UNICHECK
by Turnitin

Ім'я користувача:
приховано налаштуваннями конфіденційності

ID перевірки:
1015625295

Дата перевірки:
16.06.2023 12:41:25 EEST

Тип перевірки:
Doc vs Library

Дата звіту:
16.06.2023 12:42:25 EEST

ID користувача:
100011372

Назва документа: **КН-320_Устіянич Л.М**

Кількість сторінок: **28** Кількість слів: **4810** Кількість символів: **37828** Розмір файлу: **1.55 MB** ID файлу: **1015272197**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

15.6%
Схожість

Найбільша схожість: **5.61%** з джерелом з Бібліотеки (ID файлу: **2059961**)

Пошук збігів з Інтернетом не проводився

15.6% Джерела з Бібліотеки | **81** ..... Сторінка 30

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | **1**

Підозріле форматування | **6 сторінок**

1 АНАЛІЗ ЗАВДАННЯ І ВИЗНАЧЕННЯ ЕТАПІВ ПРОЕКТУВАННЯ МЕРЕЖІ

1.1 Аналіз об’єкту проектування

В дипломній роботі потрібно спроектувати модель офісної комп’ютерної мережі з використанням програмних засобів адміністрування для компанії Project-X. Дане підприємство займається рекламною діяльністю.

При побудові моделі мережі необхідно використати систему дистанційного моніторингу і врахувати майбутнє розширення або зменшення мережі через можливу зміну приміщення, що відзначиться на кількості працівників, а відповідно і використовуваному обладнанні.

1.2 Визначення етапів проектування

Отже, проектування моделі мережі можна розділити на чотири етапи:

- вибір програмного забезпечення,
- вибір апаратного забезпечення,
- вибір технології передачі даних,
- вибір протоколу передачі даних,
- розробка алгоритму віддаленого доступу.

1.3 Загальні відомості про організацію дистанційного моніторингу та контролю роботи мережі.

1.3.1 Принципи контролю роботи мережі

Постійний нагляд за роботою локальної мережі, яка є основою будь-якої корпоративної мережі, є необхідним для забезпечення її ефективної роботи.

Контроль є першим етапом управління мережею і виконується спеціальними засобами, відокремленими від інших функцій управління.

Процес контролю мережі складається з двох етапів: моніторингу і аналізу. На етапі моніторингу збираються первинні дані про роботу мережі, такі як статистика про кількість переданих кадрів та пакетів різних протоколів, стан портів комутаторів, маршрутизаторів і т. д. На етапі аналізу ці дані аналізуються, порівнюються зі збереженими даними та робиться припущення щодо можливих причин проблем у роботі мережі.

Для моніторингу та аналізу мережі використовуються різні засоби, які можна розділити на декілька класів. Системи управління мережею (Network Management Systems) є централізованими програмними системами, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також про трафік в мережі. Вони забезпечують моніторинг, аналіз та автоматизоване або напівавтоматизоване управління мережею, зокрема включення та відключення портів пристроїв, зміну параметрів мостів, комутаторів, маршрутизаторів тощо. Прикладами таких систем є HPOpenView, SunNetManager, IBMNetView.

Ці засоби контролю мережі допомагають адміністратору виявити проблемні ділянки та недоліки мережі, що дозволяє їх відключати або реконфігурувати вручну.Засоби управління системою (System Management). Засоби управління системою часто виконують функції, аналогічні функціям систем управління, але стосовно інших об'єктів. У першому випадку об'єктом управління є програмне і апаратне забезпечення комп'ютерів мережі, а у другому - комунікаційне устаткування. Разом з тим, деякі функції цих двох видів систем управління можуть дублюватися, наприклад, засоби управління системою можуть виконувати найпростіший аналіз мережевого трафіку. До найбільш відомих систем управління системами відносяться LANDesk, IBM Tivoli, Microsoft Systems Management Server, HP OpenView, Novell ZENworks і CA Unicenter.

Вбудовані системи діагностики і управління (Embedded Systems) представляють собою програмно-апаратні модулі або програмні модулі, які

встановлюються в комунікаційне обладнання або вбудовуються в операційні системи. Вони виконують функції діагностики і управління лише одним пристроєм і відрізняються від централізованих систем управління. Наприклад, модуль управління концентратором Distributed 5000 реалізує функції автосегментації портів при виявленні несправностей, приписування портів внутрішнім сегментам концентратора та інші.

Аналізатори протоколів (Protocol Analyzers) є програмними або апаратно-програмними системами, які займаються моніторингом і аналізом трафіку в мережах. Вони здатні захоплювати і декодувати пакети багатьох протоколів, що використовуються в мережах. Аналізатори протоколів дозволяють встановлювати логічні умови для захоплення окремих пакетів і проводять повне декодування захоплених пакетів з розшифруванням змісту полів.

Обладнання для діагностики і сертифікації кабельних систем включає мережні монітори, прилади для сертифікації кабельних систем, кабельні сканери і тестери (мультиметри). Мережні монітори призначені для тестування кабелів різних категорій, збирають статистичні показники трафіку. Прилади для сертифікації кабельних систем виконують сертифікацію відповідно до міжнародних стандартів. Кабельні сканери використовуються для діагностики мідних кабельних систем, а тестери перевіряють кабелі на наявність фізичного розриву.

Експертні системи представляють собою системи, які накопичують людські знання про виявлення причин аномальної роботи мереж і можливі способи відновлення мережі до працездатного стану. Часто експертні системи реалізуються як окремі підсистеми різних засобів моніторингу та аналізу мереж, таких як системи управління мережами, аналізатори протоколів, мережеві аналізатори. Простішим варіантом експертної системи є контекстно-залежна довідкова система. Більш складні експертні системи представляють собою бази знань з елементами штучного інтелекту. Прикладом такої системи є експертна система, вбудована в систему управління Spectrum компанії Cabletron.

