МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДВНЗ «УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»

Факультет інформаційних технологій

Кафедра програмного забезпечення систем

«АДМІНІСТРУВАННЯ КОМПЮТЕРНИХ МЕРЕЖ ТА ОПЕРАЦІЙНИХ СИСТЕМ»

Методичне видання

УЖГОРОД – 2019

Адміністрування комп'ютерних мереж та операційних систем: методичне видання для студентів за спеціальністю 121 «Інженерія програмного забезпечення» факультету інформаційних технологій УжНУ / Розробник: к.т.н., доц. Поліщук В.В. – Ужгород: 2019. – 60 с.

У методичному виданні з курсу «Адміністрування комп'ютерних мереж та операційних систем» розглянуто вісім лекційних занять, що входять до складу робочої програми. Наведений теоретичний матеріал охоплює наступні поняття: основи адміністрування та функції системного адміністратора; комп'ютерні мережі; види комп'ютерних мереж; створення локальної мережі; робота в режимі комутованого доступу; поняття мережного протоколу; служба DNS; огляд та основні можливості операційних систем Windows Server та Windows Server 2019; особливості служби DHCP в системах сімейства Windows Server; планування просторів імен AD; моделі управління безпекою. У методичному виданні наведена програма навчальної дисципліни та перелік запитань на підсумковий контроль.

Розробник: доцент кафедри програмного забезпечення систем факультету інформаційних технологій ДВНЗ «УжНУ», к.т.н., доц. Поліщук В.В.

Рецензенти:

- к.ф-м.н., доц., завідувач кафедри програмного забезпечення систем факультету інформаційних технологій ДВНЗ «УжНУ» Білак Ю.Ю.
- к.т.н., доцент кафедри інформатики та фізико-математичних дисциплін факультету інформаційних технологій ДВНЗ «УжНУ» Лях І. М.

Рекомендовано кафедрою програмного забезпечення систем від «29» січня 2019 р., протокол №6.

ЗМІСТ

Вступ

Метою дисципліни «Адміністрування комп'ютерних мереж і операційних систем» є: формування системи теоретичних і практичних знань у галузі створення та адміністрування комп'ютерних мереж, а також операційних систем.

До **завдань дисципліни** відносяться: вивчення технологій комп'ютерних мереж (протоколів, сучасного обладнання, структурованих кабельних систем); формування навиків розробки проектів комп'ютерних мереж з використанням сучасних програмних комплексів; засвоєння програмного забезпечення та методів управління мережами та принципами їх адміністрування; оволодіння знаннями адміністрування серверних операційних систем сімейства Windows.

Предмет дисципліни: технології комп'ютерних мереж та програмні засоби, що підтримують проектування комп'ютерних мереж.

В результаті вивчення дисципліни студенти повинні:

- **знати** сучасні технології комп'ютерних мереж; протоколи передачі даних; методології створення структурованих кабельних систем; еталонні моделі комп'ютерних мереж; визначення та застосування комп'ютерної мережі; історію розвитку комп'ютерних мереж; основні IP-адреси мереж з виділеними серверами; організацію локальних мереж з магістральною організацією середовища; організацію глобальних мереж та способи управління каналами зв'язку; систему доменних імен Internet (DNS); основи Internet та її безпеку.

- **вміти** спроектувати та розрахувати локальну мережу; налаштовувати стек протоколу TCP/IP; діагностувати функціональність мережі та усувати неполадки; створювати проекти комп'ютерних мереж з використанням сучасних програмних комплексів; визначати IP адреси для абонентів сегментів у мережі; здійснювати обґрунтований вибір середовищ передачі даних.

Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. ТОПОЛОГІЇ МЕРЕЖ ТА ВИДИ ОС.

Тема 1. Вступ. Предмет курсу. Основні поняття, взаємозв’язок з іншими дисциплінами.

Тема 2. Комп’ютерні мережі. Основні положення. Визначення комп'ютерної мережі. Переваги комп'ютерних мереж. Види комп'ютерних мереж.

Тема 3. Створення локальної мережі. Необхідне обладнання. Фізичне підключення до мережі. Встановлення драйвера мережної карти.

Тема 4. Робота в режимі комутованого доступу. Підключення модему. Використання модему. Підключення зовнішнього модему телефонної лінії. Налагодження модема. Налагодження з'єднання.

Тема 5. Вибір та встановлення мережного протоколу. Надання мережного імені та робочої групи комп'ютера. Надання ресурсів у загальне користування. Робота з локальною мережею.

ЗМІСТОВИЙ МОДУЛЬ 2. АДМІНІСТРУВАННЯ ОС.

Тема 6. Служба DNS: простір імен, домени. Діагностичні утиліти TCP/IP і DNS. Зони прямого і зворотного перегляду, основні і додаткові зони. Рекурсивний і ітеративний запити на дозвіл імен.

Тема 7. Огляд та основні можливості ОС Windows Server. Системні вимоги. Загальна характеристика Windows Server. Апаратні ресурси. Основні сервіси. Служба DHCP. Особливості служби DHCP в системах сімейства Windows Server.

Тема 8. Планування просторів імен AD. Встановлення контролерів доменів. Призначення служби каталогів AD. Моделі управління безпекою: робоча група; доменна модель безпеки.

Самостійна робота

№ п/п	Назва теми
1.	Вступ. Предмет курсу. Основні поняття, взаємозв’язок з іншими дисциплінами
2.	Компютерні мережі. Основні положення. Визначення комп'ютерної мережі. Переваги комп'ютерних мереж. Види комп'ютерних мереж.
3.	Топології локальних мереж.
4.	Створення локальної мережі. Необхідне обладнання. Фізичне підключення до мережі. Встановлення драйвера мережної карти.
5.	Вибір та встановлення мережного протоколу. Надання мережного імені та робочої групи комп'ютера. Надання ресурсів у загальне користування. Робота з локальною мережею.
6.	Робота в режимі комутованого доступу. Підключення модему. Використання модему. Підключення зовнішнього модему телефонної лінії. Налагодження модема. Налагодження з'єднання.
7.	Робота в режимі комутованого доступу. Підключення до Інтернет. Налаштування модуля віддаленого доступу до мережі. Налагодження сполучення із провайдером.
8.	Протоколи та методи доступу еталонної моделі взаємодії відкритих систем OSI. Вузли мережі, мережеві ОС – Novell Netware, UNIX та Windows.
9.	Протоколи TCP/IP; базові IP-адреси локальної мережі (LAN). Структура мережі Ethernet IEEE 802.3 – фізичний та канальний рівні.

Лекція №1. Вступ. Предмет курсу. Поняття про системне адміністрування

Мета заняття: ознайомити студентів із предметом дисципліни, задачами в області мережевого адміністрування, задачами системного адміністратора та технологій сучасних мереж.

Зміст заняття

1. **Вступ.**
2. **Мережне і системне адміністрування.**

Мережне і системне адміністрування

У багатокористувацькій операційній системі (ОС) повинен бути зареєстрований принаймні один користувач, який виконує роль системного адміністратора. Він відповідає за функціонування системи, володіє навичками, потрібними для усунення помилок і збоїв, забезпечує користувачів необхідними програмними засобами.

Операційна система – це базовий комплекс програмного забезпечення, що виконує управління апаратним забезпеченням комп'ютера або віртуальної машини; забезпечує керування обчислювальним процесом і організує взаємодію з користувачем. Операційна система звичайно складається з ядра операційної системи та базового набору прикладного програмного забезпечення.

Автентифікація – процес перевірки достовірності користувачем даних, введених у систему, який полягає у порівнянні його імені та пароля даними, що зберігаються в базі даних операційної системи.

Авторизація – процес надання доступу до мережних ресурсів. Зазвичай відбувається після автентифікації.

Сьогодні неминучим є 2 процеси - інтеграція **системного** і **мережного** адміністрування.

Задачі, розв'язувані в даній області, розбиваються на дві групи: **контроль за роботою мережного устаткування** й **управління функціонуванням мережі** в цілому. **У першому випадку** мова йде про моніторинг окремих мережних пристроїв (концентраторів, комутаторів, маршрутизаторів, серверів доступу й ін.), настроюванню і зміні їхньої конфігурації, усуненні виникаючих збоїв. Ця достатньо традиційна група задач одержала назву реактивного адміністрування (reactive management). **Друга група** націлена на моніторинг мережного трафіка, виявлення тенденцій його зміни й аналіз подій із метою реалізації схем пріоритеризації для забезпечення максимальної пропускної спроможності (proactive management). Сюди ж відноситься задача внесення змін

у конфігурацію мережі, управління IP-адресами користувачів, фільтрація пакетів в цілях забезпечення інформаційної безпеки і ряд інших задач.

Індустрія ПЗ мережневого управління виявилася розділеною на три частини:

1. утворюють платформи мережного управління – аналоги операційних систем, що формують середовище для запуску додатків, але при цьому вони володіють обмеженою функціональністю;
2. мережеві програм, що пов'язані з керуючими додатками виробників мережних апаратних засобів. Проте вони розраховані на управління тільки визначеною групою пристроїв і рідко дозволяють обслуговувати вироби інших компаній. Подібні додатки пропонуються практично усіма відомими постачальниками устаткування;
3. численні програми третіх фірм, націлені на рішення вузьких задач мережного адміністрування.

Системний адміністратор відповідає за виконання всіх вимог ОС і вирішує завдання, пов’язані з роботою системи.

Системний адміністратор – фахівець, відповідальний за проектування, встановлення, конфігурування, управління й обслуговування мереж і систем. Він повинен мати відповідні знання й уміння стосовно встановлення й налаштування системи для забезпечення її функціонування для багатьох користувачів. Таке конфігурування вимагає корректного виконання завдань з різними пріоритетами.

Клієнт–сервер – мережна архітектура, в якій усі пристрої є або клієнтами, або серверами. Клієнтом є машина (зазвичай ПК), що відправляє запит, сервером – машина, що відповідає на запит. Обидва терміни (клієнт і сервер) можуть бути застосовані як до фізичних пристроїв, так і до программного забезпечення.

Адміністратор повинен бути експертом з питань функціонування систем і мереж. Він повинен уміти знаходити компроміс між вимогами користувачів та можливостями їх реалізації у системі. Системний адміністратор розробляє правила роботи в корпоративній мережі та пояснює їх користувачам. Такі правила повинні базуватися на трьох основних положеннях:

I. Максимальний доступ користувачів до власних ресурсів.

   Перше положення передбачає створення розподілених ресурсів для кожного користувача мережі та надання йому повного доступу до них.

Розподілені системи можуть бути побудованими на основі однорангових мереж або на основі мереж з виділеним сервером.

Сервером є комп'ютер мережі, який надає свої ресурси (інформаційні, обчислювальні) іншим комп'ютерам, які називають клієнтами (робочими станціями). Бажано, щоб віддалений доступ до ресурсів мережі був організований різними засобами (VPN-сервер, FTP-сервер, RAS-сервер, сервер терміналів тощо).

Одноранговi мережі – такі комп'ютерні мережі, в яких відсутні сервери, а кожен користувач є як клієнтом, так і сервером одночасно.

II. Максимальне обмеження доступу до ресурсів інших користувачів.

Користувачі повинні мати доступ лише до власних ресурсів й не мати доступу до ресурсів інших користувачів або хоча б не мати доступу для внесення змін. Звичайно в деяких випадках, потрібно мати доступ до ресурсів інших користувачів. У такому разі потрібно додати «чужі» облікові записи до облікового запису групи (підрозділу) та надати відповідні дозволи для неї.

III. Відповідальність користувачів за збереження власних ресурсів.

Третє положення передбачає формування у працівників розуміння, що за цілісність власних даних першочергово несе відповідальність користувач-власник. Користувачі корпоративної мережі повинні зберігати в таємниці власні реєстраційні дані. Кожен працівник персонально несе відповідальність за конфіденційність зберігання і паролів. Із метою підвищення безпеки збереження даних, особливо від атак добору паролів, користувачам доцільно час від часу змінювати власні паролі.

Завдання, які доводиться виконувати системним адміністраторам.

1. Встановлення та конфігурування апаратного забезпечення.
2. Встановлення та конфігурування мережних ОС.
3. Керування обліковими записами користувачів. Додавання, видалення облікових записів користувачів і визначення їх привілеїв.
4. Налаштування пристроїв, розподілених і локальних ресурсів.
5. Створення резервних копій. Визначення правил створення резервних копій для зниження втрат і відновлення даних після можливих збоїв у роботі системи.
6. Вимикання системи. Коректне вимикання системи дає змогу уникнути втрат даних і збоїв файлової системи.
7. Навчання користувачів. Навчання користувачів особливостей роботи у системі для підвищення ефективності їхньої праці.

8. Надання допомоги користувачам. Адміністратор виступає в ролі експерта, який допомагає користувачам вирішувати їхні проблеми, пов’язані з експлуатацією системи.
9. Забезпечення безпеки системи. Системний адміністратор організовує взаємодію користувачів на основі їх привілеїв.
10. Ведення системного журналу та реєстрація змін у системі. Переважна більшість сучасних мережних ОС дає змогу відслідковувати зміни у системі. Для цього використовують системні журнали різноманітних форматів (як текстових, так і кодованих).
11. Документування власної діяльності щодо адміністрування мережі.

Лекція №2. Комп’ютерні мережі

Мета заняття: ознайомити студентів із класифікацією комп’ютерних мереж.

У словниках *мережа* визначена як "система взаємодіючих ліній або каналів зв'язку".

Комп'ютерна мережа - це два або більше пристроїв обробки та зберігання інформації, з'єднаних між собою каналами зв’язку з метою спільного використання мережних ресурсів.

З'єднання може бути утворене за допомогою кабелю (коаксіального, крученої пари або оптично-волоконного) або за допомогою бездротових засобів: радіосигналів, лазерного променя, інфрачервоних пристроїв, супутників зв'язку і т.д. Спільно використовуваною інформацією або ресурсами (які називаються *поділюваними ресурсами)* можуть бути файли, програми, принтери, модеми і будь-яке інше устаткуванн.

Класифікація комп'ютерних мереж

І. По області дії

Класифікація комп'ютерних мереж по області дії враховує географічний район, охоплений мережею, і, у меншому ступені, розмір мережі. При такій класифікації виділяють наступні типи комп'ютерних мереж:

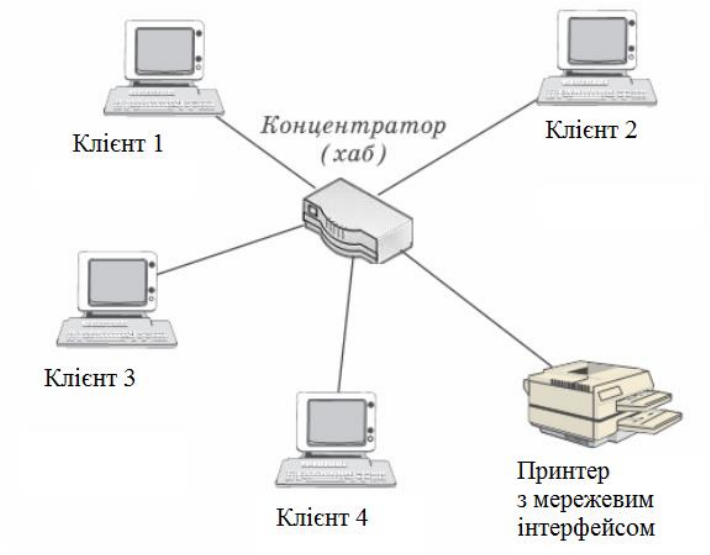
• локальні (Local Area Network - LAN);
• міські (Metropolitan Area Network - MAN);
• глобальні (Wide Area Network - WAN).

Тип мережі до деякої міри залежить від її розміру, тобто від кількості підключених комп'ютерів і користувачів: локальні мережі звичайно менше міських, котрі, у свою чергу, звичайно менше глобальних. До деякої міри тип залежить також від фінансових ресурсів: глобальні мережі, як правило, коштують дорожче і вимагають великих витрат на підтримку, ніж локальні. Однак найбільш істотним, фактором класифікації є географічна область, що покривається мережею.

