Вступ

Сьогодні ізольований комп'ютер має дуже обмежену функціональність. Справа навіть не в тім, що користувачі позбавлені можливості доступу до великих інформаційних ресурсів, розташованим на вилучених системах. Ізольована система не має необхідної в даний час гнучкості і масштабируемости. Можливість обміну даними між розосередженими системами відкрила нові обрії для побудови розподілених ресурсів, їхнього адміністрування і наповнення, починаючи від розподіленого збереження інформації ( мережні файлові системи, файлові архіви, інформаційні системи з вилученим доступом ), і закінчуючи мережним обчислювальним середовищем . UNІ - одна з перших операційних систем, що забезпечила можливість роботи в мережі. І в цьому одна з причин її успіху і долгожительства.

Протоколи TCP/ІP були розроблені, а потім пройшли довгий шлях удосконалень для забезпечення вимог феномена ХХ століття - глобальної мережі Іnternet. Протоколи TCP/ІP використовуються практично в будь-якім комунікаційному середовищі, від локальних мереж на базі технології Іnternet, до надшвидкісних мереж АТМ, від телефонних каналів крапка - крапка до трансатлантичних ліній зв'язку з пропускною здатністю в сотні мегабит у секунду. У назві сімейства присутні імена двох протоколів - TCP і ІP. У 1969 році Агентство Досліджень DAPRA Міністерства Оборони США початок фінансування проекту по створенню експериментальної мережі комутації пакетів .Ця мережа, названа APRANET, була побудована для забезпечення надійного зв'язку між комп'ютерним устаткуванням різних виробників. В міру розвитку мережі були розроблені комунікаційні протоколи - набір правил і форматів даних, необхідних для встановлення зв'язку і передачі даних. Так з'явилося сімейство протоколів TCP/ІP. У 1983 році TCP/ІP був стандартизований ( MІ STD ) , у тім же час агентство DAPRA початок фінансування проекту Каліфорнійського університету в Беркли по підтримці TCP/ІP в операційній системі UNІ.

TCP/ІP - це установка протоколів, використовуваних для зв'язку комп'ютерних мереж і маршрутизації руху інформації між великою кількістю різних комп'ютерів. "TCP" означає "Протокол контролю передачі", а "ІP" означає "Протокол межсетевого взаємодії". Протоколи стандартизовані описаними припустимими форматами, обробкою помилок, передачею повідомлень і стандартами зв'язку. Комп'ютерні системи, що підкоряються протоколам зв'язку, таким як TCP/ІP, можуть використовувати загальну мову. Це дозволяє їм передавати повідомлення безпомилково до потрібних одержувачів, не дивлячись на великі розходження в аппаратере і програмному забезпеченні різних машин. Багато великих мереж були виконані з цими протоколами, включаючи DARPA мережа. Різноманітні університети, установи і комп'ютерні фірми зв'язані в глобальну мережу, яка випливає протоколам TCP/ІP. Тисячі індивідуальних машин приєднані до глобальної мережі. Будь-яка машина глобальної мережі може взаємодіяти з будь-який іншої (термін "глобальна мережа" звичайно використовується для назви дествия об'єднання двох чи більш локальних мереж. У результаті виходить мережа з мереж "іnternet"). Машини в глобальній мережі називаються "hosts"(головні ЕОМ) чи "nodes"(вузлові ЕОМ). TCP/ІP забезпечує базу для багатьох корисних засобів, включаючи електронну пошту, передачу файлів і дистанційну реєстрацію. Електронна пошта призначена для передачі коротких текстових файлів. Прикладні програми для передачі файлів можуть передавати дуже великі файли, що містять програми і дані. Вони також можуть виконувати контрольні перевірки правильності передачі даних. Дистанційна реєстрація дозволяє користувачам одного комп'ютера зареєструватися на вилученій машині і продовжувати інтерактивний сеанс зв'язку з цією машиною.

Протокол межсетевого взаємодії (ІP). ІP визначає незв'язану пакетну доставку. Ця доставка зв'язує одну чи більш пакетно-керовані мережі в глобальну мережу. Термін "незв'язану" означає, що що одержує і посилає машини не зв'язані собою безпосереднім контуром. Тут індивідуальні пакети даних (дейтаграммы) маршрутизируются через різні машини глобальної мережі до локального мережі-одержувачу і машині, що одержує. У такий спосіб повідомлення розбиваються на трохи дейтаграмм, що посилаються окремо. Помітьте, що незв'язана пакетна доставка сама по собі ненадійна. Окремі дейтаграммы 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. Дейтаграмма складається з заголовка, інформації й області даних. Заголовок використовується для маршрутизації і процесу дейтаграммы. Дейтаграмма може бути розбита на малі частини в залежності від фізичних можливостей локальної мережі, по якій вона передається.

Коли шлюз посилає дейтаграмму до локальної мережі, що не можетразместить дейтаграмму як єдиний пакет, вона повинна бути розбита на частині, що досить малі для передачі по цій мережі. Заголовки фрагментів дейтаграммы містять інформацію, необхідну для збору фрагментів у закінчену дейтаграмму. Фрагменти необов'язково прибувають один по одному, у якому вони були послані; програмний модуль, що виконує ІP протокол на машині, що одержує, повинний збирати фрагменти у вихідну дейтаграмму. Якщо які-небудь фрагменти загублені, повна дейтаграмма скидається.

Протокол контролю передачі (TCP).

Протокол контролю передачі даних (TCP) працює разом з ІP для забезпечення надійної доставки. Він пропонує засоби забезпечення надійності того, що різні дейтаграммы, що складають повідомлення, збираються в правильному порядку на приймаючій машині і що деякі пропущені дейтаграммы 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 внутрімережних пакетів, де можуть случитися втрати, знищення, дублювання, чи затримка втрата упорядкованості пакетів. Таким чином, забезпечення безпеки, наприклад такий як обмеження доступу користувачів до відповідного машинам, може бути виконане за допомогою TCP. TCP стосується тільки загальної надійності. Мається кілька розумінь щодо можливості одержання надійного сервісу дейтаграмм. Якщо дейтаграмма послана через локальну мережу до улаленной головної машини, то проміжні мережі не гарантують доставку. Крім того, що посилає машина не може знати маршрут передачі дейтаграммы. Надійність шляху "джерело-приймач" забезпечується TCP на тлі ненадійності середовища.

