О. М. Бевз,
С. Г. Кривогубченко, А. Я. Кулик

СИСТЕМИ ТА МЕРЕЖІ ПЕРЕДАВАННЯ ДАНИХ
(Частина ІІІ)

Міністерство освіти і науки України
Вінницький національний технічний університет

О. М. Бевз,
С. Г. Кривогубченко, А. Я. Кулик

СИСТЕМИ ТА МЕРЕЖІ ПЕРЕДАВАННЯ ДАНИХ

(Частина ІІІ)

Затверджено Вченою радою Вінницького національного технічного університету як навчальний посібник для студентів напряму підготовки 0914 - "Комп`ютеризовані системи, автоматика і управління" всіх спеціальностей. Протокол № 7 від "22" лютого 2007 р.

Вінниця ВНТУ 2008

УДК 621.3
Б 36

Рецензенти:

В. М. Лисогор, доктор технічних наук професор
І. І. Хаймзон, доктор технічних наук професор
О. М. Возняк, кандидат технічних наук доцент

Рекомендовано до видання Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України

Бевз О.М., Кривогубченко С.Г., Кулик А.Я.

Б 36 **Системи та мережі передавання даних. Частина ІІІ.** Навчальний посібник. – Вінниця: ВНТУ, 2008. – 60 с.

В посібнику розглянуті цифрові мережі, мережі загального призначення, мережі персональних комп'ютерів. Посібник розроблений у відповідності з планом кафедри та програмою дисципліни "Системи та мережі передавання даних".

УДК 621.3

Зміст

Вступ

Навчальний посібник, що пропонується читачеві, є третьою частиною навчального посібника "Системи та мережі передавання даних".

В основу посібника покладено курс лекцій з дисципліни "Системи та мережі передавання даних", що читається авторами у Вінницькому національному технічному університеті на факультеті автоматики і комп`ютерних систем управління.

Посібник " Системи та мережі передавання даних" ч.3 присвячений цифровим мережам, мережам загального призначення та мережам персональних комп`ютерів.

В ньому в доступній формі розглядаються принципи роботи цих мереж та взаємодія їхніх функціональних частин.

Посібник призначений для студентів напряму підготовки 0914 "Комп`ютеризовані системи, автоматика і управління" і може бути корисним студентам інших спеціальностей, які вивчають і користуються сучасними інформаційними системами, а також широкому колу відповідних спеціалістів, які намагаються підвищити свій науково-технічний рівень.

Перший розділ цього посібника написаний Бевзом О.М., другий – Куликом А.Я., третій – Кривогубченком С.Г.

1 Цифрові мережі

1.1 Переваги цифрових систем

Причин застосування цифрових технологій при передаванні інформації декілька. По-перше, цифрові пристрої не такі дорогі, як аналогові. Наприклад, це справедливо для мультиплексорів. Більше того, цифрові системи будуються на основі схем надвисокого рівня інтеграції, які самі по собі дуже стійкі й надійні. По-друге, цифрова технологія використовується для передавання інформації різного типу: цифрові мережі передають не тільки акустичні сигнали, але й телевізійні, відеодані або ж факсимільні дані по одному каналу. По-третє, цифрові методи усувають багато обмежень передавання й зберігання даних, які властиві аналоговим технологіям.

Процес оцифровування в телефонії був розроблений в 60-х рр. з метою подолання деяких обмежень передачі аналогових сигналів і зберігання інформації. Аналоговий сигнал – це постійна зміна амплітуди в часі. Так, коли говорять у слухавку, фізичні, тобто механічні коливання повітря (чергування низького й високого тиску) перетворюються в електричний сигнал з цією ж самою характеристикою обвідної амплітуди. Телефон діє як перетворювач для зміни сигналу одного виду енергії в інший. При передаванні сигналу по комунікаційному каналу його необхідно періодично підсилювати, щоб перебороти загасання та завади.

При передаванні аналогових сигналів по каналах зв'язку виникають ряд проблем. Сигнал передається через підсилювачі й інші перетворювачі. Передавальна функція повинна бути лінійною, наскільки це можливо. Лінійність означає те, що форма хвилі, яка зображає сигнал, зберігає його характеристики протягом усього каналу - від кінця до кінця. Всі аналогові сигнали демонструють певну форму нелінійності. На жаль, включені компоненти, такі, як підсилювачі, збільшують нелінійність сигналу.

Друга проблема пов'язана з шумом в каналі. Електричний сигнал являє собою спрямований рух електронів. Тепловий шум створюється в провідниках або кабелі випадковими рухами електронів у каналі або перетворювачі. Шуми можна чути в телефонних лініях - вони нагадують шипіння. Шуми також виникають у радіопередачах через електричні розряди в атмосфері землі і сонячне та космічне випромінювання.

Сигнал зберігається в запам'ятовувальному середовищі, а саме середовище є джерелом шуму. Наприклад, жорсткість поверхні диска створює шуми.

І по-четверте, всі сигнали зменшують своє амплітудне значення

під час передавання через середовище. Це погіршення сигналу може призвести до того, що сигнал від передавача стане незрозумілим для приймача. Високоякісні кабелі з більшими діаметрами провідників зменшують цей недалік, але повністю усунути його не можуть.

Цифрові системи усувають ці проблеми, шляхом перетворення форми аналогового сигналу у вигляді цифрових (двійкових) даних. По суті аналоговий сигнал перетворюється в послідовність цифрових значень і передається по каналу зв'язку у вигляді двійкових даних. Цифрові значення являють собою відповідні значення амплітуди.

Цифрові сигнали мають ті ж недоліки і проблеми, що й аналогові сигнали – послаблення і шуми. Однак цифрові сигнали *дискретні:* двійкові відповідності обвідної аналогового сигналу подані на дискретних рівнях напруги на відміну від безперервного аналогового сигналу. Коли сигнал проходить через канал, то необхідно тільки відзначати *відсутність або наявність* двійкового цифрового імпульсу, а не його *абсолютне значення,* що важливо у випадку аналогового сигналу. Проста відсутність або наявність сигнального імпульсу розпізнається значно легше, ніж амплітуда або ж розмах аналогічного сигналу. Цифрові сигнали можна повністю реконструювати, перш ніж вони спотворяться і стануть нижче встановленого граничного значення. Отже, шуми й загасання можуть бути повністю усунуті з сигналу, що реконструюється.

Періодичне зняття значень і процес реконструювання виконуються відновлювальними *повторювачами.* Повторювачі розміщуються на каналі через певні інтервали. Довжини цих інтервалів залежать від розмірів і якості провідників, рівня шумів у провідниках, смуги пропускання частот, а також швидкості передавання (у бітах в секунду). У ранніх цифрових системах використовувалися інтервали в 6000 фут (приблизно 1830 м). У наш час оптоволоконні канали можуть забезпечити надійну передачу з регенерацією через кожні 20-30 км.

1.2 Перетворення сигналів

Для перетворення аналогових сигналів у цифрові використовують багато методів. Перший підхід, що широко використовується — *імпульсно-кодова модуляція* (ІКМ). Хоча застосування ІКМ тягне багато процесів, взагалі вона описується у вигляді трьох кроків: зняття значень, оцифровування й кодування. Пристрої, що виконують процес перетворення в цифрову форму (первинними ІКМ-мультиплексорами) мають дві основні функції. Перша – перетворення аналогового сигналу в

цифрову форму. Друга – комбінування цифрових сигналів у мультиплексований потік даних.

Імпульсно-кодова модуляція основана на теоремі Котельнікова. Яка зазначає, що якщо аналоговий сигнал відображається на регулярному інтервалі із частотою не менше ніж у два рази більшою максимальної частоти вихідного сигналу в каналі, то перетворення буде містити інформацію, яка достатня для відновлення вихідного сигналу.

Ці перетворення запам'ятовуються і зберігаються, а потім транслюються в двійкові образи. Кожне таке перетворення називається сигналом в імпульсно-амплітудній модуляції (ІАМ). Після виконання відображення сигнал в ІАМ піддається другому компоненту трансляції — *оцифровуванню*. Метою оцифровування є призначення величини кожному сигналу ІАМ. Оцифровувачі надають кожному ІАМ-сигналу значення в діапазонах 1 —128 або 1—256. Якщо оцифровувач призначає сигналу значення з діапазону до 128, то для кожного відображення потрібно 7 біт ($2^7 = 128$). Якщо ж значення вибираються з діапазону до 256, то для кожного відображення потрібно 8 біт ($2^8 = 256$).

Після того як значення ІАМ перетворені в двійкові значення в процесі оцифровування, виконується третій крок - кодування відображень у рядок двійкових бітів.

Для того щоб правильно відновити сигнал, дані необхідно подати на перетворювач «код - аналог» з тією ж швидкістю, з якою виконувалося відображення вихідного сигналу. Процес кодоаналогового перетворення результує в сигнал, який близький за формою до вихідного сигналу.

Звичайно, є проблеми й у передаванні цифрових даних. Цифровий сигнал може бути спотворений багатьма способами. По-перше, спотворення може бути викликано одержанням неадекватних перетворень. Ця проблема вирішується шляхом більш частого зняття, але це потребує дорогих компонентів і більш широкої смуги пропускання (більших швидкостей передавання) каналу. Внаслідок аналогової природи сигналу не існує методів, що повністю виключають спотворення відображень. Фундаментальна аномалія походить з того факту, що дискретні (цифрові) перетворення одержують від безперервних (аналогових) сигналів.

Друга проблема виникає через помилки оцифровування. Процес оцифровування не дозволяє подати амплітуду сигналу абсолютно точно. Оскільки спотворення сигналів у цьому процесі пропорційні розміру кроку (кількості квантів), то одним з підходів до рішення цієї проблеми є збільшення кількості кроків квантування до кількості, достатній для подання сигналу. Однак збільшений рівень кроків вимагає збільшення вартості компонентів і числа бітів, необхідних для подання сигналів.

Ранні системи демонстрували лінійні відношення між сигналами ІАМ та кодом ІКМ (що називається лінійним кодуванням). Як наслідок, у цьому випадку однакові зміни в амплітуді сигналу призводять до рівних змін в кодах ІКМ. Цей ефект створює сильні спотворення оцифровування при малих амплітудах сигналів.

У більш пізніх підходах відбувається стискання сигналів великої амплітуди до меншого діапазону сигналів при заданій кількості рівнів квантування. Сигнали меншої амплітуди розширюються.

Цей метод збільшує кількість доступних рівнів квантування й зменшує загальні спотворення в цьому процесі. Після декодування сигналу, він відновлюється до вихідних амплітудних характеристик. Ця комбінації стискання і розширення називається companding.

У сучасних системах використовується також інша концепція, так зване нелінійне кодування. Цей процес виконує подання зміни сигналів ІАМ малої амплітуди більшими варіаціями кодування, ніж таких самих змін у сигналах більших амплітуд. Помилки оцифровування зменшуються із зменшенням рівня сигналу ІАМ. Як наслідок, відношення сигналу до перешкод зберігається постійним в широкому діапазоні сигналів ІАМ.

Процес нелінійного кодування визначається у вигляді логарифмічної залежності у формі закону, який називаємо "законом мю" (у Північній Америці і Японії) або "законом А" (у Європі). Ці закони подібні, за винятком того, що закон А використовує лінійне відношення в діапазоні малих амплітуд. Мінімальний розмір кроку становить 2/4096 для закону А і 2/8159 для закону мю. Нелінійні аналогові акустичні сигнали в системі мультиплексування з розподілом часу реалізуються в сегментованому процесі. Закон мю подано 15 сегментами, закон А зображається за допомогою 13 сегментів. Обидва закони перевершують будь-які вимоги до ступеня зниження спотворень сигналів малих амплітуд.

1.3 Методи перетворень аналогових сигналів у цифрові

Крім імпульсно-кодової модуляції (ІКМ) у телефонних компаніях й інших організаціях використовується кілька методів перетворення аналогових сигналів у цифрові. Ці методи розпадаються на два широких класи: аналіз форми хвилі (обвідної) і параметричне кодування.

1.3.1 Аналіз обвідної

Раніше оговорений метод ІКМ відноситься до класу методів аналізу (і синтезу) форми хвилі. Методи називаються так тому, що в них проводиться аналіз форми хвилі, яка потім відображається в цифрові коди для наступного відновлення вихідної хвилі. У наш час у системах перетворення використовуються більш складні підходи, ніж у класичному методі ІКМ. Одна із таких систем модуляції називається диференціальною імпульсно-кодовою модуляцією (ДІКМ). Цей метод передає не фактичні перетворення, а різницю між сусідніми перетвореннями сигналу. Оскільки перетворення сигналів аналогової форми мало відрізняється одне від одного, потрібно зовсім небагато бітів для подання діапазону розходжень. ДІКМ використовує диференціальний цифровий пристрій, що запам'ятовує кожне попереднє відображення. Потім вимірюється розходження між двома послідовними відображеннями й різниця кодується цифровим образом. Диференціальна ІКМ вимагає меншої швидкості передавання оцифрованих акустичних сигналів, ніж при традиційних методах ІКМ.

Особливим видом ДІКМ є дельта-модуляція (ДМ), при якій для кожного перетворення використовується тільки один біт. При ДМ визначається знак різниці послідовних перетворень, потім якщо різниця збільшується, то біт установлюється в 1, якщо ж різниця зменшується, то сигнальний біт встановлюється в 0 (рисунок 1.1, а). Сигнал кодується як „драбинка" з таких послідовностей. Далі цифровий код можна використати для реконструкції аналогового сигналу (аналого-цифрове перетворення).

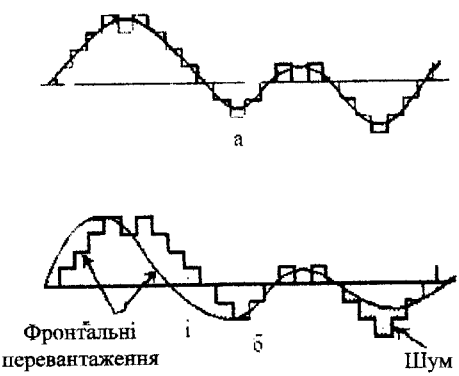


Рисунок 1.1- Дельта-модуляція без спотворення (а) і з спотворенням (б)

ДМ проста в застосуванні. Однак вона вимагає більш частого знімання перетворень, ніж при ІКМ і ДІКМ, оскільки кожне з перетворень містить занадто мало інформації. При ДМ передбачається, що форма кодованого сигналу відрізняється від форми сигналу перетворення не більше ніж на одну „сходинку". Однак сигнал може змінюватися більш швидко, ніж здатний реагувати модулятор при створенні „сходинок", створюючи проблему, іменовану „перевантаження на схилі". І навпаки, повільно змінюваний сигнал також створює перекручування, які називаються дробовим шумом. Описані ефекти неточності подання форми аналогового сигналу називаються шумом кодування; він також виникає й при використанні методів ІКМ і ДІКМ.

Широко використовується варіація методу дельта-модуляція, що називається постійно варіаційною дельта модуляцією змін сигналу (ПВДМ) (інший термін – дельта-модуляція зі стиском). ПВДМ передає розходження між двома послідовними відображеннями й використовує пристрій квантування для змін фактичних кроків квантування на основі раптового збільшення або зменшення сигналу. При ПВДМ розмір сходинки збільшується, якщо виявляється збільшення схилу форми хвилі, і зменшується, якщо нахил зменшується. Як раніше зазначено, ІКМ і ДІКМ також можуть використати ці методи стиску для зменшення кількості помилок. Змінюючи розміри кроків квантування, можна зменшити помилки квантування.

1.3.2 Параметричне кодування (вокодери)

Крім методів аналізу форм хвиль промисловість засобів зв'язку провела більші дослідження в класі методів, що отримали назву параметричне кодування (інші назви цих методів — моделювання, аналітичний синтез, вокодування (Voice coding). Системи з параметричним кодуванням не використовуються в телефонних мережах, оскільки вони призначені тільки для кодування звукових сигналів і не можуть бути пристосовані для інших аналогових сигналів, таких, як передавання від модемів. І навпаки, ІКМ може передавати і дані, і звуки.

Параметричне кодування не зберігає характеристики форми вхідної хвилі: більше того, вхідна хвиля перетвориться в набір параметрів, які визначають акустичні властивості сигналу. Потім відбувається відпрацьовування параметрів цифрового сигналу, що найбільш близький до вихідного звукового сигналу. Ці моделюючі параметри передаються через канал (або запам'ятовуються на диску) для

наступного відтворення акустичного сигналу. Вокодери звичайно використовуються для запису інформаційних повідомлень (наприклад, про погоду), для звукового виходу в персональних комп`ютерах й в електронних ігрових пристроях.

Кодування з лінійним передбаченням (КЛП) (рисунок 1.2) є розповсюдженим видом параметричного кодування. КЛП основано на тому факті, що будь-яка мова складається з голосних і приголосних звуків. Наприклад, тривале „е" є голосним звуком, а „с" у слові „сир" – приголосним звуком. Обидва ці механізми відображаються для створення потоку імпульсів. Потім імпульси можна запам'ятати як цифрові образи.

