МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Проектування комп'ютерних мереж

Методичні вказівки до лабораторних занять

Для студентів напряму підготовки
6.050102 «Комп'ютерна інженерія»
кафедри обчислювальної техніки
всіх форм навчання

Рекомендовано
Вченою радою факультету
інформатики та обчислювальної
техніки НТУУ «КПІ»
Протокол № 12 від 28.05.2012р.

Київ
НТУУ «КПІ»
2012

Проектування комп’ютерних мереж. Методичні вказівки до практичних занять. [Текст] / Уклад.: В.Ю.Куц, Р.Ю.Берест – К.: НТУУ «КПІ», 2012. – 212 с.

Методичні вказівки призначені для студентів напряму підготовки 6.050102 «Комп’ютерна інженерія» кафедри обчислювальної техніки всіх форм навчання. В посібнику наведена тематика практичних занять, основні теоретичні відомості, завдання лабораторних робіт, список літератури, контрольні питання.

Укладач — В.Ю.Куц, к.т.н.
Р.Ю.Берест

Відповідальний редактор — П.І.Кравець, к.т.н., доцент

Рецензент — Стенін О.А., д.т.н., проф. кафедри технічної кібернетики

За редакцією укладачів

ЗМІСТ

ВСТУП

Дисципліна «Проектування комп'ютерних мереж» призначена для вивчення концепцій, визначаючих стан та тенденції розвитку сучасних мережевих технологій, забезпечення знань теоретичних та практичних основ організації та функціонування комп'ютерних мереж, отримання базових навиків, необхідних для проектування комп'ютерних мереж та їх ефективного використання.

Практична частина курсу складається з одинадцяти лабораторних робіт і призначена для отримання практичних навичок проектування існуючих мережевих топологій, дослідження та порівняння їх характеристик. Всі лабораторні роботи виконуються в програмному комплексі OPNet, призначеному для створення, моделювання та вивчення мереж та їх зв'язків. Роботи послідовно логічно впорядковані за складністю та охоплюють всі теми, що вивчаються в курсі.

Матеріал для кожної лабораторної роботи містить мету, основні теоретичні відомості, загальне завдання, варіанти індивідуальних завдань, список питань для самоперевірки, зміст звіту про виконання лабораторних робіт, а також список рекомендованих інформаційних джерел для підготовки та виконання лабораторних робіт.

Лабораторна робота №1

ВИВЧЕННЯ ПРОГРАМНОГО СЕРЕДОВИЩА OPNET

Мета роботи. Моделювання корпоративної мережі та мережі масштабу міста (Metro Area Network, MAN) в програмному продукі *OpNet* та аналіз отриманих результатів. Отримати практичні навички проектування мереж масштабу підприємства; навчитися вибирати мережеві технології і компоненти і вміти обгрунтовувати свій вибір; освоїти найпростіші методи імітаційного моделювання обчислювальних мереж, оцінити отримані результати.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Основу інформаційної системи корпоративної мережі становить обчислювальна система, що включає такі компоненти, як кабельна мережа і активне мережеве обладнання, комп'ютерне та периферійне устаткування, обладнання зберігання даних (бібліотеки), системне програмне забезпечення (операційні системи, системи управління базами даних), спеціальне ПО (системи моніторингу та управління мережами) і в деяких випадках прикладне ПО. Як правило, в корпоративній мережі використовується централізована система управління мережею.

Ядро мережі являє собою маршрутизатор і сервери різного призначення. На маршрутизаторі зберігається і розраховується таблиця маршрутизації. За принципами формування таблиці маршрутизації бувають статичні і динамічні.

При моделюванні корпоративної мережі рекомендується використовувати статичні таблиці маршрутизації, так як кількість маршрутизаторів в середньому не перевищує трьох, при побудові більш великих мереж зі складною конфігурацією обладнання доцільно використовувати динамічну маршрутизацію. Доступ користувачів до ядра мережі здійснюється через

комутатори, що організують локальні мережі. Основною технологією для побудови корпоративної мережі в даний час є технологія Ethernet.

ЗАВДАННЯ НА РОБОТУ

1. Надати ескіз мережі.
2. Змоделювати мережу в OpNet.
3. Поставити профілі трафіку, налаштувати обладнання, вибрати тип збираємої статистики.
4. Провести симуляцію. Оцінити отримані результати.

МЕТОДИЧНІ ВКАЗІВКИ

1. Надати ескіз мережі. У пояснювальній записці описати підприємство, сферу діяльності, організаційну структуру, пояснити необхідність взаємодії між відділами та з зовнішніми організаціями, обгрунтувати вибір обладнання, додатків, алгоритмів маршрутизації, програмного забезпечення.

2. Змоделювати мережу в OpNet. При створенні моделі мережі спочатку необхідно дати назви проекту і сценаріям в ньому: *File-New* - назва проекту (рис. 1).

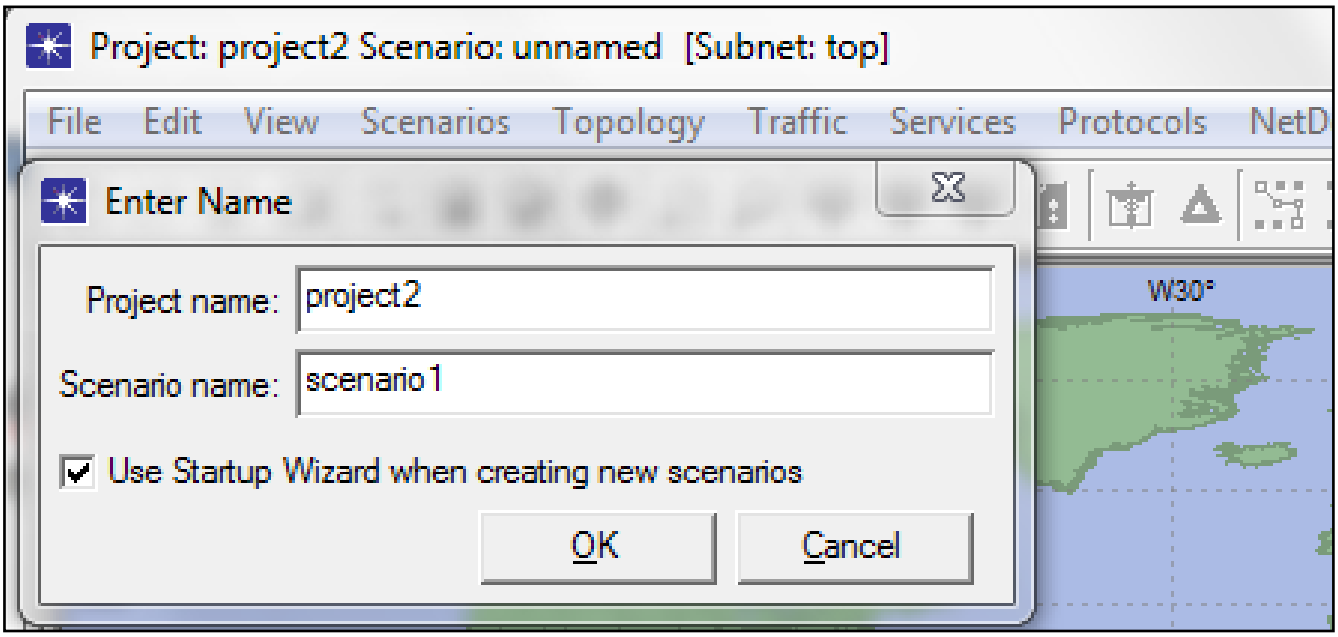


Рисунок 1 - Назва проекту

Далі вибираємо розмір мережі (у першій частині роботи будуємо корпоративну мережу, вибираємо *campus* або *office*), виділяємо необхідний і натискаємо клавішу *Next* (рис. 2).

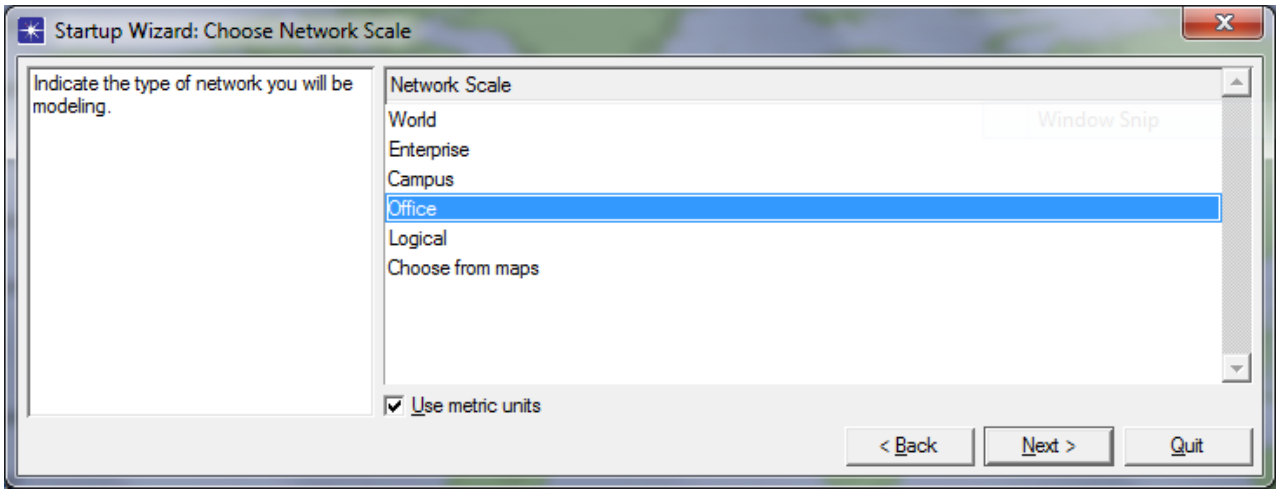


Рисунок 2 - Вибір розміру мережі

На наступному етапі необхідно вибрати конкретні розміри місцевості (м), на якій буде розташовуватися мережа (механізм вибору розмірів місцевості аналогічний вибору розміру мережі). Далі необхідно визначитися з вибором устаткування і технологій, які будуть представлені в проекті. Для цього в

списку виділяємо необхідний елемент, при цьому в поле Include з'явиться напис Yes - означає, що цей пакет включено в проект (рис. 3).

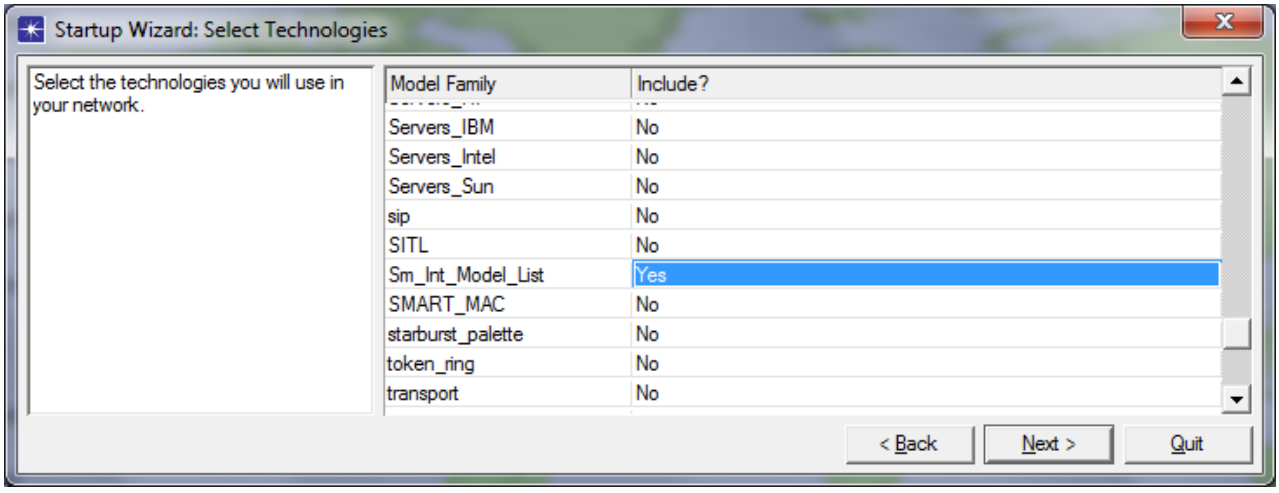


Рисунок 3 - Вибір обладнання та технологій

Після натискання клавіші *Next*, програма пропонує переконатися в правильності введених даних. Після перевірки параметрів створюваного проекту і натиснення клавіші Ок з'являється робоча область, де буде створюватися мережа, і палітра, де відображаються елементи, які можна використовувати в проекті (рис. 4).

Набір елементів можна змінити шляхом натискання клавіші *Configure Palette*. Елементи на робочу область можна переносити з палітри. Для цього виділяємо елемент у палітрі натисканням лівої кнопки миші(ЛКМ), другим аналогічним натисканням, але вже в робочій області, додаємо елемент в робочу область.

Крім того, в програмі є можливість створення комбінованих елементів з шаблонів. Для цього вибираємо на панелі інструментів *Topology -> Rapid Configuration* і, слідуючи пунктам, конфігуруємо шаблон. Приклад побудови офісної мережі представлений на рис. 5. Мережа розташована на двох поверхах, на кожному поверсі користувачі підключені до комутаторів, які в свою чергу об'єднані маршрутизатором. Один комутатор з'єднаний з сервером. Поруч з

сервером додані елементи, які визначають тип трафіку в мережі, і тип додатків, що працюють в цій мережі.

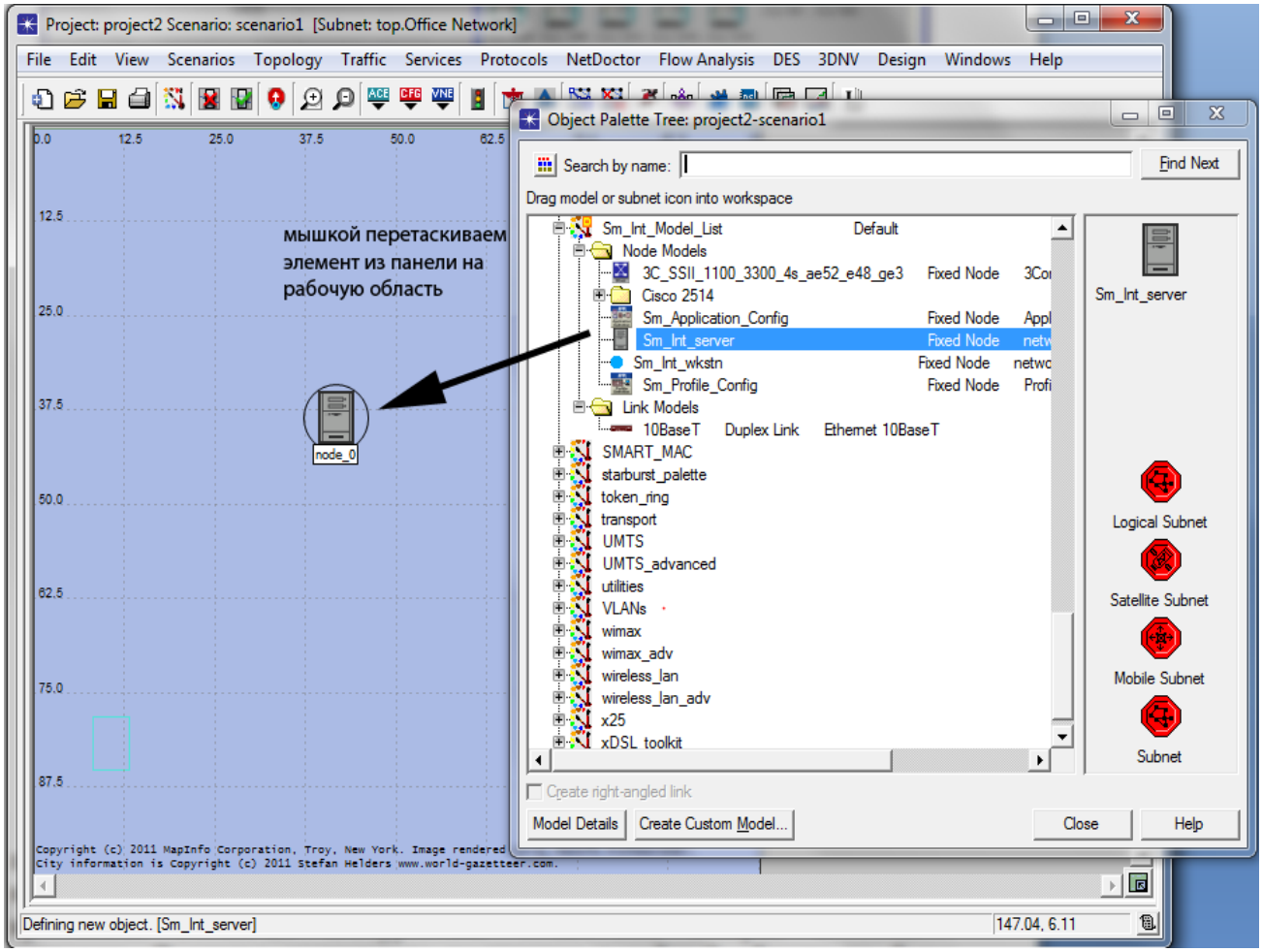


Рисунок 4 - Палітра проекту і робоча область

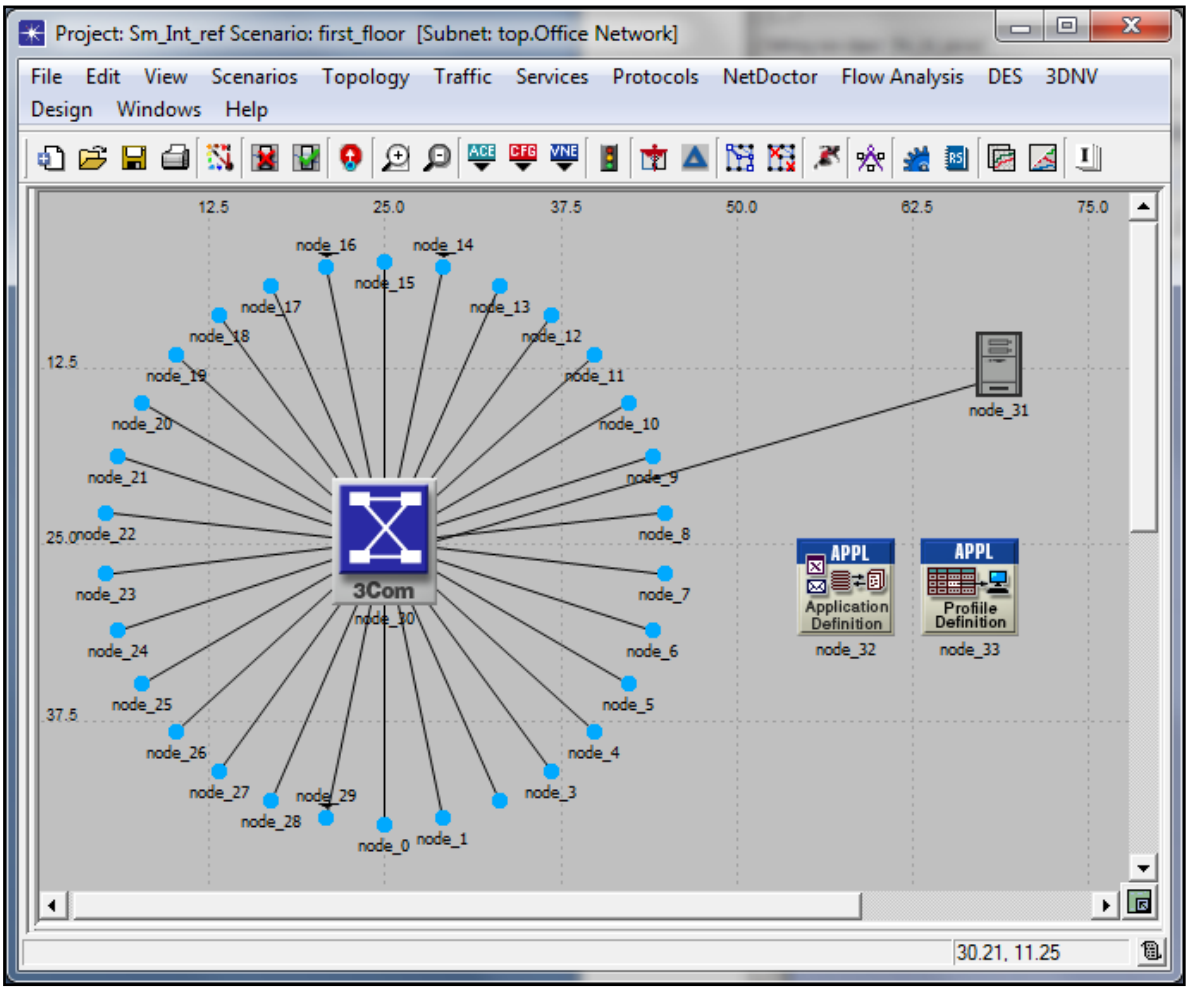


Рисунок 5 - Приклад побудови мережі

Після побудови моделі мережі її необхідно верифікувати, тобто перевірити топологію мережі. Для цього на панелі інструментів натискаємо кнопку з червоною галочкою. Якщо мережа побудована неправильно, OpNet червоними хрестиками позначить некоректні сполуки, які необхідно виправити. У разі правильної побудови в робочій області не буде ніяких змін.

3. Поставити профілі трафіку, налаштувати обладнання, вибрати тип збираємої статистики. Для налаштування обладнання необхідно натиснути правою клавішею миші(ПКМ) на цьому обладнанні і вибрати в меню пункт *Edit Attributes* (рис. 6). В залежності від обраного обладнання в робочій області з'явиться вікно з різним набором параметрів, що настроюються.

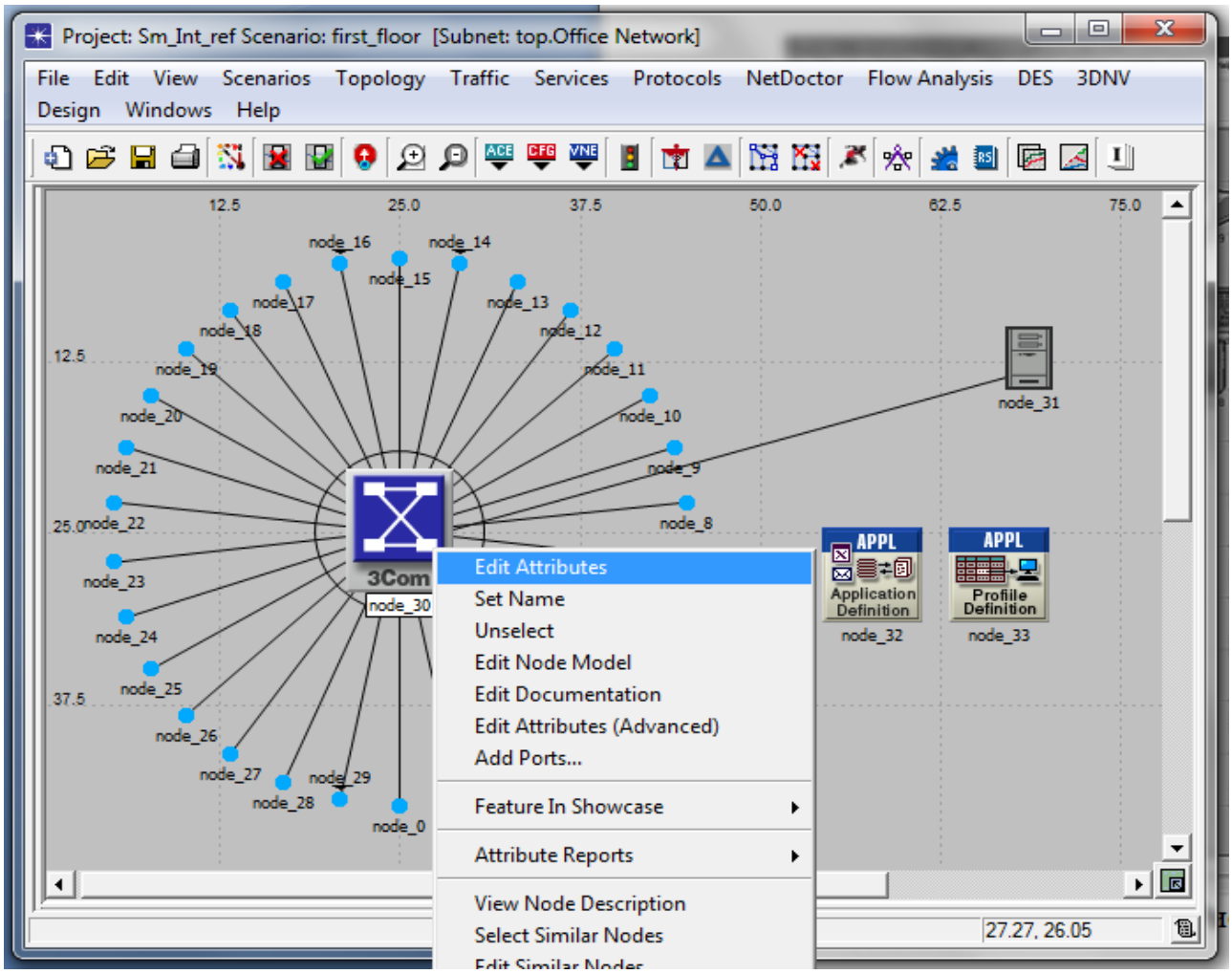


Рисунок 6 - Пункт Edit Attributes

3.1. Налаштування маршрутизатора. При налаштуванні обладнання побудувати статичну таблицю маршрутизації, задати інтерфейси, вибрати тип збираємої статистики. Оскільки моделюється невелика корпоративна мережа, що містить не більше трьох маршрутизаторів, в якій рідко відбуваються зміни (підключення нового вузла, додавання нового маршруту тощо), доцільно будувати статичну таблицю маршрутизації.

При побудові великої мережі, що містить 3 і більше маршрутизаторів, використовується динамічна таблиця маршрутизації. Для налаштування параметрів маршрутизатора потрібно натиснути правою кнопкою миші на його назву та обрати графу *Edit Attributes* (рис. 7).

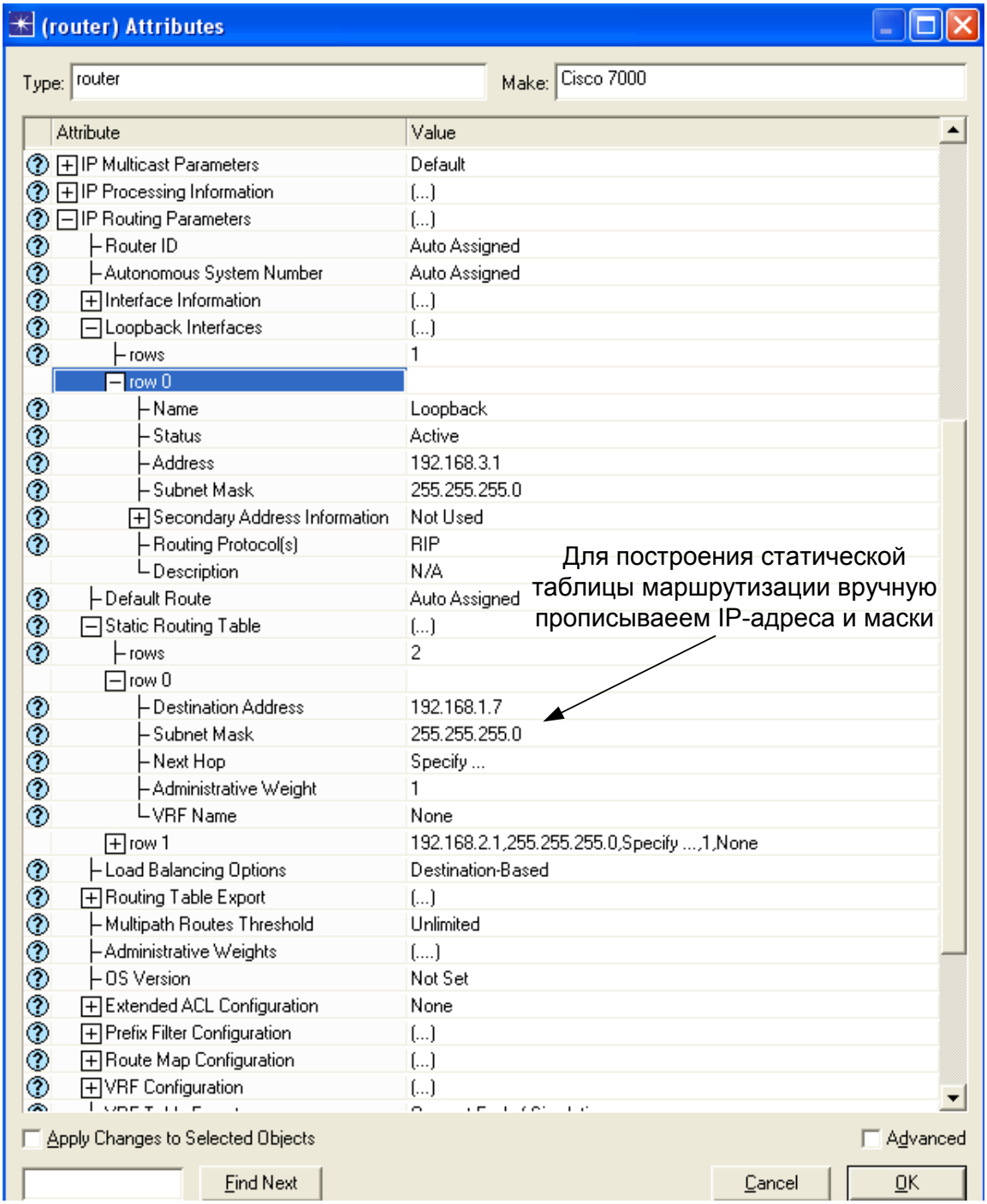


Рисунок 7 - Приклад налаштування маршрутизатора

Для побудови статичної таблиці маршрутизації необхідно вручну прописати IP-адреси і маски, для цього в полі *Attribute* обираєм пункт *IP Routing Parameters – Static Routing Table*.

В рядку *rows* вказуємо кількість активних інтерфейсів маршрутизатора. Для кожного інтерфейсу (рядки *row*) прописуємо IP-адресу та маску.

Для того, щоб задати параметри інтерфейсів, в полі *Attribute* вибираємо пункт *Interface Information*, в якому номер рядка (*row*) відповідає номеру інтерфейса. Для кожного інтерфейса, відповідного одному або декільком активним портам, задаємо IP-адресу та маску підключеного обладнання. Аналогічно налаштовуємо *Loopback Interface*.

Loopback Interface – це IP-интерфейс з адресою в мережі 127.0.0.1 використовується для адресації вузлом самого себе (loopback, інтерфейс зворотнього зв'язку). Звернення за адресою *Loopback Interface* означає зв'язок із самим собою (без виходу пакетів даних на рівень доступу до мережі); для протоколів на транспортному рівні і вище таке з'єднання не відрізняється від з'єднання яке проходить через мережу, що зручно використовувати, наприклад, для тестування мережевого ПЗ.

Для того щоб після процесу симуляції можна було подивитися таблицю маршрутизації, необхідно в полі *Attribute* обрати пункт *Routing Table Export* та встановити полю *Status* значение *Enabled*. (примітка - якщо ви заплуталися у безлічі пунктів скористайтесь пошуком він знаходиться внизу зліва біля знака питання в діалоговому вікні *Edit Attributes)*

Переглянути отриману таблицю маршрутизації після симуляції можна натиснувши *View Results* та обрав третю выбрав третью вкладку – *DES Run Tables* (Рис 8.)

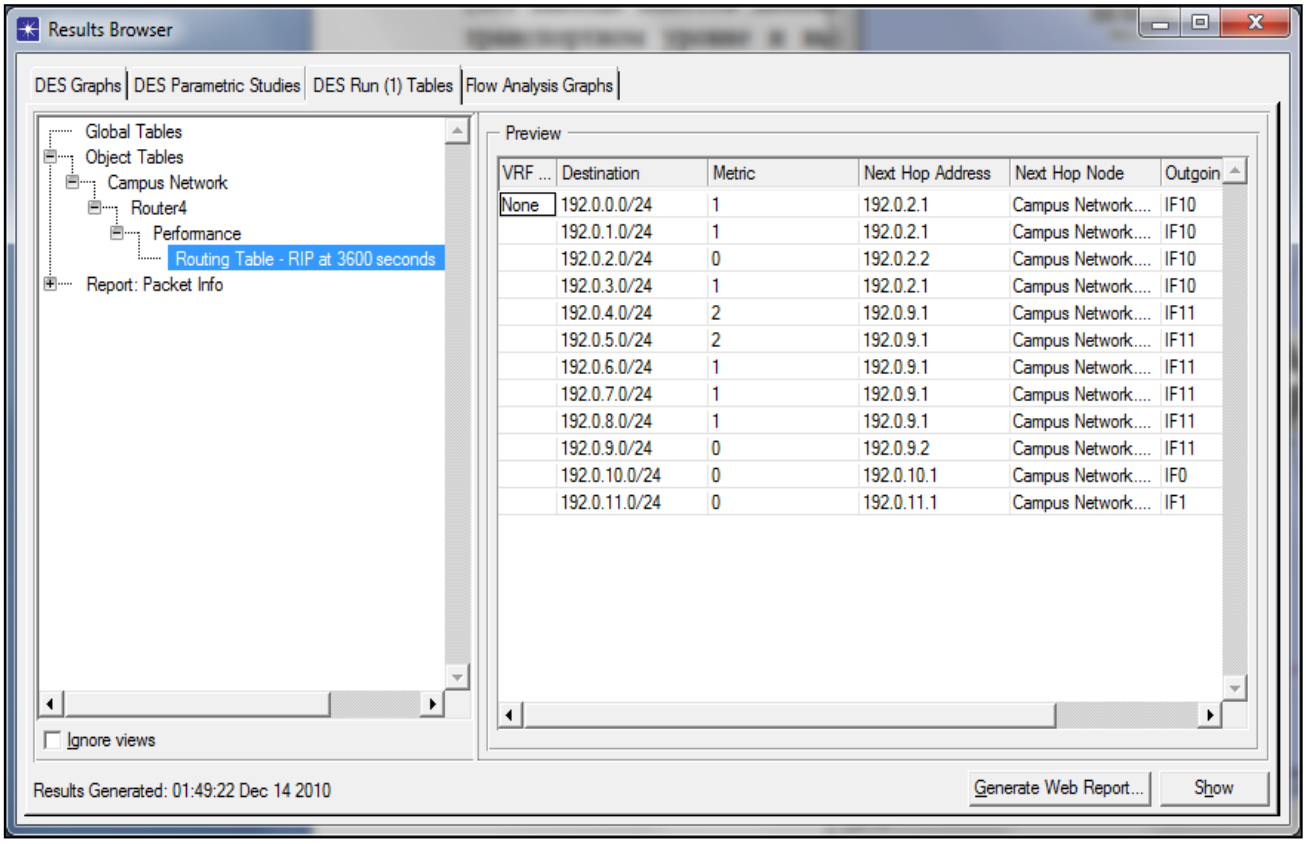


Рисунок 8 - DES Run Tables

Після того як налаштування обладнання завершено, необхідно вказати тип збираємої статистики. Для цього на досліджуваному обладнанні або сполучної лінії натиснути ПКМ і вибрати графу *Choose Individual Statistics*. Далі для кожного мережевого елементу пропонуються на вибір варіанти збору результатів моделювання (рис. 9).

Для маршрутизатора обов'язково зібрати наступні статистичні показники: завантаження процесора, обсяг трафіку переданого, отриманого, відкинутого по протоколу IP.

3.2. Налаштування комутатора. Як правило, додаткова настройка комутатора не потрібна, якщо немає необхідності реконфігурації портів або настройки VLAN. Для комутатора можна вказати тип збираємої статистики - натиснути ПКМ на комутаторі і вибрати графу *Choose Individual Statistic*. Далі галочками обрати потрібні параметри.

Для комутатора обов'язково зібрати наступні статистичні показники: *обсяг трафіку переданого, отриманого, відкинутого*.

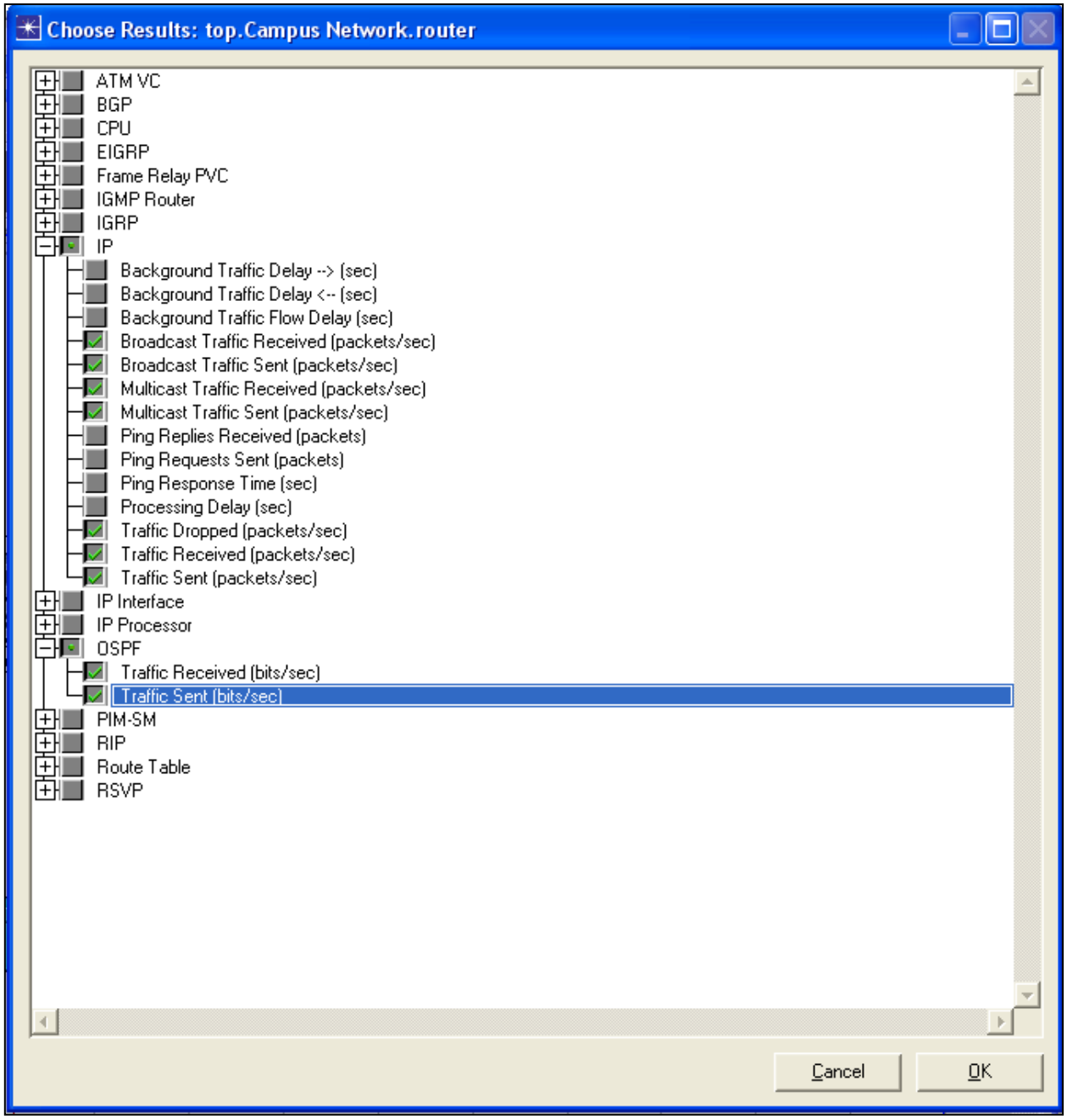


Рисунок 9 - Вибір типу збираємої статистики для маршрутизатора

3.3. Налаштування сервера. При налаштуванні сервера потрібно прописати тип трафіку, що генерується користувачами. Найпоширеніші типи трафіку: дані, голос, відео. Кожен з них пред'являє різні вимоги до передачі, забезпечення необхідної якості обслуговування, виділення достатньої

пропускної здатності. В залежності від напрямку діяльності підприємства / фірми по мережі буде передаватися трафік різного роду. Відповідно при проектуванні важливо правильно розрахувати завантаження каналів та обладнання. Перевірити розрахунки дозволяє моделювання планованої навантаженості. Так, наприклад, голос - це трафік, чутливий до затримок, але не вимагає великої пропускної здатності каналу, тому особлива увага при проектуванні мережі варто приділити забезпеченню необхідної якості обслуговування при передачі голосу.