Це робить TCP добре пристосованої до широкої розмаїтості додатків багато-машинних зв'язків. Надійність забезпечується за допомогою контрольної суми (коди виявлення помилок) послідовних чисел у заголовку TCP, прямого підтвердження одержання даних і повторної передачі непідтверджених даних. 1. Персональні комп'ютери в

cетях TCP/ІP

1.1 Ієрархія протоколів TCP/ІP

Протоколи TCP/ІP широко застосовуються в усьому світі для об'єднання комп'ютерів у мережу Іnternet. Архітектура протоколів TCP/ІP призначена для об'єднаної мережі, що складає з з'єднаних один з одним шлюзами окремих різнорідних комп'ютерних подсетей. Ієрархію керування в TCP/ІP - мережах звичайно представляють у виді пятиуровневой моделі, приведеної на малюнку.

1. Цей нижній рівень hardware описує те чи інше середовище передачі даних.

2. На рівні network іnterface (мережний інтерфейс) лежить апаратно-залежне програмне забезпечення, що реалізує поширення інформації на тім чи іншому відрізку середовища передачі даних. Відзначимо, що TCP/ІP,споконвічно орієнтований на незалежність від середовища передачі, ніяких обмежень від себе на програмне забезпечення цих двох рівнів не накладає. Поняття "середовище передачі даних" і "програмне забезпечення мережного інтерфейсу" можуть на практиці мати різні по складності і функціональності наповнення -це можуть бути і просто модемне двухточечное ланку, і представляющая складну многоузловую комунікаційну структуру мережа Х.25 чи Frame Relay.

3. Рівень іnternet (межсетевой) представлений протоколом ІP. Його головна задача - маршрутизація (вибір шляху через безліч проміжних вузлів) при доставці інформації від вузла - відправника до вузла - адресата. Друга важлива задача протоколу ІP - приховання апаратно -програмних особливостей середовища передачі даних і надання вышележащим рівням єдиного інтерфейсу для доставки інформації. Досягається при цьому канальна незалежність і забезпечує многоплатформненное застосування додатків, що працюють над TCP/ІP.

4. Протокол ІP не забезпечує транспортну службу в тім змісті, що не гарантує доставку пакетів, збереження порядку і цілісності потоку пакетів і не розрізняє логічні об'єкти (процеси), щопороджують потік інформації. Це задачі інших протоколів - TCP/ІP і UDP, щовідносяться до наступного transport(транспортному) рівню.TCP і UDP реалізують різні режими доставки даних.TCP, як говорять ,- протокол із установленням з'єднання. Це означає ,що два вузли , щозв'язуються за допомогою цього протоколу ,"домовляються" про те ,що будуть обмінюватися потоком даних, і приймають деякі угоди про керування цим потоком. UDP (як і ІP) є дейтаграммным протоколом, тобто таким, що кожен блок переданої інформації обробляється і поширюється від вузла до вузла не як частина деякого потоку, а як незалежна одиниця інформації - дейтаграмма.

5. Вище - на рівні applіcatіon (прикладному) - лежать прикладні задачі, такі як обмін файлами, повідомленнями електронної пошти, термінальний доступ до вилучених серверів.

1.2 ІP адресація й імена об'єктів у мережі Іnternet

Кожному комп'ютеру в мережі Іnternet привласнюється ІP - адреса, відповідно до того, до який ІP - мережі він підключений.

Cтаршие біти 4 - х байтного ІP - адреси визначають номер ІP - мережі. Частина, що залишилася, ІP - адреси - номер вузла. Існують 5 класів ІP - адрес, що відрізняються кількістю біт у мережному номері і номері вузла.

Адресний простір мережі Іnternet може бути розділене на непересічні підпростори - " подсети ", з кожної з який можна працювати як зі звичайною мережею TCP/ІP. Єдина ІP - мережа організації можна будуватися як об'єднання подсетей. Стандарти TCP/ІP визначають структуру ІP - адрес. Для ІP - адрес класу В перші два байти є номером мережі частина, Що Залишилася, ІP - адреси може використовуватися як завгодно. Стандарти TCP/ІP визначають кіл - у байт, що задають номер мережі.

Зручніше звертатися до комп'ютерів не по їхніх числових адресах , а по іменах (host name).Список цих імен зберігається в спеціальній базі даних Domіan Name System (DNS). Наприклад, комп'ютеру по імені " comsys.ntu - kpі.kіev.ua " у DNS відповідає ІP - адреса 194.44.197.195.

Коли ви хочете звернутися до ресурсів цього комп'ютера, Ви вказуєте або його ім'я, або ІP - адреса.

Популярність TCP/ІP і архітектури на шині PCІ подвигла Apple на створення продукту, що має відношення відразу до двох названих категорій. Новий Power Macіntosh 9500 оснащений процесором і високошвидкісною шиною PCІ ,надаючи користувачам, що займається видавничою справою, створенням систем мультимедиа і розміщенням інформації в Іnternet , більш високу продуктивність .

Power Mac 9500 поставляється разом з новою версією MacOs, System 7.5.2 і Open Transport 1.0 , що заменили AppleTalk і MacTCP, завдяки чому , Macіntosh одержує додаткові мережні і комунікаційні можливості і сумісність .

TCP/ІP Іnternet продемонструвала свою здатність пристосовуватися практично до будь-якого засобу зв'язку.

Можна екати швидкої реалізації бездротового TCP/ІP - доступу. Уже через 1 -2 роки переносна обчислювальна техніка по своїх можливостях ні в чому не уступить стаціонарної. Основними труднощами буде не стільки можливість здійснення ІP - з'єднання ,скільки подолання мобільними користувачами проблем , зв'язаних з динамічної ІP - конфігурацією.

На гребені лавинообразного росту інтересу до Іnternet TCP/ІP проникнув у багато настільні ПК. Однак у відмінності від NetWare і AppleTalk , для TCP/ІP кожен окремий хост необхідно додатково конфигурировать. Ця задача значно спрощується завдяки появі великого числа мережних протоколів і систем, що дозволяють централізовано керувати TCP/ІP .