Багатофункціональні пристрої аналізу та діагностики виникли у зв'язку з поширенням локальних мереж. Це портативні пристрої, які поєднують функції декількох пристроїв, таких як аналізатори протоколів, кабельні сканери і навіть деякі можливості програмного забезпечення мережного управління. Прикладами таких пристроїв є Compas компанії Microtest Inc. або 675 LANMeter компанії Fluke Corp.

1.3.2 Функції засобів управління мережею:

Згідно зі стандартами ISO, можна виділити наступні функції засобів управління мережею:

- Управління конфігурацією мережі охоплює конфігурацію компонентів мережі, включаючи їх місце розташування, мережні адреси, ідентифікатори та параметри мережевих операційних систем. Вона також забезпечує підтримку схеми мережі та іменування об'єктів.
- Обробка помилок включає виявлення та усунення наслідків збоїв у роботі мережі.
- Аналіз продуктивності допомагає на основі накопиченої статистичної інформації оцінювати час відповіді системи, обсяг трафіку та планувати розвиток мережі.
- Управління безпекою включає контроль доступу та збереження цілісності даних. Вона охоплює процедури аутентифікації, перевірки привілеїв, підтримку ключів шифрування та управління правами. До цієї групи також відносяться механізми управління паролями та зовнішнім доступом, а також з'єднання з іншими мережами.
- Облік роботи мережі включає реєстрацію та управління використовуваними ресурсами та пристроями. Ця функція оперує поняттями, такими як час використання та плата за ресурси.

З цього переліку видно, що системи управління не лише виконують функції моніторингу та аналізу роботи мережі для отримання вихідних даних для

налаштування мережі, але також включають функції активного впливу на мережу, такі як управління конфігурацією і безпекою. Ці функції необхідні для впровадження розробленого плану налаштування та оптимізації мережі. Зазвичай етап створення плану налаштування мережі знаходиться поза межами функцій системи управління, але деякі системи управління мають експертні підсистеми, які допомагають адміністратору або інтегратору визначити необхідні кроки для налаштування мережі.

Засоби управління мережею (Network Management) відрізняються від засобів управління комп'ютерами та їх операційними системами (System Management). Прикладами засобів управління мережами є системи HPOpenView, SunNetManager і IBMNetView.

Засоби управління системою (System Management) зазвичай виконують такі функції:

- Облік використовуваних апаратних і програмних засобів: система автоматично збирає інформацію про комп'ютери і створює записи в базі даних про апаратні і програмні ресурси. Це дозволяє адміністратору швидко отримати інформацію про наявні ресурси і їх розташування.
- Розподіл і встановлення програмного забезпечення: адміністратор може створювати пакети розсилки програмного забезпечення для ефективного розподілу та зниження вартості процедури. Система також може забезпечувати централізовану установку і адміністрування програм, що запускаються з файлових серверів, а також дозволяти кінцевим користувачам запускати такі програми з будь-якої робочої станції в мережі.
- Віддалений аналіз продуктивності і проблем: адміністратор може віддалено управляти ресурсами будь-якого комп'ютера в мережі. База даних системи управління містить детальну інформацію про конфігурацію всіх комп'ютерів в мережі для здійснення віддаленого аналізу проблем.

Останнім часом в галузі систем управління спостерігаються дві чіткі тенденції:

- Інтеграція функцій управління мережами і системами в одному продукті.

- Розподіленість системи управління, коли існує кілька консолей, що збирають інформацію про стан пристроїв і систем, а також надають керуючі можливості.

1.3.3 Стандарти управління мережею

Таблиця 1 – Стандарти управління мережею

Організація	Стандарти	Особливості
IETF	SNMP	Управління має бути простим, орієнтоване на змінні
ISO	CMIP, CMIS	Управління має бути потужним, об'єктно-орієнтованим
ITU-T	TMN	Визначена тільки архітектура
DMTF	WBEM, CIM	Управління мережами і системами, об'єктно-орієнтоване
OMG	CORBA	Архітектура віддалених об'єктів

На сьогоднішній день, найбільш успішним сімейством стандартів є SNMP. Його перевагою є велика кількість керованих систем (агентів). Однак, у сфері керуючих систем (менеджерів) підтримується безліч стандартів, тому важко говорити про беззастережне лідерство SNMP. За обсягом інвестицій, можливо, лідирує Telecommunications Management Network (TMN).

Щоб прослідкувати залежність популярності стандартів від їхнього застосування, можна прикладно аналізувати різні середовища використання. У локальних і глобальних мережах передачі даних, які використовують Протокол інтернету (IP), найширше поширений стандарт SNMP. У системах відомчих автоматичних телефонних станцій (ВАТС) та в публічних телефонних мережах частіше використовуються пропрієтарні рішення. В мобільних мережах головним чином використовуються рішення, що базуються на стандартах ISO.

Більшість успіхів SNMP пов'язані з особливостями процесу стандартизації в IETF:

- Стандарти є безкоштовними і доступними для вільного поширення.
- Стандарти легко доступні у форматі електронних документів.
- Розвиток стандартів відбувається швидко, з продуманими етапами стандартизації.
- На всіх етапах проводиться технічна експертиза.
- Робочі групи очолюють технічні експерти, а не політичні лідери.
- Прототипи систем, засновані на стандартах, демонструють їхню придатність.