Трафік VoD чутливий до затримок та втрат, і потребує високої пропускної здатності та налаштування протоколу PIM та IGMP.

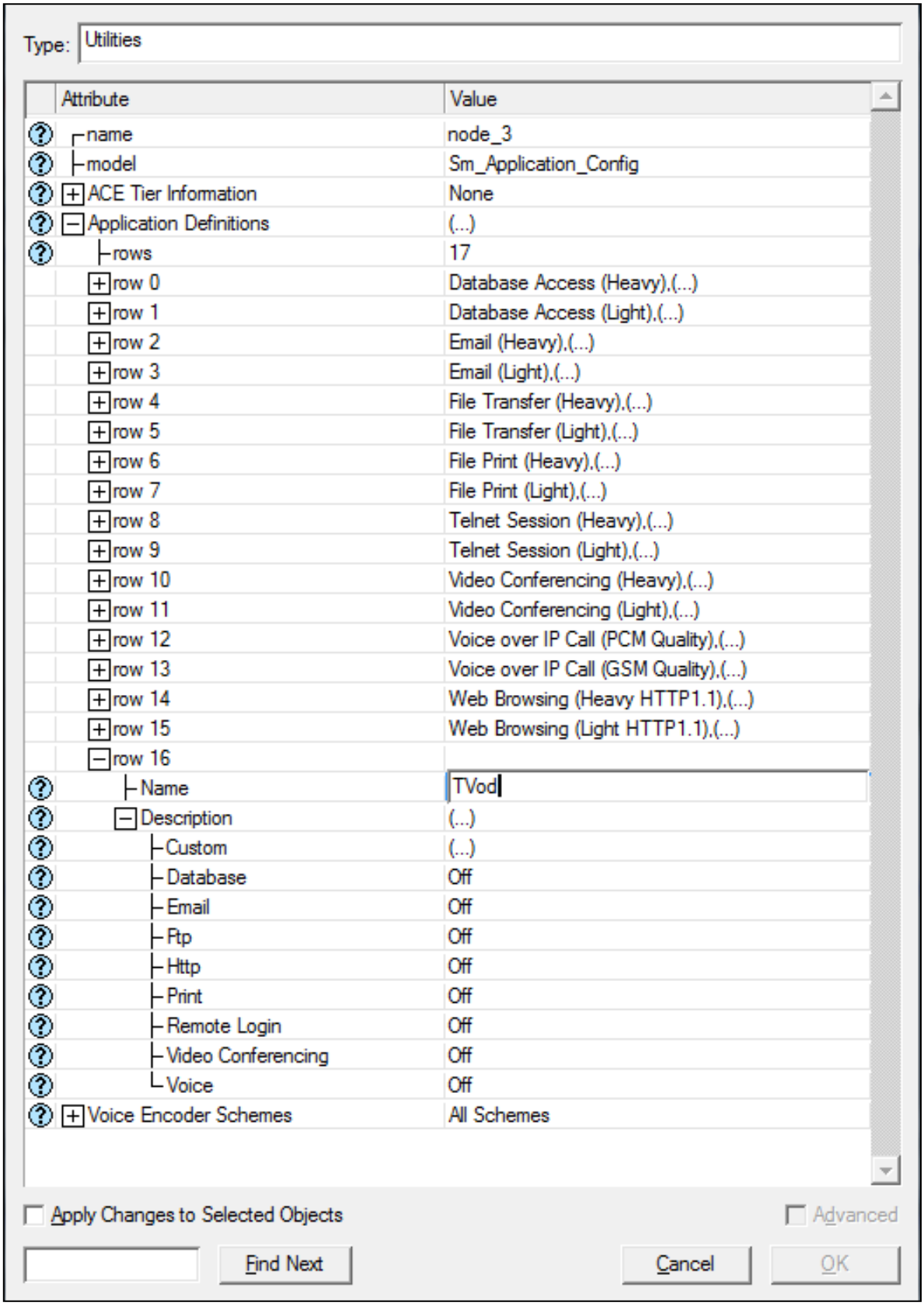


Рисунок 9 - Налаштування додатків на сервері

Тип трафіку задається за допомогою елемента палітри *Application Definition*. Елемент *Application Definition* необхідно перенести з палітри в робочу область і розмістити поряд з сервером.

Application Definition містить характеристики додатків, створюваних у вигляді потоків і мають власні параметри трафіку. Для створення потоків на *Application Definition* необхідно натиснути ПКМ і вибрати графу *Edit Attributes* (рис. 9), де створено 16 стандартних потоків для таких випадків. Сюди входить доступ до баз даних, обробка електронної пошти, передача файлів, робота в Інтернеті і т.д.

Після створення потоків програм необхідно сконфігурувати профілі користувачів, що працюють в спроектованій мережі. Цю функцію виконує елемент палітри *Profile Definition* (рис. 10).

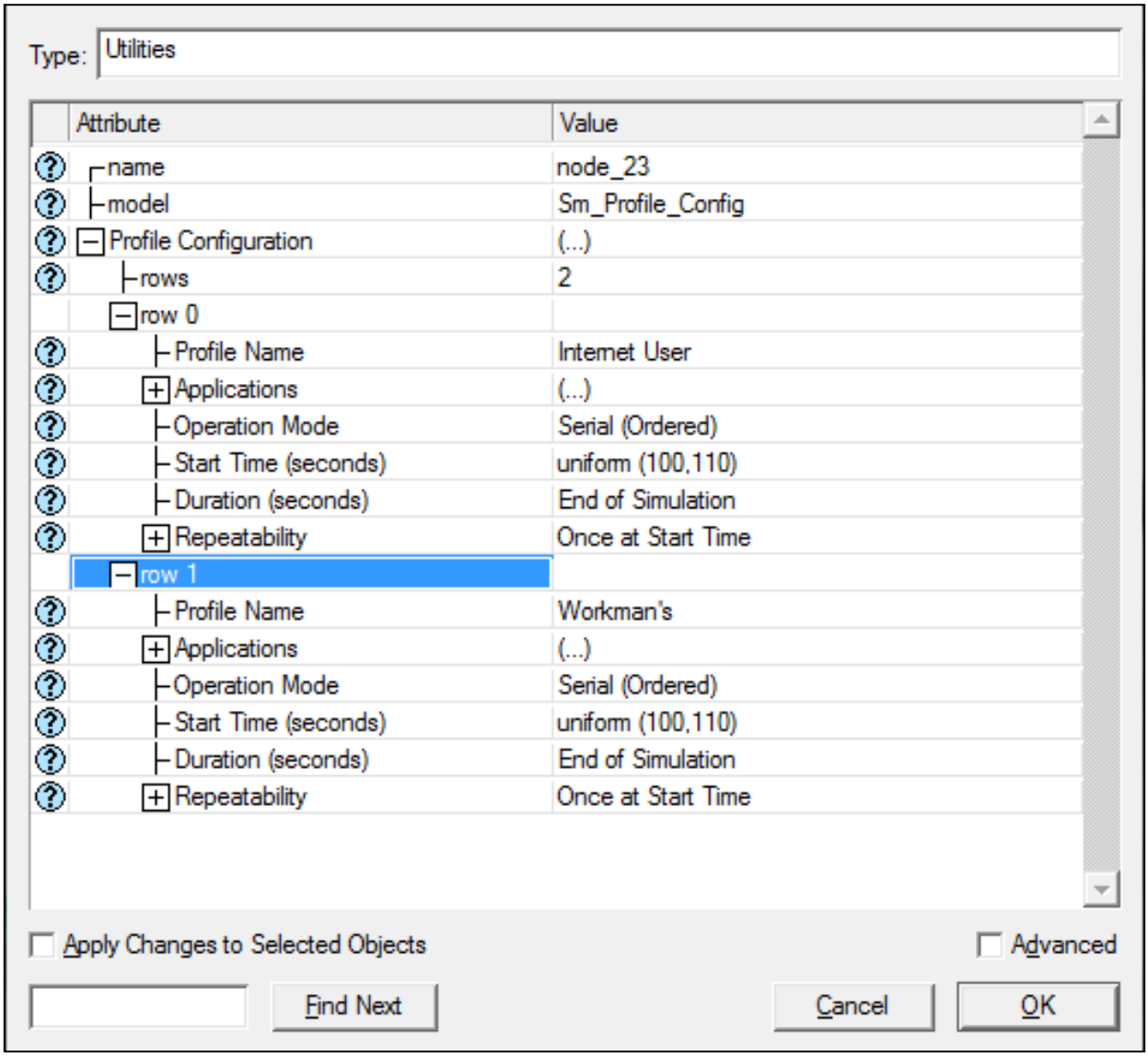


Рисунок 10 - Налаштування профілів користувачів

Кожному профілю дається назва і описується ряд користувальницьких характеристик: час початку роботи, тривалість, закінчення, інтенсивність його перебування і роботи в мережі і якими із запропонованих (створених) додатків він користується. Зазначені параметри задаються в *Application Definition* через пункт меню *Edit Attributes*.

Тип збираємої статистики вказується також через пункт меню *Choose Individual Statistics*. Для сервера необхідно зібрати наступні типи статистики: завантаження процесора, звернення до додатків сервера

- отриманий і відправлений трафік (*Application Demand – Traffic Sent, Traffic Received*);
- завантаження сервера FTP, HTTP, E-mail, DB (виберіть лише використовувані вами в роботі, але не менше двох)
- в розділі *Requesting Server Custom Applica*tion обрати *Application Response, Traffic Received/Sent, Applicayion/Group Response Time*, встановити значення завантаження в *Responding Server Custom Application*.

3.4. Налаштування кінцевих користувачів. При налаштуванні обладнання для кінцевих користувачів потрібно задати IP-адреси і маски, вказати назву і тип користувача. Кінцевий користувач може бути представлений двома способами: елементом LAN, який емітує якусь мережу абонентів, або робочою станцією.

У випадку, коли елемент LAN підключений до маршрутизатора, тобто є групою кінцевих користувачів, настройка параметрів даного елемента відбувається наступним чином. Обираємо пункт меню *Edit Attributes*. Заносимо число користувачів в графу *Number of Workstations*. Виходячи з цього параметра, заповнюється графа *Application-Supported Profiles*, яка вказує, скільки і якого роду користувачі будуть присутні у цій підмережі. Тут аналогічно серверу створюються потоки, що враховують користувачів мережі, на основі профілів, створених в елементі робочої області *Profile Definition* (рис. 11).

Необхідно вказати кількість профілів користувачів у графі *Rows*. Профілі користувачів утворюють потоки трафіку певного типу. Далі для кожного створеного таким чином потоку вказується назва профілю та число користувачів.

Число користувачів усіх типів у результаті має дорівнювати числу користувачів всієї підмережі. При налаштуванні LAN можна прописати статичну таблицю маршрутизації так само як на маршрутизаторі.

У випадку, коли кінцевим користувачем є робоча станція, настройка параметрів принципово не міняється. Тільки кількість користувачів завжди буде 1. Тип збирається статистики вказується через пункт меню *Choose Individual Statistics*.

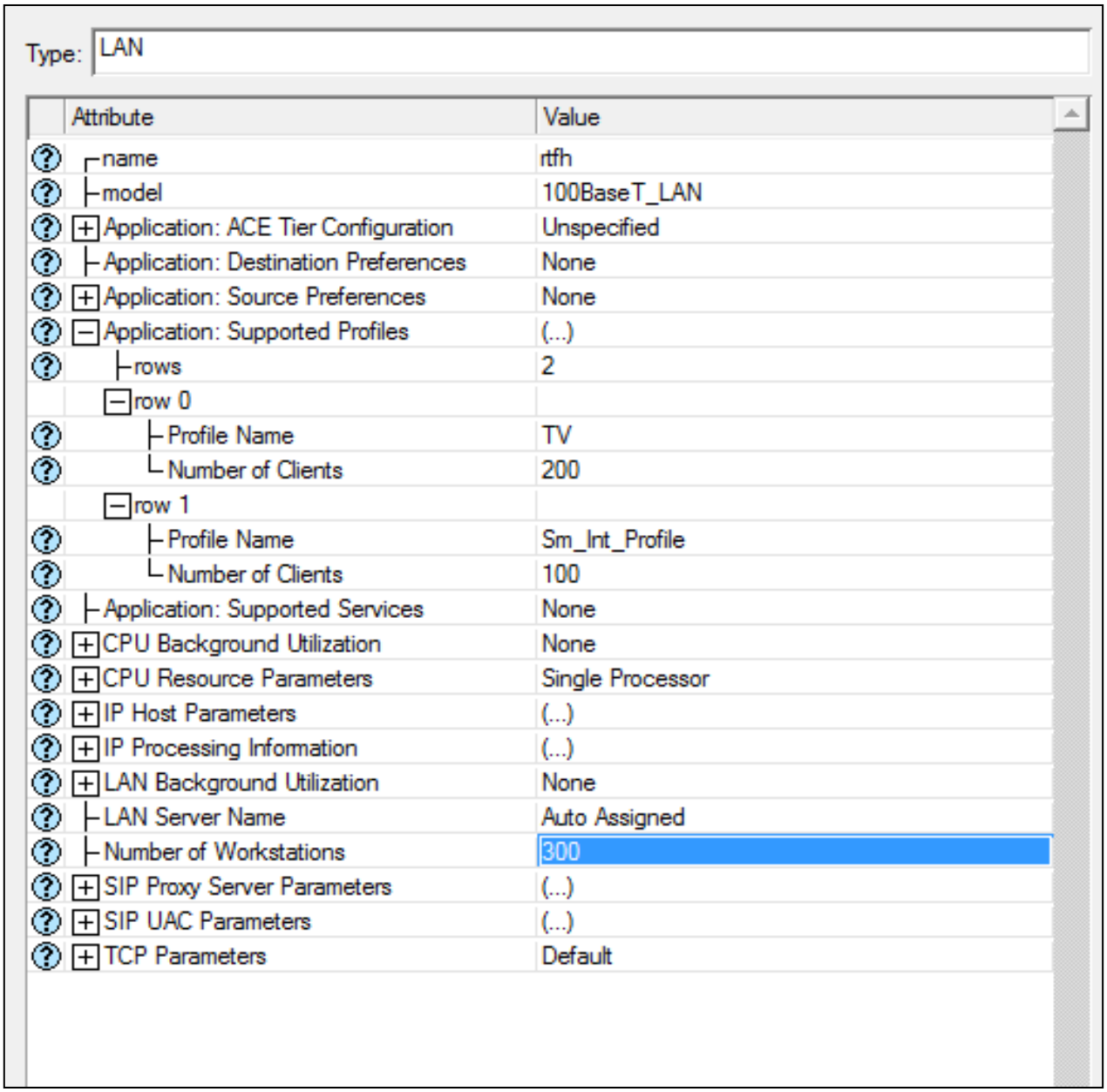


Рисунок 11 - Налаштування LAN

Для кінцевих користувачів зняти наступну статистику:

- затримку, варіацію затримки, обсяг трафіку отриманого, відправленого для типів додатків: *Video Conferencing*, *Voice Application*;
- завантаження процесора;
- кількість завантажених об'єктів / сторінок (*Downloaded Objects / Pages*) для *Client http*;
- розміри завантажених файлів (*Downloaded File Size*) та *Downloaded Response Time* для *Client Ftp*;
- обсяги отриманого / переданого трафіку (*Traffic Received/Sent*) для *Client E-mail* та *Client DB*;
- завантаження, затримку, обсяг отриманого / переданого трафіку (*Traffic Received/Sent*) в разділі *Ethernet*;
- *Utilization* в разділі *EtherChannel*.

Тепер можна приступати до симуляції, попередньо зберігши проект, натиснувши в меню проекту кнопку *Save*. Проект буде збережений в *C:\Documents and Settings\Guest\op_models*. При повторному запуску програми OpNET для відкриття існуючого проекту необхідно в меню *File* вибрати *Open* і назву свого проекту.

4. Провести симуляцію. Оцінити отримані результати.

Перед початком процесу симуляції необхідно налаштувати деякі параметри симуляції. Для цього на панелі інструментів потрібно натиснути кнопку *configure / run simulation* (або хоткей ctrl + R) і увійти в режим симуляції (рис.12).

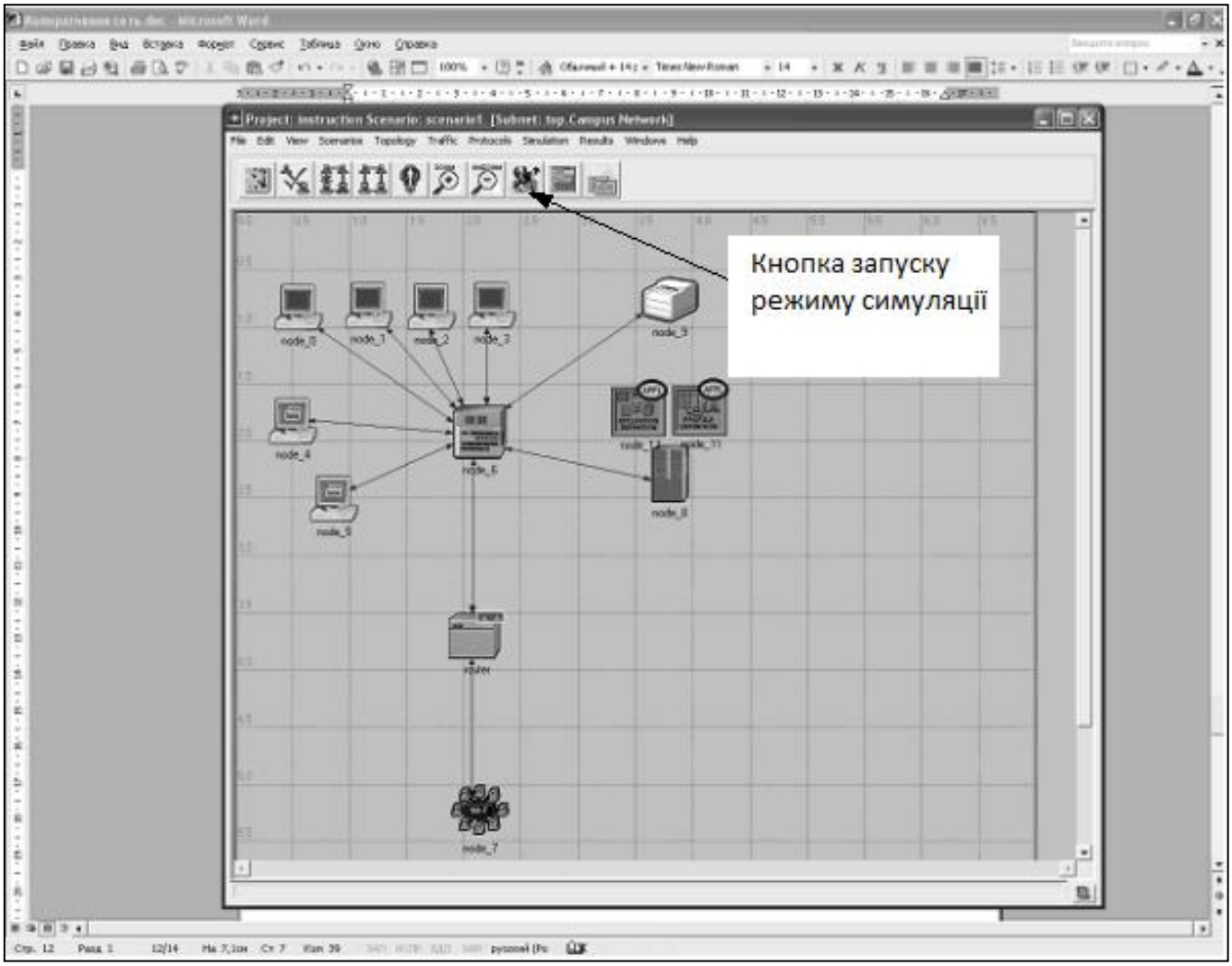


Рисунок 12 - Кнопка запуску режиму симуляції

Пакет OPNET Modeler 14.0 пропонує вказати тривалість роботи мережі (примітка - в ваших лабораторних роботах переважно не встановлювати час моделювання більш ніж 1 годину, зібраних за цей час даних буде достатньо в більшості випадків). У наступних закладках є можливість налаштування глобальних параметрів мережі, параметрів моделювання для кожного елементу, виведення звітів, анімації під час моделювання та ін.

Після вказівки часу моделювання та інтервалу оновлення можна запускати процес моделювання. Щоб запустити симуляцію потрібно натиснути кнопку *Run* (рис. 13).

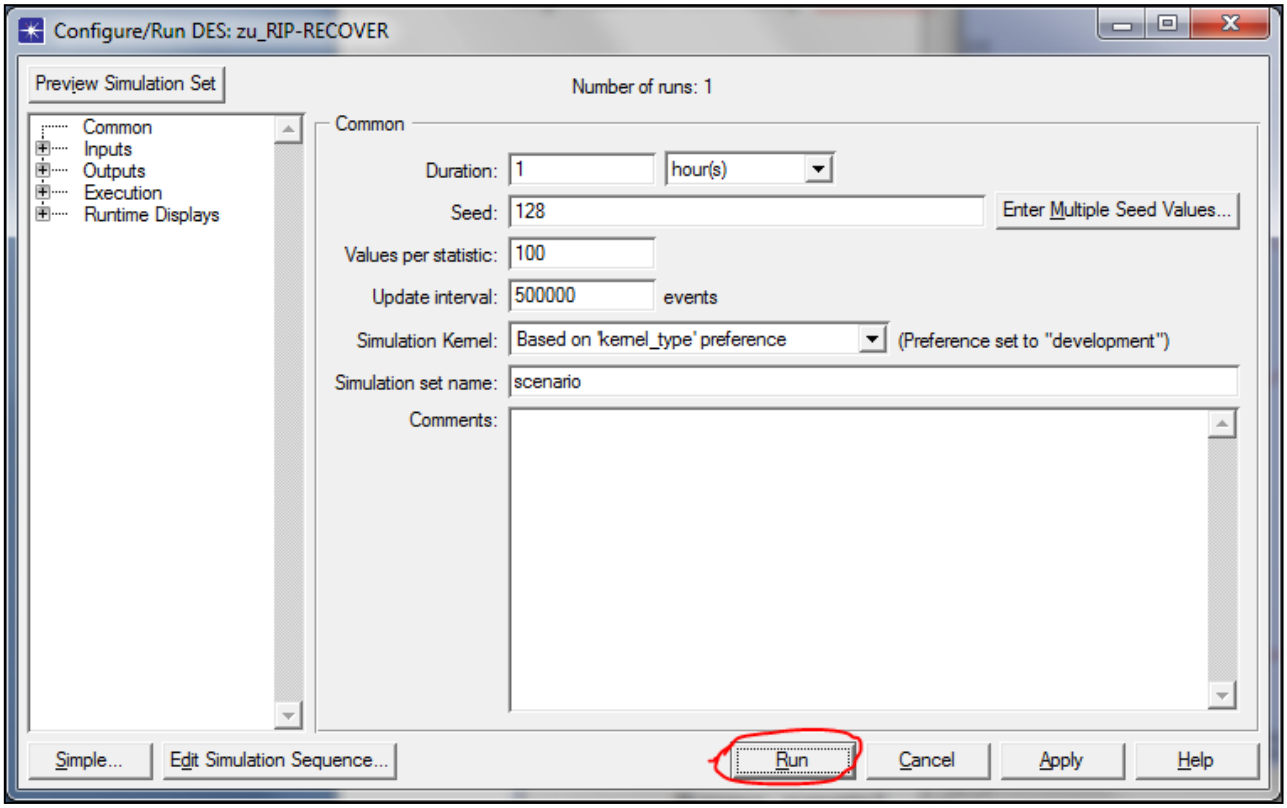


Рисунок 13 - Налаштування параметрів моделювання

Після завершення процесу симуляції навантаження на мережу можна побачити, перейшовши на закладку *Simulation Speed* (рис. 14).

Під час моделювання процесів, що відбуваються в побудованій мережі, в реальному часі на екрані будується графік активності, що складається з двох кривих: синя відображає ситуацію в кожен момент часу, (час відкладається по осі абсцис), червона показує середнє значення.

Для перегляду результатів моделювання роботи мережі «під навантаженням» вибираємо пункт *View Result*, для цього на вільному місці робочої області необхідно натиснути ПКМ і в меню вибрати відповідний пункт, або вибрати пункт меню *DES -> Results -> View Results*.

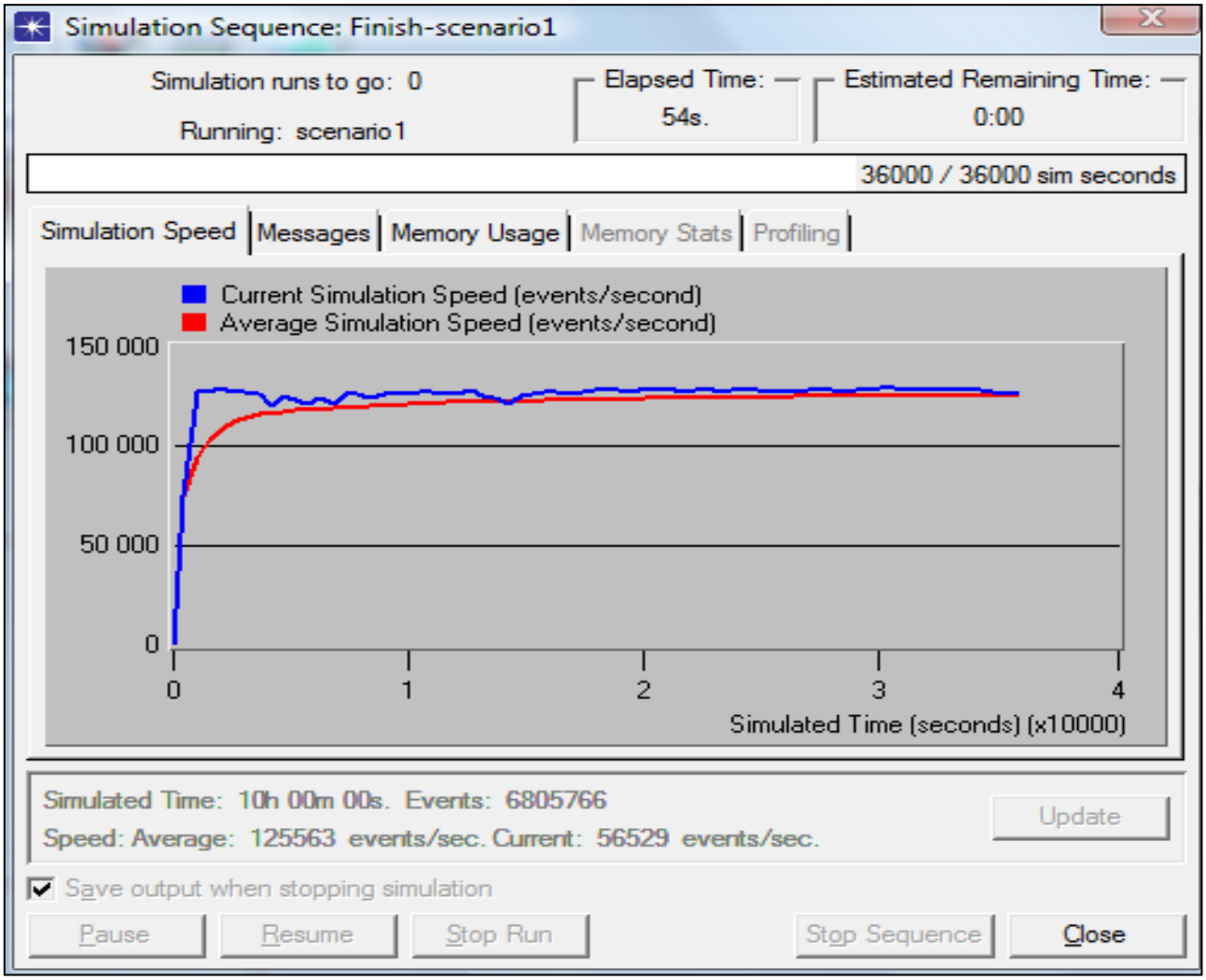


Рисунок 14 - Результати моделювання

У вікні *View Result* зеленими галочками можна обрати тип статистики, який нас цікавить, на різному устаткуванні, наприклад на рис. 15 показаний графік кількості відкинутих на маршрутизаторі пакетів за одиницю часу (*Traffic dropped*).

На рис. 16 представлений графік навантаження на канал, по якому можна оцінити пропускну здатність каналу, тобто видно, що за 2 год роботи мережі по каналу передавалося в середньому 65-70 кбіт / с.

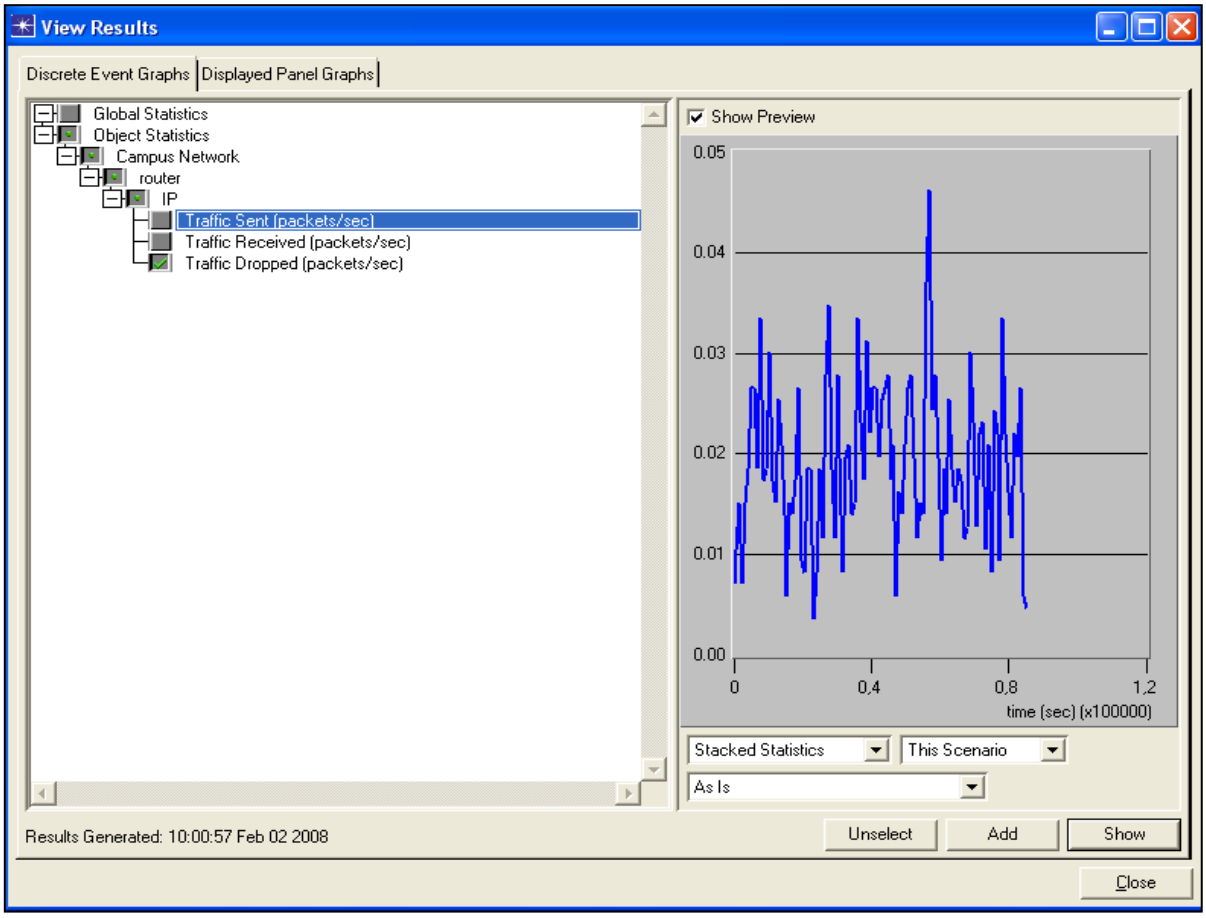


Рисунок 15 - Кількість відкинутих пакетів за одиницю часу, pack / s

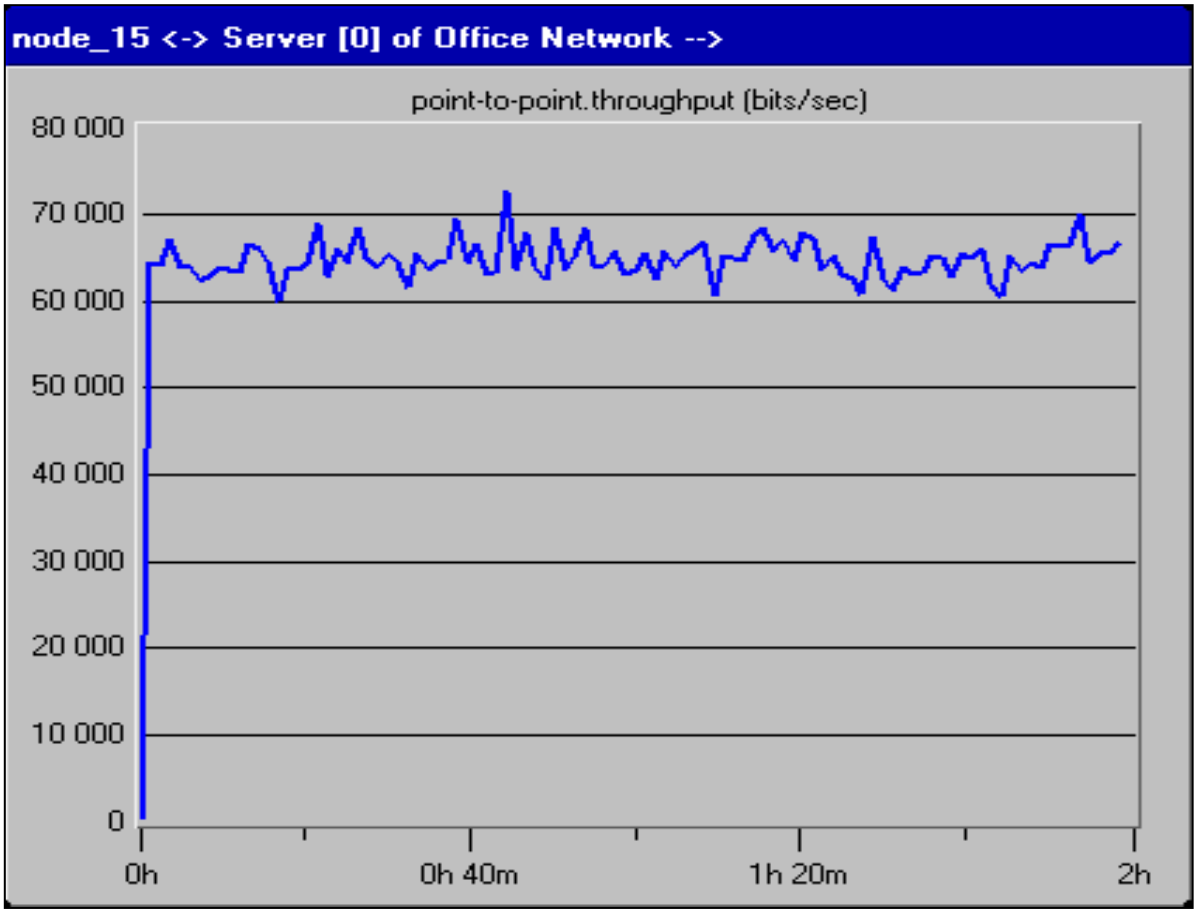


Рисунок 16 - Графік навантаження на канал

ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ

1. Надати звіт, що містить легенду, ескіз мережі, таблицю маршрутизації, приклади налаштування маршрутизатора, сервера, графіки навантаження на мережу, кілька типів збираємої статистики з ліній і устаткування, висновки за результатами моделювання:

- для маршрутизатора зібрати наступні статистичні показники: завантаження процесора, обсяг трафіку переданого, отриманого, відкинутого по протоколу IP;

- для комутатора: обсяг трафіку переданого, отриманого, відкинутого;

- для сервера: завантаження процесора, звернення до додатків сервера - трафік, отриманий і відправлений (Application Demand - Traffic Sent, Traffic Received), завантаження сервера FTP, HTTP, E-mail, DB, в розділі Requesting Server Custom Application - Application Response, Traffic Received / Sent, Applicayion / Group Response Time, завантаження в Responding Server Custom Application;

- для кінцевих користувачів зняти статистику: затримку, варіацію затримки, обсяг трафіку отриманого, відправленого для наступних типів додатків: Video Conferencing, Voice Application, завантаження процесора, для Client Http - Downloaded Objects / Pages, для Client Ftp - Downloaded File Size / Response Time, для Client E-mail - Traffic Received / Sent, для Client DB - Traffic Received / Sent, завантаження Ethernet, Traffic Received / Sent, Utilization для Ethernet Channel;

- для каналу між сервером і маршрутизатором зняти всі типи пропонованої статистики.

КОНТРОЛЬНІ ПИТАННЯ

1. Принципи побудови та технології корпоративних мереж.

2. Пояснити вибір обладнання, його конфігурацію, настройки і тип статистики.

Лабораторна робота 2

ВИВЧЕННЯ МЕРЕЖІ ETHERNET

Мета роботи. Демонстрація функціонування мережі Ethernet. Дослідження роботи мережі Ethernet в різних ситуаціях за допомогою моделювання.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Ethernet - робочий приклад більш загальної технології локальної мережі з множинним доступом до передавальної середовищі з опитуванням несучої і розв'язанням конфліктів (CSMA / CD). Ethernet - мережа колективного доступу, що означає, що ряд вузлів посилає і отримує кадри по загальнодоступному середовищу. "З опитуванням несучої" у множиному доступі до передавального середовища (CSMA / CD) означає, що всі вузли можуть розрізнити простій і зайнятість передавального середовища. "Розв'язання конфліктів" означає, що вузол прослуховує передавальну середу при передачі і тому може виявити, коли кадр, що передається, змішався (зіткнувся) з кадром, переданим іншим вузлом.

У цій лабораторній роботі Ви розробите мережу Ethernet з 30 вузлами, пов'язаними коаксіальним кабелем в шинну топологію. Коаксіальний кабель працює на швидкості передачі даних 10 Мб / с. Ви визначите, як пропускна здатність мережі залежить від мережевого завантаження і від розмірів пакетів.

ЗАВДАННЯ НА РОБОТУ

1. Надати ескіз мережі.
2. Змоделювати мережу в OpNet.
3. Поставити профілі трафіку, налаштувати обладнання, вибрати тип збираємої статистики.
4. Провести симуляцію. Оцінити отримані результати.

МЕТОДИЧНІ ВКАЗІВКИ

1. Створення нового проекту

1. Створіть новий проект для мережі Ethernet: Запустіть OPNET Modeler 14 $\Rightarrow$ Виберіть ***New*** в меню ***File***.

