Національний університет
водного господарства
та природокористування

Міністерство освіти та науки України
Національний університет водного господарства та природокористування
Кафедра автоматизації, електротехнічних та комп'ютерно-інтегрованих технологій

04-03-202

МЕТОДИЧНІ ВКАЗІВКИ
до виконання лабораторних робіт №1-5
з навчальної дисципліни
«Комп'ютерні системи та мережі в АСКТП»
для здобувачів вищої освіти другого (магістерського) рівня
за освітньо-професійною програмою
«Автоматизація та комп'ютерно-інтегровані технології»
спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» денної та заочної форм навчання

Рекомендовано науково-методичною радою з якості ННІ АКОТ

Протокол № 4 від 21.12.2019 р.

Рівне – 2019

Національний університет
водного господарства
та природокористування

Методичні вказівки до виконання лабораторних робіт №1-5 з навчальної дисципліни «Комп'ютерні системи та мережі в АСКТП» для здобувачів вищої освіти другого (магістерського) за освітньо-професійною програмою «Автоматизація та комп'ютерно-інтегровані технології» спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» денної та заочної форм навчання [Електронне видання] / Сафоник А. П., Христюк А. О – Рівне : НУВГП, 2019. – 75 с.

Укладачі: Сафоник А. П., д.т.н., професор, професор кафедри АЕКІТ;
Христюк А. О., к.т.н., доцент кафедри АЕКІТ.

Відповідальний за випуск: Древецький В. В., д.т.н., професор, завідувач кафедри АЕКІТ.

Керівник групи забезпечення спеціальності Древецький В. В.

Національний університет
водного господарства
та природокористування

© Сафоник А. П.,
Христюк А. О., 2019
© НУВГП, 2019

Національний університет
водного господарства
та природокористування

Зміст

стор.
Вступ …… 4
1. Обладнання для побудови локальних мереж …… 5
2. Створення локальної мережі за допомогою бездротової точки доступу 29
3. Підключення до глобальної мережі за допомогою телефону/модема 43
4. Служби термінального доступу 55
5. Служба каталогів Active Directory. Групові політики 67

Національний університет
водного господарства
та природокористування

Національний університет
водного господарства
та природокористування

Вступ

Якісне та осмислене засвоєння теоретичної частини курсу «Комп'ютерні системи та мережі в АСКТП» неможливе без надбання практичних навичок шляхом виконання дослідів в лабораторних умовах. Виконання запропонованих лабораторних робіт охоплює основні розділи курсу. Кожна з робіт включає в себе тему, мету, короткі теоретичні відомості, а також порядок виконання роботи. Виконавши експериментальну частину (або отримавши вихідні дані), студент заносить дані до звіту. Далі, самостійно, студент виконує необхідні операції, будує графічні залежності. Результатом цієї роботи є звіт з лабораторної роботи. Готовий звіт подається викладачу на папері або надсилається на корпоративну електронну пошту викладача. Надсилання звіту з лабораторної роботи допускається лише з корпоративної пошти студента. При цьому в темі листа обов'язково зазначається номер лабораторної роботи та навчальна дисципліна. В тіло листа прикріплюється файл зі звітом у форматі: *.doc, *.docx або *.pdf. Успішне, виконання запропонованих лабораторних робіт сформує у студента інженерні навички у подальшій професійній діяльності, а також закріпить теоретичні знання з курсу «Комп'ютерні системи та мережі в АСКТП».

Національний університет
та природокористування

Робота 1. Обладнання для побудови локальних мереж

1.1. Мета роботи

Ознайомитись з будовою і призначенням основних складових для побудови локальних мереж типу Ethernet; побудувати мережу, налаштувати TCP/IP параметри та протестувати з'єднання використовуючи утиліти ОС Windows.

1.2. Теоретичні відомості

Ethernet – базова технологія локальних обчислювальних (комп'ютерних) мереж з комутацією пакетів, що використовує протокол CSMA/CD (множинний доступ з контролем несучої та виявленням колізій). Цей протокол дозволяє в кожний момент часу лише один сеанс передачі в логічному сегменті мережі. При появі двох і більше сеансів передачі одночасно виникає колізія, яка фіксується станцією, що ініціює передачу. Станція аварійно зупиняє процес і очікує закінчення поточного сеансу передачі, а потім знову намагається повторити передачу.

Ethernet був започаткований у 1970 році (Dr. Robert M. Metcalfe) в дослідницькому центрі фірми Xerox. Перша система Ethernet працювала із швидкістю 3 Мб/с і була відома під назвою "експериментальний Ethernet". Формальна специфікація для Ethernet була опублікована в 1980 році консорціумом DIX, утвореним фірмами DEC, Intel і Xerox; ця система вже працювала із швидкістю 10 Мб/с. На початку 80-х років DIX запропонував IEEE стандарт Ethernet, який став моделлю сьогоднішнього стандарту IEEE 802.3. Після 1985 року до нього були уведені специфікації нових середовищ для 10 Мб/с Ethernet, наприклад, витої пари провідників, а наостанок – специфікації для 100 Мб/с Fast Ethernet. На сьогодні стандарт IEEE 802.3 описує всі мережі, що базуються на Ethernet, із швидкостями 10, 100 і 1000 Мб/с.

Компоненти обладнання мереж Ethernet

Ключові елементи, необхідні для побудови LAN Ethernet:

Карта мережевого інтерфейсу

Карта мережевого інтерфейсу (Network Interface Card – NIC), яку

Національний університет
також називають мережевим адаптером або мережевою картою – це пристрій, який здійснює фізичне під'єднання комп'ютера до мережі, тобто забезпечує фізичне сполучення між мережевим кабелем і внутрішньою шиною комп'ютера. У більшості випадків ця карта встановлюється безпосередньо в шину розширення комп'ютера (PCI, ISA, PCI Express). В окремих випадках карта може бути частиною окремого пристрою, до якого комп'ютер під'єднаний через паралельне або послідовне з'єднання.

Карта мережевого інтерфейсу отримує дані від персонального комп'ютера, перетворює їх до відповідного формату і пересилає через кабельну систему до іншої мережевої карти; остання приймає дані, переводить їх у форму, зрозумілу для даного комп'ютера і передає їх у цей комп'ютер.

Повторювачі Ethernet

Повторювач (repeater) – це пристрій, який отримує електричний або оптичний сигнал із кабеля через один інтерфейс, регенерує його і висилає в кабель через другий інтерфейс. Завданням повторювача є пересилання будь-якого вхідного сигналу до всіх інших портів без модифікації або непотрібної затримки. Це означає також пересилання сигналів колізій, фрагментів, глушіння, шумів. Повторювачі можуть мати два або більше портів. Прикладом багатопортового повторювача є хаб у мережі Ethernet. Порти повторювача не мусять бути ідентичними. Вони можуть передавати сигнали від входу для провідного кабеля до входу для оптоволоконного кабеля, але це можливе тільки в межах тієї самої топології. Наприклад, можна переслати сигнал від 10Base-T до 10Base-F, але не можна побудувати повторювач для мереж різних типів, наприклад, для Ethernet і TokenRing; пристрої, які можуть здійснювати такі з'єднання, називають мостами. Повторювачі відносять до пристроїв Рівня 1 (Фізичного рівня) моделі OSI.

Хаби Ethernet

Виробники мережевого обладнання впровадили пристрої, які забезпечують багато портів Ethernet. Ці пристрої відомі як хаби, які у своєму найпростішому варіанті є звичайними багатопортовими повторювачами. Хаби можна об'єднувати або каскадувати (з використанням ієрархічної схеми), що збільшує кількість портів на сегмент.

Сучасні хаби – це значно складніші пристрої, які мають ряд властивостей, подібних до комутаторів або мостів, що значно

Національний університет
покращує їх можливості при адмініструванні мереж Зокрема, наявність внутрішніх комутаторів у хабі дозволяє розділити порти хаба на декілька груп, кожна з яких відноситься до окремої області колізій. Передавання пакетів між цими групами портів може супроводжуватися їх буферизацією, фільтрацією, контролем правильності пакетів та відкиданням пошкоджених пакетів тощо. Це суттєво покращує експлуатаційні характеристики мережі за рахунок зменшення трафіку в окремих сегментах, більш ефективного використання наявної ширини смуги. Хаб може мати адресований порт подібно до станції, що дозволяє застосовувати дистанційне управління хабом з використанням відповідного протоколу високого рівня (наприклад, SNMP).

Передаючі середовища (кабелі мережі Ethernet)

Коаксіальний кабель

Коаксіальний кабель донедавна був дуже популярний, що пов'язано з його високою завадозахищеністю (завдяки металевому обплетенню), а також більшими допустимими відстанями передачі (до кілометра). До нього важче механічно підключитися для несанкціонованого прослуховування мережі, він дає також помітно менше електромагнітних випромінювань зовні. Однак монтаж і ремонт коаксіального кабелю істотно складніше, ніж витої пари, а вартість його вище (він дорожче приблизно в 1,5 – 3 рази). Складніше й установка конекторів на кінцях кабелю. Зараз його застосовують рідше, ніж виту пару. Стандарт EIA/TIA-568 містить у собі тільки один тип коаксіального кабелю, застосовуваний у мережі Ethernet.

Вита пара

Категорії кабеля

Існує декілька категорій кабеля вита пара, які нумеруються від CAT1 до CAT7 і визначають ефективний частотний пропускний діапазон. Кабель вищої категорії зазвичай містить більше пар проводів і кожна пара має більше витків на одиницю довжини. Категорії неекранованої витої пари описуються в стандарті EIA/TIA 568 (Американський стандарт проводки в приміщеннях) і в міжнародному стандарті ISO 11801.

CAT1 (смуга частот 0,1 МГц) – телефонний кабель, всього одна пара (в нас застосовується кабель взагалі без скруток – «лапша» – в неї характеристики не гірші, але більше завад). Використовується тільки

Національний університет
для передачі голосу або даних за допомогою модема.

CAT2 (смуга частот 1 МГц) – старий тип кабеля, 2 пари провідників, підтримував передачу даних на швидкостях до 4 Мбіт/с, використовувався в мережах Token ring и Arcnet. Зараз іноді зустрічається в телефонних мережах.

CAT3 (смуга частот 16 МГц) – 4-парний кабель, використовується при побудові телефонних і локальних мереж 10BASE-T и token ring, підтримує швидкість передачі даних до 10 Мбіт/с або 100 МБіт/с по технології 100BASE-T4 на відстані не більше 100 метрів.

CAT4 (смуга частот 20 МГц) – кабель складається з 4 скручених пар, використовувався в мережах token ring, 10BASE-T, 100BASE-T4, швидкість передачі даних не перевищує 16 Мбіт/с по одній парі, зараз не використовується.

CAT5 (смуга частот 100 МГц) – 4-парний кабель, використовується при побудові локальних мереж 100BASE-TX і для прокладки телефонних ліній, підтримує швидкість передачі даних до 100 Мбіт/с.

CAT5e (смуга частот 125 МГц) – 4-парний кабель, вдосконалена категорія 5. Швидкість передачі даних до 100 Мбіт/с при використанні 2 пар і до 1000 Мбіт/с при використанні 4 пар. Кабель категорії 5е є самим розповсюдженим і використовується для побудови комп'ютерних мереж.

CAT6 (смуга частот 250 МГц) – застосовується в мережах Fast Ethernet та Gigabit Ethernet, складається з 4 пар провідників і здатний передавати дані на швидкості до 1000 Мбіт/с.

CAT6a (смуга частот 500 МГц) — застосовується в мережах Ethernet, складається з 4 пар провідників і здатний передавати дані на швидкості до 10 Гбіт/с і планується використовувати його для задач обміну, що працюють на швидкості до 40 Гбіт /с.

Порівняльні характеристики найбільш вживаних кабелів

Стандарт EIA/TIA-568-A-1995 визначає мінімальні вимоги щодо телекомунікаційних кабельних систем всередині будинків і між будинками в околі кампусу. Він визначає кабельну систему з рекомендованими топологією та відстанями, окреслює провідні та оптоволоконні середовища (кабелі) за параметрами, які визначають властивості та особливості з'єднувачів, призначення їх контактів для забезпечення здатності до взаємних з'єднань.

Існують три можливості вибору структурованої кабельної системи, кожна з яких має свої характеристики та особливості виготовлення:

1. Кабельна система на основі неекранованого кабеля типу "вита

пара" (UTP) з характеристичним опором 100 Ом:

.

Рис.1. 4-парний кабель UTP.

Переваги кабелів UTP:

- кабелі UTP хороші з точки зору багатосторонності застосувань, пропускної здатності та ефективності в коштах;
- кабелі UTP Категорії 5 можуть передавати дані із швидкістю до 100 Мб/с і підтримувати новітні технології, такі як Fast Ethernet, ATM;
- кабелі UTP прості в укладанні, мають малий діаметр, малу вагу, прості у з'єднаннях і під'єднанні з'єднувачів.

Недоліки кабелів UTP:

- низька механічна захищеність від пошкоджень;
- відносна чутливість до завад, викликаних зовніщніми джерелами електромагнітних полів.

2. Кабельна система на основі екранованого кабеля типу "вита пара" (STP) з характеристичним опором 150 Ом:

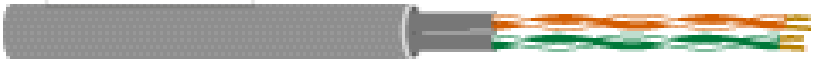


Рис. 2. 2-парний кабель STP типу 1.

Переваги кабелів STP:

- кабелі STP здатні до забезпечення сигналів даних від зовнішнього середовища, середовища від сигналів даних і сигналів даних від впливу сигналів в інших кабелях;
- кабелі STP зменшують кількість майбутніх проблем, які виникають при розміщенні багатьох різних комунікаційних систем в одному будинку.

Недоліки кабелів STP:

- кабелі STP порівняно дорожчі від кабелів UTP;
- необхідно серйозно потурбуватися про встановлення правильного заземлення тільки на одному кінці;
- кабель STP типу 1, який передбачає окремі екрани для кожної пари провідників - це старе вирішення для забезпечення малих перехресних зв'язків; розв'язання, прийняті в кабелях UTP,

забезпечують незначно кращу стійкість до проблем з NEXT без ускладнення проблем укладання кабеля.

3. Кабельні системи на основі багатомодових або одномодових оптоволоконних кабелів:

Рис. 3. 2-волоконно-оптичний кабель

Переваги оптоволоконних кабелів:

- велика ширина смуги;
- відносно мала вартість;
- низьке споживання потужності;
- потребують мало місця;
- нечутливість до електромагнітних завад.

Недоліки оптоволоконних кабелів:

- потрібні вищі кваліфікації при укладанні;
- потрібні вищі кваліфікації при під'єднанні пристроїв;
- кабелі дорожчі і вартість їх укладання більша, ніж для кабелів UTP або коаксіальних кабелів.

Кабельна система на основі коаксіального кабеля тривалий час була основним типом кабельної системи для локальних комп'ютерних мереж.

Переваги коаксіальних кабелів:

- порівняно з кабелями типу "вита пара" коаксіальний кабель має більшу ширину смуги;
- коаксіальний кабель добре захищений від електромагнітних завад на низьких та радіочастотах;
- коаксіальні кабелі мають менше загасання від кабелів типу "вита пара".

Недоліки коаксіальних кабелів:

- коаксіальні кабелі більш складні в укладанні від кабелів типу "вита пара";
- для під'єднання до іншого обладнання та устаткування коаксіальні кабелі потребують застосування спеціальних інструментів, що збільшує кошти цих робіт.

Примітка: На даний час коаксіальний кабель 50 Ом є визнаним типом середовища для передачі даних. Однак, він не рекомендований для нових кабельних інсталяцій і буде вилучений із стандарту при наступному його перегляді.

Національний університет

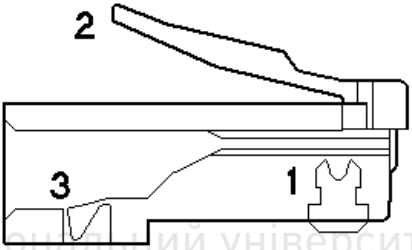
Роз'єми для витої пари

Термін «RJ45» помилково використовується для іменування роз'єму 8P8C (8 Position 8 Contact)

8P8C – використовується для створення мереж за технологіями 10BASE-T, 100BASE-T та 1000BASE-TX.

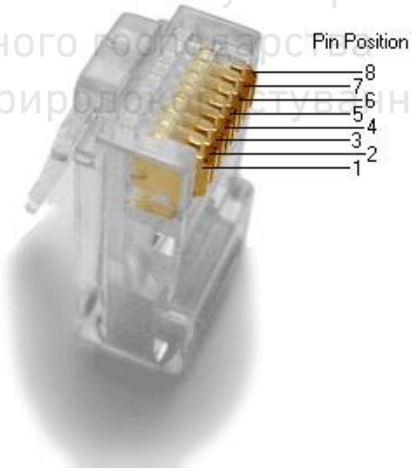
Восьмиконтактний модульний з'єднувач (Вилка, Plug). Народна назва "RJ-45"

Вилка "RJ-45" схожа на вилку від імпортних телефонів, тільки небагато більшого розміру і має вісім контактів.



1 – ножі - контакти 8 шт.
2 - фіксатор роз'єму
3 - фіксатор проводу

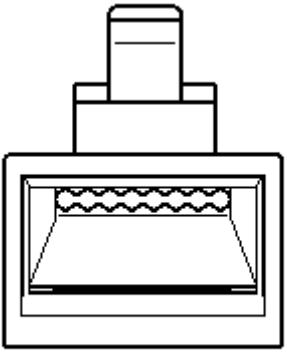
Національний університет
водного господарства
та природокористування



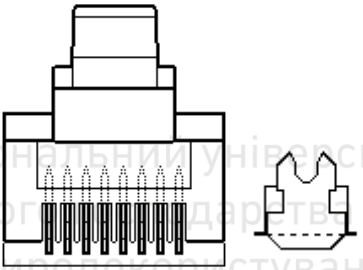
Вид з боку контактів

Національний університет
водного господарства
та природокористування

Вид з боку кабелю



Вид спереду
На новій, невикористаній вилці, контакти виходять за межі корпуса.



У процесі обтиску, вони будуть втоплені всередину корпуса, проріжуть ізоляцію проводу і встромляться в жилу.

Вилки поділяються на екрановані і неекрановані, із вставкою і без, для круглого і для плоского кабелю, для одножильного і для багатожильного кабелю, з двома і з трьома зубцями. Корисно разом з вилкою на кабель встановлювати захисний ковпачок.

