовують товстий і тонкий коаксіальний кабелі. Їхні характеристики наведені в табл. 14.

Таблиця 14

Характеристики коаксіального кабелю

Тип	Діаметр	Ефективна довжина сегмента	Швидкість передачі	Позначення по стандарту IEEE 802.3
товстий	1 см	500 м	10 Мбіт/с	10BASE-5
тонкий	0,5 см	185 м	10 Мбіт/с	10BASE-2

У позначенні кабелів по стандарту IEEE 802.3 перші дві цифри –

швидкість передачі в Мбіт/с, BASE позначає, що кабель використовується в мережах з вузькополосною передачею (baseband network), остання цифра – ефективна довжина сегмента в сотнях метрів, при якій рівень згасання сигналу залишається в припустимих межах. Тонкий підключається до мережних плат безпосередньо через *Т-конектор* (рис. 21), товстий – через спеціальний пристрій – *трансивер*.

Рис. 21. Т-конектор

Розрізняють звичайні й пленумні коаксіальні кабелі. Останні мають підвищені механічні й протипожежні характеристики й допускають прокладку під підлогою, між фальшстелею і перекриттям. При виборі для ЛОМ цього типу кабелю варто брати до уваги, що:

– це середовище для передачі мови, відео і двійкових даних;
– дозволяє передавати дані на великі відстані;
– це добре знайома технологія, що пропонує достатній рівень захисту даних.

Кручена пара. Якщо для передачі електричних сигналів скористатися звичайною парою паралельних проводів для передачі знакозмінного списку великої частоти, то магнітні потоки, що виникають навколо одного з них, будуть викликати перешкоди в іншому (рис. 22). Для уникнення цього провідники перекручують між собою (рис. 23).

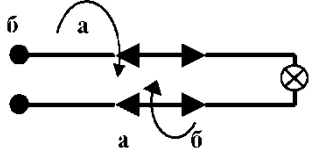


Рис. 22. Пари паралельних проводів

Рис. 23. Кручена пара

Найпростіша *кручена пара (twisted pair)* – це два переплетених

між собою, ізольованих провідники. Існує два види такого кабелю:

– неекранована кручена пара (UTP);
– екранована кручена пара (STP).

Часто кілька кручених пар поміщають в одну захисну оболонку (типу телефонного кабелю). Найпоширеніша в ЛОМ неекранована кручена пара стандарту 10Base з ефективною довжиною сегмента – 100 м. Визначено 5 категорій на основі UTP (табл. 15).

Таблиця 15

Категорії кабельних з'єднань на неекранованої кручений парі

Категорія	Швидкість передачі (Мбіт/с)	Кількість пар
1	Телефонний кабель тільки для передачі мови	1 пара
2	До 4	4 пари
3	До 10	4 пари з 9-ми витками на 1 м
4	До 16	4 пари
5	До 100	4 мідні пари

Однієї з проблем усіх цих кабелів є перехресні перешкоди, тобто наведення з боку сусідніх ліній, що може приводити до перекручування переданих даних. Для зменшення їх впливу використовують екран. У кабелях на основі екранованих кручених пар кожна пара обмотується фольгою, а сам кабель укладається в мідну оплітку, що дозволяє передавати дані з більш високою швидкістю й на більші відстані.

2.2.2. Оптоволоконні кабелі

Оптоволоконні (волоконно-оптичні кабелі) використовуються для передачі інформації за допомогою світлового променя. Передача інформації по волоконно-оптичному кабелю має низку переваг перед передачею мідним кабелем.

Широка смуга пропускання – у порівнянні з електромагнітним середовищем. Одне волокно, що працює на довжині хвилі 1300 або 1550 нм, потенційно має ширину смуги 20 ТГЦ (2х1012). Це дає можливість передачі одним оптичним волокном потоку інформації з швидкістю декілька терабіт у секунду. Цього вистачає для розміщення приблизно 250 мільйонів каналів зі швидкістю передачі 64 Кбіт/с.

Мале загасання світлового сигналу у волокні. Промислове оптичне

волокно, що випускається нині, має загасання 0,2-0,35 дБ/км на довжині хвилі 1300 і 1500 нм. При допустимому загасанні 20 дБ максимальна відстань між підсилювачами або повторювачами складає близько 100 км і більш.

Низький рівень шумів у волоконно-оптичному кабелі дозволяє збільшити смугу пропускання шляхом передачі з використанням різної модуляції сигналів без захисту і контролювати правильність прийнятої інформації тільки в крайових терміналах. Це спрощує алгоритми обробки і збільшує реальну швидкість передачі.

Захищеність від електромагнітних перешкод. Оскільки волокно виготовлене з діелектричного матеріалу, воно несприйнятливе до електромагнітних перешкод з боку оточення мідних кабельних систем і електричного устаткування, здатного індукувати електромагнітне випромінювання (лінії електропередачі, електрорухові установки і т. д.). У багатоволоконних кабелях також не виникає проблеми перехресного загасання.

Мала вага й об'єм. Волоконно-оптичні кабелі мають меншу вагу й об'єм в порівнянні з мідними кабелями з розрахунку на одну й ту ж пропускну спроможність. Наприклад, 900-парний телефонний кабель діаметром 7,5 см може бути замінений одним волокном з діаметром 0,1 см. Якщо волокно "одягнути" у безліч захисних оболонок і покрити сталевою стрічковою бронею, діаметр такого кабелю буде 1,5 см, що в декілька разів менше даного телефонного кабелю.

Висока безпека від несанкціонованого доступу. Оскільки волоконно-оптичний кабель практично не випромінює в радіодіапазоні, передавану по ньому інформацію важко підслуховувати, не порушуючи прийому/передачі. Більше того, несанкціоновані відведення в оптичній системі реалізуються складніше і вимагають підключення за допомогою складного устаткування. Несанкціоновані підключення в оптичній мережі простіше виявляються. Системи, що відстежують якість поширюваних світлових сигналів (як по різних волокнах, так і різній поляризації), мають дуже високу чутливість до коливань, невеликих перепадів тиску. Тому оптичні системи із стеженням за якістю сигналу особливо потрібні при створенні ліній зв'язку в урядових, банківських і деяких інших спеціальних службах, що пред'являють підвищені вимоги до захисту даних.

Гальванічна розв'язка елементів мережі. Ця перевага оптичного

волокна полягає в його ізолювальній властивості. Оптоволоконні кабелі не вимагають заземлення оболонки, що захищає від "блукаючих струмів" і високовольтних наведень по "землі", при яких може виникнути велика різниця потенціалів, що для електромагнітних кабелів може привести до ушкодження мережевого устаткування.

Пожежобезпечність. Через відсутність іскроутворення оптичне волокно підвищує безпеку мережі на хімічних, нафтопереробних підприємствах, при обслуговуванні технологічних процесів підвищеного ризику.

Зменшення вимог до лінійнокабельних споруд. Волоконно-оптичні кабелі звільняють переповнені кабельні трубопроводи. Як уже зазначалося вище, волоконно-оптичні кабелі мають менший об'єм з розрахунку на одну й ту ж пропускну спроможність, у зв'язку з чим переповнювання кабельних трубопроводів стає малоймовірним, навіть при інтенсивному зростанні широкосмугових послуг.

Економічність волоконно-оптичного кабелю. Волокно виготовлене з кварцу, основу якого складає двоокис кремнію, широко поширеного, а тому недорогого матеріалу, на відміну від міді. Нині вартість волокна по відношенню до мідної пари визначається як 2:5. При цьому волоконно-оптичні кабелі дозволяють передавати сигнали на великі відстані без ретрансляції. Кількість повторювачів на протяжних лініях скорочується при використанні волоконно-оптичних кабелів. Сучасні системи передачі дозволяють досягти дальності близько 400 км тільки з використанням оптичних підсилювачів на проміжних вузлах при швидкості передачі вище 10 Гбіт/с.

Тривалий термін експлуатації. З часом волокно деградує. Це означає, що загасання в прокладеному кабелі поступово зростає. Проте завдяки досконалості сучасних технологій виробництва оптичних волокон цей процес значно уповільнений, і термін служби волоконно-оптичного кабелю складає приблизно 25 років. За цей час може змінитися декілька поколінь стандартів мережевих систем. Терміни старіння оптичних кабелів значно більші, ніж терміни деградації електромагнітних кабельних споруд.

Принципи роботи оптоволоконних кабелів

Оптоволоконний кабель містить три основні елементи (рис. 24):

– обплетення;
– оболонка;

– серцевина.

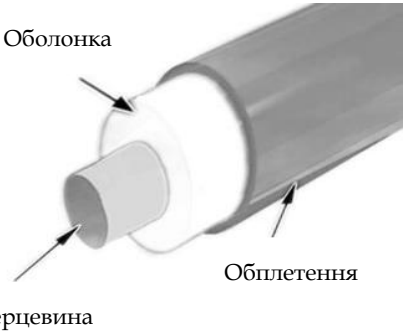


Рис. 24. Конструкція оптичного волокна

Серцевина, волоконний світлопровідний елемент, оточений оболонкою, яка має менший показник заломлення світла. Це призводить до того, що більшість світлових променів в серцевині відбивається всередину серцевини (рис. 25). Чи потрапить промінь знову всередину серцевини, залежить від кута, під яким він перетинає межу "серцевина-оболонка" (числова апертура 1). Якщо промінь входить під занадто гострим кутом до поверхні оболонки, то він поглинається. Поглинання може відбуватися при зміні в оболонці, наприклад, при згинах оптоволоконного кабелю або при неправильному зрощенні волокон.

При побудові мереж використовуються багатожильні кабелі. На рис. 26 показаний приклад кабелю з 8 волокнами. У центрі розташований сталевий трос для зміцнення кабелю, а зовнішня поверхня покрита сталевим обплетенням для захисту від гризунів і зовнішніх силових впливів.

Багатомодові волокна. На рис. 25 показаний принцип поширення променів. У тому числі видно, що при віддзеркаленні променя під певним кутом виникає інший промінь – "вторинна мода". Такі промені можуть бути використані для організації другого шляху перенесення інформації. Оптичні волокна, у яких допускається проходження променів до приймача численними шляхами, називаються багатомодовими.

У порівнянні з одномодовими кабелями (діаметр серцевини 8,5 або 9,5 мкм) багатомодові кабелі мають більший діаметр (50/62,5 мкм при діаметрі оболонки 125 мкм). Більший діаметр серцевини

спрощує їх виготовлення.

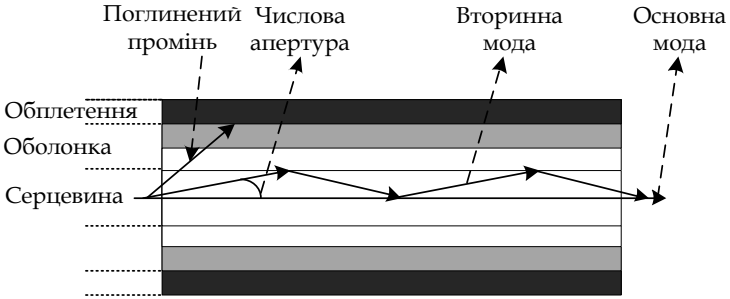


Рис. 25. Схема поширення променів в багатомодовому кабелі

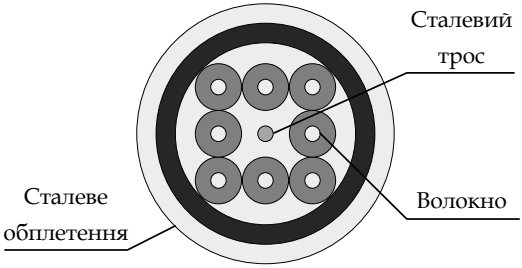


Рис. 26. Принцип розміщення волокон в оптичному кабелі

Багатомодова дисперсія. Звернемо увагу, що відбитий промінь долає більший шлях, отже, проходження інформації дещо сповільнюється. Промені, які запізнюються, призводять до розширення імпульсів, що передаються. Величина цього розширення прямо пропорційна ширині імпульсу й обернено пропорційна швидкості передачі. Отже, багатомодова дисперсія обмежує пропускну спроможність оптичного кабелю, яка характеризується коефіцієнтом широкосмугової *((BDF – Bandwidth Distance Factor)*. Типове значення BDF у багатомодових кабелів змінюється від 200 до 800 Мгц/км. Одномодові волокна більш широкосмугові, їх значення BDF дорівнює від 50-100 ГГц/км.

Такий ефект спостерігається в так званих волокон із ступінчастим показником заломлення. Це волокна, у яких на межі "оболонка-серцевина" відбувається стрибок коефіцієнта заломлення. Кращі показники BDF у волокна з плавною зміною, показника заломлення від максимального в центрі до мінімального по краях.

Таким чином, промені, що проходять ближче до центру, поширюватимуться із затримкою, в порівнянні з променями, що проходять по його краях. Тому швидкості всіх променів вирівнюються, і вони прибувають до приймача з однаковою затримкою. Волокна з показником заломлення, що змінюється, за зазначеним вище законом називаються градієнтними і мають коефіцієнт широкосмуговості на два порядки більше, ніж волокна із ступінчастим показником.

Загасання сигналу в оптичному волокні. Загасання вимірюється в дБ/км і визначається втратами на поглинання або розсіяння випромінювання в оптичному волокні. Втрати на поглинання залежать від прозорості матеріалу, з якого виготовлено волокно, також від неоднорідності заломлення матеріалу.

Загасання сигналу при певній марці кабелю на одиницю довжини лінії залежить від довжини хвилі сигналу (рис. 27). У сучасних оптичних волокнах найнижче загасання спостерігається на двох довжинах хвилі – 1300 і 1550 нм, оскільки в цих діапазонах найбільша прозорість кварцу, з якого виготовляється волокно. На цих частотах, як можна побачити з рис. 27, загасання дорівнює 0,35 і 0,2 дБ відповідно.

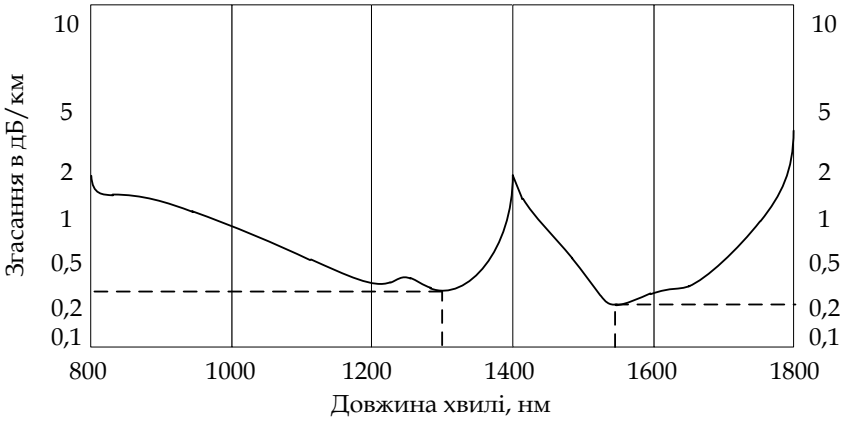


Рис. 27. Залежність загасання в оптичному волокні від довжини хвилі

Хроматична дисперсія (Chromatic Dispersion). Хроматична дисперсія виникає тоді, коли світловий сигнал складається з хвиль різних довжин. Хроматична дисперсія – один з механізмів, що

лімітують смугу пропускання волоконно-оптичних кабелів, погіршують поширення імпульсів сигналу, який складається з різних кольорів світла (некогерентність сигналу), котре проходить. Різні довжини хвиль поширюються з різною швидкістю. Хоча більшість оптичних джерел має однаковий діапазон світлового променя, кожна хвиля з різною довжиною прибуває за різний час, і тому виявляється, що імпульс розмивається.

Кількісно дисперсія вимірюється відносно швидкості поширення хвиль з різною довжиною, що входять у світловий сигнал. Велика дисперсія означає, що хвилі поширюються з великою різницею за швидкістю. Низька дисперсія вказує, що сигнали, суміжні по довжині хвилі, поширюються приблизно з однаковою швидкістю. Впорядкування дисперсії полягає в тому, щоб понизити різницю поширення сигналів різної довжини хвилі по всьому діапазону.

Хроматична дисперсія складається з матеріальної і хвилевої складових і відбувається при поширенні як в одномодовому, так і в багатомодовому волокні. Проте найвиразніше вона проявляється в одномодовому волокні, зважаючи на відсутність міжмодової дисперсії.

Матеріальна складова відбиває залежність показника заломлення волокна від довжини хвилі. У вираження для дисперсії одномодового волокна входить характеристика матеріалу, а саме залежності показника від довжини хвилі.

$\tau_{mat}(\Delta\lambda) = \Delta\lambda LM(\lambda)$,

де $\tau_{mat}(\Delta\lambda)$ дисперсія (пс/км · нм);

$\Delta\lambda$ – диференціальна залежність показника заломлення від довжини хвилі (чи коефіцієнт дисперсії волокна) в пс/км;

λ – спектр джерела в нанометрах (нм);

L – довжина кабелю.

У вираз для дисперсії одномодового волокна входить показник заломлення матеріалу, а саме – диференціальна залежність показника від довжини хвилі Δλ. Ця складова визначається швидкістю (диференціалом) зростання або зменшення показника заломлення залежно від довжини хвилі. Зі збільшенням довжини хвилі цей показник може бути позитивним (коефіцієнт заломлення зростає) або негативним (коефіцієнт заломлення спадає).

Хвилева дисперсія визначається часом поширення сигналу залежно від довжини хвилі. Диференціал такої функції завжди

позитивний (час поширення зі збільшенням довжини хвилі тільки зростає).

$$\tau_{mat}(\Delta\lambda) = \Delta\lambda L N(\lambda),$$

де $\tau_{mat}(\Delta\lambda)$ - дисперсія, виражена в пікосекундах на км на нанометр (пс/км-нм);

$N(\lambda)$ – диференціальна залежність показника заломлення від довжини хвилі;

$\Delta\lambda$ – збільшення довжини хвилі внаслідок некогерентності джерела в нанометрах;

L – довжина кабелю.

Підсумкова питома хроматична дисперсія $D(\lambda)$ дорівнює $D(\lambda) = M(\lambda) + N(\lambda)$.

І тут важливим є те, що при певній довжині хвилі (приблизно 1310±10 нм для ступінчастого одномодового волокна) відбувається взаємна компенсація $M(\lambda)$ і $N(\lambda)$, а результативна дисперсія $D(\lambda)$ перетворюється на нуль. Довжина хвилі, при якій це відбувається, називається завдовжки хвилі нульової дисперсії λ_0. Зазвичай вказується деякий діапазон довжин хвиль, в межах яких може варіюватися λ_0 для цього конкретного волокна.

Для боротьби з хроматичною дисперсією можна рекомендувати такі методи.

1. Як робочу довжину хвилі вибирати таку, при якій хроматична дисперсія мінімальна.
2. Вибирати джерело з вузьким спектром.
3. Використовувати для передачі сигналів вузькі однополярні імпульси.
4. Застосовувати оптичне волокно, що компенсує дисперсію (волокно із зміщеною або вирівняною дисперсією).

Довжина хвилі нульової дисперсії λ_0 для багатомодового градієнтного й одномодового ступінчастого кабелів – 1300 нм і для одномодового із зміщеною дисперсією – 1500 нм. У реальних кабелях унаслідок виробничих допусків типові значення дисперсії близько 1-3,5 пс/км-нм.

Встановлено, що при певній формі сигналу (рис. 28) він має найменшу дисперсію. Такі імпульси називаються солітонами.

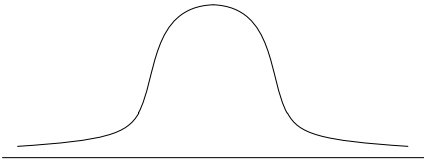


Рис. 28. Форма імпульсу типу "солітон"

Апаратне устаткування для оптоволоконних кабелів

Електрооптичні перетворювачі.

Є два типи приладів, що перетворюють електричний сигнал у світловий – світлодіоди і лазерні діоди.

Світлодіоди (LED – Light-Emitting Diode) генерують некогерентне випромінювання (сигнал містить складові з декількох довжин хвиль). Область спектру генерованого сигналу $\Delta\lambda$ = 30 − 50 нм при довжині хвилі основного сигналу 850 нм і 70 або 120 при довжині хвилі основного сигналу 1300 нм. Типове значення збуджуваної максимальної потужності для різних типів діодів різна: від 20 до 10 дБ.

Таблиця 16

Дисперсія оптичних сигналів в різних оптичних волокнах

Тип волокна	λ	**Міжмодова дисперсія, пс/км** τ_{mod}	**Питома хроматична дисперсія, пс/(нм-км)** $D(\lambda)$
MMF 50/125	850	414 1)	99,6 3)
	1310	414	1,0
	1550	414	19,2
MMF 62,5/125	850	973 2)	106,7 4)
	1310	973	4,2
	1550	973	17,3
SF 8/125	1310	0	< 1,8 5)
	1550	0	17,5
DSF 8/125	1310	0	21,2 6)
	1550	0	< 1,7

1. $\Delta = 0{,}02$, $n_1 = 1{,}46$;
2. $\lambda_0 = 1297 - 1316$ нм, $S_0 \le 0{,}101$ пс/$\left(\text{нм}^2 \cdot \text{км}\right)$;
3. $\lambda_0 = 1322 - 1354$ нм, $S_0 \le 0{,}097$ пс/$\left(\text{нм}^2 \cdot \text{км}\right)$;
4. $\lambda_0 = 1301{,}5 - 1321$ нм, $S_0 \le 0{,}092$ пс/$\left(\text{нм}^2 \cdot \text{км}\right)$;
5. $\lambda_0 = 1535 - 1565$ нм, $S_0 \le 0{,}085$ пс/$\left(\text{нм}^2 \cdot \text{км}\right)$.

Некогерентність світлодіодів обмежує їх застосування.

Переваги світловипромінювальних світлодіодів – це:

– тривалий термін служби;
– менший часовий дрейф параметрів;
– велика лінійність і менша температурна залежність випромінюваної потужності;
– низька вартість і простота експлуатації.

Для світлодіодів втрати потужності при переході в лінію складають 10 дБ. Крім того, оскільки випромінювання – некогерентне, тобто воно відбувається в деякому спектральному діапазоні, додатково спотворюється передаваний сигнал (розширення імпульсів) за рахунок відмінностей у поширенні різних спектральних складових.

Принцип випромінювання світлодіодів дозволяє модуляцію тільки за інтенсивністю випромінювання. Потужність випромінювання світлодіодів може досягати декількох десятків мкВт.

При необхідності створити лінію для передачі на великі відстані застосовують лазерні діоди, що мають кращу спектральну характеристику.

Лазерний діод забезпечує когерентне випромінювання, його промінь має вужчий спектр у порівнянні зі світлодіодом. Принцип випромінювання лазерних діодів дозволяє використовувати модуляцію за параметрами світлової хвилі, наприклад частотну. Крім того, вони характеризуються максимальною для напівпровідникових випромінювачів потужністю до декількох сотень міліват, мінімальною шириною спектру і дуже вузькою спрямованістю. Як багатомодові, так і одномодові лазерні діоди, мають значно вужчий спектр, ніж світлодіоди, що забезпечує меншу хроматичну дисперсію.

Оскільки лазерні діоди відрізняються складнішою конструкцією і великими електричними навантаженнями в порівнянні зі світлодіодами, вони поступаються останнім в надійності, зручності експлуатації та вартості. Це визначає їх застосування для здійснення передачі на далекі відстані в магістральних лініях. Характеристики світлодіодів і лазерних діодів наведені в табл. 17.

Таблиця 17

Характеристики світлодіодів і лазерних діодів

Параметри	Світлодіод	Лазерні діоди
Довжина хвилі	850, 350	1350, 550
Вихідна потужність	0,0,5-11,5 мВт	3-10 мВт
Час наростання	1-20 нс	1-2 нс
Діапазон струму зміщення	5-150 мА	100-500 мА
Ширина спектру	50-120 нм	0,4-1,0

Оптично-електричні перетворювачі.

Фотодіоди. Приймач випромінювання повинен перетворити оптичний сигнал в електричний. Оскільки інформаційний сигнал міститься в модульованому світловому потоці, цей потік має бути прийнятий якомога повніше і без спотворень. Через те, що робоча поверхня приймача набагато більша перерізу світлопровода, втрати під час переходу випромінювання в приймач будуть набагато менше, ніж при переході від джерела в лінію. Для прийому випромінювання можуть використовуватися фотодіоди – напівпровідникові прилади на основі груп кремнію і германію.

У звичайних фотодіодах формується струм, залежний від інтенсивності випромінювання, що падає, їх відрізняють хороша лінійність і стабільність роботи, малий час відгуку, але вони не забезпечують посилення фотоструму.

Фототранзистори. Ці напівпровідникові прилади також будуються на основі кремнію і германію. Вони мають високу чутливість і гарне посилення, але через велику бар'єрну місткість час відгуку в них великий, тобто частотні характеристики гірші, ніж у діодів. Гранична частота для кращих зразків досягає 200 Мгц.

PIN-фотодіоди. У p-i-n (PIN) фотодіодах між шарами з різною провідністю (pin) вводиться шар з власною провідністю (i-область), який при подачі зворотної напруги зміщення збіднюється вільними носіями. У результаті поглинання світла утворюватимуться електрони-носії, які прискорюватимуть сильне електричне поле. PIN-фотодіоду мають більшу, ніж фотодіоди, чутливість. Їх бар'єрна місткість мала, за рахунок чого забезпечуються хороші частотні характеристики (гранична частота – до 1 ГГц). Для них потрібна невелика напруга зворотного зміщення (менш 5В).

Лавинні фотодіоди. Лавинні фотодіоди мають внутрішнє посилення і відрізняються від p – i – n фотодіодів наявністю ще одного додаткового шару. При високій зворотній напрузі зміщення (близько 100 В) у них утворюється сильне прискорювальне поле, у якому відбувається лавинне розмноження носіїв, що утворюються під

впливом світла, тобто посилення фотоструму. Ці прилади характеризуються високою чутливістю, великим посиленням і високою швидкодією, проте їх використання ускладнене, високою вартістю, високою робочою напругою, необхідністю стабілізації напруги і температур і роботою тільки в режимі посилення слабкого сигналу. Характеристики оптичних приймачів наведені в табл. 18.

Таблиця 18

Характеристики оптичних приймачів

Параметри	p – i – n	Лавинний фотодіод	Фототранзистор
Чутливість	0,05 мка/мкВт	15 мка/мкВт	35 мка/мкВт
Час наростання	1 нс	2 нс	2 мкс
Напруга зміщення	10 В	100 В	10 В

Оптичні з'єднувачі. Одним з критичних місць волоконних систем є зрощення волокон і з'єднувачі. Враховуючи діаметр центральної частини волокна, неважко припустити, до яких наслідків приведе зміщення осей волокон, що стикуються, навіть на декілька мікрон (особливо в одномодовому варіанті, де діаметр центрального ядра менше 10 мікрон).

З'єднувачі для оптичних волокон мають зазвичай конструкцію, показану на рис. 29, і виготовляються з кераміки. Втрата світла в з'єднувачі складає 0,2 дБ. Для порівняння: зварювання волокон призводить до втрат не більш 0,001-0,1дБ. Існує також техніка механічного зрощення волокон, яка характеризується втратами близько 10% (splice). Оптичними атенюаторами для оптимального узгодження динамічного діапазону оптичного сигналу й інтервалу чутливості вхідного пристрою є тонкі металеві шайби, які збільшують проміжок між волокном кабелю і приймачем.

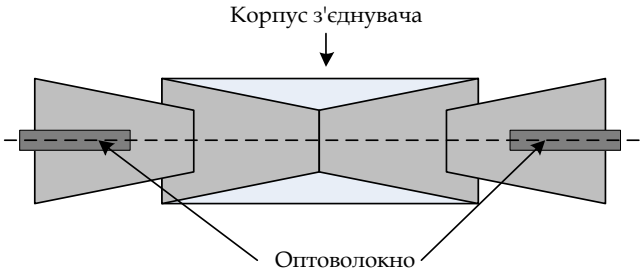


Рис. 29. Схема оптичного з'єднувача

З використанням оптичних волокон можна створювати не лише кільцеві структури. Можлива побудова фрагмента мережі за характером зв'язків еквівалентного кабельного сегменту або концентратору.

Схема такого фрагмента мережі представлена на рис. 30 (пасивний концентратор). Базовим елементом цієї субмережі є прозорий циліндр, на один з торців якого підключаються вихідні волокна всіх передавачів інтерфейсів пристроїв, що становлять субмережу. Сигнал з іншого торця через волокна поступає на вхід фотоприймачів інтерфейсів. Таким чином, сигнал, переданий одним з інтерфейсів, поступає на вхід усіх інших інтерфейсів, підключених до цієї субмережі. При цьому втрати світла складають

$$2C + S + 10\log(N),$$

де C – втрати у з'єднувачі, S – втрати у пасивному розгалужувачі, а N – число оптичних каналів (N може досягати 64). Деякі з них (наприклад, ODL 200 AT&T) здатні здійснювати перемикання на обхідний оптичний шлях (bypass) при відключенні живлення.

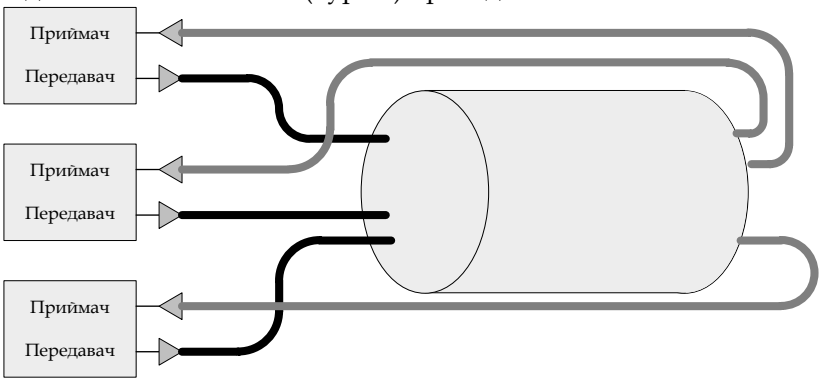


Рис. 30. Схема пасивного оптоволоконного повторювача

Крос. Крос, призначений для оптичного кабелю, відноситься до кросів високої щільності, тобто кількість пар, що підключаються, на одиницю площі перевищує попередні системи (наприклад, цифрові системи ущільнення). До такого кросу висуваються стандартні вимоги:

– урахування специфіки кросування оптоволоконного

кабелю;

– надійність і керованість кабельним господарством;
– зручність роботи;
– безпека для персоналу.

Висока щільність і крихкість (висока вірогідність ушкодження в умовах експлуатації) призводять до нових рішень.

Ще одна особливість оптичних кабелів полягає в специфіці поширення світла волокном. При перегині волокна більше захисного радіусу в 30 мм у ньому виникає розсіяння оптичної потужності, і загасання в кабелі значно зростає. Тому, окрім дбайливої експлуатації, з'являється ще одна вимога – геометричної властивості: ні за яких обставин радіус перегину не повинен перевищувати критичний.

Відповідно до нових норм і стандартів безпеки OSHA (Occupational Safety and Health Administration – закони про техніку безпеки і гігієну праці США) оптичні кроси повинні забезпечувати максимальний захист очей оператора від можливого лазерного випромінювання при кросуванні кабелів. Особливо це важливо для кросів високої щільності.

Особливістю кросів високої щільності є принципова неможливість використання вертикальних або фронтальних методів доступу до кабелів. Фронтальні методи не забезпечують повною мірою необхідну щільність кросових з'єднань і не такі безпечні для персоналу. Вертикальний доступ незручний при роботі з окремими волокнами.

Хвилеве мультиплексування (WDM). Останнім часом помітного здешевлення оптичних каналів вдалося досягти за рахунок мультиплексування з діленням за довжиною хвилі. *Хвилеве мультиплексування (Wave Division Multiplexing, WDM)* – це концепція об'єднання декількох потоків даних в одному фізичному волоконно-оптичному кабелі. Таке збільшення місткості кабелю можна досягти, застосовуючи фундаментальний принцип фізики, який полягає в тому, що промені світла з різними довжинами хвиль не взаємодіють між собою. Основна ідея систем WDM полягає у використанні декількох довжин хвиль (чи частот) для передачі окремого потоку даних на кожній з них.

За рахунок цієї техніки вдалося в 16-160 разів збільшити широкосмуговість каналу з розрахунку на одне волокно. Схема

мультиплексування показана на рис. 31. На вході каналу сигнали за допомогою призми об'єднуються в одне загальне волокно. На виході за допомогою аналогічної призми ці сигнали розділяються. Число волокон на вході і виході може досягати 32 і більш (замість призм останнім часом використовують мініатюрні дзеркала, де застосовується розгортка по довжині хвилі).

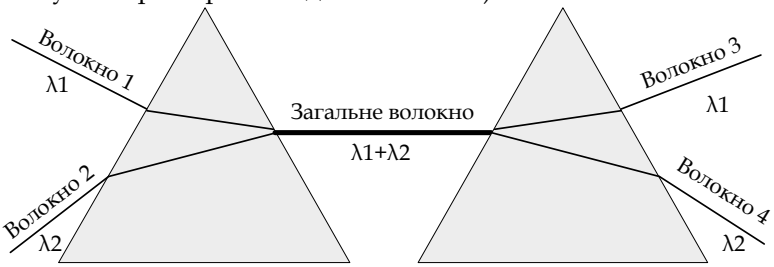


Рис. 31. Мультиплексування з діленням за довжиною хвилі в оптичному волокні

Це досягається за допомогою декількох компонент. По-перше, дані, що передаються, повинні посилатися на певній довжині хвилі. Звичайне хвилеве мультиплексування WDM здійснюється у вікні прозорості 1530-1560 нм, де забезпечується мінімальне загасання сигналу до 0,2 дБ/км. Як правило, волоконно-оптичні системи використовують 3 довжини хвилі – 850, 1310 і 1550 нм. Якщо вхідний сигнал є оптичним і передається на одній з цих довжин хвиль, він має бути перетворений для передачі з довжиною хвилі вікна прозорості WDM. За наявності декількох незалежних вхідних сигналів кожен з них має бути перетворений для передачі на своїй довжині хвилі у межах цього діапазону. Потім ці сигнали об'єднуються за допомогою оптичної системи таким чином, що велика частина потужності всіх сигналів передається по одному оптичному волокну. На іншому кінці лінії світлові сигнали розділяються за допомогою сплітера (ще однієї системи лінз) на декілька каналів. Кожен з цих каналів проходить через фільтри, що відділяють тільки одну з довжин хвиль. Урешті-решт, кожна з відокремлених довжин хвиль потрапляє на свій приймач, який перетворить її в початковий вид (оптичний на довжинах хвиль 850, 1310 і 1550 нм або мідний).

Існує два типи систем WDM, що забезпечують грубе (CWDM) мультиплексування з великим кроком рознесення, несуть щільний

(DWDM) розподіл шкали довжин хвиль. Системи CWDM зазвичай забезпечують передачу від 8 до 16 довжин хвиль з кроком в 20 нм, від 1310 до 1630 нм. Системи DWDM працюють з кількістю довжин хвиль до 144, зазвичай з кроком менше 2 нм приблизно в тому ж діапазоні довжин хвиль. WDM (CWDM або DWDM) використовується в одному з двох варіантів.

Перший і головний полягає в збільшенні обсягу інформації, що передається по оптичному волокну. У цьому разі велика кількість потоків даних передаються по невеликій кількості оптичних кабелів. Це дає можливість значно збільшити пропускну спроможність оптичного кабелю. Так, при швидкості 10 Гбіт/с на канал загальна пропускна спроможність кожного волокна складе 1,25 Тбіт/з (тобто 12 500 000 000 000 біт в секунду). Звичайно, у більшості випадків такий рівень швидкостей не вимагається, завданням є передача декількох потоків Gigabit Ethernet по одній парі волокон, коли додаткових пар уже немає. У багатьох випадках прокласти новий оптичний кабель виявляється занадто дорого або просто неможливо. Тоді використання технології WDM стає єдиною можливістю для збільшення пропускної спроможності.

Другий варіант використання WDM виник порівняно недавно, коли все більше замовників стали використовувати високошвидкісні канали зв'язку. У такому разі оператор зв'язку надає замовникам, що мають офіси в різних точках міста, довжини хвиль у своєму кабелі для організації каналів "точка-точка". Наприклад, велика компанія, що має дві будівлі в різних кінцях міста, може поставити завдання їх об'єднання. Для вирішення цієї проблеми оператор може розвернути мережу. При використанні WDM оператору не треба піклуватися про те, який протокол або технологія використовується замовниками, що дає можливість гнучкішого надання послуг.

Пристрої для організації WDM пасивні, тобто не вимагають електроживлення. Проте деякі з них потребують постійної температури. Для цього встановлюються пристрої регулювання температури, а їм потрібне електроживлення. Тоді використовується змішаний кабель, який разом з оптичними волокнами містить мідні жили.

Для забезпечення норм щодо загасання при передачі даних оптичними кабелями, застосовуються регенератори і підсилювачі

сигналів. При передачі поодинокого оптичного сигналу (см. рис. 32а) кожен регенератор перетворить оптичний сигнал в електричний, коригує часові параметри, виділяє дані, що передаються, і в результаті управляє лазерним передавачем для регенерації сигналу і послідовного введення даних в оптичний кабель для передачі їх наступною ділянкою.

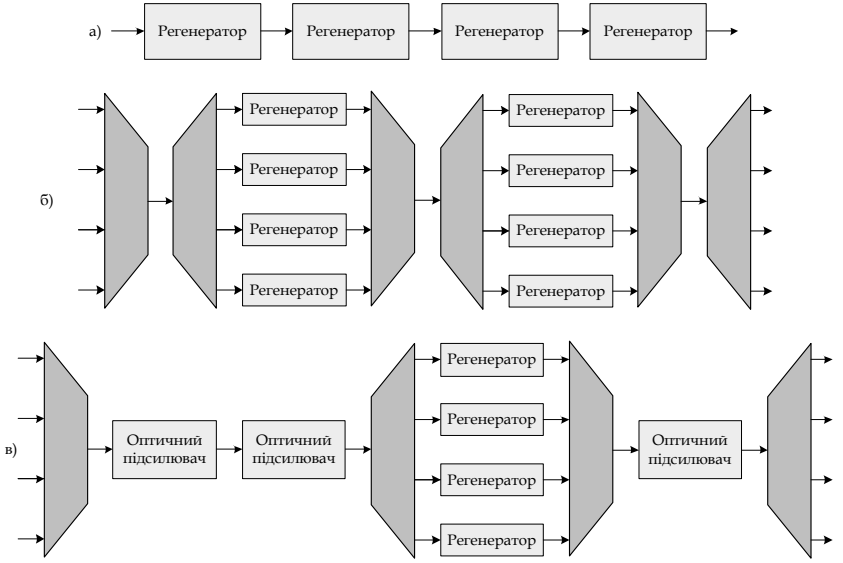


Рис. 32. Оптичні системи передачі: а) з лінійною регенерацією; б) DWDM складений сигнал з однією ділянкою розподілу за довжиною хвилі; в) DWDM складений сигнал з оптичним підсилювачем

Перетворення оптичного сигналу в електричний сигнал вимагає великих витрат, оскільки застосовує дуже дорогі компоненти (лазери і надшвидкісну електроніку).

Схема, показана на рис. 32б, передає складений WDM -сигнал. При цьому на кожній регенераторній ділянці здійснюється розбиття складеного сигналу на окремі сигнали. Далі здійснюється індивідуальне перетворення в електричну форму й індивідуальна регенерація.

Прийнятніше застосування оптичних підсилювачів, які можуть посилювати сигнал на всіх довжинах хвиль, складових WDM-сигналу. Оптичний підсилювач на оптоволокні, легованому

ербієм (Erbium-Doped Fiber Amplifier – EDFA), – це відрізок оптичного кабелю типу EDF і напівпровідниковий лазерний діод як джерело "накачування". Підсилювач приймає ослаблений сигнал і генерує потужний сигнал в оптичний кабель, легований ербієм. Від дії потужного сигналу атоми ербію збуджуються і генерують фотони в той же самій фазі і напрямі, як і сигнал, що посилається. У результаті створюється ефект посилення. Такі підсилювачі можуть бути спроектовані на всі діапазони довжин хвиль. Використання підсилювачів знижує потребу в застосуванні регенераторів, як це показано на рис. 32в. При цьому є обмеження на кількість послідовно встановлюваних підсилювачів. Проте установка підсилювачів дозволяє збільшити відстань між регенераторами і пов'язане з ними перетворення оптика-електроника до сотень і тисяч кілометрів.

Лабораторна робота №4 (2 год.)
Тема: Фізичне середовище передачі даних

Мета: сформувати вміння визначати за зовнішніми ознаками тип кабелю; встановлювати з'єднувач RJ-45;

виховувати ціннісне ставлення студентів до навчальної діяльності.

Студент повинен знати: характеристику різних видів мережевих кабелів; послідовність встановлення з'єднувача RJ-45.

Студент повинен уміти: визначати за зовнішніми ознаками тип кабелю; встановлювати з'єднувач RJ-45.

Хід роботи

Інструктаж

1. Розглянути особливості екранованої крученої пари (UTP) / неекранованої крученої пари (STP).
2. Визначити основні характеристики та правила монтажу з'єднувача RJ-45 для UTP кабелів
3. Заповнити порівняльну таблицю стеків протоколів, у якій відобразити відповідні та розбіжні функції в реалізації відповідних мережевих рівнів.

Практична робота

Монтаж з'єднувача RJ-45

Для монтажу з'єднувача RJ-45 використовується спеціальний інструмент – кримпер з 8 ножами (рис. 33).

1. Акуратно обріжте кінець кабелю. Торець кабелю повинен бути рівним.

2. Використовуючи кримпер, зніміть з кабелю зовнішню ізоляцію на довжину приблизно 30 мм і обріжте нитку, що є в кабелі (нитка призначена для зручності зняття ізоляції з кабелю на велику довжину). Будь-які ушкодження (надрізи) ізоляції провідників абсолютно неприпустимі – саме тому бажано використовувати спеціальний інструмент, лезо різака якого виступає рівно на товщину зовнішньої ізоляції.

3. Акуратно розведіть, розплетіть і вирівняйте провідники. Вирівняйте їх в один ряд, при цьому дотримуючись кольорового маркування. Провідники повинні розташовуватися лише в один ряд, без накладання один на одного. Утримуючи їх однією рукою, іншою рівно обріжте провідники так, щоб вони виступали над зовнішньою ізоляцією на 8-10 мм.

4. Тримаючи рознімання засувкою долілиць, вставте в нього кабель. Кожний провідник повинен потрапити на своє місце в з'єднувачі й упертися в обмежник. Перш ніж обжимати з'єднувач, переконайтеся, що ви не помилилися в розведенні провідників. При неправильному розведенні, крім відсутності відповідності номерам контактів на кінцях кабелю (виявляється легко за допомогою найпростішого тестера), можлива поява "розбитих пар" (splitted pairs).

Для виявлення цього браку звичайного тестера недостатньо, тому, що електричний контакт між відповідними контактами на кінцях кабелю забезпечується й начебто все нормально. Але такий кабель ніколи не зможе забезпечити нормальної якості з'єднання навіть у 10-мегабітній мережі на відстані більше 40-50 метрів. Тому потрібно бути уважним і не квапитися, особливо якщо у вас немає достатнього досвіду.

5. Вставте з'єднувач у гніздо на кримпері й обіжміть його до упору – обмежника на пристосуванні. У результаті фіксатор на з'єднувачі стане на своє місце, утримуючи кабель у з'єднувачі. Контактні ножі з'єднувача вріжуться кожний у свій провідник, забезпечуючи надійний контакт.

Рис. 33. Кримпер – пристосування для зняття ізоляції й обтискання з'єднувача RJ-45

Самостійна робота №4

Тема: Рівень доступу як основа підключення абонентів у ієрархічній комп'ютерній мережі

Мета: розвивати у студентів уміння аналізувати та визначати функції рівня доступу в реалізації ієрархічної комп'ютерної мережі.

Студент повинен знати: функції та призначення рівня доступу ієрархічної комп'ютерної мережі.

Студент повинен уміти: визначати завдання рівня доступу та формулювати стратегії їх реалізації.

Хід роботи

Теоретична частина

1. Назвіть два фактори, від яких залежить час, необхідний протоколу маршрутизації для завершення процесу збіжності.
2. Якими основними факторами визначається число маршрутизаторів, що беруть участь у процесі збіжності?
3. Назвіть первинні цілі рівня доступу мережі?

Практична частина

Використавши запропоновану літературу, визначте:

1. Які типи контролю повинні бути реалізовані в маршрутизаторі рівня доступу для блокування атак, що виходять з мережі?
2. Чи припустима в звичайній ситуації передача спрямованого широкомовлення в локальний сегмент мережі?

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Тенденції використання ліній зв'язку та перспективи їх розвитку".

МОДУЛЬНА КОНТРОЛЬНА РОБОТА №2

Оберіть номер правильної відповіді:

1. Мережеві кабелі, що володіють найбільшою швидкістю і якістю передачі даних:

а) кручена пара;

б) оптичний;

в) коаксіальний кабель.

1 б.

2. Ефективна довжина мережного кабелю "кручена пара":

а) 50 м;

б) 100 м;

в) 150 м;

г) 500 м.

1 б.

3. Для чого скручують проводи крученої пари:

а) щоб компактніше розмістити їх у захисній оболонці;

б) для зменшення перешкод, викликаних магнітними потоками;

в) для чіткого поділу кожної пари проводів.

1 б.

4. Скляне оптичне волокно передає сигнали:

а) в одному напрямку;

б) у двох напрямках.

1 б.

5. Укажіть правильний порядок проходження найменування рівнів у моделі OSI. Позначення: S – сеансовий, N – мережний, PH – фізичний, P – представницький, D – канальний, T – транспортний, A – рівень додатків.

а) S, N PH, P, D, T, A;

б) A, S, T, P, N, D, PH;

в) A, S, P, T, N, D, PH;

г) A, P, S, T, N, D, PH.

1 б.

6. Укажіть найменування блоку даних мережного рівня:

а) кадр;

б) сегмент;

в) пакет;

г) повідомлення.

1 б.

7. Укажіть пристрої, які реалізують функції фізичного рівня моделі ISO?

а) хаб;

б) міст;

в) маршрутизатор.

1 б.

8. Сукупність алгоритмів взаємодії об'єктів однойменних рівнів визначає поняття:

а) інтерфейс;

б) стек;

в) протокол;

г) рівень.

1 б.

9. На якому рівні моделі OSI комутатор виконує обробку даних?

а) канальний;

б) транспортний;

в) фізичний;

г) мережевий.

1 б.

10. Які з перерахованих функцій не реалізуються протоколами мережного рівня?

а) визначення маршруту;

б) визначення логічної адреси;

в) керування потоком.

1 б.
Всього: 10 балів.

Правильні відповіді

Питання	1	2	3	4	5	6	7	8	9	10
Відповідь	б	б	б	а	г	в	а	в	а	б

ЗМІСТОВИЙ МОДУЛЬ 3

ВИСОКОШВИДКІСНІ ТЕХНОЛОГІЇ ЛОКАЛЬНИХ МЕРЕЖ. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПРОТОКОЛІВ ЛОКАЛЬНИХ МЕРЕЖ З ВИКОРИСТАННЯМ РОЗПОДІЛЮВАНОГО СЕРЕДОВИЩА ETHERNET

Таблиця 19

Тематичний план змістового модуля

№ теми	Назва змістового модуля, теми	Усього годин	Лекції	Лабораторні заняття	Самостійна та індивідуальна робота
3.1	Загальна характеристика протоколів локальних мереж з використанням розподілюваного середовища Ethernet	9	2	2	5
3.2	Високошвидкісні технології локальних мереж	9	2	2	5
	Разом	***18***	***4***	***4***	***10***

Навчальні цілі: сприяти засвоєнню студентами знань щодо протоколів локальних мереж з використання розподілюваного середовища Ethernet; розвивати вміння аналізувати необхідність використання різних технологій локальних мереж.

Основні поняття: локальна мережа, розподілюване мережеве середовище, Мас-адреса, формат кадру, колізія, продуктивність мережі.

Методичні рекомендації щодо роботи з модулем: робота з модулем передбачає засвоєння лекційного матеріалу, участь у лабораторних заняттях, написання реферату (окремими студентами), самостійну роботу над визначеними питаннями теми, модульний контроль у формі тестування.

Після опрацювання цих тем студент може отримати бали

наведені в табл. 20.

Таблиця 20

Оцінювання навчальних досягнень студентів

Поточний контроль				Індивідуальне завдання	Контрольна рейтингова оцінка	Проміжна рейтингова оцінка
Робота на лабораторному занятті		Самостійна робота				
Тема №3.1	Тема №3.2	Тема №3.1	Тема №3.2			
5	5	2	2	5	10	29

ТЕМА 3.1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПРОТОКОЛІВ ЛОКАЛЬНИХ МЕРЕЖ З ВИКОРИСТАННЯМ РОЗПОДІЛЮВАНОГО СЕРЕДОВИЩА ETHERNET

Лекція

План

1. Технологія Ethernet
2. 10-мегабітові технології Ethernet
3. Технологія 10BASE-2
4. Технологія 10BASE-T

Література

Основна

1. *Бройдо В. Л.* Вычислительные системы, сети и телекоммуникации: учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Прикладная информатика" и "Информационные системы в экономике" / В. Л. Бройдо, О. П. Ильина. – 3-е изд. – Москва [и др.]: Питер, 2008. – 765 с.: ил., табл.; 24 см.

2. *Гук М.* Аппаратные средства локальных сетей. Энциклопедия : [Наиболее полн. и подроб. рук.] / Михаил Гук. – СПб. : Питер, 2000.– 572 с.

3. *Новиков Ю. В.* Локальные сети: Архитектура, алгоритмы, проектирование / Новиков Ю. В., Кондратенко С. В. – М.: ЭКОМ, 2002. – 311 с.: ил.; 23 см. – (Современные компьютерные технологии).

4. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов,

обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

Додаткова

1. *Бабій М. С.* Локальні мережі ЕОМ: [навч. посіб. для студ. спец. "Прикладна математика"] / Михайло Семенович Бабій. – Суми : Видавництво СумДУ, 2003. – 64 с.

2. *Бортник Г. Г.* Мережі доступу: навч. посібник для студ. напряму підготовки 0924 – "Телекомунікації" всіх спец. / Бортник Г. Г., Стальченко О. В., Яблонський В. Ф. – Вінниця : ВНТУ, 2006. – 139 с.

3. *Зайченко Ю. П.* Комп'ютерні мережі: навч. посіб. для студ. вищ. навч. закл. [Intertational Science and Technology University] / Ю. П. Зайченко. – К. : Слово, 2003. – 284 с. – (До 10-річчя Міжнародного науково-технічного ун-ту).

4. *Ибе О.* Сети и удаленный доступ: Протоколы, проблемы, решения / Оливер Ибе. – М.: ДМК Пресс, 2002. – 332 с.: ил.; 23 см. – (Серия "Защита и администрирование").

5. *Кулаков Ю. А.* Локальные сети / Ю. А. Кулаков, Г. М. Луцкий. – К. : Юниор, 1998. – 336 с.

6. *Олексюк В. П.* Організація комп'ютерної локальної мережі : [посіб.] / Олексюк В. П., Балик Н. Р., Балик А. В. – Тернопіль. : Підручники і посібники, 2006. – 80 с.

3.1.1. Технологія Ethernet

Ethernet – це найпоширеніший на сьогодні день стандарт локальних мереж.

Коли говорять Ethernet, то під цим зазвичай розуміють один з варіантів цієї технології. Більш вузький зміст: *Ethernet* – це мережевий стандарт, заснований на експериментальній мережі Ethernet Network, що фірма Xerox розробила й реалізувала в 1975 році. Метод доступу був випробуваний ще раніше: у другій половині 60-х років у радіомережі Гавайського університету використовувалися різні варіанти випадкового доступу до загального радіопростору, що одержали загальну назву Aloha. У 1980 році фірми DEC, Intel і Xerox

спільно розробили й опублікували стандарт Ethernet версії II для мережі, побудованої на основі коаксіального кабелю, що став останньою версією фірмового стандарту Ethernet. Тому фірмову версію стандарту Ethernet називають стандартом Ethernet DIX або Ethernet II.

На основі стандарту Ethernet DIX був розроблений стандарт IEEE 802.3, що багато в чому збігається зі своїм попередником, але деякі відмінності все-таки є. Тим часом як у стандарті IEEE 802.3 розрізняються рівні MAC і LLC, в оригінальному Ethernet обидва ці рівні об'єднані в єдиний канальний рівень, В Ethernet DIX визначається протокол тестування конфігурації (Ethernet Configuration Test Protocol), відсутній у IEEE 802.3. Відрізняється й формат кадру, хоча мінімальні й максимальні розміри кадрів у цих стандартах збігаються. Часто для того, щоб відрізнити Ethernet, визначений стандартом IEEE, і фірмовий Ethernet DIX, перший називають технологією 802.3, а за фірмовим залишають назву Ethernet без додаткових позначень.

Залежно від типу фізичного середовища стандарт IEEE 802.3 має різні модифікації:

- 10Base-5;
- 10Base-2;
- 10Base-T;
- 10Base-FL;
- 10Base-FB.

У 1995 році був прийнятий стандарт Fast Ethernet, що багато в чому не є самостійним, про що свідчить і той факт, що його опис просто є додатковим розділом до основного стандарту 802.3 – розділом 802.3u. Аналогічно, прийнятий у 1998 році стандарт Gigabit Ethernet описаний у розділі 802.3z.

Для передачі двійкової інформації з кабелю для всіх варіантів фізичного рівня технології Ethernet, що забезпечують пропускну здатність 10 Мбіт/с, використовується манчестерський код.

Усі види стандартів Ethernet (у тому числі Fast Ethernet і Gigabit Ethernet) використовують той самий метод розподілу середовища передачі даних – метод CSMA/CD.

Метод доступу CSMA/CD.

У мережах Ethernet використовується метод доступу до середовища передачі даних, що називається *методом колективного доступу з упізнаванням несучої й виявленням колізій (carrier-sense-multiply-*

access with collision detection, CSMA/CD).