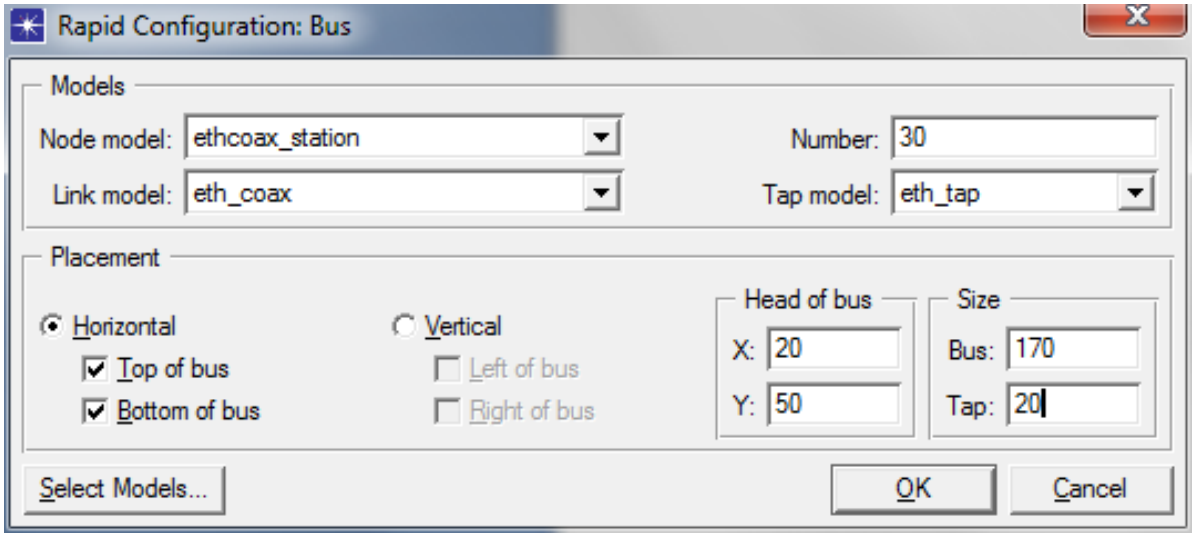
Виберіть ***Project*** ⇒ Натисніть *OK* ⇒ Назвіть проект <Ваші ініціали> _Ethernet, а сценарій Coax ⇒ Натисніть *OK*

2. У діалоговому вікні ***Initial Topology*** Майстра Запуску упевніться, що обрано ***Create Empty Scenario*** (Створити порожній сценарій) ⇒ Натисніть ***Next*** ⇒ Виберіть список ***Office Network Scale*** ⇒ Натисніть ***Next*** ⇒ Встановіть 200 в поле ***X Span*** і 100 в поле ***Y Span*** ⇒ Двічі натисніть ***Next*** ⇒ Натисніть *OK*
3. Закрийте діалогове вікно ***Object Palette***.

2. Створення мережі

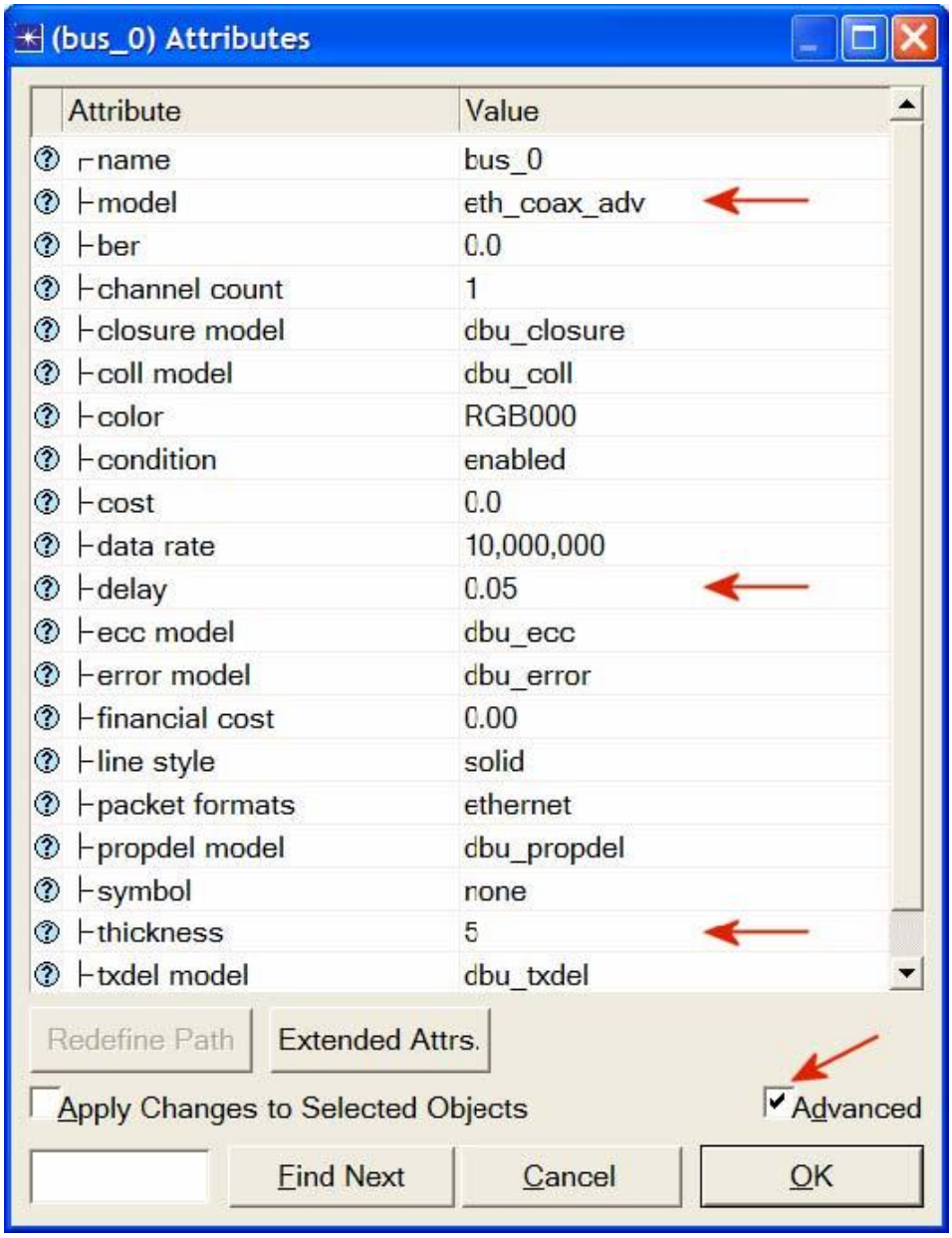
Щоб створити коаксіальну мережу Ethernet необхідно виконати наступне:

1. Оберіть ***Topology*** (Топологія) ⇒ ***Rapid Configuration*** (Швидка Конфігурація). У спадному меню виберіть *Bus* та натисніть ***OK***.
2. Натисніть кнопку ***Select Models*** в діалоговому вікні ***Rapid Configuration***. У спадному меню виберіть ethcoax, інакше у вас не з'являться вузли в полях ***Link Model*** і ***Node Model***, і натисніть ***OK***.
3. У діалоговому вікні ***Rapid Configuration*** встановіть наступні значення та натисніть ***OK***.



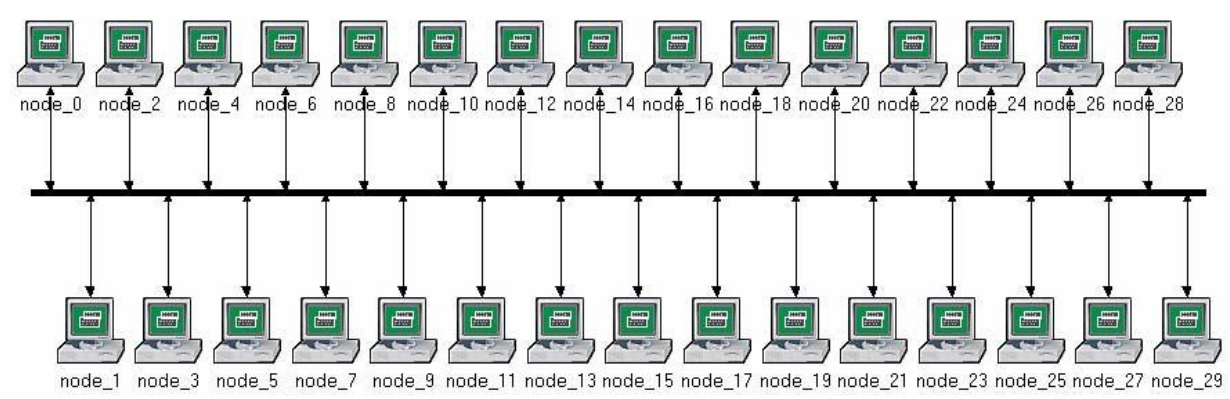
eth_tap - сигнал шини Ethernet, який з'єднує вузол з шиною. eth_coax - шина Ethernet, яка може поєднувати вузли з шинними одержувачами і передавачами через сигнали.

4. Щоб налаштувати коаксіальну шину, натисніть ПКМ на горизонтальному зв'язку ⇒ оберіть в меню ***Advanced Edit Attributes***:
   a. Клацніть на значенні параметра model ⇒ Виберіть ***Edit*** в випадаючому меню ⇒ Виберіть модель eth_coax_adv.
   b. Встановіть значення 0.05 для параметра ***delay*** (затримка розповсюдження, секунд / м.).
   c. Встановіть 5 для параметра ***thickness***.
   d. Натисніть OK.



Більш висока затримка (***delay***) використовується тут як альтернатива генерації більш високого трафіку, який вимагав би набагато більш тривалого часу моделювання. Товщина (***thickness***) визначає товщину лінії для промальовування шинного зв'язку.

Тепер Ви створили мережу. Вона повинна бути схожа на ілюстрацію нижче. Переконайтеся, що зберегли Ваш проект.



Налаштування Вузлів Мережі

Щоб налаштувати трафік, генерований вузлами:

Клацніть правою кнопкою миші на будь-якому з 30 вузлів ⇒ Select Similar Nodes (Вибрати подібні вузли). Тепер вибрані всі вузли в мережі.

1. Клацніть ПКМ на будь-якому з 30 вузлів ⇒ ***Edit Attributes*** (Редагувати параметри).
2. Встановіть прапорець ***Apply Changes to Selected Objects***. Це важливо для уникнення конфігурування кожного вузла індивідуально.
3. Розкрийте ієрархію ***Traffic Generation Parameters*** (Параметри генерації трафіку):

   Змініть значення ***ON State Time на exponential (100)*** ⇒ Змініть ***значення OFF State Time на exponential (0)***. (Зауважте: Пакети генеруються тільки в стані "ON").

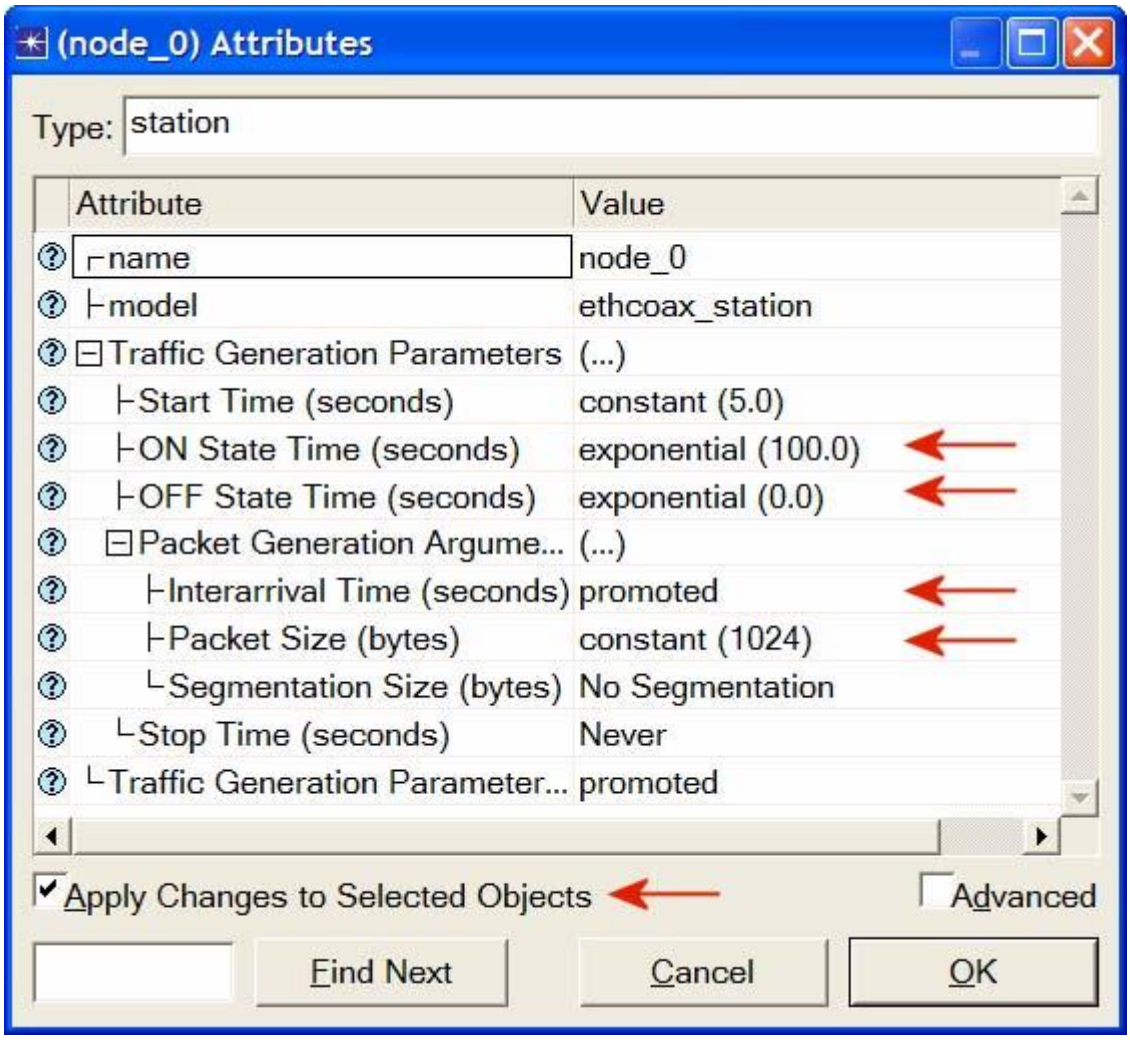
4. Розкрийте ієрархію ***Packet Generation Arguments***:

a. Змініть значення параметра ***Packet Size*** на ***constant (1024)***.

b. Клацніть ПКМ на параметрі ***Interarrival Time*** і виберіть ***Promote Attribute to Higher Level***. Це дозволяє нам призначати різні значення параметру ***Interarrival Time*** і отже перевіряти роботу мережі при різних завантаженнях.

Параметр показового розподілу (***exponential***) - середній інтервал між послідовними подіями. В показовому розподілі ймовірність виникнення

наступної події до даного часу анітрохи не залежить від часу виникнення останньої події або часу, що пройшов з тієї події.



Interarrival Time - час між послідовними генераціями пакета в стані "***ON***".

5. Натисніть **OK**, для того, щоб повернутися до ***Project Editor***(редактор проекту).

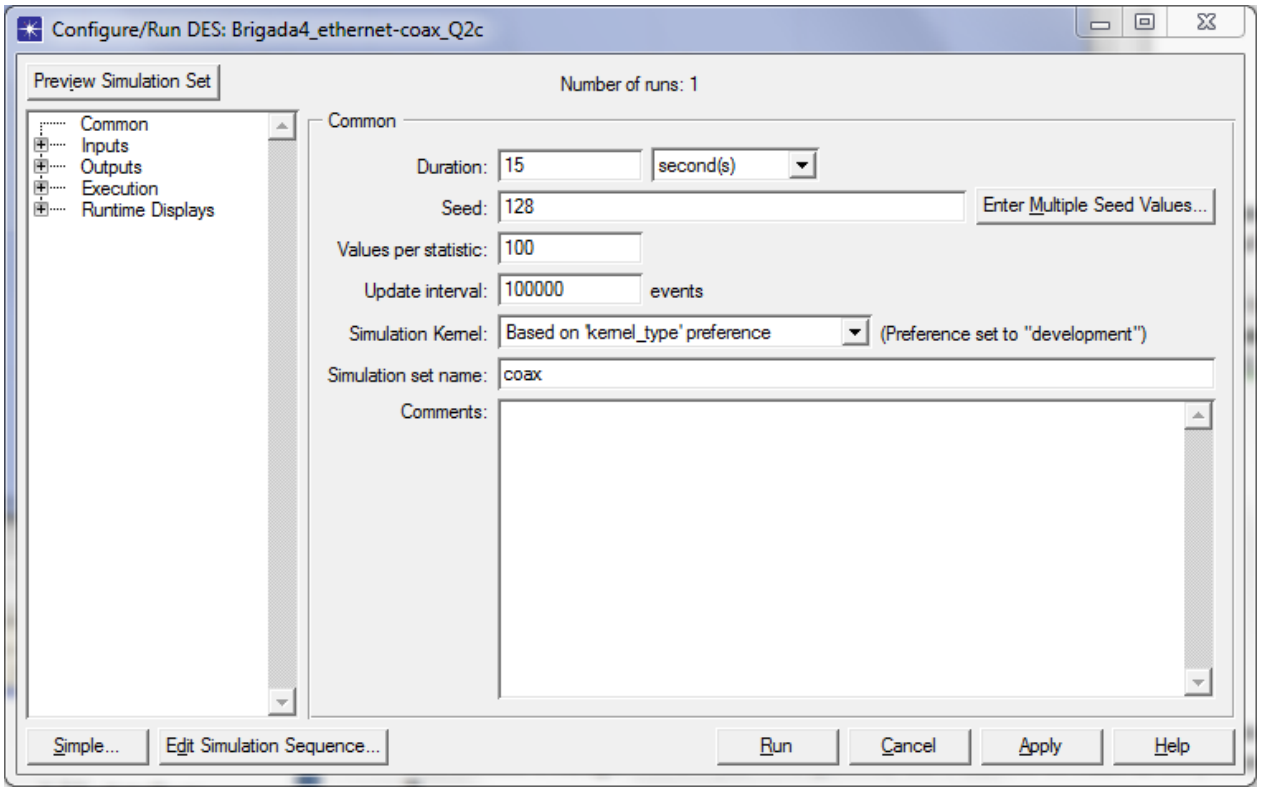
6. Переконайтеся, що зберегли Ваш проект.

Налаштування моделювання

Щоб дослідити роботу мережі при різних завантаженнях, Ви повинні запустити моделювання кілька разів, змінюючи при цьому завантаження

мережі. Є простий спосіб зробити це. Повторно виберіть параметр ***Interarrival Time***. Тут ми призначимо різні значення цього параметра:

1. Натисніть кнопку ***Configure/Run Simulation***: 
2. Переконайтеся, що обрана закладка ***Common*** ⇒ Встановіть 15 секунд в полі ***Duration***.



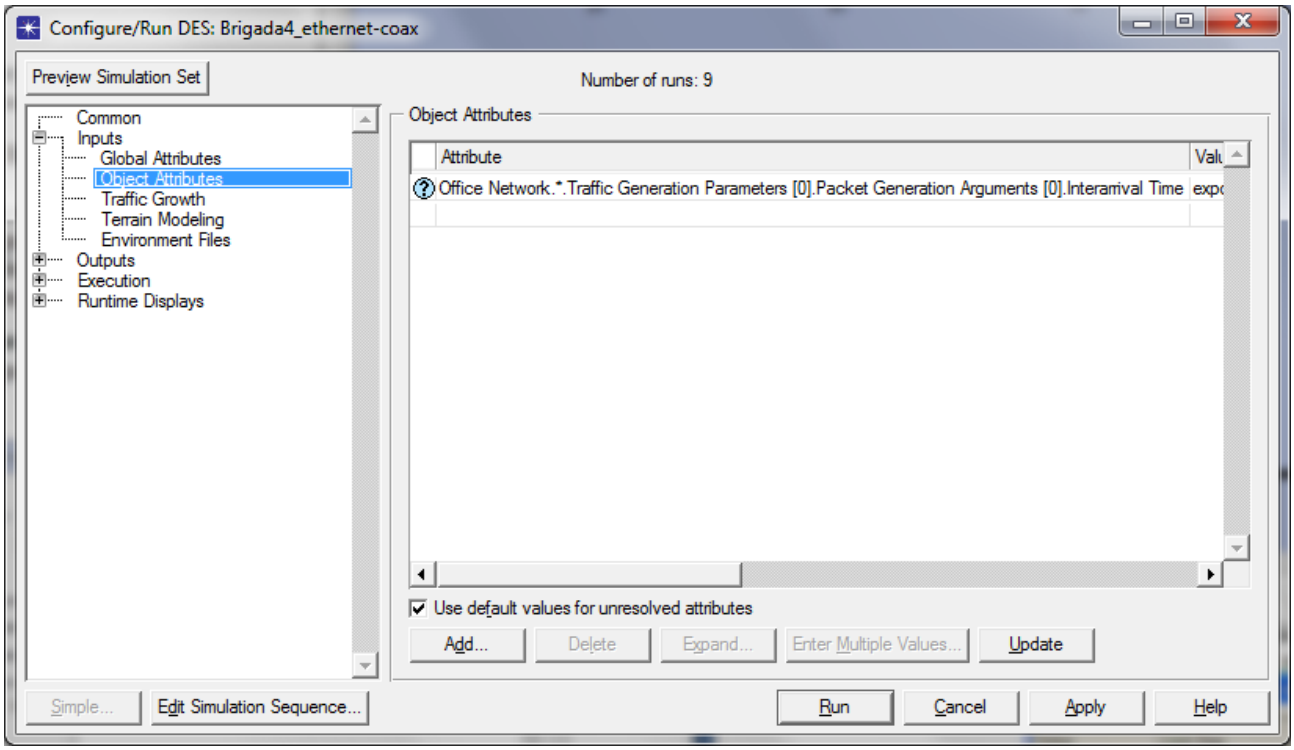
3. Перейдіть на закладку ***Object Attributes***.

4. Натисніть кнопку ***Add***. Повинно з'явитися діалогове вікно ***Add Attribute***, заповнене параметрами всіх вузлів мережі (якщо Ви не бачите параметри в списку, закрийте весь проект і повторно відкрийте його). Ви повинні додати параметр ***Interarrival Time***. Щоб зробити це:

а. Клацніть на першому параметрі в списку (***Office Network.node_0.Traffic Generation*** ....) ⇒ Натисніть кнопку ***Wildcard*** ⇒ Клікніть на ***node_0*** і виберіть (*) в випадаючому меню ⇒ Натисніть ***OK***.

b. Новий параметр, який містить зірочку, тепер згенерований (другий у списку), і Ви повинні додати його, натиснувши на відповідну клітинку в колонці ***Add***.

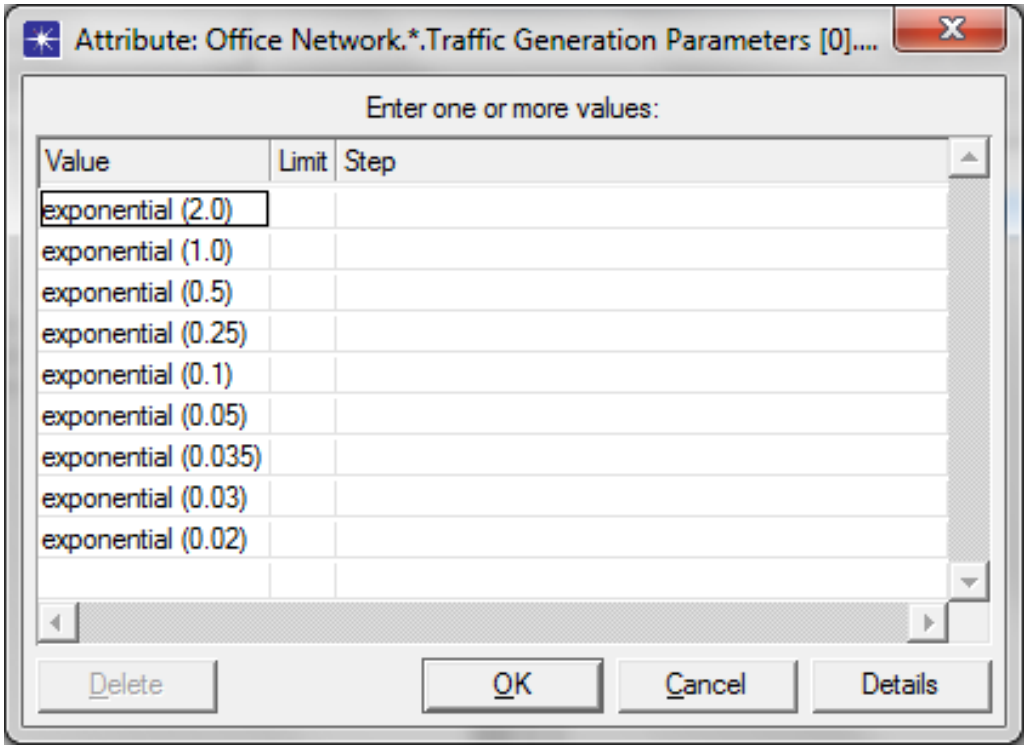
c. Діалогове вікно ***Add Attribute*** повинно бути схоже на наступне.



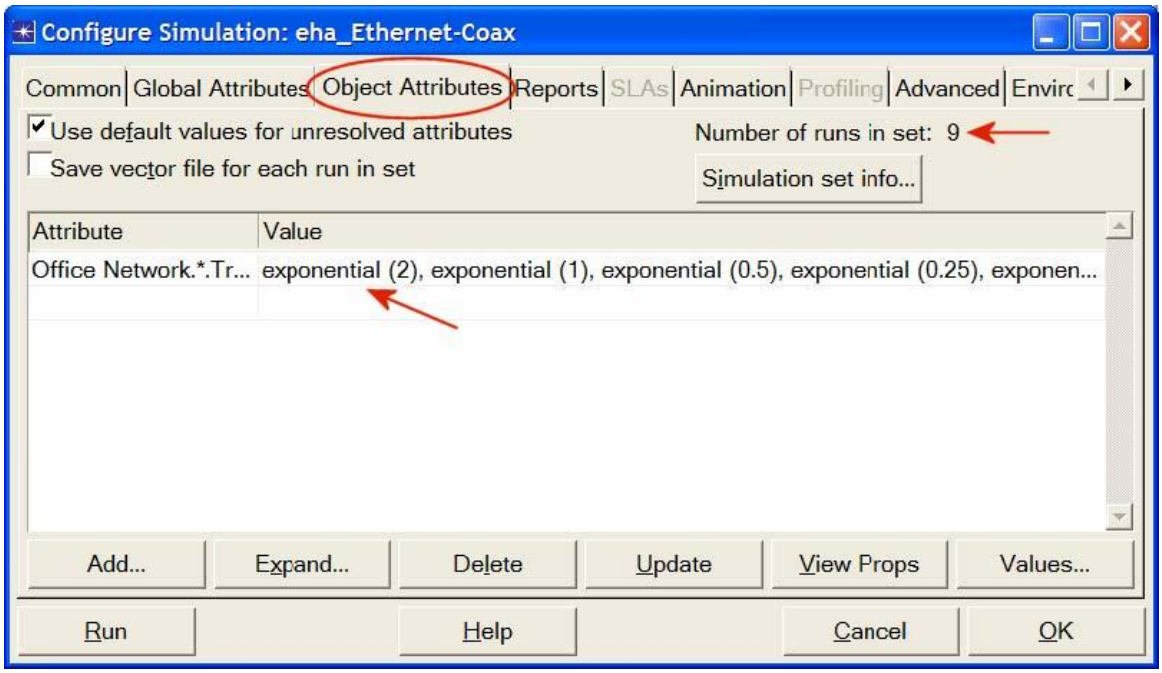
Натисніть OK.

5. Тепер Ви повинні бачити ***Office Network. *. Traffic Generation Parameter*** ... в списку параметрів моделювання. Клацніть на цьому параметрі, щоб вибрати його ⇒ Натисніть кнопку ***Values*** діалогового вікна.

6. Додайте наступні дев'ять значень. (Зауважте: щоб додати перше значення, двічі клацніть на перше значення в колонці ***Values*** ⇒ Введіть "***exponential (2)***" в текстове поле і натисніть Enter. Повторіть це для всіх дев'яти значень).



7. Натисніть OK. Тепер погляньте на правий верхній кут діалогового вікна ***Simulation Configuration*** і переконайтеся, що ***Number of runs in set*** встановлено в 9



8. Для кожного з дев'яти проходів моделювання нам потрібно, щоб програма моделювання зберегла скалярні значення, які представляють середнє

завантаження мережі і середню пропускну здатність мережі. Щоб зберегти ці скаляри, ми повинні налаштувати програму моделювання на збереження їх у файл. (Все описане в цьому пункті не потрібно для OPNET Modeler 14, цей пункт залишений для сумісності вказівок з більш старими версіями).

9. Натисніть ***OK*** і потім збережіть Ваш проект.

Вибір статистики

Щоб вибрати статистику, яка буде зібрана при моделюванні:

1. Клацніть ПКМ де-небудь в робочій області проекту (але не на одному з вузлів або зв'язків) і виберіть у контекстному меню ***Choose Individual Statistics*** $\Rightarrow$ Розкрийте ієрархію ***Global Statistics***.

a. Розкрийте ієрархію ***Traffic Sink*** $\Rightarrow$ Встановіть прапорець, наступний за ***Traffic Received (packets / sec)*** (переконайтеся, що Ви вибрали статистику з одиницями вимірювання пакетів / сек),

b. Розкрийте ієрархію ***Traffic Source*** $\Rightarrow$ Встановіть прапорець, наступний за ***Traffic Sent (packets / sec)***.

c. Натисніть ***OK***.

2. Тепер щоб зібрати середнє значення вищезгаданої статистики як скалярне значення до кінця кожного проходу моделювання:

a. Оберіть ***Choose Statistics (Advanced)*** в меню ***Simulation***.

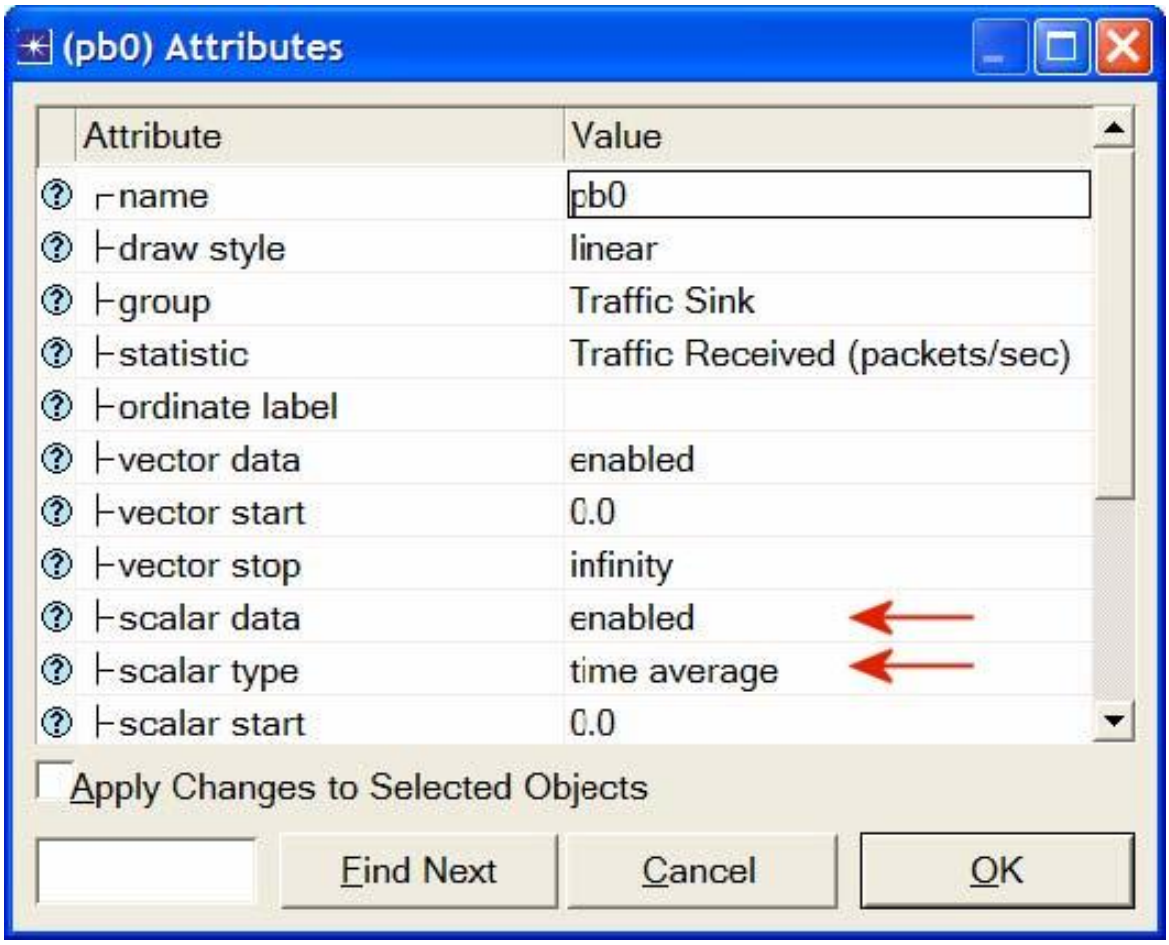
b. ***Traffic Sent*** та ***Traffic Received*** повинні з'явитися під ***Global Statistic Probes***.

c. Клацніть ПКМ на ***Traffic Received*** $\Rightarrow$ ***Edit Attributes***. Встановіть параметр ***scalar data*** в ***enabled*** $\Rightarrow$ Встановіть параметр ***scalar type*** в ***time average*** $\Rightarrow$ Порівняйте з наступним малюнком і натисніть ***OK***.

d. Повторіть попередній крок для ***Traffic Sent***.

e. Виберіть зберегти в меню ***File*** у вікні ***Probe Model*** і потім закрийте це вікно.

f. Тепер Ви повернулися до ***Project Editor***. Переконайтеся, що зберегли Ваш проект.



Запуск моделювання

Щоб запустити моделювання:

1. Натисніть кнопку ***Configure / Run DES Simulation*** ⇒ Переконайтеся, що ***Duration*** встановлено в 15 секунд (не годин) ⇒ Натисніть ***Run***. В залежності від швидкості вашого процесора моделювання може зайняти декілька хвилин.
2. Тепер програма моделювання закінчила дев'ять проходів, по одному для кожного значення параметра ***Interarrival Time***, що представляє завантаження мережі. Зверніть увагу, що кожен послідовний прохід займає більше часу, так як інтенсивність трафіку збільшується.

3. Після дев'яти повних проходів моделювання, натисніть ***Close***.

4. Збережіть ваш проект.

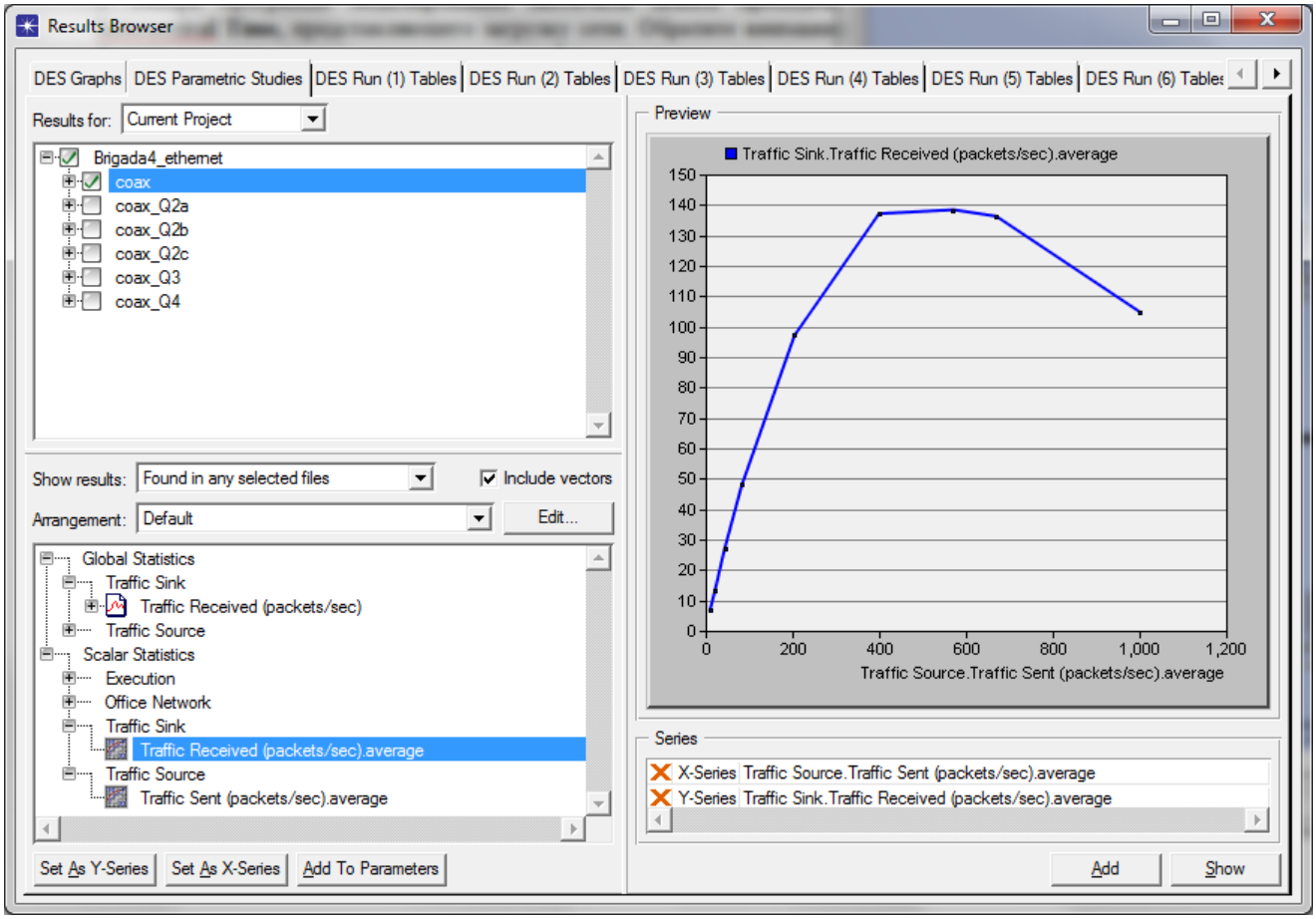
Перегляд результатів

Щоб переглянути та проаналізувати результати:

1. Виберіть ***View Results*** в меню ***Results***.

2. Відкриємо другу вкладку - ***DES Parametric Studies***, виберемо потрібний сценарій і встановимо дані для осі ***X-Traffic Source*** і для осі ***Y - Traffic Sink*** як показано на рис.

3. Одержаний графік повинен бути схожий на наступний:



ЗАВДАННЯ НА РОБОТУ

1) Поясніть графік, який ми отримали при моделюванні, який показує залежність між отриманими і посланими пакетами. Чому пропускна здатність знижується, коли завантаження є або дуже низьким або дуже високим?

2) Створіть три дубліката сценарію моделювання, реалізованого в цій лабораторній роботі. Назвіть ці сценарії Coax_Q2a, Coax_Q2b, and Coax_Q2c. Встановіть параметр ***Interarrival Time*** для ***Packet Generation Arguments*** всіх вузлів (упевніться, що вибрали ***Apply Changes to Selected Objects***, коли будете редагувати параметр) в нових сценаріях наступним чином:

- Сценарій Coax_Q2a: ***exponential*** (0.1)
- Сценарій Coax_Q2b: ***exponential*** (0.05)
- Сценарій Coax_Q2c: ***exponential*** (0.025)

У всіх вищезгаданих нових сценаріях, відкрийте діалогове ***вікно Configure Simulation*** і з ***Object Attributes*** видаліть параметр з множинними значеннями (єдиний параметр, показаний у списку).

Оберіть наступну статистику для вузла 0: Ethcoax → ***Collision Count.*** Переконайтеся, що обрана наступна глобальна статистика:

Global Statistics → Traffic Sink → Traffic Received (packet/sec). (Дивіться розділ лабораторної «Вибір Статистики»).

Запустіть моделювання для всіх трьох нових сценаріїв. Отримайте два графіки: один, щоб порівняти кількість колізій вузла 0 в цих трьох сценаріях, і другий, щоб порівняти отриманий трафік в цих трьох сценаріях. Поясніть графіки і прокоментуйте результати. (Примітка: Щоб порівнювати результати, Ви повинні вибрати ***Compare Results*** в меню ***Results*** після виконання моделювання).