1.3.4 Призначення системного та мережевого адміністрування

Інтеграція системного і мережного адміністрування примусила провідних виробників, таких як Hewlett-Packard і Computer Associates, негайно модернізувати свої продукти. Однак, навіть у цьому випадку виникли деякі перешкоди: мережне адміністрування іноді розглядалося як одна з багатьох складових частин системного адміністрування, а мережа розглядалася як один із керованих ресурсів поряд з комп'ютерами, периферійними пристроями, базами даних, додатками тощо.

Остаточною метою всіх процедур управління є досягнення параметрів функціонування інформаційних систем, які задовольняють потребам користувачів. Але користувачі оцінюють роботу інформаційних систем не за характеристиками мережного трафіка, використовуваними протоколами, часом відгуку серверів на певні типи запитів або особливостями виконання сценаріїв управління. Вони оцінюють їх за поведінкою додатків, які щодня запускаються на їх персональних комп'ютерах. В майбутньому мережне та системне адміністрування будуть замінені управлінням додатками і якістю обслуговування, незалежно від використовуваних обчислювальних платформ або мереж.

Мережне адміністрування, узагалі, можна розбити на дві основні групи задач, якщо не вдаватися у деталі:

- Контроль за роботою мережевого обладнання.

- Управління функціонуванням мережі в цілому.

У першому випадку йдеться про моніторинг окремих мережевих пристроїв, таких як концентратори, комутатори, маршрутизатори, сервери доступу та інші, налаштування і зміну їх конфігурації, а також усунення виникаючих збоїв. Цю традиційну групу задач називають реактивним адмініструванням (reactive management).

Друга група завдань спрямована на моніторинг мережного трафіку, виявлення тенденцій його зміни і аналіз подій з метою впровадження схем пріоритизації та вирішення проблем, що передують, пов'язаних з обмеженням пропускної здатності (попереджувальне адміністрування, або проактивне управління). Сюди також входять формування єдиного представлення мережі з метою внесення змін у її конфігурацію, керування мережевими ресурсами, управління IP-адресами користувачів, фільтрація пакетів для забезпечення інформаційної безпеки та інші задачі.

Необхідність контролю всієї мережі з однієї керуючої станції призвела до появи різноманітних архітектур платформ та програм для адміністрування. Найпоширенішою серед них є двохрівнева розподілена архітектура "менеджер-агенти". Програма-менеджер працює на керуючій консолі і постійно взаємодіє з модулями-агентами, що запускаються на окремих пристроях мережі. У цій схемі агенти виконують функції збору локальних даних про параметри роботи контрольованого ресурсу, внесення змін у його конфігурацію за запитом від менеджера та надання адміністративної інформації.

Хоча двохрівнева схема має свої переваги, застосування її в реальному мережному середовищі призводить до збільшення обсягів службового трафіку і, як наслідок, зниження ефективної пропускної здатності, доступної для додатків. Як часткове рішення проблеми обмеженої пропускної здатності була запропонована трьохрівнева схема, в якій деякі керуючі функції делегувалися найважливішим мережним вузлам. Програми-менеджери, встановлені на цих вузлах через власну мережу агентів, керують роботою "підзвітних" пристроїв і одночасно виступають як агенти щодо основного програми-менеджера

(менеджера менеджерів), який працює на керуючій станції. Як результат, основна частина службового трафіку обмежується локалізовано в окремих мережних сегментах, оскільки "спілкування" між локальними менеджерами та адміністративною консоллю відбувається лише тоді, коли це є необхідним.

Необхідність контролювати різноманітне обладнання в гетерогенному середовищі призвела до уніфікації основних керуючих процедур. Згадана схема "менеджер-агенти" знайшла відображення у протоколі Simple Network Management Protocol (SNMP), який швидко став основним протоколом мережного адміністрування, а також у стандарті дистанційного моніторингу RMON.

Управління настільними системами зазвичай здійснюється за допомогою стандарту Desktop Management Interface (DMI), розробленого організацією Desktop Management Task Force (DMTF). Крім згаданих базових стандартів в області мережного адміністрування існують специфікації, які відіграють меншу фундаментальну роль, наприклад, стандарт Web-Based Enterprise Management (WBEM).

Системне адміністрування є областю управління, яка включає різні функції, визначені в специфікаціях ISO. Ці функції включають:

- Вирішення проблемних ситуацій, таких як діагностика, локалізація та усунення несправностей, реєстрація помилок і тестування.
- Управління ресурсами, включаючи контроль використання ресурсів, виставлення рахунків за їх використання та обмеження доступу до них.
- Управління конфігурацією, спрямоване на забезпечення надійного та ефективного функціонування всіх компонентів інформаційної системи.
- Контроль продуктивності, включаючи збір і аналіз інформації про роботу ресурсів, прогнозування задоволення потреб користувачів та заходи для підвищення продуктивності.
- Захист даних, включаючи управління доступом користувачів до ресурсів, забезпечення цілісності даних та управління шифруванням.

На ринку існує багато продуктів, які дозволяють вирішувати завдання системного адміністрування. Ці продукти можна поділити на базові платформи

управління, такі як CA-Unicenter TNG від Computer Associates, HP OpenView і Tivoli Enterprise від IBM, які покривають весь функціонал, визначений стандартом ISO, а також на "крапкові" продукти, спрямовані на рішення конкретних задач.

Останнім часом у галузі системного адміністрування все більш активно обговорюється концепція динамічного адміністрування. Цей підхід зосереджується на задоволенні потреб користувачів інформаційних технологій та передбачає використання засобів аналізу поведінки користувачів, активного керування взаємодією між користувачами, додатками і мережею та використання аналітичних засобів підтримки прийняття рішень.