1. Локальні мережі

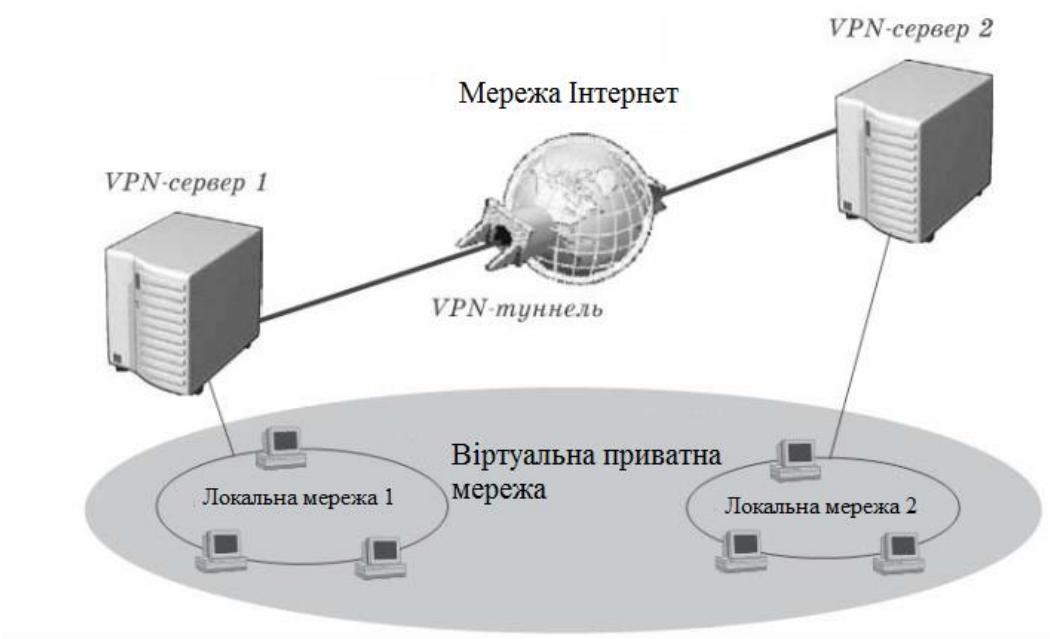
У тлумачному словнику *локальний* означає "місцевий, такий що не виходить за визначені межі". Аналогічно цьому термін "локальна мережа" означає мережу, що охоплює обмежену площу. Комп'ютери, що належать локальній мережі, розташовані недалеко один від одного.

Графічне представлення простої локальної мережі наступне.



2. Міські мережі

Міська комп'ютерна мережа складається з двох або більшої кількості локальних мереж, розташованих на площі, що приблизно відповідає великому місту, звідки і походить їхня назва. Звичайно міська мережа являє собою загальнодоступну комп'ютерну мережу з високими параметрами продуктивності. Максимальна відстань між вузлами міської мережі приблизно дорівнює 80 кілометрам.



3. Глобальні мережі

Глобальними називаються комп'ютерні мережі, що охоплюють великі географічні простори. Кращим і найбільш знайомим прикладом глобальної мережі є Internet. Однак існують і приватні глобальні мережі. У глобальних мережах для з'єднання їхніх складових частин можуть використовуватися

приватні лінії, однак найчастіше для цього використовуються загальнодоступні засоби зв'язку, наприклад система телефонного зв'язку.

II. По способах адміністрування

Комп'ютерні мережі можна класифікувати по способах адміністрування, тобто в залежності від того, хто і як керує поділюваними ресурсами. Комп'ютерна мережа може бути побудовчана в такий спосіб:

• як однорангова робоча група, у якій кожен комп'ютер виконує функції як сервера, так і клієнта, причому кожен користувач самостійно керує ресурсами свого комп'ютера;

• як мережа клієнт/сервер, у якій функції адміністрування зосереджені на центральному комп'ютері зі спеціальною мережною операційною системою; при цьому на центральному комп'ютері виконується аутентифікація користувачів, паролів і іншої реєстраційної інформації для реєстрації користувачів і надання їм доступу до ресурсів.

1. Однорангові мережі

Однорангова структура добре підходить для невеликих мереж, у яких вимоги до безпеки не дуже високі. У більшості книг по мережних технологіях рекомендується включати в однорангову мережу не більш 10 комп'ютерів.

2. Сервер/клієнт

Сервер - це комп'ютер, що надає доступ до ресурсів мережі (даних, програмного забезпечення, периферійного устаткування) в залежності від аутентифікації користувача.

Клієнт (клієнтський комп'ютер) - це комп'ютер, що одержує доступ до ресурсів мережі.

Термін клієнт може також позначати програми, що мають доступ до програм сервера.

III. По мережних операційних системах

Іноді мережі класифікують по встановленим на серверах мережним операційним системам, що використовуються для керування мережею.

1. Мережі Microsoft Windows

Найбільш поширені наступні серверні операційні системи компанії Microsoft: Windows Server, 2003, 2008, 2012, 2016, 2019. Мережі клієнт/сервер на основі Windows називаються *доменами.*

2. Мережі NetWare

Досить розповсюджена мережна операційна система NetWare компанії Novell надає реєстраційну систему безпеки і підтримує функції збереження

файлів і черги друку. NetWare містить служби каталогів, що використовують ієрархічну базу даних NDS (NetWare Directory Services), аналогічну системі Active Directory компанії Microsoft.

3. Мережі UNIX

Система Linux являє собою "варіацію на тему" UNIX. Розповсюджені версії Linux — RedHat, Caldera, Fedore Core.

4. Змішані мережі

В даний час більшість мереж, що служать проміжною ланкою для зв'язку з великими мережами, можна розглядати як змішані. Вони реалізовані на основі програмного забезпечення різних постачальників.

IV. По протоколах

Іноді комп'ютерні мережі класифікують на основі використовуваних ними протоколів. *Мережний протокол* - це набір правил, яких дотримують зв'язані комп'ютери при установці і підтримці зв'язку за допомогою мережі.

1. Мережі NetBEUI

Протокол NetBEUI (NetBIOS Extended User Interface) звичайно використовується в невеликих простих локальних мережах на базі операційних систем Microsoft. Протокол NetBEUI не може бути маршрутизованим. Це означає, що якщо мережа розділена на підмережі, то для комунікації з комп'ютерами інших підмереж потрібно використовувати інший локальний мережний протокол. Перевагами мереж NetBEUI є простота, висока швидкодія і низькі накладні витрати.

2. Мережі IPX/SPX

Стек протоколів IPX/SPX (Internet Package Exchange/Sequenced Packet Exchange) використовується як протокол локальних мереж Novell. Для мереж NetWare цей протокол є обов'язковим. Протокол IPX/SPX звичайно використовується в мережах NetWare, однак він може використовуватися й в інших мережах. Робоча група або домен комп'ютерів Microsoft теж можуть використовувати протокол IPX/SPX.

3. Мережі TCP/IP

TCP/IP - це абревіатура терміну Transmission Control Protocol/Internet Protocol (Протокол керування передачею/Протокол Internet). Фактично TCP/IP не один протокол, а декілька. Саме тому ви часто чуєте, як його називають стеком, або комплектом протоколів, серед яких TCP і IP - два основних. Фактично TCP/IP представляє цей базовий набір протоколів Інтернету, відповідальний за розбивку вихідного повідомлення на пакети (TCP), доставку пакетів на вузол адресата(IP) і збирання (відновлення) вихідного повідомлення з пакетів (TCP).

З усіх розповсюджених протоколів локальних мереж протоколові TCP/IP властива найбільша складність конфігурування. Незважаючи на це, він усе-таки отримав широке поширення. Це пояснюється наступними причинами:

• У протоколі TCP/IP використовується гнучка схема адресації, винятково вдала для маршрутизації навіть у найбільших мережах.

• Протокол TCP/IP підтримується практично у всіх операційних системах і на всіх платформах.

• До даного часу розроблене і застосовується величезна кількість інструментів і утиліт для моніторингу і керування комплектом протоколів TCP/IP.

• Протокол TCP/IP де-факто є протоколом глобальної мережі Internet. У будь-якій системі, що підключається до Internet, повинний бути реалізований протокол TCP/IP.

V. По топології

Мережі можна класифікувати також по їх фізичній або логічній *топології. Фізична топологія* означає форму мережі, тобто шлях прокладки кабелю. *Логічна топологія* означає шлях, по якому сигнали проходять з однієї точки мережі в іншу. Перелічимо найбільш розповсюджені *фізичні топології* локальних мереж:

• шинна;
• кільцева;
• зіркоподібна;
• змішана.

VI. **По архітектурі**

Ще один спосіб класифікації мереж — по архітектурі. У загальному випадку поняття *мережної архітектури* має на увазі набір специфікацій, що визначають фізичну і логічну топології, типи кабелів, обмеження на відстань, методи мережного доступу, розмір пакетів, структуру заголовків і інші фактори. Іноді ці специфікації називаються *протоколами канального рівня.*

В даний час найбільш популярною архітектурою локальних мереж є Ethernet.

1. Мережі Ethernet

Архітектура Ethernet, розроблена в 1960-х роках і удосконалена компаніями Xerox, Digital і Intel.

Мережі Ethernet фізично конфігуруються як шини або зірки. Як метод мережного доступу в Ethernet використовується множинний доступ з

контролем несущої і виявленням конфліктів (Carrier Sense Multiple Access Collision Detect - CSMA/CD).

Виділяються наступні архітектури Ethernet:

• 10Base 5;
• 10Base 2;
• 10Base T;
• 100Base T;
• 1000 Base T;
• 10Base FL/100Base FX/1000Base LX-SX/10000 Base X;

Розглянемо основні характеристики кожної архітектури Ethernet:

Ethernet 10Base5

Мережу l0Base5 іноді називають стандартною Ethernet, хоча в даний час вона вже не так поширена, як деякі інші типи Ethernet. У мережі 10Base5 використовується товстий коаксіальний кабель (товщиною небагато більше сантиметра), томе її називають товстою мережею. Число 10 у назві l0Base5 означає максимальну пропускну здатність: 10 Мбіт/с. Число 5 означає максимальну довжину сегмента: 500 метрів. У товстих мережах використовується шинна топологія.

Ethernet 10Base2

Досить поширені коаксіальні мережі 10Base2, у яких використовується більш тонкий кабель (приблизно півсантиметра діаметром). Ці мережі дешевше, а кабель більш гнучкий, чим у 10Base5. Число 2 у назві мережі означає округлене значення максимальної довжини сегмента, що дорівнює 185 метрів. Як і в 10Base5, у тонких мережах використовується шинна топологія з термінаторами на кожному кінці.

Ethernet із крученими парами

В даний час при установці нових локальних мереж найчастіше використовуються кабель "кручена пара", (буква Т означає *twisted — скручений).*

Мережі 10BaseT

Специфікація l0BaseT була популярна в локальних мережах будь-яких розмірів. Вона визначає мережі Ethernet із пропускною здатністю 10 Мбіт/с, топологія "зірка", максимальна довжина сегменту кабеля – 100 метрів.

Мережі 100BaseT (Fast Ethernet)

Специфікація 100BaseT визначає мережі Ethernet із пропускною здатністю 100 Мбіт/с, виконані на кабелях категорій 5 і 5е. У цих мережах використовуються та ж топологія і методи доступу, що й у 10BaseT. І дійсно, єдина їхня відмінність - вимоги до пропускної здатності кабелю, мережних адаптерів і концентраторів, що повинні забезпечувати швидкість передачі 100 Мбіт/с.

Використовувані категорії кручених пар

Категорія	Максимальна пропускна здатність (швидкість)	Характеристики й область застосування
Cat 1	Тільки для голосу	Тільки в телефонних мережах
Cat 2	4 Мбіт/с	Для передачі даних не рекомендується
Cat 3	16 Мбіт/с	Нижчий рівень розпізнавання даних; використовується головним чином у телефонних мережах
Cat 4	20 Мбіт/с	Придатний для Ethernet із пропускною здатністю 10 Мбіт/с
Cat 5	100Мбіт/с	Найбільш розповсюджена категорія в локальних мережах; використовується в Fast Ethernet (100 Мбит/с)
Cat 5e (Enhanced)	155 Мбіт/с	Використовується в Fast Ethernet і мережах ATM 155 Мбіт/с
Cat 6 і 7	1 Гбіт/с і вище	Використовується в нових технологіях Gigabit Ethernet

Кабелі категорії 6, 7 поки що зустрічаються не часто, оскільки їхні специфікації визначені порівняно недавно.

Мережі 1000BaseT (Gigabit Ethernet)

Перші стандарти високошвидкісний Ethernet, найчастіше називаної Gigabit Ethernet, були розроблені організацією IEEE у 1996 році й опубліковані як специфікації 802.3z. Ці стандарти передбачають передачу даних зі швидкістю 1000 Мбіт/с, у них використовуються формат кадру Ethernet 802.3 і метод доступу CSMA/CD.

Мережі 10Base FL/100Base FX/1000Base LX-SX/10000 Base X;

Букви FL у назві мереж означають *fiber link — волоконно-оптичний зв'язок*. У цих мережах використовується немодульована передача сигналів по волоконно-оптичному кабелю. У волоконно-оптических кабелях для представлення нулів і одиниць інформації застосовується не електричний сигнал, а світлові імпульси. Великою перевагою волоконної оптики в порівнянні з мідними кабелями є відсутність перешкод і *загасання* (тобто зменшення потужності сигналу з відстанню). Довжина ділянки волоконно-оптического кабелю, що задовольняє специфікаціям, може досягати від 2000 метрів до 80 кілометрів.

Лекція №3. Створення локальної мережі

Мета заняття: опанування основними поняттями створення локальної мережі в малому офісі засобами LAN, USB, WLAN та BT-з'єднанням; вивчення необхідного обладнання для створення локальної мережі.

Створення локальної офісної мережі.

Розглянемо п'ять способів створення локальної мережі в малому офісі таким засобами:

1) LAN-з'єднання;
2) USB-з'єднання;
3) FireWire-з'єднання;
4) WLAN-з'єднання; (радіоканал)
5) BT-з'єднання.

Для **LAN-з'єднання** потрібно мати LAN - адаптер і Ethernet-кабель марки Crossover (до 100 м). Встановлюють обладнання і вмикають комп'ютери. Під час завантаження операційна система знайде новий пристрій та проаналізує його. Далі ОС зареєструє цей пристрій і запропонує встановити драйвер від виробника адаптера або сумісний з ним драйвер-двійник зі своєї бібліотеки.

Після коректного встановлення систему потрібно перезавантажити. Якщо все відбулось без помилок, то мережний адаптер з'явиться у списку пристроїв. Тепер слід відкрити панель керування, а в ній - папку мережні підключення. Вибирають свій адаптер і задають його властивості щодо
взаємодії з протоколом TCP/IP ввівши у поле IP- адресу таку адресу з чотирьох груп чисел: 192.168.0.1. на першому ПК і 192.168.0.2 на другому. Маску підмережі 255.255.255.0 можна не вводити, вона буде згенерована автоматично. Більше нічого вводити не потрібно. Залишається перейти у вікно властивості системи (комбінацію клавіш Win+Break) і на закладці назва комп'ютера задати імена комп'ютера і робочої групи, наприклад PPL-1 і IFPPL. Швидкість передачі даних залежить від типу мережної карткиLAN і може бути 10,100 або 1000 Мбіт/с.

Два комп'ютери можна з'єднати через **USB-порти**. Довжини кабелів 1,5 або 5 м. Для більших відстаней потрібно встановити спеціальний концентратор. Теоретична швидкість передачі даних - до 480 Мбіт/с. Програма, яку продають разом з кабелем, повинна бути запущена одночасно на двох комп'ютерах. Саме вона відповідає за передачу даних між комп'ютерами.

Недорого кабельного з'єднання двох комп'ютерів досягають за наявності **FireWire-адаптерів**. Потрібен спеціальний FireWire кабель є довжиною до 6 м . Швидкість передачі даних - до 400 Мбіт/с.

WLAN або **Wi-Fi** . Середовища передавання - безкоштовне (повітря). Вид сигналів - високочастотні радіосигнали. Мережа працює за наявності в комп'ютері спеціального WLAN (Wi-Fi) адаптера. Під час створення бездротових мереж використовують спеціальні точки доступу радіусом дії до 200 м на відкритій місцевості і до 40 м в будинках.

Різновидом безкабельної мережі є з'єднання за технологією високочастотного випромінювання малого радіусу дії зі зміщенням частоти - **Bluetooth (BT).** Для створення такої мережі необхідно мати Bluetooth адаптер, який під'єднують до USB порта. Швидкість передачі даних невелика - від 0,4 до 0,7 Мбіт/с. Два адаптери від різних виробників можуть не працювати в парі. Відстань з'єднання - 10-100м. Рівень захисту інформацій ненадійний. Будь-які електромагнітні хвилі чи несприятливі погодні умови можуть створити перешкоди для коректної передачі даних.

