МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
КАФЕДРА ІНФОРМАЦІЙНИХ ТА КОМП'ЮТЕРНИХ СИСТЕМ

ПРОЕКТУВАННЯ

КОРПОРАТИВНОЇ МЕРЕЖІ

Методичні вказівки
до курсового проектування
з дисципліни "Комп'ютерні мережі"
для студентів спеціальності
123 "Комп'ютерна інженерія"

Затверджено

на засіданні кафедри
інформаційних і комп'ютерних систем

Протокол № 1 від «27» серпня 2018 р

Чернігів ЧНТУ 2018

Проектування корпоративної мережі. Методичні вказівки до курсового проектування з дисципліни “Комп’ютерні мережі” для студентів для студентів спеціальності 123 "Комп'ютерна інженерія" / Укл. Риндич Є. В., Зайцев С.В., Нікітенко Є.В. – Чернігів: ЧНТУ, 2018. – 27 с.

Укладачі: Риндич Євген Володимирович, кандидат технічних наук, доцент, доцент кафедри інформаційних та комп’ютерних систем;
Зайцев Сергій Васильович, доктор технічних наук, доцент, завідувач кафедри інформаційних та комп’ютерних систем;
Нікітенко Євгеній Васильович, кандидат фізико-математичних наук, доцент, доцент кафедри інформаційних та комп’ютерних систем

Відповідальний за випуск: С.В. Зайцев, зав. кафедрою інформаційних та комп’ютерних систем, д-р. техн. наук, доцент.

Рецензент: С. О. Нестеренко, канд. техн. наук, доцент, доцент кафедри інформаційних і комп'ютерних систем Чернігівського національного технологічного університету

ЗМІСТ

ВСТУП

Даний посібник призначений для студентів, що виконують курсовий проект або роботу з курсу «Комп'ютерні мережі», але може бути корисним і практичним інженерам. Курсовий проект представляє собою розробку комп'ютерної мережі невеликого підприємства і програмного забезпечення, що працює з мережевими сокетами на рівні системних функцій.

Не дивлячись на те, що локальні і корпоративні мережі є необхідним атрибутом сучасного підприємства, є істотний дефіцит навчальних матеріалів, що охоплюють комплексно питання проектування мережі. Даний посібник покликаний надати чітко структуровані знання і дати читачеві загальну картину проблем, які потрібно вирішити при побудові сучасної корпоративної мережі. Посібник задає основні напрямки, які потребують уваги при побудові корпоративної мережі і дає посилання на більш докладні джерела інформації.

1 Вимоги до курсової роботи

Курсовий проект по курсу "Комп'ютерні мережі" є значною практичною частиною курсу бакалавра, тому до даного курсового проекту пред'являються вимоги, що в більшій частині збігаються з вимогами до дипломної роботи, за винятком обсягу роботи і деяких нетехнічних розділів.

1.1 Вимоги до проекту мережі

В апаратній частині курсового проекту необхідно розробити проект локальної мережі середнього підприємства. Мережа повинна містити не менше 50 хостів, діаметр локальної мережі повинен становити не менше 800м. Мережа повинна обов'язково мати захищений вихід до мережі Інтернет. В мережі підприємства повинна бути налаштована робота системних сервісів, таких як сервіс імен DNS, сервіс конфігурації при завантаженні DHCP, WINS і файловий сервіс для мереж на ОС Windows.

Крім того, в мережі повинний бути організований зв'язок з віддаленим офісом або в межах міста з використанням технологій "останньої милі", або з використанням сервісів, що надаються телефонними компаніями, таких як FrameRelay або інших технологій, що надаються телекомунікаційними компаніями.

Вихідним матеріалом для проектування мережі є поверховий план будівель з позначеним на ньому розміщенням комп'ютерів і мережевого устаткування, розміщенням відділів підприємства, а так само докладний опис інформаційних потоків на підприємстві.

За інформаційним опису підприємства визначаються основні інформаційні потоки, їх можливості, вимоги до безпеки і т.д., тобто в кінцевому підсумку - структура мережі підприємства і сервісів, в ній розміщених.

За планом будівлі розраховується пасивне мережеве обладнання, як то: комунікаційні шафи, короби, кабель, розетки, з’єднувальні кутові елементи тощо. На плані так само вказується розміщення активного мережевого обладнання, такого як комутатори, маршрутизатори, сервери.

Результат розміщення обладнання відображається на плані будівлі і в зведених таблицях по поверхах, будівлям і проекту в цілому. Вибір активного мережевого обладнання повинен проводитися виходячи з чітко сформульованих вимог до мережі на основі як мінімум 3 альтернативних рішень, тобто в проекті повинен бути приведений порівняльний аналіз обладнання 3-х різних виробників за критерієм якість / вартість.

Не рекомендується використання в проекті застарілих типів обладнання, такого як, наприклад, концентратори. Навіть якщо проектування проводиться на основі реального підприємства з існуючою мережевою інфраструктурою, в проекті необхідно не констатувати поточний стан, а розробити проект модифікації мережі з урахуванням сучасних рішень.

Сучасна кабельна інфраструктура мережі будується з урахуванням

підведення гарантованого живлення в критичні ділянки мережі, тому в проекті повинні бути враховані джерела безперебійного живлення основних серверів та активного мережевого обладнання. Кабельна система повинна забезпечити підведення живлення до них. Крім того, в сучасній структурованої кабельної системи (СКС) прокладаються комунікації не тільки для комп'ютерної мережі, але і для телефонної мережі. Зазвичай корпоративна телефонна станція знаходиться в серверній кімнаті і використовує ту ж систему гарантованого електроживлення. Найбільш сучасні АТС можуть так само інтегрувати голосові сервіси традиційних телефонних мереж і комп'ютерні голосові сервіси. Ці моменти варто врахувати при створенні проекту мережі.

Логічна структура мережі так само повинна бути спроектована в ході роботи. У разі застосування керованих комутаторів з підтримкою функцій VLAN необхідно привести таблиці віртуальних мереж. Обов'язковою є використання протоколу IPv4 в мережі, отже, має бути здійснено планування адресного простору мережі. Планування для протоколу IPv6 не є обов’язковим, але бажане.

Важливе місце в проекті займає забезпечення безпеки в мережі. Провідним моментом в розробці засобів забезпечення безпеки є розробка політики безпеки (security policy) для мережі в цілому з подальшою деталізацією для окремих сегментів мережі і мережевих сервісів. Політика безпеки являє собою звичайний текст, що описує рівні безпеки тих чи інших інформаційних ресурсів і права доступу до них. Цей текст затверджується керівництвом або відповідними режимними службами і є основою для проектування технічних засобів захисту мережі.