1.3.5 Програми віддаленого адміністрування

Для забезпечення зручного контролю над мережами розроблені програми віддаленого адміністрування, що надають практично повний контроль над віддаленим комп'ютером. Вони дозволяють дистанційно керувати робочим столом, копіювати або видаляти файли, запускати додатки та інше. На ринку існує безліч рішень для віддаленого адміністрування, які відрізняються інтерфейсами і протоколами. Прикладами популярних програм є Windows Remote Desktop Services з клієнтом Remote Desktop Connection, Radmin, DameWare, PuTTY, VNC, UltraVNC, Apple Remote Desktop, Hamachi, TeamViewer, Remote Office Manager і Ammyy Admin.

Програма Radmin є однією з найпопулярніших і має великий функціонал. Вона складається з двох частин - серверної і клієнтської. Серверна частина запускається на віддаленому комп'ютері, а клієнтська - на комп'ютері адміністратора для з'єднання з віддаленими машинами. Radmin має такі можливості, як підтримка різних версій Windows, сканер серверів Radmin для знаходження доступних ПК в мережі, підтримка Telnet, віддалене вимкнення ПК і передача файлів.

TeamViewer є ще однією популярною програмою для віддаленого доступу. Вона пропонує безкоштовну версію для некомерційного використання і підтримує

різні операційні системи, включаючи Windows, macOS і Linux. TeamViewer також має мобільні клієнти для Android і iOS, що дозволяють керувати віддаленим комп'ютером з мобільного пристрою. Крім того, є Portable-версія програми для зручного використання без установки.

Загалом, існує багато рішень для віддаленого адміністрування, які можуть бути ефективними в залежності від конкретних потреб і операційної системи.

Після запуску програми TeamViewer, відкриваються два вікна: основне вікно TeamViewer і вікно "Комп'ютери та контакти". Якщо ви плануєте адмініструвати багато комп'ютерів, ви можете натиснути кнопку "Зареєструватися", створити обліковий запис, і потім в цьому вікні ви побачите всі комп'ютери, які ви налаштували.

Тепер давайте розберемося з основними функціями програми. Якщо вам потрібно підключитися до комп'ютера іншої сторони, вам потрібно передати їй ваш ID. Ви можете скопіювати і передати це значення за допомогою Skype, електронної пошти, SMS або просто продиктувати його по телефону. Цей ID пароль змінюється кожного разу при запуску програми. Якщо програма встановлена на вашому комп'ютері, ви можете встановити постійний особистий пароль, але це не рекомендується, оскільки пароль може бути скомпрометований, і хтось інший зможе підключитися до вашого комп'ютера.

Якщо вам потрібно підключитися до віддаленого комп'ютера, вам потрібно ввести ID віддаленої сторони і натиснути кнопку "Підключитися до партнера". Потім програма попросить вас ввести пароль, який ви отримали від віддаленої сторони. Після цього ви зможете настроювати віддалений комп'ютер у відповідному вікні.

Одна з відмінностей між TeamViewer і Radmin полягає в тому, що в TeamViewer ви повинні передати пароль адміністратора комп'ютера, якщо ви хочете настроювати його. У Radmin пароль вказується при створенні користувача. Це означає, що в Radmin потрібно мати присутність користувача на комп'ютері, під час коли TeamViewer може використовуватися для отримання доступу до комп'ютера навіть в його відсутності. Якщо вам потрібно організувати домашній

офіс і мати доступ до робочого комп'ютера, наприклад, вночі, ви можете налаштувати автозапуск TeamViewer і задати "Особистий пароль". Зверніть увагу, що ви можете задати "Особистий пароль", якщо програма запускається без встановлення на комп'ютері.

TeamViewer Host - це версія програми, яка запускається як системна служба і дозволяє цілодобовий доступ до віддаленого комп'ютера, включаючи вхід у систему та вихід з неї. TeamViewer Host може бути використана для організації сервера терміналів, підтримуючи необмежену кількість клієнтів для одного сервера. Проте для встановлення TeamViewer Host потрібні права адміністратора, які не завжди доступні. У більшості випадків користуються звичайною версією TeamViewer. Зауважується, що якщо на комп'ютері встановлена звичайна версія TeamViewer (не Host), до нього можуть підключитися інші комп'ютери для спільного адміністрування. Проте потрібно узгоджувати дії адміністраторів, оскільки клавіатура і миша використовуються спільні.

Як і Radmin, TeamViewer дозволяє обмінюватися файлами, голосовими і текстовими повідомленнями, а також віддалено перезавантажувати комп'ютер. Програма Royal TS, у свою чергу, є іншою програмою, яка може бути використана для з'єднання з віддаленими серверами. В Royal TS перед створенням підключення потрібно створити документ, і кожне підключення відповідає одному документу. У shareware-версії Royal TS є обмеження на кількість одночасно відкритих документів - десять.

Отже, TeamViewer і Royal TS мають різні підходи до з'єднання з віддаленими комп'ютерами. TeamViewer може використовуватися як сервер і клієнт, а Royal TS дозволяє підключатися до віддалених серверів, якщо сам сервер уже налаштований.

