

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри

_____ Скарга-Бандурова І.С.
«_____» _____ 20__ р.

МАГІСТЕРСЬКА РОБОТА

НА ТЕМУ:

Дослідження та розробка ПТК Головного управління
Держгеокадастру у Луганській області

Освітній ступінь “Магістр”
Спеціальність 123 “Комп’ютерна інженерія”

Науковий керівник роботи:

(підпис)

Є.В.Щербаков

(ініціали, прізвище)

Консультант з охорони праці:

(підпис)

Я.О.Критська

(ініціали, прізвище)

Студент:

(підпис)

А.С.Карпенко

(ініціали, прізвище)

Група:

КІ-17зм

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітній ступінь Магістр
Напрямок підготовки _____
(шифр і назва)
Спеціальність 123 "Комп'ютерна інженерія"
(шифр і назва)

ЗАТВЕРДЖУЮ:

Завідувач кафедри _____
I.C. Скарга-Бандурова
« _____ » _____ 20__ р.

**З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ**

Карпенко Андрію Сергійовичу

(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження та розробка ПТК Держгеокадастру
Content Mining у Луганській області

керівник проекту (роботи) Щербаков Євген Васильович, к.т.н., доц.
(прізвище, 2м.'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від «18» 10 2018 р. № 221/48

2. Строк подання студентом роботи 11.01.2018

3. Вихідні дані до роботи У результаті виконання роботи повинна бути
досліджена комп'ютерна мережа Головного управління Держгеокадастру у
Луганській області та розроблен програмно-технічний комплекс організації

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Огляд існуючих засобів побудови мереж, дослідження та
проекткування програмно-технічного комплексу, налаштування програмного
та апаратного забезпечення вузлів локальної комп'ютерної мережі, охорона
праці та безпека в надзвичайних ситуаціях, висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Електронні плакати

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та безпека в надзвичайних ситуаціях	Критська Я.О. ст. викл. кафедри КНІ		

7. Дата видачі завдання 18.10.2018

Керівник

_____ (підпис)

Завдання прийняв до виконання

_____ (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз завдання, робота з літературою	10.09.2018-15.09.2018	
2	Дослідження та проектування програмно-технічного комплексу	16.09.2018-22.09.2018	
3	Налаштування програмного та апаратного забезпечення вузлів локальної комп'ютерної мережі	26.09.2018-06.10.2018	
4	Тестування програмної системи	07.10.2018-25.11.2018	
5	Розробка частини проекту "Охорона праці та безпеки в надзвичайних ситуаціях"	26.11.2018-1.12.2018	
6	Оформлення пояснювальної записки, автореферату та презентації	2.12.2018-09.01.2019	
7			

Студент

_____ (підпис)

Карпенко А.С.

_____ (прізвище та ініціали)

Науковий керівник

_____ (підпис)

Щербаков Є.В.

_____ (прізвище та ініціали)

АНОТАЦІЯ

Карпенко А.С. Дослідження та розробка ПТК Головного управління Держгеокадастру у Луганській області.

Проаналізовані сучасні вимоги для створення програмно-технічного комплексу. Досліджені сучасні методи створення локальної мережі. Практично реалізован програмно-технічний комплекс в організації.

Ключові слова: локальна мережа, структуровані кабельні системи, розробка, програмне забезпечення, проксі-сервер.

АННОТАЦИЯ

Капренко А.С. Исследование и разработка ПТК Главного управления Госгеокадастра в Луганской области.

Проанализированы современные требования к созданию програмно-технического комплекса. Исследованы современные методы создания локальной сети. Практически реализован програмно-технический комплекс в организации.

Ключевые слова: локальная сеть, структурированные кабельные системы, разработка, программное обеспечение, прокси-сервер.

ABSTRACT

Kaprenko A.S. Research and development of the SHC of the Main Department of the State Geocadastr in the Luhansk region.

Analyzed the modern requirements for the creation of software and hardware complex. Researched modern methods of creating a local network. Practically implemented software-technical complex in the organization.

Keywords: local network, structured cabling systems, developmen, software, proxy server.

ЗМІСТ

ВСТУП.....	6
РОЗДІЛ 1.....	8
ОГЛЯД ІСНУЮЧИХ ЗАСОБІВ ПОБУДОВИ МЕРЕЖ.....	8
1.1 Поняття локальної обчислювальної мережі.....	8
1.2 Класифікація локальних обчислювальних мереж.....	8
1.3 Структуровані кабельні системи (СКС).....	14
1.4 Комутаційне обладнання.....	28
1.5 Функціональна відповідність видів комунікаційного обладнання рівнів моделі OSI.....	46
1.6 Висновки до розділу 1.....	48
РОЗДІЛ 2.....	49
ДОСЛІДЖЕННЯ ТА ПРОЕКТУВАННЯ ПРОГРАМНО-ТЕХНІЧНОГО КОМПЛЕКСУ.....	49
2.1 Постановка завдання.....	49
2.2 Стадії та етапи розробки.....	50
2.3 Розрахунок пропускнуої спроможності.....	51
2.4 Побудова локальної мережі.....	51
2.5 Комплектуючи для сервера та робочих станцій.....	52
2.6 Програмне забезпечення для сервера та робочих станцій.....	54
2.7 Висновки до розділу 2.....	55
РОЗДІЛ 3.....	57
НАЛАШТУВАННЯ ПРОГРАМНОГО ТА АППАРАТНОГО ЗАБЕЗПЕЧЕННЯ ВУЗЛІВ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ.....	57
3.1 Розробка логічної адресації вузлів локальної мережі.....	57
3.2 Налаштування мережевих інтерфейсів.....	58
3.3 Налаштування проксі-сервера.....	60
3.4 Налаштування DNS-сервера.....	62
3.5 Налаштування iptables.....	63
3.6 Налаштування ssh.....	65

3.7 Контролер домену.....	66
3.8 Налаштування мережі робочих станцій.....	69
3.9 Висновки до розділу 3.....	71
РОЗДІЛ 4.....	72
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ.....	72
4.1 Загальні положення.....	72
4.2 Вимоги безпеки перед початком роботи.....	72
4.3 Вимоги безпеки під час роботи.....	73
4.4 Вимоги безпеки у аварійних ситуаціях.....	74
4.5 Вимоги безпеки після закінчення роботи.....	74
4.6 Безпека у надзвичайних ситуаціях.....	75
4.7 Вимоги до приміщень.....	75
4.7.1 Вимоги до організації місця праці.....	76
4.7.2 Освітлення.....	77
4.7.3 Вентилювання.....	79
4.8 Охорона навколишнього природного середовища.....	80
4.9 Висновки до розділу 4.....	81
ВИСНОВКИ.....	82
ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	83
Додаток А.....	84
Додаток Б.....	85
Додаток В.....	86
Додаток Г.....	87
Додаток Д.....	93

ВСТУП

Актуальність теми. На сьогоднішній день у світі існує понад 2,5 мільярдів комп'ютерів і більш 80 % із них об'єднані в різні інформаційно-обчислювальні мережі, від малих локальних мереж в офісах до глобальних мереж типу Internet. Всесвітня тенденція до об'єднання комп'ютерів у мережі обумовлена важливими причинами, такими як прискорення передачі інформаційних повідомлень, можливість швидкого обміну інформацією між користувачами, одержання і передача повідомлень (факсів, E-Mail листів і іншого), не відходячи від робочого місця, можливість миттєвого одержання будь-якої інформації з будь-якої точки земної кулі, а так само обмін інформацією між комп'ютерами, працюючих під різним програмним забезпеченням.

В даному дипломному проекті розглядається проблема побудови програмно-технічного комплексу для Головного управління Держгеокадастру у Луганській області під управлінням операційних систем: CentOS 6.7 x64, Windows Server 2008 R2 Standard.

Реалізація запропонованого проекту дозволить скоротити паперовий документообіг всередині Головного управління, підвищити продуктивність праці, скоротити час на отримання і обробку інформації, виконувати точний і повний аналіз.

Мета і завдання дослідження. Метою дипломного проекту є дослідження та розробка ПТК Головного управління Держгеокадастру в Луганській області. Для вирішення поставленої мети в роботі вирішуються наступні завдання:

- Вибір СКС, топології, обладнання та програмного забезпечення.
- Вибір способу управління мережею.
- Розгляд питань безпеки мережі.
- Автоматизація обміну інформацією між обладнанням обробки даних.
- Використання обчислювальних ресурсів і периферійного обладнання.
- Створення умов для централізованого керування вузлами, підключеними до системи.
- Управління мережевими ресурсами та користувачами мережі.

Необхідно розробити раціональну, гнучку структурну схему мережі Головного управління, вибрати апаратну і програмну конфігурацію сервера та робочих станцій, а так само опрацювати питання забезпечення необхідного рівня захисту даних.

У більшості публікацій на цю тему зазначається, що використання засобів автоматизації в організації дає найбільший ефект у разі їх комплексної реалізації. Процес створення систем управління підприємством включає наступні етапи:

- специфікація, поставка, монтаж і налагодження обладнання та програмного забезпечення (ПЗ);
- проведення необхідних доробок і налаштувань;
- введення в дослідну експлуатацію, навчання і тестування персоналу;

- введення системи в промислову експлуатацію.

Найбільш відповідальним кроком процесу створення системи є перший - обстеження з розробкою моделей і технічних пропозицій. Головною метою цього кроку служить досягнення єдиного розуміння керівництвом організації замовника і виконавця.

Важливим моментом є вибір складу і структури устаткування і програмного забезпечення, що поєднує ефективну реалізацію цільової технології, надійність функціонування системи та мінімізацію витрат.

Об'єкт дослідження – інформаційно-телекомунікаційна система організації.

Предмет дослідження – локальна комп'ютерна мережа організації.

Практичне значення отриманих результатів. В ході роботи була проаналізована локальна мережа організації та створений і введений в експлуатацію програмно-технічний комплекс.

Зв'язок роботи з науковими програмами, планами, темами. Магістерська робота виконувалася протягом 2019 року згідно з планами науково-дослідних робіт кафедри комп'ютерних наук та інженерії в межах НДР.

Структура і обсяг роботи. Магістерська робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Робота викладена на 96 сторінках машинописного тексту, містить 82 сторінок основного тексту, 20 рисунків, 7 таблиць, 5 додатків на 14 сторінках. Бібліографічний список включає 8 найменувань.

РОЗДІЛ 1

ОГЛЯД ІСНУЮЧИХ ЗАСОБІВ ПОБУДОВИ МЕРЕЖ

1.1 Поняття локальної обчислювальної мережі

Локальна обчислювальна мережа (ЛОМ) являє собою комунікаційну систему, що дозволяє спільно використовувати ресурси комп'ютерів, підключених до мережі, таких як принтери, плоттери, диски, модеми, приводи CD-ROM і інші периферійні пристрої. Локальна мережа зазвичай обмежена територіально одним або декількома близько розташованими будівлями.

1.2 Класифікація локальних обчислювальних мереж

Обчислювальні мережі класифікуються по ряду ознак.

Залежно від відстаней між зв'язані вузлами розрізняють обчислювальні мережі:

Територіальні - охоплюють значний географічний простір. Серед територіальних мереж можна виділити мережі *регіональні* і *глобальні*, що мають, відповідно, регіональні або глобальні масштаби:

регіональні мережі іноді називаються мережами MAN (Metropolitan Area Network), а загальна англійська назва для територіальних мереж - WAN (Wide Area Network);

локальні (ЛОМ) - охоплюють обмежену територію (зазвичай в межах віддаленості станцій не більше ніж на кілька десятків чи сотень метрів один від одного, рідше на 1...2 км). Локальні мережі позначають - LAN (Local Area Network);

Корпоративні (масштабу підприємства) - сукупність пов'язаних між собою ЛОМ, що охоплюють територію, на якій розміщено одне підприємство чи установу в одному або декількох близько розташованих будівлях. Локальні та корпоративні обчислювальні мережі - основний вид обчислювальних мереж, що використовуються в системах автоматизованого проектування (САПР).

Особливо виділяють єдину у своєму роді глобальну мережу Internet (реалізована в ній інформаційна служба World Wide Web (WWW) - перекладається на українську мову як «всесвітня павутина») - це мережа мереж зі своєю технологією. У Internet існує поняття *інтрамереж* (Intranet) - *корпоративних* мереж в рамках Internet.

Мережева топологія – це геометрична форма мережі. Залежно від топології з'єднань вузлів розрізняють шинної мережі (магістральної), кільцевої, зіркову, ієрархічну довільної структури (приклади мережевих топологій наведено на рис. 1.1):

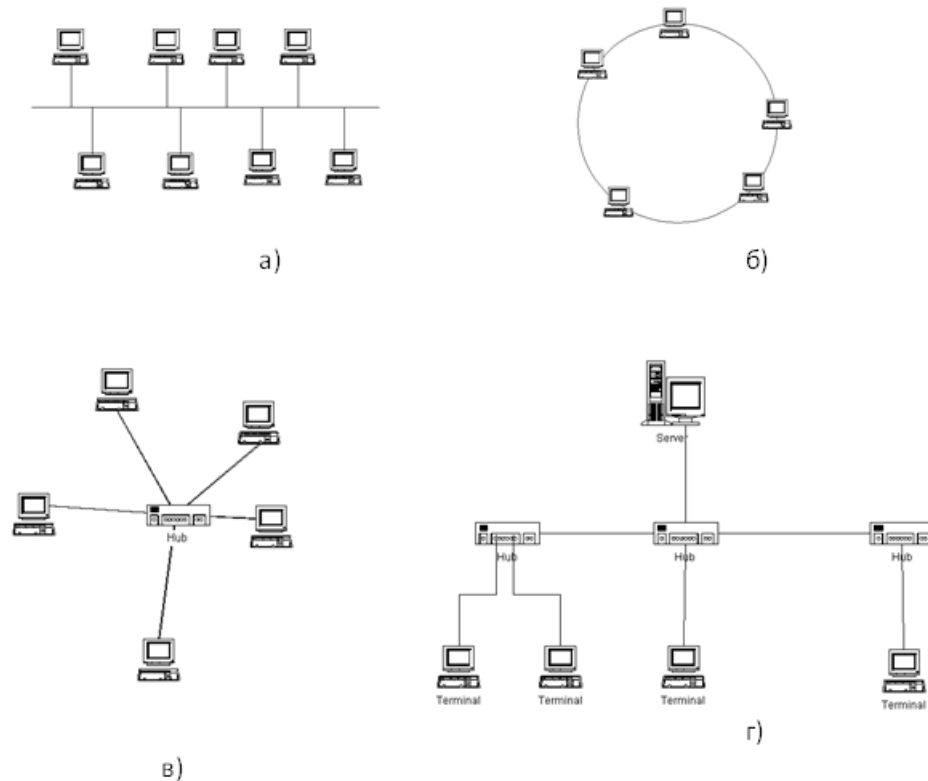


Рисунок 1.1 Мережеві топології

шинна (bus) - локальна мережа, в якій зв'язок між будь-якими двома станціями встановлюється через один спільний шлях і дані, передані будь-станцією, одночасно стають доступними для всіх інших станцій - рис. 1.1, а;

кільцева (ring) - вузли пов'язані кільцевою лінією передачі даних (до кожного вузла підходять тільки дві лінії); дані, проходячи по кільцю, по черзі стають доступними всім вузлам мережі - рис. 1.1, б;

зоряна (star) - є центральний вузол, від якого розходяться лінії передачі даних до кожного з решти вузлів - рис. 1.1, в;

ієрархічна - кожен пристрій забезпечує безпосереднє управління пристроями, що знаходяться нижче в ієрархії - рис. 1.1, г.

Порівняльний аналіз топології локально-обчислювальних мереж наведений у додатку А.

У залежності від способу управління розрізняють мережі:

"клієнт/сервер" - у них виділяється один або декілька вузлів (їх назва - сервери), які виконують мережі керуючі або спеціальні обслуговуючі функції, а інші вузли (клієнти) є

термінальними, в них працюють користувачі. Мережі клієнт/сервер розрізняються за характером розподілу функцій між серверами, іншими словами за типами серверів (наприклад, файл-сервери, сервери баз даних). При спеціалізації серверів за певних програм маємо мережу розподілених обчислень. Такі мережі відрізняють також від централізованих систем, побудованих на мейнфреймах;

однорангові - у них всі вузли рівноправні; оскільки в загальному випадку під клієнтом розуміється об'єкт (пристрій або програма), запитувач деякі послуги, а під сервером - об'єкт, що надає ці послуги, то кожен вузол в однорангових мережах може виконувати функції клієнта і сервера.

Нарешті з'явилася мережецентрична концепція, відповідно до якої користувач має лише дешеве обладнання для звернення до віддалених комп'ютерів, а мережа обслуговує замовлення на виконання обчислень і отримання інформації. Тобто користувачу не потрібно купувати програмне забезпечення для вирішення прикладних завдань, йому потрібно лише платити за виконані замовлення. Такі комп'ютери називають тонкими клієнтами або мережевими комп'ютерами.

Типова середовище передачі даних у ЛОМ - відрізок (сегмент) коаксіального кабелю. До нього через апаратуру закінчення каналу даних вузли підключаються комп'ютери і можливо загальне периферійне обладнання. Оскільки середовище передачі даних загальне, а запити на мережеві обміни сайти з'являються асинхронно, то виникає проблема поділу загальної середовища між багатьма вузлами, іншими словами, проблема забезпечення доступу до мережі.

Доступом до мережі називають взаємодію станції (вузла мережі) із середовищем передачі даних для обміну інформацією з іншими станціями. Управління доступом до середовища - це встановлення послідовності, в якій станції одержують доступ до середовища передачі даних.

Розрізняють випадкові і детерміновані методи доступу. Серед випадкових методів найбільш відомий метод множинного доступу з контролем несучої і виявленням конфліктів. Англійська назва методу - Carrier Sense Multiple Access / Collision Detection (CSMA/CD).

Протокол CSMA/CD втілює в собі ідеї перерахованих вище алгоритмів і додає важливий елемент – дозвіл колізій. Оскільки колізія руйнує всі передані в момент її виникнення кадри, то немає сенсу станції продовжувати подальшу передачу своїх кадрів, коли скоро вони (станції) виявили колізію. В іншому випадку, значною була б втрата часу при передачі довгих кадрів. Тому для своєчасного виявлення колізії станція прослуховує середовище протягом власної передачі.

Основні правила алгоритму CSMA/CD для передавальної станції.

Передача кадру:

1. Станція, що збирається передавати, прослуховує середовище, і передає, якщо середовище вільне. В іншому випадку (тобто якщо середовище зайнято), переходить до кроку 2. При передачі декількох кадрів підряд станція витримує певну паузу між посилками кадрів – міжкадровий інтервал, причому після кожної такої паузи перед відправкою наступного кадру станція знову прослуховує середовище (повернення на початок кроку 1).

2. Якщо середовище зайнято, станція продовжує прослуховувати середовище до тих пір, поки середовище не стане вільним, і потім відразу ж починає передачу.

3. Кожна станція, що веде передачу, прослуховує середовище, і, в разі виявлення колізії не припиняє відразу ж передачу, а спочатку передає короткий спеціальний сигнал колізії – jam-сигнал, інформуючи інші станції про колізії, і припиняє передачу.

4. Після передачі jam-сигналу станція замовкає і чекає деякий довільний час згідно з правилом бінарної експоненційної затримки, а потім повертається до кроку 1.

Jam-сигнал (jamming – дослівно, глушіння). Передача jam-сигналу гарантує, що жоден кадр не буде втрачений, бо всі вузли, які передавали кадри до виникнення колізії, прийнявши jam-сигнал, перервуть свої передачі і замовкнуть в очікуванні нової спроби передати кадри. Jam-сигнал повинен бути достатньої довжини, щоб він дійшов до самих віддалених станцій колізійного домена з урахуванням додаткової затримки SF (safety margin) на можливих повторювачах.

Колізійний домен (collision domain) – множина всіх станцій в мережі, одночасна передача будь-якої пари з яких призводить до колізії.

На рис. 1.2. проілюстрований процес виявлення колізії стосовно до топології "шина".

В момент часу t_0 вузол А починає передачу, природно прослуховуючи свій же сигнал. В момент часу t_1 , коли кадр майже дійшов до вузла В, цей вузол, не знаючи про те, що вже йде передача, сам починає передавати. В момент часу t_2 вузол виявляє колізію (збільшується постійна складова електричного сигналу в прослуховуванні лінії). Після цього вузол передає jam-сигнал і припиняє передачу. В момент часу t_3 сигнал колізії доходить до вузла А, після чого А також передає jam-сигнал і припиняє передачу.

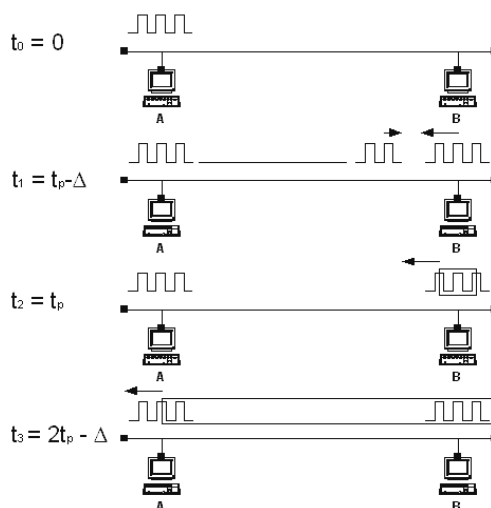


Рисунок 1.2 Виявлення колізії в шині при використанні схеми CSMA/CD стандарту Ethernet.

За стандартом Ethernet вузол не може передавати дуже короткі кадри, або, іншими словами, вести дуже короткі передачі. Навіть якщо поле даних заповнений не до кінця, то з'являється спеціальне додаткове поле, подовжуюче кадр до мінімальної довжини 64 байта без урахування преамбули.

Час каналу ST (slot time) – це мінімальний час, протягом якого вузол зобов'язаний вести передачу, займати канал. Це відповідає передачі кадру мінімально допустимого розміру, прийнятого стандарту Ethernet IEEE 802.3. Час каналу пов'язано з максимально допустимою відстанню між вузлами мережі – діаметром колізійного домена.

Стандартом Ethernet регламентовані наступні правила виявлення колізій кінцевим вузлом мережі:

1. Вузол А повинен виявити колізію до того, як передасть свій 512-й біт, включаючи біти преамбули;
2. Вузол А повинен припинити передачу раніше, ніж буде переданий кадр мінімальної довжини – передано 576 біт (512 біт після обмежувача початку кадрів SFD);
3. Перекриття між передачами вузлів А та В – бітовий інтервал, починаючи з моменту передачі першого біта преамбули вузлом А і закінчуючи прийомом вузлом А останнього біта, испущеного вузлом, - повинно бути менше, ніж 575 ВТ.

Остання умова для мережі Ethernet є найбільш важливим, оскільки його виконання веде до виконання і перших двох. Це третя умова задає обмеження на діаметр мережі. Стосовно до затримки на подвійному пробігу RTD третє умову можна сформулювати у вигляді: $RTD < 575$ ВТ.

При передачі великих кадрів, наприклад 1500 байт, колізія, якщо вона взагалі виникне, виявляється практично на самому початку передачі, не пізніше перших 64 переданих байт (якщо колізія не виникла в цей час, то пізніше вона вже не виникне, оскільки всі станції прослуховують лінію і, чуючи передачу будуть мовчати). Так як jam-сигнал значно коротше повного розміру кадру, то при використанні алгоритму CSMA/CD кількість вхолосту витраченої ємності каналу скорочується до часу, необхідного на виявлення колізії. Раннє виявлення колізій призводить до більш ефективного використання каналу. Пізніше виявлення колізій, властиве більш протяжним мережам, коли діаметр колізійного домена складає кілька кілометрів, знижує ефективність роботи мережі.

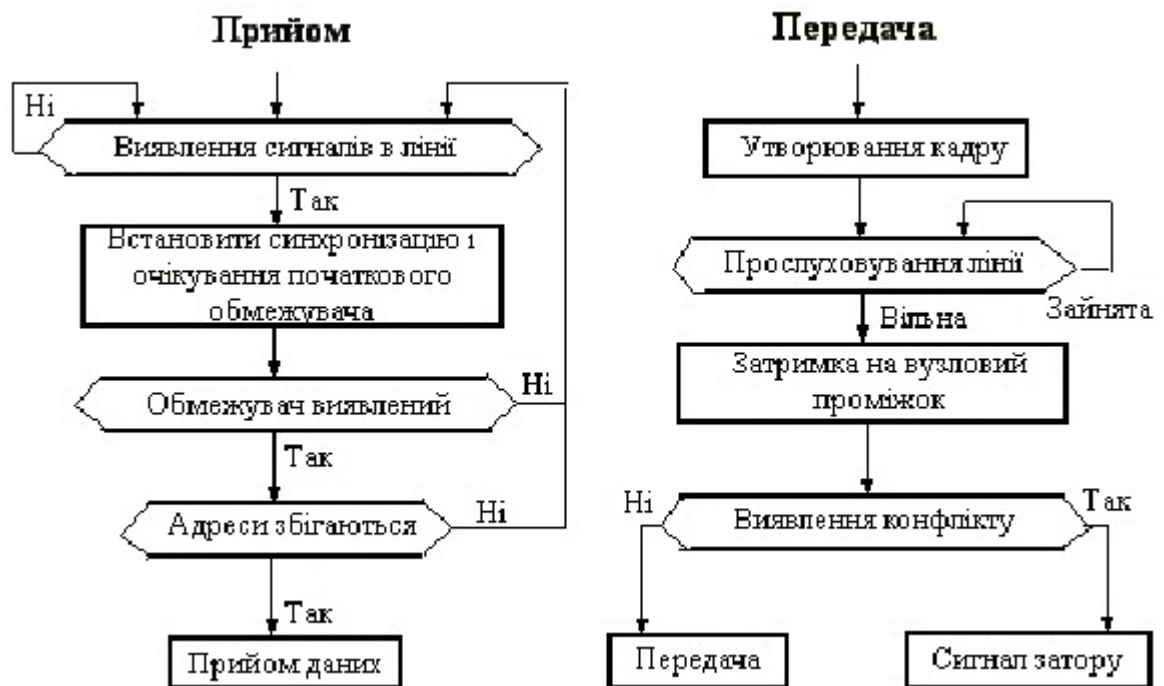


Рисунок 1.3 Алгоритми доступу по методу CSMA/CD

На рисунку 1.3 представлені алгоритми прийому і передачі даних в одному з вузлів при CSMA/CD.