Для організації необхідного рівня безпеки необхідно розбивати мережу на сегменти маршрутизаторами з функціями фільтрації трафіку. Наприклад, фінансові служби підприємства повинні знаходитися в окремому сегменті мережі, доступ до ресурсів який неможливий з сегмента мережі загального користування.

Доступ в мережу Інтернет повинен так само здійснюватися з використанням необхідних засобів захисту. Для мереж масштабу підприємства необхідно будувати доступ з урахуванням захисту внутрішньої мережі від вторгнень з Інтернету, захисту сервісів, що надаються мережею в Інтернет, а так само з урахуванням розмежування прав користувачів мережі по доступу в Інтернет.

У разі використання фільтруючих маршрутизаторів обов'язковим є опис функцій фільтра. Бажаним є написання тексту фільтра на мові застосованого обладнання.

Робота повинна містити розділ, що описує фізичну і логічну структуру спроектованої мережі (опис схеми мережі).

1.2 Вимоги до програмної частини

Програмна частина курсового проекту представляє собою програми, що працюють з мережевими сокетами на системному рівні і мають графічний користувальницький інтерфейс. Для більшості випадків програми мають архітектуру клієнт-сервер.

Серверна частина, природно, не зобов'язана мати графічний інтерфейс. Вона являє собою програму-демон (системний сервіс), який зчитує текстовий конфігураційний файл при старті або по сигналу SIGHUP. Серверна програма повинна збиратися і працювати на POSIX-сумісних системах. Для підтримки підсистеми POSIX в ОС Windows зазвичай використовують або оточення CyGNUs, або MINGW.

Клієнтська програма повинна розроблятися з урахуванням кроссплатформенності, як мінімум Windows і Linux. При розробці програми рекомендується використання крос-платформних бібліотек, таких як QT, GTK. Для даних бібліотек існують візуальні конструктори, що полегшують розробку повнофункціональних призначених для користувача інтерфейсів.

Рекомендовані мови розробки - C або C ++.

У разі спрощеного варіанту завдань можливе використання Java.

Оскільки дана робота може бути представлена як частина кваліфікаційної роботи бакалавра, особливу увагу слід приділяти якості проектування і структурування програмного проекту. Оцінка роботи проводиться не тільки на основі функціональності програми і її інтерфейсу, а й на основі аналізу вихідних текстів. В роботі повинен бути показаний належний рівень програмування і вміння оформляти текст програми.

Документування вихідних текстів слід так само приділити особливу увагу. Скрупульозне документування вихідних текстів за допомогою тегів будь-якої системи авто-документування, наприклад DoxyGen або DOC++ істотно полегшує і спрощує написання звіту в частині розділу розробки програм.

2 Приклади типових завдань на розробку програмної частини

1. ***Розробити програму, що дозволяє секретарю керівника швидко відправляти SMS повідомлення співробітникам.***

Клієнтська частина програми повинна мати зручний призначений для користувача інтерфейс, що забезпечує авторизацію, внесення користувачів і груп, пошук користувачів, редагування користувачів, відправку повідомлень з підтримкою архіву відправлених повідомлень. Клієнтська програма не повинна зберігати ніяких даних, окрім адреси сервера.

Серверна частина програми повинна відправляти SMS по електронній пошті, вибираючи адресу поштового сервера по префіксу телефонного номера, зберігати всі необхідні дані і надавати клієнтської частини необхідний сервіс черех TCP сокет. Програма повинна обслуговувати довільну кількість клієнтів. Серверна і клієнтська частини програми так само повинні забезпечувати необхідний рівень конфіденційності шляхом шифрування даних. На сервері необхідно використовувати багатопоточний режим роботи.

2. ***Розробити програму моніторингу працездатності та рівня завантаження хостів в мережі.***

Програма повинна визначати рівень завантаження процесорів, дискової підсистеми, каналів введення-виведення і мережевих пристроїв.

Швидкодія системи має бути максимальною в межах одного сегмента мережі.

Клієнтська програма, яка відображає стан хостів, не повинна вимагати ніяких налаштувань, а виявляти хости з встановленою програмою моніторингу автоматично. Відображення хостів повинно бути упорядкованим по імені, адресою, рівню завантаження тієї чи іншої підсистеми. Рівень завантаження повинен відображатися у вигляді графіка. Для передачі даних може використовуватися протокол SNMP.

3. ***Написати програму для швидкого обміну повідомленнями, спрощений варіант ICQ для використання в корпоративній мережі.***

Програма повинна забезпечувати реєстрацію користувачів, прив'язку до штатного розпису організації, пошук користувачів.

Клієнтська частина програми повинна мати зручний графічний інтерфейс. Всі дані система повинна зберігати на сервері, можливо, в базі даних.

4. ***Програма відстеження присутності користувача на робочому місці.***

Дана програма повинна запускатися на будь-якому робочому місці (Windows, Linux) як аплет робочого столу і відстежувати активність користувача з комп'ютером. Програма так само повинна мати можливість реєстрації користувача на сервері і можливість настройки таймаутів на певні події (рух миші, клавіатурне введення, специфічні події системи).Серверна частина програми повинна вести протокол активності зареєстрованих користувачів і по кожному користувачеві генерувати файл статистики в форматі

HTML. Файли статистики повинні складатися в директорію, доступну веб-серверу для перегляду.

Студенти можуть самостійно пропонувати варіанти завдань по програмній частині і погоджувати їх з викладачем. У звіті за проектом повинні міститися всі розділи, визначені стандартами кафедри.

3 Рекомендації з проектування мережі масштабу підприємства

3.1 Вихідні дані для розробки

Вихідними даними для проектування мережі є 2 документа: план будівель і результати інформаційного обстеження підприємства. Поверховий план будівель малюється в масштабі і на ньому вказується розміщення робочих місць. В ході розробки проекту мережі на плані вказуються також розетки, короби, в які проводиться укладання кабелю, комунікаційні шафи з активним мережевим обладнанням.

Інформаційне обстеження підприємства проводиться за наступним шаблоном.

1. Опис підприємства в цілому, тобто сфера діяльності підприємства (організації), зовнішні інформаційні потоки, необхідні для діяльності підприємства.
2. Для кожного відділу (підрозділу, робочої групи) підприємства описуються функції відділу, кількість робочих місць, використане програмне забезпечення, використані загальні ресурси мережі підприємства, виділені даними відділом ресурси для інших користувачів мережі, вимоги до рівня безпеки сегмента мережі даного відділу.
3. Загальні ресурси мережі, необхідні для роботи підприємства, такі як файлові сервери, сервери баз даних, сервери доступу в Інтернет, сервери голосових комунікацій і т.д.
4. Вимоги до системи забезпечення безпеки мережі, тобто які необхідні сервіси автентифікації, авторизації та обліку.

