Міністерство освіти і науки ,
молоді та спорту України
Вищий приватний навчальний заклад
Міжнародний економіко-гуманітарний
університет імені академіка Степана Дем'янчука

А.В. Ільчук

Технології комп'ютерної безпеки

Книга 4

Науковий керівник:
Р.М.Літнарович, доцент,к.т.н.

Рівне, 2011

УДК 614.2 Ільчук А.В. Технології комп'ютерної безпеки. Книга 4. МЕГУ, Рівне, 2011.-70 с. Ilchuk A.V. Technologies of computer security. Book 4. IEGU, Rivne, 2011.-70 p.
Рецензенти: В.Г.Бурачек, доктор технічних наук, професор
Є.С. Парняков, доктор технічних наук, професор
В.О.Боровий , доктор технічних наук, професор
Відповідальний за випуск: Й.В. Джунь, доктор фізико-математичних наук, професор.

Послідовно розглядаються основні принципи побудови та функціонування комп'ютерних мереж. Монографія містить актуальний матеріал довідково-аналітичного характеру по наступних темах: структура мережевих операційних систем, мережеві архітектури, опис топологій локальних мереж, мережеві Unix подібні операційні системи, мережеве адміністрування, мережеве адміністрування у системі Linux, штатні фаєрволи системи Linux, створення правил фаєрволу IPTable для корпоративних мереж.

Ключові слова: комп'ютерні мережі, мережеве адміністрування, штатні фаєрволи системи Linux, створення правил фаєрволу IPTable для корпоративних мереж

Последовательно рассматриваются основные принципы построения и функционирования компьютерных сетей. Монография содержит актуальный материал справочно аналитического характера по следующим темам: структура сетевых операционных систем, сетевые архитектуры, описание топологии локальных сетей, сетевые Unix подобные операционные системы, сетевое администрирование, сетевое администрирование в системе Linux, штатные фаерволы системы Linux, создание правил фаервола Iptable для корпоративных сетей.

Ільчук Андрій Васильович

спеціаліст системотехнік, магістрант інформаційних технологій

ІН-11М

Технології комп'ютерної безпеки

Книга 4

Комп'ютерний набір, верстка і макетування та дизайн в редакторі Microsoft®Office® Word 2003 А.В.Ільчук. Науковий керівник Р. М. Літнарович, доцент, кандидат технічних наук

Міжнародний Економіко-Гуманітарний Університет ім. акад. Степана Дем'янчука

Кафедра математичного моделювання

33027,м.Рівне,Україна

Вул.акад. С.Дем'янчука,4, корпус 1

Телефон:(+00380) 362 23-73-09

Факс:(+00380) 362 23-01-86

E-mail:mail@regi.rovno.ua

E-mail:ururu_88@mail.ru

Ключевые слова: компьютерные сети, сетевое администрирование, штатные фаерволы системы Linux, создания правил фаерволу Iptable для корпоративных сетей

Basic principles of construction and functioning of computer networks are consistently examined. A monograph contains aktual material of certificate analytical character on the followings themes: structure of the network operating systems, network architecture, description of topologies of local networks, network Unix similar operating systems, network administration, network administration in the system of Linux, regular faervol systems of Linux, creation of rules of faervol of Iptable for corporate networks.

Keywords: computer networks, network administration, regular faervol systems of Linux, creations of rules of faervol of Iptable, are for corporate networks

Ільчук Андрій Васильович

Спеціаліст системотехнік, магістрант
інформаційних технологій.

17. http://habrahabr.ru/blogs/virtualization/115630/
18. http://uk.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F

Використана література

1. Буров Є. Комп'ютерні мережі. – Львів: БАК, 1999 – 468 с.
2. Бабич М. П., Жуков І. А., Яременко К.П., Журавель С.В. Комп'ютерна схемотехніка. Курсове проектування. , р.
3. Дрововозов В.І. Експлуатація комп'ютерних систем та мереж Навчальний посібник. - К.: НАУ, 2006, 2007 р.
4. Жабін В.І., Жуков І.А., Клименко І.А., Ткаченко В.В. Прикладна теорія цифрових автоматів Навч. посібник. - К.:Книжкове вид-во НАУ, 2007. - 364 с., 2007 р.
5. І.А. Жуков, М.А. Віноградов, В.І. Дрововозов, Н.Ф. Халімон. Основи теорії мереж передачі та розподілу даних НАУ, 2006, 2006 р.
6. Кеннет Г. "Основы сетей Windows". - К.:Диалектика;
7. Локальные вычислительные сети. Принципы построения, архитектура, коммуникационные средства./ Под ред. С.В.Назарова. – М.: Фин. и стат., 1994. – 400 с.
8. Основы современных кмпьютерных технологий./ Под ред. А.Д.Хомоненко. – СПб.: Корона, 1998. – 448 с.
9. Симпсон А. "Библия пользователя Windows";
10. Тхір І.Л., Калушка И.П., Юзьків А.В. «Посібник користувача ПК»;
11. Хаусли Т. Системы передачи и телеобработки данных. – М.: Радио и связь, 1994. – 297 с.
12. Халсалл Ф. Передача данных, сети компьютеров и взаимосвязь открытых систем. – М.: Радио и св., 1995. –354 с.
13. Шатт С. Мир компьютерных сетей. – К.: BHV, 1996. – 314 с.
14. http://www.ifcity.info;
15. http://w3c.org.
16. http://cyberdrive.narod.ru/HTML/ping.htm

Зміст

Вступ

Адміністрування комп’ютерних мереж ніколи не займали домінуючих позицій в IT технологіях. Традиційно незначна роль, що їм відводилась, призвела до того, що структура і функції ПЗ даного класу виявилися в прямій залежності від архітектури обчислюванних систем і еволюціонували разом із ними.

Як відомо, на початку 90-х років ері безроздільного панування хост-комп'ютерів прийшов кінець. Бурхливе поширення розподілених архітектур клієнт-сервер призвело до кардинальних зімни й у сфері керування інформаційними системами. Основна проблема полягала в тому, що адміністраторам довелося мати справу з небаченим раніше різноманіттям ресурсів: різні комп'ютерні платформи, активні мережеві устаткування, та програмні засоби. Ця гетерогенність зажадала рішення цілком нових адміністративних задач - управління розподіленими ресурсаим, електронним поширенням ПЗ, аналіз трафіка і керування пропускною спроможністю мережі, перерозподіли серверного навантаження, відслідковування стану окремих настільних систем і т.і. Справа ускладнювалася ще і тим, що в нове середовище неможливо було перенести додатки адміністрування, що функціонували на мейнфреймах, так що виробникам довелося створювати керуюче ПЗ практично з нуля.

Еволюція концепцій адміністрування відбувалася не тільки уздовж архітектурної осі, але й у просторі тих об'єктів, що поступово утягувалися в “сферу компетенції” керуючих засобів.

З погляду розв'язуваних задач, у період, коли мейнфрейми знаходилися в зеніті слави, їхнє адміністрування можна було з повною підставою віднести до категорії системного, що не в останню чергу означало існування єдиної уяви обчислювального середовища.

Висновок

З розвитком інформаційних технологій зокрема інформаційних ситстем змінилися базові концепції щодо їх управління - мережне і системне адміністрування інтегрували в єдиний комплексний підхід.

Аналіз розвитку комерційних програм мережного і системного адміністрування дозволяє зробити висновок, що ідея адміністрування зводиться до аналізу поводження інформаційної системи, або окремих її компонентів з метою своєчасного прийняття запобіжних засобів , що в свою чергу дає змогу не допустити розвиток подій по найгіршому сценарію.

Сектор адміністративного програмного забезпечення вже декілька років як вступив у стадію зрілості. На ринку є широка гама пропозицій - від базових платформ до оптимізованих засибів для виконання широкого кола задач. Більше того, якщо розглядати засоби адміністрування найбільших виробників, то розходження між ними в плані функціональності стають усе більш розмитими, що надає користувачам додаткову свободу вибору.

В даній дипломній роботі було детально роглянуто основні етапи побудови комп’ютерних мереж а також робота з Firewall IPTables. Під час написання дипломної роботи було написано програму firewall під кампусну комп’ютерну мережу. Firewall , що служить дуже важливою роллю в мережах і захищає офісні, домашні комп’ютери в Глобальній комп’ютерній мережі від злому хакерів.

PPP-ресурсу (наприклад, з модемним пулом) можуть безпечно організувати модемні підключення в обхід бар'єрів брандмауера, так як це прямі з'єднання. Однак для користувачів, що підключаються з відкритої зовнішньої мережі, слід вжити спеціальних заходів. Ви можете дозволити в IPTables підключення віддалених клієнтів SSH і CIPE. Наприклад, щоб дозволити віддалений доступ SSH, можна використовувати наступні правила:

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p udp --sport 22 -j ACCEPT
```

Наступні правила дозволяють встановлювати CIPE-з'єднання зовні (замініть x номером вашого пристрою):

```
iptables -A INPUT -p udp -i cipcbx -j ACCEPT
iptables -A OUTPUT -p udp -o cipcbx -j ACCEPT
```

Так як в CIPE використовується власний віртуальний пристрій, що передає UDP-пакети, з'єднання з інтерфейсом cipcb дозволяється цим правилом, а не правилом, що відкриває порти джерела і одержувача (хоча їх можна використовувати замість вказаного пристрою).

Поява розподілених архітектур у якомусь змісті відкинуло всю індустрію адміністрування тому, оскільки на початку цієї епохи задача керування обмежувалися контролем за функціонуванням окремих компонентів (мережного устаткування, персональних комп'ютерів і робочих станцій, запам'ятовуючих пристроїв, периферії та ін.), причому в багатьох випадках справа зводилася до простого збору даних про ресурси замість справжнього керування їхньою роботою. Цей перехідний тип керування ще не можна віднести до мережного адміністрування в суворому значенні цього слова. Останнє виникло тільки тоді, коли в адміністратора з'явилася можливість оперувати єдиним представленням мережі. Одночасно був зроблений перехід від управління функціонуванням окремих пристроїв до аналізу трафіка в окремих ділянках мережі, керування її логічною конфігурацією і конкретними робочими параметрами, причому всі ці операції можна було виконувати з однієї керуючої консолі.

Якщо слідувати траєкторії історичного розвитку засобів адміністрування, то наступний крок полягав у реалізації функцій управління інформаційними системами в цілому, а це означало, що в перелік контрольованих об'єктів додалися мережні операційні системи, розподілені бази даних і сховища даних, додатки і, нарешті, самі користувачі.

Нові проблеми, що виникли в розподілених середовищах, призвели до того, що на якийсь час мережне управління стало розглядатися в якості головної турботи адміністраторів інформаційних систем. Системне ж адміністрування при цьому як би відійшло на другий план, а відповідний інструментарій фігурував у якості автономних служб, чужих стосовно платформ і додатків мережного управління. Ця інверсія, що не цілком відповідає логіці функціонування корпоративних інформаційних систем (оскільки мережа відіграє роль лише допоміжної інфраструктури), зберігалася протягом декількох років.

Ситуація змінилася ще раз після того, як кількість розподілених додатків, і насамперед баз даних, функціонуючих у мережі, перейшло за деяке граничне значення. Зростання ролі системного адміністрування в такій ситуації було цілком природним.

Неминучим виявився й інший процес - інтеграція системного і мережного адміністрування, що змусила провідних виробників терміново модернізувати свої продукти. Проте і тут не обійшлося без перегинів: мережне адміністрування часом стало розглядатися як одна з множини складових частин системного адміністрування, а мережа - як один із керованих ресурсів поряд із комп'ютерами, периферійними пристроями, базами даних, додатками і т.і.

Питання про те, яка подальша доля цих двох областей управління корпоративними ІС, по якому шляху – інтеграційному, або дезінтеграційному піде їхній розвиток, поки залишається відкритим. Варто врахувати, що кінцевою метою всіх процедур управління є досягнення таких параметрів функціонування інформаційних систем, що відповідали би потребам користувачів. Останні ж оцінюють роботу ІС не по характеристиках мережного трафіка, застосовуваним протоколам, часу відгуку серверів на запити визначеного типу й особливостям виконуваних сценаріїв управління, а по поводженню додатків, що щодня запускаються на робочих станціях. Цей факт дає підстави ряду експертів припустити, що на зміну мережному і системному адмініструванню в майбутньому прийде управління додатками і якістю сервісу, незалежно від використовуваних платформ, та мереж.

4. Створення правил фаєрволу IPTable для корпоративних мереж

Не пустити віддалених зловмисників в локальну мережу - одна з найважливіших задач мережевої безпеки, якщо не найважливіша. Цілісність мережі повинна бути захищена від віддалених зловмисників за допомогою точних правил брандмауера. Однак, так як політика за замовчуванням блокує всі вхідні, вихідні пакети, що пересилаються , брандмауер / шлюз і користувачі локальної мережі не здатні встановити з'єднання один з одним або з зовнішнім світом. Щоб користувачі виконували пов'язані з мережею функції і використовували мережеві програми, адміністратори повинні відкрити певні порти. Наприклад, щоб дозволити доступ до 80 порту брандмауера, додайте наступне правило:

```
iptables -A INPUT -p tcp -m tcp --sport 80
-j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 80
-j ACCEPT
```

Це дозволить переглядати веб-вміст сайтів, що працюють на порту 80. Щоб відкрити доступ до захищених веб-сайтів (наприклад, https://www.example.com/), ви також повинні відкрити порт 443.

