UNICHECK

Ім'я користувача:
приховано налаштуваннями конфіденційності

ID перевірки:
1015521887

Дата перевірки:
09.06.2023 10:26:43 EEST

Тип перевірки:
Doc vs Library

Дата звіту:
09.06.2023 10:43:25 EEST

ID користувача:
100011372

Назва документа: **Кіналь М.П. гр ТК-330**

Кількість сторінок: 23 **Кількість слів:** 4348 **Кількість символів:** 33275 **Розмір файлу:** 350.99 KB **ID файлу:** 1015175984

25.8%
Схожість

Найбільша схожість: **24.5%** з джерелом з Бібліотеки (ID файлу: **1002842243**)

Пошук збігів з Інтернетом не проводився

25.8% Джерела з Бібліотеки **89** ..... **Сторінка** 25

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

1 ХАРАКТЕРИСТИКА ОБ'ЄКТУ ПРОЄКТУВАННЯ

1.1 Комп’ютерна мережа

Локальна комп'ютерна мережа (Local Area Network, LAN) є мережею, яка об'єднує комп'ютери та інші пристрої, розташовані на обмеженій території, наприклад, в магазині, будинку, офісі або невеликому кампусі. Локальні мережі зазвичай мають невелику площу і обмежену кількість пристроїв.

В локальних мережах комп'ютери підключаються один до одного або до спільних пристроїв, таких як сервери файлів або принтери, за допомогою фізичних кабелів або бездротових з'єднань. Часто використовуються Ethernet-кабелі або Wi-Fi-технологія для забезпечення зв'язку між пристроями.

У локальних мережах комп'ютери можуть обмінюватися даними, спільно використовувати ресурси (наприклад, друкуючі пристрої або інтернет-з'єднання), запускати спільні програми і виконувати інші мережеві операції. Локальні мережі зазвичай є приватними і контролюються власниками, що дозволяє забезпечити безпеку та обмеження доступу до мережевих ресурсів.

Глобальна комп'ютерна мережа (Wide Area Network, WAN), у свою чергу, охоплює більші території і з'єднує локальні мережі між собою через розподілені географічно області. Прикладом глобальної комп'ютерної мережі є Інтернет, що об'єднує мільйони комп'ютерів і пристроїв у всьому світі.

На (рис. 1.1), як ви згадували, може бути зображено приклад побудови локальної мережі, де комп'ютери підключені до спільного комутатора (switch), який забезпечує зв'язок і передачу даних між пристроями у мережі. Також на рисунку можуть бути показані інші пристрої, такі як сервери, маршрутизатори або принтери, які можуть бути доступні для використання в мережі.

Рисунок 1.1 – Приклад побудови локальної мережі

Глобальна мережа, така як Інтернет, об'єднує комп'ютерні мережі та окремі комп'ютери з усього світу. Вона забезпечує передачу даних між різними комп'ютерами та дозволяє доступ до різноманітних ресурсів та послуг.

Класифікація комп'ютерних мереж, яку ви навели, є досить широко використовуваною і допомагає організувати мережі залежно від їхнього масштабу, призначення, топології, середовища передачі та протоколів.

LAN (Local Area Network) – це локальна мережа, яка зосереджена на обмеженій території, зазвичай не більше 1-2 км. Локальні мережі побудовані з використанням швидкого з'єднання, такого як ефірний кабель або бездротові технології, і забезпечують швидкий обмін даними між підключеними пристроями. Вони широко використовуються в домашніх мережах, офісах, навчальних закладах тощо.

WAN (Wide Area Network) – це глобальна або регіональна мережа, яка охоплює великі території, такі як країни або континенти. WAN використовує різноманітні засоби передачі даних, включаючи телефонні лінії, оптоволоконні кабелі, супутникові зв'язки та інші. Інтернет є прикладом глобальної WAN, яка з'єднує комп'ютери з усього світу.

MAN (Metropolitan Area Network) – це мережа, яка охоплює міську територію. MAN знаходиться між LAN і WAN за своїми розмірами. Вони можуть

використовувати високошвидкісні засоби зв'язку, такі як оптоволоконні кабелі, для забезпечення швидкої передачі даних в межах міста.

Абонент, сервер і клієнт є важливими поняттями в мережевій теорії. Абонент – це пристрій, підключений до мережі і активно бере участь у передачі даних. Сервер – це абонент, який надає ресурси іншим абонентам в мережі, виконуючи роль централізованої системи. Клієнт – це абонент, який використовує ресурси сервера без надання своїх ресурсів.