Серед детермінованих методів переважають маркерні методи доступу.

Маркерний метод - метод доступу до середовища передачі даних у ЛОМ, заснований на передачі повноважень передавальної станції за допомогою спеціального інформаційного об'єкта, який називається маркером. Під повноваженням розуміється право ініціювати певні дії, динамічно що надаються об'єкту, наприклад станції даних в інформаційній мережі.

Застосовується ряд різновидів маркерних методів доступу. Наприклад, в естафетному методі передача маркера виконується в порядку черговості;

У способі селекторного опитування сервер запитує станції і передає повноваження одній з тих станцій, які готові до передачі. У кільцевих однорангових мережах широко застосовується тактований маркерний доступ, при якому маркер циркулює по кільцю і використовується станціями для передачі своїх даних.

1.3 Структуровані кабельні системи (СКС)

Структурованою кабельною системою (СКС) називається кабельна система:

- має стандартизовану структуру і топологію;
- використовує стандартизовані елементи (кабелі, роз'єми, комутаційні пристрої тощо);
- забезпечує стандартизовані параметри (швидкість передачі даних, затухання та ін.);
- керована (адміністрована) стандартизованим чином.

Зазначимо, що термін "стандартизований" не означає тут "однаковий", а визначає лише, що всі різні СКС будуються за однаковими принципами і правилами та у відповідності з національними і міжнародними стандартами в області інформаційних технологій.

До 1984 року будівлі проектувалися практично без урахування тих телекомунікаційних сервісів, які повинні були згодом функціонувати в них. З'являлися програми передачі даних вимагали застосування специфічних типів кабельних продуктів. Система IBM S/3X працювала на твінаксіальних кабелях 100 Ом, а Ethernet - на коаксіальних 50 Ом. У той час як місцеві телефонні компанії мали можливість монтувати свої кабельні системи для додатків передачі мови на стадії будівництва будівлі, фахівці з установки систем передачі даних отримували доступ на об'єкт вже після того, як він був заселений. Інфраструктура піддавалась переробкам, часто за рахунок великих додаткових витрат, і до незадоволення кінцевого користувача. У цей період мовні кабельні системи мали мінімальну структуру. Типова система в комерційному будівлі будувалася на основі неекранованої крученої пари (Unshielded Twisted Pair, UTP) з робочими характеристиками, придатними тільки для передачі мови, і мала конфігурацію "зірка". Кількість пар, що приходять в ключові точки варіювалося від 1 до 25.

Максимальні відстані передачі сигналів і кількість кросових комутаційних вузлів визначалися постачальником сервісу або виготовлювачем активного обладнання.

Ранні типи кабельних систем, що застосовувалися для передачі даних в 60-ті роки, ґрунтувалися, як правило, на передачу незбалансованого сигналу по кабелю "вита пара" між хост-комп'ютерами і терміналами. Такий тип кабельної системи застосовувався тільки для низькошвидкісних комунікацій, і, по мірі того, як швидкості передачі росли, обмеження, пов'язані з технологією передачі незбалансованого сигналу по кабелів "вита пара", стали занадто очевидними.

В середині 70-х років компанія IBM почала виробництво мейнфреймів, які використовували коаксіальний кабель з опором 93 Ом. Створення кількома роками пізніше пристрою, часто званого "балун" (BALUN - BALanced/UNbalanced), дозволило використовувати активне обладнання з коаксіальними інтерфейсами в кабельних системах на основі витої пари.

Адаптер типу "балун" здійснює конвертацію незбалансованого сигналу, що передається по коаксіальній середовищі, збалансований сигнал, який може поширюватися за кабелів "вита пара".

Після виникнення технології Ethernet на початку 80-х років, коаксіальний кабель з опором 50 Ом почав заповнювати комерційні будівлі. По мірі розширення популярності Ethernet, провідні виробники, такі як Cabletron та Bay Networks (колишня Synoptics), почали пропонувати мережеві інтерфейсні карти з модульними роз'ємами замість коаксіальних коннекторів.

Ця високошвидкісна технологія (10BASE-T) вимагала застосування першокласного кабелю "вита пара", оптимізованого для передачі даних, який пізніше був класифікований як UTP категорії 3.

У середині 80-х років компанія IBM розробила технологію Token Ring, визначивши як передавальної середовища двопарний екранований кабель "вита пара" (ЕВП) 150 Ом (Shielded Twisted Pair, STP). Однак, по мірі розширення застосування витої пари в мережевих додатках передачі даних, як альтернатива STP була введена у вжиток UTP як передавальної середовища для додатків Token Ring 4 і 16 Мбіт/с.

Протягом цього періоду користувачі були поставлені перед вибором кількох типів передавальних середовищ, які включали в себе UTP, STP, коаксіал, твінаксіал, подвійний коаксіал і оптичне волокно. Конектори, що використовувалися з вищепереліченими кабелями - модульні роз'єми, універсальні конектори передачі даних (UDC), BNC, твінакс, DB9, DB15, DB25 та різноманітні оптичні конектори. При придбанні кінцевим користувачем обладнання у нового виробника або при встановленні нової системи стара система зазвичай повністю була приречена на заміну. Замість вилучення непотрібних тепер кабелів з телекомунікаційних трас, вони часто залишалися на своєму місці і нова кабельна система прокладалася поверх старої. Найчастіше старі кабельні траси ставали настільки захаращеними, що доводилося створювати нові.

Для задоволення зростаючого попиту на телекомунікаційні кабельні системи, які могли підтримувати різні додатки, виробники створювали кабельні системи, які підтримували мовні програми та специфічні програми передачі даних. Незважаючи на появу таких тенденцій, кінцеві користувачі все ще були змушені робити вибір серед безлічі кабельних систем від різних виробників. У деяких випадках була можлива сумісність, в інших її не було. Відсутність однорідності й універсальності змусило промисловість до розробки стандартів, які б

гарантували сумісність між продукцією різних виробників. Для задоволення цієї вимоги в 1985 році Асоціація електронної промисловості (EIA) та Асоціація телекомунікаційної промисловості (TIA) організували роботу технічних комітетів для розробки однорідного сімейства стандартів телекомунікаційних кабельних систем. Ці комітети працювали більше 6-ти років в напрямку розробки перших впорядкованих стандартів телекомунікаційного кабелювання, телекомунікаційних трас і приміщень. Розроблені стандарти набули поширення в багатьох країнах і були вироблені додаткові специфікації до розділів з адміністрування, систем заземлення, а також універсальні категорії кабельних продуктів і відповідних конекторів для середовища UTP/STP 100 Ом. Робота над стандартами кабельних систем була продовжена новим виданням стандарту ANSI/TIA/EIA-568-A і знаходяться в даний час на стадії публікації стандартом ANSI/TIA/EIA-568-B, а також випуском міжнародного стандарту універсальної кабельної системи ISO/IEC 11801 і європейського стандарту універсальної кабельної системи CENELEC EN 50173.

До 1991 року законодавцями в телекомунікаційних кабельних системах були компанії-виробники комп'ютерної техніки. Кінцеві користувачі найчастіше виявлялися в неприємному становищі через те що суперечили вимогам окремих виробників або один одному по робочим характеристикам систем і були змушені платити великі суми за монтаж, налагодження та експлуатацію приватних систем.

Промисловість засобів телекомунікацій визнавала необхідність створення економічної, ефективної кабельної системи, яка могла б підтримувати найбільш можливо широкий спектр додатків і устаткування. EIA, TIA і представницький консорціум провідних телекомунікаційних компаній почали спільну роботу по створенню стандарту на телекомунікаційні кабельні системи комерційних будівель ANSI/EIA/TIA-568-1991 (Commercial Building Telecommunications Cabling Standard).

Додаткові нормативні документи, що описують вимоги і правила по проектуванню і монтажу телекомунікаційних кабельних трас і приміщень, адміністрування систем, специфікації кабельних компонентів і комутаційного обладнання, були випущені слідом за ним. Стандарт ANSI/EIA/TIA-568-1991 був переглянутий у 1995 році і в даний час носить назву ANSI/TIA/EIA-568-A.

Метою зазначених стандартів є опис структурованого кабелювання - телекомунікаційної кабельної системи, яка може віртуально підтримувати будь-які додатки передачі мови, зображення і даних за бажанням кінцевого користувача.

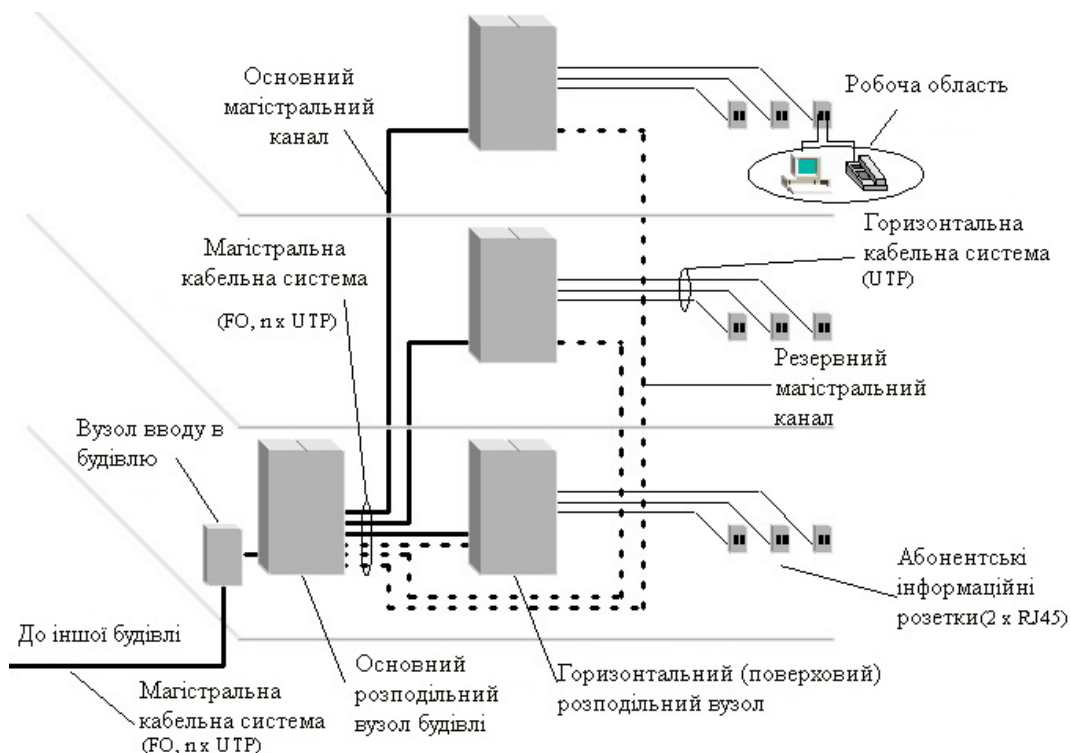


Рисунок 1.4 Схема типової СКС

В даний час у міру того, як все більша кількість користувачів переходять до застосування відкритих систем, що випускається активне обладнання проектується на основі положення, що кабельна частина інформаційної інфраструктури не відповідає вимогам стандартів, тобто є гарантовано надійною та здатною забезпечувати певні робочі характеристики. До різних ризиків, які є наслідком нестандартних кабельних систем, можна віднести наступні - мережеві робочі характеристики нижче визначених стандартами, підвищена вартість внесення змін в систему та нездатність системи підтримувати нові технології. По мірі поширення принципів структурованого каблирования вартість встановлюється мережевого обладнання падала, а ефективність передачі даних зростала з експоненціальною залежністю. Телекомунікаційна інфраструктура переросла в доступний інструмент бізнесу з широкими можливостями.

Структурована кабельна система (СКС) є основоположною базою протягом всього часу існування інформаційної мережі. Це основа, від якої залежить функціонування всіх ділових додатків. Правильно спроектована, змонтована кабельна система знижує витрати будь-якої організації на всіх фазах свого життя.

За даними статистики недосконалі кабельні системи є причиною до 70% всіх простоїв інформаційної мережі. Монтуючи СКС, створену у відповідності з положеннями стандартів, можна ефективно усувати значну частку часу простоїв.

Незважаючи на те, що кабельна система, як правило, існує довше більшості інших мережевих компонентів, її вартість становить невелику частину загальних інвестицій в

інформаційну мережу. Таким чином, використання структурованої кабельної систем є досить переконливим способом інвестування продуктивність будь-якої організації або компанії.

Кабельна система є компонентом мережі з самим тривалим часом життя, довше якого існує тільки каркас будівлі. Кабельна система, створена на основі стандартів, гарантує довготривале функціонування мережі і підтримку численних додатків, забезпечуючи віддачу від інвестицій на всьому протязі її існування.

Вита пара (twisted pair) - це кабель на мідній основі, що поєднує в оболонці одну або більше пар провідників. Кожна пара являє собою два перевитих навколо один одного ізольованих мідних провідників. Кабелі даного типу часто сильно відрізняються за якістю і можливостями передачі інформації. Відповідності характеристик кабелів певного класу чи категорії визначають загальновизнані стандарти (ISO 11801 і TIA-568). Самі характеристики безпосередньо залежать від структури кабелю і застосовуваних у ньому матеріалів, які і визначають фізичні процеси, що проходять в кабелі при передачі сигналу.

Кабель типу "вита пара" (TP, Twisted Pair) буває двох видів: екранована вита пара (STP, Shielded Twisted Pair) і неекранована вита пара (UTP, Unshielded Twisted Pair). Також підрозділяється на одножильну і багатожильну виту пару, а також виту пару для зовнішньої прокладки.

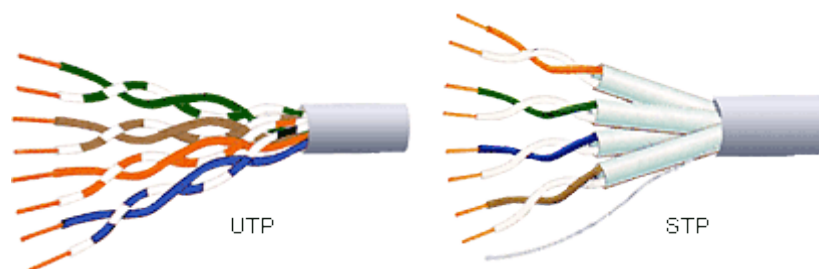


Рисунок 1.5 Кабель «вита пара»

Неекранована вита пара (Unshielded Twisted Pair): поділяється на категорії 1,2,3,4,5,5 е,6;7. Найпоширеніші нині категорії - 5 і 5-е, зі швидкістю передачі даних 10,100 і 1000 Мб/с. Кабелі випускаються в 4-парному виконанні. Всі пари мають певний колір і крок скрутки. Зазвичай дві пари призначені для передачі даних, а дві – для передачі голосу. Для з'єднання кабелю з обладнанням використовуються вилки і розетки RJ-45. Діаметр кабелю: 22 AWG, 24 AWG, 26 AWG. Чим більше номер, тим менше його діаметр.

Екранована вита пара (Shielded Twisted Pair): поділяється на категорії 5,5 е,6,7. Основне призначення цих кабелів – підтримка високошвидкісних протоколів. Екранована вита пара добре захищає передаються сигнали від зовнішніх перешкод і використовується тільки для передачі даних.

Переваги і недоліки витої пари:

Переваги: Простота установки, відмовостійкість, висока продуктивність.

Недоліки: Обмежена довжина, слабка завадостійкість від наведень (силові трансформатори, передавальні пристрої, лампи денного світла).

Таблиця 1.1 Параметри фізичного рівня для мереж Ethernet і Fast Ethernet

Мережа	10Base-2	10Base-T	100Base-TX
Кабель	Тонкий коаксіальний кабель RG-58	Неекранована на вита пара категорії 3 та 5	Неекранована вита пара категорії 5e
Максимальна довжина сегмента, м	185	100	100
Максимальна відстань між вузлами мережі (при використанні повторювачів), м	925	500	200
Максимальне число станцій у сегменті	30	1024	1024

Характеристичний імпеданс відповідає вхідного імпедансу однорідної лінії передачі нескінченної довжини, тобто лінії передачі граничної довжини, термінованим навантаженням зі значенням її власного характеристичного імпедансу. У загальному випадку, характеристичний імпеданс - це комплексне число з резистивної і реактивної компонентами. Він є функцією частоти переданого сигналу і не залежить від довжини лінії. При дуже високих частотах характеристичний імпеданс асимптотично прагне до фіксованого резистивного опору. Наприклад, коаксіальні кабелі мають імпедансом 50 або 75 Ом на високих частотах. Типове значення імпедансу для кабелів "вита пара" - 100 Ом при частотах понад 1 МГц.

Загасання сигналу - це відношення в децибелах (дБ) потужності вхідного сигналу до потужності сигналу на виході при відповідності імпедансів джерела і навантаження характеристичному імпедансу кабелю. Значення вхідної потужності може бути отримано шляхом вимірювання потужності при безпосередньому підключенні навантаження до джерела без проходження сигналу по кабелю. У випадках, коли в місцях завершення імпеданси не ідеально відповідають один одному, ставлення вхідної потужності до вихідній носить назву внесених втрат або внесеного затухання.

Перехідне загасання на ближньому кінці (Near End модуль crosstalk, NEXT) - параметр, що характеризує затухання сигналу перешкоди, наведеного сигналом, що проходять по одній

парі провідників, на іншу, розташовану поблизу. Вимірюється в дБ. Чим вище значення NEXT, тим краще ізоляція перешкод між двома парами провідників.

Зворотні втрати (втрати при відображенні). Коли імпеданс кабелю і навантаження не співпадає, сигнал, що розповсюджується по кабелю, частково буде відображатися в точці інтерфейсу кабель-навантаження.

Потужність відбитого сигналу носить назву втрат при відображенні або зворотних втрат. Чим краще сумісність імпедансів, тим менше відображається потужність і тим нижче зворотні втрати.

Тимчасова затримка поширення сигналу. Сигнал, що розповсюджується від вхідної точки до вихідній, приходять з тимчасовою затримкою, величина якої є відношенням довжини кабелю до швидкості поширення сигналу V в передавальній середовищі. У випадку ідеальної лінії передачі, що складається з двох провідників у вакуумі, швидкість поширення сигналу дорівнює швидкості поширення світла у вакуумі. На практиці швидкість поширення сигналу в кабелі залежить від властивостей діелектричних матеріалів, що оточують провідники.

Відношення сигнал-шум (SNR) - це співвідношення між рівнем сигналу і рівнем шуму приймається, причому рівень сигналу повинен значно перевищувати рівень шуму для забезпечення прийнятних умов передачі.

Ставлення до загасання перехідного загасання (ACR). Співвідношення між сигналом і шумом може бути виражена у формі відношення до загасання перехідного загасання (ACR). ACR - це різниця між ослабленим сигналом на виході і шкідливим наведеним сигналом ("шумом") NEXT.

Волоконно-оптичний кабель – кабель, що містить одне або кілька оптичних волокон для передавання даних у вигляді світла. В залежності від конструктивного виконання волоконно-оптичні кабелі поділяються на кабелі внутрішньої і зовнішньої прокладки, а також кабелі для шнурів.

Волоконно-оптичні комунікації мають ряд переваг в порівнянні з електронними системами, що використовують передавальні середовища на металевій основі. У волоконно-оптичних системах передаються сигнали спотворюються однією з форм зовнішніх електронних, магнітних або радіочастотних перешкод. Таким чином, оптичні кабелі повністю несприйнятливі до перешкод, що викликаються блискавками або джерелами високої напруги.

Цифрові обчислювальні системи, телефонія і видеовещательные системи вимагають нових напрямків для покращення передавальних характеристик. Велика ширина спектра оптичного кабелю означає підвищення ємності каналу. Крім того, більш довгі відрізки кабелю вимагають меншої кількості репітерів, так як волоконно-оптичні кабелі мають надзвичайно

низькими рівнями загасання. Це властивість ідеально підходить для широкомовних і телекомунікаційних систем.

Порівняно із звичайними коаксіальними кабелями з рівною пропускнуою здатністю, менший діаметр і вага волоконно-оптичних кабелів означає порівняно більш легкий монтаж, особливо в заповнених трасах. 300 метрів одноволоконного кабелю важать близько 2,5 кг. 300 метрів аналогічного коаксіального кабелю важать 32 кг - приблизно в 13 разів більше.

Основні елементи оптичного волокна:

Ядро. Ядро – світло-передавальна частина волокна, що виготовляється або з скла, або з пластику. Чим більше діаметр ядра, тим більша кількість світла може бути передано по волокну.

Демпфер. Призначення демпфера - забезпечення більш низького коефіцієнта заломлення на межі з ядром для перевідбиття світла в ядро таким чином, щоб світлові хвилі поширювалися по волокну.

Оболонка. Оболонки зазвичай бувають багат шаровими, виготовляються з пластику для забезпечення міцності волокна, поглинання ударів та забезпечення додаткового захисту волокна від впливу навколишнього середовища. Такі буферні оболонки мають товщину від 250 до 900 мкм.



Рисунок 1.6 Оптичний кабель

Розмір волокна у загальному випадку визначається за зовнішнім діаметром його ядра, демпфера і оболонки. Наприклад, 50/125/250 - характеристика волокна з діаметром ядра 50 мкм, діаметром демпфера 125 мкм і діаметром оболонки 250 мкм. Оболонка завжди видаляється при з'єднанні або термінаторованні волокон.

Тип волокна ідентифікується за типом шляхів, або так званих "мод", прохідних світлом в ядрі волокна. Існує два основних типи волокна - багатомодове і одномодове. Ядра багатомодових волокон можуть володіти ступінчастим або градієнтним показниками заломлення. Багатомодове волокно зі східчастим показником заломлення отримало свою назву від різкої, ступеневої, різниці між показниками заломлення ядра і демпфера. У більш

поширеному багатомодовому волокну з градієнтним показником заломлення промені світла також поширюються в волокні за численними шляхами. На відміну від волокна зі східчастим показником заломлення, ядро з градієнтним показником містить численні шари скла, кожен з яких володіє більш низьким показником заломлення порівняно з попереднім шаром по мірі віддалення від осі волокна. Результатом формування такого градієнта показника заломлення є те, що промені світла прискорюються в зовнішніх шарах і їх час поширення в волокні порівнюється з часом поширення променів, що проходять за більш короткими шляхами ближче до осі волокна.

Таким чином, волокно з градієнтним показником заломлення вирівнює час поширення різних мод так, що дані по волокну можуть бути передані на більш далекі відстані і на більш високих швидкостях до того моменту, коли імпульси світла почнуть перекриватися і ставати невидимими на стороні приймача.

Волокна з градієнтним показником представлені на ринку з діаметрами ядра 50, 62,5 і 100 мкм.

Одномодовое волокно, на відміну від багатомодового, дозволяє поширюватися тільки одного променя або моді світла в ядрі. Це усуває будь-яке спотворення, що викликається перекриттям імпульсів. Діаметр ядра одномодового волокна надзвичайно малий - приблизно 5-10 мкм. Одномодовое волокно володіє більш високою пропускнуою здатністю, ніж будь-який з багатомодових типів. Наприклад, підводні морські телекомунікаційні кабелі можуть нести 60000 мовних каналів по одній парі одномодових волокон.

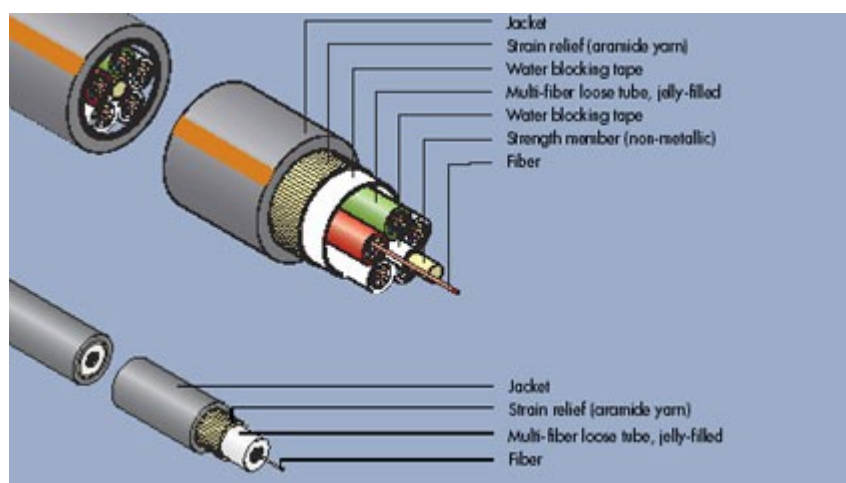


Рисунок 1.7 Одномодовий і багатомодовий кабель

Власні втрати оптичного волокна:

Світло є електромагнітною хвилею. Швидкість світла зменшується при розповсюдженні по прозорим матеріалів порівняно зі швидкістю поширення світла у вакуумі. Хвилі

інфрачервоного діапазону також поширюються по-різному по оптичному волокну. Тому затування, або втрати оптичної потужності, повинні вимірюватися на специфічних довжинах хвиль для кожного типу волокна. Довжини хвиль вимірюються в нанометрах (нм).

Втрати оптичної потужності на різних довжинах хвиль відбуваються в оптичному волокну внаслідок поглинання, відбиття та розсіювання. Ці втрати залежать від пройденої відстані і конкретного виду волокна, його розміру, робочої частоти і показника заломлення. Величина втрат оптичної потужності внаслідок поглинання і розсіювання світла на певній довжині хвилі виражається в децибелах оптичної потужності на кілометр (дБ/км).

Волокна оптимізовані для роботи на певних довжинах хвиль. Наприклад, можна досягти втрат в 1 дБ/км для багатомодового волокна 50/125 мкм на довжині хвилі 1300 нм і менше 3 дБ/км (50%-е втрати потужності) для того ж волокна на 850 нм. Ці два хвильових регіону, - 850 і 1300 нм, є областями найбільш часто визначаються для робочих характеристик оптичних волокон і використовуються сучасними комерційними приймачами і передавачами. Крім того, одномодові волокна оптимізовані для роботи в регіоні 1550 нм.

У коаксильному кабелі чим більше частота, тим більше зменшується амплітуда сигналу зі збільшенням відстані, і це явище називається загасанням. Частота для оптичного волокна постійна до тих пір, поки вона не досягне межі діапазону робочих частот. Таким чином, оптичні втрати пропорційні тільки відстані. Таке загасання у волокну викликано поглинанням і розсіюванням світлових хвиль на неоднорідностях, викликаних хімічними забрудненнями, і на молекулярній структурі матеріалу волокна. Ці мікрооб'єкти у волокну поглинають або розсіюють оптичне випромінювання, воно не потрапляє в ядро і втрачається. Загасання у волокну специфікується виробником для певних довжин хвиль: наприклад, 3 дБ/км для довжини хвилі 850 нм. Це робиться тому, що втрати волокна змінюються із зміною довжини хвилі.