Цей метод використовується винятково в мережах із загальною шиною (до яких належать й радіомережі, що породили цей метод). Усі комп'ютери такої мережі мають безпосередній доступ до загальної шини, тому вона може бути використана для передачі даних між будь-якими двома вузлами мережі. Простота схеми підключення – це один з факторів, що визначили успіх стандарту Ethernet. Говорять, що кабель, до якого підключені всі станції, працює в режимі *колективного доступу (multiply-access, MA)*.Ђ

Усі дані, передані по мережі, містяться в кадрі певної структури й забезпечуються унікальною адресою станції призначення. Потім кадр передається по кабелю. Усі станції, підключені до кабелю, можуть розпізнати факт передачі кадру, і та станція, що впізнає власну адресу в заголовках кадру, записує його вміст у свій внутрішній буфер, обробляє отримані дані й посилає по кабелю кадр-відповідь. Адреса станції-джерела також включена у вихідний кадр, тому станція-одержувач знає, кому потрібно послати відповідь.

При описаному підході можлива ситуація, коли дві станції одночасно намагаються передати кадр даних по загальному кабелю (рис. 34.). Для зменшення ймовірності цієї ситуації безпосередньо перед відправленням кадру передавальна станція слухає кабель (тобто приймає й аналізує електричні сигнали, що виникають на ньому), щоб виявити, чи не передається вже по кабелю кадр даних від іншої станції. Якщо прослуховується *несуча (carrier-sense, CS)*, то станція відкладає передачу свого кадру до закінчення чужої передачі, і тільки потім намагається знову його передати. Але навіть при такому алгоритмі дві станції одночасно можуть вирішити, що по шині в цей момент немає передачі, і почати одночасно передавати свої кадри. Говорять, що при цьому відбувається колізія, тому що вміст обох кадрів зіштовхується на загальному кабелі, що приводить до перекручування інформації.

Щоб коректно обробити колізію, усі станції одночасно спостерігають за сигналами, що виникають на кабелі. Якщо передані й спостережувані сигнали відрізняються, то фіксується *виявлення колізії (collision detection, CD)*. Для збільшення ймовірності негайного виявлення колізії всіма станціями мережі ситуація колізії підсилюється посилкою в мережу станціями, що почали передачу

своїх кадрів, спеціальної послідовності біт – jam-послідовність.

Після виявлення колізії станція зобов'язана припинити передачу й очікувати протягом короткого випадкового інтервалу часу, а потім може знову зробити спробу передачі кадру (рис. 34).

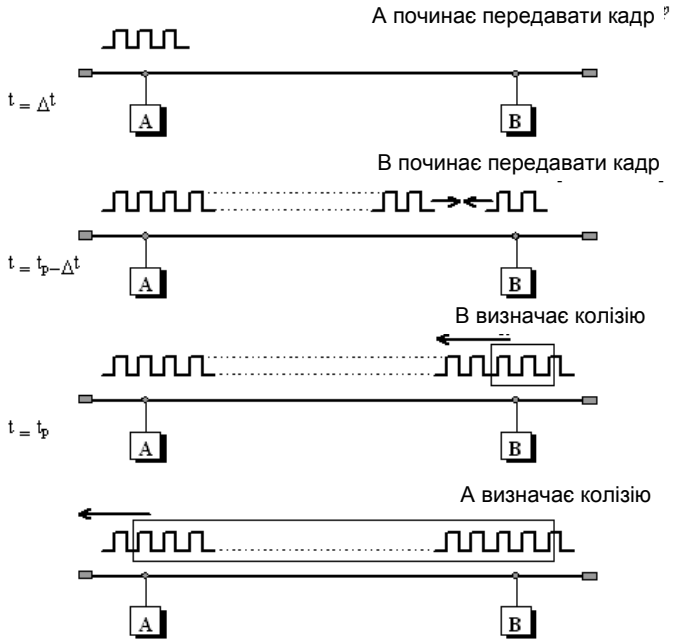


Рис. 34. Схема виникнення колізії в методі випадкового доступу CSMA/CD (tp – затримка поширення сигналу між станціями A и B)

Метод CSMA/CD визначає основні часові й логічні співвідношення, що гарантують коректну роботу всіх станцій у мережі:

– між двома послідовно переданими по загальній шині кадрами інформації повинна витримуватися пауза в 9.6 мкс; ця пауза потрібна для приведення у вихідний стан мережних адаптерів вузлів, а також для запобігання монопольного захвата середовища передачі даних однією станцією;

– при виявленні колізії (умови її виявлення залежать від застосовуваного фізичного середовища) станція видає в середовище спеціальну 32-х бітну послідовність (*jam-послідовність*), що підсилює явище колізії для більш надійного розпізнавання її всіма вузлами

мережі;

– після виявлення колізії кожний вузол, що передавав кадр і зіткнувся з колізією, після деякої затримки намагається повторно передати свій кадр. Вузол робить максимально 16 спроб передачі цього кадру інформації, після чого відмовляється від його передачі. Величина затримки вибирається як рівномірно розподілене випадкове число з інтервалу, довжина якого експоненційно збільшується з кожною спробою.

Такий алгоритм вибору величини затримки знижує ймовірність колізій і зменшує інтенсивність видачі кадрів у мережу при її високому завантаженні.

Усі параметри протоколу Ethernet підібрані так, щоб при нормальній роботі вузлів мережі колізії завжди чітко розпізнавалися. Саме для цього мінімальна довжина поля даних кадру повинна бути не менш 46 байт. Довжина кабельної системи вибирається таким чином, щоб за час передачі кадру мінімальної довжини сигнал колізії встиг би поширитися до найдальшого вузла мережі. Тому для швидкості передачі даних 10 Мб/с, використовуваної в стандартах Ethernet, максимальна відстань між двома будь-якими вузлами мережі не повинна перевищувати 2500 метрів.

Незалежно від реалізації фізичного середовища, усі мережі Ethernet повинні задовольняти двом обмеженням, пов'язаним з методом доступу:

– максимальна відстань між двома будь-якими вузлами не повинна перевищувати 2500 м;

– у мережі не повинно бути більше 1024 вузлів.

3.1.2. 10-мегабітові технології Ethernet

На рис. 35 показані різні реалізації інтерфейсів фізичного рівня, які підтримуються в технології Ethernet. Специфікації *10BASE-5, 10BASE-2* і *10BASE-T* будуть розглядатися як застарілі.

Чотири характеристики є загальними для традиційних специфікацій Ethernet:

– параметри синхронізації;
– формат фрейму;
– процес передачі;
– базові принципи побудови.

Підрівень керування логічним з'єднанням (LLC-рівень)								
802.3 підрівень керування доступом до передавального середовища (MAC-рівень)								
Фізичний сигнальний підрівень	Технологія 10BASE-5 (500 м) 50 Ом; Коаксіальний кабель; з'єднувач N-типу	Технологія 10BASE-2 (185 м) 50 Ом; коаксіальний кабель; з'єднувач BNC	Технологія 10BASE-T (500 м) 100 Ом; кабель UTP, з'єднувач RJ-45	Технологія 100BASE-TX (100 м) 100 Ом; кабель UTP, з'єднувач RJ-45	Технологія 100BASE-FX (228-412 м) багатомодовий (БМ) оптоволоконний кабель; з'єднувач SC	Технологія 1000BASE-T 100 м) 100 Ом; кабель UTP; з'єднувач RJ-45	Технологія 1000BASE-SX (220-550 м) багатомодовий (БМ) оптоволоконний кабель; з'єднувач SC	Технологія 1000BASE-LX (550-5000 м) багатомодовий (БМ) оптоволоконний кабель; з'єднувач SC
Фізичне середовище передачі								

Рис. 35. Різні технології на основі Ethernet

Після вивчення загальних для всіх трьох історично важливих версій Ethernet характеристик ми докладно розглянемо кожну з них.

Як показано в табл. 21, специфікації 10BASE-2, 10BASE-5 і 10BASE-T використовують однакові часові параметри. Варто зазначити, що час передачі одного біта (бітовий інтервал – bit time) для швидкості 10 Мбіт/с дорівнює 100 нс або 0,1 мс.

Таблиця 21

Параметри технології Ethernet зі швидкістю передачі 10 Мбіт/с

Параметр	Значення
Час передачі біта	100 нс
Канальний інтервал	512 бітових інтервалів
Інтервал між фреймами	96 біт
Кількість колізійних спроб	16
Граничний інтервал очікування в конфліктній ситуації	10
Розмір колізійного jam пакету	32 біта
Максимальний розмір фрейму без мітки	1518 октетів

Мінімальна довжина фрейму	512 біт (64 октети)

Специфікації 10BASE-2, 10BASE-5 і 10BASE-T використовують єдиний формат фрейму. На рис. 36 показаний Ethernet фрейм, який використовується на MAC-підрівні.

Преамбула 7	*Роздільник SFD 1*	*Одержувач 6*	*Відправник 6*	*Довжина/Тип 2*	*Дані / Заповнювач від 46 до 1550*	*Поле FCS 4*

Рис. 36. Ethernet фрейм

Процес передачі даних для традиційних специфікацій Ethernet однаковий аж до нижньої частини фізичного рівня еталонної моделі OSI. Протягом руху фрейму від MAC підрівня до фізичного рівня виконуються додаткові процеси, перш ніж біти опиняться в середовищі передачі фізичного рівня. Одним із найбільш важливих процесів на цій стадії є перевірка *параметра порушення якості сигналу (Signal Quality Error – SQE)*. Підхід, подібний до цього, використовується в багатьох мережевих технологіях. На фізичному рівні мережі постійно відбуваються взаємодії, не пов'язані з передачею даних користувача, необхідних для перевірки працездатності мережі. Механізм SQE завжди використовується в напівдуплексному режимі; допускається його робота в дуплексному режимі, але це не є обов'язковим. Механізм SQE використовується в таких ситуаціях:

– через 4-8 мікросекунд після звичайної передачі для вказівки того, що вихідний фрейм успішно доставлений;

– при виникненні колізій;

– з появою *дефектного сигналу* в середовищі передачі; у якості дефектних сигналів можуть виступати виявлений збійний фрейм або відбиття сигналу, що виникло внаслідок проблем з кабелем, наприклад, через замикання (для різних середовищ передачі потрібне виконання різних умов);

– у разі, якщо передача була перервана через збій, викликаний передачею понад дозволений час.

Усі варіанти структур Ethernet зі швидкістю передачі даних 10 Мбіт/с виконують над октетами, отриманими від MAC-підрівня, процедуру, яка називається *кодуванням сигналу в лінії (line encoding)*. Кодування в лінії описується алгоритмом перетворення біт в

електричні сигнали, що передаються кабелем. Найпростіші варіанти кодування, зокрема *алгоритм без повернення до нуля (nonreturn to zero – NRZ)*, у яких одиничному біту відповідають 5 Вольт, а нульовому – 0 Вольт, зазвичай мають незадовільні часові й електричні характеристики. Із цієї причини були розроблені алгоритми кодування, що володіють необхідними параметрами й підходять для будь-яких середовищ передачі. У системах зі швидкістю передачі 10 Мбіт/із застосовується алгоритм – *манчестерське кодування (manchester encoding).* На рис. 37 проілюстрований принцип манчестерського кодування: по осі Y виміряється напруга у вольтах, по осі X – час.

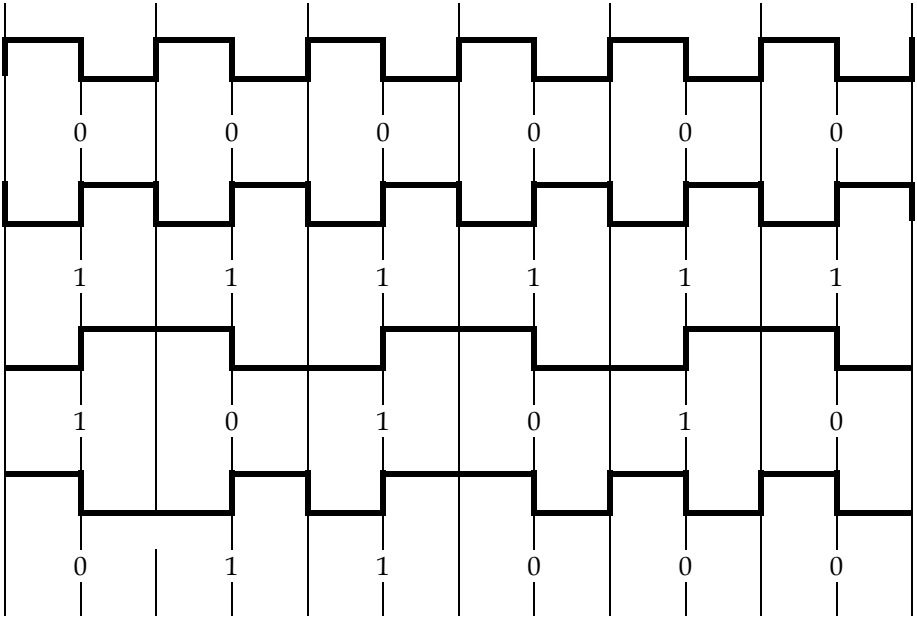


Рис. 37. Приклад манчестерського кодування

Манчестерське кодування засноване на методиці визначення двійкового числа за напрямком зміни напруги в середині бітового інтервалу. У прикладі, проілюстрованому рис. 37, часовий інтервал, необхідний для передачі одного біта, позначений вертикальним виділенням для всіх чотирьох досліджуваних хвильових форм. Зміна позитивного значення напруги на негативне в середині бітового інтервалу для верхньої з показаних хвильових форм інтерпретується

як двійкове число 0.

Для другої хвильової форми (другий графік зверху), навпаки, усередині бітового інтервалу є перехід від негативного значення до позитивного, що відповідає двійковому числу 1.

На відміну від перших двох прикладів, у яких хвильова форма задає послідовності однакових двійкових чисел (0 у першому випадку й 1 у другому), третій приклад показує хвильову форму для послідовності з чергуванням двійкових чисел. У перших двох прикладах сигнал має повертатися у вихідне значення в межах кожного періоду, щоб усередині кожного бітового інтервалу зміна сигналу була однаковою. При кодуванні різних двійкових значень немає необхідності повертати рівень сигналу до його попереднього значення, щоб створити необхідну зміну рівня сигналу в середині бітового інтервалу. Четверта хвильова форма ілюструє сигнал, що кодує послідовність різних двійкових чисел.

Застаріла технологія Ethernet має низку загальних структурних особливостей. Усі версії її називають *поділюваним середовищем Ethernet (shared Ethernet)*, оскільки в них використовується загальний домен колізій.

Часові характеристики, формат фрейму й процес передачі даних є загальними для всіх застарілих реалізацій технології Ethernet зі швидкістю 10 Мбіт/с.

Специфікації й обмеження кабелю 10BASE-5 містять у собі такі моменти:

– тільки одна станція може передавати дані в певний момент часу (а якщо ні, то виникне колізія);

– середовище й пристрої 10BASE-5 можуть працювати тільки в напівдуплексному режимі;

– у кожному сегменті 10BASE-5 можуть існувати не більше 100 станцій, включаючи повторювачі.

3.1.3. Технологія 10BASE-2

У 1985 році був запропонований стандарт 10BASE-2 (спочатку названий 802.3a, 1985), у якому використовувався більш легкий, менший за розміром кабель, що значно спрощувало його монтаж у порівнянні зі стандартом 10BASE-5. Оскільки в цьому стандарті використовується тонкий коаксіальний кабель, його часто називають *Thinnet*. Так само, як і з мережами 10BASE-5, системи 10BASE-2 залежать від стану кабелю вздовж усієї довжини колізійного домена і

є єдиною точкою відмови.

Тимчасові характеристики, формат фрейму й процес передачі є загальними для всіх застарілих реалізацій технологій Ethernet зі швидкістю передачі даних 10 Мбіт/с.

У технології 10BASE-2 використовується манчестерське кодування сигналу в тонкому коаксіальному кабелі. Сигнал у стандарті 10BASE-2 змінюється від 0 до 1 Вольта. Середовище 10BASE-2 може перебувати в стані простою (0 Вольт), якщо жодна зі станцій не передає дані. У технології 10BASE-2 використовується асинхронний режим передачі даних.

Комп'ютери в локальній мережі, яка побудована на основі описуваної технології, з'єднані у вигляді ланцюжка послідовними нерозривними відрізками коаксіального кабелю. Такі відрізки сегменти з'єднані за допомогою *BNC* з'єднувачів *(British Naval Connector – BNC)* і підключаються до Т-образного рознімання на мережевих адаптерах. Коаксіальний кабель використовується як загальна шина для всієї мережі. Наявні робочі станції можуть бути легко переміщені й підключені в новому місці, не менш легко можуть бути підключені до локальної мережі й нові станції. У всьому іншому технологія 10BASE-2 використовує той же напівдуплексний протокол стандарту Ethernet. Кожний з дозволених п'яти сегментів на основі тонкого коаксіального кабелю може мати довжину до 185 м, і кожна робоча станція підключається безпосередньо до Т-образного BNC з'єднувача врізаного в кабель.

3.1.4. Технологія 10BASE-T

З появою стандарту 10BASE-T (названий спочатку 802.3i 1990) коаксіальний кабель був замінений на більш дешевий і простий у монтажі кабель UTP (Unshielded Twisted Pair – неекранована кручена пара). Цей кабель підключався до центрального пристрою, концентратора або комутатора, який є загальною мережною шиною. Тип кабелю, що використовується в стандарті 10BASE-T, припустимі відстані між концентратором і станціями, спосіб монтажу, комутації й тестування UTP кабелів були стандартизовані в специфікаціях на структуровані кабельні системи, завдяки чому були докладно описані фізичні топології, наприклад, зіркоподібна. У стандарті 10BASE-T використовувався напівдуплексний метод передачі, однак згодом був доданий дуплексний зв'язок. Вибухоподібний ріст

популярності мереж Ethernet, коли ця технологія стала домінувальною в локальних мережах, припадає на 1990 рік і пов'язаний з використанням стандарту 10BASE-T і UTP кабелю категорії 5.

Часові характеристики, формат фрейму й процес передачі, описані вище, можуть застосовуватись й у цій технології.

У технології 10BASE-T також використовується манчестерське кодування сигналу для кабелю UTP типу категорії 3 (у сучасних мережах 5, 5е або вище).

Технологія Ethernet зі швидкістю передачі даних 10 Мбіт/с використовує асинхронний режим передачі, і кабель також часто буває не задіяний протягом тривалих проміжків часу, коли не відбувається передача даних. У стандарті 10BASE-T кожні 125 мілісекунд (вісім раз у секунду) передаються *канальні імпульси (link pulse)*, а в решта часу кабель може бути не задіяний. Таким чином, мережа 10BASE-T заповнена імпульсами з'єднання.

Кожен дріт кабелю типу неекранована кручена пара (UTP) стандарту 10BASE-T, максимальна довжина якого не може перевищувати 90 метрів, складається із цільного дроту, діаметр якого повинен перебувати в межах від 0,4 мм до 0,6 мм (від 26 до 22 AWG (American Wire Gauge – американська система оцінки дротів)). У якості сполучного кабелю, максимальна довжина якого не повинна перевищувати 10 м, використовується перехресний кабель із тими ж характеристиками, але більш гнучкий, оскільки він часто зазнає навантаження і звивається. Відповідні кабелі мають значення NVP, рівне 0,585, імпеданс 100 Ом і забезпечуються восьмиконтактними з'єднувачами RJ 45, які описані в стандарті ISO/IEC 8877. Довжина кабелю між станціями й концентратором зазвичай перебуває в діапазоні від 0 до 100 метрів (від 0 до 328 футів), хоча точне значення для максимальної довжини визначається величиною затримки сигналу в сегменті (будь-яка довжина кабелю, при якій затримка не перевищує 1000 нс, вважається припустимою й залежить від використовуваного устаткування). У більшості випадків багатопарний UTP кабель із діаметром провідника 0,5 мм (24 AWG) відповідає вимогам максимальної відстані до 100 м.

Незважаючи на те, що кабель категорії 3 підходить для використання в мережах стандарту 10BASE-T, сьогодні настійно рекомендується при монтажі нових мереж використовувати кабель

категорії 5е або вище. Також рекомендується дотримуватися стандартів T568A або T568B при розведенні дротів і запресовуванні з'єднувачів. Така практика монтажу дозволить використовувати те ж середовище передачі для роботи різних протоколів канального доступу (включаючи 1000BASE-T) без заміни кабельного господарства.

У табл. 22 показана схема розташування виводів з'єднання стандарту 10BASE-T. Зверніть увагу, що для передачі й приймання використовуються різні провідники (у коаксіальному кабелі є тільки один провідник).

Таблиця 22

Схема розташування виводів з'єднання стандарту 10BASE-T

Номер контакту	**Сигнал**
1	TD+. Передача даних, позитивний диференціальний сигнал
2	TD–. Передача даних, негативний диференціальний сигнал
3	RD+. Приймання даних, позитивний диференціальний сигнал
4	Не використовується
5	Не використовується
6	RD–. Приймання даних, негативний диференціальний сигнал
7	Не використовується
8	Не використовується

Треба звернути увагу, що всередині концентраторів реалізована та ж шинна топологія, що є доменом колізій. При підключенні робочої станції до комутатора за допомогою прямого кабелю кожне з'єднання є двохточковим. Внутрішній пристрій комутатора дозволяє використовувати повну пропускну здатність одночасно для кожної пари проводів або портів комутатора без колізій.

Оскільки при з'єднанні двох станцій, комутаторів або станції з комутатором використовуються зв'язки типу "крапка-крапка", у всіх цих випадках є два фізично розділених канали передачі по двом парам UTP кабелю. У такому разі колізії є не фізичною подією, а скоріше логічним розв'язком не допускати одночасне використання сигналів Tx і Rx. Таким чином, для розробника мережі існує вибір між напівдуплексною (з адміністративними обмеженнями, обумовленими природою алгоритму CSMA/CD) і дуплексною (без

фізичних колізій) конфігураціями. У більшості випадків використовується дуплексний режим, при якому не тільки відсутні колізії, але й подвоюється пропускна здатність з'єднання. Коли відповідний стандарт був уперше запропонований IEEE, він звався 802.3x 1997 Full Duplex. Однак у випадку з'єднання станції з концентратором, що створюють домен колізій, можливе використання тільки напівдуплексного режиму, де всі з'єднання підпорядковані правилам доступу до середовища алгоритму CSMA/CD.

Технологія 10BASE-T підтримує швидкість передачі даних 10 Мбіт/с у напівдуплексному режимі, однак у дуплексному режимі швидкість передачі трафіку може досягати 20 Мбіт/с (хоча частина пропускної здатності використовується при передачі службових, а не користувацьких даних). Використання такої концепції стало необхідним для збільшення швидкості передачі даних в Ethernet мережах.

Принципи побудови мереж 10BASE-T. Зазвичай лінія зв'язку 10BASE-T являє собою з'єднання між робочою станцією й концентратором або комутатором. Концентратори варто розглядати як багатопортові повторювачі та враховувати обмеження на кількість повторювачів між двома вилученими станціями. Комутатори за принципом роботи відповідають багатопортовим мостам, і за умов їхнього використання існує тільки обмеження по довжині лінії зв'язку, яка не повинна перевищувати 100 м. Обмежень на припустиму кількість комутаторів між віддаленими станціями немає.

Незважаючи на те, що концентратори можуть поєднуватися в стек (цей процес іноді називають каскадуванням, або послідовним з'єднанням), намагаються уникати цього, щоб не вийти за межі допустимих значень затримки сигналу між віддаленими станціями. Фізичні розміри мереж 10BASE-T у питанні про припустиму кількість повторювачів підпорядковуються тим же правилам, що й мережі стандартів 10BASE2 10BASE5. Якщо для підключення станцій потрібні кілька концентраторів, краще організувати їх в ієрархічному порядкові, сформувавши деревоподібну структуру, ніж послідовним ланцюгом. Чим менше повторювачів розділяють станції, тим вище продуктивність мережі. За допомогою поєднуваних у стек концентраторів або *концентраторів з високо продуктивною внутрішньою шиною (backplane)* можна підключити велику кількість станцій; при цьому весь стек буде розглядатися як єдиний пристрій, один концентратор. Не існує обмежень на

кількість поєднуваних у *послідовні ланцюги (daisy chaining)* концентраторів.

Теоретично між станціями припустимі будь-які відстані, однак не треба забувати про одне важливе структурне обмеження. Незалежно від структурних особливостей побудови мережі й задіяних середовищ передачі, однією з основних вимог є значення мінімуму затримок між віддаленими станціями. Чим менше максимальне значення затримки, тим вища загальна продуктивність мережі.

У з'єднаннях стандарту 10BASE-T можна створювати сегменти довжиною до 100 м без повторювачів. На перший погляд ця відстань може здатися великою, але на практиці при монтажі мережі в реальних будинках його не завжди досить. Концентратори можуть допомогти при розв'язанні цієї проблеми, однак варто пам'ятати про обмеження в чотири послідовні пристрої, яке пов'язане з часовими параметрами. Широке поширення комутаторів зробило зазначені обмеження менш принциповими. Якщо робоча станція підключена до комутатора на відстані 100 метрів, вказане з'єднання через 100 метрів може бути використане для підключення до наступного комутатора, і т.д. Оскільки більшість сучасних мереж 10BASE-T комутується, то таке обмеження ставиться тільки до відстаней між пристроями, але не до максимальної довжини сегмента мережі. У розглянутому стандарті припустиме використання топологій типу "кільце", "зірка" і "розширена зірка". Найбільш часто потрібно вирішувати проблеми, пов'язані з логічною топологією й потоками даних, але не часовими параметрами або обмеженнями відстані.

Таблиця 23

Характеристики з'єднань стандарту 10BASE-T

З'єднання	**Максимальний розмір сегмента**
Станція-Станція, станція-комутатор, комутатор-комутатор	100-м без обмежень на кількість послідовних з'єднань
Станція-Концентратор	100-м, обмеження згідно із правилом про 4-и концентратори

Лабораторна робота №5 (2 год.)

Тема: Аналіз та перевірка дієздатності комп'ютерної мережі Ethernet

Мета: розвивати у студентів аналітичні вміння щодо перевірки

дієздатності локальної мережі Ethernet, побудованої з використанням різних мережевих середовищ;

виховувати ціннісне ставлення студентів до майбутньої професійної діяльності.

Студент повинен знати: принципи побудови локальної мережі Ethernet, обмеження для локальної мережі Ethernet, алгоритм розрахунку конфігурації мережі Ethernet.

Студент повинен уміти: проводити розрахунок конфігурації мережі Ethernet.

Обладнання: комп'ютерний клас з локальною мережею на основі стандарту Fast Ethernet.

Інструктаж

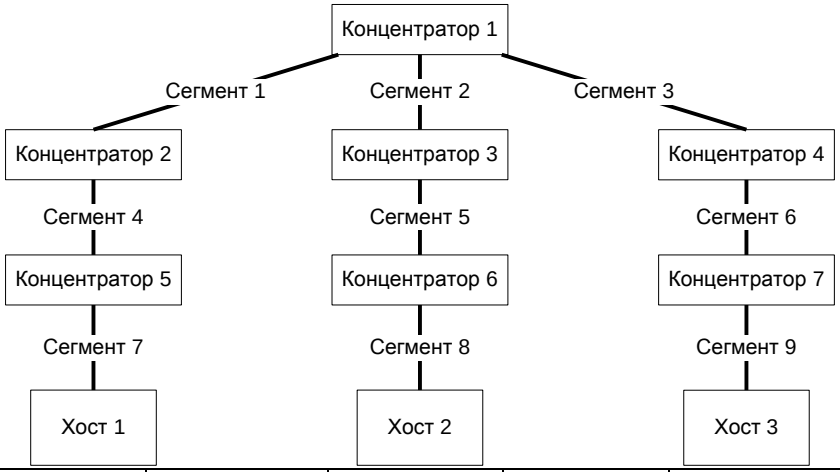
1. Визначити параметри локальної мережі Ethernet, які підлягають перевірці.
2. Обговорити обмеження локальної мережі Ethernet та визначити необхідні та достатні умови її працездатності.

Завдання для письмового звіту та спостережень:

– розрахувати коефіцієнт Path Delay Value для запропонованого варіанта завдання та зробити висновок про дієздатність мережі;

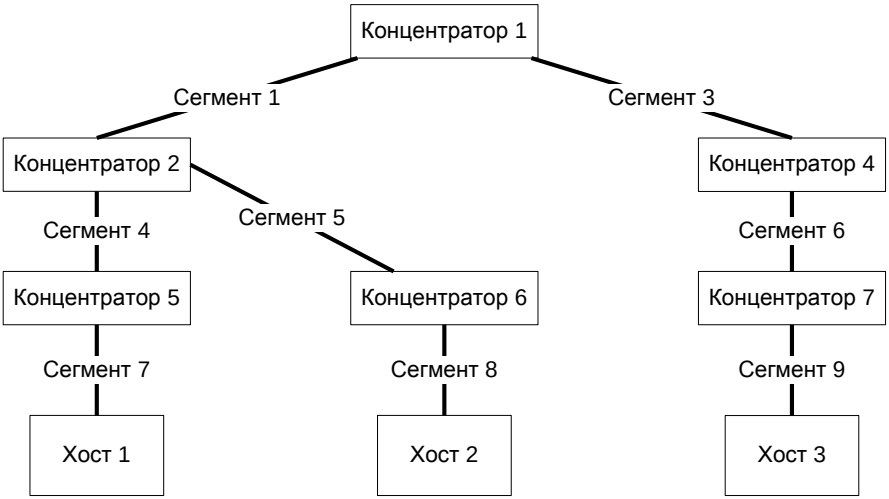
– розрахувати коефіцієнт Path Variability Value для запропонованого варіанта завдання та зробити висновок про дієздатність мережі;

Варіант 1



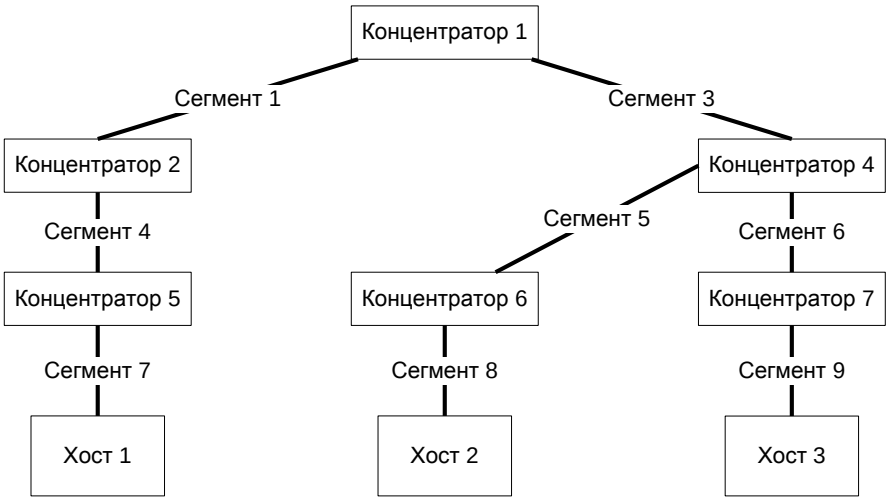
	10 Base-FB	10Base-FL	10 Base-T	Довжина, м
Сегмент 1	+			500
Сегмент 2	+			300
Сегмент 3	+			400
Сегмент 4		+		1000
Сегмент 5		+		300
Сегмент 6		+		400
Сегмент 7			+	100
Сегмент 8			+	50
Сегмент 9			+	100

Варіант 2



	10 Base-FB	10Base-FL	10 Base-T	Довжина, м
Сегмент 1	+			400
Сегмент 3	+			500
Сегмент 4		+		1100
Сегмент 5		+		1100
Сегмент 6		+		600
Сегмент 7			+	100
Сегмент 8			+	100
Сегмент 9			+	100

Варіант 3



	10 Base-FB	10Base-FL	10 Base-T	Довжина, м
Сегмент 1	+			500
Сегмент 3		+		500
Сегмент 4	+			1000
Сегмент 5	+			1000
Сегмент 6		+		500
Сегмент 7			+	80
Сегмент 8			+	80
Сегмент 9			+	100

Самостійна робота №5

Тема: Підключення до служб загального призначення при проектуванні ієрархічної мережі

Мета: розвивати аналітичні вміння студентів щодо проектування ієрархічної мережі та підключення служб загального призначення.

Студент повинен знати: принципи проектування та особливості підключення служб загального призначення в ієрархічних комп'ютерних мережах.

Студент повинен уміти: обирати тип підключення служби загального призначення в ієрархічній мережі.

Хід роботи

Теоретична частина

1. Які типи контролю повинні бути реалізовані в маршрутизаторі рівня доступу для блокування атак, що виходять з мережі?

2. Якими основними факторами визначається число маршрутизаторів, що беруть участь у процесі збіжності?

3. Чим обумовлена виняткова складність зміни способу розподілу мережних адрес?

Практична частина

Завдання

Законспектуйте основні положення щодо підключення загальних служб безпосереднє до ядра мережі та підключення через демілітаризовану зону (DeMilitarized Zone — DMZ).

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Порівняльний аналіз стандартів локальних мереж та перспективи їх розвитку"

ТЕМА 3.2. ВИСОКОШВИДКІСНІ ТЕХНОЛОГІЇ ЛОКАЛЬНИХ МЕРЕЖ

Лекція

План

1. Технологія Ethernet зі швидкістю передачі 100 Мбіт/с
2. Гігабітові технології Ethernet

3. Технологія Token Ring
4. Технологія FDDI

Література

Основна

1. *Бройдо В. Л.* Вычислительные системы, сети и телекоммуникации: учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Прикладная информатика" и "Информационные системы в экономике" / В. Л. Бройдо, О. П. Ильина. – 3-е изд. – Москва [и др.]: Питер, 2008. – 765 с.: ил., табл.; 24 см.

2. *Гук М.* Аппаратные средства локальных сетей. Энциклопедия : [Наиболее полн. и подроб. рук.] / Михаил Гук. – СПб. : Питер, 2000.– 572 с.

3. *Новиков Ю. В.* Локальные сети: Архитектура, алгоритмы, проектирование / Новиков Ю. В., Кондратенко С. В. – М.: ЭКОМ, 2002. – 311 с.: ил.; 23 см. – (Современные компьютерные технологии).

4. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

Додаткова

1. *Бабій М. С.* Локальні мережі ЕОМ: [навч. посіб. для студ. спец. "Прикладна математика"] / Михайло Семенович Бабій. – Суми : Видавництво СумДУ, 2003. – 64 с.

2. *Бортник Г. Г.* Мережі доступу: навч. посібник для студ. напряму підготовки 0924 – "Телекомунікації" всіх спец. / Бортник Г. Г., Стальченко О. В., Яблонський В. Ф. – Вінниця : ВНТУ, 2006. – 139 с.

3. *Зайченко Ю. П.* Комп'ютерні мережі: навч. посіб. для студ. вищ. навч. закл. [Intertational Science and Technology University] / Ю. П. Зайченко. – К. : Слово, 2003. – 284 с. – (До 10-річчя Міжнародного науково-технічного ун-ту).

4. *Ибе О.* Сети и удаленный доступ: Протоколы, проблемы, решения / Оливер Ибе. – М.: ДМК Пресс, 2002. – 332 с.: ил.; 23 см. – (Серия "Защита и администрирование").

5. *Кулаков Ю. А.* Локальные сети / Ю. А. Кулаков, Г. М. Луцкий. – К. : Юниор, 1998. – 336 с.

6. *Олексюк В. П.* Організація комп'ютерної локальної мережі : [посіб.] / Олексюк В. П., Балик Н. Р., Балик А. В. – Тернопіль. : Підручники і посібники, 2006. – 80 с.

3.2.1. Технологія Ethernet зі швидкістю передачі 100 Мбіт/с

Технологія Ethernet зі швидкістю передачі 100 Мбіт/с, також відома як Fast Ethernet (швидка технологія в порівнянні з оригінальною технологією Ethernet зі швидкістю передачі даних 10 Мбіт/с), містить у собі цілу серію технологій. Двома найбільш успішними комерційними реалізаціями ідеї такої технології стали стандарти 100BASE-TX (на основі мідного UTP кабелю) і 100BASE-FX (на основі багатомодового оптичного волокна).

Загальними для технологій 100BASE-TX і 100BASE-FX є:

– часові параметри;
– формат фрейму;
– деякі етапи процесу передачі даних.

У табл. 24 перераховані робочі параметри технології Fast Ethernet, яка працює на швидкості 100 Мбіт/с.

Таблиця 24

Параметри роботи 100 Мбіт/с технології Ethernet

Параметр	Значення
Час передачі одного біта (бітовий інтервал)	10 нс
Канальний інтервал	512
Інтервал між фреймами	96 біт
Кількість колізійних спроб	16
Інтервал очікування при колізії	10
Розмір jam пакета колізії	32 біта
Максимальний розмір фрейму	1518 октетів
Мінімальний розмір фрейму	512 біт (64 октетів)

Технології 100BASE-TX і 100BASE-FX використовують однакові часові параметри. Варто зазначити, що один бітовий інтервал у технології Ethernet зі швидкістю 100 Мбіт/сі становить 10 нс. Формат

фрейму для швидкості передачі даних 100 Мбіт/с повністю збігається з форматом технології 10 Мбіт/с.

Завдяки появі Fast Ethernet швидкість передачі даних збільшилася в 10 разів. У результаті з'явилися нові вимоги. Час, необхідний для передачі одного біта, зменшився, при цьому зросла частота передачі. Необхідно ретельно витримувати часові параметри; потрібні частоти, близькі до граничних значень для середовищ передачі, що використовуються. Це в результаті призвело до збільшення чутливості до перешкод. Для вирішення проблем, пов'язаних із синхронізацією, пропускною здатністю й *співвідношенням сигнал/шум (Signal to Noise Ratio – SNR)* у мережах зі швидкістю 100 Мбіт/с використовуються два роздільні етапи кодування сигналу. Основна ідея полягає у використанні систем кодування, спроектованих для одержання необхідних характеристик сигналів, їх ефективної передачі мережею, включаючи питання синхронізації, ефективного використання смуги пропущення й поліпшеного співвідношення сигнал/шум. Перша частина процесу кодування називається механізмом 4 біт/5 біт (4bit/5bit – 4B/5B), друга частина – це фактичне кодування сигналу з усіма його особливостями для передачі мідним дротом й оптичним волокном.

Обидва стандарти Ethernet, які працюють зі швидкістю 100 Мбіт/с, 100BASE-TX і 100BASE-FX, кодують напівбайти (чотири бітові групи), отримані з MAC підрівня. Чотирибітові комбінації перетворюються в п'ятибітові символи; символи несуть у собі контрольну інформацію (таку, як початок фрейму або прапор стану "середовище не зайняте"). Повний фрейм, призначений для передачі, містить контрольні символи й символи даних (груповий код даних). Таке додаткове ускладнення потрібне для того, щоб досягти десятикратного збільшення швидкості передачі.

Після застосування 4B/5B кодування біт (у формі групових кодів) необхідно передати через середовище передачі (що допускає застосування лінійного кодування). Використання алгоритму кодування 4-х бітів у 5 означає, що за той самий інтервал часу потрібно передати 125 Мбіт замість ста. Ця особливість висуває додаткові вимоги до якості середовища передачі, передатчиків і приймачів. У час, коли немає даних для передачі, передаються групи біт "заповнення" для заповнення порожніх періодів і підтримки синхронізації. У цьому й полягає основна відмінність способу

обробки даних для різних середовищ передачі: мідного дроту в стандарті 100BASE-TX та оптичного волокна стандарту 100BASE-FX.

Принципи побудови мереж Fast Ethernet. У технології Fast Ethernet зв'язки складаються в основному зі з'єднань між станціями й концентратором або комутатором. Концентратори фактично є багатопортовими повторювачами, і між віддаленими станціями припустиме використання обмеженої кількості таких пристроїв. Комутатори в найпростішому випадку можна розглядати як багатопортові мости. При використанні таких пристроїв діє обмеження на довжину UTP кабелю в 100-м, але обмежень на їхню кількість у ланцюжку немає.

Повторювачі повинні бути марковані за допомогою слова *Class (клас повторювача)* із вказівкою римської цифри I або II у кружечку для позначення пристроїв класу I або II (Class I або Class II). Концентратори першого класу вносять затримку до 140 бітових інтервалів. Будь-який повторювач, що не належить до одного із двох типів (100BASE-TX або 100BASE-FX), є повторювачем класу I. Варто зазначити, що немарковані повторювачі також є пристроями класу I. На рис. 38 показаний максимальний діаметр колізійного домену при використанні одного повторювача класу I стандарту 100BASE-TX. Використання комутаторів знімає ці обмеження, а граничні значення визначаються максимальною довжиною з'єднання між інтерфейсами, що залежить від типу середовища передавання.

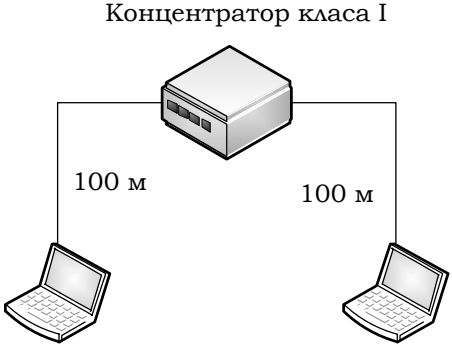


Рис. 38. Максимальний діаметр колізійного домену при використанні концентратора першого класу

Повторювач класу II вносить затримку не більш 92-х бітових інтервалів. Завдяки меншій величині затримки припустиме

використання двох послідовних пристроїв цього класу, але тільки з дуже коротким кабелем між ними. На рис. 39 показаний максимальний діаметр колізійного домену для концентраторів другого класу стандарту 100BASE-TX. Використання комутаторів знімає ці обмеження, і єдиним обмежувальним фактором є максимальна довжина кабелю між інтерфейсами, величина якої залежить від конкретного середовища передачі.

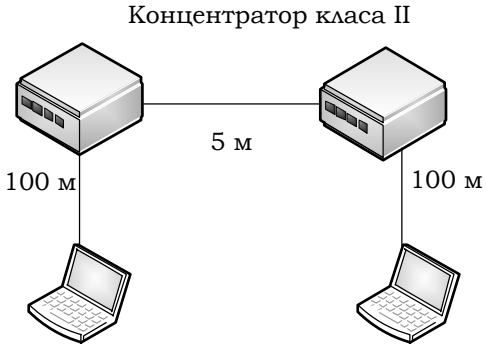


Рис. 39. Діаметр колізійного домену для концентраторів другого класу

Як і для версій технологій Ethernet зі швидкістю передачі 10 Мбіт/с, припустимі деякі зміни в принципах побудови мережі для версій зі швидкістю 100 Мбіт/с. Однак ці зміни не повинні вносити додаткові затримки. Якщо в мережі використовується нове високопродуктивне обладнання, можливо, деякі обмеження вдасться подолати. Наприклад, якщо використовується кабель, який більше припустимої довжини між повторювачами, потрібно буде більш короткий кабель для підключення станцій. Однак порушення принципів побудови мережі для стандарту 100BASE-TX настійно не рекомендується. Внесені структурні зміни не повинні суперечити часовим параметрам, описаним у статті 29 чинного стандарту 802.3, і повинні бути передбачені у використовуваному устаткуванні. Будь-який пристрій, що підтримує перетворення між декількома швидкостями передачі, наприклад, 10 і 100 Мбіт/с, є мостом другого рівня моделі OSI. Пристрій, здатний виконувати перетворення сигналу між середовищами з різними швидкостями передачі даних, не може бути повторювачем. Однак той самий пристрій може повторювати сигнал між портами, що передають на однаковій швидкості.

UTP кабель стандарту 100BASE-TX практично не відрізняється від кабелю для 10BASE-T, за винятком того, що продуктивність зв'язку повинна задовольняти більш високому стандарту категорії 5 або ISO Class D. Довжина кабелю 100BASE-TX між двома повторювачами класу II не може перевищувати 5 м.

Довжина з'єднань при роботі в дуплексному режимі може бути вище значень, зазначених у табл. 25, оскільки в такому разі істотною є тільки здатність середовища передачі доставляти придатний для декодування сигнал, а не дворазова затримка (round trip – затримка на передачу сигналу в прямому і зворотному напрямку). Не так уже рідко можна зустріти мережі Fast Ethernet, що працюють у напівдуплексному режимі. Однак використання напівдуплексної передачі не бажане, оскільки сигнальна схема розрахована на дуплексний режим роботи, і тому примусове використання напівдуплексної взаємодії є нерозумним використанням ресурсів.

Рекомендується всі з'єднання між станціями й концентратором або комутатором будувати на автоматично визначеному режимі роботи, даючи можливість використовувати максимальну продуктивність. Відключати автовизначення потрібно тільки тоді, якщо з'єднання не можуть бути встановлені з використанням функції автовизначення. У більшості випадків з'єднання повинні встановлюватися автоматично.

У табл. 25 перераховані правила побудови мереж Fast Ethernet.

Таблиця 25

Довжина з'єднань для різних структур

Структура	**100BASE-TX (м)**	**100BASE-FX (м)**	**100BASE-TX і 100BASE-FX (м)**
Станція-станція, станція-комутатор, комутатор-комутатор (напів або дуплексний)	100	412	
Один повторювач, клас I (напівдуплексний)	200	272	100 TX 160,8 FX
Один повторювач, клас II (напівдуплексний)	200	320	100 TX 208 FX
Два повторювачі, клас II (напівдуплексний)	205	228	105 TX 211,2 FX

З'єднання 100BASE-TX не вимагають повторювачів для відстаней до 100 метрів. На перший погляд така відстань видається досить великою, але в реальних будинках її часто буває недостатньо. Концентратори допомагають подолати обмеження на довжину з'єднань, але при цьому залишаються в силі правила, перераховані в табл. 25 і пов'язані з часовими параметрами обмеження. Широке поширення комутаторів зробило обмеження на довжину з'єднань менш значимими. Робоча станція може бути розташована на відстані до 100-м від комутатора, який, у свою чергу, може бути підключений іншим стометровим з'єднанням до наступного комутатора, і т.д. Максимально можлива довжина сегмента є практичним обмеженням між пристроями для мереж Fast Ethernet, більшість із яких є комутованими. Із цією технологією можна використовувати топології: "зірка" і "розширена зірка". У такому разі постає питання вибору логічної топології й маршрутів потоків даних, а не обмежень за часом або відстані.

3.2.2. Гігабітові технології Ethernet

Метод Fast Ethernet (100 Мбіт/с) продемонстрував значний розвиток технологій у порівнянні з традиційною мережею Ethernet (10 Мбіт/с). Ще більш значний прогрес, досягнутий у гігабітовій технології (Gigabit Ethernet) відносно Fast Ethernet, свідчить про якість стандартів IEEE, успіх розробок і задає напрямок розвитку ринку. Технологія Gigabit Ethernet, що працює зі швидкістю передачі даних 1000 Мбіт/с, у 100 раз збільшує швидкість передачі інформації в мережі в порівнянні з популярними мережами 10BASE-T. Хоча принципи MAC адресації, доступу CSMA/CD і, що ще більш важливо, формат фрейму збереглися такими ж, як і в попередніх версіях Ethernet, багато інших аспектів роботи MAC рівня, фізичного рівня й середовища передачі зазнали значних змін.

Сьогодні припустиме використання одного мідного дроту для швидкостей передачі даних 10/100/1000 Мбіт/с. Гігабітові комутатори й маршрутизатори з гігабітовими портами доступу до мережі нині стають звичними пристроями в монтажних шафах. Усе більше встановлюється з'єднань із використанням одно й багатомодових оптичних кабелів. Однією з відмінних рис технології Gigabit Ethernet є застосування оптичних носіїв сигналу. Однак потреба у використанні наявного кабельного господарства на основі

мідних проводів привела до появи дуже продуманої технології, що дозволяє використовувати настільки популярний в 10 Мбіт/с і 100 Мбіт/с версіях середовища Ethernet UTP кабель категорії 5. Усі технології Gigabit Ethernet за своєю природою є дуплексними. Свідченням розвитку технології служить розробка стандартів передачі даних зі швидкостями 40, 100 і 160 Гбіт/с. Найбільш вражає перехід Ethernet з технології, що використовується тільки всередині локальних мереж, у розряд рішень, що використовуються для об'єднання віддалених локальних, регіональних і розподілених обчислювальних мереж.

Технології Ethernet зі швидкістю передачі 1000 Мбіт/с

У 1998 році комісією 802.3z Інституту інженерів з електротехніки й електроніки (Institute of Electrical and Electronics Engineers – IEEE) був прийнятий стандарт 1000BASE-X, що підвищив швидкість передачі даних оптоволоконними каналами зв'язку в дуплексному режимі до 1 Гбіт/с, таким чином збільшивши швидкість у 100 разів у порівнянні зі стандартом 10BASE-T. Стандарт 1000BASE-T, який описує технологію зі швидкістю 1 Гбіт/с, що використовує мідний UTP кабель категорії 5, був прийнятий у 1999 році.

У табл. 26 перераховані робочі параметри технології Ethernet, яка працює зі швидкістю 1000 Мбіт/с

Таблиця 26

Робочі параметри середовища Gigabit Ethernet

Параметр	Значення
Час передачі одного біта	1 нс
Канальний інтервал	4096 бітових інтервалів
Інтервал між фреймами	96 біт
Кількість колізійних спроб	16
Інтервал очікування при колізії	10
Розмір колізійного jam пакета	32 біта
Максимальний розмір фрейму без мітки	1518 октетів
Мінімальний розмір фрейму	512 битов (64 октету)
Максимальний сплеск	65536 битов

Стандарти 1000BASE-T, 1000BASE-SX і 1000BASE-LX використовують однакові часові параметри. Необхідно зазначити, що 1 бітовий інтервал (час передачі одного біта) на швидкості

1000 Мбіт/с дорівнює 1 нс. Також треба пам'ятати, що деякі відмінності в часових параметрах у порівнянні з традиційною технологією Ethernet і Fast Ethernet пов'язані зі специфічними проблемами, що виникають при настільки малих значеннях бітових і канальних інтервалів.

Технологія Ethernet зі швидкістю передачі 1000 Мбіт/с (Gigabit) використовує той же формат фрейму, що й технології зі швидкостями 10 і 100 Мбіт/с. Для різних реалізацій технології Gigabit Ethernet, залежно від середовища передачі, реалізовані різні алгоритми перетворення фреймів у біти.

Метод Gigabit Ethernet збільшив швидкість передачі даних у 10 разів у порівнянні з Fast Ethernet. Так само, як це було у випадку з Fast Ethernet, збільшення швидкості висуває додаткові вимоги: біти, що передаються по з'єднанню, займають менший проміжок часу (1 нс), зросла частота передачі, що вимагає більш ретельної синхронізації. Для передачі необхідні частоти, близькі до граничних значень для середовища передачі, що викликало підвищену чутливість до перешкод. Для розв'язання проблем із синхронізацією пропускна здатність й співвідношення сигнал/шум у технології Gigabit Ethernet для кодування інформації використовуються два окремі етапи. Основна ідея полягає у використанні кодів, які забезпечують необхідні характеристики користувацьких даних, включаючи синхронізацію, ефективне використання пропускної здатності й поліпшенні співвідношення сигнал/шум.

Повторювані бітові групи MAC підрівня перетворюються в символи, які можуть контролювати таку інформацію, як початок фрейму, кінець фрейму, і вказувати стан простою середовища передачі. Повний фрейм розбивається на контрольні символи й символи даних (групи кодів даних). Додаткова складність реалізації необхідна для досягнення десятикратного збільшення швидкості мережі в порівнянні з Fast Ethernet. У стандарті 1000BASE-T для кодування першої частини використовується алгоритм, що називається 8bit 1Quinary quarter (кодування 8B1Q4). Друга частина кодування відповідає за фактичне кодування сигналу для конкретного середовища передачі й використовує принцип чотиривимірного п'ятирівневого модулювання амплітуди імпульсу (4 dimensional 5 level pulse amplitude modulation – 4D PAM5). Використання послідовних алгоритмів кодування сигналу 8B1Q4 і 4D

PAM5 забезпечує синхронізацію, необхідну пропускну здатність і необхідні характеристики для співвідношення сигнал/шум, що дозволяють передавати дані в дуплексному режимі по кожній із чотирьох пар проводів одночасно. Для стандарту 1000BASE-X використовується кодування 8 bit/10 bit (8B/10B) (засноване на принципах, аналогічних алгоритму 4B/5B) і простого NRZ кодування в лінії для оптичного сигналу.

Технологія 1000BASE-T

При розробці стандарту 1000BASE-T (802.3ab 1999 Gigabit Ethernet over twisted pair) ставилися завдання:

– надати такі можливість використовувати наявні кабельні мережі на основі крученої пари категорії 5;

– гарантувати працездатність кабелю, що пройшов тест категорії 5е, який проходить практично будь-який кабель за умови правильно встановлених і запресованих з'єднувачів на його кінцях;

– забезпечити сумісність із технологіями 10BASE-T і 100BASE-TX;

– передбачити можливість використання такого стандарту для побудови магістралей усередині будинків, зв'язків між комутаторами, кабельних вузлів, серверних блоків і підключення високошвидкісних робочих станцій;

– забезпечити десятикратне збільшення пропускної здатності в порівнянні з технологією Fast Ethernet, яка стала широко розповсюдженим середовищем, що використовується споживачами.

Для досягнення необхідної швидкості при використанні мідного дроту категорії 5е задіються всі чотири пари дротів. Кабель категорії 5е може передавати трафік до 125 Мбіт/с. Використання складної електричної схеми, дуплексної передачі для однієї пари дозволяє передавати до 250 Мбіт/с по кожній з пар, тому повна пропускна здатність для чотирьох пар становить 1000 Мбіт/с (1 Гбіт/с). При аналізі принципу роботи технології зручно розглядати ці чотири пари проводів у якості "ліній", по яких одночасно передаються дані (складання даних проводиться в точці призначення одержувачем).

Часові характеристики, формат фрейму й спосіб передачі є загальними для всіх розглянутих версій технології Ethernet, які працюють зі швидкістю передачі даних 1000 Мбіт/с.

У з'єднаннях 1000BASE-T використовується 8B1Q4 кодування й алгоритм лінійного кодування 4D PAM5 для кабелів категорії не

нижче 5е. Для досягнення швидкості в 1 Гбіт/с потрібне одночасне використання всіх чотирьох пар у дуплексному режимі. Такий механізм роботи приводить до виникнення безперервних колізій у кожній з пар проводів, природа яких відрізняється від колізій, що виникали в перших Ethernet мережах на основі коаксіального кабелю. Термін *постійні колізії* означає, що передача й приймання даних відбуваються одночасно по тому самому дроту, що приводить до дуже складного виду *фронтів імпульсу (voltage patterns)*. Однак, оскільки в розглянутій технології використовуються складні вбудовані електричні кола, які поряд з іншими технологіями використовують ще й техніку під назвою *придушення луни (echo cancellation)*, вони забезпечують надійну роботу лінії зв'язку.