Восьмиконтактний модульний з'єднувач

Гніздо (jack) і розетка (outlet)

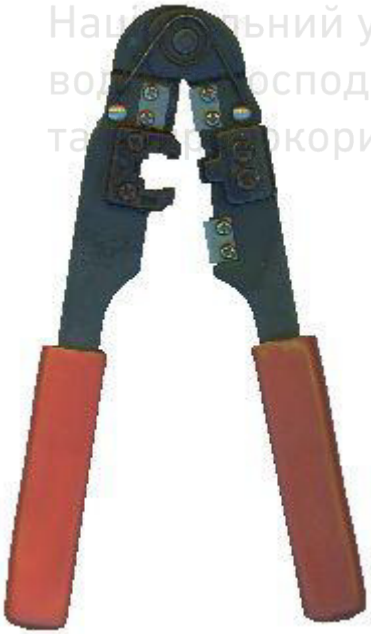
Гнізда встановлюються в мережеві картки, хаби, трансівери і інші пристрої. Сам роз'єм являє собою ряд (8 шт.) пружних контактів і виїмку для фіксатора вилки. Якщо дивитися на гніздо з боку контактів, коли вони розташовуються знизу, то відлік йде справа наліво.

Розетка представляє собою гніздо (роз'єм) з'єднувача з яким-небудь пристосуванням для кріплення кабелю і корпусом для зручності монтажу. У неї теж включається вилка.

Звичайна розетка являє собою невелику пластмасову коробочку, до якої додається шуруп і двостороння наклейка для монтажу на стіну. Якщо покриття стіни дозволяє, простіше користуватися наклейкою, якщо немає - прийдеться свердлити стінку і прикручувати розетку шурупом. З однієї сторони корпуса розташовується роз'єм для включення вилки RJ-45, бувають розетки які мають в корпусі два роз'єми і більше.

Тут використовується пластина з щілиною. Заштовхуючи провід у щілину, ви прорізаєте ізоляцію і жила кабелю входить у контакт із пластиною. Пластина повернена на 45 градусів. Для монтажу проводів продається спеціальний інструмент, що крім заштовхування проводів у щілину, обрізає зайве.

Обжимний інструмент для витої пари



Дозволяє обрізати кабель, видалити зовнішню ізоляцію і обжати конектор RJ-45.

Національний університет
водного господарства
та природокористування

Варіанти обжимки кабеля (патчкорд)

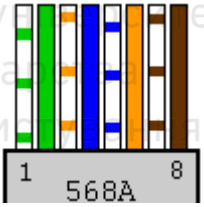
Схеми патчкорд (прямого) обжимання використовуються для з'єднання „комп'ютер"-„свіч".

Якщо кабель має тільки дві пари (4 провідника):

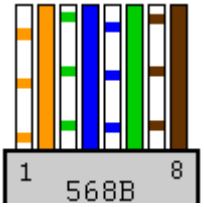
10 Base-T/100 Base-TX		
одна сторона	**колір провода**	Друга сторона
1	біло/оранж	1
2	оранж	2
3	біло/синій	3
6	синій	6

Для восьмиканального кабеля (чотири пари). Вибір стандарту 568A або 568B залежить виключно від застосованого в мережі. Ці два варіанти – еквівалентні. Рекомендовано використовувати перший.

EIA/TIA-568A		
одна сторона	**колір провода**	Друга сторона
1	біло/зелений	1
2	зелений	2
3	біло/оранж	3
4	синій	4
5	біло/синій	5
6	оранжевий	6
7	біло/коричн.	7
8	коричневий	8



EIA/TIA-568B, AT&T 258A		
одна сторона	**колір провода**	Друга сторона
1	біло/оранж	1
2	оранжевий	2
3	біло/зелений	3
4	синій	4
5	біло/синій	5
6	зелений	6
7	біло/коричн.	7
8	коричневий	8



Існують також схеми обжимання типу „кроссовер”, кабелі обжаті таким способом використовуються для з’єднання комп’ютерів між собою (без свічів чи хабів), а також для з’єднання застарілого мережевого обладнання. В принципі сучасне мережеве обладнання в змозі розпізнати схему обжимання, що використовується і підлаштуватись під неї, тому можна сміливо використовувати схему „патч корд”.

Зауважимо, що при обжиманні кабеля 5-ї категорії для швидкості передачі 100Мбіт/с використовуються лише 2 пари з 4-х (оранжева та зелена). Синя і коричнева в цьому випадку можуть бути використані для під’єднання іншого комп’ютера по цьому кабелю. Хоча дана схема може знизити швидкість передавання. При створенні гігабітної мережі вже використовуються всі 4 пари провідників.

Діагностика мережі в операційних системах сімейства Windows

До складу операційної системи Windows включено ряд комунікаційних утиліт, які дають можливість перевірити працездатність з'єднання з віддаленим вузлом (ping), прослідкувати маршрут проходження пакетів до віддаленого вузла (tracert) та інших. Для їх запуску достатньо перейти в режим командного рядка (Пуск-Программи-Стандартние-Командная строка) і ввести з клавіатури у відповідь на запрошення ім'я утиліти з відповідними параметрами.

Також ви повинні пам’ятати, що для того щоб зупинити виконання якоїсь команди/утиліти в командному рядку необхідно натиснути комбінацію клавіш Contol+C.

Для зручності користувачів у Internet кожному комп'ютеру поряд із IP-адресою дається власне символьне ім'я. Цю функцію в Internet виконує доменна служба імен – DNS (DomainNameSystem). Вона являє собою розподілену базу даних, в якій підтримується ієрархічна система символьних імен. Служба DNS призначена для автоматичного пошуку IP-адреси за відомим символьним ім'ям вузла.

База даних про відповідність символьних імен і IP-адрес не зберігається на кожному комп'ютері, а розподілена за великою кількістю DNS-серверів, розташованих на різних вузлах Internet. Кожного разу, коли в прикладній програмі виникає необхідність перетворити ім'я в IP-адресу, вона стає клієнтом служби імен. Клієнт сервера DNS знає IP-адресу сервера DNS свого адміністративного домену і направляє йому запит, у якому повідомляє відоме символьне

ім'я і просить повернути відповідну йому IP-адресу. Якщо дані про запитану відповідність вдається відшукати в базі цього DNS-сервера, то він одразу посилає відповідь клієнту. Якщо ж сервер DNS не може знайти відповіді на запит, він тимчасово стає клієнтом іншого сервера DNS, а потім – наступного сервера імен і так доти, доки не знайде такий сервер, який зможе дати відповідь на запит.

Застосування утиліт ipconfig і ping для тестування з'єднання з віддаленим хостом (за рекомендаціями Microsoft)

Для тестування з'єднання Microsoft рекомендує таку процедуру перевірки:

1. Запустіть утиліту ipconfig і визначте такі параметри, як IP-адреса локального комп'ютера (IPadressofLocalhost), маска підмережі, адреса шлюзу за замовчуванням (IP_adress of_default_gateway) і адреса DNS-сервера (IP_adress_of_DNS_server).
2. Зверніться за IP-адресою "замикання на себе": ping 127.0.0.1.
3. Перевірте відгук власного комп'ютера: ping IP_adress_of _Local_host.
4. Запитайте відгук шлюзу за замовчуванням: ping IP_adress_of_default_gateway. Якщо команду не було успішно виконано, слід перевірити правильність IP-адреси основного шлюзу і працездатність цього шлюзу (маршрутизатора).
5. Зверніться за адресою віддаленого вузла: ping IP_adress_of_reraote_host. Якщо команду не було успішно виконано, слід перевірити правильність IP-адреси віддаленого вузла, працездатність цього вузла, а також працездатність усіх шлюзів (маршрутизаторів) між локальним комп'ютером і віддаленим вузлом.
6. Зверніться за адресою DNS-сервера: ping IP_adress_of_ DNSserver. Якщо команду не було успішно виконано, слід перевірити правильність IP-адреси DNS-сервера, працездатність DNS-сервера, а також працездатність усіх шлюзів (маршрути-заторів) між локальним комп'ютером і DNS-сервером.

1.3. Програма роботи

1. Розглянути види кабелів, вилок, розеток, ознайомитися з теоретичним матеріалом.
2. Обжати кабель 5-ї категорії типу „Вита пара”.
3. Провести налаштування параметрів TCP/IP в ОС Windows.

Національний університет
водного господарства
та природокористування

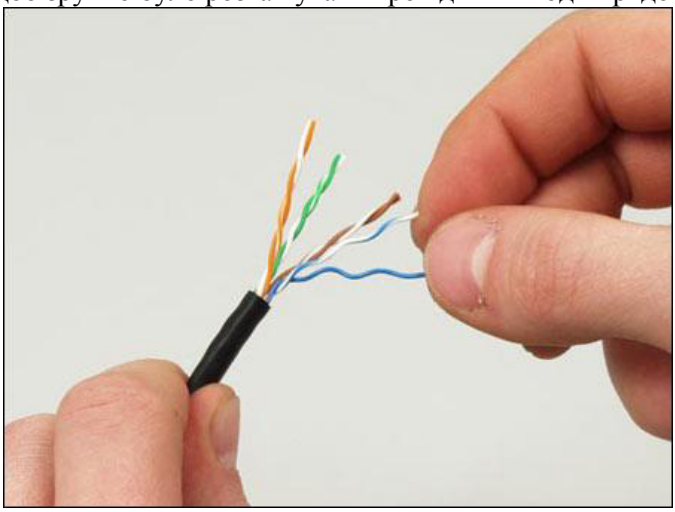
1.4. Порядок виконання роботи

1. Для обжиму кабеля «вита пара» необхідно виконати наступні кроки:

– Візьміть кабель, надягніть захисний ковпачок та зніміть ізоляції з кабеля мінімум на 20 мм:

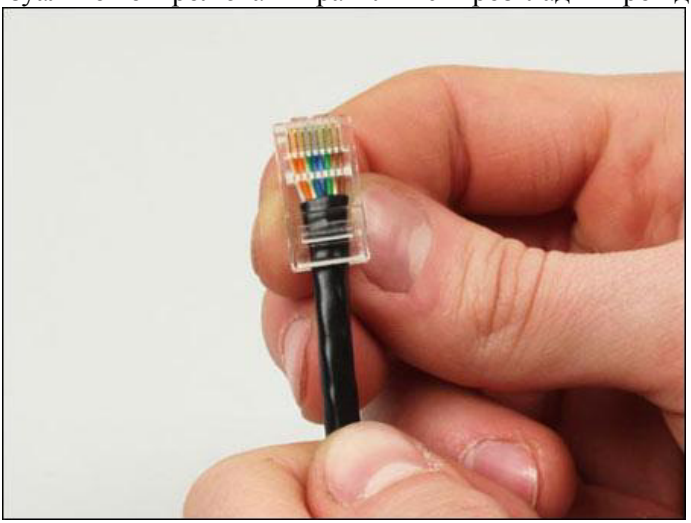
Національний університет
водного господарства
та природокористування

– Для того щоб помістити кабель в роз'єм, потрібно розплести пари. Пари розплітаються аж до краю ізоляції, якій надається плоска форма, щоб зручно було розташувати провідники в один рядок:



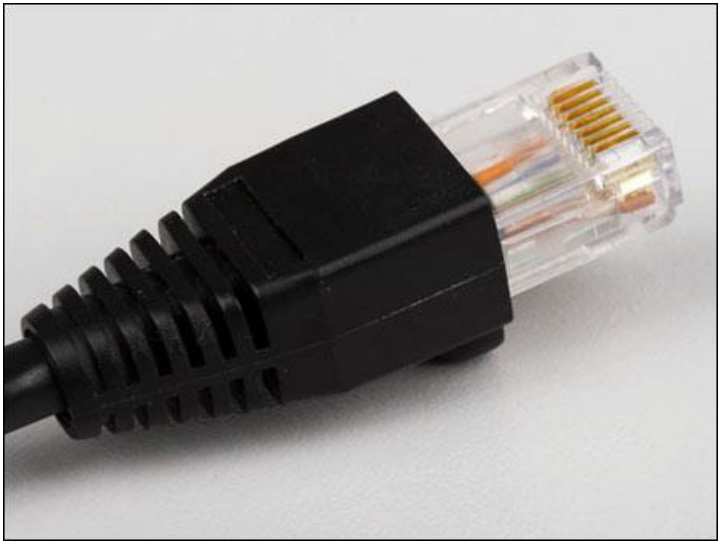
– Пари повинні бути розкладені таким чином, щоб сформувався плоский шар з паралельно розташованих провідників. За допомогою крімпера підріжте провідники на відстань близько 14 мм від краю оболонки кабелю.

– Помістіть провідники в роз'єм так, щоб вони розмістились в каналах, а оболонка кабеля заходила в роз'єм, принаймні, на 6 мм. Завдяки тому, що корпус роз'єма виготовлений з прозорого пластику, можна візуально контролювати правильність розкладки провідників:



– Для з’єднання провідників з ножами роз’єму скористайтеся професійним обжимним інструментом. Якщо спочатку ножі-контакти виступали за межі корпусу, то в процесі обжиму вони будуть вдавлені всередину корпусу, тим самим прорізавши оболонку провідників створивши електричний контакт:

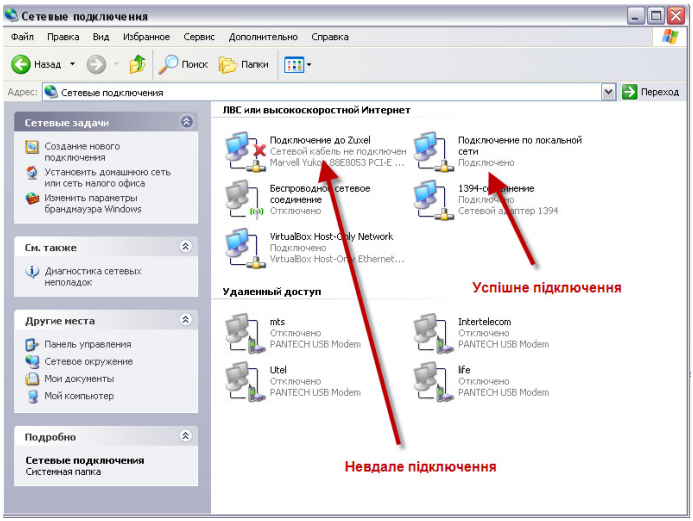
– Перевірте правильність обжимання, проконтролюйте, щоб ножі-контакти були з’єднані з жилами провідників. Після цього надіньте захисний ковпачок:



– Останній крок: перевірте правильність обжимання за допомогою тестера:

2. Після того як кабель було обжато, перевірено його правильність і підключено до іншого мереженого обладнання (комп'ютера чи комутатора/концентратора) необхідно здійснити налаштування TCP/IP параметрів. Нижче будуть наведені вказівки для системи Windows XP:

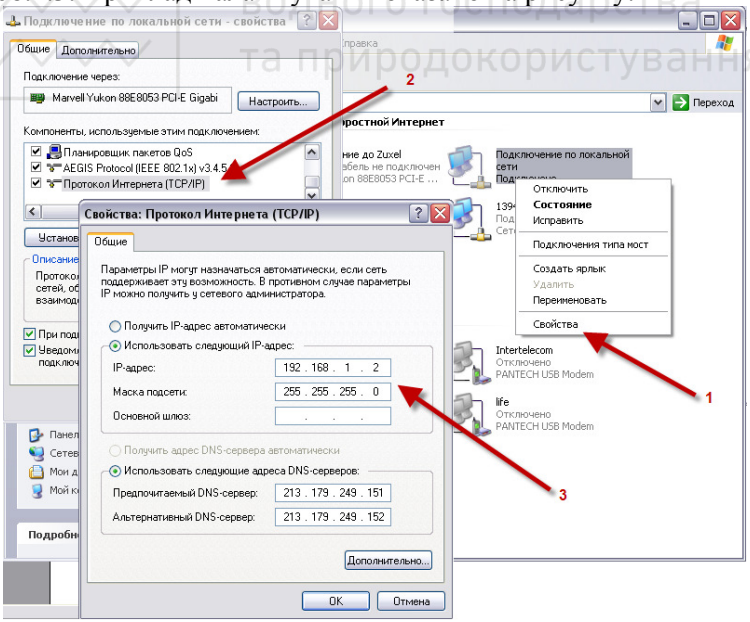
– Отже, для налаштувань TCP/IP параметрів перейдіть в меню „Сетевые подключения": „Пуск"-„ Панель управления"-„ Сетевые подключения":



– Якщо підключення було зроблено невдало з технічної точки зору, тоді на іконці мережевого інтерфейсу буде намальований хрестик і зазначено про помилку, як на рисунку зображеному вище. Тоді необхідно перевірити правильність з'єднання, правильність прокладки кабелю, чи не з'явилось пошкоджень, перекручувань і т.д.

– Якщо підключення успішне, виберіть властивості підключення та перейдіть до налаштувань протоколу TCP/IP. Операційна система Windows XP підтримує застарілий протокол IP адресації IPv4. В нових ОС типу Windows Vista, Windows 7 є також налаштування протоколу IPv6. Потрібно орієнтуватися на те, яка система IP-адресації прийнята у вашому мережевому середовищі і відповідно її налаштовувати. В нашому випадку налаштуйте IPv4.

– У властивостях протоколу можна вибрати отримання IP адреси автоматично чи задати вручну. Автоматичне отримання можливе при наявності DHCP сервера в мережі (наприклад, це може бути роутер з функцією DHCP). Задайте IP адресу вручну. Для цього вкажіть IP адресу наприклад 192.168.1.2 (клас C), а маску - 255.255.255.0. На іншому комп'ютері здійсніть ті самі налаштування і IP адресу задайте 192.168.1.3. Приклад налаштувань показано на рисунку:



– Адреси DNS серверів вказуються при наявності мережі Інтернет. Служба DNS відповідає за перетворення символьних імен, які прості

для запам’ятовування у IP адреси, наприклад, ім’я facebook.com перетвориться в IP адресу 31.13.72.36, google.com в 74.125.87.104, nuwm.edu.ua в 37.57.114.206 і т.д. Тому для локальної мережі не потрібно їх вказувати.

– Після того, як параметри TCP/IP було задано потрібно протестувати з’єднання. Для цього використовуються наступні утиліти консольні утиліти:

Ipconfig
Ping
Tracert
PathPing
Netstat
Arp

Для того щоб задіяти ці утиліти необхідно запустити інтерпретатор командної стрічки: «Пуск»-«Все программы»-«Стандартные»-«Командная строка». І далі у вікні, що з’явиться (воно буде чорного кольору), потрібно буде вводити вищевказані команди.

3. Дослідити налаштування мережевих протоколів Пк за допомогою утиліти IPCONFIG. Записати й проаналізувати отриману інформацію й дати характеристику комп'ютеру. Тут можна побачити MAC адресу комп’ютера, вона також називається фізичною адресою.

4. Перевірити з'єднання з адресатом за допомогою утиліти Ping.

Перевірити з'єднання з адресатом, якщо замість адреси вказуєте ім'я комп'ютера. (Перевірка дозволу імен). Також дослідіть які ще параметри може приймати утиліта ping. У випадку, якщо не відбувається з’єднання при вказаних доменних іменах (через блокування центральним сервером DNS запитів) виконати цю роботу вдома.