Локальна мережа

За допомогою локальної мережі один комп'ютер отримує доступ до ресурсів іншого, таких, як дані та периферійні пристрої (принтери, модеми, факси тощо). Використання комп'ютерних мереж дає можливість розподілу ресурсів великої вартості, покращання доступу до інформації, виконувати швидке та якісне прийняття рішень.

Сучасні локальні мережі будуються на основі топології **зірка** з використанням концентраторів (хабів), комутаторів (світчів) та кабелю UTP чи STP 5ї категорії (**вита пара**). Дана технологія, що носить назву Fast Ethernet дозволяє проводити обмін інформацією на швидкостях 100Мбіт/с, 1Гбіт/с, 10Гбіт/с та навіть 100Гбіт/с.

Мережеве обладнання – пристрої, необхідні для роботи комп'ютерної мережі, наприклад: маршрутизатор, комутатор, концентратор, патч-панель та ін. Зазвичай розрізняють активне та пасивне мережеве обладнання.

Хаб або мережевий концентратор – працює на фізичному рівні мережевих протоколів – розмножує дані, що надходять на один порт з усіх інших.

Мережеві маршрутизатори – він може роздавати IP-адреси по DHCP, контролювати допустимі IP-адреси. Це мережевий пристрій, який підключається між локальною мережею й інтернетом. Часто маршрутизатор не обмежується простим пересиланням даних між інтерфейсами, а також виконує й інші функції: захищає локальну мережу від зовнішніх загроз, обмежує доступ користувачів локальної мережі до ресурсів інтернету, роздає IP-адреси, шифрує трафік і багато іншого.

Лекція №4. Робота в режимі комутативного доступу

Мета заняття: опанування основними поняттями роботи в режимі комутативного доступу; вивчення технології ADSL та його необхідне обладнання; оволодіння основних схем підключення ADSL-модему до телефонної лінії.

Комутована лінія зв'язку (Dial-up link) – лінія зв'язку, встановлювана тільки на час з'єднання пристрою-передавача і пристрою-приймача.

Для зв'язку з інтернетом, як правило, в даних лініях використовується модем і телефонна лінія. В комп'ютерних мережах використовуються мережеве обладнання і різні лінії зв'язку.

Використання ущільнення, для перевищення швидкості в 56 Кбіт/сек
Стандарти V.42, V.42bis і стандарт V.44 дозволяють модему передавати дані швидше, ніж 56 Кбіт/сек.

- **V.42** - Інша назва — V.34+. Максимальна швидкість 33600 бит/с. Знижені швидкості: 31200, 24000 і 19200 бит/с.
- **V.42bis** - Протокол виявлення і корекції помилок для передачі даних з високими швидкостями.
- **V.44** - Протокол стиснення даних. Допускає перемикання з режиму стиснення в прозорий режим і назад, причому незалежно для кожного напряму

Заміна широкосмуговою мережею

Широкосмуговий зв'язок типово пропонує швидкість починаючи від 128 кбіт/сек і вище за меншу ціну, ніж dialup.

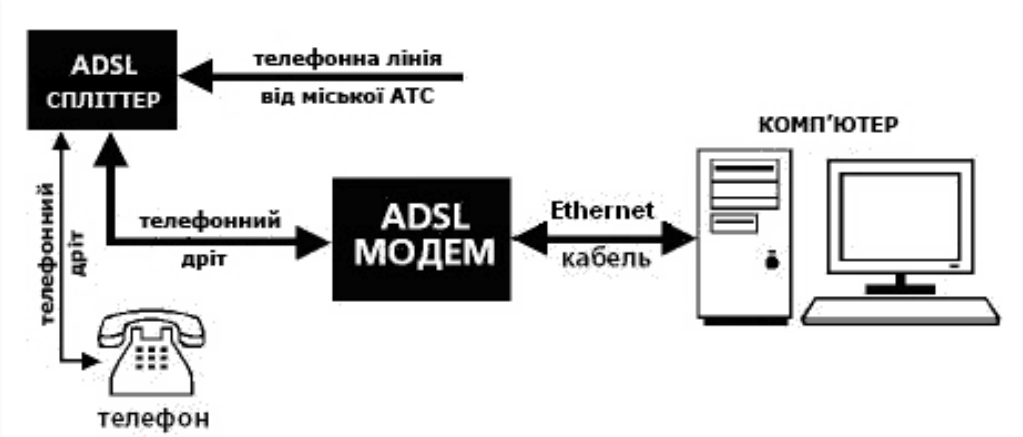
Підключення модему

Модем (*Modem* - скорочення від модулятор-демодулятор). Пристрій зв'язку для перетворення аналогового сигналу в дискретний (модуляція) та навпаки (демодуляція), що дозволяє комп'ютеру передавати дані по телефонній лінії.

Модеми поділяють на *внутрішні* (що встановлюються усередині системного блока) та *зовнішні* (що встановлюються ззовні системного блока).

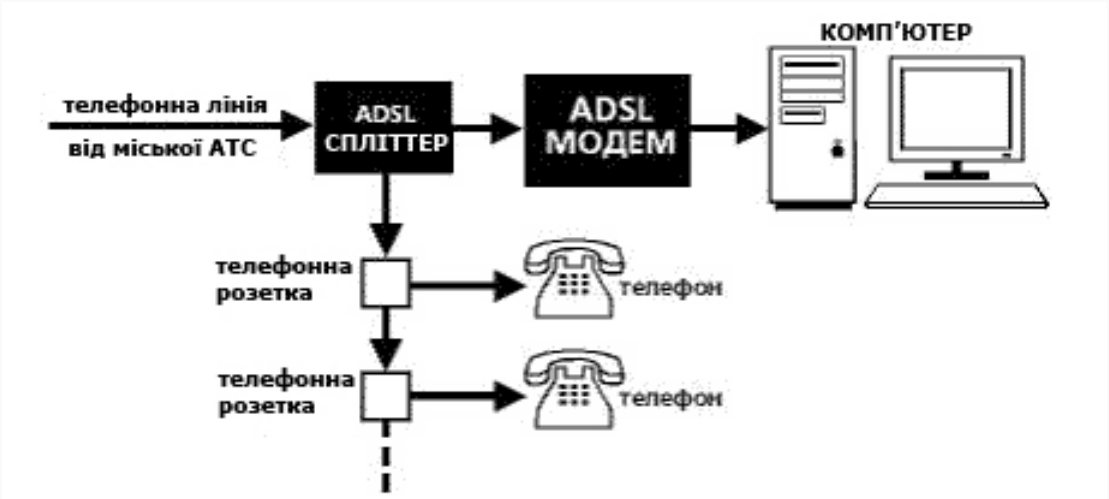
Підключення ADSL-модему до телефонної лінії

Типова схема підключення ADSL-модему:



- ADSL-спліттер розділяє частоти голосового сигналу (0,3 - 3,4 КГц) від частот, які використовуються ADSL-модемом (26 КГц - 1.4 Мгц). Таким чином, виключається взаємний вплив модему і телефонного апарату.

При використанні більш ніж одного телефонного апарату схема підключення виглядатиме таким чином:



Тобто, першим пристроєм, який буде підключений до телефонної лінії від АТС, повинен бути ADSL-спліттер, до якого підключається вся решта пристроїв. Інакше - кожен телефонний апарат необхідно підключати через окремий мікроспліттер:

ADSL(*Asymmetric Digital Subscriber Line*) – технологія широкосмугового доступу, яка забезпечує передачу швидкісного цифрового сигналу звичайною аналоговою телефонною лінією, та дозволяє одночасно користуватися телефоном і Інтернетом. Розроблена Bellcore у 1988 році. ADSL призначена для високошвидкісного доступу до Інтернет. ADSL відноситься до класу широкосмугових (broadband) технологій. Вона забезпечує швидкість передачі даних в напрямку абонента — до 24 Мбіт/сек., від абонента — до 3.5 Мбіт/сек.

ADSL модеми випускаються з двома типами інтерфейсів: USB і 10/100Base-T. Перші призначені для індивідуального підключення і зручні тим, що не потребують блока живлення. Другі зручніші при багатьох підключеннях і, як правило мають вбудовані роутери, в т.ч. бездротові. Для розділення низькочастотного аналогового сигналу та високочастотного цифрового використовується сплітер, який являє собою фільтр низької частоти.

Лекція №5. Вибір та встановлення мережевого протоколу

Мета заняття: повторення основ розуміння студентами основних принципів функціонування комп'ютерної мережі, дозволить системно та кваліфіковано підійти до адміністрування мереж. Вивчити основні принципи, поняття та твердження, на основі еталонної моделі взаємодії відкритих систем ISO OSI. Відповідність рівнів моделі OSI пізнати на найпоширенішому мережному протоколу TCP/IP. Наведені теоретичні основи дозволять чітко вибирати необхідний мережевий протокол для встановлення і передавання даних. Під час лекційного заняття виховувати потяг до наукової творчості, патріотичну свідомість.

Зміст заняття

1. **Поняття мережевого протоколу.**
2. **Модель OSI.**
3. **Мережевий протокол TCP/IP.**

1. Поняття мережевого протоколу

Мережевий протокол в комп'ютерних мережах – заснований на стандартах, що визначають принципи взаємодії комп'ютерів в мережі.

Протокол також задає загальні правила взаємодії різноманітних програм, мережевих вузлів чи систем і створює таким чином єдиний простір передачі.

Хости (будь-який вузол мережі що відправляє або приймає дані через мережу називають хостом (host)) взаємодіють між собою. Для того, щоб прийняти і обробити відповідним чином повідомлення, їм необхідно знати як сформовані повідомлення і що вони означають. Прикладами використання різних форматів повідомлень в різних протоколах можуть бути встановлення з'єднання з віддаленою машиною, відправка повідомлень електронною поштою, передача файлів. Зрозуміло, що різні служби використовують різні формати повідомлень.

Протокол описує:

1. формат повідомлення, якому програми зобов'язані слідувати;
2. спосіб обміну повідомленнями між комп'ютерами в контексті визначеної дії, як, наприклад, пересилка повідомлення по мережі.

Процес визначення адресата пакета за інформацією із його заголовків називають **демультиплексуванням пакетів.**

Мережний протокол надає два інтерфейси:

1. **Однорівневий,** або **інтерфейс протоколу** призначений для взаємодії із реалізацією протоколу того самого рівня на віддаленому мережному вузлі. Це інтерфейс протоколу, що реалізує безпосереднє передавання даних на віддалений вузол. Такий інтерфейс забезпечують заголовком пакета, який доповнюють реалізацією цього протоколу перед передаванням пакета мережею.
2. **Інтерфейс сервісу** призначений для взаємодії із засобами вищого рівня; за його допомогою реалізують мережний сервіс.

Набір протоколів різного рівня, що забезпечують реалізацію певної мережної архітектури, називають **стеком протоколів** або **набором протоколів**.

Також дуже важливо розрізняти два схожі за назвою, але діаметрально протилежні за властивостями, терміни – **маршрутизований протокол** та **протокол маршрутизації**. Ще більша плутанина виникає з оригінальною назвою — routed&routing protocols.

Маршрутизований протокол – це будь-який мережний протокол, адреса мережевого рівня якого надає достатньо інформації для доставки пакету від одного вузла мережі до іншого на основі використовуваної схеми адресації. Такий протокол задає формати полів *всередині* пакету. Пакети зазвичай передаються від однієї кінцевої системи до іншої. Маршрутизований протокол використовує таблицю маршрутизації для пересилки пакетів. Приклади маршрутизованих протоколів – Internet-протокол (IP), протокол міжмережевого пакетного обміну IPX тощо. Легше всього зрозуміти що таке маршрутизовані протоколи, якщо пам’ятати, що це протоколи передачі даних.

Протокол маршрутизації – такий протокол, який підтримує маршрутизовані протоколи і надає механізми обміну маршрутною інформацією. Повідомлення протоколу маршрутизації передаються між маршрутизаторами (роутерами). Протокол маршрутизації дозволяє роутерам обмінюватись інформацією між собою для оновлення записів і підтримки таблиці маршрутизації.

Приклади протоколів маршрутизації: RIP, IGRP, EIGRP, OSPF. Легше зрозуміти, що таке протоколи маршрутизації, якщо пам’ятати, що це протоколи обміну маршрутною інформацією.

Для того, щоб протокол був маршрутизованим, він має включати механізми призначення як номера мережі, так і номера вузла для кожного пристрою в мережі.

2. Модель OSI

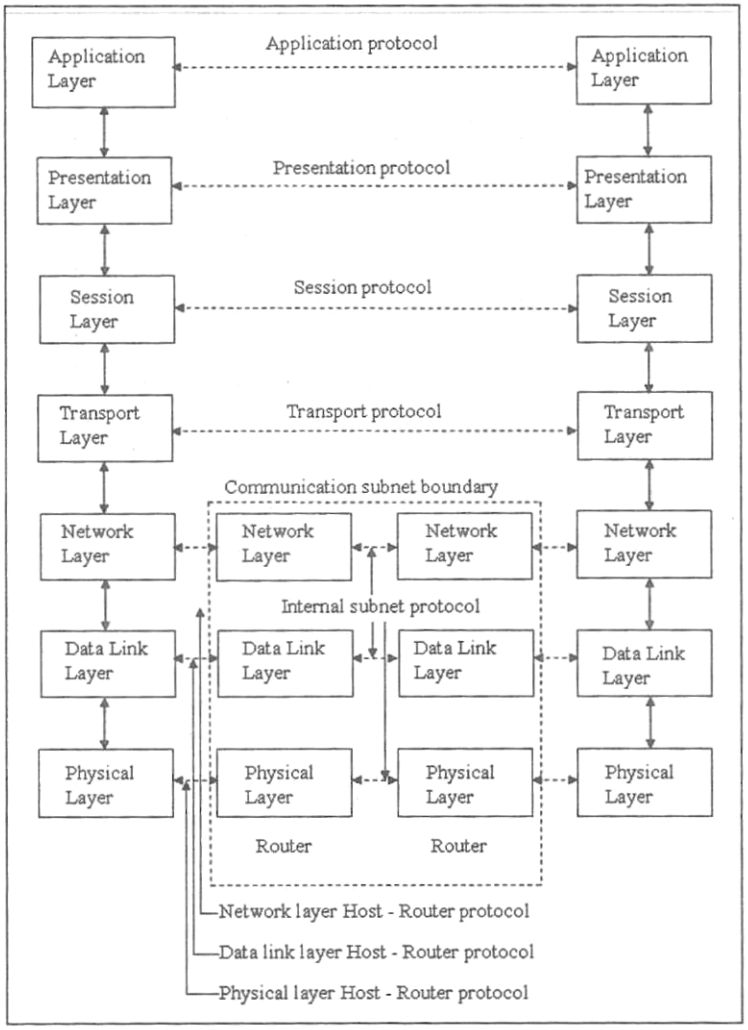
Модель OSI (EMBBC) (*базова еталонна модель взаємодії відкритих систем*, англ. *Open Systems Interconnection Basic Reference Model*, 1978 р.) – абстрактна мережева модель для комунікацій і розробки мережевих протоколів.

У 1978 р. Міжнародна організація стандартів *ISO (International Standards Organization)* випустила набір специфікацій, що описують архітектуру мережі з неоднорідними пристроями. Версія 1984 р. дістала назву еталонної моделі взаємодії відкритих систем *OSI (Open System Interconnection refrence model)* і стала міжнародним стандартом.

Представляє рівневий підхід до мережі. Кожен рівень обслуговує свою частину процесу взаємодії. Завдяки такій структурі спільна робота мережного обладнання й програмного забезпечення стає набагато простішою, прозорішою й зрозумілішою.

На даний час основним використовуваним стеком протоколів є TCP/IP, розробка якого не була пов'язана з моделлю OSI і до того ж була здійснена до її прийняття. За увесь час існування моделі OSI вона не була реалізована, і, очевидно, не буде реалізована ніколи. Сьогодні використовується тільки деяка підмножина моделі OSI. Вважається, що модель занадто складна, а її реалізація займе занадто багато часу.