На підставі плану будівлі і результатів інформаційного обстеження підприємства виконується ескізний проект мережі.

3.2 Структурована кабельна система і розміщення обладнання

Структурована кабельна система (СКС) є "скелетом", на якому ґрунтується вся комунікаційна інфраструктура підприємства, тому проектування СКС необхідно приділяти особливу увагу.

До складу СКС входять кабельні системи для передачі даних, для передачі голосу і для підведення гарантованого живлення.

Для передачі даних зі швидкістю 100 і 1000 Мбіт необхідний кабель витої пари категорії 5е. Для передачі телефонного сигналу досить кабелю категорії 2 або 3, але з метою взаємозамінності кабелів і використання резервних кабелів як для телефонних з'єднань, так і для мережевих з'єднань, всі кабелі прокладаються по вищій необхідної категорії.

В СКС так само закладаються резервні кабелі в обсязі не менше 15% від загального числа для забезпечення надійності і для полегшення розширення мережі. Короба, використовувані для укладання кабелів, повинні мати переріз, що дозволяє укласти необхідну кількість кабелів плюс запас 20% на розширення мережі.

Кабелі підведення гарантованого електроживлення так само прокладаються в загальному коробі з сигнальними кабелями, проте монтуються в спеціальну ізольовану секцію короба. Силовий кабель має 3 дроти - "фаза", "нуль" і "земля". Дуже важливе дотримання фазування кабелів і забезпечення надійного контуру заземлення.

Розетки для телефонних, мережевих і силових підключень вибираються зазвичай універсальні, з перехідними елементами на необхідний перетин короба і необхідною кількістю гнізд для роз'ємів. Телефонні мережі зазвичай використовують роз'єм RJ11, але для забезпечення взаємозамінності кабелів в СКС рекомендується і для телефонних, і для мережевих з'єднань використовувати роз'єм RJ45.

Розетки в обов'язковому порядку маркуються наклейками з позначенням їх призначення і з реєстраційним номером кабелю, підключеного до них.

Кабелі в СКС обов'язково маркуються спеціальними наклейками і складається документ, що визначає маршрут кожного кабелю. Таблиця кроссування кабелів зазвичай містить номер кабелю, точки кроссування і примітки. Ця таблиця є основним експлуатаційним документом на СКС.

Короба стикуються за допомогою спеціальних конструкційних елементів: куточків, хрестовин, переходів на інший перетин і розгалужувачів.

Кабелі повинні заводиться в комунікаційні шафи і розподілятися не в кінцеве обладнання, а в кроссувальні панелі.

Застосування крос-панелей дозволяє легко здійснити перекомутацію кабелів при заміні обладнання або при виході з ладу будь-якого каналу зв'язку.

Зміни в кроссуванні повинні відображатися в спеціальному аркуші кроссування, який або знаходиться в загальному журналі експлуатаційних документів, або в кожній комунікаційній шафі.

Комутація всередині шаф між крос-панелями і активним устаткуванням здійснюється за допомогою коротких кабелів з роз'ємами RJ45, званих патчкордами.

Магістральні кабелі між комунікаційними шафами можуть містити кілька комплектів пар (20 і більше). Перекомутація між магістральними та кінцевими кабелями так само проводиться на крос-панелі в комунікаційних шафах.

Кроссувальні панелі теж нумеруються, маркуються і заносяться в таблицю кроссування кабелів.

Оптоволоконні кабелі прокладаються в тих же коробах. Оскільки оптоволоконний канал не надає гальванічного зв'язку, немає особливих вимог по ізоляції при укладанні кабелю, проте є вимоги на мінімальний радіус заокруглення вигину кабелю, тому оптичний кабель на поворотах короба укладається в спеціальні пластикові «радіуси».

Перегин кабелю може призвести до його виходу з ладу, а недотримання мінімального радіуса - до появи відбитків в кабелі, що спричинить за собою нестабільну роботу мережі.

Комутація оптичний кабелів здійснюється за допомогою спеціальних оптичних концентраторів.

Оптичні кабелі необхідно застосовувати там, де потрібна гальванічна

розв'язка між мережами. Гальванічна розв'язка дозволяє уникнути виходу з ладу обладнання при скачках напруги між живлячими фазами, при пробої на корпус обладнання і при грозових розрядах. Зазвичай за допомогою оптичного кабелю підключають сервера, вилучені сегменти мережі і сегменти, які живляться з різних електричних мереж.

Важливою частиною СКС є система гарантованого електроживлення. Залежно від вимог до безперебійної роботи обладнання вибирається потужність джерел безперебійного живлення, які повинні забезпечити роботу мережі протягом певного проміжку часу. Зазвичай, при відсутності спеціальних вимог до електроживлення, потужність джерел живлення і ємність їх батарей вибирається такий, щоб забезпечити безаварійне відключення обладнання. Джерело живлення повинно бути приєднаний з сервера, розсилати в мережу повідомлення про перехід на автономне живлення і про час до відключення живлення. На інших вузлах мережі встановлюється ПО, що приймає ці повідомлення і реагує заданим чином на події в мережі електроживлення.

Активне обладнання розміщується в комунікаційних шафах, в які заводиться кабельна система в межах допустимого діаметра для даного типу мережі. У більшості випадків діаметр не повинен перевищувати 200 метрів. Комунікаційні шафи зазвичай розташовують на кожному поверсі.

Комунікаційні шафи повинні мати замки для запобігання несанкціонованого доступу до обладнання.

Сервера і базове мережеве обладнання, а так само АТС розміщують в окремому приміщенні - серверній кімнаті, доступ до якої обмежений.

У цій кімнаті повинні бути розташовані так само засоби підтримки безперебійного живлення, принаймні для обладнання, розміщеного тут же.

3.3 Вибір активного обладнання

Для початку варто окреслити клас технологій, застосовуваних найчастіше для побудови локальних мереж.

Єдиною, яка вижила на сьогодні технологією побудови локальних мереж, є Ethernet в різних його модифікаціях. Найбільш поширеним на сьогодні стандартом є 100BaseT, що забезпечує передачу даних зі швидкістю 100 Мбіт / с по мідній кручений парі 5-ї категорії. Останнім часом все більшого поширення набувають стандарти 1000 Мбіт і виходять на ринок виробники пристроїв 10Гбіт.

Стандарт 1000 Мбіт використовується в 2-х варіантах - мідний кабель і оптоволоконний кабель. Для стандарту 10Гбіт використовують тільки оптоволоконний кабель.