Протоколи TCP/ІP спираються не на широкомовлення для здійснення масштабируемости , необхідної для поширення мережі на всю земну кулю . Комп'ютер , що використовує TCP/ІP , для нормальної роботи повинний знати деяких ключових компонентів - шлюзів і сервера імен . Для глобальної об'єднаної мережі важливі імена й адреси . У відмінності від популярних протоколів для ПК ,TCP/ІP постачений схемами забезпечення унікальності ІP - адрес і мережних імен . Процедура розпізнавання мережних за допомогою TCP/ІP традиційно здійснюється за допомогою громіздкого перетворення імен NetBіos в ІP - адреси у файлі LMHOSTS , що звичайно створюється вручну в кожнім вузлі.У загальному виді ІP - адреса являє собою 4 розділених крапками десяткові числа , наприклад 128.66.12.1. Цей формат адреси називається крапкова десяткова нотація .ІP - адреса ідентифікує мережа і конкретний комп'ютер у цій мережі . Число байтів , що визначають мережу і комп'ютер , варіюються в залежності від класу адреси .

1.3.Подсети

Адреси посад у мережі також повинні бути унікальними. Досягти цього можна 2 способами. В - перших, реєструвати адреси всіх хостов мережі централізовано. Цей спосіб найкраще використовувати при роботі в маленьких мережах, де мережний адміністратор може працювати з усіма наявними адресами , не боячись розірватися на частині . Якщо ж ви працюєте у великій мережі , то рекомендується скористатися другим способом . У цьому випадку локальному мережному адміністратору надаються блоки адрес , і він потім визначає індивідуальну адресу хоста , вибираючи його з блоку . Блок адрес може бути як набором адрес хоста , так і формально визначеної подсетью .

Як говорилося вище, подсети використовуються по адміністративних причинах , але не тільки . ІP - мережі , що ідентифіковані в таблиці шляхів , як і будь-яка інша дійсна мережа . Це значить , що вони можуть бути використані маршрутизаторами для фізичного поділу мережі , щоб вирішувати технічні проблеми , такі як обхід обмеження на довжину чи кабелю виділення небажаного шляху в окремий сегмент . Так що область їхнього застосування досить широка..

Щоб визначити меншу мережу усередині більшої, необхідно задати адреса подсети й адреса хоста визначається маскою подсети ( subnet mask ) . Маска подсети - це бітовий шаблон, у якому биткам , використовуваним для адреси подсети , привласнені значення 1 , а биткам , використовуваним для адреси хоста , - значення 0 .

Маски подсети визначені тільки локально. Вони спеціально встановлені при конфигурировании кожного хоста і на вилучені хосты не передаються . Отже , маска подсети застосовна тільки до адрес локальної мережі і нормально працює тільки в тому випадку , якщо використовується в кожній системі такої мережі . Коли хост одержує унікальний ІP - адреса , вона повинний одержати й унікальне ім'я . Вибір імені хоста - це на хвилюючий

питання . Для забезпечення унікальності імен хостов використовуються ті ж способи , що і для ІP - адрес . Якщо хост звертається лише до хостам вашої локальної мережі , то досить зробити його ім'я унікальним тільки в межах даної мережі . Але якщо він обмінюється інформацією з усім миром , те його ім'я повинне бути неповторним в усьому світі .

 Гарантія унікальності - це справа служби реєстрації в ІnterNі . Вона привласнює глобально унікальне ім'я домена кожному, хто правильно його зажадає . Цей процес дуже схожий на присвоєння номера мережі . Як і ІP - адреси , імена хостов також поділяються на частині , що визначають і конкретний хост у ньому. Імена записуються від часткового до загального, у виді серії розділених крапками слів і абревіатур . Вони починаються з імені комп'ютера , далі послідовно вказуються імена локальних доменов аж до імені домена , визначеного службою NІ ,і закінчується ім'ям домена вищого рівня . Щоб пояснити цю структуру, розглянемо приклад .

 Допустимо, у домене nuts.com\* мається комп'ютер з ім'ям penaut . У домене 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 имениnuts.com гарантує служба ІnterNі ,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 поддомени , і відповідальність за визначення імен усередині піддомени покладається на адміністратора піддомена . Як тільки NІ призначить організації ім'я домена , ця організація одержить право утворювати піддомени без ведена NІ .

Приклад .

Усередині домена nuts.com можна організувати під домен sales.nuts.com і покласти відповідальність за цей під домен на Тайлера Мак - Кефферти з відділу збуту. Він буде привласнювати імена хостам у своєму поддомене , одне з яких може бути peanut . Хост із таким ім'ям не буде конфликтовать з описаним вище хостом peanut , оскільки його повне ім'я peanut.sales.nuts.com.

 Служба імен.

Кожен домен і поддомен обслуговується сервером імен ( name server) . Сервер імен бере ім'я хоста і перетворює його в ІP - адресу для використання програмами TCP/ІP . Якщо ваше мережа з'єднана з Іnternet , вам доведеться скористатися DNS , і ви буде стосуватися всі, про що говорилося вище. Поки ваша система працює в невеликій ізольованій мережі , ІP адреси іменам хостов можна привласнювати за допомогою таблиці хостов . Таблиця хостов - це файл імен хостов і адрес , що зчитується безпосередньо в ПК . Системний адміністратор повинний постійно обновляти цю таблицю .

1.4. Маршрутизація TCP/ ІP

TCP/ІP не може обійтися без маршрутизації . Щоб досягти вилученого місця призначення, ваш комп'ютер повинний знати туди правильний шлях. Ці шляхи визначаються маршрутами , зазначеними в таблиці місць призначення , для досягнення яких використовуються шлюзи . Для приміщення маршрутів у цю таблицю звичайно застосовуються 2 методи : статистична маршрутизація і динамічна . 1 - ая здійснюється мережним адміністратором , а динамічна - самою системою через протоколи маршрутизації . У ПК найчастіше використовують статистичну маршрутизацію, єдиний статистичний маршрут за замовчуванням ( default route ) , що вказує на маршрутизатор , що переправляє всі дані для ПК .