Далі образ акустичного сигналу визначається на інтервалах в 20—50 мс, які називаються звуковими сегментами або вузлами. Звуковий сегмент відображається й обробляється функцією КЛП, що визначає передбачувані значення відображень. Для кожного відображення виконуються деякі розрахунки. Коли значення обчислені, всі вони використовуються для видачі передбачуваного значення потрібного звукового сегмента. Основна ідея ітеративних обчислень полягає в зменшенні помилки між сигналом вхідного звукового сегмента й передбаченим виходом. При КЛП виконується безперервна адаптація за допомогою періодичних обчислень нових наборів передбачених значень.

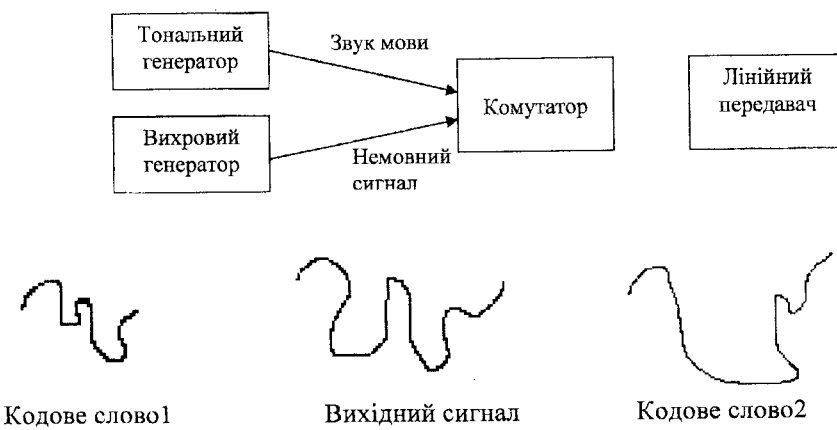


Рисунок 1.2 – Параметричне кодування

Перш ніж сигнал передається в канал, він проходить порівняння за таблицею значень. Як значення, яке фактично відсилається, використовується те значення з таблиці, що найбільш близьке до

значення сигналу. У системі КЛП сигнал приводиться у відповідність за бібліотекою значень. Ця бібліотека називається кодовою книгою. Елемент бібліотеки, значення якого дають найбільше наближення до значень сигналу, вибирається як кодове слово. Переваги цього підходу полягають у тому, що кожне кодове слово можна зобразити дуже малим числом бітов. Наприклад, якщо бібліотека містить 4000 елементів, то потрібно тільки 10-12 біт для подання і/або передачі інформації про весь звуковий сегмент.

Переваги цього методу полягають в тому, що використання кодової книги в КЛП дозволяє здійснювати передачі зі швидкістю всього лише 2,4 кбіт/с. А високоякісні телефонні лінії зі швидкістю 9,6 кбіт/с можуть підтримувати чотири 2,4 кбіт/с передачі КЛП за допомогою мультиплексування з поділом часу. Ця швидкість передачі значно нижча, ніж потрібно для методів аналізу форми хвилі (16, 32 й 64 кбіт/с). Природно, основним недоліком КЛП є більш низька (ніж в ІКМ) якість відтворення звуків.

1.4 Інтегровані цифрові мережі

1.4.1 Інтегрована мережа

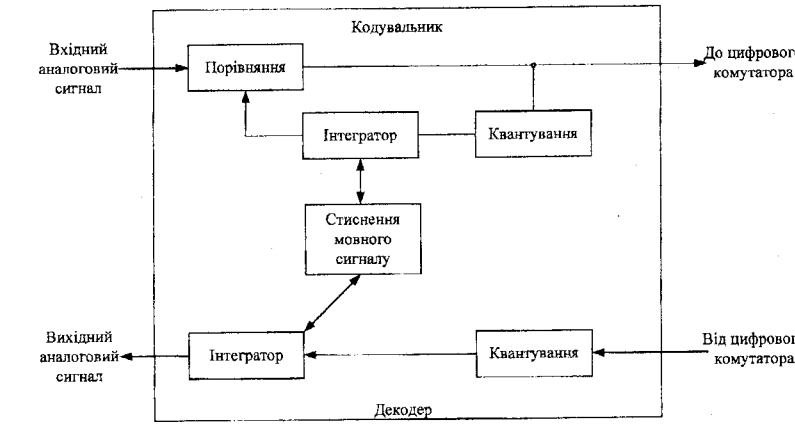
Як зазначено в розділі 5 першої частини посібника кадр протоколу TDMA може містити інформацію про мову або дані.

Мережа, що використовує кадр TDMA розміщує один мовний канал на кадр, щоб виконувати узгодження зі швидкістю передавання цифрової мови.

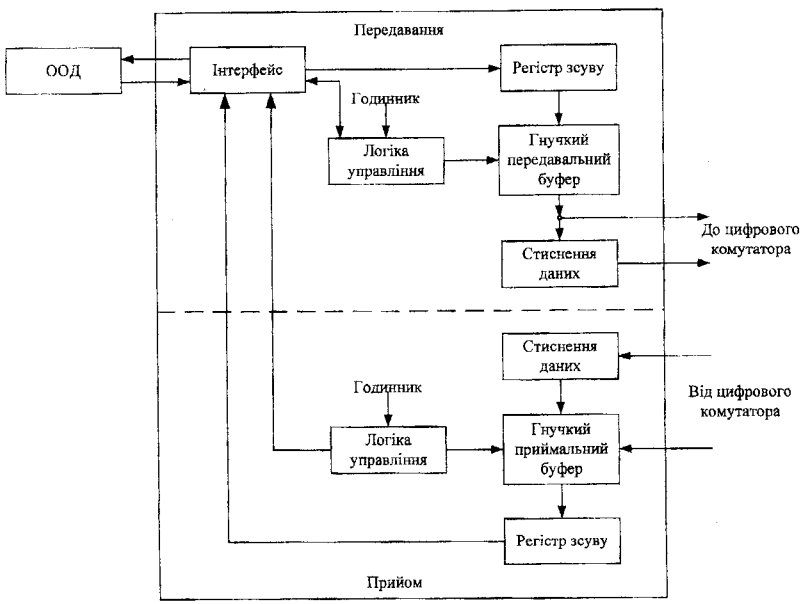
Адаптер порта зображений на рисунку 1.3. Мовний порт використовує схему з розширеною дельта-модуляцією на 32 кбіт/с (також називається логарифмічною розширеною дельта-модуляцією (ЛРДМ)). Ця модуляція допустима при передаванні мови, забезпечує низькі швидкості передавання і допустиму пропускну здатність в широкому діапазоні вхідних сигналів. Мовний порт опрацьовує виклик способом, що нагадує дії телефонної станції:

- трубка знімається з важіля (телефона або РВХ);
- мережа встановлює програму запису з'єднання і посилає абоненту тональний сигнал;
- на порт поступають цифри набору від абонента;
- контролер зв'язку зі супутником (КЗС), що викликається, посилає сигнал «спроба з'єднання» викликаному КЗС на основі протоколу TDMA;

– після того, як трубка сторони що викликається знята, канал виклику передає сигнал з'єднання і канал що ініціював виклик, відповідає «відповідь з'єднання»;



а)



б)

Рисунок 1.3 - Мовний порт (а) та порт даних (б)

- сторони ведуть розмову, а мовні порти оцифровують мову для введення в кадри TDMA;
- будь-яка зі сторін дає «відбій» і канал зв`язку передає сигнал «роз'єднання», а інша КЗС «дає відповідь на роз'єднання».

Мовний порт також виконує стиснення мовного сигналу (СМС). Будь-яка мова включає паузи (між словами та для вислуховування). СМС використовує можливості періодів мовчання для передавання даних для пристрою кодування, який відповідає відповідній частоті сигналів. Як тільки сторони, що розмовляють, потребують входу до мережі, СМС надає цю можливість, розподіляючи супутникові канали між багатьма мовними діалогами. Сорок розмов можуть потребувати всього лише 25 каналів.

Користувач може взаємодіяти з цим портом через модеми або термінали. «Еластичний буфер» компенсує часи користувача та часи каналу зв`язку. Регістри зсуву перетворюють байти інформації користувача в потоки послідовних бітів, що подають дані.

Цифрові порти також використовують методи стиснення даних (СД). Коли 480-бітовий елемент канала містить рядок символів, які збігаються з даними в іншому каналі, то цей елемент не передається по каналу. Приймальний пристрій СД реконструює вихідні дані з потоку і використовує останній елемент даних, який було отримано від окремого порту для повторення послідовності символів і відновлення каналу.

Таким чином, за допомогою мовних портів, портів даних і мультиплексування з розподіленням часу система інтегрує передавання мовних сигналів та даних. Після того, як сигнали закодовані, вони трактуються однаково і всі вимоги та проблеми в каналі вирішуються технологічно.

1.4.2 Цифрові мережі з інтегрованим обслуговуванням

Цифрові мережі з інтегрованим обслуговуванням (ЦМІО) забезпечують наскрізний зв'язок по цифрових даних для підтримки широкого діапазону послуг. В сутності, всі образи (мова, дані, телевізійні сигнали, факсимільний зв'язок тощо) передаються за допомогою цифрових технологій. ЦМІО мають 5 основних цілей:

- забезпечувати всесвітню однакову цифрову мережу, яка підтримує широкий діапазон різноманітних послуг та використовує одні й ті ж самі стандарти в усіх країнах;
- забезпечити єдиний набір стандартів для цифрового передавання в мережах та між мережами;
- забезпечити такий стандартний інтерфейс користувача ЦМІО, щоб внутрішні зміни в мережі залишалися невидимими для користувача;

- разом з попереднім пунктом забезпечити для кінцевого користувача незалежність прикладних програм;

- разом з двома попередніми пунктами забезпечити мобільність користувачів і прикладних програм.

Таким чином, ЦМІО сконцентровані на трьох основних проблемах:

- стандартизації послуг, що пропонуються абонентам для того, щоб сприяти сумісності в міжнародних маштабах;
- стандартизації інтерфейсів «користувач-мережа» для сприяння незалежній розробці як термінального, так і мережевого обладнання;
- стандартизації можливостей мереж для сприяння розвитку зв'язків між користувачами, мережею та взаємодіями між мережами.

В багатьох джерелах ЦМІО називають революційною технологією, але це не так – ЦМІО є еволюційною технологією.

ЦМІО базуються на сучасних інтегрованих цифрових технологіях телефонних мереж (ІЦМ). Відповідно багато з методів обробки цифрових даних, що раніше були обговорені в даному розділі, можна використовувати в майбутніх системах ЦМІО. Ці можливості включають швидкості передавання сигналів, коди передавання (біполярні) і навіть фізичні розніми.

Інтерфейси ЦМІО. На рисунку 1.4 зображено стандартні інтерфейси кінцевого користувача мереж ЦМІО.

Рекомендаційні стандарти ЦМІО забезпечують невеликий набір сумісних інтерфейсів, які призначені для ефективної підтримки прикладних програм користувача. Стандарт визначає, що різні інтерфейси потрібні для програм з різними швидкостями передавання і обробки даних і для різних вимог до роботи з даними.

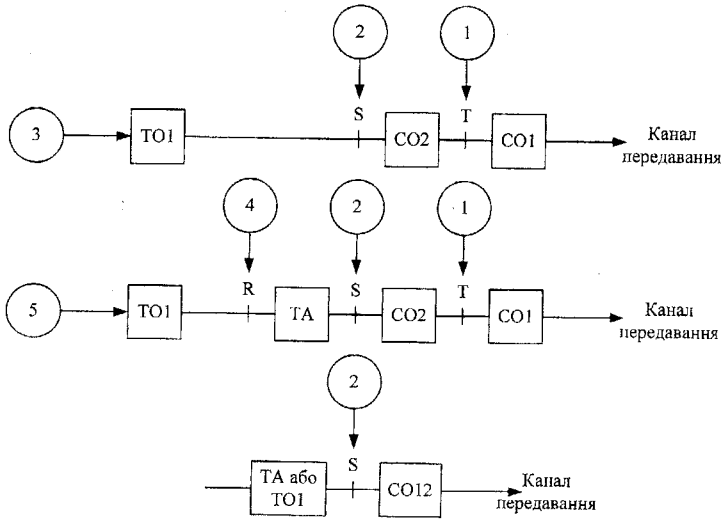
Відповідно забезпечується більше ніж один тип інтерфейсів. Перед тим як пояснити рисунок 1.4, необхідно визначити два терміни:

- функціональна група – це набір засобів, що необхідні для інтерфейсу доступа користувача до ЦМІО. Специфічні функції в функціональній групі можуть бути виконані багатьма елементами, що включають як апаратуру, так і програми.

- точки відправлення – це точки розподілення між функціональними групами. Зазвичай точки відправлення відповідають фізичним інтерфейсам між частинами апаратури.

Рисунок 1.4 відображає конфігурацію посилань для інтерфейсів «користувач – мережа» в ЦМІО.

Точки відправлення S і T використовують рекомендаційні структури канальних інтерфейсів із спеціального стандарту I.412. Фізичний інтерфейс в точці відправлення P виконується у відповідності з іншими рекомендаціями МККТТ або ЕСМА.



□ - функціональна група; + - еталонна точка (або інтерфейс); О - точка доступу

Рисунок 1.4- Основні конфігурації ЦМІО

ЦМІО також забезпечують точки доступу. Точки доступу визначаються таким чином: точка доступу 1 (точка відправлення Т) і точка доступу 2 (точка відправлення S) є точками доступу для опорного сервісу, що забезпечується ЦМІО. Функції опорного обслуговування включають три нижніх рівні із моделі ЦМІО. Точка доступу 4 включає інші види послуг, стандартизованих МККТТ, які базуються на специфічних рекомендаціях X та V, що використовуються в термінальних адаптерах (ТА).

Функціональна група NT1 (network termination) включає функції, що еквівалентні функціям фізичного рівня моделі ВВС. Ці функції пов'язані з фізичними та електричними з'єднаннями в мережі. Нижче перечислені такі основні функції групи NT1:

- закриття лінії;
- підтримка лінії на рівні 1 і управління пропускною здатністю;
- сигнали та таймування передавання;
- ресурсозабезпечення каналу;
- можливість мультиплексування в рівні 1;
- завершення інтерфейсу, включаючи у випадку необхідності закриття багатьох інтерфейсів одночасно.

Група NT1 здатна визначати межі власників мережі ЦМІО; вона також може контролюватись власником мережі. Ця група використовує

фіксований стандартний інтерфейс з ЦМІО. Група NT1 забезпечує прозорість роботи в мережі і звільняє користувачів від фізичних аспектів ЦМІО.

Функції групи NT2 еквівалентні функціям фізичного та більш високих рівнів моделі ВВС. Параметрами функцій групи NT2 є станції приватних телефонних мереж, локальні мережі, контролери терміналів і кластери. Іншими словами, група NT2 діє як інтерфейс з пристроями кінцевих користувачів. На рисунку показано, що обладнання кінцевих користувачів включається в групу NT2 через точку посилання – з'єднання S. Оскільки група T2 може зображати телефонну мережу, локальну мережу ЕОМ, контролер терміналу, вона може виконувати такі функції, як комутація, мультиплексування та обробка протоколів. Ця група функцій несе основну відповідальність за обробку проколів 2 і 3 рівнів.

Фактично виконувані цією групою функції не обумовлені рекомендаціями до ЦСІО. Однак відсутність обмежень дозволяє виконувати функції рівнів 1, 2 і 3, хоча для рівня 1 одиничною виконуваною функцією, імовірно, є просте мультиплексування з розподілом часу (МРВ).

Функціональна група NT12 (комбінація NT1 та NT2) є багатофункціональним пристроєм, що містить усі можливості груп NT1 та NT2. Пристрої включаються в цю групу через з'єднувач точки посилання S. В групу NT2 та NT12 входять такі функції:

- обробка протоколів рівнів 2 і 3;
- мультиплексування на рівнях 2 і 3;
- функції комутації;
- функції концентрації;
- функції супроводження мереж;
- завершення функцій рівня 1.

Функції термінального обладнання (ТЕ) зображають апаратуру кінцевого користувача. Вони включають пристрої, такі як цифрове телефонне обладнання станцій інтегрованого обслуговування цифрових мереж, що встановлені в організаціях. Функції термінального обладнання такі:

- обробка протоколів більш високих рівнів;
- функції підтримки працездатності;
- функції інтерфейсу;
- функції підключення іншого обладнання.

В ЦСІО визначені два види функції ТЕ. Функції ТЕ1 працюють з мережами ЦСІО і використовують інтерфейс цих мереж. Функції ТЕ2 вимагають більш загально прийнятих інтерфейсів, таких як RS-232-C чи стандартів серій V або X.

Термінальний адаптер (ТА) по суті є перетворювач протоколу, який

перетворює існуючі інтерфейси, такі як RS-232-C, V.24 або X.21, в стандартні інтерфейси ЦСІО. Ці стандарти також дозволяють комбінувати функції ТА з пристроєм кінцевого користувача. Основною ж задачею функції ТА є підтримка з'єднання ЦСІО і пристроїв, що виконують функції групи ТЕ2.

На рисунку 1.5 показані вісім інших можливих конфігурацій ЦСІО.