3) Щоб вивчити вплив числа станцій на роботу сегмента мережі ***Ethernet,*** створіть дублікат сценарію Coax_Q2c, який Ви створили в другому завданні. Назвіть новий сценарій Coax_Q3. У новому сценарії видаліть вузли з непарним

номером, у загальній складності 15 вузлів (вузол 1, вузол 3, ..., і вузол 29). Проведіть моделювання для нового сценарію. Побудуйте графік, який порівнює кількість колізій вузла 0 в сценаріях Coax_Q2c і Coax_Q3. Поясніть графік і прокоментуйте результати.

4) У моделюванні використовується розмір пакета 1024 байта (Примітка: Кожен пакет Ethernet може містити до 1500 байтів даних). Щоб вивчити вплив розміру пакета на пропускну здатність створеної мережі Ethernet, створіть дублікат сценарію Coax_Q2c, який Ви створили в завданні 2. Назвіть новий сценарій Coax_Q4. У новому сценарії використовуйте розмір пакета 512 байтів (для всіх вузлів). І для Coax_Q2c, і для сценаріїв Coax_Q4 виберіть наступну глобальну статистику: ***Global Statistics → Traffic Sink → Traffic Received (bits / sec).*** Повторно запустіть моделювання сценаріїв Coax_Q2c і Coax_Q4. Побудуйте графік, який порівнює пропускну здатність, виражену в пакетів / сек, і інший графік, який порівнює пропускну здатність, виражену в біт / сек в сценаріях Coax_Q2c і Coax_Q4. Поясніть графіки і прокоментуйте результати.

ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ

Підготуйте звіт, виконаний за рекомендаціями до лабораторної роботи. Звіт повинен включати відповіді на вищезгадані питання, а також графіки, які Ви отримали при моделюванні сценаріїв. Проаналізуйте результати, які Ви отримали і порівняйте ці результати з очікуваними. Включіть до звіту будь-які аномалії або незрозумілу з Вашої точки зору поведінку.

Лабораторна робота № 3

TOKEN RING. МЕРЕЖА МНОЖИННОГО ДОСТУПУ З КОНТРОЛЕМ ДОСТУПУ ДО ПЕРЕДАВАЛЬНОЇ СЕРЕДОВИЩІ

Мета роботи. Демонстрація застосування мереж Token Ring. Оцінка продуктивності мереж Token Ring для при різних сценаріях за допомогою моделювання.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Мережі token ring складаються з безлічі вузлів, з'єднаних у кільце. Кільце - це середа з детермінованим доступом. Технологія token ring містить розподілений алгоритм, який контролює кожен вузол на можливість передачі. Всі вузли передають усі карди, і вузол, визначений як вузол-одержувач у заголовку кадру, зберігає копію карда. У зв'язку з особливістю побудови кільця, збій будь-якого вузла або зв'язку приведе в неробочий стан всю мережу. Ця проблема може бути вирішена використанням зірки, як топології, де вузли з'єднані в token ring концентратор. Token ring концентратор працює як реле, і відомий також під назвою multistation access unit (MSAU). MSAU використовуються майже завжди, тому що забезпечують надійність і легкість додавання і видалення вузлів.

Маркер (token) - спеціальна послідовність біт, яка циркулює в кільці, кожен вузол отримує та передає маркер наступному. Коли вузол, у якого є кадр для передачі, отримує маркер, він вилучає маркер з кільця і замість маркера вставляє свій кадр в кільце. Коли кадр повертається до відправника, відправник вилучає кадр із кільця і знову повертає в кільце маркер. Час утримання маркера (token holding time або THT) - це час, протягом якого вузол може утримувати маркер. З цього визначення випливає, що THT має вплив на використання і

рівноправність вузлів мережі, де використання це міра виміру пропускної здатності мережі, яка доступна в даному кільці.

У цій лабораторній роботі, ви побудуєте мережу token ring яка складається з 14 вузлів, з'єднаних в зірку. Пропускна здатність кожного лінка - 4 Mbps. Ви вивчите, як завантаженість мережі і THT впливають на використання мережі та затримки в ній.

МЕТОДИЧНІ ВКАЗІВКИ

Створення Нового Проекту

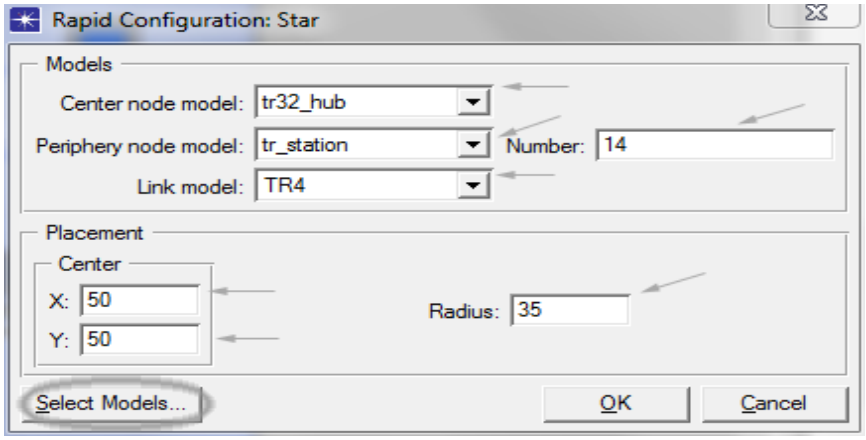
Для створення нового проекту мережі token ring необхідно зробити наступне:

1. Запустіть OPNET Modeler => Оберіть ***New*** з вкладки ***File*** в головному меню.
2. Виберіть ***Project*** і натисніть ***OK*** => Назвіть свій проект <Ваші ініціали> _Token і сценарій ***Balanced*** => Натисніть ***OK***.
3. У діалозі ***Startup Wizard: Initial Topology*** перевірте вибрано ***Create Empty Scenario*** => Натисніть ***Next*** => Виберіть ***Office*** для вказівки розміру мережі => Натисніть ***Next*** три рази => Натисніть ***OK***.
4. Виберіть ***Object Palette*** і збережіть свій проект.

Створення мережі

Для створення нашої мережі token ring необхідно:

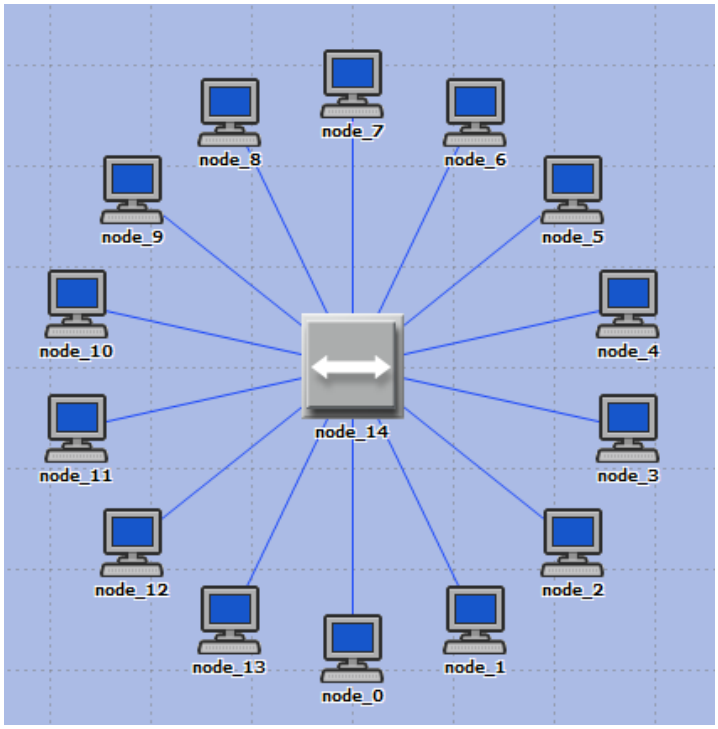
1. Виберіть ***Topology => Rapid Configuration***. З випадного меню виберіть ***Star*** і натисніть ***OK***.
2. Натисніть кнопку ***Select Models*** в діалозі ***Rapid Configuration***. З випадного меню ***Model List*** виберіть ***token_ring*** і натисніть ***OK***.
3. У діалозі ***Rapid Configuration*** встановіть наступні значення



Модель вузла tr_32hub - це концентратор token ring, що підтримує до 32 підключень з пропускною здатністю 4 і 16 Mbps. Концентратор надсилає вхідні пакети на наступний порт. Черги пакетів відсутні. Час обробки пакетів на концентраторі дорівнює нулю.

TR4 з'єднує 2 вузла мережі token ring на швидкості 4 Mbps

Тепер ви створили мережу, яка виглядає наступним чином



Перевірте чи зберегли ви проект.

Налаштування вузлів мережі

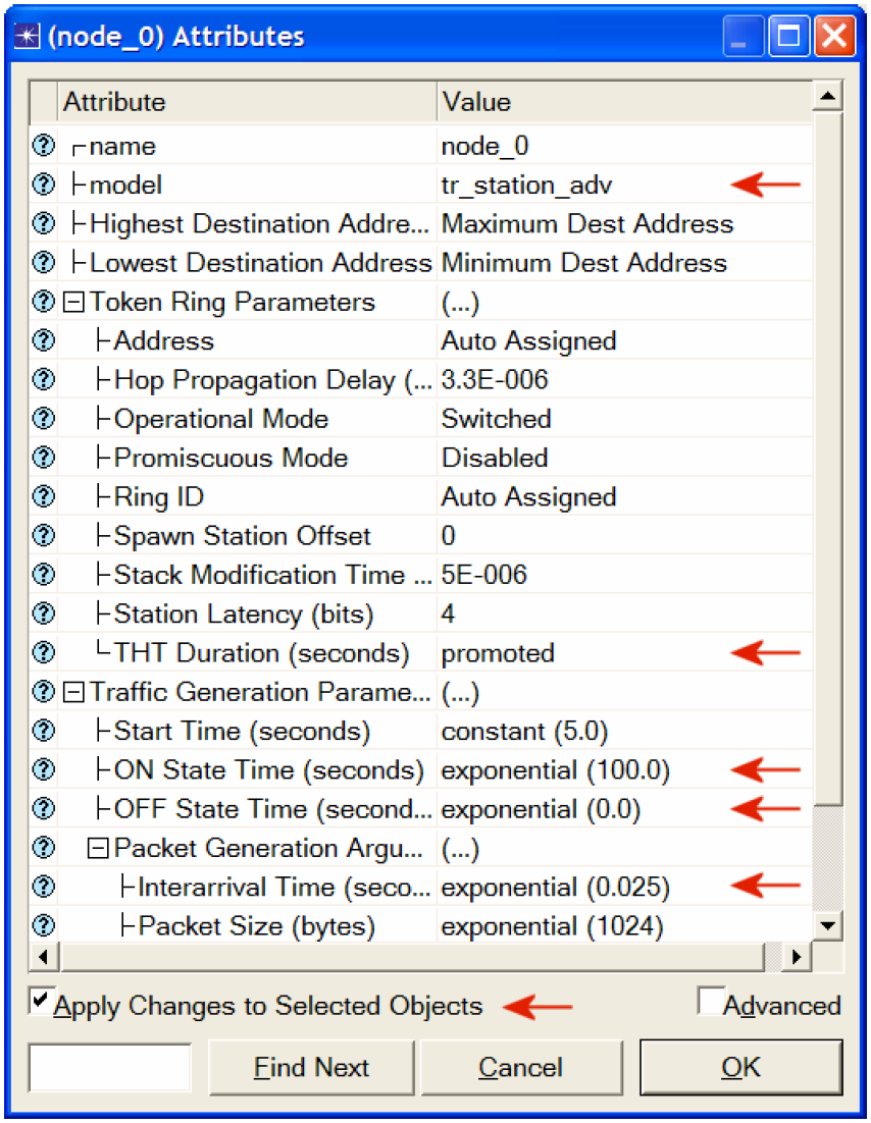
У даному пункті ви налаштуєте значення THT вузлів і, відповідно, трафік які вони генерують. Щоб налаштувати THT вузлів вам необхідно використовувати модель вузлів ***tr_station_adv***, замість поточної моделі - ***tr_station***.

1. Натисніть ПКМ на будь-якому з 14 вузлів мережі => Виберіть ***Select Similar Nodes***. Тепер вибрані всі вузли мережі.

2. Натисніть ПКМ на будь-якому з 14 вузлів мережі => ***Edit Attributes***.

   а) Виберіть ***Apply Changes*** в діалозі ***Selected Objects***. Це важливо для уникнення перенастроювання кожного вузла окремо.

   Малюнок, наведений нижче показує значення, які ми змінимо в кроках 3-6



THT (token holding time-час утримання маркера) визначає найбільший час використання маркера MAC'ом до його звільнення.

Interarrival time - час між вдалими формуваннями пакетів в "ON" стані.

3. Натисніть на змінну ***tr_station*** і виберіть ***Edit*** з випадаючого меню. Потім виберіть ***tr_station_adv*** з випадаючого меню.
4. Що б протестувати мережу для різних значень ***THT***, необхідно встановити параметр ***THT***. Це дозволить призначати різні значення параметру ***THT***.

   а. Розкрийте гілку ***Token Ring Parameters***

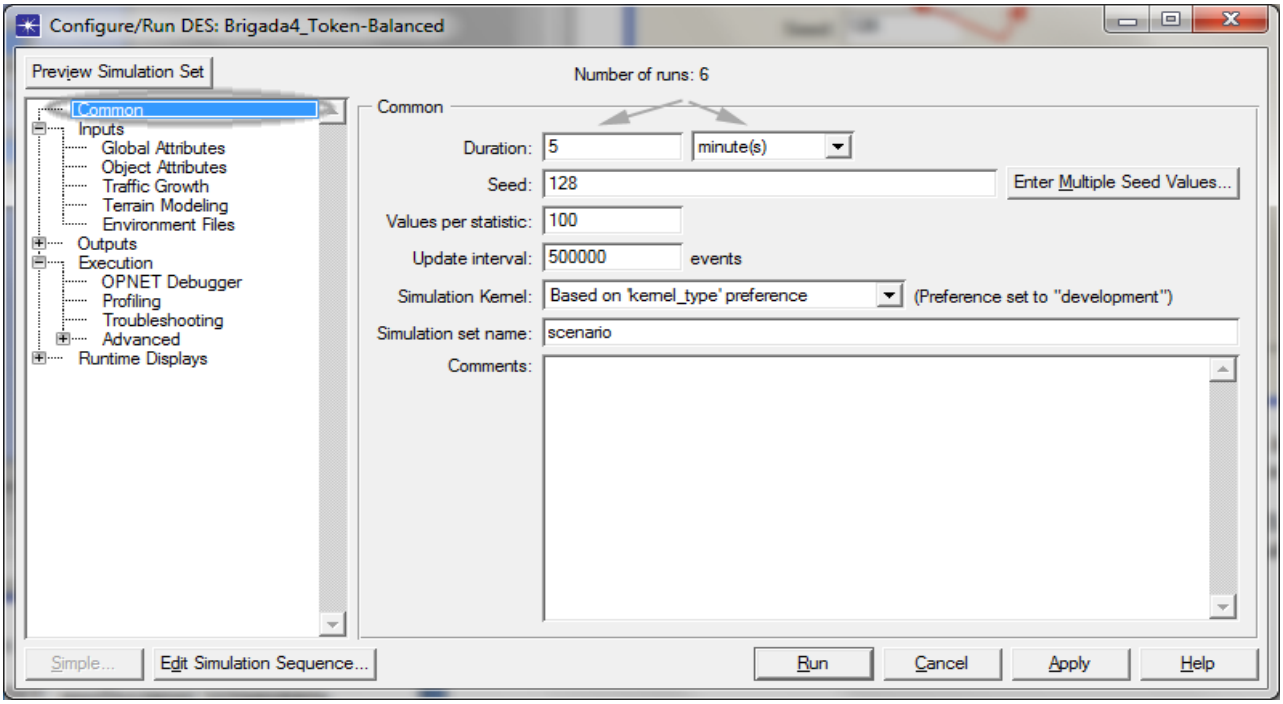
   б. ПКМ на ***THT Duration*** вибрати ***Promote Attribute to Higher Level***

5. Розкрийте гілку ***Traffic Generation Parameters*** призначте ***exponential (100)*** для ***ON State Time*** атрибута, призначте ***exponential (0)*** для ***OFF State Time*** атрибуту (примітка: пакети формуються тільки в стані "***ON***").
6. Розкрийте гілку ***Packet Generation Arguments*** призначте ***exponential (100)*** для параметра ***Interarrival Time***.
7. Натисніть ***OK*** для повернення в редактор проектів (***Project Editor***).
8. Збережіть проект.

Налаштування моделювання

Для контролю продуктивності мережі для різних ТНТ, необхідно провести моделювання кілька разів з різними значеннями ТНТ. Є простий спосіб налаштування. Для цього, раніше зустрінутому параметру ***THT Duration*** необхідно призначати різні значення:

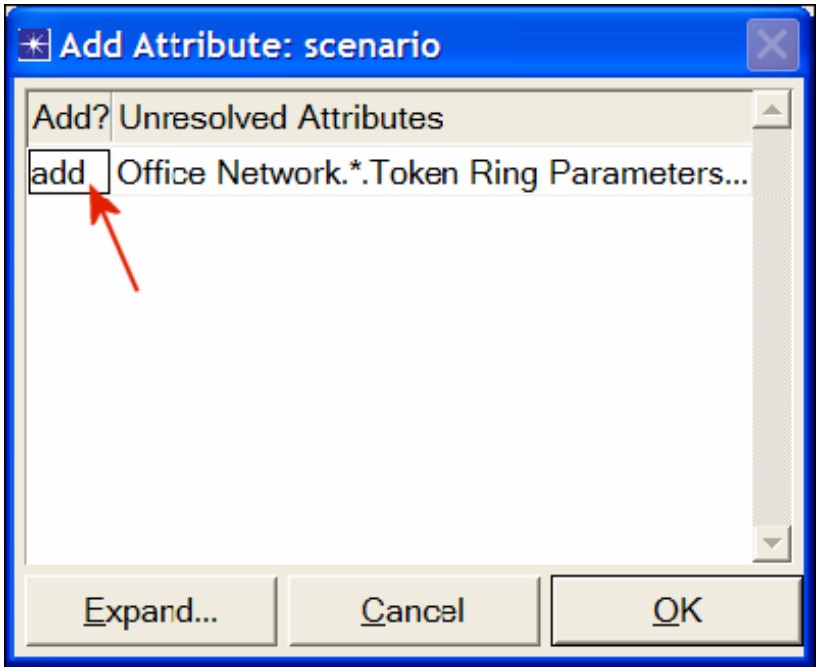
1. Натисніть кнопку ***Configure / Run Simulation***: 
2. Переконайтеся, що обрана закладка ***Common*** і присвойте параметру Duration значення 5 хвилин



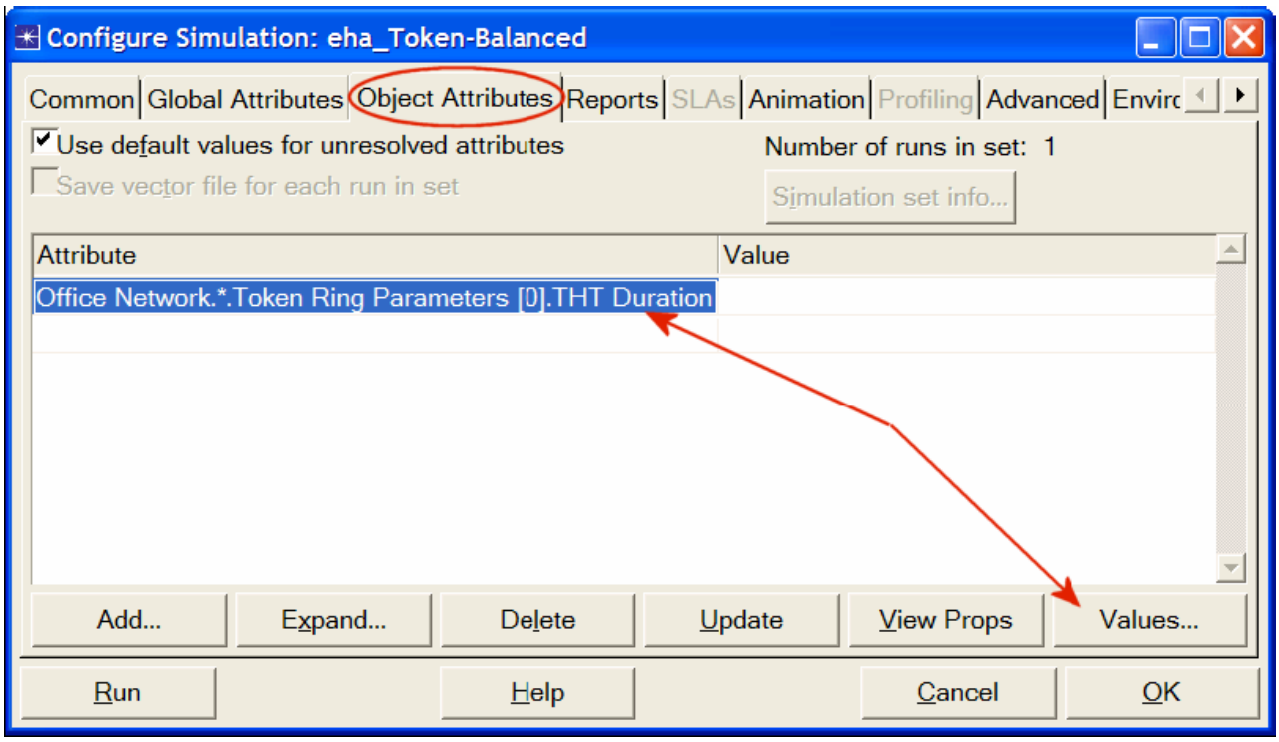
3. Виберіть вкладку ***Object Attributes*** і натисніть кнопку ***Add***.

4. Як показано далі в діалоговому вікні ***Add Attribute***, необхідно додати значення ***THT Duration*** для всіх вузлів. Для цього:

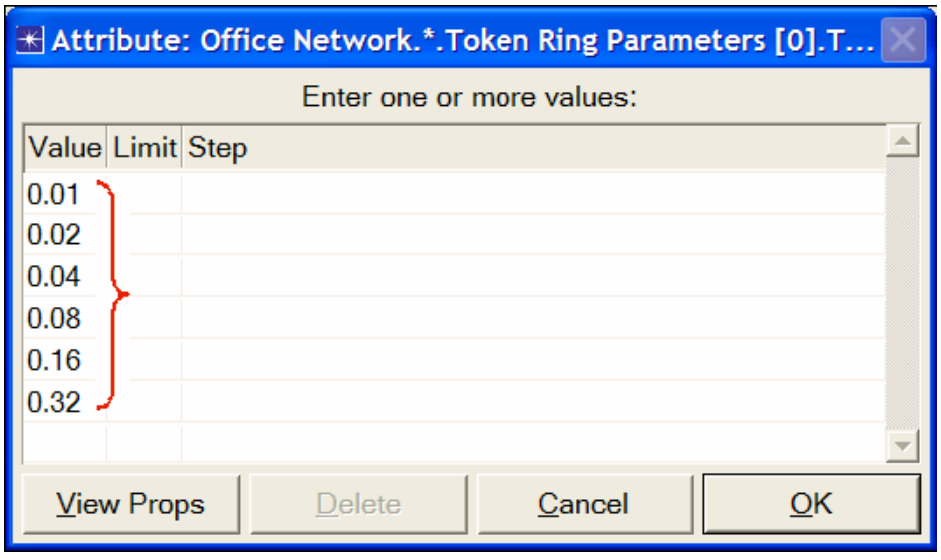
а. Додайте невизначене значення: ***Office Network. *. Token Ring Parameters [0]. THT Duration*** натисканням на відповідне поле в колонці **Add.** Натисніть ***OK***.



5. Тепер знайдіть ***Office Network. *. Token Ring Parameters [0]. THT Duration*** в списку параметрів об'єктів моделіровання. Натисніть на значення, а потім кнопку ***Values*** як показано нижче.

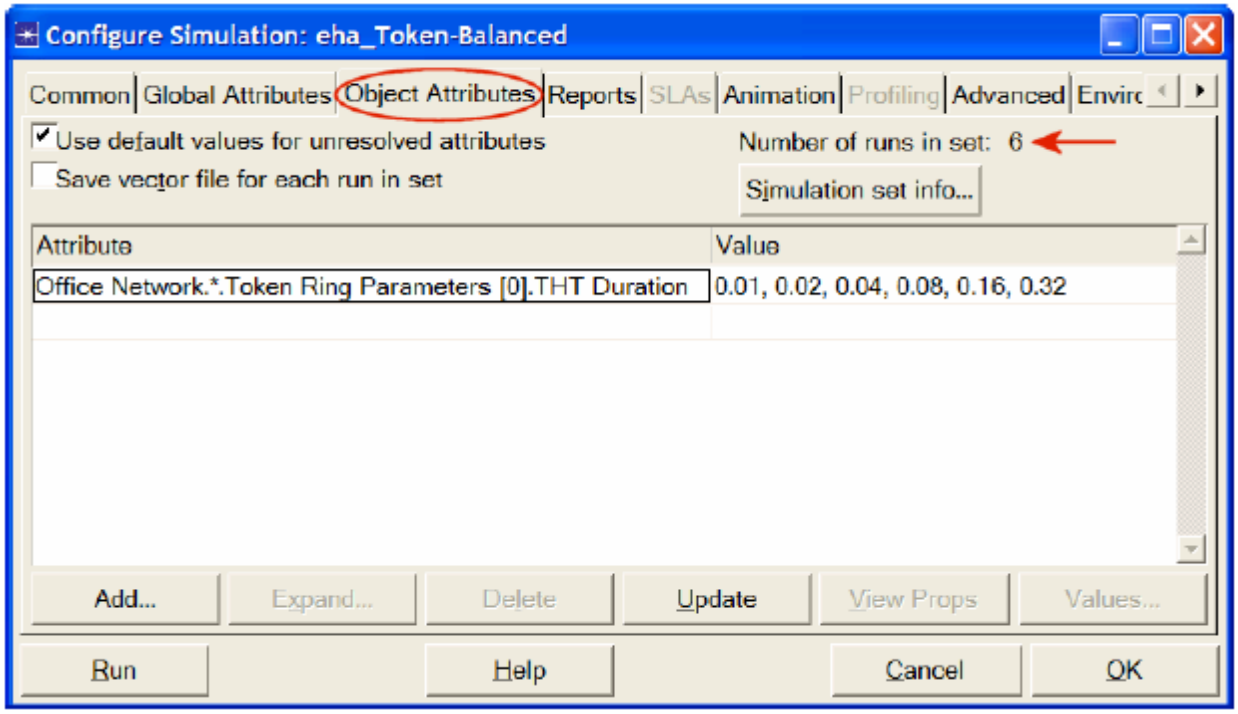


6. Додайте наступні 6 значень (Примітка: Додати перше значення можна за подвійним натискання миші на першому полі колонки ***Value***. Наберіть "0.01" і натисніть ***Enter***. Повторити дії для всіх шести значень).



7. Натисніть ***OK***. Тепер подивіться у верхній правий кут діалогового вікна ***Simulation Configuration*** і переконайтеся, що кількість запусків (***Number of runs***

in set) дорівнює шести (для OPNET Modeler 14 ви знайдете кількість запусків в вкладці ***Common*** над полем ***Duration***)



8. Натисніть ***OK*** для збереження проекту.

Збір статистичних даних

Для отримання статистичних даних в результаті моделювання, необхідно виконати наступне:

1. Натиснути ПКМ миші в будь-якому місці проекту (але не на зв'язку або ребрі) і виберіть ***Choose Individual Statistics*** з випадаючого меню

a. Виберіть ***Global Statistics***:

- Виберіть ***Traffic Sink*** і натисніть на чекбокс біля ***Traffic Received (packets / sec)***.
- Виберіть ***Traffic Source*** і натисніть на чекбокс біля ***next to Traffic Sent (packets / sec)***.

b. Виберіть ***Node Statistics***:

- Виберіть ***Token Ring*** і натисніть на чекбокс біля ***Utilization***.

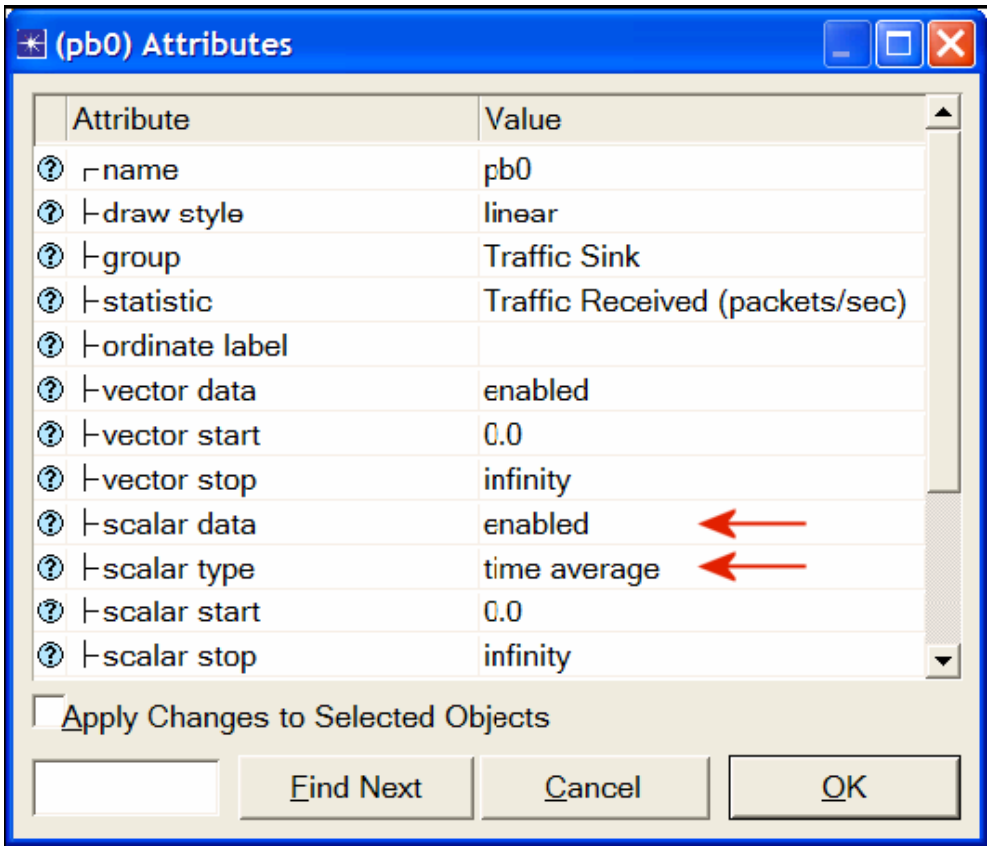
c. Натисніть ***OK***.

2. Тепер, для отримання середнього значення перерахованих вище характеристик, після кожного запуску моделювання, необхідно виконати наступне:

a. Виберіть ***Choose Statistics (Advanced)*** з меню ***Simulation***.

b. Під ***Global Statistic Probes*** повинні тепер з'явитися ***Traffic Sent*** і ***Traffic Received***. Також має з'явитися поле ***Utilization*** біля ***Node Statistics Probes***.

c. Натисніть правою кнопкою на полі ***Traffic Received - Edit Attributes***. Встановіть поле ***scalar Data*** в ***enabled***, встановіть поле ***scalar type*** в ***time average***. У результаті повинно вийти щось схоже на те, що зображено на наступному малюнку: Після цього натисніть ***OK***.



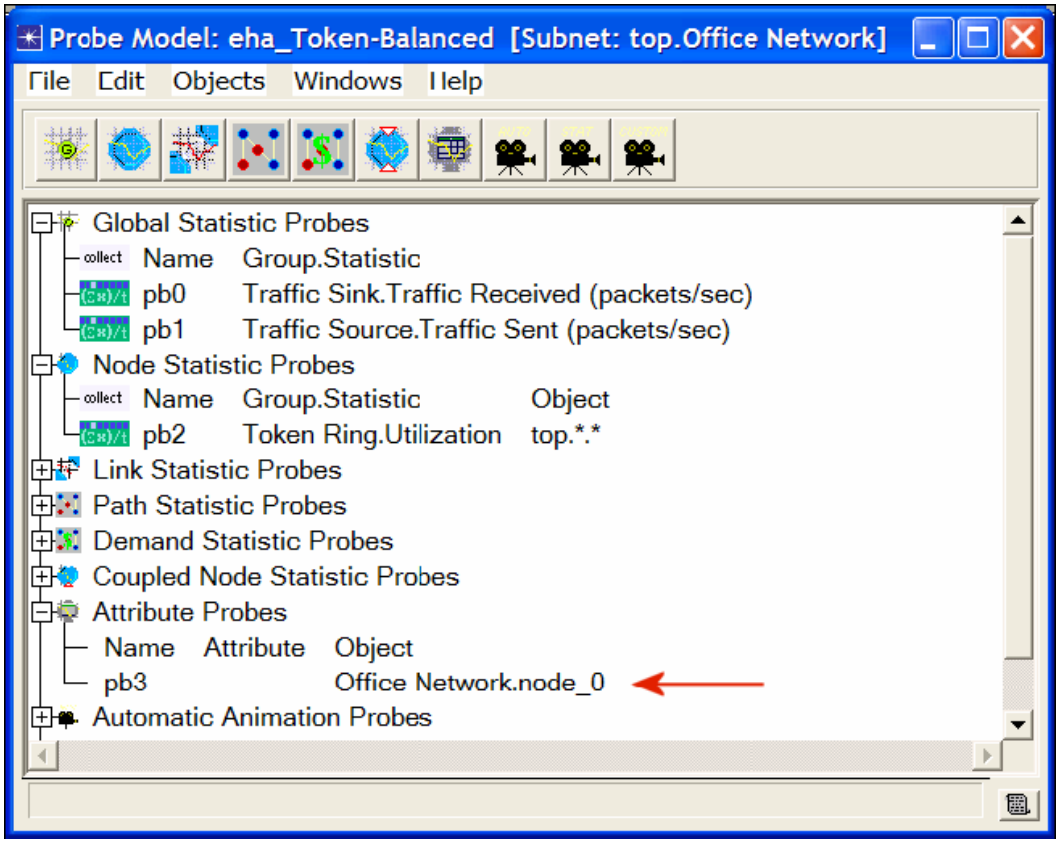
Для полів utilization і Traffic Sent виконайте попередній крок

3. Оскільки нам необхідно проаналізувати залежність ефективності мережі від ***THT***, то ***THT*** має бути доданий як вхідний параметр. Для цього робимо наступне:

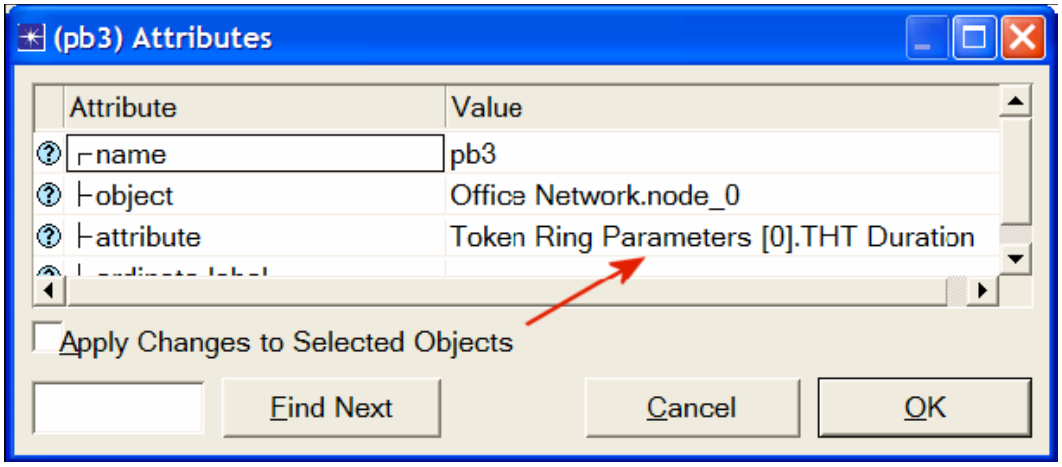
a. Вибираємо ***Create Attribute Probe*** з меню ***Objects***. Тепер створене нове поле в ***Attribute Probes***, як і показано на малюнку.

b. Натискаємо ПКМ на щойно доданому полі і вибираємо C***hoose Attributed Object*** із випадаючого меню. Вибираємо ***Office Network***. Натискаємо на ***node_0***, і потім ***OK***.

c. знову натискаємо правою кнопкою на полі і вибираємо ***Edit Attributes*** з випадаючого меню.



Встановлюємо значення ***Token Ring Parameter [0]. THT*** в "***attribute***" так, як показано на малюнку і натискаємо ОК.

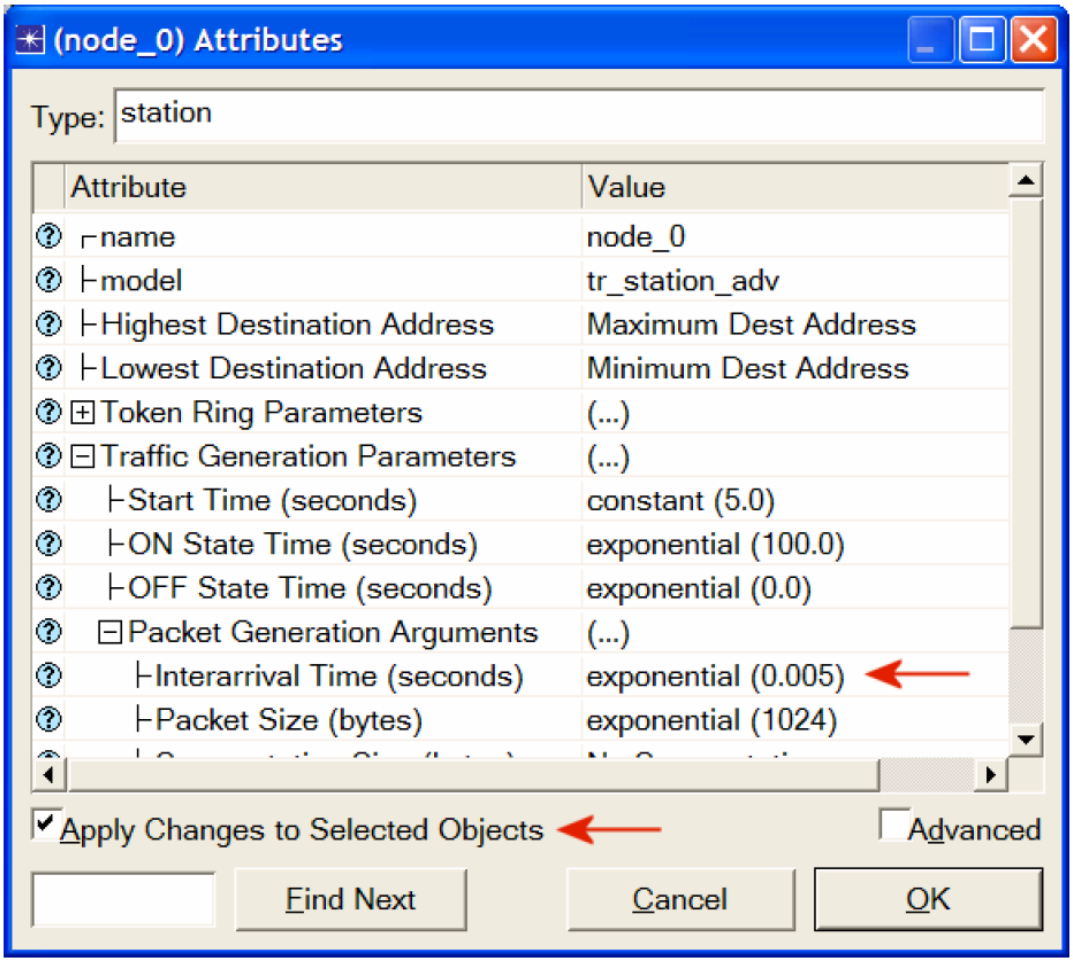


4. У вікні ***Probe Model*** в меню файл вибираємо зберегти, і потім закриваємо окно вікно.
5. Ви повернулися в ***Project Editor*** (Редактор проектів) Переконайтеся, що ви зберегли проект.