Незважаючи на постійні колізії сигналу, система все-таки працює завдяки ретельному вибору рівнів сигналу напруги й використанню механізму прямого виправлення помилок рівня 1.

У табл. 27 зібрана повна інформація про використання всіх чотирьох пар UTP кабелю. Як A, B, C і D позначені лінії передачі даних в одному кабелі. Дані від передавальної станції акуратно діляться на чотири потоки, кодуються, передаються й розпізнаються паралельно, після чого збираються в один потік.

Таблиця 27

Схема розпаювання контакту для з'єднання 1000BASE-T

Номер контакту	Сигнал
1	BI_DA+ (двонаправлені дані, позитивний напрямок)
2	BI_DA– (двонаправлені дані, негативний напрямок)
3	BI_DB+ (двонаправлені дані, позитивний напрямок)
4	BI_DB– (двонаправлені дані, негативний напрямок)
5	BI_DC+ (двонаправлені дані, позитивний напрямок)
6	BI_DC– (двонаправлені дані, негативний напрямок)
7	BI_DD+ (двонаправлені дані, позитивний напрямок)
8	BI_DD– (двонаправленні дані, негативний напрямок)

На рис. 40 схематично показана одночасна дуплексна передача чотирма парами. Кабельні з'єднання типу "станція-станція", "комутатор-комутатор" і "станція-комутатор" організують так само, як і для технології Fast Ethernet.

Важливим є те, що стандарти для Gigabit, Fast і 10BASE-T Ethernet сумісні між собою. На перший погляд це може здатися

малореальним, але з'ясовується, що якщо встановлені кабельні системи протестовані на відповідність категорії 5е, і всі вісім проводів у розніманні RJ 45 підключені, такі системи можуть використовуватися спільно для технологій Gigabit, Fast і 10BASE-T Ethernet. Аналогічно, як після появи стандартів Fast Ethernet з'являлися 10/100 інтерфейси, були розроблені інтерфейси 10/100/1000. Завдяки використанню однакового формату фрейму, сумісного кабельного господарства й розробки розумного інтерфейсу всі технології відмінно працюють разом.

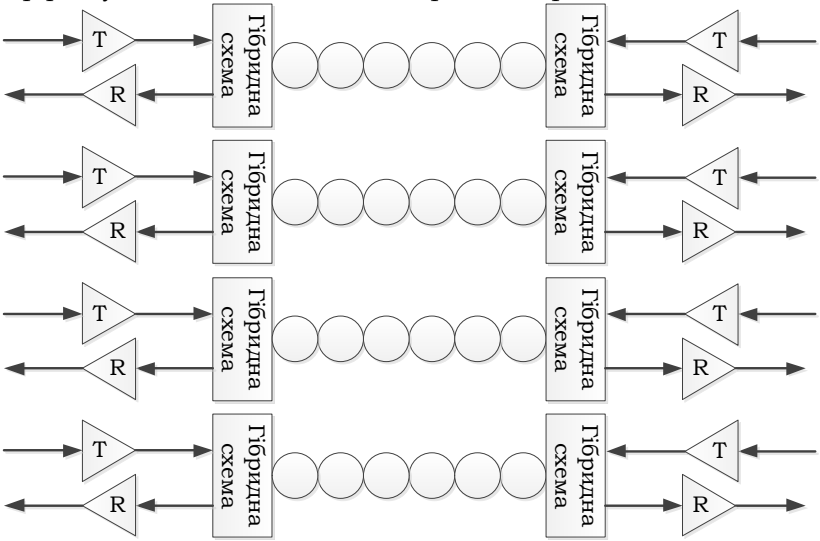


Рис. 40. Передача сигналу 1000BASE-T

З історичних причин у технології 1000BASE-T збережені режим доступу CSMA/CD і напівдуплексний режим передачі. Однак у переважній більшості випадків середовище 1000BASE-T використовується в дуплексному режимі, який досягається за допомогою складних гібридних електричних кіл, які можуть одночасно використовуватися як для передачі (Tx), так і приймання даних (Rx).

Перед початком взаємодії учасники передачі визначають, хто з них буде діяти в якості основного джерела міток часу, а хто, використовуючи потоки даних, у якості вторинного джерела. Джерела міток часу (тобто синхронізації) служать для створення

часових маркерів, що використовуються при передачі сигналу. Зазвичай процес відбувається під час відпрацьовування функції автовизначення, хоча може бути настроєний вручну. Набір інших параметрів задається аналогічно, включаючи тип режиму передачі (напівдуплексний або дуплексний). У процесі автовизначення багатопортові пристрої (комутатор або концентратор) вибираються в якості основного джерела міток часу.

Технології 1000BASE-SX і 1000BASE-LX

Технологія Gigabit Ethernet на основі оптоволоконного кабелю є однією з найкращих при створенні магістральних з'єднань. Вона має такі переваги:

– швидкість передачі даних становить 1000 Мбіт/с, що дозволяє поєднувати групи широко використовуваних пристроїв Fast Ethernet;

– стійка до перешкод;

– відсутні потенційні проблеми із заземленням між кабелем і підлогою, стінами або будинками;

– існує безліч пристроїв стандарту 1000BASE-X;

– максимально припустима довжина сегмента досить велика.

Стандарт для Gigabit Ethernet мереж був представлений як доповнення до стандарту IEEE 802.3 за назвою "802.3z 1998 1000BASE-X Gigabit Ethernet". Єдиною областю, у якій застосування стандартів 1000BASE SX і 1000BASE LX відбувається повільніше інших, є підключення настільних робочих станцій. У цих випадках стандарт 1000BASE-T вважається найбільш перевіреним і надійним для повсякденного використання, крім того, 10/100/1000 Мбіт/с інтерфейси під мідний дріт однакові.

У стандарті 1000BASE-X використовується 8B/10B кодування, перетворене в NRZ кодування сигналу в лінії. Для цього як джерело використовується або недорогий короткохвильовий лазер з довжиною хвилі 850 нм (або в деяких випадках світловий діод) і багатомодовий оптичний кабель (1000BASE SX, де літера S означає короткохвильовий або короткий) або довгохвильовий лазер 1310 нм і одномодовий оптичний кабель (1000BASE LX, де літера L означає довгохвильовий або довгий).

У табл. 28 показаний винятково простий інтерфейс взаємного підключення Gigabit Ethernet для оптичного кабелю. У більшості випадків використовуються оптичні з'єднувачі SC типу.

Таблиця 28

Інтерфейс взаємного підключення для Gigabit Ethernet

Оптичне волокно	Сигнал
1	Tx (лазерний передавач)
2	Rx (високошвидкісний фотодіодний детектор)

У застосовуваному для оптичних з'єднань MAC методі використовуються з'єднання типу "крапка-крапка". Таким чином, оптичні з'єднання завдяки використанню окремих кабелів для передачі й приймання по своїй суті є дуплексними. У технології Gigabit Ethernet дозволене використання одного повторювача між двома станціями.

Принципи побудови мереж Gigabit Ethernet

Будь-який Ethernet пристрій, здатний працювати на різних швидкостях передачі, наприклад, 100 Мбіт/с і 1000 Мбіт/с, є мостом другого рівня моделі OSI. Пристрій не може працювати з різними швидкостями й при цьому залишатися повторювачем.

Дуплексні з'єднання можуть бути значно довшими, оскільки їх довжина обмежена тільки властивостями передавального середовища, а не затримками передачі й підтвердження. В основі принципу побудови середовища Gigabit Ethernet використовуються дуплексні з'єднання типу "станція-станція", "станція-комутатор", "комутатор-комутатор" і "комутатор-маршрутизатор". Стандарт 1000BASE SX призначений для використання із багатомодовим оптичним кабелем. Стандарт 1000BASE LX використовує як багатомодові, так і одномодові оптичні кабелі.

У табл. 29 і 30 перераховані максимальні відстані при використанні стандартів 1000BASE-SX і 1000BASE-LX. Практична межа відстані між пристроями визначається характером комутованої мережі Gigabit Ethernet. Припустимі топологічні схеми побудови мережі у вигляді послідовного ланцюга, зірки й розширеної зірки. У цьому випадку питання тільки у виборі логічної топології й маршруту потоку даних, а не обмеження за часом або відстанню.

Таблиця 29

Максимально припустима довжина кабелів для стандарту 1000BASE-SX

Середовище (багатомодовий оптичний кабель, мкм)	Модальна пропускна здатність	Максимальна відстань
1	**2**	**3**
62,5	160	220

1	2	3
62,5	200	275
50	400	500
50	500	550

Таблиця 30

Максимально припустима довжина кабелів для стандарту 1000BASE-LX

Середовище (мкм)	Модальна пропускна здатність	Максимальна відстань
62,5, багатомодовий кабель	500	550
50, багатомодовий кабель	400	550
50, багатомодовий кабель	500	550
10, одномодовий кабель		5000

UTP кабель для стандарту 1000BASE-T практично не відрізняється від того, що використовується в стандартах 10BASE-T і 100BASE-TX, за винятком того, що продуктивність з'єднання повинна відповідати вищій категорії 5e або ISO класу D (2000).

Так само, як у випадку з 10 і 100 Мбіт/с версіями мережі Ethernet, припустимі незначні зміни правил побудови мережі. Однак для напівдуплексного режиму передачі додаткові затримки не припустимі. Зміна правил побудови мережі стандарту 1000BASE-T досить небажана. На відстані 100 м устаткування стандарту 1000BASE-T працює на межі фізичних можливостей із розпізнавання сигналу. При наявності проблем з кабелем або зовнішніх перешкод використання прийнятного в нормальних умовах кабелю стає неможливим навіть на припустимих для технології відстанях. Будь-які зміни в правилах побудови мережі необхідно робити відповідно до специфікацій на часові характеристики, описані в стандарті 802.3, і технічною інформацією про продуктивність використовуваного встаткування.

Дуплексні з'єднання можуть бути довшими, ніж це зазначено в табл. 31, оскільки їх довжина обмежена тільки здатністю середовища пропущення доставити сигнал, який може бути декодований. Вони не мають обмежень, пов'язаних із часом доставки й підтвердження. Дуже складно зустріти з'єднання Gigabit Ethernet, які працюють у напівдуплексному режимі. Примусова робота в напівдуплексному режимі для мережі, що використовує дуплексну сигнальну схему, нерозумна з погляду використання ресурсів. Робота в

напівдуплексному режимі накладає додаткові обмеження на ефективну довжину кабелю, крім того, суттєво зростають накладні витрати, пов'язані з розширенням несучого сигналу. Повторювачі в середовищі Gigabit Ethernet використовуються, як правило, рідко. Це означає, що в більшості випадків з'єднання здійснюються між станцією й мостом другого рівня OSI або між двома мостами, обмежуючи в такий спосіб колізійний домен.

Рекомендується, щоб усі з'єднання між станціями й комутатором були настроєні на автовизначення, що дозволить досягти максимально високої загальної продуктивності без ризику неправильної конфігурації й допоможе уникнути випадкових помилок при конфігуруванні інших необхідних для правильної роботи середовища Gigabit Ethernet параметрів.

У табл. 31 перераховані параметри напівдуплексного режиму передачі.

Таблиця 31

Довжина кабелів для різних конфігурацій у напівдуплексному режимі передачі

Схема підключення	1000BASE-T (м)	1000BASE-SX/LX (м)	1000BASE-SX/LX і 1000BASE-T (м)
Станція-станція	100	316	–
Один повторювач	200	220	100, 1000BASE-T 110, 1000BASE-SX/LX

3.2.3. Технологія Token Ring

Мережі Token Ring так само, як і мережі Ethernet, характеризує поділюване середовище передачі даних, що в такому разі складається з відрізків кабелю, які 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 в певному порядку. Це право передається за допомогою кадру спеціального формату, називаного *маркером* або *токеном (token)*.

Технологія Token Ring була розроблена компанією IBM у 1984 році, а потім передана як проект стандарту в комітет IEEE 802, що на її основі прийняв у 1985 році стандарт 802.5.

Мережі Token Ring працюють із двома бітовими швидкостями – 4 і 16 Мбіт/с. Поєднання станцій, що працюють на різних швидкостях, в одному кільці не допускається. Мережі Token Ring, що

працюють зі швидкістю 16 Мбіт/с, мають деякі вдосконалення в алгоритмі доступу в порівнянні зі стандартом 4 Мбіт/с.

Технологія Token Ring є більш складною, ніж Ethernet. Вона має властивості відмовостійкості. У мережі Token Ring визначені процедури контролю роботи мережі, які використовують зворотний зв'язок кільцеподібної структури – посланий кадр завжди вертається 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 званого *активного монітора,* який обирається під час ініціалізації кільця як станція з максимальним значенням MAC-адреси. Якщо активний монітор виходить із ладу, процедура ініціалізації кільця повторюється й обирається новий активний монітор. Щоб мережа могла виявити відмову активного монітора, останній у працездатному стані кожні 3 секунди генерує спеціальний кадр своєї присутності. Якщо цей кадр не з'являється в мережі більше 7 секунд, то інші станції мережі починають процедуру виборів нового активного монітора.

Маркерний метод доступу до поділюваного середовища

У мережах з *маркерним методом доступу* (а до них, крім мереж Token Ring, належать мережі FDDI) право на доступ до середовища передається циклічно від станції до станції по логічному кільцю.

У мережі Token Ring кільце створюється відрізками кабелю, що з'єднують сусідні станції. Таким чином, кожна станція зв'язана зі своєю попередньою й наступною і може безпосередньо обмінюватися даними тільки з ними. Для забезпечення доступу станцій до фізичного середовища по кільцю циркулює кадр спеціального формату й 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 й за відсутності в ній даних для передачі забезпечує його просування до наступної станції. Станція, що має дані для передачі, при одержанні маркера вилучає його з кільця, що дає їй право доступу до фізичного середовища й

передачі своїх даних. Потім ця станція видає в кільце кадр даних установленого формату послідовно по бітах. Передані дані проходять по кільцю завжди в одному напрямку від однієї станції до іншої. Кадр має 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 нього ознаку підтвердження прийому. Станція, що видала кадр даних у кільце, при зворотному його одержанні з підтвердженням прийому вилучає цей кадр із кільця й 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, описаних у стандарті 802.5.

На рис. 41 описаний алгоритм доступу до середовища, який ілюструється часовою діаграмою.

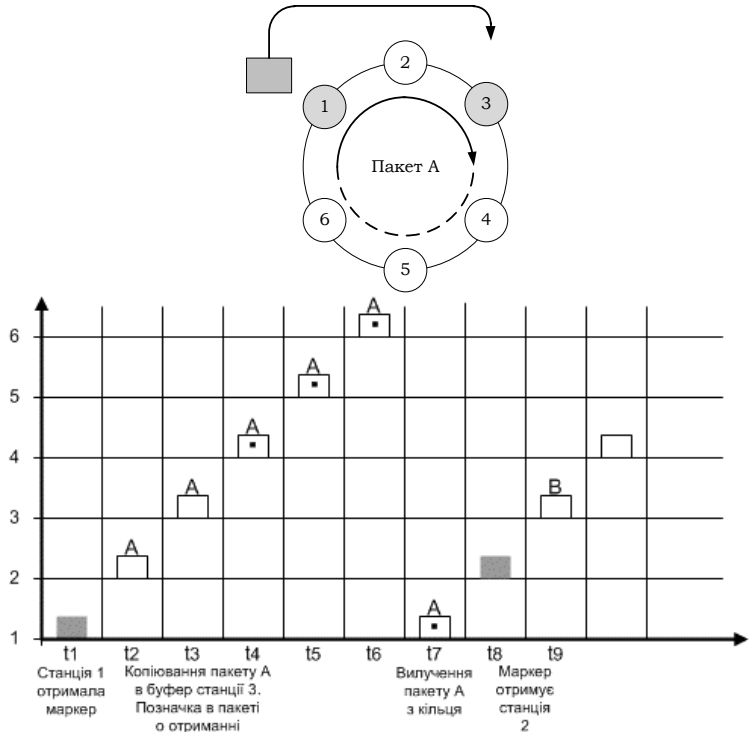


Рис. 41. Принцип маркерного доступу

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 – розпізнавання адреси й копіювання пакета в буфер (що на малюнку позначено зірочкою всередині пакета). Після повернення пакета в станцію 1 відправник розпізнає свій пакет за адресою джерела й видаляє його з кільця. Установлені станцією 3 ознаки говорять станції-відправникові про те, що пакет дійшов до адресата й був успішно скопійований ним у свій буфер.

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 або кілька кадрів залежно від розміру кадрів і величини часу втримання маркера. Звичайний час утримання маркера за замовчуванням дорівнює 10 мс.

У мережах Token Ring 16 Мбіт/с використовується трохи інший алгоритм доступу до кільця, називаний *алгоритмом раннього звільнення маркера (Early Token Release)*. Відповідно до нього станція передає маркер доступу наступної станції відразу 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 кожний момент часу може генерувати тільки одна станція – та, котра в цей 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 разі, якщо пріоритет кадру, що вона хоче передати, вище (або

дорівнює) пріоритету маркера. Інакше станція зобов'язана передати маркер наступній 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), він породжує новий маркер.

Фізичний рівень технології Token Ring

Стандарт Token Ring фірми IBM передбачав побудову зв'язків у мережі за допомогою концентраторів MAU (Multistation Access Unit) або MSAU (Multi-Station Access Unit), тобто пристроями багатостанційного доступу (рис. 42). Мережа Token Ring може включати до 260 вузлів.

Концентратор Token Ring може бути активним або пасивним. Пасивний концентратор просто з'єднує порти внутрішніми зв'язками так, щоб станції, що підключають до цих портів, утворили кільце. Такий пристрій можна вважати простим кросовим блоком за одним виключенням – MSAU забезпечує обхід якого-небудь порту, коли приєднаний до цього порту комп'ютер вимкнуть. Така функція необхідна для забезпечення зв'язності кільця поза залежністю від стану підключених комп'ютерів.

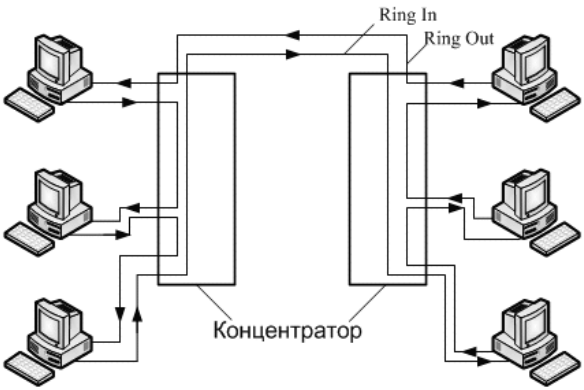


Рис. 42. Фізична конфігурація мережі Token Ring

Активний концентратор виконує функції регенерації сигналів, і тому іноді називається повторювачем, як у стандарті Ethernet.

Виникає питання: якщо концентратор є пасивним пристроєм, то забезпечується якісна передача сигналів на великі відстані, які

виникають при ввімкненні в мережу кількох сотень комп'ютерів? Відповідь полягає в тому, що роль підсилювача сигналів у цьому випадку бере на себе кожний мережний адаптер, а роль ресинхронувального блоку виконує мережний адаптер активного монітора кільця. Кожний мережний адаптер Token Ring має блок повторення, що вміє регенерувати й ресинхронізувати сигнали, однак останню функцію виконує в кільці тільки блок повторення активного монітора.

Максимальна довжина кільця Token Ring становить 4000 м. Обмеження на максимальну довжину кільця й кількість станцій у кільці в технології Token Ring не є такими чіткими, як у технології Ethernet. Тут ці обмеження багато в чому зв'язані з часом оберту маркера по кільцю (але не тільки – є й інші міркування, що диктують вибір обмежень). Так, якщо кільце складається з 260 станцій, то при часі утримання маркера в 10 мс маркер повернеться в активний монітор у найгіршому разі через 2,6 с, а цей час саме становить тайм-аут контролю оберту маркера.

Існує велика кількість апаратур для мереж Token Ring, що поліпшує деякі стандартні характеристики цих мереж: максимальну довжину мережі, відстань між концентраторами, надійність (шляхом використання подвійних кілець).

3.2.4. Технологія FDDI

Технологія FDDI (Fiber Distributed Data Interface) – оптичний інтерфейс розподілених даних – це перша технологія локальних мереж, у якій середовищем передачі даних є оптичний кабель.

Технологія FDDI багато в чому ґрунтується на технології Token Ring, розвиваючи й удосконалюючи її основні ідеї.

Мережа FDDI будується на основі двох оптичних кілець, які утворюють основний і резервний шляхи передачі даних між вузлами мережі. Наявність двох кілець – це основний спосіб підвищення відмовостійкості в мережі FDDI, і вузли, які хочуть скористатися цим підвищеним потенціалом надійності, повинні бути підключені до обох кілець.

У нормальному режимі роботи мережі дані проходять через всі вузли й всі ділянки кабелю тільки первинного (Primary) кільця, цей режим названий режимом Thru – "наскрізним" або "транзитним". Вторинне кільце (Secondary) у цьому режимі не використовується.

У разі будь-якої відмови, коли частина первинного кільця не може передавати дані (наприклад, обрив кабелю або відмова вузла), первинне кільце поєднується із вторинним (рис. 43), знову утворюючи єдине кільце. Цей режим роботи мережі називається *Wrap*, тобто "*згортання*" кілець. Операція згортання проводиться засобами концентраторів і/або мережних адаптерів FDDI. Для спрощення цієї процедури дані по первинному кільцю завжди передаються в одному напрямку (на діаграмах цей напрямок зображується проти годинникової стрілки), а по вторинному – у зворотному (зображується по годинниковій стрілці). Тому при утворенні загального кільця із двох кілець передачі станцій, як і раніше, залишаються підключеними до приймачів сусідніх станцій, що дозволяє правильно передавати й приймати інформацію сусідніми станціями.

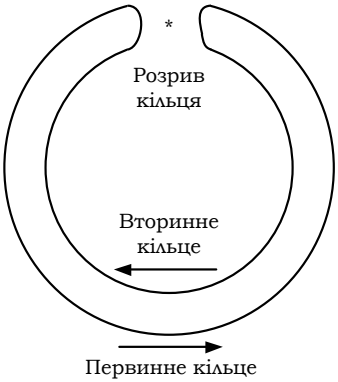


Рис. 43. Конфігурування кілець FDDI при відмові

Технологія FDDI доповнює механізми виявлення відмов технології Token Ring механізмами реконфігурування шляхів передачі даних у мережі, заснованими на наявності резервних зв'язків, забезпечуваних другим кільцем.

Кільця в мережах FDDI розглядаються як загальне поділюване середовище передачі даних, тому для неї визначений спеціальний метод доступу. Цей метод дуже близький до методу доступу мереж Token Ring і також називається методом маркерного (або токенного) кільця – token ring.

Відмінності методу доступу полягають у тому, що час утримання маркера в мережі FDDI не є постійною величиною, як у

мережі Token Ring. Він залежить від завантаження кільця – при невеликому завантаженні воно збільшується, а при великих перевантаженнях може зменшуватися до нуля. Ці зміни в методі доступу стосуються тільки асинхронного трафіку, що не критичний до невеликих затримок передачі кадрів. Для синхронного трафіку час утримання маркера, як і раніше, залишається фіксованою величиною. Механізм пріоритетів кадрів, аналогічний прийнятому в технології Token Ring, у технології FDDI відсутній. Розроблювачі технології вирішили, що досить розділити трафік на два класи – асинхронний і синхронний, останній з яких обслуговується завжди, навіть при перевантаженнях кільця.

В іншому пересилання кадрів між станціями кільця на рівні MAC повністю відповідає технології Token Ring. Станції FDDI застосовують алгоритм раннього звільнення маркера, як і мережі Token Ring зі швидкістю 16 Мбіт/с.

Адреси рівня MAC мають стандартний для технологій IEEE 802 формат. Формат кадру FDDI близький до формату кадру Token Ring, основні відмінності полягають у відсутності полів пріоритетів. Ознаки розпізнавання адреси, копіювання кадру й помилки дозволяють зберегти наявні в мережах Token Ring процедури обробки кадрів станцією-відправником, проміжними станціями й станцією-одержувачем.

На рис. 44 наведена відповідність структури протоколів технології FDDI семирівневій моделі OSI. FDDI визначає протокол фізичного рівня й протокол підрівня доступу до середовища (MAC) канального рівня.

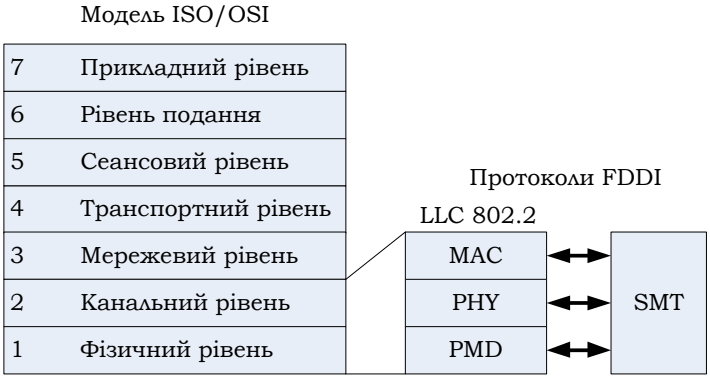


Рис. 44. Структура протоколів технології FDDI

Як і в багатьох інших технологіях локальних мереж, у технології FDDI використовується протокол підрівня керування каналом даних LLC, визначений у стандарті IEEE 802.2. Таким чином, незважаючи на те, що технологія FDDI була розроблена й стандартизована інститутом ANSI, а не комітетом IEEE, вона повністю вписується в структуру стандартів 802.

Відмінною рисою технології FDDI є *рівень керування станцією – Station Management (SMT)*. Саме рівень SMT виконує всі функції щодо керування й моніторингу всіх інших рівнів стека протоколів FDDI. У керуванні кільцем бере участь кожний вузел мережі FDDI. Тому всі вузли обмінюються спеціальними кадрами SMT для керування мережею.

Відмовостійкість мереж FDDI забезпечується протоколами й іншими рівнями: за допомогою фізичного рівня усуваються відмови мережі з фізичних причин, наприклад, через обрив кабелю, а за допомогою рівня MAC – логічні відмови мережі, наприклад, втрата потрібного внутрішнього шляху передачі маркера й кадрів даних між портами концентратора.

Особливості методу доступу FDDI. Для передачі синхронних кадрів станція завжди має право захопити маркер при його надходженні. При цьому час утримання маркера має заздалегідь задану фіксовану величину.

Якщо ж станції кільця FDDI потрібно передати асинхронний кадр (тип кадру визначається протоколами верхніх рівнів), то для з'ясування можливості захоплення маркера при його черговому надходженні станція повинна виміряти інтервал часу, що пройшов з моменту попереднього приходу маркера. Цей інтервал називається часом оберту маркера (Token Rotation Time, TRT). Інтервал TRT порівнюється з іншою величиною – максимально припустимим часом оберту маркера по кільцю T_0pr. Якщо в технології Token Ring максимально припустимий час оберту маркера є фіксованою величиною (2,6 із розрахунку 260 станцій у кільці), то в технології FDDI станції домовляються про величину T_0pr під час ініціалізації кільця. Кожна станція може запропонувати своє значення T_0pr, у результаті для кільця встановлюється мінімальний із запропонованих станціями часів. Це дозволяє враховувати потреби додатків, що працюють на станціях. Зазвичай синхронним додаткам (додаткам реального часу) потрібно частіше передавати дані в

мережу невеликими порціями, а асинхронним додаткам краще одержувати доступ до мережі рідше, але більшими порціями. Перевага віддається станціям, що передають синхронний трафік.

Відмовостійкість технології FDDI. Для забезпечення відмовостійкості в стандарті FDDI передбачене створення двох оптичних кілець – первинного й вторинного. У стандарті FDDI допускаються два види приєднання станцій до мережі. Одночасне підключення до первинного й вторинного кілець називається подвійним підключенням – Dual Attachment, DA. Підключення тільки до первинного кільця називається одиночним підключенням – Single Attachment, SA.

У стандарті FDDI передбачена наявність у мережі кінцевих вузлів-станцій (Station), а також концентраторів (Concentrator). Для станцій і концентраторів допустимий будь-який вид підключення до мережі – як одиночний, так і подвійний. Такі пристрої мають відповідні назви: SAS (Single Attachment Station), DAS (Dual Attachment Station), SAC (Single Attachment Concentrator) і DAC (Dual Attachment Concentrator).

Зазвичай концентратори мають подвійне підключення, а станції – одинарне. Щоб пристрої легше було правильно приєднувати до мережі, їхні з'єднувачі маркуються.

Порівняння FDDI з технологіями Ethernet і Token Ring. У табл. 32 представлені результати порівняння технології FDDI з технологіями Ethernet і Token Ring.

Технологія FDDI розроблялася для застосування у відповідальних ділянках мереж – на магістральних з'єднаннях між великими мережами, наприклад мережами будинків, а також для підключення до мережі високопродуктивних серверів. Тому головним для розробників було забезпечити високу швидкість передачі даних відмовостійкості на рівні протоколу й великі відстані між вузлами мережі. Усі цілі були досягнуті. У результаті технологія FDDI вийшла якісною, але досить дорогою. Навіть поява більш дешевого варіанта для крученої пари не набагато знизило вартість підключення одного вузла до мережі FDDI. Тому практика показала, що основною галуззю застосування технології FDDI стали магістралі мереж, що складаються з декількох будинків, а також мережі масштабу великого міста, тобто класу MAN. Для підключення клієнтських комп'ютерів і навіть невеликих серверів технологія

виявилася занадто дорогою. А оскільки обладнання FDDI випускається вже близько 10 років, значного зниження його вартості очікувати не доводиться.

У табл. 32 представлене зіставлення технології FDDI з технологіями Ethernet, Token Ring

Таблиця 32

Характеристики технологій FDD, Ethernet, Token Ring

Характеристика	**FDDI**	**Ethernet**	**Token Ring**
Бітова швидкість	100 Мбіт/с	10 Мбіт/с	16 Мбіт/с
Топологія	Подвійне кільце дерев	Шина/зірка	Зірка/кільце
Метод доступу	Частка від часу оберту маркера	CSDMA/CD	Пріоритетна система резервування
Середовище передачі даних	Оптичний кабель, неекранована кручена пара категорії 5	Товстий коаксіальний кабель, тонкий коаксіальний кабель, кручена пара категорії 3, оптичний кабель	Екранована і неекранована кручена пара, оптичний кабель
Максимальна довжина мережі (без мостів)	200 км (100км на кільце)	2500м	4000м
Максимальна відстань між вузлами	2 км	2500м	100м
Максимальна кількість вузлів	500	1024	260 для екранованої крученої пари, 72 для неекранованої крученої пари

Лабораторна робота №6 (2 год.)
Тема: Побудова локальної мережі на основі стандартів 802.3

Мета: сформувати вміння проектувати ЛВС відповідно до розмірів сегментів мережі та потреб підприємства згідно зі стандартами Ethernet і Fast Ethernet;

виховувати ціннісне ставлення студентів до навчальної діяльності.

Студент повинен знати: характеристики локальних мереж стандарту 802.3 та їх обмеження.

Студент повинен уміти: проектувати локальну мережу відповідно до вимог стандарту 802.3.

Хід роботи

Інструктаж

1. Розглянути характеристики локальних мереж стандарту 802.3 та їх обмеження.
2. Визначити умови використання повторювачів та концентраторів у локальних мережах стандарту 802.3.

Практична робота

Для наведеного нижче плану робочого приміщення (рис. 45) розробити структуру локальної мережі з використанням одного зі стандартів (*для проектування мережі в одному приміщенні необхідно використовувати тільки один із стандартів*). Накреслити схему розташування мережевого обладнання та прокладання кабелів і обгрунтувати вибір запропонованих проектних рішень.

Самостійна робота №6

Тема: Додавання мережевих адрес при проектуванні адресного простору в ієрархічній мережі

Мета: розвивати у студентів уміння аналізувати та визначати можливість додавання мережевих адрес у реалізації ієрархічної комп'ютерної мережі.

Студент повинен знати: функції та призначення додавання мережевих адрес.

Студент повинен уміти: здійснювати додавання мережевих адрес при проектуванні адресного простору ієрархічної комп'ютерної мережі.

Хід роботи

Теоретична частина

1. Що значить фраза "Додавання дозволяє сховати докладну інформацію про топологію"?
2. Яким чином приховування докладної інформації про топологію дозволяє поліпшити стабільність функціонування мережі?
3. На яких ділянках мережі варто проводити додавання?

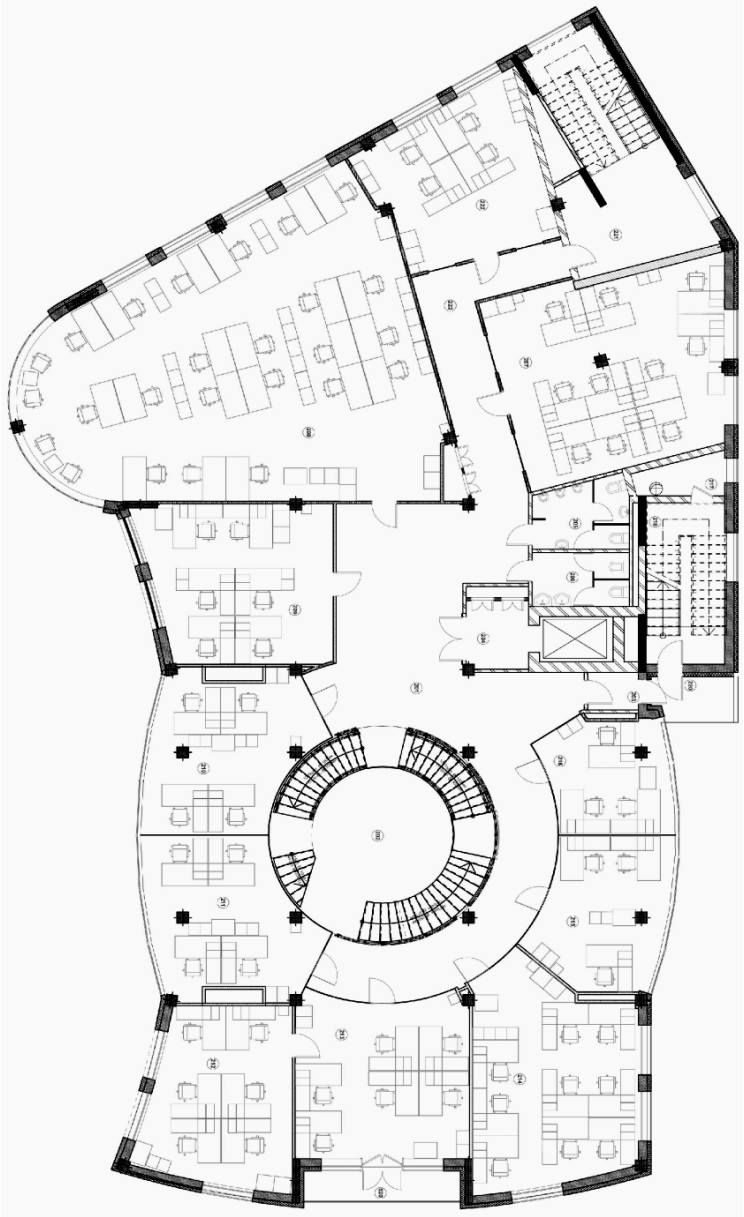


Рис. 45. План приміщення з розташуванням робочих місць

Практична робота

Визначите найбільшу довжину сумарного префікса для приведених нижче адрес.

– набір A: 172.16.1.1/30, 172.16.1.5/30, 172.16.1.9/30, 172.16.1.14/30;

– набір B: 10.100.40.14/24, 10.100.34.56/24, 10.100.59.81/24;

– набір C: 172.18.10.10/23, 17131.40.8/24, 172.24.8.1/22, 172.30.200.1/24;

– набір D: 192.168.8.10/27, 192.168.60.14/27, 192.168.74.90/27, 192.168.101.48/27.

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Сучасні тенденції розвитку високошвидкісних локальних мереж".

МОДУЛЬНА КОНТРОЛЬНА РОБОТА №3

Оберіть номер правильної відповіді:

1. Яке максимальне число послідовних колізій може виникнути в мережі Ethernet?

а) 2;

б) 8;

в) 16.

1 б.

2. Яку довжину має MAC-адреса?

а) 32 біта;

б) 48 біт;
в) 32 байта.

1 б.

3. Чому дорівнює мінімальна довжина кадру Ethernet?
а) 1024 байта;
б) 64 байта;
в) 1500 байт;
г) 46 байт.

1 б.

4. Чому дорівнює максимальна довжина кадру Ethernet?
а) 1500 байт;
б) 1024 байта;
в) 1024 біта;
г) 1.5 кб.

1 б.

5. Який комітет займається розвитком специфікацій CSMA/CD?
а) IEEE 802.5;
б) IEEE 802.1;
в) IEEE 802.3;
г) IEEE 802.2.

1 б.

6. Яка специфікація відповідає Ethernet за версією DIX?
а) 10Base2;
б) 10Base5;
в) 10Base.

1 б.

7. Чому дорівнює розмір максимального сегмента в мережі Ethernet за версією DIX?
а) 100 метрів;
б) 500 метрів;
в) 1024 метра;
г) 185 метрів.

1 б.

8. Чому дорівнює мінімальний розмір поля даних мережі Ethernet?
а) 1500 байт;
б) 64 байта;
в) 46 байт.

1 б.

9. Який тип середовища передачі даних використовується в технології 10BaseT?

а) товстий коаксіальний кабель;

б) оптичний кабель;

в) тонкий коаксіальний кабель;

г) кручена пара.

1 б.

10. Чому дорівнює розмір максимального сегмента в мережі 10BaseT?

а) 100 метрів;

б) 500 метрів;

в) 185 метрів;

г) 200 метрів.

1 б.

Всього: 10 балів.

Правильні відповіді

Питання	1	2	3	4	5	6	7	8	9	10
Відповідь	в	б	б	а	в	б	б	б	г	а

ЗМІСТОВИЙ МОДУЛЬ 4

КОМУТОВАНІ МЕРЕЖІ ETHERNET.

ІНТЕЛЕКТУАЛЬНІ ФУНКЦІЇ КОМУТАТОРІВ

Таблиця 33

Тематичний план змістового модуля

№ теми	Назва змістового модуля, теми	Усього годин	Лекції	Лабораторні заняття	Самостійна та індивідуальна робота
4.1	Комутовані мережі Ethernet	9	2	2	5
4.2	Інтелектуальні функції комутаторів	9	2	2	5
	Разом	***18***	***4***	***4***	***10***

Навчальні цілі: сприяти засвоєнню студентами знань щодо принципів функціонування мостів, комутаторів та маршрутизаторів; розвивати вміння аналізувати та налагоджувати комутатори.

Основні поняття: міст, комутатор, архітектура комутатора, обмеження комутаторів.

Методичні рекомендації щодо роботи з модулем: робота з модулем передбачає засвоєння лекційного матеріалу, участь у лабораторних заняттях, написання реферату (окремими студентами), самостійну роботу над визначеними питаннями теми, модульний контроль у формі тестування.

Після опрацювання цих тем студент може отримати бали, наведені в табл. 34.

Таблиця 34

Оцінювання навчальних досягнень студентів

Поточний контроль				
Робота на лабораторному занятті	Самостійна робота	Індивідуальне завдання	Контрольна рейтингова оцінка	Підсумкова рейтингова оцінка

Тема №4.1	**Тема №4.2**	**Тема №4.1**	**Тема №4.2**			
5	5	2	3	5	10	30

ТЕМА 4.1. КОМУТОВАНІ МЕРЕЖІ ETHERNET

Лекція

План

1. Пристрої об'єднання мереж
2. Фізична структуризація локальної мережі. Повторювачі й концентратори

Література

Основна

1. *Бройдо В. Л.* Вычислительные системы, сети и телекоммуникации: учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Прикладная информатика" и "Информационные системы в экономике" / В. Л. Бройдо, О. П. Ильина. – 3-е изд. – Москва [и др.]: Питер, 2008. – 765 с.: ил., табл.; 24 см.

2. *Гук М.* Аппаратные средства локальных сетей. Энциклопедия : [Наиболее полн. и подроб. рук.] / Михаил Гук. – СПб. : Питер, 2000.– 572 с.

3. *Новиков Ю. В.* Локальные сети: Архитектура, алгоритмы, проектирование / Новиков Ю. В., Кондратенко С. В. – М.: ЭКОМ, 2002. – 311 с.: ил.; 23 см. – (Современные компьютерные технологии).

4. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

Додаткова

1. *Бабій М. С.* Локальні мережі ЕОМ: [навч. посіб. для студ. спец. "Прикладна математика"] / Михайло Семенович Бабій. – Суми : Видавництво СумДУ, 2003. – 64 с.

2. *Бортник Г. Г.* Мережі доступу: навч. посібник для студ. напряму підготовки 0924 – "Телекомунікації" всіх спец. / Бортник Г. Г., Стальченко О. В., Яблонський В. Ф. – Вінниця : ВНТУ, 2006. – 139 с.

3. *Зайченко Ю. П.* Комп'ютерні мережі: навч. посіб. для студ. вищ. навч. закл. [Intertational Science and Technology University] / Ю. П. Зайченко. – К. : Слово, 2003. – 284 с. – (До 10-річчя Міжнародного науково-технічного ун-ту).

4. *Ибе О.* Сети и удаленный доступ: Протоколы, проблемы, решения / Оливер Ибе. – М.: ДМК Пресс, 2002. – 332 с.: ил.; 23 см. – (Серия "Защита и администрирование").

5. *Кулаков Ю. А.* Локальные сети / Ю. А. Кулаков, Г. М. Луцкий. – К. : Юниор, 1998. – 336 с.

6. *Олексюк В. П.* Організація комп'ютерної локальної мережі : [посіб.] / Олексюк В. П., Балик Н. Р., Балик А. В. – Тернопіль. : Підручники і посібники, 2006. – 80 с.

4.1.1. Пристрої об'єднання мереж

Пристрої об'єднання мереж забезпечують зв'язок між сегментами локальних мереж, окремими ЛОМ і підмережами будь-якого рівня. Ці пристрої можуть бути віднесені до певних рівнів еталонної моделі взаємодії відкритих систем.

Існують такі класи пристроїв для об'єднання сегментів і мереж.

Повторювач, що регенерує сигнали, за рахунок чого дозволяє збільшувати довжину мережі, працює на фізичному рівні.

Мережевий адаптер також працює на фізичному й частково на канальному рівнях. До фізичного рівня відноситься та частина функцій мережевого адаптера, яка пов'язана із прийомом і передачею сигналів по лінії зв'язку, а одержання доступу до поділюваного середовища передачі, розпізнавання MAC-адреси комп'ютера – це вже функція канального рівня.

Мости (bridges) і *комутатори (switches)* поєднують мережі на канальному рівні й використовують функціональні можливості фізичного рівня. Мости виконуються на основі комп'ютера, оснащеного відповідним ПО. Відмінність комутаторів від мостів у тому, що вони реалізують свої функції апаратними засобами й тому володіють більш високою швидкодією.

Для мостів мережа представляється набором MAC-адрес пристроїв. Вони виймають ці адреси із заголовків, доданих до пакетів

на канальному рівні, і використовують їх під час обробки пакетів для ухвалення рішення про те, на який порт відправити той або інший пакет. Мости не мають доступу до інформації про адреси мереж, що відноситься до більш високого рівня. Тому вони обмежені в прийнятті рішень про можливі шляхи або маршрути переміщення пакетів по мережі.

Маршрутизатори працюють на мережевому рівні моделі OSI. Для маршрутизаторів мережа – це набір мережевих адрес пристроїв і множини мережевих шляхів. Маршрутизатори аналізують усі можливі шляхи між будь-якими двома вузлами мережі й вибирають найкоротший із них.

Шлюз (gateway) – це пристрій, що виконує трансляцію протоколів, він може працювати на будь-якому рівні моделі OSI Шлюз розміщається між мережами, що взаємодіють; служить посередником, який переводить повідомлення, котрі надходять із однієї мережі, у формат іншої мережі. Шлюз може бути реалізований як чисто програмними засобами, установленими на звичайному комп'ютері, так і на базі спеціалізованого комп'ютера.

Фрагмент обчислювальної мережі (рис. 46) включає основні типи комунікаційного обладнання для утворення локальних мереж і з'єднання їх через глобальні зв'язки одна з одною.

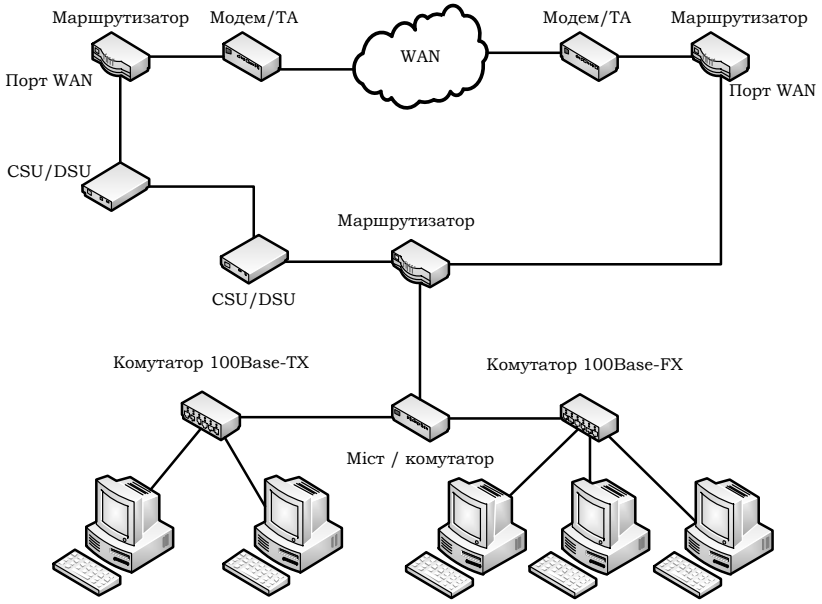


Рис. 46. Фрагмент складної мережі

Для підключення локальних мереж до глобальних зв'язків використовують спеціальні виходи (WAN-порти) мостів і маршрутизаторів, а також апаратури передачі даних по довгих лініях – модеми (при роботі з аналоговим лініям) або ж пристрої підключення до цифрових каналів (ТА – термінальні адаптери мереж ISDN, пристрої обслуговування цифрових виділених каналів типу CSU/DSU і т.п.).

4.1.2. Фізична структуризація локальної мережі. Повторювачі й концентратори

Для побудови найпростішої односегментної мережі досить мати мережеві адаптери й кабель відповідного типу. Але навіть у цьому випадку часто використовуються додаткові пристрої – повторювачі сигналів, що дозволяють перебороти обмеження на максимальну довжину кабельного сегмента.

Основна функція *повторювача (repeater)* – це повторення сигналів, що надходять на один з його портів, на всі інші порти (Ethernet) або на наступний у логічному кільці порт (Token Ring,

FDDI) синхронно із сигналами-оригіналами. Повторювач поліпшує електричні характеристики сигналів і їх синхронність, і за рахунок цього з'являється можливість збільшувати загальну довжину кабелю між найвіддаленішими станціями в мережі.

Повторювач з декількома портами часто називають *концентратором (hub, concentrator)*, оскільки він реалізує не тільки функцію повторення сигналів, але й концентрує в одному центральному пристрої функції об'єднання комп'ютерів у мережу. Майже в усіх сучасних мережних стандартах концентратор є необхідним елементом мережі, що з'єднує окремі комп'ютери в мережу.

Відрізки кабелю, що з'єднують два комп'ютери або два інших мережевих пристрої, називаються фізичними сегментам. Таким чином, концентратори й повторювачі, які використовуються для додавання нових фізичних сегментів, є засобом фізичної структуризації мережі.

Основним завданням повторювача є відновлення електричних сигналів для передачі їх в інші сегменти. За рахунок посилення й відновлення форми електричних сигналів повторювачем стає можливим розширення мереж, побудованих на основі коаксіального кабелю й збільшення загального числа користувачів мережі.

Концентратори утворять із окремих фізичних відрізків кабелю загальне середовище передачі даних – логічний сегмент. Його ще називають доменом колізій, оскільки при спробі одночасної передачі даних будь-яких двох комп'ютерів цього сегмента, хоча б і приналежним різним фізичним сегментам, виникає блокування передавального середовища. Поява пристроїв, що централізують з'єднання між окремими мережними пристроями, потенційно дозволяє поліпшити керованість мережі та її експлуатаційні характеристики (кодифікованість, ремонтопридатність і т.п.). Із цією метою розроблювачі концентраторів часто вбудовують у свої пристрої, крім основної функції повторювача, допоміжні, досить корисні для поліпшення якості мережі, зокрема:

– об'єднання сегментів з різними фізичними середовищами (наприклад, кручена пара й оптичний кабель) у єдиний логічний сегмент;

– автосегментація портів – автоматичне відключення порту при його некоректній поведінці (ушкодження кабелю, інтенсивна генерація пакетів помилкової довжини й т.п.);

– підтримка між концентраторами резервних зв'язків, які

використовуються при відмові основних;

– захист переданих по мережі даних від несанкціонованого доступу (наприклад, шляхом перекручування поля даних у кадрах, повторюваних на портах, що не містять комп'ютера з адресою призначення).

Деякі концентратори дозволяють програмним шляхом розділяти порти пристрою на незалежні сегменти – така можливість називається перемиканням портів. Концентратор, приміром, може містити три різних сегменти Ethernet.

Перемикання портів забезпечує адміністратору мережі високу гнучкість організації сегментів, дозволяючи переносити порти з одного сегмента в інший програмними засобами. Ця можливість особливо корисна для розподілу навантаження між сегментами Ethernet і зниження витрат.

Лабораторна робота №7 (2 год.)

Тема: Концепції проектування комп'ютерної мережі на основі концентраторів і комутаторів

Мета: навчити студентів проектувати комп'ютерну мережу на основі концентраторів і комутаторів; конфігурувати інтерфейси Ethernet;

виховувати ціннісне ставлення студентів до майбутньої професійної діяльності.

Студент повинен знати: принципи функціонування комутаторів та концентраторів, алгоритм розрахунку конфігурації мережі Ethernet.

Студент повинен уміти: конфігурувати інтерфейси Ethernet.

Обладнання: комп'ютерний клас з локальною мережею на основі стандарту Fast Ethernet.

Інструктаж

1. Створити комп'ютерну мережу на основі трьох комп'ютерів та концентратора (рис. 47).

2. Створити комп'ютерну мережу на основі трьох комп'ютерів та комутатора (рис. 47).

3. Встановити IP-адреси та маски мережі так:

- PC0 192.168.1.1 255.255.255.0
- PC1 192.168.1.2 255.255.255.0
- PC2 192.168.1.3 255.255.255.0
- PC3 192.168.2.1 255.255.255.0

- PC4 192.168.2.2 255.255.255.0
- PC5 192.168.2.3 255.255.255.0

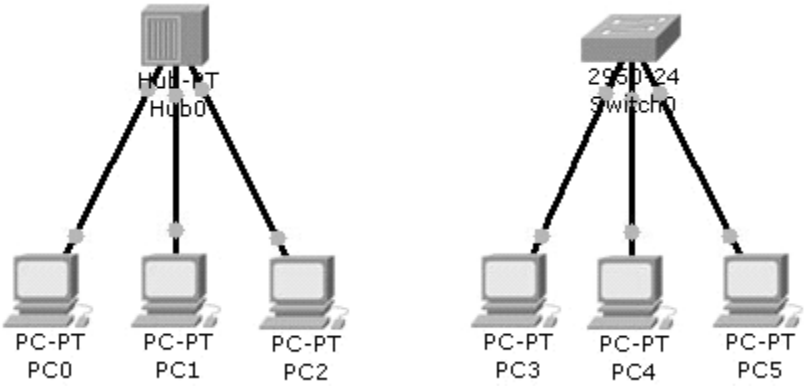


Рис. 47. Мережі на основі концентратора та комутатора

Завдання для письмового звіту та спостережень:

– запустіть команду ping з PC0 до PC1. Зверніть увагу, як концентратор опрацьовує пакети протоколів визначення адрес і ICMP. Після цього ще раз запустіть команду ping від PC1 до PC0. Як змінилася поведінка концентратора? Поясніть чому;

– запустіть команду ping з PC4 до PC3. Зверніть увагу на те, як комутатор опрацьовує пакети протоколів визначення адрес і ICMP. Після цього ще раз виконайте команду ping з PC3 до PC4. Як змінилася поведінка комутатора після другого запуску команди ping? У якому випадку комутатор опрацьовував пакети однаково з концентратором?

Самостійна робота №7

Тема: Стратегія адресації при проектуванні ієрархічної комп'ютерної мережі

Мета: розвивати аналітичні вміння студентів з визначення та вибору стратегії адресації при проектуванні ієрархічної комп'ютерної мережі.

Студент повинен знати: характеристики та особливості використання різних стратегій адресації при проектуванні ієрархічних комп'ютерних мереж.

Студент повинен уміти: вибирати та характеризувати стратегію адресації в ієрархічні комп'ютерні мережі.

Хід роботи

Теоретична частина

1. Яка зі стратегій розподілу мережних адрес є найкращою?
2. Чи існує можливість спільного використання двох різних стратегій адресації для полегшення адміністрування мережі?

Практична частина

Завдання

1. Виконайте адресацію мережі відповідно до структурного (організаційного), географічного і топологічного принципів розподілу мережевих адрес.
2. Законспектуйте основні положення щодо стратегій адресації в ієрархічних мережах.

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Порівняльний аналіз інтелектуальних комутаторів"

ТЕМА 4.1. ІНТЕЛЕКТУАЛЬНІ ФУНКЦІЇ КОМУТАТОРІВ

Лекція

План

1. Логічна структуризація мережі. Мости й комутатори.

2. Маршрутизатори.

3. Приклад підключення локальної мережі організації до Інтернет.

Література

Основна

1. *Бройдо В. Л.* Вычислительные системы, сети и телекоммуникации: учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Прикладная информатика" и "Информационные системы в экономике" / В. Л. Бройдо, О. П. Ильина. – 3-е изд. – Москва [и др.]: Питер, 2008. – 765 с.: ил., табл.; 24 см.

2. *Гук М.* Аппаратные средства локальных сетей. Энциклопедия : [Наиболее полн. и подроб. рук.] / Михаил Гук. – СПб. : Питер, 2000.– 572 с.

