Хмельницький національний університет
Факультет програмування
та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система авторизації користувачів на основі серверу LDAP
Назва теми

КвРКІ.170260.17.02.02 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія»*
Назва

Виконав: студент IV курсу, група КІ–17–2 _____ В. В. Блаута
Підпис Ініціали, прізвище

Керівник _____ Ю.П. Кльоц
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ І.В. Муляр
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки та
комп'ютерних систем і мереж _____ Ю.П. Кльоц
Підпис Ініціали, прізвище

«____» _червня_ 2021 р.

Хмельницький 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ПРОГРАМУВАННЯ ТА КОМП'ЮТЕРНИХ І ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Кафедра КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЯ ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ

Завідувач кафедри __Ю.П.Кльоц___

_____

" 05 " 02 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Блаута Вадим Віталійович

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Система авторизації користувачів на основі серверу LDAP

Керівник проекту (роботи) Кльоц Юрій Павлович

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

кандидат технічних наук, доцент

Затверджена наказом ректора університету від 05.02.2021 № 11 додаток №7

2. Строк подання студентом проекту (роботи) на кафедру 28.05.2021

3. Вихідні дані до проекту (роботи) мережа Хмельницького національного університету

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Дослідження предметної області та постановка задачі; обгрунтування базових положень щодо проєктування систем авторизації користувачів; Опис архітектури системи авторизації з використанням серверу LDAP; опис алгоритму роботи системи

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Схема авторизації користувачів (Е8)

Схема організації даних серверу LDAP (Е8)

Алгоритм авторизації роботи (Е8)

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Муляр І.В., доцент кафедри КбКСМ	-	
Антиплагіат	Муляр І.В., доцент кафедри КбКСМ	-	

7. Дата видачі завдання «_08_»_____02_____2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1.	Підготовка вступного розділу	Березень - 1 декада	
2.	Огляд існуючих методів, засобів	Березень - 2 декада	
3.	Обґрунтування обраних рішень	Березень - 3 декада	
4.	Підготовка опису системи авторизації	Квітень - 1 декада	
5.	Виконання розрахункової частини	Квітень - 1 декада	
6.	Підготовка ескізів креслень	Квітень - 2 декада	
7.	Формулювання висновків	Квітень - 3 декада	
8.	Розробка додатків	Травень - 1 декада	
9.	Погодження розділів з консультантом з нормоконтролю	Травень - 1 декада	
10.	Оформлення графічного матеріалу	Травень - 2 декада	
11.	Оформлення пояснювальної записки	Травень - 2 декада	
12.	Попередній захист кваліфікаційної роботи	Травень - 3 декада	
13.	Доопрацювання кваліфікаційної роботи	Травень - 3 декада	
14.	Подання роботи для перевірки на плагіат	Травень - 3 декада	
15.	Захист кваліфікаційної роботи	Червень - 1 декада	

Студент _____ ___ Блаута В.В._____
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ _____Ю.П. Кльоц____
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «*Система авторизації користувачів на основі серверу LDAP*».

Автор роботи: *Блаута Вадим Віталійович*.

Керівник роботи: *Кльоц Юрій Павлович*.

Пояснювальна записка: *69 с., 12 рис., 5 табл., 2 дод., 19 джерел*.

Графічна частина: *15 презентаційних слайдів*.

Авторизація користувачів, сервер LDAP, розмежування доступу.

Метою роботи є розробка системи авторизації користувачів на основі сервера LDAP.

У цій роботі розроблено алгоритм авторизації користувачів, проведено налаштування LDAP серверу, налаштовані квоти файлового серверу. Розроблена система авторизації реалізована на сервері Ubuntu 20.04. Дозволяє здійснювати облік кількості авторизованих користувачів, проводити авторизацію одночасно в декількох інформаційних системах.

Підпис студента  Дата

ЗМІСТ

ВСТУП

Аутентифікація – це процес підтвердження передбачуваної ідентифікації запитувача послуг; в той час як використовується кілька методів автентифікації, аутентифікація найчастіше виконується за допомогою простої перевірки пароля.

Авторизація, процес, що виконується після автентифікації, визначає рівень доступу або привілеї, що надається авторизованому запитувачу. Авторизація відповідає на два запитання. Чи має цей запитувач доступ до певного системного ресурсу (наприклад, до файлу чи конфігураційного об'єкта)? Якщо так, то який доступ (наприклад, створити, знищити або змінити)? Хоча існує декілька методів авторизації, авторизація зазвичай здійснюється шляхом присвоєння автентифікованого запитувача одному з низки заздалегідь визначених класів авторизації. Концептуально кожен клас перелічує доступні об'єкти разом із асоційованим типом доступу до об'єкта (часто виражається як лише для читання, лише для запису або читання та запису).

Актуальність роботи полягає у розроблені комп’ютерної мережі для закладу вищої освіти Хмельницького національного університету на базі стандартів 1000Base-T, 1000Base-FX, 100Base-T, 1000Base-FX, що надасть можливість організувати роботу кожного унікального персонального комп’ютера на більш високому рівні та без затримок та збоїв.

Метою роботи є розроблення комп’ютерної мережі з розширеним функціоналом та удосконалення надання якісних послуг.

Поставлена у кваліфікаційній роботі мета досягається рішенням таких задач:

1) вибір мережевої архітектури для комп'ютерної мережі, метод доступу, топології, типу кабельної системи;
2) вибір способу управління мережею;

3) конфігурація мережевого обладнання - кількість серверів, концентраторів, мережевих принтерів;
4) управління мережевими ресурсами та користувачами мережі;
5) вивчення питань безпеки мережі;
6) розрахунок витрат на створення мережі підприємства.

Необхідно розробити раціональну, гнучку структурну схему мережі організації, передбачити режими швидкого оновлення оперативної інформації на сервері, а так само опрацювати питання забезпечення необхідного рівня захисту даних.

1 Системи авторизації

1.1 Локальна авторизація

Аутентифікація - процес, який система використовує для того, щоб визначити, що вам слід надати доступ під час введення вашого імені користувача та пароля. Він відбувається в двох основних варіантах:

Локальна автентифікація – обмежена одним комп’ютером. Комп’ютер ідентифікує копистувача, але жоден інший комп’ютер не може використати ці результати. Налаштувати та адмініструвати таку систему на кількох комп’ютерах легко, але масштабується вкрай погано.

Централізована автентифікація – дозволяє збирати інформацію користувача та інші налаштування в одному сховищі, а потім отримувати доступ до них із довіренних комп’ютерів. Централізовані системи можуть бути набагато складнішими в налаштуванні, але значно полегшують адміністрування великих мереж комп’ютерів.

Локальна автентифікація користувачів – це простий легкий набір користувачів, який не повинен бути корпоративним постачальником аутентифікації. Вона не призначена бути високопродуктивним постачальником аутентифікації для підтримки групових політик, закінчення терміну дії пароля тощо. Це дозволяє створювати спеціальні набори користувачів, які можна використовувати для різних цілей. Наприклад, у середовищах із кількома орендарями його можна використовувати для налаштування прав адміністратора для різних орендарів, використовуючи різні облікові записи користувачів, що належать до відповідних сфер.

Типові випадки використання для автентифікації локального управління користувачами:

- при використанні локальних користувачів для програм, що потребують декількох облікових записів користувачів;
- коли постачальники корпоративних ідентифікаторів недоступні;
- для тестування.

Внутрішні користувачі – це облікові записи користувачів, які існують лише на одному комп'ютері та не залежать від домену, мережі чи операційної системи. Внутрішніми користувачами керують всередині комп'ютера, що означає, що вам не потрібно створювати або керувати ними у зовнішньому каталозі користувачів.

Існує кілька способів використання цієї функції:

- можна надати вибраним працівникам можливість створювати внутрішні облікові записи користувачів. Це надає співробітникам контроль над тим, хто може отримати новий обліковий запис, запобігаючи створенню небажаних облікових записів (наприклад, із образливими іменами користувачів).
- можна надати користувачам можливість створювати власні внутрішні облікові записи через веб-форму реєстрації. Це корисно для того, щоб надати гостям можливість зареєструвати власні рахунки та негайно розпочати друк, усуваючи необхідність втручання персоналу.
- Адміністратори можуть створити нову групу внутрішніх користувачів за допомогою імпорту текстових файлів. Можна використовувати цей файл для імпортування або оновлення набору користувачів, якими керують окремо, до звичайних користувачів домену.

1.1.1 Локальна авторизація користувачів Linux

Вбудовані модулі автентифікації (Pluggable Authentication Modules – PAM) існують з 1997 року. PAM походить від Sun Solaris, і, схоже, перше використання та популяризація відбулисяя саме там. Однак, згідно зі статтею 1997 року, першою повною реалізацією було розгортання Linux-PAM. Стаття все ще доступна в Linux Journal. Основна передумова та реалізація з тих пір не змінилися. Є кілька нових ключових слів і багато нових модулів, але загалом процес такий самий, як і 20 років тому.

Як вказує A у PAM, стосується автентифікації. У більшості випадків, коли користувач входить в систему через консоль або через всю мережу за допомогою SSH або Cockpit, задіяний PAM. Не має значення, зберігаються облікові записи користувачів локально або в централізованому місці. Скільки використовується,

як правило, безпосередньо маніпулювати файлами конфігурації PAM. Інші утиліти роблять це за користувача. Багато змін вносяться під час встановлення, наприклад, під час встановлення RPM sssd або за допомогою утиліти ipa-client-install. Найпоширеніші додаткові конфігурації можуть оброблятися authconfig (RHEL7 і старіші) або authselect (RHEL8), або навіть через веб-інтерфейс Cockpit. Більшість адміністраторів не дізнаються про файли конфігурації PAM, доки вони не беруть участь у розширених темах автентифікації та безпеки.

Що забезпечує PAM? PAM відокремлює стандартні та спеціалізовані завдання автентифікації від програм. Такі програми, як логін, gdm, sshd, ftpd та багато інших, хочуть знати, що користувач є тим, ким представляється, проте існує безліч способів зробити це. Користувач може надати ім'я користувача та пароль, які можна зберігати локально або віддалено за допомогою LDAP або Kerberos. Користувач також може надати відбиток пальця або сертифікат як облікові дані. Було б складно просити кожного розробника програми писати перевірки автентичності для кожного нового методу. Виклик бібліотек PAM залишає перевірки для експертів з автентифікації. PAM можна підключити, оскільки програми можуть мати різні додатки для запуску різних тестів і модулів, завдяки чому можна додавати нові методи до нових бібліотек.

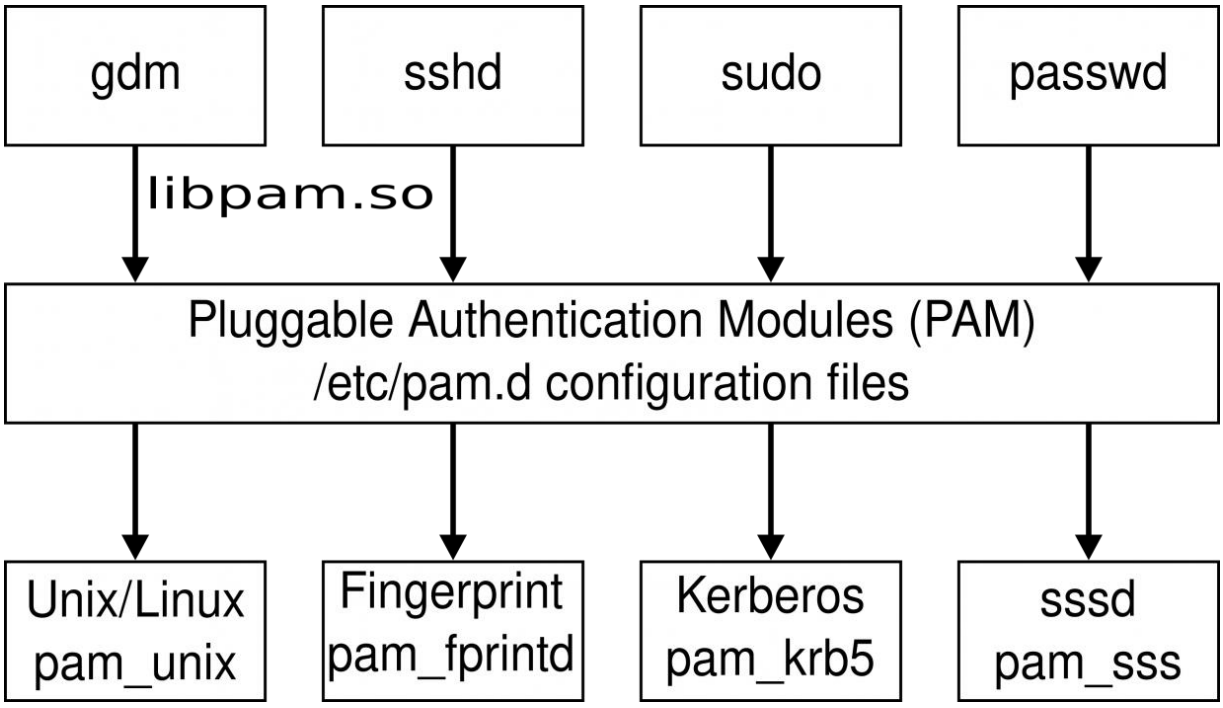

Рис. 1.1 Схема викликів модулів PAM.

Укрупнені етапи локальної авторизації користувача при вході в текстову консоль:

1. Програма для входу запитує ім’я користувача та пароль, а потім робить виклик автентифікації libpam, щоб запитати: "Це той користувач, яким він представився?" Модуль pam_unix відповідає за перевірку автентичності локального облікового запису. Інші модулі також можуть бути перевірені, і в кінцевому підсумку результат передається назад в процес входу.
2. Потім процес входу запитує: "Чи дозволено цьому користувачеві підключатися?", А потім робить виклик до акаунта libpam. Модуль pam_unix перевіряє наявність таких речей, як термін дії пароля. Інші модулі можуть перевіряти списки контролю доступу на основі хосту або часу. Загальна відповідь повертається до процесу.
3. Якщо термін дії пароля закінчився, програма реагує відповідним чином. Деякі програми просто не можуть увійти в систему користувача. Процес входу пропонує користувачеві оновити пароль.
4. Щоб перевірити та записати пароль у правильному місці, процес входу здійснює виклик пароля до libpam. Модуль pam_unix записує в локальний тіньовий файл. Для перевірки надійності пароля також можуть бути викликані інші модулі.
5. Якщо на цьому етапі процес входу триває, він готовий до створення сеансу. Виклик сеансу до libpam призводить до того, що модуль pam_unix пише мітку часу входу у файл wtmp. Інші модулі включають аутентифікацію X11 або контексти користувачів SELinux.
6. При виході з системи, коли сеанс закритий, до libpam можна зробити ще один виклик сеансу. Це коли модуль pam_unix записує позначку часу виходу у файл wtmp.

PAM передбачає використання багатьох компонентів. Якщо адміністратор вносить зміни до автентифікації за допомогою такої програми, як authconfig або authselect, і хоче перевірити змінені налаштування то необхідно перевряти наступні локації:

/ usr / lib64 / security

Колекція бібліотек PAM, які виконують різні перевірки. Більшість із цих модулів мають сторінки, де можна пояснити варіант використання та доступні варіанти.

/ etc / security

Колекція додаткових файлів конфігурації для певних модулів. Деякі модулі, такі як pam_access та pam_time, надають додаткову деталізацію для перевірок. Коли файл конфігурації програми викликає ці модулі, перевірки завершуються, використовуючи додаткову інформацію з відповідних додаткових файлів конфігурації. Інші модулі, такі як pam_pwquality, полегшують іншим утилітам модифікацію конфігурації, розміщуючи всі параметри в окремому файлі, а не в рядку модуля у файлі конфігурації програми.

/ var / log / secure

Більшість помилок безпеки та автентифікації заносяться в цей файл журналу. У ньому налаштовано дозволи для обмеження доступу.

man pam

Ця сторінка опису загального процесу, включаючи типи викликів та список задіяних файлів.

man pam.conf

Ця сторінка опису загального формату та визначає ключові слова та поля для файлів конфігурації pam.d.

man -k pam_

Цей пошук сторінок керівництва відображає сторінки, доступні для встановлених модулів.

PAM забезпечує набагато більш надійне середовище автентифікації, ніж послуги, що надаються для кожного додатка. Він працює в Linux багато років і бере участь у майже всіх процесах ідентифікації користувачів.

1.1.2 Конфігураційний файл LINUX PAM.

Перше поле у цьому файлі визначає Тип викликів, що можуть здійснюватись до PAM. Рядки одного типу згруповані між собою. Існує чотири типи: автентифікація, обліковий запис, пароль та сеанс.