5. Перевірити маршрут до адресата за допомогою утиліти Tracert.

6. Знайти комп'ютери в мережі із кількістю проміжних вузлів більше одного за допомогою утиліти PathPing.

7. Проаналізувати роботу утиліти netstat з різними ключами. Занотувати парамети та їх пояснення, навести приклади.

Відображаються всі з’єднання та порти, які очікують.

>netstat –a

```
Активные подключения

  Имя    Локальный адрес         Внешний адрес          Состояние
  TCP    nuwm-lab1:epmap  nuwm-lab1:0      LISTENING
  TCP    nuwm-lab1:microsoft-ds  nuwm-lab1:0      LISTENING
```

```
  TCP    nuwm-lab1:1025   nuwm-lab1:0      LISTENING
  TCP    nuwm-lab1:1288   lb-in-f100.1e100.net:http  ESTABLISHED
  TCP    nuwm-lab1:1095   nuwm-lab1:1096   ESTABLISHED
  TCP    nuwm-lab1:1096   nuwm-lab1:1095   ESTABLISHED
  UDP    nuwm-lab1:microsoft-ds  *:*
  UDP    nuwm-lab1:isakmp  *:*
  UDP    nuwm-lab1:1026   *:*
  UDP    nuwm-lab1:1107   *:*
  UDP    nuwm-lab1:1108   *:*
  UDP    nuwm-lab1:ipsec-msft  *:*
  UDP    nuwm-lab1:ntp    *:*
  UDP    nuwm-lab1:ntp    *:*
```

При створенні нових з'єднань, таблиця поповнюється.

>netstat –a

```
Активные подключения

  Имя    Локальный адрес        Внешний адрес          Состояние
  TCP    nuwm-lab1:epmap  nuwm-lab1:0      LISTENING
  TCP    nuwm-lab1:microsoft-ds  nuwm-lab1:0      LISTENING
  TCP    nuwm-lab1:1025   nuwm-lab1:0      LISTENING
  TCP    nuwm-lab1:1288   lb-in-f100.1e100.net:http  TIME_WAIT
  TCP    nuwm-lab1:1289   lb-in-f105.1e100.net:https  ESTABLISHED
  TCP    nuwm-lab1:1290   lb-in-f94.1e100.net:https  TIME_WAIT
  TCP    nuwm-lab1:1291   lb-in-f94.1e100.net:https  ESTABLISHED
  TCP    nuwm-lab1:1292   74.125.232.79:https    ESTABLISHED
  TCP    nuwm-lab1:1293   lb-in-f94.1e100.net:http  ESTABLISHED
  TCP    nuwm-lab1:1095   nuwm-lab1:1096   ESTABLISHED
  TCP    nuwm-lab1:1096   nuwm-lab1:1095   ESTABLISHED
  UDP    nuwm-lab1:microsoft-ds  *:*
  UDP    nuwm-lab1:isakmp  *:*
  UDP    nuwm-lab1:1026   *:*
  UDP    nuwm-lab1:1107   *:*
  UDP    nuwm-lab1:1108   *:*
  UDP    nuwm-lab1:ipsec-msft  *:*
  UDP    nuwm-lab1:ntp    *:*
  UDP    nuwm-lab1:ntp    *:*
```

Відображається статистика Ethernet

>netstat –e

```
Статистика интерфейса
                           Получено            Отправлено

Байт                      63931248         12197569
Одноадресные пакеты          55077            36247
Многоадресные пакеты         47202               20
Отброшено                        0                0
Ошибки                           0                0
Неизвестный протокол          1800
```

Виводиться статистика для кожного протоколу

>netstat –s

```
Статистика IPv4
  Получено пакетов                  = 58713
  Получено ошибок в заголовках      = 2
```

```
  Получено ошибок в адресах          = 257
  Направлено датаграмм               = 0
  Получено неизвестных протоколов    = 0
  Отброшено полученных пакетов       = 0
  Доставлено полученных пакетов      = 54583
  Запросов на вывод                  = 30410
  Отброшено маршрутов                = 0
  Отброшено выходных пакетов         = 0
  Выходных пакетов без маршрута      = 0
  Требуется сборка                   = 4012
  Успешная сборка                    = 141
  Сбоев при сборке                   = 66
  Успешно фрагментировано датаграмм  = 254
  Сбоев при фрагментации датаграмм   = 0
  Создано фрагментов                 = 6099

Статистика ICMPv4
                          Получено   Отправлено
  Сообщений               1868        2130
  Ошибок                  0           0
  'Назначение недостижимо' 2          30
  Превышений времени      145         0
  Ошибок в параметрах     0           0
  Просьб "снизить скорость" 0         0
  Переадресовано          0           0
  Эхо-сообщений           18          2082
  Ответных пакетов        1703        18
  Штампов времени         0           0
  Ответы на штампы времени 0          0
  Масок адресов           0           0
  Ответов на маски адресов 0          0

Статистика TCP для IPv4
  Активных открыто                   = 337
  Пассивных открыто                  = 58
  Сбоев при подключении              = 51
  Сброшено подключений               = 38
  Текущих подключений                = 11
  Получено сегментов                 = 47755
  Отправлено сегментов               = 26658
  Повторно отправлено сегментов      = 27

Статистика UDP для IPv4
  Получено датаграмм    = 1590
  Отсутствие портов     = 8252
  Ошибки при получении  = 338
  Отправлено датаграмм  = 1593
```

Аналіз роботи протоколу TCP

- отримано пакетів: 58713
- доставлено отриманих пакетів: 54583
- ступінь обслуговування(54583/58713): 0,93
- відкинутих пакетів або пакетів з помилками: 0

Національний університет водного господарства та природокористування

- ефективність прийому (58713/30410): 1,93

Аналіз роботи із протоколу TCP

- було зроблено неуспішних спроб з'єднань: 51
- було зроблено повторних з'єднань: 38
- повторно відправлено сегментів: 27

Аналіз роботи із протоколу UDP

- інтенсивність роботи протоколу на прийом і передачу
  - отримано: 1590/91324
  - відправлено: 1593/138546
- помилок при одержанні (338/1593): 0,21

Аналіз роботи із протоколу ICMP.

- Визначити інтенсивність роботи із протоколу на прийом і передачу
  - отримано: 1868/91324
  - відправлено: 2130/138546

Вивести таблицю маршрутизації системи.

>netstat –r

```
IPv4 таблица маршрута
===========================================================================
Список интерфейсов
0x1 ........................... MS TCP Loopback interface
0x10003 ...08 00 27 50 3a 07 ...... AMD PCNET ёхьхщёЄтю PCI Ethernet
рфряЄхЕют
===========================================================================
===========================================================================
Активные маршруты:
Сетевой адрес          Маска сети      Адрес шлюза     Интерфейс
Метрика
          0.0.0.0          0.0.0.0      77.123.70.1    77.123.70.147     20
     77.123.70.0    255.255.255.0    77.123.70.147    77.123.70.147     20
    77.123.70.147  255.255.255.255        127.0.0.1        127.0.0.1     20
  77.255.255.255  255.255.255.255    77.123.70.147    77.123.70.147     20
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1      1
        224.0.0.0        240.0.0.0    77.123.70.147    77.123.70.147     20
  255.255.255.255  255.255.255.255    77.123.70.147    77.123.70.147      1
Основной шлюз:         77.123.70.1
===========================================================================
Постоянные маршруты:  Отсутствует
```

Виводити статистику для протоколу TCP з інтервалом в 5 секунд.

>netstat -e -s -p tcp 5

```
Статистика интерфейса
                           Получено            Отправлено

Байт                       63960638            12203376
Одноадресные пакеты           55177               36366
Многоадресные пакеты          47508                  20
Отброшено                         0                   0
```

```
Ошибки                                0                0
Неизвестный протокол               1816

Статистика TCP для IPv4
  Активных открыто                    = 337
  Пассивных открыто                   = 60
  Сбоев при подключении               = 53
  Сброшено подключений                = 38
  Текущих подключений                 = 2
  Получено сегментов                  = 47823
  Отправлено сегментов                = 26742
  Повторно отправлено сегментов       = 27

Активные подключения

  Имя    Локальный адрес         Внешний адрес          Состояние
  TCP    nuwm-lab1:1095   nuwm-lab1:1096   ESTABLISHED
  TCP    nuwm-lab1:1096   nuwm-lab1:1095   ESTABLISHED

Статистика интерфейса
                           Получено            Отправлено

Байт                     63965396        12205837
Одноадресные пакеты         55211           36403
Многоадресные пакеты        47540              20
Отброшено                       0               0
Ошибки                          0               0
Неизвестный протокол         1816

Статистика TCP для IPv4
  Активных открыто                    = 340
  Пассивных открыто                   = 60
  Сбоев при подключении               = 53
  Сброшено подключений                = 38
  Текущих подключений                 = 5
  Получено сегментов                  = 47855
  Отправлено сегментов                = 26777
  Повторно отправлено сегментов       = 27

Активные подключения
  Имя    Локальный адрес         Внешний адрес          Состояние
  TCP    nuwm-lab1:1370   lb-in-f94.1e100.net:http  ESTABLISHED
  TCP    nuwm-lab1:1371   lb-in-f94.1e100.net:http  ESTABLISHED
  TCP    nuwm-lab1:1372   wikipedia-lb.esams.wikimedia.org:http
  TCP    nuwm-lab1:1095   nuwm-lab1:1096   ESTABLISHED
  TCP    nuwm-lab1:1096   nuwm-lab1:1095   ESTABLISHED
```

Виводити статистику для протоколу UDP з інтервалом в 5 секунд.

>netstat -e -s -p udp 5

```
Статистика интерфейса
                           Получено            Отправлено

Байт                     65466932        12325283
Одноадресные пакеты         57535           38274
Многоадресные пакеты        47568              20
```

```
Отброшено                       0                 0
Ошибки                          0                 0
Неизвестный протокол         1816

Статистика UDP для IPv4
  Получено датаграмм    = 1645
  Отсутствие портов     = 8344
  Ошибки при получении  = 344
  Отправлено датаграмм  = 1648

Активные подключения
  Имя     Локальный адрес         Внешний адрес          Состояние
```

Визначити динамічні характеристики станції.

Змінити роботу станції, наприклад, приєднатися до сервера/станції і повторити операцію. Проаналізувати нові отримані дані.

1.5. Контрольні запитання

1. Що таке Ethernet?
2. Які ви знаєте види кабелів?
3. Що таке термінатор?
4. Що таке Т-конектор?
5. З чого складається вита пара?
6. Який потрібно тип проводу для передачі даних зі швидкістю до 100 Мбіт за секунду (Mbps) включно?
7. Який стандарт визначає схеми обжимки і прокладання кабелів в приміщеннях?
8. Які ви знаєте варіанти обжиму кабелів витої пари?
9. Які категорії кабелів найбільш розповсюджені?
10. Що таке патчкорд?
11. Що таке кросовер?
12. Назвіть утиліти для тестування мережі в ОС сімейства Windows.
13. Для чого використовується утиліта ipconfig?
14. Що таке ARP?
15. Для чого використовується утиліта netstat?
16. Для чого використовується утиліта ping?
17. Для чого використовується утиліта tracert?
18. Як при роботі з командним рядком отримати довідку про використання утиліт ping, tracert?

Національний університет
водного господарства
та природокористування

19. Яку інформацію можна отримати з аналізу IP-адреси? Що таке MAC адреса?
20. Яку функцію в мережі виконують DNS-сервери?
21. Як протестувати з'єднання з віддаленим хостом?
22. Як визначити доменне ім'я хосту з відомою IP-адресою?
23. Як визначити IP-адресу хосту із зазначеним доменним ім'ям?
24. За допомогою якої утиліти можна з'ясувати, на яких ланках маршруту слідування відбувається затримка пакетів?

Національний університет
водного господарства
та природокористування

Національний університет
водного господарства
та природокористування

Робота 2. Створення локальної мережі за допомогою бездротової точки доступу

2.1. Мета роботи

Ознайомитись з будовою і призначенням основних складових для побудови локальних мереж за допомогою бездротової точки доступу.

2.2. Теоретичні відомості

Як правило, до устаткування, яке потрібно для розгортання бездротової мережі, відносять бездротову точку доступу й бездротові адаптери. Однак у найпростішому випадку для розгортання бездротової мережі не потрібно навіть використання точки доступу. Справа в тому, що існують два режими функціонування бездротових мереж: режим Infrastructure і режим Ad Hoc.

У режимі Ad Hoc, що також називають Independent Basic Service Set (IBSS) або режимом Peer to Peer (точка-точка), вузли мережі безпосередньо взаємодіють один з одним без участі точки доступу. Цей режим вимагає мінімального устаткування: кожний клієнт мережі повинен бути оснащений тільки бездротовим адаптером. При такій конфігурації не потрібно створення мережної інфраструктури. Основними недоліками режиму Ad Hoc є обмежений діапазон дії одержуваної мережі й неможливість підключення до зовнішньої мережі (наприклад, до Інтернету). Приміром, якщо обоє бездротових клієнта (ПК із бездротовими адаптерами) перебувають в одній кімнаті в межах прямої видимості, то режим Ad Hoc дозволяє об'єднати цих клієнтів у бездротову мережу. Це може виявитися зручним, коли потрібно оперативно скачати дані з одного ПК на іншій (приміром, до вас зайшов друг зі своїм ноутбуком). Але от якщо ставиться завдання об'єднати в локальну бездротову мережу комп'ютери, розташовані в різних кімнатах і розділені бетонною стіною з арматурами, то режим Ad Hoc швидше за все не підійде, оскільки потужності передавачів і чутливості приймачів для забезпечення стійкого з'єднання бездротових адаптерів буде недостатньо. У цьому випадку для організації бездротової мережі буде потрібно стаціонарна точка доступу. Втім, перевага точки доступу полягає не тільки в тім, що

Національний університет водного господарства та природокористування
вона дозволяє істотно розширити зону покриття (радіус дії) бездротової мережі.

Точка доступу в бездротовій мережі виконує функцію, аналогічну функції комутатора традиційної кабельної мережі, і дозволяє поєднувати всіх клієнтів у єдину мережу. Завдання точки доступу - координувати обмін даними між всіма клієнтами бездротової мережі й забезпечити всім клієнтам рівноправний доступ до середовища передачі даних.

Режим функціонування бездротової мережі на базі точки доступу називається режимом Infrastructure Mode. Розглядають два режими Infrastructure - основний режим BSS (Basic Service Set) і розширений режим ESS (Extended Service Set). У режимі BSS всі вузли мережі зв'язуються між собою тільки через одну точку доступу, що може виконувати також роль моста до зовнішньої мережі. У розширеному режимі ESS існує інфраструктура декількох мереж BSS, причому самі точки доступу взаємодіють один з одним, що дозволяє передавати трафік від однієї BSS до іншої. Між собою точки доступу з'єднуються за допомогою або сегментами кабельної мережі, або радіомостів.

Стандарти бездротового зв'язку

Існує кілька основних типів бездротових стандартів: 802.11a, 802.11b і 802.11g. Відповідно до цих стандартів використовуються різні типи устаткування. Стандарт містить наступні специфікації:

- 802.11a – високошвидкісний стандарт WLAN для частоти 5 ГГц. Підтримує швидкість передачі даних 54 Мбіт/с.
- 802.11b – стандарт WLAN для частоти 2,4 ГГц. Підтримує швидкість передачі даних 11 Мбіт/с.
- 802.11g – встановлює додаткову техніку модуляції для частоти 2,4 ГГц. Призначений для забезпечення швидкостей передачі даних до 54 Мбіт/с.

Розробкою і підтримкою стандарту IEEE 802.11 займається комітет *Wi-Fi* Alliance. Термін ***Wi-Fi*** (wireless fidelity) використовується як загальне ім'я для стандартів 802.11a і 802.11b, а також всіх подальших, що відносяться до безпровідних локальних мереж (*WLAN*).

Устаткування безпровідних мереж включає ***точки безпровідного доступу*** (Access Point) і ***безпровідні адаптери*** для кожного абонента.

Точки доступу виконують роль концентраторів, що забезпечують зв'язок між абонентами і між собою, а також функцію мостів, що здійснюють зв'язок з кабельною локальною мережею і з Інтернет.

Декілька близькорозташованих точок доступу утворюють зону доступу *Wi-Fi*, в межах якої всі абоненти, забезпечені безпровідними адаптерами, дістають доступ до мережі. Такі **зони доступу** (Hotspot) створюються в місцях масового скупчення людей: в аеропортах, студентських городках, бібліотеках, магазинах, бізнес-центрах і т.д.

Кожна точка доступу може обслуговувати декількох абонентів, але чим більше абонентів, тим менш ефективна швидкість передачі для кожного з них. *Метод доступу* до мережі – **CSMA/CA** (Carrier Sense Multiple Access/Collision Avoidance).

На українському ринку представлені точки доступу й бездротові маршрутизатори компаній 3Com, Asus, Asante, D-Link, Gigabyte, MSI, Multico, Trendnet, US Robotics, ZyXEL, SMC і ін.

Налаштування точки доступу

Найкращий спосіб налаштувати DWL-G700AP - використовувати комп'ютер (із встановленим мережним адаптером Ethernet), підключений до комутатора. IP адреса **по замовчуванню** для DWL-G700AP встановлена **192.168.0.50** з маскою підмережі **255.255.255.0.** Необхідно призначити комп'ютеру статичну IP адресу з тієї ж підмережі, що й для DWL-G700AP, для того, щоб приступити до налаштування точки доступу. Згадайте, що для налаштувань TCP/IP параметрів потрібно перейти в меню „Сетевые подключения”: „Пуск”-„ Панель управления”-„ Сетевые подключения” і там здійснити налаштування в потрібному мережевому інтерфейсі.

Запам’ятайте IP адресу і маску, для того щоб потім відновити стан комп’ютера після завершення лабораторної роботи.

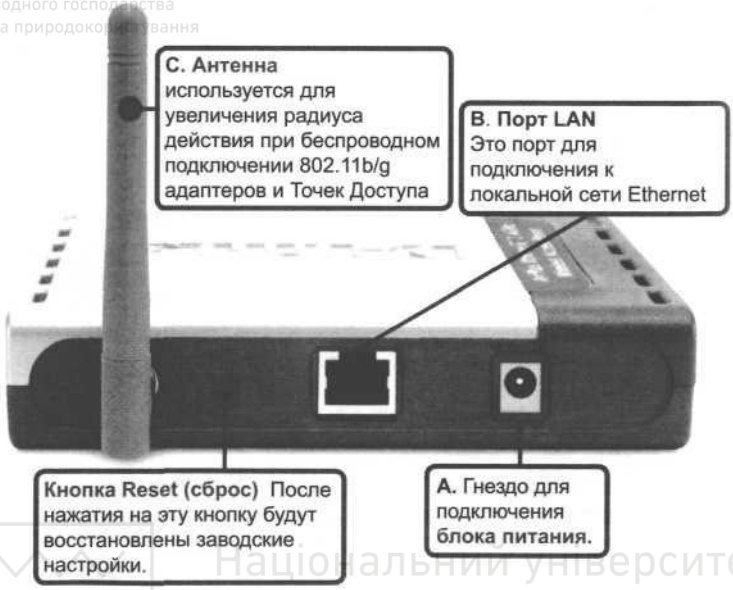
Підключення до бездротової точки доступу DWL-G700AP

Спочатку підключіть блок живлення до роз’єму живлення на задній панелі DWL-G700AP, потім приєднайте блок живлення до розетки. Світлодіод "Power" (Живлення) засвітиться, що означає, що пристрій включений.