3. *Новиков Ю. В.* Локальные сети: Архитектура, алгоритмы, проектирование / Новиков Ю. В., Кондратенко С. В. – М.: ЭКОМ, 2002. – 311 с.: ил.; 23 см. – (Современные компьютерные технологии).

4. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

Додаткова

1. *Бабій М. С.* Локальні мережі ЕОМ: [навч. посіб. для студ. спец. "Прикладна математика"] / Михайло Семенович Бабій. – Суми : Видавництво СумДУ, 2003. – 64 с.

2. *Бортник Г. Г.* Мережі доступу: навч. посібник для студ. напряму підготовки 0924 – "Телекомунікації" всіх спец. / Бортник Г. Г., Стальченко О. В., Яблонський В. Ф. – Вінниця : ВНТУ, 2006. – 139 с.

3. *Зайченко Ю. П.* Комп'ютерні мережі: навч. посіб. для студ. вищ. навч. закл. [Intertational Science and Technology University] / Ю. П. Зайченко. – К. : Слово, 2003. – 284 с. – (До 10-річчя Міжнародного науково-технічного ун-ту).

4. *Ибе О.* Сети и удаленный доступ: Протоколы, проблемы,

решения / Оливер Ибе. – М.: ДМК Пресс, 2002. – 332 с.: ил.; 23 см. – (Серия "Защита и администрирование").

5. *Кулаков Ю. А.* Локальные сети / Ю. А. Кулаков, Г. М. Луцкий. – К. : Юниор, 1998. – 336 с.

6. *Олексюк В. П.* Організація комп'ютерної локальної мережі : [посіб.] / Олексюк В. П., Балик Н. Р., Балик А. В. – Тернопіль. : Підручники і посібники, 2006. – 80 с.

4.2.1. Логічна структуризація мережі. Мости й комутатори

Незважаючи на появу нових додаткових можливостей, основною функцією концентраторів залишається передача пакетів по загальному поділюваному середовищу. Колективне використання багатьма комп'ютерами загальної кабельної системи в режимі поділу часу приводить до істотного зниження продуктивності мережі при інтенсивному трафіку. Загальне середовище перестає справлятися з потоком переданих кадрів і в мережі виникає черга комп'ютерів, що очікують доступу.

Тому мережі, побудовані на основі концентраторів, не можуть розширюватися в необхідних межах – при певній кількості комп'ютерів у мережі або з появою нових додатків завжди відбувається насичення передавального середовища, і затримки в його роботі стають неприпустимими. Ця проблема може бути вирішена шляхом логічної структуризації мережі за допомогою мостів, комутаторів і маршрутизаторів.

Мости мають багато відмінностей від повторювачів. Повторювачі передають усі пакети, а мости – тільки ті, які потрібно. Якщо пакет не потрібно передавати в інший сегмент, він фільтрується. Для мостів існують численні алгоритми (правила) передачі й фільтрації пакетів – мінімальною вимогою є фільтрація пакетів за адресою одержувача.

Іншою важливою відмінністю мостів від повторювачів є те, що сегменти, підключені до повторювача, створюють одне поділюване середовище, а сегменти, підключені до кожного порту моста, – своє середовище.

При використанні моста користувачі одного сегмента розділяють смугу, а користувачі різних сегментів використовують незалежні середовища. Отже, міст забезпечує переваги щодо розширення мережі, так і забезпечення більшої смуги для кожного

користувача.

Мости виконують нескладні функції: аналізують вступників фрейми й, базуючись на інформації, що втримується у фреймах, ухвалюють рішення щодо їх пересилання до місця призначення.

Оскільки мости функціонують на канальному рівні, вони можуть швидко приміщувати трафік, що представляє будь-який протокол мережевого рівня, не перевіряючи інформацію вищих рівнів. Ця властивість прозорості мостів для протоколів верхніх рівнів дозволяє, наприклад, приміщувати трафік протоколів Apple Talk, DECnet, TCP/IP, XNS та інших між двома й більше мережами і є основною перевагою використання мостів для створення об'єднаних мереж.

Таким чином, *переваги* використання мостів:

– мости збільшують кількість зв'язаних мережею пристроїв і ефективну довжину ЛОМ, дозволяючи підключати додаткові віддалені станції й мережні сегменти;

– розділяючи великі мережі на автономні блоки, мости зменшують трафік в окремих сегментах і створюють перешкоду для поширення деяких потенційно небезпечних для мережі несправностей.

Можна виділити два основних типи мостів:

– локальні мости забезпечують пряме з'єднання множини сегментів ЛОМ, що перебувають на одній території;

– дистанційні мости з'єднують множину сегментів ЛОМ на різних територіях, звичайно через телекомунікаційні лінії.

Міст (bridge), а також його функціональний аналог, що швидко діє – *комутатор (switching hub)*, ділить загальне середовище передачі даних на логічні сегменти. Логічний сегмент утворюється шляхом об'єднання декількох фізичних сегментів (відрізків кабелю) за допомогою одного або декількох концентраторів. Кожний логічний сегмент підключається до окремого порту моста/комутатора. При надходженні кадру на який-небудь із портів міст/комутатор повторює цей кадр, але не на всіх портах, як це робить концентратор, а тільки на той порт, до якого підключений сегмент, що містить комп'ютер-адресат.

Різниця між мостом і комутатором полягає в тому, що міст у будь-який момент часу може здійснювати передачу кадрів тільки між однією парою портів, а комутатор одночасно підтримує потоки

даних між всіма своїми портами. Інакше кажучи, міст передає кадри послідовно, а комутатор паралельно. (Для спрощення викладу далі в цьому розділі буде використовуватися термін "комутатор" для позначення цих обох різновидів пристроїв, оскільки все сказане нижче рівною мірою стосується і мостів, і комутаторів.) Варто зазначити, що останнім часом локальні мости повністю витиснуті комутаторами. Мости використовуються тільки для зв'язку локальних мереж із глобальними, тобто як засоби віддаленого доступу, оскільки в такому разі просто немає необхідності в паралельній передачі між декількома парами портів.

При роботі комутатора середовище передачі даних кожного логічного сегмента залишається загальним тільки для тих комп'ютерів, які підключені до цього сегмента безпосередньо. Комутатор здійснює зв'язок середовищ передачі даних різних логічних сегментів. Він передає кадри між логічними сегментами тільки при необхідності, тобто тільки тоді, коли комп'ютери, що взаємодіють, перебувають у різних сегментах.

Розподіл мережі на логічні сегменти поліпшує її продуктивність, якщо в мережі є групи комп'ютерів, що переважно обмінюються інформацією між собою.

Комутатори ухвалюють рішення щодо того, на який порт потрібно передати кадр, аналізуючи адресу призначення, поміщену в кадрі, а також на підставі інформації про приналежність того чи іншого комп'ютера певному сегменту, підключеному до одного з портів комутатора, тобто на підставі інформації про конфігурацію мережі. Для того, щоб зібрати й обробити інформацію про конфігурацію підключених до нього сегментів, комутатор повинен пройти стадію "навчання", тобто самостійно здійснити деяку попередню роботу з вивчення трафіку. Визначення приналежності комп'ютерів сегментам можливо за рахунок наявності в кадрі не тільки адреси призначення, але й адреси джерела. Використовуючи інформацію про адресу джерела, комутатор установлює відповідність між номерами портів і адресами комп'ютерів. У процесі вивчення мережі комутатор просто передає кадри, що з'явилися на входах його портів, на всі інші порти, працюючи якийсь час повторювачем. Після того, як комутатор довідується про приналежності адрес сегментам, він починає передавати кадри між портами тільки у разі міжсегментної передачі. Якщо вже після

завершення навчання на вході комутатора раптом з'явиться кадр із невідомою адресою призначення, він буде повторений на всіх портах.

Розглянемо принципи роботи комутатора.

Комутатор – це мережевий пристрій, що забезпечує передачу інформації від порту джерела інформації до порту призначення з мінімальними затримками й низькими накладними витратами. Ядром комутатора є комутаційна матриця, що забезпечує передачу даних між будь-якими двома точками, або шина, через яку будь-який порт може передати інформацію іншому порту. Крім того, у комутаторі повинні бути адаптери портів, що дозволяють перетворювати протокол, що використовує приєднаний до порту пристрій, у форму, прийнятну для ядра комутатора.

Джерело даних передає пакети локальної мережі в адаптер порту, до якого він підключений, а адаптер перетворить адресу призначення пакета на адресу порту комутатора. Потім адаптер передає пакет у ядро комутатора, додавши до нього обчислену адресу порту. Одержавши багатоадресне повідомлення, комутатор направляє його всім учасникам віртуальної мережі джерела повідомлення. При цьому передбачається, що мережа працює настільки швидко, що сумарний обсяг трафіку не може перевищити її пропускної здатності.

Комутатор Ethernet підтримує внутрішню таблицю, що зв'язує порти з адресами підключених до них пристроїв (табл. 35). Цю таблицю адміністратор мережі може створити самостійно або задати її автоматичне створення засобами комутатора.

Використовуючи таблицю адрес і адресу одержувача, що міститься в пакеті, комутатор організовує віртуальне з'єднання порту відправника з портом одержувача й передає пакет через це з'єднання.

Таблиця 35

Зв'язок портів з адресами підключених до них пристроїв

MAC-адреса	Номер порту
A	1
B	2
C	3
D	4

Віртуальне з'єднання між портами комутатора зберігається протягом передачі одного пакета, тобто для кожного пакета віртуальне з'єднання організується заново на основі адреси одержувача, що міститься в цьому пакеті. Оскільки пакет передається тільки в той порт, до якого підключений адресат, інші користувачі його не одержать. Таким чином, комутатори забезпечують засоби безпеки, недоступні для стандартних повторювачів.

У комутаторах Ethernet передача даних між будь-якими парами портів відбувається незалежно й, отже, для кожного віртуального з'єднання виділяється вся смуга каналу.

Наприклад, комутатор 10Мбіт/с на рис. 48 забезпечує одночасну передачу пакета з A в D і з порту B у порт C зі смугою 10Мбіт/с для кожного з'єднання.

Оскільки для кожного з'єднання надається вся смуга, сумарна пропускна здатність комутатора в наведеному прикладі становить 20Мбіт/с. Якщо дані передаються між більшим числом пар портів, інтегральна смуга відповідно розширюється. Наприклад, 24 портовий комутатор Ethernet може забезпечувати інтегральну пропускну здатність до 120Мбіт/с при одночасній організації 12 з'єднань зі смугою 10Мбіт/с для кожного з них. Теоретично інтегральна смуга комутатора росте пропорційно числу портів.

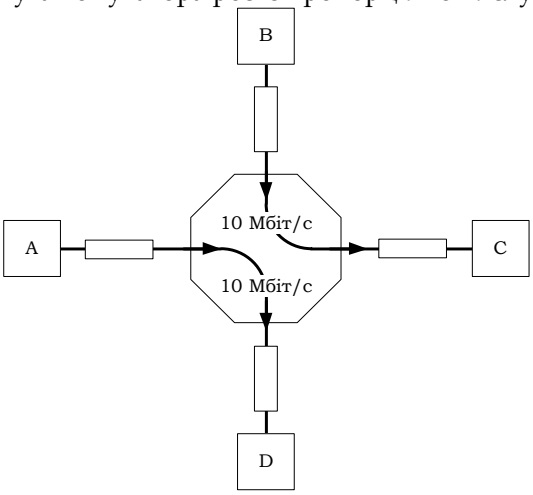


Рис. 48. Одночасні з'єднання

Комутатор Ethernet 10Мбіт/с може забезпечити високу пропускну здатність за умови організації одночасних з'єднань між

всіма парами портів. Однак у реальному житті трафік зазвичай являє собою ситуацію "один до багатьох" (наприклад, безліч користувачів мережі звертається до ресурсів одного сервера). У таких випадках пропускна здатність комутатора не буде перевищувати 10 Мбіт/с, і комутатор не забезпечить істотної переваги в порівнянні зі звичайним концентратором (повторювачем).

На рис. 49 три вузли A, B і D передають дані вузлу C. Комутатор зберігає пакети від вузлів A і B у своїй пам'яті доти, поки не завершиться передача пакета з вузла D. Після завершення передачі пакета комутатор починає передавати пакети, що зберігаються в пам'яті, від вузлів A і B. У цьому випадку пропускна здатність комутатора визначається смугою каналу C (10Мбіт/с).

Класи комутаторів Ethernet. Хоча всі комутатори мають багато спільного, доцільно поділити їх на два класи.

Комутатори для робочих груп. Комутатори для робочих груп забезпечують виділену смугу при з'єднанні будь-якої пари вузлів, підключених до портів комутатора. Комутатор забезпечує для кожного порту виділену смугу 10Мбіт/с. Кожний порт комутатора пов'язаний з унікальною адресою підключеного до певного порту пристрою Ethernet (рис. 50).

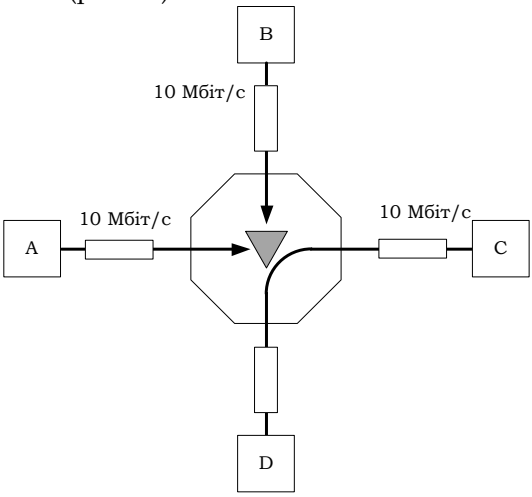


Рис. 49. З'єднання "один до багатьох"

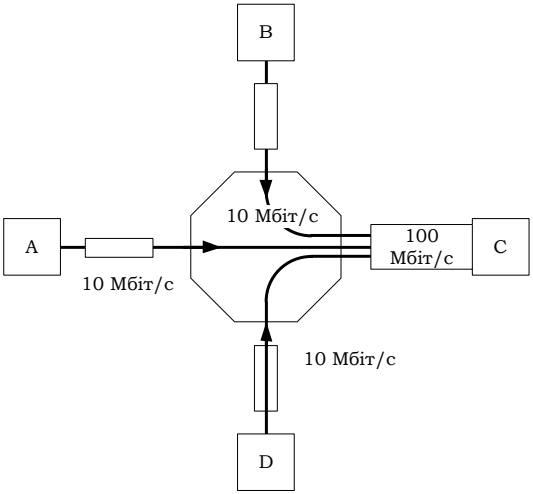


Рис. 50. Комутатор у мережі з архітектурою клієнт-сервер

Комутатори робочих груп можуть працювати зі швидкістю 10 або 100Мбіт/с для різних портів. Така можливість знижує рівень блокування при спробі організації декількох з'єднань клієнтів 10Мбіт/с з одним швидкісним портом. У робочих групах з архітектурою клієнт-сервер кілька клієнтів 10Мбіт/с можуть звертатися до сервера, підключеного до порту 100Мбіт/с. У прикладі три вузли 10Мбіт/с одночасно звертаються до сервера через порт 100Мбіт/с. Зі смуги 100Мбіт/с, відкритої для доступу до сервера, використовується 30Мбіт/с, а 70Мбіт/с доступно для одночасного підключення до сервера ще семи пристроїв 10Мбіт/с через віртуальні канали.

Основною перевагою комутаторів для робочих груп є висока продуктивність мережі за рахунок надання кожному користувачу смуги каналу (10Мбіт/с). Крім того, комутатори знижують (до нуля) кількість колізій, на відміну від магістральних комутаторів, комутатори робочих груп, не будуть передавати колізійні фрагменти адресатам. Комутатори для робочих груп дозволяють повністю зберегти мережеву інфраструктуру з боку клієнтів, включаючи програми, мережеві адаптери, кабелі. Вартість таких комутаторів з розрахунку на один порт дорівнює цінам портів керованих концентраторів.

Магістральні комутатори. Магістральні комутатори

забезпечують з'єднання зі швидкістю передачі середовища між парою незайнятих сегментів Ethernet. Якщо швидкість портів для відправника й одержувача збігаються, сегмент одержувача повинен бути вільний, щоб уникнути блокування.

На рівні робочої групи кожний вузол розділяє смугу 10Мбіт/с з іншими вузлами в тому ж сегменті. Пакет, адресований за межі групи, буде переданий магістральному комутатору, який забезпечує одночасну передачу пакетів зі швидкістю середовища між будь-якими парами своїх портів. Подібно комутаторам для робочих груп, магістральні комутатори можуть підтримувати різну швидкість для своїх портів. У більшості випадків використання магістральних комутаторів забезпечує більш простий і ефективний спосіб підвищення продуктивності мережі в порівнянні з маршрутизаторами й мостами.

Основним недоліком при роботі з магістральними комутаторами є те, що на рівні робочих груп користувачі працюють із поділюваним середовищем, якщо вони підключені до сегментів, організованих на основі повторювачів або коаксіального кабелю.

4.2.2. Маршрутизатори

Відповідно до визначення найбільшого виробника маршрутизаторів компанії Cisco, *маршрутизатор* – "це пристрій третього рівня, що використовує одну й більше метрик для визначення оптимального шляху передачі мережного трафіку на основі інформації мережевого рівня". По суті маршрутизатор являє собою "комп'ютер" з необхідним програмним забезпеченням і пристроями введення/виведення.

Маршрутизатор дозволяє організовувати в мережі надлишкові зв'язки, що утворюють петлі. Він справляється із цим завданням за рахунок того, що ухвалює рішення щодо передачі пакетів на підставі більш повної інформації про граф зв'язків у мережі, ніж міст або комутатор. Маршрутизатор має у своєму розпорядженні базу топологічної інформації, що говорить йому, наприклад, про те, між якими підмережами загальної мережі є зв'язки й у якому стані (працездатному чи ні) вони перебувають. Маючи таку карту мережі, маршрутизатор може вибрати один з декількох можливих маршрутів доставки пакета адресату. У цьому випадку під маршрутом розуміють послідовність проходження пакетом маршрутизаторів. Наприклад, на рис. 51 для зв'язку станцій L2 мережі LAN1 і L1 мережі LAN6 є два маршрути: M1-M5-M7 і M1-M6-M7.

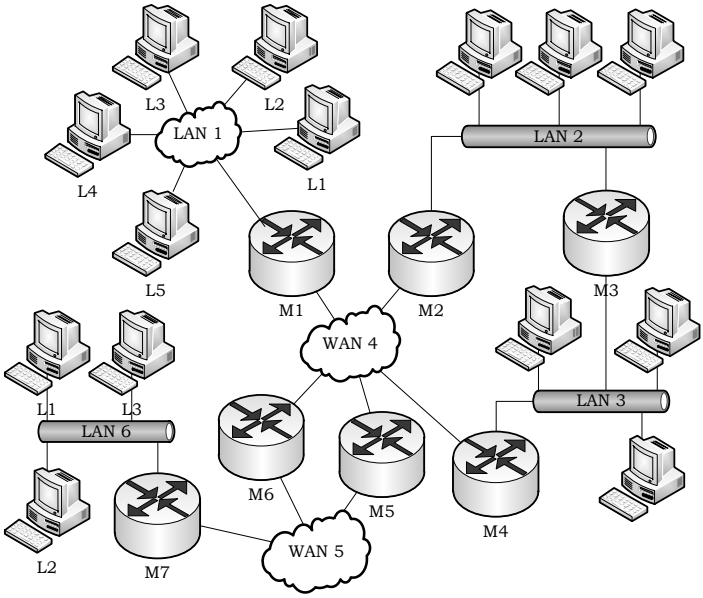


Рис. 51. Структура інтермережі, побудованої на основі маршрутизаторів: M1, M2, ... , M7 – маршрутизатори;
LAN1, LAN2, LAN3, WAN4, WAN5, LAN6 – унікальні номери мереж в єдиному форматі;
L1, L2, ... – локальні номери вузлів (дублюються, різний формат).

На відміну від моста й комутатора, які не знають, як зв'язані сегменти один з одним за межами їхніх портів, маршрутизатор бачить всю картину зв'язків підмереж один з одним, тому він може вибрати правильний маршрут і при наявності кількох альтернативних маршрутів. Рішення про вибір того або іншого маршруту приймається кожним маршрутизатором, через який проходить повідомлення.

Для того, щоб скласти карту зв'язків у мережі, маршрутизатори обмінюються спеціальними службовими повідомленнями, у яких міститься інформація про зв'язки між підмережами (ці підмережі підключені до них безпосередньо або ж вони дізналися цю інформацію від інших маршрутизаторів).

Побудова графа зв'язків між підмережами й вибір оптимального за яким-небудь критерієм маршруту на цьому графі є складним завданням. При цьому можуть використовуватися різні критерії вибору маршруту – найменша кількість проміжних вузлів,

час, вартість або надійність передачі даних.

Маршрутизатори дозволяють поєднувати мережі з різними принципами організації в єдину мережу, що в цьому випадку часто називається *інтермережа* (internet). Назва інтермережа акцентує на тому, що утворене за допомогою маршрутизаторів об'єднання комп'ютерів являє собою сукупність декількох мереж, які зберігають більший ступінь автономності, ніж кілька логічних сегментів однієї мережі.

У кожній з мереж, що утворюють інтермережу, зберігаються властиві їм принципи адресації вузлів і протоколи обміну інформацією. Тому маршрутизатори можуть поєднувати не тільки локальні мережі з різною технологією, але й локальні мережі із глобальними.

Маршрутизатори не лише поєднують мережі, але й надійно захищають їх одну від одної. Причому ця ізоляція здійснюється набагато простіше й надійніше, ніж за допомогою мостів і комутаторів. Наприклад, при надходженні кадру з неправильною адресою міст, комутатор зобов'язаний повторити його на всіх своїх портах, що робить мережу незахищеною від вузла, що некоректно працює. Маршрутизатор же в такому разі просто відмовляється передавати "помилковий" пакет далі, ізолюючи дефектний вузол від іншої мережі.

Крім того, маршрутизатор надає адміністратору зручні засоби фільтрації потоку повідомлень за рахунок того, що сам розпізнає багато полів службової інформації в пакеті й дозволяє їх іменувати зрозумілим адміністратору способом.

Крім фільтрації, маршрутизатор може забезпечувати пріоритетний порядок обслуговування пакетів, коли на підставі деяких ознак пакетам надаються переваги при виборі із черги.

Маршрутизатори часто плутають із мостами. Це пояснюється тим, що багато пристроїв поєднують у собі функції й мостів, і маршрутизаторів.

"Чистий" міст аналізує заголовки кадру канального рівня й не переглядає (а тим більше не модифікує) пакети мережного рівня всередині пакетів. Міст не знає й не повинен знати, які пакети – IP, IPX – містить у полі кадр, переданий з однієї локальної мережі в іншу.

Маршрутизатор, навпаки, знає дуже добре, з якими пакетами він працює, аналізує заголовки цих пакетів і приймає рішення

відповідно до адресної інформації, що міститься. З іншого боку, коли маршрутизатор передає пакет на канальний рівень, він не знає й не повинен знати про те, у який кадр цей пакет буде вміщений – Ethernet, Token Ring або який-небудь інший.

Маршрутизація – процес визначення в мережі шляху, по якому виклик або блок даних може досягти адресата. Основне ж завдання маршрутизації – перемикання трафіка. *Перемикання* – це процес прийому повідомлення, вибору маршруту подальшого проходження й відправлення його по цьому маршруту. Ця операція обслуговується чотирма різними процесами: вхідним драйвером, процесом вибору маршруту, чергою і вихідним драйвером.

Маршрутизація виконується на основі даних, що містяться в таблиці маршрутів. Рядок у таблиці маршрутів складається з таких полів:

– адреса мережі призначення;

– адреса наступного маршрутизатора (тобто вузла, що знає, куди далі відправити дейтаграму, адресовану в мережу призначення);

– допоміжні поля.

Маршрутизація розв'язує два завдання:

– вибір оптимального, за деяким критерієм, шляху просування інформації від джерела до пункту призначення через об'єднану мережу;

– транспортування інформаційних блоків (пакетів) за обраним маршрутом, або комутація.

Приклади маршрутизації

Розглянемо процес маршрутизації на прикладі. Припустимо (рис. 52), хости А і В перебувають у мережі 1, мережа 1 з'єднується з мережею 2 за допомогою маршрутизатора G1. До мережі 2 підключений маршрутизатор G2, що з'єднує її з мережею 3, у якій перебуває хост С.

Таблиця маршрутів хоста А виглядає, наприклад, так:

Мережа 1 – А

Інші мережі – G1

Це означає, що дейтаграми, адресовані вузлам мережі 1, відправляє сам хост А (тому що це його локальна мережа), а дейтаграми, адресовані в будь-яку іншу мережу (це називається маршрут за замовчуванням), хост А відправляє маршрутизатору G1, щоб той зайнявся їхньою подальшою долею.

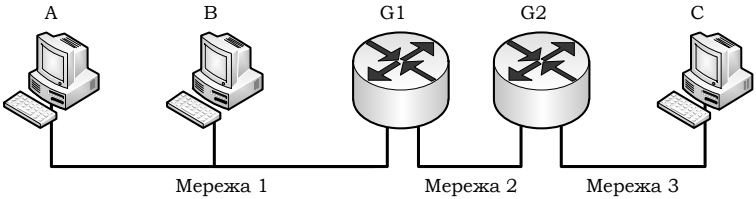


Рис. 52. Приклад маршрутизації

Припустимо, хост А посилає дейтаграму хосту В. У цьому випадку, оскільки адреса В належить тій же мережі, що й А, з таблиці маршрутів хоста А визначається, що доставка здійснюється безпосередньо самим хостом А.

Якщо хост А відправляє дейтаграмму хосту С, то він визначає зв IP-адресу С, що хост С не належить мережі 1. Відповідно до таблиці маршрутів А, всі дейтаграми з пунктами призначення, що не належить мережі 1, відправляються на маршрутизатор G1 (це називається маршрут за замовчуванням). При цьому хост А не знає, що маршрутизатор G1 буде робити з його дейтаграмою і який буде її подальший маршрут – цим займається виняткова G1. G1 за своєю таблицею маршрутів визначає, що всі дейтаграми, адресовані в мережу 3, повинні бути переслані на маршрутизатор G2. Це може бути, як прямо зазначено в таблиці, що перебуває на G1, у вигляді

Мережа 3 – G2,

так і зазначено у вигляді маршруту за замовчуванням.

На цьому функції G1 закінчуються, подальший шлях дейтаграми йому невідомий і його не цікавить. Маршрутизатор G2, одержавши дейтаграму, визначає, що вона адресована в одну з мереж (№3), до яких він приєднаний безпосередньо, і доставляє дейтаграму на хост С.

4.2.3. Приклад підключення локальної мережі організації до Інтернет.

Розглянемо реальний приклад підключення до Інтернет локальної мережі організації (рис. 53). IP-адреса локальної мережі – 194.84.124.0/24 (мережа класу С). Ця мережа містить маршрутизатор G1. IP-інтерфейс цього маршрутизатора, підключений до локальної мережі Ethernet, і має адресу 194.84.124.1. Другий IP-інтерфейс маршрутизатора підключений до виділеної лінії (синхронний послідовний канал), що веде до провайдера Інтернет. До іншого кінця цієї лінії підключений IP-інтерфейс маршрутизатора G2, що

належить провайдеру. Ці два інтерфейси утворять окрему мережу 194.84.0.116/30. У цій мережі на номер інтерфейсу відведено всього 2 біти – 4 варіанти адрес, з яких один (00) позначає саму мережу, один (11) – широкомовний; таким чином, у подібній мережі може перебувати всього 2 вузли – це мінімальна можлива мережа. Інтерфейс маршрутизатора G1 у мережі 194.84.0.116/30 має адресу 194.84.0.117, а маршрутизатора G2 – 194.84.0.118. Маршрутизатор G2 має ще деяку кількість інтерфейсів, до частини яких підключені виділені лінії від інших клієнтів, до частини – локальні мережі комунікаційного центра, інші маршрутизатори й магістральні лінії дальнього зв'язку.

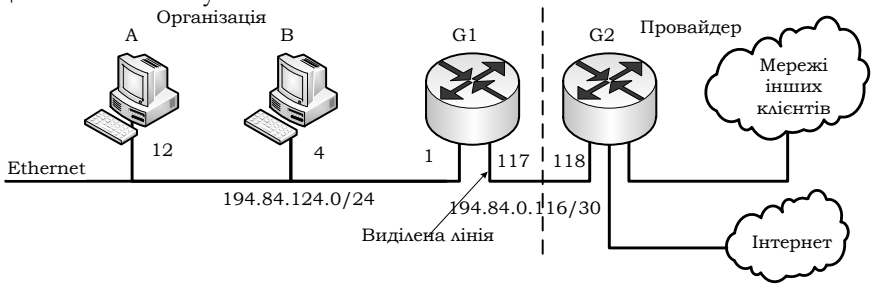


Рис. 53. Підключення локальної мережі до Інтернет

Таблиці маршрутів. Розглянемо приклади маршрутних таблиць, з якими має справу адміністратор локальної мережі 194.84.124.0/24:

Таблиця 36

Маршрути рядового хоста з адресою 194.84.124.4 (хост B)

Destination	Gateway	Flags	Interface
127.0. 0.1	127.0. 0.1	UH	lo0
194.84. 124.0	194.84. 124.4	U	le0
0.0. 0.0	194.84. 124.1	UG	

Значення прапорів: U (Up) – маршрут працює; H (Host) – пунктом призначення є окремий вузол (хост), а не мережа; G (Gateway) – маршрут до мережі призначення проходить через один або кілька проміжних маршрутизаторів. Інтерфейс le0 позначає Ethernet, lo0 – інтерфейс зворотного зв'язку (loopback).

Значення першого запису очевидне, другий запис визначає, що дейтаграми, адресовані в локальну мережу, хост відправляє

самостійно через свій інтерфейс le0. Третій запис (маршрут за замовчуванням) установлює, що всі інші дейтаграми передаються на адресу 194.84.124.1, що є адресою наступного маршрутизатора (прапор G) для подальшого пересилання. Щоб визначити спосіб досягнення самого маршрутизатора, треба, мабуть, звернутися до другого рядка таблиці, тому що адреса маршрутизатора належить мережі 194.84.124.0.

Зауважимо, що в цій таблиці для спрощення опущені маски мереж.

Приклад таблиці маршрутів маршрутизатора, що з'єднує локальну мережу із провайдером Інтернет по виділеному каналу (G1 на рис. 53):

Таблиця 37

Маршрути маршрутизатора, що з'єднує локальну мережу із провайдером Інтернет по виділеному каналу

Destination	Mask	Gateway	Interface
194.84. 124.0	255. 255.255.0	194.84. 124.1	le0
194.84. 0. 116	255. 255.255.252	194.84. 0. 117	se0
0.0. 0.0	0.0. 0.0	194.84. 0. 118	

У таблиці наведені маски мереж.

Перші два записи свідчать про те, що маршрутизатор самостійно, через свої відповідні IP-інтерфейси відправляє дейтаграми, адресовані в мережі, до яких він підключений безпосередньо. Усі інші дейтаграми перенаправляються до G2 (194.84.0.118). Інтерфейс se0 позначає послідовний (serial) канал – виділену лінію.

Таблиця маршрутів може заповнюватися різними способами. Статична маршрутизація застосовується тоді, коли використовувані маршрути не можуть змінитися протягом часу, наприклад, для вище зазначених хостів і маршрутизатора, де просто немає ніяких альтернативних маршрутів. Статичні маршрути конфігуруються адміністратором мережі або конкретного вузла.

У разі об'єднання мереж зі складною топологією, коли є кілька варіантів маршрутів від одного вузла до іншого й (або) коли стан мереж (топологія, якість каналів зв'язку) змінюється із часом, таблиці маршрутів складаються динамічно за допомогою різних протоколів маршрутизації. Протоколи маршрутизації на підставі тих або інших

алгоритмів динамічно редагують таблицю маршрутів, тобто вносять і видаляють записи, при цьому частина записів може, як і раніше, статично вноситися адміністратором.

Залежно від алгоритму роботи розрізняють дистанційно-векторні протоколи (distance vector protocols) і протоколи стану зв'язків (link state protocols). За галуззю застосування існує поділ на протоколи зовнішньої (exterior) і внутрішньої (interior) маршрутизації.

Лабораторна робота №8 (2 год.)
Тема: Інтелектуальні комутатори Ethernet

Мета: сформувати вміння управляти інтелектуальним комутатором Ethernet;

виховувати ціннісне ставлення студентів до навчальної діяльності.

Студент повинен знати: характеристики інтелектуальних комутаторів та їх властивості.

Студент повинен уміти: здійснювати управління інтелектуальним комутатором з використання web-інтерфейсу.

Хід роботи

Інструктаж

1. Розглянути характеристики інтелектуальних комутаторів Ethernet.
2. Визначити можливості налагодження інтелектуального комутатора.

Практична робота

1. Здійснити підключення до інтелектуального комутатора з використанням web-інтерфейсу.
2. Здійснити управління портами комутатора (зміна швидкості, вимкнення, перевантаження, якість обслуговування).
3. Здійснити управління віртуальними мережами (зміна параметрів Уже наявної віртуальної мережі, створення нової віртуальної мережі).
4. Здійснити управління груповим розсиланням з використанням Trunking.
5. Налагодити відображення портів в інтелектуальному комутаторі.

Самостійна робота №8
Тема: Загальні принципи адресації

Мета: розвивати у студентів уміння використовувати загальні принципи адресації в ієрархічних мережах.

Студент повинен знати: загальні принципи адресації для ієрархічних мереж.

Студент повинен уміти: використовувати принципи адресації при проектуванні ієрархічної комп'ютерної мережі.

Хід роботи

Теоретична частина

1. Опишіть ефект, що виникає внаслідок використання як стандартного маршруту широкомовного мережного інтерфейсу.

2. Поясніть відмінності між трансляцією мережних адрес (Network Address Translation — NAT) та адрес з використанням портів (Port Address Translation — PAT).

Практична робота

Законспектуйте основні положення стосовно трансляції мережевих адрес і трансляції адрес з використанням портів

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Побудова корпоративних локальних мереж на основі інтелектуальних комутаторів".

МОДУЛЬНА КОНТРОЛЬНА РОБОТА №4

Оберіть номер правильної відповіді:

1. Які пристрої поєднують мережі на фізичному рівні?

а) повторювачі;

б) мости;

в) комутатори;

г) серед перерахованих пристроїв немає правильних.

1 б.

2. Які пристрої поєднують мережі на канальному рівні?

а) мости, комутатори;

б) мости;

в) комутатори;

г) серед перерахованих пристроїв немає правильних.

1 б.

3. З яких полів складається таблиця маршрутів?

а) адреса мережі призначення, адреса наступного маршрутизатора;

б) адреса мережі призначення, адреса наступного маршрутизатора, допоміжні поля;

с) адреса мережі призначення, адреса наступного маршрутизатора, адреса попереднього маршрутизатора.

1 б.

4. Ядром якого пристрою є комутаційна матриця, що забезпечує передачу даних між будь-якими двома точками, або шина, що швидко діє, через яку будь-який порт може передати інформацію будь-якому іншому порту?

а) маршрутизатор;

б) комутатор;

в) концентратор.

1 б.

5. Для яких пристроїв мережа представляється набором MAC-адрес?

а) комутатори;

б) маршрутизатори;

в) мости, комутатори;

г) мости;

д) концентратори.

1 б.

6. Таблиця якого пристрою представлена на малюнку?

а) маршрутизатор;
б) концентратор;
в) міст;
г) комутатор.

MAC-адреса	**Номер порту**
A	1
B	2
C	3
D	4

1 б.

7. Які пристрої поєднують мережі в інтермережу?
а) маршрутизатори;
б) концентратори;
в) мости;
г) комутатори.

1 б.

8. У ядрі якого пристрою утвориться швидка "віртуальна мережа"?
а) міст;
б) повторювач;
в) комутатор;
г) маршрутизатор.

1 б.

9. Як називається багатопортовий повторювач?
а) концентратор;
б) маршрутизатор;
в) комутатор.

1 б.

10. Які завдання розв'язує маршрутизація?
а) вибір оптимального за деяким критерієм маршруту просування інформації від джерела до пункту призначення через об'єднану мережу;
б) транспортування інформаційних блоків (пакетів) за обраним маршрутом, або комутація;
в) усе невірно;
г) усе вірно.

1 б.
Всього: 10 балів.

Правильні відповіді

Питання	1	2	3	4	5	6	7	8	9	10
Відповідь	а	а	б	б	б	г	а	в	а	а

ЗМІСТОВИЙ МОДУЛЬ 5

ПРОТОКОЛ МІЖМЕРЕЖЕВОЇ ВЗАЄМОДІЇ. АДРЕСАЦІЯ В СТЕКУ ПРОТОКОЛІВ TCP/IP. ОСОБЛИВОСТІ АДРЕСАЦІЇ В СТЕКУ ПРОТОКОЛІВ TCP/IP

Таблиця 38

Тематичний план змістового модуля

№ теми	Назва змістового модуля, теми	Усього годин	Лекції	Лабораторні заняття	Самостійна та індивідуальна робота
5.1	Протокол міжмережевої взаємодії. Адресація в стеку протоколів TCP/IP	9	2	2	5
5.2	Особливості адресації в стеку протоколів TCP/IP	9	2	2	5
	Разом	***18***	***4***	***4***	***10***

Навчальні цілі: сприяти засвоєнню студентами знань щодо принципів функціонування протоколу IP, розвивати вміння керування Ip-адресацією та маршрутизацією з використанням масок.

Основні поняття: протокол IP, формат IP-пакету, локальна адреса, мережева адреса, доменне ім'я, клас IP-адреси, особливі IP-адреси, DHCP, CIDR, маршрутизація, маска мережевої адреси, маска змінної довжини.

Методичні рекомендації щодо роботи з модулем: робота з модулем передбачає засвоєння лекційного матеріалу, участь у лабораторних заняттях, написання реферату (окремими студентами), самостійну роботу над визначеними питаннями теми, модульний контроль у формі тестування.

Після опрацювання цих тем студент може отримати бали,

наведені в табл. 39.

Таблиця 39

Оцінювання навчальних досягнень студентів

Поточний контроль					**Контрольна рейтингова оцінка**	**Проміжна рейтингова оцінка**
Робота на лабораторному занятті		**Самостійна робота**		**Індивідуальне завдання**		
Тема №5.1	**Тема №5.2**	**Тема №5.1**	**Тема №5.2**			
5	5	2	2	5	10	29

ТЕМА 5.1. ПРОТОКОЛ МІЖМЕРЕЖЕВОЇ ВЗАЄМОДІЇ. АДРЕСАЦІЯ В СТЕКУ ПРОТОКОЛІВ TCP/IP

Лекція

План

1. Протокол IP
2. Ip-адреси
3. Адресація IP v.4
4. Класи Ip-Адрес: A, B, C, D і E
5. Зарезервовані IP-адреси

Література

Основна

1. *Компьютеры*, сети, Интернет: Энциклопедия: Наиболее полн. и подроб. рук. / Ю. Новиков, Д. Новиков, А. Черепанов, В. Чуркин; Под общ. ред. Ю. Новикова. – 2. изд. – М. [и др.]: Питер, 2003 (СПб.: ГПП Печ. Двор им. А.М. Горького). – 831 с.: ил.; 24 см.

2. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. –

943 с.: ил.; 24 см. – (Учебник для вузов).

3. *Олифер В. Г.* Новые технологии и оборудование IP-сетей / Виктор Олифер, Наталья Олифер. – СПб. и др.: BHV, 2000. – 512 с.: ил., табл.; 24 см. – (Мастер) (Современные сетевые технологии).

4. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. – 4-е изд. – М. [и др.]: Питер, 2005. – 991 с.: ил., табл.; 24 см. – (Классика computer science).

Додаткова

1. *Башмаков А. И.* Интеллектуальные информационные технологии: учеб. пособие для студ. вузов, обуч. по направлению подгот. дипломированных спец. "Информатика и вычислительная техника" / А. И. Башмаков, И. А. Башмаков – М. : МГТУ им.Н.Э.Баумана, 2005. – 302 с.

2. *Білоус Л. Ф.* Інформаційні мережі : навч. посібник / Білоус Л. Ф. – К. : Логос, 2005. – 140 с.

3. *Вишневский А.* Сетевые технологии Windows 2000 / Алексей Вишневский. – СПб. и др.: Питер, 2000. – 591 с.: ил., табл.; 24 см. – (Для профессионалов).

4. *Грир Т.* Сети Интернет: Пер. с англ. – М.: ИТД "Русская редакция", 2000. – 368 с.

5. *Ибе О.* Сети и удаленный доступ: Протоколы, проблемы, решения / Оливер Ибе. – М.: ДМК Пресс, 2002. – 332 с.: ил.; 23 см. – (Серия "Защита и администрирование").

6. *Камер Д.Э.* Компьютерные сети и Internet: Разработка приложений для Internet (пер. с англ. Птицына К.А.) Изд. 3-е + CD-Rom – 640 с.

7. *Коваленко А. Є.* Корпоративні комп'ютерні мережі та телекомунікації : конспект лекцій для студ. спец. 7.080401 "Інформаційні управляючі системи та технології" ден. форми навч. / Анатолій Єпіфанович Коваленко. – К. : НУХТ, 2004. – 27 с.

8. *Контроль* та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології : навчальний посібник / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. – Х. : "Компанія СМІТ", 2004. – 544 с.

5.1.1. Протокол IP

Основу стеку протоколів TCP/IP становить *протокол міжмережевої взаємодії (Internet Protocol, IP)*. Який забезпечує передачу дейтаграм від відправника до одержувачів через об'єднану систему

комп'ютерних мереж.

Назва цього протоколу – *Internet Protocol* – відбиває його суть: він повинен передавати пакети між мережами. У кожній наступній мережі, що лежить на шляху переміщення пакета, протокол IP викликає засоби транспортування, прийняті в цій мережі, щоб з їхньою допомогою передати цей пакет на маршрутизатор, що веде до іншої мережі, або безпосередньо на вузол-одержувач.

Протокол IP належить до протоколів без установлення з'єднань. Перед IP не ставиться завдання надійної доставки повідомлень від відправника до одержувача. Протокол IP обробляє кожний IP-пакет як незалежну одиницю, що не має зв'язку ні з якими іншими IP-пакетами. У протоколі IP немає механізмів, застосовуваних зазвичай для збільшення вірогідності кінцевих даних, зокрема обміну підтвердженнями між відправником і одержувачем, процедури впорядкування, повторних передач або інших подібних функцій. Якщо під час просування пакета відбулася якась помилка, то протокол IP зі своєї ініціативи нічого не робить для її виправлення. Наприклад, якщо на проміжному маршрутизаторі пакет був відкинутий через закінчення часу життя або через помилку в контрольній сумі, то модуль IP не намагається заново послати зіпсований або загублений пакет. Усі питання забезпечення надійності доставки даних по складній мережі в стеці TCP/IP вирішує протокол TCP, що працює безпосередньо над протоколом IP. Саме TCP організує повторну передачу пакетів, коли в цьому виникає необхідність.

Важливою особливістю протоколу IP, що відрізняє його від інших мережних протоколів, є його здатність виконувати динамічну фрагментацію пакетів при передачі їх між мережами з різними, максимально припустимими значеннями поля даних кадрів MTU. Властивість фрагментації багато в чому сприяло тому, що протокол IP зміг зайняти основні позиції в складних мережах.

Є прямий зв'язок між функціональною складністю протоколу й складністю заголовка пакетів, які цей протокол використовують. Це пояснюється тим, що основні службові дані, на підставі яких протокол виконує ту або іншу дію, переносяться між двома модулями, що реалізують цей протокол на різних машинах, саме в полях заголовків пакетів. Тому дуже корисно вивчити призначення кожного поля заголовка IP-пакета, і це вивчення дає не тільки формальні знання про структуру пакета, але й пояснює всі основні

режими роботи протоколу обробки й передачі IP-дейтаграм.

Формат заголовка IP-дейтаграми. IP-дейтаграма складається із заголовка й даних. Заголовок дейтаграми складається з 32-розрядних слів і має перемінну довжину, що залежить від розміру поля "Options", але завжди кратну 32 бітам. За заголовком безпосередньо ідуть дані, передані в дейтаграмі (рис. 54).

<table>
<tr><td>0</td><td>7</td><td>15</td><td colspan="2">23</td><td>31</td></tr>
<tr><td>Ver</td><td>IHL</td><td>TOS</td><td colspan="2">Total</td><td>Length</td></tr>
<tr><td colspan="3">ID</td><td>Flags</td><td>Fragment</td><td>Offset</td></tr>
<tr><td colspan="2">TTL</td><td>Protocol</td><td colspan="2">Header</td><td>Checksum</td></tr>
<tr><td colspan="6">Source Address</td></tr>
<tr><td colspan="6">Destination Address</td></tr>
<tr><td colspan="5">Options</td><td>Padding</td></tr>
</table>

Рис. 54. Формат заголовка IP-дейтаграми

Значення полів заголовка такі.

Ver (4 біти) – версія протоколу IP, у цей момент використовується версія 4, нові розробки мають номери версій 6-8.

IHL (Internet Header Length) (4 біти) – довжина заголовка в 32-бітних словах; діапазон припустимих значень від 5 (мінімальна довжина заголовка, поле "Options" відсутнє) до 15 (тобто може бути максимум 40 байт опцій).

TOS (Type Of Service) (8 біт) – значення поля визначає пріоритет дейтаграми й бажаний тип маршрутизації. Структура байта TOS представлена на рис. 55.

<table>
<tr><td>0 2</td><td colspan="5">3 7</td></tr>
<tr><td>Precedence</td><td colspan="5">Type Of Service</td></tr>
<tr><td></td><td>D</td><td>T</td><td>R</td><td>C</td><td></td></tr>
</table>

Рис. 55. Структура байта TOS

Три молодших біти ("Precedence") визначають пріоритет дейтаграми: 111 – керування мережею, 110 – міжмережеве керування, 101 – CRITIC-ECP, 100 – більш ніж миттєво, 011 – миттєво, 010 – негайно, 001 – терміново, 000 – звичайно.

Біти D,T,R,C визначають бажаний тип маршрутизації:

– D (Delay) – вибір маршруту з мінімальною затримкою;
– T (Throughput) – вибір маршруту з максимальною

пропускною здатністю;

– R (Reliability) – вибір маршруту з максимальною надійністю;
– C (Cost) – вибір маршруту з мінімальною вартістю.

У дейтаграмі може бути встановлений тільки один з біт D,T,R,C. Старший біт байта не використовується.

Реальне врахування пріоритетів і вибору маршруту відповідно до значення байта TOS залежить від маршрутизатора, його програмного забезпечення й налагоджень. Маршрутизатор може підтримувати розрахунок маршрутів для всіх типів TOS, для частини або ігнорувати TOS взагалі. Маршрутизатор може враховувати значення пріоритету при обробці всіх дейтаграм або при обробці дейтаграм, що виходять тільки з деякої обмеженої множини вузлів мережі, або зовсім ігнорувати пріоритет.

Total Length (16 біт) – довжина всієї дейтаграми в октетах, включаючи заголовок і дані, максимальне значення 65535, мінімальне – 21 (заголовок без опцій і один октет у полі даних).

ID (Identification) (16 біт), Flags (3 біти), Fragment Offset (13 біт) використовуються для фрагментації й збірки дейтаграм.

TTL (Time To Live) (8 біт) – "час життя" дейтаграми, що встановлюється відправником і вимірюється в секундах. Кожний маршрутизатор, через який проходить дейтаграма, переписує значення TTL, попередньо віднявши з нього час, витрачений на обробку дейтаграми. При досягненні значення TTL=0 дейтаграма знищується, при цьому відправнику може бути послане відповідне ICMP-повідомлення. Контроль TTL запобігає зацикленню дейтаграми в мережі.

Protocol (8 біт) – визначає програму (вищій протокол стека), якій повинні бути передані дані дейтаграми для подальшої обробки.

Header Checksum (16 біт) – контрольна сума заголовка являє собою 16 біт, що доповнюють біти в сумі всіх 16-бітових слів заголовка. Перед обчисленням контрольної суми значення поля "Header Checksum" обнуляється. Оскільки маршрутизатори змінюють значення деяких полів заголовка при обробці дейтаграми, контрольна сума кожним маршрутизатором перераховується заново. Якщо при перевірці контрольної суми виявляється помилка, дейтаграма знищується.

Source Address (32 біта) – IP-адреса відправника.

Destination Address (32 біта) – IP-адреса одержувача.

Options – опції, поле змінної довжини. Опцій може бути одна, декілька або жодної, вони визначають додаткові послуги модуля IP з обробки дейтаграми, у заголовок якої вони включені.

Padding – вирівнювання заголовка по границі 32-бітного слова, якщо список опцій займає нецілe число 32-бітних слів. Поле "Padding" заповнюється нулями.

5.1.2. Ір-адреси

Щоб будь-які дві системи могли взаємодіяти між собою, вони повинні мати можливість однозначно ідентифікувати одна одну, як це показано на рис. 56. Незважаючи на те, що показані адреси не є фактичними мережевими адресами, вони демонструють концепцію групування адрес. Літери А і Б ідентифікують мережі, послідовність номерів ідентифікує мережеву станцію. Комбінація з літери (номера мережі) і послідовності цифр (адреси станції) створює унікальну адресу для будь-якого пристрою в мережі. У повсякденному житті імена або номери часто використовуються в якості унікальних ідентифікаторів. Аналогічно цьому кожний комп'ютер у мережі зобов'язаний мати як мінімум один унікальний ідентифікатор або адресу. Така адреса дозволяє одному комп'ютеру в мережі знаходити інший.

Комп'ютери можуть бути підключені до більш ніж однієї мережі, наприклад, так, як показано на рис. 57. Подвійне підключення реалізоване за допомогою використання двох мережевих адаптерів. Пристрій із двома з'єднаннями називається пристроєм з подвійною прив'язкою, або двоканальним пристроєм (dual homed). Варто зазначити, що два інтерфейси комп'ютера перебувають в абсолютно різних мережах і, як наслідок, мають різні ідентифікатори мережі у своїх адресах. Ще одне важливе зауваження: такий комп'ютер не пересилає дані між мережами, якщо тільки він не сконфігурований для цього спеціально; він просто має доступ до обох мереж. У подібній ситуації системі має бути привласнено більше однієї адреси, кожна з яких ідентифікує його з'єднання з окремою мережею. Тобто, не самій системі привласнюється адреса, а кожному з модулів, які використовуються для підключення вузла до мережі (тобто інтерфейсам), що дозволяє

іншим комп'ютерам знаходити його у відповідних мережах.

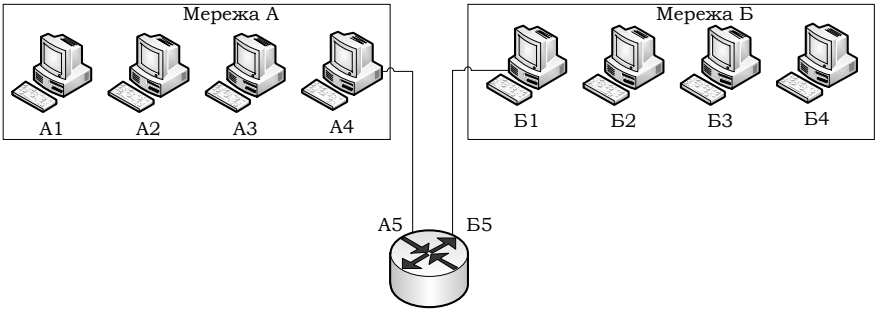


Рис. 56. Адреси вузлів

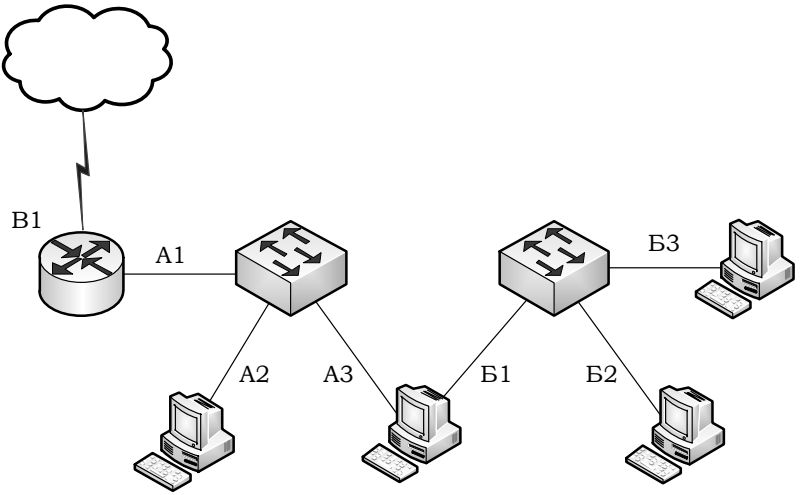


Рис. 57. Комп'ютери з подвійною прив'язкою

Комп'ютери зберігають IP-адреси у вигляді 32 бітової послідовності одиниць і нулів (рис. 58). Для простоти використання IP-адреса записується у вигляді чотирьох десяткових чисел, розділених крапками. Припустимо, адреса одного з комп'ютерів – 192.168.1.2. Другий комп'ютер може мати адресу 128.10.2.1. Такий спосіб написання адреси називається крапково-десятковим форматом. У такому вигляді кожна IP-адреса складається із чотирьох частин, розділених крапками. Кожна із частин називається октетом,

оскільки складається з восьми двійкових цифр. Наприклад, адресі 192.168.1.8 відповідає запис 11000000.10101000.00000001.00001000 у двійковій системі числення. Людина легше сприймає крапково-десятковий формат, ніж двійкові нулі й одиниці. Цей формат допомагає також уникнути помилок через перестановки цифр, що часто трапляється при використанні двійкових номерів.

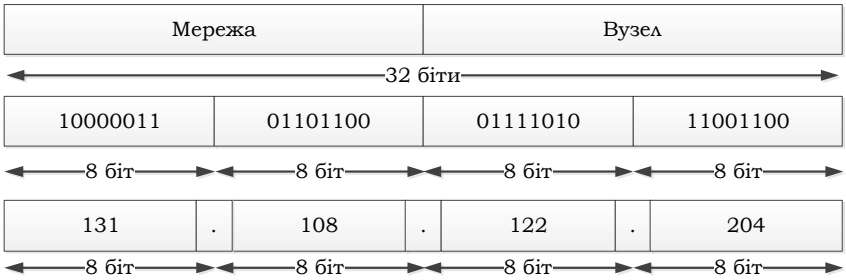


Рис. 58. Формат IP-адреси

Крапково-десятковий формат дозволяє набагато швидше розрізнити цифрові складові адреси (рис. 58). І двійковий, і десятковий номери на рисунку відповідають тій самій адресі, але в десятковому форматі вона виглядає набагато простіше й, що безсумнівно, коротше. Помилки – одна з найбільш загальних проблем при роботі із двійковими адресами. У довгих послідовностях з нулів і одиниць легко помилитися, поміняти цифри місцями або пропустити. Іншими словами, набагато простіше побачити зв'язок між такими двома номерами:

192.168.1.8 і
192.168.1.9,

ніж розпізнати той самий зв'язок у двійкових еквівалентах тих же адрес:

11000000.10101000.00000001.00001000 і
11000000.10101000.00000001.00001001.