Дублювання сценарію

Сценарій мережі токен ринг, який ми тільки що здійснювали, балансує розподіл генерованого трафіку у всіх вузлах однаково. Щоб порівняти продуктивність створіть «незбалансований» сценарій, як зазначено нижче:

1. Виберіть ***Duplicate Scenario*** з меню ***Scenarios*** і дайте йому ім'я ***Unbalanced*** ⇒ Натисніть ***OK***.
2. Виберіть ***node_0*** і ***node_7*** клікаючи з натиснутим ***shift*** на кожному з вузлів ⇒ Клацання ПКМ на одному з вибраних вузлів і виберіть ***Edit Attributes*** ⇒ Розкрийте ієрархію ***Traffic Generation Parameters*** ⇒ Розкрийте ієрархію ***Packet Generation Arguments*** ⇒ Змініть значення атрибута ***Interarrival Time*** в ***exponential (0.005)***. Переконайтеся що поле ***Apply Changes to Selected Objects*** обрано перед натисканням кнопки ***OK***.



3. Виберіть всі вузли крім ***node_0*** і ***node_7*** ⇒ Натисніть ПКМ на одному з вибраних вузлів і виберіть ***Edit Attributes*** ⇒ Змініть значення атрибута ***Interarrival Time*** на ***exponential (0.075)***, як в попередньому кроці. Переконайтеся що поле ***Apply Changes to Selected Objects*** вибрано перед натисканням кнопки ***OK***.

4. Натисніть де завгодно в робочій області, для знять виділення з об'єктів.

5. Натисніть на кнопку ***Configure / Run Simulation***: ⇒ Натисніть на вкладку ***Advanced*** в діалозі ***Configure Simulation*** ⇒ Призначте <your initials>_Token_Unbalanced текстовому полю ***Scalar file***.

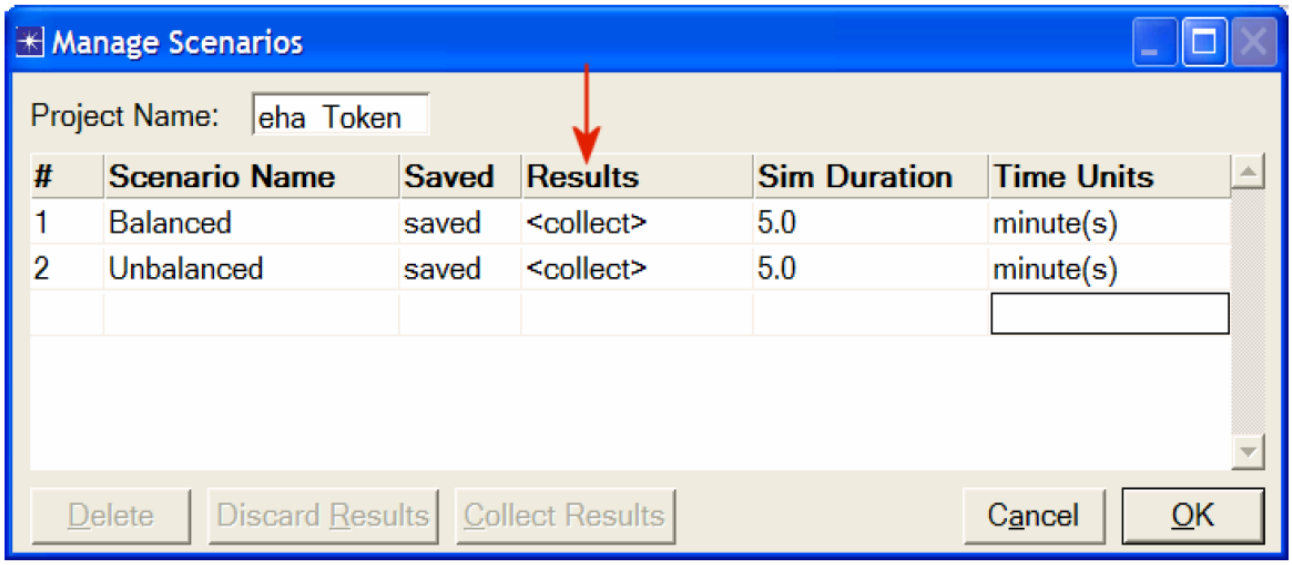
6. Натисніть ***OK***, щоб потім зберегти свій проект.

Запуск моделювання

Щоб одночасно запустити моделювання для обох сценаріїв:

1. Перейдіть до меню ***Scenarios*** ⇒ Виберіть ***Manage Scenarios***.

2. Змініть значення під колонкою ***Results*** на <collect> (або <recollect>) для обох сценаріїв. Порівняйте з наступною фігурою.



Натисніть OK, щоб виконати моделювання. В залежності від швидкості вашого процесора, це може зайняти кілька хвилин.

4. Після завершення 12 запусків, 6 для кожного із сценаріїв натисніть ***Close***.

5. Збережіть свій проект.

Коли ви повторно виконаєте моделювання, OPNET IT Guru "додасть" нові результати до існуючих результатів в скалярному файлі. Щоб уникнути цього видаліть скалярний файл перед новим запуском.

• Перейдіть в меню ***File*** ⇒ Виберіть ***Model Files*** ⇒ ***Delete Model File***s ⇒ Зі списку виберіть ***other model types*** ⇒ Виберіть (. os): ***Output Scalars*** ⇒ Виберіть скалярний файл, який потрібно видалити, у цій лабораторній це:

<your initials> _Token_Balanced_Scalar і

<your initials> _Token_Unbalanced_Scalar ⇒ НажмітеClick Close.

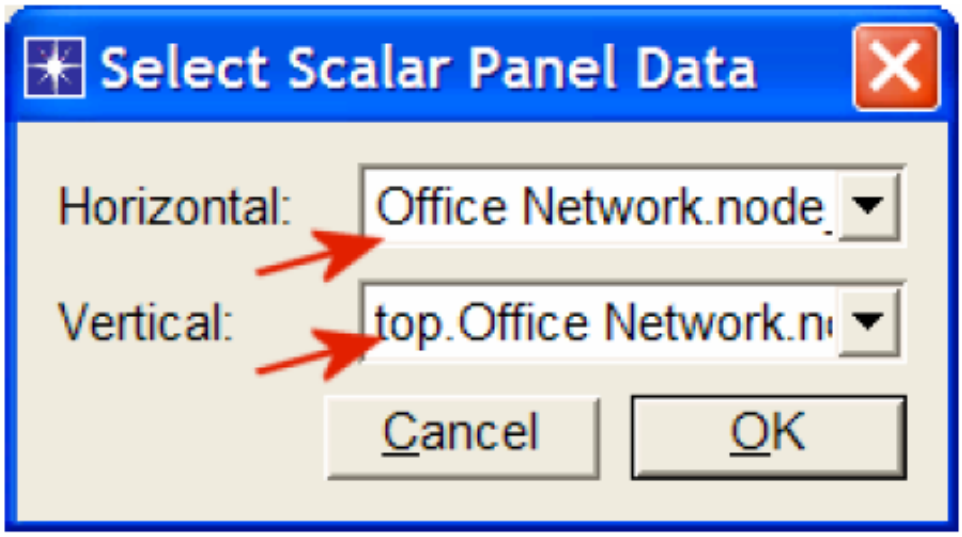
Перегляд результатів

Для перегляду та аналізу результату необхідно:

1. Виберіть ***View Results (Advanced)*** з меню ***Results***. Тепер утиліта ***Analysis Configuration*** - доступна.

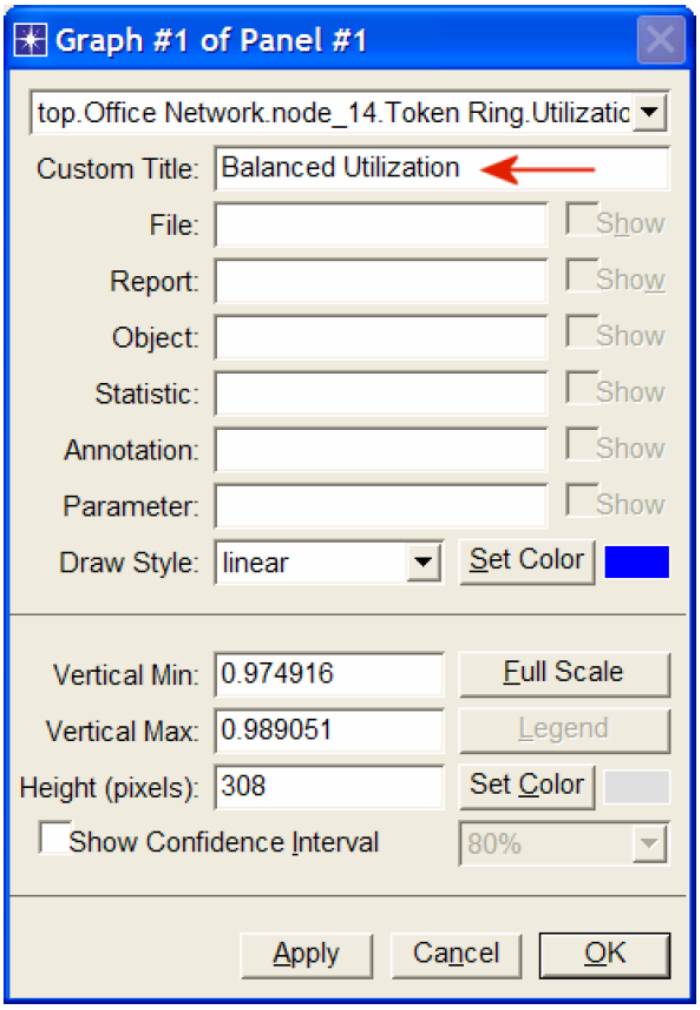
2. Ми зберегли середні результати у двох скалярних файлах, один для кожного із сценаріїв. Щоб завантажити скалярний файл для сценарію ***Balance***, виберіть ***Load Output Scalar File*** з меню ***File*** ⇒ Виберіть <your initials> _Token_Balanced із спливаючого меню.

3. Виберіть ***Create Scalar Panel*** з меню ***Panels*** ⇒ Виберіть скалярну панель даних, як показано в наступному діалоговому вікні: ***THT*** для ***Horizontal*** і ***Utilization*** для **Vertical**. (Примітка: Якщо будь-який з даних відсутній переконайтеся, що ви здійснили кроки 2.c і 2.d в ***Choose the Statistics section***.)

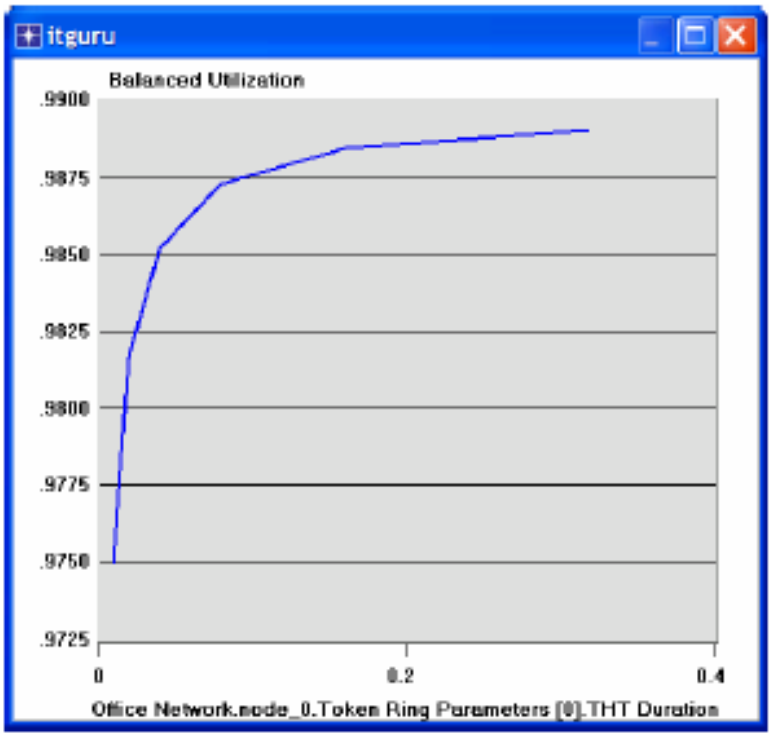


4. Натисніть ***OK***.

5. Для зміни заголовка графіка, клікніть ПКМ в області графіка і виберіть ***Edit Graph Properties*** ⇒ Змінити ***Custom Title*** на ***Balanced Utilization*** як показано.



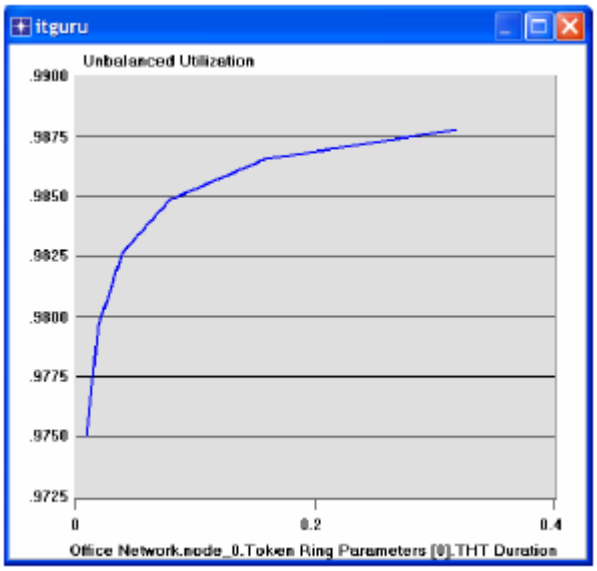
6. Клацніть ***OK***. Результуючий графік повинен бути схожим на графік показаний нижче. Не закриваючи графік продовжуйте з наступного кроку.



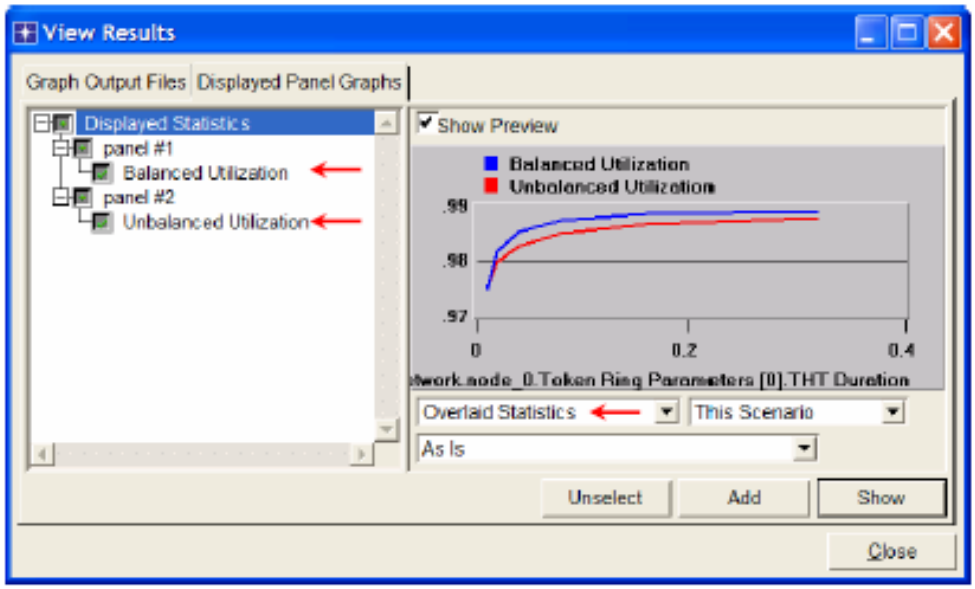
7. Для порівняння зі сценарієм ***Unbalanced***, завантажте його скалярний файл, виберіть ***Load Output Scalar File*** з меню ***File*** >> <ваші початкові> _Token_Unbalanced з випадаючого меню.

8. Виберіть ***Create Scalar Panel*** з меню ***Panels*** >> Виберіть панель скалярних даних як в кроці 3.

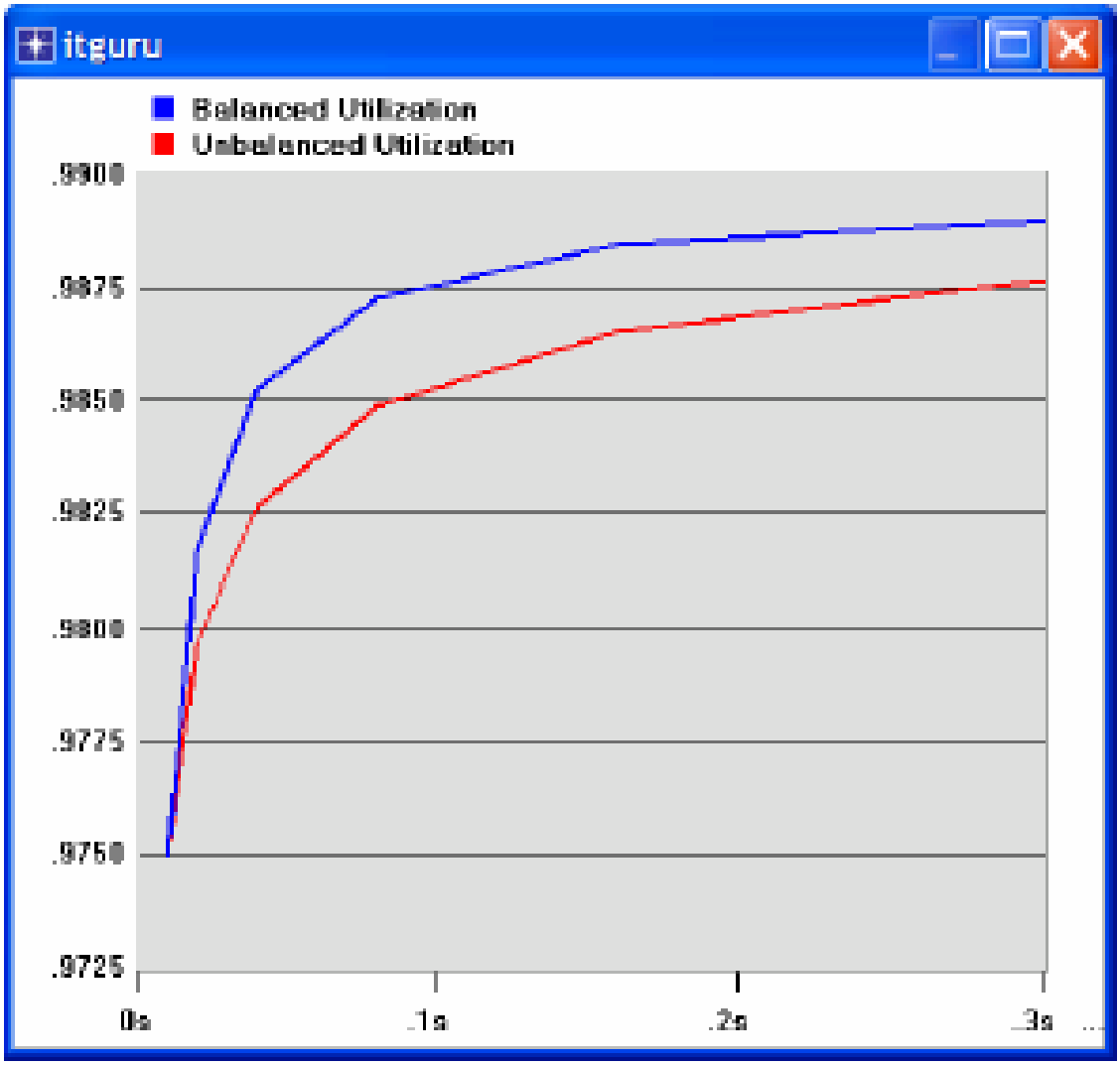
9. Виберіть ***OK*** >> Змініть назву графіка на ***Unbalanced*** як в кроці 5 >> Клацніть ***OK***. Результуючий графік повинен бути схожий на наведений нижче. Не закривайте цей графік і попередній і переходьте до наступного кроку.



10. Для комбінування графіків наведених нижче, на одному, виберіть ***Create Vector Panel*** з меню ***Panels*** клікніть на вкладці ***Display Panel Graphs*** виберіть ***Balanced*** і ***Unbalanced*** статистику, => виберіть ***Overlaid Statistics*** з випадаючого меню в правій нижній частині ділогового вікна.

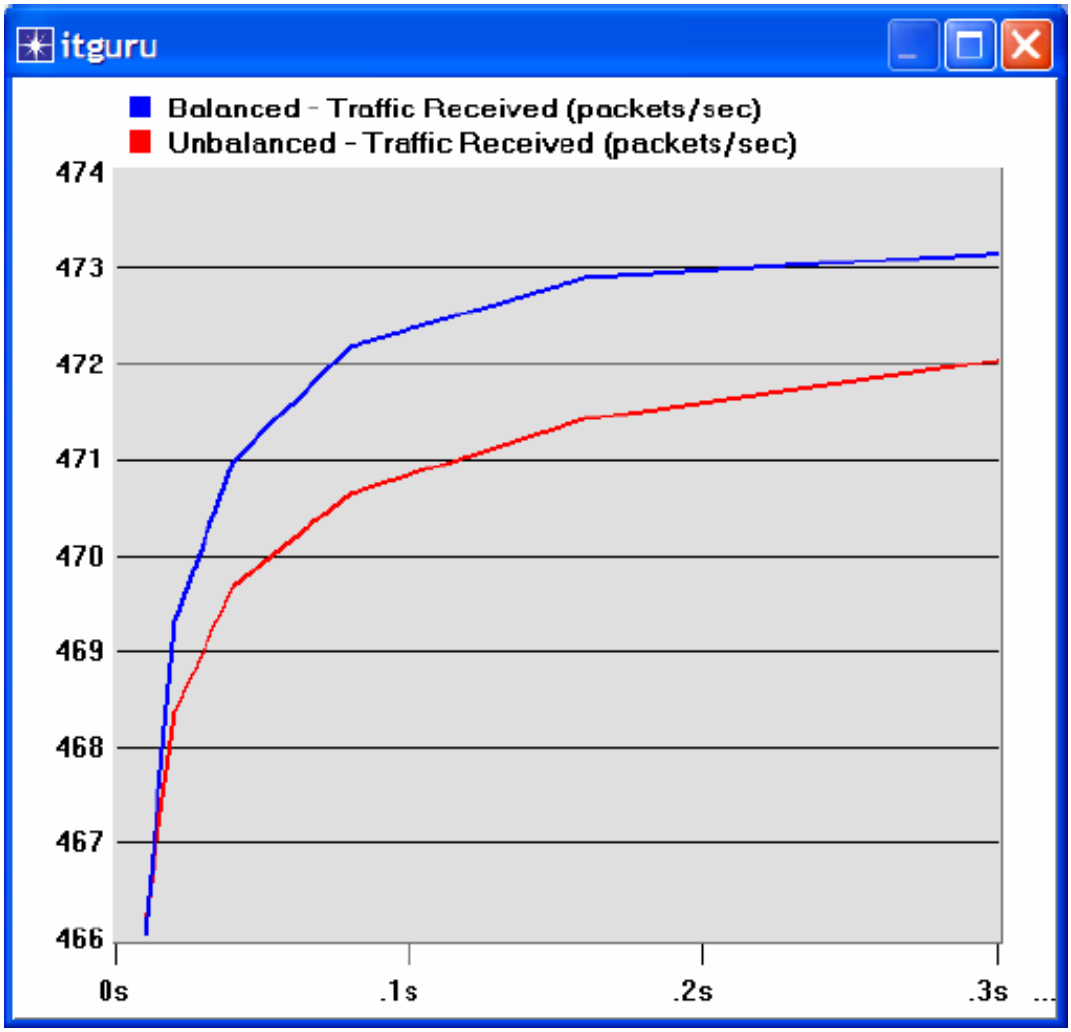


11. Клацніть ***Show*** і результуючий графік буде виглядати як нижче



12. Повторіть той же процес, тільки при впливі ***THT*** на прийнятий трафік (***Traffic Received***). Змініть назву графіків відповідним чином.

13. Результуючий графік, який об'єднує статистику по отримання трафіку для обох варіантів сценарію - збалансований (***Balanced***) і незбалансований (***UnBalanced***), має виглядати наступним чином:



Опис моделі ***Token Ring OPNET***: перебуваючи в меню ***Protocols***, вибрати ***Token Ring*** => ***Model Usage Guide***.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Чому утилізація збільшується при більш високих значеннях часу зберігання маркера (***THT***).

2. Створіть дублікат сценарію ***Balanced***. Назвіть його - Q2_HalfLoad. У цьому сценарії зменшите завантаженість мережі, тобто, навантаження від кожного вузла в мережі, на половину і повторіть симуляцію. Порівняйте утилізацію і прийнятий трафік в сценарії Q2_HalfLoad зі сценарієм ***Balanced***.

Поради:

- Зменшуючи навантаження від кожного вузла наполовину, необхідно, що б при цьому було збільшено вдвічі "***Interarrival Time***" в вузловому ***Packet Generation Arguments***.

- Не забудьте призначити певний "scalar file" для нового сценарію.

3. Створюєте дублікат сценарію ***Balanced***. Назва його - Q3_OneNode. У цьому сценарії реконфігуріруйте мережу так, щоб node_0 генерувала трафік такого навантаження, який генерували всі вузли в сценарії ***Balanced*** разом. Всі інші вузли від node_1 до node_13 трафік не генерують. Порівняйте утилізацію і прийнятий трафік в сценарії Q3_OneNode зі сценарієм ***Balanced***.

Поради:

- Один із шляхів примусити вузол не генерувати трафік - це встановити значення ***Start Time*** (це один з ***Traffic Generation Parameters***) в ***Never***.
- Не забувайте призначити певний "***scalar file***" для нового сценарію.

ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ

Підготуйте звіт, який виконаний за рекомендаціями до лабораторної роботи. Звіт повинен включати відповіді на вищезгадані питання, а також графіки, які Ви отримали при моделюванні сценаріїв. Проаналізуйте результати, які Ви отримали і порівняйте ці результати з очікуваними. Включіть до звіту будь-які аномалії або незрозумілу з Вашої точки зору поведінку.

Лабораторна робота № 4

ЗАСТОСУВАННЯ КОМУТАТОРІВ В МЕРЕЖАХ. РЯД ЛОКАЛЬНИХ МЕРЕЖ З'ЄДНАНИХ КОМУТАТОРАМИ

Мета роботи. Демонстрація застосування комутаторів у локальних мережах. Оцінка продуктивності різних способів з'єднання локальних мереж комутаторами і повторювачами.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Існує обмеження на кількість комп'ютерів, які можуть бути підключені до однієї мережі, а також обмеження на географічне рознесення мережі. Комутатори застосовуватися в мережах для з'єднання одного комп'ютера з іншим, навіть тоді, коли немає прямого з'єднання між цими комп'ютерами. Комутатор це пристрій, який має кілька входів і виходів і забезпечує передачу сигналу між комп'ютерами, які він з'єднує. Завданням комутатора є передача сигналу потрібному адресату.

Головне завдання, яке вирішує комутатор, визначення смуги пропускання його виходів. Якщо смуга пропускання виходу менше, ніж смуга пропускання вхідного сигналу, пакети повинні буферізіровать комутатором. Якщо це буде продовжуватися тривалий період часу, маршрутизатор буде відкидати пакети. Якщо пакети відкидаються занадто часто, кажуть що комутатор перевантажений.

У цій лабораторній розглядається побудова мереж за допомогою комутаторів і повторювачів. Повторювач відправляє пакет з входу на всі свої виходи незалежно від одержувача пакета. З іншого боку комутатор переправляє пакет його одержувачу або групі одержувачів. Ви вивчите, як пропускна здатність і колізії пакетів в комутованій мережі залежить від конфігурації мережі та типа перемикання використаних пристроїв.

МЕТОДИЧНІ ВКАЗІВКИ

Створити новий проект

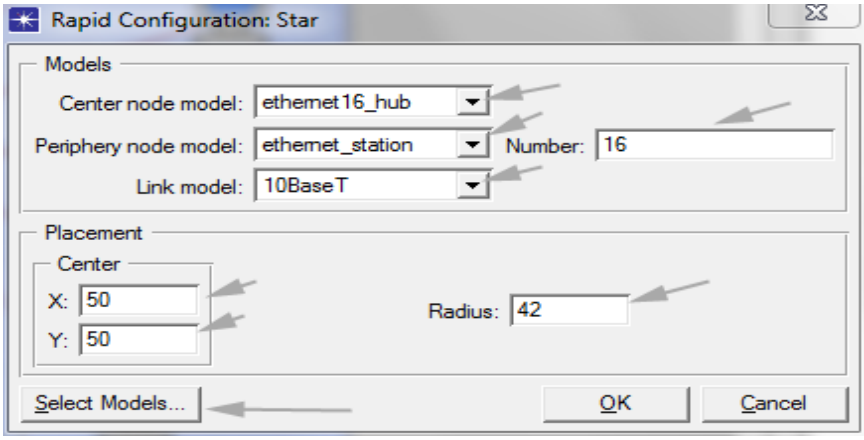
1. Запустити OPNET IT Guru Academic Edition -> Вибирати ***New*** з меню ***File***.
2. Вибрати ***Project*** і натиснути ***OK***, -> Назвати проект <ваші ініціали> _SwitchedLAN, і сценарій OnlyHub -> натиснути ***OK***.

3. У діалоговому вікні ***Startup Wizard: Initial Topology***, упевнитися, що відзначений пункт ***Create Empty Scenario***, -> натиснути ***OK*** -> вибрати ***Office*** зі списку ***Network Scale***. -> Натиснути ***Next***, три рази -> натиснути ***OK***.
4. Закрити діалогове вікно ***Object Palette***.

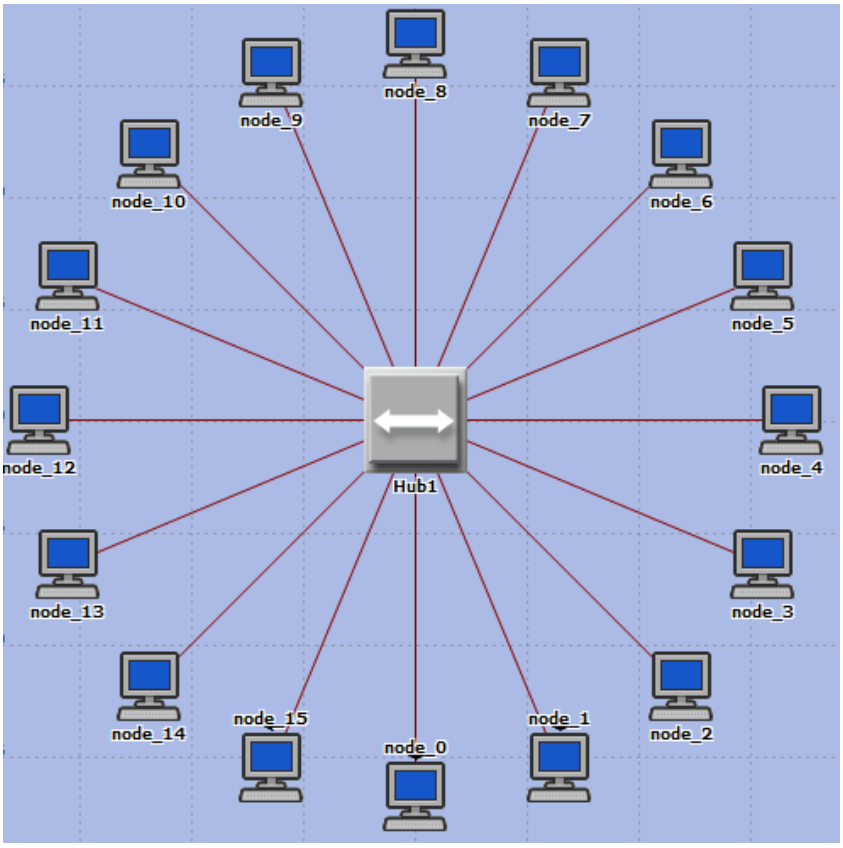
Створити мережу

Для створення нашої switched LAN:

1. Вибрати ***Topology*** -> ***Rapid Configuration***. З випливаючого меню вибрати ***Star*** і потім натиснути ***OK***.
2. Натисніть на кнопку ***Select Models*** в діалоговому вікні ***Rapid Configuration***. З випливаючого меню вибрати ***ethernet*** і натиснути ***OK***.
3. У діалоговому вікні ***Rapid Configuration***, встановити наступні п'ять значень: ***Center Node Model*** = ***ethernet16_hub***, ***Periphery Node Model*** = ***ethernet_station,*** ***Link Model*** = ***10BaseT***, ***Number*** = ***16***, ***Y*** = ***50***, і ***Radius*** = ***42*** -> натиснути ***OK***.



4. ПКМ натиснути на ***node_16 -> Edit Attributes*** -> змінити ім'я атірібута на ***Hub1*** і натиснути ***OK***.
5. Тепер мережа створена.
6. Зберегти проект.

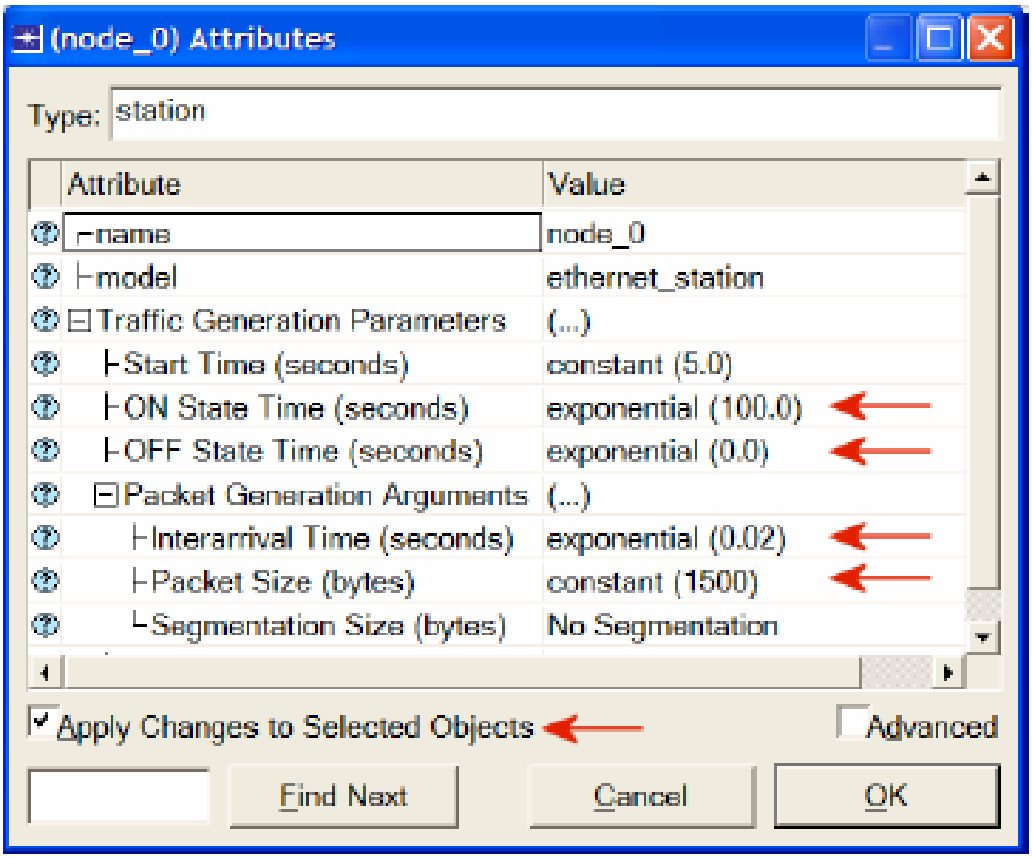


Конфігурування мережевих елементів

Тут ви налаштовуєте генеруємий трафік між станціями.

1. Клацніть ПКМ на будь-який з 16 станцій (від node_0 до node_15) => Оберіть ***Select Similar Nodes***. Тепер всі станції в мережі виділені.
2. Клацніть ПКМ на будь-який з 16 станцій => ***Edit Attributes***.

   а. Виділити прапорець ***Apply Changes*** в ***Selected Objects***. Це необхідно для уникнення реконфигурирования кожного елементу окремо.
3. Розгорніть ієрархію параметрів ***Traffic Generation Parameters*** і ієрархію параметрів ***Packet Generation Arguments*** => Встановіть наступні чотири значення:

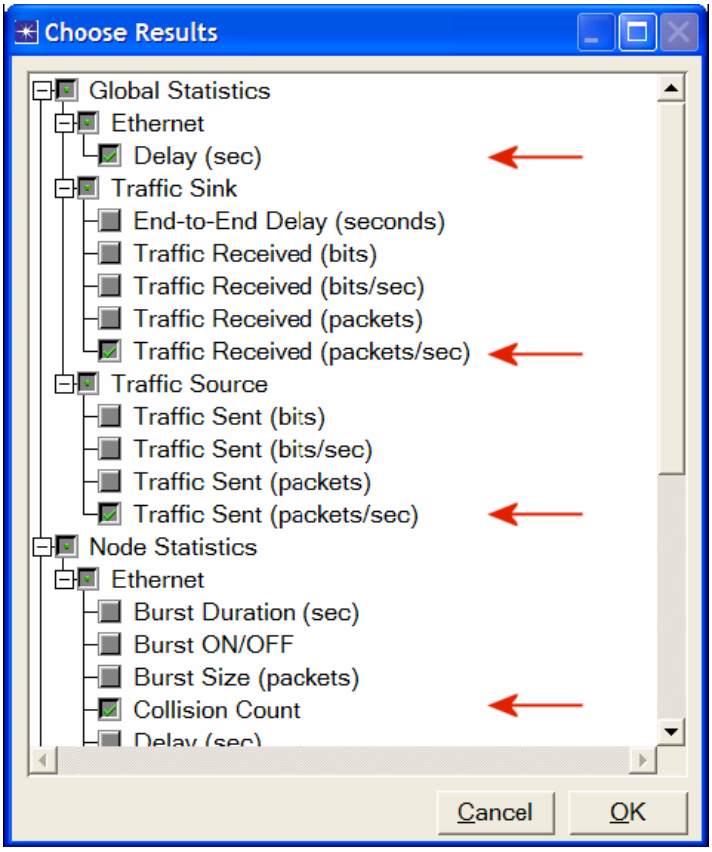


4. Натисніть ***OK*** для закриття вікна зміни параметрів. Збережіть свій проект.

Вибір статистики

Для вибору статистики, яка буде збиратися під час моделювання, необхідно:

1. Натисніть ПКМ в будь-якому місці вікна проекту і, з меню, вибрати пункт ***Choose Individual Statistics*** (Вибір індивідуальної статистики).
2. У вікні ***Choose Results*** (Вибір результатів), вибрати наступні 4 статистики:



Затримка Ethernet являє собою затримку всіх пакетів отриманих усіма станціями в мережі.

Вхідний трафік (пакетів в секунду) зменшує загальний трафік до всіх вузлів.

Вихідний трафік (пакетів в секунду) йде від джерел до всіх вузлів.

Кількість колізій - це число колізій, що відбуваються при передачі даних в мережах, заснованих на концентраторах (хабах).

3. Натисніть ***OK***.

Конфігурування режиму моделювання (*Simulation*):

Тут нам необхідно встановити час моделювання:

1. Натиснути на кнопку Конфігурування / Запуск (***Configure*** / ***Run Simulation***):
2. Встановити час моделювання 2.0 хвилини.
3. Натиснути ***OK***.