Модель OSI	
Дані	Рівень
Дані	**Прикладний** доступ до мережевих служб
Дані	**Представлення** представлення і кодування даних
Дані	**Сеансовий** керування сеансом зв'язку
Блоки	**Транспортний** безпечне та надійне з'єднання «точка - точка»
Пакети	**Мережевий** визначення маршруту та IP (логічна адресація)
Кадри	**Канальний** MAC та LLC (фізична адресація)
Біти	**Фізичний** кабель, сигнали, бінарна передача



Архітектура еталонної моделі взаємодії відкритих систем OSI

Рівень OSI	**Протоколи**
прикладний	HTTP, gopher, Telnet, DNS, DHCP, SMTP, SNMP, CMIP, FTP, TFTP, SSH, IRC, AIM, NFS, NNTP, NTP, SNTP, XMPP, FTAM, APPC, X.400, X.500, AFP, LDAP, SIP, IETF,RTP, RTCP, ITMS, ModbusTCP, BACnet IP, IMAP, POP3, SMB, MFTP, BitTorrent, e2k, PROFIBUS Це всього лише кілька найрозповсюдженіших протоколів прикладного рівня, яких існує величезна кількість.
відображення	ASN.1, XML, TDI, XDR, NCP, AFP, ASCII, Unicode
сеансовий	ASP, ADSP, DLC, Named Pipes, NBT, NetBIOS, NWLink, Printer Access Protocol, Zone

	Information Protocol, SSL, TLS, SOCKS, PPTP
транспортний	TCP, UDP, NetBEUI, AEP, ATP, IL, NBP, RTMP, SMB, SPX, SCTP, DCCP, RTP, STP, TFTP
мережевий	IPv4, IPv6, ICMP, IGMP, IPX, NWLink, NetBEUI, DDP, IPSec, ARP, SKIP
канальний (Ланки даних)	ARCnet, ATM, DTM, SLIP, SMDS, Ethernet, FDDI, Frame Relay, LocalTalk, Token Ring, PPP, PPPoE, StarLan, WiFi, PPTP , L2F, L2TP, PROFIBUS
фізичний	RS-232, RS-422, RS-423, RS-449, RS-485, ITU-T, RJ-11, T-carrier (T1, E1), модифікації стандарту Ethernet: 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX,100BASE-T, 1000BASE-T, 1000BASE-TX, 1000BASE-SX

Прикладний рівень (Application layer)

Верхній (7-й) рівень моделі, забезпечує взаємодію мережі й користувача. Рівень дозволяє додаткам користувача доступ до мережних служб, таких як обробник запитів до баз даних, доступ до файлів, пересиланню електронної пошти. Також відповідає за передачу службової інформації, надає програмам інформацію про помилки й формує запити до рівня подання.

Рівень відображення (представлення) (Presentation layer)

Цей рівень відповідає за перетворення протоколів і кодування/декодування даних. Запити додатків, отримані з прикладного рівня, він перетворить у формат для передачі по мережі, а отримані з мережі дані перетворить у формат, зрозумілий додаткам. На цьому рівні може здійснюватися стиснення/розпакування або кодування/декодування даних, а також пере направлення запитів іншому мережному ресурсу, якщо вони не можуть бути оброблені локально.

Сеансовий рівень (Session layer)

Сеансовий рівень – 5-й рівень моделі OSI, що відповідає за підтримку сеансу зв’язку, дозволяючи додаткам взаємодіяти між собою тривалий час. Рівень керує створенням/завершенням сеансу, обміном інформацією, синхронізацією завдань, визначенням права на передачу даних і підтримкою сеансу в періоди неактивності додатків. Синхронізація передачі забезпечується розміщенням у потік даних контрольних точок, починаючи з яких відновляється процес при порушенні взаємодії.

Транспортний рівень (Transport layer)

Транспортний рівень (Transport layer) – 4-й рівень моделі OSI, призначений для доставляння даних без помилок, втрат і дублювання в тій послідовності, у якій вони були передані. При цьому не має значення, які дані передаються, звідки й куди, тобто він визначає сам механізм передачі. Блоки даних він розділяє на фрагменти, розмір яких залежить від протоколу, короткі об'єднує в один, довгі розбиває. Протоколи цього рівня призначені для взаємодії типу точка-точка.

Мережевий рівень (Network layer)

Мережевий рівень 3-й рівень мережної моделі OSI, призначений для визначення шляху передачі даних. Відповідає за трансляцію логічних адрес й імен у фізичні, визначення найкоротших маршрутів, комутацію й маршрутизацію пакетів, відстеження неполадок і заторів у мережі. На цьому рівні працює такий мережний пристрій, як *маршрутизатор.*

Канальний рівень (Data Link layer)

Цей рівень призначений для забезпечення взаємодії мереж на фізичному рівні й контролю за помилками, які можуть виникнути. Отримані з фізичного рівня дані він упаковує в кадри даних, перевіряє на цілісність, якщо потрібно виправляє помилки й відправляє на мережний рівень. Канальний рівень може взаємодіяти з одним або декількома фізичними рівнями, контролюючи й управляючи цією взаємодією. Даний рівень розбивається на 2 підрівня:

- MAC (Media Access Control) регулює доступ до поділюваного фізичного середовища;

- LLC (Logical Link Control) забезпечує обслуговування мережного рівня (на цьому рівні працюють комутатори, мости й мережні адаптери).

MAC-підрівень забезпечує коректне спільне використання загального середовища, надаючи його в розпорядження тієї або іншої станції мережі. Також додає адресну інформацію до фрейму, позначає початок і кінець фрейму.

Рівень LLC відповідає за достовірну передачу кадрів даних між вузлами, а також реалізовує функції інтерфейсу з мережевим рівнем за допомогою фреймування кадрів. Також здійснює ідентифікування протоколу мережевого рівня.

У програмуванні цей рівень представляє драйвер мережної карти, в операційних системах є програмний інтерфейс взаємодії канального й мережного рівня між собою, це не новий рівень, а просто реалізація моделі для конкретної ОС. Приклади таких інтерфейсів: NDIS, ODI.

Фізичний рівень (Physical layer)

Найнижчий 1-й рівень моделі, призначений безпосередньо для передачі потоку даних. Здійснює передачу електричних або оптичних сигналів у кабель і

відповідно їхній прийом і перетворення в біти даних відповідно до методів кодування цифрових сигналів. Інакше кажучи, здійснює інтерфейс між мережним носієм і мережним пристроєм. На цьому рівні працюють концентратори й повторювачі (ретранслятори) сигналу. Фізичний рівень визначає електричні, процедурні і функціональні специфікації для середовища передачі даних, в тому числі роз'єми, розпаювання і призначення контактів, рівні напруги, синхронізацію зміни напруги, кодування сигналу.

Цей рівень приймає кадр даних від канального рівня, кодує його в послідовність сигналів, які потім передаються у лінію зв'язку. Передача кадру даних через лінію зв'язку вимагає від фізичного рівня визначення наступних елементів: тип середовища передавання (дротовий або бездротовий, мідний кабель або оптичне волокно) і відповідних конекторів; як повинні бути представлені біти даних у середовищі передавання; як кодувати дані; якими повинні бути схеми приймача і передавача.

Фізичним рівнем в лінію зв'язку кадр даних (фрейм) не передається як єдине ціле. Кадр представляється як послідовність сигналів, що передаються один за одним. Сигнали, в свою чергу, представляють біти даних кадру.

Технології фізичного рівня визначаються стандартами, що розробляються наступними організаціями: The International Organization for Standardization (ISO), The Institute of Electrical and Electronics Engineers (IEEE), The American National Standards Institute (ANSI), The International Telecommunication Union (ITU), The Electronics Industry Alliance/Telecommunications Industry Association (EIA/TIA) тощо. Дані стандарти охоплюють 4 області, що належать фізичному рівню: фізичні та електричні властивості середовища передавання, механічні властивості (матеріали, розміри, розпаювання контактів конекторів), кодування (представлення бітів сигналами), визначення сигналів для управління інформацією. Всі компоненти апаратного забезпечення такі, як мережеві карти (Network interface card, NIC), інтерфейси і конектори, матеріали кабелів та їх конструкція визначаються стандартами фізичного рівня. Можна зазначити, що функції фізичного рівня вбудовані у мережеве обладнання (hardware).

Основними функціями фізичного рівня є: фізичні компоненти, кодування даних, передача даних. Фізичні компоненти – електронне обладнання, середовище передавання і конектори, через які передаються сигнали, що представляють біти даних.

3. Мережевий протокол TCP/IP

Transmission Control Protocol, **TCP** (*Протокол керування передачею*) – один з основних мережевих протоколів Інтернету, призначений для управління передачею даних в мережах і підмережах TCP/IP.

Пакет з TCP-заголовком називають ***TCP-сегментом***. Основні характеристики протоколу TCP такі.

1. **Підтримка комунікаційних каналів** між клієнтом і сервером, які називають **з'єднаннями**. TCP-клієнт встановлює з'єднання з конкретним сервером, обмінюється даними з сервером через це з'єднання, після чого розриває його.
2. **Забезпечення надійності передавання даних.** Коли дані передають за допомогою TCP, потрібне підтвердження їхнього отримання. Якщо воно не отримане впродовж певного часу, пересилання даних автоматично повторюють, після чого протокол знову очікує підтвердження. Час очікування зростає зі збільшенням кількості спроб. Після певної кількості безуспішних спроб з'єднання розривають. Неповного передавання даних через з'єднання бути не може: або воно надійно пересилає дані, або його розривають.
3. **Встановлення послідовності даних**. Кожен сегмент, переданий за цим протоколом, супроводжує номер послідовності. Якщо сегменти приходять у невірному порядку, TCP на підставі цих номерів може переставити їх перед тим як передати повідомлення в застосування.
4. **Керування потоком даних**. Протокол TCP повідомляє віддаленому застосуванню, який обсяг даних можливо прийняти від нього у будь-який момент часу. Це значення називають **оголошеним вікном**, воно дорівнює обсягу вільного простору у буфері, призначеному для отримання даних. Вікно динамічно змінюється: під час читання даних із буфера збільшується, у разі надходження даних мережею - зменшується. Це гарантує, що буфер не може переповнитися. Якщо буфер заповнений повністю, розмір вікна зменшують до нуля. Після цього TCP, пересилаючи дані, очікуватиме, поки у буфері не вивільниться місце.

Контрольна сума – це число, яке дозволяє приймаючому TCP виявити помилки в пакеті. Коли пакет прибуває в пункт призначення, приймаючий TCP обраховує контрольну суму і порівнює її з тою, яку послав відправник TCP. Якщо значення не збігаються, то при передачі виникла помилка. Приймаючий TCP відкидає цей пакет і просить повторну передачу.

TCP-з'єднання є **повнодуплексними:** з'єднання у будь-який момент часу можна використати для пересилання даних в обидва боки. TCP відстежує номери послідовностей і розміри вікон для кожного напрямку передавання даних.

Для встановлення зв'язку між двома процесами на транспортному рівні недостатньо наявності IP-адрес. Щоб розрізнити процеси, які виконуються на одному хості, використовують концепцію ***портів***.

Порти ідентифікують цілочисловими значеннями розміром 2 байти (від 0 до 65 535). Кожний порт унікально ідентифікує процес, запущений на хості: для того щоб TCP-сегмент був доставлений цьому процесові, у його заголовку зазначається цей порт. Процес-сервер використовує заздалегідь визначений порт, на який можуть вказувати клієнти для зв'язку із цим сервером. Для клієнтів порти зазвичай резервують динамічно.

Для деяких сервісів за замовчуванням зарезервовано конкретні номери портів у діапазоні від 0 до 1023; для протоколу HTTP (веб-серверів) це порт 80, а для протоколу SMTP – 25. Відомі порти розподіляються централізовано, подібно до IP-адрес. Якщо порт зайнятий деяким процесом, то інший процес на тому самому хості повторно зайняти його не зможе.

IP-протокол (англ. *Internet Protocol*; інтернет протокол, між мережевий протокол) – протокол мережевого рівня для передачі датаграм між мережами.

Протокол IP надає засоби доставки дейтаграм неоднорідною мережею без встановлення з'єднання. Він реалізує доставку за заданою адресою, але надійність, порядок доставки і відсутність дублікатів не гарантовані. Усі засоби щодо забезпечення цих характеристик реалізуються у протоколах вищого рівня (TCP).

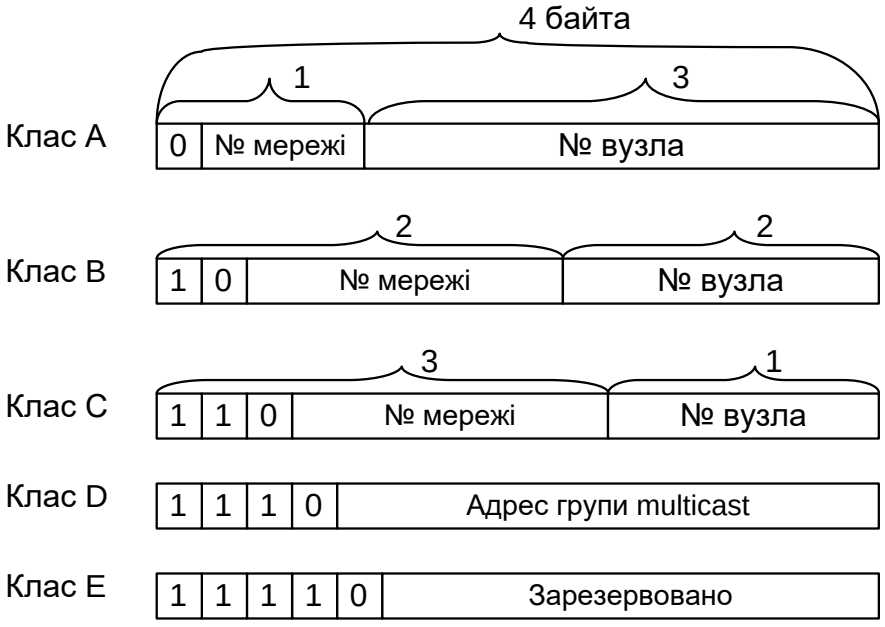
Кожний мережний інтерфейс в IP-мережі має унікальну адресу. Такі адреси називають ***IP-адресами***. Стандартною версією є IP версії 4 (IPv4), де використовують адреси завдовжки 4 байти. Їх записують у крапково-десятковому поданні (чотири десяткові числа, розділені крапками, кожне з яких відображає один байт адреси).

Наприклад:

128.10.2.30 – традиційна десяткова форма представлення адреси;

10000000 00001010 00000010 00011110 – двійкова форма представлення цієї ж адреси.

Адреса складається з двох логічних частин – номеру мережі і номеру вузла в мережі. Яка частина адреси відноситься до номера мережі, а яка – до номера вузла, визначається значеннями перших біт адреси. Значення цих біт є також ознаками того, до якого класу відноситься та або інша IP-адреса. Структура IP-адрес різних класів.



Класи IP адрес

Спеціальну адресу зворотного зв'язку 127.0.0.1 присвоюють інтерфейсу зворотного зв'язку і використовують для зв'язку із застосуваннями, запущеними на локальному хості.

IP доставляє дейтаграми мережному інтерфейсу. Пошук процесу на відповідному хості забезпечують протоколи транспортного рівня (TCP).

Протокол IPv6

Недоліком протоколу IPv4 є незначна довжина IP-адреси. Кількість адрес, які можна відобразити за допомогою 32 біт, є недостатньою з огляду на темпи росту Інтернету. Сьогодні нові IP-адреси виділяють обмежено.

Для вирішення проблеми запропоновано нову реалізацію IP-протоколу – *IP версії 6* (IPv6), відмінністю якої є довжина адреси – 128 біт (16 байт).

Інші протоколи мережного рівня

На мережному рівні реалізовано й інші протоколи. Для забезпечення мережної діагностики застосовують протокол ***ICMP*** (Internet Control Message Protocol), який використовують для передачі повідомлень про помилки під час пересилання IP-дейтаграм, а також для реалізації найпростішого ***луна-протоколу***, що реалізує обмін запитом до хосту і відповіддю на цей запит.
Сучасні ОС мають утиліту ***ping***, яку використовують для перевірки досяжності віддаленого хосту. Ця утиліта використовує луна-протокол у рамках ICMP.

Стек протоколів TCP/IP

TCP/IP — це абревіатура терміну Transmission Control Protocol / Internet Protocol (Протокол керування передачею / міжмережевий протокол). TCP/IP представляє базовий набір протоколів, відповідальний за розбивання вихідного

повідомлення на пакети (TCP), доставку пакетів на вузол адресата (IP) і збирання (відновлення) вихідного повідомлення з пакетів (TCP).

Основними протоколами транспортного рівня TCP/IP є протокол керування передачею TCP (Transmission Control Protocol) і протокол користувальницьких дейтаграм UDP (User Datagram Protocol). Транспортні послуги цих протоколів суттєво відрізняються. Протокол UDP доставляє датаграми без встановлення з'єднання. При цьому він не гарантує їхнього доставляння. Протокол TCP забезпечує надійне доставляння байтових потоків (сегментів) із попереднім встановленням транспортного дуплексного з'єднання (віртуального каналу) між модулями TCP мережних комп'ютерів.