Друге поле – ReturnCode. Це поле дозволяє PAM знати, як обробляти результати тестування модуля. Коди повернення вказують, чи є тест обов'язковим чи необов'язковим. Коди можуть також використовуватися для вказівки, що рядок – це не модульний тест із опціями, а назва іншого конфігураційного файлу з додатковими перевірками.

Решта рядка містить ім'я модуля та параметри цього модуля. Ім'я модуля повинно відповідати модулю, доступному в каталозі / etc / lib64 / security. Параметри можуть бути різними залежно від типу виклику. Деякі модулі проводять тести лише для деяких типів викликів.

Порядок записів у межах типу виклику має значення. Це здебільшого пов’язано з тим, як обробляються коди повернення, а в деяких випадках через дію модуля. Коли libpam отримує повідомлення "готово" або "завершено", він повідомляє загальний результат назад до батьківвського процесу.

Конфігурація sudo включає декілька рядків. Ці рядки вказують libpam включати всі рядки заданого типу із вказаного конфігураційного файлу. Існує також опція substack, яка дозволяє виконати різні виклики в залежності від успішності виконання поточного виклику.

Коди повернення у основному файлі конфігурації. Вказаний раніше файл /etc/pam.d/sudo досить короткий. Три із чотирьох типів викликів мають лише включення іншого файлу. Файл /etc/pam.d/system-auth є більш типовим для конфігураційного файлу, з великою кількістю перевірок для кожного типу виклику.

Ключове слово required – найпоширеніше. Це вказує на те, що модуль повинен пройти перевірку на загальний прохід, результат якої потрібно повернути додатку. Однак навіть у разі відмови наступні рядки цього типу все одно перевірятимуться.

Ключове слово requisite схоже на required, оскільки перевірка повинна пройти, але у випадку помилки воно повертає повідомлення "die". Required повідомляє libpam, що наступні рядки не перевірятимуться, а також повідомляє процес виклику загальних результатів - у цьому випадку помилка.

Ключове слово sufficient майже протилежне requisite. У разі успіху повертається повідомлення "готово", а libpam продовжує і надсилає загальні результати назад до програми, що викликає. Інші результати цього модуля ігноруються, і перевірка продовжується.

Ключове слово sufficient передбачає декілька способів перевірки критерію. Наприклад, під час перевірки пароля користувач може бути визначений у локальних файлах / etc / passwd та / etc / shadow, або вони можуть бути визначені лише в центральній системі, до якої доступний sssd. Модуль pam_unix перевіряє локальні файли. Якщо успіх є, немає необхідності продовжувати перевірку централізованих служб.

Ключове слово optional подібне до остатнього тим, що воно ігнорує будь-які помилки. Однак у випадку успіху воно діє більше як необхідне ключове слово, встановлюючи значення "готово" і продовжуючи виконувати будь-які додаткові перевірки.

Оскільки як необхідними, так і достатніми можуть бути точки виходу з стеку модулів, порядок у файлі конфігурації є важливим. Рядки після цих ключових слів можуть бути виконані або не виконані.

Однією з утиліт налаштування PAM є authconfig. Цей інструмент використовується з Red Hat Enterprise Linux, до RHEL7 включно.

Інструмент authconfig був створений для допомоги у конфігурації клієнта для централізованої автентифікації. Файли PAM – це лише частина цієї конфігурації. Наприклад, використання authconfig для ввімкнення автентифікації Kerberos вносить зміни до файлу /etc/nsswitch.conf та /etc/krb5.conf на додаток до додавання модуля pam_krb5 до /etc/pam.d/{system,password} -auth файли.

Як і багато інших утиліт для конфігурації системи, автентифікацію можна налаштувати за допомогою інструменту графічного інтерфейсу користувача

(GUI), за допомогою інтерактивного текстового інтерфейсу (TUI) або в командному рядку.

Графічний інструмент надається пакетом authconfig-gtk. Ця утиліта має кілька вкладок для налаштування параметрів Рис. 1.1.

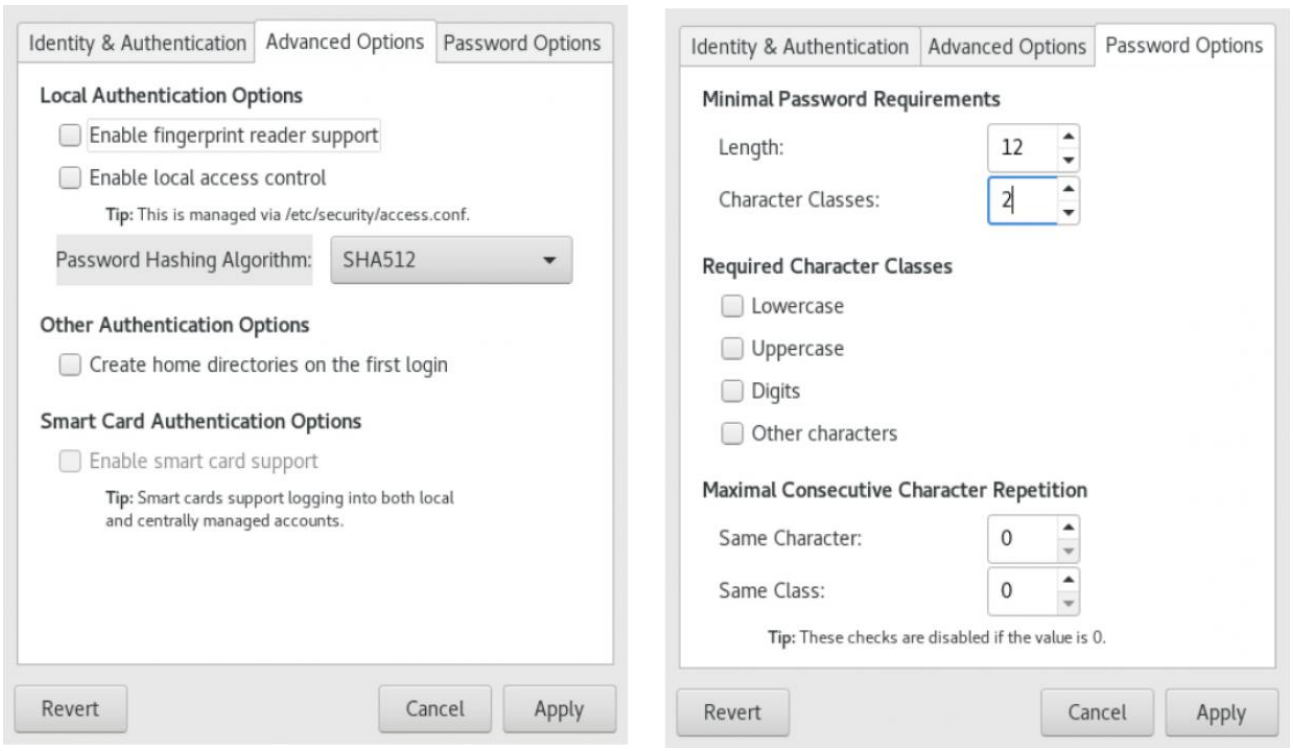

Рис. 1.1 Вікна authconfig

Інтерактивна текстова версія ("TUI") доступна за допомогою команди authconfig-tui. Клавіша TAB дозволяє переміщення між полями, а пробіл для вибору або скасування вибору Рис. 1.2.

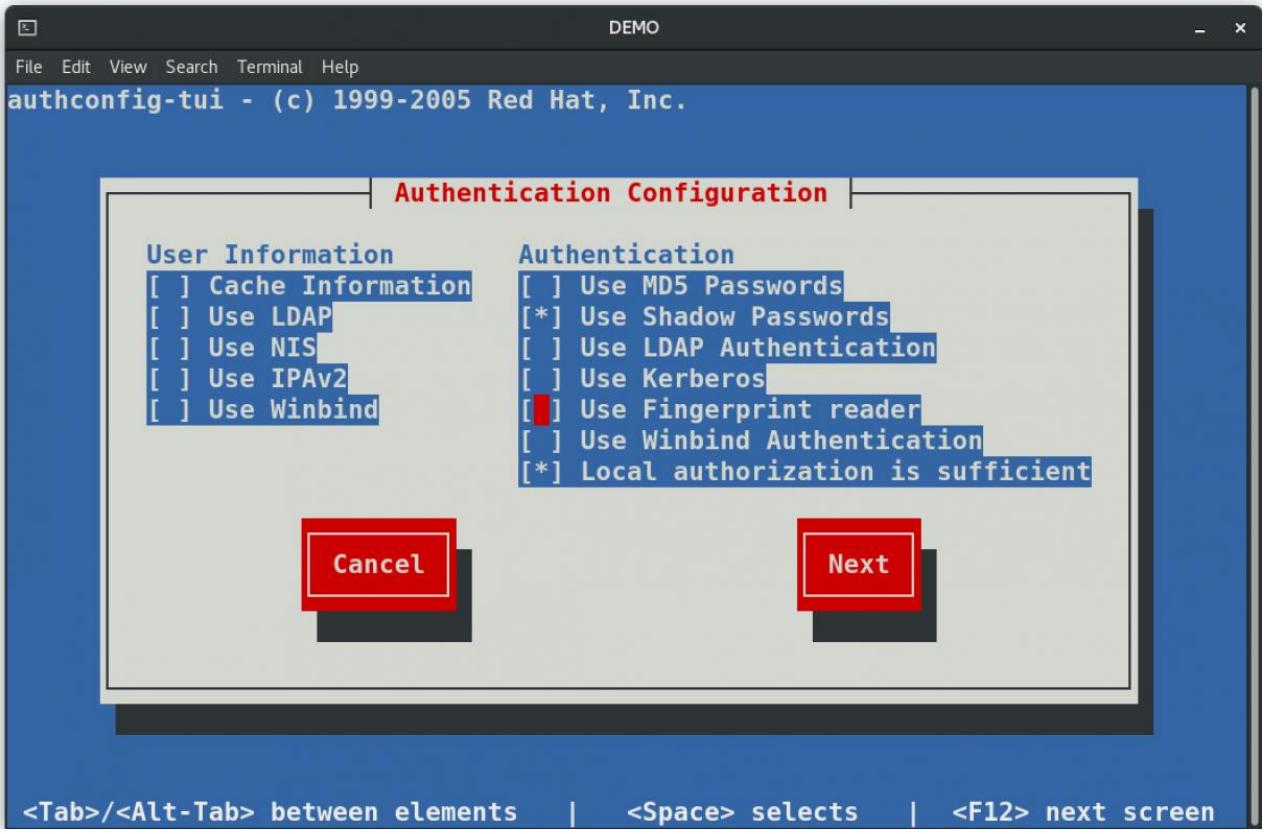

Рис. 1.2 Текстовий режим роботи authconfig

Скрипт-інструмент командного рядка authconfig має безліч опцій, які описані з параметром --help або на сторінці довідки.

Графічна та текстова версії є інтерактивними, але мають обмежені можливості. Наприклад, можна ввімкнути автентифікацію за допомогою зчитувача відбитків пальців у всіх трьох інтерфейсах, але лише інструмент командного рядка має можливість налаштувати модуль pam_faillock. Зміни надійності пароля за допомогою модуля pam_pwquality вносяться за допомогою графічного інструменту та інструменту командного рядка, але не інтерактивного текстового інтерфейсу.

1.1.2 Налаштування користувачів Linux

Однією з поширених практик безпеки на будь-яких машинах Linux є уникання використання root облікового запису для повсякденних операцій. На

щойно розгорнутому сервері, звичайно, єдиним обліковим записом є root, відповідно необхідно створити нового користувача.

```
adduser <username>
```

Рис. 1.1 Додавання нового користувача

Процедура створення користувача передбачає встановлення паролю та іншої інформації. У Linux потрібно буде вручну розблокувати новий обліковий запис, встановивши пароль наступною командою.

```
passwd <username>
```

Рис. 1.2 Встановлення паролю

Для використання облікового запису для управління системою, необхідно надати права на виконання sudo. На серверах Linux це можна зробити за допомогою команди нижче.

```
adduser <username> sudo
```

Рис. 1.3 Додавання нового адміністратора

В деякий версіях Linux система контролю доступу sudo може не встановлюватися за замовчуванням. Якщо вона відсутня, її необхідно встановити.

```
apt-get install sudo
```

Рис. 1.4 Встановлення системи контролю доступу

З дозволами sudo можна виконувати ті самі операції, що і root обліковий запис, але без шкоди для безпеки. Якщо на сервері буде декілька root користувачів, набагато безпечніше надавати їм привілеї sudo, замість того, щоб ділитися паролем root з усіма. Використання sudo над кореневим обліковим записом загалом вважається гарною практикою.

Після створення власного облікового запису, необхідно вимкнути віддалений вхід SSH для root. Налаштування сервера OpenSSH визначені у файлі конфігурації, його можна редагувати наступною командою.

```
sudo nano /etc/ssh/sshd_config
```

Рис. 1.6 Відключення доступу по SSH для root-користувача

Необхідно знайти варіанти автентифікації та змінити дозвіл на кореневий вхід, встановивши для нього значення, як нижче.

```
PermitRootLogin no
```

Рис. 1.6 Відключення доступу для root-користувача

Для внесення змін до конфігураційного файлу SSH необхідно перезапустити службу, використавши наступну команду.

```
sudo systemctl restart sshd
```

Рис. 1.6 перезапуск демона SSH

Якщо на Linux сервері багато віддалених користувачів, необхідно впроваджувати розумні правила щодо паролів за допомогою модуля Linux PAM під назвою pam_cracklib.so. Модуль перевіряє паролі користувачів в словнику, щоб запобігти слабкому використанню пароля. Також можна використовувати його для встановлення мінімальних вимог до нового пароля, таких як довжина та складність.

```
sudo apt-get install libpam-cracklib
```

Рис. 1.6 Додавання модуля перевірки паролів

Встановлення модуля на Linux вже попередньо налаштовує перевірку пароля, тому необхідно знайти відповідне налаштування та відредагувати його, як це показано на прикладі нижче.

```
password required pam_cracklib.so retry=3 minlen=8 difok=3 dcredit=1 ucredit=1
```

Рис. 1.6 Налаштування вимог до паролю

Перший параметр retry визначає, скільки разів користувач отримує повторну спробу. Наступний minlen позначає мінімальну довжину пароля, тоді як difok перевіряє максимальну кількість повторно використаних символів порівняно зі старим паролем користувача. Останні 3 параметри встановлюють вимоги до складності пароля, dcredit - це кількість цифр, ucredit для великих символів і lcredit кількість символів в нижньому регістрі.

Після встановлення вимог до пароля згідно політики, необхідно зберегти файл конфігурації та вийти з редактора. Ці правила стосуються лише звичайних облікових записів користувачів, адміністратор сам відповідаєте за надійність пароля кореневого користувача.

Сервер OpenSSH може обмежувати підключення користувачів шляхом перехресної перевірки належності їх до дозволеної групи. Це може бути корисно, якщо у вас є декілька користувачів, з яких деяким не потрібно буде віддалятись за допомогою SSH, або ви просто хочете отримати додатковий захист, наприклад, під час запуску веб-служби або бази даних з окремими користувачами.

Для створеннння групи користувачів необхідно використати наступну команду.

```
sudo groupadd sshusers
```

Рис. 1.6 Створення групи користувачів

Додавання користувача до нової групи.

```
sudo gpasswd -a <username> sshusers
```

Рис. 1.6 Додавання користувача до нової групи

Перевірка груп, до яких входить користувач.

```
groups <username>
```

Рис. 1.6 Перевірка груп, до яких входить користувач

Результат покаже усі групи, до яких належить дане ім'я користувача, включаючи групу користувачів з тим самим іменем, що і користувач.

```
user : user sudo sshusers
```

Рис. 1.6 Приналежність користувача до груп

Після цього можна вказати дозволену групу для OpenSSH. Для цього необхідно відкрити файл конфігурації в редакторі.

```
sudo nano /etc/ssh/sshd_config
```

Рис. 1.6 Редагування файлу конфігурації

В кінці файлу необхідно додати команду.

```
AllowGroups sshusers
```

Рис. 1.6 Дозвіл групи на доступ по SSH

Після зміни налаштувань необхідно перезапустити демон SSH використавши команду.

```
sudo service ssh restart
```

Рис. 1.6 Перезапуск SSH

З новою конфігурацією будь-якому користувачеві, який не належить до дозволеної групи, буде відмовлено у доступі через SSH, навіть якщо його пароль було введено правильно. Це значно зменшить шанс примусового введення пароля користувача або вгадування зі списками словників, що дає більш безпечний сервер.