```
iptables -A INPUT -p tcp -m tcp --sport 443
-j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport
443 -j ACCEPT
```

Іноді потрібно організовувати віддалений доступ до локальної мережі зовні. Для шифрування з'єднання з віддаленою мережею можуть використовуватися захищені служби, наприклад, SSH і CIPE. Адміністратори мереж з

Команда	-P **,** --policy
Приклад	iptables -P INPUT DROP
Опис	Визначає політику по-замовчуванню для заданого ланцюжка. Політика по-замовчуванню визначає дію, що застосовується до пакетів, які не потрапили під дію жодного з правил у ланцюжку. Як політика за замовчуванням допускається використовувати DROP і ACCEPT.
Команда	-E **,** --rename-chain
Приклад	iptables -E allowed disallowed
Опис	Команда-E виконує перейменування користувача ланцюжка. У прикладі ланцюжок allowed буде перейменований в ланцюжок disallowed. Ці перейменування не змінюють порядок роботи, а носять лише косметичний характер.

Команда повинна бути вказана завжди. Список доступних команд можна переглянути за допомогою команди iptables-h або, що теж саме, iptables – help.

1. Основні принципи побудови та функціонування комп'ютерних мереж

1.1. Основні типи комп'ютерних мереж

Комп'ютерні мережі можна умовно поділити на локальні, регіональні та глобальні. Мережі часто розподіляють на три основних типи залежно від розміру географічної території, яку вони охоплюють. Невелика площа, як правило, пов'язується з терміном локальна обчислювальна мережа - ЛОМ. Великі площі пов'язують з термінами регіональна обчислювальна мережа та глобальна обчислювальна мережа - ГОМ. а) Локальні мережі. Якщо мережа прив'язана до одного місця (як правило, однієї установи чи комплексу різноманітних установ), то вона називається локальною обчислювальною мережею ~ ЛОМ. ЛОМ пов'язує комп'ютерні системи і периферійні пристрої (накопичувачі на жорстких магнітних дисках, принтери тощо) під управлінням мережевої операційної системи та прикладного програмного забезпечення в групи, які розподіляють дані і периферійні пристрої на відстані від 1-2 км. Метою створення ЛОМ є можливість сумісного використання комп'ютерних ресурсів - файлів, дисків та інших пристроїв. Комп'ютерні мережі призначені для передачі інформації, тому важливою характеристикою є якість та швидкість передачі даних. Швидкість вимірюється в бодах або в бітах за секунду (1 біт/с = 1 бод). Кратні одиниці - кілобод, мегабод, гігабод тощо. Крім того, серед основних характеристик мереж важливими є: - надійність; - продуктивність; - вартість; - операційні можливості. Характерною рисою ЛОМ є велика швидкість передачі даних, низький рівень помилок та використання дешевого середовища передачі даних. Однорангові мережі не мають виділеного сервера, який би відповідав за адміністрування всієї мережі, не мають ієрархії серед комп'ютерів, тобто

користувачі самі визначають, які ресурси на власному комп'ютері зробити загальнодоступними. Багаторангові мережі працюють на основі виділеного сервера, який дозволяє адмініструвати комп'ютери, які підключені до локальної мережі. б) Регіональні обчислювальні мережі. Регіональна обчислювальна мережа – новий тип мережі, який має багато спільного з локальними, але за багатьма параметрами більш складний та комплексний. ЛОМ можуть входити до складу регіональних. Наприклад, в додаток до підтримки обміну даними дозволяють голосовий та обмін відео- й аудіоінформацією. Регіональні мережі розроблені для підтримки великих відстаней. Можуть бути використані для зв'язку декількох локальних мереж в інтегровані мережеві системи. Вони поєднують у собі найкращі характеристики локальної мережі (низький рівень помилок, велика швидкість передачі даних) з великою географічною поширеністю. Регіональні мережі використовують технології глобальних мереж для об'єднання локальних мереж у конкретному географічному регіоні, наприклад у місті. в) Глобальна мережа поширюється на країни. Комунікації здійснюються в основному засобами телефонних мереж. Глобальна мережа створюється шляхом з'єднання локальних мереж і регіональних мереж. Досить часто поєднуються різні технології. В порівнянні з локальною та регіональною мережами глобальні мережі мають меншу швидкість передачі даних та більший рівень помилок. При з'єднанні двох та більше мереж між собою виникає міжмережеве об'єднання та утворюється глобальна комп'ютерна мережа, яка може охоплювати місто, область, країну, континент та всю земну кулю, а може охоплювати географічно всю країну, але не всіх її громадян. Наприклад, Міністерство освіти може мати свою мережу, Міністерство торгівлі - свою. Географічно ці мережі поширені на всю країну, але не перетинаються. Через настільний комп'ютер глобальна мережа може надати інформацію в будь-яку точку світу. Глобальні мережі звичайно не створюються з

	додати, що якщо не вказана таблиця ключом-t (-table), то очищення ланцюжків роблять лише в таблиці filter
Команда	-Z **,** --zero
Приклад	iptables -Z INPUT
Опис	Обнулення всіх лічильників в заданому ланцюжку. Якщо ім'я ланцюжка не вказується, то маються на увазі всі ланцюжки. При використанні ключа-v спільно з командою-L, на висновок буде подано стан лічильників пакетів, що потрапили під дію кожного правила. Допускається спільне використання команд-L і-Z. У цьому випадку буде виданий спочатку список правил з лічильниками, а потім відбудеться обнулення лічильників.
Команда	-N **,** --new-chain
Приклад	iptables -N allowed
Опис	Створюється новий ланцюжок з заданим ім'ям в заданій таблиці. У вище наведеному прикладі створюється новий ланцюжок з ім'ям allowed. Ім'я ланцюжка повинно бути унікальним і не має збігатися з зарезервованими іменами ланцюжків і дій (такими як DROP, REJECT і т.п.)
Команда	-X **,** --delete-chain
Приклад	iptables -X allowed
Опис	Видалення заданого ланцюжка з заданої таблиці. Видаляємий ланцюжок не повинен мати правил і не повинно бути посилань з інших ланцюжків на видаляємий ланцюжок. Якщо ім'я ланцюжка не зазначено, то будуть видалені всі ланцюжки заданої таблиці крім вбудованих.

	правило з заданим номером. Рахунок правил у ланцюжках починається з 1.
Команда	-R **,** --replace
Приклад	iptables -R INPUT 1 -s 192.168.0.1 -j DROP
Опис	Ця команда замінює одне правило іншим. В основному вона використовується під час налагодження нових правил.
Команда	-I **,** --insert
Приклад	iptables -I INPUT 1 --dport 80 -j ACCEPT
Опис	Вставляє нове правило в ланцюжок. Число, наступне за ім'ям ланцюжка вказує номер правила, перед яким потрібно вставити нове правило, іншими словами число задає номер для вставлення правила. У прикладі вище, вказується, що дане правило має бути 1-м у ланцюжку INPUT.
Команда	-L **,** --list
Приклад	iptables -L INPUT
Опис	Виведення списку правил в заданому ланцюжку, в даному прикладі передбачається висновок правил з ланцюжка INPUT. Якщо ім'я ланцюжка не вказується, то виводиться список правил для всіх ланцюжків. Формат виведення залежить від наявності додаткових ключів у команді, наприклад-n,-v, і пр.
Команда	-F **,** --flush
Приклад	iptables -F INPUT
Опис	Скидання (видалення) всіх правил з заданого ланцюжка (таблиці). Якщо ім'я ланцюжка і таблиці не вказується, то видаляються всі правила, у всіх ланцюжках. (Хочеться від себе

нуля, бо таке рішення неефективне по затратах. Замість цього глобальні мережі надають сполучення існуючих локальних обчислювальних мереж, міських мереж тощо, створюючи мережі неймовірної складності з різноманітними середовищами передачі даних, різноманітними протоколами, що використовуються, різними прикладними програмами. Глобальні мережі повинні об’єднати велику кількість технологій, наведених сьогоднішніми мережами в погоджене оточення користувача. Причому об’єднати мережі різного роду набагато складніше. Прикладом глобальної мережі є мережа Інтерет. Internet - найбільша глобальна комп’ютерна мережа, що зв’язує десятки мільйонів абонентів у більш як 150 країнах світу. Щомісяця її поширеність зростає на 7-10%. Internet утворює немовби ядро, яке забезпечує, взаємодію інформаційних мереж, що належать різним установам у всьому світі. Якщо раніше вона використовувалася виключно як середовище для передачі файлів і повідомлень електронної пошти, то сьогодні вирішуються більш складні завдання, які підтримують функції мережного пошуку та доступу до розподілених інформаційних ресурсів й електронних архівів. Таким чином, Internet можна розглядати як деякий глобальний інформаційний простір. Мережа Internet, що служила спочатку дослідницьким і навчальним групам, стає все популярнішою в ділових колах. Компанії спокушують дешевий глобальний зв’язок і його швидкість, зручність для проведення сумісних робіт, доступні програми, унікальна база даних цієї мережі. Вони розглядають глобальну комп’ютерну мережу як доповнення до своїх власних локальних мереж. Уже кілька років розвиваються і встигли широко ввійти в практику в розвинених країнах технології Intranet, що є інформаційними технологіями великої мережі в корпоративних мережах і навіть у дуже невеликих мережах ПК підприємств малого бізнесу. При низькій вартості послуг (часто це тільки фіксована щомісячна плата за лінії зв’язку або телефон) користувачі можуть дістати

доступ до комерційних і некомерційних інформаційних служб США, Канади, Австралії, європейських країн, а тепер уже України та Росії. В архівах вільного доступу мережі Internet можна знайти інформацію практично з усіх сфер людської діяльності, починаючи з нових наукових відкриттів до прогнозу погоди на завтра. В Internet можна знайти рекламу багатьох тисяч фірм і розмістити (часто безкоштовно!) свою рекламу. Крім того, Internet надає унікальні можливості дешевого, надійного та конфіденційного глобального зв'язку. Це виявляється дуже зручним для фірм, що мають свої філіали по всьому світу, транснаціональних корпорацій і структур управління. Як правило, використання інфраструктури Internet для міжнародного зв'язку коштує набагато дешевше від прямого комп'ютерного зв'язку через супутниковий канал або телефон.

Таблиця	Опис
	програмами на самому брандмауері.

Вище ми розглянули основні відмінності трьох наявних таблиць. Кожна з них повинна використовуватися тільки в своїх цілях, і ви повинні це розуміти. Нецільове використання таблиць може привести до ослаблення захисту брандмауера і мережі, що знаходиться за ним.

Нижче наводиться список команд та правила їх використання. За допомогою команд ми повідомляємо iptables що ми припускаємо зробити. Звичайно передбачається одне з двох дій - додавання нового правила в ланцюжок чи видалення існуючого правила із творців тієї чи іншої таблиці. Далі наведено команди, які використовуються в iptables.

Таблиця 4. Команди

Команда	-A **,** --append
Приклад	iptables -A INPUT ...
Опис	Додає нове правило в кінець заданої ланцюжка.
Команда	-D **,** --delete
Приклад	iptables -D INPUT --dport 80 -j DROP **,** iptables -D INPUT 1
Опис	Видалення правила з ланцюжка. Команда має два формати запису, перший - коли задається критерій порівняння з опцією-D (див. перший приклад), другий - порядковий номер правила. Якщо задається критерій порівняння, то видаляється правило, яке має в собі цей критерій, якщо задається номер правила, то буде видалено

Таблиця	Опис
mangle	тільки на даному брандмауері) можуть використовувати це поле в своїх цілях . Таблиця має п'ять ланцюжків PREROUTING, POSTROUTING, INPUT, OUTPUT і FORWARD. PREROUTING використовується для внесення змін на вході в брандмауер, перед прийняттям рішення по маршрутизації. POSTROUTING використовується для внесення змін на виході з брандмауера, після прийняття рішення по маршрутизації. INPUT - для внесення змін у пакети перед тим як вони будуть передані локальному додатку всередині брандмауера. OUTPUT - для внесення змін в пакети, що надходять від додатків всередині брандмауера. FORWARD - для внесення змін до транзитних пакетів після першого прийняття рішення по маршрутизації, але перед останнім прийняттям рішення про маршрутизації. Зауважу, що таблиця mangle ні в якому разі не повинна використовуватися для перетворення мережевих адрес або маскорадінг (Network Address Translation, Masquerading), оскільки для цих цілей є таблиця nat.
filter	Таблиця filter використовується головним чином для фільтрації пакетів. Для прикладу, тут ми можемо виконати DROP, LOG, ACCEPT або REJECT без обмежень, які є в інших таблицях. Є три вбудованих ланцюжка. Перший - FORWARD, який використовується для фільтрації пакетів, що йдуть транзитом через брандмауер. Ланцюжок INPUT проходять пакети, які призначені локальними програмами (брандмауером). І ланцюжок OUTPUT - використовується для фільтрації вихідних пакетів, згенерованих

1.2. Середовище передавання у комп'ютерних мережах

Техніко-експлуатаційні характеристики середовищ передавання такі: час і швидкість розповсюдження сигналів, вартість, швидкість загасання на одиницю довжини кабелю з урахуванням його частоти, опір одного метра, маса одного метра, завадостійкість у різних навколишніх середовищах, випромінювання в довкілля.

На даний час використовується велика кількість кабелів різних типів (більше 2200). Однак на практиці використовують 3 основні групи кабелів:

1) коаксіальний
2) скручена пара (вита пара)
3) волоконно-оптичний

Коаксіальний кабель. Поряд зі скрученою парою є найпоширенішим середовищем передавання даних у КМ. Вони мають високу швидкість передавання, завадостійкість, довговічність, помірну вартість. Для них розроблені прості засоби спряження з локальними мережами.

Коаксіальний кабель використовується для з'єднання комп'ютерів за топологією шина. Це з'єднання є найпростішим і не вимагає додаткового обладнання.

Тонкий коаксіальний кабель використовується для локальних мереж із загальною довжиною 185м, має товщину о,5 см.

Товстий коаксіальний кабель застосовується для з'єднання декількох сегментів мережі, має товщину 1см і може передавати сигнали на відстань 500м. Для з'єднання за допомогою товстого кабелю використовують додатковий пристрій Вампера.

Для з'єднання використовують роз'єми: тонкий – BNC, твстий – AUI. Термін експлуатації 10-12років.

Скручена пара дротів. Цей тип кабелю є найдешевшим і найпоширенішим. Максимальна відстань передавання у ньому 1,5-2,0км, максимальна швидкість – 1,2Гбіт/с. має гірший, ніж у коаксіальному кабелі, захист від

завад. Тривалість поширення сигналу 8-12нс/м. Термін експлуатації – 2-6років. Канал найдешевший в укладанні. Сьогодні скручена пара є головним середовищем передавання у локальних мережах.

Розрізняють декілька типів скручених пар: неекрановану –вона найдешевша, однак під час експлуатації виникають проблеми з EMI; екрановану.

Волоконно-оптичний кабель. У цих кабелях як фізичне середовище використовують прозоре скловолокно.швидкість передавання сигналів кабелем 0,2-1,0 Гбіт/с. Теоретично можлива максимальна швидкість передавання – 200Гбіт/с Довжина сполучень 110км.

Тут значно менше (порівняно з коаксіальним) загасання сигналів, вища швидкість передавання,широка частотна смуга передавання, вони не чутливі до електромагнітних завад. Водночас такі кабелі мають малу механічну стійкість, їх не можна гнути, терти, пересувати, вони не витримують вібрації. Сьогодні волоконно-оптичні кабелі вважають найперспективнішими для нової АТМ технології передавання даних, побудови магістральних інформаційних мереж.

запис у таблиці, оскільки для даного з'єднання було отримано повідомлення про помилку.

Опція **-t** вказує на використану таблицю. По замовчуванню застосовується таблиця *filter* . З ключом **-t** застосовуються слідуюючі опції.

Таблиця 3.

Таблиця	**Опис**
nat	Таблиця nat використовується головним чином для перетворення мережевих адрес (Network Address Translation). Через цю таблицю проходить тільки перший пакет з потоку. Перетворення адрес автоматично застосовується до всіх наступних пакетів. Це один з факторів, виходячи з яких ми не повинні здійснювати будь-яку фільтрацію в цій таблиці. Ланцюжок PREROUTING використовується для внесення змін в пакети на вході в брандмауер. Ланцюжок OUTPUT використовується для перетворення адрес у пакетах, створених додатками всередині брандмауера, перед прийняттям рішення по маршрутизації. І останній ланцюжок в цій таблиці - POSTROUTING, яка використовується для перетворення пакетів перед видачею їх у мережу.
	Ця таблиця використовується для внесення змін в заголовки пакетів. Прикладом може служити зміна поля TTL, TOS чи MARK. Важливо: насправді поле MARK не змінюється, але в пам'яті ядра заводиться структура, яка супроводжує даний пакет весь час його проходження через брандмауер, так що інші правила та програми на даному брандмауері (і

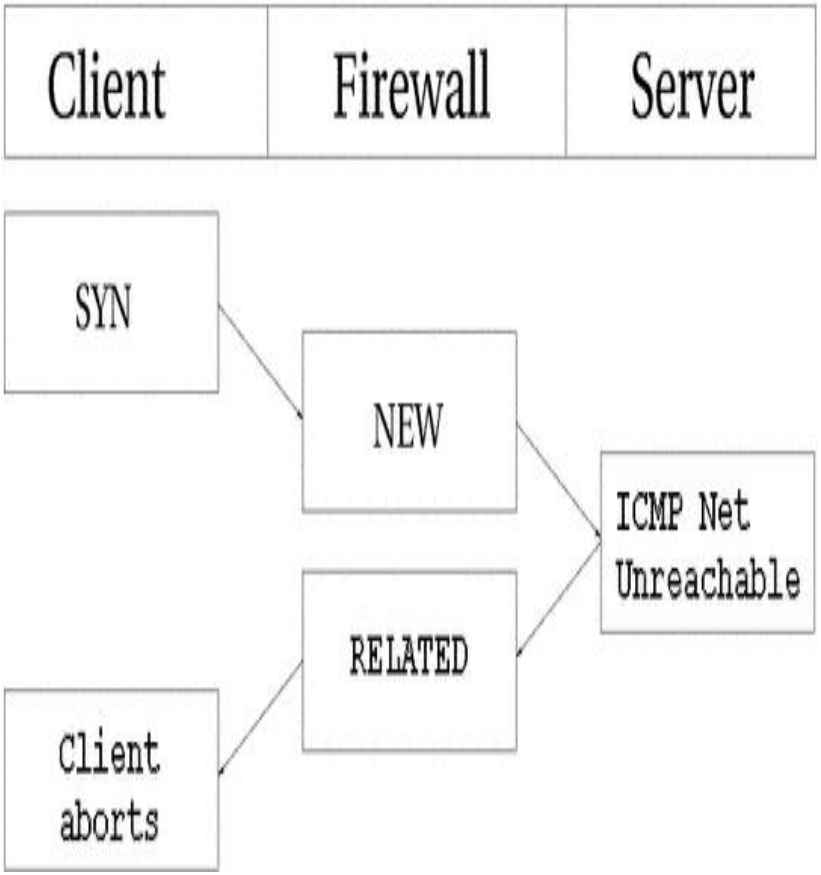


Рис.11. Передача запиту на з'єднання

У цьому прикладі деякого вузла передається запит на з'єднання *(SYN* пакет). Він набуває статусу NEW на брандмауері. Однак, у цей момент часу, мережа виявляється недоступною, тому роутер повертає пакет *ICMP Network Unreachable.* Трасувальник сполук розпізнає цей пакет як RELATED, завдяки вже наявної записи в таблиці, так що пакет благополучно буде переданий клієнту, який потім обірве невдале з'єднання. Тим часом, брандмауер знищить

1.3. Структура операційно мережевих систем

Мережева операційна система становить основу будь-якої обчислювальної мережі. Кожен комп'ютер в мережі значною мірою автономний, тому під мережевою операційною системою в широкому сенсі розуміється сукупність операційних систем окремих комп'ютерів, які взаємодіють з метою обміну повідомленнями і поділу ресурсів за єдиними правилами - протоколами. У вузькому сенсі мережева ОС - це операційна система окремого комп'ютера, що забезпечує йому можливість працювати в мережі.

Рис. 1. Структура мережевої ОС

Засоби управління локальними ресурсами комп'ютера: функції розподілу оперативної пам'яті між процесами, планування та диспетчеризації процесів, управління процесорами в мультипроцесорних машинах, управління периферійними пристроями та інші функції управління ресурсами локальних ОС.

Засоби надання власних ресурсів та послуг у спільне користування - серверна частина ОС (сервер). Ці кошти забезпечують, наприклад, блокування файлів і записів, що необхідно для їх спільного використання; ведення довідників імен мережевих ресурсів; обробку запитів віддаленого доступу до власної файлової системи і бази даних; управління чергами запитів віддалених користувачів до своїх периферійних пристроїв. Засоби запиту доступу до віддалених ресурсів і послуг і їх використання - клієнтська частина ОС (редиректор). Ця частина виконує розпізнавання і перенаправлення в мережу запитів до віддалених ресурсів від додатків і користувачів, при цьому запит поступає від програми в локальній формі, а передається в мережу в іншій формі, що відповідає вимогам сервера. Клієнтська частина також здійснює прийом відповідей від серверів і перетворення їх у локальний формат, так що для програми виконання локальних і віддалених запитів невиразне. Комунікаційні засоби ОС, за допомогою яких відбувається обмін повідомленнями в мережі. Ця частина забезпечує адресацію і буферизацію повідомлень, вибір маршруту передачі повідомлення по мережі, надійність передачі і т.і., тобто є засобом транспортування повідомлень. У залежності від функцій, покладених на конкретний комп'ютер, в його операційній системі може бути відсутнім або клієнтська, або серверна частини. На рис. 4.2 показано взаємодію мережевих компонентів. Тут комп'ютер 1 виконує роль "чистого" клієнта, а комп'ютер 2 -

проходження відповіді через netfilter, запис в таблиці трасувальника знищується.

У будь-якому випадку запит розглядається як NEW, а відповідь як ESTABLISHED.

ICMP запити мають таймаут, по-замовчуванню, 30 секунд. Цього часу, в більшості випадків, цілком достатньо. Час таймауту можна змінити в `/proc/sys/net/ipv4/netfilter/ip_ct_icmp_timeout`. (Нагадую, що змінні типу `/proc/sys/net/ipv4/netfilter/ip_ct_*` стають доступні лише після інсталяції tcp-window-tracking з patch-o-matic

Значна частина *ICMP* використовується для передачі повідомлень про те, що відбувається з тим чи іншим *UDP* або *TCP* з'єднанням. У зв'язку з цим вони дуже часто розпізнаються як пов'язані (RELATED) з існуючим з'єднанням. Простим прикладом можуть служити повідомлення *ICMP Host Unreachable* або *ICMP Network Unreachable.* Вони завжди породжуються при спробі з'єднатися з вузлом мережі коли цей вузол або мережа недоступні, в цьому випадку останній маршрутизатор поверне відповідний *ICMP* пакет, який буде розпізнаний як RELATED. На малюнку нижче показано як це відбувається.

Як видно з цього рисунка, сервер виконує *Echo Request* (луна-запит) до клієнта, який (запит) розпізнається брандмауером як NEW. На цей запит клієнт відповідає пакетом *Echo Reply,* і тепер пакет розпізнається як такий, що має стан ESTABLISHED. Після проходження першого пакету *(Echo Request)* в `ip_conntrack` з'являється запис:

```
 icmp 25 січня src = 192.168.1.6 dst =
192.168.1.10 type = 8 code = 0 \
 id = 33029 [UNREPLIED] src = 192.168.1.10
dst = 192.168.1.6 \
      type = 0 code = 0 id = 33029 use = 1
```

Цей запис дещо відрізняється від записів, властивих протоколам *TCP* і *UDP,* хоча точно так же присутні і назва протоколу і час таймауту і адреси передавача і приймача, але далі з'являються три нових поля - `type, code` і `id.` Поле `type` містить тип *ICMP,* поле `code` - код *ICMP.* Значення типів і кодів *ICMP* наводяться в додатку *Типи ICMP* . І останнє поле `id` містить ідентифікатор пакету. Кожен *ICMP-пакет* має свій ідентифікатор. Коли приймач, у відповідь на *ICMP-запит* посилає відповідь, він підставляє в пакет відповіді цей ідентифікатор, завдяки чому, передавач може коректно розпізнати у відповідь на який запит надійшла відповідь.

Наступне поле - прапор `[UNREPLIED],` який зустрічався нам раніше. Він означає, що прибув перший пакет в з'єднанні. Завершується запис характеристиками очікуваного пакета відповіді. Сюди включаються адреси відправника і одержувача. Що стосується типу та коду *ICMP* пакета, то вони відповідають правильним значенням очікуваного пакета *ICMP Echo Reply.* Ідентифікатор пакета-відповіді той же, що і в пакеті запиту.

Пакет відповіді розпізнається вже як ESTABLISHED. Однак, ми знаємо, що після передачі пакета відповіді, через це з'єднання вже нічого не очікується, тому після

роль "чистого" сервера, відповідно на першій машині відсутня серверна частина, а на другий - клієнтська. На малюнку окремо показаний компонент клієнтської частини - редиректор. Саме редиректор перехоплює всі запити, які постуають від додатків, і аналізує їх. Якщо виданий запит до ресурсу даного комп'ютера, то він переадресовується відповідної підсистемі локальної ОС, якщо ж це запит до віддаленого ресурсу, то він переправляється в мережу. При цьому клієнтська частина перетворює запит з локальної форми в мережевий формат і передає його транспортній підсистемі, яка відповідає за доставку повідомлень вказаному серверу. Серверна частина операційної системи комп'ютера 2 приймає запит, перетворює його і передає для виконання своєї локальної ОС. Після того, як результат отриманий, сервер звертається до транспортної підсистеми і направляє відповідь клієнту, який видав запит. Клієнтська частина перетворює результат у відповідний формат і адресує його тому додатку, який видав запит.

На практиці склалося кілька підходів до побудови мережевих операційних систем.

Перші мережеві ОС представляли собою сукупність існуючої локальної ОС і надбудованої над нею мережевої оболонки. При цьому в локальну ОС вбудовувався мінімум мережевих функцій, необхідних для роботи мережевої оболонки, яка виконувала основні мережеві функції. Прикладом такого підходу є використання на кожній машині мережі операційної системи MS DOS (у якої починаючи з її третьої версії з'явилися такі вбудовані функції, як блокування файлів і записів, необхідних для спільного доступу до файлів).

Принцип побудови мережевих ОС як мережевої оболонки над локальної ОС використовується і в сучасних ОС, таких, наприклад, як LANtastic або Personal Ware.

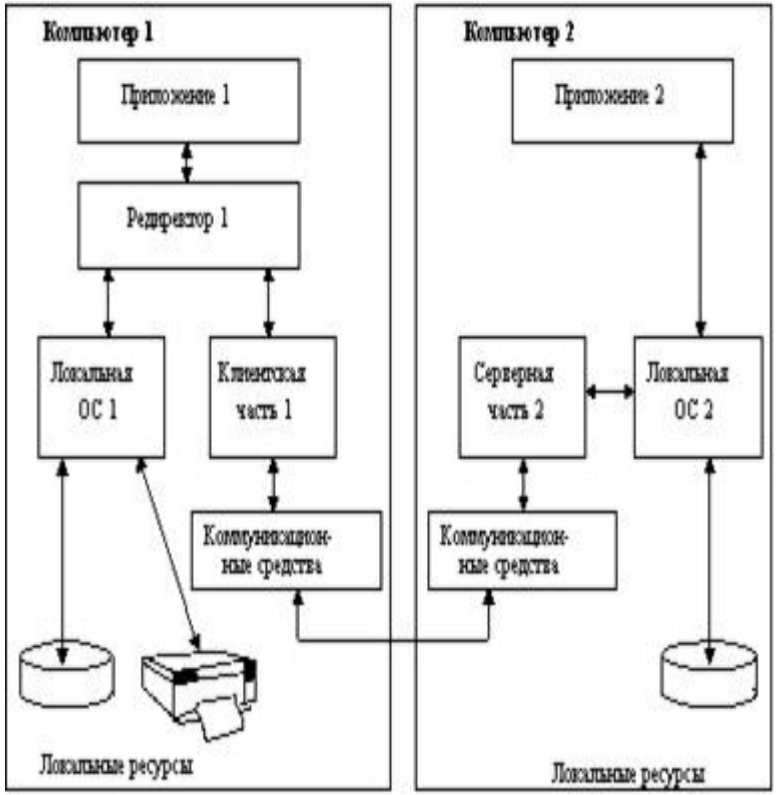


Рис. 2. Взаємодія компонентів операційної системи при взаємодії комп'ютерів

Однак більш ефективним є шлях розробки операційних систем, спочатку призначених для роботи в мережі. Мережеві функції у ОС такого типу глибоко вбудовані в основні модулі системи, що забезпечує їх логічну стрункість, простоту експлуатації та модифікації, а також високу продуктивність. Прикладом такої ОС є система Windows NT фірми Microsoft, яка за рахунок вбудованості мережевих засобів забезпечує більш високі показники продуктивності та захищеності інформації в

ICMP пакети використовуються тільки для передачі керуючих повідомлень і не організують постійного з'єднання. Однак, існує 4 типи *ICMP* пакетів, які викликають передачу відповіді, тому вони можуть мати два стани: NEW і ESTABLISHED. До цих пакетів ставляться *ICMP Echo Request / Echo Reply, ICMP Timestamp Request / Timestamp Reply, ICMP Information Request / Information Reply* і *ICMP Address Mask Request / Address Mask Repl* у. З них - *ICMP Timestamp Request / Timestamp Reply* і *ICMP Information Request / Information Reply* вважаються застарілими і тому, в більшості випадків, можуть бути безболісно скинуті (DROP). Погляньте на малюнок нижче.

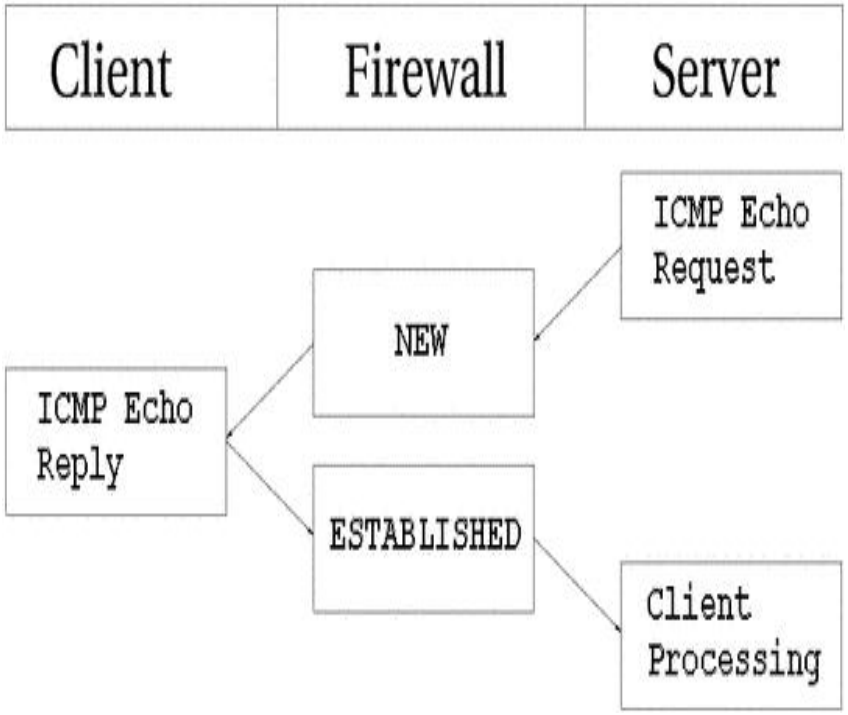


Рис.10. Передача керуючих повідомлень

часом", яке дає можливість пройти пакетам, "загрузлим" на тому чи іншому маршрутизаторі (роутері).

Якщо з'єднання закривається після отримання пакета *RST,* то воно перетворюється на стан `CLOSE`. Час очікування до фактичного закриття з'єднання за замовчуванням встановлюється рівним 10 секунд. Підтвердження на пакети *RST* не передається і з'єднання закривається відразу ж. Крім того є ряд інших внутрішніх станів. У таблиці нижче наводиться список можливих внутрішніх станів з'єднання та відповідні їм розміри таймаутів.

Таблиця 2. Internal states

Стан	**Час очікування**
NONE	30 хвилин
ESTABLISHED	5 днів
SYN_SENT	2 хвилини
SYN_RECV	60 секунд
FIN_WAIT	2 хвилини
TIME_WAIT	2 хвилини
CLOSE	10 секунд
CLOSE_WAIT	12:00
LAST_ACK	30 секунд
LISTEN>	2 хвилини

Ці значення можуть дещо змінюватися від версії до версії ядра, крім того, вони можуть бути змінені через інтерфейс файлової системи `/ proc` (змінні `proc/sys/net/ipv4/netfilter/ip_ct_tcp_ *)`.

Значення встановлюються в сотих долях секунди, так що число 3000 означає 30 секунд.

порівнянні з мережевою ОС LAN Manager тієї ж фірми (спільна розробка з IBM), що є надбудовою над локальною операційною системою OS / 2 . Однорангові мережні ОС і ОС з виділеними серверами. У залежності від того, як розподілені функції між комп'ютерами мережі, мережеві операційні системи, а отже, і мережі діляться на два класи: однорангові і двухрангові (рис. 4). Останні частіше називають мережами з виділеними серверами.

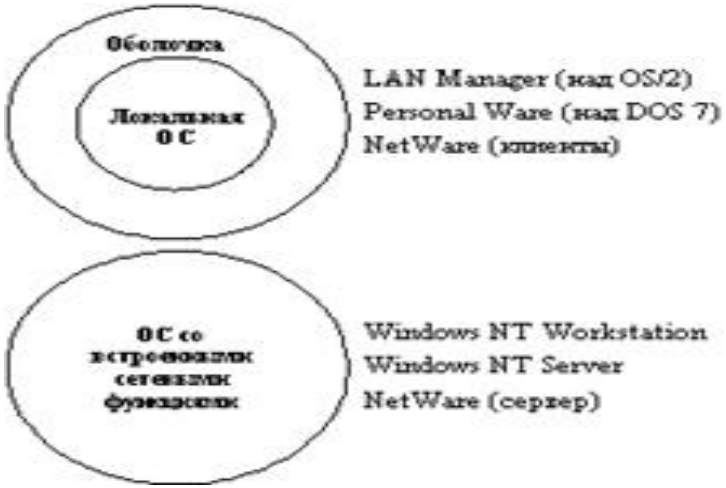
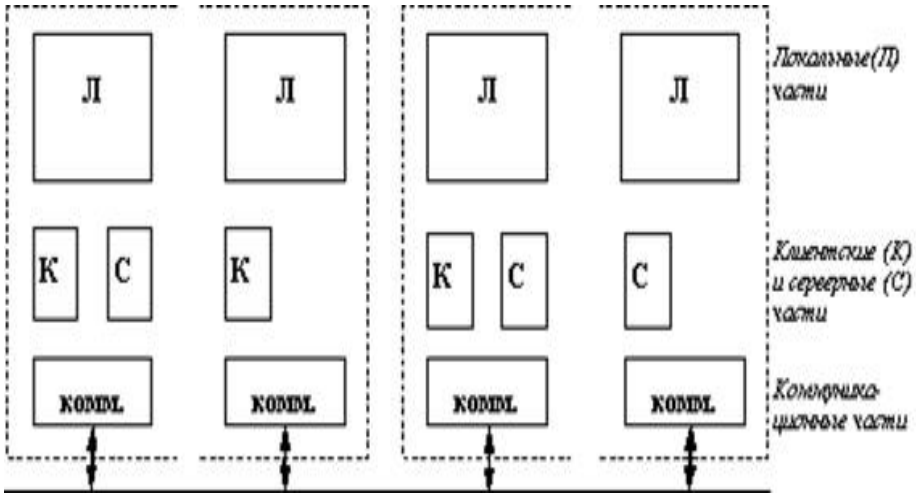


Рис. 3. Варіанти побудови мережних ОС

Якщо комп'ютер надає свої ресурси іншим користувачам мережі, то він грає роль сервера. При цьому комп'ютер, який звертається до ресурсів іншої машини, є клієнтом. Як вже було сказано, комп'ютер, що працює в мережі, може виконувати функції або клієнта, або сервера, або поєднувати обидві ці функції.



(А)

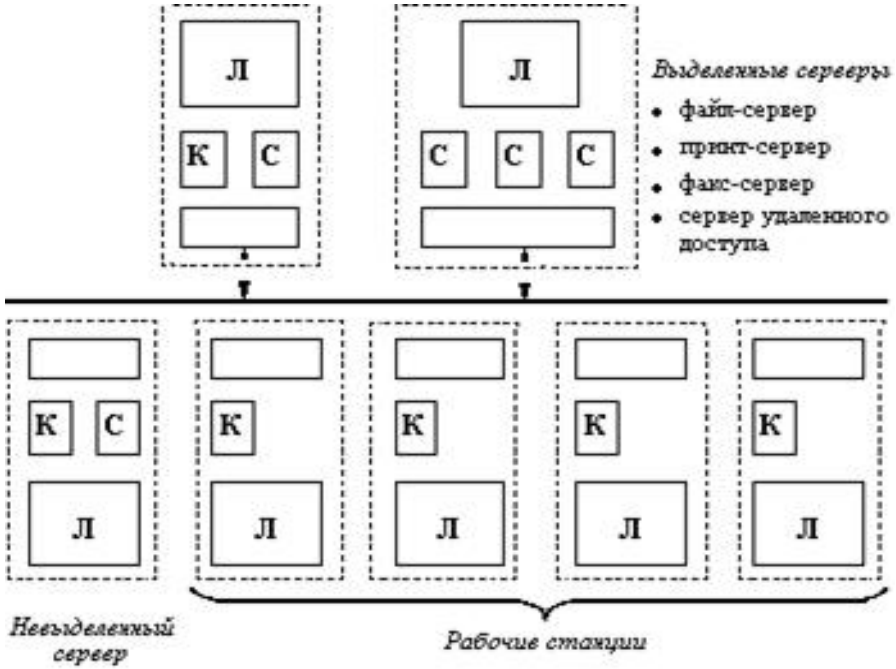


Рис. 4. (А) - Тимчасова мережа,

При закритті, *TCP* з'єднання проходить через наступні стани.

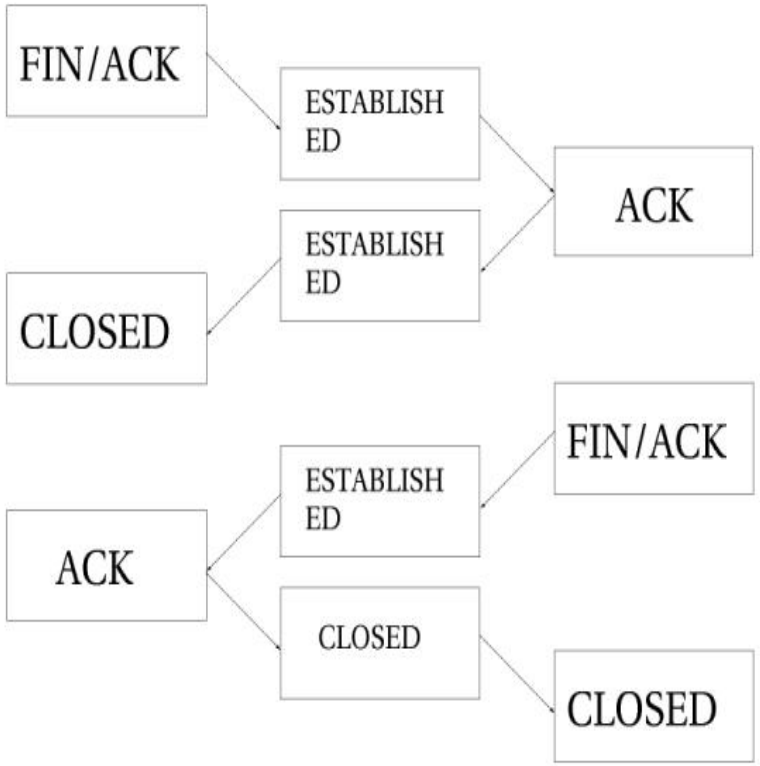


Рис.9. При закритті, TCP *з'єднання проходить через наступні стани*

Як видно з рис.9, з'єднання не закривається до тих пір поки не буде переданий останній пакет *ACK*. Зверніть увагу - ця картинка описує нормальний процес закриття з'єднання. Крім того, якщо з'єднання відкидається, то воно може бути закрите передачею пакета *RST* (скидання). У цьому випадку буде закрито по витіканню визначеного часу.

При закритті, з'єднання переводиться в стан `TIME_WAIT`, тривалість якого по-замовчуванню відповідає 2 хвилинам, протягом яких ще можливо проходження пакетів через брандмауер. Це є свого роду "буферним