Ці поняття використовуються для опису ролей та взаємодії між різними пристроями в мережі і є основою багатьох мережевих архітектур і моделей.

Дана класифікація та термінологія надалі еволюціонували і розширилися з розвитком технологій та мережевих стандартів. Проте, основні принципи і концепції залишаються актуальними для розуміння структури та функціонування комп'ютерних мереж

1.2 Віртуальна приватна мережа (virtual private network, VPN)

Віртуальна приватна мережа (VPN) дійсно дозволяє розширити приватну мережу і забезпечується з'єднанням двох комп'ютерів через загальнодоступну мережу, таку як Інтернет. Її ціль полягає в тому, щоб створити приватне підключення "точка-точка" між цими комп'ютерами, яке імітує безпечне і приватне з'єднання, незалежно від фактичної фізичної мережі, через яку вони підключені.

Для створення цього приватного з'єднання, дані, які потрібно передати, упаковуються в пакети, які містять заголовки з інформацією про маршрутизацію. Ця інформація допомагає данним дійти до свого призначення через загальнодоступну мережу. Крім того, для забезпечення безпеки дані шифруються. Шифрування забезпечує захист від перехоплення пакетів в загальнодоступній мережі, оскільки їх не можна розшифрувати без належних шифрувальних ключів. Таке з'єднання, де приватні дані інкапсулюються і шифруються, називається віртуальним приватним підключенням або VPN-підключенням.

Користувачі, які працюють вдома або перебувають у дорозі, можуть використовувати VPN-підключення для встановлення віддаленого з'єднання з сервером організації через загальнодоступну мережу, таку як Інтернет. З точки зору користувача, VPN-підключення виглядає як безпосереднє приватне з'єднання "точка-точка" між його комп'ютером (клієнтом VPN) і сервером організації (сервером VPN). Інфраструктура загальнодоступної мережі, через яку відбувається передача даних, не має значення, оскільки логічно дані передаються через приватне підключення.

Організації також можуть використовувати VPN-підключення для забезпечення зв'язку між географічно розташованими відділеннями або для підключення до серверів інших організацій через загальнодоступні мережі з підтримкою безпечного зв'язку. Роутинговані VPN-підключення через Інтернет логічно виглядають як виділені підключення через глобальну мережу (виділені WAN-підключення)

Технологія VPN (віртуальної приватної мережі) дозволяє забезпечити безпеку та захист інформації при передачі через ненадійні мережі, такі як Інтернет. Вона дозволяє об'єднати розподілені філії організації в єдину захищену мережу або надати віддалений доступ до корпоративних ресурсів.

VPN можна класифікувати за типом використовуваного середовища:

– Захищені VPN: Найпоширеніший тип VPN, який дозволяє створити надійну та захищену підмережу на основі ненадійної мережі, зазвичай, Інтернету. Протоколи, які використовуються для захищених VPN, включають IPsec, SSL та PPTP.

– Довірчі VPN: Використовуються в ситуаціях, коли середовище передачі даних вважається надійним, і головною метою є створення віртуальної підмережі в рамках більшої мережі. Прикладами довірчих VPN є Multi-protocol label switching (MPLS) і Layer 2 Tunnelling Protocol (L2TP).

Захист інформації в VPN включає такі аспекти:

– Шифрування (encryption): Інформація, передана через VPN, шифрується, тобто кодується таким чином, що лише володар ключа може розкодувати її. Популярні алгоритми шифрування включають DES, Triple DES і AES.

– Підтвердження справжності (authentication): Перевірка цілісності даних та ідентифікація осіб та об'єктів, задіяних у VPN. Популярні алгоритми перевірки цілісності даних включають MD5 і SHA1.

– Контроль доступу (access control): Керування пріоритетами використання пропускної здатності VPN для різних мережевих додатків.

2 ПОСТАНОВКА ЗАВДАННЯ НА РОЗРОБКУ

2.1 Вибір компонентів мережі

VPN – це технологія, яка дозволяє створити безпечне з'єднання між двома або більше пристроями або мережами через незахищену мережу, таку як Інтернет. Вона створює логічну мережу поверх існуючих мереж і використовує шифрування для захисту передаваних даних.

За допомогою VPN можна об'єднати географічно віддалені мережі організації в єдину віртуальну мережу. Це дозволяє співробітникам доступатися до ресурсів організації, як якби вони знаходилися в одній фізичній мережі. Використання непідконтрольних каналів, таких як Інтернет, для зв'язку між вузлами VPN забезпечує гнучкість і можливість підключення з будь-якого місця.