1.1.3 Локальна авторизація користувачів Windows

Віві

Ві

Ві

Ві

ві

1.2 Централізована авторизація користувачів

віавіаві

1.2.1 Авторизації користувачів Linux

Кук

Ук

Ук

1.2.2 Авторизації користувачів Windows

Під локальною мережею (ЛОМ, LAN) зазвичай мають на увазі об'єднання комп'ютерів, розташованих в обмеженому просторі.

Існує велика кількість технологій: Ethernet, FDDI, Token Ring, ARCNet, ATM, UltraNet і інші.

2 Авторизація користувачів на основі серверу LDAP

2.1 Початкове налаштування LDAP

2.2 Додавання користувачів

2.3 Резервні сервери

Кожна організація формулює власні вимоги до конфігурації мережі, зумовлені характером вирішуваних завдань. В першу чергу необхідно визначити, скільки чоловік будуть працювати в мережі. Від цього рішення, по суті, будуть залежати всі наступні етапи створення мережі.

3 Взаємодія LDAP з інформаційними системами

3.1. Аналіз вимог до проектованої локальної мережі

Кожна організація формулює власні вимоги до конфігурації мережі, зумовлені характером вирішуваних завдань. В першу чергу необхідно визначити, скільки чоловік будуть працювати в мережі. Від цього рішення, по суті, будуть залежати всі наступні етапи створення мережі.

Кількість робочих станцій безпосередньо залежить від передбачуваного числа співробітників. Іншим фактором є ієрархія компанії. Для фірми з горизонтальною структурою, де всі співробітники повинні мати доступ до даних один одного, оптимальним рішенням є проста однорангова мережа. Фірмі, побудованої за принципом вертикальної структури, в якій точно відомо, який співробітник і до якої інформації повинен мати доступ, слід орієнтуватися на більш дорогий варіант мережі - з виділеним сервером. Тільки в такій мережі існує можливість адміністрування прав доступу. У додатку В представлений вибір типу мережі.

В даному випадку в університеті потрібно об'єднати в локальну мережу багато локальних станцій. Причому вони об'єднані в наступні групи:

1) відділи та підрозділи;
2) бугалтерія;
3) адміністрація;
4) навчльні аудиторії;
5) адміністративний відділ;
6) відділ охорони:
7) факультети.

Слідуючи зі схеми вибору типу мережі, можна вирішити, що в даному випадку потрібна установка двох серверів - це сервер BKS і сервер SET для роботи з торговим обладнанням. Одним з головних етапів планування є створення попередньої схеми. При цьому в залежності від типу мережі виникає питання про обмеження довжини кабельного сегмента. Це може бути несуттєво для невеликого офісу, однак якщо мережа охоплює кілька поверхів будівлі, проблема

постає в зовсім іншому світлі. У такому випадку необхідна установка додаткових репітерів (repeater).

У ситуації з ХНУ вся мережа буде розташовуватися на різних поверхах різних корпусів, і відстань між сегментами мережі достатньо велика, тому необхідне використання репітерів.

Так само не маловажним вимогам, які ставляться до локальної мережі, є виконання мережею її основної функції - забезпечення користувачам потенційної можливості доступу до ресурсів всіх комп'ютерів, об'єднаних в мережу. Всі інші вимоги - продуктивність, надійність, сумісність, керованість і масшабіруемость - пов'язані з якістю виконання цієї основної задачі.

Продуктивність - це властивість забезпечується можливістю розпаралелювання робіт між декількома комп'ютерами мережі. Існують наступні основні характеристики продуктивності мережі - час реакції, пропускна здатність і затримка передачі і варіація затримки передачі. Час реакції мережі є інтегральною характеристикою продуктивності з точки зору користувача. У загальному випадку час реакції визначається як інтервал часу між виникненням запиту користувача до якої-небудь мережевої служби і отриманням відповіді на цей запит. Пропускна здатність відображає обсяг даних, переданих мережею чи її частиною за одиницю часу. Затримка передачі визначається як затримка між моментом надходження пакету на вхід якого-небудь мережевого пристрою або частини мережі і моментом появи його на виході цього пристрою.

Надійність локальної мережі визначається наступними показниками: Готовністю або коефіцієнтом готовності (availability), який означає частку часу, протягом якого система може бути використана. Ймовірністю доставки пакета вузлу призначення без спотворень (ймовірність втрати пакета, ймовірність спотворення окремого біта переданих даних, ставлення втрачених пакетів до доставленим) Здатністю системи захистити дані від несанкціонованого доступу (безпекою). Відмовостійкість (fault tolerance) - здатністю приховати від користувача відмову окремих елементів мережі.

Можливість розширення (extensibility) означає можливість порівняно легкого додавання окремих елементів мережі (користувачів, комп'ютерів, додатків

і служб), нарощуючи довжини сегментів мережі і заміни існуючої апаратури більш потужною.

Масштабованість (scalability) означає, що мережа дозволяє нарощувати кількість вузлів і протяжність зв'язків в дуже широких межах, при цьому продуктивність мережі не погіршується.

Прозорість (transparency) мережі досягається в тому випадку, коли мережа представляється користувачам не як безліч окремих комп'ютерів, зв'язаних між собою системою кабелів, а як єдина традиційна обчислювальна машина з системою поділу часу.

Підтримка різних видів трафіку. Мережа повинна забезпечити спільну передача традиційного комп'ютерного та мультимедійного трафіку (в тому числі відео та мови).

Керованість на увазі собою можливість централізовано контролювати стан основних елементів мережі, виявляти і вирішувати проблеми, що виникають при роботі мережі, виконувати аналіз продуктивності мережі і планувати її розвиток.

Сумісність або інтегрувальність означає, що мережа здатна включати в себе найрізноманітніше програмне й апаратне забезпечення, тобто в ній можуть співіснувати різні операційні системи, що підтримують різні стеки комунікаційних протоколів, і працювати апаратні засоби і додатки від різних виробників.

3.2 Обгрунтування вибору технології локальної мережі

Ethernet використовує метод передачі даних CSMACD-множинний доступ до середовища з контролем несучої і виявленням колізій. Fast Ethernet використовує розмір пакета 15160 байт. Крім того, Fast Ethernet накладає обмеження на відстань між підключаються пристроями - не більше 100 метрів. Для того щоб знизити перевантаження, мережі стандарту Fast Ethernet розбиваються на сегменти, які об'єднуються за допомогою мостів і маршрутизаторів. Сьогодні при побудові центральної магістралі, яка об'єднує сервери, використовують комутований Fast Ethernet. Fast Ethernet-комутатори

можна розглядати як високошвидкісні багато портові мости, які в змозі самостійно визначити, в якій із його портів адресований пакет. Комутатор переглядає заголовки пакетів і таким чином складає таблицю, що визначає, де знаходиться той чи інший абонент з такою фізичною адресою. Це дозволяє обмежити область розповсюдження пакету і понизити вірогідність переповнення, посилаючи його тільки в потрібний порт. Тільки широкомовні пакети розсилаються по всіх портах. Офіційний стандарт 803.u встановив три різних специфікації для фізичного рівня Fast Ethernet.

Офіційний стандарт 803.u встановив три різних специфікації для фізичного рівня Fast Ethernet:

1) 100Base-TX - для двохпарного кабелю на неекранованої кручений парі UTP категорії 5 або екранованої кручений парі STP Type1;

2) 100Base-T4 - для чотіріпарного кабелю на неекранованої кручений парі UTP категорії 3, 4 або 5;

3) 100Base-FX - для багатомодового оптоволоконного кабелю, використовуються два волокна

Стандарт 100BaseTX вимагає застосування двох пар UTP або STP. Одна пара служить для передачі, інша - для прийому. Цим вимогам відповідають два основних кабельних стандарту: EIA / TIA-568 UTP Категорії 5 і STP Типу 1 компанії IBM [15].

На рисунку 2.1 зображений інсталяційний кабель EIA / TIA-568 UTP категорії 5.

Рисунок 2.1 – Кабель в розрізі

Мережева архітектура – це процедура збігів топології, стандартів, методів доступу необхідних для створення працюючої мережі. Вибір топології здійснюється, в більшій мірі за допомогою планувань приміщень, де має знаходитись мережа. Так само дуже велику роль відіграють витрати на закупку та встановлення мережевого обладнання, що є дуже важливим питанням для університету, тому що вартість по обладнаню в різних топологіях категорично різний.

Топологія «Зірка» являє собою, найбільш довільну структуру, кожен комп'ютер, в тому ж рахунку і сервер, з'єднуються між собою окремим сегментом кабеля с центральним концентратором. Головним позитивним фактором цієї топології, є її стійкість до збоїв системи.

Найважливішою характеристикою обміну інформацією в локальних мережах є так звані методи доступу (access methods), що регламентують порядок, в якому робоча станція отримує доступ до мережевих ресурсів і може обмінюватися даними.

Для розробки мережі використаємо такі типи кабелю:

1000Base-FX - оптоволоконний кабель, Передача також здійснюється відповідно до стандарту передачі даних в волоконно-оптичному середовищі.

1000Base-T - цей стандарт визначає роботу Gigabit Ethernet при передачі даних на відстань до 100 м з використанням всіх чотирьох пар кабелю "неекранована мідна кручена пара п'ятої категорії".

100Base-FX - дві жили, волоконно-оптичного кабелю. Передача також здійснюється відповідно до стандарту передачі даних в волоконно-оптичному середовищі, якої розроблений ANSI. Використовує алгоритм кодування даних 4B / 5B і метод фізичного кодування NRZI.

100Base-T - Технологія Ethernet 100 Мбіт / с, вона ж «швидкий Ethernet» (Fast Ethernet). Має багато різновидів, при цьому позначення 100BASE-T найчастіше використовується як збірна назва. Як і в технології 10BASE-T, в роботі тільки зелена і помаранчева пари (прийом контакти 3, 6, передача контакти 1, 2), хоча поводились експерименти по використанню всіх 4 пар, які потім привели до створення гігабітного Ethernet (див. 1000BASE- T). Для реалізації програм 100-мегабітного Ethernet використовується кручена пара категорії 5 (без букви «е») або вище.

Широко використовувати оптоволоконний кабель в Ethernet почали порівняно недавно. Його застосування дозволило відразу ж значно збільшити допустиму довжину сегмента й істотно підвищити стійкість передачі. Важлива також і повна гальванічна розв'язка комп'ютерів мережі, яка досягається тут без жодної додаткової апаратури, просто в силу специфіки середовища передачі. Ще одна перевага оптоволоконних кабелів полягає в можливості плавного переходу на Fast Ethernet, оскільки пропускна спроможність оптоволокна дозволяє досягти не тільки 100 Мбіт / с, але і більш високих швидкостей передачі.

Передача інформації в цьому випадку йде по двох оптоволоконним кабелях, що передають сигнали в різні сторони (як і в 100BASE - T). Іноді використовуються двопровідні оптоволоконні кабелі, що містять два кабелі в загальній зовнішній оболонці, але частіше - два одиночних кабелю. Всупереч поширеній думці вартість оптоволоконного кабелю не занадто висока (вона

близька до вартості тонкого коаксіального кабелю). Правда, в цілому апаратура в даному випадку виявляється помітно дорожче, тому що вимагає використання дорогих оптоволоконних трансиверів.

Апаратура 100BASE -FX має схожість як з апаратурою 10BASE5 (тут теж застосовуються зовнішні трансивери, з'єднані з адаптером трансиверного кабелем, так і з апаратурою 100BASE -T, тут також застосовується топологія "пасивна зірка » і два різноспрямовані кабелю).

Оптоволоконний трансивер називається FOMAU (Волоконно -оптичні МАУ). Він виконує всі функції звичайного трансивера (МАУ), крім того, перетворює електричний сигнал в оптичний при передачі і назад при прийомі. FOMAU також формує і контролює сигнал цілісності лінії зв'язку, що передається в паузах між переданими пакетами. Цілісність лінії зв'язку, як і у випадку 100BASE -T, індиціюється світлодіодами «Посилання». Для приєднання трансивера до адаптера застосовується стандартний АШ - кабель, такий же, як і у випадку 1000BASE5, але довжина його не повинна перевищувати 25м.

Довжина оптоволоконних кабелів, що з'єднують трансивер і концентратор, може досягати 2 км без застосування яких би то не було ретрансляторів. Таким чином, можливе об'єднання в локальну мережу комп'ютерів, що знаходяться в різних будівлях, сильно рознесених територіально.

Спочатку оптоволоконний зв'язок застосовувалася переважно для зв'язку між репітерами. Тому перший стандарт FOIRL (Волоконно-оптичні Інтер-ретранслятора Лінк), розроблений на початку вісімдесятих, припускав якраз зв'язок між двома репітерами на відстань до 1000 метрів. Потім були розроблені оптоволоконні трансивери для підключення дорепітери окремих комп'ютерів і стандарт 1000BASE -F, що включає в себе три типи сегментів.

1000BASE -FL - замінив старий стандарт FOIRL. Він найбільш поширений в даний час. Він забезпечує зв'язок між двома комп'ютерами, між двома репітерами або між комп'ютером і репитером. Максимальна відстань - до 2000 м.

Стандартний оптоволоконний кабель 100BASE -FL повинен мати на обох кінцях оптоволоконні байонетні ST- роз'єми, (стандарт BFOC/2.5). Приєднання цього роз'єму до трансивера або концентратора не складніше, ніж BNC -роз'єму в

мережі 10BASE2. Використовуються також роз'єми типу SC, що приєднуються подібно RJ- 45 шляхом простого вставляння в гніздо. Роз'єми SC зазвичай жорстко з'єднані по два для двох кабелів. Існують також роз'єми типу MIC FDDI, подібно роз'ємів SC вставляються в гніздо. При купівлі обладнання треба стежити за відповідністю роз'ємів, встановлених на кабелі, і відповідь роз'ємів трансиверів або концентраторів.

Відповідно до стандарту, в 1000BASE -FL використовується мультимодових кабель і світло з довжиною хвилі 850 нм, хоча в перспективі не виключений перехід на одномодовий кабель. Сумарні оптичні втрати в сегменті (як у кабелі, так і в роз'ємі) не повинні перевищувати 12,5 дБ. При цьому втрати в кабелі складають близько 4-5 дБ на кілометр довжини кабелю, а втрати в роз'ємі - від 0,5 до 2,0 дБ (ця величина сильно залежить від якості установки роз'єму) . Тільки за таких величинах втрат можна гарантувати стійкий зв'язок на граничній довжині кабелю. На практиці краще не ризикувати і брати довжину кабелю відсотків на десять менше граничної.

Наступний тип кабелю, який було використано, 100Base-T4 - неекранована вита пара . Максимальна довжина кабельного сегмента - 100 метрів(стандарт і в цьому випадку рекомендує обмежуватися 90 м для 10-процентного запасу). Топологія - «зірка». Його технологія - специфікація фізичного рівня технології Fast Ethernet, що є високошвидкісним варіантом технології Ethernet. Забезпечує передачу даних зі швидкістю до 100 Мб / сек.

100Base- T4 - найпізніша реалізація Fast Ethernet, вона з'явилася пізніше специфікацій 100Base -TX і 100Base - FX. Як і інші специфікації Fast Ethernet вона описується стандартом IEEE 802.3u. У цій технології використовується кабель, що складається з чотирьох кручених пар третьої категорії. При цьому з чотирьох пар одна завжди спрямована до концентратора, одна від концентратора, а інші дві перемикаються в залежності від поточного напрямку передачі даних. Таким чином в кожен момент часу з чотирьох пар для передачі використовується три, а одна використовується для прослуховування несучої частоти з метою виявлення колізій.

Інтерфейс 100Base-T4 має один істотний недолік - принципову неможливість підтримки дуплексного режиму передачі. І якщо при будівництві невеликих мереж Fast Ethernet з використанням повторювачів, 100Base-TX не має переваг перед 100Base-T4 (існує колізійних домен, смуга пропускання якого не більше 100 Мбіт / с), то при будівництві мереж з використанням комутаторів недолік інтерфейсу 100Base-T4 стає очевидним і дуже серйозним. Тому даний інтерфейс не отримай настільки великого поширення, як 100Base-TX і 100Base-FX.

Як і у випадку 100BASE-TX, для підключення мережевого кабелю до адаптера (трансивер) і до концентратора використовуються 8-контактні роз'єми типу RJ-45. Але в даному випадку задіяні всі 8 контактів роз'єму.

Також згідно завдання задана мережа класу С. Адреси класу С – це найчастіше використовувані адреси, призначені для використання в малих мережах. Адреса даного класу починається з двійкової комбінації 110. Отже, найменше доступне число – 11000000 (десяткове 192), а найбільше – 1101111 (десяткове значення 223). Якщо адреса в першому октеті містить числа від 192 до 223, значить він на-лежить до класу С.

В даний час технологія, яка застосовує кабель на основі витої пари (100Base - T і 1000Base - T), є найбільш популярною. Такий кабель не викликає труднощів при прокладці.