```
tcp 6117 SYN_SENT src = 192.168.1.5 dst =
192.168.1.35 sport = 1031 \
dport = 23 [UNREPLIED] src = 192.168.1.35
dst = 192.168.1.5 sport = 23 \
dport = 1031 use = 1
```

Як бачите, запис у таблиці відображає точний стан з'єднання – він був відзначений факт передачі пакету SYN (прапор SYN_SENT), на який відповіді поки не було (прапор [UNREPLIED]). Після отримання пакета-відповіді, з'єднання перетворюється на такий внутрішній стан:

```
 tcp 6 57 SYN_RECV src = 192.168.1.5 dst =
192.168.1.35 sport = 1031 \
      dport = 23 src = 192.168.1.35 dst =
192.168.1.5 sport = 23 dport = 1031 \
      use = 1
```

Тепер запис повідомляє про те, що назад пройшов пакет *SYN / ACK*. На цей раз з'єднання переводиться в стан SYN_RECV. Цей стан говорить про те, що пакет *SYN* був благополучно доставлений одержувачу і у відповідь на нього прийшов пакет-підтвердження *(SYN / ACK)*. Крім того, механізм визначення стану "побачивши" пакети наступні в обох напрямках, знімає прапор [UNREPLIED]. І нарешті після передачі заключного *ACK-пакета,* в процедурі встановлення з'єднання