Дивлячись на двійкову форму запису двох адрес, практично неможливо зрозуміти, що вони являють собою послідовні номери вузлів.

5.1.3. Адресація IP v.4

Протокол IP пересилає пакети, породжені в одній з мереж, в

іншу, тобто в мережу призначення, використовуючи деякі унікальні параметри (рис. 59). Отже, у цій схемі повинні бути задані ідентифікатори мережі відправника й мережі одержувача. Використовуючи ідентифікатор мережі призначення, протокол IP доставляє пакети в мережу, якій вони адресовані. Коли пакет досягає інтерфейсу маршрутизатора, підключеного до мережі одержувача, протокол IP повинен ідентифікувати певний комп'ютер, підключений до цієї ж мережі, якому адресований пакет. Описаний процес складається із двох етапів.

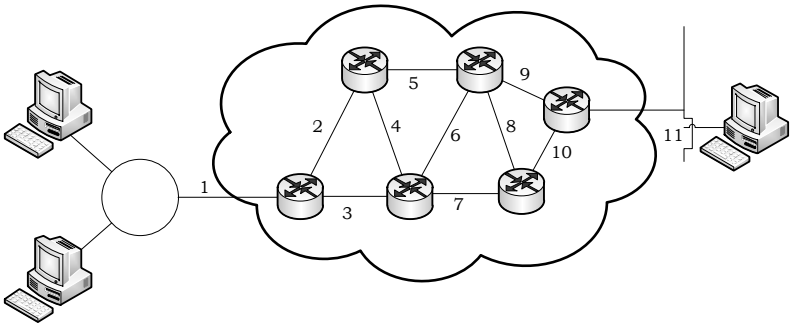


Рис. 59. Комунікаційний маршрут

IP-адреси складаються із двох частин, як це показано на рис. 60. Одна частина ідентифікує мережу, до якої підключена система, друга служить ідентифікатором самої системи. Така адресація називається ієрархічною, оскільки включає кілька рівнів, як показано на рис. 61. Значення будь-якого октету перебувають у діапазоні від 0 до 255. У розглянутому прикладі другий октет може бути розбитий на 256 підгруп, кожна з яких також може бути розбита на 256 підгруп з 256-ма адресами в кожній. Адреса групи, що перебуває в ієрархічній схемі (рис. 61) безпосередньо над групою, є ідентифікатором для всіх породжуваних областей адрес та мереж і може розглядатися як єдине ціле. IP-адреса поєднує обидва ідентифікатори в одну адресу. Такий номер повинен бути унікальним, оскільки дублювання адрес не допускається; його перша частина ідентифікує адресу мережі, а друга – адреса вузла – однозначно задає машину в цій мережі.

Як же користувач може відрізнити, яку частину адреси задає адреса мережі, а яка – адреса вузла? Уперше це запитання поставили собі творці мережі Інтернет, які вважали, що будуть створюватися мережі різного розміру, виходячи з необхідного числа комп'ютерів,

котрі входять до її складу, що проілюстровано в табл. 40.

При розробці такої схеми передбачалося, що дуже великих мереж, які міститимуть мільйони підключених комп'ютерів, буде порівняно мало. Розробники передбачили велику кількість мереж середнього масштабу з тисячами комп'ютерів у кожній з них. І, звичайно ж, вони припускали, що буде створена величезна кількість дрібних мереж з декількома сотнями машин або навіть менше. Виходячи з цього, розробники розділили доступні IP-адреси на класи й задали в такий спосіб розмір мереж: великі (клас A), середні (клас B) і дрібні (клас C) (табл. 41). Інформація про клас адреси – це перша підказка, яка використовується, щоб визначити, яка частина адреси описує мережу, а яка – адресу вузла.

Мережа	Вузел
1	1 2 3
2	1
3	1

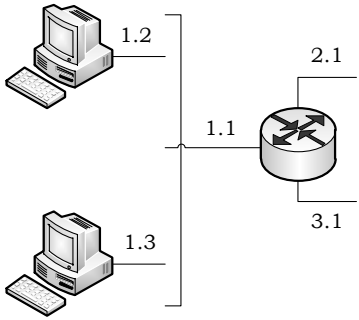


Рис. 60. Дві частини IP-адреси

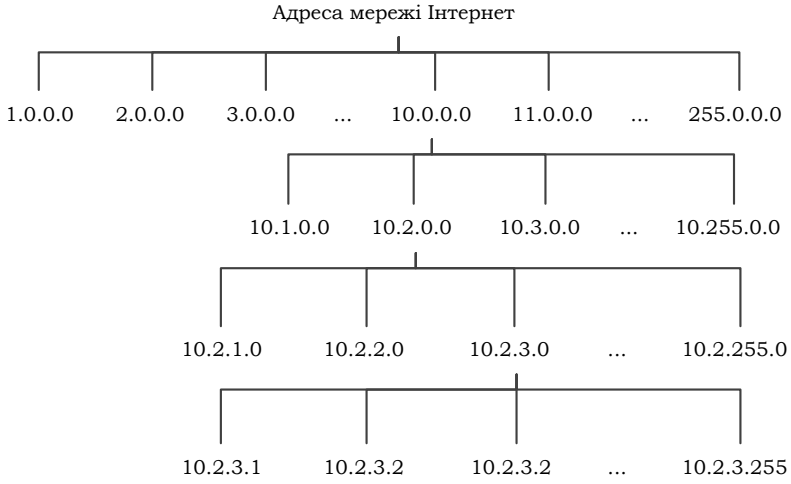


Рис. 61. Ієрархічні IP-адреси

Таблиця 40

Класи IP-адрес

Клас адреси	Кількість мереж	Кількість вузлів
A	1262	16777216
B	16384	65535
C	2097152	254
D (багатоадресатний)	-	-

Таблиця 41

Визначення класів адрес

Клас адреси	Початкові біти адреси	Діапазон значень першого октету адреси	Кількість біт у мережевій частині адреси
A	0	від 0 до 127	8
B	10	від 128 до 191	16
C	110	від 192 до 223	24
D	1110	від 224 до 239	28

5.1.4. Класи Ip-Адрес: A, B, C, D і E

Щоб мати можливість описати мережі різного розміру й полегшити їхню класифікацію, IP-адреси були розділені на групи, що називаються класами. Така схема адресації називається класовою. Кожна повна 32 бітова IP-адреса ділиться на дві частини, що описують мережу й вузол. Біт або послідовність біт на початку кожної адреси задають його клас. Існують п'ять класів IP-адрес (рис. 62).

Кількість початкових біт префіксу	1	7	24
Клас A: значення префіксу	0	Біти мережі	Біти вузла

Кількість початкових біт префіксу	2	14	16
Клас B: значення префіксу	10	Біти мережі	Біти вузла

Кількість початкових біт префіксу	3	21	8

Клас C: значення префіксу	110	Біти мережі	Біти вузла
Кількість початкових біт префіксу	4	28	
Клас D: значення префіксу	1110	Адреса	
Кількість початкових біт префіксу	4	28	
Клас E: значення префіксу	1111	Адреса	

Рис. 62. Початкові біти, що утворюють класи адрес

Адреси класу A (рис. 63) призначені для дуже великих мереж. В адресі класу A використовується тільки перший октет як ідентифікатор мережі. Три октети, що залишилися, виділені для перерахування адрес вузлів.

Перший біт в адресі класу A завжди рівний 0. Враховуючи це, найменше припустиме число буде рівним 00000000 (десятковий 0), а найбільше – 01111111 (десяткове число 127). Варто зазначити, що обидва номери, 0 і 127, є зарезервованими й не можуть бути використані в якості мережевих адрес. Будь-які адреси, що починаються із числа в діапазоні від 1 до 126 у першому октеті, є адресами класу A.

Мережа з номером 127.0.0.0 зарезервована для зворотного петлевого (loopback) тестування (маршрутизатори або локальні вузли можуть використовувати його для передачі пакетів самим собі). Отже, така адреса не може бути привласнена мережі.

Рис. 63. Адреси класу A

Адреси класу B використовуються для мереж середнього й великого розміру (рис. 64). В IP-адресі класу B використовуються два перші октети для мережевої адреси. Два октети, що залишилися представляють адресу вузла.

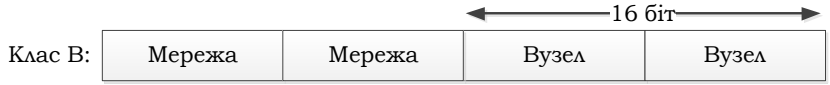


Рис. 64. Адреси класу B

Перші два біти першого октету завжди дорівнюють 10, 6 біт,

що залишилися, можуть складатися з будь-яких комбінацій нулів і одиниць. Таким чином, найменше число, яке може бути використане для адрес цього класу, дорівнює 10000000 (десяткове 128), і найбільше – 10111111 (десяткове значення рівне 191). Будь-які адреси, що містять у першому октеті числа від 128 до 191, є адресами класу B.

Адреси класу C (рис. 65) – це найчастіше використовуваний клас вихідних адрес, призначений для використання в малих мережах.

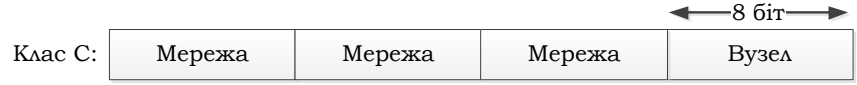


Рис. 65. Адреси класу C

Адреси цього класу починаються із двійкової комбінації 110. Таким чином, найменше доступне число – 11000000 (десяткове 192), а найбільше – 11011111 (десяткове значення 223). Якщо адреса в першому октеті містить числа від 192 до 223, то вона відноситься до класу C.

Адреси класу D (рис. 66) були створені для реалізації в IP-адресах механізму багатоадресного розсилання. Груповою адресою (multicast address) називається унікальна мережева адреса, що використовується для відправлення пакетів, що містять адресу розглянутого класу в полі одержувача, визначеним групами мережевих пристроїв. Таким чином, одна мережева станція може передавати один потік даних декільком одержувачам.

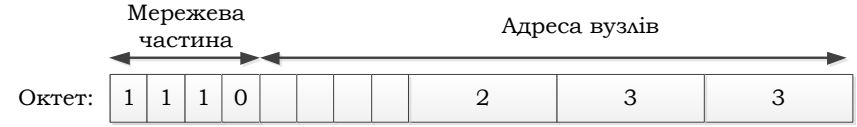


Рис. 66. Адреси класу D

Діапазон адрес класу D так само, як і інших класів, певним чином обмежений. Перші чотири біти адреси класу D повинні бути рівні 1110. Отже, перший октет адрес цього класу може приймати значення від 11100000 до 11101111 або, у десятковому записі, від 224 до 239. Групова IP-адреса, перший октет якого починається із чисел у діапазоні від 224 до 239, є адресою класу D.

Адреси класу E (рис. 67) також були описані в стандартах і виділені в окремий блок. Однак вони були зарезервовані проблемною групою проектування Інтернет (Internet Engineering

Task Force – IETF) для власних дослідницьких потреб. У результаті адреси класу E ніколи не використовувалися в мережі. Перші чотири біти адрес класу E завжди містять 1. Отже, значення першого октету перебуває в діапазоні від 11110000 до 11111111 або від 240 до 255 – у десятковому виді.

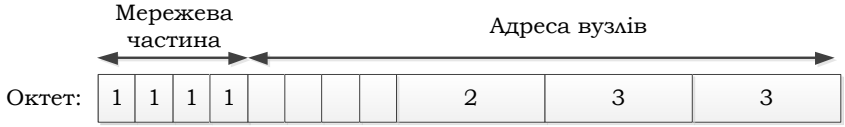


Рис. 67. Адреси класу E

Діапазони значень першого октету в IP-адресах для кожного із класів наведені в табл. 42.

Таблиця 42

Класи IP-адрес: діапазон значень першого октету

Клас IP-адреси	**Діапазон IP-адрес (десяткове число першого октету)**
Клас A	від 1 до 126 (від 00000001 до 01111111)
Клас B	від 128 до 191 (від 10000000 до 10111111)
Клас C	від 192 до 223 (від 11000000 до 11011111)
Клас D	від 224 до 239 (від 11100000 до 11101111)
Клас E	від 240 до 255 (від 11110000 до 11111111)

5.1.5. Зарезервовані IP-адреси

Деякі адреси є зарезервованими і не можуть бути призначені мережевим пристроям. До них відносяться такі:

– мережеві адреси, що ідентифікують саму мережу (рис. 68). Верхній прямокутник на малюнку позначає мережу з адресою 198.150.11.0. Дані, адресовані кожному з вузлів, що перебувають у цій мережі (198.150.11.1 або 198.150.11.254), поза цією мережею виглядають як дані, які відправлено на адресу 198.150.11.0. Адреса вузла береться до уваги тільки тоді, коли пакет з даними потрібно адресувати одержувачу всередині локальної мережі. Нижній прямокутник на малюнку позначає іншу таку ж локальну мережу, але з адресою 198.150.12.0;

– широкомовна (групова) адреса використовується для широкомовного розсилання всім мережевим пристроям (рис. 69). Верхній прямокутник схематично пояснює широкомовну адресу 198.150.11.255. Дані, відправлені за цією адресою, будуть отримані

кожним з вузлів у мережі (від 198.150.11.1 до 198.150.11.254). Нижній прямокутник ілюструє подібну ситуацію для широкомовної адреси 198.150.12.255.

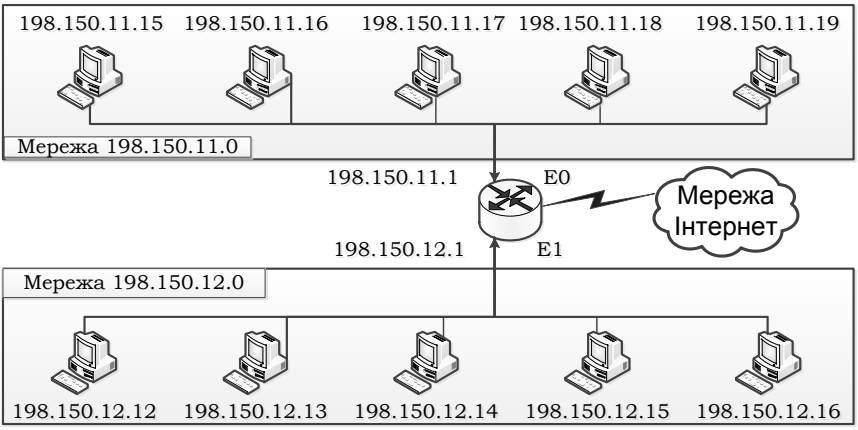


Рис. 68. Адреса мережі

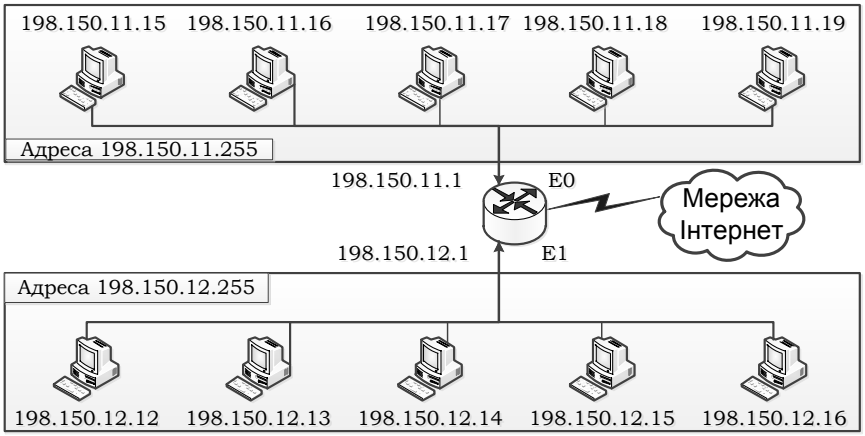


Рис. 69. Широкомовна адреса

IP-адреса, у якої всі біти, відведені під адресу вузла, заповнені нулями, зарезервована під адресу мережі (рис. 70). Показана адреса класу B має нулі в усіх бітах, відведених під адресу вузла. Таким чином, у прикладі для мережі класу A число 113.0.0.0 є адресою мережі, що містить вузол 113.1.2.3. Маршрутизатор використовує IP-

адресу мережі при пересиланні даних через мережу Інтернет. Прикладом для мережі класу B може служити адреса 176.10.0.0, показана на рис. 70.

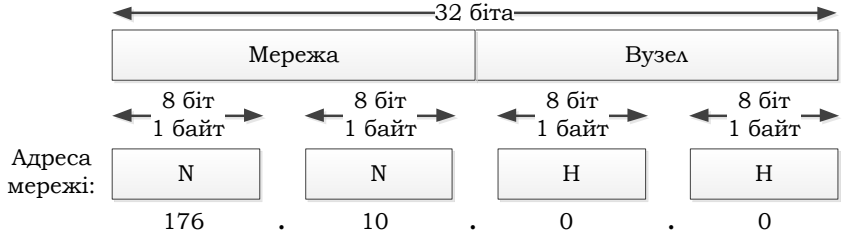


Рис. 70. Структура адреси мережі

Для адреси мережі класу B, записаного у вигляді чисел у крапково-десятковому форматі, перші два октети стандартно ідентифікують мережу. Останні два октети містять нулі, оскільки саме ці 16 біт є тою частиною адреси, яка відведена для ідентифікації підключених до мережі пристроїв. Така адреса називається одноадресатною (unicast), де "uni" позначає "один". Одноадресатна адреса вказує тільки на один вузол у всій мережі. IP-адреса з розглянутого вище прикладу (176.10.0.0) зарезервована у якості адреси мережі й ні за яких умов не може бути використана як адреса підключеного до мережі пристрою. Прикладом IP-адреси мережевого пристрою в мережі 176.10.0.0 може бути 176.10.16.1. У даному прикладі 176.10 є мережевою частиною адреси, а 16.1 – це частина, що визначає вузол.

Для передачі даних усім вузлам у мережі потрібна широкомовна адреса. Широкомовне розсилання використовується, коли відправник пересилає дані всім пристроям у мережі (рис. 71). Адреса класу B, показана на рис. 71, є широкомовною для даної мережі. Коли пакети будуть отримуватися відповідно до широкомовної адреси одержувача, дані будуть оброблені на кожному з комп'ютерів. Щоб бути впевненим у тому, що всі пристрої в мережі одержали й обробили пакети широкомовного розсилання, відправник повинен використовувати спеціальну IP-адресу, яка буде зрозумілою і правильно обробленою іншими пристроями. У широкомовних IP-адресах усі біти, відведені під адресу вузла (поле вузла), дорівнюють одиниці.

Для мережі з адресою 176.10.0.0, у якій останні 16 біт формують

поле вузла (або відведену для вузла частину адреси), адресою широкомовного розсилання, за якою пакети будуть відправлені всім мережевим пристроям, є адреса 176.10.255.255 (оскільки десяткове число 255 відповідає двійковому октету 11111111).

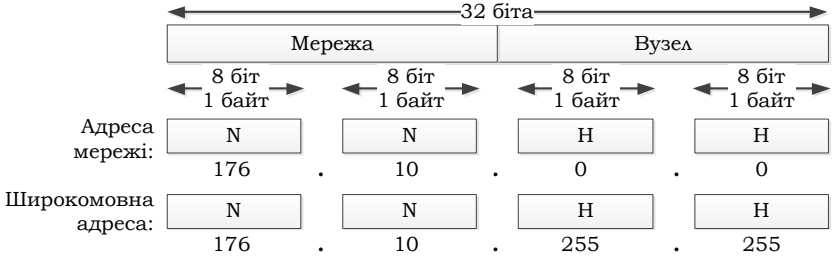


Рис. 71. Широкомовна адреса

5.1.6. Відкриті й приватні адреси

Стабільне функціонування мережі Інтернет залежить від унікальності публічних адрес, що використовуються в мережі. Як показано на рис. 72, при використанні мережевої схеми адресації можуть виникнути деякі проблеми. У проілюстрованій на рисунку структурі обидві мережі мають адресу 198.150.11.0. Коли дані приходять на маршрутизатор, у яку з мереж вони повинні бути спрямовані? Схеми, подібні цій, можуть значно збільшити обсяг мережевого трафіку й зробити неможливим виконання основної функції маршрутизатора; отже, потрібно передбачити, які механізми будуть використані для перевірки унікальності використання адрес. Такі функції спочатку були надані організації Internic (Internet Network Information Center – Інформаційний Центр Інтернет). Зараз функції цієї організації передані Агентству з виділення імен і унікальних параметрів протоколів Інтернет (Internet Assigned Numbers Authority – IANA). Вона ретельно стежить за тим, щоб серед видаваних для публічного використання незадіяних адрес не зустрічалися повторення. Наявність адрес, що дублюються, могла б привести до нестабільності роботи мережі Інтернет і додаткового навантаження на пристрої через доставку пакетів мережам, що використовують ці адреси.

Відкриті IP-адреси унікальні. Не має двох пристроїв з однаковими IP-адресами, які були б підключені до відкритої мережі, оскільки такі адреси використовуються в глобальному масштабі й

відповідають стандарту. Усі комп'ютери, підключені до мережі Інтернет, додержуються такої вимоги. Відкриті IP-адреси повинні виділятися постачальниками послуг Інтернет (Internet Service Provider – ISP) або реєструватися за певну плату.

Унаслідок швидкого росту мережі Інтернет кількість незайнятих IP-адрес зменшується, тому з'являються нові схеми адресації, зокрема *безкласова міждоменна маршрутизація (Classless Interdomain Routing – CIDR)*, покликані допомогти розв'язати проблему вичерпання адресного простору.

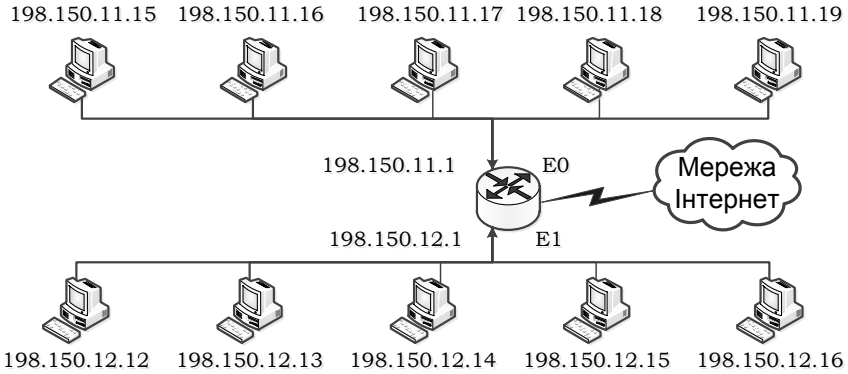


Рис. 72. Унікальність адрес

Щоб частково розв'язати проблему нестачі адресного простору, був розроблений альтернативний варіант використання елементів IP-адрес (табл. 43). Як уже зазначалося, вузли в мережі Інтернет повинні мати глобально унікальні адреси. Однак приватні мережі, не підключені до відкритої мережі, можуть використовувати будь-які дійсні адреси, які повинні бути унікальні тільки всередині локальної мережі. Багато приватних мереж використовуються разом з відкритими, тому використання обраних довільно адрес настійно не рекомендується, оскільки одного разу приватна мережа може виявитися підключеною до глобальної мережі Інтернет.

У специфікації RFC 19184 виділено три блоки IP-адрес (одна адреса класу A, серія адрес класу B і набір адрес класу C) для внутрішнього використання в приватних мережах. Адреси із цих діапазонів не передаються магістральними маршрутизаторами мережі Інтернет, і пакети з адресами із приватних мереж негайно будуть відкинуті такими пристроями.

Таблиця 43

IP-адреси для використання в приватних мережах

Клас IP-адреси	**Діапазон адрес (для внутрішнього використання, RFC 1918)**
Клас A	від 10.0.0.0 до 10.255.255.255
Клас B	від 172.16.0.0 до 176.31.255.255
Клас C	від 192.168.0.0 до 192.168.255.255

У тому випадку, коли потрібно вибрати схему адресації для внутрішньої мережі приватної лабораторії або домашньої мережі, можна використовувати діапазони адрес, перераховані в табл. 43, замість глобально унікальних. Елементи IP-адреси можуть використовуватися разом з публічними для внутрішніх з'єднань, що дозволяє заощаджувати відкриті унікальні адреси.

При підключенні мережі підприємства, у якій використовуються приватні адреси, до мережі Інтернет необхідно забезпечити перетворення приватних адрес у відкриті. Такий процес називається трансляцією мережевих адрес (Network Address Translation – NAT) і зазвичай виконується маршрутизатором.

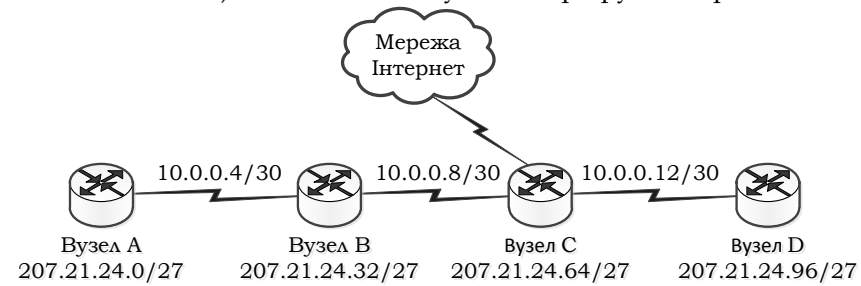


Рис. 73. Використання приватних адрес у розподіленій мережі організації

Лабораторна робота №9 (2 год.)

Тема: Керування IP-адресацією з використанням класів і масок

Мета: навчити студентів управляти IP-адресами та їх діапазонами з використанням класів та масок;

виховувати ціннісне ставлення студентів до майбутньої професійної діяльності.

Студент повинен знати: принципи управління IP-адресацією,

алгоритм використання маски для IP-адреси.

Студент повинен уміти: визначати клас IP-адреси, номер мережі та хосту.

Обладнання: комп'ютерний клас з локальною мережею на основі стандарту Fast Ethernet.

Інструктаж

Завдання 1. Для заданих IP-адрес класів A, B і C, а також запропонованих масок (див. варіанти завдань) визначити:

– клас адреси;

– максимально можливу кількість підмереж, яку можна утворити відповідно до класу IP-адреси;

– кількість підмереж, яку можна утворити відповідно до класу IP-адреси та відповідної маски;

– діапазон зміни адрес підмереж, утворених з використанням маски;

– максимальну кількість вузлів у підмережах, утворених з використанням маски;

Таблиця 44

Варіанти завдання

№ варіанта	Параметр	Значення параметра
1.	Адреса	156.131.183.69
	Маска	11111111.11111111.11111100.00000000
2.	Адреса	99.57.162.1
	Маска	11111111.11111100.00000000.00000000
3.	Адреса	207.112.5.102
	Маска	11111111.11111111.11111111.10000000
4.	Адреса	170.190.200.134
	Маска	11111111.11111111.11111000.00000000
5.	Адреса	167.33.194.104
	Маска	11111111.11111111.11110000.00000000
6.	Адреса	99.15.57.65
	Маска	11111111.11111110.00000000.00000000
7.	Адреса	222.217.166.187
	Маска	11111111.11111111.11111111.11000000
8.	Адреса	173.113.182.243
	Маска	11111111.11111111.11100000.00000000
9.	Адреса	221.5.128.193
	Маска	11111111.11111111.11111111.11100000
10.	Адреса	79.84.191.118

	Маска	11111111.11111111.00000000.00000000
11.	Адреса	196.168.106.38
	Маска	11111111.11111111.11111111.11110000
12.	Адреса	57.234.47.26
	Маска	11111111.11111111.10000000.00000000
13.	Адреса	156.131.229.160
	Маска	11111111.11111111.11000000.00000000
14.	Адреса	74.31.189.243
	Маска	11111111.11111111.11000000.00000000
15.	Адреса	193.83.135.215
	Маска	11111111.11111111.11111111.11111000

Самостійна робота №9

Тема: Мета та стратегія надлишковості в ієрархічних мережах

Мета: розвивати аналітичні вміння студентів з визначення та вибору стратегії надлишковості в ієрархічних мережах.

Студент повинен знати: характеристики та особливості використання різних стратегій надлишковості при проектуванні ієрархічних комп'ютерних мереж.

Студент повинен уміти: обирати та характеризувати стратегію надлишковості в ієрархічній комп'ютерній мережі.

Хід роботи

Теоретична частина

1. Назвіть найбільш важливий фактор, що використовується при ухваленні рішення про використання того або іншого маршруту для досягнення заданого пункту призначення.
2. Назвіть два основних принципи, що повинні бути дотримані при реалізації надлишковості в мережі.
3. Визначте кількість різних маршрутів у базовій мережі, що складається з 25 маршрутизаторів і має структуру з повним об'єднанням.
4. Який метод застосовується в маршрутизаторах для порівняння двох маршрутів, оголошених різними протоколами маршрутизації?

Практична частина

Завдання

1. Законспектуйте основні положення щодо стратегій

надлишковості в ієрархічних мережах.

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Сучасний стан розвитку протоколу IP".

ТЕМА 5.2. ОСОБЛИВОСТІ АДРЕСАЦІЇ В СТЕКУ ПРОТОКОЛІВ TCP/IP

Лекція

План

1. Підмережі
2. Присвоєння IP-адрес
3. Протокол перетворення адрес (ARP)
4. Протокол ICMP

Література

Основна

1. *Компьютеры*, сети, Интернет: Энциклопедия: Наиболее полн. и подроб. рук. / Ю. Новиков, Д. Новиков, А. Черепанов, В. Чуркин; Под общ. ред. Ю. Новикова. – 2. изд. – М. [и др.]: Питер, 2003 (СПб.: ГПП Печ. Двор им. А.М. Горького). – 831 с.: ил.; 24 см.

2. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины,

комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

3. *Олифер В. Г.* Новые технологии и оборудование IP-сетей / Виктор Олифер, Наталья Олифер. – СПб. и др.: BHV, 2000. – 512 с.: ил., табл.; 24 см. – (Мастер) (Современные сетевые технологии).

4. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. – 4-е изд. – М. [и др.]: Питер, 2005. – 991 с.: ил., табл.; 24 см. – (Классика computer science).

Додаткова

1. *Башмаков А. И.* Интеллектуальные информационные технологии: учеб. пособие для студ. вузов, обуч. по направлению подгот. дипломированных спец. "Информатика и вычислительная техника" / А. И. Башмаков, И. А. Башмаков – М. : МГТУ им.Н.Э.Баумана, 2005. – 302 с.

2. *Білоус Л. Ф.* Інформаційні мережі : навч. посібник / Білоус Л. Ф. – К. : Логос, 2005. – 140 с.

3. *Вишневский А.* Сетевые технологии Windows 2000 / Алексей Вишневский. – СПб. и др.: Питер, 2000. – 591 с.: ил., табл.; 24 см. – (Для профессионалов).

4. *Грир Т.* Сети Интернет: Пер. с англ. – М.: ИТД "Русская редакция", 2000. – 368 с.

5. *Ибе О.* Сети и удаленный доступ: Протоколы, проблемы, решения / Оливер Ибе. – М.: ДМК Пресс, 2002. – 332 с.: ил.; 23 см. – (Серия "Защита и администрирование").

6. *Камер Д.Э.* Компьютерные сети и Internet: Разработка приложений для Internet (пер. с англ. Птицына К.А.) Изд. 3-е + CD-Rom – 640 с.

7. *Коваленко А. Є.* Корпоративні комп'ютерні мережі та телекомунікації : конспект лекцій для студ. спец. 7.080401 "Інформаційні управляючі системи та технології" ден. форми навч. / Анатолій Єпіфанович Коваленко. – К. : НУХТ, 2004. – 27 с.

8. *Контроль* та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології : навчальний посібник / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. –

Х. : "Компанія СМІТ", 2004. – 544 с.

5.2.1. Підмережі

Ще одним способом економії IP-адрес є механізм використання підмереж (subnetting). Цей метод дозволяє розбивати повні класові блоки мережевих адрес на менші й допомагає уникнути повного вичерпання IP-адрес. На рис. 74 показана мережа класу B (131.108.0.0), розбита на три підмережі. Кожний мережевий адміністратор повинен розуміти механізм створення підмереж як спосіб розподілу й ідентифікації окремих мереж усередині локальної мережі. Невеликі мережі потрібно розбивати на більш дрібні досить рідко, але в разі використання великих блоків адрес і дуже великих мереж такий розподіл необхідний. Згідно з визначенням створення в мережі підмереж означає використання маски підмережі для поділу її на більш дрібні, більш ефективні, легко керовані сегменти, як показано на рис. 75.

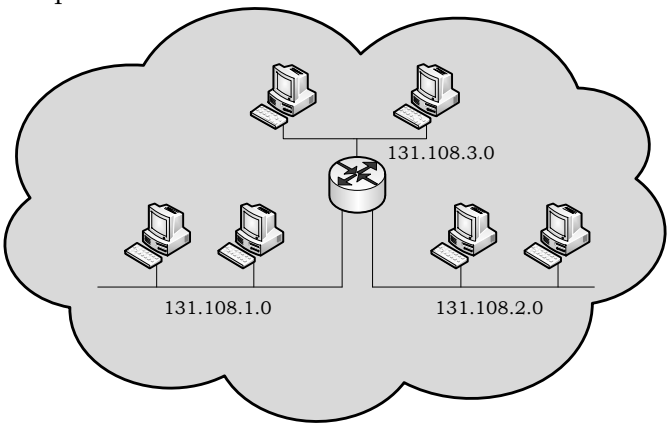


Рис. 74. Схема адресації з використанням підмереж

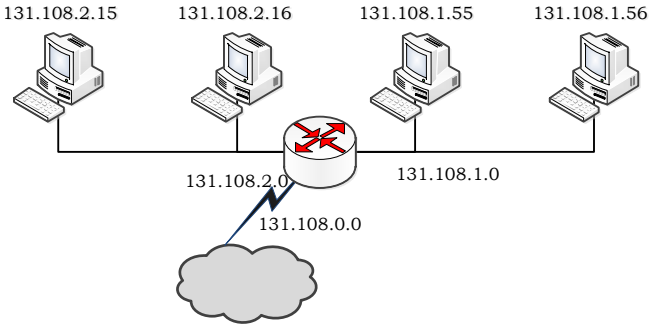


Рис. 75. Адреси підмереж

Системний адміністратор повинен уміти розв'язувати проблеми, що виникають при додаванні нових сегментів в інфраструктуру й розширення мережі. Найбільш важливе питання, на яке необхідно дати відповідь, пов'язано з визначенням потрібної кількості підмереж і припустимою кількістю вузлів, які можуть входити в кожну з отриманих у процесі розбивки мереж. Завдяки використанню механізму підмереж можна створити гнучку структуру мережі, яка не буде обмежуватися масками або рамками стандартних мереж класів A, B и C.

Адреси підмереж складаються з мережевої частини класів A, B або C, полів підмережі й поля адреси вузла. Зазначені поля формуються з вихідної адреси всієї мережі. Уміння визначити, яким чином розділити вихідне поле адреси вузла на поля адреси підмережі й адреси вузла, дає мережевим адміністраторам певну волю при виборі схеми адресації.

Щоб створити підмережу, мережевий адміністратор запозичує біти з поля адрес вузлів вихідної адреси всієї мережі й призначає їх як адреси підмережі (табл. 45). Мінімальна кількість запозичених біт - два. Якщо використовувати всього один біт, то після розбивки буде отримана тільки одна мережева адреса (.0 – адреса мережі) і один широкомовний (.255). Максимальне число біт, які дозволено запозичити, може бути довільним (у рамках максимальної довжини вузлової частини адреси), за умови, що залишаться незадіяними не менше двох біт для адрес вузлів. У табл. 45 показано, що для мережі класу C може бути запозичено не більше 6 біт з поля адреси вузла для створення підмережі.

Таблиця 45

Адреси підмереж

Перший октет адреси вузла у десятковій нотації	Кількість підмереж	Кількість вузлів класу А в кожній підмережі	Кількість вузлів класу В у кожній підмережі	Кількість вузлів класу С у кожній підмережі
.192	2	4194302	16382	62
.224	6	2097150	8190	30
.240	14	1048574	4094	14
.248	30	524286	2046	6
.252	62	262142	1022	2
.254	126	131070	510	
.255	254	65534	254	

Використання масок для виділення підмереж. Часто адміністратори мереж зазнають незручності, через те, що кількість централізовано виділених їм номерів мереж недостатня для того, щоб структурувати мережу належним чином, наприклад, розмістити по різних мережах усі комп'ютери, що слабо взаємодіють.

У такій ситуації можливі два шляхи. Перший з них пов'язаний з одержанням від NIC додаткових номерів мереж. Другий спосіб, що застосовується більш частіше, пов'язаний з використанням так званих масок, які дозволяють розділяти одну мережу на кілька мереж.

Маска – це число, двійковий запис якого містить одиниці в тих розрядах, які повинні інтерпретуватися як номер мережі.

Наприклад, для стандартних класів мереж маски мають такі значення:

– 255.0.0.0 – маска для мережі класу А,
– 255.255.0.0 – маска для мережі класу В,
– 255.255.255.0 – маска для мережі класу С.

У масках, які використовує адміністратор для збільшення кількості мереж, кількість одиниць у послідовності, що визначає границю номера мережі, не обов'язково повинна бути кратною 8, щоб здійснити розподіл адреси на байти.

Розглянемо приклад. Нехай маска має значення 255.255.192.0 (11111111.11111111.11000000.00000000), і мережа має номер 129.44.0.0 (10000001 00101100 00000000 00000000), з якого видно, що вона належить до класу В. Після накладення маски на цю адресу кількість розрядів, що визначаються як номер мережі, збільшилося з 16 до 18, тобто адміністратор одержав можливість використати замість одного,

централізовано заданого йому номера мережі, чотири:

129.44.0.0 (10000001 00101100 00000000 00000000)
129.44.64.0 (10000001 00101100 01000000 00000000)
129.44.128.0 (10000001 00101100 10000000 00000000)
129.44.192.0 (10000001 00101100 11000000 00000000)

Наприклад, IP-адреса 129.44.141.15 (10000001 00101100 10001101 00001111), що за стандартами IP задає номер мережі 129.44.0.0 і номер вузла 0.0.141.15, тепер, при використанні маски, буде інтерпретуватися як пара: 129.44.128.0 – номер мережі, 0.0.13.15 – номер вузла.

Таким чином, установивши нове значення маски, можна змусити маршрутизатор інакше інтерпретувати IP-адресу. При цьому два додаткових останніх біти номера мережі часто інтерпретуються як номер підмережі.

Приклад. Нехай деяка мережа належить до класу B і має адресу 128.10.0.0. Ця адреса використовується маршрутизатором, що з'єднує мережу з іншою частиною інтермережі. І нехай серед всіх станцій мережі є станції, що погано взаємодіють між собою. Їх бажано було б ізолювати в різних мережах. Для цього мережу можна розділити на дві підмережі, підключивши їх до відповідних портів маршрутизатора, і задати для цих портів маску, наприклад, число 255.255.255.0, тобто організувати всередині вихідної мережі із централізовано заданим номером – дві підмережі класу C (можна було б вибрати й інший розмір для поля адреси підмережі). Ззовні мережа, як і раніше, буде виглядати як єдина мережа класу B, а на місцевому рівні це будуть дві окремі мережі класу C. Зовнішній загальний трафік буде розділятися місцевим маршрутизатором між підмережами.

Розглянемо приклад використання безкласової моделі (CIDR). Припустимо, у локальній мережі підключеній до Інтернет, перебуває 2000 комп'ютерів. Кожному з них потрібно видати IP-адресу. Для одержання необхідного адресного простору потрібні або 8 мереж класу C, або одна мережа класу B. Мережа класу B вміщає 65534 адреси, що набагато більше необхідної кількості. При загальному дефіциті IP-адрес таке використання мереж класу B марне. Однак якщо ми будемо використовувати 8 мереж класу C, виникне така проблема: кожна така IP-мережа повинна бути представлена окремим рядком у таблицях маршрутів на маршрутизаторах, тому що з погляду маршрутизаторів – це 8 абсолютно не зв'язаних між

собою мереж, маршрутизація дейтаграм здійснюється незалежно, хоча фактично ці IP-мережі й розташовані в одній фізичній локальній мережі й маршрути до них ідентичні. Таким чином, заощаджуючи адресний простір, ми багаторазово збільшуємо службовий трафік у мережі й витрати з підтримки й обробки маршрутних таблиць.

З іншого боку, немає ніяких формальних причин проводити границю мережа-хост в IP-адресі саме по межі октету. Це було зроблено винятково для зручності подання IP-адрес і розбивки їх на класи. Якщо вибрати довжину мережної частини в 21 біт, а на номер хоста відвести, відповідно, 11 біт, ми одержимо мережу, адресний простір якої містить 2046 IP-адрес, що максимально точно відповідає поставленій вимозі. Це буде одна мережа, обумовлена своїм унікальним 21-бітним номером, отже, для її обслуговування буде потрібно тільки один запис у таблиці маршрутів.

Залишилося розв'язати проблему: як визначити, що на мережну частину відведений 21 біт? У разі класової моделі старші біти IP-адреси визначали приналежність цієї адреси до того або іншого класу й, отже, кількість біт, відведених на номер мережі.

У випадку адресації поза класами, з довільним положенням межі мережа-хост усередині IP-адреси, до IP-адреси додається 32-бітова маска.

Описана вище модель адресації називається безкласовою (CIDR – Classless Internet Direct Routing, пряма безкласова маршрутизація в Інтернет). Сьогодні класова модель вважається застарілою, і маршрутизація, і (здебільшого) видача блоків IP-адрес здійснюються за моделлю CIDR, хоча класи мереж ще міцно втримуються в термінології.

Запис адрес у безкласовій моделі. Для зручності запису IP-адреса в моделі CIDR часто представляється у вигляді a.b.c.d / n, де a.b.c.d – IP адреса, n – кількість біт у мережевій частині.

Приклад: 137.158.128.0/17.

Маска мережі для цієї адреси: 17 одиниць (мережева частина), за ними 15 нулів (хостова частина), що в октетному поданні дорівнює

11111111.11111111.10000000.00000000 = 255.255.128.0.

Представивши IP-адресу у двійковому виді й побітно помноживши її на маску мережі, ми одержимо номер мережі (усі нулі в хостовій частині). Номер хоста в цій мережі ми можемо одержати, побітно помноживши IP-адресу на інвертовану маску

мережі.

Приклад: IP = 205.37. 193. 134/26 або, що те ж, IP = 205.37. 193. 134 netmask = 255.255.255.192.

Розпишемо у двійковому виді:

IP = 11001101 00100101 11000111 10000110 маска = 11111111 11111111 11111111 11000000

Помноживши побітно, одержуємо номер мережі (у хостовій частини – нулі):

network = 11001101 00100101 11000111 10000000

або, в октетному поданні, 205.37.193.128/26, або, що теж саме, 205.37.193.128 netmask 255.255.255.192.

Хостова частина розглянутої IP адреси дорівнює 000110, або 6. Таким чином, 205.37.193.134/26 адресує хост номер 6 у мережі 205.37.193.128/26. У класовій моделі адреса 205.37.193.134 визначила би хост 134 у мережі класу C 205.37.193.0, однак зазначення маски мережі (або кількості біт у мережевій частині) однозначно визначає приналежність адреси до безкласової моделі.

Очевидно, що мережі класів A, B, C у безкласової моделі представляються за допомогою масок, відповідно, 255.0.0.0 (або /8), 255.255.0.0 (або /16) і 255.255.255.0 (або /24).

5.2.2. Присвоєння IP-адрес

Розглянемо, як мережевим пристроям привласнюються IP-адреси. Для нормального функціонування мережі IP-адреси повинні призначатися відповідно до певної ієрархії. IP-адреси можуть виділятися статично або динамічно, обидва варіанти присвоєння адрес розглянуті нижче.

Одержання Інтернет-Адреси

Щоб вузол міг функціонувати в мережі Інтернет, йому необхідно привласнити глобально унікальну адресу. Фізична, або MAC адреса (Media Access Control – адреса протоколу керування доступом до передавального середовища) важлива тільки для локальної взаємодії. Це означає, що за допомогою такої адреси вузол може бути ідентифікований тільки в межах його власної локальної мережі, і адреса не має ніякого значення для пристроїв, не розташованих у ній.

IP – це найпоширеніша схема адресації. Вона є ієрархічною й дозволяє окремим адресам бути асоційованими з групами інших. Подібні групи дозволяють організовувати ефективну передачу

інформації в мережі Інтернет.

Існують два методи призначення IP-адрес – *статична адресація (static addressing)* і *динамічна (dynamic addressing)*. Незалежно від обраної схеми не можуть існувати два інтерфейси з однаковими адресами, оскільки подібна ситуація може привести до конфлікту, у якому жоден із залучених у нього вузлів не зможе нормально функціонувати.

Статичне призначення IP-адрес

Коли IP-адреси розподіляються статично, кожний пристрій зобов'язаний мати свою адресу. Операційні системи по-різному конфігурують стек протоколів TCP/IP. При використанні цього методу необхідно зберігати записи про призначені IP-адреси, оскільки використання адрес, що дублюються, може викликати проблеми в роботі мережі. Деякі операційні системи розсилають ARP запити, перевіряючи унікальність призначених адрес при спробі ініціалізації засобів стеку TCP/IP. Якщо виявлене дублювання, протокол ініціалізований не буде, що викличе відповідне повідомлення про помилку. Не всі операційні системи ідентифікують адреси, що дублюються. Ця особливість підкреслює необхідність мати докладні записи про адресацію пристроїв.

Основною причиною, з якої пристроєм може бути виділена постійна адреса, є необхідність надати іншим пристроям можливість посилатися на нього. Гарним прикладом може служити Web-сервер. Якби Web-сервер щораз при запуску одержував нову IP-адресу, його було б складно знайти. Як наочний приклад того, до чого можуть привести подібні зміни адреси, можна уявити собі ситуацію, коли в місті постійно міняються назви вулиць і адреси будинків. Пошук потрібного будинку стане неможливим, оскільки жодна карта не буде відповідати дійсності. Якщо потрібний будинок неможливо знайти, люди перестануть навіть намагатися його шукати.

Пристрої певного типу потребують використання статичних IP-адрес. Web-сервери, мережеві принтери, сервери додатків і маршрутизатори є прикладами пристроїв, що вимагають для своєї роботи постійних IP-адрес.

Призначення IP-адрес за протоколом RARP

Протокол визначення мережевої адреси за місцем розташування вузла (Reverse Address Resolution Protocol – RARP) встановлює відповідність між MAC адресами й IP-адресами. Така

прив'язка дозволяє деяким мережевим пристроям інкапсулювати дані до їхнього відправлення через мережу. Можлива ситуація, коли мережевому пристрою або робочій станції відома MAC адреса, але не відома власна IP-адреса. Для пристроїв, що використовують протокол RARP, потрібен RARP сервера, як показано на рис. 76.

Розглянемо приклад, у якому пристрій-відправник передає дані деякому пристрою. Відправник знає MAC-адресу одержувача, але не може знайти власну IP-адресу в ARP таблиці. З іншого боку, пристрої одержувача, щоб прийняти дані, передати їхнім протоколам верхнього рівня моделі OSI і відповісти відправнику, повинні бути відомі як MAC, так і IP-адреси відправника. По цьому відправник ініціює процес, називаний RARP запитом, який допоможе визначити йому свою IP-адресу. Пристрій створює пакет RARP запиту і відправляє його через мережу. Для того щоб усі пристрої в мережі могли одержати пакети RARP запиту, використовується широкомовна MAC адреса.

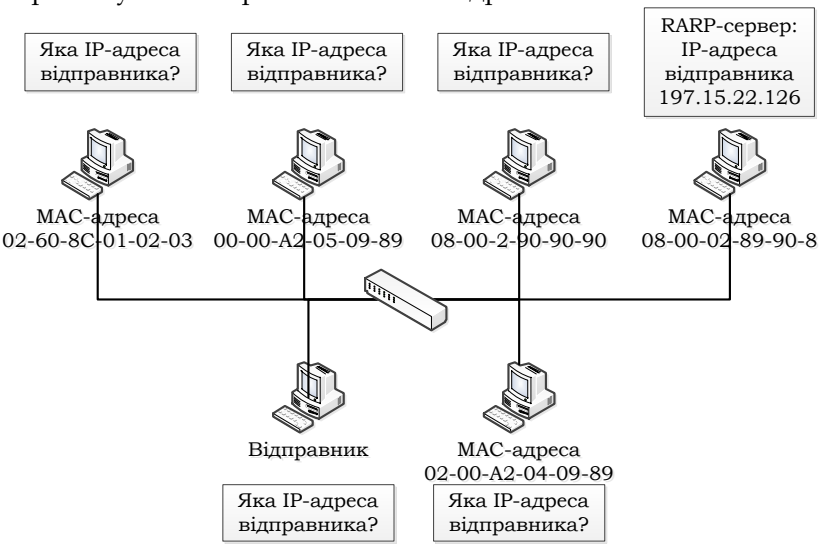


Рис. 76. Схема роботи протоколу RARP

Протокол RARP використовує той же формат пакета, що й протокол ARP. Однак значення MAC заголовка й коду операції для RARP запиту відрізняються від аналогічних полів ARP запиту. Формат пакета RARP містить позиції для MAC адрес відправника й

одержувача, поле IP-адреси відправника порожнє. Широкомовний запит адресується всім абонентам у мережі, для цього адреса одержувача складається з одних одиниць. Станція, що використовує протокол RARP, містить у своєму ПЗУ програмний код, який запускає процес пошуку адреси RARP (рис. 76).

Виділення адрес за допомогою протоколу DHCP

Протокол динамічної конфігурації вузла (Dynamic Host Configuration Protocol – DHCP) є спадкоємцем протоколу BOOTP. На відміну від останнього, протокол DHCP дозволяє динамічно одержати IP-адресу, не прибігаючи до створювання адміністратором профілів для кожної конкретної машини. Усе, що потрібно, це визначити діапазон доступних адрес на DHCP сервері. Вузли, що з'єднуються з мережею, підключаються до DHCP сервера й запитують необхідні їм IP-адреси. Сервер обирає одну з незайнятих адрес і виділяє її вузлу. За допомогою протоколу DHCP уся необхідна інформація про конфігурацію протоколу TCP/IP може бути передана клієнту в одному повідомленні. Вона включає всі відомості, які може передавати протокол BOOTP, плюс виділену IP-адресу й маску підмережі.

Основна перевага протоколу DHCP полягає в тому, що він дає користувачам мобільність. Вони можуть вільно переміщатися з місця на місце, міняючи точку підключення до мережі. При використанні сервера DHCP більше немає необхідності в створенні твердих профілів для кожного мережевого пристрою. Така гнучкість досягається завдяки тому, що протокол DHCP може виділяти IP-адресу одному пристрою, а після його звільнення – передавати іншому. Такий механізм роботи означає, що для IP-адрес виконується відношення "один до багатьох" і, отже, адреса може бути доступною будь-якому пристрою, підключеному до мережі.

Повідомлення й стан протоколу DHCP. Протокол DHCP використовує той же формат повідомлення, що й BOOTP, але з декількома винятками (рис. 77). Поле, яке не використовується в механізмі BOOTP, у цьому протоколі зарезервоване в якості поля прапора. Найбільш значимим бітом є прапор: він задає широкомовне повідомлення. Протокол DHCP, як і BOOTP, зберігає інформацію, що задається виробником:

– однобайтове поле опцій;
– однобайтове поле довжини;

– поле змінної довжини (задається в полі довжини) даних, опції.

Для різних типів Dhcp-повідомлень припустимі такі значення:

– число 53 у полі опцій указує на DHCP-повідомлення;

– одиниця в значенні довжини поля вказує на те, що поле даних має довжину 1 байт.

У процесі завантаження DHCP-клієнт входить у режим ініціалізації. Він посилає широкомовне повідомлення DHCPDISCOVER, що є UDP-пакетом, з номером порту, таким же, як у протоколі BOOTP. Після відправлення пакетів DHCPDISCOVER клієнт переходить у режим прослуховування відповідей DHCPOFFER від сервера й вибору сервера. Клієнт обробляє першу отриману відповідь і починає процедуру утвердження часу дії обраної адреси, відправляючи DHCP-серверу пакет DHCPREQUEST. На наступному етапі сервер підтверджує запит клієнта за допомогою пакета DHCPACK. Після цього клієнт переходить у так званий зв'язаний стан і може починати використання виділеної йому Ip-адреси. На рис. 78 проілюстрована узагальнена інформація про Dhcp-режими.

0 7 біти	**8 15 біти**	**16 24 біти**	**25 31 біти**
Op (1)	Htype (1)	Hlen (1)	Hops (1)
Xid (4 байтів)			
Секунди (2 байта)		Прапори (2 байта)	
Ciaddr (4 байта)			
Yiaddr (4 байта)			
Siaddr (4 байта)			
Giaddr (4 байта)			
Chaddr (16 байтів)			
Ім'я сервера (32 байта)			
Ім'я завантажувального файлу (64 байта)			
Область, що залежить від виробника (32 байта)			

Рис. 77. Структура DHCP повідомлення

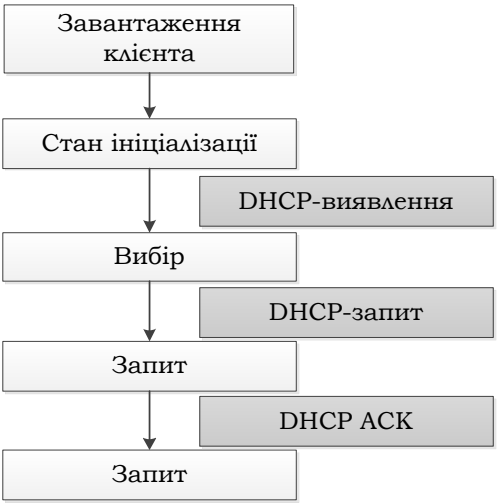


Рис. 78. Режими протоколу DHCP

Проблеми при визначенні адрес

Однією з основних проблем мережевих технологій є питання про те, як організувати взаємодію між мережевими пристроями. У TCP/IP взаємодіях дейтаграма в локальній мережі має містити як MAC-адресу, так і IP-адресу одержувача. На рис. 79 комп'ютер з адресою 176.10.16.1 прагне передати інформацію комп'ютеру з адресою 176.10.16.4. Як же він одержує необхідну для такого обміну даними MAC-адресу?