Мережа на основі кручений пари, на відміну від тонкого і товстого коаксиала, будується по топології зірка. Щоб побудувати мережу по зіркоподібною топології, потрібна більша кількість кабелю (але ціна кручений пари не велика). Подібна схема має і неоціненне перевагу - високу відмовостійкість. Вихід з ладу однієї або декількох робочих станцій не призводить до відмови всієї системи. Правда якщо з ладу вийде хаб, його відмова торкнеться всіх підключені через нього пристрої.

Ще однією перевагою даного варіанту є простота розширення мережі, оскільки при використанні додаткових хабів (до чотирьох послідовно) з'являється можливість підключення великої кількості робочих станцій (до 1024). При застосуванні неекранованої кручений пари (UTP) довжина сегмента між

концентратором і робочою станцією не повинна перевищувати 10000 метрів, чого не спостерігається в підприємстві.

У 100BaseTX привабливо забезпечення повнодуплексного режиму при роботі з мережевими серверами, а також використання всього двох з чотирьох пар восьмижильного кабелю - дві інші пари залишаються вільними і можуть бути використані в подальшому для розширення можливостей мережі.

Недоліки це кабелю полягає в тому, що він дорожче інших восьмижильний кабелів, крім того, для роботи з ним потрібне використання пробійної, роз'ємів і комутаційних панелей, що задовольняють вимогам категорії 5. Потрібно додати, що для підтримки повнодуплексного режиму слід встановити повнодуплексні комутатори.

BaseT є розширенням стандарту 10BaseT з пропускною спроможністю від 10 М біт / с до 100 Мбіт / с. Стандарт 100BaseT включає в себе протокол обробки множинного доступу з пізнанням несучої і виявленням конфліктів CSMA / CD. У 100BaseT4 використовуються всі чотири пари восьмижильного кабелю: одна для передачі, інша для прийому, а що залишилися дві працюють як на передачу, так і на прийом. Таким чином, в 100BaseT4 і прийом, і передача даних можуть здійснюватися по трьох парах. Розкладаючи 100 Мбіт / с на три пари. 100BaseT4 зменшує частоту сигналу, тому для його передачі досить і менш високоякісного кабелю. Для реалізації мереж 100BaseT4 підійдуть кабелі UTP Категорій 3 і 5, так само як і UTP Категорії 5 і STP Типу 1.В 10BaseT відстань між концентратором і робочою станцією не повинна перевищувати 100 метрів. Оскільки сполучні пристрої (повторювачі) вносять додаткові затримки, реальна робоча відстань між вузлами може опинитися ще менше.

Недоліки ж полягають в тому, що для 100BaseT4 потрібні всі чотири пари і що повнодуплексний режим цим протоколом не поддержівается.Ethernet включає також стандарт для роботи з багатомодовим оптоволокном з 62.5-мікронним ядром і 125-мікронною оболонкою. Стандарт 100BaseFX орієнтований в основному на магістралі - на з'єднання повторювачів Fast Ethernet в межах однієї будівлі. Традиційні переваги оптичного кабелю властиві і стандарту 100BaseFX:

стійкість до електромагнітних шумів, поліпшений захист даних і великі відстані між мережевими пристроями [16].

Проаналізувавши уважно інформацію про різні технології, можна прийти до висновку, що мережа з вертикальною підсистемою можна організувати на основі технології Fast Ethernet, так як вона використовує поширений кабель UTP 5 - категорії, що дозволяє використовувати топологію ієрархічна зірка, що є актуальним для даного об'єкта дипломної роботи і має великий вибір комунікаційного обладнання.

3.3 Обгрунтування вибору топології і моделі локальної мережі

Вибір топології визначається, зокрема, плануванням приміщення, в якому розгортається дана мережа. Крім того, велике значення мають витрати на придбання та установку мережевого устаткування, що є важливим питанням для організації.

Велике значення, у виборі топології мережі, має план приміщень.

У даній дипломній роботі, об'єкт дослідження має 4 корпуси [Додаток Г]:

1) 1 корпус;
2) 2 корпус;
3) 3 корпус;
4) 4 корпус

Після визначення місця установки сервера можна відразу визначити, яка кількість кабелю буде потрібно.

У таблиці 2.2 показані основні характеристики мереж різної топології.Згідно завдання потрібно спроектувати локальну мережу із застосуванням таких типів кабелю, як 100Base-FX та 100Base-T.

Таблиця 2.2 - Основні характеристики мереж різної топології

Додавання абонентів	Без докладання зусиль	Активне	Без докладання зусиль

Захист від відмов	Незначна	Незначна	Висока
Розміри системи	Будь-які	Будь-які	Обмежена
Вартість підключення	Незначна	Незначна	Висока
Поведінка системи при високих навантаженнях	Добре	Задовільна	Погана
Характеристики	Топологія		
	«Зірка»	«Кільце»	«Шина»
Можливість роботи в реальному режимі	Дуже хороша	Хороша	Погана
Розведення кабелю	Хороша	Дуже хороша	Хороша
Обслуговування	Дуже добре	Середня	Середня

Топологія у вигляді «зірки» є найбільш надійною і швидкодіючої з усіх топологій обчислювальних мереж, оскільки передача даних між комп'ютерами проходить через сервер (при його гарній продуктивності) по окремих лініях, використовуваним тільки цими комп'ютерами. Частота запитів передачі інформації, від одного комп'ютера до іншого невисока, порівняно з частотою, що спостерігається при інших топологіях.

У Додатку Д зображена схема ХНУ. Дана схема переважає через недооцінену перевагу, це висока відмовостійкість. Тобто вихід з ладу однієї не впливає на роботоспроможність загальної системи. Та якщо з ладу вийде комутатор (Switch), то це понесе великі ризики, та вихід з ладу системи

3.4 Відбір апаратури для різних пристроїв для різних рівнів еталонної моделі взаємодії відкритих систем (OSI), операційних систем та характеристик

Задано 124 вузлів, 2 сервери, 5 концентраторів, 4 комутатора,. Усі вузли та обладнання розташовуються у чотирьох корпусах.

Якщо розділити структуру розробленої мережі на логічні групи, то їх вийде чотири.

Перша група складається з сервера, комутатора КМ1(4 корпус), персональних комп'ютерів ПК1 – ПК425. Усі елементи логічної групи з'єднуються за допомогою кабелю 100Base-T. Максимальна довжина кабелю - 1450 метрів. Також КМ1 під'єднується до комутатора та концентратора інших робочих груп. З'єднання між аудиторіями проводиться оптоволоконним кабелем 100Base-FX, тому що відстань становить більше ніж 100 метрів.

Друга робоча група складається із комутатора КМ2(3 корпус), комутатора та ПК426 – П480. З'єднання вузлів з КМ2 відбувається також за допомогою кабелю 100Base-T. Максимальна довжина між комутатором та найвіддаленішим елементом групи складає 400 метрів.

Наступна - третя логічна група (корпус 2)складається із концентратора КЦ1 і ПК. Ця логічна група вміщає ПК481 – ПК490 під'єднанні до концентратора кабелем 10Base-FL. Максимальна довжина кабелю між комутатором і найвіддаленішим вузлом - 120 метрів.

Четверта робоча група складається(1 корпус) з КМ3 та ПК490 – ПК620, а також роутера, який свою чергу виконує функцію брандмауера. Максимальна довжина кабелю у групі становить 700 метрів.

Для серверів та робочих комп'ютерів, згідно із завдання на курсовий проект, обрано операційні системи windows serwer 2008.

На персональних комп'ютерах встановлено прикладне програмне забезпечення, яке орієнтоване на роботу студентів та персоналу.

Отже, у даному розділі описується процес вибору та аналізу логічної структури мережі та її компонентів. Вибір апаратної частини відбувається відповідно до завдання, щоб задовольнити вимоги користувачів для роботи з базами данних і забезпечити комфортну та надійну роботу мережі.

Тому для робочих станцій ПК1 – ПК620 обрано компоненти з наступними характеристиками, їх наведено у таблиці 2.3. Вибір складових та цін проводиться із використанням прайс-листу фірми «Розетка» станом на 16.06.2021р.

Таблиця 3.3 - Перелік комплектуючих для робочих станцій

Пристрій	Марка і модель
Процесор	Intel Core i3- 3220 3.3GHz
Материнська плата	Asus H87-PRO
Відео карта	nVidia GeForce GT 630
Оперативна пам'ять	Kingston DDR3-1600 4096MB PC3-12800 HyperX
Вінчестер	Hitachi (HGST) Travelstar 5K1000 1TB 5400rpm 8MB HTS541010A9E680_0J22413 2.5 SATAIII
Монітор	18.5" LG 19M35A-B
Клавіатура	Speedlink Verdana Multimedia Keyboard
Мишка	Trust Vivy Wireless Mini Mouse Black Solid
Корпус	Thermaltake Urban S21 Black
Мережева карта	TP-LINK TG-3468
Блок живлення	Chieftec CTG-650C

Комплектація сервера наведена у таблиці 2.4

Початок таблиці 3.4 – Перелік комплектуючих для сервера

Пристрій	Марка і модель
Процесор	Intel Core i3- 3220 3.3GHz
Материнська плата	Asus H87-PRO
Відео карта	nVidia GeForce GT 630
Оперативна пам'ять	2x Kingston DDR3-1600 4096MB PC3-12800 HyperX
Вінчестер	Hitachi Ultrastar 7K4000 4TB 7200rpm 64MB
Монітор	21.5" LG 22MP65D-P
Клавіатура	Speedlink Verdana Multimedia Keyboard

Кінець таблиці 3.4 – Перелік комплектуючих для сервера

Миша	Trust Vivy Wireless Mini Mouse Black Solid
Корпус	Thermaltake Urban S21 Black
Мережева карта	TP-LINK TG-3468
Блок живлення	Seasonic Platinum-760

Перелік мережевого обладнання приведено у таблиці 2.5

Таблиця 3.5 - Перелік мережевого обладнання

Пристрій	Марка і модель
Комутатори	TP-LINK TL-SF1024D
Концентратори	D-Link DUB-H7

Class-of-Service - це функція, що дозволяє адміністратору назначити будь-яким різновидам кадрів, необхідні для нього пріорітети обробки. Основна прична створення цих функцій, це декілька різних черг які не оброблють дані, налаштовані на передач одного пакету, хоча передача мала б бути до 10 вископріортетих. Дана властивість пригодиться на низькошвидкісних лініях та при наявності всіхдодатків які представляють різноманітні потреби до класичних затримок. Протокли канального рівня не всі мають змогу підтримувати ось ці пля пріорітетів кадрів, саме у Ethernet воно завжди відсутнє, тому комутатор має використовувати любий додатковий метод для прив’язки кадру з конкретно його пріоритетом. Самий поширений метод - перепідписування портів на комутаторі. При чому регує комутатор на цей спосіб переміщенням кадру в черзі кадрів необхідного прорітету, що напряму залежить від входу сигналу на відповідний порт .Даний спосіб легкий але зовсім важко використовувати під свої конкрені задачі. Наприклад якщо до відповідого порту комутатора підключити інший сегмент, то всі вузли даного сегменту отримують однаковий пріоритет. Більш орієнтованим на проблему є призначення пріоритетів MAC-адресами вузлів, але цей спосіб вимагає виконання величезного обсягу ручної роботи адміну.

Віртуальної мережею (VLAN),- є група конкретних вузлів мережі, де трафік якої, в тому числі і широкомовний, знаходиться на канальному рівні повністю відокремлений від інших вузлів нашої мережі. Що означає, що дана передача кадрів між різними віртуальними сегментами на підставі адреси канального рівня неможлива, незалежно від типу адреси - унікального, групового або широкомовного. У той же час усередині віртуальної мережі кадри за технологією комутації передаються, тобто можливо тільки на той конкретниц порт, який пов'язаний з фактичною адресою призначення кадру.

Віртуальна мережа створює домен широкомовного трафіку (broadcast domain), за методологією побудови з доменом колізій, що створюється повторювачами сигналів мереж Ethernet.

Під час створення локальних віртуальних мереж беручи за основу одного комутатора, частіше за все використовується метод групування в мережі портів. Зазвичай так і є так як віртуальних мереж, побудованих на основі єдиного комутатора, не може бути більша кількість чим портів самого комутатора. Якщо до одного вільного порту підключити сегмент, збудований на основі повторювача сигналу, то вузли даного сегменту не має сенсу вмикати в різні віртуальні мережі,тому що трафік цих вузлів всерівно буде формуватись як загальний.

Створення таких локальних мереж на основі згрупування вільних портів не вимагає від керуючого адміністратора ручної роботи, лише досить вільний порт прописати до декількох перейменованих потрібних мереж. Загалом дана операція відбувається за допомогою перетягування графічних знаків мереж та портів.

Отже оберемо комутатор для побудови локальної мережі в організації.

У проектованої мережі передбачається встановити два сервера. В основному всі робочі станції працюватимуть з ресурсами серверів, отже, в цьому випадку з'являється потенційна вузьке місце в мережі, а саме - порт комутатора для підключення сервера. Так як всі сегменти нових робочих груп будуть підключатися на швидкості 100 Мбіт / сек, і сервера підключаються теж на цій швидкості, то все робочі групи будуть ділити між собою смугу пропускання в 100 Мбіт / сек. Залежно від створюваного ними трафіку, час очікування відповіді серверів може варіюватися в значних межах. Розширити смугу пропускання між

сервером і комутатором, можна кількома способами: або використовуючи комутатор з одним високошвидкісним гігабітним портом для підключення сервера і декількома портами на 100 Мбіт / сек для підключення робочих станцій і груп, або використовуючи для підключення сервера спеціальних двохканальних повнодуплексних мережевих карт. Друге рішення видається більш економічним довстановлення серверу.

Операційна система це не просто комплекс управлінських і оброблюючих програмних компонентів що можуть виступати як інтерфейс між апаратурою системи і різними прикладними програмами, а також вони обов'язково призначені для управління апаратурою та розрахунковими процесами, ефективного розподілу допоміжних ресурсів між всіма вагомими процесами і організації надійних обчислень. Конкретно дане визначення потрібно впроваджувати до більшості новітніх ОС різного призначення.

Операційну систему необхідно вибирати, виходячи з декількох показників:

1) Мінімальні вимоги до апаратного забезпечення.
2) Поширеність і наявність драйверів пристроїв для даної ОС.
3) Надійність і швидкість роботи.
4) Легкість освоєння.

Тому на всі ПК даної мережі будемо встановлювати операційну систему Windows 10.

Операційна система Windows Server нового покоління, яка допомагає IT-фахівцям повністю контролювати інфраструктуру, забезпечуючи безпрецедентну доступність і керованість, що дозволяє досягти більш високого, ніж будь-коли, рівня безпеки, надійності і стійкості серверного середовища. OCWindows Server 2008 відкриває перед організаціями нові можливості, надаючи всім користувачам, незалежно від їх місцезнаходження, доступ до повного набору мережевих послуг. Крім того, в Windows Server є засоби для аналізу стану і діагности операційної системи, що допомагають адміністраторам приділяти більше часу розвитку бізнесу.

В основу Windows Server покладена успішна і потужна операційна система Windows Server 2003, а також удосконалення, реалізовані в пакеті оновлень 1

(SP1) і випуску Windows Server 2003 R2. Проте ОС Windows Server 2008 - не просто удосконалення попередньої операційної системи. Вона розроблена для того, щоб забезпечити організації найбільш продуктивною платформою, що дозволяє розширити функціональність додатків, мереж і веб-служб, від робочих груп до центрів даних, і значно поліпшити якість базової операційної системи.

У Windows Server 2008 не тільки додані нові функції, а й значно удосконалені багато можливостей базової ОСWindows Server 2003. Серед них слід відзначити роботу з мережею, розширені функції безпеки, віддалений доступ до додатків, централізоване керування ролями сервера, засоби моніторингу продуктивності і надійності, відмовостійкість кластерів, розгортання і файлову систему. Ці та багато інших поліпшення допомагають вивести сервери на максимальний рівень гнучкості, безвідмовності і керованості [21].

3.5 Рекомендовані технічні, програмні засоби і адміністративні заходи для забезпечення безпеки і захисту інформації

Всі технічні засоби захисту інформації, які на даний момент присутні на ринку, поділяються з умовної класифікації. Вона включає кілька груп. До складу першої групи входять активні і пасивні технічні засоби, які забезпечують захищеність від витоку інформаційного обсягу у напрямку різних фізичних полів, які з'являються в хвилину застосування засобів її оброблення. Друга група включає в себе програмні та програмно-технічні засоби, які забезпечують розмежування доступності інформації, щодо різних рівнів і ідентифікацію з аутенфікацією користувача. Третя група це група на основі програмних і програмно-технічних засобів, які забезпечують захист інформації і підтвердження її справжнього стану, коли передається по каналах. Четверта група включає в себе програмно-апаратні засоби, які забезпечують цілісність програмного продукту і захист його від незаконного копіювання. У п'яту групу входять кошти, які забезпечують захист від впливу програмних вірусів і інших програм, що шкодять комп'ютера.