Одним з ключових аспектів VPN є його здатність забезпечити безпеку передавання пакетів даних через загальнодоступні мережі. Шифрування даних забезпечує конфіденційність та захист інформації від несанкціонованого доступу. Це робить VPN популярним інструментом для захисту конфіденційної і комерційної інформації, особливо при використанні відкритих мереж, таких як громадські Wi-Fi точки доступу.

Загалом, VPN є потужним інструментом для забезпечення безпеки та приватності під час передачі даних через незахищені мережі, а також для з'єднання географічно розташованих мереж в єдину мережу.

1С: Бухгалтерія є програмним комплексом, розробленим компанією 1С для автоматизації бухгалтерського обліку і фінансового управління. Вона надає можливість вести різні типи бухгалтерського обліку, включаючи облік доходів і витрат, фінансовий облік, податковий облік, заробітну плату, складський облік та інше.

1С: Бухгалтерія має широкі функціональні можливості і може бути настроєна під потреби конкретної організації. Вона забезпечує автоматизацію процесів обліку, звітності, контролю фінансових операцій і допомагає забезпечити

дотримання законодавчих вимог щодо бухгалтерського обліку.

Програмний комплекс 1С: Бухгалтерія є популярним і широко використовується в багатьох організаціях різного розміру і сфери діяльності. Він забезпечує зручний і ефективний спосіб ведення обліку та аналізу фінансових показників.

Рисунок 2.1 – Вигляд програми 1С бухгалтерія

1С: Бухгалтерія забезпечує рішення для широкого спектру задач, що стоять перед бухгалтерською службою підприємства. Основна функція програмного комплексу полягає в обліку фінансових операцій, включаючи виписку первинних документів, облік продажів, покупок, заробітної плати, складського обліку та інших операцій.

1С: Бухгалтерія має можливість інтеграції з іншими системами підприємства, що дозволяє співробітникам суміжних служб вводити інформацію про окремі види діяльності, торгові або виробничі операції. Це означає, що необхідна інформація може бути внесена співробітниками з інших відділів підприємства, які не є бухгалтерами.

У такому випадку, бухгалтерська служба виконує методичне керівництво і контроль за налаштуваннями інформаційної бази, яка забезпечує автоматичне

відображення документів в бухгалтерському і податковому обліку. Це дозволяє забезпечити збалансованість і точність фінансової звітності, а також виконання податкових вимог.

2.2 Вибір клієнтської частини

В комп'ютерній термінології термін "сервер" використовується для посилання на окремий комп'ютер або програму, які надають певні послуги і виконують завдання без втручання людини.

Сервер як фізичний комп'ютер зазвичай знаходиться в локальній або глобальній мережі і надає ресурси і послуги користувачам. Він працює автономно і може працювати цілодобово для задоволення потреб користувачів. Такий сервер може бути сервером баз даних, файловим сервером, поштовим сервером, сервером друку, веб-сервером, ігровим сервером або іншим типом сервера в залежності від послуг, які він надає.

Сервер як програма також надає послуги іншим програмам, відомим як клієнти. Цей тип сервера зазвичай працює на серверному комп'ютері або віртуальній машині і обробляє запити від клієнтських програм через мережу. Часто комунікація між клієнтом і сервером відбувається за допомогою передачі повідомлень через мережу з використанням певного протоколу.

Загальне призначення сервера полягає в наданні обчислювальних ресурсів і послуг іншим комп'ютерам або програмам у мережі. Він може бути центром обробки даних і надавати доступ до ресурсів, обслуговувати запити користувачів і забезпечувати виконання певних служб. Сервери можуть бути використані в корпоративних мережах або доступні через Інтернет для громадських користувачів.

У випадку фізичних серверів, продуктивність залежить від комп'ютера, який використовується в якості сервера. Існує можливість вибору готових серверів, запропонованих виробниками, або можна зібрати сервер самостійно, враховуючи потреби і вимоги. Розмаїтість компонентів і можливостей збірки дозволяє вибрати

найкращі компоненти для покращення продуктивності сервера.

Важливо враховувати потреби і вимоги до сервера, а також вибирати компоненти, які забезпечують найкращу продуктивність. Професійні адміністратори серверів з вищою кваліфікацією можуть встановлювати, налаштовувати і обслуговувати сервери для забезпечення надійної роботи і виконання потрібних завдань

Конфігурація сервера, має належні можливості для виконання вказаних функцій. Процесор AMD Opteron 6380 з 16 ядрами і частотою 2,5 ГГц, разом з великою кількістю кеш-пам'яті, забезпечує достатню потужність обчислень для обробки завдань сервера.