Втрати на мікро згинах. Без спеціального захисту оптичне волокно схильне втрачати кількість оптичної потужності внаслідок мікро згинів. Мікро згини - це мікроскопічні спотворення волокна, що викликаються зовнішніми силами, які призводять до втрати оптичної потужності з ядра. Для запобігання виникнення мікро згинів застосовуються різні типи захисту волокна. Волокна зі східчастим показником щодо більш стійкі до втрат на мікро згинах, ніж волокна з градієнтним показником.

Смуга пропускання (ширина спектра) - це міра здатності волокна передавати певні обсяги інформації в одиницю часу. Чим ширше смуга, тим вище інформаційна ємність волокна. Смуга виражається в МГц-км.

Наприклад, по волокну з смугою 200 МГц-км можна передавати дані з частотою 200 МГц на відстані до 1 км або з частотою 100 МГц на відстані до 2 км. Завдяки порівняно великій смузі пропускання, волокна можуть передавати значні обсяги інформації. Одне волокно з градієнтним

показником заломлення може з легкістю передавати 500 мільйонів біт інформації в секунду. Тим не менш, для всіх типів волокон існують обмеження ширини смуги, що залежать від властивостей волокна і типу використовуваного джерела оптичної потужності.

Для точного відтворення передаються дані по волокну світлові імпульси повинні поширюватися окремо один від одного, маючи чітко помітну форму і межі імпульсні проміжки. Однак промені, що несуть кожен з імпульсів, що проходять різними шляхами всередині багатомодового волокна. Для волокон зі східчастим показником заломлення променів, проходячи зигзагоподібно по волокну під різними кутами, досягають приймача в різний час.

Це розходження в часі прибуття імпульсів в точку прийому призводить до того, що імпульси на виході лінії спотворюються і накладаються один на одного. Це так зване модальне розсіювання, або модальна дисперсія, або розширення світлового імпульсу обмежує можливу для передачі частоту, так як детектор не може визначити, де закінчується один імпульс і починається наступний. Різниця в часах проходження найшвидшою і самої повільної мод світла, що входять у волокно в один і той же час і проходять 1 км, може бути всього лише 1-3 нс, проте така модальна дисперсія тягне за собою обмеження по швидкості в системах, що працюють на великих відстанях. Подвоєння відстані подвоює ефект дисперсії.

Модальна дисперсія часто виражається в наносекундах на кілометр, наприклад, 30 нс/км. Також вона може бути виражена і в частотній формі, наприклад 200 МГц-км. Це означає, що волокно або система будуть ефективно працювати в межах частот до 200 МГц, перш ніж розсіювання почне позначатися на пропускну здатності на відстанях більше одного кілометра. Ця ж система зможе передавати сигнал з частотою 100 МГц на відстань у два кілометри.

Дисперсія робить багатомодове волокно зі східчастим показником заломлення найменш ефективним по ширині смуги серед усіх трьох типів волокна. Тому воно використовується на більш коротких ділянках і низьких частотах передачі. Типовим значенням ширини ступеневої смуги волокна є 20 МГц-км.

Розміри ядра одномодового волокна малі - від 8 до 10 мкм, що дозволяє проходити по волокну тільки одному променю світла. Так як модальна дисперсія в цьому випадку повністю відсутня, смуга пропускання у такого волокна набагато більше, ніж у багатомодового, що дозволяє досягати робочих частот понад кілька сотень гігагерц на кілометр (ГГц-км).

Оптичні волокна володіють ще одним різновидом дисперсії, що виникає внаслідок того, що різні довжини хвиль, що поширюються в середовищі з різною швидкістю. Таку "спектральну дисперсію" можна спостерігати, коли білий світ розпадається на сім кольорів веселки, проходячи через скляну призму. Хвилі, що представляють різні кольори рухаються в середовищі з різною швидкістю, що призводить до розбіжностей в траєкторії поширення променів. Якби оптичне джерело волоконної системи випромінював світло однієї частоти,

спектральна дисперсія або матеріальна дисперсія (або хроматична дисперсія, як її ще часто називають) була б усунута. Насправді, абсолютно монохроматичних джерел світла не існує. Лазери володіють певним, хоча і дуже невеликим, розширенням спектру випромінюваного світла. У джерел світла на основі LED (напівпровідникові світлодіоди) спектральний діапазон в 20 разів більше ніж у лазера, і спектральна дисперсія, в свою, чергу набагато вище. Дисперсія в скляному волокні мінімальна в регіоні близько 1300 нм, дозволяючи одномодовим волокнам мати значну смугу на даній довжині хвилі.

Одномодовое волокно зазвичай використовується з лазерними джерелами завдяки своїй високій спектральній чистоті. Для забезпечення ефективного функціонування таких систем потрібні прецизійні коннектори і муфти.

Завдяки своїм низьким втратам і високим пропусковим характеристиками, одномодові волокна, як правило, є найкращим і, як правило, єдиним вибором для монтажу протяжних високошвидкісних ліній, таких як міжміські телекомунікаційні системи.

Між одномодовим волокном і волокном зі східчастим показником заломлення волокна розташовуються з градієнтним показником заломлення. Для зменшення ефекту модальної дисперсії промені в таких волокнах поступово перенаправляються назад до осі ядра. Волокна з градієнтним показником заломлення мають набагато більшу смугу, ніж волокна зі східчастим показником заломлення. За волокні з градієнтним показником заломлення з смугою 600 МГц-км можна передавати сигнал з модуляцією 20 МГц на відстань до 30 км. Вартість такого скляного волокна є однією з найнижчих. Малі втрати потужності сигналу, який передається плюс велика смуга дозволяють використовувати його для монтажу локальних мереж.

Бездротові комп'ютерні мережі – це технологія, що дозволяє створювати обчислювальні мережі, повністю відповідні стандартам для звичайних дротяних мереж (наприклад, Ethernet), без використання кабельної проводки. В якості носія інформації в таких мережах виступають радіохвилі НВЧ-діапазону.

Бездротові мережі використовуються там, де кабельна проводка утруднена або неможлива. Мережа розгорнута у відповідності зі стандартом "RadioEthernet", являє собою аналог звичайної кабельної мережі Ethernet з колізійним механізмом доступу до середовища передачі даних. Різниця полягає лише в характері цього середовища. Radio Ethernet повністю забезпечує всі потреби бездротової передачі даних усередині приміщень.

При зовнішньому застосуванні RadioEthernet дуже зручно використовувати мережі "останньої милі" натомість кабельної, тобто – для з'єднання між абонентом та найближчим вузлом опорної мережі. При цьому реальна протяжність "останньої милі" може бути від кількох сотень метрів до 20-30 км і обмежена лише наявністю прямої видимості.

Горизонтальна кабельна система починається телекомунікаційною розеткою на робочому місці і закінчується горизонтальним кросом в телекомунікаційній шафі. Вона включає в себе: розетку, горизонтальний кабель, точки завершення і патч-корди (кросировочні перемички), що представляють собою горизонтальний крос.

Горизонтальна кабельна система повинна мати топологічну конфігурацію "зірка". Кожне робоче місце з'єднано безпосередньо з горизонтальним кросом в телекомунікаційній шафі. Максимальна довжина будь-якого горизонтального кабельного сегменту не повинна перевищувати 90 м незалежно від типу використовуваної передавальної середовища.

Горизонтальні кабелі за своєю кількістю займають перше місце в усьому обсязі кабельних сегментів телекомунікаційної інфраструктури будівлі. Незважаючи на те, що стандарт E1A/T1A 568 звужує коло можливих варіантів кабельної продукції, одним з основних моментів при плануванні СКС є правильний вибір типу передавальної середовища для забезпечення підтримки можливих змін в майбутньому.

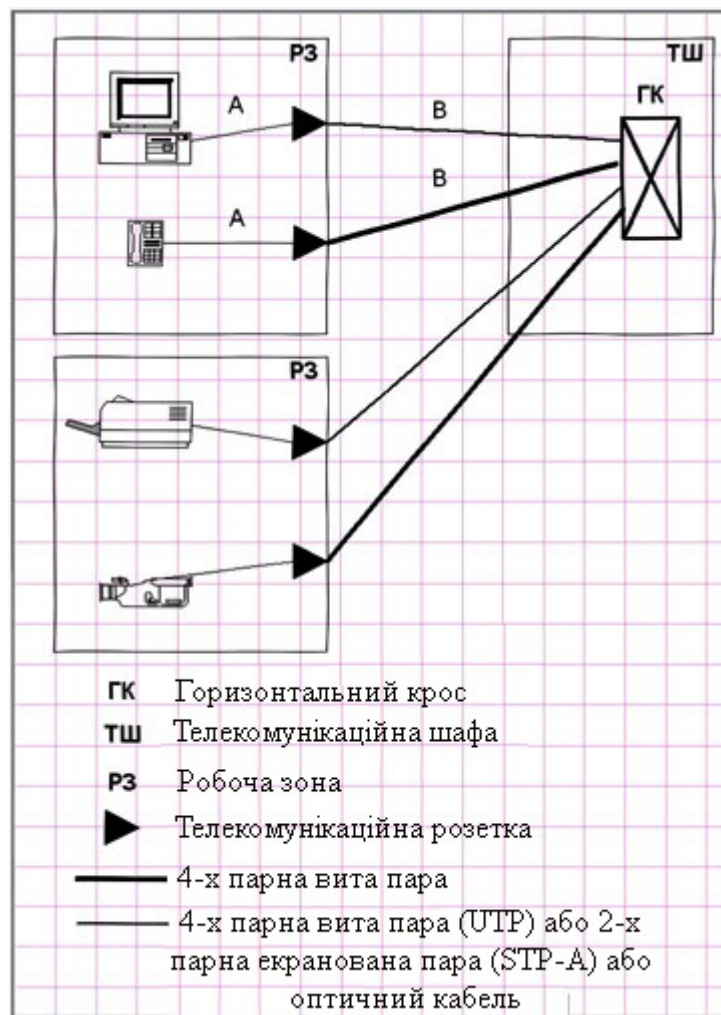


Рисунок 1.8 Приклад горизонтальної кабельної системи

Застосовуваний тип кабелю повинен служити більше одного планованого періоду розвитку телекомунікаційної мережі. У горизонтальній підсистемі стандартом 586 дозволяється використовувати наступні типи передавальних середовищ:

- Кабель UTP 4 пари, 100 ом;
- Багатомодове оптичне волокно 62,5/125 мкм;
- Кабель STP-A 2 пари, 150 ом;
- Коаксіальний кабель 50 ом.

Коаксіальний кабель 50 Ом визнається стандартом '568 як передавальної середовища, але не рекомендується для нових систем. Дозволяється монтаж додаткових коаксіальних розеток. Такі розетки є доповненням і не можуть замінювати мінімально необхідні стандартом.

Компоненти, призначені для підтримки специфічних додатків (наприклад, різноманітні типи адаптерів і конверторів), не можуть бути використані в якості елемента горизонтальної кабельної системи. При необхідності вони повинні розташовуватися поза, відносно телекомунікаційної розетки або горизонтальному кросу. Це вимога стандарту має своєю метою забезпечення максимальної універсальності кабельної системи та її незалежність від конкретних додатків і інтерфейсів.

Однією з основних проблем "мідних" кабельних систем є їх схильність до впливу електромагнітних завад. З цієї причини стандарт '568 наказує при проектуванні кабельних систем враховувати розташування потенційних джерел перешкод. Конкретні специфікації по розділенню кабельних інфраструктур та джерел перешкод визначені у стандарті ANSI/EIA/TIA-569.

При каблірованні відкритих офісних просторів часто застосовується плоский 4-парний кабель. Місце сполучення такого кабелю і круглого розподільного кабелю, що приходить від горизонтального кросу, носить назву "перехідною точки" (TP -Transition Point). Стандарт допускає застосування однієї перехідною точки між різними формами одного типу кабелю на одному сегменті горизонтального кабелю.

Стандарт забороняє використання в горизонталі шунтированих відводів, (тобто поява одних і тих же пар кабелю на декількох телекомунікаційних розетках, або, говорячи простою мовою, - запаралелювання ліній), а також використання муфт для металевих кабелів. Необхідність використання муфт горизонтальних сегментах, довжина яких не може перевищувати 90 м, необґрунтована, в той час як їх наявність може значно погіршувати робочі передавальні характеристики горизонтальної лінії.

У разі волоконно-оптичних систем встановлення муфт дозволена, але рекомендується обмежити їх застосування телекомунікаційних шафою. Як правило, муфти у волоконно-оптичних системах і застосовуються в телекомунікаційних шафах при термінуванні

розподільних волоконно-оптичних кабелів так званими шнурами pig-tail. Ця технологія дозволяє здійснювати перехід і підключення розподільчих кабелів, що містять в собі волокна, як правило, невеликого розміру (діаметр буфера ~ 250 мкм) з коннекторами, потребують завершення волокна з буферами більшого розміру (~ 900 мкм). Шнур pig-tail являє собою короткий відрізок волоконно-оптичного кабелю довжиною близько 1-3 м, термінований в заводських умовах коннектором. З'єднання розподільного кабелю і шнура pig-tail здійснюється з допомогою, як правило, зварної муфти, забезпечує високоякісний перехід з низькими втратами близько 0,01 - 0,1 дБ.

При каблюванні робочих місць стандарт 568 для забезпечення мінімального універсального сервісу кінцевому користувачеві наказує встановлювати, як мінімум, дві телекомунікаційні розетки на кожному індивідуальному робочому місці. Кількість розеток (2) було обрано на підставі середньостатистичної конфігурації сучасного телекомунікаційного сервісу - телефонія і програми передачі даних (ЛОМ). Одна з двох розеток на вимогу стандарту повинна бути сумісна з 4-парним кабелем UTP 100 Ом (категорії 3 або вище), а друга - або з 4-парним кабелем UTP 100 Ом (рекомендується категорія 5), або з 2-парним кабелем STP-A 150 Ом або з многомодовим волоконно-оптичним кабелем 62,5/125 мкм. Якщо горизонтальної кабельної системи були застосовані екрановані компоненти, що потребують під'єднання до телекомунікаційної системи заземлення, стандарт вимагає, щоб ця система заземлення відповідала відповідним будівельним нормативам, а також стандарту ANSI/TIA/EIA-607. Оскільки в різних регіонах і країнах можуть діяти місцеві національні нормативи заземлення, наведене вище вимога стандарту можна трактувати наступним чином: "... система заземлення повинна відповідати відповідним будівельним нормативам, а також місцевим і національним нормативам і інструкцій з систем заземлення".

1.4 Комутаційне обладнання

Робоче місце за визначенням стандарту служить інтерфейсом між горизонтальної кабельної системою, яка закінчується телекомунікаційної розеткою, і активним обладнанням кінцевого користувача. Обладнання робочого місця та кабель (апаратний шнур), використовуваний для підключення активного обладнання, що не входять у сферу дії стандарту '568. Нижче перераховані деякі специфікації, що відносяться до каблірованого робочого місця.

Довжини горизонтальних кабелів визначаються з припущення, що максимально допустима довжина кабелю для підключення активного обладнання на робочому місці дорівнює 3 м. Робочі характеристики (категорія) шнурів активного обладнання повинні відповідати або бути краще робочих характеристик патч-кордів тієї ж категорії.

Адаптери та пристрої, що призначені для підтримки специфічних додатків, повинні встановлюватись поза, відносно телекомунікаційної розетки. При використанні таких адаптерів передбачається, що вони сумісні з категорією того горизонтального кабелю, до якого вони приєднуються.

Телекомунікаційні шафи в загальному випадку розглядаються як пристрої, призначені для обслуговування горизонтальній розподільної системи. Крім цієї основної функції, вони можуть виконувати й додаткові - у них допускається розміщення проміжних і головних кросів. Нижче перераховані деякі специфікації, що відносяться до каблірованих телекомунікаційних шаф.



Рисунок 1.9 Телекомунікаційна шафа

Не дозволяється використовувати перетермінованих горизонтальних кабелів для внесення штатних змін в кабельну систему. Для цих цілей слід використовувати кросировочні перемички і патч-корди.

Пристрої, призначені для підтримки специфічних додатків (наприклад, різного роду адаптери), не можуть бути частиною горизонтальної кабельної системи і повинні встановлюватися поза по відношенню до горизонтального кросу.

Для уникнення деформації кабелів внаслідок тугого скручування в пучки, занадто крутих вигинів і розтягуючих зусиль, слід використовувати обладнання, спеціально призначене для укладання і маршрутизації кабельних потоків.

Кабелі та шнури, використовувані для підключення активного обладнання, не розглядаються стандартом в якості елементів кабельної системи. Максимально допустима сумарна довжина всіх патч-кордів і апаратних шнурів на обох кінцях лінії -10м.

Дозволяється використовувати лише обладнання, що відповідає вимогам стандартів. Телекомунікаційні шафи повинні бути спроектовані й обладнані відповідно до вимог стандарту ANSI/EIA/TIA-569.

Підключення активного обладнання в телекомунікаційній шафі дозволяється здійснювати за допомогою двох типів сполук - "міжсполучення" та "крос-з'єднання".

Крос-з'єднання - застосовується для комутації кабельних підсистем між собою і для підключення активного обладнання з багатопортовим коннекторами. Багатопортовим коннекторами називаються конструкції, вузли, за допомогою яких реалізується одночасне підключення більше одного (декількох) адресного телекомунікаційного порту. Типовим зразком багатопортового коннектора є так званий Telco-коннектор (коннектор "телефонної компанії", Telephone Company connector) - 25-парний коннектор, який знайшов масове застосування в телефонії для підключення офісних АТС, а також іноді використовується для підключення активного мережевого обладнання. Метод крос-з'єднання (cross-connection) на відміну від описаного нижче методу міжз'єднання дозволяє гнучко переконфігурувати кабельну систему у всіх випадках, але в той же час і вимагає наявності в кросі, як мінімум, двох одиниць комутаційного обладнання, що підвищує вартість системи. Якщо поняття "крос" (cross-connect) використовується для визначення засобу, що дозволяє здійснювати обтиск кабелів і їх міжз'єднання або крос-з'єднання (або обидва) з допомогою патч-кордів, кроссировочних перемичок або кабелів активного обладнання, то поняття "крос-з'єднання" відноситься до конкретної конфігурації, в якій кабелі і патч-корди або перемички використовуються для комутації окремих розподільчих полів, які обслуговують горизонтальну і магістральну кабельні системи та обладнання телекомунікаційних приміщень.

Міжз'єднання - дозволяється використовувати тільки для підключення активного обладнання з однопортовими коннекторами. В протилежність багатопортовим коннекторів однопортові дозволяють здійснювати комутацію між собою тільки двох адресних портів. Метод міжз'єднання корисний у тих випадках, коли здійснюватися підключення до кабельної системи активного обладнання з однопортовими (модульними) коннекторами, яке саме по собі як би є одиницею комутаційного кросового обладнання, такого, наприклад, як патч-панель. У цьому випадку з'являється можливість необмеженого перемикання адресних портів та, за рахунок виключення другої одиниці комутаційного обладнання з конфігурації кросу, зниження витрат на підключення.

Основним компонентом, призначеним для завершення кабелів і провідників в телекомунікаційних шафах і на робочих місцях, є комутаційний блок. Комутаційні блоки можуть мати найрізноманітніші форми та конструкції і за роки свого розвитку вони перетворилися в досить складний "системний" компонент. Комутаційний блок може бути

інтегрований і в патч-панель. Існує два основних типи комутаційних блоків - блок типу 66 і блок типу 110. Обидва типу в даний час пропонуються великою кількістю виробників, і багато версії термінаційних блоків інтегровані у такі компоненти, як коннектори розеток і патч-панелі. Ці два типи домінують у встановлених системах і на нових ринках збуту, тому їм буде приділено детальне увагу. Крім того, розглянуто пара "приватних" термінаційних систем, які виробляються тільки одним виробником і поширені не так широко (BIX і KRONE). На ринку можна знайти кілька інших типів блоків, але незалежно від типу, всі вони використовують один і той же метод створення контакту шляхом зміщенням ізоляції – провідник проштовхується між двома металевими поверхнями контакту (зазвичай за допомогою спеціального терминирующего інструменту) і ізоляція або віддаляється, або прорізається, або зміщується.

Найбільш часто застосовуються чотири типи комутаційних блоків - 66, 110, BIX, і KRONE.

Стандарт EIA/TIA-568-A наказує використання комутаційних блоків з типом контакту IDC - "контакт зі зміщенням ізоляції" (IDC - Insulation Displacement Connection). Блоки 110, KRONE та BIX використовують контакти IDC. Тип 66, незважаючи на відповідність вимогам категорії 5, використовує старий тип контакту - технологію руйнування ізоляції. Метод створення контакту шляхом зсуву ізоляції (IDC), в загальному випадку, визнається як більш швидкий і більш надійний спосіб завершення провідників порівняно з методом намотування провідника на штирковий контакт. При методі IDC ізоляція не видаляється з провідника, а сам провідник проштовхується в двосторонній обтискующий ніж з гострими внутрішніми краями, який прорізає ізоляцію і створює міцне електричне і механічне з'єднання. Провідник щільно сидить між двома металевими контактами і, таким чином, формується вакуумно-щільна ізоляція місця з'єднання. Більшість систем IDC вимагає застосування спеціальних інструментів. Вакуумно-щільне IDC-обтискування виключає ймовірність біметалевої корозії, яка виникає при використанні різьбових контактів, коли оголений мідний провідник і контактний гвинт, що виготовляється з іншого матеріалу (зазвичай оцинкованого), з'єднуються у присутності атмосферного кисню.

Всі IDC-типи розроблені для застосування щодо постійних з'єднань. Якщо вимагається внесення змін до системи, провідник повинен бути спочатку видалений, коннектор очищений від усіх залишків металу і пластика, а потім провідник підрізається і переобтискується.

Комутаційні блоки типу 66М.

Самим першим термінувальним блоком, що знайшли застосування в телекомунікаційних системах, був комутаційний блок типу 66. Цей вид конструкції використовувався протягом десятиліть і на сьогоднішній день його роль у телефонній промисловості досить значна.

Існує кілька видів блоків 66, але найбільш поширеним є 66М 1-50. Цей блок має 50 горизонтальних рядів контактів для завершення провідників. Кожен ряд складається з чотирьох вилкообразних контактних ножів. Кожен такий контакт, що носить назву "виделка", штампується з одного шматка металу. Чотири виделки в кожному ряду згруповані у дві групи 1-2 і 3-4, у якому кожна пара контактів з'єднана механічно і електрично. Деякі варіанти блоків 66М мають всі чотири контакту з'єднаними, а деякі - всі чотири незалежними один від одного. Горизонтальні або магістральні кабелі прокладаються під монтажними рамами блоків 66, а потім виходять на зовнішню сторону через спеціальні отвори в монтажних рамах. Зовнішня оболонка кабелю видаляється. Пари розлучаються згідно з колірним кодуванням і укладаються в щілини, розташовані на бічних сторонах блоку і відповідні певному контакту. Як правило, провідники пари проходять через щілину, розташовану вище контакту, а потім заходять в його ніж. Контакт обладнаний крюком для полегшення фіксації провідника під час завершення. Бічні щілини служать тільки для позиціонування провідників - вони не забезпечують ні кріплення, ні ослаблення натягу провідників. Після розкладки і фіксації провідників вони обтискуються в коннекторах за допомогою спеціального інструменту.

Блок 66 має маркування "ВЕРХ" ("ТОР") для орієнтації при монтажі. Всі провідники кабелю повинні бути терміновані незалежно від їх подальшого використання. Якщо ж з якихось причин необхідно термінувати число пар менше, ніж число пар в кабелі, зайві пари повинні бути підрізані до рівня краю зовнішньої оболонки кабелю або трохи глибше.

Блоки 66 призначені для завершення одножильних мідних провідників розміром від 20 до 26 AWG в пластиковій ізоляції. Використання багатожильних провідників не рекомендується. При обтискуванні провідник запресовується в щілину між двома лезами контакту з допомогою спеціального термінування інструменту, ізоляція розрізається (зміщується) і створюється вакуумнощільний контакт між мідним провідником і коннектором з фосфорної бронзи. Пружинне дію лудженого коннектора утримує провідник. Терминируючий інструмент також і видаляє надлишок провідника. Допускається обтиск тільки одного провідника в одному коннекторі. Після видалення провідника з контакту контакт може бути використаний повторно за умови, що знову обтискуєми провідник буде такого ж або більшого розміру. Використання провідників розміром менше допустимого, багаторазове використання коннектора і термінування двох провідників в одному коннекторі рано чи пізно призведе до деградації якості контакту.

Технологія розвитку пари при обтискуванні і довжина розвитку пари створюють проблему використання вищих категорій робочих характеристик, таких як категорія 5. Комутуючі кліпси, що представляють з себе (з точки зору технологій високочастотної передачі сигналу) досить великі металеві об'єкти, також можуть вносити значний внесок у деградацію узгодження

імпедансу і перехідного загасання на високих частотах. З цієї причини стандартні блоки 66М не придатні для роботи з категоріями вище категорії 3.

Деякі виробники пропонують блоки 66 з низькими рівнями NEXT, здатні працювати в системах категорії 5. Стандартний метод розведення провідників "один провідник на щілину" створює високі рівні перехресних перешкод навіть на спеціальних блоках категорії 5. Для забезпечення відповідності вимогам високошвидкісних технологій пари укладаються в щілини цілком без розвитку провідників і укладання їх у дві щілини. Цей метод дозволяє підтримувати пари нерозвиненими на мінімальну відстань від точок завершення. Єдиним незначним недоліком такої технології є утруднене читання кольорового кодування обтискувальних провідників.

Існує версія блоку 66, подібна блокам з telco-коннекторами, але виконана на основі 8-позиційних модульних гнізд.

Гнізда монтуються на бічних сторонах блоку групами по 4. Такий тип блоку усуває необхідність використання додаткової патч-панелі для підключення до кабельної системи активного обладнання з однопортовими модульними коннекторами. При використанні таких систем потрібно упевнитися в тому, що конкретний блок специфікований для роботи з високошвидкісними додатками. Провідники і пари, що з'єднують модульні гнізда і контакти блоку, можуть не володіти достатнім рівнем робочих характеристик. У цьому випадку блок не може бути використаний в системах категорій 4 і 5.