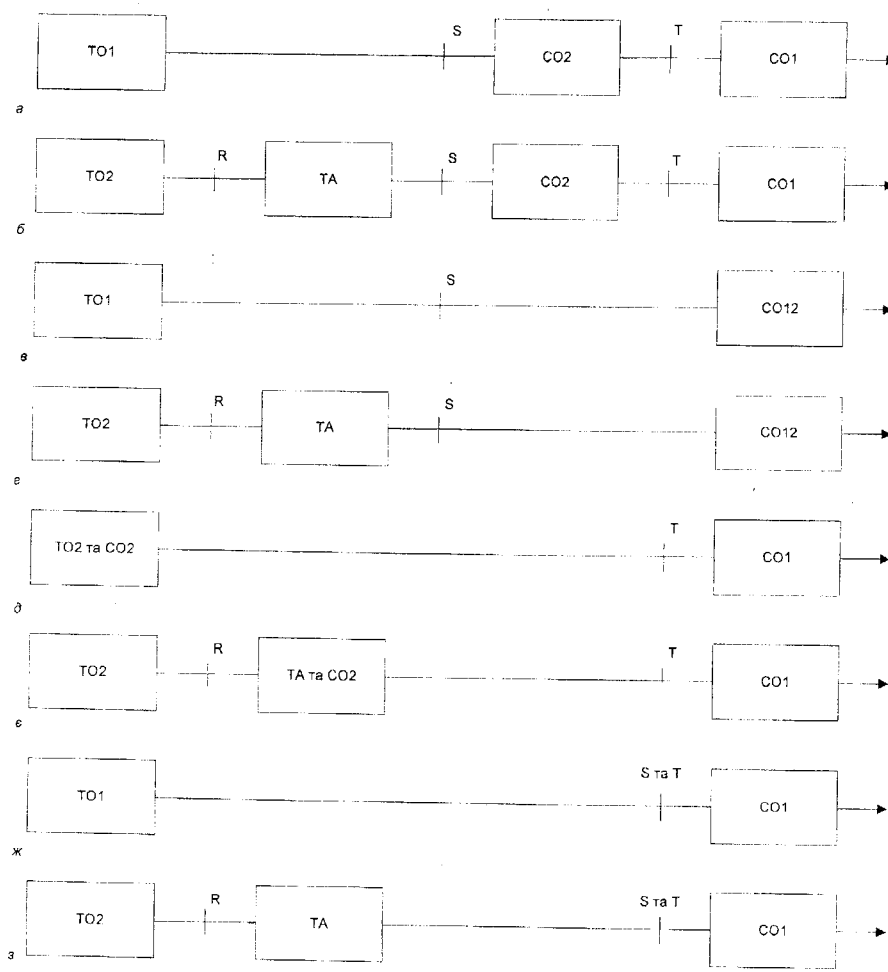


Рисунок 1.5 – Інші можливі інтерфейси ЦСІО

Конфігурації на рисунку 1.5, *а* і *б* показують інтерфейси ЦСІО в точках посилання S та T. На рисунку 1.5, *в* і *г* показані конфігурації, в яких

інтерфейси ЦСІО існують тільки в точці S. На рисунку 1.5, *д* і *є* інтерфейси ЦСІО створені тільки в точці T. І нарешті, рисунки 1.5, *ж* і *з* показують єдині інтерфейси ЦСІО, в яких точки S і T з`єднані.

Канали ЦСІО. Найбільш загальний інтерфейс ЦСІО складається з каналу B та каналу D. В доповнення до цих каналів ЦСІО забезпечує двійкове передавання даних для керування кадруванням та інших цілей, що збільшує сумарну швидкість передавання. Інтерфейси передбачають мультиплексування з розподіленням часу для двох каналів. Стандарт передбачає подальше мультиплексування каналів B на підканали. Наприклад, канали B можна розподілити на підканали. Два канали B можуть бути скомбіновані разом або розподілені за бажанням користувача.

Канали B призначені для передавання протоколів даних користувачів. Вони забезпечують декілька різних видів послуг для прикладних задач. Наприклад, канал B може передавати мову на швидкості, передавати дані, забезпечувати широкополосну передачу акустичних сигналів.

Канал D призначений для передачі інформації керування і сигналізації, хоча в деяких випадках ЦСІО дозволяє каналу D передавати і дані користувача. Однак канал B, безумовно, не може передавати сигнальну інформацію. В ЦСІО сигнальна інформація позначається як дані типу S, пакети – типу F і телеметрична інформація – типу T. Канал D може передавати інформацію усіх певних типів за допомогою мультиплексування.

Робочі комітети із ЦСІО передбачають розробку інших видів каналів (E та H). Ці канали призначені для значно більших швидкостей передавання. Так, канал E переносить сигнальну інформацію для комутації ланцюгів.

ЦСІО потребують інтерфейси каналу B в точках S і T, що погоджує ці інтерфейси одною з трьох структур:

Тип 1: структури інтерфейсу каналу B. Основна структура інтерфейсу, яка складається з двох каналів B і одного каналу D. Ця структура потребує, щоб обидва канали B і один канал D були подані в інтерфейсі користувача мережі. Цей тип структури відомий під позначенням 2.

Тип 2: структура інтерфейсу на основі початкової швидкості передачі каналу B. Ця альтернатива призначена для структур, що відповідають загальним швидкостям передавання. Початкові канали утворені з каналів B і одного каналу D. Північноамериканський стандарт потребує структури інтерфейсу, що складається з 23 каналів B і одного каналу D (23B+D). Європейський підхід потребує структури інтерфейсу, що складається з 30 каналів B і одного каналу D (30B+D).

Тип 3: структура інтерфейсу на основі альтернативної початкової швидкості передачі каналу B. Цей тип структури можна використовувати,

коли пристрій NT2 під'єднується до мережі за допомогою більш ніж одного каналу В. Так, для швидкості 1,544 Мбіт/с структура інтерфейсу складається з 23 каналів В і одного каналу Е (23В+Е). Для швидкості 2,048 Мбіт/с структура інтерфейсу складається з 30 каналів В і одного каналу Е (30В+Е).

В ЦСІО підтримуються і інші стандарти, а допоміжні можливості досліджуються.

Рівні ЦСІО. Підхід ЦСІО призначений для забезпечення кінцевого користувача повною підтримкою на всіх семи рівнях моделі ВВС. Таким чином, ЦСІО підрозділяється на два види послуг: базові послуги, що відповідають за підтримку нижніх трьох рівнів з семирівневого стандарту, і на телесервіс (наприклад, телефони, телекс, відеотелекс, обробка повідомлень), який відповідає за підтримку всіх семи рівнів моделі і взагалі використовує можливості послуг базових рівнів. Відповідно всі послуги називаються послугами нижніх і вищих рівнів. Функції ЦСІО розташовуються згідно з принципами рівневого розподілу в стандартах МОС або МККТТ. Ці функції зображені на рисунку 1.6. Відмінності в сутності рівнів використовуються для забезпечення повного набору можливостей в мережах. Ці засоби можуть бути забезпечені державними відомствами зв'язку, телефонними компаніями, промисловими фірмами.

<table>
<tr><td rowspan="7">Функції високих рівнів (телесервіс)</td><td>7</td><td colspan="8">Прикладні функції</td></tr>
<tr><td>6</td><td colspan="2">Кодування\декодування</td><td colspan="3">Стиснення/розширення</td><td colspan="2"></td></tr>
<tr><td>5</td><td>Установлення з'єднання сеансу</td><td>Звільнення з'єднання сеансу</td><td colspan="2">Відображення сеансу в транспортне з'єднання</td><td>Синхронізація з'єднання сеансу</td><td>Управління сеансом</td><td></td></tr>
<tr><td>4</td><td colspan="2">Рівень 4 Мультиплексування з'єднання</td><td>Рівень 4 Установлення з'єднання</td><td>Рівень 4 Звільнення з'єднання</td><td>Виявлення помилок/ відновлення</td><td>Управління потоком</td><td>Сегментація/блокування</td></tr>
<tr><td rowspan="3">Функції низьких рівнів (базове обслуговування)</td><td>3</td><td>Сегментація/перемикання</td><td>Установлення з'єднання в мережі</td><td>Звільнення з'єднання в мережі</td><td>Мультиплексування мережевих з'єднань</td><td>Управління зчепленням</td><td>адресація</td><td></td></tr>
<tr><td>2</td><td>Установлення з'єднань кільця даних</td><td>Звільнення з`єднань кільця даних</td><td>Управління потоком</td><td>Контроль помилок</td><td>Контроль послідовностей</td><td>Синхронізація кадрів</td><td></td></tr>
<tr><td>1</td><td colspan="2">Активація з'єднань фізичного рівня</td><td colspan="2">Дизактивація з'єднань фізичного рівня</td><td>Передача бітів</td><td colspan="2">Мультиплексування структури каналу</td></tr>
</table>

Рисунок 1.6 – Багаторівнева модель ЦМІО

Об'єднання компонентів ЦСІО і взаємодія двох кінцевих користувачів в ЦСІО може виконуватися за допомогою каналу D і мережі комутації пакетів X.25. Так, пристрій зв`язку А, який в термінології ЦСІО розглядається як конфігурація ТЕ1, використовує зі своєї сторони всі сім рівнів. Пристрій зв`язку взаємодіє з фізичним рівнем ЦСІО через інтерфейс S/T з пристроєм NT1. Зі своєї сторони, механізм NT1 передає інформацію користувача обробнику пакетів. Обробник пакетів взаємодіє з мережею комутації пакетів через протокол X.75. Дані перетинають мережу комутації пакетів. Вони передаються віддаленим оброблювачем пакетів до NT1 і в кінцевому випадку до пристрою зв`язку В кінцевого користувача на інтерфейс S/T.

LAPD. В ЦСІО забезпечений протокол рівня каналу логічного зв'язку даних, які дозволяють пристрою зв`язку взаємодіяти між собою по каналу D. Цим протоколом є LAPD, підмножина HDLC. LAPD діє на рівні зв'язку даних архітектури ВВС. Протокол не залежить від швидкості передавання і вимагає дуплексного прозорого каналу.

Протокол LAPD має формат кадру, схожий на формат HDLC. Більше того, подібно до HDLC, цей формат забезпечує ненумеровані, супервізорні і інформаційні кадри. Таблиця 1.1 показує команди і відгуки LAPD, а також відмінність та подібність між LAPD і HDLC. Протокол LAPD також дозволяє здійснити операції за модулем 128. Керуючий байт, який визначає відмінності між форматами інформаційного, супервізорного і ненумерованого кадрів, ідентичний структурі байта в HDLC. LAPD передбачає два байти для адресного поля (рисунок 1.7). це особливо важливо для мультиплексування багатьох функцій в каналі D. Адресне поле містить біти розширення адресного поля, біт індикації команди або відгуку, ідентифікатор точки входу в сервісний засіб (ІТВС) та ідентифікатор точки завершення (ІТЗ). Ці точки входів розглядаються нижче.

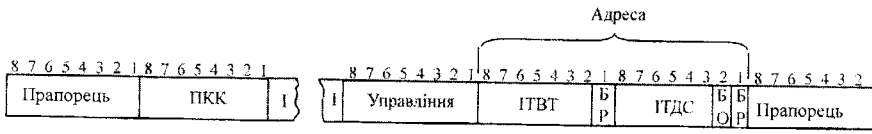
Розширення адресного входу призначене для забезпечення більшої кількості бітів в цьому полі. Якщо в першому біті байта адресного поля міститься одиниця, то тим самим відзначається, що цей байт – останній в адресному полі. Відповідно, двобайтова адреса має значення розширення адресного поля, рівне 0 в першому байті та рівне 1 в другому байті. Біт розширення адресного поля дозволяє використовувати й ІТВС в першому байті та ІТЗ в другому байті.

Біт в полі вказання команди/відповіді (К/В) ідентифікує, чим є кадр 0 – командою або відповіддю. Зі сторони користувача відсилаються команди з бітом К/В, встановленим в 0, відповіді з цієї ж сторони йдуть з бітом К/В, що дорівнює 1.

Мережа виконує все в оберненому порядку. Вона відправляє команди, вказуючи 1 в біті К/В, а відповіді – вказуючи 0. Всі можливі умови установлення значень біта К/В наведені в таблиці 1.2.

Таблиця 1.1 – Команди і відповіді LAPD

Формат	Команди	Відповіді	Управляюче поле								Подібне з HDLC
			8	7	6	5	4	3	2	1	
Передача даних	I (інформація)		—N(R)—			P	—N(S)—			0	Да
Супервізор	RR (готовність до прийому)	RR (готовність до прийому)	—N(R)—			P/F	0	0	0	1	»
	RNR (неготовність до прийому)	RNR (неготовність до прийому)	—N(R)—			P/F	0	1	0	1	»
	REJ (відмова)	REJ (відмова)	—N(R)—			P/F	1	0	0	1	»
Ненумерований кадр			0	0	1	P	1	1	1	1	»
	SABM (установлення асинхронного збалансованого режиму)	DM (режим відокремлення)	0	0	0	F	1	1	1	1	Ні
	SI0 (послідовна інформація 0)	SI0 (послідовна інформація 0)	0	1	1	P/F	0	1	1	1	»
	SI1 (послідовна інформація 1)	SI1 (послідовна інформація 1)	1	1	1	P/F	0	1	1	1	Ні
	UI (ненумерована інформація)		0	0	0	P	0	0	1	1	Да
	DISC (відокремлення)		0	1	0	P	0	0	1	1	»
		UA (ненумероване підтвердження)	0	1	1	F	0	0	1	1	»
		FRMR (скидання кадру)	1	0	0	F	0	1	1	1	»



ПРАПОРЕЦЬ=01111110
БР - біт розширеного адресного поля
БО - біт ознаки команди/відповіді
ІТДС – індикатор точки доступу до сервісного засобу
ІТВТ – індикатор точки входу в термінал
I – інформаційне поле
ПКК – послідовність контролю кадру

} Ідентифікатор з`єднання кільця даних

Рисунок 1.7 – Формат кадру LAPD

Таблиця 1.2 – Біти поля вказання команди/відповіді

	Біт від мережі	Біт від користувача
Прийом команди	1	0
Відсилання відповіді	1	0
Відсилання команди	0	1
Прийом відповіді	0	1

Ідентифікатор точки входу в сервісний засіб (ІТВЗ) визначає точку, в якій послуги рівня зв'язку даних надаються більш високому рівню (тобто рівню 3).

Ідентифікатор точки завершення (ІТЗ) визначає або одиничний термінал, або множину терміналів ІТЗ, призначається автоматично за допомогою окремої процедури призначення. Поле управління ідентифікує тип кадру, а також номери послідовностей, що використовуються для підтримки режиму вікон і підтверджень між пристроями.

У таблиці 1.2 показані дві команди і відповіді, що не існують у множині HDLC. Це послідовна інформація 0(SI0) і послідовна інформація 1(SI1). Команди SI0/SI1 призначені для передавання інформації з використанням послідовно кадрів підтвердження. Інформаційні команди перевіряються за допомогою останнього поля (SI). Біт P встановлений у 1 для всіх команд SI0/SI1. Відповіді SI0 і SI1 використовуються при виконанні дій над одиничним кадром для підтвердження прийому кадрів команд SI0 і SI1, а також для індикації втрат кадрів або проблем із синхронізацією. LAPD не дозволяє розрізняти інформаційні поля в кадрах відповідей SI0 і SI1. Природно, інформаційні поля присутні в командних кадрах SI0 і SI1.

ЦСІО також працюють на рівні даних. Специфікації цього рівня включають з'єднання комутації ланцюгів, з'єднання комутацій пакетів і з'єднання між користувачами.

Таблиця 1.3 наводить стани мереж ЦСІО і процедур, установлення часу сеансів, а також процедур передавання даних і закінчення сеансів. Сукупність застосування цих двох технологій комутації – ланцюгів і пакетів при використанні в ЦСІО набула широкого обговорення. Критика основана на впевненості, що однієї технології, а саме, комутації пакетів, досить для узгодження з будь-якими прикладними потребами в мережах ЦСІО. Наприклад, система SBS успішно використовує єдиний підхід. Однак завдяки багатоканальності сигналів супутника SBS комутація і маршрутизація сигналів не береться до уваги.