Сукупність номера мережі і номера підмережі **називають розширеним мережевим префіксом**. Для виділення номера підмережі використовується маска підмережі (Subnet Mask). Формат маски підмережі аналогічний формату IP-адреси. Проте маска підмережі в двійковому представленні завжди містить послідовність одиниць в тій частині, яка відповідає номеру мережі і підмережі, і послідовність нулів в тій частині, яка відповідає номеру вузла.

		Мережевий префікс		Підмережа	Вузол
		Розширений мережевий префікс			
IP адрес	144.144.19.22	10010000	10010000	00010011	00010110
Маска	255.255.255.0	11111111	11111111	11111111	00000000
		Маска			

Елементи IP адреси і маска

Мережні протоколи стека TCP/IP використовуються для зв'язку між рівноправними сторонами, найчастіше такий зв'язок відбувається за принципом **«клієнт-сервер»,** коли одна сторона (**сервер**) очікує появи дейтаграм або встановлення з'єднання, а інша (**клієнт**) відсилає дейтаграми або створює з'єднання.

Основні етапи процесу обміну даними між клієнтом і сервером із використанням протоколу TCP/IP.

1. Застосування-клієнт (веб-браузер) у режимі користувача формує HTTP-запит до веб-сервера. Формат запиту визначений протоколом прикладного рівня (HTTP), зокрема у ньому зберігають шлях до потрібного документа на сервері. Після цього браузер виконує ряд системних викликів. При цьому у ядро ОС передають вміст HTTP-запиту, IP-адресу комп'ютера, на якому запущено веб-сервер, і номер порту, що відповідає цьому серверу.

2. Далі перетворення даних пакета відбувається в ядрі. Спочатку повідомлення обробляють засобами підтримки протоколу транспортного рівня (TCP). Його доповнюють TCP-заголовком, що містить номер порту веб-сервера та інформацію, необхідну для надійного пересилання даних. HTTP-запит перетворюється у TCP-сегмент, який пересилають для обробки в режимі користувача.
3. TCP-сегмент обробляють засобами підтримки протоколу мережного рівня (IP). При цьому він перетворюється в IP-дейтаграму (його доповнюють IP-заголовком, що містить IP-адресу віддаленого комп'ютера та іншу інформацію, необхідну для передавання мережею).
4. IP-дейтаграма надходить на рівень драйвера мережного пристрою (Ethernet), який додає до неї інформацію, необхідну для передавання за допомогою Ethernet-пристрою. Пакет з Ethernet-інформацією називають **Ethernet-фреймом**. Фрейм передають мережному пристрою, який відсилає його мережею. Фрейм містить адресу призначення. Апаратне забезпечення Ethernet забезпечує реалізацію передавання даних фізичною мережею у вигляді потоку бітів.

Дотепер пакет переходив від засобів підтримки протоколів вищого рівня до протоколів нижчого.

Тепер пакет переміщатиметься мережею.

Далі відбувається декілька етапів демультиплексування пакетів. *Кажуть, що пакет піднімається у стеку протоколів:*

1. Драйвер мережного пристрою Ethernet виділяє IP-дейтаграму із фрейму і передає її засобам підтримки протоколу IP.
2. Засоби підтримки IP перевіряють IP-адресу в заголовку, і, якщо вона збігається з локальною IP-адресою, виділяють TCP-сегмент із дейтаграми і передають його засобам підтримки TCP.
3. Засоби підтримки TCP визначають застосування-адресат за номером порту, заданим у TCP-заголовку (це веб-сервер, що очікує запитів від клієнтів). Після цього виділяють HTTP-запит із TCP-сегмента і передають його цьому застосуванню для обробки в режимі користувача.
4. Сервер обробляє HTTP-запит (наприклад, відшукує на локальному диску відповідний документ).

Лекція №6. Служба DNS: простір імен, домени

Мета заняття: ознайомитись зі простором імен DNS та його основних компонент; опанувати категорії імен для доменів верхнього рівня; отримати представлення та розуміння серверів імен та зон у службі DNS.

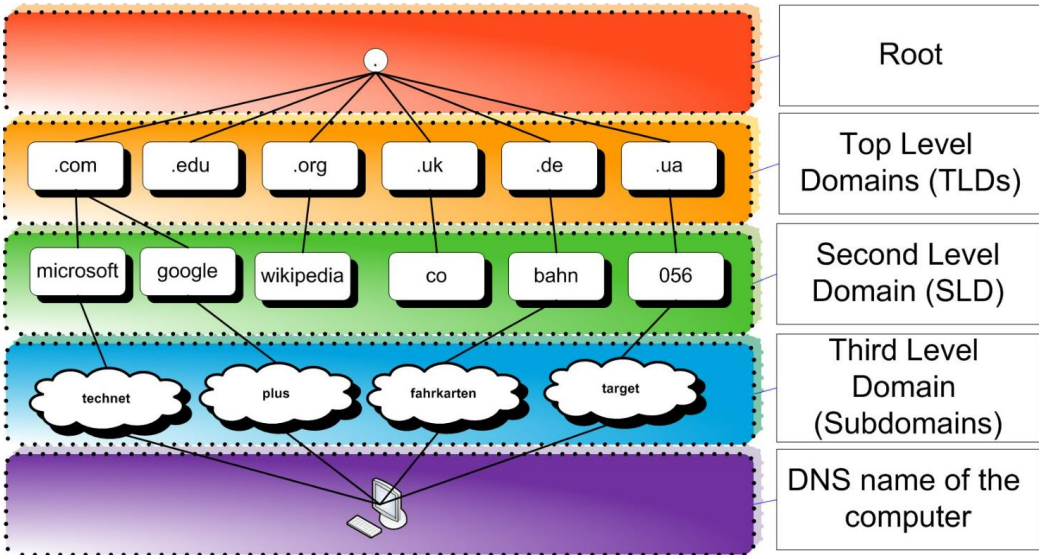
DNS (Domain Name System) – це ієрархічна база даних, що зіставляє імена мережевих вузлів і їх мережевих служб IP-адресам вузлів. Вміст цієї бази, з одного боку, розподілений по великій кількості серверів служби DNS, а з іншого боку, є централізованим керованим. У основі ієрархічної структури бази даних DNS лежить доменний простір імен (domain name space), основною структурною одиницею якого є домен, об'єднуючий мережеві вузли (хости), а також під домени. Процес пошуку в БД служби DNS імені якогось мережевого вузла та зіставлення цьому імені IP-адреси називається "*Дозволом імені вузла в просторі імен DNS*".

Служба DNS складається з трьох основних компонент:

1. **Простір імен DNS і відповідні ресурсні записи (RR, resource record)** – це сама розподілена база даних DNS;
2. **Сервери імен DNS** – комп'ютери, що зберігають базу даних DNS і що відповідають на запити DNS-клієнтів;
3. **DNS-клієнти (DNS-clients, DNS-resolvers)** – комп'ютери, що посилають запити серверам DNS для отримання ресурсних записів.

Простір імен.

Простір імен DNS – ієрархічна деревовидна структура, що починається з кореня, що не має імені і що позначається точкою ".". Схему побудови простору імен DNS краще всього проілюструвати на прикладі мережі Інтернет.



Для доменів 1-го рівня розрізняють 3 категорії імен:

- **ARPA** – спеціальне ім'я, використовуване для зворотного дозволу DNS (з IP-адрес повне ім'я вузла);
- **Загальні (generic) імена 1-го рівня** – 16 (на даний момент) імен (aero, biz, com, edu…);
- **Двохбуквені імена для країн** – імена для доменів, зареєстрованих у відповідних країнах (наприклад ua - для України, uk - для Великобританії і так далі).

Для безпосереднього відображення простору імен в простір IP-адрес служать **ресурсні записи (RR, resource record)**. Кожен сервер DNS містить ресурсні записи для тієї частини простору імен, за яку він несе відповідальність (authoritative). В табл. містить опис найбільш часто використовуваних типів ресурсних записів.

Тип ресурсного запису	Функція запису	Опис використання
A	Host Address Адреса хоста, або вузла	Відображає ім'я вузла на IP-адреса
CNAME	Canonical Name (alias) Канонічне ім'я (псевдонім)	Відображає одне ім'я на інше
MX	Mail Exchanger Обмін поштою	Управляє маршрутизацією поштових повідомлень для протоколу SMTP
NS	Name Server Сервер імен	Указує на сервери DNS, відповідальні за конкретний домен і його піддомени
PTR	Pointer Покажчик	Використовується для зворотного дозволу IP-адресаов в імена вузлів в домені in-addr.arpa
SOA	Start of Authority Початковий запис зони	Використовується для вказівки основного сервера для даної зони і опису властивостей зони
SRV	Service Locator Покажчик на службу	Використовується для пошуку серверів, на яких функціонують певні служби (наприклад, контроллери доменів Active Directory або сервери глобального каталога)

Сервери імен DNS (або DNS-сервери) – це комп'ютери, на яких зберігаються ті частини БД простору імен DNS, за які дані сервери відповідають, і функціонує програмне забезпечення, яке обробляє запити DNS-клієнтів на дозвіл імен і видає відповіді на отримані запити.

DNS-клієнт – це будь-який мережевий вузол, який звернувся до DNS-серверу для дозволу імені вузла в IP-адресу або, назад, IP-адреси в ім'я вузла.

Служба DNS: домени і зони

Кожен DNS-сервер відповідає за обслуговування певної частини простору імен DNS. Інформація про домени, що зберігається в БД сервера DNS, організовується в особливі одиниці, звані зонами (zones). **Зона** – основна одиниця реплікації даних між серверами DNS. Кожна зона містить певну кількість ресурсних записів для відповідного домена і його піддоменів.

Системи сімейства Windows Server підтримують наступні типи зон:

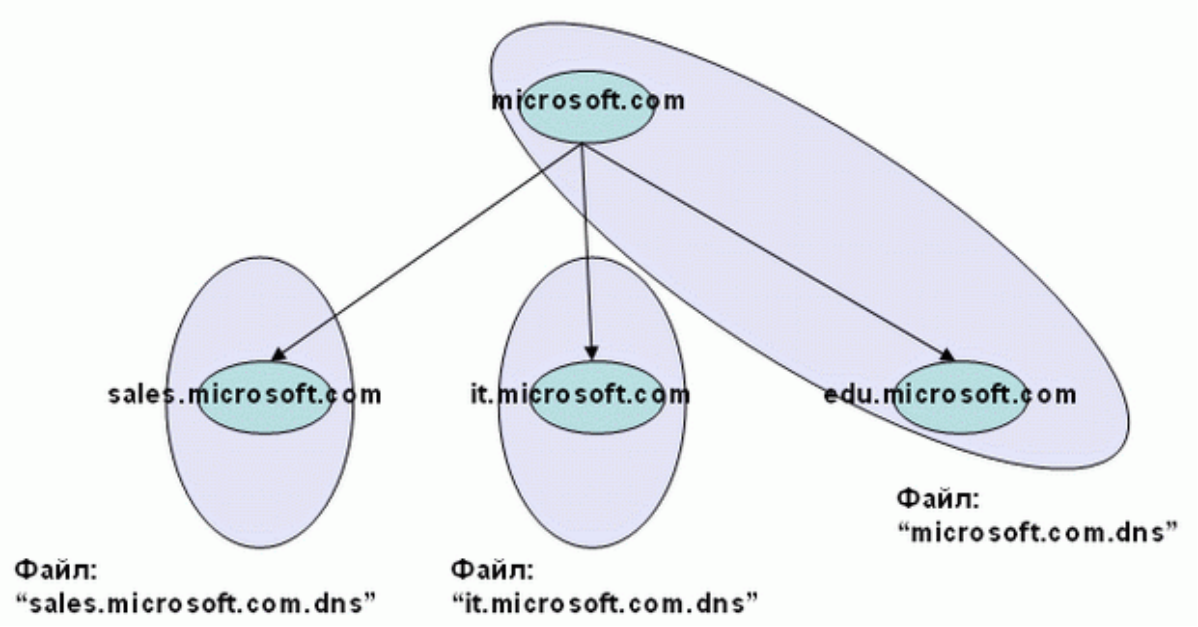
- **Стандартна основна (standard primary)** – головна копія стандартної зони; тільки у даному екземплярі зони допускається проводити які-небудь зміни, які потім реплікуються на сервери, що зберігають додаткові зони;

- **Стандартна додаткова (standard secondary)** – копія основної зони, доступна в режимі "тільки-читання", призначена для підвищення відмовостійкої і розподілу навантаження між серверами, що відповідають за певну зону; процес реплікації змін в записах зон називається "Передачею зони" (*zone transfer*) (інформація в стандартних зонах зберігається в тестових файлах, файли створюються в теці "%system root%\system32\dns", ім'я файлу, як правило, утворюється з імені зони з додаванням розширення файлу ".dns"; термін "стандартна" використовується тільки в системах сімейства Windows);

- **Інтегрована в Active Directory (Active Directory–integrated)** – вся інформація про зону зберігається у вигляді одного запису в базі даних Active Directory (такі типи зон можуть існувати тільки на серверах Windows, доменів Active Directory, що є контроллерами; у інтегрованих зонах можна жорсткіше управляти правами доступу до записів зони; зміни в записах зони між різними екземплярами інтегрованої зони проводяться не за технологією передачі зони службою DNS, а механізмами реплікації служби Active Directory);

- **Зона-заглушка** (**stub**; тільки у Windows 2003) - особливий тип зони, яка для даної частини простору імен DNS містить наймінімальніший набір ресурсних записів (початковий запис зони SOA, список серверів імен, що відповідають за дану зону, і декілька записів типу A для посилань на сервери імен для даної зони).

Розглянемо на прикладі співвідношення між поняттями домена і зони на рис.



Лекція №7. Огляд та основні можливості ОС Windows Server. Основні сервіси. Служба DHCP

Мета заняття: вивчення понять ActiveDirectory, IntelliMirror, TerminalServices та WindowsScriptHost у сімействі WindowsServer; освоєння поняття служби DHCP та рекомендації планування серверів DHCP.

Системні вимоги

При плануванні придбання і інсталяції сервера (або декількох серверів) службі IT будь-якої компанії або організації необхідно вирішити цілий комплекс завдань:

1. визначити набір завдань, що покладаються на кожен сервер (сервер мережевої інфраструктури, сервер служби каталогів, сервер файлів/друку, сервер видаленого доступу, сервер електронної пошти, сервер баз даних і так далі);
2. визначити передбачуване навантаження на сервер, виходячи з виконуваних ним ролей і кількості користувачів, які працюватимуть з сервером;
3. виходячи з отриманої інформації, визначити апаратну конфігурацію сервера (тип і кількість процесорів, об'єм оперативної пам'яті, параметри дискової підсистеми, мережеві адаптери та ін.) та редакцію операційної системи (Standard, Enterprise, Datacenter, Web);
4. спланувати процедуру інсталяції і параметри системи (чи проводитиметься модернізація системи з попередньої версії або нова інсталяція, як конфігурувати дискову підсистему, визначити мережеві параметри і так далі).

Основні можливості системи Windows Server

Історія Windows Server налічує вже понад 25 років: Windows NT 3.1 Advanced Server був випущений 27 липня 1993 року.