Усі адреси повинні бути коректними й точно відповідати MAC і IP-адресі вузла, а якщо ні, то одержувач просто відкине неправильні пакети. Таким чином, у локальній мережі повинен існувати механізм автоматичного перетворення (або трансляції) IP-адрес в адреси фізичного рівня – MAC. Виконати таке завдання вручну було б для користувачів обтяжливо й вимагало б багато часу. Такий розв'язок застосовний тільки для локальних мереж; у випадку, коли дані адресуються за межі локальної мережі, виникають нові проблеми.

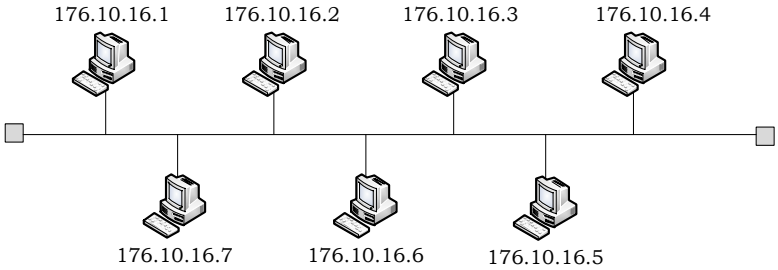


Рис. 79. Проблеми перетворення адрес

При взаємодії із пристроями, що не перебувають у локальному мережевому сегменті, виникають два питання:

– як одержати MAC-адреси проміжних пристроїв;

– як передавати пакети з даними з одного мережевого сегмента в інший доти, поки вони не дійдуть до одержувача.

Приклад, наведений на рис. 80, служить ілюстрацією такої проблеми. Комп'ютеру з адресою 192.168.10.34 необхідно передати інформацію іншому комп'ютеру з адресою 192.168.1.1. Яким чином він може одержати MAC-адресу для IP-адреси 192.168.1.1? Варто пам'ятати, що MAC-адреса може бути використана тільки в межах локальної мережі. Від неї буде мало користі поза мережею з адресою 192.168.10.0. Виходить, для того щоб передати дані з локальної мережі в мережу глобальну, необхідно знати MAC-адресу маршрутизатора.

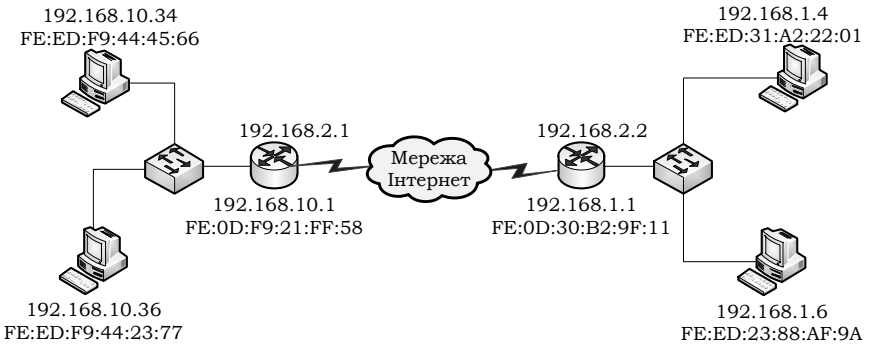


Рис. 80. Проблеми перетворення адрес

5.2.3. Протокол перетворення адрес (ARP)

Для взаємодії пристроїв необхідно, щоб у передавального пристрою були IP- і MAC-адреси одержувача. Коли один із пристроїв намагається встановити зв'язок з іншим, з відомою IP-адресою, йому необхідно визначити MAC-адресу одержувача. Набір протоколів TCP/IP має у своєму складі спеціальний протокол, що має назву ARP (Address Resolution Protocol – протокол перетворення адрес), який дозволяє автоматично одержати MAC-адресу. На рис. 81 проілюстрований процес, що дозволяє визначити MAC-адресу, пов'язану з відомою IP-адресою.

Деякі пристрої зберігають спеціальні ARP-таблиці, у яких утримується інформація про MAC- і IP-адреси інших пристроїв, підключених до тієї ж локальної мережі. ARP таблиці дозволяють установити однозначну відповідність між IP і MAC адресами. Такі таблиці зберігаються в певних областях оперативної пам'яті й обслуговуються автоматично на кожному з мережевих пристроїв (табл. 46 і 47). У рідких випадках доводиться створювати ARP-таблиці вручну. Зверніть увагу, що кожний комп'ютер у мережі підтримує свою власну ARP таблицю.

Таблиця 46

Запис в ARP таблиці

Інтернет адреса	Фізична адреса	Тип
68.2.168.1	00 50 57 00 76 84	Динамічний

Таблиця 47

ARP таблиця для адреси 198.150.11.36

MAC адреса	IP-адреса
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:AB:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36

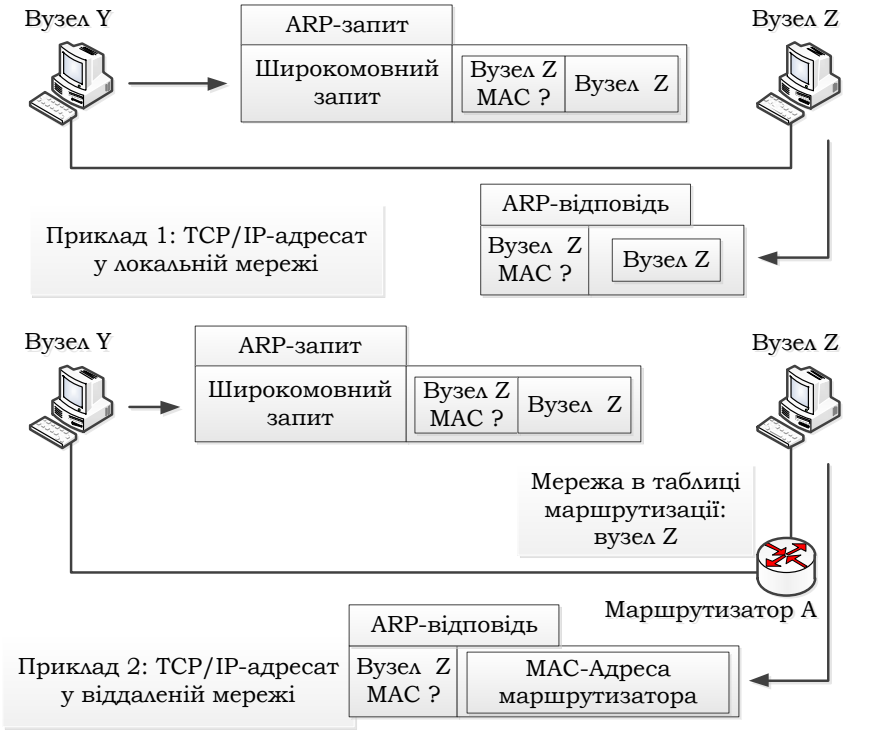


Рис. 81. Одержання IP-адрес через MAC-адреси

Куди б не передавалися мережевим пристроєм дані, для їхнього пересилання завжди використовується інформація, що зберігається в ARP-таблиці.

Функціонування протоколу ARP у підмережах. Для передачі даних від одного вузла до іншого відправник повинен знати IP і MAC-адреси одержувача. Якщо він не може одержати шукану фізичну адресу із власної ARP-таблиці, ініціюється процес, що називається ARP-запитом.

ARP-запит дозволяє вузлу визначити MAC-адресу одержувача. Вузол створює фрейм ARP-запиту й розсилає його всім мережевим пристроям. Фрейм ARP-запиту складається із двох частин:

– заголовка фрейму;
– повідомлення ARP-запиту.

Для того, щоб усі пристрої могли одержати ARP-запит, використовується широкомовна MAC-адреса. У схемі MAC-адресації

широкомовна адреса містить у всіх бітах шістнадцяткове число F і має такий вигляд FF FF FF FF FF FF. Оскільки пакети ARP-запиту передаються в широкомовному режимі, усі мережеві пристрої, підключені до локальної мережі, можуть одержати такі пакети й передати їх протоколам більш високих рівнів для подальшої обробки. Якщо IP-адреса пристрою збігається з IP-адресою одержувача в широкомовному ARP-запиті, цей пристрій відповідає відправнику, повідомляючи свою MAC-адресу. Таке повідомлення називається ARP-відповіддю.

Після одержання ARP-відповіді пристрій відправник широкомовного ARP-запиту витягає MAC-адресу з поля апаратної адреси відправника й оновлює свою ARP-таблицю. Тепер цей пристрій може належним чином адресувати пакети, використовуючи як MAC, так і IP-адреси. Отримана інформація використовується для інкапсуляції даних на другому й третьому рівнях перед їх відправленням мережею. Коли дані досягають пункту призначення, на канальному рівні проводиться перевірка на відповідність адреси, відкидається канальний заголовок, який містить MAC-адреси, і дані передаються на мережевий рівень. На мережевому рівні перевіряється відповідність власної IP-адреси й IP-адреси одержувача, що міститься в заголовку третього рівня. На мережевому рівні відкидається IP-заголовок, і інкапсульовані дані передаються на наступний рівень моделі OSI – транспортний (рівень 4). Подібний процес повторюється доти, поки частково розпаковані дані, що залишилися, не досягнуть програми (рівень 7), у якій буде прочитана користувацька частина даних.

5.2.4. Протокол ICMP

Протокол ICMP (Internet Control Message Protocol – протокол керуючих повідомлень Інтернет виконує такі завдання:

– повідомляє вузлу-джерелу про відмови маршрутизації;

– перевіряє спроможності вузлів утворювати повторну луну в об'єднаній мережі (повідомлення Echo і Reply ICMP);

– стимулює більш ефективну маршрутизацію (за допомогою повідомлень Redirect ICMP – переадресації ICMP);

– інформує вузол-джерело про те, що деяка дейтаграма перевищила призначене їй час існування в межах певної мережі (повідомлення Time Exceeded ICMP – "час перевищений");

– забезпечує новим вузлам можливість знаходження маски підмережі, що використовується в об'єднаній мережі в цей момент.

Протокол ICMP є невід'ємною частиною IP-модуля. Він забезпечує зворотний зв'язок у вигляді діагностичних повідомлень, що посилають відправнику при неможливості доставки його дейтаграми й в інших випадках.

ICMP-повідомлення не породжуються при неможливості доставки:

– дейтаграм, що містять ICMP-повідомлення;

– не перших фрагментів дейтаграм;

– дейтаграм, спрямованих по груповій адресі (широкомовлення, мультикастинг);

– дейтаграм, адреса відправника яких нульова або групова, усі ICMP-повідомлення мають IP-заголовок, значення поля "Protocol" дорівнює 1.

Такі дейтаграми з ICMP-повідомленням не передаються вверх по стеку протоколів для обробки, а обробляються IP-модулем.

Після IP-заголовка слідує 32-бітне слово з полями "Тип", "Код" і "Контрольна сума". Поля типу й коду визначають зміст ICMP-повідомлення. Формат іншої частини дейтаграми залежить від виду повідомлення. Контрольна сума рахується так само, як і в IP-заголовку, але в цьому випадку підсумовується вміст ICMP-повідомлення, включаючи поля "Тип" і "Код".

Лабораторна робота №10 (2 год.)
Тема: Управління адресами підмереж

Мета: сформувати уміння управляти адресами підмереж, здійснювати розрахунок номеру підмережі спираючись на її маску;

виховувати ціннісне ставлення студентів до навчальної діяльності.

Студент повинен знати: призначення маски підмережі, властивості IP-адреси.

Студент повинен уміти: здійснювати управління адресами підмереж з використання маски.

Хід роботи

Інструктаж

Завдання 1. Відповідно до заданих класів (A, B або C), кількості підмереж N і максимальній кількості комп'ютерів M1..MN у кожній

підмережі визначити *маску* для розбиття на підмережі. Зробити висновок про можливість такого розбиття. Якщо розбиття неможливе, сформулювати рекомендації зі зміни початкових даних для забезпечення можливості розбиття.

Таблиця 48

Варіанти завдання

№ варіанта	Параметр	Значення параметра				
1.	Клас	A				
	N	3				
	M1...MN	1568	55996	1555847	512	256
2.	Клас	B				
	N	4				
	M1...MN	1024	2048	4069	512	256
3.	Клас	C				
	N	8				
	M1...MN	12	10	5	8	15
4.	Клас	A				
	N	9				
	M1...MN	4096	1024	1044096	4096	1051448
5.	Клас	B				
	N	7				
	M1...MN	512	128	256	1024	2048
6.	Клас	C				
	N	3				
	M1...MN	8	16	31	64	4
7.	Клас	A				
	N	8				
	M1...MN	4096	1045448	4096	1024	8192
8.	Клас	B				
	N	4				
	M1...MN	1024	512	4094	8190	16
9.	Клас	C				
	N	2				
	M1...MN	30	60	2	4	16
10.	Клас	A				
	N	10				
	M1...MN	512	8192	4096	1044096	1024
11.	Клас	B				

	N	6				
	M1...MN	1024	2048	4069	512	8191
12.	Клас	C				
	N	8				
	M1...MN	8	14	11	5	6
13.	Клас	A				
	N	8				
	M1...MN	4096	1045448	8192	1024	556258
14.	Клас	B				
	N	7				
	M1...MN	512	128	256	1024	2048
15.	Клас	A				
	N	10				
	M1...MN	512	1044096	1024	4096	8192

Завдання 2. Визначити максимальну довжину маски мережі та її адресу, щоб зазначені IP-адреси перебували в одній мережі.

Варіанти завдання

Варіант 1

221.220.88.73 – 223.222.74.206
32.102.0.46 – 32.102.0.47
102.244.10.49 – 102.244.10.26
235.41.199.239 – 235.41.41.139

Варіант 2

251.252.230.152 – 251.250.29.97
54.134.17.147 – 54.10.33.193
162.235.231.229 – 160.93.14.253
18.10.124.128 – 18.10.124.169

Варіант 3

99.149.26.16 – 99.149.26.16
199.225.66.216 – 199.225.66.247
250.54.84.49 – 214.7.75.249
149.182.180.56 – 151.66.167.26

Варіант 4

231.81.216.237 – 231.81.212.30
177.77.34.213 – 191.35.196.43
115.115.32.253 – 114.14.56.227
62.225.77.124 – 62.225.76.103

Варіант 5

184.155.179.54 – 184.155.66.71
251.106.185.206 – 251.126.234.156
246.168.67.154 – 246.169.9.220
48.107.202.223 – 48.107.203.56

Варіант 6

23.115.247.150 – 23.48.37.248
95.129.111.1 – 95.129.111.3
207.234.120.181 – 207.234.120.181
38.23.81.102 – 38.127.45.239

Варіант 7

150.27.130.246 – 150.18.140.87
166.220.34.180 – 166.220.34.183
51.79.155.111 – 51.75.182.175
112.56.206.224 – 112.56.202.104

Варіант 8

236.74.83.193 – 236.75.195.217
12.95.127.35 – 12.131.135.175
123.157.136.13 – 123.165.203.131
196.200.12.115 – 196.200.12.116

Варіант 9

91.1.129.158 – 91.1.172.242
220.225.247.23 – 220.225.71.91
5.35.95.106 – 9.58.248.150
226.4.22.186 – 226.163.205.38

Варіант 10

159.218.202.36 – 159.218.156.20
141.85.107.17 – 141.85.107.97
247.242.52.247 – 247.66.88.19
2.57.42.80 – 2.56.92.124

Варіант 11

120.149.163.181 – 120.186.35.7
41.0.254.221 – 47.86.238.81
179.76.216.76 – 179.76.216.76
0.42.239.218 – 19.83.23.66

Варіант 12

182.133.171.215 – 182.133.221.50
122.186.87.171 – 122.186.87.170

11.204.240.150 – 11.204.240.222
225.185.154.217 – 225.185.154.208

Варіант 13

226.61.98.224 – 226.61.18.215
24.173.207.45 – 24.177.233.169
35.115.185.74 – 35.113.230.137
208.114.254.251 – 208.114.254.203

Варіант 14

221.220.88.73 – 223.222.74.206
32.102.0.46 – 32.102.0.47
162.235.231.229 – 160.93.14.253
18.10.124.128 – 18.10.124.169

Варіант 15

99.149.26.16 – 99.149.26.16
199.225.66.216 – 199.225.66.247
115.115.32.253 – 114.14.56.227
62.225.77.124 – 62.225.76.103

Самостійна робота №10

Тема: Надлишковість, що реалізується на рівні ядра ієрархічної мережі

Мета: розвивати у студентів уміння проектувати реалізацію надлишковості на рівні ядра в ієрархічних комп'ютерних мережах.

Студент повинен знати: підходи до реалізації надлишковості на рівні ядра в ієрархічних мереж.

Студент повинен уміти: реалізовувати надлишковість на рівні ядра при проектуванні ієрархічної комп'ютерної мережі.

Хід роботи

Теоретична частина

1. Чому реалізація надмірності на рівні ядра ієрархічної мережі простіше реалізації надмірності на рівні розподілу й доступу?
2. Назвіть найбільш природний спосіб реалізації надмірності на рівні ядра в разі розміщення всіх базових маршрутизаторів мережі в одному будинку.
3. Скільки каналів передачі інформації повинно бути ушкоджено для ізоляції принаймні однієї ділянки ядра зі структурою типу "кільце"?
4. Чи є прийнятним збільшення кількості базових

маршрутизаторів ядра зі структурою типу "кільце", через які може пройти пакет у разі ушкодження одного каналу передачі інформації?

Практична робота

Законспектуйте основі положення стосовно реалізації надлишковості в ядрі ієрархічної мережі.

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Динамічне виділення IP-адрес та протокол DHCP".

МОДУЛЬНА КОНТРОЛЬНА РОБОТА №5

Оберіть номер правильної відповіді:

1. На якому рівні стека протоколу TCP/IP перебуває протокол IP?

а) представлення;

б) сеансовий;

в) транспортний;

г) міжмережевий.

1 б.

2. Основне завдання, що розв'язується протоколом IP:

а) маршрутизація;

б) додавання заголовка;

в) аналіз правильності доставки.

1 б.

3. З якої кількості байт складається IP-адреса?

а) 1;
б) 2;
в) 3;
г) 4.

1 б.

4. Мас-адреса – це:
а) адреса, призначається динамічно при вході в мережу;
б) адреса, призначається виробником обладнання і є унікальною;
в) адреса, обирається користувачем при вході в мережу.

1 б.

5. Старші біти 4-байтної IP-адреси визначають:
а) номер мережі;
б) номер підмережі;
в) номер хоста;
г) Мас-адресу.

1 б.

6. Скільки класів IP-адрес ви знаєте?
а) 2;
б) 3;
в) 5;
г) 9.

1 б.

7. Виберіть IP-адресу, що відповідає інтерфейсу зворотного зв'язка:
а) 192.168.1.123;
б) 127.0.0.1;
в) 13.45.12.1;
г) 1.1.1.1;

1 б.

8. Виберіть IP-адресу, що відповідає всій цілій мережі:
а) 192.168.1.1;
б) 127.0.0.0;
в) 255.255.255.255;
г) 0.0.0.0.

1 б.

9. Виберіть IP-адресу, що відповідає широкомовній передачі:
а) 192.168.1.1;
б) 127.0.0.0;

в) 255.255.255.255;

г) 1.1.1.1.

1 б.

10. Протокол ICMP:

а) забезпечує зворотний зв'язок у вигляді діагностичних повідомлень, що посилають відправнику при неможливості доставки його дейтаграми й в інших випадках;

б) відповідає безпосередньо за передачу даних;

в) відповідає за коректне прийняття даних;

г) посилає широкомовне повідомлення.

1 б.

Всього: 10 балів.

Правильні відповіді

Питання	1	2	3	4	5	6	7	8	9	10
Відповідь	г	а	г	б	б	в	б	г	в	а

ЗМІСТОВИЙ МОДУЛЬ 6

БАЗОВІ ТРАНСПОРТНІ ПРОТОКОЛИ СТЕКУ TCP/IP.

ЗАГАЛЬНІ ВЛАСТИВОСТІ ТА КЛАСИФІКАЦІЯ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ

Таблиця 49

Тематичний план змістового модуля

№ теми	Назва змістового модуля, теми	Усього годин	Лекції	Лабораторні заняття	Самостійна та індивідуальна робота
6.1	Базові транспортні протоколи стеку TCP/IP	9	2	2	5
6.2	Загальні властивості та класифікація протоколів маршрутизації	9	2	2	5
	Разом	***18***	***4***	***4***	***10***

Навчальні цілі: сприяти засвоєнню студентами знань щодо транспортного рівня комп'ютерних мереж, та властивостей і класифікації протоколів маршрутизації.

Основні поняття: транспортний рівень, протокол TCP, порт, сонет, протокол UDP, логічне з'єднання, ковзне вікно, протокол RIP протокол OSPF, утиліта traceroute, утиліта ping.

Методичні рекомендації щодо роботи з модулем: робота з модулем передбачає засвоєння лекційного матеріалу, участь у лабораторних заняттях, написання реферату (окремими студентами), самостійну роботу над визначеними питаннями теми, модульний контроль у формі тестування.

Після опрацювання цих тем студент може отримати бали, наведені в табл. 50.

Таблиця 50

Оцінювання навчальних досягнень студентів

Поточний контроль				Індивідуальне завдання	Контрольна рейтингова оцінка	Проміжна рейтингова оцінка
Робота на лабораторному занятті		Самостійна робота				
Тема №6.1	Тема №6.2	Тема №6.1	Тема №6.2			

ТЕМА 6.1. БАЗОВІ ТРАНСПОРТНІ ПРОТОКОЛИ СТЕКУ TCP/IP

Лекція

План

1. Принципи об'єднання мереж на основі мережевого рівня
2. Обмеження мостів і комутаторів
3. Поняття internetworking
4. Принципи маршрутизації
5. Протоколи маршрутизації

Література

Основна

1. *Компьютеры*, сети, Интернет: Энциклопедия: Наиболее полн. и подроб. рук. / Ю. Новиков, Д. Новиков, А. Черепанов, В. Чуркин; Под общ. ред. Ю. Новикова. – 2. изд. – М. [и др.]: Питер, 2003 (СПб.: ГПП Печ. Двор им. А.М. Горького). – 831 с.: ил.; 24 см.

2. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

3. *Олифер В. Г.* Новые технологии и оборудование IP-сетей / Виктор Олифер, Наталья Олифер. – СПб. и др.: BHV, 2000. – 512 с.: ил., табл.; 24 см. – (Мастер) (Современные сетевые технологии).

4. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. – 4-е изд. – М. [и др.]: Питер, 2005. – 991 с.: ил., табл.; 24 см. – (Классика computer science).

Додаткова

1. *Башмаков А. И.* Интеллектуальные информационные технологии: учеб. пособие для студ. вузов, обуч. по направлению подгот. дипломированных спец. "Информатика и вычислительная техника" / А. И. Башмаков, И. А. Башмаков – М. : МГТУ им.Н.Э.Баумана, 2005. – 302 с.

2. *Білоус Л. Ф.* Інформаційні мережі : навч. посібник / Білоус Л. Ф. – К. : Логос, 2005. – 140 с.

3. *Вишневский А.* Сетевые технологии Windows 2000 / Алексей Вишневский. – СПб. и др.: Питер, 2000. – 591 с.: ил., табл.; 24 см. – (Для профессионалов).

4. *Грир Т.* Сети Интернет: Пер. с англ. – М.: ИТД "Русская редакция", 2000. – 368 с.

5. *Ибе О.* Сети и удаленный доступ: Протоколы, проблемы, решения / Оливер Ибе. – М.: ДМК Пресс, 2002. – 332 с.: ил.; 23 см. – (Серия "Защита и администрирование").

6. *Камер Д.Э.* Компьютерные сети и Internet: Разработка приложений для Internet (пер. с англ. Птицына К.А.) Изд. 3-е + CD-Rom – 640 с.

7. *Коваленко А. Є.* Корпоративні комп'ютерні мережі та телекомунікації : конспект лекцій для студ. спец. 7.080401 "Інформаційні управляючі системи та технології" ден. форми навч. / Анатолій Єпіфанович Коваленко. – К. : НУХТ, 2004. – 27 с.

8. *Контроль* та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології : навчальний посібник / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. – Х. : "Компанія СМІТ", 2004. – 544 с.

6.1.1. Принципи об'єднання мереж на основі мережевого рівня

У стандартній моделі взаємодії відкритих систем у функції мережевого рівня входить розв'язання таких завдань:

– передача пакетів між кінцевими вузлами в складених мережах;

– вибір маршруту передачі пакетів, найкращого за деяким критерієм;

– узгодження різних протоколів канального рівня, що використовуються в окремих підмережах однієї складеної мережі.

Протоколи мережевого рівня реалізуються, як правило, у вигляді програмних модулів і виконуються на кінцевих хостах, а також на проміжних вузлах-маршрутизаторах, що називаються *шлюзами*. Функції маршрутизаторів можуть виконувати як спеціалізовані пристрої, так і універсальні комп'ютери з відповідним програмним забезпеченням.

6.1.2. Обмеження мостів і комутаторів

Створення складної, структурованої мережі, що інтегрує різні базові технології, може здійснюватися і засобами канального рівня: для цього можуть бути використані деякі типи мостів і комутаторів. Міст або комутатор розділяє мережу на сегменти, локалізуючи трафік усередині сегменту, що робить лінії зв'язку такими, що розділяються переважно між станціями цього сегменту. Тим самим мережа розпадається на окремі підмережі, з яких можуть бути побудовані складені мережі досить великих розмірів.

Проте побудова складних мереж тільки на основі повторювачів, мостів і комутаторів має істотні обмеження і недоліки.

По-перше, у топології мережі, що вийшла, мають бути відсутніми петлі. Дійсно, міст/комутатор може вирішувати завдання доставки пакету адресатові тільки тоді, коли між відправником і одержувачем існує єдиний шлях. Тим же часом наявність надлишкових зв'язків, які і утворюють петлі, часто потрібна для кращого балансування навантаження, а також для підвищення надійності мережі за рахунок утворення резервних шляхів.

По-друге, логічні сегменти мережі, розташовані між мостами або комутаторами, слабо ізольовані один від одного, не захищені від так званих широкомовних штормів. Якщо яка-небудь станція посилає широкомовне повідомлення, то воно передається усім станціям всіх логічних сегментів мережі. Захист від широкомовних штормів у мережах, побудованих на основі мостів і комутаторів, має кількісний, а не якісний характер: адміністратор просто обмежує кількість широкомовних пакетів, яку дозволяється генерувати деякому вузлу в одиницю часу. Використання ж механізму віртуальних мереж, реалізованого в багатьох комутаторах, хоча і дозволяє досить гнучко створювати ізольовані по трафіку групи

станцій, але при цьому ізолює їх повністю, так що вузли однієї віртуальної мережі не можуть взаємодіяти з вузлами іншої віртуальної мережі.

По-третє, у мережах, побудованих на основі мостів і комутаторів, досить складно вирішується завдання управління трафіком на основі значень даних, що містяться в пакеті. У таких мережах це можливо тільки за допомогою призначених для користувача фільтрів, для завдання яких адміністраторові доводиться мати справу з двійковим представленням вмісту пакетів.

По-четверте, реалізація транспортної підсистеми тільки засобами фізичного і канального рівнів, до яких відносяться мости і комутатори, призводить до недостатньо гнучкої, однорівневої системи адресації: як адреса призначення використовується MAC-адреса, жорстко пов'язана з мережевим адаптером.

Нарешті, можливість трансляції протоколів канального рівня мають далеко не всі типи мостів і комутаторів, до того ж ці можливості обмежені. Зокрема, в об'єднуваних мережах повинні збігатися максимально допустимі розміри полів даних у кадрах, оскільки мостами і комутаторами не підтримується функція фрагментації кадрів.

Наявність серйозних обмежень у протоколів канального рівня показує, що побудова на основі засобів цього рівня великих неоднорідних мереж є дуже проблематичною. Природне рішення в цих випадках – це залучення засобів вищого мережевого рівня.

6.1.3. Поняття internetworking

Основна ідея використання мережевого рівня полягає в тому, що мережа зазвичай розглядається як сукупність декількох мереж і називається *складеною мережею* або *інтермережею (internetwork* або *internet)*. Мережі, що до неї входять, називаються *підмережами (subnet)*, *складовими мережами* або просто мережами.

Підмережі з'єднуються між собою маршрутизаторами. Компонентами складеної мережі можуть бути як локальні, так і глобальні мережі. Усі вузли в межах однієї підмережі взаємодіють, використовуючи єдину для них технологію. Кожна з цих технологій достатня для того, щоб організувати взаємодію всіх вузлів у своїй підмережі, але не здатна побудувати інформаційний зв'язок між довільно вибраними вузлами, що належать різним підмережам.

Отже, для організації взаємодії між будь-якою довільною парою вузлів цієї "великої" складеної мережі вимагаються додаткові засоби. Такі засоби і надає мережевий рівень.

Мережевий рівень виступає координатором, що організовує роботу всіх підмереж, які лежать на шляху просування пакету по складеній мережі. Для переміщення даних у межах підмереж мережевий рівень звертається до використовуваних в цих підмережах технологій.

Хоча багато технологій локальних мереж (Ethernet, Token Ring, FDDI, Fast Ethernet та ін.) використовують одну і ту ж систему адресації вузлів на основі MAC-адрес, існує немало технологій (X.25, ATM, Frame Relay), у яких застосовуються інші схеми адресації. Адреси, присвоєні вузлам відповідно до технологій підмереж, називають локальними. Щоб мережевий рівень міг виконати своє завдання, йому потрібна власна система адресації, не залежна від способів адресації вузлів в окремих підмережах, яка дозволила б на мережевому рівні універсальним і однозначним способами ідентифікувати будь-який вузол складеної мережі.

Природним способом формування мережевої адреси є унікальна нумерація всіх підмереж складеної мережі й нумерація всіх вузлів у межах кожної підмережі. Таким чином, мережева адреса є парою: номер мережі (підмережі) і номер вузла.

Номером вузла може виступати або локальна адреса цього вузла (така схема прийнята в стеку IPX/SPX), або деяке число, ніяк не пов'язане з локальною технологією, яке однозначно ідентифікує вузол у межах цієї підмережі. У першому випадку мережева адреса стає залежною від локальних технологій, що обмежує його застосування. Наприклад, мережеві адреси IPX/SPX розраховані на роботу в складених мережах, що об'єднують мережі, у яких використовуються тільки MAC-адреси або адреси аналогічного формату. Другий підхід більш універсальний, він характерний для стека TCP/IP. І в тому, і в іншому випадку кожен вузол складеної мережі має разом зі своєю локальною адресою ще один – *універсальну мережеву адресу*.

Дані, які надходять на мережевий рівень і які необхідно передати через складену мережу, забезпечуються заголовком мережевого рівня. Вони разом із заголовком утворюють пакет.

Заголовок пакету мережевого рівня має уніфікований формат, не залежний від форматів кадрів канального рівня тих мереж, які можуть входити в об'єднану мережу, і несе разом з іншою службовою інформацією дані про номер мережі, якій призначається цей пакет. Мережевий рівень визначає маршрут і переміщує пакет між підмережами.

При передачі пакету з однієї підмережі в іншу пакет мережевого рівня, інкапсульований у прибулий канальний кадр першої підмережі, звільняється від заголовків цього кадру й оточується заголовками кадру канального рівня наступної підмережі. Інформацією, на основі якої робиться ця заміна, є службові поля пакету мережевого рівня. У полі адреси призначення нового кадру зазначається локальна адреса наступного маршрутизатора.

Основним полем заголовка мережевого рівня є номер мережі-адресата. У розглянутих раніше протоколах локальних мереж такого поля в кадрах не було – передбачалося, що всі вузли належать одній мережі. Нумерація мереж дозволяє протоколам мережевого рівня складати точну карту міжмережевих зв'язків і вибирати раціональні маршрути при будь-якій їх топології, у тому числі альтернативні маршрути (якщо вони є) що не вміють робити мости і комутатори.

Окрім номера мережі, заголовок мережевого рівня повинен містити й іншу інформацію, необхідну для успішного переходу пакету з мережі одного типу в мережу іншого типу. До такої інформації може відноситися:

– номер фрагмента пакету, необхідний для успішного проведення операцій збирання-розбирання фрагментів при з'єднанні мереж з різними максимальними розмірами пакетів;

– час життя пакету, що вказує, як довго він подорожує по інтермережі, цей час може використовуватися для знищення пакетів, що "заблукали";

– якість послуги – критерій вибору маршруту при міжмережевих передачах – наприклад, вузол-відправник може зажадати передати пакет з максимальною надійністю, можливо, у збиток часу доставки.

Коли дві або більше мереж організовують спільну транспортну службу, то такий режим взаємодії зазвичай називають міжмережевою взаємодією (internetworking).

6.1.4. Принципи маршрутизації

Найважливішим завданням мережевого рівня є *маршрутизація* – передача пакетів між двома кінцевими вузлами в складеній мережі.

Маршрутизатори мають декілька портів (принаймні, два), до яких приєднуються мережі. Кожен порт маршрутизатора можна розглядати як окремий вузол мережі: він має власну мережеву і локальну адресу в тій підмережі, яка до нього підключена. Таким чином, маршрутизатор можна розглядати як сукупність декількох вузлів, кожен з яких входить у свою мережу. Як єдиний пристрій маршрутизатор немає ні окремої мережевої адреси, ні якої-небудь локальної адреси.

У складних мережах майже завжди існує декілька альтернативних маршрутів для передачі пакетів між двома кінцевими вузлами.

Маршрут – це послідовність маршрутизаторів, які повинен пройти пакет від відправника до пункту призначення.

Завдання вибору маршруту з декількох можливих вирішують маршрутизатори, а також кінцеві вузли.

Щоб за адресою мережі призначення можна було вибрати раціональний маршрут подальшого отримання пакету, кожен кінцевий вузол і маршрутизатор аналізують спеціальну інформаційну структуру, яка називається *таблицею маршрутизації*.

Коли на маршрутизатор надходить новий пакет, номер мережі призначення витягається з кадру, що надійшов, послідовно порівнюється з номерами мереж з кожного рядка таблиці. Рядок з номером мережі, що збігається, вказує, на який найближчий маршрутизатор треба направити пакет.

Деякі реалізації мережевих протоколів допускають наявність у таблиці маршрутизації відразу декількох рядків, відповідних одному і тому ж адресу мережі призначення. У цьому випадку при виборі маршруту береться до уваги стовпець "*Відстань до мережі призначення*". При цьому під відстанню розуміється будь-яка метрика, що використовується відповідно до заданого в мережевому пакеті критерію (часто називається *класом сервісу*). Відстань може вимірюватися хопами, часом проходження пакету лініями зв'язку, якою-небудь характеристикою надійності ліній зв'язку на цьому маршруті або іншою величиною, що відбиває якість цього маршруту

по відношенню до заданого критерію. Якщо маршрутизатор підтримує декілька класів сервісу пакетів, то таблиця маршрутів складається і застосовується окремо для кожного виду сервісу (критерію вибору маршруту).

Наявність декількох маршрутів до одного вузла роблять можливою передачу трафіку до цього вузла паралельно по декількох каналах зв'язку, що підвищує пропускну спроможність і надійність мережі.

6.1.5. Протоколи маршрутизації

Завдання маршрутизації вирішується на основі аналізу таблиць маршрутизації, розміщених у всіх маршрутизаторах і кінцевих вузлах мережі. Основна робота зі створення таблиць маршрутизації виконується автоматично, але, як правило, передбачається і можливість вручну скоректувати або доповнити таблицю.

Для автоматичної побудови таблиць маршрутизації маршрутизатори обмінюються інформацією про топологію складеної мережі відповідно до спеціального службового протоколу. Протоколи цього типу називаються *протоколами маршрутизації*. Протоколи маршрутизації (наприклад, RIP, OSPF, NLSP) необхідно відрізняти від власне мережевих протоколів (наприклад, IP, IPX). І ті і інші виконують функції мережевого рівня моделі OSI – беруть участь у доставці пакетів адресатові через різнорідну складену мережу. Але тоді як перші збирають і передають по мережі тільки службову інформацію, другі призначені для передачі користувачів даних, як це роблять протоколи канального рівня. Протоколи маршрутизації використовують мережеві протоколи як транспортний засіб.

За допомогою протоколів маршрутизації маршрутизатори складають карту зв'язків мережі. На підставі цієї інформації для кожного номера мережі приймається рішення про те, якому наступному маршрутизатору потрібно передавати пакети, що направляються в цю мережу, щоб маршрут виявився раціональним. Результати цих рішень заносяться в таблицю маршрутизації. При зміні конфігурації мережі деякі записи в таблиці стають не дійсними. У таких випадках пакети, відправлені помилковим маршрутом, можуть зациклюватися і втрачатися. Від того, наскільки швидко протокол маршрутизації приводить у відповідність вміст таблиці реальному стану мережі, залежить якість роботи всієї мережі.

Протоколи маршрутизації можуть бути побудовані на основі різних алгоритмів, що відрізняються способами побудови таблиць маршрутизації, способами вибору найкращого маршруту і іншими особливостями своєї роботи.

У всіх описаних вище прикладах при виборі раціонального маршруту визначався тільки наступний (найближчий) маршрутизатор, а не вся послідовність маршрутизаторів від початкового до кінцевого вузла. Відповідно до цього підходу маршрутизація виконується за розподіленою схемою – кожен маршрутизатор відповідальний за вибір тільки одного кроку маршруту, а остаточний маршрут складається в результаті роботи усіх маршрутизаторів, через які проходить цей пакет. Такі алгоритми маршрутизації називаються однокроковими.

Існує і прямо протилежний, багатокроковий підхід – *маршрутизація від джерела (Source Routing)*. Відповідно до нього вузол-джерело задає в пакеті, що відправляється в мережу, повний маршрут його отримання через усі проміжні маршрутизатори. При використанні багатокрокової маршрутизації немає необхідності будувати й аналізувати таблиці маршрутизації. Це прискорює проходження пакету мережею, розвантажує маршрутизатори, але при цьому велике навантаження лягає на кінцеві вузли. Ця схема в обчислювальних мережах застосовується сьогодні набагато рідше, ніж схема розподіленої однокрокової маршрутизації. Проте в новій версії протоколу IP разом з класичною однокроковою маршрутизацією буде дозволена і маршрутизація від джерела.

Однокрокові алгоритми залежно від способу формування таблиць маршрутизації діляться на три класи:

- алгоритми фіксованої (чи статичної) маршрутизації;
- алгоритми простої маршрутизації;
- алгоритми адаптивної (чи динамічної) маршрутизації.

В алгоритмах фіксованої маршрутизації всі записи в таблиці маршрутизації є статичними. Адміністратор мережі сам вирішує, на які маршрутизатори потрібно передавати пакети з тими або іншими адресами, і вручну (наприклад, за допомогою утиліти route ОС Unix або Windows) заносить відповідні записи в таблицю маршрутизації. Таблиця, як правило, створюється в процесі завантаження, надалі вона використовується без змін до тих пір, поки її вміст не буде відредагований вручну. Такі виправлення можуть знадобитися,

наприклад, якщо в мережі відмовляє який-небудь маршрутизатор і його функції покладаються на інший. Алгоритм фіксованої маршрутизації з його ручним способом формування таблиць маршрутизації прийнятний тільки в невеликих мережах з простою топологією.

В алгоритмах простої маршрутизації таблиця маршрутизації або зовсім не використовується, або будується без участі протоколів маршрутизації. Виділяють три типи простої маршрутизації:

– випадкова маршрутизація, коли прибулий пакет посилається у першому випадковому напрямі, що потрапив, окрім початкового;

– лавинна маршрутизація, коли пакет широкомовно посилається всіма можливими напрямами, окрім початкового (подібно обробці мостами кадрів з невідомою адресою);

– маршрутизація за попереднім досвідом, коли вибір маршруту здійснюється по таблиці, але таблиця будується за принципом моста шляхом аналізу адресних полів пакетів, що з'являються на вхідних портах.

Найпоширенішими є алгоритми адаптивної (чи динамічною) маршрутизації. Вони забезпечують автоматичне оновлення таблиць маршрутизації після зміни конфігурації мережі. Протоколи, побудовані на основі адаптивних алгоритмів, дозволяють усім маршрутизаторам збирати інформацію про топологію зв'язків у мережі, оперативно відпрацьовують усі зміни конфігурації зв'язків. У таблицях маршрутизації при адаптивній маршрутизації зазвичай є інформація про інтервал часу, протягом якого цей маршрут залишатиметься дійсним. Цей час називають часом життя маршруту (Time To Live, TTL).

Адаптивні алгоритми зазвичай мають розподілений характер, який виражається в тому, що в мережі відсутні будь-які виділені маршрутизатори, які збирали б і узагальнювали топологічну інформацію: ця робота розподілена між усіма маршрутизаторами.

Адаптивні протоколи обміну маршрутною інформацією, що використовуються сьогодні в обчислювальних мережах, діляться на дві групи, кожна з яких пов'язана з одним із типів алгоритмів:

– дистанційно-векторні алгоритми (Distance Vector Algorithms, DVA);

– алгоритми стану зв'язків (Link State Algorithms, LSA).

У алгоритмах дистанційно-векторного типу кожен маршрутизатор періодично і широкомовно розсилає мережею вектор, компонентами якого є відстані від цього маршрутизатора до всіх відомих йому мереж. Під відстанню зазвичай розуміється число хопів. Можлива й інша метрика, що враховує не лише число проміжних маршрутизаторів, але й час проходження пакетів мережею між сусідніми маршрутизаторами. При отриманні вектора від сусіда маршрутизатор нарощує відстані до зазначених у векторі мереж на відстань до цього сусіда. Отримавши вектор від сусіднього маршрутизатора, кожний маршрутизатор додає до нього інформацію про відомі йому інші мережі, про які він дізнався безпосередньо (якщо вони підключені до його портів) або з аналогічних оголошень інших маршрутизаторів, а потім знову розсилає нове значення вектора мережею. Урешті-решт, кожен маршрутизатор дізнається інформацію про всі наявні в інтермережі мережі і про відстань до них через сусідні маршрутизатори.

Дистанційно-векторні алгоритми добре працюють тільки в невеликих мережах. У великих мережах вони засмічують лінії зв'язку інтенсивним широкомовним трафіком, до того ж зміни конфігурації можуть відпрацьовуватися по цьому алгоритму не завжди коректно, оскільки маршрутизатори не мають точного уявлення про топологію зв'язків у мережі, а мають у розпорядженні тільки узагальнену інформацію – вектор дистанцій, до того ж отриманий через посередників. Робота маршрутизатора відповідно до дистанційно-векторного протоколу нагадує роботу моста, оскільки точної топологічної картини мережі такий маршрутизатор не має.

Найбільш поширеним протоколом, заснованим на дистанційно-векторному алгоритмі, є протокол RIP, поширений у двох версіях, – RIP IP, що працює з протоколом IP, і RIP IPX, що працює з протоколом IPX.

Алгоритми стану зв'язків забезпечують кожен маршрутизатор інформацією, достатньою для побудови точного графа зв'язків мережі. Усі маршрутизатори працюють на підставі однакових графів, що робить процес маршрутизації стійкішим до змін конфігурації. "Широкомовна" розсилка (передача пакету всім безпосереднім сусідам маршрутизатора) використовується тут тільки при змінах стану зв'язків, що відбувається в надійних мережах не так часто. Вершинами графа є як маршрутизатори, так і об'єднувані

ними мережі. Поширювана мережею інформація складається з опису зв'язків різних типів: маршрутизатор-маршрутизатор, маршрутизатор-мережа.

Щоб зрозуміти, у якому стані перебувають лінії зв'язку, підключені до його портів, маршрутизатор періодично обмінюється короткими пакетами HELLO зі своїми найближчими сусідами. Цей службовий трафік також засмічує мережу, але не такою мірою як, наприклад, RIP-пакети, оскільки пакети HELLO мають набагато менший об'єм.

Протоколами, заснованими на алгоритмі стану зв'язків, є протоколи IS-IS (Intermediate System to Intermediate System) стека OSI, OSPF (Open Shortest Path First) стека TCP/IP і протокол NLSP стека Novell.

Лабораторна робота №11 (2 год.)

Тема: Перевірка TCP/IP-з'єднання за допомогою команди ping.

Мета: виробити навички діагностування роботи комп'ютерної мережі за допомогою вбудованих мережевих засобів операційної системи;

виховувати ціннісне ставлення студентів до майбутньої професійної діяльності.

Студент повинен знати: основні команди операційної системи для діагностування дієздатності мережевого підключення.

Студент повинен уміти: здійснювати перевірку TCP/IP-з'єднання за допомогою команди ping.

Обладнання: комп'ютерний клас з локальною мережею на основі стандарту Fast Ethernet.

Інструктаж

Команда Ping

За допомогою відправки запитів протоколом ICMP перевіряє з'єднання на рівні протоколу IP з іншим комп'ютером, що підтримує TCP/IP. Після кожної передачі виводиться відповідне з'єднання з луна-відповіддю. Ping – це основна TCP/IP-команда, яка використовується для усунення огріхів у з'єднанні, перевірки можливості доступу і дозволу імен. Команда ping, запущена без параметрів, виводить довідку.

Команда ping дозволяє перевірити ім'я та IP-адресу комп'ютера. Якщо перевірка IP-адреси успішна, і перевірка імені – ні, то виникає проблема дозволу імен. У такому разі за допомогою

запитів DNS (Domain Name System) або методів дозволу імен NetBIOS перевірте, щоб ім'я комп'ютера, що задається, було дозволене в локальному файлі Hosts.

Ця команда доступна, якщо у властивостях мережевого адаптера в об'єкті "Мережеві підключення" як компонент встановлений протокол Інтернету (TCP/IP).

Приклади. Для відправки повідомлення точці призначення 10.0.1.1 і зіставлення з її мережевим ім'ям введіть:

ping -a 10.0.1.1

Для відправки точці призначення 10.0.1.1 десяти повідомлень з луна-запитом, кожне з яких має поле даних з 1000 байт, введіть:

ping -n 10 -l 1000 10.0.1.1

Для відправки повідомлення точці призначення 10.0.1.1 і записи маршруту для 4 переходів введіть:

ping -r 4 10.0.1.1

Для відправки повідомлення точці призначення 10.0.1.1 і завдання вільної маршрутизації для точок призначення 10.12.0.1-10.29.3.1-10.1.44.1 введіть:

ping – j 10.12.0.1 10.29.3.1 10.1.44.1 10.0.1.1

Ipconfig

Служить для відображення всіх поточних параметрів мережі TCP/IP й оновлення параметрів DHCP і DNS. При виклику команди ipconfig без параметрів виводиться тільки IP-адреса, маска підмережі й основний шлюз для кожного мережевого адаптера.

Щоб вивести основну конфігурацію TCP/IP для всіх адаптерів, введіть: ipconfig.

Щоб вивести повну конфігурацію TCP/IP для всіх адаптерів, введіть: ipconfig /all.

Щоб відновити конфігурацію IP-адреса, призначеного DHCP-сервером тільки для адаптера "Підключення по локальній мережі", введіть: ipconfig /renew "Підключення по локальній мережі".

Щоб скинути кеш зіставлення імен DNS за наявності огріхів у зіставленні імен, введіть: ipconfig /flushdns.

Щоб вивести код класу DHCP для всіх адаптерів з іменами, що починаються із слова "Підключення", введіть: ipconfig /showclassid Підключення.

Практична частина

Перевірка конфігурації TCP/IP за допомогою команди ping.

1. Щоб швидко одержати значень параметрів конфігурації TCP/IP на комп'ютері, відкрийте командний рядок (cmd.exe) і виконайте команду ipconfig. За допомогою відомостей, відображених командою ipconfig, переконайтеся, що мережевий адаптер, що перевіряється не перебуває в стані "Мережа відключена".

2. У командному рядку зверніться за адресою loopback, для чого виконайте команду: ping 127.0.0.1.

3. Зверніться командою "ping" за IP-адресою комп'ютера.

4. Зверніться командою "ping" за IP-адресою основного шлюзу. Якщо команда ping не була успішно виконана, перевірте правильність IP-адреси основного шлюзу і його працездатність (маршрутизатора).

5. Зверніться з командою "ping" за IP-адресою віддаленого вузла (вузла, що перебуває в іншій підмережі). Якщо команда ping не була успішно виконана, перевірте правильність IP-адреси віддаленого вузла, працездатність цього вузла, а також працездатність усіх шлюзів (маршрутизаторів) між локальним комп'ютером і видаленим вузлом.

6. Зверніться командою "ping" за IP-адресою DNS-сервера. Якщо команда ping не була успішно виконана, перевірте правильність IP-адреси DNS-сервера, працездатність DNS-сервера, а також працездатність усіх шлюзів (маршрутизаторів) між локальним комп'ютером і DNS-сервером.

Самостійна робота №11

Тема: Надлишковість, що реалізується на рівні розподілення ієрархічної мережі

Мета: розвивати аналітичні вміння студентів з реалізації надлишковості на рівні розподілення ієрархічної мережі.

Студент повинен знати: методи та засоби реалізації надлишковості на рівні розподілення ієрархічної мережі.

Студент повинен уміти: обирати та реалізовувати засоби надлишковості на рівні розподілення ієрархічної мережі.

Хід роботи

Теоретична частина

1. Назвіть технології кільцевих мереж, що забезпечують надмірність на рівні 2 – еталонної моделі OSI.

2. Чи дозволяють технології кільцевих мереж з надмірністю забезпечити відмовостійкість мережі в разі ушкодження вхідних у неї пристроїв?

Практична частина

Завдання

Законспектуйте основні положення щодо методів та засобів реалізації надлишковості на рівні розподілення ієрархічної мережі.

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Транспортні протоколи – особливості функціонування".

ТЕМА 6.2. ЗАГАЛЬНІ ВЛАСТИВОСТІ ТА КЛАСИФІКАЦІЯ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ

Лекція

План

1. Протокол керування передачею TCP
2. Протокол дейтаграм користувача UDP
3. Зв'язок протоколів мережного й транспортного рівнів

Література

Основна

1.*Компьютеры*, сети, Интернет: Энциклопедия: Наиболее полн. и подроб. рук. / Ю. Новиков, Д. Новиков, А. Черепанов, В. Чуркин;

Под общ. ред. Ю. Новикова. – 2. изд. – М. [и др.]: Питер, 2003 (СПб.: ГПП Печ. Двор им. А.М. Горького). – 831 с.: ил.; 24 см.

2. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

3. *Олифер В. Г.* Новые технологии и оборудование IP-сетей / Виктор Олифер, Наталья Олифер. – СПб. и др.: BHV, 2000. – 512 с.: ил., табл.; 24 см. – (Мастер) (Современные сетевые технологии).

4. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. – 4-е изд. – М. [и др.]: Питер, 2005. – 991 с.: ил., табл.; 24 см. – (Классика computer science).

Додаткова

1. *Башмаков А. И.* Интеллектуальные информационные технологии: учеб. пособие для студ. вузов, обуч. по направлению подгот. дипломированных спец. "Информатика и вычислительная техника" / А. И. Башмаков, И. А. Башмаков – М. : МГТУ им.Н.Э.Баумана, 2005. – 302 с.

2. *Білоус Л. Ф.* Інформаційні мережі : навч. посібник / Білоус Л. Ф. – К. : Логос, 2005. – 140 с.

3. *Вишневский А.* Сетевые технологии Windows 2000 / Алексей Вишневский. – СПб. и др.: Питер, 2000. – 591 с.: ил., табл.; 24 см. – (Для профессионалов).

4. *Грир Т.* Сети Интернет: Пер. с англ. – М.: ИТД "Русская редакция", 2000. – 368 с.

5. *Ибе О.* Сети и удаленный доступ: Протоколы, проблемы, решения / Оливер Ибе. – М.: ДМК Пресс, 2002. – 332 с.: ил.; 23 см. – (Серия "Защита и администрирование").

6. *Камер Д.Э.* Компьютерные сети и Internet: Разработка приложений для Internet (пер. с англ. Птицына К.А.) Изд. 3-е + CD-Rom – 640 с.

7. *Коваленко А. Є.* Корпоративні комп'ютерні мережі та телекомунікації : конспект лекцій для студ. спец. 7.080401

"Інформаційні управляючі системи та технології" ден. форми навч. / Анатолій Єпіфанович Коваленко. – К. : НУХТ, 2004. – 27 с.

8. *Контроль* та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології : навчальний посібник / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. – Х. : "Компанія СМІТ", 2004. – 544 с.

6.2.1. Протокол керування передачею TCP

Транспортний рівень Інтернет реалізується протоколом TCP (Transmission Control Protocol – Протокол контролю передачі) і протоколом UDP (User Datagram Protocol – протокол дейтаграм користувача). TCP забезпечує транспортування даних із установленням з'єднання, тим часом як UDP працює без установлення з'єднання.

Протокол TCP надає транспортні послуги, що відрізняються від послуг UDP. Замість ненадійної доставки дейтаграм без установлення з'єднань, він забезпечує гарантовану доставку із установленням з'єднань у вигляді байтових потоків (рис. 82).

Протокол TCP використовується в тих випадках, коли потрібна надійна доставка повідомлень. Він звільняє прикладні процеси від необхідності використовувати тайм-аути й повторні передачі для забезпечення надійності. Внутрішня структура модуля TCP набагато складніша структури модуля UDP.

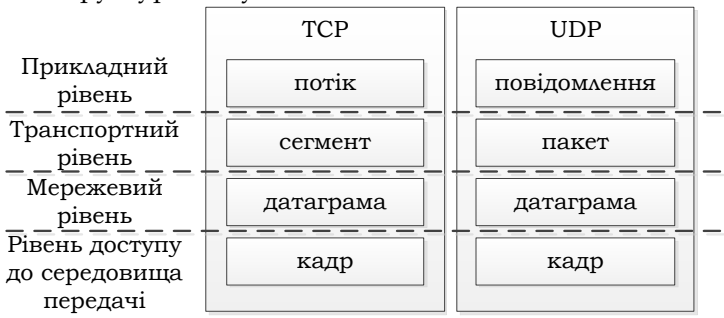


Рис. 82. Протоколи транспортного рівня TCP і UDP

TCP – надійний байт-орієнтований (byte-stream) протокол із *установленням з'єднання*. TCP перебуває на транспортному рівні стека TCP/IP, між протоколом IP і власне програмою. Протокол IP займається пересиланням дейтаграм по мережі, ніяк не гарантуючи

доставку, цілісність, порядок прибуття інформації й готовність одержувача до прийому даних; усі ці завдання покладені на протокол TCP.