Таблиця 1.3 – Стани ЦСІО для викликів з комутацією ланцюгів

Назва стану	Значення стану
U0	Нульовий стан – немає викликів

Продовження таблиці 1.3

Назва стану	Значення стану
U1	Блок виклику – стан існує для вихідного виклику як результат дії користувача, який зробив запит установлення виклику
U2	Посилка з перекриттям – стан існує для вихідного виклику в той час, коли користувач посилає інформацію установлення виклику в режимі перекриття
U3	Проведення вихідного виклику – стан існує для вихідного виклику, коли мережа підтвердила прийом інформації, необхідної для проведення виклику, а користувач очікує подальших відповідей мережі
U4	Виклик доставлений – стан для вихідного виклику, що виникає, коли мережа завершила проведення виклику в точку прийому сигналу від інтерфейсу користувача з мережею, зазначеного адресою виклику, або від альтернативного інтерфейсу, визначеного або викликаного користувачем або мережею
U5	Узгодження – стан існує для вхідного виклику протягом узгодження виділення відповідного каналу В
U7	Виклик отриманий, і стан існує для вхідного виклику протягом часу, коли відповідь/відгук від користувача, що викликається, знаходиться в стані очікування
U8	Запит на з'єднання – стан існує для вхідного виклику при очікуванні прийому від мережі підтвердження з'єднання
U9	Проведення вхідного виклику – стан існує для вхідного виклику, коли користувач підтвердив прийом інформації, необхідної для проходження виклику, а мережа очікує наступного відгуку користувача
U10	Активність – стан існує, коли при виклику виконуються наскрізні зв'язки
U11	Вимоги роз'єднання – стан існує як реакція на вимогу користувача роз'єднання виклику раніше, ніж отримане підтвердження від мережі
U12	Запит на роз'єднання – стан існує, коли мережа вказує на роз'єднання, а користувач не зазначив звільнення або від'єднання

Продовження таблиці 1.3

Назва стану	Значення стану
U13	Запит на від'єднання – стан існує, коли користувач зробив запит на від'єднання, перед тим, як отримав підтвердження від мережі
U14	Від'єднання – стан існує, коли канал У звільнений, але виклик не очищений
U15	Запит на припинення – стан існує у відповідь на дію користувача, що приводить до переходу термінала в режим локальних процедур, а мережа ще не видала підтвердження
U16	Локальне припинення – стан існує у відповідь на запит припинення, що випливає за прийомом підтвердження запиту на припинення від мережі
U17	Запит на поновлення – стан існує у відповідь на запит відновити раніше припинений виклик, перед тим, як це підтверджується мережею
U19	Запит на звільнення – стан існує у відповідь на запит, перед тим, як отримується підтвердження від мережі
U20	Запит на віддалений засіб – стан існує у відповідь на запит від мережі на активізацію засобу раніше, ніж користувач відгукнувся
U21	Запит на локальний засіб – стан існує після запиту користувача до мережі на активізацію засобу, перед тим , як мережа відгукнулася
№0	Нульовий стан – немає викликів
№1	Посилка звуку тональності набору – стан існує для вихідного виклику, коли мережа посилає звук тональності набору до прийому першого повідомлення
№2	Посилка з перекриттям – стан існує для вихідного виклику в той час, коли мережа очікує подальшої інформації від користувача до повного установлення виклику
№3	Проведення вихідного виклику – стан існує для вихідного виклику, коли мережа підтвердила прийом інформації, необхідної для проведення виклику, а користувач очікує від мережі подальшого відгуку
№4	Виклик доставлений – стан існує для вихідного виклику, коли передбачається, що на інтерфейсі, який викликається користувачем, існує сумісна апаратура, що може прийняти виклик
№5	Узгодження – стан існує для вхідного виклику, коли користувач і мережа намагаються вибрати канал У, по якому буде виконаний виклик

Продовження таблиці 1.3

Назва стану	Значення стану
№6	Виклик присутності – стан існує для вхідного виклику, коли мережа виконала індикацію виклику, але жодний із користувачів не зазначив, чи може він прийняти виклик
№7	Виклик отриманий – стан існує для вхідного виклику після того, як устаткування користувача видає індикацію початку сигналізації користувачу
№8	Запит на з'єднання – стан існує, коли виклик що входить, очікує відповіді на повідомлення про з'єднання до користувача
№9	Проведення вхідного виклику – стан існує для вхідного виклику, коли користувач підтвердив прийом інформації, необхідної для проведення виклику, а мережа очікує подальших відповідей від мережі
№10	Активність – стан існує, коли при виклику виконуються прямі зв'язки
№11	Вимога роз'єднання – стан існує після того, як користувач дав індикацію на роз'єднання, а мережа ще не очистила з'єднання
№12	Індикація роз'єднання – стан існує, коли мережа видала індикацію про роз'єднання, а користувач все ще не одержав індикації про роз'єднання
№13	Запит на від'єднання – стан існує, коли мережа потребувала від'єднання виклику раніше, ніж виконалось підтвердження користувачем
№14	Роз'єднання – стан існує, коли В-канал звільнений, але виклик не очищений ні мережею, ні користувачем
№15	Запит на припинення – стан існує, коли мережа одержала запит на припинення, але ще не відіслала відповідь користувачу
№16	Локальне припинення – стан існує, коли мережа позитивно підтвердила запит на припинення виклику
№17	Запит на поновлення – стан існує, коли мережа одержала запит на поновлення, але ще не відправила відповідь користувачу
№18	Звукова тональність активного стану – стан існує після запиту роз'єднання мережі, коли використовується режим посилки тональності в смузі пропускання
№19	Запит на звільнення – стан існує, коли мережа ініціює звільнення виклику (тобто роз'єднання каналу В і звільнення посланого значення виклику) і очікує підтвердження від користувача

Продовження таблиці 1.3

Назва стану	Значення стану
№20	Запит на віддалений засіб – стан існує після запиту від мережі на активізацію засобу раніше, чим відповість користувач
№21	Запит на локальний засіб – стан існує після запиту від користувача на активізацію засобу, перед тим , як мережа відгукнулася

Повідомлення рівня даних ЦСІО розподіляються на чотири категорії: повідомлення установлення виклику, повідомлення зняття виклику, повідомлення фази інформації виклику, інші повідомлення. До повідомлень першої категорії (установлення виклику) належать:

- ALERTing (сигналізація);
- CALL PROCeeding (проведення виклику);
- CONNect (з'єднання)
- CONNect ACKnowledge (підтвердження з'єднання)
- SETUP(установлення)
- SETUPACKnowledge(підтвердження установлення).

До повідомлень другої категорії (зняття виклику) належать:

- DETach (від'єднання);
- DETach ACKnowledge (підтвердження від'єднання);
- Disconnect (роз'єднання);
- RELease (звільнення) ;
- RELease COMplete (виконання звільнення).

До повідомлень третьої категорії (фази інформації виклику) належать:

- RESume (відновити);
- RESume ACKnowledge (підтвердження відновлення);
- RESume REJect (відмова від відновлення);
- SUSPend (призупинити);
- SUSPend ACKnowledge (підтвердження призупинення);
- SUSPend REJect (відмова від призупинення);
- USER INFOrmation (інформація користувача).

До повідомлень четвертої категорії належать:

- CANCel (скасувати);
- CANCel ACKnowledge (підтвердження скасування);
- CANCel REJect (відмова від скасування);
- CONgestion CONtrol (контроль переповнення);
- FACility (засіб);

- FACility ACKnowledge (підтвердження засобу);
- FACility REJect (відмова від засобу);
- INFOrmation (інформація);
- REGister (регістр);
- REGister ACKnowledge (підтвердження регістра);
- REGister REJect (відмова від регістра);
- STATUS (статус).

Мережі типу ЦСІО найбільш доцільно використовувати в таких прикладних галузях де необхідні можливості відбору суттєвих і несуттєвих типів послуг, режимів каналів, швидкостей передавання даних.

1.5 Цифрова комутація

Повністю інтегрована цифрова мережа повинна мати можливість комутувати сигнали серед різних вхідних компонентів. Тому застосовується технологія цифрової комутації для виконання функцій маршрутизації і переключення цифрових, імпульсно-кодових способів. На рисунку 1.8 наведений простий цифровий комутатор із розподілом часу.

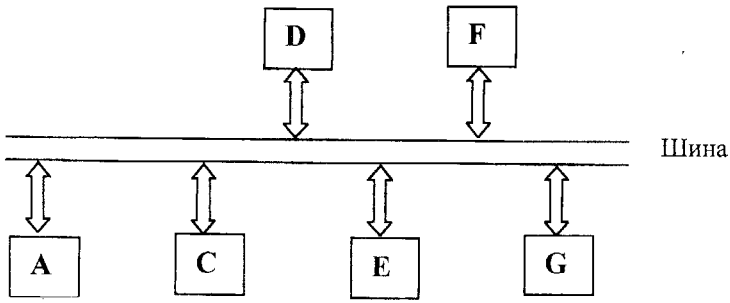


Рисунок 1.8 – Простий цифровий комутатор з розподіленням часу

Комутатор управляє шлюзами в шині. Шлюзи відкриваються і закриваються, це дозволяє передавати цифрові біти між пристроями, що приєднані до шини.

На цьому рисунку, коли пристрій А взаємодіє з пристроєм F, комутатор закриває шлюзи до пристрою А і пристрою F протягом такого періоду обслуговування, що дозволяє передавати через шину сегменти промови або даних.

Доступні два види цифрової комутації: просторова і з розподілом часу. При просторовій комутації вхідний елемент окремої певної тривалості з'єднується з будь-яким вихідним елементом тієї ж тривалості. Таким чином, з'єднання існує тільки протягом існування елемента передавання.

Більш досконала цифрова комутація – комутація з розподіленням часу. Вона відокремлює індивідуальні сигнали в ІКМ і комутує їх за допомогою механізму обміну елементами передавання (МОЕП) (рисунок 1.9).

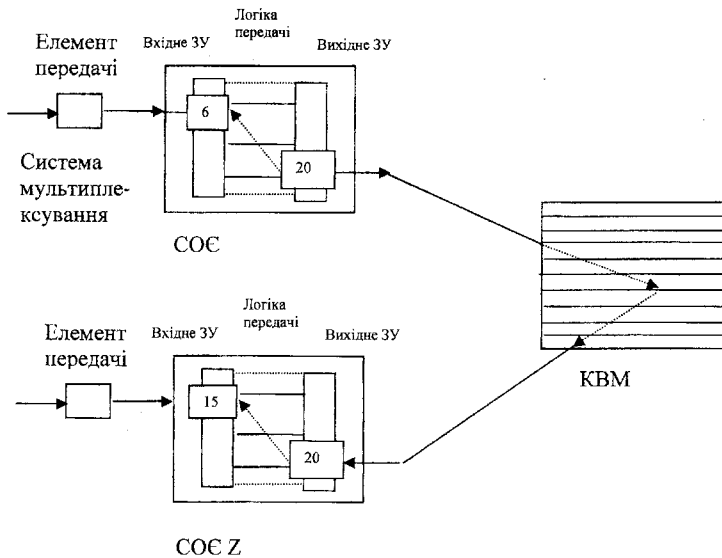


Рисунок 1.9 – Цифрова комутація з тимчасовим мультиплексуванням

МОЕП може не виконувати блокування, і тоді на виході буде стільки ж елементів, скільки і на вході. Канал можна переключити з тимчасового стану X у вхідному кадрі в тимчасовий стан Y у вихідному кадрі. У більш складних системах один МОЕП звичайно з'єднується з іншим для утворення комутаторів із тимчасовим мультиплексуванням (КТМ). Він у сутності є перемикачем (nXn), де n – число з'єднань; однак КТМ виконує цю дію в іншому вимірі – у часі. На відміну від інших систем комутації і багатьох місцевих станцій, що зберігають канал відкритим протягом всього виклику, КТМ змінює стани каналу для кожного з n тимчасових елементів у цифрових кадрах, що виходять із мультиплексора з розподіленням часу.

Ця концепція близька до концепції віртуального з'єднання при комутації пакетів і протоколу X.25. Фізичний канал (або радіоканал) розподіляється між багатьма користувачами. Це ясно видно на рисунку 1.9 МОЕП А приймає мультиплексований потік у свої вхідні регістри пам'яті і запам'ятовує елемент передавання в позиції буфера 6. Незабаром після цього МОЕП передає ці дані у вихідний буфер із позицією 20. У визначений час КВМ з'єднає вихідний буфер МОЕП А с вхідним буфером МОЕП Z. У цьому випадку протягом тривалості елемента 20 перетворення з МОЕП А пересилаються до елемента 20 МОЕП Z. Після цього МОЕП Z пересилає 20-й елемент передавання з вхідного буфера в елемент вихідного буфера з номером 15, що забезпечує передавання даних. Подібним способом виконується комутація цифрових даних у цифрових комутаторах із розподіленням часу. Хоча це не показано на рисунку 1.9 механізм МОЕП/КВМ забезпечує двонаправлені передавання і використовує одні і ті ж тимчасові ділянки для перекриття в них даних, що йдуть у різних напрямках, забезпечуючи, таким чином, передавання в режимі повного дуплекса.

1.6 Пакетне передавання мови

У цьому розділі описується передавання аналогових сигналу – мови і зорових образів у потоках цифрових даних.

Подібно до передавання даних, передавання мови має такий же характер "спалахів" – звук межує з періодами мовчання. Тому пакети мови можуть розподіляти загальний канал, так само, як це відбувається з пакетами даних. Обґрунтуванням пакетного передавання мови є та ж можливість, що й у випадку пакетного передавання даних: спільне використання засобів комутації і передавання.

Концепція пакетного передавання мови зображена на рисунку 1.10.

Рисунок 1.10 – Система пакетного передавання мови

Пакетний мовний термінал (ПМТ) призначений для зв'язку аналогового телефонного пристрою і терміналу даних. В наш час проведені роботи, що сфокусовані на таких методах аналого-кодового перетворення сигналів, як дельта-модуляція з фронтами, що постійно змінюються, або кодування з лінійним передбаченням. Мовний процесор призначений для аналогових і цифрових перетворень мови. Протокольний процесор відповідає за керування підключеними модулями ПМТ. Він генерує й інтерпретує пакети, необхідні для установлення викликів або сеансу. Він також має буфери для вхідних і вихідних пакетів. Інтерфейсний мережевий процесор забезпечує інтерфейс пакетів із мережею.

Пакетне передавання мови має серйозні проблеми. По-перше, необхідно використовувати існуючі пакетні мережі для передавання мови, щоб уникнути створення додаткових мереж. Передавання даних вразливе до помилок, тому сучасні протоколи комутації пакетів, такі, як X.25, припускають необхідність виправлення всіх помилок. У той же час передавання мови толерантне до випадкових помилок. Наприклад, втрата 40-мілісекундного сегмента промови не вплине на розмову двох користувачів.

Однак існують складності. Наприклад, якщо мережа без з'єднання підтримує пакетне передавання мови, випадкова втрата пакета, можливо, не спричинить ніякого шкідливого ефекту. Але, з іншого боку, втрата багатьох пакетів може змінити зміст повідомлення. Наприклад, розглянемо діалог із пакетним передаванням мови: " Так, зустрінемося в аеропорту Томська". Якщо пакет, що передає звук "Т" у слові "Томськ", загубиться, тоді утворитися слово " Омськ", а це зовсім інше місто. Тому зустріч не відбудеться.

Інша проблема пов'язана із затримками в передаванні пакетів через проміжні вузли мережі. Це призводить до затримок їхнього прибуття до приймачів. У пакетних мережах даних пакети враховують розходження в затримках, особливо якщо вони проходять через мережу, неорієнтовану на сеанси. Відтворення мови вимагає гарантованого рівня реконструкції пакетів і гарантії видачі мови на приймачі. Оскільки пакети прибувають у різні моменти часу, то вони повинні бути відстрочені і збережені в буферах приймальної сторони для того, щоб забезпечити складання будь-яких пізніше доставлених пакетів. Однак може бути досягнутий стан, коли пакети пізно прибулі, не прибули або блукають. Такі пакети повинні бути попросту усунуті, а в результаті користувач одержить неповну реконструкцію повідомлення. Внаслідок цього можуть виникнути розриви мови при істотних затримках.

Один із підходів у вирішенні проблем затримки оснований на аналізі мережі і наступному визначенні цільового виходу за оцінкою

доставки більшої частини пакетів. Після досягнення деякого граничного значення пакети надходять на вихід.

Третя проблема пов'язана з вибором розмірів пакетів. Для зниження затримок і зменшення втрат пакетів бажано, щоб пакети були мінімальної довжини. Короткі пакети дають набагато швидше проходження, ніж довгі. Однак довгі пакети забезпечують краще використання каналу, оскільки в коротких пакетах міститься більше інформації, непотрібної користувачу – міток пакетів, полів управління. Оптимальний розмір пакета повинен врахувати час відповіді, пропускну спроможність мережі, а також ефекти запізнювання і втрати пакетів.

2 Мережі загального призначення та можливості мережевих середовищ

Із проникненням комп`ютерів в ділову галузь і в побут існує необхідність з'єднання цих пристроїв для сумісного використання програмних засобів, даних і ресурсів обробки. В даному розділі достатньо детально обговорюється використання мереж загального призначення та найбільш розповсюджених мережевих середовищ. Неможливо, звичайно, розглянути всі доступні системи. Отже, вибрані приклади тільки ілюструють велику кількість різноманітних, часто протилежних можливостей.

2.1 Мережі загального призначення

2.1.1 TELENET

TELENET є однією з перших мереж загального призначення в Сполучених Штатах Америки. Вона також була першою мережею в США на основі комутації пакетів. Telenet пропонує послуги всім 50 штатам і федеральному округу Колумбія. Окрім цього вона забезпечує зв'язки більш ніж в 40 інших держав і підлеглих територій. Цей широкий географічний обсяг є привабливим для ділових людей, які здійснюють свої операції в США і за кордоном.

Telenet перетворює поток даних користувача в пакети, які передаються по мережі. Пакети можуть містити не більше 1024 біт. Доступ до основи мережі Telenet забезпечується завдяки кільком можливостям. Можливо користувачу знадобиться порт окремого каналу на центральному комутаторі мережі Telenet. Інша можливість – засіб відокремленого доступу, він забезпечує інтерфейс мережі X.25. Цю можливість також

можна використовувати через дублюючий набирач номера у випадку якщо засіб відокремленого доступу вийде із ладу.