Підключіть кабель однією стороною до Ethernet порту, що розташований на задній панелі DWL-G700AP, а іншою стороною до власного комп’ютера, маршрутизатора або до комутатора.

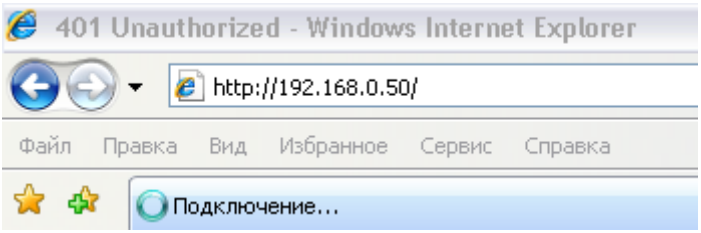
При правильному підключенні до мережі Ethernet засвітиться світлодіод «Link» (з'єднання).

Національний університет
водного господарства
та природокористування



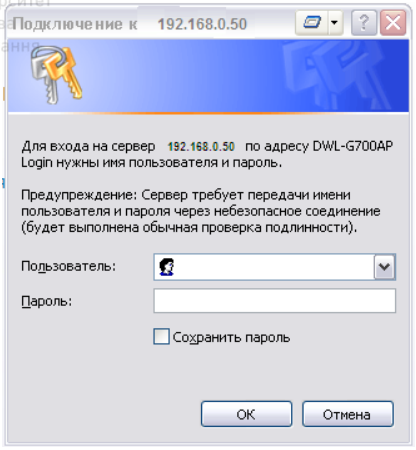
Національний університет
водного господарства
та природокористування

Отже, після того як було підключено точку доступу до мережі потрібно її налаштувати. Для цього перейдіть у браузері по адресі **192.168.0.50:**



Перед вами з’явиться вікно авторизації:

Національний університет
водного господарства
та природокористування

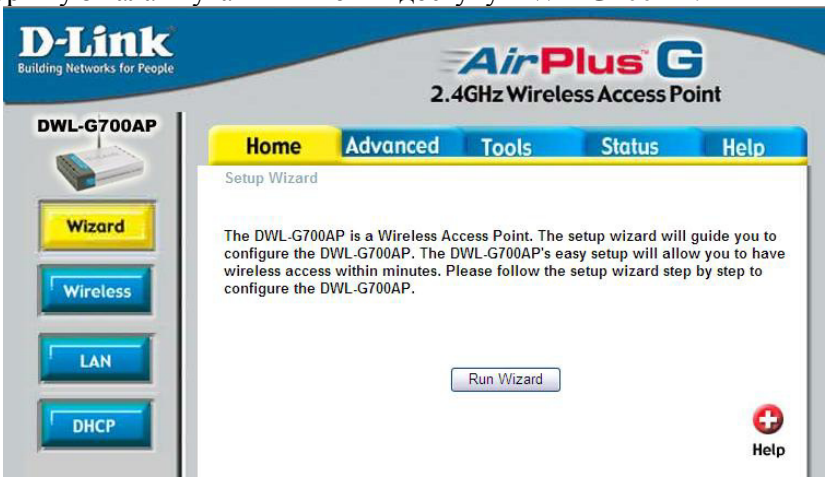


За замовчуванням використовуйте логін **admin** і пустий пароль.

Якщо вікно авторизації не з'явилось, тоді перевірте чи є мережеве з'єднання з точкою доступу. Для цього скористайтеся утилітою ping. В командній стрічці введіть Ping 192.168.0.50.

У випадку коли адреса 192.168.0.50 не пінгується, тоді потрібно скинути налаштування точки доступу до заводських. Для цього скористайтеся кнопкою reset, що знаходиться на корпусі. Нажміть її, потримайте 10 секунд після чого зачекайте поки світлодіоди знову засвітяться – це буде означати, що налаштування відновлені.

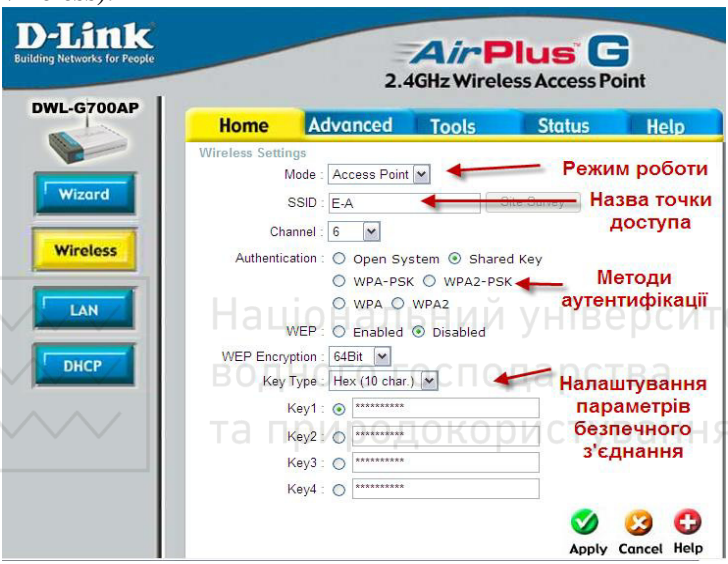
Після успішної авторизації ви потрапляєте на домашню веб сторінку з налаштуваннями точки доступу **DWL-G700AP**:



Перелік пунктів головного (горизонтального) меню:

Home – домашняя початкова сторінка, яку вже було зображено вище. Тут проводяться всі основні налаштування: безпровідникової мережі (пункт меню **Wireless**), підключення до локальної (пункт меню **LAN**), DHCP сервера (пункт меню **DHCP**) та можна запустити помічника налаштувань (пункт меню **Wizard**).

Розглянте основні налаштування для безпровідникової мережі (пункт **Wireless**):



Технології захисту безпровідникового зв'язку

WEP (англ. Wired Equivalent Privacy) — найстаріший стандарт захисту безпровідникового трафіку, заснований на методі потокового кодування з використанням алгоритму RC4 (з використанням загального секретного ключа). Існують варіанти з різною довжиною ключа. Сьогодні використання WEP для захисту мереж не можна вважати надійним способом гарантування безпеки. Тому цей протокол в даний момент майже не використовується.

WPA (Wi-Fi Protected Access). Основа WPA - Temporal Key Integrity Protocol (TKIP). Загалом, TKIP набагато краще WEP: механізм шифрування більш стійкий, до того ж його можна використовувати на існуючому обладнанні. TKIP змінює ключ для кожного пакета, що передається і тим самим усуває будь-яку

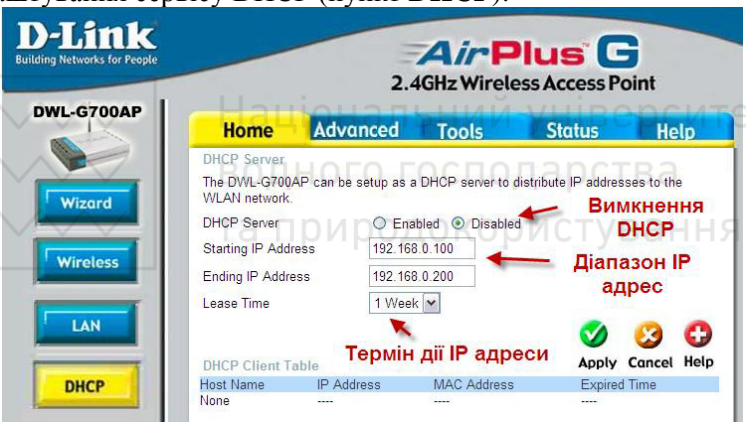
можливість підбору ключа. (Існує і полегшена версія WPA - WPA Pre-Shared Key (WPA-PSK).

WPA-PSK (WPA Pre-Shared Key). Полегшена версія WPA. Дана технологія захисту більше підходить для невеликих мереж. У ній як і в WEP існує статичний ключ, але використовується і TKIP, що автоматично змінює ключ в певних часових інтервалах.

WPA2 (Wi-Fi Protected Access). Дана технологія є покращеною версією WPA. Більш захищена внаслідок заміни TKIP на CCMP (блочне шифрування з кодом аутентичності повідомлень). З 2006-го року підтримка WPA2 є обов'язковою для всіх сертифікованих Wi-Fi пристроїв

WPA2-PSK (Wi-Fi Protected Access). Полегшена версія WPA2, аналогічно WPA PSK, але з AES-шифруванням.

Налаштування сервісу DHCP (пункт **DHCP**):

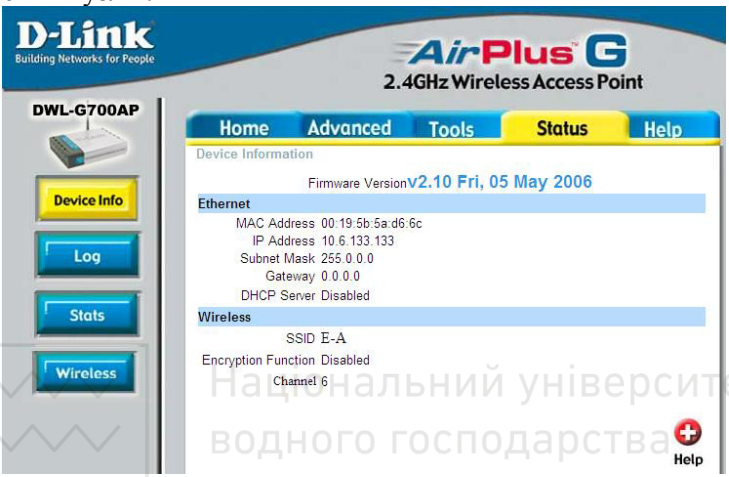


В даному випадку служба DHCP вимкнена і вузли, що будуть підключатися до безпровідникової точки доступу, повинні задавати IP адресу в ручному режимі. Але якщо є сервер DHCP вони можуть отримати автоматично IP адресу. У разі ввімкнення служби DHCP (пункт **enabled**) безпровідні пристрої отримають IP адресу з діапазону вказаного нижче (starting IP address – ending IP address). Ця IP адреса буде дійсна протягом часу **Lease Time**. Це якраз той випадок коли IP адреса буде називатися динамічною. Тобто буде змінюватися через певні проміжки часу. Зверніть увагу, що мобільні телефони та смартфони часто не мають налаштувань для статичної IP, тому вони потребують ввімкненого DHCP сервера.

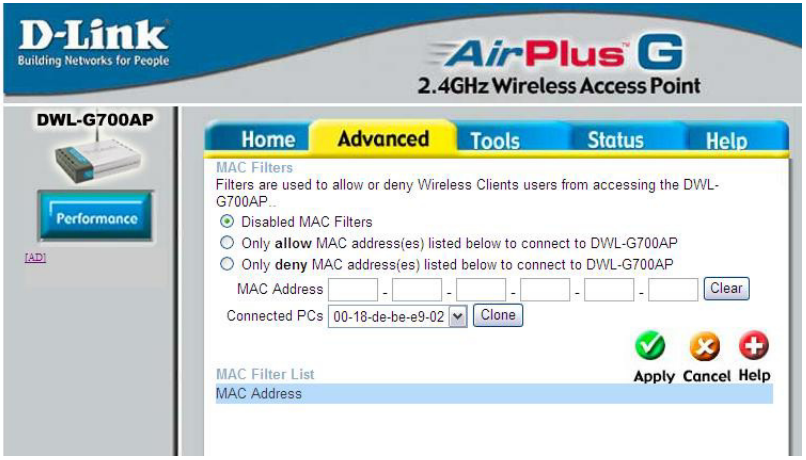
Змініть назву точки доступу. Підключіться до неї.

Ввімкніть якесь шифрування і також підключіться. Знайдіть ваш пристрій серед під'єднаних до точки доступу вузлів. Запам'ятайте його MAC адресу. Для перегляду статистики скористайтесь меню **Status.**

Status – меню для різної статистичної інформації, логів, списку підключених вузлів:

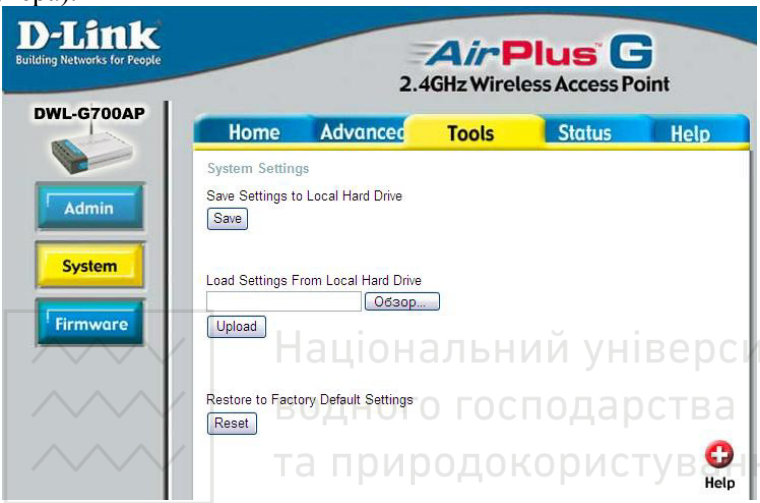


Advanced – додаткові налаштування. Налаштування списку дозволених комп'ютерів по MAC адресах ітд ітп.



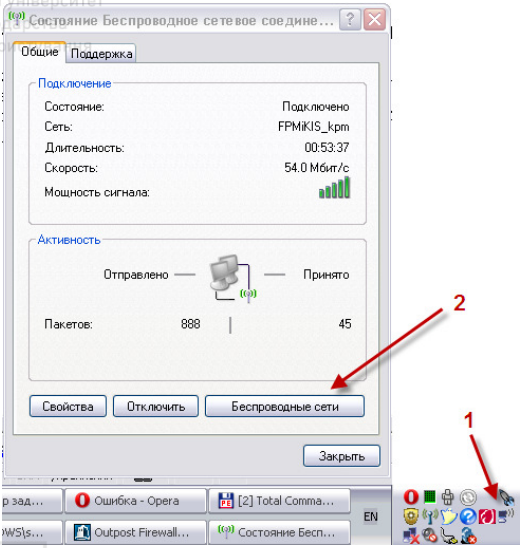
Ще одним методом обмеження доступу до точки доступу для небажаних клієнтів є приховування назви точки доступу. Приховайте назву точки доступу та підключіться до неї знаючи її ім'я.

Tools – меню для задання прав доступу для налаштувань роутера, збереження його налаштувань на локальний диск, для подальшого можливого відновлення, зміни програмного забезпечення (прошивки роутера).



Налаштування бездротового Wi-Fi з'єднання на локальному компютері (OS Windows XP)

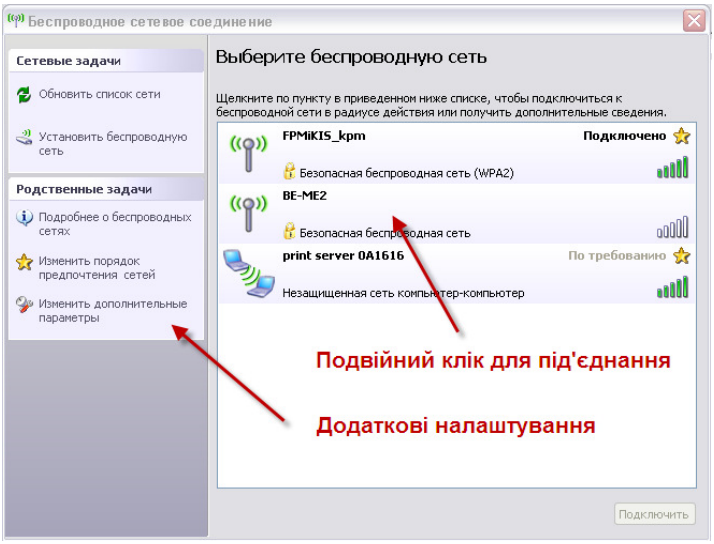
Для того щоб переглянути доступні безпровідні мережі і під'єднатися до Wi-Fi мережі на локальному комп'ютері з операційною системою Windows XP перейдіть в меню „Панель управления" -> „Сетевые подключения" -> „Беспроводное сетевое соединение" і далі натисніть кнопку „Беспроводные сети" або просто клікніть в треї на іконці безпровідних мереж і отримаєте ті самі налаштування:



Якщо у вас комп’ютер автоматично підключається, тоді вікно буде нагадувати наведене вище, де стан буде вказаний як “Подключено”.

Для переходу до списку безпровідних мереж натисніть „Беспроводные сети”

Список безпровідних мереж:

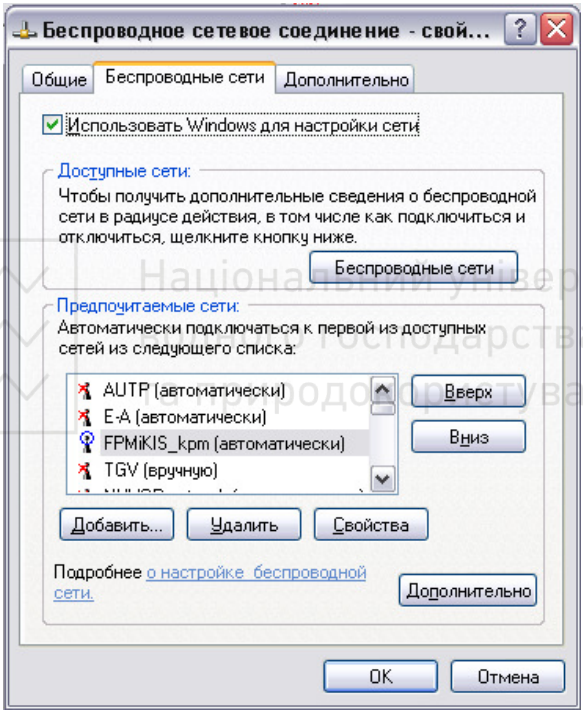


Національний університет
та природокористування

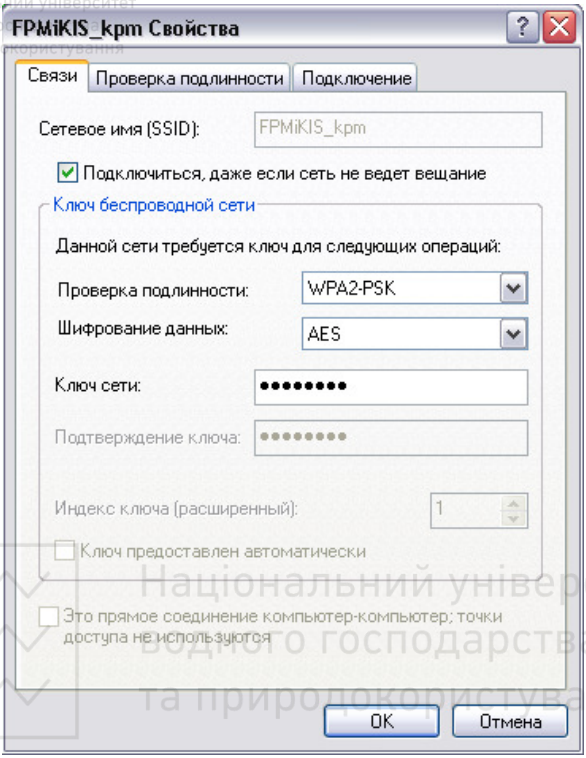
Для під'єднання просто клікніть два рази на потрібній мережі.