При одержанні дейтаграм у полі Protocol якого зазначений код протоколу TCP (6), модуль IP передає дані цієї дейтаграми модулю TCP. Ці дані являють собою TCP-сегмент, що містить TCP-заголовок і дані користувача (прикладного процесу). Модуль TCP аналізує службову інформацію заголовка, визначає, якому саме процесу призначені дані користувача, перевіряє цілісність і порядок надходження даних і підтверджує їхній прийом іншою стороною. У міру одержання правильної послідовності неспотворених даних користувача вони передаються прикладному процесу.

Нижче розглянуті основні функції протоколу TCP їхня реалізація більш докладно.

Базова передача даних. Модуль TCP виконує передачу безперервних потоків даних між своїми клієнтами в обох напрямках. Клієнтами TCP є прикладні процеси, що викликають модуль TCP при необхідності одержати або відправити дані процесу-клієнтові на іншому вузлі.

Протокол TCP розглядає дані клієнта як безперервний потік октетів. TCP розділяє цей потік на частини для пересилання на інший вузол у TCP-сегментах деякого розміру. Для відправлення або одержання сегмента модуль TCP викликає модуль IP.

Негайне відправлення даних може бути викликано процесом-клієнтом від TCP-модуля за допомогою спеціальної функції PUSH, інакше TCP сам буде вирішувати, як накопичувати й коли відправляти дані клієнта або коли передавати клієнту отримані дані.

Забезпечення вірогідності. Модуль TCP забезпечує захист від ушкодження, втрати, дублювання й порушення послідовності одержання даних.

Для виконання цих завдань усі октети в потоці даних наскрізним образом пронумеровані в зростаючому порядку. Заголовок кожного сегмента містить число октетів даних у сегменті й порядковий номер першого октету тієї частини потоку даних, що пересилається в даному сегменті. Наприклад, якщо в сегменті пересилаються октети з номерами від 2001 до 3000, то номер першого октету в даному сегменті дорівнює 2001, а число октетів дорівнює 1000.

Номер першого байта в потоці визначається на етапі встановлення з'єднання й позначається ISN+1. Наприклад, ISN+1=1.

Також для кожного сегмента обчислюється контрольна сума, що дозволяє виявити ушкодження даних.

При вдалому прийомі октету даних модуль, що приймає, посилає відправнику підтвердження про прийом – номер вдало прийнятого октету. Якщо протягом деякого часу відправник не одержить підтвердження, уважається, що октет не дійшов або був ушкоджений, і він посилає знову. Цей механізм контролю надійності називається PAR (Positive Acknowledgment with Retransmission). У дійсності підтвердження посилає не для одного октету, а для деякого числа послідовних октетів.

Нумерація октетів використовується також для впорядкування даних у порядку черговості й виявлення дублікатів (які можуть бути послані через велику затримку при передачі підтвердження або втрати підтвердження).

Поділ каналів. Протокол TCP забезпечує роботу одночасно декількох з'єднань. Кожний прикладний процес ідентифікується номером порту. Заголовок TCP-сегмента містить номери портів процесу-відправника й процесу-одержувача. При одержанні сегмента модуль TCP аналізує номер порту одержувача й відправляє дані відповідному прикладному процесу.

Усі розповсюджені сервіси Інтернет мають стандартизовані номери портів. Наприклад, номер порту сервера електронної пошти – 25, сервера FTP – 21.

Сукупність IP-адреси й номера порту називається *сокетом*. Сокет унікально ідентифікує прикладний процес в Інтернет. Наприклад, сокет сервера електронної пошти на хості 194.84.124.4 позначається як 194.84.124.4.25; часто номер порту відділяється двокрапкою.

Керування з'єднаннями. *З'єднання* – це сукупність інформації про стан потоку даних, що включає сокети, номери відісланих, прийнятих і підтверджених октетів, розміри вікон.

Кожне з'єднання унікально ідентифікується в Інтернет парою сокетів. З'єднання характеризується для клієнта ім'ям, що є покажчиком на структуру TCB (Transmission Control Block), що містить інформацію про з'єднання.

Відкриття з'єднання клієнтом здійснюється викликом функції OPEN, що передається сокету, з яким потрібно встановити з'єднання.

Функція повертає ім'я з'єднання. Розрізняють два типи відкриття з'єднання: активне й пасивне.

При активному відкритті TCP-модуль починає процедуру встановлення з'єднання із зазначеним сокетом, при пасивному – очікує, що віддалений TCP-модуль почне процедуру встановлення з'єднання із зазначеного сокету.

Вказівка 0.0.0.0:0 у якості сокету при пасивному відкритті означає, що очікується з'єднання з будь-якого сокету. Такий спосіб застосовується в демонах – серверах Інтернет, які чекають установлення з'єднання від клієнта. Клієнт же застосовує процедуру активного відкриття; сокет при цьому формується з IP-адреси сервера й стандартного номера порту для цього сервісу. Закриття з'єднання клієнтом провадиться за допомогою функції CLOSE, якій передається ім'я з'єднання. Процедура встановлення з'єднання відбувається в такий спосіб (рис. 83).

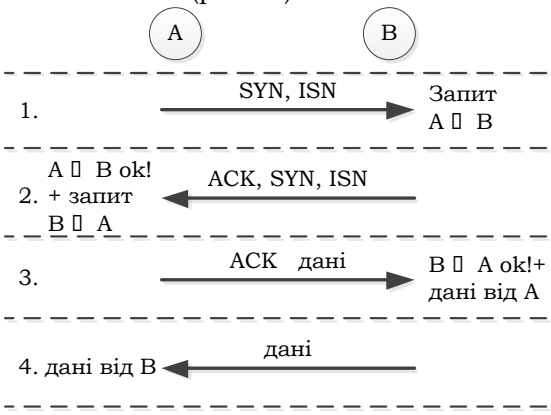


Рис. 83. Встановлення TCP-з'єднання

Припустимо, вузол A бажає встановити з'єднання з вузлом B. Перший відправляє з A в B TCP-сегмент, що не містить корисних даних, а служить для встановлення з'єднання. У його заголовку встановлений біт SYN, що означає запит зв'язку, і втримується ISN (Initial Sequence Number – початковий номер послідовності) – число, починаючи з якого вузол A буде нумерувати відправлені октети (наприклад, 0). У відповідь на одержання такого сегмента вузол B відгукується посилкою TCP-сегмента, у заголовку якого встановлений біт ACK, що підтверджує встановлення з'єднання для

одержання даних від вузла А. Тому що протокол TCP забезпечує повнодуплексну передачу даних, вузол В у цьому ж сегменті встановлює біт SYN, що означає запит зв'язку для передачі даних від В к А, і передає свій ISN (наприклад, 0). Корисних даних цей сегмент також не містить. Третій TCP-сегмент у сеансі посилає А в В у відповідь на сегмент, отриманий з В. Оскільки з'єднання А → В можна вважати встановленим (отримане підтвердження від В), вузол А включає у свій сегмент корисні дані, нумерація яких починається з номера ISN(A)+1. Дані нумеруються по кількості відправлених октетів. У заголовку цього ж сегмента вузол А встановлює біт ACK, що підтверджує встановлення зв'язку В → А, який дозволяє хосту В включити у свій наступний сегмент корисні дані для А.

Сеанс обміну даними закінчується процедурою розриву з'єднання, яка подібна процедурі установки, з тією різницею, що замість SYN для розриву використовується службовий біт FIN ("даних для відправлення більше не маю"), що встановлюється в заголовку останнього сегмента з даними, які відправляє вузлом.

Формат заголовка TCP-сегмента. TCP-сегмент складається із заголовка й даних. Заголовок сегмента складається з 32-розрядних слів і має змінну довжину, що залежить від розміру поля Options, але завжди кратну 32 бітам. За заголовком безпосередньо ідуть дані – частина потоку даних користувача, передана в даному сегменті. Формат заголовка представлений на рис. 84.

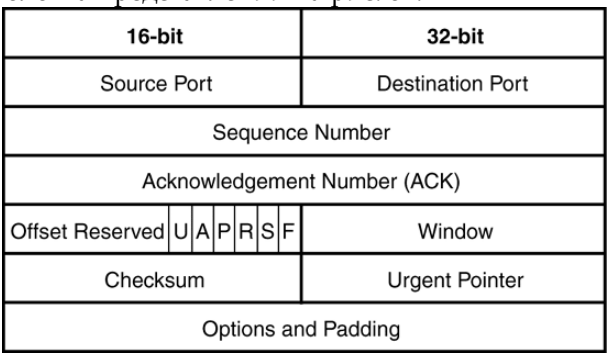


Рис. 84. Формат заголовка TCP-сегмента

Значення полів заголовка такі.

Source Port (16 біт), Destination Port (16 біт) – номери портів процесу-відправника й процесу-одержувача відповідно.

Sequence Number (SN) (32 біта) – порядковий номер першого октету в полі даних сегмента серед всіх октетів потоку даних для поточного з'єднання, тобто якщо в сегменті пересилаються октети з 2001-го по 3000-й, т0 SN=2001. Якщо в заголовку сегмента встановлений біт SYN (фаза встановлення з'єднання), то в полі SN записується початковий номер (ISN), наприклад, 0. Номер першого октету даних, що посилають після завершення фази встановлення з'єднання, дорівнює ISN+1.

Acknowledgment Number (ACK) (32 біта) – якщо встановлено біт ACK, то це поле містить порядковий номер октету, що відправник даного сегмента бажає одержати. Це означає, що всі попередні октети (з номерами від ISN+1 до ACK-1 включно) були успішно отримані.

Data Offset (4 біти) – довжина TCP-заголовка в 32-бітних словах.

Reserved (6 біт) – зарезервовано; заповнюється нулями.

Control Bits (6 біт) – керуючі біти; активним є положення "біт установлений".

U – поле термінового покажчика (Urgent Pointer) задіяно;

A – поле номера підтвердження (Acknowledgment Number) задіяно;

P – здійснити "проштовхування" – якщо модуль TCP одержує сегмент із установленим прапором PSH, то він негайно передає всі дані з буфера прийому процесу-одержувачеві для обробки, навіть якщо буфер не був заповнений;

R – перезавантаження поточного з'єднання;

S – запит на встановлення з'єднання;

F – немає більше даних для передачі.

Window (16 біт) – розмір вікна в октетах.

Checksum (16 біт) – контрольна сума, являє собою 16 біт, що доповнюють біти в сумі всіх 16-бітових слів сегмента (саме поле контрольної суми перед обчисленням обнуляється). Контрольна сума, крім заголовка сегмента й поля даних, нараховує 96 біт псевдозаголовку, що для внутрішнього вживання ставиться перед TCP-заголовком. Цей псевдозаголовок містить IP-адресу відправника (4 октети), IP-адресу одержувача (4 октети), нульовий октет, 8-бітне поле "Протокол", аналогічне полю в IP-заголовку, і 16 біт довжини TCP сегмента. Такий підхід забезпечує захист протоколу TCP від сегментів, що схибив в маршруті. Інформація для псевдозаголовку

передається через інтерфейс "Протокол TCP/міжмережевий рівень" як аргументи або результатів запитів від протоколу TCP до протоколу IP.

Urgent Pointer (16 біт) – використовується для вказівки довжини термінових даних, які розміщаються на початку поля даних сегмента. Указує зсув октету, що йде за терміновими даними щодо першого октету в сегменті. Наприклад, у сегменті передаються октети з 2001-го по 3000-й, при цьому перші 100 октетів є терміновими даними, тоді Urgent Pointer = 100. Протокол TCP не визначає, як саме повинні оброблятися термінові дані, але припускає, що прикладний процес буде докладали зусилля для їхньої швидкої обробки. Поле Urgent Pointer задіяне, якщо встановлено прапор U.

Options – поле змінної довжини; може бути відсутнім, містити одну опцію або список опцій, що реалізують додаткові послуги протоколу TCP. Опція складається з октету "Тип опції", за яким можуть іти октет "Довжина опції в октетах" і октети з даними для опції.

Стандарт протоколу TCP визначає три опції (типи 0,1,2).

Опції типів 0 і 1 ("Кінець списку опцій" і "Немає операції" відповідно) складаються з одного октету, що містить значення типу опції. При виявленні в списку опції "Кінець списку опцій" розбір опцій припиняється, навіть якщо довжина заголовка сегмента (Data Offset) ще не вичерпана. Опція "Немає операції" може використатися для вирівнювання між опціями по границі 32 біт.

Опція типу 2 "Максимальний розмір сегмента" складається з 4 октетів: одного октету типу опції (значення дорівнює 2), одного октету довжини (значення дорівнює 4) і двох октетів, що містять максимальний розмір сегмента, здатного одержувати TCP-модуль, який відправив сегмент із цією опцією. Опцію варто використати тільки в SYN-сегментах на етапі установки з'єднання.

Padding – вирівнювання заголовка по границі 32-бітного слова, якщо список опцій займає неціле число 32-бітних слів. Поле Padding заповнюється нулями.

6.2.2. Протокол дейтаграм користувача UDP

Протокол UDP (User Datagram Protocol, протокол користувальницьких дейтаграм) використовується в тих випадках, коли

потужні засоби забезпечення надійності протоколу TCP не потрібні. Реалізація UDP набагато простіша, ніж TCP.

Протокол UDP використовується або при пересиланні коротких повідомлень, коли накладні витрати на встановлення сеансу й перевірку успішної доставки даних виявляються вищими витрат на повторну (у випадку невдачі) пересилання повідомлення, або в тому випадку, коли сама організація процесу-додатка забезпечує встановлення з'єднання й перевірку доставки пакетів (наприклад, NFS).

Користувацькі дані, що надійшли від прикладного рівня, випереджаються UDP-заголовком, і сформований у такий спосіб UDP-пакет відправляється на міжмережевий рівень. UDP-заголовок складається із двох 32-бітних слів (рис. 85).

Заголовок UDP має чотири поля:

– порт джерела (source port) – ті ж функції, що й у заголовку TCP;

– порт пункту призначення (destination port) – ті ж функції, що й у заголовку TCP;

– довжина (length) – довжина заголовка UDP і даних;

– контрольна сума UDP (checksum UDP) – забезпечує перевірку цілісності пакета (факультативна можливість).

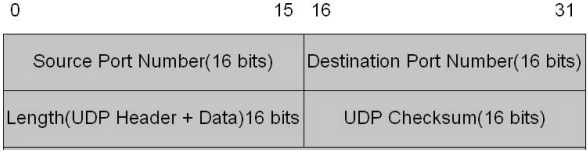


Рис. 85. UDP-заголовок

Контрольна сума обчислюється в такий же спосіб, як і в TCP-заголовку; якщо UDP-пакет має непарну довжину, то при обчисленні контрольної суми до нього додається нульовий октет.

Після заголовка безпосередньо йдуть користувацькі дані, передані модулю UDP прикладним рівнем за один виклик. Протокол UDP розглядає ці дані як цілісне повідомлення; він ніколи не розбиває повідомлення для передачі в декількох пакетах і не поєднує кілька повідомлень для пересилання в одному пакеті. Якщо прикладний процес N раз викликав модуль UDP для відправлення даних (тобто запросив відправлення N повідомлень), то модулем UDP буде сформовано й відправлено N пакетів, і процес-одержувач

буде повинен N раз викликати свій модуль UDP для одержання всіх повідомлень.

При одержанні пакета від міжмережевого рівня модуль UDP перевіряє контрольну суму й передає вміст повідомлення прикладному процесу, чий номер порту зазначений у полі "Destination Port".

Якщо перевірка контрольної суми виявила помилку або якщо процесу, підключеного до необхідного порту, не існує, пакет ігнорується. Якщо пакети надходять швидше, ніж модуль UDP устигає їх обробляти, то пакети, що надходять, також ігноруються. Протокол UDP не має ніяких засобів підтвердження безпомилкового прийому даних або повідомлення про помилку, не забезпечує прихід повідомлень у порядку відправлення, не робить попереднього встановлення сеансу зв'язку між прикладними процесами, тому він є ненадійним протоколом без установлення з'єднання. Якщо програма має потребу в подібних послугах, він повинен використовувати на транспортному рівні протокол TCP.

Максимальна довжина UDP-повідомлення дорівнює максимальній довжині IP-дейтаграми (65535 октетів) за винятком мінімального IP-заголовка (20) і UDP-заголовка (8), тобто 65507 октетів. На практиці зазвичай використовуються повідомлення довжиною 8192 октету.

Приклади прикладних процесів, що використовують протокол UDP: NFS (Network File System – мережна файлова система), TFTP (Trivial File Transfer Protocol – простий протокол передачі файлів), SNMP (Simple Network Management Protocol – простий протокол керування мережею), DNS (Domain Name Service – доменна служба імен).

Порти. Взаємодія між прикладними процесами й модулем UDP здійснюється через UDP-порти. Порти нумеруються починаючи з нуля.

Прикладний процес, що надає деякі послуги іншим прикладним процесам (сервер), очікує надходження повідомлень у порт, спеціально виділений для цих послуг. Повідомлення повинні містити запити на надання послуг. Вони відправляються процесами-клієнтами.

Наприклад, сервер SNMP завжди очікує надходжень повідомлень у порт 161. Якщо клієнт SNMP бажає одержати послугу,

він надсилає запит в UDP порт 161 на машину, де працює сервер. У кожному вузлі може бути тільки один сервер SNMP, тому що існує тільки один UDP-порт 161. Цей номер порту є загальновідомим, тобто фіксованим номером, офіційно виділеним для послуг SNMP. Загальновідомі номери визначаються стандартами Internet.

Дані, що відправляють прикладним процесом через модуль UDP, досягають місця призначення як єдине ціле. Наприклад, якщо процес відправник робить 5 записів у UDP-порт, то процес-одержувач повинен буде зробити 5 читань. Розмір кожного записаного повідомлення буде збігатися з розміром кожного прочитаного. Протокол UDP зберігає межі повідомлень, обумовлені прикладним процесом. Він ніколи не поєднує кілька повідомлень в одне й не ділить одне повідомлення на частини.

За номером порту транспортні протоколи визначають, якому додатку передати вміст пакетів.

6.2.3. Зв'язок протоколів мережного й транспортного рівнів

TCP/IP – збірна назва для стека мережних протоколів різних рівнів, використовуваних в Інтернет. Термін "TCP/IP" позначає технологію міжмережевої взаємодії на основі сімейства протоколів TCP і IP (рис. 86).

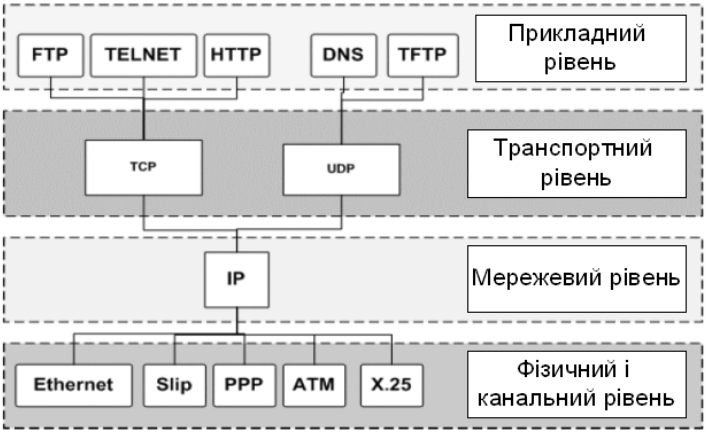


Рис. 86. Зв'язок протоколів TCP/IP

У це сімейство входять протоколи UDP, ARP, ICMP, TELNET, FTP і багато інших. Робота TCP/IP полягає в наступному. Протокол

TCP розбиває інформацію на порції й нумерує всі порції, щоб при одержанні можна було правильно зібрати інформацію. Далі за допомогою протоколу IP усі частини передаються одержувачу, де за допомогою протоколу TCP перевіряється, чи всі вони отримані. Оскільки окремі частини можуть подорожувати Інтернетом різними шляхами, то порядок їх приходу може бути порушений. Після одержання частин TCP розташовує їх у потрібному порядку й збирає в одне ціле.

Для протоколу TCP не має значення, якими шляхами інформація подорожує по Інтернет. Цим займається протокол IP. До кожної отриманої порції інформації протокол IP додає службову інформацію, з якої можна довідатися адреси відправника й одержувача інформації. За аналогією до пошти, дані поміщаються в конверт, на якому пишеться адреса одержувача. Далі протокол IP, як і пошта, забезпечує доставку всіх конвертів одержувачу. При цьому швидкість і шляхи проходження різних конвертів можуть бути різними. Якщо під час подорожі окремого конверта спостерігалися перешкоди, й інформація прийшла пошкодженою, треба повторний запит про відправлення пошкодженої частини доти, поки вона не буде прийнята без пошкоджень (це є це однією перевагою прийому-передачі інформації порціями).

Архітектура протоколів TCP/IP призначена для об'єднаної мережі, що складається із з'єднаних один з одним шлюзами окремих різнорідних підмереж, до яких підключаються різні машини. Кожна з підмереж працює відповідно до своїх специфічних вимог і має свою природу засобів зв'язку. Однак передбачається, що кожна підмережа може прийняти пакет інформації (дані з відповідним мережним заголовком) і доставити його за визначеною адресою в цій конкретній підмережі. Не потрібно, щоб підмережа гарантувала обов'язкову доставку пакетів і мала надійний наскрізний протокол. Таким чином, дві машини, підключені до однієї підмережі, можуть обмінюватися пакетами.

Коли необхідно передати пакет між машинами, підключеними до різних підмереж, то машина-відправник посилає пакет у відповідний шлюз (шлюз підключений до підмережі також як звичайний вузол). Звідти пакет направляється за певним маршрутом через систему шлюзів і підмереж, поки не досягне шлюзу, підключеного до тієї ж підмережі, що й машина-одержувач; там

пакет направляється до одержувача. Об'єднана мережа забезпечує дейтаграмний сервіс.

Використання в усіх вузлах і маршрутизаторах міжмережевого протоколу IP вирішує проблему доставки пакетів. Таким чином, забезпечується дейтаграмний сервіс на міжмережевому рівні Internet. Цей рівень забезпечує можливість стандартизації протоколів верхніх рівнів і є основою архітектури TCP/IP.

Лабораторна робота №12 (2 год.)

Тема: Перевірка TCP/IP-з'єднання за допомогою команд ping і net view

Мета: сформувати вміння діагностувати дієздатність мережевого з'єднання;

виховувати ціннісне ставлення студентів до навчальної діяльності.

Студент повинен знати: функції та особливості використання команд ping і net view; алгоритм перевірки мережевого з'єднання.

Студент повинен уміти: здійснювати перевірку TCP/IP-з'єднання за допомогою команд ping і net view.

Хід роботи

Інструктаж

Команда Net view

Виводить список доменів, комп'ютерів або загальних ресурсів на цьому комп'ютері. Викликана без параметрів, команда net view виводить список комп'ютерів в поточному домені.

Команда net view виводить список комп'ютерів, який виглядає так:

```
Ім'я сервера     Помітка
-------------------------------------------------
\\Production     Файловий сервер факультету
\\Print1         Принтер кафедри КТУН
\\Print2         Принтер кафедри КСМ
```

Приклади. Список загальних ресурсів комп'ютера \\A308-02 може бути отриманий за допомогою команди: net view \\A308-02.

Для перегляду ресурсів сервера NetWare з ім'ям \\IOIPT призначена команда: net view /network: nw \\IOIPT.

Для виведення списку комп'ютерів у домені або робочій групі education призначена команда: net view /domain: education.

Для виведення списку всіх серверів у мережі NetWare можна використовувати таку команду: net view /network: nw.

Netstat

Відображення активних підключень TCP, портів, що прослуховуються комп'ютером, статистики Ethernet, таблиці маршрутизації IP, статистики IPv4 (для протоколів IP, ICMP, TCP і UDP) і IPv6 (для протоколів IPv6, ICMPv6, TCP через IPv6 і UDP через IPv6). Запущена без параметрів, команда netstat відображує підключення TCP.

Приклади. Для виведення статистики Ethernet і статистики по всіх протоколах введіть наступну команду: netstat -e -s.

Для виведення статистики тільки протоколами TCP і UDP введіть наступну команду: netstat -s -p tcp udp.

Для виведення активних підключень TCP і кодів процесів кожні 5 секунд уведіть таку команду: netstat -o 5.

Для виведення активних підключень TCP і кодів процесів кожні з використанням числового формату введіть таку команду: netstat -n -o.

Nslookup

Надає відомості, призначені для діагностики інфраструктури DNS. Для використання цього засобу необхідно знати принцип роботи системи DNS. Засіб командного рядка Nslookup доступний, якщо встановлений протокол TCP/IP.

Практична частина

1. Щоб перевірити TCP/IP-з'єднання за допомогою команди ping, використайте команду ipconfig для перевірки мережевого адаптера який перебуває в стані "Мережа відключена".

2. Відкрийте командний рядок і зверніться командою "ping" до вузла призначення за його IP-адресою. Якщо команда ping видає повідомлення "Перевищений інтервал очікування для запиту", перевірте правильність IP-адреси віддаленого вузла, його працездатність, а також працездатність усіх шлюзів (маршрутизаторів) між локальним комп'ютером і віддаленим вузлом.

3. Щоб перевірити перетворення імен вузлів, зверніться командою ping до вузла за його іменем. Якщо команда ping видає повідомлення "Не вдається перетворити системне ім'я вузла", перевірте правильність імені вузла і з'ясуєте, чи може воно перетворюватися DNS -сервером.

4. Щоб перевірити TCP/IP-з'єднання за допомогою команди net view, відкрийте командний рядок і виконайте команду net view \\ім'я_комп'ютера. Команда net view виводить список загальних директорій і принтерів комп'ютера, що працює під управлінням Windows, створюючи тимчасовий сеанс з цим комп'ютером. Якщо на зазначеному комп'ютері немає загальних директорій і принтерів, команда net view видає повідомлення "У списку немає елементів".

Якщо команда net view видає повідомлення "Системна помилка 53", перевірте правильність імені, зазначеного в параметрі ім'я_комп'ютера, працездатність комп'ютера під управлінням Windows XP, а також працездатність усіх шлюзів (маршрутизаторів) між локальним комп'ютером і віддаленим комп'ютером з операційною системою Windows.

Якщо команда net view видає повідомлення "Сталася системна помилка 5. Відмовлено в доступі", перевірте, що вхід у систему був здійснений обліковим записом, який має дозвіл переглядати загальні ресурси на віддаленому комп'ютері.

Для усунення цієї неполадки виконайте такі дії.

– За допомогою команди ping виконайте обмін пакетами з комп'ютером "ім'я_комп'ютера".

Якщо команда ping видає повідомлення "Не вдається перетворити системне ім'я вузла", то "ім'я_комп'ютера" не вдається перетворити в IP -адрес.

– Зверніться командою net view за IP-адресою комп'ютера з операційною системою Windows XP: net view \\IP-адрес

Якщо команда net view виконується успішно, то "ім'я_комп'ютера" перетворюється в правильну IP-адресу.

Якщо команда net view видає повідомлення "Системна помилка 53", то на видаленому комп'ютері не працює служба доступу до файлів і принтерів мереж Microsoft.

Самостійна робота №12

Тема: Надлишковість, що реалізується на рівні доступу ієрархічної мережі

Мета: розвивати у студентів уміння проектувати реалізацію надлишковості на рівні доступу в ієрархічних комп'ютерних мережах.

Студент повинен знати: підходи до реалізації надлишковості на рівні доступу в ієрархічних мереж.

Студент повинен уміти: реалізовувати надлишковість на рівні доступу при проектуванні ієрархічної комп'ютерної мережі.

Хід роботи

Теоретична частина

1. Назвіть основну проблему, з яка виникає при реалізації подвійного підключення маршрутизатора рівня розподілу або маршрутизатора рівня доступу.

2. Яким питанням варто приділити особливу увагу при взаємному з'єднанні маршрутизаторів рівня розподілу або маршрутизаторів рівня доступу з метою забезпечення надмірності мережі?

3. Назвіть два основних принципи, яких треба дотримуватися при реалізації надмірності в мережі.

Практична робота

Законспектуйте основі положення стосовно реалізації надлишковості на рівні доступу ієрархічної мережі.

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Зв'язок прикладних протоколів з транспортним рівням стеку TCP/IP.

МОДУЛЬНА КОНТРОЛЬНА РОБОТА №6

Оберіть номер правильної відповіді:

1. До якого з перерахованих протоколів підходить визначення "Дейтаграмний протокол транспортного рівня"?

а) TFTP;
б) SPX;
в) TCP;
г) UDP.

2 б.

2. Протокол TCP працює:

а) із установленням з'єднання;
б) без установлення з'єднання.

2 б.

3. Сокет – це:

а) IP-адреса;
б) номер мережі, що входить в IP-адресу;
в) порт ПК, що перебуває в мережі;
г) IP-адреса й номер порту.

2 б.

4. Команда PING використовується:

а) для перегляду локальної Mac-адреси;
б) для перегляду IP-адреси ПК;
в) для перевірки з'єднання з віддаленим хостом;
г) для відправлення широкомовного повідомлення.

2 б.

5. DNS – це:

а) віддалений файл-сервер;
б) сервер доменних імен;
в) потужний пошуковий сервер.

2 б.

Всього: 10 балів.

Правильні відповіді

Питання	1	2	3	4	5
Відповідь	г	а	г	в	б

ЗМІСТОВИЙ МОДУЛЬ 7

ЕЛЕКТРОННА ПОШТА ТА ПРОТОКОЛ ПЕРЕДАЧІ ФАЙЛІВ. ПРОТОКОЛ ПЕРЕДАЧІ ГІПЕРТЕКСТОВИХ ПОВІДОМЛЕНЬ

Таблиця 51

Тематичний план змістового модуля

№ теми	Назва змістового модуля, теми	Усього годин	Лекції	Лабораторні заняття	Самостійна та індивідуальна робота
7.1	Електронна пошта та протокол передачі файлів	9	2	2	5
7.2	Протокол передачі гіпертекстових повідомлень	9	2	2	5
	Разом	***18***	***4***	***4***	***10***

Навчальні цілі: сприяти засвоєнню студентами знань щодо принципів функціонування електронної пошти та відповідних протоколів; основних модулів служби FTP.

Основні поняття: електронні листи, протокол SMTP, безпосередня взаємодія клієнта і сервера, схема з виділеним поштовим сервером, схема з двома поштовими серверами-посередниками, протоколи POP3 і IMAP, керуючий сеанс і сеанс передачі даних, команди взаємодії FTP-клієнта з FTP-сервером.

Методичні рекомендації щодо роботи з модулем: робота з модулем передбачає засвоєння лекційного матеріалу, участь у лабораторних заняттях, написання реферату (окремими студентами), самостійну роботу над визначеними питаннями теми, модульний контроль у формі тестування.

Після опрацювання цих тем студент може отримати бали,

наведені в табл. 52.

Таблиця 52

Оцінювання навчальних досягнень студентів

Поточний контроль					**Контрольна рейтингова оцінка**	**Проміжна рейтингова оцінка**
Робота на лабораторному занятті		**Самостійна робота**		**Індивідуальне завдання**		
Тема №7.1	**Тема №7.2**	**Тема №7.1**	**Тема №7.2**			
5	5	2	2	5	10	29

ТЕМА 7.1. ЕЛЕКТРОННА ПОШТА ТА ПРОТОКОЛ ПЕРЕДАЧІ ФАЙЛІВ

Лекція

План

1. Електронна пошта в Internet
2. Протокол SMTP
3. Протокол POP
4. Формат подання поштових повідомлень MIME
5. Служба архівів FTP

Література

Основна

1. *Компьютеры*, сети, Интернет: Энциклопедия: Наиболее полн. и подроб. рук. / Ю. Новиков, Д. Новиков, А. Черепанов, В. Чуркин; Под общ. ред. Ю. Новикова. – 2. изд. – М. [и др.]: Питер, 2003 (СПб.: ГПП Печ. Двор им. А.М. Горького). – 831 с.: ил.; 24 см.

2. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943

с.: ил.; 24 см. – (Учебник для вузов).

3. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. – 4-е изд. – М. [и др.]: Питер, 2005. – 991 с.: ил., табл.; 24 см. – (Классика computer science).

4. *Антонов В. М.* Сучасні комп'ютерні мережі / Валерій Миколайович Антонов. – К. : МК-Прес, 2005. – 480 с.

Додаткова

1. *Вишневский А.* Сетевые технологии Windows 2000 / Алексей Вишневский. – СПб. и др.: Питер, 2000. – 591 с.: ил., табл.; 24 см. – (Для профессионалов).

2. *Грир Т.* Сети Интернет: Пер. с англ. – М.: ИТД "Русская редакция", 2000. – 368 с.

3. *Джонс А.* Руководство системного администратора Windows: Windows 98. Windows NT. Windows 2000 / Аллен Джонс; [Пер. с англ. А. Файзрахманов]. – СПб.: Питер, 2000. – 367 с.: ил.; 24 см. – (Для профессионалов).

4. *Интеллектуальные* сети связи / Б.Я. Лихтциндер, М.А. Кузякин, А.В. Росляков, С.М. Фомичев. – 2. изд. – М.: Эко-Трендз, 2002. – 205 с.: ил., табл.; 24 см. – (Инженерная энциклопедия) (Технологии электронных коммуникаций: ТЭК).

5. *Камер Д.Э.* Компьютерные сети и Internet: Разработка приложений для Internet (пер. с англ. Птицына К.А.) Изд. 3-е + CD-Rom – 640 с.

6. *Комп'ютерні* мережі. Практикум : для студ. комп'ютерних спец. денної і заоч. форм навч. / [уклад. В. В. Швидкий]. – Черкаси : ЧДТУ, 2002. – 56 с.

7. *Методические* рекомендации к выполнению лабораторных работ по курсу "Internet-технологии и язык Java": для студ. спец. 7.080401, 7.080407 всех форм обучения / Харьковский гос. экономический ун-т / Сост. С. В. Минухин, С. В. Знахур. – Х. : ХГЭУ, 2004. – 103с.

8. *Рамський Ю. С.* Вивчення інформаційно-пошукових систем мережі Інтернет: навч.-метод. посіб. / Ю. С. Рамський, О. В. Рєзіна. – К. : РННЦ "ДІНІТ", 2004. – 60 с.

7.1.1. Електронна пошта в Internet

Електронна пошта – один з найважливіших інформаційних ресурсів Internet. Вона є масовим засобом електронних комунікацій,

призначеним для обміну повідомленнями (листами). Також через пошту можна одержати доступ до інформаційних ресурсів інших мереж.

Стандартною програмою відправлення є програма sendmail, що працює як поштовий кур'єр, який доставляє звичайну пошту у відділення зв'язку для подальшого розсилання. В Unix-системах sendmail сама є відділенням зв'язку. Вона сортує пошту й розсилає її адресатам.

Електронна пошта працює за принципом "клієнт"-"сервер". Клієнт (MS Outlook, The bat) готовить ("упаковує") і посилає серверу (поштове відділення) повідомлення, приймає й переглядає його. Сервер електронної пошти (Sendmail, MS Exchange) обробляє повідомлення (сортує) і відправляє локальному адресату або віддаленому серверу (поштовому відділенню).

Основні протоколи:

– *SMTP (Simple Mail Transfer Protocol)* – простий протокол передачі пошти, використовується для відправлення пошти, як клієнтом на сервер, так і сервером на інший сервер.

– *POP3 (Post Office Protocol)* – використовується для прийому пошти клієнтом із сервера.

– *UUCP (Unix-Unix-CoPy)* – використовується для відправлення й прийому пошти, як клієнтом на (з) сервер(а), так і сервером на інший сервер. Тепер майже не використовується, тому розглядати не будемо.

SMTP є протоколом прикладного рівня й використовує транспортний протокол TCP. Разом із цим протоколом використовується й UUCP протокол. Різниця між SMTP і UUCP полягає в тому, що при використанні першого протоколу sendmail намагається знайти машину-одержувача пошти й установити з нею взаємодію в режимі on-line для того, щоб передати пошту в її поштову скриньку, пошта досягає поштової скриньки одержувача за лічені хвилини й час одержання повідомлення залежить тільки від того, як часто одержувач переглядає свою поштову скриньку. При використанні ж UUCP пошта передається за принципом "stop-go", тобто повідомлення передається по ланцюжку поштових серверів від однієї машини до іншої поки не досягне машини-одержувача або не буде відкинуто через відсутність абонента-одержувача. З одного боку, UUCP дозволяє доставляти пошту по поганих телефонних

каналах, а з іншого – можна одержати повернене повідомлення через добу після його відправлення через те, що допущено помилку в імені користувача.

Основою будь-якої поштової служби є система адрес. В Internet прийнята система адрес, що базується на доменній адресі машини, підключеної до мережі. Наприклад, для користувача paul машини з адресою polyn.net.kiae.su поштова адреса буде виглядати як: paul@polyn.net.kiae.su.

Таким чином, адреса складається із двох частин: ідентифікатора користувача, що записується перед знаком "комерційного @", і доменної адреси машини, що записується після знака "@".

7.1.2. Протокол SMTP

SMTP – Simple Mail Transfer Protocol, використовує порт за замовчуванням – 25. Основним недоліком протоколу є відсутність аутентифікація й "до завантаження" (як в FTP, HTTP) повідомлень, тобто якщо посилає великий лист (10Мбайт), то в разі розриву з'єднання повідомлення доведеться передавати заново. Тому великі листи необхідно різати на частини.

Модель протоколу: клієнт ініціює з'єднання із сервером; клієнт посилає запити на обслуговування; сервер відповідає на ці запити.

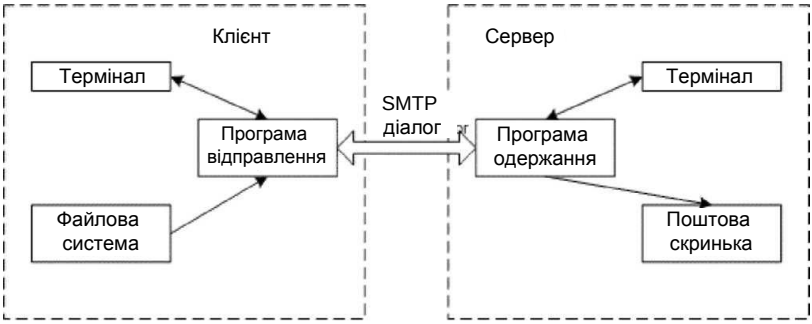


Рис. 87. Модель протоколу SMTP

7.1.3. Протокол POP

Post Office Protocol (POP) – протокол доставки пошти користувачеві з його поштової скриньки поштового сервера POP. Коли пошта прийшла на сервер (по SMTP), вона розкладається по поштових скриньках. Щоб забрати пошту із скриньки, потрібний

POP.

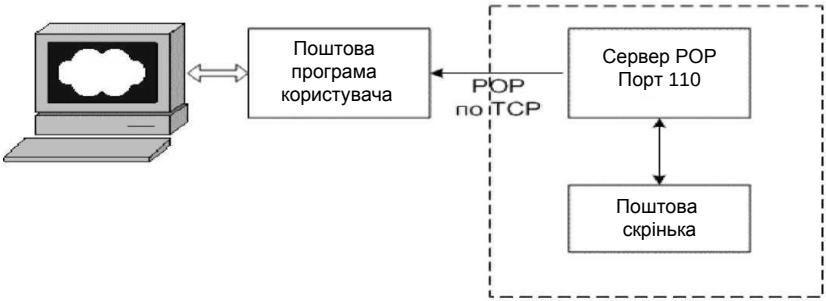


Рис. 88. Модель протоколу POP

У протоколі POP3 обговорені три стадії процесу одержання пошти:

- авторизація;
- транзакція;
- оновлення (завершення транзакції).

Після того як сервер і клієнт POP3 установили з'єднання, починається стадія авторизації, на якій клієнт ідентифікує себе для сервера. Якщо авторизація пройшла успішно, сервер відкриває поштову скриньку клієнта й починається стадія транзакції. У ній клієнт або запитує в сервера інформацію (наприклад, список поштових повідомлень), або просить його зробити певну дію (наприклад, видалити поштове повідомлення). Нарешті, на стадії оновлення сеанс зв'язку закінчується.

Відповідь сервера може бути або позитивною або негативною.

7.1.4. Формат подання поштових повідомлень MIME

MIME означає "Multipurpose Internet Mail Extensions" (Багатоцільові розширення поштового стандарту Internet). Цей стандарт описує, як пересилати по електронній пошті програми, графічні, мультимедійні, змішані дані. Типове застосування MIME – пересилання графічних зображень, аудіо, документів Word, програм і навіть просто текстових файлів, тобто, коли важливо, щоб у ході пересилання не провадилося ніяких перетворень над даними. MIME також дозволяє розмічати лист на частині різних типів так, щоб одержувач (поштова програма) міг визначити, що робити з кожною із частин листа.

Оскільки файли можуть бути різними (.gif, .doc, .pdf), браузер

повинен розуміти, що з ними робити. Цю проблему вирішує стандарт "MIME – типи". Він повідомляє клієнту, який тип файлів отриманий, наприклад: Content-type: image/gif (графіка GIF), Content-type: image/jpeg (графіка JPG)

Браузери використовують MIME-типи у своїх HTTP-заголовках для того, щоб повідомити, у яких форматах вони бажають приймати дані (якщо сервер може видати файл у різних форматах). Сервери використовують MIME-типи в HTTP-заголовках Content-Type, щоб повідомити клієнту про те, у якому форматі передається прикладений уміст: чи те це HTML, якому потрібно форматувати, чи то це GIF або JPEG, що вимагає візуалізації, чи те це дані у форматі PDF, для якого потрібно відкривати зовнішню програму перегляду або використати додатковий програмний засіб.

Стандарт MIME призначений для опису тіла поштового повідомлення Internet. Попередником MIME є стандарт поштового повідомлення ARPA (RFC-822). Стандарт RFC-822 був розроблений для обміну текстовими повідомленнями. З моменту опублікування стандарту можливості апаратних і програмних засобів пішли далеко вперед і стало ясно, що багато типів інформації, які широко використаються в мережі, неможливо передати поштою без спеціальних перетворень.

7.1.5. Служба архівів FTP

Технологія FTP була розроблена в рамках проекту ARPA і призначена для обміну великими обсягами інформації між машинами з різною архітектурою. Головним у проекті було забезпечення надійної передачі й тому із сучасної точки зору FTP здається перевантаженим зайвими, рідко використовуваними можливостями. Стрижень технології складає FTP-протокол.

FTP-архіви є одним з основних інформаційних ресурсів Internet. Фактично, це розподілене сховище текстів, програм, фільмів, фотографій, аудіозаписів та іншої інформації, що зберігається у вигляді файлів на різних комп'ютерах у всьому світі.

Типи інформаційних ресурсів. Інформація в FTP-архівах розділена на три категорії:

– захищена інформація, режим доступу до якої визначається її власниками й дозволяється за спеціальною згодою зі споживачем; до цього виду ресурсів належать комерційні архіви, закриті

некомерційні ресурси, приватна некомерційна інформація;

– інформаційні ресурси обмеженого використання; сюди можуть належати ресурси обмеженого часу використання або обмеженого часу дії, тобто користувач може використати поточну версію, але ніхто не буде надавати йому підтримку;

– вільно розповсюджувані інформаційні ресурси; до яких належить все, що можна вільно одержати по мережі без спеціальної реєстрації. Це може бути документація, програми і т.д. Варто зазначити, що вільно розповсюджуване програмне забезпечення не має сертифіката якості, але, як правило, його розроблювачі відкриті для обміну досвідом.

З вище перерахованих ресурсів найцікавішими, із зрозумілих причин, є дві останніх категорії, які, як правило, оформлені у вигляді FTP-архівів.

Служба FTP (від протоколу – File Transfer Protocol) призначена для обміну файлами й побудована за технологією "клієнт-сервер".

File Transfer Protocol – протокол прикладного рівня, який використовує службу FTP для передачі файлів. FTP відрізняється від інших програм тим, що він використовує два TCP з'єднання для передачі файлу.

Керуюче з'єднання – з'єднання для посилки команд серверу й одержання відповідей від нього. Для каналу керування використовується протокол Telnet.

З'єднання даних – з'єднання для передачі файлів.

У FTP з'єднання ініціюється інтерпретатором протоколу користувача. Керування обміном здійснюється по каналу керування в стандарті протоколу Telnet. Команди FTP генеруються інтерпретатором протоколу користувача й передаються на сервер. Відповіді сервера відправляються користувачу також по каналу керування. Зазвичай користувач має можливість установити контакт з інтерпретатором протоколу сервера й відмінними від інтерпретатора користувача засобами.

Команди FTP визначають параметри каналу передачі даних, самого процесу передачі, а також характер роботи з віддаленими й локальною файловими системами. Сесія керування ініціює канал передачі даних. При організації каналу передачі даних послідовність дій інша, відмінна від організації каналу керування. У цьому випадку сервер ініціює обмін даними відповідно до погодженого в сесії

керування параметрами.

Канал даних встановлюється для хоста той же, що й для каналу керування, через який ведеться настроювання каналу даних. Канал даних може бути використаний як для прийому, так і для передачі даних.

Можлива ситуація, коли дані можуть передаватися на третю машину. У такому разі користувач організує канал керування із двома серверами й організує прямий канал даних між ними. Команди керування йдуть через користувача, а дані прямо між серверами.

Канал керування повинен бути відкритий при передачі даних між машинами. У разі його закриття передача даних припиняється.

Протокол FTP визначає запит-відповідний спосіб взаємодії між програмою-клієнтом і програмою-сервером.

Робота FTP на прикладному рівні складається з кількох етапів:

1. Ідентифікація (введення імені й пароля).
2. Вибір каталогу.
3. Визначення режиму обміну (поблочний, потоковий, ascii або двійковий).
4. Виконання команд обміну (get, mget, dir, mdel, mput або put).
5. Завершення процедури (quit або close).

У старих версіях для передачі даних використався тільки 20-й порт (активний режим), у сучасних версіях FTP-серверів порт для каналу даних може призначається сервером з нестандартних (N > 1024) портів (пасивний режим).

Лабораторна робота №13 (2 год.)
Тема: Використання протоколу FTP.

Мета: виробити основні навички підключення до FTP-сервера з використанням вбудованого клієнта операційної системи;

виховувати ціннісне ставлення студентів до майбутньої професійної діяльності.

Студент повинен знати: основні команди для управління пересиланням файлів протоколом FTP, принципи роботи з FTP-клієнтом.

Студент повинен уміти: здійснювати перегляд каталогів та

переселення фалів з використання протоколу FTP.

Обладнання: комп'ютерний клас з локальною мережею на основі стандарту Fast Ethernet, сервер FTP, операційна система з вбудованим консольним FTP-клієнтом.

Інструктаж

FTP вимагає вказати комп'ютер, з яким ви бажаєте з'єднатися. Команда:

ftp <ім'я видаленого комп'ютера>

запускає програму і встановлює з'єднання з певним комп'ютером. Після цього вимагається вказати ім'я користувача і пароль.

ftp sonne.uiuc.edu
Connected to sonne.uiuc.edu.
220 sonne FTP server (SunOS 4.1) ready.
Name (ux.uiuc.edu) : krol - ім'я користувача krol
331 Password required for krol.
Password: - пароль на екрані не відображується
230 Users krol logged in.

При роботі з ftp не завжди відомо, які файли потрібні і де вони знаходяться. Для отримання інформації про зміст каталогів видаленого комп'ютера використовуються команди dir і ls. Вони мають однаковий формат:

ftp > dir ім'я_каталогу ім'я_локального_файлу
ftp > ls ім'я_каталогу ім'я_локального_файлу

Практична частина

Підключитися до сервера FTP.
Здійснити перегляд списку файлів у каталогах FTP.
Скопіювати файли на сервер.
Скопіювати файли на локальний комп'ютер.

Самостійна робота №13

Тема: Реорганізація ієрархічної комп'ютерної мережі для стабілізації її роботи

Мета: розвивати аналітичні вміння студентів з упровадження заходів щодо стабілізації роботи мережі.

Студент повинен знати: методи та засоби реорганізації комп'ютерної мережі.

Студент повинен уміти: обирати та реалізовувати засоби

стабілізації комп'ютерної мережі.

Хід роботи

Теоретична частина

1. Яку роль відіграє ієрархія у вдало спроектованій мережі?
2. Назвіть основний інструмент мережевого інженера, що дозволяє обмежити ділянку мережі, на яку впливає зміна топології.
3. Як виявити канали передачі інформації, усунення яких з ядра зі структурою з повним об'єднанням дозволить зменшити загальну кількість маршрутів, що проходять через ядро?

Практична частина

Завдання

Законспектуйте основні положення щодо реорганізації ієрархічної комп'ютерної мережі для стабілізації її роботи.

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Засоби безпеки, що реалізуються в поштових протоколах".

ТЕМА 7.2. ПРОТОКОЛ ПЕРЕДАЧІ ГІПЕРТЕКСТОВИХ ПОВІДОМЛЕНЬ

Лекція

План

1. Служба WWW

2. Протокол обміну гіпертекстовою інформацією

Література

Основна

1. *Компьютеры*, сети, Интернет: Энциклопедия: Наиболее полн. и подроб. рук. / Ю. Новиков, Д. Новиков, А. Черепанов, В. Чуркин; Под общ. ред. Ю. Новикова. – 2. изд. – М. [и др.]: Питер, 2003 (СПб.: ГПП Печ. Двор им. А.М. Горького). – 831 с.: ил.; 24 см.

2. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

3. *Олифер В. Г.* Новые технологии и оборудование IP-сетей / Виктор Олифер, Наталья Олифер. – СПб. и др.: BHV, 2000. – 512 с.: ил., табл.; 24 см. – (Мастер) (Современные сетевые технологии).

4. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. – 4-е изд. – М. [и др.]: Питер, 2005. – 991 с.: ил., табл.; 24 см. – (Классика computer science).

Додаткова

1. *Башмаков А. И.* Интеллектуальные информационные технологии: учеб. пособие для студ. вузов, обуч. по направлению подгот. дипломированных спец. "Информатика и вычислительная техника" / А. И. Башмаков, И. А. Башмаков – М. : МГТУ им.Н.Э.Баумана, 2005. – 302 с.

2. *Білоус Л. Ф.* Інформаційні мережі : навч. посібник / Білоус Л. Ф. – К. : Логос, 2005. – 140 с.

3. *Вишневский А.* Сетевые технологии Windows 2000 / Алексей Вишневский. – СПб. и др.: Питер, 2000. – 591 с.: ил., табл.; 24 см. – (Для профессионалов).

4. *Грир Т.* Сети Интернет: Пер. с англ. – М.: ИТД "Русская редакция", 2000. – 368 с.

5. *Ибе О.* Сети и удаленный доступ: Протоколы, проблемы, решения / Оливер Ибе. – М.: ДМК Пресс, 2002. – 332 с.: ил.; 23 см. – (Серия "Защита и администрирование").

6. *Камер Д.Э.* Компьютерные сети и Internet: Разработка приложений для Internet (пер. с англ. Птицына К.А.) Изд. 3-е + CD-

Rom – 640 с.

7. *Коваленко А. Є.* Корпоративні комп'ютерні мережі та телекомунікації : конспект лекцій для студ. спец. 7.080401 "Інформаційні управляючі системи та технології" ден. форми навч. / Анатолій Єпіфанович Коваленко. – К. : НУХТ, 2004. – 27 с.

8. *Контроль* та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології : навчальний посібник / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. – Х. : "Компанія СМІТ", 2004. – 544 с.

7.2.1. Служба WWW

Служба WWW (World Wide Web) призначена для обміну гіпертекстовою інформацією та побудована за схемою "клієнт-сервер".

Браузер (Internet Explorer, Opera) є мультипротокольним клієнтом та інтерпретатором HTML. Як типовий інтерпретатор, клієнт залежно від команд (тегів) виконує різні функції. У коло цих функцій входить не тільки розміщення тексту на екрані, але обмін інформацією із сервером у міру аналізу отриманого HTML-тексту, що найбільш наочно відбувається при відображенні вбудованих у текст графічних образів.

Сервер HTTP (Apache, IIS) обробляє запити клієнта на одержання файлу.

На початку служба WWW базувалася на трьох стандартах:

– *HTML (HyperText Markup Language)* – мова гіпертекстової розмітки документів;

– *URL (Universal Resource Locator)* – універсальний спосіб адресації ресурсів у мережі;

– *HTTP (HyperText Transfer Protocol)* – протокол обміну гіпертекстовою інформацією.

Пізніше додали *CGI (Common Gateway Interface)* – універсальний інтерфейс шлюзів. Створений для взаємодії HTTP – сервера з іншими програмами установленими на сервері.

Розглянемо схему роботи WWW сервера.

WWW сервер – це така частина глобальної або корпоративної мережі, що дає можливість користувачам мережі одержувати доступ до гіпертекстових документів, розташованих на сервері. Для взаємодії з WWW сервером користувач мережі повинен використовувати спеціалізоване програмне забезпечення – *браузер*

(від англ. browser) – програма перегляду.

Розглянемо схему роботи WWW-сервера:

1. Користувач мережі запускає браузер, у функції якого входить:
   - встановлення зв'язку з сервером;
   - одержання необхідного документа;
   - відображення отриманого документа;
   - реагування на дії користувача – доступ до нового документа.

Після запуску браузер по команді користувача або автоматично встановлює зв'язок із заданим WWW – сервером і передає йому запит на отримання заданого документа.

2. WWW сервер шукає запитуваний документ і повертає результати браузеру.

3. Браузер, одержавши документ, відображає його користувачу й очікує його реакції. Можливі варіанти:
   - уведення адреси нового документа;
   - друк, пошук, інші операції з поточним документом;
   - активізація (натискання) спеціальних зон отриманого документа, названих посиланнями (link) і асоційованими з адресою нового документа. У першому й третьому випадку відбувається звернення за новим документом.

7.2.2. Протокол обміну гіпертекстовою інформацією

HTTP – це протокол прикладного рівня, розроблений для обміну гіпертекстовою інформацією в мережі Internet, який використовується Word Wide Web з 1990 року.