І остання група це фізико-хімічні засоби захисту, що забезпечують підтвердження автентичності документів, безпеку їх транспортування і захист від копіювання.

Окремо стоять захищені загальносистемні програмні продукти, що виключають можливість використання декларованих програмних можливостей. Таких систем поки ще не дуже багато.

У цьому ж ряду стоять і спеціальні пристрої - міжмережеві екрани, - щоб забезпечити захист корпоративних мереж від вторгнення з глобальних інформаційних мереж типу Internet.

В даний час засоби і системи, призначені для захисту інформації та підтвердження її справжності при передачі по каналах зв'язку і, в першу чергу, криптографічні пристрої, виробляються більш ніж 700 закордонними фірмами.

Останнім часом все більш широке поширення на ринку програмно-апаратних засобів захисту інформації отримують системи запобігання несанкціонованого копіювання програмних продуктів типу "HASP - ключів".

Найпопулярнішими програмними засобами захисту інформації є антивірусні програми і засоби архівації даних. Вони спрямовані на захист функціонування програмного забезпечення. Дуже часто користувачам персональних комп'ютерів доводиться виконувати резервні копії, коли резерву місця не залишається для розміщення ресурсів. Тоді використовуються програмна архівація, яка обумовлює злиття в один файл - архів, кілька каталогів. Таким чином, скорочується загальний обсяг, але всі дані зберігаються без втрат. Їх можна відновити до початкового стану.

Найбільш відомі і популярні наступні архівні формати: ZIP, ARJ для операційних систем DOS і Windows; TAR для операційної системи Unix; межплатформний формат JAR (Java ARchive). Користувач вибирає ту програму, з якою легше працювати при обраному форматі файлу.

Що стосується роботи антивірусних програм, то вони розроблені спеціально для захисту інформації від атаки вірусних програм. Справа в тому, що існує велика кількість вірусів, алгоритм яких практично скопійований з алгоритму інших вірусів. Як правило, такі варіації створюють непрофесійні програмісти, які

з якихось причин вирішили написати вірус. Для боротьби з такими "копіями" придумано нову зброю - евристичні аналізатори. З їх допомогою антивірус здатний знаходити подібні аналоги відомих вірусів, повідомляючи користувачеві, що у нього, схоже, завівся вірус. Природно, надійність евристичного аналізатора не 100%, але все ж його коефіцієнт корисної дії більше 0,5. Таким чином, в цій інформаційній війні, як, втім, і в будь-який інший, залишаються найсильніші. Віруси, які розпізнаються антивірусними детекторами, здатні написати тільки найбільш досвідчені і кваліфіковані програмісти. Таким чином, на 100% захиститися від вірусів практично неможливо (мається на увазі, що користувач змінюється дискетами з друзями і грає в ігри, а також отримує інформацію з інших джерел, наприклад з мереж). Якщо ж не вносити інформацію в комп'ютер ззовні, заразитися вірусом неможливо - сам він не народиться.

Останнім часом стрімко зростає популярність антивірусної програми - Doctor Web. Dr.Web відноситься до класу детекторів - докторів, має так званий "евристичний аналізатор" - алгоритм, що дозволяє виявляти невідомі віруси. "Антивірусне павутиння", як перекладається з англійської назва програми, стала відповіддю вітчизняних програмістів на навала самомодифицирующихся вірусів-мутантів. Останні при розмноженні модифікують своє тіло так, що не залишається жодної характерною ланцюжка байт, яка була присутня в вихідної версії вірусу. Користувач може вказати програмі, тестувати як весь диск, так і окремі підкаталоги або групи файлів, або ж відмовитися від перевірки дисків і тестувати тільки оперативну пам'ять. У свою чергу можна тестувати або тільки базову пам'ять, або, до того ж, ще й розширену. Doctor Web може створювати звіт про роботу, завантажувати знакогенератор Кирилиці, підтримує роботу з програмно-апаратним комплексом Sheriff.

Основною ціллю "Антивірусної павутини" є наявність евристичного аналізатора. Резонансу між швидкістю і якістю можна отримати, шляхом вказання ключа рівеня аналізу: де 0 - мінімальний, 1 - оптимальний, 2 - максимальний; при цьому, якість швидкості зменшується рівно пропорційно збільшенню якості пошуку. Dr.Web допомагає тестувати файли, заражені CPAV, а також архівовані. Основною функцією є контролювання враження тестованих файлів додатковим

вірусом. При скануванні дисків немає особливої гарантії, що "Антивірусна павутинна" віднайде всі можливі віруси, що знаходяться всередині. Тестування комп'ютерної пам'яті Dr.Web-ом займає великий проміжок часу, тому не кожен юзер може собі дозволити втратити стільки часу на щоденну постійну перевірку всього вмісту жорсткого диска.Але таки потрібно хоча б один раз в два квартали робити максимальну перевірку "жорсткого диску" на віруси та зараження із завданням максимально-якісного рівня евристичного аналізу [2] .Antivirus, це особливий продукт, назначений для захисту комп'ютерів від вірусів і шкідливих програм та їх наслідків. Сума функцій даної програми містить в собі: файловий, поштовий і веб антивіруси. Коли у вас виникне необхідність комплексного захисту вашого комп'ютера і звичайного антивіруса вам недостатньо, то рекомендується звернути особливу увагу на версію Internet Security, яка до стандартних можливостей Kaspersky Antivirus добавляє функції: фаєрвол, захист від реклами та захист від шкідливих програм.

Антивірус Касперського 6.0 це в цілому інший підхід до захисту інформації. Головне в цій програмі, це функція об'єднання і реально помітне покращення поточних функцій та можливостей всіх продуктів даної компанії, що об'єднується в одне вагоме рішення захисту. Така програма забезпечує не лише захист, але і захист від невідомих загроз (нових). Такий комплекс поданий на захист створюється на всіх каналах походження і передачі даних. В програмі є можливість налаштувати будь-який компонент під свої проблеми, що дозволяє максимально сильно адаптувати Антивірус під необхідність конкретного юзера. Тут також передбачена єдине налаштування всіх компонентів захисту.

Захист Антивірус Касперського будується виходячи з джерел загроз, тобто на кожне джерело передбачений окремий компонент програми, що забезпечує його контроль і необхідні заходи щодо запобігання шкідливого впливу цього джерела на дані користувача. Така побудова системи захисту дозволяє гнучко використовувати і налаштовувати будь-який з компонентів під потреби конкретного користувача або підприємства в цілому [12].

Антивірус Касперського включає:

Компоненти захисту, що забезпечують захист вашого комп'ютера на всіх каналах надходження і передачі інформації.

Розширений пошук вірусів - це процес перевірки комп'ютера або окремих файлів, каталогів, дисків та областей, або ж комплексно, на присутність вірусів.

Функції сервісів, це ті що допомагають розібратись вскладностях роботи з програмами та здійснють розширення функціоналу.

Ще одна дуже ефективна, вона зхаищає від троянів, вірусів, інтернет-хробаків. Вона має дуже маленький розмір, але не поступається характеристиками таких як і в сучасних антивірусах. Має функцію евристиного аналізатора, що надає досліджувати нові віруси це ESET NOD32 Antivirus.

Такі програми McAfee VirusScan Enterprise забезпечують різностороній захист комп’ютерних мереж, серверів що працють проти вірусів та робочих станцій, захист віл троянів, хробаків. Ці всі програми McAfee VirusScan Enterprise це оперативні, надточні, та продукти швидкого розвитку, зручні для початкової роботи та впровадження на підприємствах, тому що вони поєднують забезпечення безпеки та ефективне виявлення та опрацювання.

Головним вагомим плюсом є те, що адміністратор можуть легко на практиці показати результативність та всі свої кроки по захисту щодо збереження конфіденційності даних, і за допомогю правильних дій зожуть швидко знайти зловмисника, та представивши звіт своїх дій по закону покарати його. Але нажаль дуже мале поширення цих програм на сьогодні, тому важко однозначно вказувати їх ефективність та розвиток.Якщо її вміло використовувати за допомогою ряду спеціальних адміністративних заходів, то криптографія здатна забезпечити повне збереження вашої інформації [14].

4. ОБЧИСЛЕННЯ ЗАПРОПОНОВАНОГО МЕРЕЖЕВОГО ВИБОРУ, ДЛЯ ВІДПОВІДНОСТІ ВИМОГАМ СТАНДАРТУ

4.1 Розрахунок продуктивності локальної мережі

Щоб стоворити мережу Ethernet між самими дальніми комп'ютерами рекомендовано використовувати не більше 26 концентраторів, багато відрізків кабелів і 3-х навантажених сегментів. Звідси загруженим сегментом являється концентратор з підключеними до нього кабелем комп'ютерами. Чи не навантаженим сегментом називається концентратор тільки з підключеними до нього іншими концентраторами.

Така аксіома правильно називається правилом 5-4-3. Найважливішим елементом, що вказує на роботоспособність цієї мережі, являється коефіцієнт навантаження сегменту мережі S:

$$S = \frac{P \cdot m_i}{f}, \qquad (3.1)$$

де P - визначена кількість ПК у розглядаємій частці мережі

mi - кадр/секунду, які надсилаються в мережу і-м вузлом;

f - пропускна здатність сегменту, рівна14880 кадр / с.

Тому здійснимо імітацію моделювання мережі Ethernet та дослідимо її працездатність на основі протоколів-аналізаторів. Це дослідження показало нам, якщо вказаний коефіцієнт завантаження S> 0,5 то однозначно розпочинається неймовірношвидке зростання числа колізій та відповідно до цього, з того що ми описували вище випливає те, що збільшується час очікування доступу до локальної мережі.

Найбільш позитивне значення коефіцієнта завантаження S для мережі стандарту Ethernet, повинна бути: 0,3

Дані експерименту показали нам, що кожен з комп'ютерів передає в мережу в здебільшого від 4800 до 980 кадрів/секунду. З цього випливає, що коефіцієнт

навантаження сегменту рівен [17]. Після проведення розрахунків для кожної крупи коеіфіцієнт не перевищував 0,3.

4.2 Розрахунок локальної обчислювальної системи на відповідність вимогам стандарту для обраної технології

Дотримання численних обмежень, встановлених для різних стандартів фізичного рівня мереж Ethernet, гарантує конкретну роботу мережі (природно, при справному стані всіх елементів фізичного рівня).

Можлива ситуація, коли дві станції одночасно намагаються передати кадр даних по загальному середовищі. При цьому відбувається колізія (collision), так як вміст обох кадрів зіштовхується на загальному кабелі і відбувається спотворення інформації. Більш ймовірно колізія виникає через те, що один вузол починає передачу раніше іншого, але до другого вузла сигнали першого просто не встигають дійти до того часу, коли другий вузол вирішує почати передачу свого кадру. Тобто колізії - це наслідок розподіленого характеру мережі. Колізія - це нормальна ситуація у мережі Ethernet.

Для того щоб дійсно правильно опрацювати колізію, усі необхідні точки одночасно переглядають та зчитують сигнали, що проходять кабель. Тільки якщо дані які передавались і які зчитуються координально різні то фіксується факт виявлення колізії. Після цього виявлена колізія, передавальна станція має зупинити передачу та паузу в найперший малий випадковий інтервал часу. Після чого знову може розпочати свою роботу з захопленням середовища з передачею кадру. При маленькому навантеженні середовища, ймовірність цієї колізії маленька, та виникає нюанс при постійному використанні цієї мережі, такий як важкість з отриманям досвіду.

Його називають часом подвійного обороту (Path Delay Value, PDV).

IEEE 802.3 це такий комітет, що вказує вхідні дані що вказують затримки, які видають повторювачі сигналів та різними середовищами в яких проходять дані. Щоб обрахувати самостійно максимально достатню кількість повторювачів і максимальну довжину всієї мережі, не беручи до уваги значень із правил «5-4-3» і

«4-х хабів». Після правильного прорахування цей коефіцієнт загруження мережі Ethernet обраховуються показники PDV, що більш чим позитивізує умові: PDV ≤ 575

Узагальнене визначення PDV прирівнюється до суми всіх необхідних значень PDVi у кожному сегменті, а саме значення PDVi рівне сумі всіх затримок, що вносяться і- базою сегменту та затримкою, що вноситься характерним кабелем:

$$PDV=\sum PDVi, \quad (3.2)$$

де PDVi = ti бази + ti кабелю

В свою чергу:

$$ti\ кабелю = Li \times bti \quad (3.3)$$

У таблиці 3.1 наведені значення затухання, для обчислення PDV вказуються частинами мережі в bt. Вищеописані нтервали bt приведені в таблиці вже вказані помноженими на 2, для того щоб, правильно прорахувати подвійний час проходження сигналу.

Таблиця 4.1 - Дані затухання, для розрахунку PVV вносяться елементами мережі в бітових інтервалах bt

Тип сегмента	База лівого сегмента, bt	База проміжного сегмента	База правого сегмента	Затримка середовища на 1 м
		сегментуbt	сегменту, bt	
100Base-T	11,8	46,5	169,5	0,0866
100Base-FX	11,8	46,5	169,5	0,1026
1000base-T	15,3	42	165	0,113
1000Base-FX	12,3	33,5	156,5	0,1

У таблиці 4.2 наведені значення затухання, для розрахунку PDV.

Таблиця 4.2 - Значення затухання, для розрахунку PVV

Тип сегменту	Лівий сегмент, bt	Проміжний сегмент,bt
1000Base-T	19	9
1000Base-FX	19	9
100Base-T	8,5	6
100Base-FX	8,5	6

У наведених вище таблицях застосовуються поняття: лівий сегмент, правий сегмент і проміжний сегмент. Окрім того що ми можемо помічати затухання, які вносяться лініями зв’язку, також відслідковувати підключення до концентраторів, також ці сегменти передають власні затримки, що називаються базами.

Лівим сегментом є такий сегмент, в якому розпочинає шлях сигналу від виходу конфентратора кінцевого вузла. Такиц сигнал зазвичай проходить через так завані проміжні сегменти, а потім проходить до отримувача самого великого віддаленого вузла який розташований у найбільш віддаленого сегмента, такий сегмент називається правим. Розглядаючи кожен сегмент окремо, з кожним сегментом пов'язана окрема постійна затримка, названа базовою, вона залежить тільки від виду конкретного сегмента і від його положення на дорозі сигналу відповідно до лівого проміжного або правого. Більше того з кожним сегментом зв’язана затримка розповсюдження сигналу поздовж кабелю цього сегмента, яка напряму залежить від його довжини та розраховується методом множення часу розповсюдження сигналу по одному метру кабелю звісно ж краще визначати в бітових інтервалах на довжину кабелю в метрах [17].

Спрощуючи ці всі розрахунки в цілому зазвичай будуть використовуватись дані довідок, які розміщують в собі дані значень затримки розповсюдження сигналів в повторювачах, прийомо-передавачах та в інших різних фізичних сферах. У таблиці 3.3 приведені дані, які важливі для обчислення значення PDV що зазначені для всіх фізичних стандартів мереж таких як Ethernet і Fast Ethernet, витягнуті з довідника під назвою Technical Reference Pocket Guide, що створила компанія Bay Networks.

Таблиця 4.3 - Сталі коефіцієнти PDV для всіх можливих фізичних стандартів мереж Ethernet і Fast Ethernet

Тип сегменту	База проміжного сегмента	База правого сегмента	Затримка середовища на 1 м	Максимальна довжина сегмента
1000Base-T	46.5	169.5	0.0866	500
1000Base-FX	46.5	169.5	0.1026	185
100Base-T	42.0	165.0	0.113	100
100Base-FX	24.0	-	0.1	2000

Таким чином, PDV мережі одно:

PDV = 19.8 + 45.4 + 42.2 + 42.6 + 42.3 + 42.2 + 42.2 = 441.9

Результатом формули, виявили числове значенння PDV воно значно менше максимально допустимої величини 578, тоді конкретно ця мережа відповідає вимогам за величиною максимально можливої затримки обороту сигналу.Оскільки значення PDV менше максимально припустимої величини 512 або 575, то ця мережа спроектована правильно і колізії будуть виявлятись

4.4. Схема логічної та фізичної адресації в мережі

Всі IP-адреси представляють собою основний вид адрес, на базі яких мережевий рівень надсилає пакети між локальними мережами. Також конкретно ці адреси складаються з 4 байт, наприклад 155.31.5.3. Така адреса надається адміном під час процесу підбору конфігурування комп'ютерів та допоміжого обладнання. Також кожна IP-адреса складається із двох частин - номера мережі й номера вузла. Кожен номер мережі у свою чергу може бути довільно обраний адміністратором або ж рекомендовано призначений спеціальним підрозділом Internet, в томк випадку якщо мережа в майбутньому має реалізуватись так, як основна частина Internet. Поставники таких послуг Internet отримують рамки адрес у підвідлів InterNIC, а потім особисто розподіляють їх серед своїх абонентів.. Кожен номер вузла в визначеному протоколі IP надається незалежно

від локальної адреси даного вузла. Зазвичай такий пристрій як, маршрутизатор по тлумаченню має бути вхідним одночасно в декілька мереж.