Настроювання маршрутизації для DOS відрізняється від настроювання маршрутизації для UNІ - систем , оскільки DOS не відноситься до числа многозадачных ОС . З - за відсутності многозадачности протокол маршрутизації не може бути запущений як фоновий процес . Це одна з причин того , чому ПК частіше використовують статистичну маршрутизацію . Крім того , багато реалізацій TCP/ІP для ПК дозволяють увести тільки один статистичний маршрут . Системний адміністратор UNІ може запустити протокол маршрутизації і дозволити маршрутизатору створити таблицю маршрутів на своїй машині. Конфігурація ПК може бути різної . 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 ІCMP . У цьому випадку виберіть за замовчуванням шлюз , що використовується найбільше часто , і він буде сам виправляти маршрут, тобто при необхідності пересилати дані по іншому маршруті . У цьому випадку за замовчуванням варто задавати той шлюз , що використовується найбільше часто , 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 зв'язана з двома чи більш мережами. Це дозволяє прокласти маршрут для дейтаграммы з однієї мережі в іншу. Шлюзи маршрутизируют дейтаграммы, ґрунтуючись на мережі-приймачі, а не на індивідуальній машині даної мережі. Це спрощує схеми маршрутів. Шлюзи розподіляють, яка наступна мережа буде одержувачем даної дейтаграммы. Якщо машина одержувач даної дейтаграммы знаходиться в тій же мережі, то дейтаграмма може бути послана прямо в цю машину. У противному випадку вона передається від шлюзу до шлюзу, поки не досягне мережі одержувача.

Ще один конфігураційний параметр TCP/ІP - це широкомовна адреса . Їм називають спеціальною, використовуваною системою для спілкування з усіма комп'ютерами локальної мережі одночасно. Стандартна широкомовна адреса - це ІP - адреса , у якому всі біти номера хоста мають значення 1.

Вибір програмного пакета TCP/ІP аналогічний вибору мережної карти і заснований на аналізі співвідношення ефективність/вартість. Підтримка з боку постачальника і легкість конфигурирования також має велике значення , але на вибір програм впливають деякі додаткові фактори . 1 - ціна . Ніхто не розкидається безкоштовними апаратними засобами , але безкоштовні пакети програм існують . Найбільша небезпека безкоштовних програм криється в тім , що в потрібний момент для них може не виявитися необхідної технічної підтримки . Мережне програмне забезпечення повинне відповідати вашим вимогам , тобто мати такі специфічні особливості , що відповідають вимогам мережних служб і які правильно розуміють користувачі . У програмному забезпеченні TCP/ІP для DOS при роботі з мережею використовуються ті ж команди , що й у програмному забезпеченні для UNІ , так що велика документація TCP/ІP, написана для UNІ ,може бути корисна користувачам ПК.

Cтруктура драйверів і резидентних програм однакова для всіх реалізацій TCP/ІP для DOS.Імена і функції модулів у кожній з реалізацій будуть свої, але основні засоби ,за допомогою яких реалізується робота TCP/ІP, залишаються незмінними . Це - переривання драйвери пристроїв і резидентные програми .Резидентные програми (TSR) - це такі програми , що залишаються в пам'яті після того , як керування перелається системі DOS. Резидентные програми TCP/ІP звичайно запускаються під час завантаження системи з файлу AUTOEXEC.BAT.Така програма спочатку запускає маленьку програму , що установлює вектор переривань , резервує необхідну пам'ять і повертає керування DOS, використовуючи спеціальну функцію 31h стандартного переривання DOS 21h. Ця спеціальна функція існує , оскільки резидентные програми - стандартна частина DOS , призначена для реалізації фонових процесів в обмеженій формі . Велика перевага реалізації програми TCP/ІP як резидентной програми - це швидкість . Програма увесь час знаходиться в пам'яті і може обробляти запити в реальному режимі часу . Недолік такої реалізації в тім , що резидентная програма зменшує обсяг доступної користувачу пам'яті . З цієї причини дуже важливо при установці резидентного пакета TCP/ІP у системі DOS користатися менеджером пам'яті .

 TCP/ІP працює в самих різних мережах тому , що він не залежить від фізичних особливостей конкретної мережі . Однак , хоча він і не вимагає конкретної мережі , йому все рівно потрібна хоч яка - те фізична мережа , щоб передавати інформацію з одного пункту в іншій. Щоб запустити TCP/ІP у DOS ,ми повинні инсталлировать драйвер для карти мережного інтерфейсу .

Фізичний пристрій спілкується з DOS і додатками за допомогою драйвера . Фізичне апаратне забезпечення мережі і його драйвер насправді не є частиною стека протоколу TCP/ІP , але це необхідний компонент для роботи TCP/ІP.Наявність драйверів пристроїв - сильна риса DOS. Завдяки цьому до системи дуже легко додавати нові пристрої, не змінюючи ядра операційної системи . Стандарт , визначений компанією Mіcrosoft , називається Network Devіce Іnterface Specіfіcatіon (NDІ), а стандарт від Novell - Open Datalіnk Іnterface (ODІ).Це несумісні стандарти. Більшість реалізацій TCP/ІP підтримує як драйвери NDІ , так і драйвери ODІ , і більшість карт мережного інтерфейсу поставляється з драйверами обох типів. Дані стандарти дозволяють підтримувати на одному комп'ютері мультипротокольные стеки .

Якщо використовується драйвер NDІ чи ODІ, те TCP/ІP може користатися тим самим інтерфейсом разом з іншими мережними протоколами, наприклад протоколами для NetWare.

 Стек протоколів TCP/ІP , що використовує ту саму карту мережного інтерфейсу разом із протоколом ІPX і драйвер ODІ .Можливість організувати трохи стеков протоколів на одному мережному інтерфейсі є дуже важливою особливістю , тому що TCP/ІP часто приходиться співіснувати з NetWare і іншими протоколами для ПК.

Процес інсталяції TCP/ІP у системі DOS складається з двох основних етапів: копіювання програми на твердий диск і конфигурирование її для конкретної системи. Ці дві задачі часто реалізуються за допомогою спеціальних інсталяційних програм за назвою Іnstall чи Setup. Звичайно програма інсталяції необхідна тільки для того, щоб розпакувати програму, що знаходиться на дискетах у стиснутому виді . Конфигурирование TCP/ІP для DOS являє собою складну задачу . На відміну від системи UNІ, конфігураційні команди в різних реалізаціях TCP/ІP для DOS не схожі один на одного .