Найбільш поширеним на сьогодні є стандарт IEEE 802.11g, або WiFi, що забезпечує передачу даних зі швидкістю до 11 Мбіт. Застосування бездротової технології дозволяє забезпечити доступ до мережі для мобільних користувачів з такими пристроями, як, наприклад, ноутбуки, планшети, смартфони.

Для доступу в мережу через WiFi встановлюютьсямаршрутизатори(точки

доступу) або радіо-концентратори, які підключаються безпосередньо в локальну мережу Ethernet. Зазвичай такі пристрої містять комутатор на кілька портів і маршрутизатор з 1 портом, який дозволяє виділити бездротовий сегмент в окрему мережу.

Мережі на основі інших технологій не знайшли поширення при побудові локальних мереж.

Для глобальних мереж і для об'єднання віддалених сегментів корпоративних мереж використовуються інші технології, які описані в окремому розділі.

Активне обладнання локальних мереж може бути розбите на наступні групи:

Концентратори - це пристрої, що дозволяють з'єднати мережеве обладнання в один фізичний сегмент. Концентратори не обробляють мережеві пакети (кадри), а лише забезпечують необхідне узгодження сигналів середовища передачі і посилення слабкого сигналу.

Концентратори забезпечують підключення до одного загального фізичного середовища передачі всіх пристроїв, отже трафік в цьому середовищі буде загальним для всіх мережевих пристроїв, і, трафік між тими чи двома пристроями буде заважати третьому пристрою.

Концентратори є пристроями рівня 1 по моделі взаємодії відкритих систем OSI.

Для мережі Ethernet 100 Мбіт застосування концентраторів не доцільно, оскільки комутатори мають приблизно таку ж вартість, але забезпечують поділ трафіку між портами і пропускна здатність мережі значно зростає. Для оптичних кабелів застосування концентратора може виявитися виправданим.

Комутатори - це пристрої другого рівня моделі OSI, які працюють з пакетами (кадрами) мережі. Кожен порт комутатора має свою буферну пам'ять і асоційовану з портом пам'ять для зберігання MAC адресі. Комутація пакетів між портами здійснюється через комутаційну матрицю по MAC адресі. Пропускна здатність комутаційної матриці повинна дозволяти обробляти пакети "зі швидкістю дроту", тобто, з тією швидкістю, з якою пакети надходять з фізичного середовища передачі. Пропускна здатність комутаційної матриці повинна дорівнювати сумі пропускних спроможностей всіх портів комутатора, тоді будь-яка пара портів комутатора буде працювати незалежно і не буде впливати на роботу іншої пари. Через деякий час після включення комутатор накопичує інформацію про те, які MAC адреси знаходяться на якому порту, і пересилає пакети тільки в потрібний порт, а не на всі порти, як відбувається в разі використання концентратора. Широкомовні (broadcast) пакети пересилаються, природно, на всі порти комутатора.

Керовані комутатори мають додаткові функції, основними з яких є підтримка віртуальних мереж і жорстка прив'язка MAC адреси до порту. Ці функції дозволяють підвищити безпеку в мережі одночасно з гнучкістю налаштування. Оскільки учасники однієї віртуальної мережі "не бачать" учасників іншої мережі на рівні MAC адрес, можливе створення декількох

незалежних мереж на основі однієї мережі Ethernet. Обмін даними між цими мережами буде можливий тільки на 3-му рівні, тобто через маршрутизатор, що дозволяє більш гнучко контролювати трафік в мережі. Прив'язка порту до конкретної MAC адреси не дозволить користувачеві несанкціоновано потрапити в іншу віртуальну мережу шляхом заміни MAC адреси. Ще однією, зручною для провайдерів мережевих сервісів, функцією, є можливість підрахунку трафіку по порту і по MAC адресі.

Комутатори з підтримкою віртуальних мереж VLAN за стандартом IEEE 802.1q дозволяють розділити одну фізичну мережу на кілька ізольованих логічних мереж, використовуючи або групи портів, або, в загальному випадку, додаткові поля (теги) в кадрі Ethernet.

Комутатори з пріорітизацією трафіку дозволяють більш ефективно використовувати наявну смугу пропускання.

Комутатори з підтримкою аутентифікації на рівні 2

Маршрутизатори - це пристрої 3-го рівня OSI, з деякими функціями 4-го рівня. Маршрутизатори працюють на рівні мережевого протоколу, наприклад, на рівні протоколів IP або IPX. Оскільки IPX потихеньку відходить у небуття, будемо розглядати тільки сімейство протоколів TCP / IP. До основних функцій маршрутизаторів можна віднести наступні;

1. Маршрутизація. Власне, цілком зрозуміло, що це основна функція маршрутизатора, у якій є 2 важливих аспекти: динамічна маршрутизація забезпечує живучість мережі за рахунок використання альтернативних маршрутів; маршрутизація відбувається на рівні мережевого протоколу, а не на 2-му рівні, тому виключається залежність від конкретної несучої мережі і з'являється можливість об'єднання мереж різної природи.

2. Управління трафіком. Найважливішим аспектом управління трафіком є пріоритизації трафіку за різними ознаками, як то за адресами, полю TOS, по використовуваних протоколах і т.д. Іншим важливим аспектом є фільтрація трафіку по всіляких критеріях, заснованих на розборі заголовків мережевого і транспортного рівнів, а іноді і рівня доступу до мережі, відповідно до моделі взаємодії в мережах TCP / IP.

3. Маршрутизатор необхідно встановлювати в разі об'єднання мереж різної природи, в разі необхідності розділити мережу на сегменти з метою забезпечення безпеки і при необхідності забезпечення живучості мережі за рахунок використання альтернативних маршрутів.

Маршрутизуючі комутатори - пристрої, що поєднують в собі функції комутатора і маршрутизатора.

Маршрутизатор - це спеціалізований комп'ютер з різними мережевими інтерфейсами, який здійснює операції над пакетами в ОЗУ з використанням свого процесора. Маршрутизуючий комутатор має величезну комутаційну матрицю, в якій є апаратні структури не тільки для розбору заголовків рівня 2, але і для рівнів 3 та 4. Комутаційна матриця програмується "на льоту" процесором пристрою для відображення поточної конфігурації, стану таблиць маршрутизації і т.д. На відміну від маршрутизаторів, ці пристрої зазвичай

мають набагато більшу пропускну здатність, що дозволяє вести обробку трафіку "зі швидкістю дроту", однак, можуть працювати тільки в мережах однієї природи, наприклад, в мережах Ethernet.