Фінальний вузол самостійно має можливість бути приєднаним в кілька IP-мереж. Якщо є такий випадок, то комп'ютер мусить мати декілька IP-адрес, їх визначити можливо по конкретній кількості мережевих зв'язків.

Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання.

При організації Internet-шлюзу на базі однієї з машин локальної мережі стає небажаним використовувати усередині мережі IP-адреси, що можуть дублювати реальні адреси реальних машин у Internet. У документі RFC1597 перераховані зарезервовані діапазони IP-адрес, які можна використовувати в ізольованих від Internet локальних мережах: 10.0.0.0 (маска мережі 255.0.0.0); 172.16.0.0 (маска мережі 255.255.0.0); 192.168.0.0 (маска мережі 255.255.255.0). Найчастіше в малих мережах з виходом в Internet використовуються адреси з діапазону 192.168.X.0 з маскою мережі 255.255.255.0, або ж 128.X.X.0 з маскою 255.255.0.0

Таким чином, у спроектованій мережі було обрано IP-адреси у діапазоні 192.0.0.0 з маскою мережі 255.255.255.192

Кожен з адаптерів Ethernet містить ПЗП адреси, в якому знаходиться унікальна мережева адреса комп'ютера (MAC-адреса), встановлена фірмою-виробником адаптера, жодна з яких унікальна. Кожна такий виробник має список адрес з певного діапазону регіонів.

MAC-адресу (від англ. Media Access Control - нагляд за доступом до середовища, також Hardware Address, також фізичну адресу) - унікальною характеристикою, що надається будь-якій одиниці мережевого обладнання або ж деяким окремим інтерфейсам в даній комп'ютерній мережі Ethernet.

4.5 Налаштування, підключення та особливості Windows server

Головним елементом точкового адміністрування Windows Server являється домен. Домен, це така група серверів які працюють під керуванням Windows Server,та яка працює, як одна злагоджена система. Конкретно всі сервери Windows в домені обирають один і той же набір юзерів, тому доволі важко ввести масив даних усіх користувачів мережі. Тому краще їх вносити з різних комп'ютерів, різними адмінами для спрощення роботи, а потім вони розпізнаються на інших серверах цього домену.

DHCP це збільшення можливостей протоколу BOOTP, що озволяє динамічно визначати IP-адреси (на додаток до віддаленої завантаженні бездіскових станцій). Під час чого DHCP видає всі необхідні дані для налаштування стеку протоколів таких як TCP / IP та як додаткові дані використання серверів зазначених вище.

Середовище DHCP. Середовище DHCP, це таке адміністративне згрупування, індентифікує повністю абсолютно заповнені послідовні границі IP-адрес, щоб не конфліктували юзери DHCP у локальній комп'ютерній підмережі. Середовища дають повну оцінку логічної підмережі, яка має виступати клієнтом служби DHCP, що дозволяє серверу зазначати приклади потрібних конфігураційних збірок, які доступні всім можливим клієнтам DHCP в локальній підмережі. Середовище має бути зазначено швидше чим розпочнуть клієнти DHCP користуватись сервером DHCP для стоврення динамічних конфігурацій TCP / IP.

Блок IP-адрес. Наприклад у нас є певний вказаний діапазон DHCP та вказані (прописані) рамки виключень, то всі інші адреси визначаються блоком всіх доступних IP-адрес в рамках визначених діапазонів задані діапазони ісклю¬ченія, то решта адрес називається пулом доступних адрес (address pool). Так ці IP-адреси можуть бути вказані як і вручну так і динамічно назначаються клієнтами DHCP в рамках мережі.

Границі адрес. Границі адрес, це обмежений масив послідовних IP-адрес в рамках блоку , що мають бути витягнуті з подання необхідної служби DHCP.

Функція резерву. Reservation, допомагає визначити юзерові постійну адресу та може гарантувати що кожен вказаний пристрій в цій підмережі має можливість використовувати однакову IP-адресу.

Суперобласть - твердження, що зазвичай задіяне в функціоналі DHCP,що вказує на множину угрупувань в кожному відповідному вгрупувані кожного окремого адміна, тобто суперобласть (superscope). Суперобласті використовуються для вирішення множини задач служби DHCP.

Фунції DHCP, це додаткові функції встановлення клієнтів, які конкрений сервер DHCP при необхідності має можливість визначити для обслуговування орендни DHCP. Для прикладу IP-адреси шлюза та/або маршрутизатора необхідних серверів WINS, DNS в основному призначаються для кожної області, регіону чи загалом для всіх об’єктів глобальної мережі, що керуються нашим сервером DHCP. Більше того, сервер DHCP надає можливість встановити і добавляти ряд своїх функцій.

Протокол спрощує роботу мережевого адміністратора, який повинен вручну створювати лише конкретно єдиний сервер DHCP. При підключенні нового персонального копм’ютера до локальної мережі, яка опрацьовується нашим DHCP сервером, він подає запити на унікальність IP-адресів та сервер DHCP встановлює їх з усіх моливих в пулі вільних адресів, так цю дію функціонально можна розділити на декілька поступових дій:

1. DHCP Discover, пошук та виявлення ,

2. DHCP Offer, пропонує ряд доступних адрес,

3. DHCP Request, подає запит, на пропозицію, та під час цього адреса автоматично-офіційно визначається та вказується сервером DHCP Acknowledgement, який здійснює підтвердження.

Для того, щоб конкретна адреса не була вільною наш сервер DHCP відправляє її на визначений адміном термін, така маніпуляція носить назву орендного договору (lease). Коли проходить половина орендованого терміну, клієнт DHCP надає запит про його відновлення, і цей самий конкретно встановлений сервер DHCP пролонгує даний орендний договір. Саме це забезпечує те, що коли виникає ситуація, що машина перестає бронювати наданий їй адрес , наприклад при переїзді чи переміщені, і після закінчення орендного договору, ця адреса відправляться в пул, щоб використовуватись повторно в інтеграціях з DNS. Сервери DNS забезпечують дозвіл імен для мережевих ресурсів та міцно

зв’язуються з протоколами та службами DHCP. Для Windows конкретні сервери DHCP та відповідні їм клієнти претендують на реєстрацію в DNS.

Покрешення моніторингу та керування. Удосконаленна та допрацьована функція, яка полягає у тому, що здійснює забезпечення отримання повідомлень про поведінку, стан та рівень впровадження пулу IP-адрес. Сповіщення зя’вляється у вигляді знаку або повідомлення.

Групові адреси та їх розподілення. Вкладенна додаткова функційність групових адресРозподіл групових адрес. Звичайні програмні продукти для забезпечення роботи в групах, наприклад: трансляцій, конференцій, потребують специфічного налаштування адрес груп.

Захист від появи неправомірних сервісів DHCP. Якщо в одному сегменті локальної мережі, знаходяться декілька серверів це в певний момент часу може викликати неполадки (конфлікти) в системі. Удосконалені механізми допомагають встановити неполадки і припинити неправильну роботу сервера, щоб наладити повністю новий процес функціонування DHCP.

Безпека та захист під час процесу заміни серверів. Щоб зареєструвати сервер DHCP необхідно використовувати надані засоби Active Directory. Якщо неможливо встановити сервер в теці, то ймовірно він не зможе правильно працювати і тим більше давати відповідь на запит юзера.

Після установлення Windows Server потрібно здійснити налаштування користувачів. Основним елементом централізованого керування є домен. Групування комп’ютерів в домени дає такі важливі переваги як: єдиний адміністративний блок, єдину службу безпеки.

Мінімальні вимоги до домену це мінімум один сервер, що працює з системою Windows Server.

Наступним важливим кроком є вибір побудови домену.

Розрізняють чотири побудови домену, для розгортання локальної мережі: побудова одного-єдиного домену, побудова основного домену, побудова множини багатьох головних доменів та повної взаємодовіри в структурі.

Модель єдиного домену

Якщо мережа має не надто багато користувачів і не повинна ділитися з організаційних причин, можна використовувати найпростішу модель - модель єдиного домену. У цій моделі мережа має тільки один домен. Природно, всі користувачі реєструються в цьому домені.

Ніяких зв'язків довіри не потрібно, оскільки в мережі існує тільки один домен (рис. 4.1).

Рисунок 4.1 – Побудова єдиного домену

Для того щоб забезпечити надійну роботу локальної мережі, потрібно застосовувати побудову домену - єдину, але тільки якщо нею користується мала кількість юзерів та їхніх груп. Кількість юзерів та їхніх груп розраховується в залежності від певної кількості в домені серверів та апаратури.

Наведена побудова домену не може бути використана для підприємства, так як мережа ділиться з організаційних причин.

Модель основного домену, в якому конкретна локальна мережа містить малу групу юзерів і їхніх групувань, але обов’язково має бути розмежована на домени згідно організаційних процесів роботи, саме конкретно ця модель є найуспішнішим варіантом (рис.4.2).

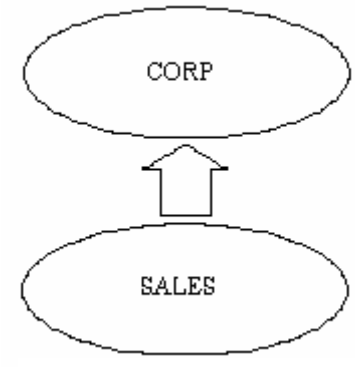

Рисунок 4.2 – Будова головного домену

В ході даного проєкту ми використовуємо єдиний домен для адміністрування.

4.6 Технологія перетворення мережевих адрес (NAT)

NAT (Network Address Translation) - методика трансляції мережевих адрес в TCP / IP мережах, що дозволяє змінювати IP заголовка пакета, який передається через маршрутизатор.

Всього виділяють 4 типи NAT:

1. Статична. Безперервно зіставляє публічний хост з приватним, який був створений маршрутизатором. Це тип найчастіше використовується в мережах, де необхідно забезпечити будь-якої доступ ззовні. Оптимальне рішення для організації доступу користувача до поштових служб і веб-серверів.

2. Динамічна. Базується на пулі публічних IP, що застосовуються для виявлення приватних мереж. Їх призначають інтернет-провайдери, і будь-який внутрішній вузол такий NAT має свою унікальну адресу, який перекладається маршрутизатором на перший знайдений вільний публічний адресу в публічному пулі IP.

3. Перенаправлення порту. Завдяки цій NAT окремо взятому адресою можна підключатися до різних серверів.

4. Переклад адрес портів. Найпопулярніша використовувана NAT. Забезпечує мультиплексування одночасно декількох внутрішніх вузлів з подальшим створенням одного публічного адреси. При цьому номери портів джерела можуть бути різними.

Використовуючи NAT, можна значною мірою зменшити природне виснаження публічного простору адрес. Крім того, сучасні мережі можуть використовувати простір адрес RFC 1918 всередині, не втрачаючи при цьому доступ в інтернет.

Реалізація NAT програмним шляхом відбувається так:

Якщо є сервер, який працює під певною операційною системою, то трансляцію хостів можна організувати без придбання будь-якого додаткового обладнання.

Для реалізації NAT на рівні програмного забезпечення сервер повинен бути оснащений як мінімум двома мережевими картами (реалізації NAT на базі машини з одним портом можливо в разі наявності Trunk-VLan).

Абсолютно всі сучасні серверні операційні системи мають підтримку трансляції хостів найпростішого класу. Найкраще в роботі NAT себе показали UNIX-системи (в плані високопродуктивних, стійкості до відмов і гнучкості).

Багато з ОС по типу * BSD-систем, GNU / Linux і OpenSolaris дозволяють розгорнути NAT «з коробки», а в інших ОС реалізація можлива при використанні модулів і міжмережевих екранів, які підтримують функцію трансляції хостів.

Крім вищеописаних серверних операційних систем NAT може повноцінно працювати на серверах, що знаходяться під керуванням ОС із сімейства Windows Server.

Щоб впровадити NAT на базі Windows server потрібно:

1. Налаштувати Windows server в такому порядку:

1) контролер домену

2) рядовий сервер AD з встановленими службами ролей маршрутизації, DirectAccess і VPN (RAS)

3) сервера RRAS потрібні два інтерфейси:

4) Один інтерфейс, підключений до Інтернету (буде використовуватися як інтерфейс NAT)

5) Інший інтерфейсний адаптер, підключений до внутрішньої мережі (буде використовувати NAT в Інтернеті)

Виконати такі дії по увімкненню та налаштуванню NAT:

1) підключення служби перетворення мережевих адрес (NAT) в Windows Server

2) перевірити настройку NAT

3) змінити налаштування NAT

Для роботи NAT вам буде потрібно наявність:

1) DNS-сервер, який дозволяє як внутрішні, так і зовнішні адреси

2) DHCP-сервер з робочим об'ємом

3) Конфігурація цих двох останніх служб не включена в цю службу.

Область DHCP повинна бути налаштована для параметра 003 Router (шлюз), щоб вказувати на IP-адресу сервера RAS. Крім того, параметри 006 DNS-сервери повинні вказувати на IP-адресу вашого DNS-сервера як зображено на рисунку 4.1.