Материнська плата Hewlett Packard 990XTTs-aQ також підтримує потрібні функції і відповідає вимогам для серверної роботи. За потреби можна вибрати відповідний форм-фактор (4 c3000 або 2 c1000) залежно від розміру і масштабів вашої організації.

Що стосується пам'яті, дві модулі PC3-10600 Registered DDR3-1333 дадуть достатню кількість оперативної пам'яті для обробки завдань сервера.

Чотири вінчестера Western Digital Caviar Black є добрим вибором для забезпечення простору зберігання даних і обробки дій з файлами.

Мережева карта з чотирма портами 1Гб/с NC551i FlexFabric забезпечить швидку мережеву комунікацію і можливість маршрутизації даних в мережі.

Стосовно робочих станцій для співробітників магазинів, наведена конфігурація також має відповідні можливості. Процесор AMD FX-6350 разом з відеокартою AMD Radeon R7 260X надасть достатню продуктивність для роботи з програмами і виконання завдань.

Материнська плата, оперативна пам'ять і вінчестер також відповідають потребам робочих станцій і забезпечать швидку та надійну роботу.

Щодо джерела безперебійного живлення Chieftec CTG-750C, його потужність і захист від різних перешкод дозволяють забезпечити стабільне живлення і захист від можливих проблем з електропостачанням.

У кінцевому підсумку, наведена конфігурація сервера і робочих станцій

виглядає придатною для виконання описаних функцій і може задовольнити потреби організації.

RAID (англ. redundant array of independent/inexpensive disks) – надлишковий масив незалежних/недорогих дисків для комп'ютера. Дисковий масив — це набір дискових пристроїв, що працюють разом, щоб підвищити швидкість і/або надійність системи вводу/виводу. Цим набором пристроїв керує спеціальний RAID-контролер (контролер масиву), який забезпечує функції розміщення даних по масиву; а для решти всієї системи дозволяє представляти весь масив як один логічний пристрій вводу/виводу. За рахунок паралельного виконання операцій читання і запису на кількох дисках, масив забезпечує підвищену швидкість обмінів в порівнянні з одним великим диском.

Масиви також можуть забезпечувати надмірне зберігання даних, з тим, щоб дані не були втрачені у разі виходу з ладу одного з дисків. Залежно від рівня RAID, проводиться або дзеркалювання або розподіл даних по дисках.

RAID 0: Технологія розподілу даних (data striping) без надмірності. Забезпечує підвищену пропускну здатність та зниження латентності. Однак, немає надійності в разі виходу з ладу одного диска.

RAID 1: Технологія дзеркалювання (disk mirroring) з надмірністю. Копії даних зберігаються на різних дисках, що забезпечує високу надійність. Продуктивність читання може бути покращена. Час запису трохи збільшується.

RAID 2 і 3: Технології з паралельним доступом до дисків і зберіганням бітів парності. RAID 2 використовує кілька дисків для зберігання парності, тоді як RAID 3 використовує лише один. Відновлення даних можливе в разі виходу з ладу диска. Велика продуктивність для великих обсягів даних, але скромна для малих обсягів.

RAID 4 і 5: RAID 4 використовує великі сегменти даних з окремим диском для зберігання парності. RAID 5 розподіляє інформацію парності по всіх дискам. Обидва рівні забезпечують як читання, так і запис даних, і мають покращену продуктивність для невеликих обсягів даних.

Таблиця 2.1 – Переваги і вади рівнів RAID

Рівень RAID	Механізм забезпечення надійності	Ефективна місткість масиву	Продуктивність	Область застосування
0	–	100%	висока	застосування без істотних вимог до надійності
1	дзеркалювання	50%	висока або середня	застосування без істотних вимог до вартості
3	парність	80%	середня	застосування для роботи з великими обсягами даних (графіка, CAD/CAM тощо)
5	парність	80%	середня	застосунки, що працюють з невеликими обсягами даних (обробка транзакцій)
10	дзеркалювання групи RAID 0	50%	висока або середня	застосунки, що вимагають надійності RAID 1 з хорошою продуктивністю

Комбіновані і додаткові рівні RAID

– RAID Levels 0+1 (Рівень 0+1): Комбінація RAID 0 і RAID 1. Цей рівень забезпечує надмірність за рахунок дзеркалювання.