Маршрутизуючі комутатори застосовують в разі необхідності динамічної маршрутизації в великих мережах на основі технології Ethernet. У зв’язку з їх високою вартістю інше застосування не виправдано. Якщо необхідно розмежування доступу в мережу для віртуальних локальних мереж, має сенс використовувати керований комутатор в парі з маршрутизатором на основі ПК під управлінням ОС Linux або FreeBSD і портом Ethernet 1000Мбіт. Маршрутизатор включається у усі віртуальні мережі і на нього встановлюється маршрут за замовчуванням (default route) всіх хостів у всіх віртуальних з мережах. Таким чином, всі пакети, що проходять з однієї мережі в іншу, будуть потрапляти спочатку на маршрутизатор, там оброблятися відповідними фільтрами, і потім потрапляти за призначенням. Природно, пропускна здатність такого маршрутизатора буде визначати швидкість обміну між віртуальними мережами.

4 Рекомендації щодо застосування мережевого обладнання

Виходячи з викладеного в попередніх розділах, можна сформулювати наступні рекомендації по вибору типу і розміщення активного мережевого обладнання.

1. Робочі групи зі стандартними вимогами до швидкості включаються в порти 100 Мбіт некерованого комутатора. Для виходу в загальний сегмент бажано використовувати порт 1000 Мбіт.

2. Робочі групи з підвищеними вимогами до пропускної здатності мережі включаються в некерований комутатор з портами 1000Мбіт, при чому файловий сервер для таких груп необхідно розміщувати в цьому ж сегменті мережі, тобто включати в той же комутатор.

3. Робочі групи без додаткових вимог до безпеки або сегменти мережі з одними і тими ж логічними рівнями доступу об'єднуються в один сегмент мережі Ethernet за допомогою швидкісного некерованого комутатора.

4. Робочі групи з додатковими вимогами до мережевої безпеки включаються в окремий сегмент мережі, фізичний, або логічний (VLAN). Для поділу мережі на логічні сегменти (віртуальні локальні мережі) використовують керовані комутатори.

5. Всі сегменти мережі об'єднуються за допомогою маршрутизатора. Оскільки маршрутизатор обробляє пакети в пам'яті, то далеко не завжди можна досягти потрібної швидкості передачі даних між сегментами мережі через низьку швидкодію маршрутизаторів. Для вирішення проблеми швидкості обміну потрібно розміщувати спільно використовувані ресурси в тих сегментах, де швидкість доступу до них найбільш критична і де відбувається основна маса звернень до даних ресурсів. Якщо вчинити так з яких-небудь причин не вдається, то замість маршрутизатора потрібно використовувати маршрутизуючий комутатор.

Основною причиною об'єднання сегментів мережі за допомогою маршрутизатора є можливість додаткового управління трафіком з метою підтримки певної політики безпеки. Наприклад, добре відомо, що працівники фінансових служб підприємства часто є простими користувачами і не володіють достатньою кваліфікацією для забезпечення належного рівня безпеки своїх персональних комп'ютерів. Однак, саме їх робочі комп'ютери можуть містити комерційні та інші секрети, які не повинні випадково потрапити в сегмент загального користування. З іншого боку, ці співробітники повинні мати повний доступ до інформаційних ресурсів мережі.

Вирішити таку задачу можна, застосувавши пакетні фільтри на маршрутизаторі, що об'єднує локальну мережу фінансової служби з іншими сегментами корпоративної мережі.

Устаткування "останньої милі"

Традиційно проблема "останньої милі" - це проблема передачі сигналу від міської АТС до квартири абонента. З розвитком цифрових телекомунікаційних технологій це поняття набуло більш широкий зміст - передача сигналу в межах

невеликих відстаней.

Для вирішення проблеми "останньої милі", тобто подачі мережевого трафіку від телекомунікаційного провайдера до кінцевого споживача або для з'єднання мереж, розташованих в невеликому радіусі (приблизно до 7 км) використовується ряд технологій, проте ми зупинимося тільки на обладнанні, призначеному для передачі IP трафіку без жорстких вимог до нижнього рівня.

Очевидно, що споживачеві найзручніше приймати IP трафік в порт Ethernet. Підстава - поширеність і, отже, невелика вартість устаткування. Однак, в окремих випадках доводиться використовувати порти з синхронними протоколами, такими як V.35 / V.36, X.21 або E1. Синхронні порти використовуються для роботи через глобальні мережі провайдерів послуг традиційної телефонії або мережі FrameRelay.

Устаткування для зв’язування комп'ютера з синхронним потоком в десятки і навіть в сотні разів дорожче, ніж обладнання Ethernet.

Однак, яка б технологія не використовувалася для глобальної мережі, в кінці кінців IP трафік повинен потрапити в локальну мережу на базі Ethernet.

Спочатку визначимо, що є фізичним середовищем передачі.

1. Ефір є найбільш зручним способом досягти з'єднання мереж в межах прямої видимості. Складність полягає в тому, що в Україні для використання радіочастот необхідна наявність досить дорогої ліцензії, і навіть для обладнання WiFi, що працює з шумоподібним сигналом на частоті мікрохвильових печей немає вільно використовуваного діапазону частот. За українським законодавством держава може конфіскувати обладнання та накласти штраф, як тільки побачить використання обладнання WiFi за межами будівлі. Отже, використання WiFi (IEEE 802.11) для вирішення проблеми "останньої милі" можливо тільки в разі договору з ліцензіатом.

2. Мідні пари діаметром 0.4 мм використовуються для подачі телефонного сигналу від АТС до кінцевого абонента. Вартість оренди однієї пари в межах кабельного господарства однієї АТС становить приблизно 5 $ в місяць. Устаткування має прийнятні ціни. Швидкість передачі даних в межах 2 Мбіт / с. Проблема в одному - в дефіциті (як повіяло радянською історією!) цих пар.

3. Оптоволоконні кабелі - найбільш зручне середовище для передачі даних. Вартість кабелів і кінцевого обладнання прийнятна. Проблема полягає в тому, що прокладка кабелю повинно здійснюватися по криницям, що належать іншим організаціям або в власні траншеї, на що потрібно досить багато офіційних дозволів від державних та інших органів. Чужою оптоволоконною структурою скористатися практично не можливо, оскільки в оренду кабельну систему здавати не вигідно, набагато вигідніше надавати сервіс з передачі даних.

5 Використання протоколів і адресація в мережі

На сьогоднішній день практично немає необхідності використовувати будь-які протоколи, крім родини TCP/IP по тій простій причині, що дане сімейство протоколів використовується в мережі Інтернет і фактично витіснило інші протоколи. Для доступу до мережних служб, специфічним для мереж Windows застосовується спеціальний варіант протоколу NetBIOS, що працює поверх протоколів сімейства TCP / IP. Застосування «чистого» NetBIOS і IPX не виправдано з точки зору безпеки та дані протоколи повинні фільтруватися маршрутизаторами.

