

СТРУКТУРНІ КОМПОНЕНТИ РОЗПОДІЛЕНИХ КОРПОРАТИВНИХ МЕРЕЖ

Вінницький національний технічний університет

Анотація

Розглядається перелік вимог до корпоративних комп'ютерних мереж і як це планується реалізувати, розглянуто найбільш актуальний варіант топології мережі та призначення основних елементів.

Ключові слова : комп'ютерна мережа, надійність системи, клієнт, топологія, сервер, робоча станція, елементи, зірка, мережевий екран, WLAN.

Abstract

The list of requirements for corporate computer networks is considered and how it is planned to be implemented, the most actual variant of the topology of the network and the appointment of the main elements is considered.

Keywords: computer network, system reliability, client, topology, server, workstation, elements, star, network screen, WLAN.

Результати дослідження

До корпоративних комп'ютерних мереж, як і до інших типів комп'ютерних мереж, пред'являється ряд вимог. Головна вимога – виконання мережею її основної функції: забезпечення користувачам потенційної можливості доступу до ресурсів всіх комп'ютерів, об'єднаних в мережу. Вирішенню цієї основної задачі підпорядковані інші вимоги: по продуктивності, надійності, відмовостійкості, безпеки, керованості, сумісності, розширюваності, масштабованості, прозорості та підтримці різних видів трафіку.

Найважливішою характеристикою обчислювальної мережі є надійність – здатність правильно функціонувати протягом тривалого періоду часу. Ця властивість має три складових: власне надійність, готовність і зручність обслуговування.

Для оцінки надійності складних систем застосовується наступний набір характеристик:

- Доступність (availability) – означає частку часу, протягом якого система може бути використана. Готовність може бути поліпшена шляхом введення надмірності в структуру системи. Щоб мережу можна було віднести до високонадійної, вона повинна як мінімум мати високу готовність, необхідно забезпечити збереження даних і захист їх від спотворень, повинна підтримуватися узгодженість (несуперечність) даних (наприклад, якщо для підвищення надійності на декількох файлових серверах зберігається кілька копій даних, то потрібно постійно забезпечувати їхню ідентичність).
- Захищеність (security) – здатність системи захистити дані від несанкціонованого доступу.
- Відмовостійкість (fault tolerance) – у мережах під відмовостійкістю розуміється здатність системи приховати від користувача відмову окремих її елементів. У відмовостійкій системі відмова одного з її елементів приводить до деякого зниження якості її роботи (деградації), а не до повного останову. В цілому система буде продовжувати виконувати свої функції;

Основою надійності всіх корпоративних мереж, є надійність мереж зв'язку (СС), але забезпечення високої надійності не є самоціллю, а являє собою засіб досягнення максимальної ефективності мережі[1].

Для реалізації всіх вищезазначених вимог необхідно вірно обрати топологію мережі. Аналізуючи, можна стверджувати, що актуальна на даний момент - топологія «зірка», при цій топології кожен комп'ютер підключаються своїм кабелем до мережного пристрою, наприклад комутатора. Таке

підключення виглядає як зірка, звідки й походить його назва. Даний тип топології - найпоширеніший завдяки надійності мережі і її безмежній розширюваності. З недоліків такої мережі можна назвати тільки високу вартість. До кожного робочого місця потрібно підвести окремий дріт. Кабелі підключаються до багатопортового комутатора або маршрутизатора, який також коштує дорого. З одного боку, вихід з ладу комутатора зупиняє роботу всієї мережі, з іншого - поломка одного з комп'ютерів не впливає на працездатність інших. Для розширення мережі, побудованої за топологією «зірка», потрібно підключити додатковий комутатор, що володіє достатньою кількістю портів. Комутатор є одночасно підсилювачем сигналу, що дозволяє подовжити сегменти мережі. Сигнал, що надходить від передавального комп'ютера, йде на вхід комутатора, посилюється і передається відразу всім комп'ютерам, тому не може загубитися по дорозі[2].

Для того, щоб підвищити рівень надійності мережі необхідно використовувати мережевий екран (Firewall). Він служить захисною стіною між локальною мережею та зовнішньою мережею і запобігає будь-яким загрозам. Щоб задовольнити вимогам широкого кола користувачів, існує три типи мережевих екранів: мережного рівня, прикладного рівня і рівня з'єднання. Кожен з цих трьох типів використовує свій, відмінний від інших підхід до захисту мережі.

Мережевий екран мережного рівня представлений екрануючим маршрутизатором. Він контролює лише дані службової інформації пакетів мережевого і транспортного рівнів моделі OSI. Мінусом таких маршрутизаторів є те, що ще п'ять рівнів залишаються неконтрольованими.

Нарешті, адміністратори, які працюють з екрануючими маршрутизаторами, повинні пам'ятати, що у більшості приладів, що здійснюють фільтрацію пакетів, відсутні механізми аудиту та подачі сигналу тривоги. Іншими словами, маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не будуть проінформовані.

Мережевий екран прикладного рівня також відомий як проксі-сервер (сервер-посередник). Фаєрволи прикладного рівня встановлюють певний фізичний поділ між локальною мережею і Internet, тому вони відповідають найвищим вимогам безпеки. Проте, оскільки програма повинна аналізувати пакети і приймати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність мережі, тому як сервер-посередник використовуються швидші комп'ютери.

Мережевий екран рівня з'єднання схожий на мережевий екран прикладного рівня тим, що обидва вони є серверами-посередниками. Відмінність полягає в тому, що фаєрволи прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби на зразок FTP або HTTP. Натомість, фаєрволи рівня з'єднання обслуговують велику кількість протоколів.