Підключення до невидимої мережі

Щоб налаштувати підключення до невидимої мережі (тієї яка не надсилає широкомовне повідомлення з власним SSID ідентифікатором) потрібно перейти в пункт „Изменить дополнительные параметры" і перейти в закладку „Беспроводные сети".:



Далі вибираємо мережу, що нас цікавить і здійснюємо налаштування:



Тобто вказали, що потрібно підключатися навіть тоді, коли мережа не передає сигнал (галочка зверху). Також при необхідності задаються методі аутентифікації.

2.3. Програма роботи

1. Під’єднати точку доступу до локального комп’ютера.
2. Налаштувати TCP/IP властивості для під’єднання до точки доступу, записати попередні налаштування.
3. Перевірити зв’язок з точкою доступу. Для цього скористайтеся утилітою ping.
4. Повернути налаштування точки доступу до заводських у разі необхідності.
5. Ознайомитись з заводськими налаштуваннями.
6. Змінити назву точки доступу (SSID) на довільну.
7. Під’єднатися до точки доступу довільним пристроєм.

8. Протестувати з’єднання (утиліти ping, netstat ітд).
9. Змінити параметри аутентифікації (WPA-PSK, WPA2-PSK, ітд), почергово перевіряючи та доналаштовуючи з’єднання на безпровідному клієнті.
10. Знайти під’єднаний пристрій в меню статистики на точці доступу. Зафіксувати його MAC адресу.
11. Протестувати роботу фільтру MAC адрес. Для цього спочатку заблокуйте доступ вашого пристрою вказавши його MAC адресу, а потім дозвольте підключення тільки вашому пристрою.
12. Приховати точку доступу (SSID broadcasting disabled).
13. Перевірити прихованість безпровідної мережі на безпровідному клієнті.
14. Під’єднатися до прихованої мережі.
15. Протестувати з’єднання.
16. Завантажити збережені параметри налаштувань точки доступу (load settings from local hard drive). Місце знаходження файлу зі збереженими параметрами уточніть у викладача
17. Від’єднати точку доступу від локального комп’ютера. Налаштування TCP/IP локального комп’ютера повернути до початкових.
18. Перевірити справність роботи локальної мережі.
19. Внести отримані результати до звіту.

2.4. Контрольні запитання

1. Що таке Wi-Fi?
2. Які стандарти Wi-Fi ви знаєте?
3. Яка максимальна швидкість Wi-Fi?
4. Яке обладнання використовується для безпровідникового доступу?
5. Де і як здійснюється налаштування безпровідникової точки доступу?
6. Які налаштування потрібно задати для підключення на локальному комп’ютері?
7. Що таке SSID?
8. Які режими функціонування безпровідної точки доступу бувають?
9. Які стандарти шифрування ви знаєте?

Національний університет
водного господарства
та природокористування

10. Як приховати точку доступу?
11. Що таке DHCP? Для чого він використовується?
12. Як дозволити доступ до точки доступу лише певним комп'ютерам?
13. Що таке прошивка?
14. Як відновити налаштування роутера?
15. Як повернути налаштування роутера в початковий стан?

Національний університет
водного господарства
та природокористування

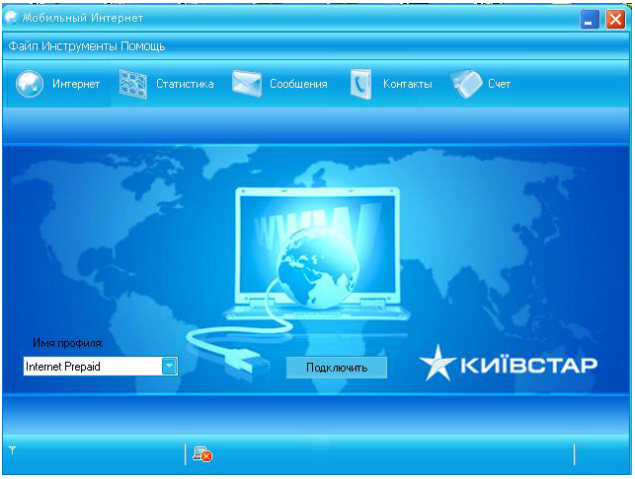
Робота 3. Підключення до глобальної мережі за допомогою телефону/модема

3.1. Мета роботи

Отримати навики у створенні та налаштуванні підключення до глобальної мережі інтернет за допомогою 3G модему/телефону.

3.2. Теоретичні відомості

Вже минули часи Dial-up модемів, з швидкістю передачі даних 64 Кбіт/сек. На зміну їм прийшли мобільні телефони/модеми з технологіями передачі даних GPRS, EDGE, HSDPA, HSUPA та інших. Проте принцип підключення залишився той самий – пристрій стає присутнім в системі як модем і всі комунікації з зовнішнім світом відбуваються через нього. Разом з тим з'явилися також допоміжні утиліти, які автоматизують створення Інтернет-з'єднання і контролюють трафік. Ці утиліти отримали назву **дашбордів**. Вони найчастіше є вже встановлені на пристроях (3G модемах) і при під'єднанні до комп'ютера автоматично встановлюють необхідні драйвери і запускають себе. Ось так виглядає типовий дашборд від компанії „Київстар", що йде в комплекті з 3G модемами ZTE MF100:



Дана програма дозволить з'єднуватись з мережею Інтернет і вам не потрібно буде пам’ятати номери телефонів дозвону, логіни та паролі; також ви зможете читати та відправляти смс повідомлення, здійснювати голосові дзвінки (якщо це підтримує ваш пристрій), контролювати стан рахунку, к-ть прийнятих та переданих даних та виконувати інші корисні дії.

Проте, іноді трапляються непередбачувані випадки і робота дашборда може бути порушена (внаслідок дії вірусів, зміни налаштувань з боку оператора і т.д.), тому параметри ручного налаштування потрібно знати і вміти робити.

Стандарти мобільного зв’язку

0G - радіотелефони

1G

Перше покоління мобільного зв'язку (1G) виникло в 70-х роках. Всі перші системи стільникового зв'язку були аналоговими. Вони призначалися тільки для передачі голосу. Стандарти AMPS, NMT, TACS - найбільш відомі представники 1G. Ці стандарти безперервно модернізувалися, збагачувалися новими можливостями і, таким чином, служать до цього дня.

2G

Друге покоління (2G) пішло по шляху прогресу, забезпечивши абоненту передачу і прийом голосу, даних і факсових повідомлень. В даний час, системи другого покоління все ще розвиваються з постійно зростаючими швидкостями передачі даних, за допомогою технологій

типу HSCSD і GPRS. Системи другого покоління включають GSM, DAMPS (IS-136), cdmaOne (IS-95) та PDC. DAMPS / PDC структурно були накладені на існуючі системи першого покоління і обслуговували паралельно з ними. GSM/IS-95, з іншого боку, засновані на повністю новій концепції, і набули найбільшого поширення в усьому світі.

Загальний сервіс пакетної радіопередачі (англ**. General Packet Radio Service, GPRS**) — стандарт, який використовує не зайняту голосовим зв'язком смугу частот для передачі інформації. Використовується в мобільних пристроях для передачі MMS, WAP-серфінгу та повноцінного з'єднання з Інтернетом. Розрізняють так звані класи GPRS — рівень підтримки стандарту конкретним приладом. Існують класи від першого до дванадцятого — чим вищий клас, тим більшу швидкість передачі даних може, теоретично, забезпечити телефон. висока середня швидкість передачі даних — 20-40 Кбіт/сек.;

EDGE (англ. Enhanced Data Rates for GSM Evolution) — сучасна технологія, що забезпечує передачу великих обсягів інформації в мережі мобільного зв'язку. Технологія EDGE підтримує у середньому в три рази вищу швидкість передачі даних, ніж GPRS, крім того, забезпечується більш ефективне використання частотних ресурсів і поліпшення покриття мережі в порівнянні зі звичайною мережею GSM. Максимально досяжна (у теорії) швидкість передачі інформації в мережі EDGE — 474,6 кбіт/с.

CDMA2000 1xRTT (IS-2000) - широкий діапазон швидкостей передачі інформації від 60 до 100 kbps з можливістю гнучкої зміни ширини спектра випромінюваних сигналів;

3G

В світі існує два стандарти 3G: UMTS (або W-CDMA) і CDMA2000. UMTS розповсюджений в основному в Європі, CDMA2000 — в Азії і США.

Універсальна Мобільна Телекомунікаційна Система (англ. Universal Mobile Telecommunications System, UMTS) — є однією з технологій мобільного зв'язку третього покоління (3G). Походить від існуючого GSM стандарту, але надає можливість високошвидкісної передачі даних з використанням радіо доступу широкосмугової кодової модуляції WCDMA, використовуючи протоколи HSDPA та HSUPA.

W-CDMA (англ. Wideband Code Division Multiple Access) — широкосмуговий множинний доступ із кодовим розподілом каналів, який використовує дві широкі смуги радіочастот по 5 МГц (тому й називається — широкий CDMA).

Термін W-CDMA також використовується для опису самостійного стандарту стільникової мережі, що проектувався як надбудова над GSM та працює в діапазоні 1900—2100 МГц.

HSDPA (англ. High-Speed Downlink Packet Access — високошвидкісний пакетний доступ у напрямку «вниз») — протокол високошвидкісного приймання пакетних даних стандарту мобільного зв'язку 3-го покоління. Max Speed theoretical 14 Mbitps

High Speed Uplink Packet Access, **HSUPA** — технологія високошвидкісної пакетної передачі даних аналогічно HSDPA, за напрямком «вверх», представляє собою стандарт мобільного звязку, що дозволяє прискорити передачу даних від W-CDMA пристроїв кінцевого користувача до базової станції за рахунок застосування більш досконалих методів модуляції. Теоретично стандарт HSUPA розрахований на максимальну швидкість передачі даних до 5,8 Мбит/с

EV-DO (Evolution Data Only або Evolution-Data Optimized) — це технологія мереж мобільного зв'язку третього покоління 3G, стандартизована 3GPP2 в межах розвитку CDMA2000 1x та забезпечення високошвидкісну передачу даних зі швидкістю до 2.4 Мб/с (rev0), до 3,1 Мб/с (revA) та ще більше в подальших модіфікаціях.

В Україні, станом на 2011 рік, послуги EV-DO надають МТС Україна (450 мГц, rev0), Інтертелеком (800 мГц, revA), CDMA UKRAINE (800 мГц, revA) PEOPLEnet (800 мГц, revA).

3.3. Програма роботи

1. Підключити модем, перевірити запуск дашборда.
2. Ознайомитись з налаштуваннями, перевірити параметри підключення.
3. Здійснити підключення і перевірити швидкість за допомогою сайту www.speedtest.net.

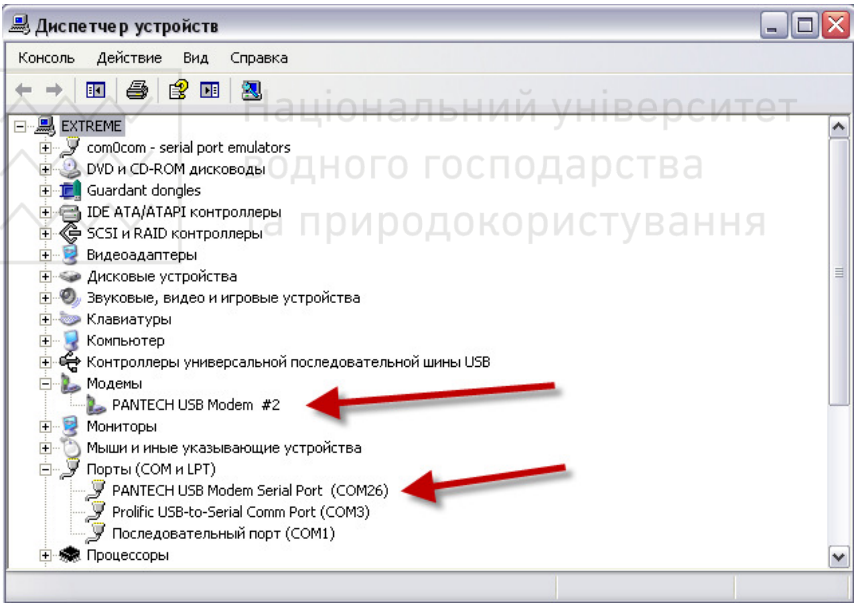
Національний університет
та природокористування

3.4. Порядок виконання роботи

1.Підключіть модем, автоматично повинен запуститися дашборд.

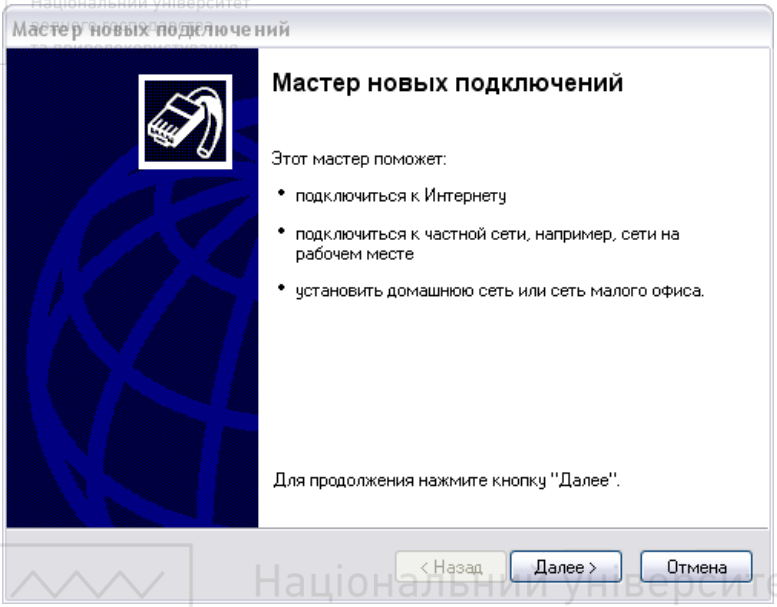
Після з'єднання телефону/модему з комп'ютером операційна система повинна знайти новий пристрій і встановити його як модем. Для цього етапу можуть знадобитися драйвери (програмне забезпечення) з диску, який може надаватися у комплекті до телефонного апарату, або ж ви можете завантажити їх з web-сайту виробника вашого телефону.

2. Ознайомтесь з налаштуваннями, перевірте параметри підключення.
Перевіряємо чи присутній модем в диспетчері пристроїв:

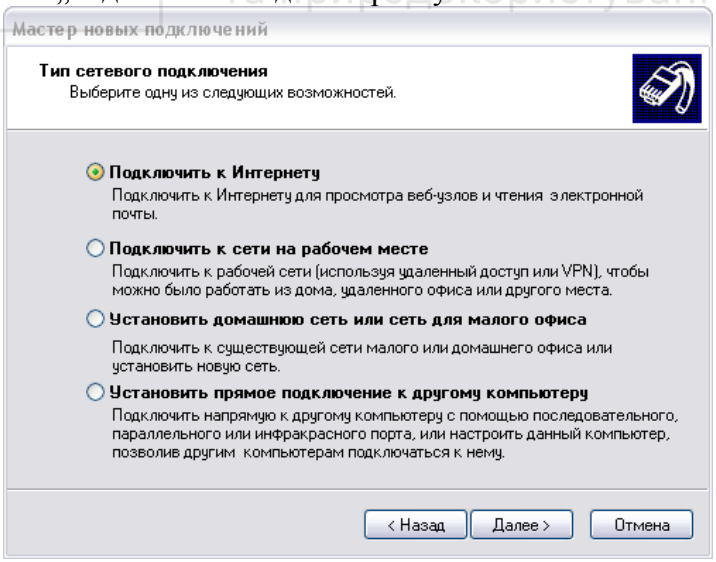


Створюємо нове з'єднання на Windows 2000, XP:

Виберіть на комп'ютері: „Пуск – Програми – Стандартні – Майстер нових підключень":

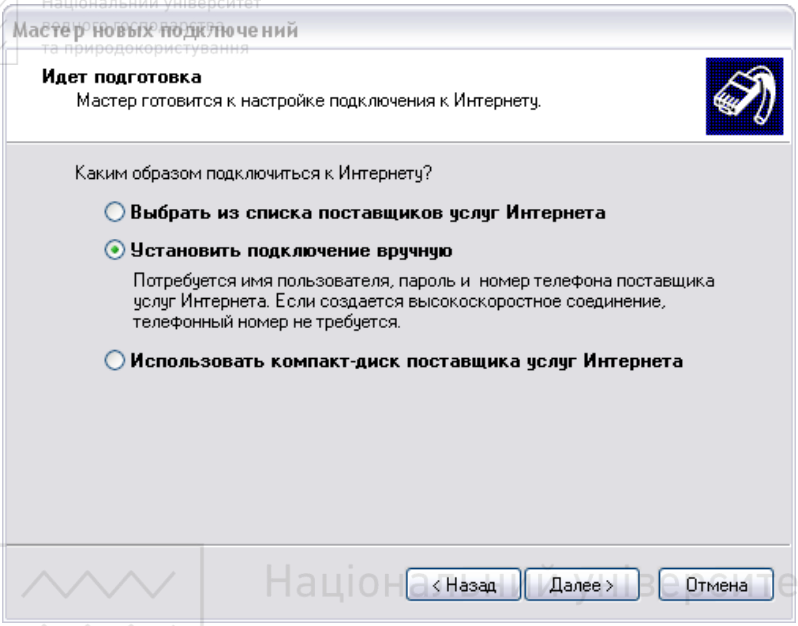


Після натиснення кнопки „Далі” виберіть „Підключитись до Інтернету”:



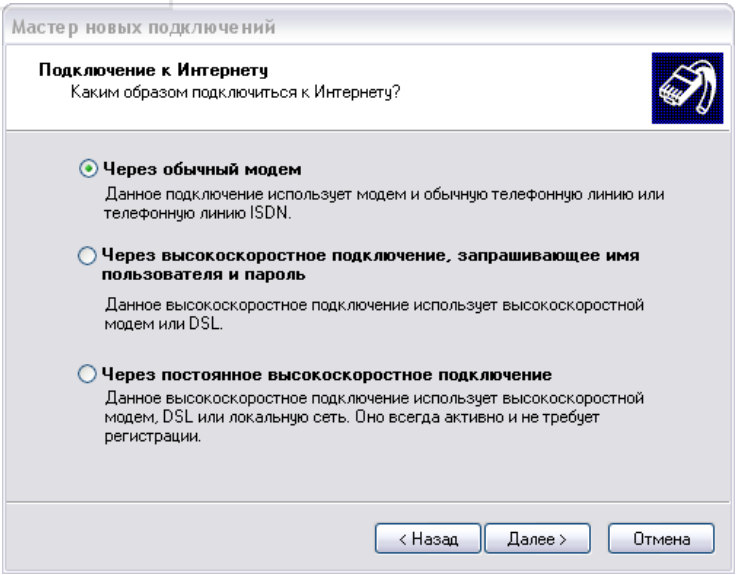
Далі – „Встановити з’єднання вручну”:

Національний університет
водного господарства
та природокористування



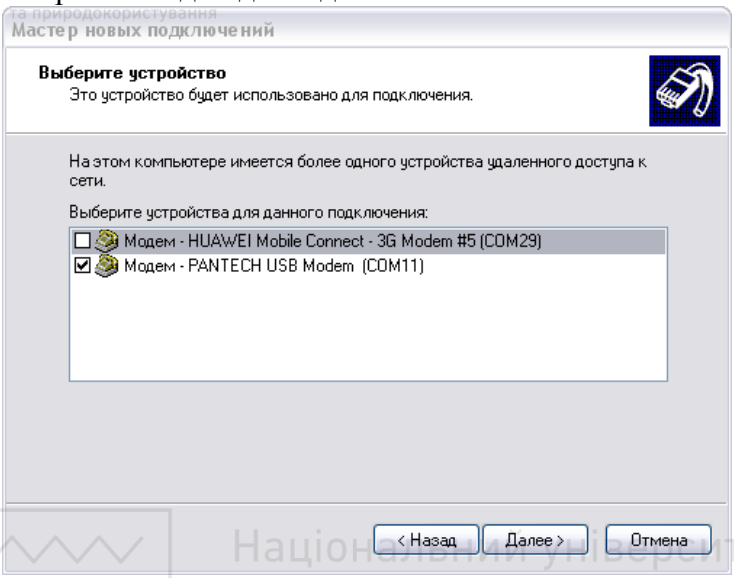
Національний університет
водного господарства
та природокористування

За допомогою звичайного модему:



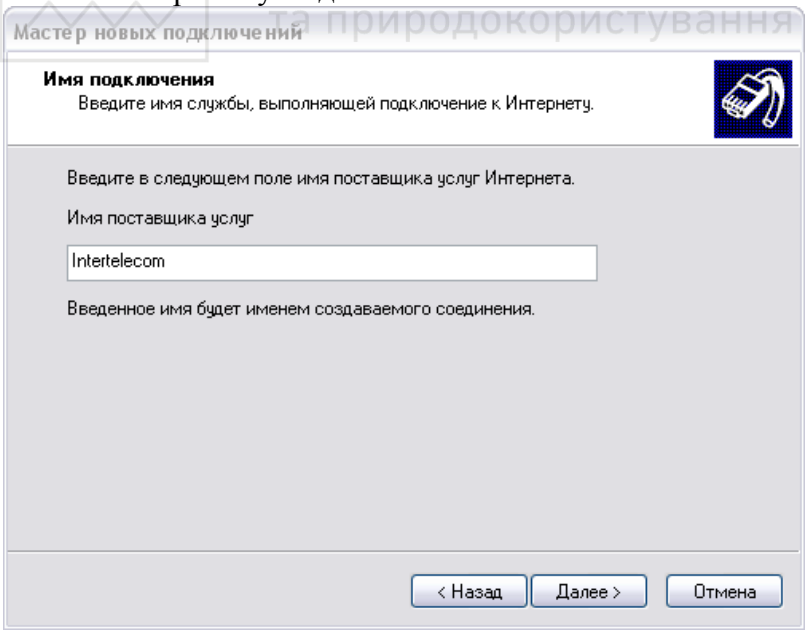
Національний університет
та природокористування

Далі вибираємо модем для підключення:

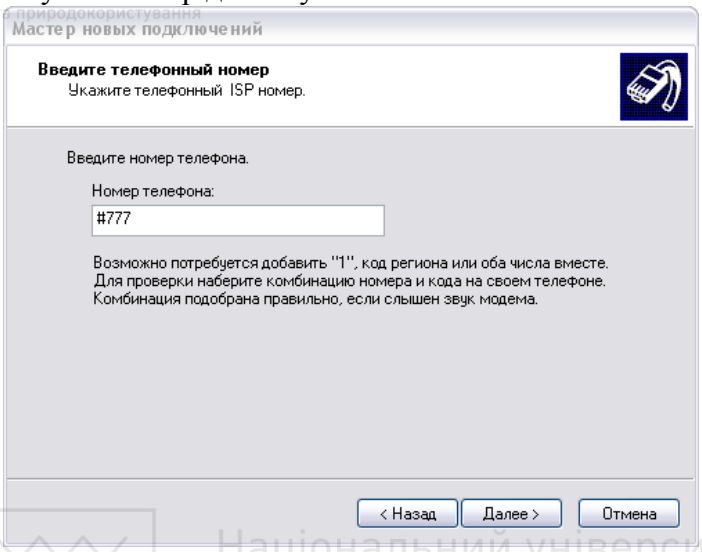


Національний університет
водного господарства
та природокористування

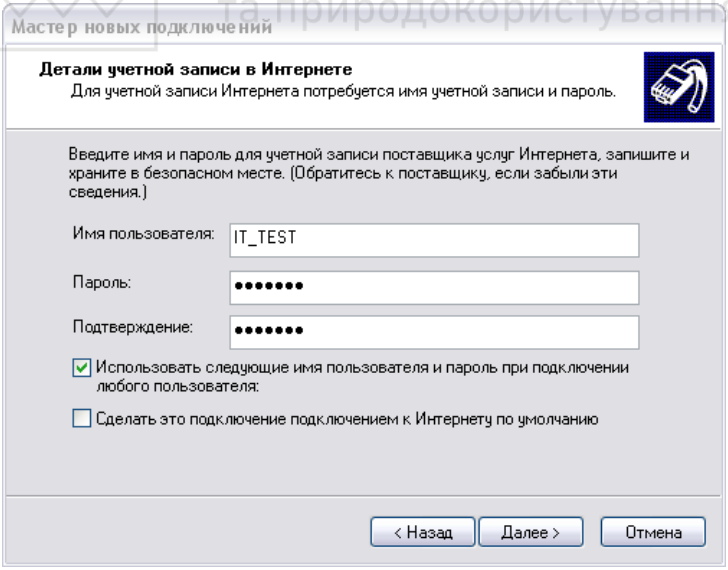
Даємо ім’я створеному з’єднанню:



Вказуємо номер дозвону:



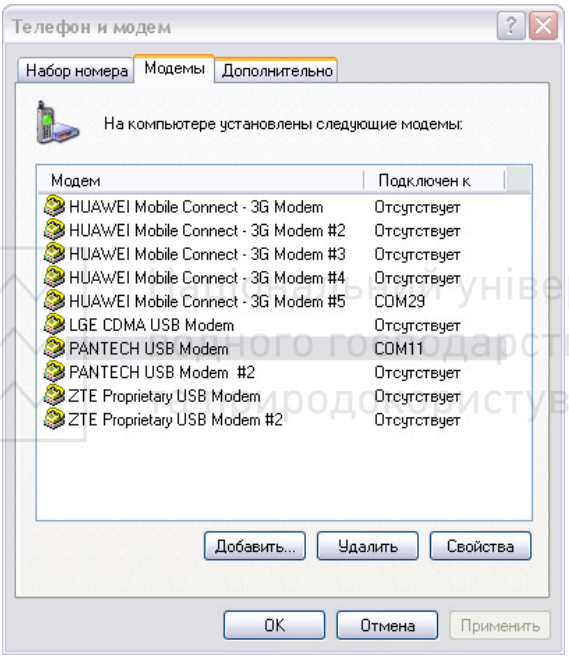
Задаємо деталі облікового запису для авторизації:



Отже, тепер є налаштоване мережне підключення, залишилось тільки внести деякі корективи до налаштувань модему, а саме прописати рядок ініціалізації.

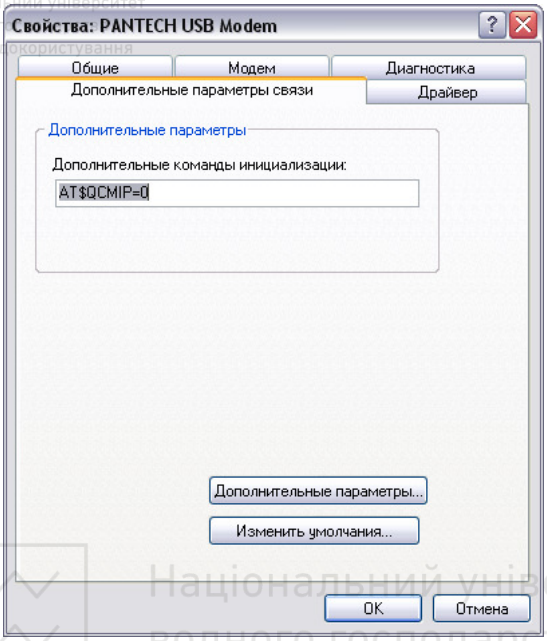
Налаштування параметрів ініціалізації модему:

- Виберіть „Пуск – Панель управління – Телефон і модем” – закладка „Модеми „ оберіть свій модем і натисніть „Властивості”



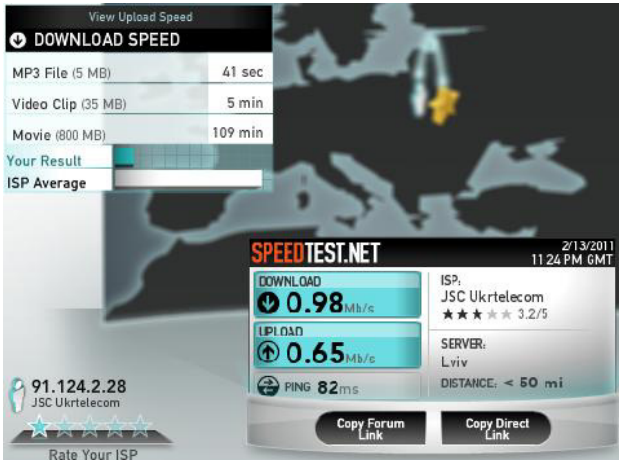
Вибираємо закладку „Додаткові параметри зв’язку – Додатковий рядок ініціалізації”

Національний університет
водного господарства
та природокористування



Національний університет
водного господарства
та природокористування

2. Для тестування швидкості використайте сайт www.speedtest.net**:**



Національний університет
та природокористування

3.5. Контрольні запитання

1. Які пристрої можна використати для під’єднання до мережі Інтернет?
2. Які налаштування потрібно здійснити для ручного підключення до мережі Інтернет?
3. Що таке номер дозвону?
4. Що таке рядок ініціалізації?
5. Які модеми ви знаєте?
6. Які технології передачі даних ви знаєте?
7. Які покоління мобільного зв’язку ви знаєте?
8. Які оператори мобільного зв’язку ви знаєте?
9. Які тарифи на користування мобільним Інтернетом?
10. Що таке дашборд?

Національний університет
водного господарства
та природокористування

Національний університет водного господарства та природокористування

Робота 4. Служби термінального доступу

4.1. Мета роботи

Навчитися розгорнути сервер терміналів на базі ОС Windows 2003. Вивчити можливості служб термінального доступу.

4.2. Теоретичні відомості

Служби терміналів забезпечують віддалений доступ до робочого столу Microsoft ® Windows ® за допомогою програмного забезпечення «тонкий клієнт», що дозволяє комп'ютеру клієнта працювати в якості емулятора терміналу. Служби терміналів передають клієнтові тільки користувацький інтерфейс програми. Потім клієнт повертає натиснення клавіш клавіатури і кнопок миші для виконання на сервері. При вході кожен клієнт бачить тільки свої сеанси, які керуються операційною системою сервера і є незалежними від сеансів інших користувачів. Для підключення до комп'ютера через служби терміналів, слід використовувати програму «Підключення до віддаленого робочого столу».

З використанням сервера терміналів одна точка установки надає декільком користувачам доступ до робочого столу комп'ютера, на якому виконується одна з операційних систем сімейства Microsoft Windows Server ™ 2003, де вони можуть запускати програми, зберігати файли і використовувати мережеві ресурси.

Сервер терміналів

У сімействі операційних систем Microsoft ® Windows Server ™ 2003 сервер терміналів дає користувачам комп'ютерів-клієнтів мережі доступ до програм Windows, встановленим на серверах терміналів. За допомогою сервера терміналів можна в одній точці (комп'ютері) встановити програму, що дозволить безлічі віддалених користувачів запускати програми на робочому столі сімейства операційних систем Windows Server 2003, зберігати файли, використовувати мережеві ресурси, як на власних комп'ютерах.

На комп'ютерах з операційними системами Microsoft ® Windows ® XP або Windows Server 2003 клієнт сервера терміналів («Підключення до віддаленого робочого столу») вже встановлений.

Програма «Підключення до віддаленого робочого столу» може бути також встановлена на іншу 32-розрядну операційну систему

Національний університет
господарства
та природокористування
Windows.

Переваги служб терміналів

Істотне збільшення швидкодії мережевих додатків. Служби терміналів дозволяють багаторазово прискорити роботу мережевих додатків (програм), одночасно знизивши навантаження на локальну мережу. Завдяки емуляції "клієнт-серверної" схеми роботи службами терміналів, обробка великих обсягів даних здійснюється безпосередньо на сервері, а клієнтському ПК по мережі передається тільки результат обчислень.

Наприклад сервер з процесором Pentium 4 або Athlon з тактовою частотою ~ 2800-3000 MHz і оперативною пам'яттю від 512 MB, здатний забезпечити комфортну роботу в новій системі з 1С: Бухгалтерією до 10-ти мережевих користувачів одночасно, як якби всі вони працювали безпосередньо на сервері! Зі збільшенням обсягу оперативної яті до 1GB одночасно працюючих користувачів може бути вже більше 15-ти.

Зниження витрат на модернізацію старого парку персональних комп'ютерів. Служби терміналів дозволяють підключати, без додаткових витрат на модернізацію апаратного забезпечення, новий інтерфейс Microsoft ® Windows ® XP Professional на старі ПК, продуктивності яких вистачало тільки для ранніх версій Windows (95,98, NT4, 2000).

Підвищена надійність зберігання даних. Служби терміналів дозволяють централізувати зберігання даних. Завдяки фізичному розташуванню всіх критичних даних (документи, бази даних бухгалтерії та пошти, прикладні програми) на жорстких дисках сервера знижуються витрати на підтримку відмовостійкості систем. А у випадку використання в якості носіїв (зберігачів) інформації дзеркальних масивів жорстких дисків (RAID-масивів), майже повністю відпадає необхідність періодичного архівування даних, при цьому істотно підвищується продуктивність дискової підсистеми.

Можливість використання повного набору переваг даного обладнання. Служби терміналів розширюють модель розподілених обчислень, дозволяючи комп'ютерам одночасно виконувати операції в якості "тонкого клієнта" і повноцінні операції. Комп'ютери можуть продовжувати працювати в існуючій мережі і одночасно з цим виконувати функції «тонких клієнтів», емулюючи робочий стіл Windows XP Professional.

Централізоване розгортання програм. При використанні сервера

терміналів виконання всіх програм, обробка та зберігання даних відбуваються на сервері. Таким чином відбувається централізація розгортання програм. Сервер терміналів забезпечує всім клієнтам доступ до однакових версій програм. Замість установки на кожний комп'ютер всередині організації програмне забезпечення встановлюється один раз на сервер, що зменшує вартість його встановлення.

Висока надійність. Вдосконалений механізм попередження аварійних ситуацій на сервері(збій живлення, критичні помилки додатків, збої в локальній мережі) дозволяє продовжити перервану роботу з того місця, після якого відбувся збій, не втративши при цьому зробленого до цього

Протокол віддаленого робочого стола

RDP (англ. Remote Desktop Protocol, протокол віддаленого робочого стола) — протокол прикладного рівня, що використовується для забезпечення віддаленої роботи користувача із сервером, на якому запущений сервіс термінальних з'єднань. Клієнти існують практично для всіх версій Windows (включаючи Windows CE та Mobile), Linux, FreeBSD, Mac OS X. За замовчанням використовується порт TCP 3389. Офіційна назва Майкрософт для клієнтського ПЗ — Remote Desktop Connection або Terminal Services Client (TSC), зокрема, клієнт у Windows XP/2003/Vista називається mstsc.exe.

Особливості:

- Підтримка 32-бітного кольору (в додаток до 8-, 15-, 16- і 24-бітному в попередніх версіях)
- 128-бітове кодування, використовуючи алгоритм кодування RC4 (значення безпеки за замовчанням; старі клієнти можуть використовувати слабкіше кодування).
- Звук із віддаленого ПК переадресовується і відтворюється на локальному комп'ютері.
- Дозволяє під'єднувати локальні ресурси до віддаленої машині (мапити їх)
- Дозволяє використовувати локальний або мережевий принтери на віддаленому ПК
- Дозволяє додаткам, що виконуються в межах поточного сеансу звертатися до локальних послідовних і

паралельних портів.

- Можна обмінюватися інформацією через буфер обміну.

У Windows Server 2008 та Windows Vista/Seven використовується

Національний університет
та природокористування
нова версія протокола, RDP 6.

4.3. Програма роботи

1. Встановити та налаштувати термінальний сервер.
2. Провести налаштування термінальних користувачів.
3. Здійснити тестування термінального сервера.

4.4. Порядок виконання роботи

Налаштування термінального серверу

Служби терміналів можуть працювати в двох режимах:

1) Remote Desktop for Administration (раніше відомий як Terminal Services in Remote Administration mode)

Цей режим призначений для надання операторам і адміністраторам можливості віддаленого доступу до серверів і контролерів домену. Сервер, налаштований для віддаленого адміністрування не вимагає додаткового ліцензування, в цьому режимі можливо тільки два одночасних підключення.