Окрім відокремлених каналів в Telenet, середовище також підтримує обслуговування звичайних телефонів загального призначення з набором номера. Telenet має доступ через місцеві станції посередництвом набору номера для більше ніж 95% службових телефонів в США. Вартість використання мережі основана на класифікації міст: клас А та клас В. Міста, віднесені до класу А, мають високу інтенсивність і великі об'єми даних, що передаються. Міста з відносно малими об'ємами даних, що передаються, відносяться до класу В.

Абоненти можуть встановити віртуальні з'єднання з іншими користувачами, які підключені до мерсжі Telenet. Telenet також забезпечує засіб, подібний до засобу замкнутих груп користувачів в мережах X.25 Ця можливість дозволяє абонентам встановлювати зв'язки тільки з необхідними станціями.

Мережа Telenet також забезпечує функції, подібні складанню-розбиранню пакетів протоколу X.25. Різні станції абонентів з різними протоколами можуть взаємодіяти між собою в режимі віртуального термінала мережі Telenet. Цей режим узгоджує відмінності терміналів в наборах символів, таймерних приладів і форматів.

Як і в випадках багатьох інших пакетних мереж, Telenet пропонує спеціальні засоби. Наприклад, служба "гарячої лінії" дозволяє користувачу взаємодіяти між двома портами саме в той період часу, коли один із портів діє зі швидкістю до 12 кбіт/с.

Також є можливість для користувача знизити витрати за рахунок використання мережі в нічний час, вихідні дні і під час зниженого навантаження в мережі. Telenet пропонує електронну почту Telemail. Користувач також може мати в себе обладнання доступу до мережі Telenet. Це обладнання називається процесором мережі Telenet, воно встановлюється та обслуговується фірмою Telenet-System. Процесор Telenet пропонується в декількох версіях.

Додатковий сервіс, який надається цією мережею:

- режим повторення по відокремленій лінії доступу;
- отримання ідентифікатора лінії, порти загального доступу;
- деталізований звіт з'єднань:

2.1.2 TYMNET

TYMNET є іншою мережею загального призначення, яка пропонує користувачу багато видів послуг. TYMNET використовує метод комутації пакетів з широким діапазоном функцій складання-розбирання пакетів для користувачів мережі. Можна використовувати TYMNET для передавання

повідомлень як на низьких, так і на високих швидкостях. TYMNET доступна через набірні лінії загального призначення, приватні канали або прямим з'єднанням на концентратори TYMNET, які знаходяться у абонентів.

TYMNET пропонує декілька видів послуг термінального інтерфейсу.

1. Асинхронні інтерфейси – цей засіб забезпечує додаткові 5 режимів:

а) режим забезпечує локальні порти набірних ліній загального призначення. Ці порти підтримують термінали IBM типу 2741. Такі порти знаходяться більше ніж в 400 місцях в США;

б) порт WATS загального призначення є іншим асинхронним режимом. В цьому режимі користувач звільняється від оплати, а весь рахунок за час з'єднання поступає на головний прилад;

в) третій вид асинхронних послуг – відокремлені порти для набірних ліній. TYMNET надає відокремлений порт через мережу з набором загального призначення;

г) четверта асинхронна послуга забезпечує відокремлені орендовані канали до вузла TYMNET;

д) п'ятий вид послуг надає відокремлений процесор, розташований на місці.

2. Мережа TYMNET забезпечує платну асинхронну підтримку для засобів користувача. Абоненти підключені до вузлу TYMNET через відокремленні орендовані канали.

3. Бісинхронне з'єднання. Цей режим використовується для інших відокремлених орендованих каналів або відокремлених синхронних портів з набором.

4. TYMNET також підтримує прямий зв'язок в X.25 через відокремлені орендовані канали і відокремлені синхронні порти.

5. Через відокремлені орендовані канали забезпечується зв'язок SDLC.

6. Відокремлені орендовані канали або відокремлені синхронні порти також мають доступ для RJE/HASP. Це підтримує деяких представників із сімейства терміналів IBM, які використовують бісинхронні протоколи на двоточковій основі.

TYMNET також забезпечує такі функції підтримки інтерфейсів для центральних (host) ЕОМ:

а) асинхронні на відокремлених каналах;

б) платні асинхронні на відокремлених каналах,

в) 3270 бісинхронних центральних ЕОМ на відокремлених орендованих каналах;

г) інтерфейси X.25;

д) центральна ЕОМ, орієнтована на SDLC;

е) інтерфейс RJE/HASP центральної ЕОМ.

Подібно іншим мережевим носіям, TYMNET забезпечує електронну почту, яка має назву Tyme-Gram.

TYMNET має засоби доступу до міжнародних мереж. Наприклад, через канадську мережу DATAPACK на основі X.25 мережа TYMNET пов'язана більше ніж з 60 містами Канади. Зв'язок між США та Далеким Сходом здійснюється через службу доступу до міжнародних баз даних. Більше 40 інших країн можна підключити через TYMNET за згодою між TYMNET та відомствами зв'язку в інших країнах.

2.1.3 AUTONET

Іншою мережею комутації пакетів загального призначення є AUTONET. Подібно іншим мережам загального призначення, AUTONET зв'язує більше 120 міст, забезпечує доступ в мережу без додаткової оплати для більше ніж 270 локальних розміщень. Ця мережа забезпечує інтерфейси до інших мереж загального призначення в США та до мереж більш ніж в 30 інших держав. AUTONET забезпечує послуги, подібні послугам в раніше розглянутих мережах: засоби набору місцевого номера, послуги in-Wats, приватні зв'язки з відокремленими портами, адресні зв'язки з портами, основні інтерфейси з асинхронними та синхронними приладами. Інтерфейс X.25 також підтримується AUTONET. Підтримуються різноманітні швидкості передавання в залежності від конкретного виду послуг. Мережа AUTONET також забезпечує засіб електронної пошти під назвою Automail. Цей засіб створює електронні поштові скриньки в усій мережі AUTONET. Засіб має доступ кожен день тижня і кожен час протягом дня. Електронна пошта забезпечує спеціальну обробку, призначення пріоритетів, розмноження повідомлень багатьом адресатам, зберсження отриманих даних в поштових скриньках. Мережа також забезпечує для деяких станцій сервіс для випуску електронних бюлетнів, а також засоби передавання великих об'ємів даних. Вона дозволяє проводити редагування електронних повідомлень, як тільки вони введені в систему. Засіб Automail взаємодіє з іншими додатками, такими, як TELEX та TWX.

2.1.4 GRAPHNET

Мережа фірми Graphnet Incorporated має деякі відмінності від мереж загального призначення, описаних раніше. Абоненти GRAPHNET забезпечуються зв'язком факсимільних зразків, такими, як графічна та текстова інформація. Користувач може підключитись до сервісу Graphnet

через набірні телефонні лінії, приватні канали, TELEX або TWX. GRAPHNET передає факсимільні дані до великої кількості міст США або до іншого кінцевого пункту призначення через пряме обслуговування відправника повідомлення. Документ також може бути відправлений поштою першого класу в місто, де знаходиться кінцевий користувач. Мережа GRAPHNET пропонує декілька зручних можливостей вибору, таких, як виправлення повідомлень збереження даних для наступних корекцій, забезпечення статусу доставки звітів кінцевим користувачам, засоби складання-розбирання пакетів, такі, як зв'язок між приладами, які працюють на різних швидкостях. Доступ до мережі можливий через TELEX/TWX, телефонну систему та приватні канали. Після передавання повідомлення доставляються поштою, телефоном, факсимільним обладнанням або через термінали.

2.1.5 PACNET

PACNET – це тихоокеанська мережева корпорація. Ця мережа пропонує набір зв'язків для більше ніж 30 регіонів в континентальній частині США, а також в Канаді, на о. Гуам, на Алясці та Гавайських о-вах. Абоненти підключаються до мережі PACNET через відокремлені орендовані канали. Подібно іншим мережевим носіям, PACNET пропонує режими або повсякчасне користування (7-денне 24-часове обслуговування), або використання протягом робочого часу (з 8.00 до 17.30 з понеділка по п'ятницю). Система використовує багато методів роботи з асинхронними, синхронними та мультиплексними приладами, а також знаходження помилок та підвищення захищеності від помилок.

2.2 Можливості мережевих середовищ

2.2.1 ISACOM

ISACOM є мережею з додатковими послугами, яка забезпечує велику різноманітність видів сервісу як для аналогового, так і для цифрового передавання. Середовище забезпечує два типи послуг для аналогових сигналів. Послуги типу А1 призначені для зв'язків комутуючих звукових каналів та цифроаналогових зв'язків. Послуги типу А3 є іншим видом обслуговування при засобах автоматичної комутації. Крім того, ISACOMM забезпечує цифрові зв'язки для синхронних приладів. ISACOMM забезпечує багатоточкові зв'язки, а також деякі функції підвищеної цінності, пов'язані з винайденням та виправленням помилок (наприклад, попередження помилок, заглушення ехо-сигналу).

Мережа ISACOMM також забезпечує телеконференції, розповсюдження факсміле, мультиплексування та супутниковий зв'язок. Користувач має декілька способів доступу до цих послуг: через мережу з адресованим набором загального призначення, через відокремлені орендовані канали, через персональні мікрохвильові переговорні прилади.

2.2.2 Канали взаємообміну

Можливо ніде більше ефект неузгодженності та конкуренції не є настільки помітним для суспільства, як в адресованих та приватних каналах взаємообміну.

Нижче наведено деякі з широкорозповсюджених послуг, які надаються цими каналами:

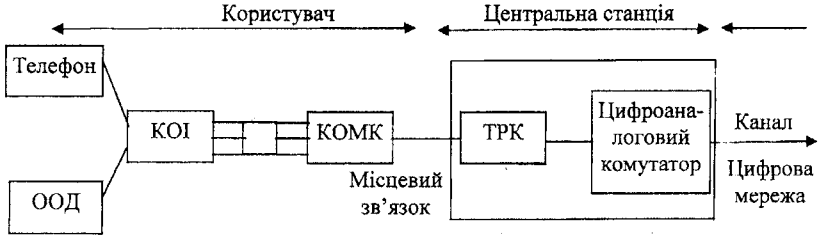
- *Послуги для обміну текстами* (TWX). Передавання тексту в коді ASCII з 4-рядкових термінальних клавіатур; обладнання доступне тільки для приймача (RU), клавіатури приймання-передавання(KSR), автоматичного приймання-передавання (ASR) за допомогою стрічок.
- *Infocom.* Користувачі можуть створити приватну мережу, використовуючи термінали TWX або Telex. Все передавання має приватний характер, користувачі створюють замкнуту групу при підтримці в режимі півдуплекса або дуплекса.
- *Infomaster.* Цей вид послуг також має назву комп'ютерних послуг для обміну текстами (TCS). Ця послуга являє собою запам'ятовування та наступне відправлення повідомлень, які доступні користувачам на засобах TWX, Infocom та Telex.
- *Datagram.* Засіб Datagram дозволяє користувачу направляти повідомлення для доставки до специфічних засобів TWX, Infocom.

2.3 Цифровий засіб комутації ланцюгів(ЦЗКЛ)

Іншим видом мережевих середовищ є повністю цифровий сервіс, який має назву цифрового засобу комутації ланцюгів (ЦЗКЛ) (рисунок 2.1).

Вагомою та унікальною властивістю цього виду обслуговування є те, що дозволяється користувачу підключатись до тих же двопроводових місцевих ліній, до яких підключені звичайні телефони. ЦЗКЛ, звичайно, потребує установлення в місцях використання додаткового обладнання. Місцеві лінії, а також апаратура центрального комутатора також потребують незначних модифікацій.

ЦЗКЛ не використовують для повного заміщення звичайного виду обслуговування, відомого як Dataphone Digital Service (DDS).



КОІ: кінцеве обладнання інтерфейсу; КОМК: кінцеве обладнання мережевого каналу; ТРК: термінал ручної комутації; ООД: окреме обладнання даних.

Рисунок 2.1 – Цифровий засіб комутації ланцюгів

Новий засіб є альтернативним для більш простих та менш об'ємних використань. Тобто, ЦЗКЛ заповнює розрив в потребах між локальним передаванням даних (ЛПД, розглянута нижче) та DDS.

З боку абонента є два додаткових прилади: кінцеве обладнання інтерфейсу (КОІ), зв'язане з телефоном або пристроєм зв`язку. На КОІ підтримується стандартний інтерфейс, наприклад RS-232-c, або ж МККТТ V.35.

Інший прилад є кінцевим обладнанням мережевого каналу (КОМК), який взаємодіє з мережею. Розглянуті два прилади з'єднані чотирьма витими парами. Одна пара забезпечує передавання даних, інша забезпечує прийняття, третя пара передає аналогові мовні канали і, нарешті, четверта пара забезпечує передавання керуючих сигналів для переключення передавання даних або мови. Як раніше встановлено, в звичайній місцевій телефонній мережі повинні бути зроблені незначні зміни. Наприклад, певні елементи обладнання (навантажувальні індуктивності) та надлишкові зв'язки повинні бути видалені. В деяких випадках можуть знадобитись розширювачі рівня. Розширювачі рівня підсилюють аналогові сигнали та відновлюють цифрові. Ці невеликі зміни не займають увагу кінцевого користувача, оскільки вони повністю виконуються поставником.

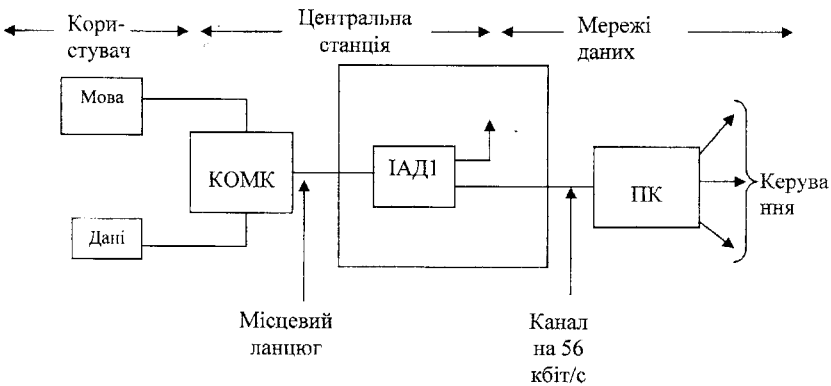
Однією з цікавих властивостей цього виду обслуговування є використання мультиплексування з тимчасовим стисненням (МТС). Передавання, яке використовує МТС, є півдуплексним, проте швидкість побітового передання вища, ніж встановлена швидкість сигналу. При такому підході канал *дуже швидко* переключається з одного напрямку в інший, що створює враження дуплексного передавання. Іншими словами, половину всього часу передавання відбувається на подвоєній швидкості.

2.4 Локальне передавання даних (ЛПД)

Локальне передавання даних – це метод, який дозволяє водночас передавати мову та дані по одному й тому ж телефонному каналу. Для цього виду послуг підходить звичайна телефонна мережа. Система, яка використовує цей метод, це комбінація засобів відеотексту (наприклад, для таких доданків, як електронна пошта або банкові операції) та звичайних засобів передавання мови.

Система ЛПД показана на рисунку 2.2. В місцезнаходженні абонента є рознім для підключення до стандартного телефону. КОМК модулює сигнали терміналу для передавання даних на несучій 4кГц, що нижче частоти несучої для передавання даних. Таким чином забезпечується передавання і мови, і даних водночас.

ЛПД пропонує дві основні форми доступу: з набором номера та власноруч. Прямий доступ забезпечується для передавання і голосу і даних до абонента водночас по двох проводах. Проводи підключені до місцевого мультиплексора даних, який виконує комбінування потоків мови та даних. Передавання мови виконується на стандартному комутаторі, а дані абонента з його терміналу відсилаються на пакетний комутатор. Мультиплексування виконується на КОМК.



КОМК: кінцеве обладнання мережевого каналу; ІАД: інтерфейс абонента даних; ПК: пакетний комутатор.

Рисунок 2.2 – Локальне передавання даних (ЛПД)

Ця технологія використовує дуплексне передавання даних. Привабливою особливістю є можливість використовувати вже існуючі місцеві телефонні мережі. Доступ з набором номера теж виконується на звичайних вже існуючих телефонних лініях. Технологія ЛПД попереджає набір номера абонентом під час передавання даних по його каналу.

Керування передаванням даних виконується за допомогою звичайних пакетних методів, а також за допомогою мережевих протоколів X.25, та лінійного протоколу LAPB. ЛПД створює одиничну ланку даних до центральної ЕОМ, через яку відбувається доступ до багатьох абонентів в даному регіоні. Це дозволяє центральній ЕОМ підтримувати до 511 активних терміналів користувачів на одній телефонній лінії DDS. Цей підхід виключає необхідність окремих портів та модемів для кожного термінала.

Як і інші засоби стандарту X.25, ЛПД використовують для підтримки ланцюгів віртуальних викликів або постійних віртуальних зв'язків в залежності від індивідуальних вимог користувача. ЛПД використовує стандартні розміри пакетів, визначених стандартом X.25, з максимальною довжиною пакетів користувача 255 байтів.

2.5 Пакетне обслуговування ACCUNET

Пакетне обслуговування ACCUNET (раніше мало назву базового обслуговування комутації пакетів(BPSS)) є службою, яка основана на використанні комутації пакетів в приватних каналах. Це обслуговування особливо ефективне для передавання даних великого об'єму і/або потоків з характерними "сплесками". ACCUNET забезпечує віртуальні виклики або зв'язки постійних віртуальних ланцюгів та підтримує як 128-байтові, так і 256-байтові пакети даних..