– RAID Levels 10 (Рівень 10): Комбінує (об'єднує) RAID 0 і RAID 1, тобто дзеркалювання групи дисководів, об'єднаних в RAID 0 для забезпечення максимальної швидкодії. Цей рівень забезпечує надмірність за рахунок дзеркального відображення.

– RAID Levels 30 (Рівень 30): Комбінує (об'єднує) RAID 0 і RAID 3, тобто використовується контрольна сума для групи дисководів, об'єднаних в RAID 0 для забезпечення максимальної швидкодії. Інформація про парність може використовуватися для відновлення даних.

– RAID Levels 50 (Рівень 50): Комбінує (об'єднує) RAID 0 і RAID 5, тобто використовується переміщувана контрольна сума для групи дисководів, об'єднаних в RAID 0 для забезпечення максимальної швидкодії. Інформація про парність може використовуватися для відновлення даних.

2.3 Вибір комунікаційного обладнання

Основні ключові принципи Інтернету включають:

– Децентралізація: Інтернет є децентралізованою мережею, що означає, що він не має одного центрального вузла контролю. Замість цього, він складається з багатьох мереж, які взаємодіють і обмінюються даними.

– Протокол IP: Інтернет працює на базі протоколу IP (Internet Protocol), який визначає формат та адресацію пакетів даних. Протокол IP дозволяє ідентифікувати та маршрутизувати пакети даних відправника до отримувача через різні мережі.

– Маршрутизація: Мережеві маршрутизатори відповідають за перенаправлення пакетів даних через мережі Інтернету. Вони використовують інформацію з IP-адрес пакетів для визначення найкоротшого шляху до призначення.

– Єдиний адресний простір: Протокол IP забезпечує унікальність IP-адрес для кожного пристрою у мережі. Це дозволяє маршрутизаторам однозначно визначати, куди направити пакет даних, щоб він дістався до свого призначення.

– Відкритість і доступність: Інтернет заснований на відкритих стандартах, що дозволяє різним мережам і пристроям взаємодіяти між собою. Це стимулює інновації, співпрацю та доступність інформації для всіх користувачів.

– Розділення послуг: Інтернет розділяє транспорт даних та послуги, що надаються над ним. Незалежно від типу даних (передача файлів, електронна пошта, веб-сторінки тощо), вони можуть передаватися по спільній інфраструктурі Інтернету.

– Розширюваність: Інтернет розроблений з урахуванням можливості розширення мережі. Завдяки гнучкій архітектурі та протоколам, нові мережі можуть приєднуватися до Інтернету, розширюючи його покриття та збільшуючи доступність.

Ці принципи допомагають забезпечити глобальну сполучність, комунікацію та обмін інформацією в Інтернеті.

Протокол IP був розроблений та стандартизований в рамках роботи групи IETF (Internet Engineering Task Force). IETF є організацією, яка займається розвитком та стандартизацією протоколів Інтернету. Група складається з відкритих для публічної участі експертів, які спільно працюють над вирішенням різних проблем та задач, пов'язаних з проектуванням Інтернету.

Одним з результатів роботи IETF є документи RFC (Request for Comments), які містять технічні специфікації та інструкції щодо протоколів та технологій Інтернету. Ці документи є відкритими для обговорення та публічного висвітлення. Деякі з них, після визнання його придатними та стабільними, можуть бути прийняті IAB як стандарти Інтернету, відомі як "Internet Standards".

Організація IAB (Internet Architecture Board) відіграє роль в рамках IETF, сприяючи розвитку архітектури Інтернету і координуючи стандартизацію. Вона відповідає за огляд та затвердження документів RFC в якості стандартів Інтернету.

IETF, IAB та інші організації, такі як Internet Society (ISOC), яка включає в себе IETF, працюють разом для розвитку та підтримки Інтернету, створюючи організаційну основу для дослідницьких та консультативних груп, що займаються різними аспектами розвитку мережі

2.4 Вибір прикладного програмного забезпечення

"1С:Бухгалтерія-Проф." є універсальною бухгалтерською програмою, яка є розширеною версією "1С:Бухгалтерії", найбільш поширеної бухгалтерської програми. Вона надає багато можливостей для налагодження і ведення бухгалтерського обліку відповідно до потреб підприємства, з урахуванням змін у законодавстві та форм звітності.