Інсталяція, налаштування і використання системи Windows Server залежить від тих завдань, які повинна виконувати конкретна інсталяція. Типові завдання системи корпорація Microsoft об'єднала у вигляді т.з. "ролей" сервера. Всі ролі можна побачити при запуску майстрів "Майстер налаштування сервера" або "Управління даним сервером". Перерахуємо ці ролі:

1. файловий сервер (сервер, що надає доступ до файлів і керівник ними; вибір цієї ролі дозволить швидко набудувати параметри квотування і індексування);

2. сервер друку (сервер, організуючий доступ до мережевих принтерів і керівник чергами друку і драйверами принтерів; вибір цієї ролі дозволить швидко набудувати параметри принтерів і драйверів);

3. сервер додатків (сервер, на якому виконуються Web-служби XML, Web-додатки і розподілені застосування; при призначенні серверу цієї ролі на нім автоматично встановлюються IIS, COM+ і Microsoft .NET Framework; за бажання ви можете додати до них серверні розширення Microsoft FrontPage, а також включити або вимкнути ASP.NET);

4. поштовий сервер (сервер, на якому працюють основні поштові служби POP3 (Post Office Protocol 3) і SMTP (Simple Mail Transfer Protocol), завдяки чому поштові POP3-клієнти домена можуть відправляти і отримувати електронну пошту; вибравши цю роль, ви визначаєте домен за замовчунням для обміну поштою і створюєте поштові скриньки);

5. сервер терміналів (сервер, що виконує завдання для клієнтських комп'ютерів, які працюють в режимі термінальної служби; вибір цієї ролі приводить до встановлення служб терміналів, що працюють в режимі сервера додатків);

6. сервер видаленого доступу/сервер віртуальної приватної мережі (сервер, що здійснює маршрутизацію мережевого трафіку і керівник телефонними з'єднаннями і з'єднаннями через віртуальні приватні мережі (virtual private network, VPN); вибравши цю роль, ви запустите Майстер налаштувань сервера маршрутизації і видаленого доступу (Routing and Remote Access Server Setup Wizard); за допомогою параметрів маршрутизації і видаленого доступу ви можете вирішити тільки підключення, вхідні і вихідні підключення або повністю заборонити доступ ззовні);

7. служба каталогів (контроллер домена Active Directory — сервер, на якому працюють служби каталогів і розташовуються сховище даних каталога; контроллери домена також відповідають за вхід в мережу і пошук в каталозі; при виборі цієї ролі на сервері будуть встановлені DNS і Active Directory);

8. система доменних імен (сервер, на якому запущена служба DNS, що вирішує імена комп'ютерів в IP-адресу і навпаки; при виборі цієї ролі на сервері буде встановлена DNS і запущений Майстер налаштування DNS-сервера);

9. сервер протоколу динамічного налаштування вузлів (сервер, на якому запущена служба DHCP (Dynamic Host Configuration Protocol), що дозволяє автоматизувати призначення IP-адрес вузлам мережі; при виборі цієї ролі на сервері буде встановлена служба DHCP і запущений Майстер створення області);

10. сервер Windows Internet Naming Service (сервер, на якому запущена служба WINS (Windows Internet Name Service), що вирішує імена NETBIOS в IP-адресі і навпаки; вибір цієї ролі приводить до встановлення служби WINS);

11. сервер потокове мультимедіа-мовлення (сервер, що надає мультимедійні потоки іншим системам мережі або Інтернету; вибір цієї ролі приводить до встановлення служб Windows Media; ця роль підтримується тільки у версіях Standard Edition і Enterprise Edition).

Microsoft Windows Server – наймогутніша ОС для ПК. У ній реалізовані засоби управління системою і адміністрування:

Active Directory – розширювана і масштабована служба каталогів, в якій використовується простір імен, заснований на стандартній Інтернет-службі іменування доменів (Domain Name System, DNS);

IntelliMirror – засоби конфігурації, що підтримують дзеркальне відображення призначених для користувача даних і параметрів середовища, а також центральне адміністрування встановлення і обслуговування програмного забезпечення;

Terminal Services – служби терміналів, що забезпечують видалений вхід в систему і управління іншими системами Windows Server 2003;

Windows Script Host – сервер сценаріїв Windows для автоматизації таких поширених завдань адміністрування, як створення облікових записів користувачів і звітів по журналах подій.

Windows Server 2019

У жовтні 2018 року, через три роки після попереднього великого релізу, був випущений Windows Server 2019.

Починаючи з Windows Server 2016 був прийнятий новий цикл виходу релізів. Зараз є два канали поширення: ***LTSC*** *(Long-term servicing channel) - реліз, що виходить через 2-3 роки, з 5-річною основний і 5-річною розширеною підтримкою, а також* ***Semi-Annual Channel*** *- релізи, які виходять кожні півроку, мають основний цикл підтримки протягом 6 місяців і розширену підтримку протягом 18 місяців. Для чого потрібні ці два канали? Microsoft активно впроваджує нововведення в свою хмарну платформу Azure. Це підтримка віртуальних машин Linux, контейнери з Linux і Windows, і багато інших технології.*

Замовники, які використовують ці технології в хмарі, також хочуть їх використовувати і в своїх датацентрах. ***Semi-Annual Channel*** *скорочує розрив у можливостях між Azure і локальними датацентрами. Піврічні релізи призначені для динамічних у розвитку компаній, які перейшли до гнучкої сервісної моделі надання IT-послуг бізнесу. Релізи* ***LTSC*** *призначені для компаній, які використовують усталені додатки з тривалим циклом*

підтримки, наприклад, Exchange Server, SharePoint Server, SQL Server, а також інфраструктурні ролі, програмно-які визначаються датацентри і гіперконвергентную інфраструктуру.

Windows Server 2019 - це саме реліз в каналі LTSC. Він включає в себе всі оновлення функціоналу з Windows Server 2016 і наступних піврічних релізів.

Основні зусилля розробників Windows Server 2019 були спрямовані на чотири ключові області:

Гібридне хмара - Windows Server 2019 і новий центр адміністрування Windows Admin Center дозволяють легко використовувати спільно з серверної операційної системою хмарні служби Azure: Azure Backup, Azure Site Recovery, управління оновленнями Azure, Azure AD Authentication і іншими.

Безпека - є одним з найважливіших пріоритетів для замовників. Windows Server 2019 має вбудовані можливості для ускладнення зловмисникам проникнути і закріпитися в системі. Це відомі по Windows 10 технології Defender ATP і Defender Exploit Guard.

Платформа додатків - контейнери стають сучасним трендом для упаковки і доставки додатків в різні системи. При цьому Windows Server може виконувати не тільки рідні для Windows програми, а й додатки Linux. Для цього в Windows Server 2019 є контейнери Linux, підсистема Windows для Linux (WSL), а також значно знижені обсяги образів контейнерів.

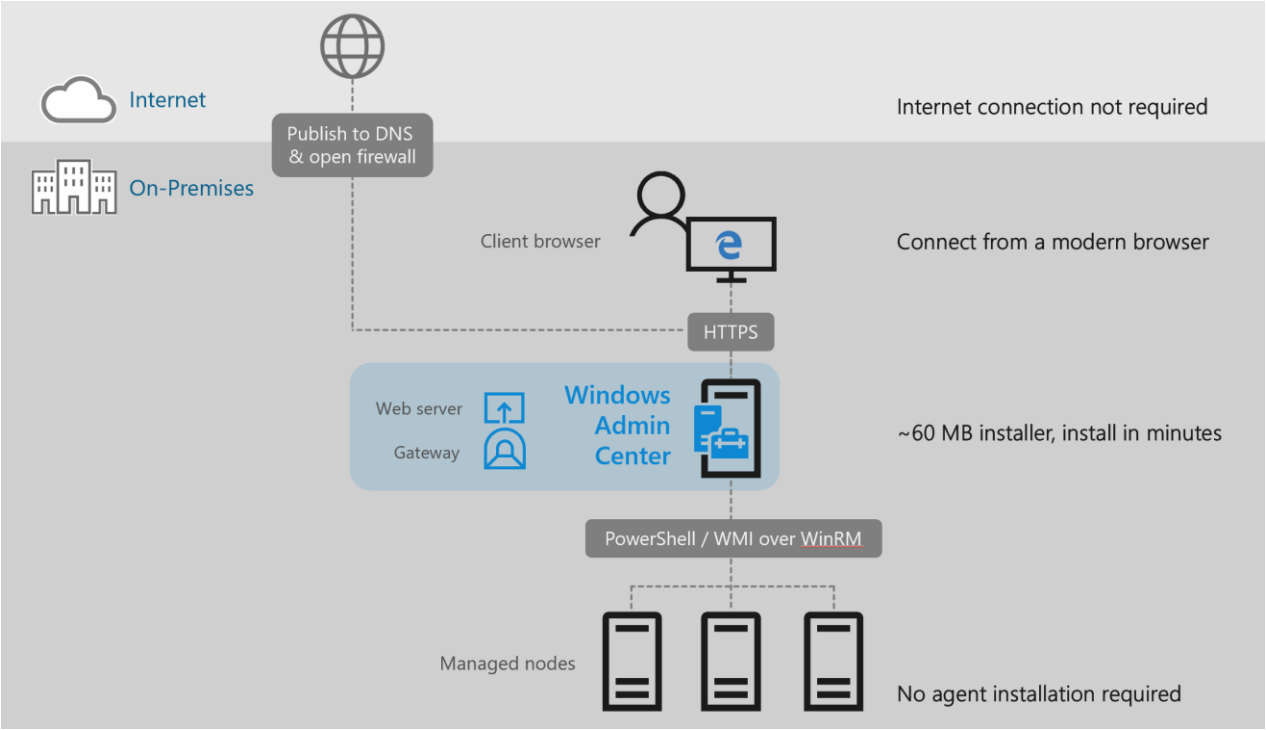
Гіперконвергентна інфраструктура – дозволяє поєднати в рамках одного сервера стандартної архітектури і обчислення, і сховище. Цей підхід значно знижує вартість інфраструктури, при цьому забезпечуючи відмінну продуктивність і масштабованість.

Windows Admin Center (WAC) – це новий засіб адміністрування серверів. Встановлюється локально в інфраструктурі і дозволяє адмініструвати локальні і хмарні екземпляри Windows Server, комп'ютери Windows 10, кластери і гіперконвергентну інфраструктуру.

WAC доповнює, а не замінює існуючі засоби адміністрування, такі як консолі mmc, Server Manager. Підключення до WAC здійснюється з браузера.

Для виконання завдань використовується технології віддаленого управління WinRM, WMI і скрипти PowerShell.

Можна опублікувати WAC і адмініструвати сервери ззовні периметра організації. Служби багатофакторної аутентифікації і проксі додатків Azure AD допоможуть захистити такий доступ ззовні, а використання рішення Microsoft Enterprise Mobility + Security (EMS) дозволить надавати або відмовляти в доступі в залежності від відповідності пристрою політикам, ризикам, розташування та інших факторів.



Системна аналітика

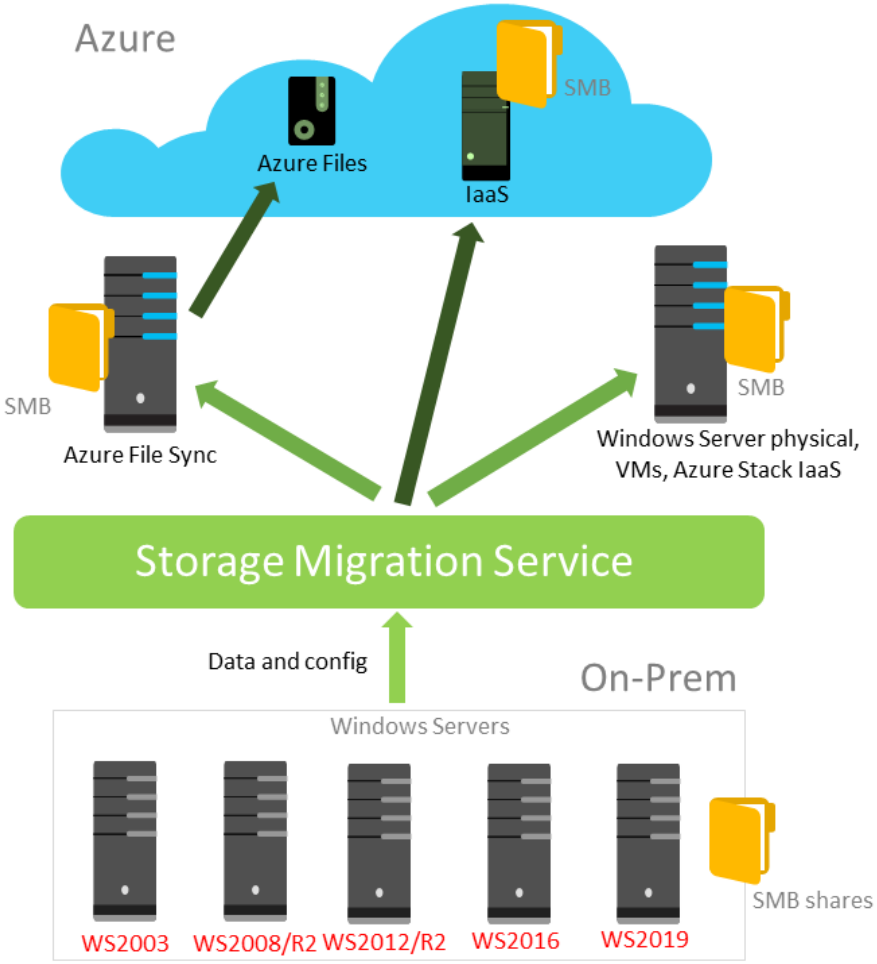
Windows Server 2019 став інтеллектуальнішим. За допомогою нової функції **System Insights** реалізується прогнозна аналітика, що дозволяє перейти від реактивного до проактивного управління серверами. Модель машинного навчання враховує лічильники продуктивності і події для точного передбачення проблем з вільним місцем на дискових підсистемах, визначення трендів для процесорних обчислень, мережну взаємодію і продуктивність сховища.

Новинки в підсистемі зберігання

Storage Migration Service – нова технологія для міграції даних зі старих серверів на нові.

Міграція відбувається в кілька етапів:

- ✓ інвентаризація даних на різних серверах;
- ✓ швидке перенесення файлів, мережевих папок і конфігурацій безпеки з вихідних серверів;
- ✓ захоплення управління і підміна ідентифікатора сервера і налаштувань мережі зі старого сервера на новий.



Azure File Sync трансформує традиційні файлові сервери і розширює обсяг зберігання до практично недосяжних в реальному житті обсягів. Дані розподіляються по декількох рівнях: гарячий кеш - це дані, що зберігаються на дисках файлового сервера і доступні з максимальною швидкістю для користувачів. У міру остивання дані непомітно переміщуються в Azure. Azure File Sync можна використовувати спільно з будь-якими протоколами для доступу до файлів: SMB, NFS і FTPS.

Storage Replica. Ця технологія захисту від катастроф вперше з'явилася в Windows Server 2016. У версії 2019 з'явилася обмежена підтримка редакції Windows Server Standard. Зараз і невеликі компанії можуть робити автоматичну копію (репліку) сховища в віртуальній машині Azure, якщо в інфраструктурі компанії немає другого віддаленого датацентру.

Storage Spaces Direct. Локальні дискові простору – це необхідний компонент для побудови гіперконвергентної інфраструктури і масштабування файл-сервера.

Зміни в відмовостійкої кластеризації

З'явилися набори кластерів (Cluster sets), що збільшують масштабованість до сотень вузлів.

Для забезпечення кворуму в кластерах з парною кількістю вузлів використовується спеціальний ресурс – диск-свідок. За часів Windows Server 2012 R2 для диска-свідка необхідно було виділяти диск на сховище, в Windows Server 2016 стало можливо використовувати мережеву папку або хмарний диск-свідок. Покращення в Windows Server 2019 пов'язані зі скороченням вимог до інфраструктури для малих підприємств. Як диска-свідка може виступати USB-диск, підключений, наприклад, до роутера.

З'явилася міграція кластерів між доменами і інші поліпшення в службі відмовостійкої кластеризації.

Windows Server 2019 поставляється в двох редакціях: **Standard** і **Datacenter**.

Редакція для датацентрів має розширені можливості: підтримка гіперконвергентної інфраструктури, локальних дискових просторів, розширеними ліцензійними правами при використанні віртуалізації.

Служба DHCP

Служба *DHCP* (*Dynamic Host Configuration Protocol*) – це одна із служб підтримки протоколу TCP/IP, розроблена для спрощення адміністрування IP-мережі за рахунок використання спеціально налаштованого серверу для централізованого управління IP-адресами та іншими параметрами протоколу TCP/IP, необхідними мережевим вузлам. Сервер DHCP позбавляє мережевого адміністратора від необхідності ручного виконання таких операцій, як:

1. автоматичне призначення мережевим вузлам IP-адрес та інших параметрів протоколу TCP/IP (наприклад, маска підмережі, адреса основного шлюзу підмережі, адреси серверів DNS і WINS);
2. недопущення дублювання IP-адрес, що призначаються різним вузлам мережі;
3. звільнення IP-адрес вузлів, видалених з мережі;
4. ведення централізованої БД виданих IP-адрес.

Особливості служби DHCP в системах сімейства Windows Server:

I. **Інтеграція з DNS** — DHCP-сервери можуть здійснювати динамічну реєстрацію видаваних IP-адрес і FQDN-імен мережевих вузлів в базі даних DNS-серверу (це особливо актуально для мережевих клієнтів, які не підтримують динамічну реєстрацію на сервері DNS);

II. **Авторизація сервера DHCP в Active Directory** — якщо мережевий адміністратор встановить службу DHCP на сервері Windows, то сервер не функціонуватиме, поки не буде авторизований в AD (це забезпечує захист від встановлення несанкціонованих DHCP-серверів);

III. **Резервне копіювання бази даних DHCP** — Створена резервна копія може використовуватися згодом для відновлення працездатності DHCP-сервера.