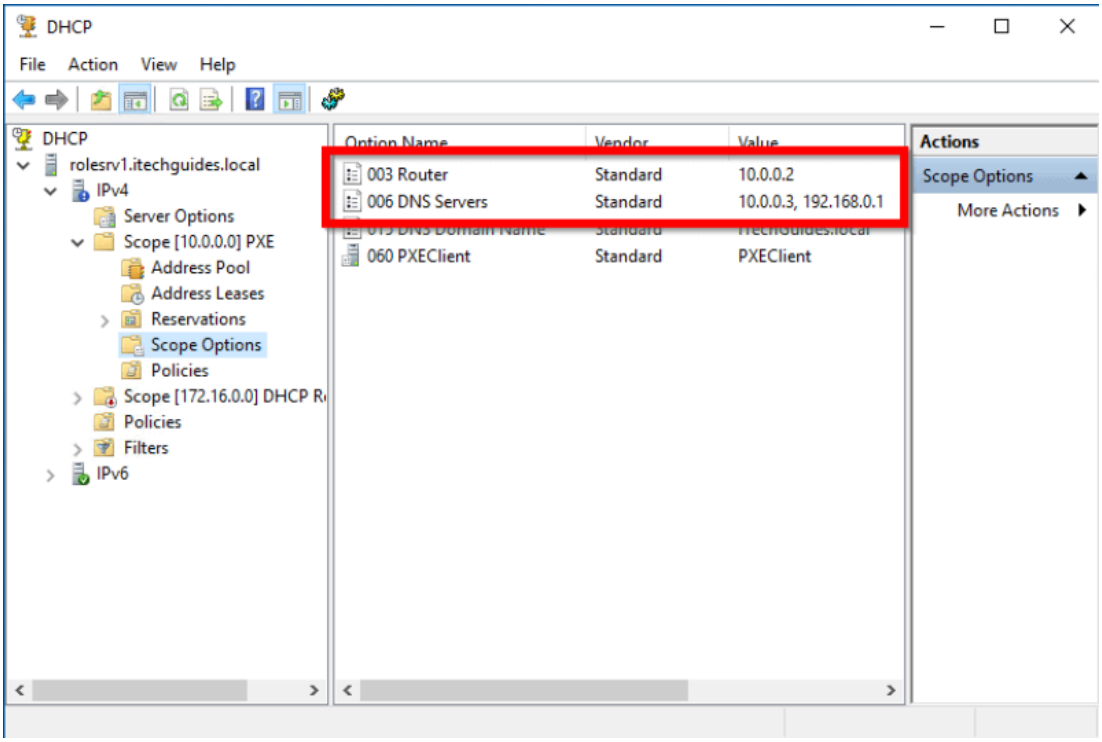

Рисунок 4.1 – Налаштування DHCP

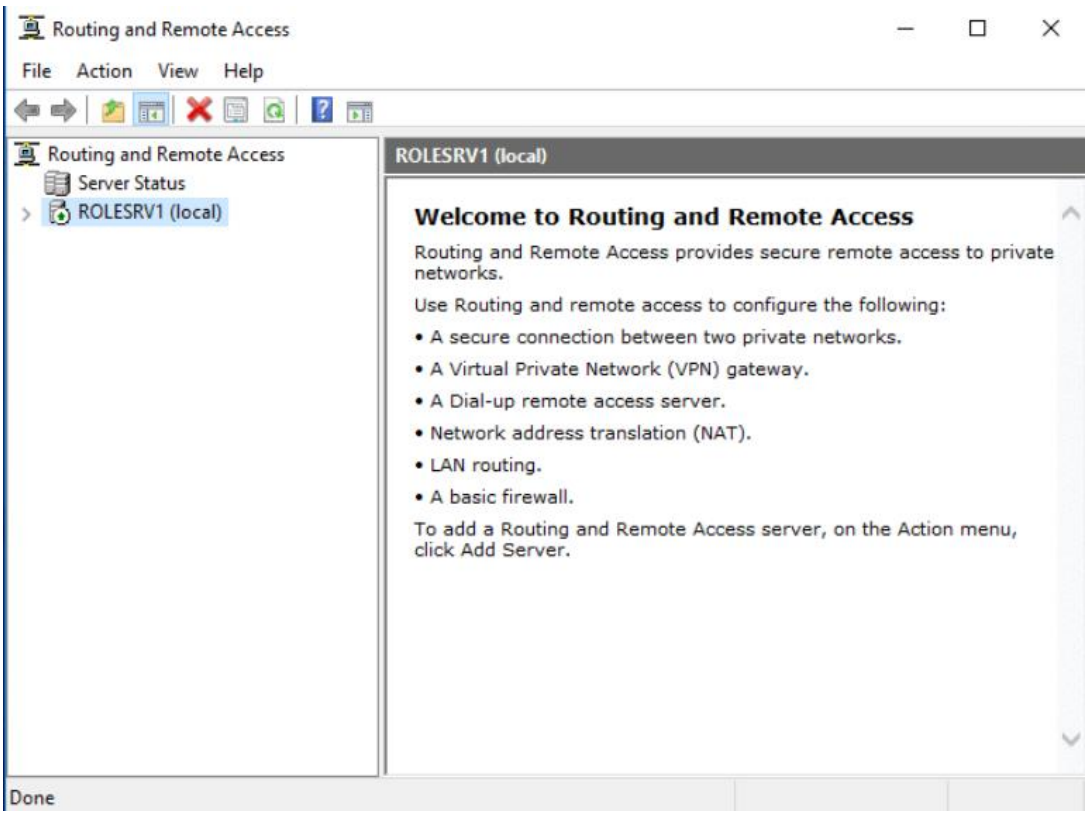

Рисунок 4.2 – Увімкнення служби NAT

Щоб увімкнути NAT входимо на рядовий сервер із встановленою роллю віддаленого доступу. Потім відкриваємо диспетчер серверів. У диспетчері сервера обираємо «Інструменти» та «Маршрутизація та віддалений доступ» (рис 4.3).

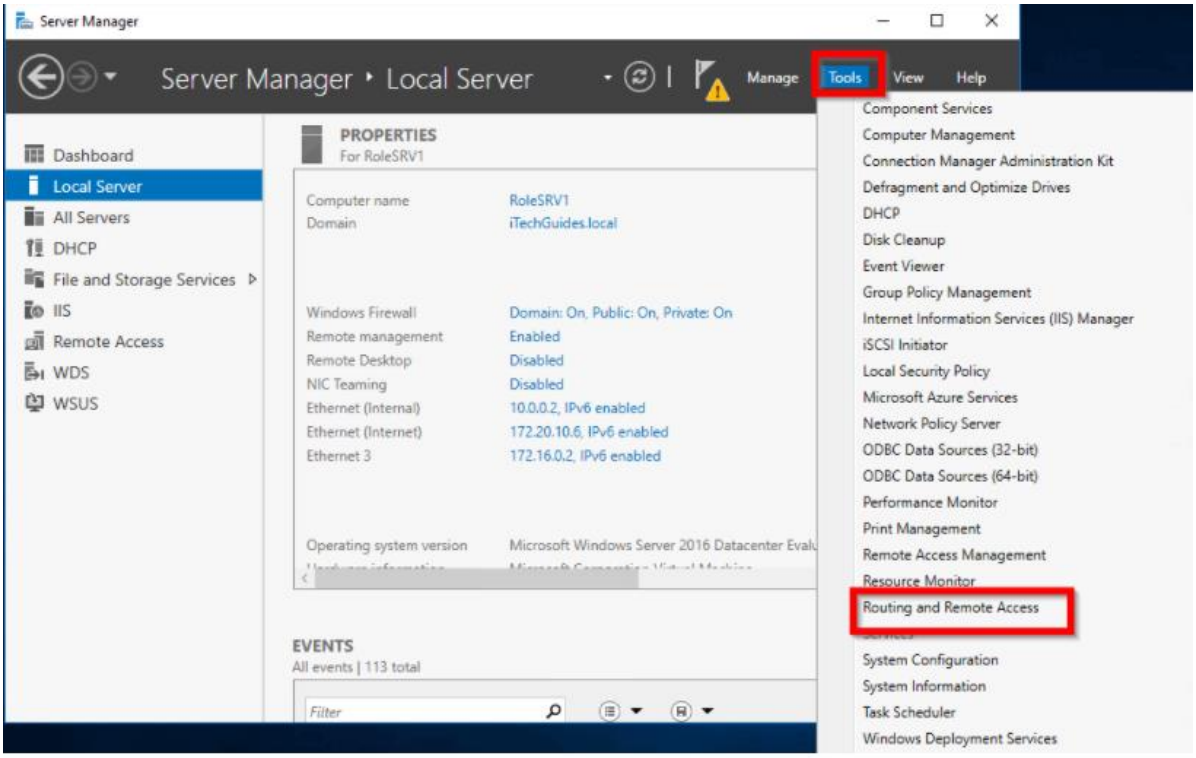

Рисунок 4.3 – Диспетчер серверів

Коли відкриються настройки маршрутизації і віддаленого доступу, клацніть сервер правою кнопкою миші. Потім виберіть «Налаштувати і включити маршрутизацію і віддалений доступ»(рис. 4.4).

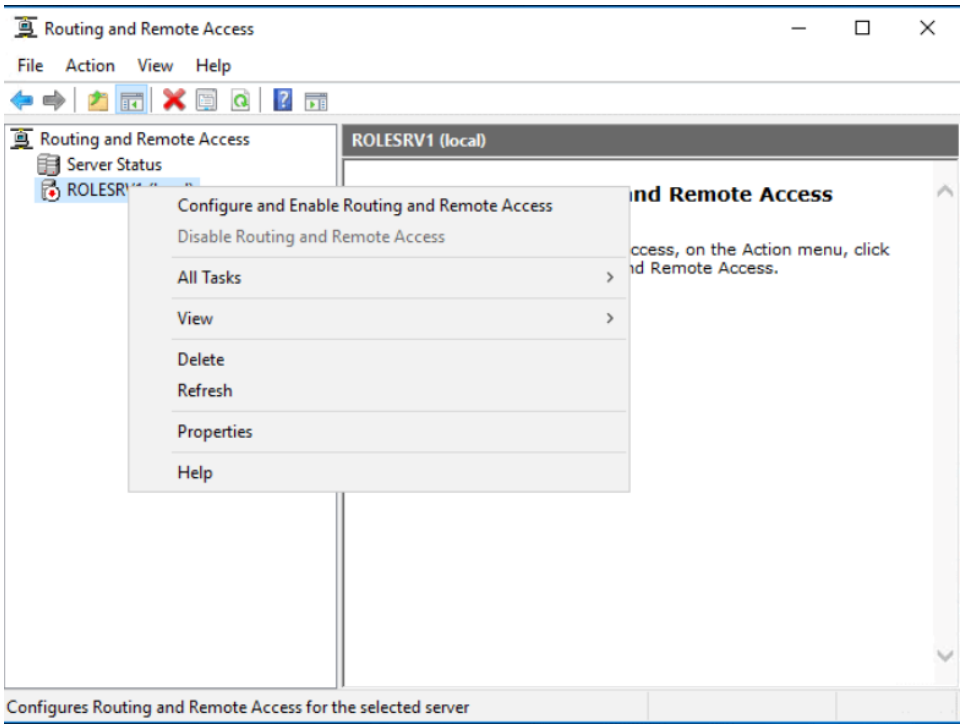

Рисунок 4.4 – Налаштування маршрутизації

Далі обираємо NAT . Обираємо мережевий інтерфейс, через який користувачі будуть підключатись в інтернет (рис 4.5).

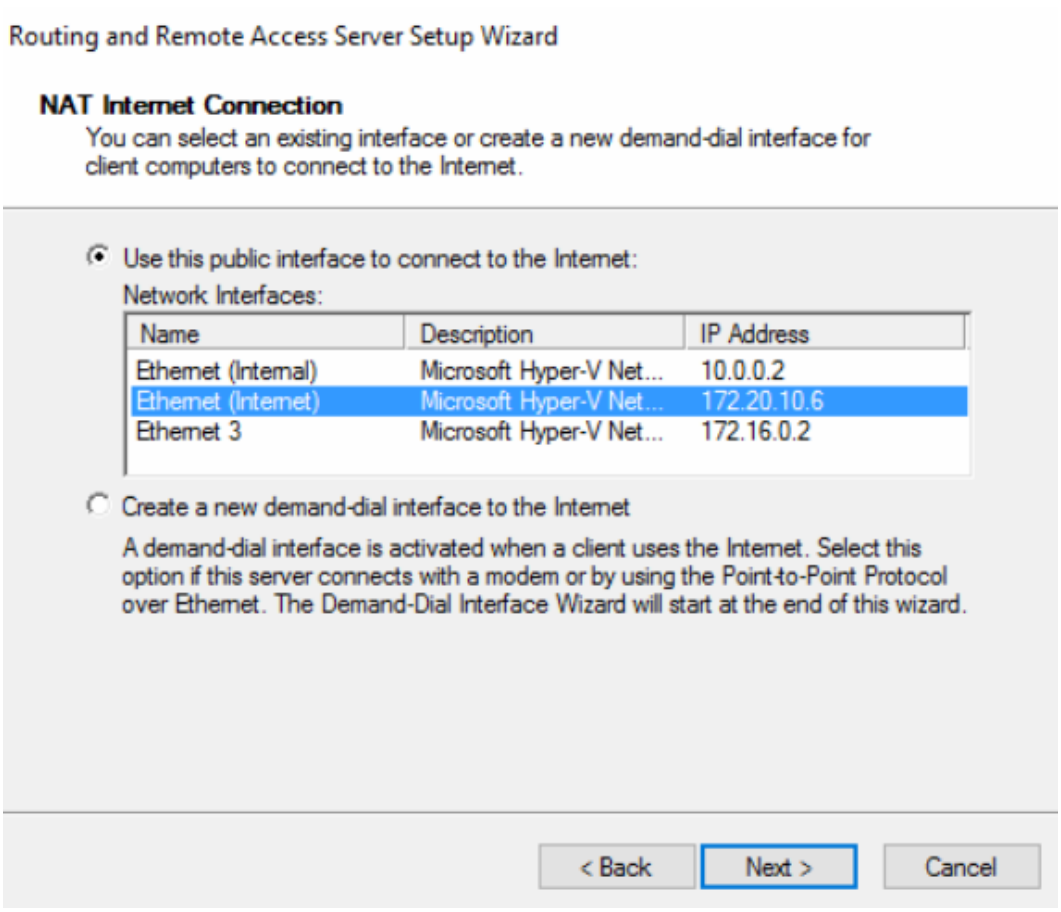

Рисунок 4.5 – Вибір мережевого інтерфейсу

Далі необхідно обрати мережу та мережевий адаптер сервера, який буде розділяти підключення до інтернету. Далі завершуємо уставновлення та перезагружуємо сервер.

Конфігурація NAT повинна дозволяти клієнтам у мережі підключатися до Інтернету за допомогою одного загальнодоступної IP-адреси.

Щоб перевірити, чи працює ваша служба перетворення мережевих адрес (NAT) в Windows Server необхідно увійти в систему на ПК з Windows 10, який підключений до внутрішньої мережі. Щоб підтвердити IP-інформацію комп'ютера, відкриваємо командний рядок. Потім уводимо команду ipconfig /all.

4.7 Протокол мережевого керування SNMP

SNMP - створений для перевірення функцій мережевого обладнання такого як: мости та комутатори. Трішки з часом діапазон робіт цього протоколу стали розширюватись та працювати з більш широким колом мережевої апаратури: шлюзи,машини під керуванням Windows NT, термінальні сервера, хаби, LAN Manager сервера і т.д. А також SNMP виконує за необхідності функцію внесення корективів у роботу вищеописаних пристроїв.

Це безпечна система мережевого керування, що забезпечує постійне спостереження для всієї мережі. Основні характеристики продукту:

1) моніторинг пристроїв, WAN-з'єднань, серверів і додатків;
2) підтримка інтернет-протоколу версії 6 (IPv6);
3) підтримка SNMP v1, v2c і захищеною версією v3;
4) швидка і розподілена архітектура;
5) підтримка інтеграції з мережевими звітами SNMPc OnLine;
6) основні / резервні сервери з автоматичною отказоустойчивостью;
7) реєстрація подій в Syslog;
8) віддалена консоль Windows;
9) автоматичне виявлення мережі;
10) середовище для програмування і написання скриптів.

Вказівки SNMP побудовані з таких складових: community name (імені об’єднання) та даних . Об’єднання ommunity name визначає обмеження доступу для наборів NMS, що задіюють цю назву. Інформативна частка вказівки містить в собі потужну операцію SNMP (get, set) а також всі можливі зв’язані операнди. Ці операнди вказують на ступінь реалізації необхідного об’єкту, який прописаний конкретно в цьому пакеті SNMP.

SNMP дозволяє проводити різні необхідні тестування пропускних вимог апаратів мережі, з будь-якого пристрою мережі. Необхідним це тестування буває дуже часто, тому-що саме просте спостереження за статистичними даними не відає таких результативних відповідей, щоб точно визначити, що сталось в мережі.

Для інтерфейсів Ethernet, встановлене спеціальне тестування Time-domain reflectometry (TDR), воно допомагає встановити небхідну довжину до поломки в в коаксіалі кабелю. Для запуску Time-domain reflectometry ми маємо визначити необхідний показник зміної ifdExtnstTesttiCods (9.1.1.7.2.5.8.5.3.7.0), що містить тип виконуваного тесту, так, щоб вона містила ідентифікатор тесту TDR в MIB: (9.1.1.7.2.5.8.64.3.7.0).

Тестування завершиться з результатом значення змінної ifdExtnstTesttiCods (9.11.7.2.5.8.64.3.7.0), що конкретизує дану перевірку так:

1) відсутність результату
2) успіх
3) виконується
4) не підтримується
5) неможливо запустити
6) припинений
7) негативний результат

Ще одним вагомим важілем є число змінної ifdExtnstTesttiCods (9.11.7.2.5.8.64.3.7.0) якщо воно вміщатиме в собі показник зміної, який в свою чергу передає результат тестування. То сам результат тестування буде встановлено як числовий діапазон в 200-нансек вимірних значеннях між вхідним та вихідним тестовим пакетом даних. Якщо взяти це правило до уваги то на

підставі нього ми можемо встановити потрібну нам довжину. Необхідним новим рішенням в SNMPv2 являється такий фактор, що кожна одиниця, що адмініструє мережу, матиме змогу працювати в будь-якій ролі та при необхідності зможе використовувати комбіновані ролі. Що дає вирішення проблематики користувачів використовувати SNMP в своїй розробленій ієрархічній будові мережі, де відбувається контроль вертикальний за користувачами зверху вниз.Дуже багато часу зазвичай надається проблематиці безпеки захисту SNMP, що являється найвразливішим місцем цього протоколу.