Для монтажу блоків 66М використовуються кілька методів. Найбільш поширеним є безпосереднє кріплення на спеціальних настінних панелях. Зазвичай такі панелі виготовляються з листа фанери або ДСП розміром 2,5 м x 1,5 м x 2 см, кріпляться до стіни і покриваються вогнетривкими фарбами світлого кольору. Блок 66, як правило, складається з двох частин - передньої, містить контакти і монтажні щілини, і монтажної рамки, що кріпиться на стіновій панелі. Після монтажу рамки на стіні блок 66 встановлюється на неї і фіксується з допомогою засувки, які є частиною рамки. У блоках з приєднаними конекторами коннектори, як правило, монтуються на рамці і блок може бути встановлений тільки як єдине ціле. Крім монтажу на стінових панелях, блоки 66 можуть встановлюватися на монтажних металевих рамах. Потім рами можуть монтуватися на настінних панелях або у стандартних апаратних стійках розміром 19". Колірне кодування блоків 66 наступне: загальна колірна схема розбита на п'ять 5-парних груп. Кожна група має власний первинний колір, однаковий для всіх пар у групі. Первинні кольори по порядку - білий, червоний, чорний, жовтий і фіолетовий (або пурпурний) мають скорочені позначення W, R, BK, Y, V (або P). Можуть зустрічатися і такі скорочення - WHT, RED, BLK, YEL і VIO або PUR. Наприклад, перша тупа провідників має провідник білого кольору в кожній парі; другий провідник пофарбований у вторинний колір. Вторинні кольори -

блакитний, помаранчевий, зелений і сріблясто-сірий мають скорочені позначення -BL, G, B і S (або VШ, ORG, CRN, BRN та SLT). Слід зазначити, що відповідно до ТІА 568-А використовуються скорочені аббревіатури (перша буква кольору або дві букви, де це необхідно).

Кожен провідник у парі має спіральну або кільцеву смужку на оболонці кольору парного йому провідника. Пари ідентифікуються з їх первинного і вторинного кольорів. Таким чином, перша пара в першій групі - W/BL ("біло-блакитна" або "white-blue") і складається з білого провідника з блакитною смугою і блакитного провідника з білою смугою. Провідник, пофарбований первинним кольором, завжди обтискається першим (у блоці 66 зверху вниз).

Комутаційні блоки типу 110.

Широко використовуваний термінальний блок типу 110 застосовується порівняно нещодавно – близько двох десятиліть. Як альтернатива старим систем, система 110 була розроблена для високих щільностей завершення провідників і кращого поділу "вхідних" і "вихідних" кабелів. Крім цього, система 110 має велике значення, тому що її 4-парні коннектори використовуються в більшості патч-панелей і розеткових модулях, що випускаються різними виробниками.

Система 110 складається з двох базових компонентів - комутаційного блоку 110 і коннектора 110С. Комутаційний блок 110 – це штампований монтажний пластиковий вузол з горизонтальними індексованими гребінками, на кожній з яких укладаються і фіксуються 25 пар провідників. Блоки виготовляються різної ємності - 50, 100, 200 і 300 пар. 100-парний блок має чотири горизонтальні гребінки, 300-парний - 12. Блок 110А має вільний простір глибиною 80 мм під монтажною рамкою для укладання кабелів і використовується в стандартних програмах. Блок 110D випускається в низькопрофільному виконанні з вільним простором глибиною 30 мм для спеціальних додатків. Блок 110Т з розмикачем лінії забезпечує можливість розривати лінію при тестуванні її в будь-якому напрямку. Між гребінками залишено простір для акуратної розкладки термінуємих провідників. Сам комутаційний блок не створює електричного контакту з провідником, а тільки надійно фіксує його. Після розподілу і фіксації пар кабелю вони термінуються з створенням електричного контакту шляхом посадки коннектора 110С в гребінку блоку.

Конектор 110С являє собою суцільнопластиковий вузол, в якому розташовані луджені металеві контакти, призначені для завершення провідників розміром 22, 24 і 26 AWG за допомогою технології IDC. Коннектори виготовляються в 3-, 4-і 5-парних конфігураціях і кріпляться на комутаційному блоці з допомогою замкового механізму. Верхній край коннектора 110С використовується для завершення кроссировочних провідників або, іноді, інших кабелів, або для підключення адаптерів. Конектор має систему кольорового кодування, що полегшує розкладку провідників і їх обтиску. Кроссировочні провідники являють собою пари в ізоляції

без зовнішньої оболонки. Система 110 призначена для роботи з ізольованими провідниками розміром від 22 до 26 AWG, Коннектори 110 призначені для завершення тільки одножильних провідників.

Система 110 використовується для завершення багатопарних станційних кабелів і створення кросс-з'єднань з іншими точками завершення. У типовій ЛВС-інсталяції може бути змонтовано кілька настінних або стоечних блоків 110, сполучених з патч-панелями кроссировочними кабелями. Існують рамні вузли 110 із заздалегідь термінованими 25-парними кабелями. На іншому кінці цих кабелів встановлено 50-контактні telco-коннектори, з допомогою яких можна здійснювати підключення до активного мережного обладнання, телефонних комутаторів та інших пристроїв з багатопортовим виходами. У загальному випадку, система 110 може працювати в мережах категорії 5. Ця властивість забезпечується за рахунок невеликих розмірів коннектора 110 і можливості підтримувати цілісність витків пари практично до самої точки завершення.

Комутаційний блок 110 є важливою складовою частиною багатьох розеткових модулів і патч-панелей. Він володіє перевагами простоти використання в додаток до здатності створювати високоякісний контакт. Головним недоліком блоку 110 є розташування контактів в одному ряду, що робить його ширше деяких інших систем IDC. Це заважає близькому розташуванню гнізд на одній платі розетки. Деякі виробники патч-панелей вирішують цю проблему розташуванням гребінок 110 в два ряди, від яких пари розходяться до гнізд,

Система кольорового кодування блоків 110 аналогічна схемі для блоків 66. До переваг блоків 110 можна віднести наявність маркерів, нанесених на верхній край гребінки коннектора 110, що значно полегшує розкладку провідників і знижує ймовірність помилок при термінованні.

Інші комутаційні системи.

Дві комутаційні системи використовуються в багатьох інсталяціях. Це - система VIX від NORDX/CDT (колишній Nortel Northern Telecom) і KRONE. Обидві забезпечують функціональність, еквівалентну системі 110, і значно кращу, ніж стара система 66.

Комутаційна система VIX є основою СКС категорії 5 виробництва компанії NORDX/CDT, і носить назву IBDN (Integrated Building Distribution Network). Незважаючи на те, що конектор був створений в 1980 році, всі сучасні коннектори VIX відповідають специфікаціям категорії 5.

Система NORDX/CDT VIX дуже подібна за своєю концепцією з системою 110. Це - двосторонній 50-контактний роз'єм, монтується горизонтально на монтажній рамі. На відміну від системи 110, магістральні або горизонтальні кабелі обтискаються безпосередньо на задній стороні коннектора. Матриця коннекторів VIX, встановлених на 50-, 250 або 300-парні рами,

формує "модуль". Модулі можуть монтуватися безпосередньо на стінах, на настінних панелях або в апаратних стійках при використанні комплекту для монтажу в стійках. Модулі також можуть бути встановлені на спеціальних рамах, формуючи таким чином готовий розподільний щит.

Конструкція коннектора V1X забезпечує відмінні характеристики перехідного загукання. Кросування здійснюється з зовнішньої сторони коннектора V1X. Коннектори маркуються з 4 - або 5-парними інтервалами, 4-парні версії, як правило, застосовуються для більшості додатків ЛВС, а 5-парні версії добре підходять для завершення кабелів з 25 і великою кількістю пар.

Всі з'єднання виконуються за допомогою спеціального інструменту, функціонально аналогічного інструментів, використовуваних для завершення блоків 66 і 110. В комплекти насадок стандартних інструментів часто включаються насадки для завершення коннекторів V1X. Кабелі при обтиску заводяться або з двох сторін монтажної рами, або зверху, або знизу коннектора. Монтажні рами обладнані маркувальними смугами, встановлюваними між парами коннекторів V1X. Для комутації двох позицій вертикально розташованої суміжної пари коннекторів передбачені спеціальні комутаційні кліпси.

Комутаційні блоки V1X використовуються також в якості коннекторів в модульних телекомунікаційних розетках і патч-панелі. Розетки і патч-панелі постачаються кількома виробниками, але самі блоки виготовляються тільки NORDX/CDT.

Комутаційні блоки KRONE.

Комутаційна система KRONE існує у 8-, 10- і 25-парному виконанні базових коннекторних модулів, що монтуються в різних поєднаннях. 8 - і 10-парні коннектори можуть встановлюватися окремі монтажні рами загальною сумарною ємністю 20 коннекторів. Такі рами в підсумку здатні до обтиску 160 або 200 пар провідників, 8-парний коннектор зазвичай використовується для завершення двох горизонтальних 4-парних кабелів. Монтажні модульні рами можуть встановлюватися окремо на стіні або трійками в апаратних стійках 19 дюймів. Для 25-парних додатків існують 25-парні коннектори і монтажна рама. 25-парний комутаційний модуль по конструкції аналогічний системі 110 - він складається з передньої і задньої частин. Як і у випадку 8 - і 10-парних конекторів, 25-парний коннектор встановлюється горизонтально на монтажній рамі. Можна використовувати спеціальний вузол з двох 25-парних модулів з монтажною рамою такого ж розміру, як у стандартного блоку 66. Такі вузли, як і блоки 66, дозволяють обтискати 50 пар і ідеально підходять для тих випадків, коли необхідно замінити старі на нові, більш продуктивні. Для багатьох компаній-контракторів технологія завершення з допомогою блоків KRONE є найбільш прийнятною при роботі з розподільними панелями. Найбільшу популярність набула система KRONE в телефонній промисловості. Унікальний срібний IDC-контакт KRONE, врізається в провідник під кутом до його осі 45°, забезпечує

надійне, вакуумно-щільне з'єднання одножильних або багатожильних провідників розміром 22-26 AWG. Затискачі фіксують ізоляцію надійно утримують провідник і ізолюють місце контакту від впливу вібрації і механічних сил. Осьові і крутні сили дозволяють підтримувати довготривале з'єднання. Втоплені контакти і провідники забезпечують захист ланцюгів від аварій і коротких замикань. Для завершення блоків KRONE потрібен спеціальний інструмент.

Патч-панелі (або панелі перемикання) призначені для забезпечення гнучких з'єднань між горизонтальними або магістральними кабелями і портами активного обладнання в телекомунікаційних шафах. Патч-панелі мають модульні гнізда, аналогічні гнізд телекомунікаційних розеток або активного обладнання. В якості портів активного обладнання ЛОМ найбільш часто використовуються 8 -позиційні модульні гнізда, тому зручно з'єднувати порт активного обладнання і порт патч-панелі з допомогою модульного апаратного шнура (або патч-корду).

Патч-панелі більш зручні для використання в порівнянні з технологією завершення, використовуваної в комутаційних блоках, особливо для кінцевих користувачів, оскільки кожне гніздо на патч-панелі однозначно відповідає розетки на робочому місці.

Коннектори на патч-панелі розташовуються у відповідності з проектом виробника, і можна зустріти як коннектори, розташовані через однакові інтервали, так і розташовані групами по 4 або 6. Як правило, нумеруються коннектори у відповідності з порядком їх слідування на патч-панелі, але майже завжди передбачається можливість альтернативної маркування портів.

Патч-панелі підтримують стандартні схеми розводки (T568A і T568B). Можна використовувати патч-панель зі схемою розводки T568A для реалізації схеми B, але в такому випадку необхідно провести реверсування пар на коннекторі і, крім того, при такому підході різко зростає ймовірність помилок в комутації внаслідок внесеної плутанини.

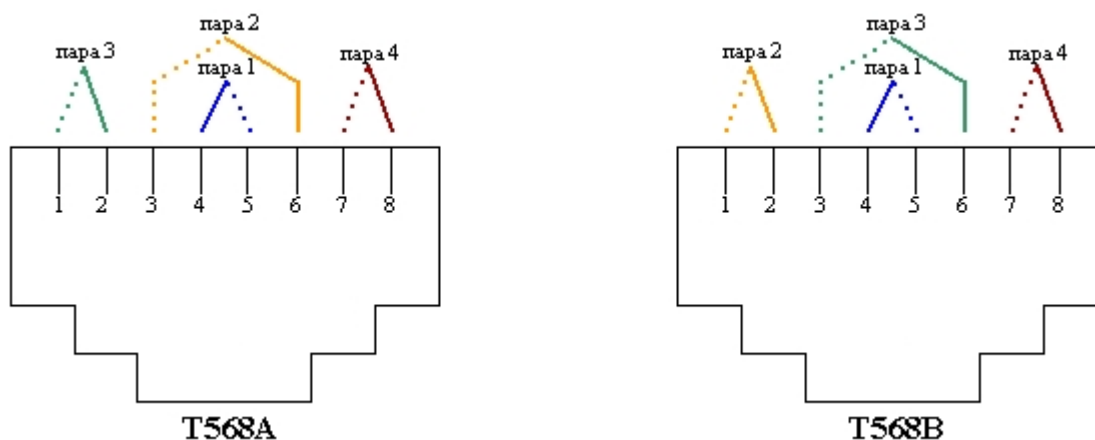


Рисунок 1.10 Схеми розводки T568A і T568B, визначені у стандарті ANSI/TIA/EIA-568-A.

Стандартні патч-панелі, в загальному випадку, використовують один з видів контакту зі зміщенням ізоляції (IDC) на задній панелі для завершення магістральних або горизонтальних кабелів. Існує дві основні конструкційні версії патч-панелей.

Перша - панелі, використовують або групи коннекторів з загальним термінаційним блоком або індивідуальні коннектори з власними точками завершення, розташованими на зворотному їхньому боці. Друга - панелі з багатопортовими коннекторами, призначені в основному для спеціальних використань.

Технологія завершення патч-панелей ідентична обтиску коннекторів телекомунікаційних розеток на робочому місці або комутаційних блоків. Існують патч-панелі, які використовують окремі контакти IDC, блоки 110, блоки 66, блоки VIX і блоки KRONE. Кожен метод має свої переваги і недоліки і, як правило, вибір залежить від особистого ставлення компанії-монтажника. Слід зазначити, що використання стандартних блоків 66, загалом, не рекомендується у високошвидкісних кабельних системах, особливо в системах з характеристиками вище категорії 3. Використання сучасних блоків категорії 5 можна рекомендувати за умов наявності сертифіката UL.



Рисунок 1.11 Патч-панелі

Патч-панелі, з точки зору стандартів, відносяться до розряду комутаційного обладнання і повинні володіти певним категорійним рейтингом робочих характеристик для забезпечення функціонування відповідних додатків. Більшість сучасних панелей специфіковані для роботи з компонентами категорії 3, 4 або 5. Стандарт TIA 568-A і інші кабельні стандарти вимагають, щоб всі комутаційне обладнання мало маркування категорії його робочих характеристик. В якості маркування визначені наступні позначення "Category n" або "Cat n", де n - номер категорії 3, 4 або 5. Допускається позначення "3" з розташованим всередині номером категорії. При

відсутності маркування можна вважати панель не категорійної і не придатною для високопродуктивних кабельних систем.

До числа найбільш ймовірних проблем, пов'язаних з використанням патч-панелей, можна віднести організацію обтискувальних кабельних потоків і підключаються патч-кордів. Для вирішення подібних проблем існує величезна розмаїтість спеціальних пристосувань для керування кабельними потоками, так званих кабельних органайзерів. Деякі патч-панелі випускаються з інтегрованими органайзерами і пристроями компенсації натягу кабелів, як із зворотного, так і з зовнішнього боку. На бічних сторонах апаратних стійок можуть монтуватися бічні вертикальні органайзери, що спрощують організацію кабелів і патч-кордів, які проходять від однієї патч-панелі до іншої. Для організації кабелів між стійками використовуються кабельні лотки і сходи (відкриті лотки з поперечними перекладинами), що з'єднують верхні частини стійок. У великих телекомунікаційних шафах і апаратних можуть бути використані телекомунікаційні траси під фальшполами.

Патч-корд являє собою короткий відрізок гнучкого кабелю, обтискувальний з обох кінців 8-позиційними модульними вилками. Патч-корд аналогічний користувальницьким шнурах на робочому місці і в телекомунікаційній шафі. Загалом, всі ці кабельні шнури згадуються під різними назвами, що відображають більшою мірою їх призначення, а не конструкцію.

Наприклад, шнур, комутуючих дві точки підключення (patch) називається патч-кордом або шнуром перемикачів, а ідентичний йому шнур, комутуючих точку підключення і хаб носить назву апаратна мотузка або шнур активного обладнання. Шнур, що з'єднує робочу станцію з коннектором телекомунікаційної розетки також називається апаратним шнуром. Апаратні шнури іноді носять назву користувальницьких шнурів, оскільки вони в основному підключаються кінцевим користувачем, а не монтажником. І, нарешті, всі ці шнури іноді називають кабелями. Єдиною умовною межею, що відрізняє патч-корд від шнура, є його менша довжина.



Рисунок 1.12 Патч-корд

Основною характеристикою патч-корду є його гнучкість. Це означає, що він повинен бути виготовлений з багатожильних провідників і мати гнучку пластикову зовнішню оболонку.

Як правило, патч-корди складаються з чотирьох мідних багатожильних пар 100 Ом з розміром провідника 24 AWG в пластиковій ізоляції і в загальній пластиковій оболонці. Дозволяється використовувати провідники розміром 22 AWG, але вони рідко застосовуються. Пластикові ізоляції - це зазвичай PVC (ПВХ) або компаунд з подібними характеристиками. Оскільки патч-корди використовуються на робочих місцях і в телекомунікаційних шафах, які не є просторами категорії *plenum*, вони не вимагають застосування спеціальних матеріалів оболонки.

Колірна кодування провідників патч-кордів може бути найрізноманітнішою, але, в основному, застосовується стандартний 4-парний код. Стандарт TIA 568-A, крім основного, пропонує альтернативний код кольору, в який входять вісім унікальних чистих кольорів.

Для патч-кордів існує окрема система вимог до робочих характеристик, які дещо відрізняються від характеристик горизонтального кабелю. Більшість вимог до передає властивостями такі ж, за винятком допущення збільшення загасання на 20% (TIA 568-A) порівняно з одножильними провідниками та деяких вимог до конструкції. Ця вимога більш жорстка порівняно з вимогою ISO 11801, в якому допустиме відхилення значень загасання визначено у 50%. Межі загасання різні для трьох категорій робочих характеристик і визначені для довжини 100 м. При придбанні готових патч-кордів необхідно упевнитися, що вони сертифіковані виробником на відповідність вимогам стандарту TIA 568-A до певної категорії робочих характеристик. Сертифікаційне тестування незалежною організацією, такий як, наприклад, UL, є показником якості та гарантій. Тестування патч-кордів являє собою досить складну задачу для кінцевого користувача і для виробника. Стандарти містять детальні специфікації вимог до робочих характеристик кабельних компонентів і комутаційного обладнання, але на даний момент не існує специфікацій для патч-кордів в зборі. Крім цього, деякі тести, такі як тест NEXT, не дають достовірні результати для ліній коротше 15 м внаслідок явища, званого резонансом. Багато тестерів не здатні вимірювати характеристики кабелю коротше 6 м. Виробники телекомунікаційних компонентів для тестування патч-кордів використовують мережеві аналізатори - лабораторні аналізатори частотних характеристик з високими рівнями точності вимірювань. Внаслідок цього, при виготовленні патч-кордів в невикробничих умовах єдиною гарантією якості робочих характеристик патч-корду є використання високоякісних компонентів, і ретельне дотримання технологічних правил. Якість роботи має першорядне значення, оскільки необхідно здійснити розвиток пари перед приєднанням модульної вилки. Якщо розвиток пари не вдалося мінімізувати, вилка обтискається подібним чином, внесе свій внесок у деградацію робочих характеристик лінії в набагато більшою мірою, ніж недоліки її конструкції. Саме з цієї причини, внаслідок неминучого розвитку пар при обтиску, конструкція модульної вилки досі не має специфікацій високочастотних робочих характеристик.

Кабельні конектори.

Існує три основних типу "мідних" кабельних конекторів-модульні конектори, коаксіальні конектори і конектори IBM Data, та волоконно-оптичні конектори. Модульний конектор є найбільш поширеним у сучасних телекомунікаційних системах внаслідок зростаючого використання кабелю вита пара. Коаксіал протягом тривалого часу використовувався в традиційних системах Ethernet і Arcnet, але поступово він виключається з більшості інсталяцій. Конектор IBM Data Connector є одним з основних компонентів у системах на основі ЕВП і специфікований для застосування стандартом TIA 568-A.

Модульні конектори.

Основою інформаційної розетки є модульний роз'єм. Провідники, вкриті плівкою золота, забезпечують стабільний, надійний електричний контакт з ламелями модульної вилки. Якість контакту також поліпшується за рахунок механізму притирання провідників роз'єму і ламелей вилки під час її вставляння в роз'єм. Корпус розетки забезпечений інтегрованим замком, який після вставляння вилки дозволяє витримувати значні зусилля розтягування на стику розетка-вилка.

Модульний роз'єм в інформаційній розетки може бути двох видів - 6 - або. 8-позиційний. Контакти у всіх роз'ємах нумеруються зліва направо по відношенню до передньої сторони роз'єму при орієнтованому вниз ключі замку.

Модульні конектори, що використовуються в телекомунікаційних системах, аналогічні конекторів, застосовуваним в кабельних системах телефонії. Конектор існує в декількох варіантах розмірів і конфігурацій контактів, починаючи з чотирьох і закінчуючи вісьмома позиціями і від двох до восьми контактів. Самим популярним типом роз'єму є так званий USOC (Universal Service Order Code), який має номенклатурні префікси "RJ", за якими слід номер серії. Часто цими назвами користуються для позначення додатків, які не мають до коду ніякого відношення. Так, наприклад, звичайну 6-контактну телефонну вилку часто називають RJ-11, а 8-контактну модульну вилку - RJ-45. 8-контактна модульна вилка використовується відповідно до TIA 568-A як для телефонії, так і для додатків передачі даних, 8-контактний модульний роз'єм також служить інтерфейсом для таких додатків як 10BaseT, 100BaseT, 100 VG-AnyLAN, Token-Ring/UTP.

8-позиційний модульний роз'єм дуже часто невірно називають ім'ям спеціалізованого конектора RJ-45.

Рисунок 1.13
RJ-45

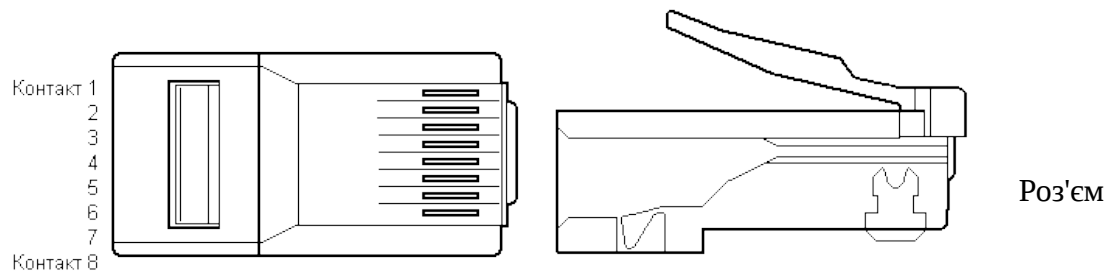


Схема розведення інтерфейсу RJ-45 (включає в себе інтерфейсний програмний резистор) настільки радикально відрізняється від схем T568A і T568B, що немає абсолютно ніяких підстав для змішування цих двох назв. Правильна назва для роз'єму - "8-позиційний модульний". Насправді всі модульні коннектори з однаковою кількістю позицій конструкційно однакові до моменту завершення. Після завершення можливо називати їх по імені схеми розводки. Наприклад, при реалізації інтерфейсу і схеми розводки 10BaseT можна підключити тільки чотири пари 8-позиційного модульного роз'єму. У цьому випадку, він не може називатися ні T568A, ні, так як обидві ці схеми вимагають підключення всіх восьми контактів. Також він не буде відповідати схемі RJ-45, так як схема розводки буде невірною, а програмний резистор відсутній.

8-позиційний модульний роз'єм, який використовується в стандартних кабельних і стемах, описаний в стандарті IEC 603-7. Цей же роз'єм визначений в стандарті TIA 568-A і супутніх документах, а також в ISO/IEC IS-11801.

Модульні коннектори, в основному, призначені для завершення кабелів з багатожильними провідниками. Спочатку коннектор був створений для завершення плоского кабелю, що складається з 2-8 багатожильних провідників. Його призначення було обмежено аудіочастотами телефонних ліній, хоча офіційно його робочі частотні характеристики визначені до 3 МГц. На жаль, промисловість не тільки змушена використовувати ці коннектори на частотах набагато перевищують специфіковані стандартом, але і використовувати їх для завершення кручених пар круглих кабелів. Для того, щоб дозволити використання модульних коннекторів на робочих частотах кабельних систем від 10 до 100 МГц, TIA просто визначає критерії робочих характеристик (в основному, загасання і NEXT), яким повинен відповідати коннектор. За умови відповідності конкретного коннектора цим специфікаціям, він може бути використаний для роботи з додатками до категорії 5.

Існують модульні коннектори, призначені для завершення одножильних провідників, незважаючи на те, що обтиск одножильних провідників навіть за допомогою спеціальних коннекторів настійно не рекомендується. Модульний контакт являє собою плоский контакт з загостреним кінцем, який при обтиску прорізає ізоляцію провідника і створює електричний

контакт з мідним багатожильним провідником. Контакт може створюватися в одній або декількох точках.

Якщо застосовувати цю технологію до одножильного провідника, при обтиску він може зрушити в бік від кінців контакту і може утворитися неповноцінний контакт або взагалі відсутність контакту. З цієї причини контакти для завершення одножильних провідників мають три загострених виступу на нижній стороні. При обтиску провідник центрується між трьома виступами і утримується ними з створенням надійного контакту.