Планування серверів DHCP

При плануванні серверів DHCP необхідно враховувати в першу чергу вимоги продуктивності і відмовостійкої (доступності) даної служби. Тому основні рекомендації при розгортанні служби DHCP в корпоративній мережі будуть наступними:

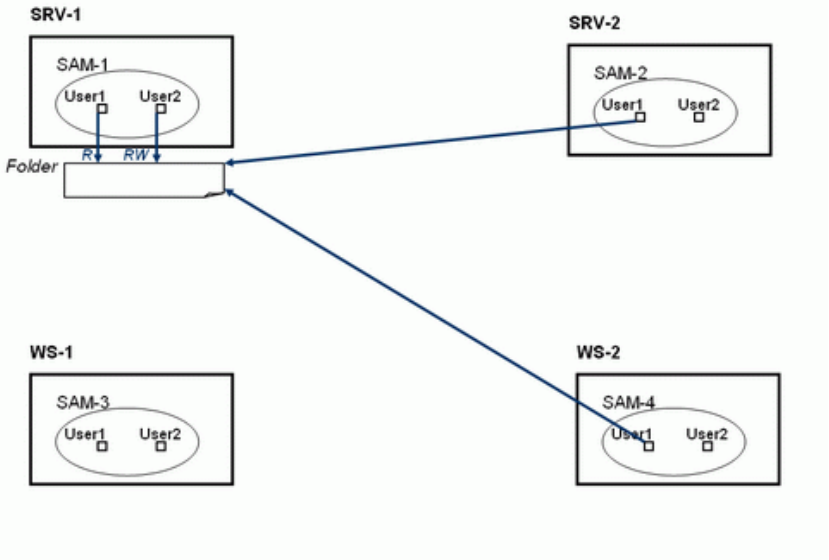
- бажано в кожній IP-мережі встановити окремий DHCP-сервер;
- якщо немає можливості встановити свій сервер в кожній IP- мережі, необхідно на маршрутизаторах, об'єднуючих IP-мережі, запустити і набудувати *агент ретрансляції DHCP-запитів* (*DHCP Relay Agent*) так, щоб він пересилав широкомовні запити DHCP з підмережі, в якій немає DHCP-серверу, на відповідний DHCP-сервер, а на самому DHCP-сервере створити області для всіх обслуговуваних IP-мереж;
- для підвищення відмовостійкої слід встановити декілька серверів DHCP, при цьому на кожному DHCP-сервері, окрім областей для "своїх" IP-мереж, необхідно створити області для інших підмереж (при цьому діапазони IP-адресов в таких резервних областях не повинні перетинатися з основними областями, створеними на серверах DHCP в "своїх" підмережах);
- у великих IP-мережах DHCP-сервери повинні мати могутні процесори, достатньо великі об'єми оперативної пам'яті і швидкодіючі дискові підсистеми, оскільки обслуговування великої кількості клієнтів вимагає інтенсивної роботи з базою даних DHCP-сервера.

Лекція №8. Планування простору імен AD. Моделі управління безпекою

Мета заняття: ознайомитись з моделлю управління безпекою «Робоча група» та «Доменна модель»; дослідити призначення служби каталогів Active Directory; вивчити поняття домен, дерево, ліс; планування простору імен і структури AD.

Модель "Робоча група"

Дана модель управління безпекою корпоративної мережі — найпримітивніша. Вона призначена для використання в невеликих однорангових мережах (3–10 комп'ютерів) і заснована на тому, що кожен комп'ютер в мережі з операційними системами Windows має свою власну локальну базу даних облікових записів і за допомогою цієї локальної БД здійснюється управління доступом до ресурсів даного комп'ютера. Локальна БД облікових записів називається база даних *SAM* (*Security Account Manager*) і зберігається в реєстрі операційної системи. Бази даних окремих комп'ютерів повністю ізольовані один від одного і ніяк не зв'язані між собою. Приклад управління доступом при використанні такої моделі наступний:

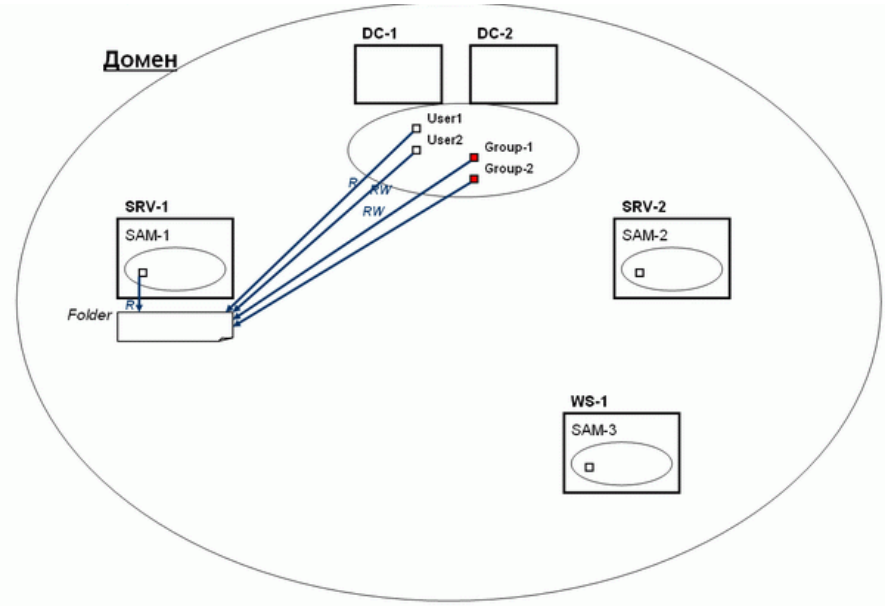


Модель "Робоча група" простіша для вивчення, тут немає необхідності вивчати складні поняття Active Directory. Але при використанні в мережі з великою кількістю комп'ютерів і мережевих ресурсів стає дуже складним управляти іменами користувачів і їх паролями — доводиться на кожному комп'ютері (який надає свої ресурси для сумісного використання в мережі) уручну створювати одні і ті ж облікові записи з однаковими паролями, що дуже трудомістко, або робити один обліковий запис на всіх користувачів з одним на всіх паролем (або взагалі без пароля), що сильно знижує рівень захисту інформації. Тому модель "Робоча група" рекомендується тільки для

мереж з числом комп'ютерів від 3 до 10 (а ще краще — не більше 5), за умови що серед всіх комп'ютерів немає жодного з системою Windows Server.

Доменна модель

У доменній моделі існує єдина база даних служб каталогів, доступна всім комп'ютерам мережі. Для цього в мережі встановлюються спеціалізовані сервери, звані *контроллерами домена*, які зберігають на своїх жорстких дисках цю базу.



Із рисунка сервери DC-1 і DC-2 — контроллери домена, вони зберігають доменну базу даних облікових записів (кожен контроллер зберігає у себе свою власну копію БД, але всі зміни, вироблювані в БД на одному з серверів, реплицируются на решту контроллерів).

У доменній моделі управління безпекою користувач реєструється на комп'ютері ("входить в систему") зі своїм доменним *обліковим записом* і, незалежно від комп'ютера, на якому була виконана реєстрація, дістає доступ до необхідних мережевих ресурсів. І немає необхідності на кожному комп'ютері створювати велику кількість локальних облікових записів, всі записи створені одноразово *в доменній БД.* І за допомогою доменної бази даних здійснюється централізоване *управління доступом* до мережевих ресурсів незалежно від *кількості комп'ютерів в мережі.*

Призначення служби каталогів Active Directory

Каталог (довідник) може зберігати різну інформацію, що відноситься до користувачів, груп, комп'ютерів, мережевих принтерів, загальним файловим ресурсам і так далі — називатимемо все це об'єктами. Каталог зберігає також інформацію про сам об'єкт, або його властивості, звані атрибутами.

Active Directory відповідає не тільки за створення і організацію цих невеликих об'єктів, але також і за великі об'єкти, такі як домени, OU (організаційні підрозділи) і сайти.

Служба каталогів Active Directory (скорочено — AD) забезпечує ефективну роботу складного корпоративного середовища, надаючи наступні можливості:

1. *Єдина реєстрація в мережі*; Користувачі можуть реєструватися в мережі з одним ім'ям і паролем і діставати при цьому доступ до всіх мережевих ресурсів і служб (служби мережевої інфраструктури, служби файлів і друку, сервери додатків і баз даних і т. д.);
2. *Безпека інформації*. Засоби аутентифікації і управління доступом до ресурсів, вбудовані в службу Active Directory, забезпечують централізований захист мережі;
3. *Централізоване управління*. Адміністратори можуть централізовано управляти всіма корпоративними ресурсами;
4. *Адміністрування з використанням групових політик*. При завантаженні комп'ютера або реєстрації користувача в системі виконуються вимоги групових політик; їх налаштування зберігаються в об'єктах групових політик (GPO) і застосовуються до всіх облікових записів користувачів і комп'ютерів, розташованих в сайтах, доменах або організаційних підрозділах;
5. *Інтеграція з DNS*. Функціонування служб каталогів повністю залежить від роботи служби DNS. У свою чергу сервери DNS можуть зберігати інформацію про зони в базі даних Active Directory;
6. *Розширюваність каталога*. Адміністратори можуть додавати в схему каталога нові класи об'єктів або додавати нові атрибути до існуючих класів;
7. *Масштабованість*. Служба Active Directory може охоплювати як один домен, так і безліч доменів, об'єднаних в дерево доменів, а з декількох дерев доменів може бути побудований ліс;
8. *Реплікація інформації*. У службі Active Directory використовується реплікація службової інформації в схемі з багатьма ведучими (multi-master), що дозволяє модифікувати БД Active Directory на будь-якому контроллері домена. Наявність в домені декількох контроллерів забезпечує відмовостійку і можливість розподілу мережевого навантаження;
9. *Гнучкість запитів до каталога*. БД Active Directory може використовуватися для швидкого пошуку будь-якого об'єкту AD, використовуючи його властивості (наприклад, ім'я користувача або адреса його електронної пошти, тип принтера або його місцеположення і т. п.);

10. *Стандартні інтерфейси програмування.* Для розробників програмного забезпечення служба каталогів надає доступ до всіх можливостей (засобам) каталога і підтримує прийняті стандарти і інтерфейси програмування (API).

***LDAP* (*Lightweight Directory Access Protocol*)** – спрощена (полегшена) версія стандарту побудови каталогів, що отримала назву. Протокол LDAP зберігає всі основні властивості X.500 (ієрархічна система побудови довідника, масштабованість, розширюваність), але при цьому дозволяє достатньо ефективно реалізувати даний стандарт на практиці. Термін "*lightweight" ("полегшений* ") в назві LDAP відображає основну мету розробки протоколу: створити інструментарій для побудови служби каталогів, яка володіє достатньою функціональною потужністю для вирішення базових завдань, але не переобтяжена складними технологіями, що роблять реалізацію служб каталогів неефективної. В даний час LDAP є стандартним методом доступу до інформації мережевих каталогів і грає роль фундаменту в безлічі продуктів, таких як системи аутентифікації, поштові програми і додатки електронної комерції. Сьогодні на ринку присутньо більше 60 комерційних серверів LDAP, причому близько 90% з них є самостійними серверами каталогів LDAP, а останні пропонуються як компоненти інших застосувань.

Протокол LDAP чітко визначає круг операцій над каталогами, які може виконувати клієнтське застосування. Ці операції розпадаються на п'ять груп:

1. встановлення зв'язку з каталогом;
2. пошук в нім інформації;
3. модифікація його вмісту;
4. додавання об'єкту;
5. видалення об'єкту.

Окрім протоколу LDAP служба каталогів Active Directory використовує також протокол аутентифікації *Kerberos* і службу DNS для пошуку в мережі компонент служб каталогів (контроллери доменів, сервери глобального каталога, службу Kerberos і ін.).

Домен

Основною одиницею системи безпеки Active Directory є *домен*. Домен формує область адміністративної відповідальності. База даних домена містить облікові записи *користувачів*, *груп* і *комп'ютерів*. Велика частина функцій по управлінню службою каталогів працює на рівні домена (аутентифікація користувачів, управління доступом до ресурсів, управління службами, управління реплікацією, політики безпеки).

Імена доменів Active Directory формуються по тій же схемі, що і імена в просторі імен DNS. І це не випадково. Служба DNS є засобом пошуку компонент домена — в першу чергу контроллерів домена.

Контроллери домена — спеціальні сервери, які зберігають відповідну даному домену частина бази даних Active Directory. Основні функції контроллерів домена:

- **зберігання БД Active Directory** (організація доступу до інформації, що міститься в каталозі, включаючи управління цією інформацією і її модифікацію);
- **синхронізація змін в AD** (зміни в базу даних AD можуть бути внесені на будь-якому з контроллерів домена, будь-які зміни, здійснювані на одному з контроллерів, будуть синхронізовані з копіями, що зберігаються на інших контроллерах);
- **аутентифікація користувачів** (будь-який з контроллерів домена здійснює перевірку повноважень користувачів, що реєструються на клієнтських системах).

Настійно рекомендується в кожному домені встановлювати не менше двох контроллерів домена — по-перше, для захисту від втрати БД Active Directory у разі виходу з ладу якого-небудь контроллера, по-друге, для розподілу навантаження між контроллерами.

Дерево

Дерево є набором доменів, які використовують єдиний зв'язаний простір імен. В цьому випадку "дочірній" домен успадковує своє ім'я від "батьківського" домена. Дочірній домен автоматично встановлює двосторонні транзитивні довірчі відносини з батьківським доменом.

Корпорація Microsoft рекомендує будувати Active Directory у вигляді одного домена. Побудова дерева, що складається з багатьох доменів необхідно в наступних випадках:

1. для децентралізації адміністрування служб каталогів (наприклад, у разі, коли компанія має філії, географічно віддалені один від одного, і централізоване управління утруднене по технічних причинах);
2. для підвищення продуктивності (для компаній з великою кількістю користувачів і серверів актуальне питання підвищення продуктивності роботи контроллерів домена);
3. для ефективнішого управління реплікацією (якщо контроллери доменів віддалені один від одного, то реплікація в одному може зажадати більше часу і створювати проблеми з використанням несинхронізованих даних);

4. для застосування різних політик безпеки для різних підрозділів компанії;

5. при великій кількості об'єктів в БД Active Directory.

Ліс – найбільш крупна структура в Active Directory. Ліс об'єднує дерева, які підтримують єдину схему (*схема Active Directory* – набір визначень типів, або класів, об'єктів в БД Active Directory). У лісі між всіма доменами встановлені двосторонні відносини, що дозволяють користувачам будь-якого домена діставати доступ до ресурсів решти всіх доменів, якщо вони мають відповідні дозволи на доступ. За замовчуванням, перший домен, що створюється в лісі, вважається його кореневим доменом, в кореневому домені зберігається схема AD.

При управлінні деревами і лісами потрібно пам'ятати два дуже важливих моменту:

- перше створене в лісі доменів дерево є кореневим деревом, перший створений в дереві домен називається *кореневим доменом дерева* (*tree root domain*);
- перший домен, створений в лісі доменів, називається *кореневим доменом лісу* (*forest root domain*), даний домен не може бути видалений (він зберігає інформацію про конфігурацію лісу і дерева доменів, його створюючих).

Організаційні підрозділи (*Organizational Units, OU*) — контейнери усередині AD, які створюються для об'єднання об'єктів в цілях *делегування адміністративних прав* і *застосування групових політик* в домені. ОП існують *тільки усередині доменів* і можуть об'єднувати *тільки об'єкти зі свого домена*. ОП можуть бути вкладеними один в одного, що дозволяє будувати усередині домена складну деревовидну ієрархію з контейнерів і здійснювати гнучкіший адміністративний контроль. Крім того, ОП можуть створюватися для віддзеркалення адміністративної ієрархії і організаційної структури компанії.

Глобальний каталог є переліком *всіх об'єктів*, які існують в лісі Active Directory. За умовчанням, контроллери домена містять тільки інформацію про об'єкти свого домена. Сервер Глобального каталога є контроллером домена, в якому міститься інформація про кожен об'єкт (хоча і не про всі атрибути цих об'єктів), що знаходиться в даному лісі.