Іншим засобом, який викликав велику увагу, є адаптація до стандарту X.75, який дає можливість користувачам ACCUNET отримати доступ до інших мереж, орієнтованих на пакети. Це забезпечує користувачам ACCUNET доступ до мереж інших країн.

Широкодоступним засобом ACCUNET, є REDI-ACCSESS. Цей засіб забезпечує адресацію набором в мережах загального призначення та доступ у відокремлених каналах до пакетного обслуговування ACCUNET, а також підтримку багатьох протоколів. Засоби REDI-ACCESS мають такі переваги:

1.Термінальний доступ з набірною адресацією в асинхронному режимі до мереж загального призначення.

2. Знижка з оплати при великих об'ємах передавання в мережах з набором загального призначення.

3. Під`єднання комутуючих портів, виділених каналів, модемів до найближчого розміщення інтерфейсу REDI–ACCESS в пакетному середовищі.

Синхронний інтерфейс складається з інтерфейсу на основі стандарту X.25 (програмні засоби X.25 на обладнанні користувача). Асинхронні засоби до інтерфейсу X.25 використовують складання-розбирання пакетів на апаратурі користувача.

3 Мережі персональних комп`ютерів

Сьогодні ізольований комп'ютер має дуже обмежену функціональність. Ізольована система не має необхідної в наш час гнучкості і масштабованості. Можливість обміну даними між розсередженими системами відкрила нові аспекти для побудови розподілених ресурсів, їхнього адміністрування і наповнення. За допомогою цього виконується розподілене збереження інформації (мережеві файлові системи, файлові архіви, інформаційні системи з віддаленим доступом), і мережеві обчислювальні завдання. UNIX - одна з перших операційних систем, що забезпечила можливість роботи в мережі. І в цьому одна з причин її успіху і довготривалості.

Протоколи TCP/IP були розроблені, а потім пройшли довгий шлях удосконалення для забезпечення вимог, які висуває глобальна мережа Internet. Протоколи TCP/IP використовуються практично в будь-якім комунікаційному середовищі. У назві сімейства цих протоколів присутні імена двох протоколів - TCP і IP.

У 1969 році Агентство досліджень DAPRA Міністерства Оборони США поклало початок фінансування проекту для створення експериментальної мережі комутації пакетів. Ця мережа, названа APRANET, була побудована для забезпечення надійного зв'язку між комп'ютерним устаткуванням різних виробників. Із розвитком мережі були розроблені комунікаційні протоколи - набір правил і форматів даних, необхідних для встановлення зв'язку і передачі даних. Так з'явилося сімейство протоколів TCP/IP.

У 1983 році TCP/IP був стандартизований (MIL STD). У той же час агентство DAPRA почало фінансування проекту Каліфорнійського університету в Берклі для підтримки TCP/IP в операційній системі UNIX. TCP/IP - це набір протоколів, що використовуються для зв'язку комп'ютерних мереж і маршрутизації руху інформації між великою кількістю різних комп'ютерів. "TCP" означає "Протокол контролю передачі", а "IP" означає "Протокол міжмережевої взаємодії". Протоколи стандартизовані окремими форматами, обробкою помилок, передаванням повідомлень і стандартами зв'язку. Комп'ютерні системи, що

використовують TCP/IP, можуть використовувати єдині правила взаємодії між собою. Це дозволяє їм передавати повідомлення безпомилково до потрібних користувачів, не зважаючи на велику відмінність аппаратури і програмного забезпечення різних машин. Багато великих мереж були створені на основі цих протоколів, зокрема DARPA мережа. Різноманітні університети, установи і комп'ютерні фірми зв'язані в глобальну мережу, яка використовує протоколи TCP/IP.

Мільйони індивідуальних машин приєднані до глобальної мережі. Будь-яка машина глобальної мережі може взаємодіяти з будь-якою іншою. Персональні комп`ютери в глобальній мережі мають назву "hosts" чи "nodes". TCP/IP забезпечує базу для багатьох корисних засобів, включаючи електронну пошту, передавання файлів і дистанційну реєстрацію. Електронна пошта призначена для передавання коротких текстових файлів. Прикладні програми для передавання файлів можуть передавати дуже великі файли, що містять програми і дані. Вони також можуть виконувати контрольні перевірки правильності передавання даних. Дистанційна реєстрація дозволяє користувачам одного комп'ютера зареєструватися на віддаленій машині і продовжувати інтерактивний сеанс зв'язку з цією машиною.

Протокол міжмережевої взаємодії (IP) визначає незв'язану пакетну доставку. Ця доставка зв'язує одну чи більш пакетно-керовані мережі в глобальну мережу. Термін "незв'язана" означає, що машини не зв'язані між собою безпосереднім фізичним середовищем. Тут індивідуальні пакети даних (дейтаграми) маршрутизуються через різні машини глобальної мережі до локальної мережі-одержувача і до машини, що повинна прийняти інформацію. У такий спосіб повідомлення розбиваються на ряд дейтаграм, які посилаються окремо. Незв'язана пакетна доставка сама по собі ненадійна. Окремі дейтаграми можуть бути отримані чи не отримані і з великою імовірністю можуть бути отримані не в тім порядку, у якому вони були послані. TCP збільшує надійність. Дейтаграма складається із заголовка, інформації й області даних. Заголовок використовується для маршрутизації і процесу дейтаграми. Дейтаграма може бути розбита на малі частини в залежності від фізичних можливостей локальної мережі, по якій вона передається. Коли шлюз посилає дейтаграму до локальної мережі, яка не може розмістити дейтаграму як єдиний пакет, вона повинна бути розбита на частини, що малі для передавання по цій мережі. Заголовки фрагментів дейтаграми містять інформацію, необхідну для збору фрагментів у закінчену дейтаграму. Фрагменти необов'язково прибувають один по одному як вони були послані. Програмний модуль IP протоколу, що виконується на машині-приймачі, повиннен збирати фрагменти у вихідну дейтаграму. Якщо які-небудь фрагменти загублені, повна дейтаграма скасовується.

Протокол контролю передавання даних (TCP) працює разом з IP

для забезпечення надійної доставки. Він пропонує засоби забезпечення надійності того, що різні дейтаграми, які складають повідомлення, збираються в правильному порядку на приймальній машині і що деякі пропущені дейтаграми будуть послані знову, поки вони не будуть прийняті правильно.

Перша мета TCP - це забезпечення надійності, безпеки і сервісу віртуального контуру зв'язку між парами зв'язаних процесів на рівні ненадійних внутрішньомережевих пакетів. На цьому рівні можуть виникнути втрати, знищення, дублювання, чи втрата упорядкованості пакетів. TCP забезпечує лише загальні аспекти надійності. Надійне отримання дейтаграми виконується різними шляхами. Якщо дейтаграма послана через локальну мережу до віддаленого серверу, то проміжні мережі не гарантують доставку. Крім того, машина-передавач не може знати маршрут передавання дейтаграми. Надійність шляху "джерело-приймач" забезпечує протокол TCP. Надійність забезпечується за допомогою контрольної суми (коди виявлення помилок) послідовних чисел у заголовку TCP, прямого підтвердження одержання даних і повторного передавання непідтверджених даних.

3.1 Ієрархія протоколів TCP/IP

Протоколи TCP/IP широко застосовуються в усьому світі для об'єднання комп'ютерів у мережу Internet. Архітектура протоколів TCP/IP призначена для загальної мережі. Ця мережа складається із з'єднаних один з одним шлюзами окремих різнорідних комп'ютерних підмереж. Ієрархію керування в TCP/IP-мережах звичайно подають у вигляді п`ятирівневої моделі.

Нижній рівень hardware описує те чи інше середовище передавання даних.

На рівні network interface (мережевий інтерфейс) знаходиться апаратно-залежне програмне забезпечення, що реалізує поширення інформації на різних відрізках середовища передавання даних. Відзначимо, що TCP/IP орієнтований на незалежність від середовища передавання. Тому ніякі обмеження на програмне забезпечення цих двох рівнів не накладаються. Цей рівень може бути поданий і як модемна двоточкова ланка, і як складна багатовузлова комунікаційна мережа X.25 чи Frame Relay.

Рівень internet (міжмережевий) поданий протоколом IP. Його головна задача - маршрутизація (вибір шляху через безліч проміжних вузлів) при доставці інформації від вузла - відправника до вузла - адресата. Друга важлива задача протоколу IP - приховання апаратно-програмних особливостей середовища передавання даних і надання вищим рівням

єдиного інтерфейсу для доставки інформації. Канальна незалежність, що досягається при цьому, забезпечує багатоплатформну можливість застосування додатків, що працюють над TCP/IP.

Протокол IP не забезпечує транспортну службу в тому смислі, що не гарантує доставку пакетів, збереження порядку і цілісності потоку пакетів. Цей пропротокол не розрізняє логічні об'єкти (процеси), що породжують потік інформації. Це задачі інших протоколів - TCP/IP і UDP, що відносяться до наступного transport(транспортного) рівня. TCP і UDP реалізують різні режими доставки даних. TCP - протокол зі встановленням з'єднання. Це означає, що два вузли, що зв'язуються за допомогою цього протоколу, "домовляються" про те, що будуть обмінюватися потоком даних, і приймають деякі угоди про керування цим потоком. UDP (як і IP) є дейтаграмним протоколом. Таким протоколом, що кожний блок інформації обробляється і поширюється від вузла до вузла не як частина деякого потоку, а як незалежна одиниця інформації - дейтаграма.

На рівні application (прикладного потоку) - лежать прикладні задачі, такі як обмін файлами, повідомленнями електронної пошти, термінальний доступ до вилучених серверів.

3.2 IP адресація й імена об'єктів у мережі Internet

Кожному комп'ютеру в мережі Internet присвоюють IP-адресу, відповідно до якої IP-мережі він підключений. Старші біти чотирибайтової IP - адреси визначають номер IP - мережі. Частина IP-адреси, що залишилася - номер вузла. Існують 5 класів IP-адрес, що відрізняються кількістю біт у мережевому номері і номері вузла. Адресний простір мережі Internet може бути розділений на непересічні підпростори - "підмережі", з кожною з яких можна працювати як зі звичайною мережею TCP/IP. Єдина IP-мережа організації може будуватися як об'єднання підмереж. Стандарти TCP/IP визначають структуру IP - адрес.

Для IP-адрес класу B перші два байти є номером мережі, інша частина може використовуватися як завгодно. Стандарти TCP/IP визначають кількість байт, що задають номер мережі. Зручніше звертатися до комп'ютерів не за їх чисельними адресами, а за іменами (host name). Список цих імен зберігається в спеціальній базі даних Domian Name System (DNS). Наприклад, комп'ютеру, що має назву "comsys.ntu - pi.kiev.ua", у DNS відповідає IP-адреса 194.44.197.195. Коли ви хочете звернутися до ресурсів цього комп'ютера, ви вказуєте або його ім'я, або IP - адресу.

Через причину лавиноподібного росту інтересу до Internet TCP/IP

проникнув у настільні ПК. Однак для TCP/IP кожен окремий хост необхідно додатково конфігурувати. Ця задача значно спрощується завдяки появі великого числа мережних протоколів і систем, що дозволяють централізовано керувати TCP/IP.

Комп'ютер, що використовує TCP/IP, для нормальної роботи повинен знати деякі ключові компоненти - шлюзів і сервера імен. Для глобальної об'єднаної мережі важливі імена й адреси. На відмінність від популярних протоколів для ПК, TCP/IP оснащений схемами забезпечення унікальності IP-адрес і імен мережі. Процедура розпізнавання мережі за допомогою TCP/IP традиційно здійснюється за допомогою перетворення імен NetBios у IP - адреси у файлі LMHOSTS, що звичайно створюється вручну в кожнім вузлі. У загальному вигляді IP - адреса являє собою 4 розділених крапками десяткові числа, наприклад 128.66.12.1. Цей формат адреси називається крапкова десяткова нотація. IP-адреса ідентифікує мережу і конкретний комп'ютер у цій мережі. Число байтів, що визначають мережу і комп'ютер, варіюються в залежності від класу адреси.

3.3 Підмережі

Адреси хостів у мережі також повинні бути унікальними. Досягти цього можна 2 способами. По - перше, реєструвати адреси всіх хостів мережі централізовано. Цей спосіб найкраще використовувати при роботі в маленьких мережах, де мережевий адміністратор може працювати з усіма наявними адресами. Якщо ж ви працюєте у великій мережі, то рекомендується скористатися іншим способом. У цьому випадку локальному мережевому адміністратору надаються блоки адрес, і він потім визначає індивідуальну адресу хоста, вибираючи його з блока. Блок адрес може бути як набором адрес хоста, так і формально визначеною підмережею.

Як наведено вище, підмережі використовуються через адміністративні причини, але не тільки. IP-мережі – це мережі, що ідентифіковані таблицями шляхів, як і будь-яка інша дійсна мережа. Це значить, що вони можуть бути використані маршрутизаторами для фізичного розподілу мережі, щоб вирішувати технічні проблеми, такі як фіксування небажаного шляху в окремому сегменті. Тому область їхнього застосування досить широка. Щоб визначити меншу мережу усередині більшої, необхідно задати адресу підмережі. Адреса хоста визначається маскою підмережі (subnet mask). Маска підмережі - це бітовий шаблон, у якому бітам, що використовуються для адреси підмережі, присвоєні значення 1, а бітам, що використовуються для адреси хоста, - значення 0. Маски підмережі визначені тільки локально. Вони спеціально встановлені

при конфігурації кожного хоста і на віддалені хости не передаються. Маска підмережі застосовується тільки до адрес локальної мережі і нормально працює тільки в тому випадку, якщо використовується в кожній системі такої мережі. Коли хост отримує унікальну IP-адресу, він повинен одержати й унікальне ім'я. Вибір імені хоста - це актуальне питання. Для забезпечення унікальності імен хостів використовуються ті ж способи, що і для IP-адрес. Якщо хост звертається лише до хостів вашої локальної мережі, то досить зробити його ім'я унікальним тільки в межах даної мережі. Але якщо він обмінюється інформацією з усім світом, то його ім'я повинно бути унікальним в усьому світі. Гарантія унікальності - це справа служби реєстрації в InterNIC. Вона присвоює глобально унікальне ім'я домена кожному, хто правильно його буде вимагати. Цей процес дуже схожий на присвоєння номера мережі. Як і IP - адреси, імена хостів також розділяються на частини, що визначають і конкретний хост у ньому. Імена записуються від часткового до загального, у вигляді серії розподілених крапками слів і абревіатур. Вони починаються з імені комп'ютера, далі послідовно вказуються імена локальних доменів аж до імені домену, визначеного службою NIC, і закінчується ім'ям домену вищого рівня. Щоб пояснити цю структуру, розглянемо приклад. Допустимо, у домені nuts.com* є комп'ютер з ім'ям penaut. У домені nuts.com ви можете використовувати коротке ім'я penaut, але користувачі з іншої сторони земної кулі повинні звертатися до нього тільки по імені penaut.nuts.com. Унікальність імені nuts.com гарантує служба InterNIC, а унікальність імені penaut усередині nuts.com - адміністратор локального домена. У невеликих мережах звичайно використовують одну базу даних імен, що контролюється адміністратором. Домени великих мереж підрозділяються на піддомени, а відповідальність за визначення імен усередині піддомену покладається на адміністратора піддомену. Як тільки NIC призначить організації ім'я домена, ця організація одержить право утворювати піддомени без відома NIC. Усередині домену nuts.com можна організувати піддомен sales.nuts.com і покласти відповідальність за цей піддомен на будь-яку особу. Ця особа буде присвоювати імена хостам у своєму піддомені, одне з яких може бути peanut. Хост із таким ім'ям не буде конфліктувати з описаним вище хостом peanut, оскільки його повне ім'я peanut.sales.nuts.com. Кожен домен і піддомен обслуговується сервером імен (name server). Сервер імен бере ім'я хоста і перетворює його в IP-адресу для використання програмами TCP/IP. Якщо мережа з'єднана з Internet, необхідно застосовувати службу DNS.

Якщо система працює в невеликій ізольованій мережі, IP-адреси іменам хостів можна присвоювати за допомогою таблиці хостів. Таблиця хостів - це файл імен хостів і адрес, що знаходиться безпосередньо в ПК. Адміністратор мережі повинен постійно поновлювати цю таблицю.