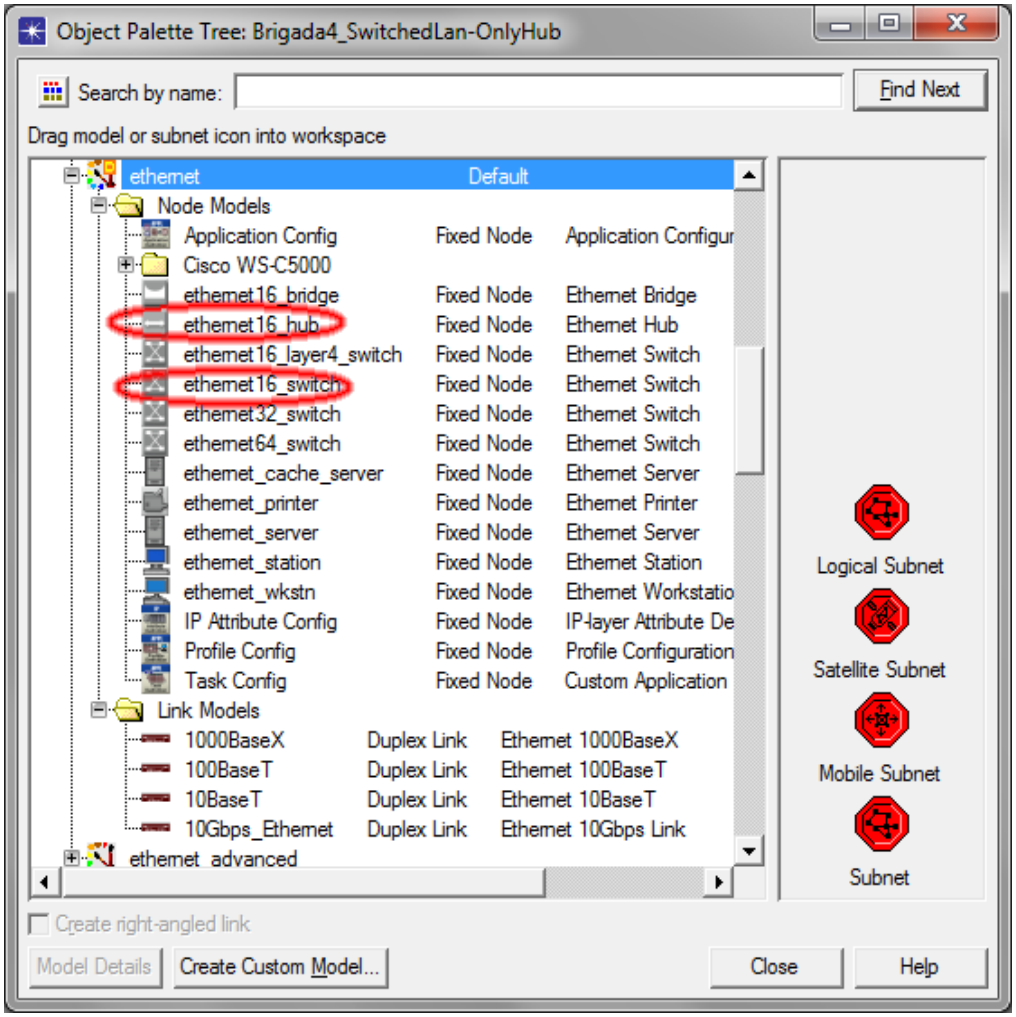
Дублікат сценарію

Мережа, яку ми тільки що створили, використовує тільки один концентратор для підключення 16 комп'ютерів. Нам необхідно створити іншу мережу, яка використовує комутатор, і поспостерігати, як це позначиться на продуктивності мережі. Для того, щоб зробити це, ми створимо дублікат поточної мережі:

1. Виберіть ***Duplicate Scenario*** з меню ***Scenarios*** і дайте йому ім'я ***HubAndSwitch*** і натисніть ***OK***.

2. Відкрийте ***Object Palette*** клацнувши на  цей значок. Переконайтеся в тому, що обрано ***Ethernet*** в спадному списку.

3. Нам необхідно помістити концентратор і комутатор в новий сценарій.



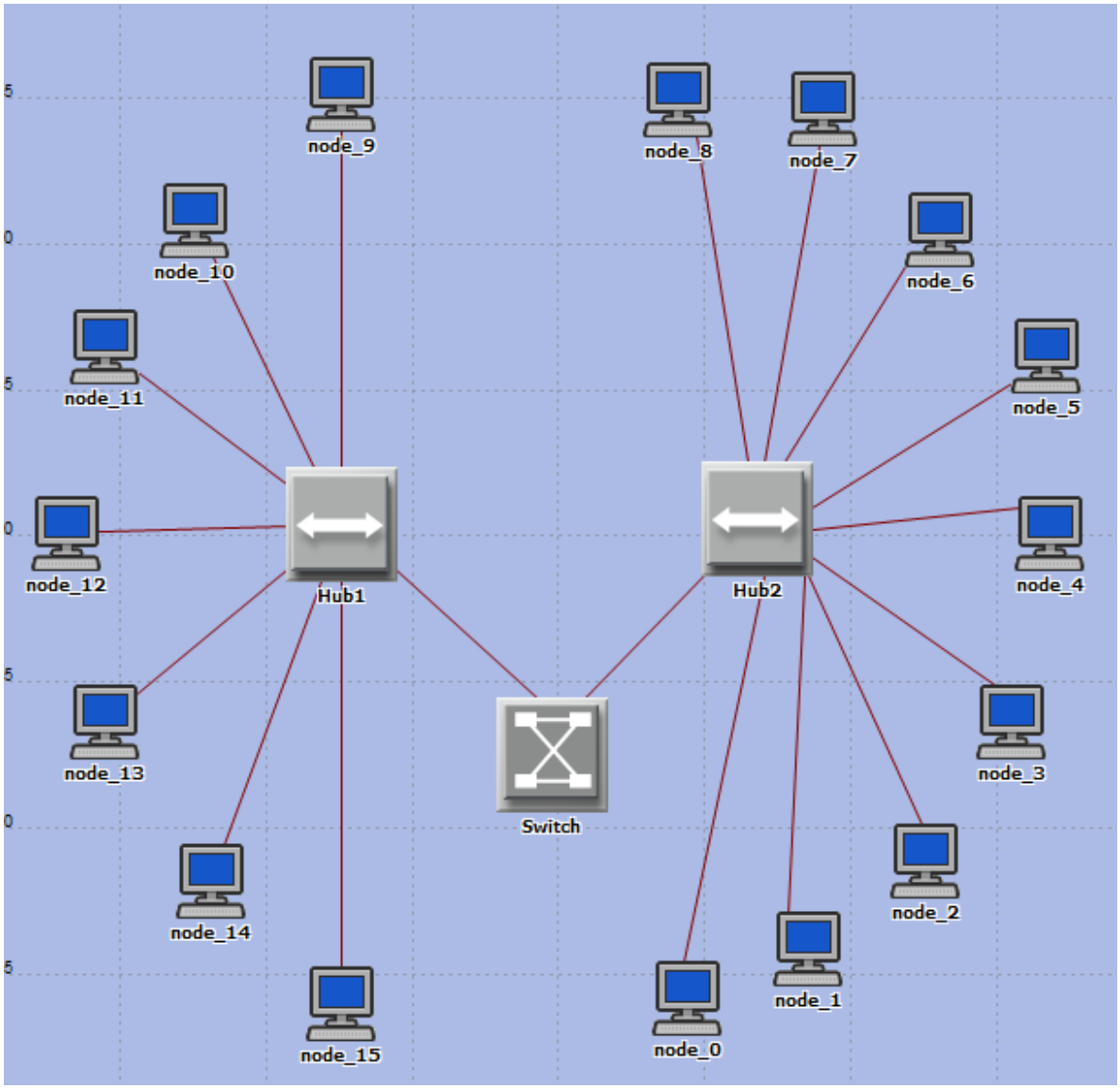
4. Для додавання концентратора натисніть на його іконку і перемістіть курсор на робоче місце. Натисніть ЛКМ для того щоб помістити концентратор в обрану вами область. Натисніть ПКМ, щоб показати, що ви закінчили використовувати об'єкт «концентратор».

5. Подібним же чином додайте комутатор.
6. Закрийте ***Object Palette***.
7. Клік правою кнопкою по концентратору, виберіть ***Edit Attributes***, змініть ім'я атрибута на ***Hub2*** і натисніть ***OK***.
8. Клік правою кнопкою по комутатора, виберіть ***Edit Attributes***, змініть ім'я атрибута на ***Switch*** та натисніть ***OK***.
9. Переконфигурирует мережа сценарію ***HubAndSwitch*** щоб вона виглядала наступним чином.

Примітки:

a. Для видалення зв'язків виберіть ***Cut*** з меню ***Edit*** (або натисніть ***Delete*** на вашому маніпуляторі типу клавіатура). Ви можете вибрати кілька зв'язків і видалити їх всі разом.

b. Щоб додати новий зв'язку використовуйте ***10BaseT*** зв'язок з ***Object Palette***.

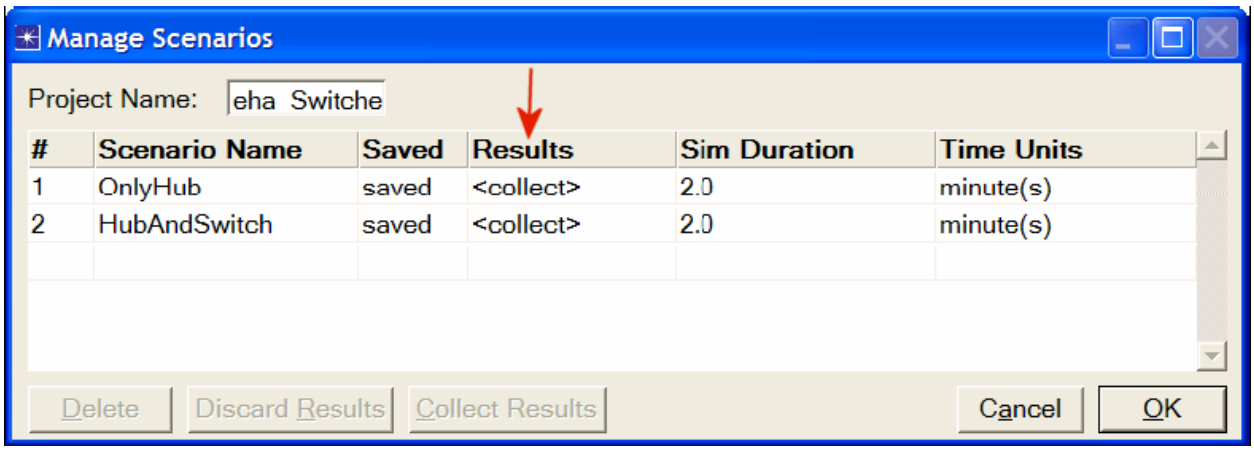


Збережіть ваш проект.

Запуск моделювання

Для запуску обох сценаріїв одночасно:

1. Виберіть ***Manage Scenarios*** з меню ***Scenarios***.
2. Змініть значення в колонці ***Results*** на <***collect***> (або <***recollect***>) для обох сценаріїв. Порівняйте з наступним видом:

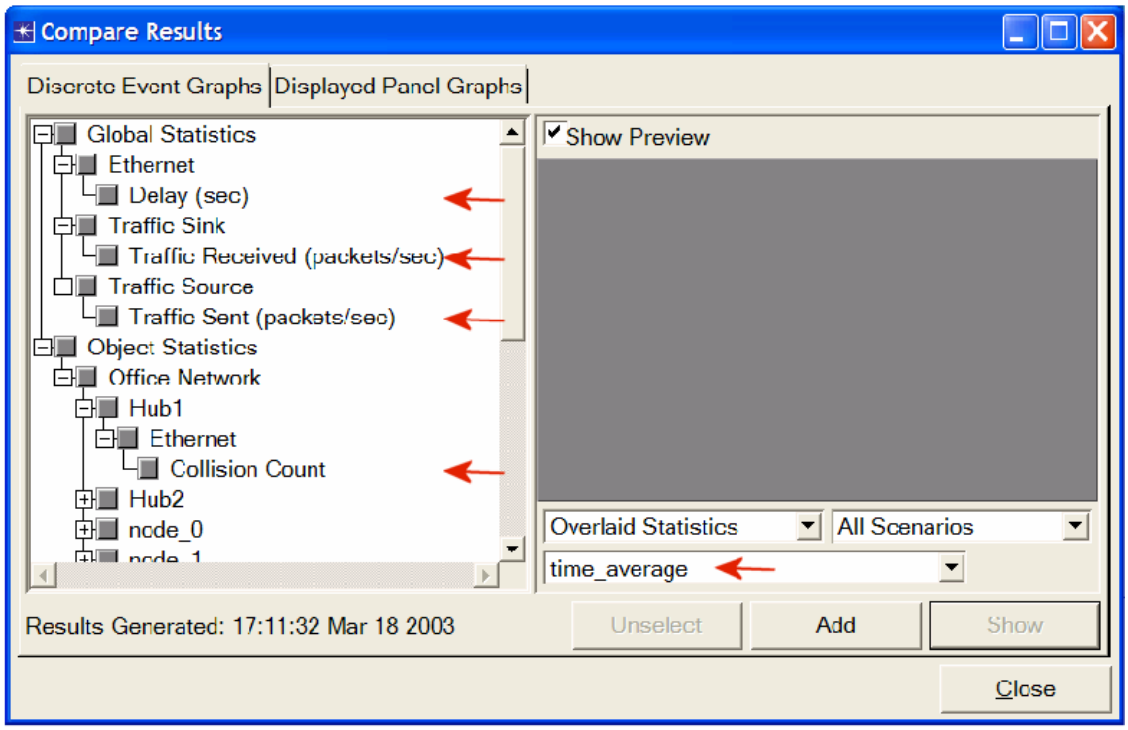


3. Натисніть ***Ok*** для того щоб запустити обидва моделювання. В залежності від швидкості вашого процесора це може зайняти до декількох хвилин.
4. Після того як обидва моделювання завершені, натисніть ***Close.***
5. Збережіть ваш проект.

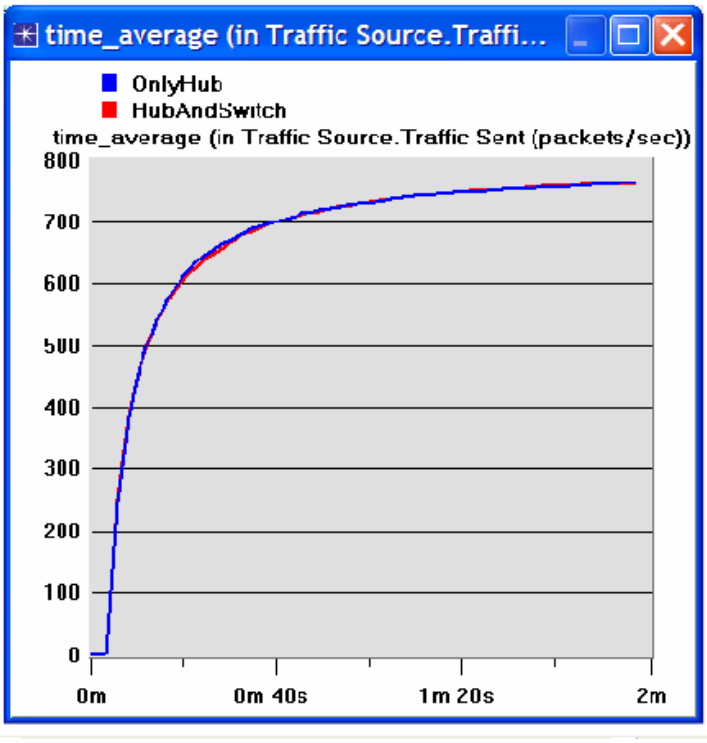
Перегляд результатів

Для перегляду та аналізу результатів:

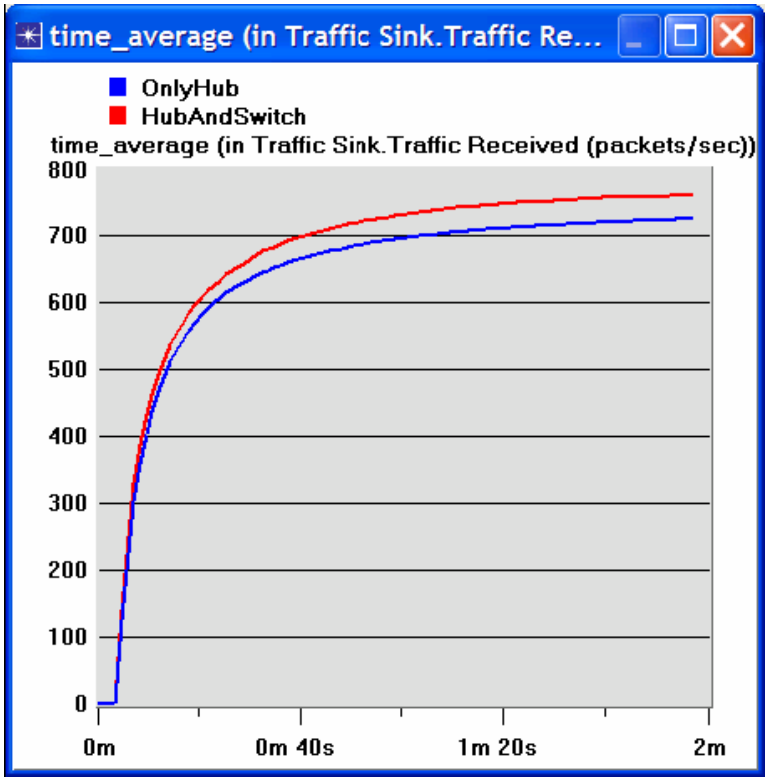
1. Оберить «Порівняти результати» в меню «Результати»
2. У правому нижньому випадаючому меню виберете пункт ***time_average***



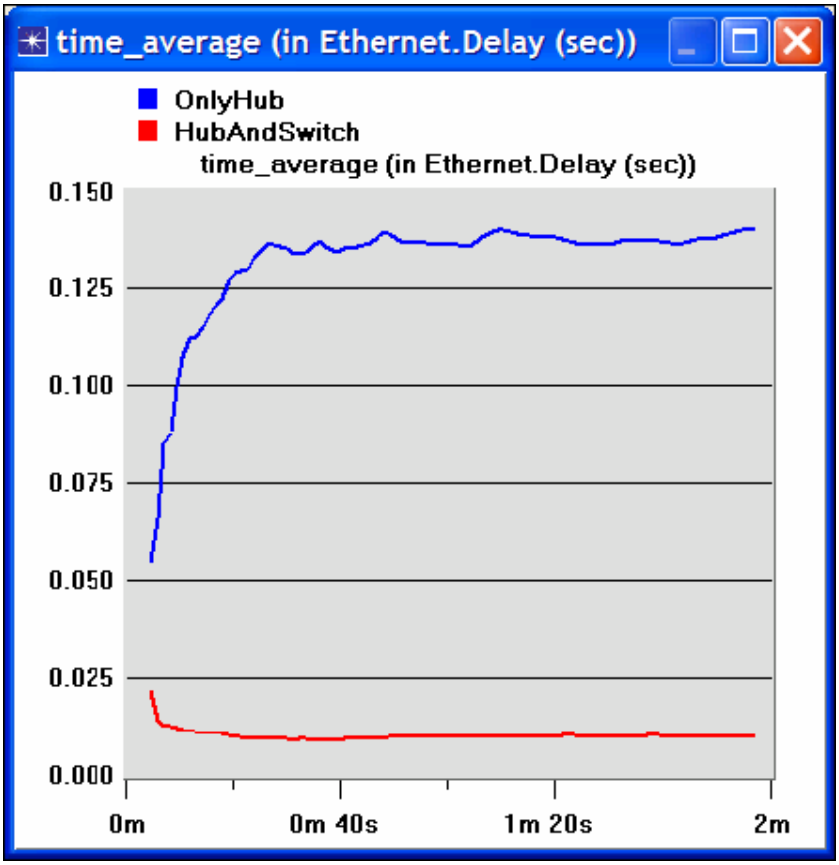
3. Оберіть статистику ***Traffic Send*** і натисніть ***Show***. Результуючий граф повинен відобразиться в низу. Як Ви бачите, статистика ***Traffic Send***, в обох сценаріях, практично ідентична.



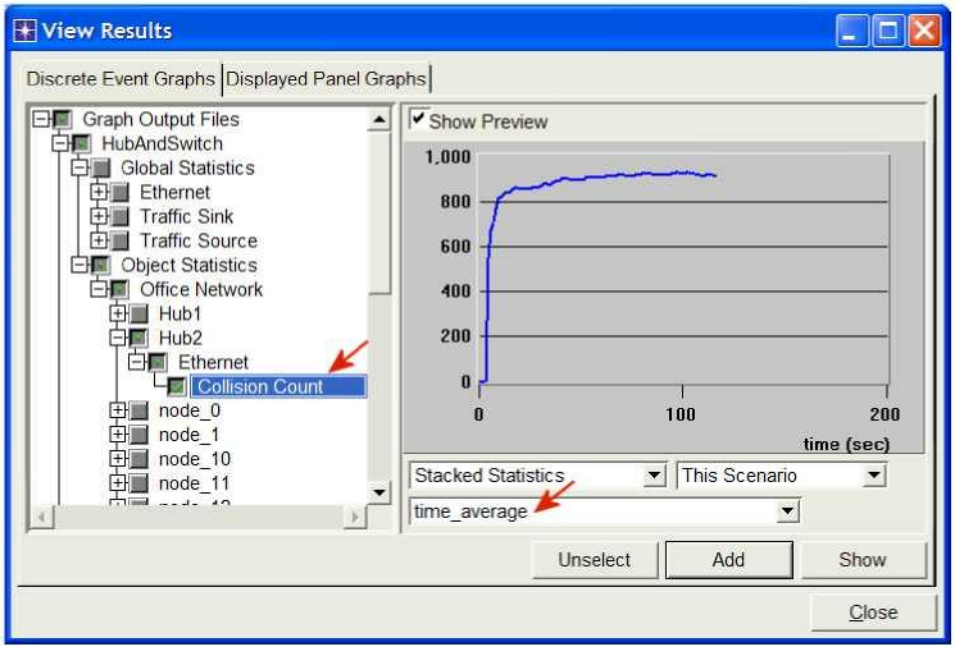
4. Виберіть статистику ***Traffic Received (packets / sec)*** і натисніть ***Show***. Результуючий графік повинен бути схожий на намальований нижче. Як бачите трафік отриманий з другого сценарію ***HubAndSwitch***, вище, ніж зі сценарію ***OnlyHub***.



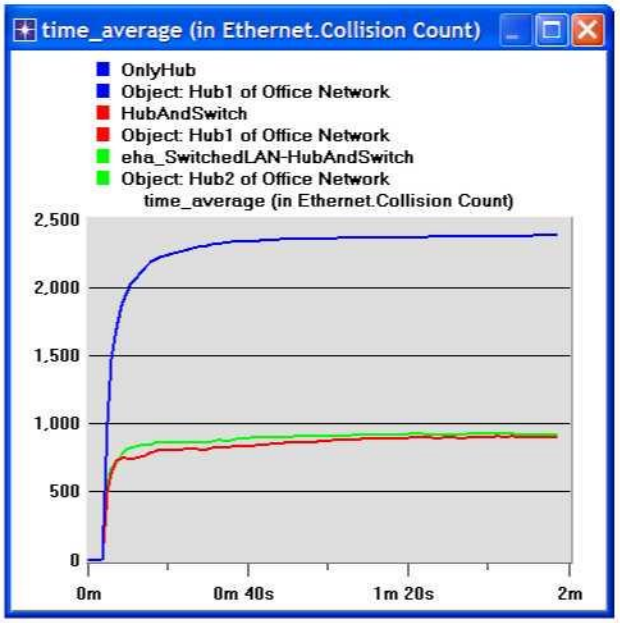
5. Виберіть статистику ***Delay (sec)*** і натисніть ***Show***. Результуючий граф повинен бути схожий на нижній (Прим. Результати можуть змінюватись в залежності від різного розташування вузлів).



6. Вибрати ***Collision Count***, статистичний для ***Hub1*** і клацнути ***Show***.
7. На графі натисніть ПКМ де-небудь в області графа ==>, виберіть ***AddStatistic*** ==> Відкрийте дерево, як показано нижче ==> Оберіть ***Collision Count statistic*** для ***Hub2*** ==>, змініть на ***time_average*** як показано це на малюнку ==>, Натисніть кнопку ***Add***.



8. Результуючий граф повинен бути схожий на графік знизу.



9. Збережіть ваш проект.

КОНТРОЛЬНІ ЗАПИТАННЯ

1) Поясніть чому додавання концентратора (***switch***) змушує мережу показувати найкращій час затримки.

2) Проаналізуйте колізії в хабі. Поясніть вашу відповідь.

3) Створіть два нових сценарія. Перший той же самий, тільки замініть hab концентратором. Другий новий сценарій той же самий як попередній сценарій, але замініть обидва hab-а двома концентраторами і видаліть старий вимикач, і з'єднайте два вимикачі, які ви тільки що додали разом з допомогою лінку 10BaseT. Порівняйте роботу цих чотирьох сценаріїв на тимчасові затримки, продуктивності, і колізії. проаналізуйте результати. Зверніть увагу: щоб замінити hab-и концентратором, клацніть ПКМ на hab-і і вимикачі і переназначте йому ethernet16.

ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ

Підготуйте звіт, виконаний за рекомендаціями до лабораторної роботи. Звіт повинен включати відповіді на вищезгадані питання, а також графіки, які Ви отримали при моделюванні сценаріїв. Проаналізуйте результати, які Ви отримали і порівняйте ці результати з очікуваними. Включіть до звіту будь-які аномалії або незрозумілу з Вашої точки зору поведінку.

Лабораторна робота №5

ПРОЕКТУВАННЯ МЕРЕЖІ

Мета роботи. Демонстрація основ проектування мережі, огляд понять користувачі, послуги, розміщення хостів.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Основним питанням є оптимізація мережевого проекту. Моделювання широко використовуються для аналізу концептуального проекту мережі. Зазвичай, до кінцевого рішення по здійсненню проекту, первинний

концептуальний проект кілька разів вдосконалюється. Метою цього є отримання проекту, який оптимізує роботу мережі з урахуванням обмеження вартості і надання необхідних послуг різним користувачам. Після реалізації мережі повинна проводиться періодична оптимізація мережі, аж до завершення її експлуатації, щоб забезпечити максимально ефективну роботу мережі і контроль з використання мережевих ресурсів.

У даній лабораторній роботі ви спроектуєте мережу для організації, що складається з чотирьох відділів: дослідницький відділ, відділ розробки, відділ електронної торгівлі, і відділ продажів. За допомогою моделі локальної мережі (LAN) ви можете промоделювати кілька серверів і клієнтів в одному об'єкті моделювання. Дана модель значно скорочує як обсяг роботи по конфігурації мережі, так і обсяг пам'яті, необхідної для моделювання. Ви зможете визначати необхідний профіль, який визначатиме шаблон додатків, використовуваних користувачами кожного з департаментів організації. В кінці цієї лабораторної роботи ви зможете вивчити, як різні рішення проектування можуть впливати на ефективність роботи мережі.

МЕТОДИЧНІ ВКАЗІВКИ

Створення нового проекту

1. Запустіть ***OPNET IT Guru Academic Edition*** **,** виберіть ***New*** з меню ***File*****.**
2. Виберіть ***Project*** і натисніть ***OK*** **.** Назвіть проект <***Your initials***> ***_NetDesign*****,** виберіть сценарій ***SimpleNetwork***.Натисніть ***OK*****.**
3. У майстрі запуску: діалогове вікно ***Initial Topology***, упевнитися, що обраний сценарій ***Create Empty Scenario***, натисніть ***Next***, Виберіть ***Campus*** зі списку ***Network Scale***, натисніть ***Next***. Виберіть ***Miles*** з випадаючого меню ***Size*** і встановіть 1 для осей ***X Span*** і ***Y Span***, двічі натисніть ***Next***, натисніть ***OK*****.**

Створення і конфігурація мережі

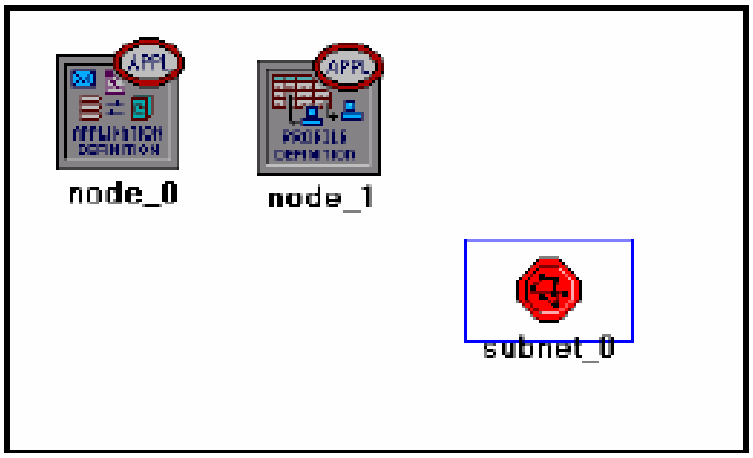
Ініціалізація мережі:

1. Діалогове вікно ***Object Palette*** тепер має перебувати вгорі робочого вікна проекту.

Якщо це не так, натисніть для його відкриття. Переконайтеся, що ***internet_toolbox*** обраний у випадаючому меню на панелі об'єктів.

2. Додайте на робоче вікно проекту наступні об'єкти: ***Application Config***, ***Profile Config*** і ***subnet.***

a. Щоб додати об'єкт з панелі натисніть його іконку на панелі об'єктів, перейдіть на робоче вікно, ЛКМ для розміщення об'єкта. ПКМ щоб закінчити. Робоче вікно повинно містити наступні три об'єкти:



Закрийте діалогове вікно ***Object Pallet*** (панель об'єктів) і збережіть проект.

Конфігурація служб:

1. Правий клік на закладці ***Application Config*** ➔ ***Edit Attributes*** ➔ Замініть атрибут ***name*** на ***Applications*** ➔ Замініть атрибут ***Application Definitions*** на ***Default*** ➔ Натисніть ***OK.***
2. Правий клік на закладці ***Profile Config*** ➔ ***Edit Attributes*** ➔ Замініть атрибут ***name*** на ***Profiles*** ➔ Замініть атрибут ***Profile Configuration*** на ***Sample Profiles*** ➔ Натисніть ***OK. Sample Profiles*** забезпечують шаблони додатків, задіяні

користувачами, такими як інженери, дослідники, продавці, і користувачі мультимедіа.

Конфігурація підмережі:

1. ПКМ на закладці ***subnet*** ➔ ***Edit Attributes*** ➔ Замініть атрибут ***name*** на ***Engineering*** і натисніть ***OK.***
2. Подвійний клік на закладці ***Engineering***. Ви бачите пусте робоче вікно, що показує, що підмережа не містить об'єктів.
3. Відкрийте панель об'єктів і переконайтеся, що як і раніше встановлений ***internet_toolbox.***
4. Додайте наступні елементи робочого вікна підмережі: ***10BaseT LAN***, ***ethernet16***

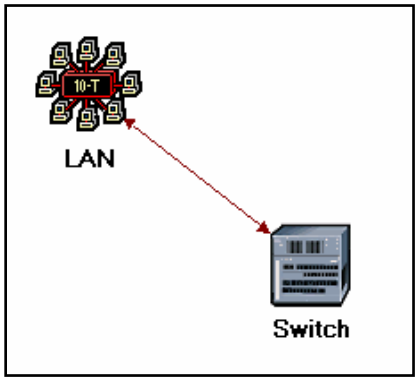
   Switch, і ***10BaseT link*** для з'єднання ***LAN*** з комутатором (***Switch***) ➔ Закрийте панель.
5. ПКМ на закладці ***10BaseT LAN*** ➔ ***Edit Attributes*** ➔ Замініть атрибут ***name*** на ***LAN*** ➔ Переконайтеся, що атрибут ***Number of Workstations*** має значення 10.

   Натисніть на колонці ***Value*** для атрибута ***Application***: ***Supported Profiles*** і виберіть ***Edit.*** Ви повинні отримати таблицю, в якій вам треба:

   a. Встановити число рядів ***rows*** в 1.
   b. Встановити ***Profile Name*** в ***Engineer***.
   c. Натисніть ***OK*** двічі.

   Щойно створений об'єкт це еквівалент ***LAN*** топології «зірка» з 10 робочих станцій.

Трафік вироблений користувачами цієї ***LAN***-мережі походить на трафік вироблений інженерами.

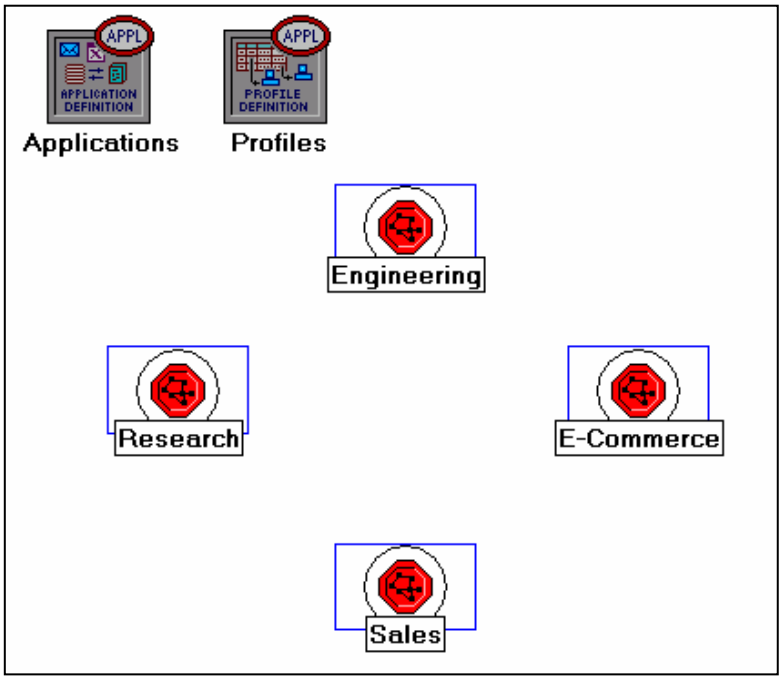


6. Змініть назву комутатора ***ethernet16 Switch*** на ***Switch***.

7. Підмережа повинна виглядати приблизно так.
8. Збережіть проект.

Конфігурування відділів*:*

1. Ви закінчили конфігурацію підмережі відділу Інженерів. Щоб повернутися до вікна головного проекту, натисніть кнопку ***Go to the higher level***. Підмережі інших департаментів організації повинні бути такими ж, за винятком підтриманих конфігурацій.
2. Зробіть три копії щойно створеної підмережі ***Engineering***: Натисніть на закладці ***Engineering*** ➔ З меню ***Edit*** виберіть ***Copy*** ➔ З меню ***Edit*** виберіть ***Paste*** три рази помістивши підмережу на робоче вікно для створення нових підмереж.
3. Змініть назву (ПКМ на підмережі і виберіть ***Set Name***) і розмістіть підмережі як показано нижче:



4. Подвійний клік на закладці ***Research*** ➔ виберіть для атрибутів цієї ***LAN***-мережі ***Edit*** ➔ виберіть ***Edit*** для значення ***Application***: атрибут ***Supported***

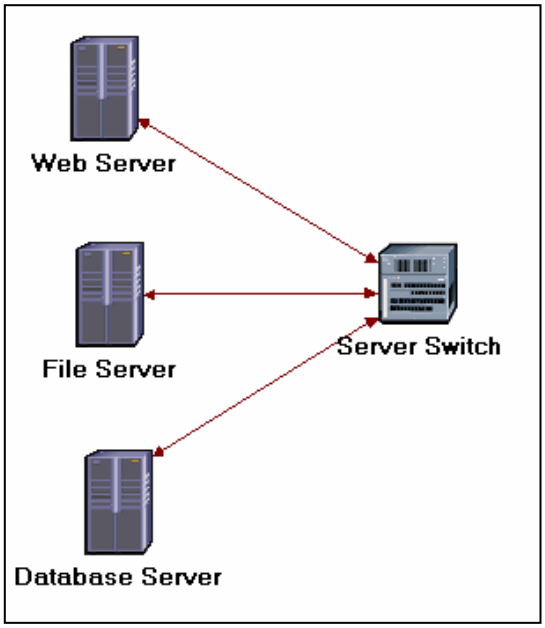
Profiles ➔ Замініть значення ***Profile Name*** з ***Engineer*** на ***Researcher*** ➔ Натисніть ***OK*** двічі ➔Поверніться на верхній рівень натиснувши кнопку  .

5. Повторіть крок 4 із закладкою ***Sales*** і призначте для ***Profile Name*** профіль ***Sales Person***.
6. Повторіть крок 4 із закладкою ***E-Commerce*** і призначте для ***Profile Name*** профіль ***E-commerce Customer***.
7. Збережіть проект.

Конфігурація серверів:

Тепер ми повинні налаштувати підмережу, що містить сервера. Сервери повинні підтримувати програми, визначені в призначених профілях. Ви можете двічі вибрати ці програми, змінюючи атрибути нашої закладки ***Profile***. Перевірте кожен ряд під ієрархією ***Applications***, яка в свою чергу знаходиться під ієрархією ***Profile Configuration***. Ви побачите, що нам потрібні сервери, які підтримують наступні програми: перегляд ***Web***, ***Email***, ***Telnet***, обмін файлами, БД та друк файлів.

1. Відкрийте панель ***Object Palette*** і додайте нову підмережу ***subnet*** ➔ Змініть назву підмережі на ***Servers*** ➔ Подвійний клік на закладці ***Servers*** щоб увійти в її робоче вікно.
2. З панелі ***Object Palette*** додайте три сервера ***ethernet_servers***, один ***thernet16_switch***, і три ***10BaseT*** зв'язків щоб з'єднати сервери з комутатором.
3. Закрийте панель ***Object Palette***.
4. Змініть назви серверів і комутатора як показано нижче:



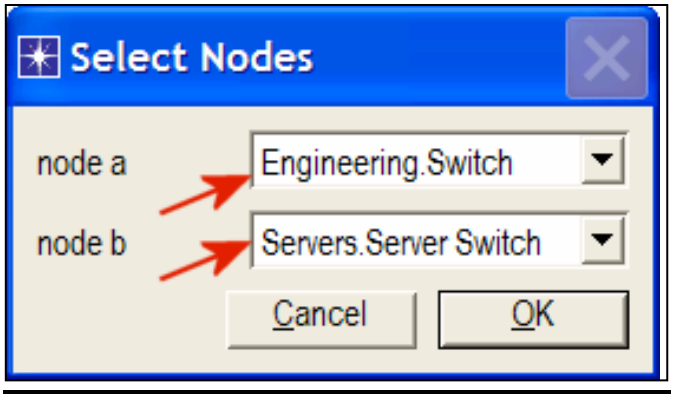
5. ПКМ на кожному з серверів і виберіть ***Edit*** значення ***Application***: атрибут ***Supported Services***.
    a. Для Веб-сервера Додайте чотири рядка, щоб підтримувати наступні служби: ***Web Browsing (Light HTTP1.1)***, ***Web Browsing (Heavy HTTP1.1)***, ***Email (Light) і Telnet Session (Light)***.
    b. Для Файлового сервера Додайте чотири рядка, щоб підтримувати наступні служби***: File Transfer (Light) і File Print (Light)***.
    c. Для сервера БД Додайте чотири рядка, щоб підтримувати наступні служби: ***Database Access (Light)***.
6. Поверніться на робоче вікно проекту натиснувши кнопку Go to the higher level  .
7. Збережіть проект.

З'єднання підмереж:

Тепер підмережі готові до з'єднання.

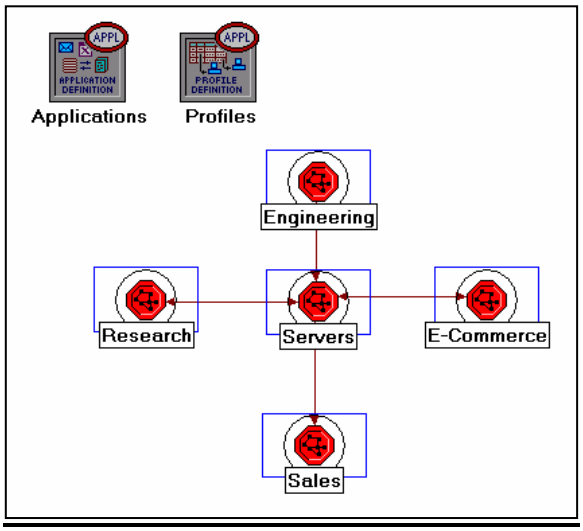
1. Натисніть ***Open*** панелі ***Object Palette*** і додайте 4 зв'язку ***100BaseT*** для з'єднання підмереж відділів до підмережі ***Servers***. Після того встановите кожний зв'язок, переконайтеся що він налаштований на з'єднання з

"Комутаторами" в обох підмережах. Зробіть це вибравши їх із випадаючого меню як показано нижче:



2. Закрийте панель ***Object Palette***.