Використання NetBIOS в «чистому» вигляді, на перший погляд, може полегшити адміністрування невеликих мереж, однак на практиці призводить до виникнення суттєвої плутанини в мережі, оскільки користувачі надані самі собі і в питаннях призначення імен і в питаннях адресації. Це а врешті-решт призводить до хаосу в мережі.

Використання протоколів родини TCP/IP має на увазі планування мережі, централізовану схему видачі адрес і присвоєння імен, а так само певну політику маршрутизації.

Розглянемо приклад планування адресного простору мережі і розміщення необхідних системних мережевих сервісів.

Для корпоративних мереж виділені наступні блоки адрес:

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

Наведені блоки адрес не маршрутизуються в Інтернеті, адміністратор мережі може брати будь-який блок для використання в своїй мережі.

Оскільки адрес більш ніж достатньо для створення мережі масштабу корпорації, розбивати на дрібні блоки адреси немає необхідності. Однак, слід пам'ятати, що "плоска" модель мережі, без розбивки на ієрархічні сегменти, вразлива з точки зору організації безпеки.

Оптимальним є використання маски 255.255.255.0 для сегментів мережі, що дозволить ввести додаткову сегментацію при необхідності, з одного боку, і є зручним блоком для маршрутизації, з іншого боку. Таким чином, в сегменті може бути до 254 хостів, при чому один і з них - це і інтерфейс маршрутизатора, що забезпечує вихід назовні з даної підмережі.

Маршрути за замовчуванням для робочих станцій встановлюються саме на адресу даного інтерфейсу (192.169.5.1). У наведеному прикладі мережі можна використовувати статичну маршрутизацію, однак це пов'язано з труднощами при подальшому зростанні мережі. Для локальних мереж цілком зручний протокол RIP, який майже не потребує налаштувань і реалізований в кожному маршрутизаторі. Для UNIX систем рекомендується використовувати демон ripd з пакета zebra. Для мереж з множинними альтернативними маршрутами і віддаленими сегментами з невеликою пропускною здатністю каналів рекомендується використовувати протокол OSPF, проте даний сервіс складніший в налаштуванні.

5.1 Вихід в інтернет і надання інтернет-сервісів

Перш, ніж говорити про технічні засоби підключення мережі підприємства до Інтернет, необхідно сформулювати і виписати у вигляді звичайного тексту політику надання сервісів Інтернет у внутрішню мережу і політику надання сервісів корпоративної мережі в Інтернет. На основі цієї політики, узгодженої з керівництвом, проводиться розміщення сервісів для надання інформації в мережу Інтернет і для доступу користувачів корпоративної мережі в інтернет.

Приклад такої політики наведено нижче. Даний приклад підходить для більшості випадків.

Доступ до інформаційних ресурсів корпоративної мережі користувачів мережі Інтернет здійснюється через інформаційний веб-сайт підприємства, який повинен бути видно для всієї мережі Інтернет. Доступ фірм-партнерів до інформаційних ресурсів підприємства проводиться через інший веб-сайт з можливістю контролю доступу за допомогою пароля і криптографічного захисту каналу. Повинна бути так само врахована можливість контролю електронних сертифікатів користувачів.

Доступ співробітників підприємства як мобільних користувачів до внутрішніх ресурсів корпоративної мережі повинен здійснюватися через мережу Інтернет з використанням сервера віртуальних приватних мереж по протоколу PPTP з криптографічними розширеннями.

Доступ співробітників підприємства з внутрішньої мережі підприємства в мережу Інтернет повинен здійснюватися в залежності від посади з певних робочих станцій при введенні облікового імені та пароля для доступу в мережу. Для деяких робочих станцій і серверів доступ в мережу Інтернет повинен бути не можливий ні за яких обставин.

Використання програм моментальних повідомлень дозволяється необмежено, за винятком зазначених вище комп'ютерів.

Використання протоколу віддаленого доступу до UNIX-системам ssh дозволяється тільки з певних робочих станцій в декількох відділах.

Природно, слова "*деякі", "певні*" і т.п. повинні бути конкретизовані в реальному документі.

Після формування такого документа можна говорити про технічні засоби, необхідні для реалізації описаної політики доступу.

Оскільки в наведеному прикладі є веб-сервера і сервера віртуальних приватних мереж, то доступ в мережу інтернет повинен здійснюватися по високонадійному виділеному каналу. Крім того, зазначені сервера повинні мати постійний IP адреси і відповідні записи в публічно доступному сервері імен DNS.

Організація фізичного каналу до провайдера мережевих послуг в більшості випадків залежить від провайдера, однак ці технічні засоби повинні бути відображені в проекті мережі.

Для підключення мережі підприємства до Інтеренет зазвичай використовується схема, коли прикордонний маршрутизатор забезпечує

максимальний захист мережі за допомогою пакетного фільтра, налаштованого для блокування всього трафіку, крім того, який надходить на гарантовано обслуговувані сервіси в демілітаризованій зоні (DMZ) і певного вихідного плюс відповідного йому вхідного трафіку з внутрішньої мережі відповідно до політики доступу.

Сам маршрутизатор практично не може бути зламаний, оскільки не виконує ніяких програм, доступних в зовнішню мережу.

Таким чином, доступ із зовнішньої мережі можливий тільки до сервісів, розташованим в демілітаризованій зоні. і ці сервіси знаходяться під постійним спостереженням і контролюються мережевими адміністраторами. Інша мережа не доступна ззовні без ініціювання певного трафіку зсередини самої корпоративної мережі.

Доступ з внутрішньої мережі в мережу Інтернет повинен також бути під контролем адміністратора. Для найбільш ресурсномістких протоколів, таких, як ftp і http, зазвичай використовують проксі-сервер з контролем списків доступу. У найпростішому випадку контроль проводиться за логіном і паролем, однак, сучасні проксі-сервера, такі як Squid, мають широкий набір засобів авторизації і автентифікації; nt-domain, RADIUS, LDAP, SQL-bsed і т.д. Вибирається зазвичай та система обліку, авторизації та автентифікації (AAA), яка застосовується для інших сервісів в корпоративній мережі.

Доступ в мережу Інтернет для інших протоколів, таких як ICQ, ssh може проводиться через маршрутизатор з підтримкою трансляції мережевих адрес (NAT).

Протоколи, які не використовуються, повинні бути закриті на прикордонних маршрутизаторах, а так само повинна бути налаштована система журналювання пакетів, заблокованих прикордонними маршрутизаторами.