1.3.6 Протокол SNMP

Системи управління мережами потребують орієнтації на певні стандарти через розмаїтість управляючого програмного забезпечення та мережевого

обладнання, що розробляються багатьма компаніями. Оскільки корпоративні мережі зазвичай неоднорідні, керуючі інструменти не можуть відображати специфіки кожної окремої системи або мережі. Найбільш поширеним протоколом управління мережами є протокол SNMP (Simple Network Management Protocol), який підтримується багатьма виробниками. Основні переваги протоколу SNMP полягають у його простоті, доступності та незалежності від виробників. Ця популярність SNMP утримує прийняття CMIP, варіанта керуючого протоколу відповідно до стандартів OSI. Протокол SNMP спеціально розроблений для управління маршрутизаторами в мережі Інтернет та є частиною стеку TCP/IP.

У системах управління, побудованих на основі протоколу SNMP, стандартизуються такі елементи:

- протокол взаємодії агента та менеджера;
- мова опису моделей MIB (Management Information Base) та повідомлень SNMP - мова абстрактної синтаксичної нотації ASN.1 (стандарт ISO 8824:1987, рекомендації ITU-T X.208);
- кілька конкретних моделей MIB (MIB-I, MIB-II, RMON, RMON 2), імена об'єктів яких реєструються в дереві стандартів ISO. Інші аспекти системи управління залишаються на розсуд розробника. Протокол SNMP та пов'язана з ним концепція SNMP MIB спочатку були розроблені для управління маршрутизаторами Інтернету як тимчасове рішення. Але завдяки своїй простоті та ефективності цей протокол здобув популярність і сьогодні використовується для управління практично будь-яким обладнанням та програмним забезпеченням обчислювальних мереж.

Хоча в управлінні телекомунікаційними мережами є тенденція застосування стандартів ITU-T, включаючи протокол CMIP, успішні приклади використання SNMP-управління є досить поширеними. Агенти SNMP вбудовуються в аналогові модеми, модеми ADSL, комутатори ATM та інші пристрої. SNMP є протоколом, який використовується для отримання інформації про статус, продуктивність та характеристики мережевих пристроїв, яка зберігається в спеціальній базі даних

мережевих пристроїв, від них. ця база даних називається MIB (Management Information Base).

Існують стандарти, які визначають структуру MIB, включаючи набір типів змінних (об'єктів в термінології ISO), їх назви та допустимі операції (наприклад, читання). У MIB можуть зберігатися мережеві та / або MAC-адреси пристроїв, значення лічильників оброблених пакетів та помилок, номери, пріоритети та інформація про стан портів. Деревоподібна структура MIB містить обов'язкові (стандартні) піддерева, а також приватні (private) піддерева, які дозволяють виробникам інтелектуального обладнання реалізувати будь-які специфічні функції на основі їх власних змінних.

Агент в протоколі SNMP є складовою, яка надає менеджерам, розташованим на керуючих станціях мережі, доступ до значень змінних MIB та, таким чином, дозволяє їм реалізовувати функції управління та спостереження за пристроями.

Типова структура системи управління зображена на рисунку 1.1:

Рисунок 1.1 – Робота протоколу SNMP

2 ВИБІР АПАРАТНОГО ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1 Вибір обладнання та розробка структурної схеми мережі

В дипломній роботі потрібно спроектувати модель офісної комп'ютерної мережі з використанням програмних засобів адміністрування для компанії Project-X. Дане підприємство займається рекламною діяльністю. Керування мережею буде здійснюватися адміністратором віддалено через сервер мережі, який має доступ в Internet. Враховуючи особливості організації, мережа буде складатися з наступного обладнання:

- Серверний комп'ютер з виходом до мережі Internet;
- Серверний комутатор;
- 2 Wi-Fi маршрутизатора;
- 4 ПК адміністраторів.

В якості обладнання я вибрав:

Серверний комп'ютер – Моноблок Lenovo IdeaCentre 5 27IMB05 (F0FA0069UA) Windows 10. Характеристики: Екран 27 "IPS (2560x1440) WQHD / Intel Core i5-10400T (2.0 - 3.6 ГГц) / RAM 16 ГБ / HDD 1 ТБ + SSD 256 ГБ / nVidia GeForce GTX 1650, 4 ГБ / без ОД / LAN / Wi-Fi / Bluetooth / кардрідер / веб-камера / Windows 10 Home Rus / 9.22 кг / Сірий / клавіатура + миша

Серверний комутатор - TP-LINK TL-SG1016D гігабітний (TL-SG1016D). Характеристики: 6 x RJ-45 10/100/1000 Мбит/с с автосогласованием, авто-MDI/MDIX

2 Wi-Fi маршрутизатори - TP-LINK Archer AX50. Характеристики: 5 ГГц + 2.4 ГГц (двохдіапазонний), 1 x 1 Гбіт / с WAN, 4 x 1 Гбіт / с LAN, 1 x USB 3.0 802.11b / g / a, Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac),Wi-Fi 6 (802.11ax)

4 ПК адміністраторів – ноутбуки Acer Aspire 5 A515-56G-54JD (NX.A1LEU.00A) Pure Silver. Характеристики: Екран 15.6 "IPS (1920x1080) Full HD, матовий / Intel Core i5-1135G7 (4.2 ГГц) / RAM 8 ГБ / SSD 512 ГБ / nVidia

GeForce MX350, 2 ГБ / без ОД / LAN / Wi-Fi / Bluetooth / веб камера / без ОС / 1.9 кг / сріблястий

Структурна схема мережі показана на рисунку 2.1:

Рисунок 2.1 – Структурна схема мережі

2.2 Вибір програмного забезпечення мережі

2.2.1 Вибір серверної операційної системи

В якості серверної операційної системи будемо використовувати Windows Server 2010.