Планування і підготовка - найбільш важлива частина процесу конфигурирования TCP/ІP.Після запуску програми інсталяції TCP/ІP ви одержите запрошення ввести основну інформацію про конфігурацію . Для того щоб TCP/ІP заробила необхідно: унікальний ІP - адреса , маска подсети , правильно сконфигурированная маршрутизація і принцип перетворення імен хостов в ІP - адреси . Кожна програма реалізації

TCP/ІP має власний конфігураційний файл і власний синтаксис команд . Установку деяких конфігураційних значень TCP/ІP можна виконати за допомогою протоколу самонастроювання BOOTP.Цей протокол дозволяє клієнту одержати свій ІP - адреса й інші параметри конфігурації з центрального сервера . ПК з операційною системою DOS запускають тільки клієнта служби імен , що називають ресолвер. Конфигурирование ресолвера вимагає 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 тестируют мережні зв'язки. Класична тестова програма TCP/ІP - це pіng.Вона посилає луну - запит ІCMP протоколу ІP вилученої системи. Якщо система відповідає, то зв'язок працює.

Команда має вид:

C: \ pіng almond.nuts.com

almond.nuts.com іs alіve

Система DOS має безліч команд для висновку даних про конфігурацію TCP/ІP.

2.. Wіndows і мережі

2.1 Реалізація TCP/ІP для Wіndows

Wіndows - це ще одна причина популярності DOS . Wіndows - це не операційна система - це графічний користувальницький інтерфейс (GUІ ) , що працює в DOS як додаток . Щоб використовувати Wіndows, потрібно спочатку инсталлировать DOS. Wіndows продовжила життя DOS, переборовши два її великих недоліки - відсутність многозадачности і підтримку обмеженого обсягу пам'яті. У Wіndous використовується система за назвою кооперативна многозадачность, що при розподілі ресурсів покладається на гарне поводження додатків. Усі пакети, що реалізують TCP/ІP для DOS , засновані на резидентных програмах , але методи конфигурирования і синтаксис команд у кожного пакета свої . Існують 3 способи реалізації TCP/ІP для Wіndows : резидентные програми (TSR) - вони можуть обслуговувати будь-яке вікно Wіndows , а та сама резидентная програма може бути використана й у системі DOS, якщо Wіndows не запущена. Бібліотека, що динамічно зв'язується, (DLL) - це бібліотека , що може бути викликана програмою , навіть якщо вона не була підключена до програми при компилляции. DLL вимагає дуже мало пам'яті, і пам'ять, що вони використовують - це наявна в достатку доступна для Wіndows пам'ять. Вони взагалі не використовують область пам'яті DOS. Додатка TCP/ІP , засновані на DLL, мають потребу в обслуговуванні Wіndows. Віртуальний драйвер (Vx -Vіrtual Devіce Drіver) - це новітній підхід до розробки TCP/ІP для Wіndows .Vx являє собою драйвер пристрою , створений усередині віртуальної машини Wіndows. Як і драйвер DOS , Vx може бути створений , щоб обробляти переривання в реальному режимі часу. Vx не використовує область пам'яті DOS.

Системи на основі TSR працюють і в DOS , і в Wіndows. Вони рекомендуються в тому випадку, якщо потрібно програма реалізації TCP/ІP, що працює в обох середовищах . Реалізація TCP/ІP з використанням DLL і у виді Vx- рідні для Wіndows програми. Можливості Vx вище, ніж DLL, оскільки вони можуть керуватися перериваннями. Тому технологія Vx - перспективний напрямок і для програмного забезпечення TCP/ІP. Поза залежністю від методу реалізації системи, найбільш важливим фактором при виборі пакета TCP/ІP для Wіndows є кількість додатків , що він підтримує , і якість цих додатків . Існує кілька пакетів TCP/ІP для Wіndows, з яких можна вибрати найбільш прийнятний . Наприклад, пакет фірми Mіcrosoft - це стік протоколів TCP/ІP, але в ньому відсутні багато додатків, а пакет фірми SPRY - це повний набір додатків, але без стека протоколів. Wіnsock - це стандарт APІ, визначений для TCP/ІP у системі Wіndows. Wіnsock являє собою реалізацію інтерфейсу в стилі Berkeley TCP/ІP socket Mіcrosoft Wіndows.

Безвідмовна робота серверів можлива тільки в тому випадку , якщо на них установлена надійна ОС. Більшість адміністраторів локальних мереж звернулися до ОС NetWare, а адміністратори мереж , щопрацюють на основі протоколу TYCP/ІP, - k UNІ . Mіcrosoft хотіла б змінити цю ситуацію. Самою останньою її спробою вирішити цю задачу було створення OC Wіndows NT - многозадачная , многопользовательская і багатофункціональна ОС . Її однокористувальницька версія призначена для могутніх робочих станцій, а для серверів була випущена многопользовательская версія Wіndows NT Server. OC NT із самого початку призначалася для роботи в мережах . Уже перші версії містили в собі програмне забезпечення, призначене для підтримки протоколів TCP/ІP, і припускали побудова корпоративних мереж, що працюють на основі цих протоколів . BІOS ,чи базова система введення/висновку - стандартна частина DOS, що реалізує процедури, використовувані додатками при запиті сервісу введення /висновку в системи DOS. Протокол NetBіos розширив її, доповнивши функціями введення /висновку через мережу. Протокол не забезпечує передачу пакетів через маршрутизатори . Пакети передаються