2) Terminal Server mode

Цей режим не має обмежень по кількості підключень, але вимагає додаткового ліцензування. В неліцензованому стані сервер термінального доступу пропрацює 120 днів (в Windows 2000 - 90 днів).

В першу чергу потрібно додати роль Terminal Server для нашого сервера. Для цього зайдіть в меню “Start”->”Manage Your Server”->”Add or remove a role” і додайте роль “Terminal server”.

Під час процесу встановлення система може попросити інсталяційний диск. Також після завершення встановлення буде перезавантажено комп'ютер.

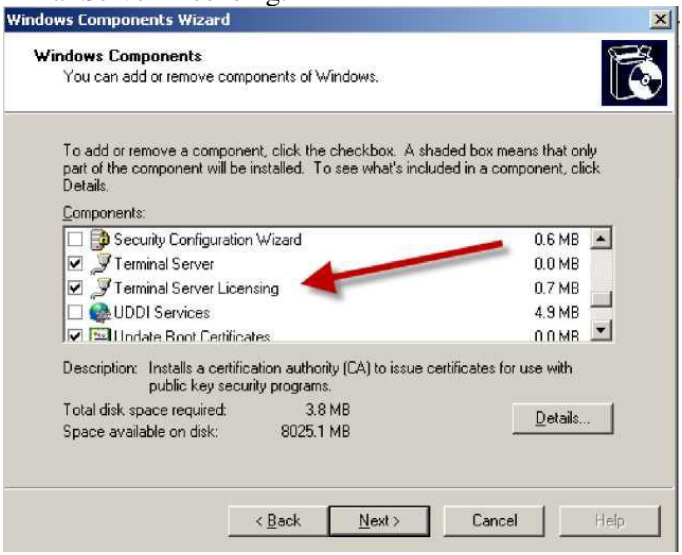
У разі успішного встановлення, після перезавантаження комп'ютера з'явиться наступне вікно:

Тепер можна користуватися термінальним сервером.

Але як було сказано вище, він буде працювати 120 днів. Тому необхідно провести ліцензування. Цьому присвячені наступні кроки.

Встановлення служби ліцензування терміналів

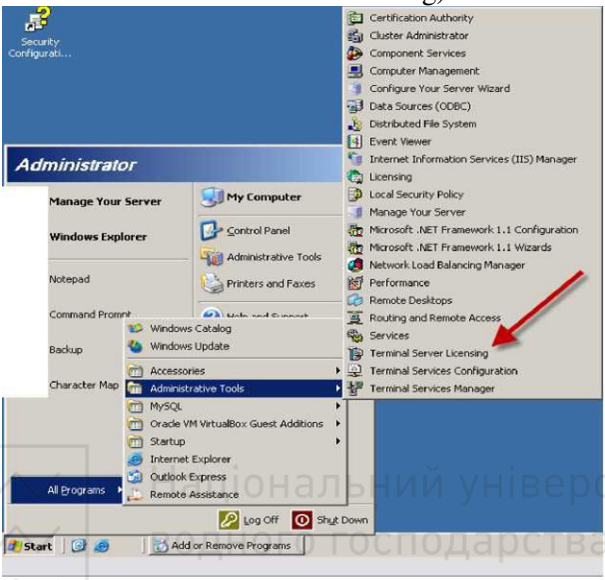
Для встановлення потрібно перейти „Control Panel”-> “Add or Remove Programs” -> “Add/Remove Windows Components” і вибрати Terminal Server Licensing:



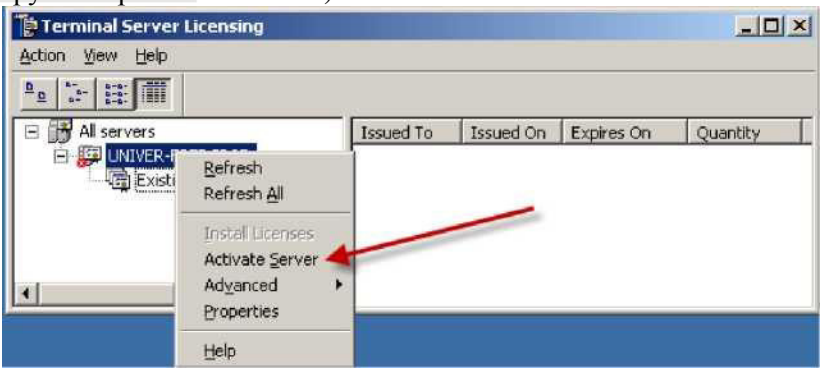
В ході встановлення параметри виберіть за замовчуванням.

Активація термінального сервера

Запустіть Terminal Server Licensing (Start -> Control Panel -> Administrative Tools-> Terminal Server Licensing) :



Виберіть активацію сервера (клік правою кнопкою по нашому серверу і вибір Activate Server):



Запуститься Terminal Server License Server Activation Wizard. Ознайомтеся з описом та натисніть Next.

Наступним кроком вибираємо автоматичний метод активації (Automatic connection). Для цього методу потрібний доступ до мережі Інтернет.

Національний університет водного господарства та природокористування

У випадку методу Web connection потрібно вручну перейти на сайт https://activate.microsoft.com/ для отримання license server ID, а в автоматичному режимі візард зробить це за вас ©.

Також існує варіант активації по телефону. У цьому випадку користувач повинен зателефонувати і в телефонному режимі отримати необхідні параметри.

Отже, вибравши автоматичний метод та заповнивши основну інформацію про компанію (Last name, First Name, Company, Country), чекаємо на з'єднання з активаційним сервером Майкрософт та отриманням активації термінального сервера.

У разі успіху з'явиться таке повідомлення:

Your license server has been successfully activated.

To install client licenses now, click Next.

To postpone client license installation, clear the check box below, and then click Finish.

Для встановлення client access licenses (CALs), наступна частина, потрібно перевірити, щоб галочка Start Terminal Server Client Licensing Wizard була встановлена і натиснути Next.

Тепер переходимо до процесу встановлення ліцензій для терміналів.

Встановлення ліцензій для терміналів (Terminal Server CAL Installation Wizard)

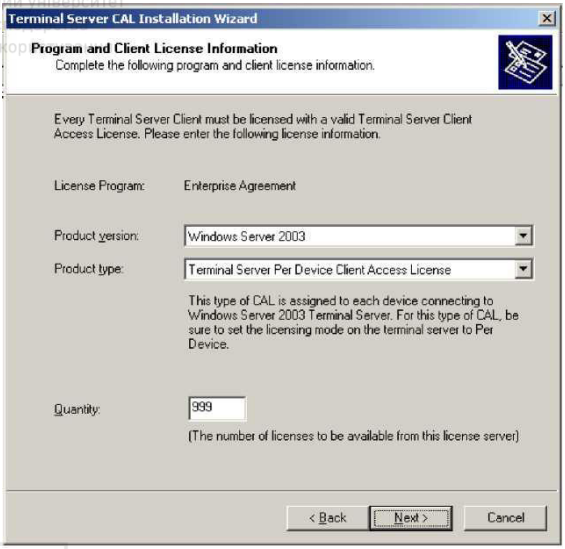
Ознайомтесь з вітанням майстра установки клієнтських ліцензій та натисніть Next.

В полі License Program потрібно вибрати Enterprise

Agreement. Це вид ліцензії, в нашому випадку це ліцензія Enterprise:

В наступному вікні система запитає Agreement Number. Введіть 4526017.

Далі потрібно вибрати версію продукту і тип ліцензування:



У разі успішного завершення отримаєте повідомлення

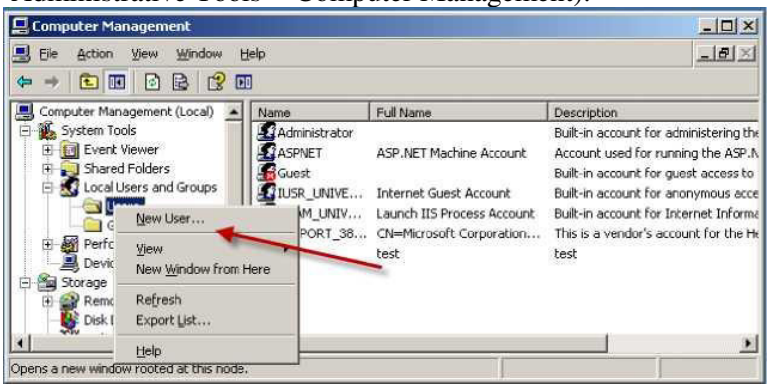
The new client license key pack has been successfully installed.

На цьому основні налаштування термінального серверу закінчуються. Можна тестувати роботу.

Налаштування термінальних користувачів

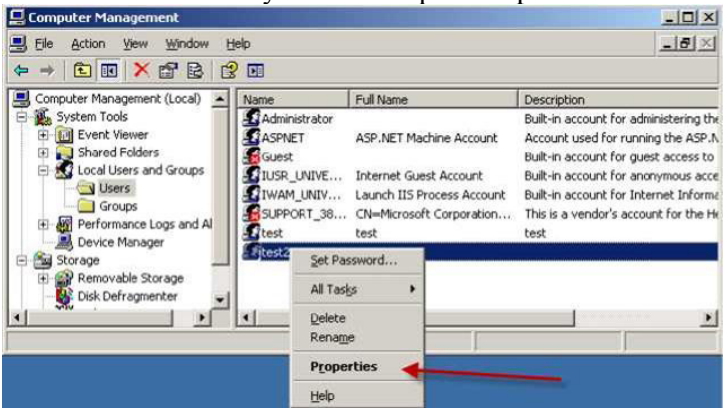
За замовчуванням лише адміністратор (або група адміністраторів) має змогу користуватися службою терміналів. Тому необхідно створити нового користувача і дати йому необхідні права або додати вже існуючого користувача до групи Remote Desktop Users.

Створіть нового користувача через оснастку Computer Management (Start->Administrative Tools-> Computer Management):

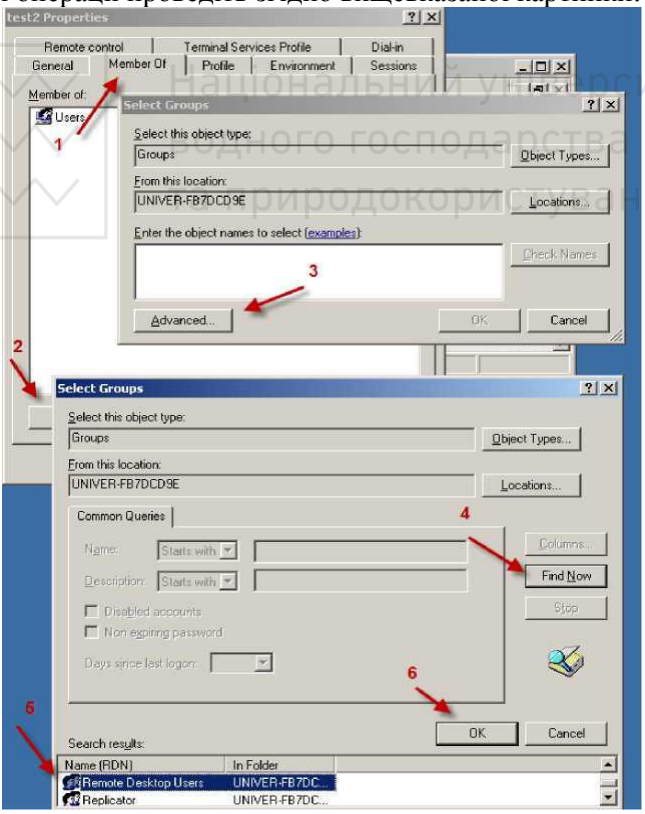


Додайте новоствореного користувача до групи Remote Desktop

Users. Для цього спочатку виберіть користувача, натисніть праву кнопку миші і в контекстному меню виберіть Properties:

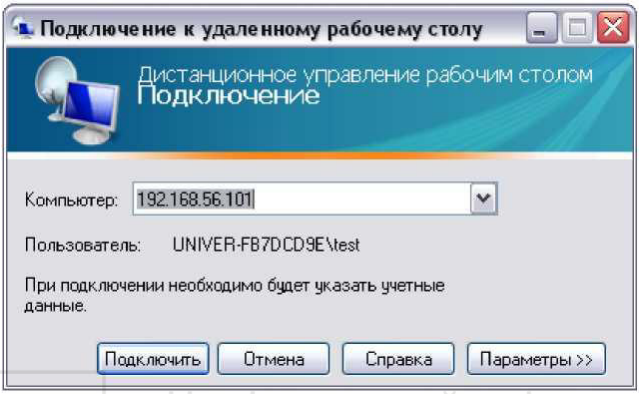


Наступні операції проведіть згідно вищевказаної картинки:



Тестування термінального з'єднання

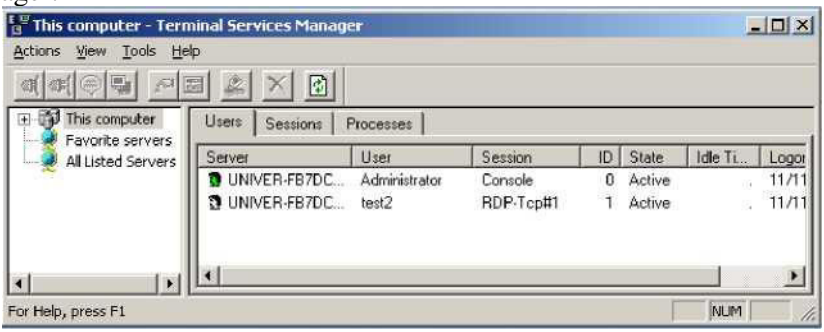
Запустіть на іншій машині (наприклад на хост-машині) утиліту «Підключення до віддаленого робочого столу»: Пуск->Все программы- >Стандартные->Подключение к удаленному рабочему столу:



Введіть адресу термінального серверу та авторизуйтеся в системі використовуючи логін на пароль новоствореного користувача. Також перевірте з'єднання використовуючи обліковий запис адміністратора. Знайдіть відмінності між сеансами адміністратора і новоствореного користувача.

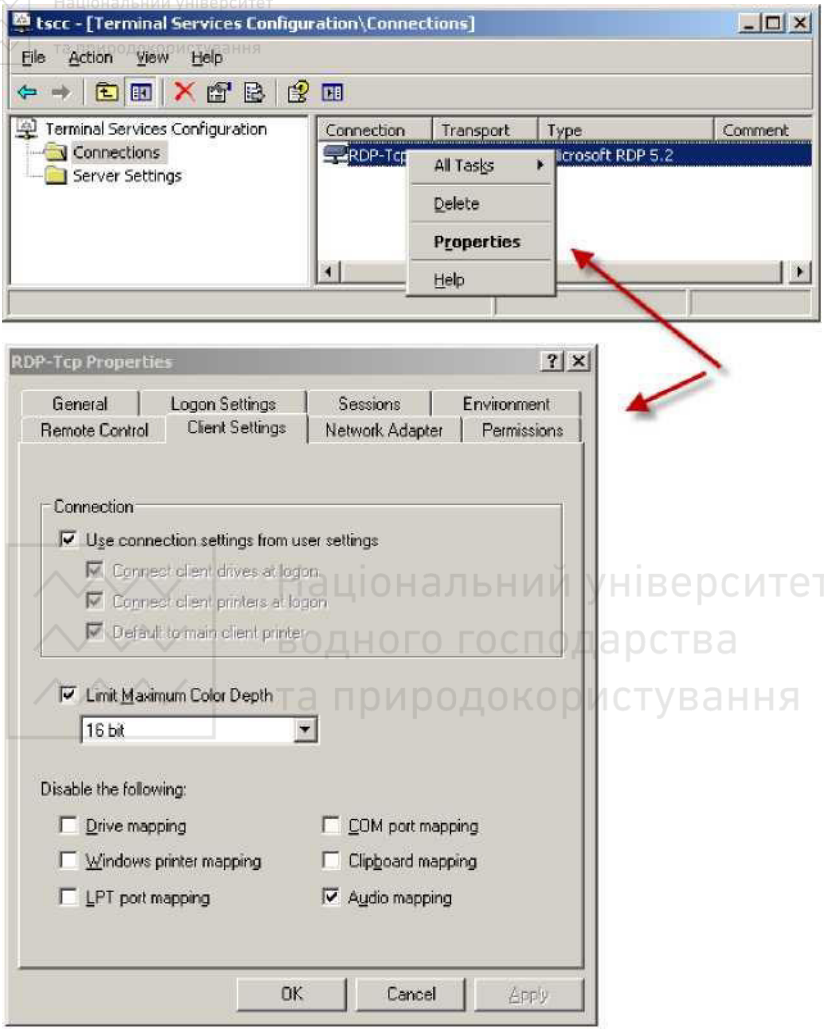
Керування термінальним сервером

Основні засоби керування знаходяться в оснастці Terminal Services Manager:



Та в оснастці Terminal Services Configuration. В ній можна вибрати налаштування для протоколу RDP, а саме вказати пристрої потрібно мапити (прокидати) на термінальну машину, програму початкового завантаження, ступінь шифрування даних для RDP протоколу ітд.

Ознайомтеся з можливими налаштуваннями:



Занесіть результати до звіту.

4.5. Контрольні запитання

1. Що таке тонкий клієнт?
2. Що таке термінальна служба?
3. Що таке термінальний сервер?
4. Які переваги служб терміналів?

Національний університет
водного господарства
та природокористування

5. Які обмеження при використанні неактивованого сервера терміналів?
6. Який протокол використовується на прикладному рівні для служб терміналів?
7. Як приєднатися до термінального сервера?
8. Які налаштування термінального сервера ви знаєте?
9. Яке призначення компоненти Terminal Server Licensing?
10. Які права доступу повинен мати користувач щоб користуватися термінальним доступом?

Національний університет
водного господарства
та природокористування

Національний університет водного господарства та природокористування

Робота 5. Служба каталогів Active Directory. Групові політики

5.1. Мета роботи

Навчитися розгортати службу каталогів Active Directory, створювати власну консоль керування груповими політиками.

5.2. Теоретичні відомості

Служба каталогів Active Directory

Active Directory - це універсальне розподілене сховище даних, доступ до об'єктів якого можливий із будь-якої точки мережі. Це ієрархічна база даних, яка включає найнеобхідніші об'єкти, служби, принтери, комп'ютери, програмне забезпечення.

Основою всієї структури Active Directory є DIB (Directory Information Base), яка наповнена відомостями про об'єкти, що зберігаються в каталогах.

Отримання доступу до DIB, а також до користувачів і їх комп'ютерів відбувається за ієрархічною структуро.

Active Directory дозволяє адміністраторам використовувати групові політики (GPO) для забезпечення детального налаштування користувацького робочого середовища, розгортати ПЗ на великій кількості комп'ютерів (через групові політики або за допомогою Microsoft Systems Management Server 2003 (або System Center Configuration Manager)), встановлювати оновлення ОС, прикладного та серверного ПЗ на всіх комп'ютерах в мережі ітд ітп.