До десяти основних функцій Windows Server відносяться: масштаб і продуктивність корпоративного рівня, динамічна міграція даних без поділу ресурсів, віртуалізація мережі Hyper-V Hyper-V Replica, недороге сховище на основі файлів, що забезпечує високу доступність; Windows PowerShell 3.0; гібридні програми; многоарендние веб-сайти з високою щільністю; спрощена інфраструктура віртуальних робочих столів з широкими можливостями; динамічне управління доступом.

2.2.2 Вибір програмного забезпечення віддаленого доступу мережі

Розглянувши в пункті 1.3.5 переваги та недоліки програм віддаленого адміністрування, обираємо повну версію програми TeamViewer Host та програму OpenVPN.

TeamViewer підтримує Windows, OS X, Linux і на відміну від більшості конкурентів підтримує необмежену кількість безкоштовних хост-модулів з усіма ліцензіями – оплачується тільки ліцензія адміністратора мережі, а віддалені сервера підключаються безкоштовно.

Особливості TeamViewer:

- Простота (програма простіше, ніж Radmin, - величезна перевага для непідготовлених користувачів, яким доведеться встановити її на віддаленій стороні).
- Програма повністю не вимагає установки: як на клієнті, так і на сервері. Установка проводиться за бажанням.

- Працює через порт 80 (і ще деякі додаткові порти), завдяки чому не вимагає настройки брандмауера.
- Наявність версій для інших ОС.
- Наявність мобільних клієнтів для Android, iOS і Windows Phone 8 (тобто ти можеш керувати віддаленим комп'ютером прямо зі свого iPad).
- Можливість організації інтерактивних конференцій (до 25 учасників).
- е вимагає прав адміністратора для віддаленого доступу.
- Вантажить процесор помітно більше, ніж Radmin.
- Мобільні клієнти хоч і є, але вони не дуже зручні (втім, це краще, ніж нічого).

OpenVPN - вільна реалізація технології віртуальної приватної мережі (VPN) з відкритим кодом для створення шифрованих з'єднань між двома клієнтськими машинами або забезпечення роботи централізованого VPN-сервера для одночасної роботи декількох клієнтів. OpenVPN дозволяє встановлювати з'єднання між комп'ютерами, що перебувають за NAT-екраном, без необхідності зміни їхніх налаштувань. OpenVPN використовується в операційних системах Solaris, OpenBSD, FreeBSD, NetBSD, GNU/Linux, Apple Mac OS X, QNX і Microsoft Windows.

2.2.3 Вибір програмного забезпечення моніторингу мережі

Основна ідея адміністрування, що випереджає, зводиться до того, щоб, проаналізувавши поводження корпоративної ІС або окремих її компонентів, почати превентивні міри, що дозволяють не припустити розвитку подій по найгіршому сценарію. Проведення подібної профілактики потребує застосування іншого інструментарія, ніж при звичайному (реактивному) управлінні.

Як відомо, традиційна методологія адміністрування заснована на використанні правил. Останні наказують системі адміністрування почати визначені дії (наприклад, видати попереджуюче повідомлення на керуючу

консоль) у випадку настання визначених подій (скажемо, перевищенні інтенсивністю трафіка заздалегідь визначеного граничного значення).

В даний час системи управління на базі правил випускають багато виробників. Так, цей підхід використовується в сімействі продуктів OpenView фірми Hewlett-Packard або Tivoli Enterprise корпорації IBM.

Засоби профілактичного управління сьогодні пропонуються поруч фірм. Як приклад можна згадати продукти Hewlett-Packard - OpenView Service Simulator (розроблений разом із компанією MIL 3), MeasureWare і PerfView.

Проте воістину революційний крок у цьому напрямку порівняно нещодавно зробила компанія Computer Associates. У грудні минулого року фірма випустила ПО Neugents, що базується на технології нейроних мереж і призначене для управління системами під Windows NT. Після навчання на ретроспективних даних, зібраних за допомогою традиційної схеми “менеджер - агенти”, нейрона мережа виявляється в стані як виявляти поточні проблеми, так і пророкувати ті, що можуть виникнути в майбутньому. Основну роль у цьому процесі грає розбивка множини можливих станів системи на класи і прогнозування можливостей її міграції з одного класу в інший.

Для проектованої системи будемо використовувати HP OpenView (HP OV) - сімейство програмних продуктів компанії Hewlett Packard по управлінню системами і мережами зв'язку.

HP OpenView є всеосяжним рішенням з управління IT-інфраструктурою підприємства будь-якого розміру і напрямки діяльності. Побудована на основі модульної архітектури. Надає широкі можливості з моніторингу та управління локальними обчислювальними мережами, серверними платформами (такими як HP-UX, Solaris, AIX, Novell, Linux, весь спектр Windows, платформ), додатками (SAP, Oracle, Sybase, MS SQL, Exchange, DB2, Informix, MS Active Directory, ...), робочі місця користувачів (інвентаризація, віддалена установка ОСИ, оновлень, програмне забезпечення, налаштування користувачів, контроль за використання ПЗ), організація диспетчерської служби, надання інструментарій для вибудовування IT-інфраструктура згідно процесам ITIL / ITSM. Більше 50

програмних продуктів, які вирішують найрізноманітніші завдання - від резервного копіювання до моніторингу стану бізнес процесів в реальному часі.