В даній мережі буде використано такі основні елементи:

- Сервер - комп'ютер, який керує обслуговуванням в мережі за допомогою своїх пристроїв, програм і даних, що надає іншим комп'ютерам (робочих станцій мережі, клієнтам) послуги з зв'язку, отримання, пересилання і обробки інформації, а також спільно використовувани ресурси.
- Робоча станція, або хост (host), - комп'ютер, підключений до мережі і має в мережі власний адресу.
- Клієнт - комп'ютер в локальній мережі, на якому користувач запускає прикладні програми та з якого звертається до сервера за забезпеченням зв'язку з іншими комп'ютерами і доступом до мережевих ресурсів (файлів, програм і пристроїв). На відміну від сервера клієнт хоча і підключений фізично до мережі, в окремі моменти часу може бути логічно (програмно) відключений від неї. Ще одна відмінність - у клієнта в різні моменти часу може бути як постійний, так і різний (мінливий в кожному сеансі роботи в мережі) адреса.
- Крім основних дійових осіб (клієнтів, серверів), в мережі є багато інших службових пристроїв, з якими користувач безпосередньо не працює, але від яких серйозно залежить і швидкість роботи в мережі, і її безпеку. Тому користувач повинен знати, які пристрої можна встановити самостійно для посилення захищеності свого комп'ютера або сегмента мережі, якщо вони відсутні на ділянці: комп'ютер користувача - сервер провайдера.
- Комутатор, або світч (switch, switching hub), - комунікаційний пристрій, в якому можлива паралельна незалежна обробка інформації, що надходить на різні порти (входи). Це відрізняє його від моста, де інформація, яка надходить з різних портів, обробляється один за одним (послідовно).
- Маршрутизатор (router) - комплекс програмних і апаратних засобів, що забезпечують в мережі передачу за призначенням (по заданому маршруту) пакетів даних і розділяють інформаційні потоки окремих частин мережі один від одного.

- Шлюз (gateway) - пристрій для з'єднання різнотипних мереж, що працюють з відмінним мережевим програмним забезпеченням і по різних протоколах[3].
- Точка доступу (Access point) призначена для забезпечення бездротового доступу за допомогою технології Wi-Fi мобільних апаратів користувачів до існуючої бездротової або провідної мережі. Вона також може застосовуватися для створення нової бездротової мережі. Точка доступу забезпечує зв'язок у межах прямої видимості на відстанях, що не перевищують 250 м, і на значно менших, якщо на шляху радіохвиль є металеві екрани (металоконструкції, залізобетонні перекриття). З декількох точок доступу може бути побудована локальна корпоративна бездротова мережа (WLAN -Wireless Local Area Network). До кожної точки доступу можуть підключатися до 254 мобільних апаратів. Однак зі зростанням їхньої кількості знижуються швидкості передачі і прийому даних. Рекомендується приєднувати до однієї точки доступу близько 10 мобільних пристроїв. При утворенні бездротової корпоративної мережі з точок доступу здійснюється роумінг, і користувач може підтримувати зв'язок в радіусі її дії. Для точки доступу можливі три режими роботи: безпосередньо в режимі "точка доступу", в режимі "повторювача" і в режимі "моста". Режим "точка доступу" в новому обладнанні встановлений за замовчуванням. При роботі в ньому користувач, оснащений мобільним пристроєм з адаптером Wi-Fi, підключається без всяких налаштувань до бездротової мережі. У режимі "повторювача" (ретранслятора) точка доступу працює як приймач. Вона приймає слабкий сигнал від іншої точки доступу, посилює його і передає на тій же частоті далі, до необхідного адресата. У режимі "моста" точка доступу забезпечує зв'язок між віддаленими об'єктами, об'єднуючи фізично віддалені сегменти мережі в одне ціле. Щоб здійснювалася нормальна робота в режимах "ретранслятор" і "міст", ідентифікатор бездротової мережі (SSID), канал і тип шифрування повинні збігатися[4].

Висновки

Проаналізувавши перелік вимог до корпоративних комп'ютерних мереж було визначено актуальну топологію. Особливу увагу треба звернути на надійність, доступність та захищеність, на основі цього було визначено основні елементи. Саме це дасть змогу забезпечити відповідну роботу систем та якість роботи мережі загалом.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Компьютерные сети. Нисходящий подход. 6-е изд / Куроуз Джеймс, Росс Кит //Т18—Москва.: Издательство «Э», 2016. — 912 с
2. Полный справочник по Cisco 3-е изд. //Пер. С англ. – К.Птицын. :2009. – 1088с.
3. Короткий курс комп'ютерних мереж /Ю. Чекмарьов // Видавництво: ДМК, 2012.
4. Собираем компьютер своими руками / А. Ватаманюк // Видавництво: Питер, 2008.
5. Информатика и информационные технологии : учебник для СПО / М. В. Гаврилов, В. А. Климов // — 4-е изд., перераб. и доп. — М. : Издательство Юрайт, 2015. — 383 с.
6. Инновационные технологии в коммерции и бизнесе : учебник для бакалавров / Л. П. Гаврилов. — М // :Издательство Юрайт, 2016. — 372 с.

Кучмей Денис Вілерійович – студент групи ІКІ-156, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: 1ki15b.kuchmei@gmail.com;

Захарченко Сергій Михайлович – кандидат технічних наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: zahar@vntu.net;

Kuchmei Denys V. – Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : 1ki15b.kuchmei@gmail.com;

Zaharchenko Sergiy M. – Cand. Sc. (Eng.), Associate Professor of the Computer Techniques Chair, Vinnitsa National Technical University, Vinnytsia, e-mail: zahar@vntu.net.