Екрановані модульні вилки були розроблені для завершення екранованих кабелів різних типів. Як правило, вилка складається з стандартного модульного коннектора з металевим рукавом, що проходять по зовнішній поверхні коннектора і повторює його форму. При використанні таких вилок необхідно застосовувати розетки, сумісні з цими вилками для забезпечення правильного функціонування екрану. Іноді заземлюючий провідник екрану кабелю може обтискуватись на одному з контактів вилки 8-позиційного модульного роз'єму, але при цьому втрачається можливість стандартного з'єднання чотирьох збалансованих пар. Єдиним екранованим коннектором, рекомендованим стандартом TIA, є так званий IBM Data Connector (STP-A, 2 пари, 150 Ом).

Процедура завершення кабелю модульної виделкою полягає в наступному. Оболонка кабелю видаляється на відстань як мінімум 20 мм від кінця провідників. Пари розкладаються в тому ж порядку цв'ітів, який відповідає обраної схемою розводки (наприклад, 1-2, 3-6, 4-5 і 7-8).

Колір перших двох пар залежить від обраної схеми - T568A або T568B. Кінця оболонки кабелю надається плоска форма для забезпечення можливості розташування пар в один ряд. Пари розвиваються аж до краю оболонки кабелю. Провідники розкладаються таким чином, щоб формувався плоский шар з паралельно розташованих провідників. Провідник 6 повинен перетинати провідники 4 і 5 так, щоб кросовер знаходився на відстані не більше 4 мм від краю оболонки кабелю.

Провідники підрізають на відстань близько 14 мм від краю оболонки кабелю. Вилка поміщається на провідники так, що вони проходять до обтискувальних каналів в вилці, а оболонка кабелю заходить у вилку, принаймні, на відстань 6 мм. Вилка обжимається з допомогою спеціального обтискного інструменту. Після завершення обох кінців кабелю, він перевіряється на безперервність і схему розводки.

Типи пристроїв Fast Ethernet

Трансивер (Transiever) – це двухпортовий пристрій, що має з однієї сторони, МІІ інтерфейс, з іншого – один з середозалежних фізичних інтерфейсів (100Base-FX, 100Base-TX або 100Base-T4). Трансивери використовуються порівняно рідко, як і рідко використовуються мережеві карти, повторювачі і комутатори з інтерфейсом МІІ.

Мережева карта (Netcard). Найбільш широке поширення одержали мережеві карти з інтерфейсом 100Base-TX на шину PCI. Необов'язковими, але вкрай бажаними, функціями порту RJ-45 є автоконфігурування 100/10 Мбіт/с і підтримка дуплексного режиму. Більшість сучасних карт, що випускаються підтримують ці функції. В даний час набирає обертів випуск мережевих карт з підтримкою 1000 Мбіт/сек. Випускаються також мережеві карти з оптичним інтерфейсом 100Base-FX – з основним оптичним роз'ємом SC на багатомодове волокно.

Конвертер (Converter) – це двухпортовий пристрій, обидва порти якого представляють середозалежні інтерфейси. Конвертери, на відміну від повторювачів, можуть працювати в дуплексному режимі. Поширені конвертери 100Base-TX/100Base-FX.

Повторювач (Repeater) – многопортовий пристрій, який дозволяє об'єднати декілька сегментів. Беручи кадр або сигнал колізії з одного з своїх портів, повторювач перенаправляє його на всі інші порти. Поширені пристрої з декількома портами на виту пару (12, 16 або 24 порти RJ-45), одним портом BNC і одним портом AUI. Повторювачі працюють на фізичному рівні моделі OSI. По параметру максимальних тимчасових затримок при ретрансляції кадрів, повторювачі Fast Ethernet поділяються на два класи:

Клас I. Затримка на подвійному пробігу RTD не повинна перевищувати 130 нс. В силу менш жорстких вимог, повторювачі цього класу можуть мати порти T4 і TX/FX, а також об'єднуватися в стек.

Клас II. До повторювачам цього класу пред'являються більш жорсткі вимоги по затримці на подвійному пробіг: $RTD < 92$ нс, якщо порти типу TX/FX, і $RTD < 67$ нс, якщо всі порти типу T4. (В силу значних відмінностей в організації фізичних рівнів виникає велика затримка кадру при ретрансляції між портами інтерфейсів T4 і TX/FX. Тому повторювачі, що поєднують в межах одного пристрою порти T4 з TX/FX віднесені до класу I.).

Комутатор (Switch) – одне з найбільш важливих пристроїв при побудові корпоративних мереж. Комутатор працює на другому каналному рівні моделі OSI. Головне призначення комутатора – розвантаження мережі за допомогою локалізації трафіку в межах окремих сегментів.

Ключовою ланкою комутатора є архітектура без блокування (non-blocking), яка дозволяє встановити множинні зв'язки Ethernet між різними парами портів одночасно, причому кадри не втрачаються в процесі комутації. Сам трафік між взаємодіючими мережевими пристроями залишається локалізованими. Локалізація здійснюється з допомогою адресних таблиць, що встановлюють зв'язок кожного порту з адресами мережевих пристроїв, що відносяться до сегменту цього порту. Таблиця заповнюється в процесі аналізу комутатором адрес станцій відправників до переданих ними кадрах. Кадр передається через комутатор локально у відповідний порт тільки тоді, коли адреса станції призначення, зазначений в полі кадру, вже

міститься в адресній таблиці цього порту. У разі відсутності в таблиці адреси станції призначення, кадр розсилається в усі інші сегменти. Якщо комутатор виявляє, що MAC-адресу станції призначення приходить кадру знаходиться в таблиці MAC-адрес, приписаної за портом, то цей кадр скидається – його безпосередньо отримає станція призначення, що знаходиться в даному сегменті. І, нарешті, якщо приходить кадр є ширококомовним (broadcast), тобто якщо всі біти поля MAC-адреси одержувача в кадрі задаються рівними 1, то такий кадр буде розмножений комутатором (подібно концентратора), тобто спрямовуються на всі інші порти.

Концентратор (Hub) - це багатопортовий повторювач мережі з автосегментацією. Усі порти концентратора рівноправні. Одержавши сигнал від однієї з підключених до нього станцій, концентратор транслює його на усі свої активні порти. При цьому, якщо на якому-небудь з портів виявлена несправність, те цей порт автоматично відключається (сегментується), а після її усунення знову робиться активним. Автосегментація необхідна для підвищення надійності мережі. Обробка колізій і поточний контроль за станом каналів зв'язку звичайно здійснюється самим концентратором. Концентратори можна використовувати як автономні пристрої або з'єднувати один з одним, збільшуючи тим самим розмір мережі і створюючи більш складні топології.

Маршрутизатор (Router). Основною функцією маршрутизаторів є забезпечення з'єднань, маршрутів передачі даних між вузлами різних мереж, які можуть бути розділені значною географічною відстанню і кількома проміжними мережами. Маршрутизатор створює канал передачі даних, знаходячи відповідний маршрут та ініціюючи початкове з'єднання по цьому маршруту.

На практиці маршрутизація реалізується апаратно-програмним забезпеченням, що працює на мережному рівні еталонної моделі OSI. Апаратні засоби маршрутизації можуть бути як внутрішніми, так і зовнішніми. Внутрішні маршрутизатори являють собою спеціальні плати, що встановлюються в роз'єм розширеного комп'ютера і харчуються від загального блоку живлення. Зовнішні маршрутизатори – це окремі пристрої зі своїм власним блоком живлення.

Завдання маршрутизатора полягає в пошуку маршруту для передачі пакетів даних від вузлів однієї мережі до іншої і пересилання пакетів по цьому маршруту. Маршрутизатори працюють на мережному рівні і тому є протоколо-незалежними. Це пов'язано з тим, що в пакетах різних протоколів використовуються різні формати адресних полів. Наприклад, маршрутизатор, призначений для використання з протоколом IP (Internet Protocol), не зможе коректно обробляти пакети з адресами у форматі ISO і навпаки. Більшість маршрутизаторів підтримують кілька протоколів канального рівня. Ранні моделі маршрутизаторів працювали лише з одним мережевим протоколом, а сучасні підтримують одночасно кілька протоколів.

Особливості роботи маршрутизатора дозволяють використовувати його в якості пакетного фільтра. Незалежність від протоколів канального рівня дозволяє використовувати маршрутизатори для об'єднання мереж з різними архітектурами — наприклад, з'єднання мереж Ethernet і Token Ring або Ethernet і FDDI.

Міст (bridge) - пристрій, призначений для передачі пакетів даних з однієї мережі в іншу. З функціональної точки зору, мости відносяться до канального рівня еталонної моделі OSI. Мости дозволяють програм і протоколів, що працюють на більш високих рівнях, розглядати об'єднання декількох мереж, як одне ціле. Поряд з передачею даних, мости можуть також виконувати їх фільтрацію. Це означає, що в мережу N2 будуть потрапляти тільки ті пакети, які призначені для вузлів цієї мережі. А пакети, призначені для вузлів мережі N1, з якої вони надходять, будуть повертатися назад.

Значення термінів «міст» і «маршрутизатор» багато в чому схоже. Основна відмінність від мостів полягає в тому, що маршрутизатори працюють на мережному рівні еталонної моделі OSI.

Канал (Channel) каналом називається фізичний або логічний шлях для передачі сигналів. у контексті комп'ютерних мереж найчастіше зустрічаються згадки каналів двох типів: комунікаційних і дискових. Комунікаційним каналом називається маршрут, за яким відбувається передача даних, мови або відеозображення. Сучасні технології передачі даних дозволяють організувати кілька комунікаційних каналів всередині одного фізичного кабелю.

Дисковим каналом, в конфігурації з жорстким диском, називаються компоненти, за допомогою яких здійснюється взаємодія операційної системи з накопичувачем на жорсткому диску.

1.5 Функціональна відповідність видів комунікаційного обладнання рівнів моделі OSI

Кращим способом для розуміння відмінностей між мережевими адаптерами, повторювачами, мостами/комутаторами і маршрутизаторами є розгляд їх роботи в термінах моделі OSI. Відповідність між функціями цих пристроїв і рівнями моделі OSI показано на рисунку 1.14.

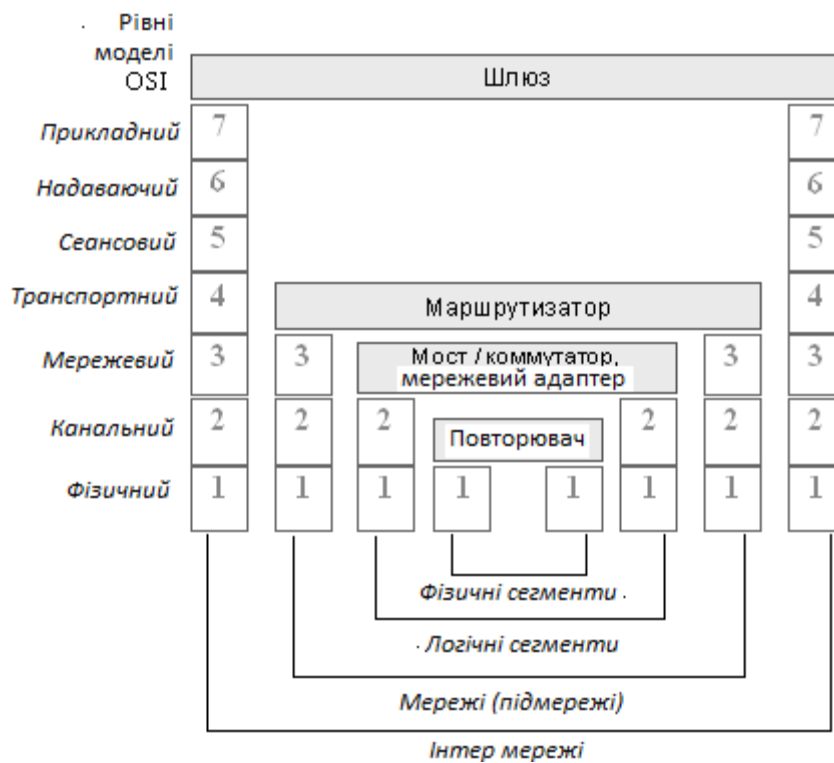


Рисунок 1.14 Відповідність функцій комунікаційного обладнання моделі OSI

Повторювач, який регенерує сигнали, за рахунок чого дозволяє збільшувати довжину мережі, працює на фізичному рівні.

Мережевий адаптер працює на фізичному і канальному рівнях. До фізичного рівня відноситься та частина функцій мережевого адаптера, яка пов'язана з прийомом і передачею сигналів по лінії зв'язку, а отримання доступу до поділюваної середовищі передачі, розпізнавання MAC-адреси комп'ютера - це вже функція канального рівня.

Мости виконують велику частину своєї роботи на канальному рівні. Для них мережа представляється набором MAC-адрес пристроїв. Вони отримують ці адреси з заголовків, доданих до пакетів на канальному рівні, і їх використовують під час обробки пакетів для прийняття рішення про те, на який порт відправити той чи інший пакет. Мости не мають доступу до інформації про адреси мереж, що відноситься до більш високого рівня. Тому вони обмежені в прийнятті рішень щодо можливих шляхів або маршрути переміщення пакетів по мережі.

Маршрутизатори працюють на мережному рівні моделі OSI. Для маршрутизаторів мережа - це набір мережевих адрес пристроїв і безліч мережевих шляхів. Маршрутизатори аналізують всі можливі шляхи між будь-якими двома вузлами мережі і вибирають найкоротший з них. При виборі можуть братися до уваги і інші фактори, наприклад, стан проміжних вузлів і ліній зв'язку, пропускну здатність ліній або вартість передачі даних.

Для того, щоб маршрутизатор міг виконувати покладені на нього функції йому повинна бути доступна більш розгорнута інформація про мережі, ніж та, яка доступна мосту. У заголовку пакету мережевого рівня крім мережевої адреси є дані, наприклад, про критерій, який повинен бути використаний при виборі маршруту, про час життя пакету в мережі, про те, до протоколу верхнього рівня належить пакет.

Завдяки використанню додаткової інформації, маршрутизатор може здійснювати більше операцій з пакетами, ніж міст/комутатор. Тому програмне забезпечення, необхідне для роботи маршрутизатора, є більш складним.

Ще один тип комунікаційних пристроїв - шлюз, який може працювати на будь-якому рівні моделі OSI. Шлюз (gateway) - це пристрій, що виконує трансляцію протоколів. Шлюз розміщується між взаємодіючими мережами і служить посередником, перекладаючим повідомлення, що надходять з однієї мережі, у формат іншої мережі. Шлюз може бути реалізований як чисто програмними засобами, встановленими на звичайному комп'ютері, так і на базі спеціалізованого комп'ютера. Трансляція одного стека протоколів в іншій являє собою складну інтелектуальну задачу, що вимагає максимально повної інформації про мережі, тому шлюз використовує заголовки всіх трансльованих протоколів.

1.6 Висновки до розділу 1

В даному розділі було розглянуто поняття локальної обчислювальної мережі, як класифікують локальну мережу, які існують топології локальних мереж, структуровані кабельні системи, за допомогою яких кабелів відбувається з'єднання між вузлами, також було розглянуте комутаційне обладнання. Розглянуто існуючі принципи побудови локальної мережі.

РОЗДІЛ 2

ДОСЛІДЖЕННЯ ТА ПРОЕКТУВАННЯ ПРОГРАМНО-ТЕХНІЧНОГО КОМПЛЕКСУ

2.1 Постановка завдання

Дослідити та спроектувати локальну комп'ютерну мережу Головного управління Держгеокадастру у Луганській області.

При обстеженні локальної мережі організації було виявлено схему підключення комп'ютерів, яка представлена у додатку Б. Доступ до мережі Інтернет здійснювався за допомогою маршрутизатору TP-LINK TL-WR741ND.

У нашому випадку Головне управління буде мати 70 робочих станцій, які і потрібно об'єднати в корпоративну мережу.

В таблиці 2.1 наведено перелік структурних підрозділів, в яких будуть розміщуватись робочі станції працівників.

Таблиця 2.1 перелік структурних підрозділів.

№	Назва структурного підрозділу	Кількість робочих місць
1	Керівництво	3
2	Управління землеустрою та охорони земель	6
3	Відділ ринку та оцінки земель	7
4	Відділ державної земельпорядної експертизи	5
5	Управління адміністративно-організаційного забезпечення	10
6	Юридичне управління	12
7	Фінансове управління	9
8	Сектор інформаційних технологій та захисту інформації	3
9	Відділ державного геодезичного нагляду	5
10	Управління персоналом	7
11	Управління державного земельного кадастру	3

Мережа, що розробляється, повинна об'єднати між собою всі робочі станції, забезпечити доступ до мережевих ресурсів, як локальних так і глобальних.

Основні вимоги до локальної мережі:

- об'єднання парку робочих станцій;
- маршрутизація трафіку локальної мережі;
- надійність. Забезпечити надійну роботу локальної мережі;
- закласти при проектуванні певний запас пропускної здатності, який буде використаний в майбутньому при збільшенні потоків трафіку;

- передбачити можливість фільтрування трафіку, що передається між локальною мережею та мережею Інтернет;
- підтримка можливості розширення та масштабування;
- керованість. Забезпечити розширені засоби моніторингу та адміністрування локальної мережі, сервера.
- якість обслуговування (QoS).

Дана розробка знайде своє практичне застосування для локальних мереж фірм, підприємств, установ враховуючи ряд переваг перед аналогічними рішеннями.

До особливостей локальної мережі можна віднести:

- порівняно невеликі затрати на її реалізацію.
- можливість спільного використання локальних мережевих ресурсів.
- сегментованість з можливістю передачі трафіку між підмережами та налаштування правил фільтрації останнього.
- спільне використання мережі Інтернет та централізований захист.
- можливість збереження вкладених інвестицій при розширенні або модернізації мережі.

2.2 Стадії та етапи розробки

Проектування локальної мережі поділяється на наступні етапи:

- Планування етапів розробки локальної мережі, та вибір для цього необхідного активного та пасивного обладнання;
- Розробка СКС локальної мережі;
- Розробка логічної топології;
- Встановлення комутаційних шаф та підключення комунікаційного обладнання.
- Налаштування сервера.
- Конфігурування стеку протоколів TCP/IP робочих станцій.
- Тестування мережі.

2.2.1 Характеристика активного та пасивного комунікаційного обладнання локальної комп'ютерної мережі

Для локальної мережі буде використано таке пасивне та активне мережеве обладнання:

- Мережений кабель. Неекранована вита пара;

- Мережеві розетки. Будуть монтуватися на стіні біля коробу, по якому проходитимуть мережеві кабелі горизонтальної підсистеми;
- Комутаційні шафи;
- Патч-панелі;
- Сервер доступу до мережі Інтернет.

2.3 Розрахунок пропускної спроможності

Розробляючи локально-обчислювальну мережу Головного управління з сімдесятьма комп'ютерами. Основними завданнями якої є робота в інтернеті, пошта, обмін даними всередині мережі, робота в базах даних.

Збір статистичної інформації доцільно збирати в пік робочої діяльності для отримання найбільш наближених результатів до істини. Найбільша активність в мережі спостерігається на початку та наприкінці місяця так як необхідно надавати звітність і здавати плани.

Найпростіший приклад розрахунку можна зробити на прикладі поштового клієнта. Припустимо, що в певний момент часу всім працівникам підприємства необхідно передати документ обсягом не менше 1 мб по електронній пошті. Варто розуміти, що тимчасові витрати на передачу повідомлення повинні бути комфортними для кінцевих користувачів.

Виходячи з отриманої інформації раніше можна розрахувати навантаження, створювану поштовим клієнтом на пропускну здатність мережі. Таке навантаження трафіку складе:

$\text{кілобайти} * 70 \text{ робочих станцій} / 1 \text{ секунду} = 70 \text{ мегабайт в секунду}$. Поглянувши на розрахунок можна зробити висновок що поштовий сервер повинен бути з'єднаний з комутатором на швидкостях не менше 0,54 гігабіт на секунду. Сам відправник може бути з'єднаний звичайною витю парою швидкість 100 мегабіт. Цього цілком вистачить для передачі файлів обсягами і більш одного мегабайта. Особливу увагу потрібно приділити комутації серверів з мережевими вузлами.

2.4 Побудова локальної мережі

Для організації локальної мережі потрібна додаткова відносно базової апаратура і програмні засоби.

Мережна плата (Network Interface Card – NIC), або інакше мережний адаптер – це плата розширення, яка встановлюється у вільний слот системної плати та виконує функції сполучення комп'ютера з каналами зв'язку. Існують мережні карти, які виконані на системній платі, тому для таких системних плат немає необхідності застосовувати додаткову плату розширення.

Фізичне з'єднання комп'ютерів у локальній мережі виконується кабелем. За стандартом 10Base-T з'єднання виконується кабелем звита пара п'ятої категорії, яка забезпечує швидкість передачі інформації 100 Мбіт/с. Кабель являє собою декілька (2 або 4 або 8) пар провідників, які закручені один відносно другого і з більшим кроком – одна пара відносно другої. Відстань між з'єднаними абонентами може бути до 100 метрів.

За стандартом 10Base-2 з'єднання виконується тонким коаксіальним кабелем. Швидкість передачі даних може досягати 10 Мбіт/с. Відстань між абонентами може складати до 185 метрів.

Стандарт 10Base-F – з'єднання виконує волоконно-оптичний кабель. Швидкість передачі даних до 10 Гбіт/с. Відстань між абонентами може складати до 2000 метрів (але з підвищенням швидкості передачі даних максимальна відстань буде скороченою).

Для з'єднання комп'ютерів кабелем звита пара потрібно застосувати 8-контактний роз'єм RJ-45. За його допомогою, в залежності від топології мережі, з'єднуються або комп'ютер з комп'ютером, або комп'ютер з комутатором чи іншим пристроєм у мережі. Для використання коаксіального кабелю треба застосувати T-коннектори, роз'єми CP-50 та термінатори.

З'єднати комп'ютери у мережі можна різними способами. Схема з'єднань комп'ютерів та інших пристроїв у мережі називається топологією мережі. У комп'ютерній техніці існує декілька схем мереж, які виправдані практикою їх застосування.

Логічна топологія локальної мережі – деревоподібна, відображена у додатку В.

2.5 Комплектуючи для сервера та робочих станцій

В таблиці 2.2 наведено апаратну конфігурацію, яка буде використана для сервера доступу до мережі Інтернет.

Таблиця 2.2 Апаратна конфігурація серверу.

№	комплектуючі	кількість штук
1	Серверна Платформа : Supermicro SYS-5029S-C 19" 2U, 1xPSU, Intel C232, 1xLGA1151, up to 64GB (4 slots) DDR4 2133MHz ECC Unbuffered, 8x3.5" SAS/SATA hot-swap drive bay, 8 ports SAS 12Gb/s LSI 3008 (RAID levels: 0,1,10), 2 ports SuperDOM, 2x1GbE (Intel i210AT, RJ45), IP-KVM, Video, 1xPCI-E (x8 in x16), 1xPCI-E (x4 in x8), 1xPCI-E (x1), Black	1
2	Процесор: Intel Xeon E3-1230 v5 4x3.4GHz, DMI 8.0GT/sec, 2xDDR4-2133MHz, 8MB Cache, HT, Turbo Boost ^A 3.8GHz, Skylake, 14nm, 80W, LGA1151	1
3	Пам'ять: 16GB DDR4-2133 ECC Unbuffered Supermicro certified for Intel C232, C236 chipsets	2
4	HDD: 200GB SSD Intel DC S3700 SATA 6Gb/s , Full Disk Writes Per Day: 10	2
5	HDD: 1000GB 3.5" SATA 7200rpm Enterprise, MTBF 1,200,000 hours, half duplex, single port, no T10 PI (Protection Information)	2
6	Мережевий адаптер : Dual Port Gigabit Ethernet Server Adapter 2 ports 10/100/1000 Base-T , Intel i350	1

В таблиці 2.3 наведено апаратну конфігурацію робочих станцій.

Таблиця 2.3 Апаратна конфігурація робочих станцій

№	комплектуючі	кількість штук
1	Процесор AMD Athlon 200GE 3.2GHz AM4	70
2	Материнська плата BIOSTAR A320MH	70
3	Модуль пам'яті PATRIOT Signature Line DDR4 2666MHz 4GB (PSD44G266641)	70
4	Корпус FRONTIER Yoda FC-F56A (400W)	70
5	SSD GOODRAM CL100 240GB 2.5" SATA (SSDPR-CL100-240)	70
6	Монітор 21.5" Philips 223V5LSB2/10/62	70
7	Миша Logitech M90 USB Grey	70
8	Клавіатура дротова A4Tech KL-7MU-R PS/2 UKR Silver/Black	70

2.6 Програмне забезпечення для сервера та робочих станцій

В даний час присутній величезний вибір програмного забезпечення від різних виробників.

Розглянемо основні відмінності між двома операційними системами: Windows та Linux.

Перше з безлічі відмінностей між цими операційними системами в тому, що Windows підтримується і розробляється однією єдиною корпорацією Microsoft. Цій компанії належать всі права на програмне забезпечення, і вона ж займається поширенням своєї операційної системи на платній основі. Отже, за використання програмного забезпечення компанії Microsoft необхідно платити.

Операційні системи сімейства Linux розробляються і допрацьовуються безліччю програмістів і навіть компаній у всьому світі. Поширюється ця операційна система вільно. Компанії здійснюють платну підтримку цієї операційної системи, однак саме використання Linux в якості операційної системи безкоштовно. Тобто для установки в якості операційної системи немає необхідності будь-коли за неї платити.

Другою відмінністю є те що, якщо порівнювати Windows з чистою операційною системою Linux, то остання не має ніякої графічної оболонки. Тобто для роботи з операційною системою Linux необхідно знати консоль.

Варто розуміти, що графічна оболонка операційних систем - це одна з найважливіших функцій для рядового користувача, яка значно спрощує і навіть прискорює роботу з такими операційними системами. Порівнюючи графічну частину цих двох систем варто розуміти, що ми порівнюємо Windows не з Linux, а з однією з безлічі оболонок.

Третя відмінність полягає в тому, що операційна система Windows укомплектована невеликою кількістю стандартних програм, функціонал яких недостатній. Для розширення цього функціоналу ми встановлюємо стороннє програмне забезпечення, за яке також потрібно платити. Варто розуміти, що з коробки більш функціональною може бути операційна система Linux.

Плюси операційної системи від Microsoft:

- великий асортимент обладнання, що підтримується. В даний час все, що випускається виробниками комп'ютерного обладнання оптимізоване і працює під операційною системою Windows;

- величезний асортимент прикладного програмного забезпечення. Для кожної окремої задачі в операційній системі Windows знайдеться безліч рішень у вигляді прикладних програм;

- величезне число фахівців в операційних системах сімейства Windows. На сьогоднішній день навіть пересічний користувач персонального комп'ютера може здійснювати мінімальну підтримку.