Основні особливості "1С:Бухгалтерія-Проф." включають:

– синтетичний і аналітичний облік, що відповідає потребам підприємства;

– кількісний і багатовалютний облік;

– генерація необхідних звітів і документів по синтетичному і аналітичному

обліку;

– повна налагоджуваність, що дозволяє змінювати план рахунків, систему проводок, налаштування аналітичного обліку, форми первинних документів та форми звітності.

– можливість автоматичного друку вихідних (первинних) документів.

Програма "1С:Бухгалтерія-Проф." пропонує зручність в роботі, швидкість проведення операцій та легкість освоєння. Вона дозволяє вести облік для однієї організації на кількох комп'ютерах або на одному комп'ютері для декількох організацій.

Окрім синтетичного обліку, програма "1С:Бухгалтерія-Проф." надає можливість вести аналітичний облік. Аналітичний облік дозволяє простежувати розрахунки з конкретними покупцями та постачальниками, враховувати наявність і рух товарів і основних засобів, виконувати договори, розраховувати зарплату та робити розрахунки з підзвітними особами тощо.

Програма "1С:Бухгалтерія-Проф." також надає різноманітні сервісні можливості, які полегшують роботу користувача. До таких можливостей належать система контекстної допомоги, меню дій, можливість ведення страхових копій інформації, засоби ведення архіву текстових документів, вбудований текстовий редактор, калькулятор, підтримка миші та інші.

Загалом, "1С:Бухгалтерія-Проф." є потужною програмою, яка забезпечує багато функціональних можливостей для ведення бухгалтерського обліку на різних типах підприємств.

2.5 Опис фізичної та логічної структури мережі

VPN (Віртуальна приватна мережа, англ. Virtual Private Network) – це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією.

VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

Структура VPN

VPN (Virtual Private Network) складається з двох частин: внутрішньої (підконтрольної) мережі і зовнішньої мережі, через яку проходять зашифровані з'єднання. Внутрішня мережа може складатися з декількох частин, а зовнішня мережа зазвичай є загальнодоступним Інтернетом.

При підключенні до VPN віддаленого користувача використовується сервер доступу, який підключений до внутрішньої та зовнішньої мережі. Під час підключення сервер доступу вимагає ідентифікації та аутентифікації віддаленого користувача. Після успішної ідентифікації та аутентифікації віддалений користувач отримує повноваження для роботи в мережі, що означає процес авторизації.

Одним з ключових елементів VPN є VPN-тунель, який є каналом типу точка-точка, створеним в незахищеній мережі, такій як Інтернет. Кожен вузол відповідає за шифрування даних перед відправкою їх у тунель і розшифрування після виходу з тунелю. VPN-тунелі можуть бути встановлені між різними вузлами, і для кожного тунелю може бути використаний один і той самий VPN-шлюз.

VPN-шлюз виконує роль посередника між внутрішньою та зовнішньою мережею. Він полегшує управління політикою безпеки та контроль вхідного та вихідного трафіку мережі. Користувачі встановлюють з'єднання з VPN-шлюзом, і після цього отримують доступ до мережі.

У VPN використовуються тунелі з режимом шифрування, де шифрується весь пакет IP, до якого додається новий IP-заголовок.

Зазвичай, при створенні VPN, використовують підключення типу точка-точка до певного сервера, або установку ethernet-тунелю з певним сервером, при якій тунелю призначають певну підмережу. Сервер VPN при цьому виконує функції маршрутизації та фільтрування трафіку для доступу до локальної мережі через VPN.

При використанні такого підходу ми все ще маємо можливість фільтрувати трафік на підставі способу підключення але виключається необхідність налаштування маршрутизації, а віддалені машини включаються прямо в локальну мережу, бачать ресурси, навіть здатні використовувати широкосмугові посилки взагалі без додаткового налаштування. Через такий VPN у них відображаються всі комп'ютери локальної мережі Windows, всі доступні XDMCP-сервери при XDMCP broadcast.

Рисунок 2.2 –Загальна структура VPN-сервера

3 ПОБУДОВА СТРУКТУРИ МЕРЕЖІ

3.1 Принципова схема топології мережі та схема логічної структури мережі

Зазвичай топологія мережі використовується для локальних мереж (LAN), де структура з'єднань може бути легко встановлена і керована.

У глобальних мережах, таких як Інтернет, структура з'єднань є більш складною і не відома користувачам. Кожен сеанс зв'язку в глобальній мережі може проходити різним шляхом через різні мережні вузли і маршрутизатори. Така мережева топологія називається логічною топологією, оскільки вона не пов'язана з фізичним розташуванням комп'ютерів, а лише з логічними шляхами передачі даних.