```
 tcp 6 431999 ESTABLISHED src = 192.168.1.5
dst = 192.168.1.35 \
 sport = 1031 dport = 23 src = 192.168.1.35
dst = 192.168.1.5 \
      sport = 23 dport = 1031 use = 1
```

з'єднання переходить в стан ESTABLISHED (встановлене). Після прийому кількох пакетів через це з'єднання, до нього додасться прапор [ASSURED] (впевнене).

Якщо комп'ютер надає свої ресурси іншим користувачам мережі, то він грає роль сервера. При цьому комп'ютер, який звертається до ресурсів іншої машини, є клієнтом. Як вже було сказано, комп'ютер, що працює в мережі, може виконувати функції або клієнта, або сервера, або поєднувати обидві ці функції.

Якщо виконання будь-яких серверних функцій є основним призначенням комп'ютера (наприклад, надання файлів у спільне користування всім іншим користувачам мережі або організація спільного використання факсу, або надання всім користувачам мережі можливості запуску на комп'ютері своїх додатків), то такий комп'ютер називається виділеним сервером. У залежності від того, який ресурс сервера розділяється, він називається файл-сервером, факс-сервером, принт-сервером, сервером додатків і т.і.

Очевидно, що на виділених серверах бажано встановлювати ОС, спеціально оптимізовані для виконання тих чи інших серверних функцій. Тому в мережах з виділеними серверами найчастіше використовують мережні операційні системи, до складу яких входить декілька варіантів ОС, відмінних можливостями серверних частин. Наприклад, мережева ОС Novell NetWare має серверний варіант, оптимізований для роботи як файл-сервера, а також варіанти оболонок для робочих станцій з різними локальними ОС, причому ці оболонки виконують виключно функції клієнта. Іншим прикладом ОС, орієнтованої на побудову мережі з виділеним сервером, є операційна система Windows NT. На відміну від NetWare, обидва варіанти даної мережевої ОС - Windows NT Server (для виділеного сервера) і Windows NT Workstation (для робочої станції) - можуть підтримувати функції і клієнта і сервера. Але серверний варіант Windows NT має більше можливостей для надання ресурсів свого комп'ютера іншим користувачам мережі, так як може виконувати більш широкий набір функцій, підтримує

більшу кількість одночасних з'єднань з клієнтами, реалізує централізоване управління мережею, має розвинені засоби захисту.

Виділений сервер не прийнято використовувати в якості комп'ютера для виконання поточних завдань, не пов'язаних з його основним призначенням, так як це може зменшити продуктивність його роботи як сервера. У зв'язку з такими міркуваннями в ОС Novell NetWare на серверній частині можливість нормального виконання прикладних програм взагалі не передбачена, тобто сервер не містить клієнтської частини, а на робочих станціях відсутні серверні компоненти. Однак в інших мережевих ОС функціонування на виділеному сервері клієнтської частини цілком можливо. Наприклад, під управлінням Windows NT Server можуть запускатися звичайні програми локального користувача, які можуть зажадати виконання клієнтських функцій ОС при появі запитів до ресурсів інших комп'ютерів мережі. При цьому робочі станції, на яких встановлена ОС Windows NT Workstation, можуть виконувати функції невиділеного сервера.

Важливо зрозуміти, що незважаючи на те, що в мережі з виділеним сервером всі комп'ютери в загальному випадку можуть виконувати одночасно ролі і сервера, і клієнта, ця мережа функціонально не симетрична: апаратно та програмно в ній реалізовані два типи комп'ютерів - одні, більшою мірою орієнтовані на виконання серверних функцій і працюють під управлінням спеціалізованих серверних ОС, а інші - в основному виконують клієнтські функції та працюють під управлінням відповідного цьому призначенню варіанти ОС. Функціональна несиметричність, як правило, викликає і несиметричність апаратури - для виділених серверів використовуються більш потужні комп'ютери з великими обсягами оперативної і зовнішньої пам'яті. Таким чином, функціональна несиметричність в мережах з виділеним сервером супроводжується

NEW пакетів в локальну мережу. З точки зору ядра все виглядає більш складним, оскільки в просторі ядра *TCP* з'єднання мають ряд проміжних станів, недоступних в просторі користувача. У загальних рисах вони відповідають специфікації *RFC 793 - Transmission Control Protocol*

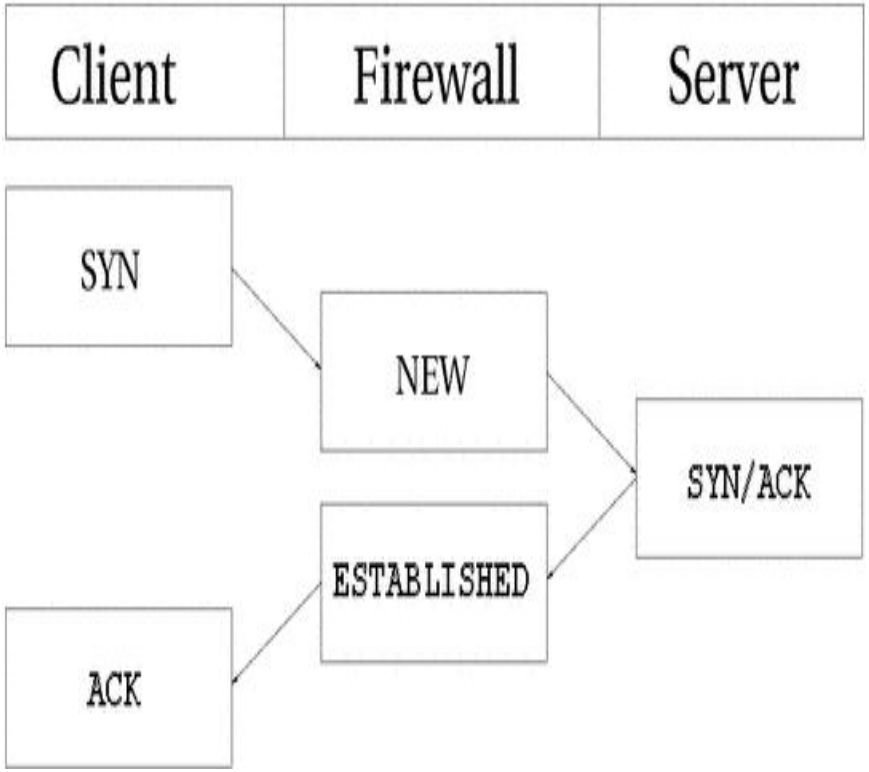


Рис 8. Стадії встановлення з'єднання

З точки зору користувача все виглядає досить просто, проте якщо подивитися з точки зору ядра, то все виглядає дещо складніше. Розглянемо порядок зміни стану з'єднання в таблиці `/ proc / net / ip_conntrack`. Після передачі першого пакету SYN.

доступ тільки для зворотного (відповідь) трафіку, припиняючи спроби встановлення з'єднань ззовні .

TCP з'єднання. У цьому і в наступних розділах ми ближче розглянемо ознаки станів і порядок їх обробки кожним з трьох базових протоколів *TCP, UDP* і *ICMP,* а так само торкнемося випадку, коли протокол з'єднання не може бути класифікований на приналежність до трьох, вищевказаних, протоколів. Почнемо розгляд з протоколу TCP, оскільки він має безліч цікавих особливостей щодо механізму визначення стану в iptables.

TCP з'єднання завжди встановлюється передачею трьох пакетів, які ініціалізують і встановлюють з'єднання, через яке в подальшому будуть передаватися дані. Сесія починається з передачі *SYN* пакета, у відповідь на який передається *SYN / ACK* пакет і підтверджує встановлення з'єднання пакет *ACK*. Після цього з'єднання вважається встановленим і готовим до передачі даних. Може виникнути питання: "А як же трасується з'єднання?". Насправді все досить просто.

Для всіх типів з'єднань, трасування проходить практично однаково. Погляньте на малюнок нижче, де показані всі стадії встановлення з'єднання. Як бачите, трасировщик, з точки зору користувача, фактично не стежить за ходом встановлення з'єднання. Просто, як тільки трассировщик "побачив" перший *(SYN)* пакет, то привласнює йому статус NEW. Як тільки через трасувальника проходить другий пакет *(SYN / ACK),* то з'єднанню присвоюється статус ESTABLISHED. Чому саме другий пакет? Зараз розберемося. Будуючи свій набір правил, ви можете дозволити залишати локальну мережу пакетів зі статусом NEW і ESTABLISHED, а по вхідному трафіку пропускати пакети тільки зі статусом ESTABLISHED і все буде працювати прекрасно. І навпаки, якби трасувальник продовжував вважати з'єднання як NEW, то фактично вам ніколи не вдалося б встановити з'єднання з "зовнішнім світом", або довелося б дозволити проходження

несиметричністю операційних систем (спеціалізація ОС) і апаратної несиметричністю (спеціалізація комп'ютерів).

У однорангових мережах всі комп'ютери рівні в правах доступу до ресурсів один до другого. Кожний користувач може за своїм бажанням оголосити який-небудь ресурс свого комп'ютера роздільчим, після чого інші користувачі можуть його експлуатувати. У таких мережах на всіх комп'ютерах встановлюється одна і та ж ОС, яка надає всім комп'ютерам в мережі потенційно рівні можливості. Однорангові мережі можуть бути побудовані, наприклад, на базі ОС LANtastic, Personal Ware, Windows for Workgroup, Windows NT Workstation.

У однорангових мережах також може виникнути функціональна несиметричність: одні користувачі не бажають розділяти свої ресурси з іншими, і в такому випадку їхні комп'ютери виконують роль клієнта, за іншими комп'ютерами адміністратор закріпив тільки функції щодо організації спільного використання ресурсів, а значить вони є серверами, у третьому випадку, коли локальний користувач не заперечує проти використання його ресурсів і сам не виключає можливості звернення до інших комп'ютерів, ОС, що встановлюється на його комп'ютері, повинна включати і серверну, і клієнтську частини. На відміну від мереж з виділеними серверами, у тимчасових мережах відсутня спеціалізація ОС в залежності від переважної функціональної спрямованості - клієнта чи сервера. Всі варіації реалізуються засобами конфігурації одного і того ж варіанти ОС.

Однорангові мережі простіші в організації та експлуатації, проте вони застосовуються в основному для об'єднання невеликих груп користувачів, що не пред'являють великих вимог до обсягів збереженої інформації, її захищеності від несанкціонованого доступу і до швидкості доступу. При підвищених вимогах до цих характеристик більш придатними є двохрангові мережі, де сервер краще вирішує задачу обслуговування користувачів

своїми ресурсами, так як його апаратура і мережна операційна система спеціально спроектовані для цієї мети.

Мережеві операційні системи мають різні властивості в залежності від того, призначені вони для мереж масштабу робочої групи (відділу), для мереж масштабу кампусу або для мереж масштабу підприємства.

Мережі відділів - використовуються невеликою групою співробітників, які вирішують спільні завдання. Головною метою мережі відділу є розділення локальних ресурсів, таких як додатки, дані, лазерні принтери та модеми. Мережі відділів звичайно не розділяються на підмережі. Мережі кампусів - з'єднують декілька мереж відділів всередині окремої будівлі або всередині однієї території підприємства. Ці мережі є все ще локальними мережами, хоча і можуть покривати територію в кілька квадратних кілометрів. Сервіси такої мережі включають взаємодію між мережами відділів, доступ до баз даних підприємства, доступ до факс-серверів, високошвидкісних модемів і високошвидкісних принтерів. Мережі підприємства (корпоративні мережі) - об'єднують всі комп'ютери всіх територій окремого підприємства. Вони можуть покривати місто, регіон або навіть континент. У таких мережах користувачам надається доступ до інформації і додатків, що знаходяться в інших робочих групах, інших відділах, підрозділах і штаб-квартирах корпорації.

Наступним кроком в еволюції мереж є об'єднання локальних мереж кількох відділів в єдину мережу будівлі або групи будівель. Такі мережі називають мережами кампусів. Мережі кампусів можуть тягнутися на кілька кілометрів, але при цьому глобальні з'єднання не потрібні.

Операційна система, що працює в мережі кампусу, повинна забезпечувати для співробітників одних відділів доступ до деяких файлів і ресурсів мереж інших відділів. Послуги, що надаються ОС мереж кампусів, не обмежуються простим розділенням файлів і принтерів, а

Стан	Опис
	досить складні і передають інформацію про з'єднання через область даних *TCP* або UDP пакетів і тому вимагають наявності спеціальних допоміжних модулів для коректної роботи.
ESTABLISHED	Стан **ESTABLISHED** говорить про те, що це не перший пакет в з'єднанні. Схема установки стану ESTABLISHED достатня проста для розуміння. Єдина вимога, що пред'являється до з'єднання, полягає в тому, що для переходу в стан ESTABLISHED необхідно щоб вузол мережі передав пакет і отримав на нього відповідь від іншого вузла (хоста). Після отримання відповіді стан з'єднання NEW або RELATED буде замінено на ESTABLISHED.
INVALID	Ознака **INVALID** говорить про те, що пакет не може бути ідентифікований і тому не може мати певного статусу. Це може відбуватися з різних причин, наприклад при нестачі пам'яті або при отриманні ICMP-повідомлення про помилку, яке не відповідає якому небудь відому з'єднанню. Напевно, найкращим варіантом було б застосування дії DROP до таких пакетів.

Ці чотири стани можуть використовуватися в критерії **- state.** Механізм визначення стану дозволяє будувати надзвичайно потужний і ефективний захист. Раніше доводилося відкривати всі порти вище 1024, щоб пропустити зворотний трафік в локальну мережу, тепер же, при наявності механізму визначення стану, необхідність в цьому відпала, оскільки з'явилася можливість "відкривати"

ESTABLISHED, RELATED і **INVALID.** У таблиці, наведеній нижче, розглядаються кожне з можливих станів.

Таблиця 1. Перелік станів у просторі користувача

Стан	**Опис**