Мінуси операційної системи від Microsoft:

- платне поширення всього сімейства Windows. Якщо необхідно укомплектувати персональний комп'ютер цією операційною системою, то необхідно заплатити;
- величезне число шкідливих програм або програм для отримання конфіденційної інформації. Варто розуміти, що грамотне використання цієї операційної системи і її професійне налаштування, а також всього супутнього обладнання зводить ці загрози до мінімуму.

Плюси операційної системи сімейства Linux:

- відсутність будь-якої плати за використання. Абсолютно безкоштовна операційна система;
- майже повна відсутність шкідливих програм. Спіймати вірус з глобальної мережі, користуючись цією операційною системою, вкрай мала.

Мінуси операційної системи сімейства Linux:

- погана підтримка стороннього обладнання. Досить часта проблема подібних систем - у відсутності драйверів для пристроїв. Варто розуміти, що багато виробників не вважають за потрібне випускати периферію з підтримкою Linux-систем;
- невелика кількість стороннього програмного забезпечення. Тут Linux-системи сильно програють. Особливо це сильно стосується потужних програмних пакетів від таких виробників, як Adobe.

Оптимальний варіант для організації - це поєднання обох операційних систем.

Таким чином, для сервера та робочих станцій буде використано таке програмне забезпечення:

- Стек протоколів TCP/IP, який реалізовано на базі ОС Windows та ОС Linux.
- Операційні системи робочих станцій: ОС Windows 10 pro x64.
- Операційна система сервера: CentOS 6.7 x64.
- Операційна система сервера: Windows Server 2008 R2 Standard.

2.7 Висновки до розділу 2

В даному розділі визначено стадії та етапи розробки програмно-технічного комплексу, розрахована пропускна спроможність локальної мережі, визначені комплектуючі та програмне забезпечення для серверу та робочих станцій. Розроблена логічна топологія локальної мережі.

РОЗДІЛ 3

НАЛАШТУВАННЯ ПРОГРАМНОГО ТА АППАРАТНОГО ЗАБЕЗПЕЧЕННЯ ВУЗЛІВ
ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Розробка логічної адресації вузлів локальної мережі

Для мережі використано діапазони приватних (білих) IP-адрес. Згідно документу, опублікованого IANA RFC2544, для приватних мереж виділяється 3 блоки IP-адрес (10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12). В 2002 році вийшов документ RFC3330, згідно якого зарезервовані блоки IP-адрес стають доступні широкому загалу користувачів. В нашому випадку буде використано локальну мережу з пулом IP-адрес 192.168.0.0/24. В таблиці 3.1 наведено розподіл IP-адрес локальної мережі.

Таблиця 3.1 Розподіл IP-адрес локальної мережі

№	№ каб	Структурний підрозділ	ір-адреси	Шлюз	DNS
1	2	3	4	5	6
1	101 - 103	Керівництво	192.168.0.11/32 -192.168.0.13/32	192.168.0.5	192.168.0.6
2	104	Управління землеустрою та охорони земель	192.168.0.14/32 - 192.168.0.19/32	192.168.0.5	192.168.0.6
3	105 - 106	Відділ ринку та оцінки земель	192.168.0.20/32 - 192.168.0.26/32	192.168.0.5	192.168.0.6
4	107	Сектор державної землевпорядної експертизи	192.168.0.27/32 - 192.168.0.31/32	192.168.0.5	192.168.0.6
5	108 - 109	Управління адміністративно-організаційного забезпечення	192.168.0.32/32 - 192.168.0.41/32	192.168.0.5	192.168.0.6
6	110	Юридичне управ-	192.168.0.42/32 –	192.168.0.5	192.168.0.6
1	2 - ління	3	4 192.168.0.53/32	5	6

	111				
7	112 - 113	Фінансове управління	192.168.0.54/32 - 192.168.0.62/32	192.168.0.5	192.168.0.6
8	114	Сектор інформаційних технологій та захисту інформації	192.168.0.63/32 - 192.168.0.65/32	192.168.0.5	192.168.0.6
9	115	Відділ державного геодезичного нагляду	192.168.0.66/32 - 192.168.0.70/32	192.168.0.5	192.168.0.6
10	116 - 117	Управління персоналом	192.168.0.71/32 - 192.168.0.77/32	192.168.0.5	192.168.0.6
11	118	Управління державного земельного кадастру	192.168.0.78/32 - 192.168.0.80/32	192.168.0.5	192.168.0.6

3.2 Налаштування мережевих інтерфейсів

Після встановлення операційної системи CentOS 6.7 x64 переходимо до налаштування. Насамперед нам потрібно перейти в так званий "привілейований режим" (root), в якому можна конфігурувати сервер, на відміну від того, в якому ми знаходимося за замовчуванням (режим користувача) і маємо обмежені можливості з управління сервером. "Привілейований режим" - це щось подібне до входу на Windows під профілем administrator.

Перехід в цей привілейований режим здійснюється просто – відкриваємо термінал і пишемо su - та вводимо пароль:

```
login as: test
dank@192.168.0.5's password:
Last login: Thu Dec 27 12:58:27 2018 from 192.168.0.5
[test@severlg ~]$ su -
Password:
[root@severlg ~]#
```

Налаштовуємо мережеві інтерфейси, що виконується командою `nano /etc/sysconfig/network-scripts/ifcfg-eth0`. Цей мережевий інтерфейс буде використовуватися для глобальної мережі:

```

DEVICE=eth0
HWADDR=00:E0:4C:74:80:39
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=static
IPADDR=94.93.52.47
NETMASK=255.255.255.192
USERCTL=no
NETWORKING_IPV6=no
IPV6INIT=no
NOZEROCONF=yes

```

Командою `nano /etc/sysconfig/network-scripts/ifcfg-eth1` налаштуємо мережевий інтерфейс для локальної мережі:

```

DEVICE=eth1
HWADDR=03:37:11:A0:DA:85
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=static
IPADDR=192.168.0.5
NETMASK=255.255.255.0
NETWORK=192.168.0.0
USERCTL=no
NETWORKING_IPV6=no
IPV6INIT=no
NOZEROCONF=yes

```

Властивості:

`DEVICE` – назва пристрою (може надалі використовуватися скриптами);

`HWADDR` - MAC-адреса можлива зміна на котрий нам потрібен;

`BOOTPROTO` - приймає наступні параметри - none, dhcp, bootp. None – використовується для заборони автоматичного налаштування (в нашому випадку ми встановлюємо параметри в CentOS 6 вручну), DHCP – для автоматичного отримання адреса від DHCP-сервера, BOOTP – застаріла версія котра була замінена DHCP, використовується рідко;

`IPADDR` – адреса мережевого інтерфейсу у CentOS;

`NETMASK` - маска підмережі;

`NETWORK` - мережа;

`BROADCAST` - Broadcast;

`ONBOOT` - приймає yes или no в залежності від того, завантажувать мережевий інтерфейс під час загрузки системи;

`USERCTL` - приймає true или false в залежності від того, можливо користувачу, а не root змінювати параметри інтерфейсу.

Після того, як мережеві параметри будуть збережені, необхідно виконати команду:

```
[root@sever1g ~]# service network restart
```

Після чого всі параметри вступають в дію.

3.3 Налаштування проксі-сервера

Squid найпоширеніший проксі-сервер для Linux. Проксі-сервер дозволяє організувати контрольований доступ до мережі інтернет, а також здійснювати моніторинг ресурсів, на які заходив користувач. Може бути прозорим (непомітним) для користувача або ні, проксіровать (пропускати через себе) різні протоколи, авторизувати користувачів через домен або по паролю, використовувати списки доступу (ACL).

Squid - програмний пакет, який реалізує функцію кешуючого проксі-сервера для протоколів HTTP, FTP, Gopher і (в разі відповідних налаштувань) HTTPS. Розроблено співтовариством як програма з відкритим вихідним кодом (поширюється відповідно з GNU GPL). Всі запити виконує як один неблокований процес введення-виведення.

Програмний пакет Squid використовується в UNIX-подібних системах і в ОС сімейства Windows NT. Має можливість взаємодії з Active Directory Windows Server шляхом аутентифікації через LDAP, що дозволяє використовувати розмежування доступу до інтернет ресурсів користувачів, які мають облікові записи на Windows Server, також дозволяє організувати «нарізку» інтернет трафіку для різних користувачів.

3.3.1 Списки контролю доступу

Для контролю доступу до ресурсів і визначення ряду дій використовуються списки контролю доступу (access control list, acl). Кожен ACL може складатися з декількох критеріїв (але тільки одного типу):

- адреса (мережа) джерела запиту, цілі запиту;
- ім'я (доменне ім'я) джерела запиту, ім'я мети запиту;
- частини URL запиту;
- протокол;
- порт (одержувача, відправника, самого squid'a);
- метод (POST або GET) при передачі даних по HTTP;
- браузер (User-agent);
- ident (запит до робочої станції).

Номер з'єднання (найчастіше використовується для обмеження кількості з'єднань):

- SNMP.

Ідентифікація - Squid підтримує кілька видів ідентифікації користувачів:

- за IP-адресою (або доменному імені вузла);
- за переданим реквізитами (логін / пароль);
- за ідентифікатором користувача агента (браузера).

Для ідентифікації за логіном / паролем можливо використовувати:

- звичайні логін / пароль;
- NTLM-авторизацію;
- зовнішні програми авторизації (що визначають формат авторизації).

Встановлюємо проксі-сервер командою:

```
[root@sever1g ~]# yum install squid
```

Після завершення установки необхідно виконати налаштування Squid. Основним файлом налаштування є файл `/etc/squid/squid.conf`. Його можна редагувати звичайним текстовим редактором, наприклад Vi, Nano і т.п. Squid має досить велику кількість налаштувань. Файл конфігурації працює зверху вниз - тобто те, що описано вище в файлі спрацює першим. Розглянемо мінімально необхідні з них.

- `acl localnet src ...` і `acl localnet src 10.0.0.0/8` - визначають які мережі для Squid будуть локальними. Необхідно залишити одну, інші потрібно закоментувати;
- `acl ... ports` і `acl Safe_ports 21` - визначають які порти контролюватиме Squid;
- `http_access`;
- `http_access deny! Safe_ports`;
- `http_access deny all`;
- правила доступу: `deny` - заборона, `allow` дозвіл;
- забороняє з'єднання по всіх портах, крім групи! `Safe_ports`;
- забороняє всі з'єднання, крім тим що були описані вище. після цих слів не повинно бути інших описів правил доступу інакше вони не спрацюють;
- `http_port` вказує на якому порту працює проксі-сервер;
- `transparent` вказує що проксі буде прозорим;
- `cache_dir ufs / var / spool / squid 4096 32 256` - вказує де будуть створені каталоги під кеш, сумарний розмір, і кількість каталогів 1 і другого рівня.

Відкриваємо конфігураційний файл:

```
[root@sever1g ~]# nano /etc/squid/squid.conf
```

Робимо відповідні налаштування:

```

# Recommended minimum configuration:
#
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl localhost src ::1/128
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32
acl to_localhost dst ::1/128
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
#acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
acl localnet src 192.168.0.0/24 # RFC1918 possible internal network
#acl localnet src fc00::/7 # RFC 4193 local private network range
#acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl viber_ports port 5242 # viber
acl viber_ports port 4244 # viber
acl viber_ports port 5243 # viber
acl viber_ports port 9785 # viber
acl teamspeak3_ports port 9987 # TeamSpeak3
acl teamspeak3_ports port 30033 # TeamSpeak3
acl CONNECT method CONNECT

```

Після того як налаштування виконано, Squid необхідно проініціалізувати командою squid -z. Це створить структуру папок для кеша:

```
[root@severlg ~]# service squid start -Z
```

Додаємо проксі-сервер до автоматичного запуску при включенні серверу командою:

```
[root@severlg ~]# /sbin/chkconfig --levels 345 squid on
```

Конфігурація проксі-сервера наведена у додатку Г.

3.4 Налаштування DNS-сервера

DNS-сервер використовується для отримання IP-адреси по імені хоста (комп'ютера або пристрою), отримання інформації про маршрутизацію пошти, обслуговуючих вузлах для протоколів в домені.

Встановлюємо DNS-сервер:

```
[root@sever1g ~]# yum install bind bind-utils
```

Конфігураційний файл DNS-серверу знаходиться по шляху /etc/named.conf. Відкриваємо його командою:

```
[root@sever1g ~]# nano /etc/named.conf
```

Знаходимо рядки:

```
listen-on port 53 { 127.0.0.1;192.168.0.5; };
```

та додаємо ір-адресу нашого серверу 192.168.0.5

```
allow-query { localhost;192.168.0.0/24; };
```

додаємо нашу підмережу 192.168.0.0/24.

Запуск DNS-сервера здійснюється командою:

```
[root@sever1g ~]# service named start
```

Додавання в автоматичний запуск DNS-сервера здійснюється командою:

```
[root@sever1g ~]# chkconfig --level 345 named on
```

Також, пропишемо DNS, які знаходяться у файлі resolv.conf, командою:

```
[root@sever1g ~]# nano /etc/resolv.conf
```

```
nameserver 127.0.0.1
```

Після цього зберігаємо та перезапускаємо мережеві інтерфейси. Правило для між мережевого екрану приведене у налаштуваннях iptables.

3.5 Налаштування iptables

Iptables - це міжмережевий екран для операційних систем Linux, який представляє собою утиліту, яка виконує функції брандмауера. Налаштування iptables проводиться в терміналі. За допомогою правил iptables можна дозволяти або блокувати проходження трафіку. Коли відбувається спроба встановлення з'єднання з поточної машиною, iptables переглядає список правил в списку, щоб зрозуміти, як потрібно вчинити в цьому випадку. Якщо правила немає, то виконується дія за замовчуванням.

3.5.1 Типи правил

Існує три типи правил iptables - input, forward і output:

input - такі ланцюжки використовуються для контролю поведінки вхідних з'єднань.

Наприклад, якщо користувач спробує підключитися до сервера по SSH, то iptables порівняє його IP-адресу зі своїм списком, щоб дозволити або заборонити доступ.

forward - правила цього типу використовуються для обробки вхідних повідомлень, кінцевий пункт призначення яких не є поточним сервером. Наприклад, в разі маршрутизатора, до нього підключаються багато користувачів і додатки, але дані не надсилаються на сам маршрутизатор, вони лише передаються йому, щоб він міг перенаправити їх адресату.

output - такі ланцюжки використовуються для вихідних з'єднань. Якщо користувач намагається відправити запит ping до сайту, iptables вивчить ланцюжок правил, щоб зрозуміти, що потрібно робити в разі ping і цього сайту, і тільки потім дозволить або заборонить з'єднання.

Перш ніж приступати до безпосередньої налаштування брандмауера, слід визначитися з тим, яким має бути поведінка ланцюжків правил за замовчуванням. Побачити поточні налаштування iptables за замовчуванням можна за допомогою команди:

```
[root@sever1g ~]# iptables -L
```

3.5.2 Дії зі з'єднаннями

Після налаштування поведінки брандмауера за замовчуванням, можна переходити до створення правил обробки трафіку, щоб iptables розумів, що робити з конкретним з'єднанням:

Accept - дозволити з'єднання;

Drop - ігнорувати з'єднання, вести себе так, ніби його ніколи не було. Дія підходить для випадків, коли потрібно зробити так, щоб джерело запиту не дізнався про його блокування;

Reject - заблокувати з'єднання і відправити у відповідь повідомлення про помилку. Дія підходить для тих випадків, коли власник сервера хоче дати зрозуміти, що з'єднання заблоковано фаїрволом.

Налаштуємо міжмережевий екран.

Весь трафік локальної мережі 192.168.0.0/24 пускаємо через проксі-сервер командою:

```
[root@sever1g ~]# iptables -A INPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 3128 -j ACCEPT
```

Дозволяємо локальній мережі 192.168.0.0/24 використовувати DNS-сервер:

```
[root@sever1g ~]# iptables -A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 53 -j ACCEPT
```

Забезпечуємо видалену роботу адміністратору з доменом (ip-адреса домену 192.168.0.6/32):

```
[root@sever]g ~]# iptables -t nat -A PREROUTING -d 94.93.52.47/32 -p tcp -m tcp --dport 43389 -j DNAT --to-destination 192.168.0.6:3389
[root@sever]g ~]# iptables -t nat -A POSTROUTING -d 192.168.0.5/32 -p tcp -m tcp --dport 43389 -j SNAT --to-source 94.93.52.47
[root@sever]g ~]# iptables -A FORWARD -d 192.168.0.6/32 -p tcp -m tcp --dport 3389 -j ACCEPT
```

Для збереження налаштувань використовуємо команду:

```
[root@sever]g ~]# service iptables save
```

Відкрити порт до Інтернету для локальної мережі можна командою:

```
[root@sever]g ~]# iptables -A OUTPUT -p tcp -m tcp --sport 80 -j ACCEPT
```

Повний перелік правил для між мережевого екрану наведений у додатку Д.

3.6 Налаштування ssh

SSH-сервер дозволяє проводити віддалене управління операційною системою, а також копіювання файлів між комп'ютерами по шифрованому каналу зв'язку. SSH розшифровується як Secure Shell. OpenSSH забезпечує надійну авторизацію та безпечну передачу даних по відкритих каналах зв'язку.

Встановлюємо SSH-сервер, використовуємо команду:

```
[root@sever]g ~]# yum install openssh-server
```

Тепер потрібно внести зміни у конфігураційний файл, який знаходиться по шляху / etc / ssh / sshd_config. Щоб будь-який параметр вступив в силу, його слід розкоментувати. Для зміни порту підключення ми розкоментуємо рядок з його вказівкою і прописуємо потрібний нам порт (п'ятизначний порт).

З метою безпеки крім зміни порту SSH слід заборонити в нього входити віддалено в систему під root. Для цього в цьому ж файлі знаходимо рядок:

```
PermitRootLogin yes
```

та міняємо параметр yes на no, залишаючи рядок розкоментованим.

```
PermitEmptyPasswords - встановлюємо в no.
```

Додаємо порт ssh в між мережевий екран.

Тепер можна запустити ssh командою:

```
[root@sever]g ~]# service sshd start
```

Після цього додаємо автоматичний запуск при повторній перезагрузці або загрузці системи:

```
[root@sever]g ~]# chkconfig sshd on
```

3.7 Контролер домену

Контролери доменів є серверами, що підтримують роботу Active Directory. Кожен контролер домену має власну копію бази даних Active Directory, що підтримує запис. Контролери домену виступають в ролі центрального компонента безпеки в домені.

Всі операції безпеки і перевірки облікових записів виконуються на контролері домену. Кожен домен повинен мати як мінімум один контролер домену. Для забезпечення стійкості до помилок рекомендується для кожного домена встановлювати як мінімум два контролера домену.

В операційній системі Windows NT запис в базу даних підтримував тільки один контролер домену, тобто для створення і зміни параметрів облікових записів користувачів необхідно було підключення до контролера домену.

Такий контролер називався первинним контролером домену (Primary Domain Controller - PDC). Починаючи з операційної системи Windows 2000 архітектура контролерів доменів була змінена таким чином, щоб забезпечити можливість поновлення бази даних Active Directory на будь-якому контролері домена. Після оновлення бази даних на одному контролері домену, зміни репліцироваться на всі інші контролери.

Active Directory - основний засіб створення, налаштування і управління обліковими записами користувачів і комп'ютерів локальної мережі.

Одним з безумовних плюсів доменної системи є можливість гнучкого налаштування групових політик, за допомогою яких можна обмежувати доступ не тільки до програмної, але і до апаратної частини комп'ютера.

Так як у локальній мережі використовується більше 20 робочих станцій, доцільно буде використання контролеру домену в організації.

Після установки та налаштування Windows Server 2008 R2 Standard створюємо користувача, для чого потрібно виконати: «Пуск» - «Адміністрування» - «Active Directory-користувачі і комп'ютери», а потім «користувачі». У таблиці праворуч ми бачимо вже існуючого користувача. Натискаємо правою кнопкою миші у вільному місці таблиці і вибираємо: «Створити» - «користувач». Створення користувача представлено на рисунку 3.1.

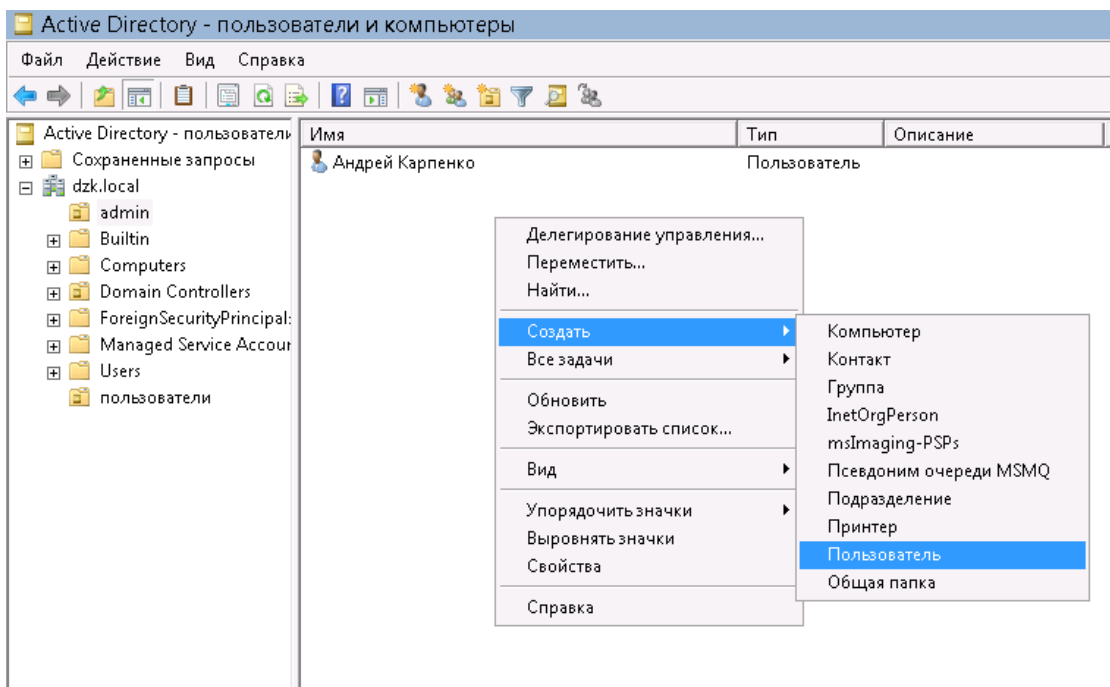


Рисунок 3.1 Меню створення користувача

Відкриється вікно введення даних користувача. Поле «Ім'я» і «Прізвище» можуть бути будь-якими. В поле «Ім'я входу користувача» необхідно вказати ім'я, під яким користувач буде логінуватися на сервер. Далі вводимо 2 рази пароль. За замовчуванням пароль повинен відповідати вимогам складності. Якщо залишити галочку «Вимагати зміни пароля при наступному вході в систему», то, відповідно, при першому вході користувача система попросить його ввести новий пароль. Тут також можна взагалі заборонити йому міняти свій пароль. І, нарешті, якщо не ставити галочку «Термін дії пароля не обмежений», то через кількість днів, зазначених у політиці безпеки паролів, система попросить у користувача ввести новий пароль. Після того як всі налаштування визначені (їх можна поміняти в будь-який час). Створення користувача представлена на рис. 3.2 та рис. 3.3.