Планування простору імен і структури AD – дуже відповідальний момент, від якого залежить ефективність функціонування майбутньої корпоративної системи безпеки. При цьому треба мати на увазі, що створену спочатку структуру в процесі експлуатації буде дуже важко змінити. При плануванні AD необхідно враховувати наступні моменти:

1. ретельний вибір імен доменів верхнього рівня;

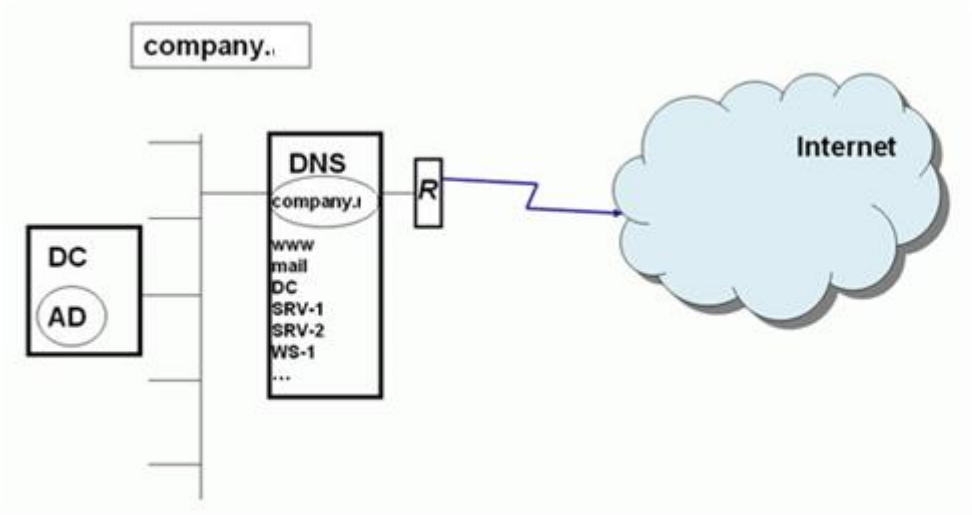
2. якість комунікацій в компанії (зв'язок між окремими підрозділами і філіями);
3. організаційна структура компанії;
4. кількість користувачів і комп'ютерів у момент планування;
5. прогноз темпів зростання кількості користувачів і комп'ютерів.

Простір імен AD

При плануванні імен доменів верхнього рівня можна використовувати різні стратегії і правила. В першу чергу необхідно враховувати питання інтеграції внутрішнього простору імен і простору імен мережі Інтернет — оскільки простір імен AD базується на просторі імен DNS, при неправильному плануванні можуть виникнути проблеми з безпекою, а також конфлікти із зовнішніми іменами.

1. Один домен, одна зона DNS.

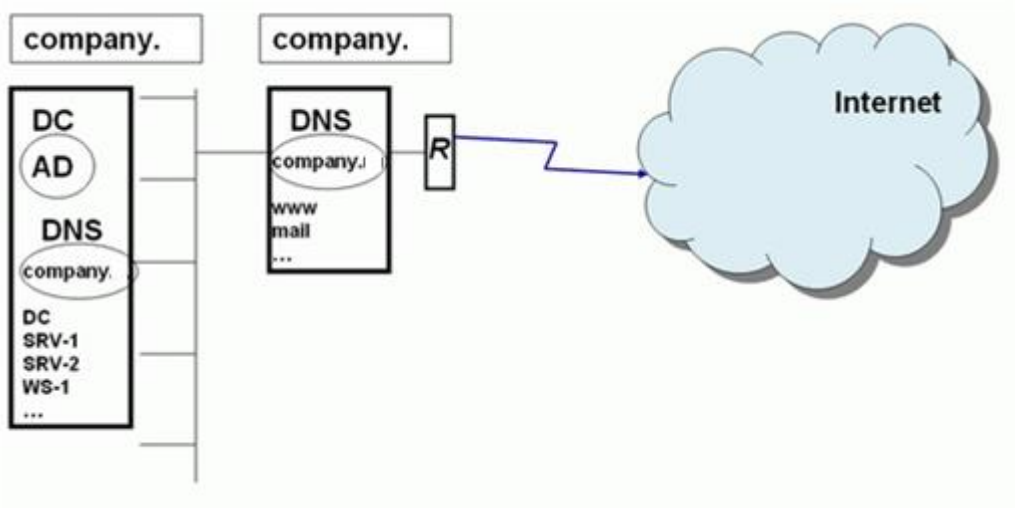
На малюнку в лівій частині — внутрішня мережа компанії, справа — мережа Інтернет, дві мережі розділено маршрутизатором "*R" (*окрім маршрутизатора, на межі можуть бути також проксі-сервер або міжмережевий екран).



У даному прикладі використовується одна і та ж зона DNS (company.ua) як для підтримки внутрішнього домена AD з тим же ім'ям (записи DC, SRV-1, SRV-2, WS-1), так і зберігання посилань на зовнішні ресурси компанії — веб-сайт, поштовий сервер.

Такий спосіб максимально спрощує роботу системного адміністратора, але при цьому DNS-сервер, доступний для всієї мережі Інтернет, зберігає зону company.ua і надає доступ до записів цієї зони всім користувачам Інтернету. Таким чином, зовнішні зловмисники можуть отримати повний список внутрішніх вузлів корпоративної мережі.

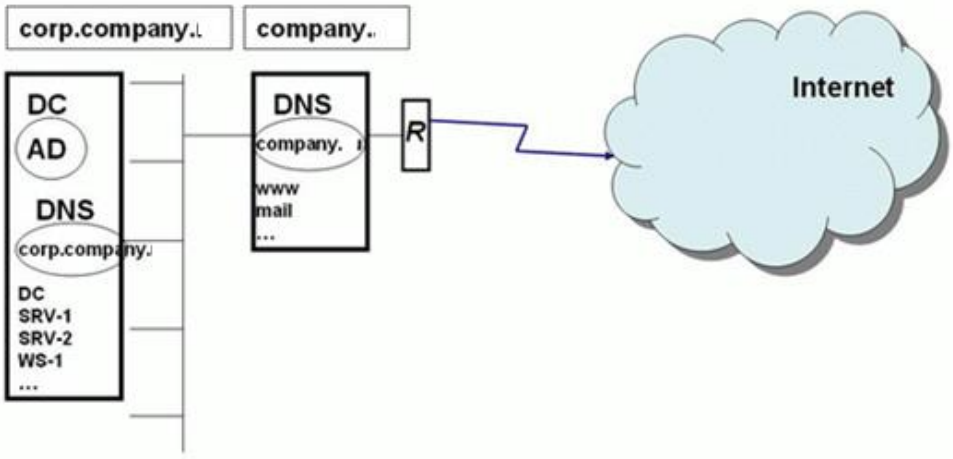
2. **"Розщеплювання" простору імен DNS** - одне ім'я домена, дві різні зони DNS.



В даному випадку на різних серверах DNS створюються різні зони з одним і тим же ім'ям company. На внутрішньому DNS-сервері функціонує зона company. для Active Directory, на зовнішньому DNS-сервере — зона з таким же ім'ям, але для посилань на зовнішні ресурси. Важливий момент — дані зони ніяк між собою не зв'язані — ні механізмами реплікації, ні ручною синхронізацією.

Тут в зовнішній зоні зберігаються посилання на зовнішні ресурси, а у внутрішній на внутрішні ресурси, використовувані для роботи Active Directory. Даний варіант нескладно реалізувати, але для мережевого адміністратора виникає навантаження управління двома різними доменами з одним ім'ям.

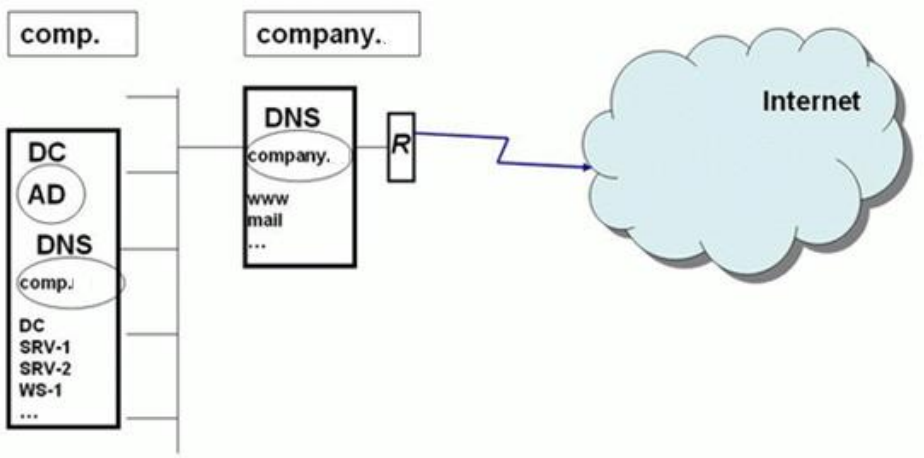
3. **Піддомен в просторі імен DNS для підтримки Active Directory**.



У даному прикладі кореневий домен компанії company.ua служить для зберігання посилань на зовнішні ресурси. У домені company.ua настроюється делегування управління піддоменом corp.company.ua на внутрішній DNS-сервер, і саме на базі домена corp.company.ua створюється домен Active Directory. В цьому випадку в зовнішній зоні зберігаються посилання на

зовнішні ресурси, а також посилання на делегування управління піддоменом на внутрішній DNS-сервер. Таким чином, користувачам Інтернету доступний мінімум інформації про внутрішню мережу. Такий варіант організації простору імен досить часто використовується компаніями.

4. **Два різні домени DNS для зовнішніх ресурсів і для Active Directory**.



У цьому сценарії компанія реєструє в Інтернет-органах два доменні імена: одне для публікації зовнішніх ресурсів, інше — для розгортання Active Directory.

Даний сценарій планування простору імен найоптимальніший. По-перше, ім'я зовнішнього домена ніяк не пов'язане з ім'ям внутрішнього домена, і не виникає жодних проблем з можливість показу в Інтернет внутрішньої структури. По-друге, реєстрація (покупка) внутрішнього імені гарантує відсутність потенційних конфліктів, викликаних тим, що якась інша компанія може зареєструвати в Інтернеті ім'я, співпадаюче з внутрішнім ім'ям вашої компанії.

Перелік питань на підсумковий контроль

1. Дайте визначення операційної системи.
2. Вкажіть, які задачі розв’язуються в області мережевого адміністрування та охарактеризуйте їх.
3. Вкажіть на які частини була розділена індустрія ПЗ мережевого управління.
4. Вкажіть на основі якої технології будуються сучасні мережі.
5. Дайте визначення системного адміністратора.
6. Дайте визначення клієнт-сервера.
7. Вкажіть на яких положеннях повинні базуватися правила роботи в корпоративній мережі.
8. Дайте визначення сервера та однорангової мережі.
9. Вкажіть, які завдання виконує системний адміністратор.
10. Розкрийте поняття автентифікації та авторизації.
11. Вкажіть, як класифікуються комп’ютерні мережі по області дії.
12. Вкажіть, як класифікуються комп’ютерні мережі по способах адмініструванням.
13. Вкажіть, як класифікуються комп’ютерні мережі по мережних операційних системах.
14. Вкажіть, як класифікуються комп’ютерні мережі по протоколах.
15. Вкажіть чим зумовлюється популярність протоколу TCP/IP?
16. Вкажіть, як класифікуються комп’ютерні мережі по топології.
17. Вкажіть, як класифікуються комп’ютерні мережі по архітектурі.
18. Опишіть використовувані категорії кручених пар.
19. Опишіть спосіб створення локальної мережі в малому офісі засобами LAN та USB -з’єднанням.
20. Опишіть спосіб створення локальної мережі в малому офісі засобами WLAN та BT -з’єднанням.
21. Вкажіть, необхідне обладнання для створення локальної мережі.
22. Розкрийте зміст мережевого протоколу.
23. Вкажіть, що представляє собою маршрутизований протокол та протокол маршрутизації.
24. Вкажіть, що представляє собою модель OSI.
25. Охарактеризуйте прикладний рівень моделі OSI та вкажіть його найпоширеніші протоколи.
26. Охарактеризуйте рівень відображення моделі OSI та вкажіть його найпоширеніші протоколи.

27. Охарактеризуйте сеансовий рівень моделі OSI та вкажіть його найпоширеніші протоколи.
28. Охарактеризуйте транспортний рівень моделі OSI та вкажіть його найпоширеніші протоколи.
29. Охарактеризуйте мережевий рівень моделі OSI та вкажіть його найпоширеніші протоколи.
30. Охарактеризуйте канальний рівень моделі OSI та вкажіть його найпоширеніші протоколи.
31. Охарактеризуйте фізичний рівень моделі OSI та вкажіть його найпоширеніші протоколи.
32. Вкажіть якими організаціями визначаються стандарти технології фізичного рівня моделі OSI.
33. Вкажіть основні функції фізичного рівня моделі OSI.
34. Вкажіть, що представляє собою кодування у фізичному рівні моделі OSI.
35. Опишіть алгоритм передавання інформації протоколом TCP.
36. Вкажіть, що собою представляє IP-протокол.
37. Розкрийте поняття IP-адреси та зобразіть її структуру різних класів.
38. Розкрийте основні етапи процесу обміну даними між клієнтом і сервером з використанням протоколу TCP/IP.
39. Розкрийте поняття DNS та його основних компонент.
40. Вкажіть, що собою представляє простір імен DNS.
41. Вкажіть, які категорії імен розрізняють для доменів верхнього рівня.
42. Вкажіть, що собою представляють сервери імен та зони у службі DNS.
43. Вкажіть для чого служать діагностичні утиліти ipconfig, ping, tracert.
44. Вкажіть для чого служать діагностичні утиліти pathping, netstat, nbtstat.
45. Опишіть роботу в режимі комутативного доступу.
46. Вкажіть, що собою представляє технологія ADSL та опишіть необхідне обладнання.
47. Зобразіть типову схему підключення ADSL-модему до телефонної лінії.
48. Розкрийте характеристику файлового серверу, серверу друку і серверу додатків у сімействі WindowsServer.
49. Розкрийте характеристику файлового поштового серверу, серверу терміналів і серверу видаленого доступу у сімействі WindowsServer.
50. Розкрийте характеристику файлової служби каталогів, системи доменних імен та серверу протоколу динамічного налаштування вузлів у сімействі WindowsServer.
51. Розкрийте поняття ActiveDirectory, IntelliMirror, TerminalServices та WindowsScriptHost у сімействі WindowsServer.
52. Розкрийте поняття служби DHCP.

53. Вкажіть рекомендації планування серверів DHCP.
54. Опишіть модель управління безпекою – «робоча група».
55. Опишіть «доменну модель» управління безпекою корпоративної мережі.
56. Вкажіть, яку інформацію зберігає каталог у службі ActiveDirectory.
57. Розкрийте можливості служби каталогів ActiveDirectory.
58. Розкрийте поняття протоколу LDAP.
59. Розкрийте функції контролерів домена у ActiveDirectory.
60. Розкрийте поняття «дерева» та «лісу» у домені ActiveDirectory.
61. Розкрийте поняття глобального каталогу та механізм іменування об’єктів у службі каталогів.
62. Опишіть поняття планування простору імен ActiveDirectory та, що потрібно при цьому враховувати.
63. Опишіть варіант планування імен доменів верхнього рівня – один домен, одна зона DNS.
64. Опишіть варіант планування імен доменів верхнього рівня – одне ім’я домена, дві різні зони DNS.
65. Опишіть варіант планування імен доменів верхнього рівня – під домен простору імен DNS для підтримки ActiveDirectory.
66. Опишіть варіант планування імен доменів верхнього рівня – два різні домени DNS для зовнішніх ресурсів і для ActiveDirectory.
67. Вкажіть основні вимоги до серверної кімнати.
68. Опишіть механізм нумерації розеток в комп’ютерній мережі.
69. Вкажіть, які завдання необхідно вирішити при плануванні, придбання і встановлення сервера?

Література та джерела

Основна література

1. Методичне видання: Адміністрування комп’ютерних мереж та операційних систем / [уклад.: В.В. Поліщук]. – Ужгород: УжНУ, 2019. – 60 с.
2. Методичне видання: Адміністрування комп’ютерних мереж та операційних систем (вказівки до практичних робіт) / [уклад.: В.В. Поліщук]. – Ужгород: УжНУ, 2020. – 43 с.
3. Основи адміністрування LAN у середовищі MS Windows. Навчальний посібник / Б. А. Демида, К. М. Обельовська, В. С. Яковина. Львів: Видавництво Львівської політехніки, 2013. 488 с.

Допоміжна література

4. Абрамов В.О. Базові технологи комп'ютерних мереж: навч. посіб. / В.О. Абрамов, СЮ. Клименко. - К.: Київ, ун-т ім. Б. Грінченка, 2011. - 291 с.
5. Буров Є.В. Комп'ютерні мережі: підруч. - Львів: Магнолія плюс, 2006. - 264 с.