Топологія мережі має значний вплив на вимоги до обладнання, типи кабелю, методи керування обміном даних, надійність роботи мережі та її можливості розширення. Кожна топологія має свої переваги і недоліки, і вибір конкретної топології залежить від потреб і вимог конкретної мережі.

Топологія визначає вимоги до устаткування, тип використовуваного кабелю, можливі й найбільш зручні методи керування обміном, надійність роботи, можливості розширення мережі.

Існує три основних топології мережі:

– шина (bus), при якій всі комп’ютери паралельно підключаються до однієї лінії зв’язку й інформація від кожного комп’ютера одночасно передається всім іншим комп’ютерам (рис. 3.1);

– зірка (star), при якій до одного центрального комп’ютера приєднуються інші периферійні комп’ютери, причому кожний з них використовує свою окрему лінію зв’язку (рис. 3.2);

– кільце (ring), при якій кожний комп’ютер передає інформацію завжди тільки одному комп’ютеру, наступному в ланцюжку, а одержує інформацію тільки від попереднього комп’ютера в ланцюжку, і цей ланцюжок замкнутий в «кільце»

(рис. 3.3).

Рисунок 3.1 – Мережна топологія «шина»

Рисунок 3.2 – Мережна топологія «зірка»

Рисунок 3.3 – Мережна топологія «кільце»

Так, топологія зірки дійсно має свої особливості. Основні характеристики топології зірки включають наступне:

Централізована структура: В топології зірки є явно виділений центральний вузол, до якого підключаються всі інші вузли. Центральний вузол може бути сервером, комутатором або концентратором. Всі комунікації відбуваються через центральний вузол.

Висока надійність периферійних вузлів: В периферійних вузлах (клієнтах) мережі зазвичай використовуються менш потужні комп'ютери або пристрої. В разі відмови одного з периферійних вузлів або його мережного обладнання, це не впливає на роботу інших вузлів мережі.

Залежність від центрального вузла: У разі відмови центрального вузла мережі (наприклад, сервера) вся мережа стає непрацездатною. Тому важливо приділяти особливу увагу надійності центрального вузла і забезпечувати резервні канали зв'язку або механізми відновлення для забезпечення безперебійної роботи мережі.

Менша вразливість до конфліктів: Топологія зірки зменшує можливість виникнення конфліктів в мережі, оскільки комунікація відбувається через центральний вузол. Це спрощує управління мережею і знижує ймовірність колізій даних.

Однак, варто враховувати, що топологія зірки має свої обмеження. Залежність від центрального вузла може створювати одиничну точку відмови, і в разі його відмови мережа стає непрацездатною. Також, використання багатошляхових каналів для забезпечення високої доступності може збільшити складність і вартість мережі.

На практиці можуть використовуватися комбінації базових топологій, наприклад, мережа зірки з розподіленою підтримкою (star-bus) або зірка зі з'єднаними центральними вузлами (extended star). Вибір топології залежить від потреб, обмежень і вимог конкретної мережі. На рис.3.4 зображено структуру схеми мережі п'яти магазинів згідно технічного завдання на дипломну роботу.

Рисунок 3.4 – Схема мережі магазинів

3.2 Маршрутизація

Маршрутизація VPN (Virtual Private Network) відноситься до процесу визначення шляху передачі даних між вашим комп'ютером і сервером VPN. При підключенні до VPN створюється шифрований тунель, через який протікає обмін даними. Маршрутизація VPN визначає, які мережеві шляхи використовуються для передачі даних від вашого комп'ютера до сервера VPN і назад.

Коли ви підключаєтесь до VPN-сервісу, маршрутизація VPN встановлює таблицю маршрутизації на вашому комп'ютері. Ця таблиця містить інформацію про IP-адреси мереж та вузлів, маски підмереж, шлюзів і метрики. Метрика вказує на пріоритет або відстань до певного шляху. Чим менше значення метрики, тим

пріоритетніший шлях.

При передачі даних через VPN, пакети даних відправляються з вашого комп'ютера через шифрований тунель до сервера VPN. Сервер VPN розшифровує пакети і пересилає їх до призначеного сервера або мережі. Зворотний шлях працює аналогічно: пакети від сервера або мережі надсилаються через сервер VPN, шифруються і передаються до вашого комп'ютера.