В наш час питання мережевої безпеки набувають особливого значення, особливо коли мова йде про протоколи передачі даних, тим більше в корпоративних мережах. Навіть після поверхневого знайомства з SNMP v1 / v2 стає зрозуміло, що розробники протоколу думали про це востанню чергу або ж їх жорстко тиснули терміни здачі проекту% -). Створюється враження що протокол розрахований на роботу в середовищі так званих "довірених хостів". Уявімо собі якусь віртуальну особистість, точніше якийсь IP адреса, володар якого має намір отримати вигоду, або ж просто насолити адміністратору шляхом порушення роботи якоїсь мережі. Станом на місце цієї особи. Розгляд цього питання зведемо до двох пунктів:

а) ми знаходимося поза "ворожої мережі". Яким же чином ми можемо зробити свою чорну справу? В першу чергу припускаємо що ми знаємо адреса шлюзу мережі. Згідно RFC, з'єднання системи керування з агентом відбувається по 161-ому порту (UDP). Згадаймо про те що дляуспішної роботи необхідне знання групи. Тут зловмисникові на допомогу приходить то, що часто адміністратори залишають значення (імені) груп, виставлені за замовчуванням, а за замовчуванням для SNMP існує дві групи - "private" і "public". У разі якщо адміністратор не передбачив подібного розвитку подій, недоброзичливець може доставити йому масу неприємностей. Як відомо, SNMP протокол є частиною FingerPrintering. При бажанні, завдяки групі system MIB II, є можливість дізнатися досить великий обсяг інформації про систему. Чого хоча б коштує read-only параметр sysDescr. Адже знаючи точно версію програмного забезпечення, є шанс, використовуючи засоби для відповідної ОС отримати повний контроль над

системою. Я не даремно згадав атрибут read-only цього параметра. Адже якщо не дивитись в початковий код snmpd (в разі UNIX подібної ОС), цей параметр змінити не можна, тобто агент сумлінно видасть зловмисникові все необхідні для нього дані. Але ж не треба забувати про те, що реалізації агентів під Windows поставляються без вихідних кодів, а знання операційної системи - 50% успіху атаки. Крім того, згадаємо про те, що безліч параметрів мають атрибут rw (read-write), і серед таких параметрів - форвардного! Уявіть собі наслідки установки його в режим "notForwarding (2)". Наприклад в Linux реалізації ПО для SNMP під назву ucd-snmp є можливість віддаленого запуску скриптів на сервера, шляхом надсилання відповідного запиту. В такому випадку ймовірність звільнення адміна різко зростає. Адже перебування в одному сегменті мережі дає можливість простим сніффінгом відловити назви груп, а з ними і безліч системної інформації. Цього випадку також стосується все сказане в пункті. Перейдемо до "практичних занять". Що ж може на знадобитися. В першу чергу програмне забезпечення.

Приклади я буду приводити для ОС Windows . Встановлення даного пакету звичайне:

tar -fghjio-snmp-7.5.9.tar

gunzip udc-snmp-7.5.9.tar.gz

cd udc-snmp-7.5.9

make

/klkconfigure

Install1

Запуск демона (агента)

Snmpd11

Отже після встановлення нам будуть відкриті так програмні засоби: Snmpget, snmpgetnext, snmptranstat, snmpbulkwalk, snmpcheck, snmptrapd snmptest, snmpnetstat, snmptable, snmpdelta, snmptrap, snmpwalk, snmpstatus, snmpset, snmptable.

Подивимося, як виглядають описані вище операції на практиці. Запит GetRequest реалізує однойменна програма snmpget. Для отримання необхідної інформації виконаємо наступну команду:

root~ #@ darkstar: public system.sysDescr.0 snmpget 10.0.0.2

Сервер повідомляє:

COMPATIBLE - Windows Version 10.0 Software:

system.sysD11= Hardware: 68 Model 51 x86 Family Stepping 0 AT / AT

Припустимо, ми хочемо щось змінити в настройках агента. Проробимо наступну операцію:

root @ darkstar: ~ # snmpset 10.0.0.2 public system.sysContact.0 s

test@test.com і отримаємо відповідь:

system.sysContact.0 = test@test.com

4.8 Опис пакету MRTG

MRTG служить для побудови графіків завантаження каналу, трафіку. Але за допомогою MRTG можна дивитися багато інших речей. Наприклад, можна подивитися, в який час на сервері запускається найбільша кількість процесів http, MySQL і т.д.

MRTG генерує HTML-сторінки із зображеннями у форматі PNG (Portable Network Graphics) для графічного представлення статистики трафіку. Можна сконфігурувати його для моніторингу будь-яких змінних SNMP, наприклад навантаження систем або мережевих інтерфейсів. Найбільш корисним MRTG є для адміністраторів, так як він дає їм можливість контролювати використання мережевих ресурсів. Програма була написана на мові Perl Тобіасом Оутайкером з Національного інституту Данії з досліджень навколишнього середовища в 1994 р. і спочатку призначалася для спостереження за навантаженням каналу, який зв'язує мережу інституту з Інтернет. Пізніше співробітник компанії Cisco Systems Дейв Ренд поліпшив ефективність програмного коду MRTG, написавши для нього модуль на мові C.

Пакет MRTG працює на платформах Unix, Linux і Microsoft Windows. Краще за все він функціонує під керуванням ОС Solaris, Linux, Windows NT, 2000 і XP. MRTG працює наступним чином. Команда GET протоколу SNMP періодично зчитує значення лічильників SNMP, наприклад ifInOctets (OID

1.3.6.1.2.1.2.2.1.10) і ifOutOctets (1.3.6.1.2.1.2.2.1.16), які реєструють число вхідних (ifInOctetes) і вихідних (ifOutOctets) байтів для даного інтерфейсу. Обидва параметра відображаються у вигляді тимчасового графіка в форматі PNG на HTML-сторінці.

Ці параметри можуть відноситися до будь-якого пристрою, від маршрутизатора до сервера.

Дані викреслюються у вигляді графіків двох різних кольорів - за замовчуванням блакитного та зеленого, з відповідними підписами, що відзначають мінімальні, максимальні і середні величини. У підсумку отримується повне уявлення про поточний стан контрольованого пристрою.

MRTG виводить середні значення контрольованих параметрів за тиждень, місяць і рік, обчислювані на основі вимірів з інтервалами 5 хв. Тижневий графік будується на основі півгодинних інтервалів, усереднюючий результати шести послідовних вимірів. Відповідно місячний графік будується за даними за тиждень з інтервалом усереднення 2 год, а річний - за даними за місяць, розподілених кожні 24 год.

ВИСНОВКИ

Метою дипломної роботи була розробка локальної комп'ютерної мережі окремо взятого магазину, що належить до ОАОТ «Дабрабит». Для досягнення поставленої мети були вирішені

наступні завдання:

1) обрана мережева архітектура для комп'ютерної мережі, метод доступу, топологія, тип кабельної системи;

2) обраний спосіб управління мережею;

3) підібрані конфігурації мережевого устаткування - кількість серверів, концентраторів, мережевих принтерів;

4) розроблені рекомендації з управління мережевими ресурсами та користувачами мережі;

5) вивчені питання безпеки мережі;

6) розраховані витрати на створення мережі підприємства.

Була розроблена раціональна, гнучка структурна схема мережі організації, передбачені режими швидкого оновлення оперативної інформації на сервері, а так само опрацьовані питання забезпечення необхідного рівня захисту даних.

На сьогоднішній день розробка і впровадження локальних інформаційних мереж є однією з найцікавіших і важливих завдань в області інформаційних технологій. З'являється потреба у використанні новітніх технологій передачі інформації. Інтенсивне використання інформаційних технологій вже зараз є найсильнішим аргументом в конкурентній боротьбі, що розгорнулася на світовому ринку.

Реалізована технологія Fast Ethernet і Gigabit Ethernet. Робочі станції в різних приміщеннях підключаються до комутатора, що стоїть в кабінеті завідуючої магазином. Для зручності прокладки кабелю і його структуризації використовується структурована кабельна система. Є можливість розширення мережі, тому що у комутатора залишаються незадіяні порти. При необхідності можна передбачити додаткові місця підключення робочих станцій (додаткові

розетки), так що підключення робочих станцій до мережі буде визначатися часом настройки мережевого програмного забезпечення.

Розглянуто проблеми забезпечення безпеки життєдіяльності у відповідності з керівними документами. У ході розробки мережі було розраховано конфігурацію спроектованої локальної мережі, що підтвердила правильність її побудови. Також було оцінено вартість розробленої схеми мережі і проаналізовано варіанти закупівлі необхідного обладнання, розглянуто характеристики мережі, а саме PDV, PVV, швидкість проходження трафіку в каналі (за допомогою пакета MRTG). Також розглянуто налаштування Windows Servera та Nat

На основі всього вищевикладеного, можна зробити висновок, що спроектована мережа є функціонально коректною і надійно захищеною.

Під час створення комп'ютерної мережі можна визначити переваги та недоліки, які виникли під час розробки.

До переваг можна віднести:

1) Мережа з'єднана за допомогою кабелю з пропускною здатністю 100Мбіт/с ;
2) Ефективне виявлення колізій;
3) Підтримка протоколів більшістю програмного забезпечення;
4) Серверне обладнання дуже потужне;
5) Робочі станції обладнанні усім потрібним для роботи ліцензійним програмним забезпеченням;

Але присутні і не значні недоліки:

1) Не дуже легка фізична реалізація мережі;
2) Використання дорогого обладнання і ПЗ;
3) Велика відстань між корпусами і аудиторіями, що потребує велику кількість кабелю та великих затрат коштів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1) Антонов А.О. Особливості впровадження систем електронного документообігу в підрозділах ДСНС України / А.О. Антонов, Н.Є. Бурак //Проблеми та перспективи забезпечення цивільного захисту: матеріали міжнар. наук.-практ. конф. молодих учених. – Харків: НУЦЗ України, 2018. – С. 12.

2) Бобрікова, І. С., & Барабаш, Т. Н. (2018). Особливості взаємодії декількох протоколів маршрутизації у складній комп‘ютерній мережі. Refrigeration Engineering and Technology, 53(6). https://doi.org/10.15673/ret.v53i6.928

3) Бобрікова, І. С., & Барабаш, Т. Н. (2018). Особливості функціонування і налаштувань маршрутизаторів в різних областях дії протоколу динамічної маршрутизації OSPF. Refrigeration Engineering and Technology, 54(1). https://doi.org/10.15673/ret.v54i1.990

4) Вачевський О. Реалізація алгоритмів пошуку найкоротших шляхів та їх практичні відомості застосування / О. Вачевський // Молодь і ринок. - 2014. - №1 - С. 142-148. - Режим доступу: http://nbuv.gov.ua/UJRN/Mir_2014_1_30.

5) Впровадження автоматизованих інформаційно-аналітичних систем в роботу служб доставки товарів / О.О. Смотр, Н.Є. Бурак, Р.Р. Головатий, І.О. Антоненко // Матеріали IX міжнародної школи-семінару «Теорія прийняття рішень». – Ужгород, 2019. – С. 194–195.

6) Голубничий Д.Ю. Порівняльний аналіз методів маршрутизації в інформаційно-телекомунікаційній мережі АСУ авіацією та протиповітряною обороною / Д.Ю. Голубничий, Є.А. Мінаєв, А.О. Мінаєва // Збірник наукових праць Харківського національного університету Повітряних Сил , 2017 .– 4(53) – С. 90-92.

7) Жовтянський М. С. Моделювання проектного середовища впровадження «хмарних сервісів» у вищі навчальні заклади системи цивільного захисту / М. С. Жовтянський, Н. Є. Бурак // Управління проектами, програмами, портфелями : Тези доповідей І Міжнар. наук.-практ. конф.: [у 2т.]. – Одеса, 2016.– Том 1. – С. 54–56.

8) . Ирвин Дж. Передача данных в сетях: инженерный подход / Дж. Ирвин, Д. Харль. – СПб.: БХВ-Петербург, 2003. – 448 с.

9) Киричик Б.М. Аналіз методів підвищення продуктивності комп'ютерної мережі / Б.М. Киричик, Н.Є. Бурак // Захист інформації в інформаційно-комунікаційних системах: Зб. тез доповідей III Всеукр. наук.- практ. конф. молодих вчених, курсантів та студентів. – Львів: ЛДУ БЖД, 2019. – С. 223-225.

10) Комп'ютерні мережі : навчальний посібник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.] – Вінниця : ВНТУ, 2013. – 371 с.

11) Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. – Львів: «Магнолія 2006», 2013. – 256 с.

12) Лосев Ю. І. Комп'ютерні мережі: навчальний посібник / Ю. І. Лосев, К. М. Руккас, С. І. Шматков / За редакцією Ю. І. Лосева. – Х. : ХНУ імені В. Н.Каразіна, 2013. – 248 с.

13) Національна стратегія розвитку освіти в Україні на 2012–2021 роки. [Електронний ресурс]. Режим доступу: http://www.mon.gov.ua/images/files/news/12/05/4455.pdf

14) Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы [Текст] / Н.А. Олифер, В.Г. Олифер. – СПб.: Питер, 2012. – 944 с.

15) Палмер М. Проектирование и внедрение компьютерных сетей / М.Палмер, Р. Синклер. – СПб.: БХВ-Петербург, 2004. – 752с.

16) Пахомова В. М. Можливості модернізації комп'ютерної мережі інформаційно-телекомунікаційної системи Придніпровської залізниці / В. М. Пахомова // Інформаційно-керуючі системи на залізничному транспорті. – 2015.– № 5. – С. 32-38. – Режим доступу: http://nbuv.gov.ua/UJRN/Ikszt_2015_5_7.

17) Про Національну програму інформатизації : Закон України від 04 лютого 1998 р. №74/98-ВР. – Режим доступу : http://zakon.rada.gov.ua

18) Про охорону праці № 2694-XII: Закон України від 14 жовтня 1992 року із змінами та доповненнями у редакція від 05.12.2019 – Режим доступу : http://zakon.rada.gov.ua

19) Рак Ю.П. Формування проектів методом візуалізації інформації для підвищення стану безпеки торгово-розважальних центрів / Ю.П. Рак, Р.Р.

Головатий // Управління проектами у розвитку суспільства: зб. тез доповідей XII Міжнар. конф. – Київ: КНУБА, 2015. – С. 226 – 228.

20) Черкасов Д. І. Маршрутизація в мережі сучасного підприємства / Д. І.Черкасов // Наукові записки НаУКМА. Комп'ютерні науки. - 2016. - Т. 190. - С. 46-51. - Режим доступу: http://nbuv.gov.ua/UJRN/NaUKMAkn_2016_190_11.

21) Чмир П.О. Оптимізації ресурсів комп’ютерних лабораторій навчальних закладів шляхом використання термінального сервера / П.О. Чмир, Н.Є. Бурак // Проблеми та перспективи розвитку системи безпеки життєдіяльності: Зб. наук. праць XIV Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів. – Львів: ЛДУ БЖД, 2019. – С. 240-241.

22) Cisco - Україна [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/uk_ua/index.html

23) Cisco Networking Academy [Електронний ресурс]. – Режим доступу: https://www.netacad.com/

24) Patel, Brijesh & Bhatt, Priyang. (2013). Wireless Networks Simulation with Assessment in PT Software. International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169. Volume: 1. 870-875.

25) Smotr, O., Burak, N., Borzov,Yu., Ljaskovska, S.:Implementation of Information Technologies in the organization of Forest Fire Suppression Process. In: Proceedings of the 2018 IEEE Second International Conference on Data StreamMining & Processing (DSMP), pp. 157-161. Lviv, Ukraine, August 21-25, 2018

Мережа 4-го корпусу
Оптоволокно
5-й поверх
4-й поверх
3-й поверх
2-й поверх
1-й поверх
4-304
Switch 8
Switch 16

UNICHECK

User name:
Кафедра кибербезпеки

Check ID:
1008321739

Check date:
17.06.2021 15:52:52 EEST

Check type:
Doc vs Internet

Report date:
17.06.2021 15:54:48 EEST

User ID:
100005590

File name: Блаута диплом_пл

Page count: **69** Word count: **16607** Character count: **124862** File size: **1.31 MB** File ID: **1008393615**

4.7% Matches

Highest match: **2.44%** with Internet source (**https://uadoc.zavantag.com/text/18809/index-10.html**)

4.7% Internet sources	33	Page 1

No Library search was conducted

0% Quotes

Exclusion of quotes is off

Exclusion of references is off

0% Exclusions

No exclusions

Modifind

Text modifications detected. Find more details in the online report.

Replaced characters	1

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 5.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 9%**

ID: 94569 Название: Система авторизації користувачів на основі серверу LDAP Добавлено в БД: 2021-06-17 Авторы: Блаута Вадим Віталійович Руководители: Кльоц Ю.П. Консультанты: Опоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	105093	907	19657 (6%)	189 (6%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА СИСТЕМНОГО ПРОГРАМУВАННЯ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система авторизації користувачів на основі серверу LDAP

Автор: Блаута Вадим Віталійович

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Кльоц Ю.П., к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-30 джерелами на один фрагмент речення;
4) в якості запозичень в окремих місцях системою зафіксовано набори команд налаштування обладнання, що є типовими для налаштування мережевого обладнання і не можуть розглядатися як об'єкт авторських прав і, відповідно, їх порушення;
5) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 6.26% і адресується до 401 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Ю.П. Кльоц

Гарант ОП _____ С.М. Лисенко

Завідувач кафедри КБКСМ _____ Ю.П. Кльоц