Програмне забезпечення системи дистанційного моніторингу показане на Рисунку 2.2:

Рисунок 2.2 – Система дистанційного моніторингу інформаційної мережі

2.3 Алгоритм роботи проектованої системи

Алгоритм роботи проектованої системи дистанційного моніторингу показаний на Рисунку 2.3:

Рисунок 2.3 – Алгоритм роботи системи дистанційного моніторингу

3 НАЛАШТУВАННЯ СИСТЕМИ ДИСТАНЦІЙНОГО МОНІТОРИНГУ

3.1 Налаштування TeamViewer Host

При необхідності застосовувати TeamViewer на службових комп'ютерах, які працюють без користувача треба встановити модуль TeamViewer Host. Він буде працювати в якості системної служби. Налаштування TeamViewer для постійного підключення дозволяє в будь-який час здійснювати доступ до пристроїв без оператора. При цьому встановити вихідні з'єднання з таких ПК буде неможливо.

Перед налаштуванням скачуємо TeamViewer Host на комп'ютер. Запускаємо установник. Після встановлення з'явиться вікно «Інформація» (Рисунок 3.1).

Рисунок 3.1 – вікно «Інформація» програми TeamViewer Host

Для настройки модуля користуємося розташованим на панелі управління пунктом «Опції» (Рисунок 3.2).

Рисунок 3.2 – вікно «Опції» програми TeamViewer Host

Рисунок 3.3 – вікно «Очікування сеансу» програми TeamViewer Host

Запустивши TW на комп'ютері, потрібно перейти у вкладку «Удаленное управление». Переконайтеся, що програма запущена на віддаленому комп'ютері. Для здійснення сеансу вам знадобиться ID користувача і його пароль.

Після того як ви натиснули кнопку підключення до користувача, має відкритися діалогове вікно, в якому потрібно буде ввести пароль. Після входу на вашому робочому столі відкриється вікно робочого столу віддаленого пристрою. При встановленому з'єднання вам доступні:: удаленное управление ПК, создание виртуальной сети, передача файлов и другие функции.

Рисунок 3.4 – вікно «Ідентифікація» програми TeamViewer Host

Як запустити TeamViewer на віддаленому комп'ютері. Запуск TeamViewer на віддаленому ПК по суті нічим не відрізняється від запуску на комп'ютері адміністратора. Необхідно виконати аналогічні дії по встановленню та налагодженню опцій програми. Якщо вам потрібно ПЗ, щоб до вас підключалися для техпідтримки, досить буде звичайної установки без додаткових налаштувань.

Після успішної інсталяції запустіть TeamViewer на своєму комп'ютері. Щоб користувач міг до вас підключитися, потрібно повідомити йому ID і пароль, які будуть відображені в діалоговому вікні програми. При наступному запуску ПЗ даний пароль буде недійсним.

Як за допомогою TeamViewer включити віддалений комп'ютер

Вище наведені рекомендації, як налаштувати TeamViewer, щоб включити віддалений пристрій, якщо він відключений від мережі. Після налаштування мережевої карти, брандмауера, BIOS і самої програми, можна будити від сну віддалений ПК.

Для цього у вкладці меню «Комп'ютери та контакти» виберіть зі списку потрібне підключення. Після того, як ви натиснули потрібну ID, навпаки облікового запису повинна з'явиться кнопка «Розбудити». Після виконання даних дій, віддалений пристрій буде включиться.

Як через TeamViewer підключитися до телефону

За допомогою TeamViewer можна підключитися і не тільки до комп'ютера, але і планшету, а також смартфону. Що важливо, комп'ютер може працювати не тільки під управлінням ОС Windows, але також Mac або Linux. Для здійснення сеансу зв'язку на комп'ютері необхідно встановити програму TW, скориставшись посібником з установки. А на мобільному пристрої має бути встановлено ПО TeamViewer QuickSupport.

Якщо вам потрібен постійний доступ до пристрою, знадобиться установка модуля TeamViewer Host. Для того щоб надавати віддалену техпідтримку підключившись до телефону, необхідно мати ліцензію Corporate або Premium. Ви можете легко підключитися до віддаленого комп'ютера з телефону, ввівши пароль і ID. Таким чином, ви отримаєте повноцінний доступ до комп'ютера.

VPN TeamViewer: як підключити. Процес підключення через VPN здійснюється точно також, як і при звичайному сеансі зв'язку. Запустіть програму на комп'ютері і у вкладці «Віддалене управління» впишіть ID користувача і пароль. Після входу в систему вам відкриється VPN-TeamViewer.

У вас є можливість декількох одночасних підключень, ви зможете вибрати потрібний. Ви можете закрити то VPN-підключення, яке вам найближчим часом не знадобиться. Щоб отримати доступ до ресурсів віддаленого комп'ютера потрібно буде вибрати опцію «Windows Explorer».

Налаштування TeamViewer для постійного підключення без пароля

Якщо ви здійснюєте підключення до своїх комп'ютерів, то пароль не потрібен. Для пристроїв, які знаходяться під вашим обліковим записом, пароль для здійснення доступу вводити не потрібно. Доступ без пароля можна встановити в налаштуваннях повної версії програми. Ви можете підключатися без пароля, тільки якщо ви перебуваєте під своїм обліковим записом.

Для включення легкого доступу необхідно у вкладці Інструменти увійти в меню «Опції» та вибрати розділ «Безпека». Після цього буде потрібно, якщо ПК ще не пов'язаний з обліковим записом, зв'язати його і вибрати пункт «Надати легкий доступ».