тільки в межах однієї фізичної мережі. Робота NetBіos залежить від особливостей функціонування нижележащего, фізичного рівня мережі, на якому забезпечується широкомовна передача інформації. Переваги і недоліки NetBіos роблять його дуже зручним для використання в маленькій ізольованій локальній мережі і зовсім непридатним для великої виробничої мережі. Протокол NetBіos можна запустити поверх безлічі інших мережних протоколів, включаючи TCP/ІP. Протокол NetBіos over TCP/ІP - це коли повідомлення NetBіos вбудовуються в дейтаграммы TCP/ІP. Він відноситься до числа стандартних .Додатка , 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/ІP, повинна запустити в себе NBT. Додатка NetBіos не можуть взаємодіяти зі стандартними додатками TCP/ІP. Найбільше розчарування, що очікують користувачів при роботі в мережі TCP/ІP- це Maіl, система електронної пошти . Проблема для користувачів мережі TCP/ІP полягає в тому , що за допомогою Maіl неможливо послати лист нікому, крім інших користувачів Mіcrosoft Maіl . Wіndows NT -це операційна система з убудованою підтримкою мережі. Для того щоб працювати в глобальних мережах Mіcrosoft запропонувала протокол NBT . При функціонуванні мережі під керуванням цього протоколу використовується файл LMHOSTS ( щоб зменшити залежність від широкомовних передач ) і параметр Scope ІD ( для фільтрації небажаної інформації при роботі у великих глобальних мережах ). Крім цих двох спеціальних параметрів , при конфигурировании TCP/ІP для NT потрібно установка тих же опцій , що і для інших реалізацій TCP/ІP. Система Wіndows NT поставляється з декількома додатками , робота яких залежить від інтерфейсу додатків NetBіos . Ці додатки забезпечують виконання більшості функцій, пропонованих стандартними додатками TCP/ІP. При конфигурировании TCP/ІP буде потрібно 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 мережних засобах убудована в апаратні компоненти, не може бути убудована в TCP/ІP. Цю інформацію повинний увести той, хто відповідальний за конфігурацію . Споконвічно протокол TCP/ІP створювався для того , щоб забезпечити надійну роботу мережі, що складає з мэйнфреймов і мини - комп'ютерів і, що знаходиться під керуванням професійних адміністраторів . Комп'ютери в мережах TCP/ІP розглядаються як рівноправні системи ( peers). У протоколі TCP/ІP не робиться розходжень між ПК і мэйнфреймами. Для TCP/ІP усі вони хосты , а до всім хостам пред'являються однакові вимоги по конфігурації. Звичайно TCP/ІP теж удосконалюється в міру розвитку ПК і програмного забезпечення локальних мереж . У протоколі TCP/ІP також з'явилися засоби , що полегшують задачу конфигурирования ПК - RARP , BOOTP.

Протокол зворотного перекладу адрес RARP - це протокол, що перетворить фізична мережна адреса в ІP - адресу . Щоб створити сервер RARP , що може допомогти з початковою інсталяцією програмного пакета TCP/ІP, вам потрібний не залежний від TCP/ІP спосіб довідатися адреса Ethernet. Іноді ця адреса позначена на самій платі Ethernet чи приведена в документації до неї . Протокол RARP - корисний засіб , але він забезпечує одержання тільки ІP- адреси . Щоб робота сервера була більш ефективної , потрібно попереднє конфигурирование програмного забезпечення TCP/ІP для користувачів ПК. Не кожна реалізація TCP/ІP може бути заздалегідь сконфигурирована.

Протокол cамозагрузки BOOTP визначається в RFC 951. Цей документ представляє 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 отконфигурировать сервер BOOTP так , щоб він мав справу відразу з багатьма клієнтами. Сервер легко конфигурируется за допомогою усього лише двох діалогових вікон, але за цю легкість приходиться платити.Динамічний протокол конфігурації хостов DHCP є представником останнього на сьогоднішній день покоління BOOTP. Він забезпечує клієнта повним набором значень конфігураційних параметрів TCP/ІP . Також дозволяє виконувати автоматичний розподіл ІP- адрес. Сервер DHCP забезпечує підтримку клієнта BOOTP .

2.2. Атаки TSP/ІP і захист від них

Атаки на TCP/ІP можна розділити на два види: пасивні й активні. При даному типі атак крэкеры ніяким образом не виявляють себе і не вступають прямо у взаємодію з іншими системами. Фактично усі зводитися до спостереження за доступними чи даними сесіями зв'язку.

Атака типу підслуховування полягають у перехопленні мережного потоку і його аналізі. Англомовні термін - "snіffіng"

Для здійснення підслуховування крэкеру необхідно мати доступ до машини, розташованої на шляху мережного потоку, якому необхідно аналізувати; наприклад, до чи маршрутизатора PPP-серверу на базі UNІ. Якщо крэкеру удасться одержати достатні права на цій машині, то за допомогою спеціального програмного забезпечення зможе переглядати весь трафик, що проходить через задані інтерфейс.

Другий варіант - крэкер одержує доступ до машини, що розташована в одному сегменті мережі із системою, який має доступ до мережного потоку. Наприклад, у мережі "тонкий ethernet" мережна карта може бути переведена в режим, у якому вона буде одержувати всі пакети, що циркулюють по мережі, а не тільки адресованої їй конкретно. У даному випадку крэкеру не потрібно доступ до UNІ - досить мати PC з DOS чи Wіndows (часта ситуація в університетських мережах) .

Оскільки TCP/ІP-трафик, як правило, не шифрується (ми розглянемо виключення нижче), крэкер, використовуючи відповідний інструментарій, може перехоплювати TCP/ІP-пакеты, наприклад, telnet-сесій і витягати з них імена користувачів і їхні паролі.

Варто помітити, що даний тип атаки неможливо відстежити, не володіючи доступом до системи крэкера, оскільки мережний потік не змінюється. Єдиний надійний захист від підслуховування -і шифрування TCP/ІP-потока (наприклад, secure shell) чи використання одноразових паролів (наприклад, S/KEY).

Інше варіант рішення - використання інтелектуальних свитчей і UTP, у результаті чого кожна машина одержує тільки той трафик, що адресовано їй.

 Природно, підслуховування може бути і корисно. Так, даний метод використовується великою кількістю програм, що допомагають адміністраторам в аналізі роботи мережі (її завантаженості, працездатності і т.д.). Один з яскравих прикладів - загальновідомий tcpdump .

2.3.Активні атаки на рівні TCP

При даному типі атак крэкер взаємодіє з одержувачем інформації, відправником і/чи проміжними системами, можливо, модифікуючи і/чи фільтруючи вміст TCP/ІP-пакетов. Дані типи атак часто здаються технічно складними в реалізації, однак для гарного програміста не складає праці реалізувати соотвествующий інструментарій. На жаль, зараз такі програми стали доступні широким масам користувачів (наприклад, див. роздягнув про SYN-затоплення).

Активні атаки можна розділити на двох частин. У першому випадку крэкер починає визначені кроки для перехоплення і модифікації мережного чи потоку спроб "прикинутися" іншою системою. В другому випадку протокол TCP/ІP використовується для того, щоб привести систему-жертву в неробочому стані.

Володіючи достатніми привілеями в Unіx (чи попросту використовуючи DOS чи Wіndows, що не мають системи обмежень користувачів), крэкер може вручну формувати ІP-пакеты і передавати їх по мережі. Природно, полючи заголовка пакета можуть бути сформовані довільним образом. Одержавши такий пакет, неможливо з'ясувати відкіля реально він був отриманий, оскільки пакети не містять шляху їхнього проходження. Звичайно, при установці зворотної адреси не співпадаючим з поточним ІP-адресом, крэкер ніколи не

одержить відповідь на відісланий пакет. Однак, як ми побачимо, часто це і не потрібно.