NEW	Ознака **NEW** повідомляє про те, що пакет є першим для даного з'єднання. Це означає, що це перший пакет у даному сполученні, який побачив модуль трасувальника. Наприклад якщо отримано SYN пакет є першим пакетом для даного з'єднання, то він отримає статус NEW. Однак, пакет може і не бути SYN пакетом і тим не менш отримати статус NEW. Це може породити певні проблеми в окремих випадках, але може виявитися і досить корисним, наприклад коли бажано "підхопити" сполуки, "втрачені" іншими брандмауерами або у випадках, коли таймаут з'єднання вже минув, але саме з'єднання не було закрито.
RELATED	Стан **RELATED** одне з "хитрих". З'єднання отримує статус RELATED якщо воно пов'язане з іншим з'єднанням, які мають ознака ESTABLISHED. Це означає, що з'єднання отримує ознака RELATED тоді, коли воно ініційоване з вже встановленого з'єднання, що має ознаку ESTABLISHED. Хорошим прикладом сполуки, яка може розглядатися як RELATED, є з'єднання FTP-data, яке є пов'язане з портом FTP control, а так само DCC з'єднання, запущене з IRC. Зверніть увагу на те, що більшість протоколів TCP і деякі з протоколів UDP

часто надають доступ і до серверів інших типів, наприклад, до факс-серверів і до серверів високошвидкісних модемів. Важливим сервісом, наданих операційними системами даного класу, є доступ до корпоративних баз даних, незалежно від того, розташовуються вони на серверах баз даних або на мінікомп'ютерах.
Саме на рівні мережі кампуса починаються проблеми інтеграції. У загальному випадку, відділи вже вибрали для себе типи комп'ютерів, мережевого обладнання та мережевих операційних систем. Наприклад, інженерний відділ може використовувати операційну систему UNIX та мережеве обладнання Ethernet, відділ продажів може використовувати операційні середовища DOS / Novell і обладнання Token Ring. Дуже часто мережа кампусу з'єднує різнорідні комп'ютерні системи, у той час як мережі відділів використовують однотипні комп'ютери.

Корпоративна мережа з'єднує мережі всіх підрозділів підприємства, в загальному випадку знаходяться на значних відстанях. Корпоративні мережі використовують глобальні зв'язки (WAN links) для з'єднання локальних мереж або окремих комп'ютерів.

Користувачам корпоративних мереж потрібні всі ті додатки і послуги, які є в мережах відділів та кампусів, плюс деякі додаткові додатки і послуги, наприклад, доступ до додатків мінікомп’ютерів і до глобальних зв'язків. Коли ОС розробляється для локальної мережі або робочої групи, то її головним обов'язком є поділ файлів і інших мережевих ресурсів (зазвичай принтерів) між локально підключеними користувачами. Такий підхід не застосовний для рівня підприємства. Поряд з базовими сервісами, пов'язаними з розділенням файлів і принтерів, мережева ОС, яка розробляється для корпорацій, повинна підтримувати більш широкий набір сервісів, в який зазвичай входять поштова служба, засоби колективної роботи, підтримка віддалених користувачів, факс-сервіс, обробка голосових повідомлень, організація відеоконференцій і ін

Крім того, багато існуючих методів і підходів до вирішення традиційних завдань мереж менших масштабів для корпоративної мережі виявилися непридатними. На перший план вийшли такі задачі і проблеми, які в мережах робочих груп, відділів і навіть кампусів або мали другорядне значення, або взагалі не виявлялися. Наприклад, найпростіше для невеликої мережі завдання ведення облікової інформації про користувачів виросла на складну проблему для мережі масштабу підприємства. А використання глобальних зв'язків вимагає від корпоративних ОС підтримки протоколів, що добре працюють на низькошвидкісних лініях, і відмови від деяких традиційно використовуваних протоколів (наприклад, тих, які активно використовують широкомовні повідомлення). Особливе значення набули завдання подолання гетерогенності - в мережі з'явилися численні шлюзи, що забезпечують узгоджену роботу різних ОС і мережевих системних додатків. До ознак корпоративних ОС можуть бути віднесені також такі особливості.

Підтримка програм. У корпоративних мережах виконуються складні додатки, що вимагають для виконання великої обчислювальної потужності. Такі програми поділяються на кілька частин, наприклад, на одному комп'ютері виконується частина програми, пов'язана з виконанням запитів до бази даних, на іншому - запитів до файлового сервісу, а на клієнтських машинах - частина, що реалізує логіку обробки даних програми і організує інтерфейс з користувачем. Обчислювальна частина загальна для корпорації програмних систем може бути дуже об'ємною і важкою для робочих станцій клієнтів, тому додатки будуть виконуватися більш ефективно, якщо їх найбільш складні в обчислювальному відношенні частини перенести на спеціально призначений для цього потужний комп'ютер - сервер додатків. Сервер додатків має базуватися на потужній апаратній платформі мультипроцесорної системи, часто на базі RISC-процесорів, спеціалізованої

SNAT (Source Network Address Translation) використовується для зміни вихідних адрес пакетів. За допомогою цієї дії можна приховати структуру локальної мережі, а заодно і розділити єдиний зовнішній IP адрес між комп'ютерами локальної мережі для виходу в Інтернет. У цьому випадку брандмауер, за допомогою SNAT, автоматично виробляє пряме і зворотне перетворення адрес, тим самим даючи можливість виконувати підключення до серверів в Інтернеті з комп'ютерів в локальній мережі.

Маскування **(MASQUERADE)** застосовується в тих же цілях, що і SNAT**,** але на відміну від останньої, MASQUERADE дає більш сильне навантаження на систему. Відбувається це тому, що кожен раз, коли потрібне виконання цієї дії - виробляється запит IP адреси для зазначеного в дії мережевого інтерфейсу, у той час як для SNAT IP адреса вказується безпосередньо. Однак, завдяки такій відмінності, MASQUERADE може працювати у випадках з динамічною IP адресою, тобто коли ви підключаєтеся до Інтернет, скажімо через *PPP, SLIP* або *DHCP*.

Таблиця Filter. Як випливає з назви, в цій таблиці мають міститися набори правил для виконання фільтрації пакетів. Пакети можуть пропускатися далі, або відхилятися (дії **ACCEPT** і **DROP** відповідно), в залежності від їх вмісту. Звичайно ж, ми можемо фільтрувати пакети і в інших таблицях, але ця таблиця існує саме для потреб фільтрації. У цій таблиці допускається використання більшості з існуючих дій, проте ряд дій, які ми розглянули вище в цьому розділі, повинні виконуватися тільки у властивих їм таблицях.

Як ви вже напевно помітили, у просторі ядра, залежно від типу протоколу, пакети можуть мати кілька різних станів. Однак, поза ядром пакети можуть мати тільки 4 стани. В основному стан пакета використовується критерієм **- state.** Припустимими є стани **NEW,**

поле, може бути прийняте неправильне рішення при виборі маршруту.

Дія **TTL** використовується для встановлення значення поля *TTL* (Time To Live) пакета. Є одне непогане застосування цієї дії. Ми можемо привласнювати певне значення цього поля, щоб приховати наш брандмауер від надто цікавих провайдерів (Internet Service Providers). Справа в тому, що окремі провайдери дуже не люблять коли одне підключення розділяється декількома комп'ютерами. і тоді вони починають перевіряти значення *TTL* пакетів, що приходять і використовують його як один з критеріїв визначення того, чи один комп'ютер "сидить" на підключенні або декілька.

Дія **MARK** встановлює спеціальну позначку на пакет, яка потім може бути перевірена іншими правилами в iptables або іншими програмами, наприклад iproute2. За допомогою "міток" можна управляти маршрутизацією пакетів, обмежувати трафік і т.і.

Таблиця Nat. Ця таблиця використовується для виконання перетворень мережевих адрес *NAT* (Network Address Translation). Як вже згадувалося раніше, тільки перший пакет з потоку проходить через ланцюжки цієї таблиці, трансляція адрес або маскування застосовуються до всіх наступних пакетів в потоці автоматично. Для цієї таблиці характерні дії:

- DNAT
- SNAT
- MASQUERADE

Дія **DNAT** (Destination Network Address Translation) виробляє перетворення адрес призначення в заголовках пакетів. Іншими словами, ця дія проводиться перенаправлення пакетів на інші адреси, відмінні від зазначених у заголовках пакетів.

кластерної архітектури. ОС сервера додатків повинна забезпечувати високу продуктивність обчислень, а значить підтримувати багатонитковоу обробку, витісняючу багатозадачність, мультипроцесування , віртуальну пам'ять і найбільш популярні прикладні середовища (UNIX, Windows, MS-DOS, OS / .

У цьому відношенні мережну ОС NetWare важко віднести до корпоративних продуктів, тому що в ній відсутні майже всі вимоги, які пред'являються до сервера додатків. У той же час хороша підтримка універсальних додатків в Windows NT власне і дозволяє їй претендувати на місце в світі корпоративних продуктів.

Довідкова служба. Корпоративна ОС повинна володіти здатністю зберігати інформацію про всіх користувачів і ресурсах таким чином, щоб забезпечувалося управління нею з однієї центральної точки. Подібно до великої організації, корпоративна мережа потребує централізоване зберігання як можна більш повної довідкової інформації про саму себе (починаючи з даних про користувачів, серверах, робочих станціях і закінчуючи даними про кабельні системи). Природно організувати цю інформацію у вигляді бази даних. Дані з цієї бази можуть бути затребувані багатьма мережевими системними додатками, в першу чергу системами управління та адміністрування. Крім цього, така база корисна при організації електронної пошти, систем колективної роботи, служби безпеки, служби інвентаризації програмного і апаратного забезпечення мережі, та й для практично будь-якого великого бізнес-додатка. В ідеалі мережева довідкова інформація повинна бути реалізована у вигляді єдиної бази даних, а не являти собою набір баз даних, що спеціалізуються на зберіганні інформації того чи іншого виду, як це часто буває в реальних операційних системах. Наприклад, в Windows NT є принаймні п'ять різних типів довідкових баз даних. Головний довідник домену (NT Domain Directory Service) зберігає інформацію про

користувачів, яка використовується при організації їх логічного входу в мережу. Дані про тих же користувачів можуть міститися і в іншому довіднику, використовуваному електронною поштою Microsoft Mail. Ще три бази даних підтримують дозвіл низькорівневих адрес: WINS - встановлює відповідність Netbios-імен IP-адресами, довідник DNS - сервер імен домену - виявляється корисним при підключенні NT-мережі до Internet, і нарешті, довідник протоколу DHCP використовується для автоматичного призначення IP-адрес комп'ютерів мережі. Ближче до ідеалу знаходяться довідкові служби, що поставляються фірмою Banyan (продукт Streettalk III) та фірмою Novell (NetWare Directory Services), що пропонують єдиний довідник для всіх мережевих додатків. Наявність єдиної довідкової служби для мережевої операційної системи - один з найважливіших ознак її корпоративності.

Безпека. Особливу важливість для ОС корпоративної мережі набувають питання безпеки даних. З одного боку, у великомасштабній мережі об'єктивно існує більше можливостей для несанкціонованого доступу - через децентралізації даних і великої розподіленості "законних" точок доступу, із-за великого числа користувачів, благонадійність яких важко встановити, а також із-за великого числа можливих точок несанкціонованого підключення до мережі. З іншого боку, корпоративні бізнес-додатки працюють з даними, які мають життєво важливе значення для успішної роботи корпорації в цілому. І для захисту таких даних в корпоративних мережах поряд з різними апаратними засобами використовується весь спектр засобів захисту, що надається операційною системою: виборчі або мандатні права доступу, складні процедури аутентифікації користувачів, програмна шифрація.

мережевих додатків і користувацьких процесів.

Sunbelt Kerio Personal Firewall — *безкоштовна програма для захисту вашого ПК від проникнення хакерів і витоку даних.*