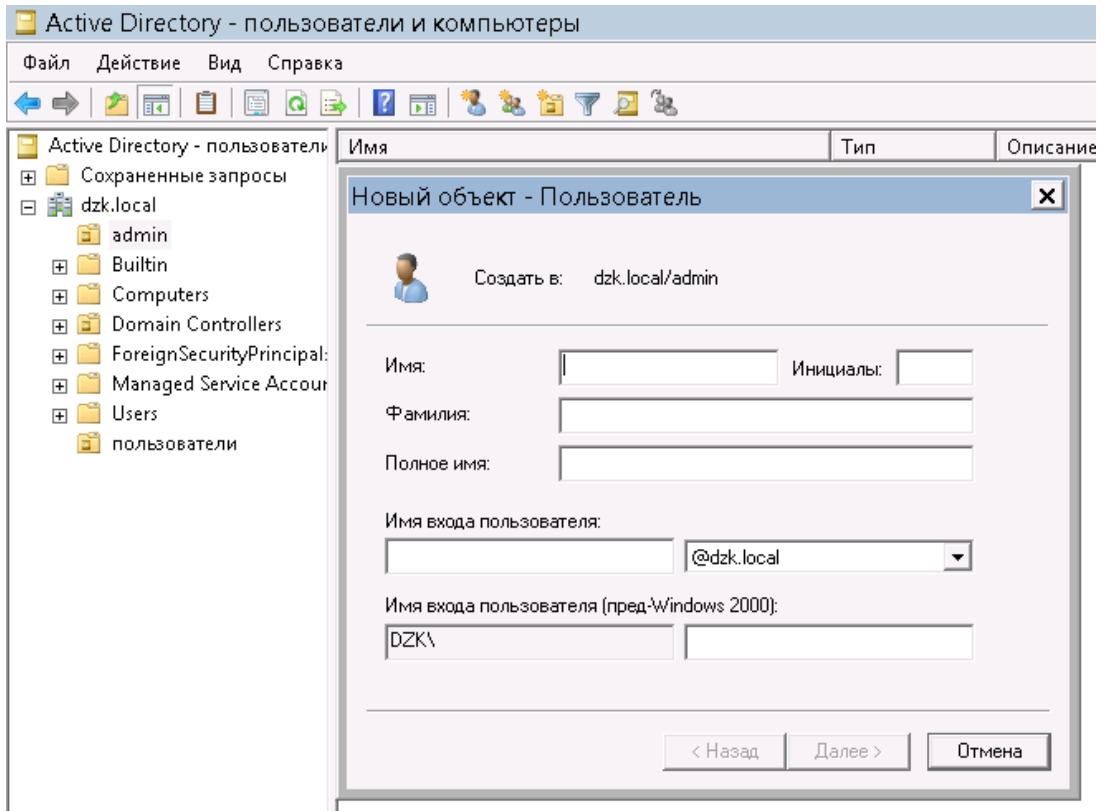


Рисунок 3.2 Створення користувача

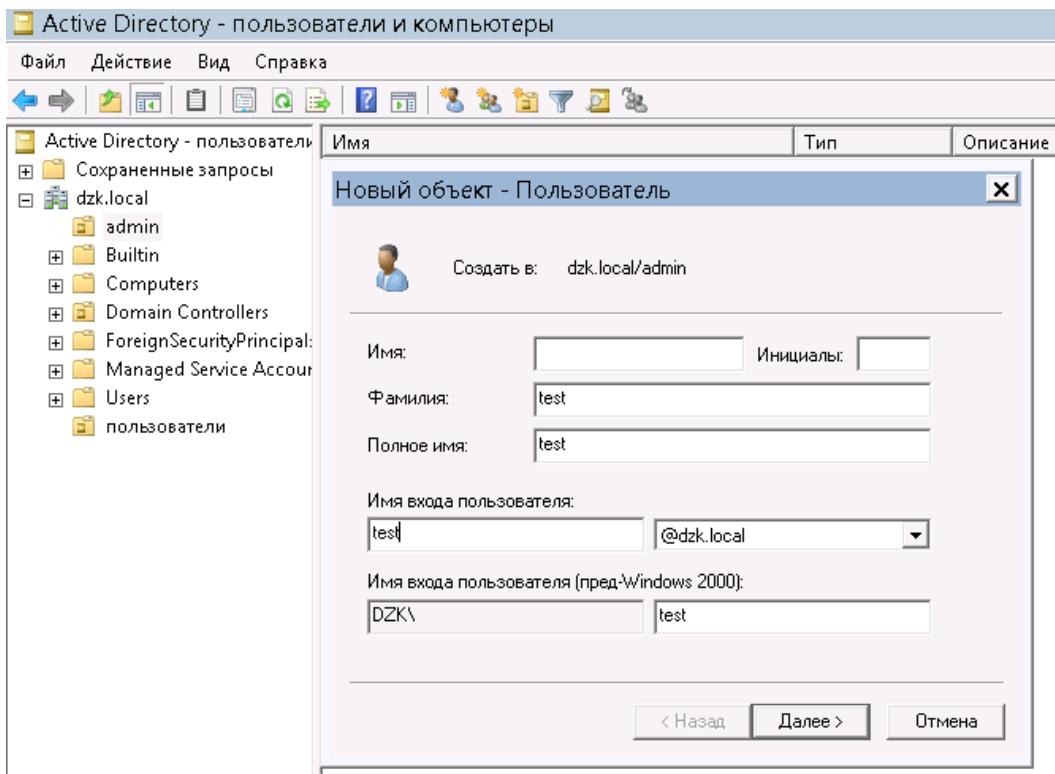


Рисунок 3.3 Створення користувача

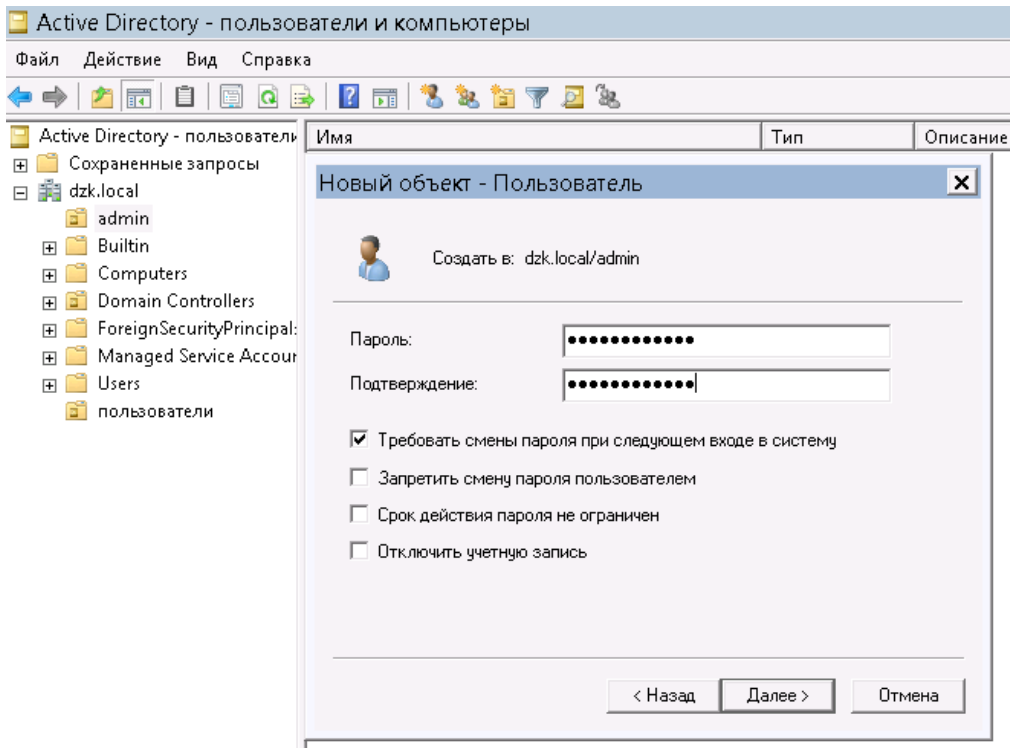


Рисунок 3.4 Створення користувача

У списку повинен з'явитися щойно створений користувач. Клікнувши по ньому правою кнопкою миші, побачимо, що з цього меню можна змінити пароль користувача, видалити, перейменувати користувача, а також відредагувати його властивості.

Після створення і налаштування користувача можна також змінити додаткові властивості користувача, якщо в цьому є необхідність.

3.8 Налаштування мережі робочих станцій

Для налаштування мережі робочих станцій, треба натиснути на панель керування, там знайти центр управління мережами та загальним доступом, потім натиснути на зміни параметрів адаптера, обрати підключення по локальній мережі і у властивостях прописати мережеві налаштування котрі наведені на рис. 3.5.

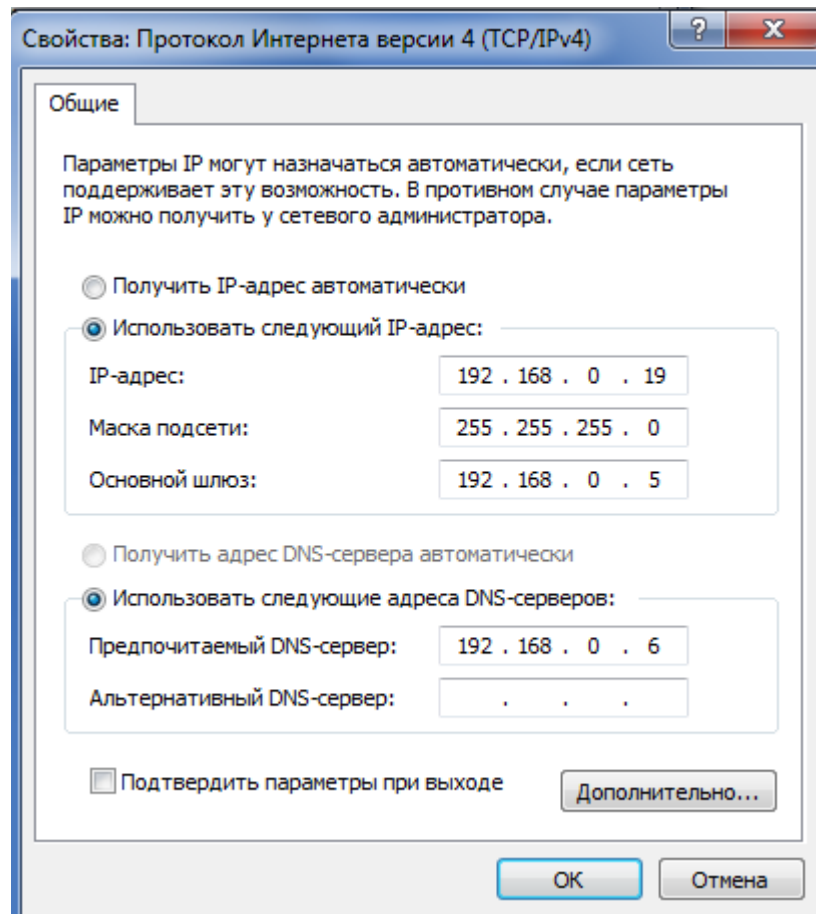


Рисунок 3.5 Мережеві налаштування

Також для того, щоб запрацював internet, треба у властивостях користувача, котрі знаходяться у панелі керування зазначити проксі-сервер (рис 3.6).

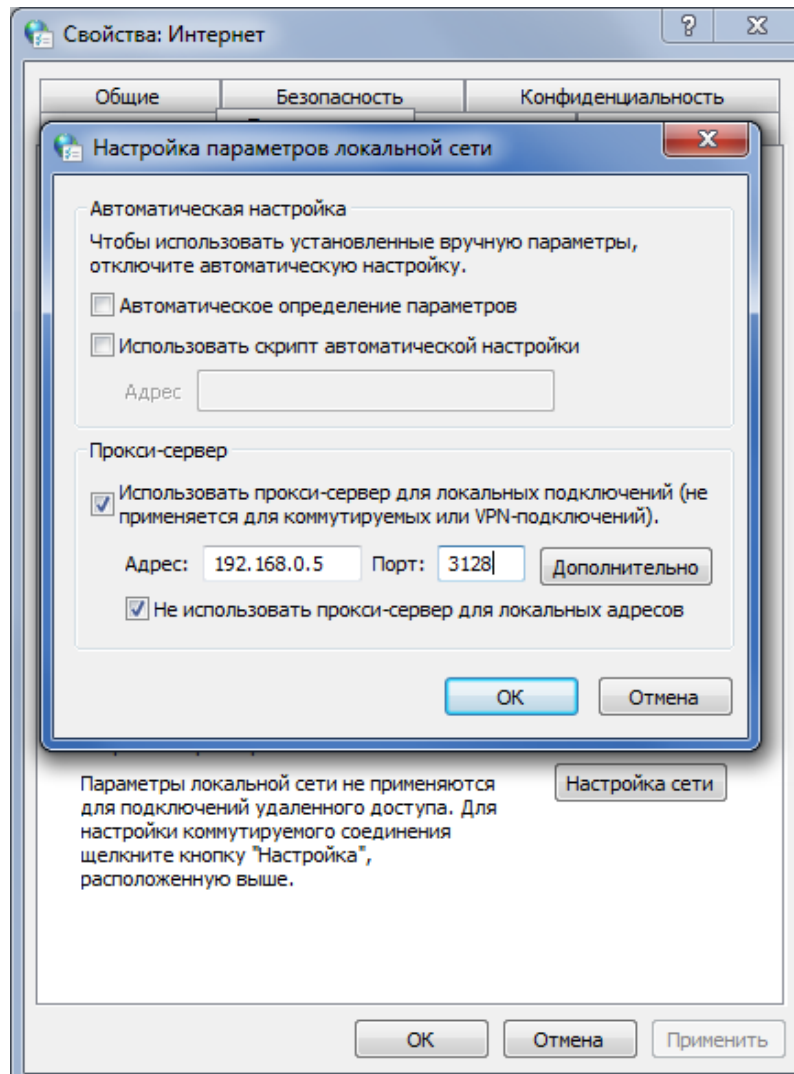


Рисунок 3.6 Налаштування проксі-серверу

3.9 Висновки до розділу 3

В даному розділі розроблена логічна адресація вузлів локальної мережі, налаштовано мережеві інтерфейси, проксі-сервер, DNS-сервер, між мережевий екран, SSH-сервер під управлінням операційної системи CentOS 6.7, створені користувачі в Active Directory, налаштовано мережу робочих станцій.

РОЗДІЛ 4

ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Загальні положення

4.1.1 Ця інструкція розроблена для зайнятих експлуатацією ПЕОМ (далі операторів): оператор ПЕОМ, робота яких пов'язана з прийомом і введенням інформації, спостереженням і коригуванням вирішуваних завдань по готових програмах; програмістів, зайнятих на ПЕОМ розробкою, перевіркою, налагодженням програм; інженерів і техніків ПЕОМ, що виконують профілактичні та ремонтні роботи, що встановлюють причини збоїв, що працюють зі схемами та іншою техдокументації; користувачів ПЕОМ, які суміщають роботу оператора з основною роботою і зайнятими роботою з ПЕОМ менше половини свого робочого часу.

4.1.2 Робота оператора ПЕОМ відноситься до категорії робіт, пов'язаних з небезпечними і шкідливими факторами. В процесі на оператора ПЕОМ надають дію такі небезпечні і шкідливі виробничі фактори.

4.1.3 До робіт оператором, програмістом, інженером і техніком ПЕОМ, користувачем ПЕОМ допускаються:

- Особи не молодше 18 років;
- ті хто пройшов вступний інструктаж з охорони праці;
- ті хто пройшов навчання безпечним прийомом і методам, і пройшли перевірку знань, в тому числі з електробезпеки з присвоєнням 1-ої кваліфікації групи по електробезопасності;
- ті хто пройшов курс навчання принципам роботи з обчислювальним технікою, спеціальне навчання по роботі на персональному комп'ютері з використанням конкретного програмного забезпечення;
- ті хто пройшов інструктаж з охорони праці на конкретному робочому місці по даній та інструкції.

4.2 Вимоги безпеки перед початком роботи

4.2.1 Перед початком роботи:

- оглянути і привести в порядок робоче місце;
- відреглювати освітленість на робочому місці, переконатися в достатності освітленості, відсутності відображень на екрані, відсутності зустрічного світлового потоку;
- перевірити правильність підключення обладнання в електромережу;

- перевірити правильності установки столу, стільця, підставки для ніг, пюпітра, положення обладнання, кута нахилу екрану, положення клавіатури і, при необхідності, провести регулювання робочого столу і крісла, а також розташування елементів комп'ютера відповідно до вимог ергономіки і з метою виключення незручних поз і тривалих напруг тіла.

4.2.2 При включенні комп'ютера оператор зобов'язаний дотримуватися наступну послідовність включення обладнання:

- увімкнути живлення;
- увімкнути периферійні пристрої (принтер, монітор, сканер і ін.);
- увімкнути системний блок.

4.3 Вимоги безпеки під час роботи

4.3.1 Оператор під час роботи зобов'язаний:

- виконувати тільки ту роботу, яка йому доручена і по якій він був проінструктований;
- протягом всього робочого дня тримати в порядку і чистоті робоче місце;
- тримати відкритими всі вентиляційні отвори пристрою;
- при необхідності припинення роботи на деякий час коректно закрити всі активні завдання;
- виконувати санітарні норми і дотримуватися режими роботи і відпочинку;
- дотримуватися правила експлуатації обчислювальної техніки відповідно до інструкцій по експлуатації;
- при роботі з текстовою інформацією вибирати найбільш фізіологічний режим чорних символів на білому фоні;
- дотримуватися встановлені режимом робочого часу регламентовані перерви в роботі і виконувати в фізкультпаузах і фізкультминутках рекомендовані вправи для очей, шиї, рук, тулуба, ніг;
- дотримуватися відстань від очей до екрана в межах 60-80 см.

4.3.2 Оператору під час роботи забороняється:

- торкатись одночасно екрана монітора і клавіатури;
- торкатись до задньої панелі системного блоку при включеному живленні;
- перемикати роз'єми інтерфейсних кабелів периферійних пристроїв при включенні живлення, крім роз'ємів стандарту USB;
- складати верхні панелі пристроїв паперами та сторонніми предметами;
- збирати на робочому місці купи документів з метою недопущення накопичення органічного пилу;

- вимикати живлення під час виконання активної задачі;
- не допускати попадання вологи на поверхню клавіатури, принтерів та ін. пристроїв;
- вмикати охолоджене обладнання (принесене з вулиці в зимовий час);
- самостійний ремонт обладнання.

4.4 Вимоги безпеки у аварійних ситуаціях

4.4.1 Оператор зобов'язаний:

- у всіх випадках виявлення обриву проводів живлення - несправності заземлення та інших пошкоджень електрообладнання, появи запаху гару негайно відключити живлення і повідомити про аварійну ситуацію керівнику і черговому електрику;
 - для виявлення людини, що потрапила під напругу - негайно звільнити його від дії струму шляхом відключення електроживлення і до прибуття лікаря надати потерпілому медичному допомогу;
 - при будь-яких випадках збою в роботі технічного обладнання програмного забезпечення негайно викликати представника інженерно-технічної служби обчислювальної техніки;
 - у разі появи різі в очах, різкому погіршенні видимості; неможливості сфокусувати погляд або навести його на різкість, появі болю в пальцях і кистях рук, посилення серцебиття негайно покинути робоче місце, повідомити про те, що сталося, керівника і звернутися до лікаря;
 - при загорянні обладнання відключити живлення і вжити заходів до гасіння вогнища пожежі за допомогою вуглекислотного або порошкового вогнегасника, викликати пожежну команду і повідомити про подію керівника.

4.5 Вимоги безпеки після закінчення роботи

4.5.1 Після закінчення робіт оператор зобов'язаний дотримуватися наступну послідовність виключення обчислювальної техніки:

- провести закриття всіх активних завдань;
- вимкнути живлення системного блоку засобами ОС;
- вимкнути харчування всіх периферійних пристроїв;
- відключити живлення.

4.5.2 Після закінчення робіт оператор зобов'язаний оглянути і привести в порядок робоче місце.

4.6 Безпека у надзвичайних ситуаціях

У разі виникнення надзвичайної ситуації, організація:

-дотримується планів цивільного захисту і заходів щодо запобігання виникненню надзвичайних ситуацій та ліквідації їх наслідків;

-дотримується нормативно - правових актів у справах цивільної оборони;

-організує здійснення заходів щодо евакуації працівників підприємства із зон надзвичайних ситуацій та зон можливих бойових дій в особливий період;

У разі виникнення надзвичайної ситуації, відповідальна особа:

-забезпечує оперативне оповіщення керівного складу про загрозу виникнення та виникнення надзвичайної ситуації;

-здійснює у межах своїх повноважень збір, накопичення, обробку і аналіз інформації про стан техногенної та природної безпеки;

-забезпечує здійснення заходів щодо удосконалення організації цивільного захисту.

4.7 Вимоги до приміщень

Геометричні розміри приміщення зазначені в табл. 4.1.

Таблиця 4.1 – Розміри приміщення

Найменування	Значення
Довжина, м	6
Ширина, м	4
Висота, м	3
Площа, м ²	24
Об'єм, м ³	75

Згідно з ДСН 3.3.6.042-99 [11] розмір площі для одного робочого місця оператора персонального комп'ютера має бути не менше 6 кв. м, а об'єм — не менше 20 куб. м. Отже, дане

приміщення цілком відповідає зазначеним нормам.

Для забезпечення потрібного рівного освітленості кімната має три вікна та система загального рівномірного освітлення, що встановлена на стелі.

4.7.1 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за ДСанПіН 3.3.2.007-98 [11] і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Таблиця 4.2 - Характеристики робочого місця

Найменування параметра	Фактичне значення	Нормативне значення
Висота робочої поверхні, мм	750	680 ÷ 800
Висота простору для ніг, мм	730	не менше 600
Ширина простору для ніг, мм	660	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	470	400 ÷ 500
Ширина сидіння, мм	400	не менше 400
Глибина сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700 ÷ 800

Робочий стіл на досліджуваному місці також містить достатньо простору для ніг. Крісло, що використовується в якості робочого сидіння, є підйомно поворотним, має підлокітники і можливість регулювання за висотою і кутом нахилу спинки, також воно м'яке і виконане з екологічної шкіри, що дає можливість працювати у комфорті. Екран монітору знаходиться на відстані 0.8 м, клавіатура має можливість регулювання кута нахилу 5-15°. Отже, за всіма параметрами робоче місце відповідає нормативним вимогам.

Розміщення вікон забезпечує природне освітлення з коефіцієнтом природного освітлення не менше 1,5%, а загальне штучне освітлення, яке здійснюється за допомогою люстри, забезпечує рівень освітленості не менше 200 Лк.

У кімнаті є електрична мережа з напругою 220 В, яка створює небезпеку ураження

електричним струмом. ПК та периферійні пристрої можуть бути джерелами електромагнітних випромінювань, аерозолів та шкідливих речовин (часток тонеру, оксидів нітрогену та озону).

4.7.2 Освітлення

Робота на ПЕОМ може здійснюватися за таких видах освітлення:

- загальному штучному освітленні, коли відео монітори розташовуються по периметру приміщення або при центральному розташуванні робочих місць у два ряди по довжині кімнати з екранами, звернені в протилежні сторони;

- суміщене освітлення (природне + штучне) тільки при одному і трьох рядном розташуванні робочих місць, коли екран і поверхню робочого столу знаходяться перпендикулярно світла несучій стіні.

Природне освітлення, коли робочі місця з ПЕОМ розташовуються в один ряд по довжині приміщення на відстані 0,8 - 1,0 м від стіни з віконними прорізами, і екрани знаходяться перпендикулярно цієї стіни. Основний потік природного світла при цій повинен бути зліва.

У проекті, що розробляється, передбачається використовувати суміщене освітлення. У світлий час доби використовуватиметься природне освітлення приміщення через віконні отвори, в решту часу використовуватиметься штучне освітлення. Штучне освітлення створюється газорозрядними лампами.

Штучне освітлення в робочому приміщенні передбачається здійснювати з використанням люмінесцентних джерел світла в світильниках загального освітлення, оскільки люмінесцентні лампи мають високу потужність (80 Вт), тривалий термін служби (до 10000 годин), спектральний складом випромінюваного світла, близький до сонячного. При експлуатації ЕОМ виконується зорова робота IVв розряду точності (середня точність). При цьому нормована освітленість на робочому місці (E_n) рівна 200 лк. Джерелом природного освітлення є сонячне світло.

У приміщенні, де розташовані ЕОМ передбачається природне бічне освітлення, рівень якого відповідає ДБН В.2.5-28:2015 [9]. Джерелом природного освітлення є сонячне світло.

Для будівель виробництв світловий коефіцієнт приймається в межах 1/6 - 1/10:

$$\sqrt{a^2 + b^2} \times S_b = (1/8 \text{ - } 1/10) S_n \quad (4.1)$$

де S_b – площа віконних прорізів, м²;

S_n – площа підлоги, м².

$$S_{\text{вікна}} = a \cdot b = 6 \cdot 4 = 24 \text{ м}^2 \quad (4.2)$$

$$S_{\text{вік}} = 1/8 \cdot 24 = 3 \text{ м}^2 \quad (4.3)$$

Приймаємо 2 вікна площею $S = 1,6 \text{ м}^2$ кожне.

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 5 м, ширина 5 м, світильниками ЛПО2П, оснащеними лампами типа ЛБ (дві по 80 Вт) з світловим потоком 5400 лм кожна.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників n виробляється по формулі (4.4):

$$n = \frac{E \times S \times Z \times K}{F \times U \times M} \quad (4.4)$$

де E – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м^2 ;

$S = 24 \text{ м}^2$;

Z – поправочний коефіцієнт світильника ($Z = 1,15$ для ламп розжарювання та ДРЛ; $Z = 1,1$ для люмінесцентних ламп);

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 5400лм (для ЛБ-80).

Підставивши числові значення у формулу (4.2), отримуємо:

$$n = \frac{300 \cdot 24 \cdot 1,15 \cdot 1,5}{5400 \cdot 0,575 \cdot 2} \approx 2$$

(4.5)

Приймаємо освітлювальну установку, яка складається з 2-х світильників, які складаються з двох люмінесцентних ламп загальною потужністю 160 Вт, напругою – 220 В.

4.7.3 Вентилювання

У приміщенні, де знаходяться ПЕОМ, повітрообмін реалізується за допомогою вікна та установки кондиціонера. Цей метод забезпечує приток потрібної кількості свіжого повітря.

4.7.4 Розрахунок захисного заземлення

Загальний опір захисного заземлення визначається за формулою:

$$R_{\text{зп}} = \frac{R_3 \cdot R_n}{R_n \cdot \eta_3 + R_3 \cdot \eta_n} \quad (4.6)$$

де R_3 - опір заземлення, якими когут бать труби, опори, кути і т.п., Ом;

$R_{\text{ш}}$ - опір опори, яке з'єднує заземлювачі, Ом;

n - кількість заземлювачів;

η_3 - коефіцієнт екранування заземлювача;

приймається в межах $0,2 \div 0,9$;

$\eta_3 = 0,7$

$\eta_{\text{ш}}$ - коефіцієнт екранування сполучної стійки; приймається в межах $0,1 \div 0,7$;

$\eta_{\text{ш}} = 0,5$;

Опір заземлення визначається за формулою:

$$R_3 = \frac{\rho}{2\pi \cdot l} \left[\ln \frac{2 \cdot l}{d} + \frac{1}{2} \ln \frac{4 \cdot t + l}{4 \cdot t - l} \right] \quad (4.7)$$

де ρ - питомий опір ґрунту, залежить від типу ґрунту, Ом·м;

для піску - $400 \div 700$ Ом·м; приймаємо $\rho = 400$ Ом·м;

l - довжина заземлювача, м; для труб - 2-3 м; $l = 3$ м;

d - діаметр заземлювача, м; для труб - 0,03-0,05 м; $d = 0,05$ м;

t - відстань від середини забитого в ґрунт заземлювача до рівня землі, м; $t = 2$ м.

$$R_3 = \frac{400}{2 \cdot 3,14 \cdot 3} \left[\ln \frac{2 \cdot 3}{0,05} + \frac{1}{2} \ln \frac{4 \cdot 2 + 3}{4 \cdot 2 - 3} \right] = 110, \text{ Ом} \quad (4.8)$$

Опір смуги, що з'єднує заземлювачі, визначається за формулою:

$$R_w = \frac{\rho}{2\pi \cdot L} \cdot \ln \frac{2 \cdot L^2}{b \cdot t^1}, \quad (4.9)$$

де L - довжина смуги, що з'єднує заземлювачі (м) і приблизно дорівнює периметру будівлі: $P_{\text{буд.}} = 42 \cdot 2 + 38 \cdot 2 = 160$ м; $L = 160$ м;

b - ширина смуги, м; $b = 0,03$ м;

t_1 - глибина заземлення від рівня землі, м; $t_1 = 0,5$ м.

$$R_n = \frac{400}{2 \cdot 3,14 \cdot 160} \cdot \ln \frac{2 \cdot 160^2}{0,03 \cdot 0,5} = 5,99, \text{ Ом} \quad (4.10)$$

Кількість заземлювачів захисного заземлення визначається за формулою:

$$n = \frac{2 \cdot R_3}{4 \cdot \eta_3}, \quad (4.11)$$

де 4 - допустимий загальний опір, Ом;

2 - коефіцієнт сезонності.