Доступ мобільних користувачів в корпоративну мережу здійснюється через сервер віртуальних приватних мереж (VPN). Як сервер можна використовувати рішення під керуванням ОС Windows, який має сервіс PPTP в якості стандартного сервісу віддаленого доступу, проте в такому випадку дуже великий ризик несанкціонованого доступу в мережу шляхом злому даного сервера. Справа скоріше не в низькій захищеності даної ОС, а в її популярності в поєднанні з закритістю. Популярність робить даний сервіс мішенню номер один для зловмисників, а закритість ускладнює несвоєчасне оновлення системи з метою вирішення проблем безпеки. Як сервер VPN рекомендується використовувати або спеціалізований пристрій, або UNIX-подібну вільно поширювану ОС з відповідним ПО підтримки PPTP сервісу та необхідних засобів авторизації і автентифікації. На сервері VPN не повинно виконуватися більше ніяких сервісів для виключення можливості злому, а віддалений доступ по протоколу ssh повинен бути відкритий тільки з робочих станцій мережевих адміністраторів. Жорсткість вимог до даного сервера визначається його положенням в мережі: з одного боку, він повинен бути доступний з мережі Інтернет для мобільних користувачів, а з іншого - він відкриває шлях у внутрішню мережу підприємства. Саме тому, що злом даного сервера відкриває повний доступ до корпоративної мережі, рекомендується використовувати

операційні системи і додатки з бездоганною репутацією, наприклад такі як FreeBSD або Solaris.

5.2 Налаштування фільтруючих маршрутизаторів

Налаштування пакетних фільтрів є окремою великою темою, тому попередньо варто ознайомитися з наступним матеріалом.

Налаштування пакетних фільтрів проводиться на основі все тих же писаних правил, що визначають політику доступу до тих чи інших інформаційних ресурсів.

Якщо мова йде про прикордонний маршрутизатор між корпоративною мережею та мережею інтернет, то пакетний фільтр проектується на основі наведеної вище політики доступу в Інтернет. Якщо мова йде про маршрутизатори між різними сегментами корпоративної мережі, то повинна бути сформульована політика, що описує інформаційний обмін між сегментами мережі.

Політика інформаційного обміну між мережами наступна:

Доступ з інших сегментів мережі в підмережу фінансових служб повинен бути заборонений по всіх протоколах. Мобільні користувачі можуть отримати доступ тільки пройшовши авторизацію в окремій групі користувачів з обов'язковим використанням засобів криптографічного захисту. Доступ з фінансової підмережі до інформаційних ресурсів корпоративної мережі повинен бути необмеженим за протоколами ssh, smb.

За протоколом http і ftp доступ можливий в Інтернет і до корпоративних ресурсів. Доступ по протоколу ODBC для драйверів баз динних PostgreSQL повинен бути можливий до корпоративних серверів баз даних. Доступ до служб миттєвих повідомлень можливий тільки через корпоративний сервер Jabber. Всі інші протоколи повинні блокуватися.

На закінчення даної теми слід сказати, що наявність загальної політики доступу до інформаційних ресурсів обов'язково, оскільки це зачіпає налаштування не тільки конкретних пакетних фільтрів, але і налаштування серверів доступу, авторизації, автентифікації і т.д. Повинен також бути писаний документ, що визначає, як технічно реалізований той чи інший пункт політики доступу до інформаційних ресурсів. Форма таких документів довільна, проте документування мережі є запорукою її безпечної експлуатації, і, отже, є обов'язковим.

5.3 Інтеграція голосових сервісів локальної мережі з телефонною мережею

Сучасні мережі передачі даних мають достатню смугу для передачі голосових даних, а комп'ютери і периферія - достатню швидкодію для обробки звуку в реальному масштабі часу. З іншого боку, вартість передачі даних по мережах IP в кілька разів, а іноді і в кілька десятків разів нижче, ніж передача голосу через телефонні мережі загального користування. Очевидно, що зазначені фактори актуалізують проблему інтеграції голосових сервісів

телефонної мережі і мережі передачі даних.

Розглянемо наступні аспекти даної проблеми: обладнання кінцевого користувача, пару телефонної мережі підприємства з комп'ютерною мережею, використання зовнішніх каналів передачі даних для телефонного трафіку.

Устаткування кінцевого користувача для роботи з телефонною мережею не вимагає ніяких змін, оскільки АТС підприємства повністю визначає стандартне обладнання, допустиме для використання.

Єдиний момент, який потребує уваги - це використання однієї і тієї ж СКС для телефонної та комп'ютерної мережі.

Устаткування для мережевих голосових сервісів так само стандартне - гарнітура (мікрофон плюс навушники) і дуплексна звукова карта.

Увагу слід приділити програмному забезпеченню підтримки голосових сервісів. В даний час є ряд стандартів, таких як H.232, які повинні підтримуватися клієнтським ПО для успішної інтеграції з серверної частиною голосових служб. На сьогоднішній день існує досить багато програм, що реалізують ці стандарти. Найбільш популярними є для платформи NetMeeting Windows GnomeMeeting Linux.

Крім того, існує ряд апаратних реалізацій клієнтського обладнання для голосових сервісів, т.зв. EthernetPhones.

Для сполучення телефонної мережі підприємства з голосовими службами комп'ютерної мережі необхідно обладнання, що підтримує, з одного боку, групу стандартів H.232, з іншого боку, інтерфейси до АТС. Такий клас устаткування називається голосовими шлюзами (voice gateways). Стандарти H.232 підтримуються програмно, а на інтерфейс з АТС слід зупинитися окремо. У разі використання аналогової АТС або звичайних аналогових портів цифрової АТС в голосовий шлюз додаються модулі підтримки аналогових ліній, які імітують звичайні аналогові лінії АТС.

Якщо встановлюється сучасна АТС, то найбільш зручним сполученням її з голосовим шлюзом є інтерфейс ISDN BRI, що забезпечує передачу даних в цифровому вигляді для 30 голосових каналів одночасно.

Приклад такого обладнання - сервера голосових шлюзів.

Наведена на малюнку схема включення устаткування дозволяє використовувати для передачі голосу між віддаленими офісами корпоративну мережу або з традиційними телефонами, або за допомогою комп'ютера, або між комп'ютером і звичайним телефоном.

Природно, для якісної передачі голосу по мережі необхідно мати достатній запас пропускної здатності мережі (як мінімум 16 Кбіт / с для одного стисненого каналу) і мінімальну затримку в каналі. Використання асиметричних супутникових каналів практично неприйнятно через асиметрію смуг пропускання, а з симетричними супутниковими каналами можуть виникнути проблеми через значні (350 мс і більше) затримки на поширення сигналу. Тому для організації голосових мережевих сервісів зазвичай використовують наземні канали. Оскільки мережі на основі протоколу IP не пропонують гарантій якості обслуговування (QoS), таких як фіксована затримка і гарантована смуга, необхідно так само не перевантажувати канали, які

використовуються для голосових сервісів. Для передачі голосу часто використовують мережі FrameRelay, які мають кошти забезпечення QoS, однак розцінки на даний сервіс не сильно поступаються розцінками на передачу голосу. а обладнання досить дороге.