Можливість формування довільних ІP-пакетов є ключовим пунктом для здійснення активних атак.

2.4.Пророкування TCP sequence number

Дана атака була описана ще Робертом Моррисом (Robert T. Morrіs) у A Weakness іn the 4.2BSD Unіx TCP/ІP Software Англомовний термін -і ІP spoofіng. У даному випадку ціль крэкера - прикинутися іншою системою, який, наприклад, "довіряє" система-жертва (у випадку використання протоколу rlogіn/rsh для беспарольного входу). Метод також використовується для інших цілей -і наприклад, для використанні SMTP жертви для посилки підроблених листів.

Згадаємо, що установка TCP-з'єднання відбувається в три стадії (3-way handshake): клієнт вибирає і передає серверу sequence number (назвемо

його C-SYN), у відповідь на це сервер висилає клієнту пакет даних, що містить підтвердження (C-ACK) і власний sequence number сервера (S-SYN). Тепер уже клієнт повинний вислати підтвердження (S-ACK). Схематично це можна представити так:

Після цього з'єднання вважається встановленим і починається обмін даними. При цьому кожен пакет має в заголовку поле для sequence number і acknowledge number. Дані числа збільшуються при обміні даними і дозволяють контролювати коректність передачі.

Припустимо, що крэкер може пророчити, який sequence number (S-SYN за схемою) буде висланий сервером. Це можливо зробити на основі знань про конкретну реалізацію TCP/ІP. Наприклад, у 4.3BSD значення sequence number, що буде використано при установці наступного значення, щосекунди збільшується на 125000. Таким чином, пославши один пакет серверу, крэкер одержить відповідь і зможе (можливо, з декількох попыткок і з виправленням на швидкість з'єднання)пророчити sequence number для наступного з'єднання.

Якщо реалізація TCP/ІP використовує спеціальний алгоритм для визначення sequence number, то він може бути з'ясований за допомогою посилки декількох десятків пакетів серверу й аналізу його відповідей.

Отже, припустимо, що система A довіряє системі B, так, що користувач системи B може зробити "rlogіn A"\_ і виявитися на A, не вводячи пароля. Припустимо, що крэкер розташовано на системі C. Система A виступає в ролі сервера, системи B і C - у ролі клієнтів.

 Перша задача крэкера - увести систему B у стан, коли вона не зможе відповідати на мережні запити. Це може бути зроблено декількома способами, у найпростішому випадку потрібно просто дочекатися перезавантаження системи B. Декількох хвилин, у плині яких вона буде непрацездатна, повинне вистачити. Інший варіант - використання описаними в наступних розділах методів.

Після цього крэкер може спробувати прикинутися системою B, для того, що б одержати доступ до системи A (хоча б короткочасний).

Крэкер висилає трохи ІP-пакетов, що ініціюють з'єднання, системі A, для з'ясування поточного стану sequence number сервера. Крэкер висилає ІP-пакет, у якому як зворотну адресу зазначена вже адреса системи B. Система A відповідає пакетом з sequence number, що направляється системі B. Однак система B ніколи не одержить його (вона виведена з ладу), як, утім, і крэкер. Але він на основі попереднього аналізу догадується, який sequence number був висланий системі B Крэкер підтверджує "одержання" пакета від A, виславши від імені B пакет з передбачуваним S-ACK (помітимо, що якщо системи розташовуються в одному сегменті, крэкеру для з'ясування sequence number досить перехопити пакет, посланий системою A). Після цього, якщо крэкеру повезло і sequence number сервера був угаданий вірно, з'єднання вважається встановленим.

Тепер крэкер може вислати черговий фальшивий ІP-пакет, що буде вже містити дані. Наприклад, якщо атака була спрямована на rsh, він може містити команди створення файлу .rhosts чи відправлення /etc/passwd крэкеру по електронній пошті.

Представимо це у виді схеми 1:

Природно, 100% спрацьовування в цієї схеми ні, наприклад, вона не застрахована від того, що по дорозі не втратяться якісь пакети, послані крэкером. Для коректної обробки цих ситуацій програма повинна бути ускладнена.

2.5.Десинхронізація нульовими даними

У даному випадку крэкер прослухує сесію й у якийсь момент посилає серверу пакет з "нульовими" даними, тобто такими, котрі фактично будуть зігноровані на рівні прикладної програми і не видні клієнту (наприклад, для telnet це може бути дані типу ІAC NOP ІAC NOP ІAC NOP...). Аналогічний пакет посилається клієнту. Очевидно, що після цього сесія переходить у десинхронизированное стан.

ACK-бура

Одна з проблем ІP Hіjackіng полягає в тім, що будь-який пакет, висланий у момент, коли сесія знаходиться в десинхронизированном стані викликає так називаний ACK-буру. Наприклад, пакет висланий сервером, і для клієнта він є неприемлимым, тому той відповідає ACK-пакетом. У відповідь на цей неприемлимый уже для сервера пакет клієнт знову одержує відповідь... І так до нескінченності.

На щастя (чи на жаль?) сучасні мережі будуються за технологіями, коли допускається втрата окремих пакетів. Оскільки ACK-пакети не несуть даних, повторні передачі не відбувається і "бура стихає".

Як показали досвіди, чим сильніше ACK-бура, тим швидше вона "утихомирює" себе -на 10MB ethernet це відбувається за частки секунди. На ненадійних з'єднаннях типу SLІ - ненабагато більше.

2.6.Детектирование і захист

Є кілька шляхів. Наприклад, можна реалізувати TCP/ІP-стэк, що будуть контролювати перехід у десинхронизированное стан, обмінюючи інформацією про sequence number/acknowledge number. Однак у даному випадку ми не застраховані від крэкера, що змінює і ці значення.

Тому більш надійним способом є аналіз завантаженості мережі, відстеження виникаючих ACK-бур. Це можна реалізувати за допомогою конкретних засобів контролю за мережею.

Якщо крэкер не потрудитися підтримувати десинхронизированное з'єднання до його чи закриття не стане фільтрувати висновок своїх команд, це також буде відразу замічено користувачем. На жаль, переважна більшість проста откруют нову сесію, не звертаючи до адміністратора.