Active Directory (AD) має ієрархічну структуру, що складається з об'єктів. Об'єкти поділяються на три основні категорії:

- ресурси (наприклад, принтери),
- служби (наприклад, електронна пошта)
- люди (облікові записи користувачів і груп користувачів).

Active Directory надає інформацію про об'єкти, дозволяє організовувати об'єкти, керувати доступом до них, а також встановлює правила безпеки.

Кожен об'єкт представляє окрему сутність - користувача, комп'ютер, принтер, програму або спільну мережеву папку - і його атрибути. Об'єкти можуть також бути контейнерами для інших об'єктів. Об'єкт унікально ідентифікується своїм ім'ям і має набір атрибутів - характеристик і даних, які об'єкт може містити; останні, у

Національний університет
свою чергу, залежать від типу об'єкта.

Microsoft Management Console (MMC) (консоль управління) - компонент операційної системи Windows 2000 і пізніших версій Windows. Дозволяє системним адміністраторам і досвідченим користувачам за допомогою гнучкого інтерфейсу конфігурувати роботу системи. Консоль управління надає широкі можливості для керування комп'ютером. Основний принцип дії полягає в оснастках - невеликих підпрограмах, що дозволяють налаштувати різні аспекти операційної системи. Найбільш примітною є оснастка «Групові політики». Також з консолі управління можна отримати розширені функції управління користувачами і групами, в ній можна налаштувати практично все, що завгодно (навіть заголовок Internet Explorer). Більшим вбудованим інструментом управління Windows є тільки реєстр Windows.

Групова політика

Групова політика - це набір правил, відповідно до яких відбувається налаштування робочого середовища Windows. Групові політики створюються в домені та реплікуються в межах домену. Об'єкт групової політики (Group Policy Object, GPO) складається з двох фізично розділених складових: контейнера групової політики (Group Policy Container, GPC) та шаблону групової політики (Group Policy Template, GPT). Ці два компоненти містять в собі всю інформацію про параметри робочого середовища, що входять до складу об'єкту групової політики. Продумане застосування об'єктів GPO до елементів каталогу Active Directory дозволяє створювати ефективне та легко кероване комп'ютерне робоче середовище на базі ОС Windows. Політики застосовуються зверху вниз по ієрархії каталогу Active Directory.

Сценарії підключення та відключення

Операційна система Windows NT дозволяє призначити кожному користувачеві сценарій, що містить команди, які необхідно виконати при підключенні даного користувача до системи. Зазвичай сценарії підключення використовуються для початкового налаштування робочого оточення користувача. Крім сценаріїв підключення Windows 2000 підтримує також сценарії відключення. Мало того, в новій операційній системі для кожного комп'ютера можна призначити сценарії початку і завершення роботи системи. Система виконання сценаріїв Windows Scripting Host (WSH) підтримує виконання сценаріїв, написаних такими мовами, як Visual Basic або Jscript, що

дозволяють безпосередньо звертатися до функцій Windows API. Розглянемо деякі можливості, пов'язані з використанням сценаріїв в середовищі Windows 2000.

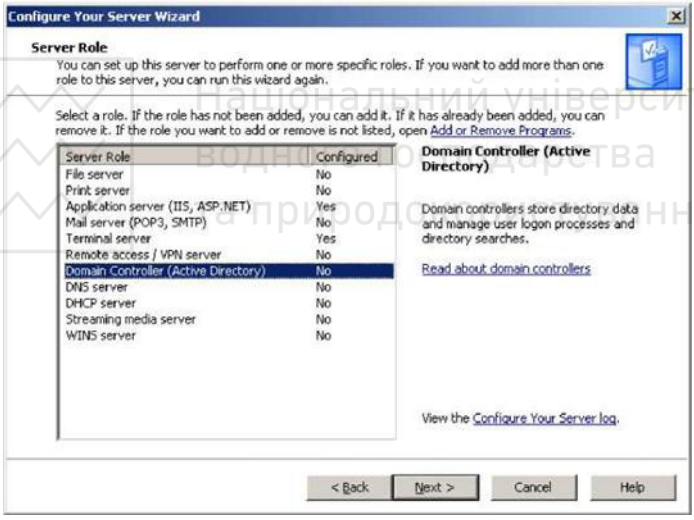
5.3. Програма роботи

1. Встановити та налаштувати Active Directory.
2. Провести приєднання клієнтської машини до домену.
3. Здійснити налаштування параметрів групових політик.

5.4. Порядок виконання роботи

Встановлення Active Directory

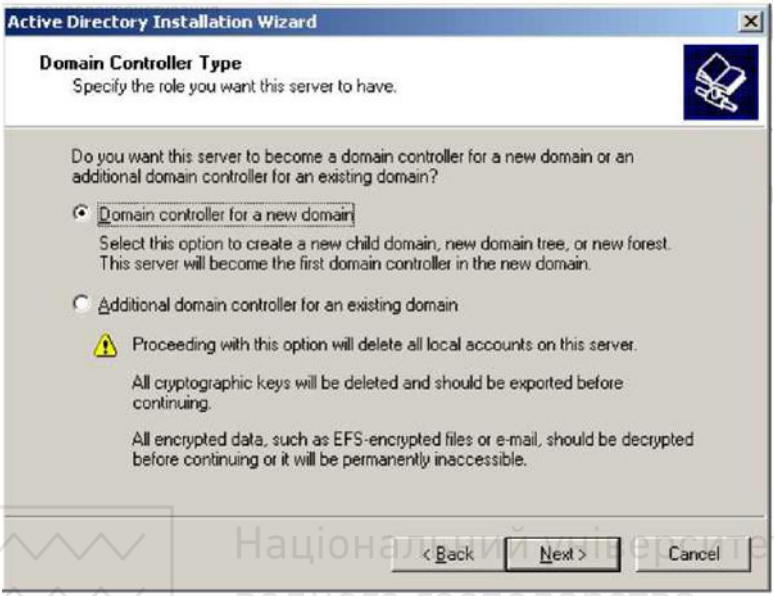
Додамо нову роль Domain Controller (Active Directory) для сервера:



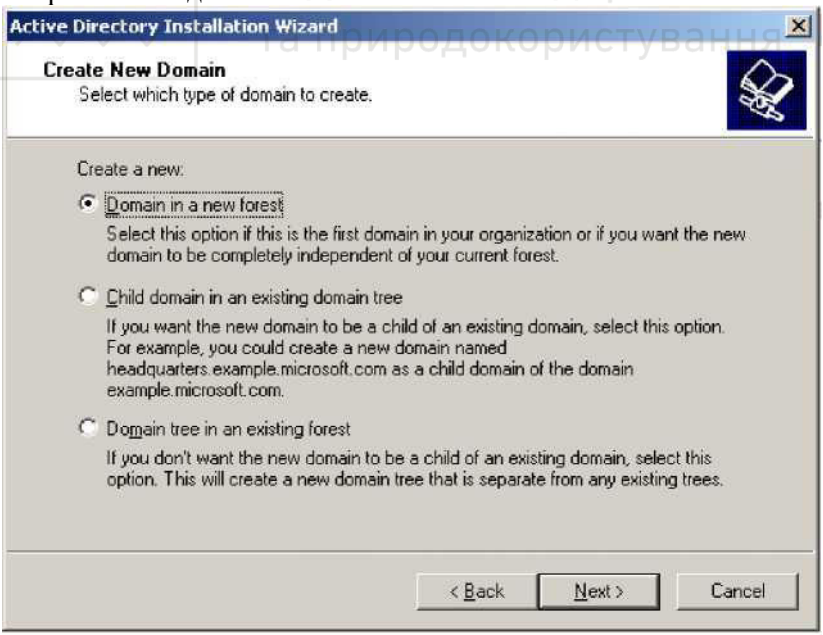
В процесі встановлення локальні користувачі і групи будуть розповсюджуватись на весь домен, тому можлива поява інформаційних повідомлень про зміну прав доступу до певних служб (наприклад, служби термінального доступу). Ознайомтеся з такими повідомленнями і продовжуйте встановлення.

Також сервер служби каталогів висуває підвищені вимоги до безпеки, тому необхідна файлова система NTFS. В разі потреби сконвертуйте FAT32 в NTFS використовуючи консольну утиліту CONVERT.

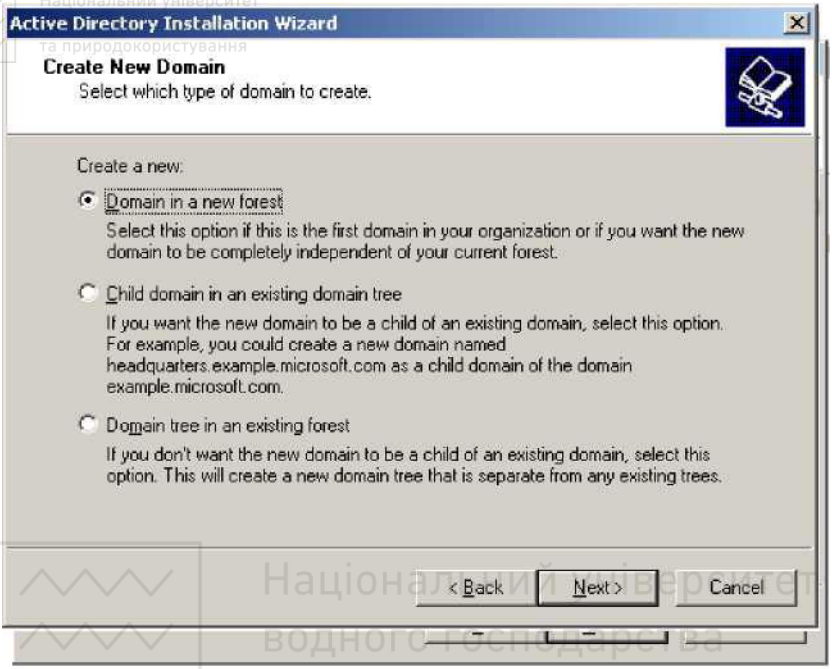
Вибір ролі контролера домену:



Виберіть новий домен:



Вибір типу домену. Виберіть новий ліс:



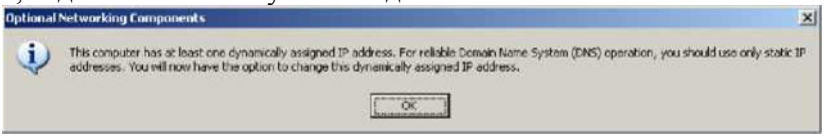
Наступним кроком буде вибір імені для домену.

Всі наступні параметри залиште за замовчуванням.

Також в процесі встановлення система може запропонувати встановити службу DNS. Погоджуйтесь, адже це є також необхідною умовою для успішного функціонування служби каталогів.

За бажанням можете задати пароль для режиму відновлення служби каталогів.

Якщо сервер був налаштований на використання динамічних IP адрес, тоді з'явиться наступне повідомлення:



Після цього необхідно налаштувати мережу на використання статичної IP адреси.

Через деякий час, після копіювання файлів, встановлення DNS, система запропонує перенавантажитись.

І у разі успішного встановлення, після перезавантаження комп'ютера з'явиться вікно підтвердження встановлення:

Тепер можна користуватися контролером домену.

Наступний крок - завести клієнтські машини в домен.

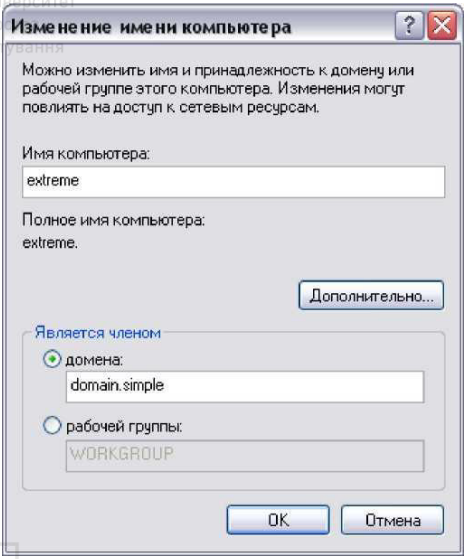
Приєднання клієнтської машини до домена

Для цього скористайтеся іншою віртуальною машиною, на якій налаштуйте мережу у відповідності до контролеру домена (той самий клас мережі, та сама маска).

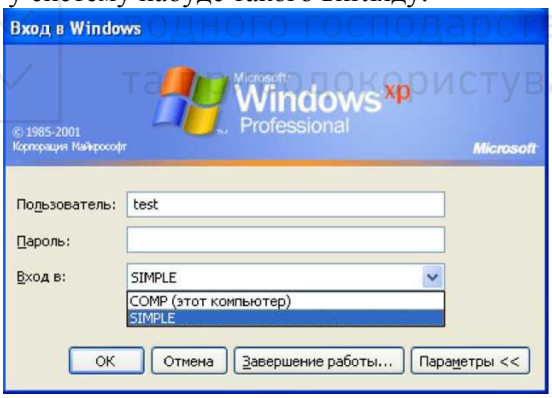
Процес під'єднання дуже простий: необхідно зайти у властивості „Мого комп'ютера":

У властивостях виберіть вкладку „Имя компьютера" - „Изменить" і введіть назву домену, яку ви вказали при створенні:

Національний університет
водного господарства
та природокористування



Перезавантажте комп'ютер і після цього він стане членом домену. Вікно входу у систему набуде такого вигляду:



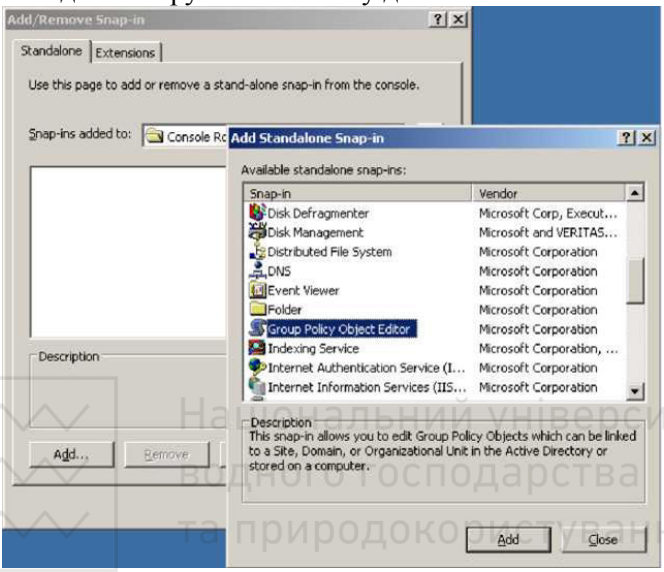
Тобто можна буде вибирати завантаження параметрів як локального комп'ютера (COMP) так і контролеру домену (SIMPLE).

Авторизуйтесь в системі використовуючи обліковий запис створений в попередній лабораторній або створіть новий.

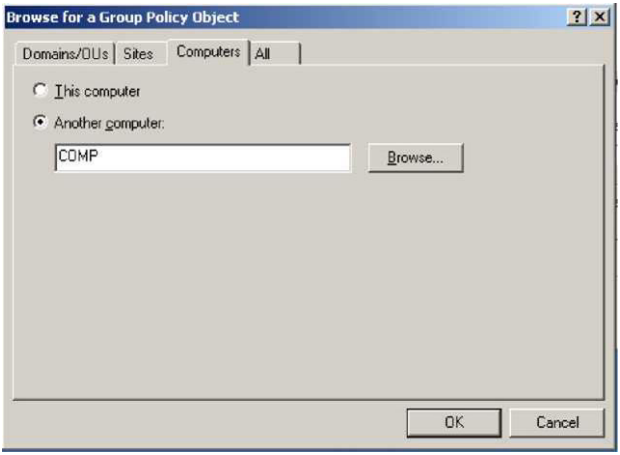
Групові політики

Щоб ви могли керувати груповими політиками, вам слід вручну додати компонент, створивши власну MMC (оснастку керування/консоль керування). Цей процес аналогічний створенню MMC для Active Directory. Клацніть кнопку "Start", виберіть "Run" і введіть у вікні "mmc". Відкриється пусте вікно MMC. З меню File

виберіть Add / Remove Snap-in. Відкриється вікно Add / Remove Snap-in. Клацніть Add, і у вікні Add Standalone Snap-in з'явиться список самостійних компонентів. Виберіть Group Policy. Клацніть OK і тепер можете вибрати об'єкт політики Local Computer, або можна натиснути кнопку Browse для вибору в локальному домені.

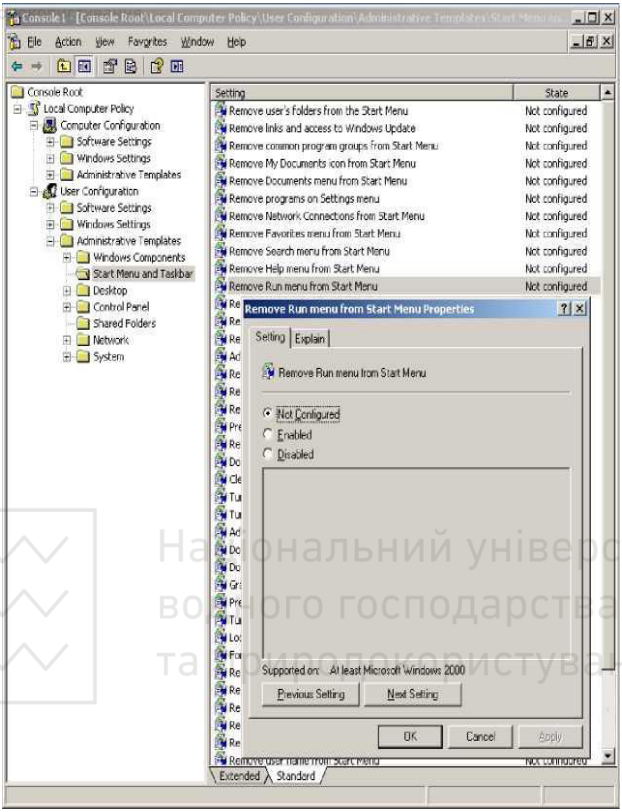


Але для того щоб побачити дію цієї політики в контексті клієнтського комп'ютера виберіть його в якості об'єкта групової політики:



Після цього ви можете приступати до налаштування

користувацького оточення:



Налаштуйте будь-який параметр і перевірте його роботу на клієнтській машині.

Занесіть результати до звіту.

5.5. Контрольні запитання

1. Що таке Active Directory?
2. Що таке групова політика?
3. Що таке MMC?
4. Яка структура служби каталогів?
5. Як налаштувати службу каталогів?
6. Як ви розумієте вираз „завести машину в домен”?
7. Що таке домен?
8. Які налаштування користувацького оточення ви знаєте?