3. Тепер ваша мережа повинна виглядати так:



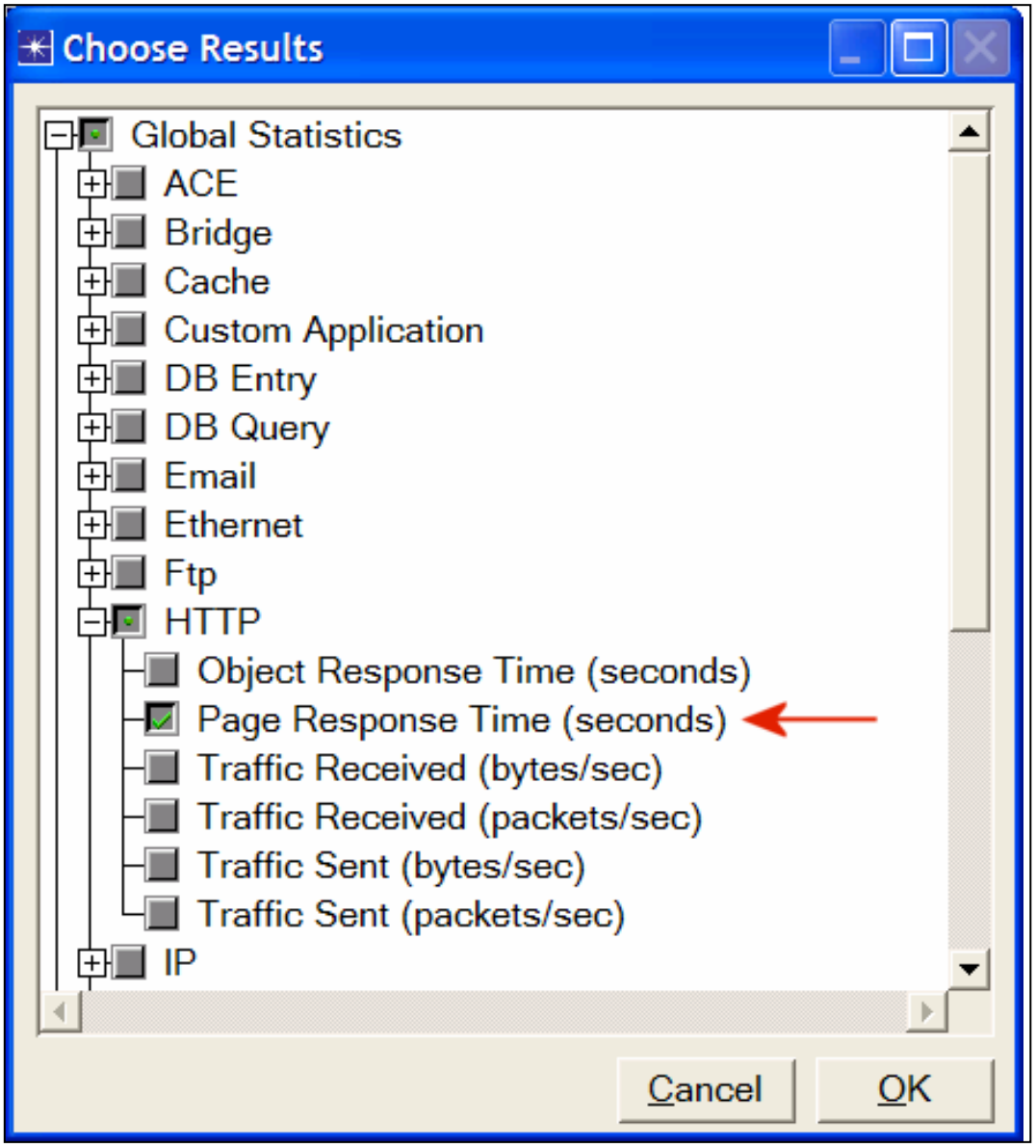
4. Збережіть проект.

Вибір статистики:

Щоб протестувати ефективність нашої мережі ми зберемо одну з можливих статистик:

1. ПКМ на робочому вікні і виберіть ***Choose Individual Statistics*** з випадаючого меню.

2. У діалоговому вікні ***Choose Results***, виберіть наступну статистику:



3. Натисніть ***OK***.

Конфігурація симуляції:

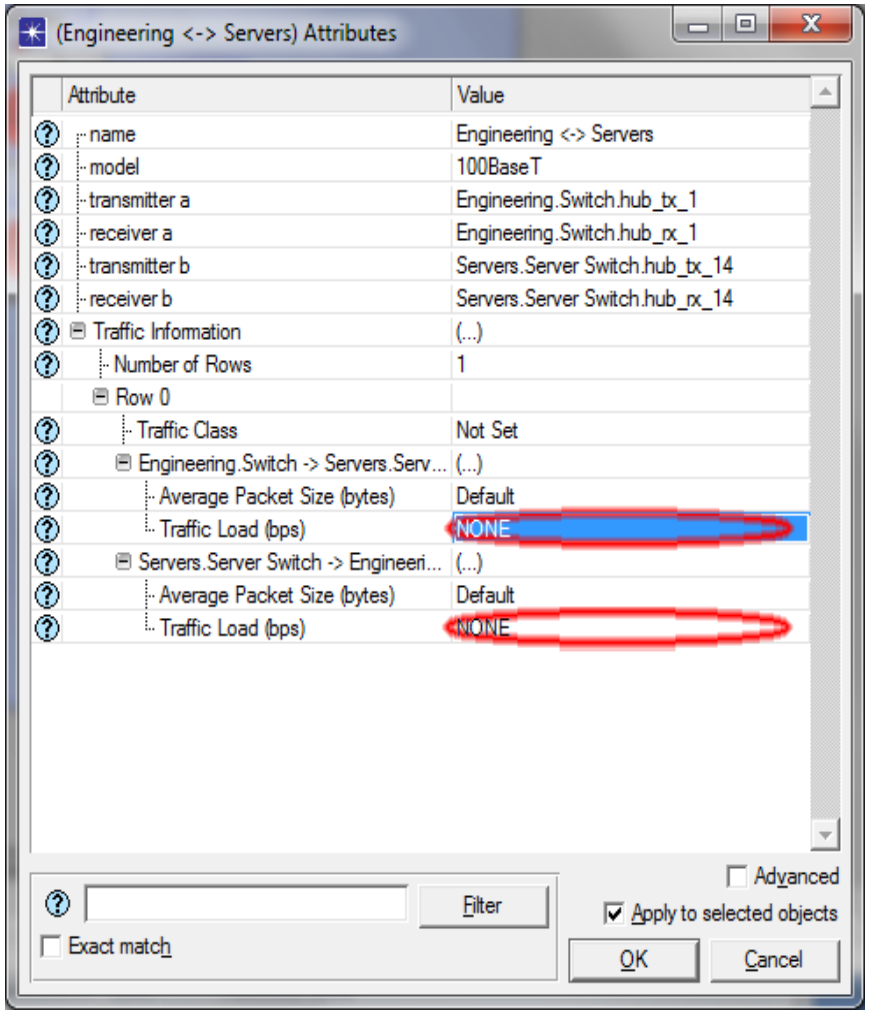
Тепер ми налаштуємо тривалість моделювання:

1. Натисніть на кнопці ***Configure / Run Simulation*** .
2. Встановіть тривалість ***30.0 minutes***.
3. Натисніть ***OK***.

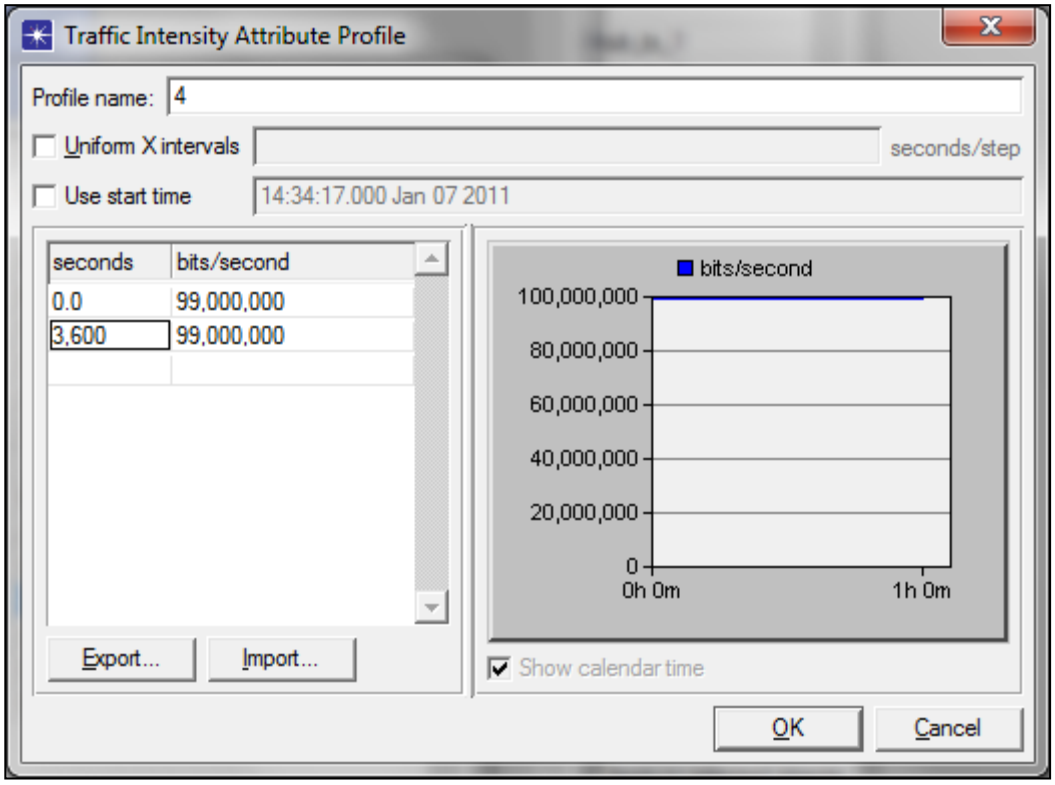
Дублювання сценарію:

У щойно створеної мережі ми домовилися, що в зв'язках відсутній зворотний трафік. У реальних мережах це найчастіше не так. Ми створимо дублікат сценарію ***SimpleNetwork***, але з двонаправленим трафіком у зв'язках ***100BaseT***.

1. Виберіть ***Duplicate Scenario*** з меню ***Scenarios*** і назвіть його ***BusyNetwork*** ➔ Натисніть ***OK***.
2. Виберіть всі зв'язки ***100BaseT*** одночасно (натисніть на всіх них утримуючи кнопку ***Shift***) ➔ ПКМ на одній з них ➔ ***Edit Attributes*** ➔ Встановіть ***Apply to Selected Objects*** чек-бокс.
3. Щоб задати фонове навантаження виберіть пункт ***Traffic information*** , встановіть ***rows*** в 1 і змініть значення ***NONE*** , відмічені на малюнку.



При натисканні ***NONE*** -> ***Edit*** відкриється вікно ***Traffic Intensity***



У цьому вікні встановіть значення як показано на малюнку, це змоделює 99% фонової навантаженності на мережу.

4. Натисніть OK.

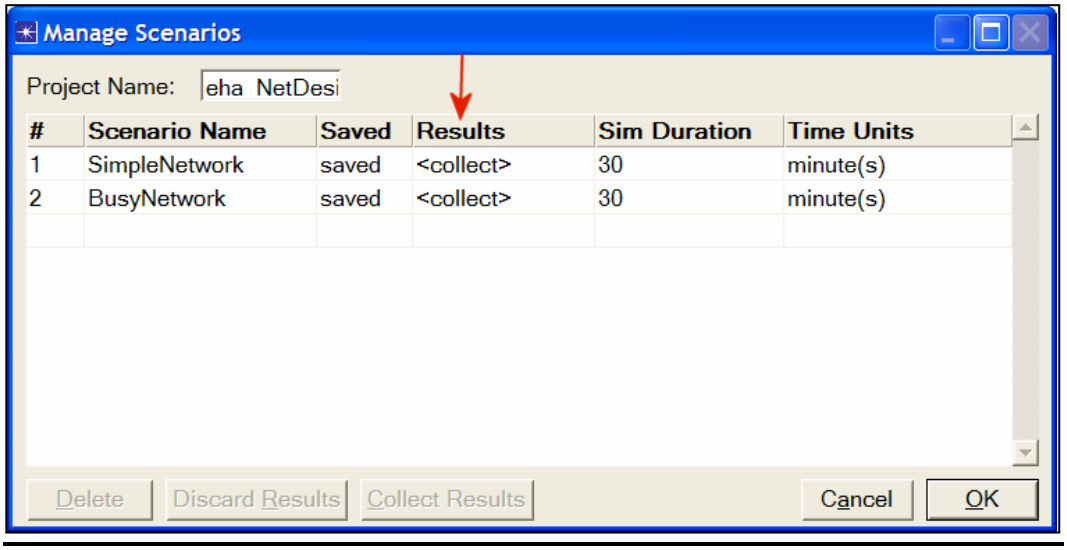
5. Збережіть проект.

Запуск симуляції:

Щоб запустити моделювання для обох сценаріїв одночасно:

1. Ідіть до меню ***Scenarios*** ➔ Виберіть ***Manage Scenarios***.

2. Замініть значення під колонкою ***Results*** на <***collect***> (або <***recollect***>) для обох сценаріїв. Порівняйте з прикладом

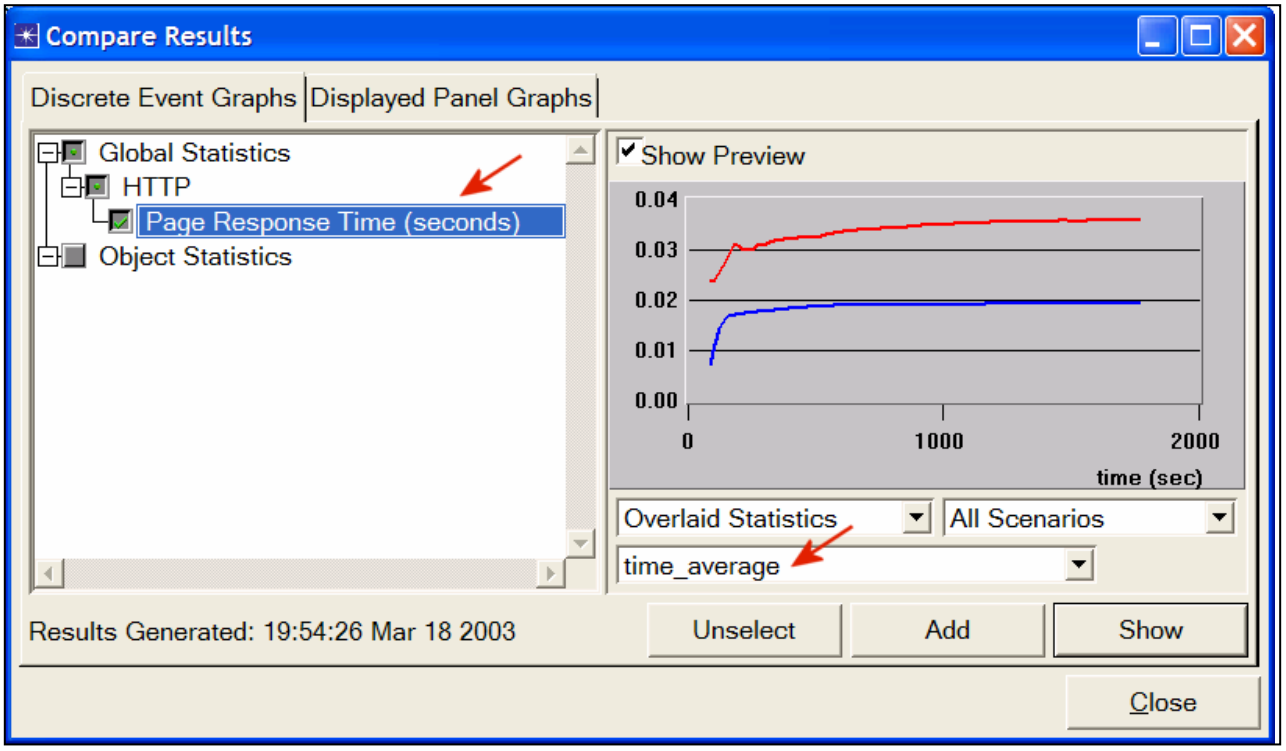


3. Натисніть ***OK*** щоб запустити два моделювання. В залежності від швидкості вашого процесора вони можуть тривати кілька секунд.
4. Після завершення двох моделювань, натисніть ***Close***.
5. Збережіть проект.

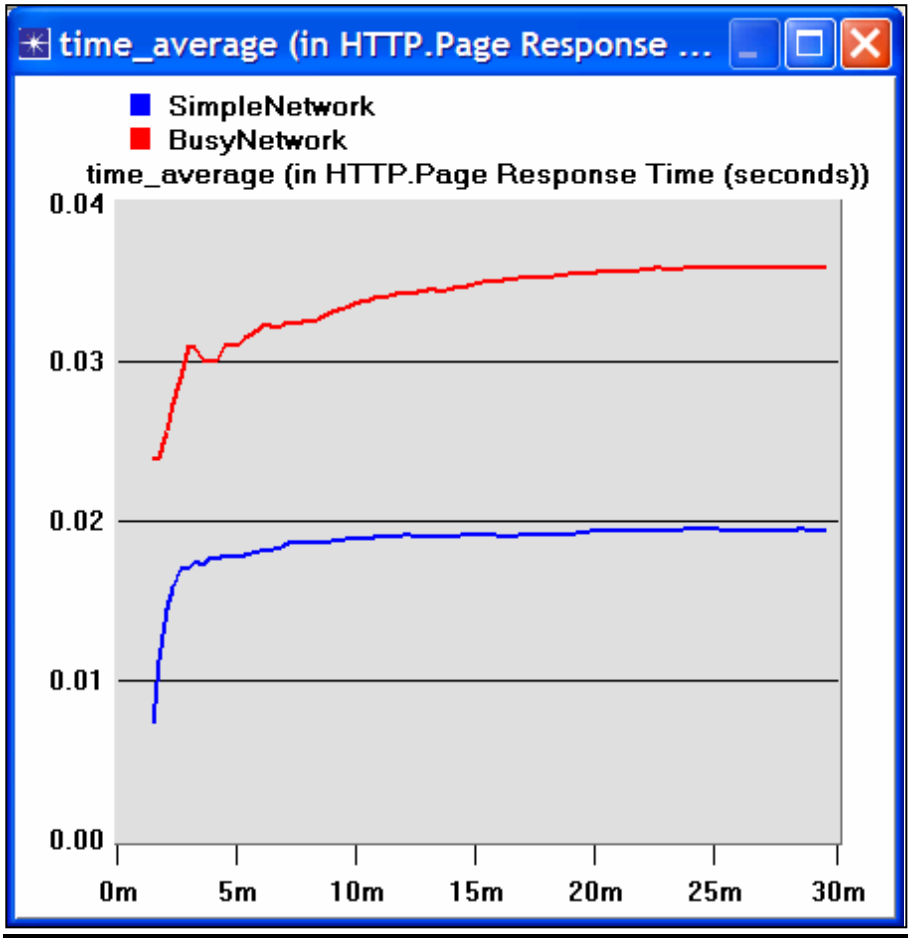
Перегляд результатів:

Для перегляду та аналізу результатів:

1. Виберіть ***Compare Results*** з ***Results*** menu.
2. Замініть меню, що випадає в правій нижній частині діалогового вікна ***Compare Results*** з ***As Is*** до ***time_average*** як показано нижче.



3. Виберіть статистику ***Page Response Time*** (***seconds***) і натисніть ***Show***. Результуючий графік повинен виглядати приблизно так.



ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ

Підготуйте звіт, виконаний за рекомендаціями до лабораторної роботи. Звіт повинен включати відповіді на вищезгадані питання, а також графіки, які Ви отримали при моделюванні сценаріїв. Проаналізуйте результати, які Ви отримали і порівняйте ці результати з очікуваними. Включіть до звіту будь-які аномалії або незрозумілу з Вашої точки зору поведінку.

Лабораторна робота №6

МЕРЕЖІ ATM

Мета роботи. Розглянути результат адаптації рівнів і сервісів ATM грунтуючись на продуктивності мережі.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Асинхронний метод передачі (ATM) це мережа з маршрутизацією інформації на основі технології комутації пакетів. Комутовані пакети в ATM мережах мають фіксовану довжину 53 байта, і називаються осередками. Такий розмір осередка дозволяє ефективніше передавати мовний трафік. Рівень Адаптації (ATM Adaptation Layer - AAL) розташований між ATM та протоколами, які використовують ATM. Ці протоколи мають змінну довжину кадрів. Прикладом може служити протокол IP. AAL заголовки містять інформацію, необхідну одержувачу, для того що б зібрати окремі осередки в початкове повідомлення. Оскільки ATM був розроблений для підтримки будь-яких видів сервісів, включаючи мову, відео та дані це означало що для різних сервісів повинні існувати різні AAL. AAL1 і AAL2 були розроблені для підтримки мовного трафіку, який вимагає гарантованої швидкості передачі. AAL3 / 4 і AAL5 надають підтримку для передачі даних через ATM.

ATM надає QoS можливості використовуючи його п'ять сервісів: CBR, VBR-rt, VBR-nrt, ABR, і UBR. В CBR (constant bit rate), джерело передає потік даних з фіксованою швидкістю. CBR найбільш прийнятна для мовного трафіку. Тому CBR дуже необхідний для телефонних компаній. UBR (unspecified bit rate), найбільш "робочий" сервіс ATM. ATM завжди вимагає сигналізує фазу перед посилкою даних, UBR надає можливість джерела вказати максимальну швидкість на якій буде відбуватися передача. Комутатор повинен використовувати цю інформацію для того щоб дозволити або заборонити встановлення віртуального каналу.

У даній роботі необхідно організувати ATM мережу в якій будуть передаватися: мовні дані, Email і FTP. Ви навчитеся, як зробити вибір адаптаційного рівня як мережевої служби, здатної ефективно задіяти роботу додатків.

МЕТОДИЧНІ ВКАЗІВКИ

Процедура створення нового проекту

1. Запустіть ***OPNET IT Guru Academic Edition***. Виберіть ***New*** з меню ***File***.
2. Виберіть ***Project*** і натисніть ***OK***. Назва проекту***: <Ініціали> _ATM***, і сценарій ***CBR_UBR***. Натисніть ***OK***.
3. В ***Startup Wizard***: діалогове вікно ***Initial Topology***. Переконайтеся, що вибрано ***Create Empty Scenario*** => натисніть ***Next*** => виберіть ***Choose From Maps*** з ***Network Scale list*** => натисніть ***Next*** => Виберіть ***USA*** з карт => натисніть ***Next*** => У списку ***Select Technologies*** включіть ***atm_advanced***, як показано на малюнку => натисніть ***Next*** => натисніть ***OK***.

Створення та налагодження мережі

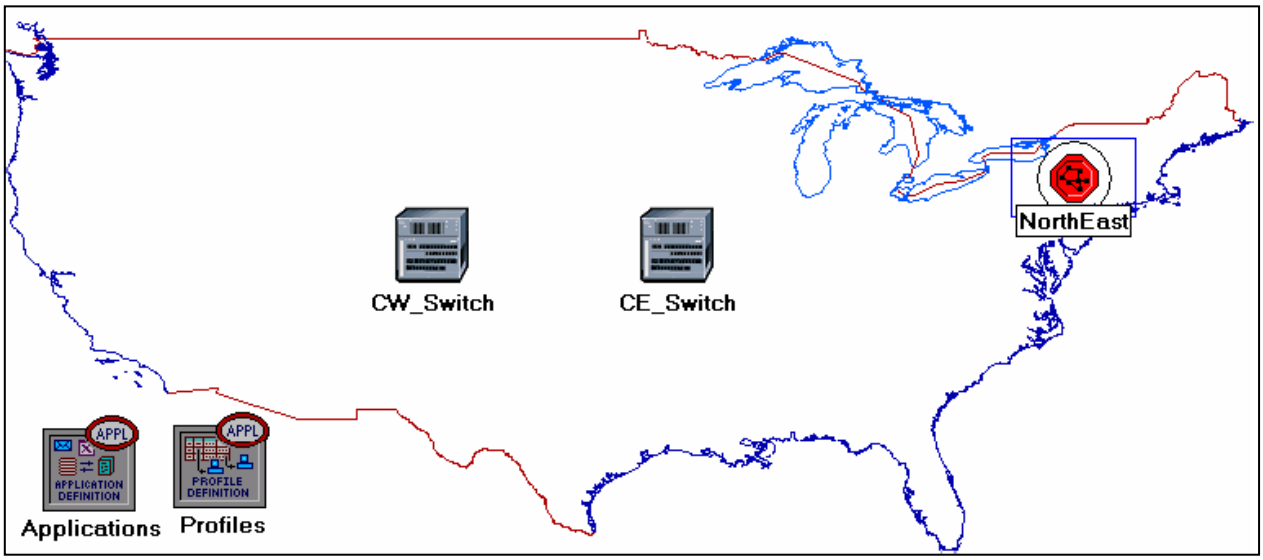
Ініціалізація мережі

1. Вікно ***Object Palette*** має бути зверху вашого робочого простору. Якщо це не так, натисніть  . Переконайтеся, що прапор ***atm_advanced*** встановлений з випадаючого меню панелі об'єкта.

2. Додати в робочий простір наступні об'єкти з панелі: ***Application Config***, ***Profile Config***, два перемикача ***atm8_crossconn_adv***, і ***subnet***

   а. Для додавання об'єкта з панелі, натисніть на відповідну іконку з панелі => перемістіть за допомогою мишки на робочий простір і клацніть для розташування об'єкта => правий клік дозволить вийти з режиму створення об'єкта.

3. Закрийте вікно ***Object Palette*** і змініть назву (ПКМ на вузлі => ***Set Name***) об'єкта, який ви додали як показано нижче і збережіть ваш проект.



Конфігурація додатків

1. ПКМ на вузлі ***Applications*** => ***Edit Attributes*** => розгорніть ***Application Definitions*** і встановіть значення ***rows*** рівним 3 => Ім'я рядків ***FTP***, ***EMAIL*** і ***VOICE***.

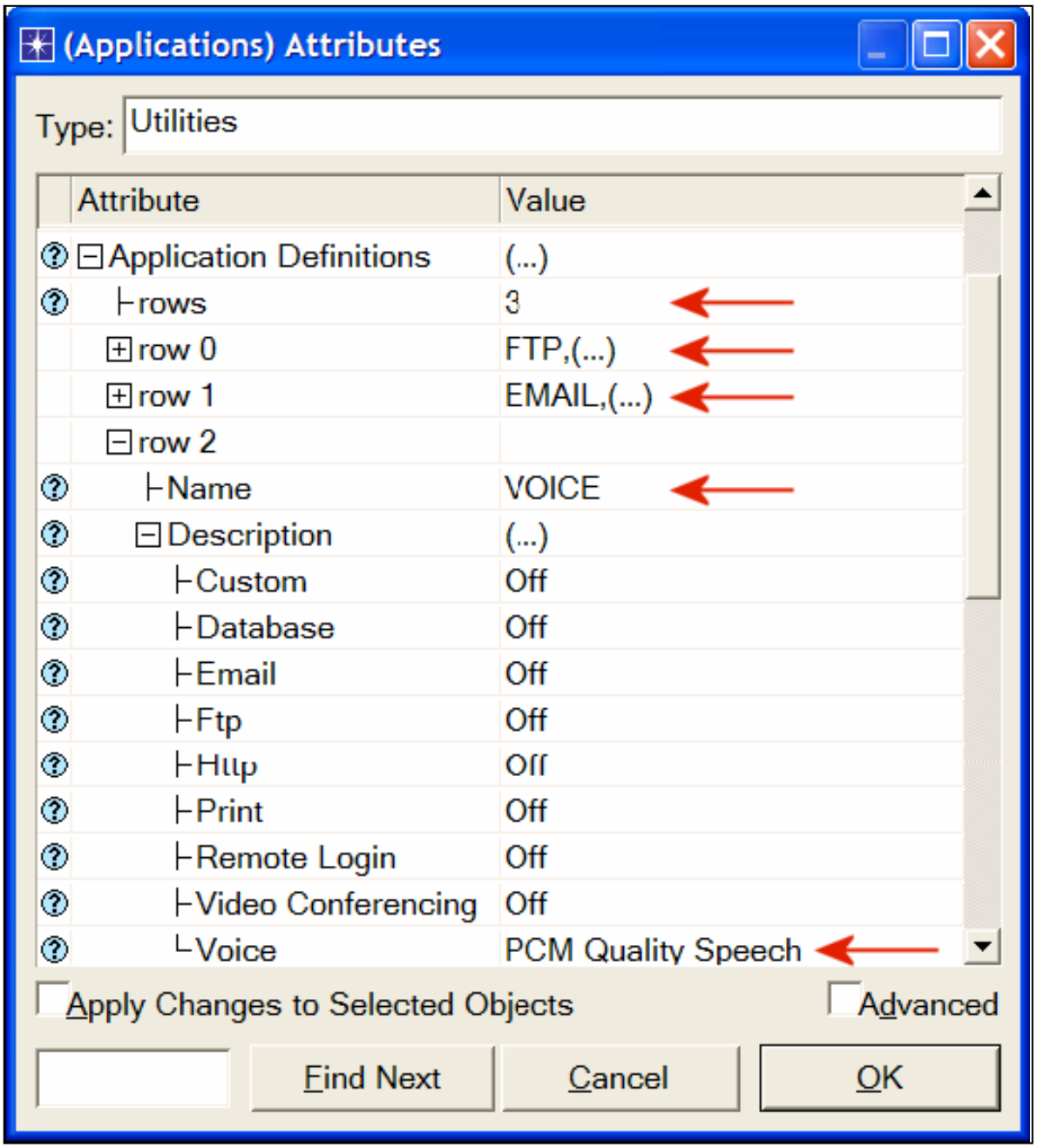
   а) увійдіть в рядок ***FTP*** => розгорніть ієрархію ***Description*** => встановіть значення ***High Load*** для ***FTP***.

   б) увійдіть в рядок ***EMAIL*** => розгорніть ієрархію ***Description*** => встановіть значення ***High Load*** для ***EMAIL***.

   в) увійдіть в рядок ***VOICE*** => розгорніть ієрархію ***Description*** => встановіть значення ***PCM * Quality Speech*** для ***VOICE***.

* Pulse

Code Modulation. (Імпульсно-кодова модуляція) це процедура оцифровки звуку для подальшої передачі через Інтернет.

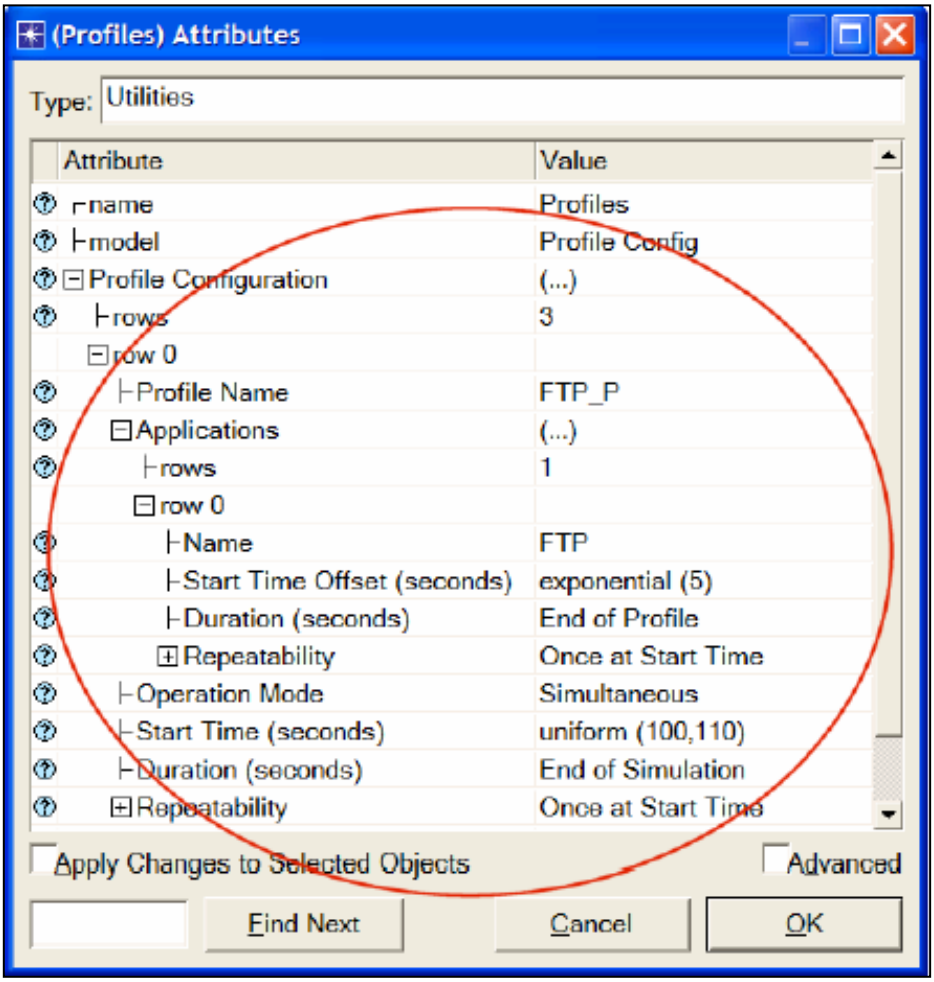


2. Натисніть ***OK*** і збережіть Ваш проект.

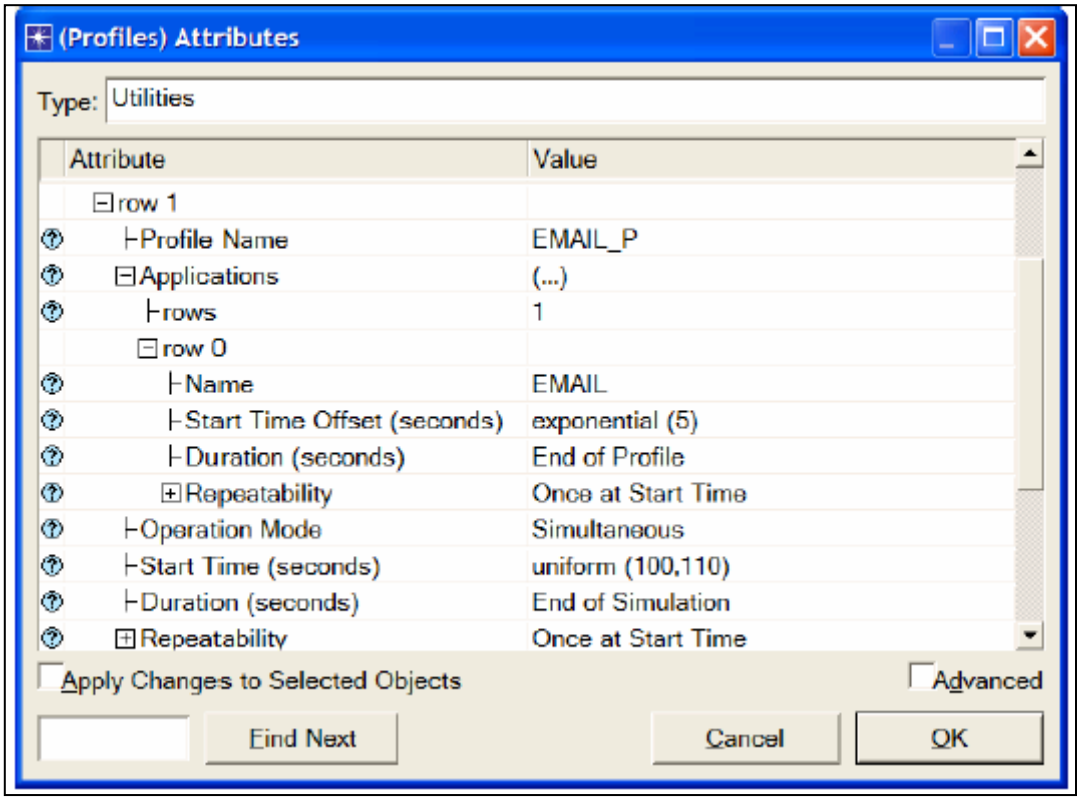
Налаштування подання

1. ПКМ на пункт меню ***Profiles*** → ***Edit Attributes*** → оберіть ***Profile Configuration*** і встановіть значення ***rows*** рівним 3;

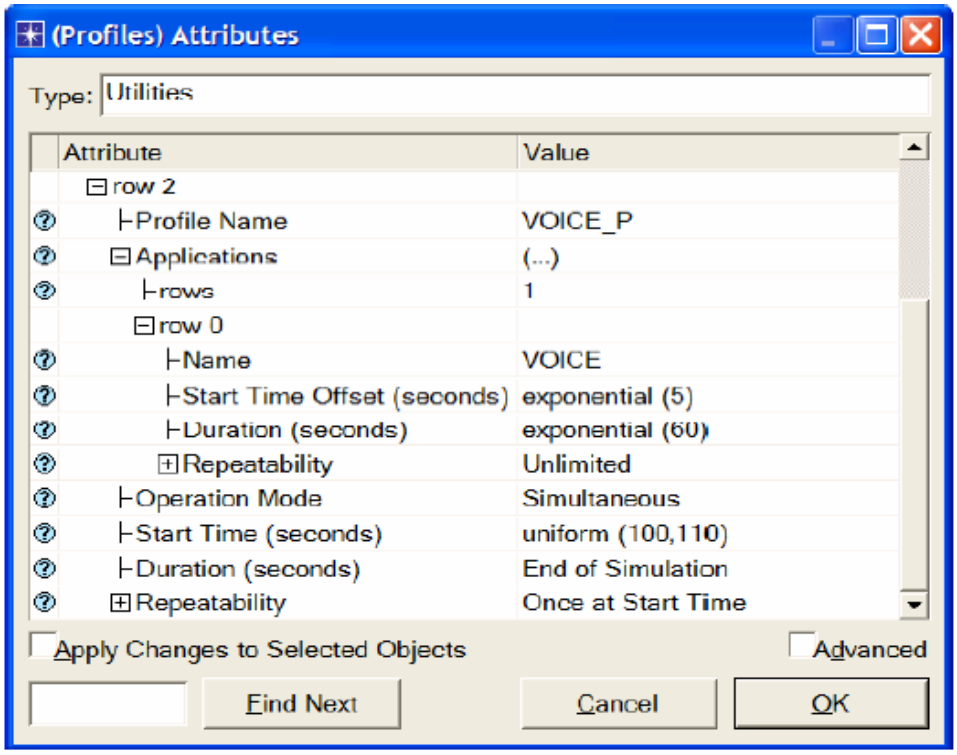
• Назвіть і встановіть ***row0*** як показано.



• Назвіть і встановіть row1 як показано.

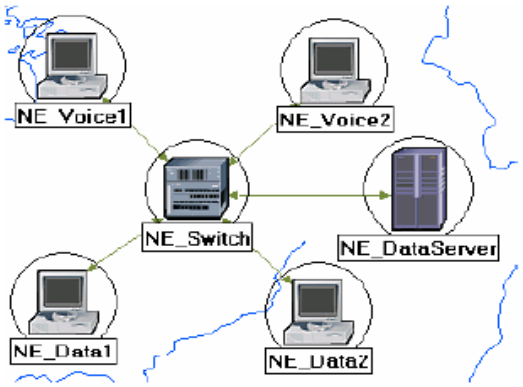


• Назвіть і встановіть значення атрибутів 2-го стовпця як показано на малюнку. (Прим.: Щоб встановити ***Duration to exponential (60)***, ви повинні будете привласнити "***Special Value***" значення "***Not Used***") => Закрийте діалогове вікно ***Object Palette***.



Конфігурування підмережі NorthEast

1. Зробіть подвійний клік по вузлу підмережі ***NorthEast***. Ви отримаєте просто порожню робочу середу в якій не буде міститися жодних об'єктів.
2. Відкрийте панель об'єктів  і переконайтеся в тому, що ***atm_advanced*** вибрано з випадаючого меню в панелі об'єктів.
3. Додайте наступні об'єкти в робочий простір підмережі: один ***atm8_crossconn_adv switch***, один ***atm_uni_server_adv***, чотири ***atm_uni_client_adv*** і зв’яжіть їх за допомогою двонаправлених ***atm_adv*** зв'язків => Закрийте палітру => Змініть назву об’єктів як показано.