3.2 Налаштування адресації інформаційної мережі

Згідно завдання офісна комп’ютерна мережа компанії Project-X складається з сервера, серверного комутатора, 2 Wi-Fi маршрутизаторів та чотирьох ПК працівників. Між собою 4 ПК працівників та 2 Wi-Fi маршрутизатора зв’язані через серверний комутатор та керуються сервером з виходом до мережі Internet;

Налаштування адресації наступні:

Сервер
44.24.1.14/ Маска: 255.255.255.0 / Шлюз: 44.24.1.1, DNS сервер: 8.8.8.8;
192.168.0.1 / Маска: 255.255.0.0 / Шлюз: 192.168.0.1, DNS сервер: 8.8.8.8;

Серверний комутатор:
192.168.0.11 / Маска: 255.255.0.0 / Шлюз: 192.168.0.1, DNS сервер: 8.8.8.8;

4 офісних ПК:

192.168.1.1 / Маска: 255.255.0.0 / Шлюз: 192.168.1.0, DNS сервер: 8.8.8.8;

192.168.1.2 / Маска: 255.255.0.0 / Шлюз: 192.168.1.0, DNS сервер: 8.8.8.8;

192.168.1.3 / Маска: 255.255.0.0 / Шлюз: 192.168.1.0, DNS сервер: 8.8.8.8;

192.168.1.4 / Маска: 255.255.0.0 / Шлюз: 192.168.1.0, DNS сервер: 8.8.8.8;

Wi-Fi маршрутизатор 1:

192.168.1.5 / Маска: 255.255.0.0 / Шлюз: 192.168.1.0, DNS сервер: 8.8.8.8.

Wi-Fi маршрутизатор 2:

192.168.1.6 / Маска: 255.255.0.0 / Шлюз: 192.168.1.0, DNS сервер: 8.8.8.8.

Схожість

Джерела з Бібліотеки 81

1	Студентська робота	ID файлу: 2059961	Навчальний заклад: Lviv Polytechnic National University	12 Джерело	5.61%
2	Студентська робота	ID файлу: 1008323048	Навчальний заклад: National Technical University of Ukra	4 Джерело	4.24%
3	Студентська робота	ID файлу: 1008431559	Навчальний заклад: Lutsk National Technical University	7 Джерело	3.06%
4	Студентська робота	ID файлу: 1008277703	Навчальний заклад: National Aviation University	2 Джерело	2.56%
5	Студентська робота	ID файлу: 1005729007	Навчальний заклад: National Aviation University		2.52%
6	Студентська робота	ID файлу: 1009724344	Навчальний заклад: Lutsk National Technical University		2.2%
7	Студентська робота	ID файлу: 1009419698	Навчальний заклад: National Aviation University		2.08%
8	Студентська робота	ID файлу: 3299154	Навчальний заклад: Lviv Polytechnic National University		1.89%
9	Студентська робота	ID файлу: 1000779259	Навчальний заклад: Cherkasy State Technological University		1.83%
10	Студентська робота	ID файлу: 1001306019	Навчальний заклад: National Aviation University	2 Джерело	1.83%
11	Студентська робота	ID файлу: 1009721247	Навчальний заклад: National Aviation University		1.7%
12	Студентська робота	ID файлу: 103168	Навчальний заклад: Lviv Polytechnic National University		1.66%
13	Студентська робота	ID файлу: 1006821718	Навчальний заклад: National Aviation University		1.64%
14	Студентська робота	ID файлу: 1009702677	Навчальний заклад: National Technical University of Ukraine "Kyi...		1.31%
15	Студентська робота	ID файлу: 1003939954	Навчальний заклад: National Technical University of Ukraine "Kyi...		1.29%
16	Студентська робота	ID файлу: 1005831909	Навчальний заклад: National University of Water Manage	5 Джерело	1.1%
17	Студентська робота	ID файлу: 1015225050	Навчальний заклад: V.I. Vernadsky Taurida National University		0.87%
18	Студентська робота	ID файлу: 1004182237	Навчальний заклад: National Aviation University		0.81%
19	Студентська робота	ID файлу: 1003891612	Навчальний заклад: National Technical University of Ukra	2 Джерело	0.75%
20	Студентська робота	ID файлу: 1004182219	Навчальний заклад: National Aviation University		0.75%

21	Студентська робота	ID файлу: 1005717571	Навчальний заклад: National University of Water Management an...		0.69%
22	Студентська робота	ID файлу: 1012558929	Навчальний заклад: National Aviation University		0.56%
23	Студентська робота	ID файлу: 1015269871	Навчальний заклад: National Technical University of Ukraine "Kyi...		0.54%
24	Студентська робота	ID файлу: 1001197468	Навчальний заклад: National Aviation University	4 Джерело	0.46%
25	Студентська робота	ID файлу: 1015271659	Навчальний заклад: Lviv Polytechnic National University		0.42%
26	Студентська робота	ID файлу: 1009137674	Навчальний заклад: Ternopil Volodymyr Hnatiuk Nationa	3 Джерело	0.42%
27	Студентська робота	ID файлу: 1015235366	Навчальний заклад: Yuriy Fedkovych Chernivtsi National	10 Джерело	0.4%
28	Студентська робота	ID файлу: 1001166075	Навчальний заклад: National Aviation University	2 Джерело	0.4%
29	Студентська робота	ID файлу: 1008227121	Навчальний заклад: Lviv Polytechnic National University	3 Джерело	0.35%
30	Студентська робота	ID файлу: 1000744115	Навчальний заклад: Cherkasy State Technological Univers	4 Джерело	0.27%
31	Студентська робота	ID файлу: 1015012812	Навчальний заклад: V.I. Vernadsky Taurida National University		0.25%
32	Студентська робота	ID файлу: 1000756407	Навчальний заклад: National Technical University of Ukraine "Kyi...		0.25%
33	Студентська робота	ID файлу: 1010382228	Навчальний заклад: Lviv Polytechnic National University		0.23%
34	Студентська робота	ID файлу: 1011442788	Навчальний заклад: National Aviation University		0.17%