При використанні VPN2+ (якщо такий сервіс надається), ваш маршрут буде проходити через два сервера VPN. Другий сервер не буде знати вашої реальної IP-адреси, а побачить лише IP-адресу першого сервера. Це додатково забезпечує анонімність, але може призвести до деякого збільшення часу на передачу даних через два сервери.

Загалом, маршрутизація VPN дозволяє забезпечити безпеку та конфіденційність вашого інтернет-трафіку, шляхом шифрування і використання безпечного тунелю

3.3 Налаштування сервісів даної мережі

Підключення до VPN віддаленого користувача робиться за допомогою сервера доступу, який підключений як до внутрішньої, так і до зовнішньої (загальнодоступною) мережі. При підключенні віддаленого користувача (або при установці з'єднання з іншою захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів, віддалений користувач (віддалена мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації.

Налаштування інтернету за допомогою VPN

На комп’ютерах (далі – машини), необхідно налаштувати спеціальне VPN з’єднання. У загальних рисах це включає в себе конфігурування імені ви-пі-ен сервера, його адреси та пароля, необхідного для успішного коннекта. Але ж все ОС різні! Розглянемо найпопулярніші з використовуваних.

Налаштування VPN підключення в Windows 10

– Пуск – Панель управління – Центр мережних підключень і спільного доступу.

– Зліва знайдіть «установка підключення або мережі», натисніть.

– «Підключення до робочого місця», тиснемо «Далі».

– На чемний питання системи відповідаємо: «Ні, створити нове підключення» і натискаємо «Далі».

– Клікаємо по «Використовувати моє підключення до Інтернету». З підключенням визначимося пізніше, вибираємо пункт «відкласти рішення». Press «Далі» button.

– В поле «адреса» вводимо ім'я (або адресу!) вашого VPN-сервера. В поле «ім'я» вводимо прийнятне для вас назву майбутнього з'єднання.

– Дозволяємо (або забороняємо) іншим користувачем локальної машини підключення через створене з'єднання. Галочка «Дозволити використовувати це підключення іншим користувачам». Я заборонив, тобто галочку знімав.

– Вводимо логін і пароль для підключення до віртуальної приватної мережі. Допоможе вам ваш провайдер (XP-шники не з чуток знають, хто це) або системний адміністратор.

– Тиснемо «створити».

Готово! Ви можете розмістити ярлик вашого VPN з'єднання на робочому столі, для цього виведіть його контекстне меню (клік правою клавішею миші по ньому) і виберіть пункт «Створити ярлик». Сміливо натискаємо «Так».

Тепер можна підключатися до VPN. Знаходимо на робочому столі потрібний ярлик, виконуємо подвійний клік на ньому (не обов'язково: можна і правою клавішею миші вивести горезвісне контекстне меню і вибрати «підключити». Або з шкідливості знайти третій шлях: виділити одиничним кліком ярлик і притупнути на клавішу «Enter») .

Рекомендую вам відзначити пункт «Зберігати ім'я користувача та пароль», щоб не вводити пароль кожного разу при установці підключення.

Коли ви запускаєте VPN-з'єднання вперше, система запропонує вам обрати

ваше місце розташування. Вибирайте «Громадське місце» і тоді Windows 10 забезпечить вам належну безпеку при роботі. Так, натисніть «Закрити».

Щоб відкрити їх, виконуємо клік правою клавішею миші по з'єднанню в списку з'єднань, пункт «властивості». Тут ви можете керувати параметрами шифрування, використовувати інші пристрої в якості модему за умовчанням і так далі.

Схожість

Джерела з Бібліотеки 89

1	Студентська робота	ID файлу: 1002842243	Навчальний заклад: Ternopil Volodymyr Hnatiuk Nation	80 Джерело	24.5%
2	Студентська робота	ID файлу: 1008250397	Навчальний заклад: Cherkasy State Technological University		2.09%
3	Студентська робота	ID файлу: 1013034127	Навчальний заклад: National Technical University of Ukra	2 Джерело	0.41%
4	Студентська робота	ID файлу: 1014972905	Навчальний заклад: Lutsk National Technical University	3 Джерело	0.37%
5	Студентська робота	ID файлу: 1014961082	Навчальний заклад: Interregional Academy of Personnel Managem...		0.32%
6	Студентська робота	ID файлу: 1004175269	Навчальний заклад: Lviv Polytechnic National University		0.23%
7	Студентська робота	ID файлу: 1014813427	Навчальний заклад: State University Kyiv National Economic Univ...		0.21%