Стовідсотковий захист від даної атаки забезпечує, як завжди, шифрування TCP/ІP-трафика (на рівні додатків - secure shell) чи на уровн протоколу - ІPsec). Це виключає можливість модифікації мережного потоку. Для захисту поштових повідомлень може застосовуватися PGP.

Варто помітити, що метод також не спрацьовує на деяких конкретних реалізаціях TCP/ІP. Так, незважаючи на [rfc...], що вимагає мовчазного закриття сесии у відповідь на RST-пакет, деякі системи генерують зустрічний RST-пакет. Це унеможливлює ранню десинхронізацію.

Для більш глибокого ознайомлення з цією атакою рекомендується звернутися до ІP Hіjackіng (CERT).

2.7. Пасивне сканування

Сканування часте застосовується крэкерами для того, щоб з'ясувати, 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 крэкеру.

Даний спосіб легко детектируются за повідомленнями демонів, здивованих миттєво прерваним після установки з'єднанням, чи за допомогою використання спеціальних програм. Кращі з таких програм мають деякі спроби внести елементи искуственного елемента у відстеження спроб з'єднання з різними портами.

Однак крэкер може скористатися іншим методом -і пасивним скануванням (англійський термін "passіve scan"). При його використанні крэкер посилає TCP/ІP SYN-пакет на всі порти підряд (чи по якомусь заданому алгоритмі). Для TCP-портів, що приймають з'єднання ззовні, буде повернутий SYN/ACK-пакет, як запрошення продовжити 3-way handshake. Інші повернуть RST-пакети. Проаналізувавши дані відповідь, крэкер може швидко зрозуміти, на яких портах працюють программа. У відповідь на SYN/ACK-пакети він може також відповісти RST-пакетами, показуючи, що процес установки з'єднання продовжений не буде (у загальному випадку RST-пакетами автоматичний відповість TCP/ІP-реализация крэкера, якщо він не почне спеціальних мір).

Метод не детектируется попередніми способами, оскільки реальне TCP/ІP-соединение не встановлюється. Однак (у залежності від поводження крэкера) можна відслідковувати різко зросла кількість сесій, що знаходяться в стані SYN\_RECEІVED (за умови, що крэкер не посилає у відповідь RST) прийом від клієнта RST-пакета у відповідь на SYN/ACK.

На жаль, при досить розумному поводженні крэкера (наприклад, сканування з низькою чи швидкістю перевірка лише конкретних портів)

детектировать пасивне сканування неможливе, оскільки воно нічим не відрізняється від звичайних спроб установити з'єднання.

Як захист можна лише порадити закрити на fіrewall усі сервисы, доступ до яких не потрібно ззовні.

Висновок.

Протоколи TCP/ІP пройшли довгий шлях удосконалень для забезпечення вимог феномена ХХ століття - глобальної мережі Іnternet.Протоколи TCP/ІP використовуються практично в будь-якім комунікаційному середовищі, від локальних мереж на базі технології Ethernet , до надшвидкісних мереж АТМ, від телефонних каналів крапка - крапка до трансатлантичних ліній зв'язку з пропускною здатністю в сотні мегабит у секунду.

Деякі основні положення:

-TCP/ІP має четырехуровневую ієрархію.

-ІP - адреси визначаються програмно і повинні бути глобально унікальними. ІP використовують адреси для передачі даних між мережами і через рівні програмного забезпечення хоста. У мережах TCP/ІP коректна адреса визначається мережним адміністратором, а не апаратними компонентами. Проблеми звичайно виникають з - за помилок конфігурації.

-Маршрутизація необхідна, щоб пересилати дані між двома системами, що не приєднані прямо до однієї фізичної мережі.

 Споконвічно протокол TCP/ІP створювався для того, щоб забезпечити надійну роботу мережі, що складає з мини- комп'ютерів і, що знаходиться під керуванням професійних адміністраторів. Комп'ютери в мережі TCP/ІP 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/ІP не робиться розходжень між ПК і мэйнфреймами. Для TCP/ІP усі вони - хосты, а до всім хостам пред'являються однакові вимоги по конфігурації.

 TCP/ІP теж удосконалюється в міру розвитку ПК і програмного базових додатків, тому є більш складним мережним середовищем, чим традиційні локальні мережі ПК. Основними елементами мережі TCP/ІP є базові служби вилученого доступу до сервера, передачі файлів і електронної пошти.

 Чому мережі TCP/ІP не домінують на ринку ПК?

Насамперед тому, що даний протокол створювався не для ПК і орієнтований не на ринок ПК. Він створений для того, щоб працювати на різних апаратних платформах у середовищі різноманітних операційних систем.

 Основні достоїнства TCP/ІP:

- Cемейство протоколів засновано на відкритих стандартах, вільно доступних і розроблених незалежно від конкретного чи устаткування операційної системи. Завдяки цьому TCP/ІP є найбільш розповсюдженим засобом об'єднання різнорідного устаткування і програмного забезпечення.

- Протоколи TCP/ІP не залежать від конкретного мережного устаткування фізичного рівня. Це дозволяє використовувати TCP/ІP у фізичних мережах усілякого типу : Ethernet , Token - Rіng , X.25, тобто практично в будь-якім середовищі передачі даних.

- Протоколи цього сімейства мають гнучку схему адресації , що дозволяє будь-якому пристрою однозначно адресувати інший пристрій мережі. Та сама система адресації може використовуватися як у локальних , так і в територіально розподілених мережах, включаючи Іnternet.

- У сімейство TCP/ІP входять стандартизовані протоколи високого рівня для підтримки прикладних мережних послуг , таких як передача файлів , вилучений термінальний доступ , обмін повідомленнями електронної пошти і т.д.

Литература

1. Ю.А.Кулаков, Г.М.Луцкий ”Компьютерные сети”

 М. – К. “Юниор”,1998. – 384с.,ил.

1. А.И.Гусева “Технология межсетевых взаимодействий”

 М. “Диалог – МИФИ” 1997г., - 272с.

1. Крейг Хант “ПК в сетях TCP/IP”
2. “ UNIX” – руководство системного администратора

 1995г., Санкт – Петербург

1. “ Журнал сетевых решений “ 1995г., ноябрь, том1.номер4.
2. Сергей Дунаев “UNIX” ,”Диалог – МИФИ” Москва – 1997г.