3.1. Про IPTables

IPTables це між мережний екранний фаєрвол. У цьому розділі ми розглянемо порядок проходження таблиць і ланцюжків у кожній таблиці. Ця інформація буде дуже важлива для нас пізніше, коли ми почнем будувати свої набори правил, особливо коли в набори правил будуть включатися такі дії як DNAT, SNAT і звичайно ж TOS.

Коли пакет приходить на наш брандмауер, то він спершу потрапляє на мережевий пристрій, перехоплюється відповідним драйвером і далі передається в ядро. Далі пакет проходить ряд таблиць і потім передається або локальним додатком, або переправляється на іншу машину.

Як уже згадувалося, ця таблиця призначена, головним чином для внесення змін в заголовки пакетів (mangle - спотворювати, змінювати.). Тобто у цій таблиці ви можете встановлювати біти *TOS* (Type Of Service) і т.і.

У цій таблиці допускається виконувати тільки перелічені нижче дії:

- TOS
- TTL
- MARK

Дія **TOS** виконує установку бітів поля *Type of Service* в пакеті. Це поле використовується для призначення мережної політики обслуговування пакету, тобто задає бажаний варіант маршрутизації. Однак, слід зауважити, що дана властивість насправді використовується на незначній кількості маршрутизаторів в Інтернеті. Іншими словами, не слід змінювати стан цього поля для пакетів, що йдуть в Інтернет, тому що на роутерах, які такі обслуговують це

суперкористувача, однак бажано практично їх опанувати, враховуючи їх значимість в повсякденній роботі з ОС.

3. Штатні фаєрволи операційної системи Linux

Файервол (мережевий екран, брандмауер) — програма, що здійснює контроль і фільтрацію мережевих пакетів, що проходять через нього відповідно до заданих правил. Основним завданням фаєрвола є захист від несанкціонованого доступу. Також мережеві екрани часто називають фільтрами, оскільки їх основне завдання — не пропускати пакети.


Online Armor Personal Firewall Free — *один з найкращих персональних фаєрволів з системою HIPS і безліччю корисних функцій для захисту вашого ПК.*


Outpost Firewall Free — *це персональний файрвол з відкритою архітектурою і підтримкою плагінів, що захистить вас від атак хакерів.*


ZoneAlarm Free — *потужний файервол для захисту комп'ютера під час його роботи в локальній мережі або в Інтернеті.*


PC Tools Firewall Plus — *безкоштовний брандмауер для захисту від несанкціонованого доступу до вашого персонального комп'ютера.*


Comodo Firewall Pro — *один з кращих безкоштовних файерволів, що надає надійних захист від Інтернет загроз.*


Kerio Control — *програма від компаній Kerio Technologies і Tiny Software, для використання в корпоративних мережах невеликих організацій.*


Jetico Personal Firewall *організовує трирівневий захист: контроль і фільтрація мережевих пакетів, дій*

1.4. Мережеві архітектури

Мережева архітектура – це комбінація стандартів, топологій і протоколів, які утворюють працездатну мережу.

МА характеризує загальну структуру мережі, тобто всі компоненти завдяки яким мережа функціонує як апаратні засоби так і системи ПЗ. Кожна МА має свої характеристики, параметри продуктивності, апаратні та програмні засоби. Це дає проектувальнику полегшенні можливості створення мережі, яка має задовольняти вимогам функціонування. Тобто проектувальник обгрунтовує вибір МА і не проводить внутрішнього аналізу та розрахунку мережі.

Так як уже згадувалося існують такі мережеві архітектури як:

Ethernet, Token Ring, Arcnet.¢

Ethernet – найпопулярніша в даний час МА, вона використовує немодульовану передачу із швидкістю 10, 100,1000 мг біт/с, топологію шина або шина-зірка і метод доступу CSMA/CD.

Кадр Ethernet складається з:

- приамбули – відмічає початок кадра
- приймача – адреса комп'ютера-приймача
- джерела – відреса комп'ютера відправника
- типу – ідентифікатор протокола мережевого рівня (IP, IPX)
- дані – розміром 46-1500 байт
- CDR – циклічний надлишковий код для перевірки помилок

10 Base-5 – товстий Ethernet

Максимальна довжина одного сегмента – 500м. Кабель RG6 коштує дорого, має високу механічну стійкість. Для приєднання до мережі потрібні адаптери з AUI-роз'єднувачами та блоки трансерверів (приймача та передавача), які монтують безпосередньо на кабелі з

проколюванням. На кінцях кабелю встановлюють узгоджувальні індуктивності – термінатори.

10 Base-2 – тонкий Ethernet

Максимальна довжина одного сегмента становить 185м. мережа має шинну багатосегментну топологію. У мережі застосовують дешевий кабель RG 58C/U. Цей кабель погано захищений від завад, контакти його приєднання до станцій ненадійні та незахищені від дій користувача. Порушення контакту спричиняє розрив мережі.

10 Base-7 – Ethernet на скрученій парі

топологія з'єднань – розподілена зірка. Максимальна станція до концентратора – 100-160м. Кабель дешевий та простий для прокладання. Цей тип кабелю використовують в інших засобах зв'язку та мережах (Token Ring, Arcnet). Обмеження на відстань до конденсатора, якщо конденсаторів є велика кількість, немає великого значення. Мережа на скрученій парі проста в обслуговуванні, експлуатації та діагностуванні пошкоджень. Вона поступово стає головним варіантом мереж Ethernet.

10 Base-F – волоконно-оптичний Ethernet

Мережа побудована на волоконно-оптичному кабелі, що забезпечує повну гальванічну ізоляцію. Максимальна відстань передавання – до 2км. Кабель легкий, має менші габарити, ніж товстий Ethernet, однак дорожчий від нього. Забезпечує тільки двопунктове сполучення, тому його використовують тільки для магістральних ліній як доповнення до Ethernet на скрученій парі.

10 Base-T (10 – швидкість передачі 10 мг біт/с, T– сручена пара). Використовують переважно UTP. Має топологію зірка де концентратором є багатопортовий повторювач. Максимальна довжина – 100м, а мінімальна – 2,5м.

100 Base-T, на відмінну від 10 Base-T, можливе передавання не тільки через різні передавальні середовища, але й використанням різних алгоритмів кодування.

Останнім часом у закордонній літературі усе активніше обговорюється концепція динамічного адміністрування. Її поява відповідає загальній тенденції у світі мережного і системного адміністрування - переносу акцентів із контролю за окремими ресурсами, або їхніми групами, із керування робочими характеристиками ІС на максимальне задоволення запитів кінцевих користувачів інформаційних технологій.

2.1. Мережеве адміністрування у системі Linux

Вивчення основних операцій адміністрування в Linux: керування режимами завантаження ОС, редагування конфігураційних файлів, монтування файлових систем, додавання нових користувачів і груп, архівування та ущільнення файлів.

До основних задач системного адміністратора (суперкористувача) в Linux можна віднести:

- інсталяцію (установку) ОС;
- керування процесом завантаження ОС;
- установку режимів роботи ОС;
- редагування конфігураційних файлів;
- монтування і демонтування файлових систем;
- введення та вилучення користувачів ОС;
- оновлення програмного забезпечення;
- конфігурування ядра ОС;
- забезпечення надійного функціонування ОС;
- конфігурування комп'ютерної мережі.

Деякі із перерахованих задач далі будуть розглянуті більш детально. В цій роботі будуть також розглянуті питання ущільнення та архівування файлів. Хоча для виконання цих задач не потрібні повноваження

компаній. Подібні додатки пропонуються практично усіма відомими постачальниками устаткування. Третя група - численні програми третіх фірм, націлені на рішення вузьких задач мережного адміністрування.

Функціональна область управління, що відноситься до цієї сфери, чітко визначена в специфікаціях ISO:

• рішення проблемних ситуацій (діагностика, локалізація й усунення несправностей, реєстрація помилок, тестування);

• управління ресурсами (врахування, контроль використання ресурсів, виставлення рахунків за використані ресурси й обмеження доступу до них);

• управління конфігурацією, спрямоване на забезпечення надійного й ефективного функціонування всіх компонентів інформаційної системи;

• контроль продуктивності (збір і аналіз інформації про роботу окремих ресурсів, прогнозування ступеня задоволення потреб користувачів/додатків, заходи для збільшення продуктивності);

• захист даних (управління доступом користувачів до ресурсів, забезпечення цілісності даних і управління їхнім шифруванням).

Основним результатом тривалого розвитку галузі системного адміністрування стало те, що з функціональної точки зору основні платформи управління мережею в даний час досить схожі одна на одну. Розходження між ними криються в сфері структурного виконання і пов'язані з тими вихідними цілями, що ставилися на початкових етапах їх розробки.

Серед численних категорій користувачів ПЗ системного адміністрування усе більшої популярності набувають продукти фірм середнього розміру, які забезпечують потужними засобами вирішення досить широкого кола задач, мають інтуїтивний Web-інтерфейс і прийнятну ціну.

100 Base-T4 це локальна мережа зіркової топології, яка використовує для передавання даних 4 пари провідників скрученої пари категорії 3,4 або 5.

1.5. Опис топологій локальних мереж

Спосіб об'єднання комп'ютерів між собою в мережі називають топологією. Топологія – це фізичне розташування комп'ютерів, кабелів та інших мережевих компонентів. Розрізняють три найбільш розповсюджені мережні топології, що використовують і для однорангових мереж, і для мереж з виділеним файлом-сервером. Це так звані шина, кільцева і зіркоподібна структури.

Топологія визначає ряд вимог:

- використання конкретного типу кабеля;
- спосіб прокладання кабелю;
- способи та методи взаємодії комп'ютерів.

Базові топології – це три топології, що мають суттєві відмінності між собою.

Шина (bus) – топологія при якій всі комп'ютери під'єднюються до одного кабеля. Кабель називається магістраллю або сегментом. Ця топологія є найбільш поширеною і простою у використанні. При передачі даних електричний сигнал від комп'ютера передавача поширюється у кабелі одночасно до решти комп'ютерів.

Дані приймає тільки той комп'ютер, адреса якого співпадає з адресою вказаного у повідомленні. Сигнал також надходить до країв кабеля і відбивається. Відбитий сигнал накладається на корисний і спотворює його, що призводить до помилок передачі і мережа стає нероботоздатною. Для того, щоб відбивання хвиль не було на кінцях кабеля встановлюються термінатори.

Термінатори – електричний опір, який поглинає відбиті електричні сигнали.

Недоліками цієї топології є:

- при розриві кабеля, або відсутності термінатора, мережа перестає функціонувати;
- низька пропускна здатність;
- не підсилює сигнал при передачі.

Перевагами цієї топології є:

- простота у використанні і дешевизна;
- при виході з ладу одного комп'ютера, мережа продовжує працювати але без нього.

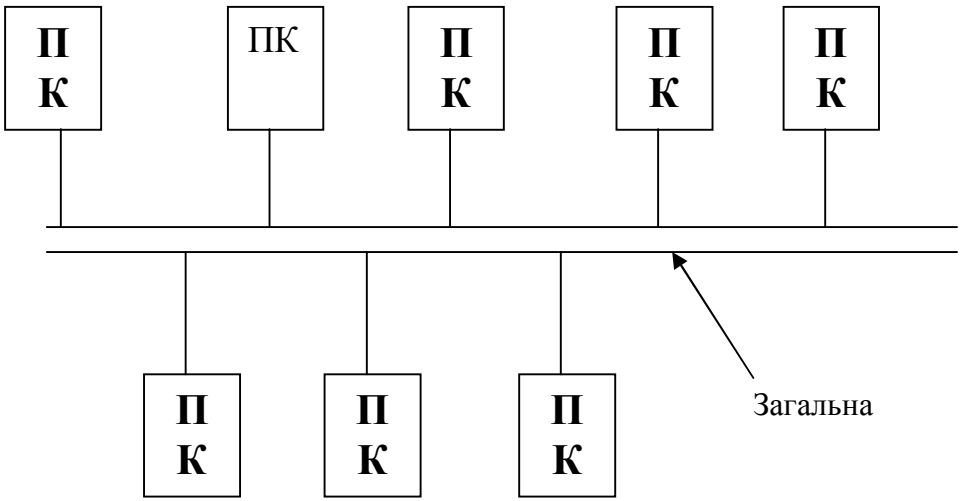


Рисунок 5 – Топологія шина

<u>Кільце (ring)</u> *<u>(рисунок 5):</u>* **–** топологія при якій всі комп'ютери під'єднюються до кабеля, який замкнутий у кільце.

замітний у складних сегментованих мережах, що містять велику кількість активних пристроїв. У якості часткового рішення проблеми вичерпання пропускної спроможності була запропонована трьохрівнева архітектура, у якій частина керуючих функцій делегувалася найважливішим мережним вузлам. Інстальовані в цих вузлах програми-менеджери через власну мережу агентів управляють роботою "підзвітних" їм пристроїв і в той же час самі виступають у ролі агентів стосовно основної програми-менеджера (менеджеру менеджерів), запущеної на керуючій станції. У результаті основна частина службового трафіка надається локалізованим в окремих мережних сегментах менеджерам, оскільки «спілкування» локальних менеджерів з адміністративною консоллю здійснюється тільки тоді, коли в цьому дійсно виникає необхідність.