Реальна інформаційна система вимагає набагато більшої кількості функцій, ніж просто пошук. HTTP дозволяє реалізувати в рамках обміну даними набір методів доступу, що базуються на специфікації універсального ідентифікатора ресурсів (URI), застосовуваного у формі універсального локатора ресурсів (URL) або універсального імені ресурсу (URN). Повідомлення по мережі при використанні протоколу HTTP передаються у форматі, схожому з форматом поштового повідомлення Internet або з форматом повідомлень MIME. HTTP використовується для взаємодії програм-клієнтів із програмами-шлюзами, що дозволяють доступ до ресурсів електронної пошти Internet (SMTP), списків новин (NNTP), файлових архівів (FTP), систем Gopher і WAIS. Протокол розроблений для

доступу до цих ресурсів за допомогою проміжних програм-серверів (proxy), які дозволяють передавати інформацію між різними інформаційними службами без втрат. Протокол реалізує принцип "запит/відповідь". Програма, що запитує, – клієнт – ініціює взаємодію із програмою, що відповідає, – сервером, і надсилає запит, що включає в себе метод доступу, адресу URI, версію протоколу, інформацію клієнта, і, можливо, тіло повідомлення клієнта. Сервер відповідає рядком стану, що включає версію протоколу й код повернення. Таке повідомлення містить інформацію сервера, метаінформацію й тіло повідомлення.

При роботі в Internet для обслуговування HTTP-запитів використовується 80 порт TCP/IP. Практика використання протоколу така, що клієнт установлює з'єднання й чекає відповіді сервера. Після відправлення відповіді сервер ініціює розрив з'єднання. Таким чином, при передачі складних гіпертекстових сторінок з'єднання може встановлюватися кілька разів. Розглянемо більш докладно механізм взаємодії та форму переданої інформації.

Форма запиту клієнта. Програма-клієнт посилає після встановлення з'єднання запит серверу, який може мати дві форми: форму повного запиту і форму простого запиту. Простий запит містить метод доступу й запит ресурсу. Наприклад:

```
GET http://polyn.net.kiae.su/
```

У цьому записі слово GET позначає метод доступу GET, а http://polyn.net.kiae.su/ – це запит ресурсу.

Загальний вид повного запиту виглядає так: <Повний запит>:= <Рядок Запиту> (<Загальний заголовок>|<Заголовок запиту>|<Заголовок позначення ресурсу>)<символ нового рядка>[<тіло ресурсу>].

Квадратні дужки тут позначають необов'язкові елементи заголовка. Рядок запиту – це, практично, простий запит ресурсу. Відмінність полягає в тому, що в рядку запиту можна вказувати різні методи доступу й за запитом ресурсу варто вказувати версію протоколу. Наприклад, для виклику зовнішньої програми можна використати такий рядок запиту:

```
POST http://polyn.net.kiae.su/cgi-bin/test HTTP/1.0
```

У цьому випадку використовується метод POST і протокол

версії 1.0.

В обох формах запиту важливе місце займає форма запиту ресурсу, що кодується відповідно до специфікації URI. При звертанні до сервера можна використати як повну форму URL, так і спрощену.

Методи доступу. Нині в практиці World Wide Web реально використовуються тільки три методи доступу: POST, GET, HEAD.

GET – метод, що дозволяє одержати дані, задані у формі URI у запиті ресурсу. Якщо посилаються на програму, то вертається результат виконання цієї програми, але не текст програми. Додаткові дані, які треба передати для обробки, кодуються в запит ресурсу. При використанні методу GET у поле тіла ресурсу вертається власне викликана інформація (текст HTML-документа, наприклад).

HEAD – метод, аналогічний GET, але не повертає тіла ресурсу. Використовується для одержання інформації про ресурс і для тестування гіпертекстових посилань.

POST – цей метод розроблений для передачі великого обсягу інформації на сервер. Ним користуються для анотування наявних ресурсів, посилки поштових повідомлень, роботи з формами інтерфейсів до зовнішніх баз даних і зовнішнім програмам, що на відміну від GET і HEAD, у POST передається тіло ресурсу, що і є інформацією з поля форм або інших джерел введення.

Відповідь сервера. Відповідь сервера може бути, як і запит, спрощеною або повною. При спрощеній відповіді сервер повертає тільки тіло ресурсу (наприклад, текст HTML-документа). При повній – клієнту вертається рядок стану, загальний заголовок, заголовок відповіді, заголовок ресурсу й тіло ресурсу. Повна відповідь виглядає так: <Повна відповідь>:= <Рядок стану> (<Загальний заголовок>|<Заголовок відповіді>|<Заголовок ресурсу>) <символ нового рядка>[<тіло ресурсу>].

Рядок стану складається з версії протоколу, коду повернення й короткого опису цього коду. Наприклад, вона може виглядати так:

```
HTTP/1.0 200 Ok.
```

Заголовок відповіді сервера може складатися з адреси URI запитуваного ресурсу, і/або найменування програми сервера, і/або коду ідентифікації для роботи в захищеному режимі. Склад полів заголовка ресурсу є однаковим і для запиту клієнта і для відповіді сервера, і складається з дозволу на метод доступу, типу кодування тіла ресурсу (змісту ресурсу), довжини тіла ресурсу, типу ресурсу, час дії певної копії ресурсу, часу останньої зміни ресурсу й

розширення заголовка.

Лабораторна робота №14 (2 год.)
Тема: Дослідження роботи протоколу HTTP

Мета: сформувати вміння аналізувати діяльність протоколу HTTP;

виховувати ціннісне ставлення студентів до навчальної діяльності.

Студент повинен знати: методи протоколу HTTP, структуру запитів та відповідей протоколу HTTP.

Студент повинен уміти: здійснювати аналіз діяльності протоколу HTTP.

Хід роботи

Інструктаж

Протокол HTTP працює поверх TCP/IP. Фактично, це означає, що клієнт відкриває сокет до сервера, пише туди HTTP запит (request), сервер читає його, обробляє і посилає результат обробки (response) назад клієнту.

Будь-який HTTP-запит, як і будь-яка відповідь по цьому протоколу, складається з двох блоків: заголовка і даних. Заголовок відокремлений від даних подвійним символом перенесення рядка.

Оскільки HTTP був спочатку орієнтований на пересилку передусім текстової інформації, то HTTP-заголовок є повністю текстовим, усі символи, що передаються в ньому, є друкованими (передусім цифри і літери латинського алфавіту A-Z, a-z, а також набір інших відображуваних символів та символ перенесення рядка). При передачі в HTTP-заголовку інших символів буде видана помилка "400 Bad request" – помилковий запит.

HTTP запит. Розберемо HTTP-заголовок запиту. Перший рядок, перше слово – ім'я методу запиту. Це слово може бути одне з наступних: OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, CONNECT.

Ми розглянемо методи – GET і POST.

Відразу після слова, що визначає метод, іде символ пропуску і вказаний URI документу, що запрошується з сервера. Після URI документу йде ще один символ пропуску і назва протоколу (рядок "HTTP/1.1").

Для HTTP існує різновид стандарту URI, що називається URL (Uniform Resource Location – формат запису знаходження ресурсу),

наприклад:

```
http://devresource.org:80/javalinks/catalog.php3?
name=java&cat=2#section1
```

Як і кожен рядок HTTP заголовка, перший рядок запиту закінчується символом перенесення рядка.

Далі приведені основні параметри для HTTP-заголовка. Кожен рядок, що містить параметр починається з ключового слова (наприклад "Host"), потім іде символ "двокрапка", "пропуск", "значення параметра" і "символ перенесення рядка". Тут наводиться не весь список можливих полів запиту та їх значень.

```
Host: localhost
```

Параметр "Host" містить ім'я хоста, наприклад "localhost" або "localhost:80" (якщо порт 80, то його можна не вказувати, якщо порт відрізняється від 80, то його треба обов'язково вказати). Це другий обов'язковий параметр HTTP заголовка (перший – HTTP метод і ім'я протоколу).

```
Accept: image/gif, image/x – xbitmap, image/jpeg,
image/pjpeg, */*
```

У цьому параметрі через кому вказані MIME типи документів, які здатний обробити браузер. Так само в MIME типі вказуються доступні до обробки кодування документів. Символ "*" означає, що браузер може обробити увесь клас документів. Приміром, image/* означає, що браузер може обробити і image/gif, і image/x – xbitmap, і image/jpeg, і image/pjpeg і взагалі будь-які документи зображень, а завершальний тип – */* вказує, що браузер обробить будь-які документи, прислані сервером. Насправді це зазвичай означає, що якщо MIME тип присланого сервером документа браузеру невідомий, то він запропонує зберегти його на диск.

```
Accept – Language: ru, en
Accept – Charset: windows-1251, KOI8-R
```

Ці параметри відповідають за визначення мови. У першому – через кому вказуються головні мови для сервера. Зокрема Google.com, обробивши цей параметр, переспрямує вас на російськомовну сторінку. У другому – кодування, у якому закодовані символи в CGI запиті. Також через кому можуть бути вказані кодування, яким віддається перевага для відповіді сервера.

```
Accept – Encoding: compressed, gzip
```

Тут вказані можливі варіанти пересилки даних. Зокрема, як приклад запиту, браузер готовий приймати HTML документ в

архівованому виді.

```
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.0; MyIE2; .NET CLR 1.0.3705)
```

User-Agent – ім'я HTTP клієнта. Багато браузерів тут же вказують операційну систему, плагіни і інше.

```
Referer: http://localhost/?test=test
```

"Referer" – дуже корисний параметр. Значенням цього поля є URL ресурсу, з якою був здійснений перехід. Фактично, коли ви натискаєте на посилання в HTML документі, швидше за все адреса цього документу буде записана в цей параметр.

```
Cookie: param1=value1; param2=value2
```

У параметрі "Cookie" браузер відправляє cookie (чи просто кукі) – дані, записані сервером на комп'ютер клієнта. Як видно, кукі відправляються не за допомогою CGI інтерфейсу, їх форматування відрізняється:

```
[ім'я параметра1]=[значення параметра1];
[ім'я параметра2]=[значення параметра2];
```

Утім, значення параметрів кодуються точно так, як і в CGI – "неправильні" символи замінюються за допомогою %NN.

```
Range-Unit: 2015|1024
```

Дуже корисний параметр "Range-Unit", що дозволяє отримати з сервера не весь документ, а тільки його частину. Саме цей параметр використовують менеджери докачок типу flashget. У цьому прикладі зазначено, що клієнт хоче отримати частину документа, починаючи з 2015 байта і завдовжки в 1 кілобайт. Якщо сервер підтримує докачку і документ не є динамічним, то буде видана запрошувана частина. Інакше сервер поверне помилку про те, що дія не підтримується або почне видавати документ повністю.

```
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
```

"Pragma" та "Cache-Control" – параметри, які вказують серверу, що цей документ не потрібно брати з кеша. Інші варіанти значень можуть бути:

– "public" – документ є публічним, його може брати будь-який клієнт з кеша;

– "private" – документ є приватним, тільки для цього клієнта;

– "no-store" – не зберігати в кеш;

– "no-transform" – не модифікувати документ, що вже міститься в кеші;

– "must-revalidate" – зобов'язаний відновити документ, що

лежить у кеші (і браузер і проксі);

– "proxy-revalidate" – у кеші повинен відновити тільки проксі сервер;

– "max-age=[seconds]" – зберігає в кеш на кількість секунд, вказаних у параметрі, починаючи з часу збереження; після закінчення цього часу, документ видаляється.

Допустимо вказівка параметра в такому вигляді:

```
Pragma: must-revalidate, max-age=1000
```

але деякі комбінації значень можуть викликати помилку "400 Bad request"

```
Proxy-Connection: Keep-Alive
```

Параметр "Proxy-Connection" вказує на те, що з'єднання з сервером підтримуватиметься постійно. Інший варіант – Proxy-Connection: close, означає, що браузер уже послав усі дані серверу і тепер тільки чекатиме відповіді.

Для запиту до сервера обов'язковими є лише два параметри: перший рядок, що уточнює метод запиту й адресу ресурсу параметра "Host", що містить ім'я хосту і порт сервера.

Відправка файлу методом POST. Окремо варто розповісти про відправку файлів за допомогою методу POST. Для того, щоб відправити файл цим методом, треба у формі відправки повідомлень вказати спеціальний параметр "enctype='multipart/form-data":

```
enctype='multipart/form-data'
```

Припустимо, ми відправляємо файл "c:\est.txt" розміру 14 байт, що містить текст "This a test!". У цьому випадку дані будуть відправлені таким чином:

```
POST http://localhost/ HTTP/1.1
Content-Type: multipart/form-data; boundary=---------------
-----------7d33188e01e4
Host: localhost
Content-Length: 254

--------------------------7d33188e01e4
Content-Disposition: form-data; name="test"

test
--------------------------7d33188e01e4
Content-Disposition: form-data; name="testfile";
filename="c:\est.txt"
Content-Type: text/plain
```

```
This a test!!!
```

Як видно з прикладу, додається ще два HTTP-параметри:

```
Content-Type: multipart/form-data; boundary=---------------
------------7d33188e01e4
```

Цей рядок свідчить, що усі дані передаватимуться частинами, а дільником цих частин виступатиме рядок "----------7d33188e01e4". Взагалі-то, дільником може виступати абсолютно будь-який набір символів, аби подібного не було в даних, що передаються.

```
Content-Length: 342
```

Цей параметр повідомляє серверу кількість даних, що містяться після HTTP-заголовка.

Самі дані передаються також за допомогою HTTP-subheader (субзаголовок HTTP)

```
Content-Disposition: form-data; name="test"
```

Тут зазначається назва змінної, після чого йдуть два символи перенесення рядка й самі дані. Кінець даних визначає або символ перенесення рядка і дільника (boundary), або кінець одержаних даних.

Інший субзаголовок – Content–Type: text/plain

Він передає серверу MIME тип файлу, що відправляється. Треба зазначити, що при передачі даних у такий спосіб не цензуровані символи не замінюються на %NN, а передаються, як є.

HTTP-відповідь. Перейдемо до відповіді сервера. Ось приклад відповіді сервера клієнту (сервер видає текстовий файл, що містить рядок "This a test!"):

```
HTTP/1.1 200 OK
Date: Mon, 07 Apr 2003 14:40:25 GMT
Server: Apache/1.3.20 (Win32) PHP/4.3.0
Keep – Alive: timeout=15, max=100
Connection: Keep – Alive
Transfer – Encoding: chunked
Content – Type: text/plane

This a test!!!
```

Сервер видає файл test.zip:

```
HTTP/1.1 200 OK
Date: Mon, 07 Apr 2003 14:51:19 GMT
Server: Apache/1.3.20 (Win32) PHP/4.3.0
Last – Modified: Mon, 07 Apr 2003 14:51:00 GMT
Accept – Ranges: bytes
```

```
Content – Length: 673
Keep – Alive: timeout=15, max=100
Connection: Keep – Alive
Content – Type: application/zip
Content – Disposition: attachment; filename=test.zip
Pragma: no – cache

.......(вміст zip файлу)
```

Тут ми теж бачимо HTTP-заголовок, відокремлений від тіла документа двома символами перенесення рядка.

Розберемо заголовок. Він починається з назви протоколу "HTTP/1.1", після чого йде пропуск, потім – код повернення "200 OK". Після коду повернення йде символ перенесення рядка.

Параметри HTTP-відповіді. Продовжимо розбір параметрів заголовка відповіді сервера. Передусім згадаємо, що параметри "Cache-Control", "Pragma" і "Proxy-Connection" ідентичні як для запиту, так і для відповіді, тому все сказане про них вище, застосовується і тут.

```
Set-Cookie: name=value;expires=date;path=PATH;
            domain=HOSTNAME;secure
```

Детально не зупинятимемося на цьому параметрі. Він встановлює або видаляє cookie.

```
Location: http://www.devresource.org
```

Цей параметр вказує браузеру, що треба відкрити ресурс http://www.devresource.org замість поточного. У значенні цього параметра вказується URI ресурсу для переходу.

```
Date: Mon, 07 Apr 2003 14:51:19 GMT
```

Параметр показує дату документу. Це або поточна дата (якщо документ динамічний), або дата створення файлу. Дата представлена у форматі GMT.

```
Last-Modified: Mon, 07 Apr 2003 14:51:00 GMT
```

Параметр показує дату останньої зміни документу.

```
Server: Apache/1.3.20 (Win32) PHP/4.3.0
```

Параметр містить ім'я сервера.

```
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
```

Ці два параметри повідомляють, що підтримується постійне з'єднання з сервером (навпаки було б "Connection: close"), що поточний час timeout для сокета сервера складає 15 секунд і клієнт може змінити цей час максимум до 100 секунд.

```
Accept-Ranges: bytes
```

Цей параметр існує, щоб вказати клієнту, яка частина документа пересилається йому (у разі присутності "Range-Unit" в запиті). Параметр цей може містити значення "bytes", це означає, що пересилається файл повністю. Так само "none" (цей параметр може бути просто опущений), що означає – докачка не використовується або не підтримується, а рядок "Accept-Ranges: 1:637" означатиме, що пересилається частина документа з байта під номером 1 і завдовжки в 637 байт.

```
Content-Length: 673
```

довжина документу, що пересилається.

```
Content-Type: application/zip
```

MIME тип документа, що пересилається.

```
Content-Disposition: attachment; filename=test.zip
```

вказує, що файл, який пересилається, має назву "test.zip".

```
Accept-Charset: windows-1251
```

вказує кодування тексту документа (в цьому випадку – російське кодування windows).

```
Accept-Encoding: compress, gzip
```

цей параметр використовується сервером, щоб вказати клієнту, що документ йому передається в стислому вигляді (і для стискання використовується стандарт gzip).

```
Accept-Language: ru
```

параметр вказує на мову, використану сервером для документа.

```
Transfer-Encoding: chunked
```

цей параметр показує метод видачі даних сервером. У цьому випадку сервер видаватиме дані частинами, а не все відразу.

Практична частина

Використовуючи програму Telnet підключитися до веб-серверів і провести аналіз заголовків HTTP відповідей на запит таких адрес:

1. http://bdpu.org
2. http://bdpu.org/simple.html
3. http:// 10.10.2.251
4. http://ya.ru

Підключення з використанням Telnet зорганізується так:

1. $ telnet tonycode.com 80
2. Після підключення натиснути Ctrl+], для вмикання локальної луни.
3. Ввести:

```
GET / HTTP/1.1
Host: tonycode.com
```

4. Два рази натиснути Enter.

У звіт з лабораторної роботи включити характеристики всіх кодів і полів відповідей.

Самостійна робота №12

Тема: Реорганізація адресації рівня розподілення та рівня доступу для стабілізації роботи ієрархічної мережі

Мета: розвивати у студентів уміння впорядковувати адресацію для стабілізації роботи мережі.

Студент повинен знати: особливості впорядкування адресації для стабілізації роботи мережі.

Студент повинен уміти: впорядковувати адресацію на рівнях доступу та розподілення ієрархічної комп'ютерної мережі.

Хід роботи

Теоретична частина

1. Яка властивість мережі передбачає наявність альтернативних маршрутів в обхід поодиноких точок відмови?
2. Які дві властивості повинен мати протокол маршрутизації?
3. Як протокол маршрутизації може зменшити навантаження, що лягає на вузли мережі, які не беруть участь у процесі маршрутизації?
4. Назвіть проблеми адресації, які можуть виникнути в разі декількох підключень до зовнішніх мереж.

Практична робота

Законспектуйте основі положення стосовно впорядкування адресації рівня розподілення та рівня доступу для стабілізації роботи ієрархічної мережі.

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол.

справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Встановлення та налагодження веб-сервера Apache".

МОДУЛЬНА КОНТРОЛЬНА РОБОТА №7

Оберіть номер правильної відповіді:

1. Протокол відправлення листів:

а) FTP;
б) HTTP;
в) POP3;
г) SMTP;
д) SMTP, POP3.

1 б.

2. Який із нижче перерахованих методів дозволяє одержати дані, що повертаються веб-сервером у формі URL?

а) GET;
б) POST;
в) HEAD.

1 б.

3. У рядку відповіді сервера "HTTP/1.0 … Ok" замість крапок вкажіть код успішного повернення.

а) 200;
б) 201;
в) 400;
г) 440.

1 б.

4. Метод для передачі даних на сервер

а) GET;
б) POST;
в) HEAD.

1 б.

5. Найбільш верхній рівень моделі OSI

а) передачі даних;
б) фізичний;
в) рівень представлення;
г) прикладний;

г) транспортний;
д) сеансовий;
є) мережевий.

1 б.

6. Протокол FTP дозволяє
а) реєструватися і працювати на видаленому сервері;
б) перетворювати імена хостів у мережеві адреси;
в) прочитувати сторінки і файли з www;
г) переміщати файли з клієнта на сервер і навпаки.

1 б.

7. При перевірці пошти розділ, у якому накопичуються повідомлення, що прийшли, називається:
а) чернетки;
б) кошик;
в) відправлені;
г) що входять.

1 б.

8. Виберіть правильний варіант запису електронної пошти.
а) ion baciu@registru.md;
б) ion_baciu@registru.md;
в) ion baciu@registru md;
г) ion_baciu.registru.md.

1 б.

9. Чи можна передавати файли разом з електронною поштою?
а) можна, але тільки текстові файли;
б) можна, якщо розмір файлу не перевищує 100 Кб;
в) можна;
г) не можна.

1 б.

10. Метод POST в протоколі HTTP
а) відправляє поштове повідомлення по e-mail;
б) передає дані або файл на веб-сервер;
в) прочитує файл з веб-сервера;
г) проводить утентифікацію користувача ресурсу;
г) встановлює HTTP-тунель через проміжний сервер.

1 б.

Усього: 10 балів.

Правильні відповіді

Питання	1	2	3	4	5	6	7	8	9	10

Відповідь	г	в	а	б	г	г	г	б	в	б

ЗМІСТОВИЙ МОДУЛЬ 8

ПРИКЛАДНІ ПРОТОКОЛИ В АДМІНІСТРУВАННІ КОМП'ЮТЕРНИХ МЕРЕЖ

Таблиця 53

Тематичний план змістового модуля

№ теми	Назва змістового модуля, теми	Усього годин	Лекції	Лабораторні заняття	Самостійна та індивідуальна робота
8.1-8.2	Прикладні протоколи в адмініструванні комп'ютерних мереж	18	4	4	10
	Разом	***18***	***4***	***4***	***10***

Навчальні цілі: сприяти засвоєнню студентами знань щодо системи доменних імен, стандартів і програмних засобів реалізації віддаленого доступу.

Основні поняття: плоскі символьні імена, ієрархічні символьні імена, схема роботи DNS, зворотна зона, принтер і клавіатура NVT, структура команд Telnet, безпека.

Методичні рекомендації щодо роботи з модулем: робота з модулем передбачає засвоєння лекційного матеріалу, участь у лабораторних заняттях, написання реферату (окремими студентами), самостійну роботу над визначеними питаннями теми, модульний контроль у формі тестування.

Після опрацювання цих тем студент може отримати бали, наведені в табл. 54

Таблиця 54

Оцінювання навчальних досягнень студентів

Поточний контроль			Контрольна рейтингова оцінка	Проміжна рейтингова оцінка
Робота на лабораторному занятті	Самостійна робота	Індивідуальне завдання		
Тема №8.1-8.2	Тема №8.1-8.2			

10	5	5	10	30

ТЕМА 8.1-8.2. ПРИКЛАДНІ ПРОТОКОЛИ В АДМІНІСТРУВАННІ КОМП'ЮТЕРНИХ МЕРЕЖ

Лекція

План

1. Система доменних імен
2. Віддалений доступ до ресурсів мережі. Протокол Telnet
3. Універсальний ідентифікатор ресурсів URI

Література

Основна

1. *Компьютеры*, сети, Интернет: Энциклопедия: Наиболее полн. и подроб. рук. / Ю. Новиков, Д. Новиков, А. Черепанов, В. Чуркин; Под общ. ред. Ю. Новикова. – 2. изд. – М. [и др.]: Питер, 2003 (СПб.: ГПП Печ. Двор им. А.М. Горького). – 831 с.: ил.; 24 см.

2. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. – 4-е изд. – Москва [и др.]: Питер, 2010. – 943 с.: ил.; 24 см. – (Учебник для вузов).

3. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. – 4-е изд. – М. [и др.]: Питер, 2005. – 991 с.: ил., табл.; 24 см. – (Классика computer science).

4. *Антонов В. М.* Сучасні комп'ютерні мережі / Валерій Миколайович Антонов. – К. : МК-Прес, 2005. – 480 с.

Додаткова

1. *Вишневский А.* Сетевые технологии Windows 2000 / Алексей Вишневский. – СПб. и др.: Питер, 2000. – 591 с.: ил., табл.; 24 см. – (Для профессионалов).

2. *Грир Т.* Сети Интернет: Пер. с англ. – М.: ИТД "Русская редакция", 2000. – 368 с.

3. *Джонс А.* Руководство системного администратора Windows: Windows 98. Windows NT. Windows 2000 / Аллен Джонс; [Пер. с англ. А. Файзрахманов]. – СПб.: Питер, 2000. – 367 с.: ил.; 24 см. – (Для

профессионалов).

4. *Интеллектуальные* сети связи / Б.Я. Лихтциндер, М.А. Кузякин, А.В. Росляков, С.М. Фомичев. – 2. изд. – М.: Эко-Трендз, 2002. – 205 с.: ил., табл.; 24 см. – (Инженерная энциклопедия) (Технологии электронных коммуникаций: ТЭК).

5. *Камер Д.Э.* Компьютерные сети и Internet: Разработка приложений для Internet (пер. с англ. Птицына К.А.) Изд. 3-е + CD-Rom – 640 с.

6. *Комп'ютерні* мережі. Практикум : для студ. комп'ютерних спец. денної і заоч. форм навч. / [уклад. В. В. Швидкий]. – Черкаси : ЧДТУ, 2002. – 56 с.

7. *Методические* рекомендации к выполнению лабораторных работ по курсу "Internet-технологии и язык Java": для студ. спец. 7.080401, 7.080407 всех форм обучения / Харьковский гос. экономический ун-т / Сост. С. В. Минухин, С. В. Знахур. – Х. : ХГЭУ, 2004. – 103с.

8. *Рамський Ю. С.* Вивчення інформаційно-пошукових систем мережі Інтернет: навч.-метод. посіб. / Ю. С. Рамський, О. В. Рєзіна. – К. : РННЦ "ДІНІТ", 2004. – 60 с.

8.1.1. Система доменних імен

Числова адресація зручна для машинної обробки таблиць маршрутів, але зовсім не прийнятна для використання її людиною. Запам'ятати набори цифр набагато складніше, ніж осмислені імена. Для полегшення взаємодії в мережі Internet спочатку використовувалися таблиці відповідності числових адрес іменам машин. Ці таблиці збереглися дотепер і використовуються багатьма прикладними програмами. Якийсь час навіть існувало центральне сховище відповідностей, яке можна було по FTP скачати на свою машину з ftp.internic.net. Це файли з ім'ям *hosts*. Якщо йдеться про систему типу Unix, то цей файл розташований у директорії /etc і має такий вигляд (табл. 55).

Таблиця 55

Приклад таблиці імен хостів (файл /etc/hosts)

IP-адреса	Ім'я машини	синоніми
127.0. 0.1	localhost	localhost
144. 206.160.32	polyn	polyn

144. 206.160.40	apollo	www.apollo

Останній стовпець у цій таблиці є необов'язковим. Користувач для звернення до машини може використати як IP-адресу машини, так і її ім'я або синонім (alias). Звернення, наведені нижче, приведуть до одного й того ж результату – ініціювання сеансу telnet з машиною Apollo:

telnet 144.206.160.40 або
telnet apollo або
telnet www.apollo

У локальних мережах файли hosts використовуються досить успішно дотепер. Практично всі операційні системи підтримують цю систему відповідності IP-адрес доменним іменам.

Однак такий спосіб присвоєння символьних імен був гарний доти, поки Internet був невеликим. У міру збільшення мережі стало складно тримати великі списки імен на кожному комп'ютері. Для того, що б розв'язати цю проблему, була придумана *DNS (Domain Name System)*.

Розглянемо принципи організації DNS. Будь-яка DNS є прикладним процесом, що працює над стеком TCP/IP. Таким чином, базовим елементом адресації є IP-адреса, а доменна адресація виконує роль сервісу. DNS – це інформаційний сервіс Internet, і, отже, протоколи його належать до протоколів прикладного рівня стандартної моделі OSI.

Система доменних адрес спроектована по ієрархічному принципу. Однак ієрархія ця не строга, тому що немає єдиного кореня всіх доменів Internet. Якщо більш точно, то такий корінь у моделі DNS є. Він так і називається "ROOT". Однак єдиного адміністрування цього кореня немає. Адміністрування починається з доменів верхнього, або першого, рівня. У 80-і роки були визначені перші домени цього рівня й розраховані на США:

- gov – державні організації;
- mil – військові установи;
- edu – освітні установи;
- com – комерційні організації;
- net – мережні організації.

Пізніше, коли мережа переступила національні кордони США, з'явилися національні домени типу:

- uk – Об'єднане королівство;

– jp – Японія;
– au – Австралія;
– ch – Чехія;
– ua – Україна;
– ru – Росія й т.п.

Для СРСР також був виділений домен su. Після 1991 року, коли республіки стали суверенними, більшість з них одержали свої власні домени: ua, ru, la, li, і т.п.

Услід за доменами першого рівня йдуть або географічні домени (kiev.ua, dn.ua), або організації (gov.ua). У цей час практично будь-яка організація або фізична особа може одержати свій власний домен другого рівня.

Далі йдуть домени третього рівня, наприклад: edu.bdpu.org

Система доменної адресації представлена на рис. 89.

Служба доменних імен працює як розподілена база, дані якої розподілені по DNS-серверах. Сервіс DNS будується за схемою "клієнт-сервер", де як клієнтська частина виступає процедура вирішення імен – resolver, а як сервер DNS-сервер.

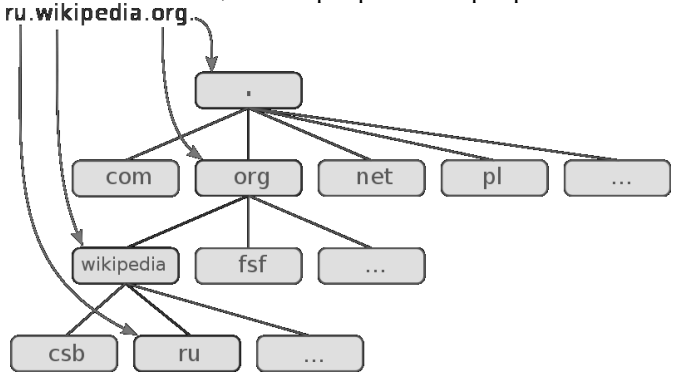


Рис. 89. Система доменної адресації

Наприклад, коли звертаються до сервера ipm.kstu.ru, браузер, використовуючи resolver, робить таке:

1. Шукає запис ipm.kstu.ru у файлі hosts.
2. Надсилає запит на відомий DNS-кешуючий сервер (як правило, локальний), якщо на ньому запис не знайдений, то, запит переадресовується іншому серверу.
3. Сервер DNS-кешуючий звертається до DNS-ROOT сервера із

запитом адреси DNS сервера відповідального за домен першого рівня ru, якщо одержує адресу, то, запит переадресовується іншому серверу.

4. Сервер DNS-кешуючий звертається до DNS сервера, відповідального за домен першого рівня ru, із запитом адреси DNS сервера, відповідального за домен другого рівня kstu.ru, якщо одержує адресу, то, запит переадресовується іншому серверу.

5. Сервер DNS-кешуючий надсилає запит на DNS сервер, відповідальний за домен другого рівня kstu.ru, якщо одержує адресу, то, запит переадресовується іншому серверу.

6. Сервер DNS-кешуючий кешує адресу й передає клієнту,

7. Клієнт звертається за IP адресою – 195.208.44.20.

Первинний сервер містить повну інформацію про зону.

Вторинний сервер, що містить копію повної інформації про зону, отриману з первинного сервера.

Кешуючий – містить записи, які вже були запитані.

8.1.2. Віддалений доступ до ресурсів мережі. Протокол Telnet

Telnet – це одна із най старіших інформаційних технологій Internet.

Призначення Telnet-протоколу – дати загальний опис взаємодії термінального пристрою й термінал-орієнтованого процесу. При цьому цей протокол може бути використаний і для організації взаємодій "термінал-термінал" (зв'язок) і "процес-процес" (розподілені обчислення). Стандартним портом TCP для telnet є порт 23.

Telnet розроблявся як прикладний протокол над транспортним протоколом TCP. В основу telnet покладені три фундаментальні ідеї:

– концепція мережевого віртуального термінала (Network Virtual Terminal) або NVT;

– принцип договірних опцій (узгодження параметрів взаємодії);

– симетрія зв'язку "термінал-процес".

У протоколі Telnet NVT визначений як "двуспрямований символьний пристрій, що складається із принтера й клавіатури". Принтер призначений для відображення інформації, що надходить з мережі, а клавіатура – для уведення даних, переданих мережею. NVT передбачається буферизованим пристроєм.

Це означає, що дані, що вводять із клавіатури, не посилають

відразу по мережі, а збираються в пакети, які відправляються або в міру заповнення буфера, або по спеціальній команді. Така організація NVT покликана, з одного боку, мінімізувати мережний трафік, а з іншого – забезпечити сумісність із реальними буферизованими терміналами.

NVT – це стандартний опис найбільш широко використовуваних можливостей реальних фізичних термінальних пристроїв. NVT дозволяє описати й перетворити в стандартну форму способи відображення й уведення інформації. Термінальна програма ("user") і процес ("server"), що працює з нею, перетворюють характеристики фізичних пристроїв у специфікацію NVT, що дозволяє, з одного боку, уніфікувати характеристики фізичних пристроїв, а з іншого – забезпечити принцип сумісності пристроїв з різними можливостями. Характеристики діалогу диктуються пристроєм з меншими можливостями.

Якщо взаємодія здійснюється за принципом "термінал-термінал" або "процес-процес", то "user" – це сторона, що ініціює з'єднання, а "server" – пасивна сторона.

Принцип договірних опцій або команд дозволяє погодити можливості подання інформації на термінальних пристроях. NVT – це мінімально необхідний набір параметрів, що дозволяє працювати по telnet навіть несучасним пристроям, реальні сучасні пристрої мають набагато більші можливості подання інформації. Принцип договірних команд дозволяє використати ці можливості. Симетрія взаємодії по протоколу telnet дозволяє протягом однієї сесії програмі –"user" і програмі –"server" мінятися місцями. Це принципово відрізняє взаємодію в рамках telnet від традиційної схеми "клієнт-сервер".

Симетрія взаємодії тісно пов'язана із процесом узгодження форми обміну даними між учасниками telnet-з'єднання. Коли йдеться про роботу на віддаленій машині в режимі термінала, то можливості введення й відображення інформації визначаються тільки конкретним фізичним терміналом і договірний процес зводиться до замовлення термінальною програмою характеристик цього термінала.

8.1.3. Універсальний ідентифікатор ресурсів URI

URI (Uniform Resource Identifier, Універсальний ідентифікатор ресурсу) – компактний рядок символів для ідентифікації абстрактного або фізичного ресурсу. Під ресурсом розуміється будь-

який об'єкт, що належить деякому простору.

Необхідність в URI була зрозуміла розроблювачам WWW з моменту зародження системи, тому що передбачалося об'єднання в єдине інформаційне середовище засобів, що використовують різні способи ідентифікації інформаційних ресурсів. Була розроблена специфікація, що містила в собі звертання до FTP, Gopher, WAIS, Usenet, E-mail, Prospero, Telnet, X.500 і, звичайно, HTTP (WWW). У результаті була розроблена універсальна специфікація, що дозволяє розширювати список адресованих ресурсів за рахунок появи нових схем.

Місце застосування URI – гіпертекстові посилання, які записуються в тегах <A HREF=URI> і <LINK HREF=URI>. Графічні об'єкти, що вбудовують, також адресуються по специфікації URI у тегах <IMG SRC=URI> і <FIG SRC=URI>. Реалізація URI для WWW називається URL (Uniform Resource Locator). Точніше, URL – це реалізація схеми URI, відображена на алгоритм доступу до ресурсів по мережевих протоколах. Існує ще й *URN (Uniform Resource Name)*, що відображає URI у простір імен на мережі.

Поява URN пов'язана з бажанням адресувати частини поштового повідомлення MIME.

Принципи побудови адреси WWW. В основу URI були закладені такі принципи:

– *розширюваність* – нові адресні схеми повинні легко вписуватися в існуючий синтаксис URI;

– *повнота* – по можливості, кожна із наявних схем повинна описуватися за допомогою URI;

– *читаність* – адреса повинна легко читатися користувачем, що взагалі характерно для технології WWW – документи разом з посиланнями можуть розроблятися у звичайному текстовому редакторі.

Перш, ніж розглянути різні схеми подання адрес, наведемо приклад простої адреси URI:

```
http://polyn.net.kiae.su/polyn/index.html
```

Перед двокрапкою стоїть ідентифікатор схеми адреси – "http". Це ім'я відділене двокрапкою від остачі URI, що називається "шлях". У цьому випадку шлях складається з доменної адреси машини, на якій установлений сервер HTTP і шляху від кореня дерева сервера до файлу "index.html".

Крім представленого вище повного запису URI, існує спрощений. Він передбачає, що до моменту її використання багато

параметрів адреси ресурсу вже визначені (протокол, адреса машини в мережі, деякі елементи шляху). При таких припущеннях автор гіпертекстових сторінок може вказувати тільки відносну адресу ресурсу, тобто адресу щодо певних базових ресурсів.

Деякі підмножини URL:

URL (Uniform Resource Locator, Універсальний покажчик ресурсу) – підмножина схем URI, що ідентифікує ресурс по способу доступу до нього (наприклад, його "місцезнаходженню в мережі") замість того, щоб ідентифікувати його за назвою або іншими атрибутами цього ресурсу.

URL – Uniform Resource Locators явно описує, як добратися до об'єкта.

Синтаксис: <scheme>:<scheme-specific-part> де: scheme = "http" | "ftp" | "gopher" | "mailto" | "news" | "telnet" | "file" | "man" | "info" | "whatis" | "ldap" | "wais" | ... – ім'я схеми scheme-specific-part – залежить від схеми.

У scheme-specific-part можна використати шістнадцяткові значення у вигляді: %5f. Обов'язково повинні кодуватися недруковані октети: 00-1F, 7F, 80-FF.

Приклади URL:

```
http://www.ipm.kstu.ru/index.php
ftp://www.ipm.kstu.ru/
```

У HTML записується так:

```
<a href="http://www.ipm.kstu.ru/index.php"></a>
```

URN (Uniform Resource Name, Універсальне ім'я ресурсу) – приватна URI-схема "urn:" з підмножиною "простору імен", що повинен бути унікальним і незмінним навіть у тому випадку, коли ресурс уже не існує або недоступний.

Передбачається що, наприклад браузер, знає, де шукати цей ресурс. Синтаксис: urn:namespace: data1.data2,more-data, де namespace (простір імен) визначає, як використовуються дані, зазначені після другої ":".

Приклад URN:

```
urn:ISBN: 0-395-36341-6,
```

де: ISBN – тематичний класифікатор для видавництв, 0-395-36341-6 – конкретний номер тематики книги або журналу.

При одержанні URN клієнтська програма звертається до ISBN (каталогу "тематичний класифікатор для видавництв" в Інтернеті). І одержує розшифровку номера тематики "0-395-36341-6" (наприклад:

"квантова хімія"). URN прийнятий порівняно недавно, у поточні версії HTML не включений і служби каталогів поки не розвинені, тому URN не так широко розповсюджений, як URL.

Лабораторна робота №15 (2 год.)
Тема: Використання протоколів віддаленого адміністрування

Мета: сформувати вміння використовувати протоколи віддаленого адміністрування;

виховувати ціннісне ставлення студентів до навчальної діяльності.

Студент повинен знати: можливості протоколу Telnet, структуру команд Telnet для підключення до віддаленого серверу.

Студент повинен уміти: здійснювати підключення та управління віддаленим сервером.

Хід роботи

Інструктаж

Відправка пошти через telnet

Як перевірити працездатність відправки пошти на сервері mail.server.ua, використовуючи утиліту telnet?

1. Команда для входу на поштовий сервер:telnet mail.server.ua 25Trying aaa.bbb.ccc.ddd..Connected to mail.server.ua (aaa.bbb.ccc.ddd).Escape character is '^]'.220 mail.server.ua ESMTP Sendmail x.y.z/x.y.z; Fri, 7 Mar 2008 10:09:22 +0200
2. Введіть команду вітання : helo eee.fff.ggg.hhh(де eee.fff.ggg.hhh ваш IP -адрес з якого ви запустили telnet)250 mail.server.ua Hello mail.server.ua [aaa.bbb.ccc.ddd] pleased to meet you
3. Вкажіть адресу відправника (має бути в тому ж домені, що і поштовий сервер: server.ua)mail from : taras@server.ua250 2.1.0 taras@server.ua.. Sender ok
4. Вкажіть адресата (mailto@mail.kiev.ua) :rcpt to: mailto@mail.kiev.ua250 2.1.5 taras.. Recipient ok
5. Введіть команду data354 Enter mail, end with "". on a line by itself
6. Subject: тема тестового листа
7. Текст листа, а у кінці листа одну точку в рядку, щоб закінчити.

8. 250 2.0.0 x2789MjQ008048 Message accepted for delivery
9. Введіть для виходу quit
10. 221 2.0.0 mail.server.ua closing connectionConnection closed by foreign host.

Перевірка пошти через telnet

Як перевірити працездатність пошти на сервері mail.server.ua використовуючи утиліту telnet?

1. Команда для входу на поштовий сервер: telnet mail.server.ua 110.
2. Задати ім'я користувача: user user@server.ua.
3. Задати пароль для користувача: pass PassW0rd.
4. Отримати список листів: list.
5. Прочитати лист retr x (де x - це номер листа).
6. Для виходу введіть команду quit.

Самостійна робота №15

Тема: Застосування принципів ієрархічного проектування мережі

Мета: розвивати у студентів уміння застосовувати принципи ієрархічного проектування мережі.

Студент повинен знати: принципи ієрархічного проектування мережі.

Студент повинен уміти: реалізовувати принципи ієрархічного проектування мережі на практиці.

Хід роботи

Теоретична частина

1. Реорганізувати мережу (рис. 90) на основі принципів ієрархічного проектування.

Практична робота

1. Проведіть аналіз і при необхідності реорганізацію мережі на рис. 90.
2. Визначте межі ядра, рівня розподілу і рівня доступу мережі, зображеної на рис. 90.
3. Усуньте усі недоліки топології, які могли б негативно позначитися на стабільності функціонування мережі, представленої на рис. 90. Поясніть свої дії.
4. Проведіть адресацію мережі, зображеної на рис. 90, щоб звести до мінімуму кількість маршрутів, що надаються пристроям

ядра.

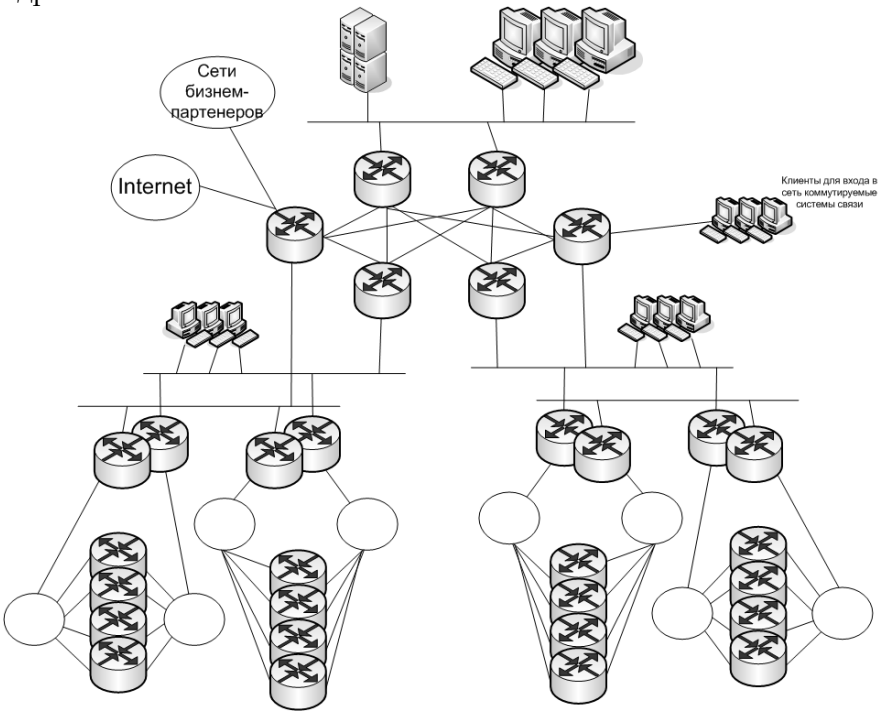


Рис. 90. Мережа, що потребує реорганізації

Література

1. *Ретана А.* Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. – М. [и др.]: Вильямс, 2002. – 367 с.: ил.; 24 см. – (Сертифицированный специалист по межсетевому обмену CISCO).

2. *Руководство* по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. – 4-е изд. – М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). – 1033 с.: ил., табл.; 24 см.

Індивідуальна робота

Напишіть реферат на тему "Використання протоколу SHH для

віддаленого адміністрування серверів".

МОДУЛЬНА КОНТРОЛЬНА РОБОТА №8

Оберіть номер правильної відповіді:

1. На основі якого принципу будується система доменних адрес?

а) ієрархічного;

б) паралельного;

в) послідовного;

г) усі вірні;

д) усі не вірні.

1 б.

2. Що входить в основу telnet?

а) концепція мережного віртуального термінала (Network Virtual Terminal) або NVT;

б) принцип договірних опцій (узгодження параметрів взаємодії);

в) симетрія зв'язку "термінал-процес";

г) усі не входять;

д) усі входять.

2 б.

3. Який із принципів побудови адрес www зайвий:

а) розширюваність;

б) повнота;

в) читаність;

г) унікальність.

1 б.

4. Скільки існує схем адресації ресурсів в Internet

а) 8 і більше;

б) 2;

в) 6;

г) 3.

2 б.

5. Номер порту протоколу TCP/IP для telnet.

а) 20;

б) 30;

в) 23;

г) 80.

1 б.

6. Аутентифікація дозволяє:

а) синхронізувати час комп'ютера з точним часом;
б) забезпечити шифрування і секретність інформації;
в) визначити співрозмовника і перевірити права доступу;
г) встановити версію сервера і тип браузеру.

2 б.

7. Що означають дві останні букви адреси www.test.ru?
а) розширення файлу головної сторінки веб-сайта;
б) домен першого рівня;
в) мова веб-сайта;
г) тематику веб-сайта.

1 б.
Всього: 10 балів.

Правильні відповіді

Питання	1	2	3	4	5	6	7
Відповідь	а	д	г	б	в	в	б

ТЕСТИ ЗАКРИТОЇ ФОРМИ

Обведіть номер правильної відповіді

1. Одноранговi мережі – це:

а) мережі з одним виділеним сервером;

б) мережі з одним і більше виділеними серверами;

в) мережі, де всі комп'ютери рівноправні.

1 б.

2. Мережі кампусів – це:

а) мережі, що поєднують множину мереж різних відділів одного підприємства в межах окремого будинку або однієї території:

б) підмережі мереж відділів;

в) локальні мережі, що не мають вихід у глобальну мережу Internet і функціонують без виділеного сервера.

1 б.

3. Технологія передачі даних, що використовуються в мережах:

а) бітова;

б) символьна;

в) широкомовна (від одного до багатьох).

1 б.

4. Мережеві кабелі, що володіють найбільшою швидкістю і якістю передачі даних:

а) кручена пара;

б) оптичний;

в) коаксіальний кабель.

1 б.

5. Ефективна довжина мережного кабелю кручена пара?

а) 50 м;

б) 100 м;

в) 150 м;

г) 500 м.

1 б.

6. Сукупність алгоритмів взаємодії об'єктів однойменних рівнів визначає поняття:

а) інтерфейс;

б) стек;

в) протокол;
г) рівень.

1 б.

7. Які з перерахованих функцій не реалізуються протоколами мережного рівня?

а) визначення маршруту;
б) визначення логічної адреси;
в) керування потоком.

1 б.

8. Яке максимальне число послідовних колізій може виникнути в мережі Ethernet?

а) 2;
б) 8;
в) 16.

1 б.

9. Чому дорівнює мінімальна довжина кадру Ethernet?

а) 1024 байта;
б) 64 байта;
в) 1500 байт;
г) 46 байт.

1 б.

10. Який комітет займається розвитком специфікацій CSMA/CD?

а) IEEE 802.5;
б) IEEE 802.1;
в) IEEE 802.3;
г) IEEE 802.2.

1 б.

11. Чому дорівнює розмір максимального сегмента в мережі 10BaseT?

а) 100 метрів;
б) 500 метрів;
в) 185 метрів;
г) 200 метрів.

1 б.

12. Які пристрої поєднують мережі на фізичному рівні?

а) повторювачі;
б) мости;
в) комутатори;
г) серед перерахованих пристроїв немає правильних.

1 б.

13. Ядром якого пристрою є комутаційна матриця, що забезпечує передачу даних між будь-якими двома точками, або швидкодіюча шина, через яку будь-який порт може передати інформацію будь-якому іншому порту?

а) маршрутизатор;

б) комутатор;

в) концентратор.

1 б.

14. У ядрі якого пристрою утвориться швидка "віртуальна мережа"?

а) міст;

б) повторювач;

в) комутатор;

г) маршрутизатор.

1 б.

15. Основне завдання, що розв'язується протоколом IP:

а) маршрутизація;

б) додавання заголовка;

в) аналіз правильності доставки.

1 б.

16. Мас-адреса – це:

а) адреса, що призначається динамічно при вході в мережу;

б) адреса, що призначається виробником обладнання і є унікальною;

в) адреса, що обирається користувачем при вході в мережу.

1 б.

17. Виберіть IP-адресу, що відповідає інтерфейсу зворотного зв'язка:

а) 192.168.1.123;

б) 127.0.0.1;

в) 13.45.12.1;

г) 1.1.1.1;

1 б.

18. Виберіть IP-адресу, що відповідає широкомовній передачі:

а) 192.168.1.1;

б) 127.0.0.0;

в) 255.255.255.255;

г) 1.1.1.1.

1 б.

19. Протокол ICMP:

а) забезпечує зворотний зв'язок у вигляді діагностичних повідомлень, що посилають відправнику при неможливості доставки його дейтаграми й в інших випадках;

б) відповідає безпосередньо за передачу даних;

в) відповідає за коректне прийняття даних;

г) посилає широкомовне повідомлення.

1 б.

20. Сокет – це:

а) IP-адреса;

б) номер мережі, що входить в IP-адресу;

в) порт ПК, що перебуває в мережі;

г) IP-адреса й номер порту.

1 б.

21. Команда PING використовується:

а) для перегляду локальної Mac-адреси;

б) для перегляду IP-адреси ПК;

в) для перевірки з'єднання з віддаленим хостом;

г) для відправлення широкомовного повідомлення.

1 б.

22. У рядку відповіді сервера "HTTP/1.0 … Ok" замість крапок вкажіть код успішного повернення.

а) 200;

б) 201;

в) 400;

г) 440.

1 б.

23. Метод для передачі даних на сервер

а) GET;

б) POST;

в) HEAD.

1 б.

24. Протокол FTP дозволяє

а) реєструватися і працювати на видаленому сервері;

б) перетворювати імена хостів в мережеві адреси;

в) прочитувати сторінки і файли з WWW;

г) переміщати файли з клієнта на сервер і навпаки.

1 б.

1. Виберіть правильний варіант запису електронної пошти.

а) ion baciu@registru.md;

б) ion_baciu@registru.md;

в) ion baciu@registru md;

г) ion_baciu.registru.md.

1 б.

25. Що входить в основу telnet?

а) концепція мережного віртуального термінала (Network Virtual Terminal) або NVT;

б) принцип договірних опцій (узгодження параметрів взаємодії);

в) симетрія зв'язку "термінал-процес";

г) усі не входять;

д) усі входять.

1 б.

26. Що означають дві останні букви адреси www.test.ru?

а) розширення файлу головної сторінки веб-сайта;

б) домен першого рівня;

в) мова веб-сайта;

г) тематику веб-сайта.

1 б.

ТЕСТИ ВІДКРИТОЇ ФОРМИ

1. Відповідно до заданих класів (A, B або C), кількості підмереж N і максимальної кількості комп'ютерів M1..MN у кожній підмережі визначити *маску* для розбиття на підмережі. Зробити висновок про можливість такого розбиття. Якщо розбиття неможливе, то сформулювати рекомендації зі зміни початкових даних для забезпечення можливості розбиття.

Параметр	**Значення параметра**				
Клас	B				
N	4				
M1...MN	1024	2048	4069	512	256

5 б.

2. Визначити максимальну довжину маски мережі та її адресу, щоб вказані IP-адреси перебували в одній мережі.

231.81.216.237 – 231.81.212.30

177.77.34.213 – 191.35.196.43

115.115.32.253 – 114.14.56.227
62.225.77.124 – 62.225.76.103

5 б.

3. Для заданих IP-адрес класів A, B і C, а також запропонованих масок (див. варіанти завдань) визначити:

– клас адреси;

– максимально можливу кількість підмереж, яку можна утворити відповідно до класу IP-адреси;

– кількість підмереж, яку можна утворити відповідно до класу IP-адреси та відповідної маски;

– діапазон зміни адрес підмереж, утворених з використанням маски;

– максимальну кількість вузлів у підмережах, утворених з використанням маски;

Параметр	**Значення параметра**
Адреса	207.112.5.102
Маска	11111111.11111111.11111111.10000000

5 б.

Наукове видання

Хоменко Віталій Григорович
Павленко Максим Петрович

КОМП'ЮТЕРНІ МЕРЕЖІ

Навчальний посібник

Комп'ютерна верстка *М.П. Павленко, С.К. Акімов*
Дизайн обкладинки *С.К. Акімов*
Технічний редактор *О.В.Хатунцева*

Надруковано з оригінал-макету, наданого авторами

Підписано до друку 2.11.2011 р.
Формат 60x84/16. Папір офсетний.
Гарнітура "Book Antiqua". Друк – лазерний.
Ум.-друк. арк. 9,77. Обл.-вид. арк. 8,15.
Наклад 300 прим. Вид. №165. Зам. №168.

Видавництво та друк ПП "ЛАНДОН-ХХІ"
Свідоцтво про реєстрацію: серія ДЦ №159 від 22.10.2010 р.
83120, м. Донецьк, вул. Петровського, 126-А/32.
Тел./факс: (062) 334-49-66, e-mail: elenah66@gmail.com