6 Рекомендації щодо програмної частини проекту

6.1 Розробка клієнтської частини програм

Розробка клієнтської частини програм повинно здійснюватися з урахуванням переносимості програми на різні платформи. Природно, що написання таких програм "з нуля" заняття дуже трудомістке, особливо. якщо мова йде про створення графічного інтерфейсу. Тому для реалізації клієнтського додатка необхідно використовувати спеціальні Кросплатформені бібліотеки. З вільно розповсюджуваних бібліотек найбільш популярними є wxWidjets, gtk2 для мови C і gtkmm, qt4 для мови C ++. Зазначені бібліотеки дозволяють один і той же код скомпілювати як додаток для ОС Windows, так і для великої кількості систем, що використовують X-Window system і інші графічні системи. Використання одного і того ж коду для різних платформ дозволяє розробнику зосередитися на розробці функціональності системи, а не на перенесенні коду, що істотно підвищує якість програмного продукту. Застосування інтерпретуючих систем є альтернативним шляхом вирішення проблеми переносимості коду, проте це вимагає установки інтерпретатора на цільову систему. Крім того, не всі інтерпретовані мови володіють достатньою швидкістю роботи додатків і тим більше не всі мають достатньо виразних засобів для об'єктного програмування. З найбільш зручних засобів даного класу варто згадати мову Python. Використання Java і компонентів swing є хорошим компромісом між першим і другим варіантом, оскільки забезпечує досить високу швидкість роботи програми за рахунок механізму компіляції JIT, проте все ж таки вимагає установки системи підтримки підчас виконання. До недоліків останніх двох слід так само віднести повільний старт програми. Для реалізації клієнтської частини програми можливий вибір будь-якого із згаданих інструментів, проте вимога до використання одного і того ж коду для різних платформ є істотною.

6.2 Розробка серверної частини програм

Серверна частина програми як правило не має призначеного для користувача інтерфейсу, проте не дивлячись на наявність стандартів ISO на мову C і його стандартну бібліотеку, проблема переносимості ПО стоїть дуже гостро і вимагає від програміста знання кількох операційних систем для написання портованого коду. Навіть для POSIX-сумісних систем є труднощі портування ПО, пов'язані з різними інтерфейсами до системних ресурсів. Можна виділити наступний набір рекомендацій, що полегшують портування вашої програми.

1. Відокремлюйте логіку роботи програми і інтерфейс з системою. Наприклад, для роботи з файловою системою потрібно використовувати свої інтерфейсні функції, що перетворюють рядок шляху до виду, прийнятного для даної ОС.

2. Використовуйте по можливості не системні бібліотеки, а крос-платформенні бібліотеки або надбудови над системними функціями. Наприклад,

для роботи з XML краще користуватися libxml2, а не інтерфейсом, що надаються Visual C ++.

3. При необхідності використання специфічних для даної системи функцій виносьте код, що викликає їх, в окремий модуль компіляції (* .h, * .c) з власними інтерфейсними функціями, однаковими для всіх систем.

4. Не застосовуйте непереносимого коду ніде, крім чітко обумовлених у п.1 трьох місць. Численні макрооператори "#idef OS ..." по тексту програми ускладнюють її сприйняття і ведуть до логічних помилок.

5. Користуйтеся загальноприйнятими стандартами для роботи з підсистемами. Наприклад, для доступу до баз даних використовуйте SQL і ODBC.

6. Не використовуйте бібліотек, що надаються будь-яким окремим компілятором. Наприклад, середовища розробки Borland надають на перший погляд зручний набір інтерфейсних функцій, які ускладнюють перенесення програм не те що на іншу систему, а й на інший компілятор в тій же ОС, оскільки вихідні тексти цих інтерфейсних бібліотек не доступні або використовують специфічні для даного компілятора директиви.

Якщо потрібно написати серверний додаток, але витрати на ретельне портування коду не виправдані, можна писати його під POSIX-сумісну ОС, а для перенесення на MINGW.

Висновок

Результатом даної курсового роботи є проект мережевої кабельної інфраструктури підприємства і проект логічної структури мережі з розміщеними активними мережевими пристроями і системними мережевими сервісами. Результатом програмної частини проекту є набір програм (як мінімум клієнт і сервер) для надання будь-якого мережевого сервісу. Дана робота повинна підтвердити кваліфікацію бакалавра в області проектування мереж і мережевого програмного забезпечення.

Рекомендована література

1. Carla Schroder. Linux Networking Cookbook. M.: O'Reilly Media, 2007.
2. Tony Bautts, Terry Dawson, Gregor N. Purdy. Linux Network Administrator's Guide. M.: O'Reilly Media, 2005.
3. Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley. UNIX and Linux System Administration Handbook (4th Edition). M.: Prentice Hall, 2010.
4. James Turnbull. Hardening Linux. M.: Apress, 2005.
5. Ed Sawicki. Advanced Guide to Linux Networking and Security. M.: Course Technology, 2005.
6. Mike Erwin, Charlie Scott, Paul Wolfe. Virtual Private Networks, 2nd Edition. M.: O'Reilly Media, 1998.
7. Oleg Kolesnikov, Brian Hatch. Building Linux Virtual Private Networks (VPNs). M.: Sams, 2002.
8. Jonathan Hassell. RADIUS. Securing Public Access to Private Resources. M.: O'Reilly Media, 2002.
9. Michael Rash. Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort. M.: No Starch Press, 2007.
10. Steve Suehring, Robert Ziegler. Linux Firewalls (3rd Edition). M.: Novell Press, 2005.
11. Kyle Dent D. Postfix: The Definitive Guide. M.: O'Reilly Media, 2003.
12. Don R Crawley. The Accidental Administrator: Linux Server Step-by-Step Configuration Guide. M.: CreateSpace, 2010.
13. Alistair McDonald. SpamAssassin: A Practical Guide to Integration and Configuration. M.: Packt Publishing, 2004.
14. Alan Schwartz PH.D. SpamAssassin. M.: O'Reilly Media, 2004.
15. Duane Wessels. Web Caching. M.: O'Reilly Media, 2001.
16. Ari Luotonen. Web Proxy Servers. M.: Prentice Hall PTR, 1997.
17. Duane Wessels. Squid: The Definitive Guide. M.: O'Reilly Media, 2004.