3.4 Маршрутизація TCP/ IP

TCP/IP не може працювати без маршрутизації. Щоб з`єднатися з іншим комп`ютером мережі, окремий комп'ютер повинен знати правильний шлях до цього комп`ютера. Ці шляхи визначаються маршрутами, визначеними в таблиці місць призначення, для досягнення яких використовуються шлюзи. Для розміщення маршрутів у цю таблицю застосовуються 2 методи: статистична маршрутизація і динамічна. Першу маршрутизацію виконує адміністратор мережі, а динамічну - сама система через протоколи маршрутизації. У персональних комп`ютерах найчастіше використовують статистичну маршрутизацію. Ця маршрутизація використовує один статистичний маршрут за замовчуванням (default route), що вказує на маршрутизатор, який переправляє всі дані для комп`ютера. Багато реалізацій TCP/IP для ПК дозволяють ввести тільки один статистичний маршрут. Системний адміністратор UNIX може запустити протокол маршрутизації і дозволити маршрутизатору створити таблицю маршрутів на своїй машині. Конфігурація ПК може бути різною. ПК дозволяє ввести тільки один маршрут, навіть якщо їх насправді два. Якщо ж дані необхідно передати через інший маршрутизатор, це буде виконано за допомогою протоколу ICMP. У цьому випадку вибирається за замовчуванням шлюз, що використовується найчастіше, і він буде сам формувати маршрут, тобто при необхідності пересилати дані по іншому маршруті. У цьому випадку за замовчуванням варто задавати той шлюз, що використовується найчастіше, а не той, через який проходить більше всього маршрутів. Різні мережі, що складають глобальну мережу, зв'язані за допомогою машинних шлюзів. Шлюз - це машина, що з'єднана з двома чи більшою кількістю мереж. Це дозволяє прокласти маршрут для дейтаграми з однієї мережі в іншу. Шлюзи маршрутизують дейтаграми, ґрунтуючись на мережі-приймачі, а не на індивідуальній машині даної мережі. Це спрощує схеми маршрутів. Шлюзи розподіляють, яка наступна мережа буде одержувачем даної дейтаграми. Якщо машина-одержувач даної дейтаграми знаходиться в тій же мережі, то дейтаграма може бути послана прямо в цю машину. У протилежному випадку вона передається від шлюзу до шлюзу, поки не досягне мережі одержувача.

Ще один параметр конфігурації TCP/IP - це широкомовна адреса. Цим параметром називають адресу, що використовується системою одночасно для спілкування з усіма комп'ютерами локальної мережі. Стандартна широкомовна адреса – це IP-адреса, у якій всі біти номера хоста мають значення 1. Вибір програмного пакета TCP/IP аналогічний вибору мережевої карточки і оснований на аналізі співвідношення ефективність/вартість. Підтримка з боку постачальника і простота конфігурації також має велике значення, але на вибір програм впливають деякі додаткові фактори. Безкоштовні апаратні засоби не

існують, але безкоштовні пакети програм існують. Найбільша небезпека безкоштовних програм полягає в тім, що в потрібний момент для них може не виявитися необхідної технічної підтримки. Мережеве програмне забезпечення повинне відповідати вимогам - мати такі специфічні особливості, що відповідають вимогам служб мережі. У програмному забезпеченні TCP/IP для Windows при роботі з мережею використовуються ті ж команди, що й у програмному забезпеченні для UNIX. Структура драйверів і резидентних програм однакова для всіх реалізацій TCP/IP. Імена і функції модулів у кожній реалізації операційної системи різні, але основні засоби, за допомогою яких реалізується робота TCP/IP, залишаються незмінними. Це – переривання, драйвери пристроїв і резидентні програми. Резидентні програми (TSR) - це такі програми, що залишаються в пам'яті після того, як керування передається операційній системі. Резидентні програми TCP/IP звичайно запускаються під час завантаження операційної системи. Така програма спочатку запускає маленьку програму, що установлює вектор переривань, резервує необхідну пам'ять і повертає керування операційній системі, використовуючи спеціальну функцію 31h стандартного переривання DOS 21h. Ця спеціальна функція існує, оскільки резидентні програми - стандартна частина операційної системи і призначена для реалізації онових процесів в обмеженій формі. Велика перевага реалізації програми TCP/IP як резидентної програми – це швидкість. Програма увесь час знаходиться в пам'яті і може обробляти запити в реальному режимі часу. Недолік такої реалізації в тім, що резидентна програма зменшує обсяг доступної користувачу пам'яті. Через цю причину дуже важливо при установленні резидентного пакета TCP/IP у операційній системі використовувати менеджер пам'яті. TCP/IP працює в самих різних мережах тому, що цей протокол не залежить від фізичних особливостей конкретної мережі. Однак, хоча він і не вимагає конкретної мережі, йому все одно потрібна фізична мережа, щоб передавати інформацію з одного пункту в інший. Щоб запустити TCP/IP у операційній системі, необхідно проінсталювати драйвер для карти мережевого інтерфейсу. Фізичний пристрій спілкується з операційною системою і додатками за допомогою драйвера. Фізичне апаратне забезпечення мережі і його драйвер насправді не є частиною стека протоколу TCP/IP, але це необхідний компонент для роботи TCP/IP. Наявність драйверів пристроїв допомагає додавати нові пристрої, не змінюючи ядра операційної системи. Стандарт, визначений компанією Microsoft, називається Network Device Interface Specification (NDIS), а стандарт від Novell - Open Datalink Interface (ODI). Це несумісні стандарти. Більшість реалізацій TCP/IP підтримує як драйвери NDIS, так і драйвери ODI, і більшість карт мережевого інтерфейсу, постачається з драйверами обох типів. Дані стандарти дозволяють підтримувати на одному комп'ютері мультипротокольні стеки. Можливість організувати декілька

стеків протоколів на одному мережевому інтерфейсі є дуже важливою особливістю, тому що TCP/IP часто приходиться співіснувати з NetWare і іншими протоколами для ПК. Процес інсталяції TCP/IP у операційній системі складається з двох основних етапів: копіювання програми на твердий диск і конфігурування її для конкретної системи. Ці дві задачі часто реалізуються за допомогою спеціальних інсталяційних програм за назвою Install чи Setup. Звичайно програма інсталяції необхідна тільки для того, щоб розпакувати програму, яка знаходиться на дискетах у стиснутому вигляді. Для прикладу, конфігурування TCP/IP для операційної системи DOS являє собою складну задачу. На відміну від системи UNIX, конфігураційні команди в різних реалізаціях TCP/IP для DOS не схожі одна на одну. Планування і підготовка - найбільш важлива частина процесу конфігурування TCP/IP. Після запуску програми інсталяції TCP/IP ви отримаєте запрошення ввести основну інформацію про конфігурацію. Для того щоб TCP/IP почала працювати необхідні: унікальна IP - адреса, маска підмережі, правильно сконфігурована маршрутизація і принцип перетворення імен хостів у IP - адреси. Кожна програма реалізації TCP/IP має власний конфігураційний файл і власний синтаксис команд. Установлення деяких конфігураційних значень TCP/IP можна виконати за допомогою протоколу самонастроювання BOOTP. Цей протокол дозволяє клієнту одержати свою IP-адресу й інші параметри конфігурації з центрального сервера. ПК з операційною системою DOS запускали тільки клієнта служби імен, який називали ресолвер. Конфігурування ресолвера потребує тільки зазначеного за замовчуванням імені домена й адреси одного сервера імен. У процесі налагодження нової конфігурації використовується 2 типи команд: команди, що виводять поточну конфігурацію, і команди, що тестують зв'язки мережі. Класична тестова програма TCP/IP - це ping. Вона посилає луну - запит ICMP протоколу IP вилученої системи. Якщо система відповідає, то зв'язок працює.

3.5 Реалізація TCP/IP для Windows

Операційна система Windows продовжила життя DOS, переборовши два її великих недоліки - відсутність багатозадачності і підтримку обмеженого обсягу пам'яті. У Windows використовується система за назвою кооперативна багатозадачність, що при розподілі ресурсів покладається на правильну роботу програмних додатків. Усі пакети програм, що реалізовували TCP/IP для DOS, основані на резидентних програмах. Але методи конфігурації і синтаксис команд у кожного пакета свої. Існують 3 способи реалізації TCP/IP для Windows.

Перший спосіб - резидентні програми (TSR). Ці програми можуть

обслуговувати будь-яке вікно Windows, а сама резидентна програма може бути використана й у системі DOS, якщо Windows не запущена. Другий спосіб - бібліотеки динамічного зв'язку (DLL). Це бібліотека, що може бути викликана програмою, навіть якщо вона не була підключена до програми при компіляції. DLL потребують дуже мало пам'яті, і пам'ять, що вони використовують – це наявна і доступна для Windows пам'ять. Вони взагалі не використовують системну область пам'яті. Додатки TCP/IP, основані на DLL, мають потребу в обслуговуванні Windows. Третій спосіб – віртуальний драйвер (VxD -Virtual Device Driver). VxD - це новітній підхід до розробки TCP/IP для Windows. VxD являє собою драйвер пристрою, створений усередині віртуальної машини Windows. Як і драйвер DOS, VxD може бути створений, щоб обробляти переривання в реальному режимі часу. VxD не використовує область системної пам'яті DOS. Системи на основі TSR працюють і в DOS, і в Windows. Вони рекомендуються в тому випадку, якщо потрібна програма реалізації TCP/IP, що працює в обох середовищах. Реалізація TCP/IP з використанням DLL і у вигляді VxD працюють в лише в операційній системі Windows. Можливості VxD вищі, ніж DLL, оскільки вони можуть керуватися перериваннями. Тому технологія VxD – перспективний напрямок і для програмного забезпечення TCP/IP. Незалежно від методу реалізації системи, найбільш важливим фактором при виборі пакета TCP/IP для Windows є кількість додатків, що він підтримує, і якість цих додатків. Існує кілька пакетів TCP/IP для Windows, з яких можна вибрати найбільш прийнятний. Наприклад, пакет фірми Microsoft - це стек протоколів TCP/IP, але в ньому відсутні багато додатків, а пакет фірми SPRY - це повний набір додатків, але без стека протоколів. Winsock - це стандарт API, визначений для TCP/IP у системі Windows. Winsock являє собою реалізацію інтерфейсу в стилі Berkeley TCP/IP socket Microsoft Windows. Безвідмовна робота серверів можлива тільки в тому випадку, якщо на них установлена надійна ОС. Більшість адміністраторів локальних мереж раніше використовували ОС NetWare, а адміністратори мереж, що працюють на основі протоколу TCP/IP, - використовували UNIX.

Microsoft змінила цю ситуацію за допомогою створення ОС Windows NT – багатозадачної, багатофункціональної ОС. Її версія для одного користувача призначена для потужніх робочих станцій, а для серверів розроблена версія Windows NT Server. ОС NT із самого початку призначалася для роботи в мережах. Уже перші версії містили в собі програмне забезпечення, призначене для підтримки протоколів TCP/IP, і припускали побудову корпоративних мереж, що працюють на основі цих протоколів. BIOS - це базова система введення/виведення - стандартна частина DOS, що реалізує процедури, які використовуються додатками при запиті сервісу введення/виведення в системі DOS.

Протокол NetBios розширив її, доповнивши функціями введення-

виведення через мережу. Цей протокол не забезпечує передачу пакетів через маршрутизатори. Пакети передаються тільки в межах однієї фізичної мережі. Робота NetBios залежить від особливостей функціонування фізичного рівня мережі, на якому забезпечується широкомовна передача інформації.

Переваги і недоліки NetBios роблять його дуже зручним для використання в ізольованій локальній мережі і зовсім непридатним для великої виробничої мережі. Протокол NetBios можна запустити поверх безлічі інших мережевих протоколів, включаючи TCP/IP. Протокол NetBios over TCP/IP - повідомлення NetBios, що вбудовуються в дейтаграми TCP/IP. Він належить до числа стандартних. Додатки, що використовують NBT, можуть працювати тільки разом з тими додатками, що також використовують NBT. Вони не можуть взаємодіяти з додатками, що працюють поверх NBT. Кожна система, що очікує зв'язки через глобальну мережу TCP/IP, повинна запустити в себе NBT. Додатки NetBios не можуть взаємодіяти зі стандартними додатками TCP/IP.

Windows NT – це операційна система з вбудованою підтримкою мережі. Для того щоб працювати в глобальних мережах Microsoft запропонувала протокол NBT. При функціонуванні мережі під керуванням цього протоколу використовується файл LMHOSTS (щоб зменшити залежність від широкомовних передач) і параметр Scope ID (для фільтрації небажаної інформації при роботі у великих глобальних мережах). Крім цих двох спеціальних параметрів, при конфігурації TCP/IP для NT потрібно встановлення тих же опцій, що і для інших реалізацій TCP/IP. Система Windows NT поставляється з декількома додатками, робота яких залежить від інтерфейсу додатків NetBios. Ці додатки забезпечують виконання більшості функцій, що пропонуються стандартними додатками TCP/IP.

При конфігурації TCP/IP потрібна інформація про апаратне забезпечення, адреси і маршрутизацію, тому що цей протокол створювався в розрахунку на незалежність від будь-якого конкретного апаратного забезпечення. Інформація, що у деяких інших засобах мережі вбудована в апаратні компоненти, не може бути вбудована в TCP/IP. Цю інформацію повинен ввести той, хто відповідальний за конфігурацію. Протокол TCP/IP створювався для того, щоб забезпечити надійну роботу мережі, що складається з мейнфреймів і комп'ютерів, якими керують професійні адміністратори. Комп'ютери в мережах TCP/IP розглядаються як рівноправні системи (peers). Для TCP/IP усі комп`ютери - хости, а до всіх хостів висуваються однакові вимоги до конфігурації. Звичайно TCP/IP теж удосконалюється із розвитком ПК і програмного забезпечення локальних мереж.

У протоколі TCP/IP також з'явилися засоби, що полегшують задачу

конфігурації ПК - RARP, BOOTP. Протокол зворотного перекладу адрес RARP - це протокол, що перетворить фізичну адресу мережі в IP - адресу. Щоб створити сервер RARP, що може допомогти з початковою інсталяцією програмного пакета TCP/IP, вам потрібний незалежний від TCP/IP спосіб узнати адресу Ethernet. Іноді ця адреса позначена на самій платі Ethernet чи наведена в документації до неї. Протокол RARP - ефективний засіб, але він забезпечує отримання лише IP-адреси. Щоб робота сервера була більш ефективною, потрібно попереднє конфігурування програмного забезпечення TCP/IP для користувачів ПК. Не кожна реалізація TCP/IP може бути заздалегідь сконфігурована.

Протокол самозавантаження BOOTP визначається в RFC 951. Цей документ подає BOOTP як альтернативу RARP, тобто коли використовується BOOTP, потреба RARP відпадає. BOOTP забезпечує набагато більше конфігураційної інформації і постійно удосконалюється. Вихідна специфікація протоколу дозволяла постачальникам без проблем розширювати його можливості, що дуже сприяло його подальшому розвитку. Можна сконфігурувати сервер BOOTP так, щоб він мав справу зразу з багатьма клієнтами. Сервер легко конфігурується за допомогою усього лише двох діалогових вікон, але за цю легкість приходиться платити.

Динамічний протокол конфігурації хостів DHCP є представником останнього на сьогоднішній день покоління BOOTP. Він забезпечує клієнта повним набором значень конфігураційних параметрів TCP/IP. Також дозволяє виконувати автоматичний розподіл IP- адрес. Сервер DHCP забезпечує підтримку клієнта BOOTP.

3.6 Атаки TCP/IP і захист від них

Атаки на TCP/IP можна розділити на два види: пасивні й активні. Пасивні атаки ніяким чином не виявляють себе і не використовують взаємодію з іншими системами. Фактично усе полягає в спостереженні за доступними сесіями зв'язку. Так, атака цього типу, що має назву підслуховування, полягає у перехопленні потоку мережі і його аналізі. Для здійснення підслуховування необхідно мати доступ до машини, що розташована на шляху потоку мережі, чи до маршрутизатора PPP-сервера на базі UNIX. Якщо можливо одержати достатні права на цій машині, то за допомогою спеціального програмного забезпечення, буде можливо переглядати увесь трафік, що проходить через заданий інтерфейс.

Другий варіант - полягає в одержанні доступу до машини, що розташована в одному сегменті мережі із системою, яка має доступ до потоку мережі. Наприклад, у мережі "тонкий ethernet" карта мережі може

бути переведена в режим, у якому вона буде одержувати всі пакети, що циркулюють по мережі, а не тільки адресовані їй конкретно. У даному випадку не потрібно мати доступ до UNIX - досить мати ПК з Windows (часта ситуація в університетських мережах) . Оскільки TCP/IP-трафік, як правило, не шифрується при використанні відповідного інструментарію, можна перехоплювати TCP/IP-пакети, наприклад, telnet-сесії і отримувати з них імена користувачів і їхні паролі. Варто помітити, що даний тип атаки неможливо відстежити, не маючи доступ до системи, з якої відбувалась атака, оскільки потік мережі не змінюється.

Єдиний надійний захист від підслуховування - шифрування TCP/IP-потоку (наприклад, secure shell) чи використання одноразових паролів (наприклад, S/K EY). Інший варіант рішення – використання інтелектуальних ключів у результаті чого кожна машина одержує тільки той трафік, що адресований їй. Але підслуховування може бути і корисним. Так, даний метод активно використовується великою кількістю програм, що допомагають адміністраторам в аналізі роботи мережі (її завантаженості, працездатності і т.д.). Один з яскравих прикладів – загальновідома програма „tcpdump".

При активному типі атак відбувається взаємодія з одержувачем інформації, відправником і/чи проміжними системами. Ця взаємодія виконується шляхом модифікації і/чи фільтрації змісту TCP/IP-пакетів. Дані типи атак часто здаються технічно складними в реалізації, однак для кваліфікованого програміста не складно реалізувати відповідний інструментарій. Зараз такі програми стали доступні широким масам користувачів.

Активні атаки можна розділити на два типи. Перший тип полягає в перехопленні і модифікації інформаційного потоку мережі. В другому випадку протокол TCP/IP використовується для того, щоб привести систему-жертву в неробочий стан.