Визначаємо загальний опір захисного заземлення:

$$R_{\text{ззп}} = \frac{110 \cdot 5,99}{5,99 \cdot 79 \cdot 0,7 + 110 \cdot 0,5} = 1,7 \text{ Ом} \quad (4.12)$$

Висновок: дане захисне заземлення буде забезпечувати електробезпеку будівлі, так як виконується умова: $R_{\text{ззп}} < 4$ Ом.

4.8 Охорона навколишнього природного середовища

Основним екологічним аспектом в процесі діяльності за даними спеціальностями є процеси впливу на атмосферне повітря та процеси поводження з відходами, які утворюються, збираються, розміщуються, передаються на видалення (знешкодження), утилізацію, тощо в ІТ галузі.

Вплив на атмосферне повітря при нормальних умовах праці не оказує, бо не має в приміщенні сканерів, принтерів та інших джерел викиду забруднюючих речовин в повітря робочої зони.

З метою визначення та прогнозування впливу відходів на навколишнє середовище, своєчасного виявлення негативних наслідків, їх запобігання відповідно до Закону України «Про відходи» повинен здійснюватися моніторинг місць утворення, зберігання, і видалення відходів.

Відомості про місце утворення та місце розташування відходів:

- Відходи комунальні - зовнішній сміттєвий бак для зберігання побутових відходів;
- Макулатура паперова – відро для сміття, будинок 17 кабінет 105;
- Змінні носії інформації – відро для сміття, будинок 17 кабінет 105;
- Батарейки та акумулятори - зовнішній сміттєвий бак для зберігання побутових відходів;

4.9 Висновки до розділу 4

В даному розділі визначені загальні положення, розроблені вимоги безпеки перед початком роботи, вимоги безпеки під час роботи, вимоги безпеки у аварійних ситуаціях, вимоги безпеки після закінчення роботи, визначені завдання для безпеки у надзвичайних ситуаціях. Визначено параметри і певні характеристики приміщення, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника. Приведені рекомендації щодо організації робочого місця.

ВИСНОВКИ

На основі аналізу технічного завдання спроектовані логічна та фізична топології мережі для Головного управління Держгеокадастру у Луганській області. Вибрано операційні системи та всі технічні засоби і комплектуючі як для серверу так і для робочих станцій. Розроблено процедуру налаштування сервера на базі ОС CentOS 6.7. Розглянуто контролер домену, розроблено таблицю IP-адрес.

Для проектування СКС було використане програмне забезпечення Microsoft Visio.

Так як працівники організації можуть користуватися всіма ресурсами мережі або тільки їх частиною, в дипломному проекті розроблені методики та алгоритм поділу доступу по категоріям. Для кожної категорії користувачів створені групи користувачів з певним переліком функцій і прав доступу.

Також була розроблена конфігурація мережі, яка задовольняє критеріям по швидкодії, надійності та інформаційної безпеки.

Локальна мережа побудована по деревовидній топології, в якій кожен комп'ютер через спеціальний мережевий адаптер (з пропусною здатністю 100 Mbit / s) підключається окремим кабелем до об'єднаного пристрою. За рахунок цього забезпечується захист від розриву кабелю, тобто якщо кабель робочої станції буде пошкоджений, це не призведе до виходу з ладу всього сегмента мережі, що забезпечує надійність всієї мережі.

У локальну мережу об'єднані такі пристрої:

робочі станції;

серверна станція;

комутатори.

В побудованій локальній мережі забезпечується спільна обробка інформації, спільне використання файлів, централізоване управління робочими станціями, контроль за доступом до інформації, спільний доступ в Інтернет.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Microsoft. Установка та налаштування серверів:
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc755183\(v=ws.11\);](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc755183(v=ws.11);)
2. Буров Є. Комп'ютерні мережі. – Львів: БАК, 1999 – 468 с.
<http://194.44.152.155/elib/local/sk629495.pdf>
3. Оліфер В. Р., Оліфер Н.А. «Комп'ютерні мережі. Принципи, технології, протоколи, 2-е изд» СПб, Пітер-прес, 2002
https://www.bsuir.by/m/12_100229_1_85460.pdf
4. А. Б. Семенов, С. К. Стрижаков, В. Р. Сунчелей. «Структуровані Кабельні Системи Айті-СКС, видання 3-е». Москва, Айті-Прес, 2001
<https://rucont.ru/file.ashx?guid=e59da1ab-72f8-42ce-ac38-4c8b199abfcc>
5. Новіков Ю. «Локальні мережі: архітектура, алгоритми, проектування». Москва, ЕКОМ, 2000
http://kitab.ttnda.az/upload-files/books/09/869/lokalniye_seti.pdf
6. «LAN/Журнал мережевих рішень». Москва, Відкриті системи, січень 2004
7. <http://www.oхранatruda.in.ua/>
8. <https://jobs.ua/kzot/part-11>
9. НПАОП 0.00-1.28-10 Правила охорони праці під час експлуатації електронно-обчислювальних машин.
10. ДБН В.2.5-28:2015 Природне і штучне освітлення
11. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих

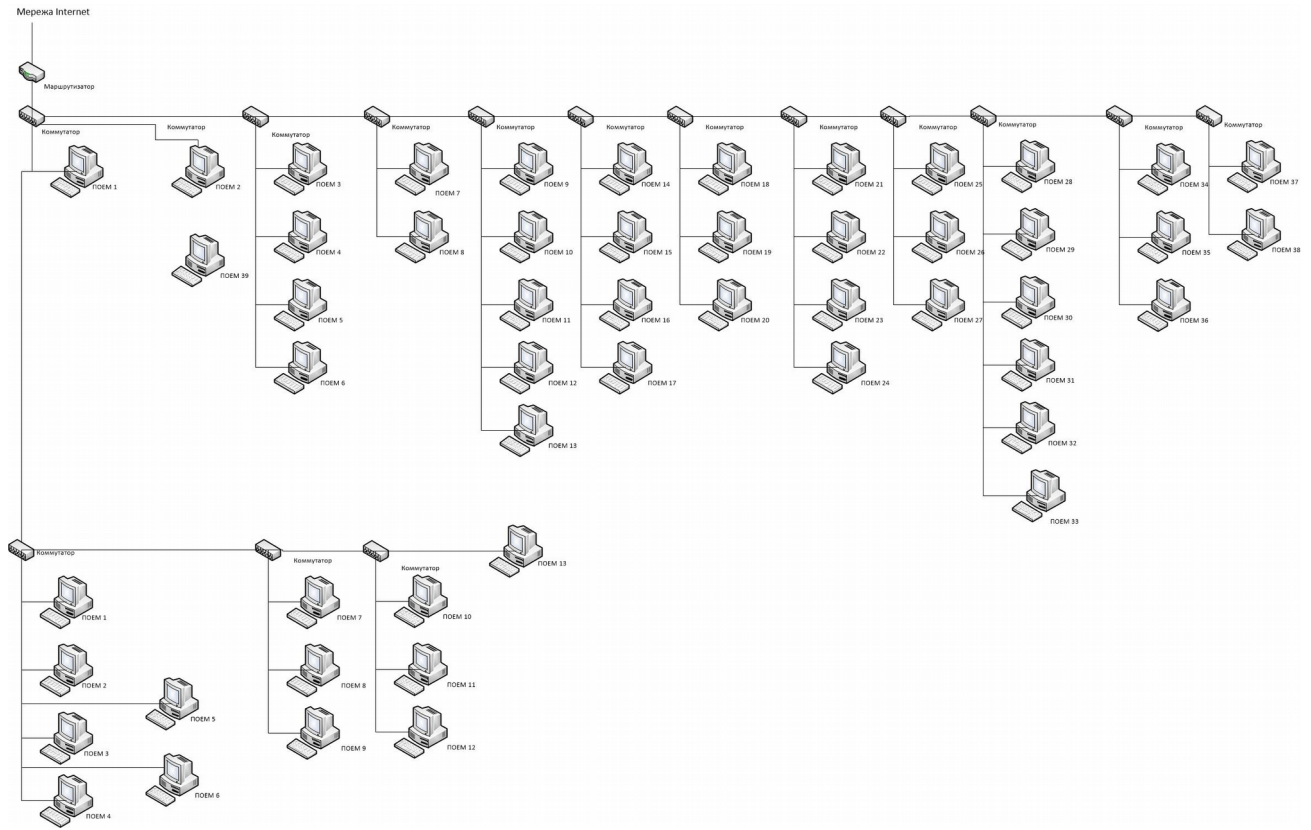
Додаток А

Порівняльний аналіз топології локально-обчислювальних мереж

Характеристики	Топології обчислювальних мереж		
	Зірка	Кільце	Шина
Вартість розширення	Незначна	Середня	Середня
приєднання абонентів	Пасивне	Активне	Пасивне
Захист від відмов	Незначна	Незначна	Висока
Розміри системи	будь-які	будь-які	обмежені
Захищеність від прослуховування	Хороша	Хороша	Незначна
Стоимость підключення	Незначна	Незначна	Висока
Поведінка системи при високих навантаженнях	Хороша	Задовільна	Незначна
Можливість роботи в реальному режимі часу	Відмінна	Хороша	Незначна
Розведення кабелю	Хороша	Задовільна	Хороша
Обслуговування	Відмінна	Середнє	Середнє

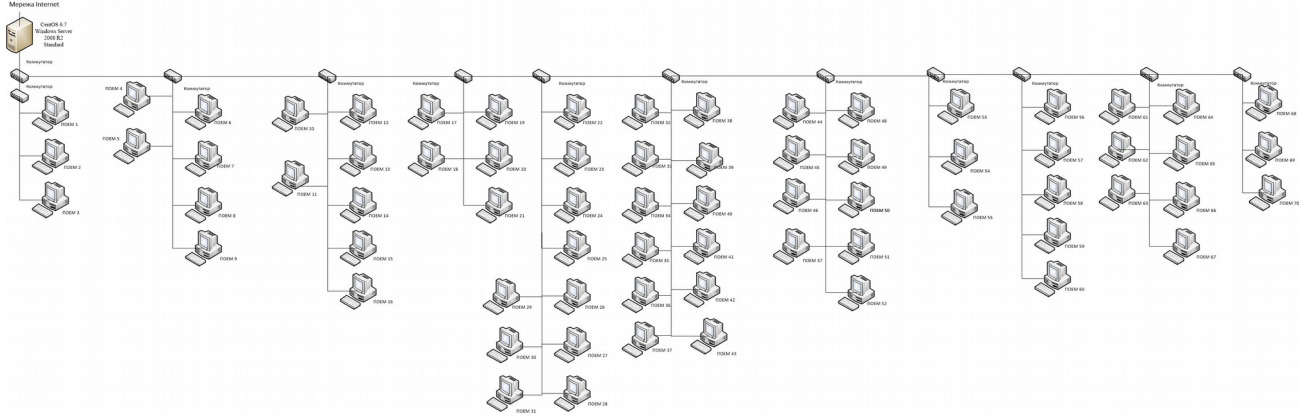
Додаток Б

Інформаційно-телекомунікаційна система Головного управління Держгеокадастру у Луганській області



Додаток В

Логічна топологія локальної комп'ютерної мережі Головного управління Держгеокадастру у Луганській області



Додаток Г
Конфігурація проксі-серверу

```
#
# Recommended minimum configuration:
#
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl localhost src ::1/128
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32
acl to_localhost dst ::1/128
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
#acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
acl localnet src 192.168.0.0/24 # RFC1918 possible internal network
#acl localnet src fc00::/7 # RFC 4193 local private network range
#acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl viber_ports port 5242 # viber
acl viber_ports port 4244 # viber
acl viber_ports port 5243 # viber
acl viber_ports port 9785 # viber
```



```

acl teamspeak3_ports port 9987      # TeamSpeak3
acl teamspeak3_ports port 30033     # TeamSpeak3
acl CONNECT method CONNECT

#acl INSIDE_IP dst
#always_direct allow INSIDE_IP

# ban_siu
#acl ban_siu src 192.168.0.50

#ban_ip
#acl ban src
#CḡPµ·CḡPµC€PµPSPSCḡPµ CÍPµC,Pë
acl UsersNet src 192.168.0.0/24
# CḡC,Pḡ-C,Pḡ PjPḡPḡPSPḡ :)
#acl Allow! src
# PjPḡPḡPSPḡ PICÍPµ
acl AllowAll src 192.168.0.18

# streaming download
acl fails rep_mime_type ^.*mms.*
acl fails rep_mime_type ^.*ms-hdr.*
acl fails rep_mime_type ^.*x-fcs.*
acl fails rep_mime_type ^.*x-ms-asf.*
acl fails2 urlpath_regex dvplayer mediastream mms://
acl fails2 urlpath_regex \.asf$ \.afx$ \.flv$
acl deny_rep_mime_flashvideo rep_mime_type -i video/flv
acl x-type req_mime_type -i ^application/x-mplayer2$
acl x-type req_mime_type -i application/x-mplayer2
acl x-type req_mime_type -i application/x-pncommand
acl x-type req_mime_type -i ^video/x-ms-asf$
acl x-type2 rep_mime_type -i ^application/x-mplayer2$
acl x-type2 rep_mime_type -i application/x-mplayer2
acl x-type2 rep_mime_type -i application/x-pncommand
acl x-type2 rep_mime_type -i ^video/x-ms-asf$
http_reply_access deny deny_rep_mime_flashvideo

```

```
#####
```

```
#acl sites_nocache dstdomain '/etc/squid/sites_nocache'
acl advertisement url_regex "/etc/squid/list/advertisement.acl"
acl banners dstdomain "/etc/squid/list/banner.list"
acl anonymizer dstdomain "/etc/squid/list/anonymizer.list"
acl gamez dstdomain "/etc/squid/list/gamez.list"
acl exua dstdomain -i .ex.ua .ok.ru .facebook.com .vk.com .vk.me .instagram.com .yandex.ru
.fotostrana.ru .privet.ru .liveinternet.ru .toodoo.ru .rossia.org .blogs.mail.ru .mylivepage.ru .mirtesen.ru
.blogs.tks.ru .klerk.ru .beon.ru .babyblog.ru .blogus.ru .itblogs.ru .fion.ru .ruspace.ru .revision.ru
.diary.ru .livelib.ru .fishingmap.ru .ilovecinema.ru .100druzei.ru .dogster.ru .facultet.ru .mmm-
tasty.ru .webkrug.ru .venividi.ru .yatalant.ru .my.mail.ru .limpa.ru .spaces.ru .moikrug.ru .sosed-
online.ru .zabarankoi.ru .u-mama.ru .autokadabra.ru .otdohnuli.ru .telefoner.ru .vkrugudruzei.ru
.photobucket.com .toknowall.com

acl odnoglazniki dstdomain -i .odnoklassniki.ua .odnoklassniki.ru .vk.com .vk.me
#acl local dstdomain 10.222.0.4 10.222.0.7
#acl cool_local dst edi.su translate.ru translate.google.com
#acl cool_local2 dstdomain "/etc/squid/list/maps.list"
#acl cool_ex_ua src
#acl cool_odnoglazniki src
acl teamview_dasha_moloko src 192.168.0.15 192.168.0.35
acl activate dstdomain -i .pointdev.com .activate.adobe.com .praactivate.adobe.com
.download.windowsupdate.com update.microsoft.com windowsupdate.microsoft.com
acl remote dstdomain -i .teamviewer.com .dyngate.com 216.108.224.222 80.237.220.185
85.214.154.223 85.214.78.0-85.214.78.254 77.41.13.0-77.41.13.254 80.237.157.95 85.25.143.69
217.23.49.0-217.23.49.24 87.230.74.0-87.230.74.24 87.230.73.0-87.230.73.24 89.185.96.0-
89.185.96.254 91.121.4.0-91.121.4.254 91.121.28.0-91.121.28.254 93.186.48.0-93.186.48.254
178.75.246.0-178.75.246.254 178.77.120.0-178.77.120.254 85.25.147.0-85.25.147.254 62.75.215.0-
62.75.215.254 62.75.246.0-62.75.246.254 69.64.74.0-69.64.74.254 89.189.96.0-89.189.96.245
acl stream dstdomain "/etc/squid/list/stream.list"
#reklama
#acl cool_advertisement src 10.222.1.55 10.222.2.183 10.222.2.103 10.222.1.74 10.222.2.104

# POOL #
```

```

delay_pools 1
delay_class 1 1
#Adelay_access 1 allow stream !AllowAll
delay_parameters 1 8000/64000

##### streaming #####
http_access deny UsersNet fails
http_reply_access deny UsersNet fails
http_access deny UsersNet fails2
http_reply_access deny UsersNet fails2
http_access deny UsersNet x-type
http_reply_access deny UsersNet x-type
http_access deny UsersNet x-type2
http_reply_access deny UsersNet x-type2
##### streaming #####

http_access allow AllowAll
#http_access deny UsersNet local
#http_access deny ban_siu
#http_access deny advertisement !Allow! !cool_advertisement
#http_access deny UsersNet banners !Allow! !cool_advertisement
http_access deny UsersNet anonymizer
http_access deny UsersNet gamez
#http_access deny ban !cool_local !cool_local2
http_access deny UsersNet exua
#http_access deny UsersNet odnoglazniki !cool_odnoglazniki
http_access deny UsersNet activate
http_access deny UsersNet remote !teamview_dasha_moloko
http_access allow UsersNet all
#no_cache deny sites_nocache
#
# Recommended minimum Access Permission configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost

```

```
http_access deny manager

# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

ignore_expect_100 on

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 192.168.0.5:3128

dns_v4_first on

visible_hostname severlg.local
```

We recommend you to use at least the following line.

```
hierarchy_stoplist cgi-bin ?
```

Uncomment and adjust the following to add a disk cache directory.

```
cache_dir ufs /var/spool/squid 8000 16 256
```

```
cache_effective_user squid
```

```
cache_effective_group squid
```

Leave coredumps in the first cache dir

```
coredump_dir /var/spool/squid
```

Add any of your own refresh_pattern entries above these.

```
refresh_pattern ^ftp:          1440 20% 10080
```

```
refresh_pattern ^gopher:      1440 0% 1440
```

```
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
```

```
refresh_pattern .              0 20% 4320
```

Додаток Д
Повний перелік правил для міжмережевого екрану

```
# Generated by iptables-save v1.4.7 on Thu Oct 25 19:26:51 2018
*nat
:PREROUTING ACCEPT [58512:3897882]
:POSTROUTING ACCEPT [22679:1520694]
:OUTPUT ACCEPT [19116:1335418]
-A PREROUTING -d 94.93.52.47/32 -p tcp -m tcp --dport 554 -j DNAT --to-destination
192.168.0.4:554
-A PREROUTING -d 94.93.52.47/32 -p tcp -m tcp --dport 8000 -j DNAT --to-destination
192.168.0.4:8000
-A PREROUTING -d 94.93.52.47/32 -p tcp -m tcp --dport 53389 -j DNAT --to-destination
192.168.0.6:3389
-A POSTROUTING -s 192.168.0.192/26 ! -d 192.168.0.0/24 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.64/26 ! -d 192.168.0.0/24 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.128/26 ! -d 192.168.0.0/24 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.0/24 -p tcp -m tcp -m multiport --dports 36699 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.21/32 -p tcp -m tcp -m multiport --dports 11122 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.21/32 -p tcp -m tcp -m multiport --dports 11121 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.21/32 -p tcp -m tcp -m multiport --dports 10057 -j SNAT
--to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.52/32 -p tcp -m tcp -m multiport --dports 11122 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.52/32 -p tcp -m tcp -m multiport --dports 11121 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.52/32 -p tcp -m tcp -m multiport --dports 10057 -j SNAT
--to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.19/32 -p tcp -m tcp -m multiport --dports 11122 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.19/32 -p tcp -m tcp -m multiport --dports 11121 -j SNAT --to-
source 94.93.52.47
```

```
-A POSTROUTING -s 192.168.0.19/32 -p tcp -m tcp -m multiport --dports 10057 -j SNAT
--to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.22/32 -p tcp -m tcp -m multiport --dports 11122 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.22/32 -p tcp -m tcp -m multiport --dports 11121 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.22/32 -p tcp -m tcp -m multiport --dports 10057 -j SNAT
--to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.23/32 -p tcp -m tcp -m multiport --dports 11122 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.23/32 -p tcp -m tcp -m multiport --dports 11121 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.23/32 -p tcp -m tcp -m multiport --dports 10057 -j SNAT
--to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.33/32 -p tcp -m tcp -m multiport --dports 10080 -j SNAT
--to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.33/32 -p tcp -m tcp -m multiport --dports 10022 -j SNAT
--to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.33/32 -p tcp -m tcp -m multiport --dports 10021 -j SNAT
--to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.33/32 -p tcp -m tcp -m multiport --dports 10443 -j SNAT
--to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.37/32 -p tcp -m tcp -m multiport --dports 11122 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.37/32 -p tcp -m tcp -m multiport --dports 11121 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.37/32 -p tcp -m tcp -m multiport --dports 10057 -j SNAT
--to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.24/32 -p tcp -m tcp -m multiport --dports 143 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.24/32 -p tcp -m tcp -m multiport --dports 587 -j SNAT --to-
source 94.93.52.47
-A POSTROUTING -s 192.168.0.35/32 -p tcp -m tcp -m multiport --dports 5242 -j SNAT --to-
source 94.93.52.47
```

```
-A POSTROUTING -s 192.168.0.35/32 -p tcp -m tcp -m multiport --dports 4244 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.35/32 -p tcp -m tcp -m multiport --dports 5243 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.35/32 -p tcp -m tcp -m multiport --dports 9785 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.24/32 -p tcp -m tcp -m multiport --dports 5242 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.24/32 -p tcp -m tcp -m multiport --dports 4244 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.24/32 -p tcp -m tcp -m multiport --dports 5243 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.24/32 -p tcp -m tcp -m multiport --dports 9785 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.27/32 -p tcp -m tcp -m multiport --dports 5242 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.27/32 -p tcp -m tcp -m multiport --dports 4244 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.27/32 -p tcp -m tcp -m multiport --dports 5243 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.27/32 -p tcp -m tcp -m multiport --dports 9785 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.24/32 -p tcp -m tcp -m multiport --dports 993 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.24/32 -p tcp -m tcp -m multiport --dports 465 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.43/32 ! -d 192.168.0.0/24 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.35/32 ! -d 192.168.0.0/24 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -s 192.168.0.13/32 ! -d 192.168.0.0/24 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -d 192.168.0.4/32 -p tcp -m tcp --dport 554 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -d 192.168.0.4/32 -p tcp -m tcp --dport 8000 -j SNAT --to-source 94.93.52.47
-A POSTROUTING -d 192.168.0.6/32 -p tcp -m tcp --dport 53389 -j SNAT --to-source 94.93.52.47
```



```
-A POSTROUTING -s 192.168.0.17/32 -p tcp -m tcp -m multiport --dports 11122 -j SNAT --to-source 94.93.52.47
```

```
-A POSTROUTING -s 192.168.0.17/32 -p tcp -m tcp -m multiport --dports 11121 -j SNAT --to-source 94.93.52.47
```

```
-A POSTROUTING -s 192.168.0.17/32 -p tcp -m tcp -m multiport --dports 10057 -j SNAT --to-source 94.93.52.47
```

```
-A POSTROUTING -s 192.168.0.17/32 -p tcp -m tcp -m multiport --dports 443 -j SNAT --to-source 94.93.52.47
```

```
-A POSTROUTING -s 192.168.0.17/32 -p tcp -m tcp -m multiport --dports 998 -j SNAT --to-source 94.93.52.47
```

```
COMMIT
```

```
# Completed on Thu Oct 25 19:26:51 2018
```

```
# Generated by iptables-save v1.4.7 on Thu Oct 25 19:26:51 2018
```

```
*filter
```

```
:INPUT DROP [5902:468560]
```

```
:FORWARD DROP [0:0]
```

```
:OUTPUT ACCEPT [872947:904499689]
```

```
:f2b-SSH - [0:0]
```

```
-A INPUT -p tcp -m tcp --dport 22 -j f2b-SSH
```

```
-A INPUT -i lo -j ACCEPT
```

```
-A INPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 3128 -j ACCEPT
```

```
-A INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
```

```
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 48374 -j ACCEPT
```

```
#ssh
```

```
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 53 -j ACCEPT
```

```
#dns
```

```
-A INPUT -p udp -m multiport --dports 135,136,137,138,139,445,631,1433,1434,5938 -j
```

```
DROP
```

```
-A INPUT -p tcp -m multiport --dports 135,136,137,138,139,445,631,1433,1434,5938 -j DROP
```

```
-A INPUT -p udp -m multiport --dports 135,136,137,138,139,445,631,1433,1434,5938 -j
```

```
DROP
```

```
-A INPUT -p tcp -m multiport --dports 135,136,137,138,139,445,631,1433,1434,5938 -j DROP
```

```
-A INPUT -d 192.168.0.0/24 -p tcp -m tcp -j ACCEPT
```

```
-A INPUT -s 192.168.0.0/24 -p udp -m state --state NEW -m udp --dport 53 -j ACCEPT
#dns
-A INPUT -s 91.121.109.209/32 -j DROP
-A INPUT -s 217.12.202.40/32 -j DROP
-A INPUT -s 94.242.222.68/32 -j DROP
-A INPUT -s 82.118.242.124/32 -j DROP
-A INPUT -s 46.151.209.33/32 -j DROP
-A INPUT -s 217.79.179.14/32 -j DROP
-A INPUT -s 91.214.203.144/32 -j DROP
-A INPUT -s 95.211.198.231/32 -j DROP
-A INPUT -s 195.154.180.60/32 -j DROP
-A INPUT -s 5.149.250.54/32 -j DROP
-A INPUT -s 91.200.13.76/32 -j DROP
-A INPUT -s 94.185.80.82/32 -j DROP
-A INPUT -s 62.210.180.229/32 -j DROP
-A INPUT -s 91.200.13.76/32 -j DROP
-A INPUT -s 23.111.177.114/32 -j DROP
-A FORWARD -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -s 192.168.0.0/24 -j ACCEPT
-A FORWARD -d 192.168.0.0/24 -j ACCEPT
-A FORWARD -d 192.168.0.4/32 -p tcp -m tcp --dport 8000 -j ACCEPT
-A FORWARD -d 192.168.0.4/32 -p tcp -m tcp --dport 554 -j ACCEPT
-A FORWARD -d 192.168.0.6/32 -p tcp -m tcp --dport 3389 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 20 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 21 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 80 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A f2b-SSH -j RETURN
COMMIT
# Completed on Thu Oct 25 19:26:51 2018
```