Необхідність контролювати роботу різноманітного устаткування в гетерогенному середовищі зажадала уніфікації основних керуючих процедур. Згадана схема «менеджер - агенти» знайшла вираження в протоколі Simple Network Management Protocol (SNMP), що швидко став базовим протоколом мережевого адміністрування, і в стандарті дистанційного моніторингу RMON. Управління настільними системами звичайно здійснюється на базі стандарту Desktop Management Interface (DMI), розробленого організацією Desktop Management Task Force (DMTF).

Результат такого розвитку подій неважко передбачити наперед: індустрія ПЗ мережневого управління виявилася розділеною на три частини. Першу утворюють платформи мережного управління - аналоги операційних систем, що формують середовище для запуску додатків, але при цьому вони володіють обмеженою функціональністю. Друга група мережевих програм пов'язана з керуючими додатками виробників мережних апаратних засобів. Проте вони розраховані на управління тільки визначеною групою пристроїв і рідко дозволяють обслуговувати вироби інших

2. Мережне адміністрування

Якщо не вдаватися в деталі, то задачі, розв'язувані в даній області, розбиваються на дві групи: контроль за роботою мережного устаткування й управління функціонуванням мережі в цілому. У першому випадку мова йде про моніторинг окремих мережних пристроїв (концентраторів, комутаторів, маршрутизаторів, серверів доступу й ін.), настроюванню і зміні їхньої конфігурації, усуненні виникаючих збоїв. Ця достатньо традиційна група задач одержала назву реактивного адміністрування (reactive management). Друга група націлена на моніторинг мережного трафіка, виявлення тенденцій його зміни й аналіз подій із метою реалізації схем пріоритеризації для забезпечення максимальної пропускної спроможності (proactive management). Сюди ж відноситься задача внесення змін у конфігурацію мережі, управління IP-адресами користувачів, фільтрація пакетів в цілях забезпечення інформаційної безпеки і ряд інших задач.

Потреба в контролі за мережею в цілому з однієї керуючої станції стала причиною появи різних архітектур платформ і додатків адміністрування. Найбільше поширення серед них набула двохрівнева розподілена архітектура "менеджер–агенти". Програма-менеджер функціонує на керуючій консолі, постійно взаємодіє з модулями-агентами, що запускаються в окремих пристроях мережі. На агента в такій схемі покладаються функції збору локальних даних про параметри роботи контрольованого ресурсу, внесення змін у його конфігурацію по запиті від менеджера, надання останньому адміністративної інформації.

Незважаючи на очевидні зручності двохрівневої архітектури, її застосування в реальному мережевому середовищі призводить до зростання обсягів службового трафіка і, як наслідок, до зниження пропускної спроможності, доступної додаткам. Цей ефект особливо

Тут сигнали передаються послідовно від одного комп'ютера до наступного, одночасно при цьому підсилюються.

Для організації передачі використовується маркер.

Маркер (token) –це особливий пакет, що передається по кільцю і надає комп'ютеру на який він прийшов, можливість передавати дані.

Недоліком цієї топології є:

- при виході з ладу комп'ютера чи обриві кабеля мережа перестає працювати.

Первагами цієї топології є:

- підсилення сигналу;
- надійна організація передачі даних, можливість збільшення загальної довжини кабеля.
-

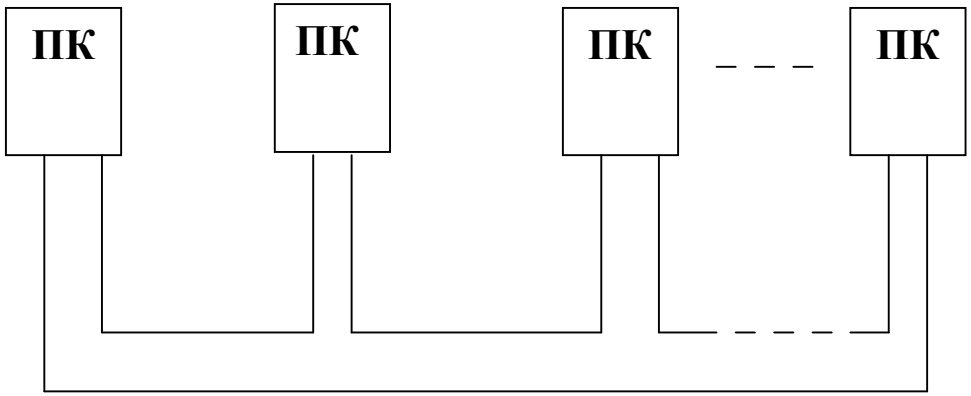


Рисунок 6 – Топологія кільце

Зірка (start) *(рисунок.6):* – топологія при якій всі комп'ютери за допомогою кабелів під'єднюється до центрального компонента-концентратора (hub).

Дані передаються від комп'ютера передавача до концентратора, а від концентратора – всій решті комп'ютерів.

У інтелектуальних концентраторах може відбуватися адресація, тобто сигнал від концентратора буде передаватися тільки вказаному комп'ютеру.

Недоліками цієї топології є:

- великий розхід кабелю;
- потреба додаткового концентратора;
- при виході з ладу концентратора припиняється робота всієї мережі.

Перевагами цієї топології є:

- вихід з ладу одного комп'ютера чи обриві кабеля, не впливають на роботу решти комп'ютерів мережі.

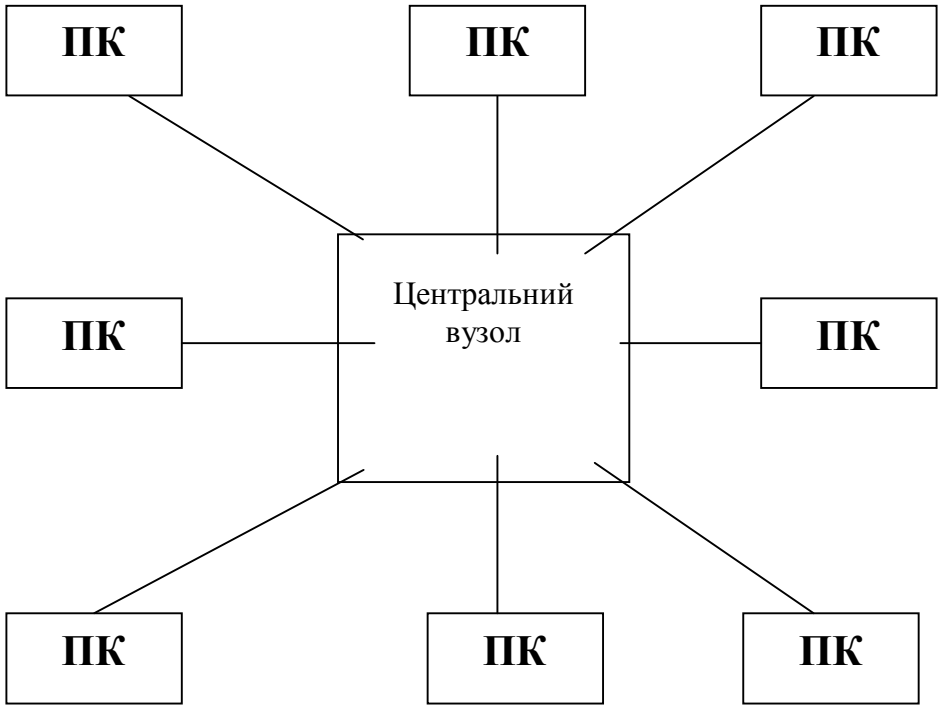


Рисунок 7 – Топопогія зірка

конструкцій, що дозволяють маніпулювати з текстовими рядками й будувати складні команди на основі простих команд; вбудованих команд, виконуваних безпосередньо інтерпретатором командної мови; команд, що представляються окремими виконуваними файлами.

Процеси. Процес в ОС UNIX - це програма, виконувана у власному віртуальному адресному просторі. Коли користувач входить у систему, автоматично створюється процес, у якому виконується програма командного інтерпретатора. Якщо командному інтерпретаторові зустрічається команда, що відповідає виконуваному файлу, то він створює новий процес і запускає в ньому відповідну програму, починаючи з функції main. Ця запущена програма, у свою чергу, може створити процес і запустити в ньому іншу програму (вона теж повинна містити функцію main).

Перенаправлення введення/виводу. Механізм перенаправлення введення/виводу є одним з найбільш елегантних, потужних і одночасно простих механізмів ОС UNIX. Ціль, що ставилася при розробці цього механізму, полягає в наступному. Оскільки UNIX - це інтерактивна система, то звичайні програми вводять текстові рядки з термінала й виводять результуючі текстові рядки на екран термінала. Для того, щоб забезпечити більше гнучке використання таких програм, бажано вміти забезпечити їм введення з файлу або з виводу інших програм і направити їхній вивід у файл або на введення іншим програмам.

командних інтерпретаторів (залежно від параметрів, що зберігаються у файлі /etc/passwd). Звичайно в системі підтримується кілька командних інтерпретаторів зі схожими, але можливостями, що розрізняються своїми командними мовами. Загальна назва для будь-якого командного інтерпретатора ОС UNIX - shell (оболонка), оскільки будь-який інтерпретатор представляє зовнішнє оточення ядра системи.

Привілейований користувач. Ядро ОС UNIX ідентифікує кожного користувача по його ідентифікаторі (UID - User Identifier), унікальному цілому значенню, що привласнюється користувачеві при реєстрації в системі. Крім того, кожний користувач ставиться до деякої групи користувачів, що також ідентифікується деяким цілим значенням (GID - Group IDentifier). Зрозуміло, що адміністратор системи, що, природно, теж є зареєстрованим користувачем, повинен мати більші можливості, чим звичайні користувачі. В ОС UNIX це завдання вирішується шляхом виділення одного значення UID (нульового). Користувач із таким UID називається суперкористувачем (superuser) або root. Він має необмежені права на доступ до будь-якого файлу й на виконання будь-якої програми. Крім того, такий користувач має можливість повного контролю над системою. Він може зупинити її й навіть зруйнувати.

Програми - ОС UNIX одночасно є операційним середовищем використання існуючих прикладних програм і середовищем розробки нових додатків. Нові програми можуть писатися на різних мовах (Фортран, Паскаль, Модула, Ада й ін.). Однак стандартною мовою програмування в середовищі ОС UNIX є мова С (який останнім часом усе більше заміняється на С++). Це пояснюється тим, що по-перше, сама система UNIX написана мовою С, а, по-друге, мова С є одним з найбільше якісно стандартизованих мов.

Команди - будь-яка командна мова сімейства shell фактично складається із трьох частин: службових

Будь-яку з цих топологій рідко можна зустріти на практиці в чистому вигляді. Як правило, сучасні мережі є складним поєднанням базових топологій та їх видозмін.

Пропускна здатність мережі визначається обчислювальною потужністю вузла і гарантується для кожної робочої станції. Колізій (зіткнень) даних не виникає.

Кабельне з'єднання зв'язане з всіма пристроями, тому що кожна робоча станція зв'язана з вузлом. Витрати на прокладку кабелів високі, особливо коли центральний вузол географічно розташований не в центрі топології.

При розширенні обчислювальних мереж не можуть бути використані раніше виконані кабельні зв'язки: до нового робочого місця необхідно прокладати окремий кабель з центра мережі.

Топологія у виді зірки є найбільш швидкодіючою з усіх топологій обчислювальних мереж, оскільки передача даних між робочими станціями проходить через центральний вузол (при його гарній продуктивності) по окремих лініях, використовуваними тільки цими робочими станціями. Частота запитів передачі інформації від однієї станції до іншої невисока в порівнянні з іншими топологіями.

Продуктивність обчислювальної мережі в першу чергу залежить від потужності центрального файлового сервера. Він може бути вузьким місцем обчислювальної мережі. У випадку виходу з ладу центрального вузла порушується робота всієї мережі.

Центральний вузол керування – файловий сервер може реалізувати оптимальний механізм захисту проти несанкціонованого доступу до інформації. Вся обчислювальна мережа може керуватися з її центра.

1.6. Мережеві Unix подібні операційні системи

Вперше система UNIX була описана в 1974 році в статті Кена Томпсона й Денніса Річі в журналі "Communications of the ACM". Із цього часу вона одержала широке поширення й завоювала широку популярність серед виробників ЕОМ, які все частіше стали оснащувати нею свої машини. Особливою популярністю вона користується в університетах, де досить часто бере участь у дослідницькому й навчальному процесі.

Основними дистрибутивами мережевих Unix подібних операційних систем є:

- FreeBSD
- Fedora Core
- CentOS
- RedHat

Незалежно від версії, загальними для UNIX рисами є:

- ✓ багатокористувальницький режим із засобами захисту даних від несанкціонованого доступу
- ✓ реалізація мультипрограмної обробки в режимі поділу часу, заснований на використанні алгоритмів багатозадачності, що витісняє (preemptive multitasking)
- ✓ використання механізмів віртуальної пам'яті й свопингу для підвищення рівня мультипрограмування
- ✓ уніфікація операцій введення-виводу на основі розширеного використання поняття "файл"
- ✓ ієрархічна файлова система, що утворює єдине дерево каталогів незалежно від кількості фізичних пристроїв, використовуваних для розміщення файлів
- ✓ переносимість системи за рахунок написання її основної частини мовою С

- ✓ різноманітні засоби взаємодії процесів, у тому числі й через мережу
- ✓ кешування диска для зменшення середнього часу доступу до файлів.

Хоча операційна система й більшість команд написані на С, система UNIX підтримує ряд інших мов, таких як Фортран, Бейсик, Паскаль, Ада, Кобол, Лісп і Пролог. Система UNIX може підтримувати будь-яку мову програмування, для якого є компілятор або інтерпретатор, і забезпечувати системний інтерфейс, що встановлює відповідність між користувальницькими запитами до операційної системи й набором запитів, прийнятих в UNIX.

Однією з переваг ОС UNIX є те, що система базується на невеликому числі інтуїтивно ясних понять. Однак, незважаючи на простоту цих понять, до них потрібно звикнути. Без цього неможливо зрозуміти суть ОС UNIX.

Користувач - із самого початку ОС UNIX планувалася як інтерактивна система. Інакше кажучи, UNIX призначений для термінальної роботи. Щоб почати працювати, людина повинна "увійти" у систему, ввівши з вільного термінала своє облікове ім'я (account name) і, можливо, пароль (password). Людина, зареєстрована в облікових файлах системи, і, отже, що має облікове ім'я, називається зареєстрованим користувачем системи. Реєстрацію нових користувачів звичайно виконує адміністратор системи. Користувач не може змінити своє облікове ім'я, але може встановити й/або змінити свій пароль. Паролі зберігаються в окремому файлі в закодованому виді. Не забувайте свій пароль, знову довідатися його не допоможе навіть адміністратор!

Інтерфейс користувача - традиційний спосіб взаємодії користувача із системою UNIX ґрунтується на використанні командних мов (правда, у цей час все більше поширення одержують графічні інтерфейси). Після входу користувача в систему для нього запускається один з