Маючи достатні привілеї в Unix (або використовуючи DOS, або Windows, що не мають системних обмежень користувачів), можна вручну формувати IP-пакети і передавати їх по мережі. Так поля чи заголовки пакета можуть бути сформовані довільним чином. Одержавши такий пакет, неможливо з'ясувати звідки реально він був отриманий, оскільки пакети не містять шляху їхнього проходження. Звичайно, при установленні зворотної адреси, що не збігається з поточною IP-адресою, ніколи не сформується відповідь на відісланий пакет. Однак, як ми побачимо, часто це не потрібно. Можливість формування довільних IP-пакетів є ключовим пунктом для здійснення активних атак.

Атака TCP sequence number була описана ще Робертом Моррісом (Robert T. Morris) у Weakness in the 4.2BSD Unix TCP/IP Software. Англомовний термін - IP spoofing. У даному випадку мета атаки - прикинутися іншою системою, якій, наприклад, "довіряє" система-жертва

(у випадку використання протоколу rlogin/rsh для безпарольного входу). Ця атака також використовується для інших цілей - наприклад, для посилання підроблених листів. Установлення TCP-з'єднання відбувається в три стадії (3- way handshake): клієнт вибирає і передає серверу порядковий номер (sequence number) назвемо його C-SYN), у відповідь на це сервер висилає клієнту пакет даних, що містить підтвердження (C-ACK) і власний порядковий номер сервера (S-SYN). Тепер уже клієнт повинен вислати підтвердження (S-ACK).

Після цього з'єднання вважається встановленим і починається обмін даними. При цьому кожний пакет має в заголовку поле для номера підтвердження і номер підтвердження. Дані числа збільшуються при обміні даними і дозволяють контролювати коректність передавання. Припустимо, що можливо передбачити, який порядковий номер серевера (S-SYN за схемою) буде висланий сервером. Це можливо зробити на основі знань про конкретну реалізацію TCP/IP. Наприклад, у 4.3BSD значення порядкового номера, що буде використано при установці наступного значення, щосекунди збільшується на 125000. Таким чином, пославши один пакет серверу, крекер одержить відповідь і зможе передбачити порядковий номер для наступного з'єднання. Якщо реалізація TCP/IP використовує спеціальний алгоритм для визначення порядкового номера, то він може бути з'ясований за допомогою посилання декількох десятків пакетів сервера й аналізу його відповідей. Отже, припустимо, що система А довіряє системі В так, що користувач системи В може виконати команду "rlogin A"_ і виявитися в А, не вводячи пароля. Припустимо, що хакер знаходиться в системі С. Система А виступає в ролі сервера, системи В і С - у ролі клієнтів. Перша задача - перевести систему В у стан, коли вона не зможе відповідати на запити мережі. Це може бути зроблено декількома способами, у найпростішому випадку потрібно просто дочекатися перезавантаження системи В. Декількох хвилин, протягом яких вона буде непрацездатна, повинне вистачити. Після цього хакер може спробувати прикинутися системою В, для того, що б одержати доступ до системи А (хоча б короткочасний). Хакер висилає кілька IP-пакетів, що ініціюють з'єднання, системі А, для з'ясування поточного стану порядкового номера сервера. Хакер висилає IP-пакет, у якому як зворотна адреса зазначена вже адреса системи В. Система А відповідає пакетом з sequence number, що направляється системі В. Однак система В ніколи не одержить його (вона виведена з ладу). Хакер на основі попереднього аналізу здогадується, який порядковий номер був висланий системі В. Він підтверджує "одержання" пакета від А і висилає від імені В пакет з передбачуваним S-ACK (зазначимо, що якщо системи розташовуються в одному сегменті, хакеру для з'ясування порядкового номера досить перехопити пакет, посланий системою А). Після цього, якщо порядковий номер сервера був угаданий правильно, з'єднання вважається

встановленим. Хакер може передавати черговий фальшивий IP-пакет, що буде вже містити дані. Наприклад, якщо атака була спрямована на rsh, пакет може містити команди створення файла .rhosts чи команди відправлення "/etc/passwd" на електронну пошту хакеру. В реальному житті не відбудеться спрацьовування всієї схеми. Можуть втратитися в мережі пакети, що посилає хакер. Для коректної обробки цих ситуацій програма повинна бути ускладнена.

Десинхронізація нульовими даними – інша атака. В цій атаці відбувається прослуховування сесії. У будь-який момент серверу посилається пакет з "нульовими" даними, тобто такими, які фактично будуть проігноровані на рівні прикладної програми (наприклад, для telnet це можуть бути дані типу IAC NOP IAC NOP IAC NOP...). Аналогічний пакет посилається клієнту. Очевидно, що після цього сесія переходить у десинхронізований стан. Одна з проблем полягає в тому, що будь-який пакет, посланий у момент, коли сесія знаходиться в десинхронізованому стані, викликає так звану ACK-бурю. Наприклад, пакет посланий сервером, і для клієнта він є неприйнятним, тому той відповідає ACK-пакетом. У відповідь на цей неприйнятний уже для сервера пакет знову одержує відповідь. І так до нескінченності. Сучасні мережі будуються за технологіями, коли допускається втрата окремих пакетів. Оскільки ACK-пакети не несуть даних, повторні передачі не відбуваються і "буря стихає". Як показали досвіди, чим сильніше ACK-буря, тим швидше вона "заспокоюється". Так, на 10MB ethernet це відбувається за частки секунди. На ненадійних з'єднаннях типу SLIP - ненабагато більше.

Є кілька шляхів протидії цій атаці. Наприклад, можна реалізувати TCP/IP-стек, що буде контролювати перехід у десинхронізований стан, і здійснювати обмін інформацією про порядковий номер підтвердження. Однак у даному випадку ми не застраховані від хакера, що змінює і ці значення. Тому більш надійним способом є аналіз завантаженості мережі, відстеження ACK-штормів. Це можна реалізувати за допомогою конкретних засобів контролю за мережею. Якщо не відбудиться підтримка десинхронізованого з'єднання і не стане фільтруватися виведення своїх команд це буде помічено користувачем. На жаль, переважна більшість користувачів просто відкривають нову сесію, не звертаючись до адміністратора. Стовідсотковий захист від даної атаки забезпечує, як завжди, шифрування TCP/IP-трафіка (на рівні додатків - secure shell) чи на рівні протоколу - IPsec). Це виключає можливість модифікації потоку мережі. Для захисту повідомлень електронної пошти може застосовуватися програма шифрування даних PGP.

Пасивне сканування, ще один тип атаки. Сканування часто застосовується для з'ясування, на яких TCP-портах працюють демони, що відповідають на запити з мережі. Звичайна програма-сканер послідовно відкриває з'єднання з різними портами. У випадку, коли з'єднання

встановлюється, програма скидає його, повідомляючи номер порту. Даний спосіб легко детектується за повідомленнями демонів, які фіксують миттєво перерване після установлення з'єднання, чи за допомогою використання спеціальних програм. Кращі з таких програм мають спроби виконувати відстеження спроб з'єднання з різними портами. Однак існує інший метод - пасивне сканування (англійський термін "passive scan"). При його використанні посилається TCP/IP SYN-пакет на всі порти підряд. Для TCP-портів, що приймають з'єднання ззовні, буде повернутий SYN/ACK-пакет, як запрошення продовжити з`єднання (3-way handshake). Інші повернуть RST-пакети. Проаналізувавши дану відповідь, можна швидко зрозуміти, на яких портах працюють програми. У відповідь на SYN/ACK-пакети він може також відповісти RST-пакетами, показуючи, що процес установлення з'єднання продовжений не буде. Цей метод не детектується попередніми способами, оскільки реальне TCP/IP-з'єднання не встановлюється. Однак, можна відслідкувати як різко зросла кількість сесій, що знаходяться в стані SYN_RECEIVED у відповідь на SYN/ACK. На жаль, при досить розумній поведінці хакера (наприклад, сканування з низькою швидкістю чи перевірка лише конкретних портів) детектувати пасивне сканування неможливо, оскільки воно нічим не відрізняється від звичайних спроб установити з'єднання. Як захист можна лише застосувати захистний екран (firewall – брандмауер) для усіх сервісів, доступ до яких не потрібний ззовні. У сфері комп'ютерних мереж брандмауер являє собою бар'єр, що захищає від фігуральної пожежі - спроби зловмисників вторгнутися в мережу для того, щоб скопіювати, чи змінити, стерти інформацію, або, щоб скористатися смугою пропускання, чи пам'яттю комп'ютерів мережі. Брандмауер встановлюється на границі мережі, і фільтрує усі вхідні і вихідні дані, пропускаючи тільки авторизовані пакети. Брандмауер є набором компонентів, набудованих таким чином, щоб реалізувати певну політику контролю зовнішнього доступу до вашої мережі. Звичайно брандмауери захищають внутрішню мережу компанії від вторгнень з Internet, однак вони можуть використовуватися і для захисту від нападів, наприклад, з корпоративної мережі, до якої підключена і ваша мережа. Як і у випадку реалізації будь-якого іншого механізму мережевого захисту, організація, що використовує конкретну політику безпеки, крім всього іншого, повинна визначити тип трафіка TCP/IP, що буде сприйматися брандмауером як авторизований. Наприклад, необхідно вирішити, чи буде обмежений доступ користувачів до певних служб на базі TCP/IP, і якщо буде, то до якого ступеня. Вироблення політики безпеки допоможе зрозуміти, які компоненти брандмауера вам необхідні і як їх сконфігурувати, щоб забезпечити задані обмеження доступу.

Сімейство протоколів TCP/IP широко застосовується в усьому світі для об'єднання комп'ютерів у мережу Internet. Єдина мережа Internet складається з безлічі мереж різної фізичної природи, від локальних мереж

типу Ethernet і Token Ring, до глобальних мереж типу NSFNET. Термін "TCP/IP" звичайно позначає усе, що пов'язано з протоколами TCP і IP. Він охоплює ціле сімейство протоколів, прикладні програми і навіть саму мережу. До складу сімейства входять протоколи UDP, ARP, ICMP, TELNET, FTP і багато інших. TCP/IP - це технологія міжмережевої взаємодії, технологія internet. Модуль IP створює єдину логічну мережу. Архітектура протоколів TCP/IP призначена для мережі, що складається із з'єднаних одна з одною шлюзами окремих різнорідних пакетних мереж, до яких підключаються різнорідні машини. Кожна з підмереж працює у відповідності зі своїми специфічними вимогами і має свою природу засобів зв'язку. Однак передбачається, що кожна підмережа може прийняти пакет інформації (дані з відповідним заголовком мережі) і доставити його на адресу цієї конкретної підмережі. Не потрібно, щоб підмережа гарантувала обов'язкову доставку пакетів і мала надійний наскрізний протокол. Таким чином, дві машини, підключені до одної підмережі, можуть обмінюватися пакетами. Коли необхідно передати пакет між машинами, підключеними до різних підмереж, то машина-відправник посилає пакет у відповідний шлюз. Звідти пакет направляється за певним маршрутом через систему шлюзів і підмереж, поки не досягне шлюзу, підключеного до тієї ж підмережі, що і машина-одержувач. Об'єднана мережа забезпечує дейтограмний сервіс. Проблема доставки пакетів у такій системі здійснюється шляхом реалізації у всіх вузлах і шлюзах міжмережевого протоколу IP. Міжмережевий рівень є власне кажучи базовим елементом у всій архітектурі протоколів, забезпечуючи можливість стандартизації протоколів верхніх рівнів. Протоколи TCP/IP пройшли довгий шлях удосконалень для забезпечення роботи глобальної мережі Internet. Протоколи TCP/IP використовуються практично в будь-якім комунікаційному середовищі, від локальних мереж на базі технології Ethernet , до надшвидкісних мереж, від телефонних каналів точка–точка до трансатлантичних ліній зв'язку з пропускною здатністю в сотні мегабіт у секунду. TCP/IP має чотирирівневу ієрархію. IP-адреси визначаються програмно і повинні бути глобально унікальними. IP-протокол використовує адреси для передачі даних між мережами і через рівні програмного забезпечення хоста. У мережах TCP/IP коректна адреса визначається адміністратором мережі, а не апаратними компонентами.

Протокол TCP/IP створювався для забезпечення надійної роботи мережі, що складається з міні-комп'ютерів, які знаходяться під керуванням професійних адміністраторів. Комп'ютери в мережі TCP/IP розглядаються як рівноправні системи. Це означає, що вони можуть виступати як сервери для одного додатка й одночасно працювати як клієнти для іншого. У протоколі TCP/IP не має розходжень між ПК і мейнфреймами. Для TCP/IP усі вони – хости, а до всіх хостів висуваються

однакові вимоги щодо конфігурації. TCP/IP теж удосконалюється із розвитком ПК. Він є більш складним мережевим середовищем, ніж традиційні локальні мережі ПК. Основними елементами мережі TCP/IP є базові служби віддаленого доступу до сервера, передавання файлів і електронної пошти.

Основні переваги TCP/IP:

- сукупність протоколів основана на відкритих стандартах, вільнодоступних і розроблених незалежно від конкретного устаткування чи операційної системи. Завдяки цьому TCP/IP є найбільш розповсюдженим засобом об'єднання різнорідного устаткування і програмного забезпечення;
- протоколи TCP/IP не залежать від конкретного устаткування фізичного рівня. Це дозволяє використовувати TCP/IP у фізичних мережах будь-якого типу: Ethernet, Token-ring, X.25, практично в будь-якім середовищі передачі даних.
- протоколи цього сімейства мають гнучку схему адресації, що дозволяє будь-якому пристрою однозначно адресувати інший пристрій мережі. Одна і та ж система адресації може використовуватися як у локальних, так і в територіально розподілених мережах, включаючи Internet;
- до сімейства TCP/IP входять стандартизовані протоколи високого рівня для підтримки прикладних послуг мережі, таких як передача файлів, вилучений термінальний доступ, обмін повідомленнями електронної пошти.

ЛІТЕРАТУРА

1 Ги К. Введение в локальные вычислительные сети. – М.: Радио и связь.- 1996. – 176 с.

2 Cole R. Computer Communications. – Macmillan. – London. – 1992. – 231pp.

3 IEE Computer Society Local Area Networcks Standards Committee.- Functional Requirements Document, Document, Version 5.2. – IEEE. – New York. – 1981. – 245 pp.

4 Дэвис Дюб Бербер Д. Сети связи для вычислительных машин. - М.: Мир. 1976. – 680 с.

5 Вычислительные сети и сетевые протоколы. Д. Дэвис и др. - М.: Мир, 1982 – 562 с.

6 Клейнрок Л. Теория массового обслуживания. – М.: Машиностроениеб 1979. – 356 с.

7 Вейцман К. распределенные системы мини- и микро-ЭВМ. Пер. с англ. под ред. Г.П. Васильева. – М.: Финансы и статистика 1983. – 232 с.

8 Автоматическая коммутация и телефония. Ч.И. Основи телефонии и автоматической коммутации. Под ред. Г.Б. Метельского. М.: - Связь, 1968.

9 И.М. Жданов, Е.И. Кучерявый. Построение городских телефонных сетей. – М.: Связь, 1972.

10 Г. Б. Давыдов, В. Н. Рогинский, А. Я. Толчан. Сети электоросвязи. – М.: Связь, 1977

11 ITU- T. Generic functional architecture of transport networks. Recommendation G.805. – Geneva. 1995.

12 Н.А. Соколов. Сети абонентского доступа. Принципы построения – Пермь, "Энтер - профи", 1999.

13 Теория сетей связи: Учебник для вузов связи. Рогинский В.Н., Харкевич А.Д., Шнепс М.А. и др. – М.: Радио и Связь, 1981.

14 Л.М. Невдяев, А.А. Смирнов. Персональная спутниковая связь. – М.: ЭКО-ТРЕНДЗ, 1998.

15 Н.А. Соколов. Цифровизация телефонных сетей. В книге Перспективные телекоммуникационные технологии. Потенциальные возможности // Под.ред. Л.Д. Реймана, Л.Е. Варакина. – М.: МАС, 2001.

16 R.A. Thomson. Telephone Switching Systems. – Artech House, Bostone, London, 2000.

17 S.R.Ali. Digital Switching Systems: Systems Reliability and Analysis. – McGraw – Hill, Inc, 1998.

18 А.И.Гусева "Технология межсетевых взаимодействий" – М.: Діалог-МИФИ. – 1997. – 272 с.

19 Мафтик С.М. Механізми захисту в мережах ЕОМ. - М.: Світ, 1993. - 256 с.

Навчальне видання

О. М. Бевз,
С. Г. Кривогубченко, А. Я. Кулик

СИСТЕМИ ТА МЕРЕЖІ ПЕРЕДАВАННЯ ДАНИХ

(Частина ІІІ)

Навчальний посібник

Оригінал-макет підготовлено Олександром Миколайовичем Бевзом

Редактор В.О. Дружиніна
Коректор З.В. Поліщук

Науково-методичний відділ ВНТУ
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ

Підписано до друку 28.05.2008 р. Гарнітура Times New Roman
Формат 29,7х42 ¼ Папір офсетний
Друк різографічний Ум. друк. арк. 3,7
Тираж 85 прим.
Зам. № 2008-074

Віддруковано в комп`ютерному інформаційно-видавничому центрі
Вінницького національного технічного університету
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