4. Змініть атрибут ***data rate*** для всіх зв'язків в ***DS1***
5. Для ***NE_Voice1*** і ***Ne_Voice2*** встановіть наступні атрибути:
   a. Встановіть ***ATM Application Parametrs*** в ***CBR*** only
   b. Раскройте ***ATM Parameters*** ієрархію -> встановіть ***Queue Configuration*** в ***CBR only***
   c. Розкрийте ***Application***: ***Supported Profiles*** ієрархію -> встановіть ***rows*** в 1 - Розкрийте ***row 0*** ієрархію - встановіть ***Profile name*** в ***Voice_P***
   d. ***Application: Supported Services*** -> відредагуйте це значення -> встановіть ***rows*** в 1 ->встановіть ***Name*** доданого рядка в ***VOICE*** -> натисніть ***OK***.
   e. Розкрийте ***Application***: ***Transport Protocol*** ієрархію -> ***Voice Transport*** = ***AAL2***.
6. Для ***NE_Voice1***, виберете ***Edit Attributes*** -> змініть значення атрибуту ***Client Address*** і запишіть туди ***NE_Voice1***
7. Для ***NE_Voice2***, оберіть ***Edit Attributes*** -> змініть значення атрибуту ***Client Address*** і запишіть туди ***NE_Voice2***
8. Налаштуйте ***NE_DataServer*** наступним чином:
   - ***Application***: ***Supported Services*** -> встановіть ***rows*** в 2 -> Впишіть ***Name*** доданих рядків в: ***EMAIL*** і ***FTP*** -> натисніть ***OK***.
   - Розкрийте ***Application***: ***Transport Protocol Specification*** ієрархію -> ***Voice Transport*** = ***AAL2***.

a. змініть значення атрибуту ***Server Address*** і запишіть туди ***NE_DataServer***

9. Для ***NE_Data1*** і ***NE_Data2*** встановіть наступні атрибути:
   - Раскройте ***ATM Parameters*** ієрархію -> встановіть ***Queue Configuration*** в ***UBR***.
   - Розкрийте ***Application***: ***Supported Profiles*** ієрархію -> встановіть ***rows*** в 2 -> встановіть ***Profile name*** в ***FTP_P*** (для ***row*** 0) і ***EMAIL_P*** (для row 1).
10. Для ***NE_Data1***, оберіть ***Edit Attributes*** -> змініть значення атрибуту ***Client Address*** і запишіть туди ***NE_Data1***
11. Для ***NE_Data2***, оберіть ***Edit Attributes*** -> змініть значення атрибуту ***Client Address*** і запишіть туди ***NE_Data2***
12. Збережіть проект.

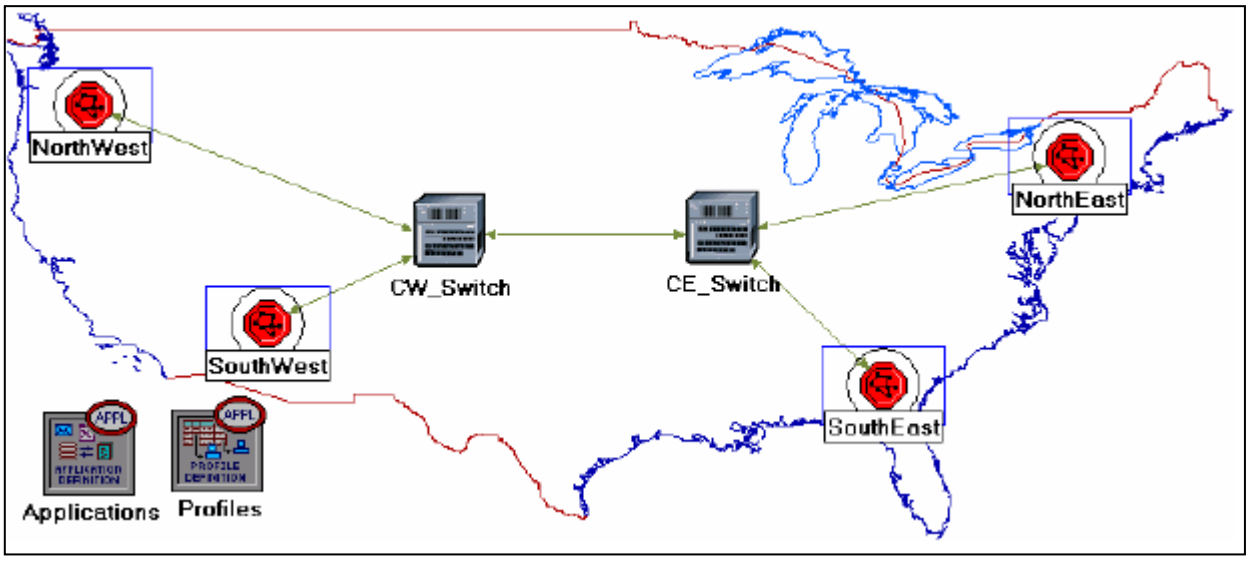
Порада: Для того щоб редагувати атрибути декількох вузлів однією операцією, виділіть по черзі всі вузли використовуючи shift і ЛКМ; після чого ***Edit Attributes*** одного з вузлів і оберіть ***Apply Changes to Selected Objects***. ***Client Address*** - це транспортний адаптаційний рівень (TAP), адреса вузла. Це значення має бути унікальним для кожного вузла. TAP модель являє однорідний інтерфейс між додатками і моделлю транспортного рівня. Всі взаємодії з віддаленим додатком через TAP організовані в сеанси. Сеанс це єдина взаємодія між двома додатками через транспортний протокол.

Додаванн підмереж, що залишилися.

1. Тепер ви можете завершити конфігурацію Північно-Східної підмережі. Для повернення в робочу область проекту натисніть на кнопку Перейти на рівень вище  .

   Підмережі інших регіонів повинні бути схожі на Північно-Східну підмережу. Відмінність буде лише в іменах і адресах клієнтів.
2. Зробіть 3 копії підмережі, яку ми тільки що створили.

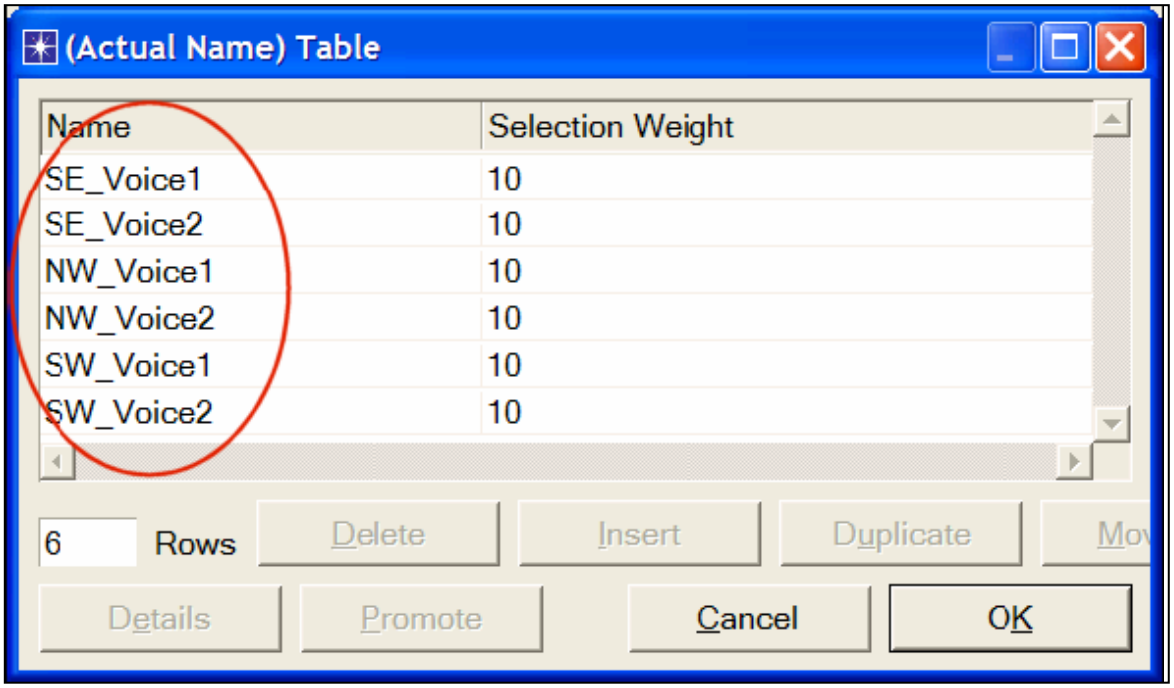
3. Змініть назву (ПКМ на вузлі => ***Set Name***) підмережі і приєднайте їх до свічу з реверсивним ***atm_adv*** як показано. (Примітка: вас попросять вибрати вузол всередині підмережі, який буде сполучений із зовнішнім ланком. Переконайтеся, що вибрали «***switch***» всередині кожної підмережі, яка буде з'єднана).



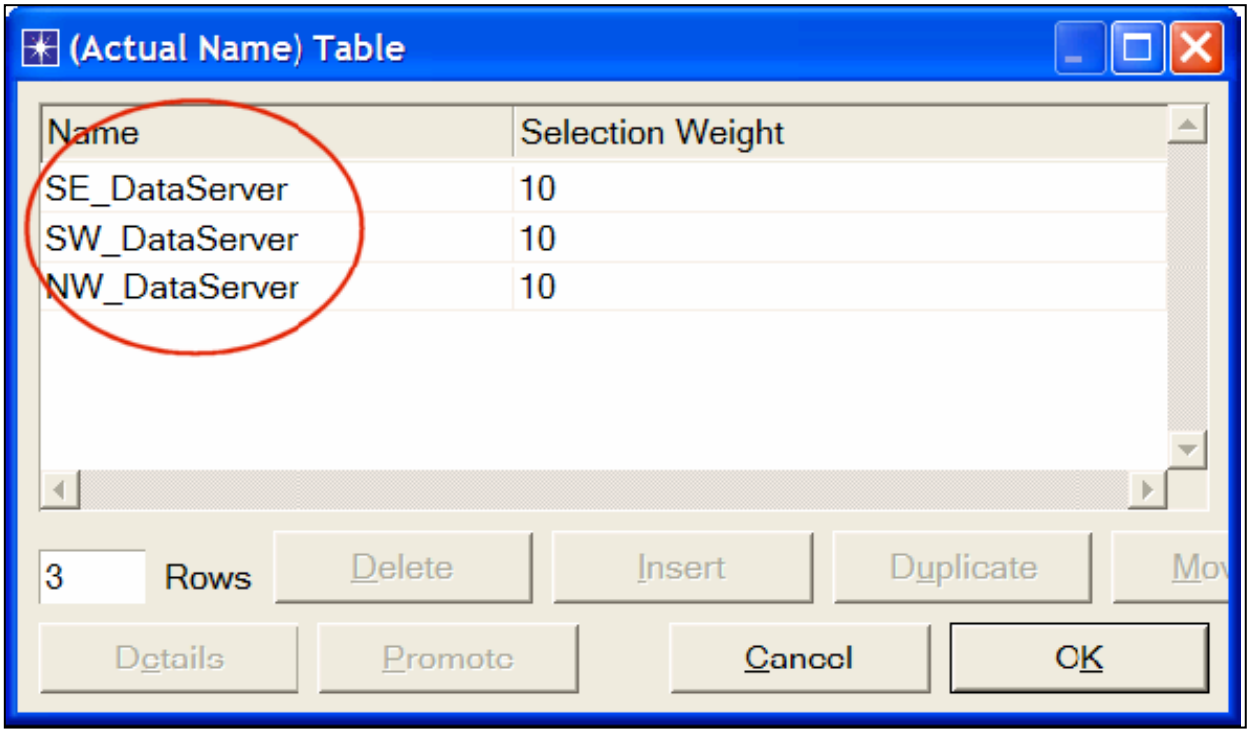
4.Змініть ***data rate*** для всіх зв'язків на ***DS1***

5. Подвійний клік для створення нової підмережі (тепер їх 4) і змініть ім'я (**name**), адресу клієнта (***client address***), і адресу сервера (***server address***) всередині цієї підмережі відповідно (наприклад замініть ***NE*** на ***SW*** для Південно-Західної підмережі (***SouthWest***)).

6. Для всіх станцій ***voice*** у всіх підмережах (усього 8 шт.), відредагуйте значення властивості ***Application***: ***Destination Preferences*** наступним чином: А) встановіть ***rows*** в 1 => встановіть символьне ім'я для ***Voice Destination*** => Натисніть на (...) під колонкою ***Actual Name*** => встановіть ***rows*** в 6 => для кожного рядка виберіть голосову станцію, яка знаходиться за межами поточної підмережі. На малюнку показані імена для однієї з голосових станцій в підмережі ***NorthEast***.



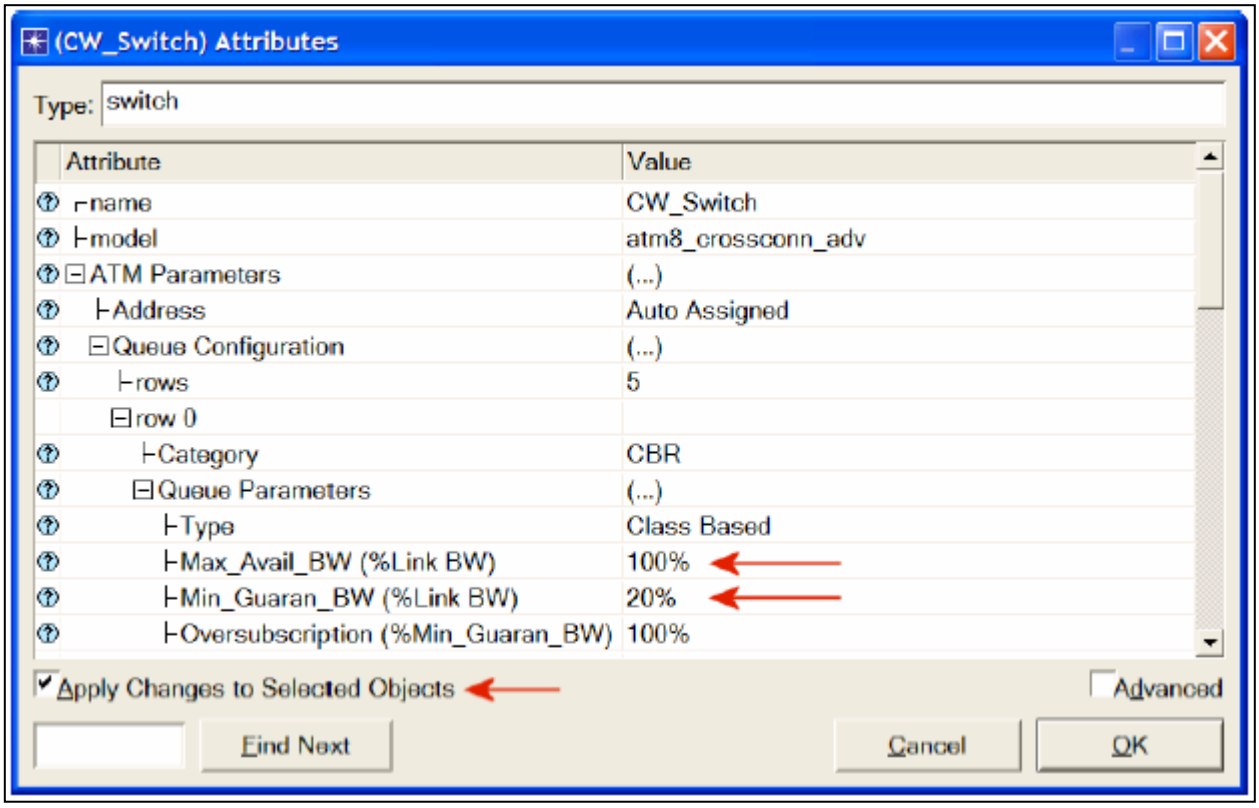
7. Підказка: щоб виконати крок 6 вам потрібно натиснути ПКМ на будь-який з голосових станцій і вибрати ***Edit Similar Nodes***. Це видасть таблицю в якій кожен вузол займає один рядок а властивості показані в колонках. Виконайте ту ж дію в цій роботі.
8. Для всіх станцій ***data*** (дані) у всіх підмережах (усього 8 шт.), Налаштуйте ***Application: Destination Preferences*** властивості як зазначено нижче: А) встановіть ***rows*** = 2 => встановіть символьне ім'я = «***FTP Server***» для одного рядка і ***Email Server*** для іншого => Для кожного з символьних імен (наприклад ***FTP Server***, ***Email Server***) натисніть на (**...**) під колонкою ***Actual Name*** => Встановіть ***rows*** = 3 => Для кождого рядка оберіть сервер даних, що не входить в поточну підмережу. На малюнку нижче показані ***actual names*** для однієї зі станцій даних в підмережі ***NorthEast***.



9. Для всіх комутаторів в мережі (всього 6 комутаторів), встановіть значення ***Max_Avail_BW*** в категорії ***CBR*** рівним 100%, як показано нижче, і ***Min_Guaran_BW*** в 20%.

Підказка:

- Для виконання 8 кроку як 1 операції, ви можете використовувати ПКМ на будь якому комутаторі і вибрати ***Similar Node***s, потім ***Edit Attributes***, і перевірити ***Apply Changes*** для вибраного об'єкта. Ця можливість працює навіть для об'єктів в різних підмережах.
- ***Max_Avail_BW*** це максимальна довжина для черги. Виклик буде прийматися в чергу тільки в тому випадку, якщо він не перевищує максимальну вимогу.

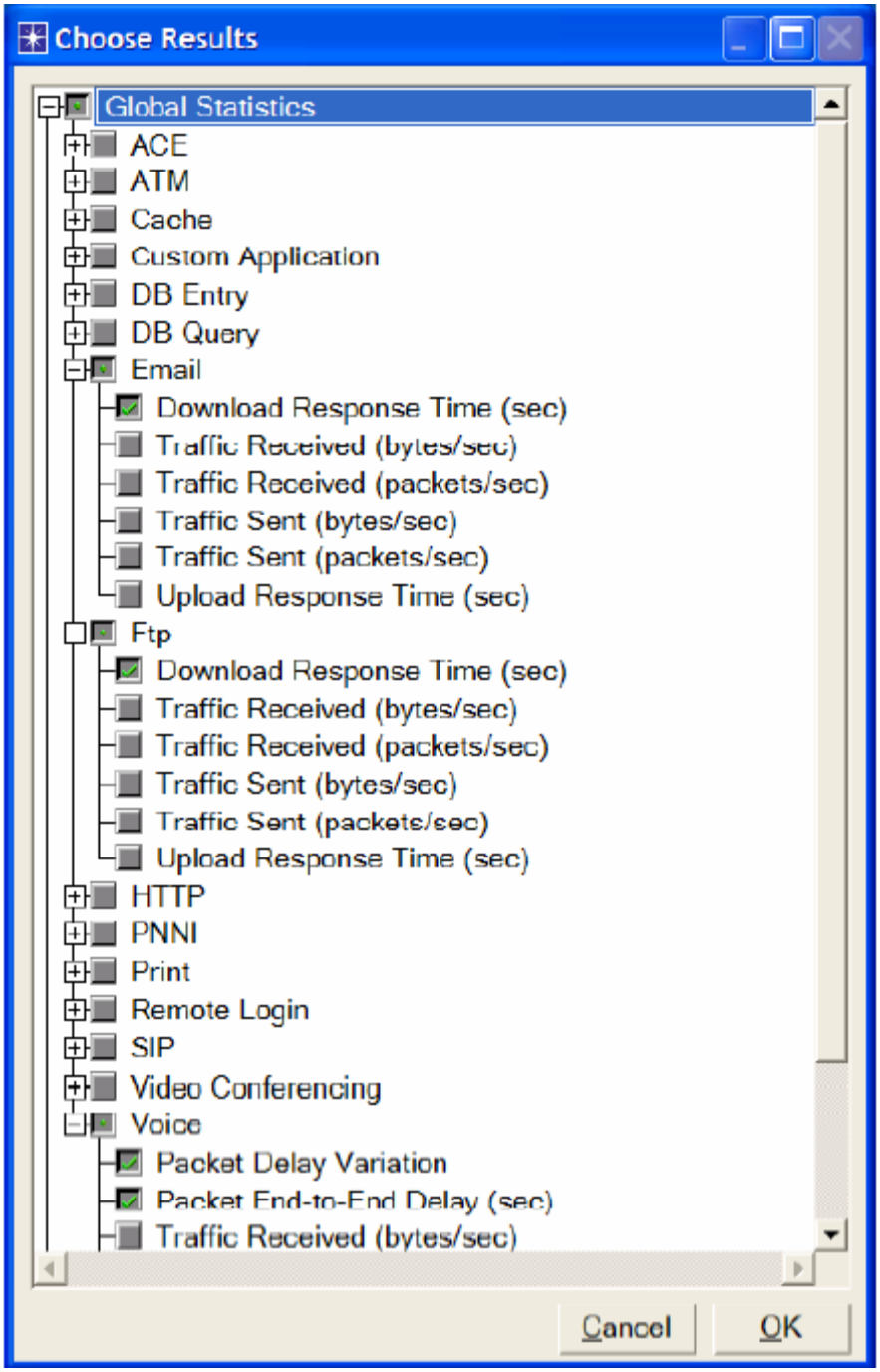


10. Збережіть проект.

Вибір статистики

Щоб протестувати продуктивність додатків, визначених у мережі, ми виберемо одну з багатьох доступних статистик. Зробимо це таким чином:

1. ПКМ де небудь у просторі проекту і оберіть ***Choose Individual Statistics*** з випадаючого меню.
2. У діалоговому вікні ***Choose Results***, виберете такі типи статистик:



3.Натисніть ***OK***.

Конфігурація моделювання

Тут нам необхідно налаштувати тривалість моделювання:

1. Клацніть на кнопці **Configure / Run Simulation**.

2. встановіть тривалість в 10.0 хвилин.

3. Клацніть ***OK***. Запуск моделювання запустимо пізніше.

Дублювання сценарію

У створених нами мережах, ми використовували ***CBR*** сервіс для мовних додатків і ***UBR*** для ***FTP*** і ***EMAIL*** додатків. Для того щоб проаналізувати ефект таких різних сервісів, ми створимо інший сценарій, подібний до ***CBR_UBR***, створений нами, але в ньому буде використовуватися тільки один клас сервісу, ***UBR***, для всіх додатків. В додаток, щоб відчути результат адаптаційного рівня ***ATM***, в новому сценарії ми будемо використовувати ***AAL5*** для мовних додатків, який краще ніж ***AAL2***.

1. Виберіть ***Duplicate Scenario*** з меню ***Scenarios*** і назвіть його **UBR_UBR** -> натисніть ***OK***.
2. Для всіх мовних станцій у всіх підмережах, реконфігуріруйте їх наступним чином: (читай примітку).

- Встановіть параметр ***ATM Application Parameters*** в ***UBR only***.
- ***ATM Parameters*** -> встановіть ***Queue Configuration*** в ***UBR***
- ***Application: Transport Protocol*** -> встановіть ***Voice Transport в AAL5***.

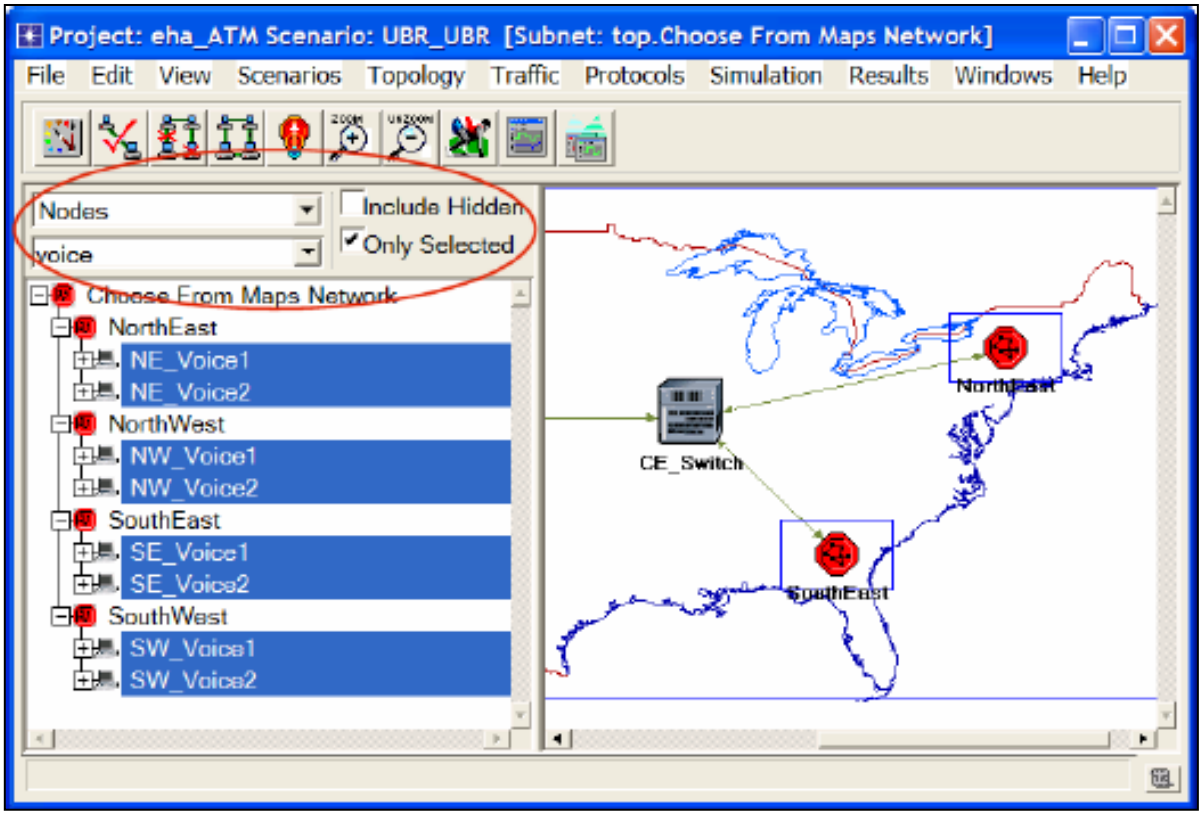
3. Збережіть проект.

Примітка:

Більш простий спосіб здійснити останні 2 кроки використовуючи ***network browser***:

- Виберіть в меню ***View Show Network Browser***
- Виберіть вузли з випадаючого меню, і перевірте поле ***Only Selected*** як показано на малюнку нижче.
- Напишіть ***voice*** в полі пошуку та натисніть ***Enter***.
- У ***Network Browser*** ви побачите список всіх виділених мовних станцій.
- ПКМ на мовнії станції в списку, виділіть ***Edit Attributes***, і оберіть ***Apply Changes to Selected Objects***.
- Виконайте зміни в налаштуваннях в кроку 2 вище.

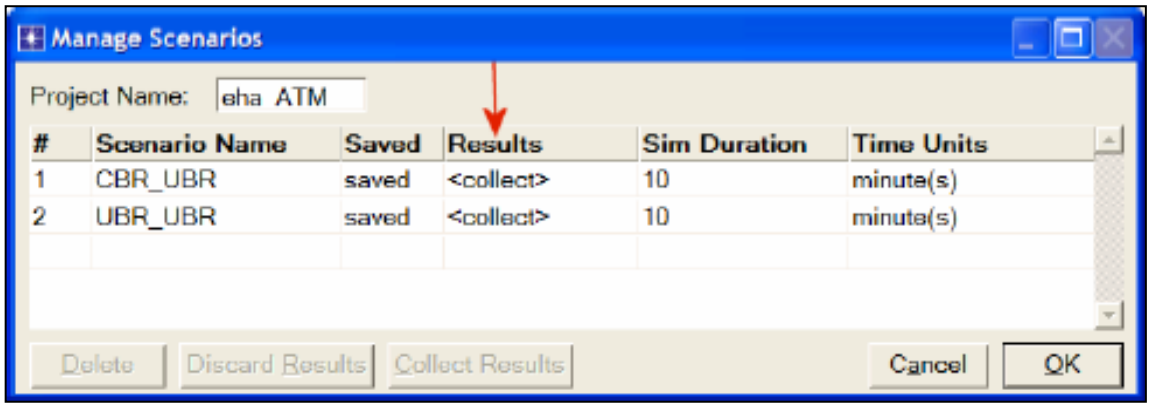
- Щоб заховати ***Network Browser***, зніміть прапорець ***Show Network Browser*** в меню ***View***.



Запуск симулятора:

Запуск симулятора для обох сценаріїв одночасно:

1. - Перейти в меню ***Scenarios***. Виберіть ***Manage Scenarios***
2. Змініть значення в колонці ***Results*** на <***collect***> або <***recollect***> для обох сценаріїв. Порівняйте з малюнком.

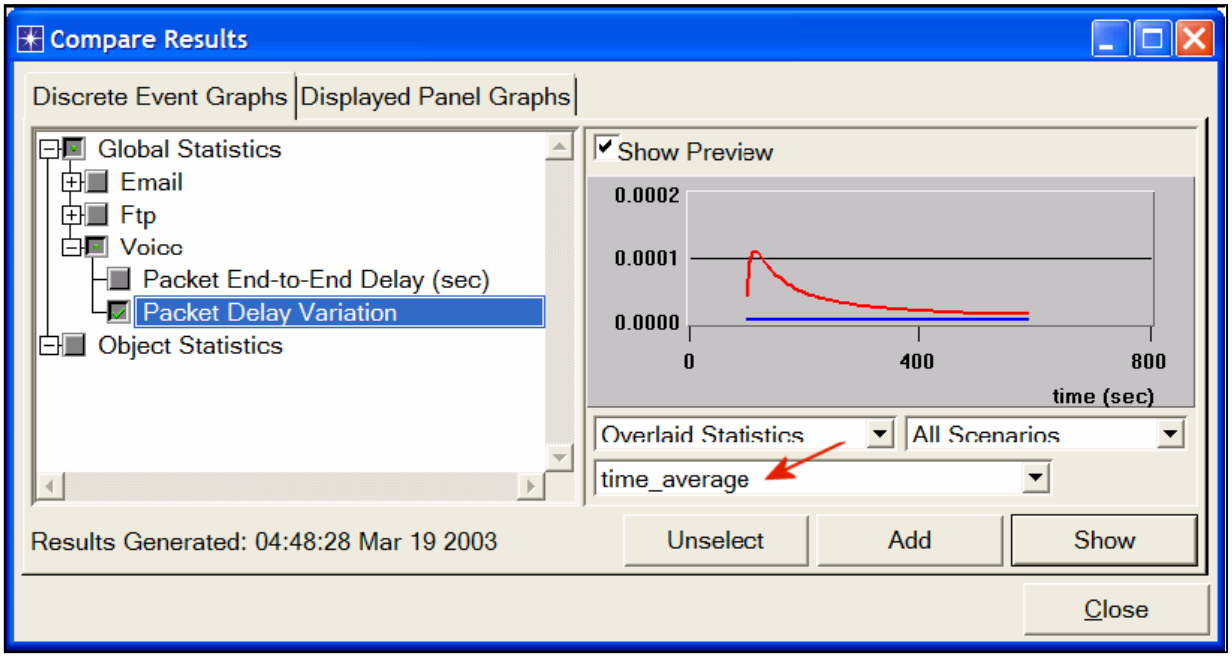


3. Натисніть ***OK*** для запуску двох симуляторів. В залежності від швидкості вашого процесора це повинно зайняти кілька хвилин до завершення.
4. Після завершення моделювання, натисніть ***Close*** для кожного сценарію
5. Збережіть проект

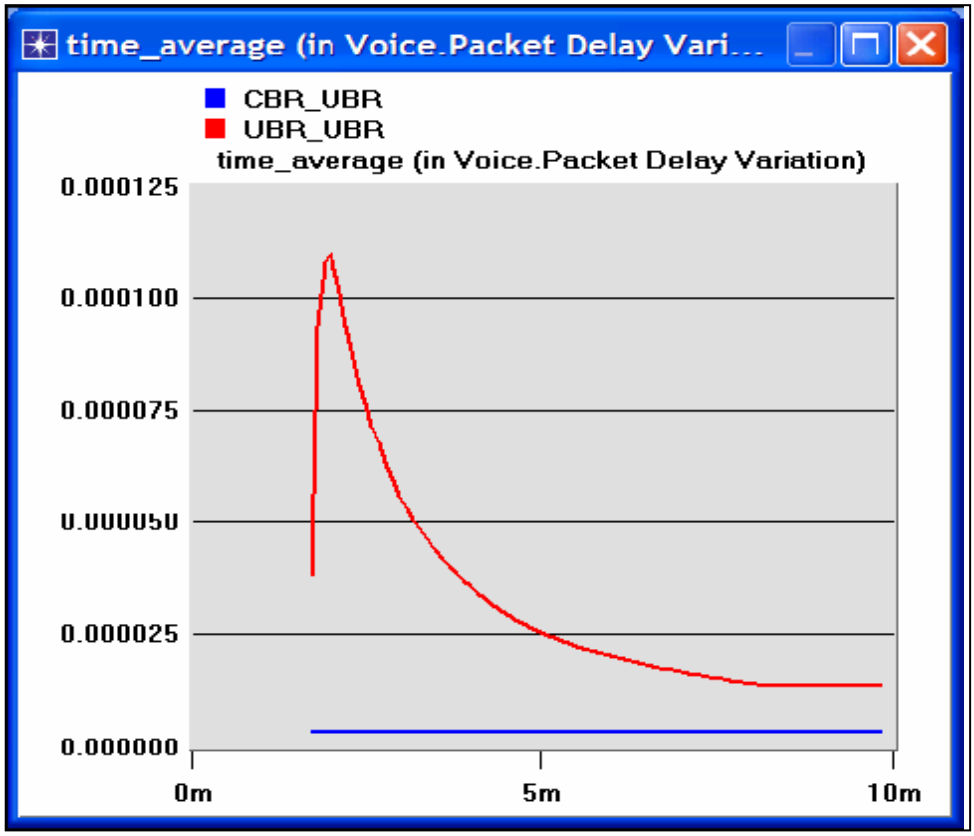
Перегляд результатів

Для перегляду та аналізу результатів зробіть наступне:

1. Оберіть ***Compare Results*** з меню ***Results***.
2. Оберіть у спадному меню в правій нижній частині діалогу ***Compare Results*** Значення ***time_average*** як показано на малюнку.



3. Оберіть голосову статистику ***Packet Delay Variation*** та натисніть ***Show***. Результуючий графік повинен нагадувати малюнок (але може трохи відрізнятися в залежності від розташування вузлів).



КОНТРОЛЬНІ ЗАПИТАННЯ

1. Аналізуючи, результат ми виявляємо, зміну затримки пакетів. Отримавши граф, ми порівнюємо, заявку безперервної передачі, час відповіді для скачування пошти та час відповіді Ftp для обох сценаріїв. Прокоментуйте результат.
2. Створіть інший сценарій як копію ***CBR_UBR*** сценарію. Назвіть новий сценарій ***Q2_CBR_ABR***. У новому сценарії використовуйте ***ABR*** клас сервісу для даних, тобто ***FTP*** або ***Email*** програм для розташування даних. Порівняйте ***CBR_ABR*** сценарій з ***CBR_UBR*** сценарієм.

Підказка:

- Для встановлювання ***ABR*** класу сервісу для вузла, встановіть ***ATM*** параметр "***ABR only***" для цієї черги.

- Для всіх комутаторів в мережі (всього 6 комутаторів), встановіть значення ***Max_Avail_BW*** в категорії ***CBR*** рівним 100%, як показано нижче, і ***Min_Guaran_BW*** в 20%.

3. Відредагуйте ***Fpt*** завдання, визначивши, в задачі вузол, розмір файлу якого буде в 2 рази більше поточного розміру (зробіть 10000 байт замість 5000). Відредагуйте ***Email*** завдання, визначивши, в задачі вузол, розмір файлу якого дорівнює п'ятірного розміром поточного файлу (зробіть 10000 замість 2000). Вивчіть, як вплинула ця зміна на виконання заявки завдання в обох ***CBR_ABR*** і ***CBR_UBR*** сценаріях.

Підказка:

Для відповіді на це питання вам, можливо, необхідно створити копію ***CBR_ABR*** і ***CBR_UBR*** сценаріїв. Імена нових сценаріїв ***Q3_CBR_UBR*** і ***Q3_UBR_UBR*** відповідно.

ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ

Підготуйте звіт, виконаний за рекомендаціями до лабораторної роботи. Звіт повинен включати відповіді на вищезгадані питання, а також графіки, які Ви отримали при моделюванні сценаріїв. Проаналізуйте результати, які Ви отримали і порівняйте ці результати з очікуваними. Включіть до звіту будь-які аномалії або незрозумілу з Вашої точки зору поведінку.

ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

- **OPNET ATM** опис моделі: в меню ***Protocols*** вибрати ***ATM → Model Usage Guide***.

Лабораторна робота №7

RIP: ROUTING INFORMATION PROTOCOL
ПРОТОКОЛ МАРШРУТИЗАЦІЇ НА БАЗІ ДИСТАНЦІЙНО-ВЕКТОРНОГО АЛГОРИТМУ

Мета роботи. Зконфігурувати і проаналізувати продуктивність моделі RIP.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Маршрутизатор в мережі повинен мати можливість дізнатися адресу призначення пакета і потім визначити, який з вихідних портів найкраще підходить для доставки пакета на цю адресу. Маршрутизатор робить вибір згідно з таблицею переадресації. Основна проблема маршрутизації: як маршрутизатори отримують дані для своїх таблиць?

Протоколи маршрутизації потрібні для того, щоб збирати таблиці маршрутизації, і, отже, таблиці переадресації. Головним завданням маршрутизації є знаходження оптимального шляху між двома вузлами, де ціна шляху визначається як сума ваг усіх ребер графа, які складають шлях. У реальних мережах трасування між вузлами реалізується за допомогою протоколів маршрутизації. Протоколи реалізують розподілений, динамічний спосіб вирішення проблеми знаходження найкоротшого шляху в умовах відмов вузлів і зв'язків, а також змін ваг ребер.

Дистанційно-векторний алгоритм є одним з основних класів алгоритмів маршрутизації. Кожен вузол складає вектор, що містить відстані до всіх інших вузлів, і розсилає цей вектор безпосереднім сусідам. RIP - канонічний приклад протоколу, побудованого на дистанційно-векторному алгоритмі. Маршрутизатори, використовують RIP, регулярно розсилають свої оголошення

(наприклад, кожні 30 секунд). Також маршрутизатор посилає оновлюючe повідомлення, коли отримане ним від іншого маршрутизатора оновлення служить причиною змін в його маршрутнії таблиці.

Внутрішній протокол маршрутизації RIP

Цей протокол маршрутизації призначений для порівняно невеликих і відносно однорідних мереж (алгоритм Белмана-Форда). Протокол розроблений в університеті Каліфорнії (Берклі), базується на розробках фірми Ксерокс і реалізує ті ж принципи, що й програма маршрутизації ***routed***, яка використовується в ОС Unix. Маршрут тут характеризується вектором відстані до місця призначення. Передбачається, що кожен маршрутизатор є відправною точкою кількох маршрутів до мереж, з якими він пов'язаний. Опис цих маршрутів зберігається в спеціальній таблиці, званої маршрутної. Таблиця маршрутизації RIP містить по запису на кожну з машин, що обслуговується (на кожен маршрут). Запис повинен включати в себе:

IP-адресу місця призначення.

Метрика маршруту (від 1 до 15; число кроків до місця призначення).

IP-адреса найближчого маршрутизатора (gateway) по дорозі до місця призначення.

Таймери маршруту.

Першим двом полям запису зобов'язана поява терміну вектор відстані (місце призначення - напрямок; метрика - модуль вектора). Періодично (раз на 30 сек) кожний маршрутизатор посилає широкомовно копію своєї маршрутної таблиці всім сусідам-маршрутизаторам, з якими пов'язаний безпосередньо. Маршрутизатор-одержувач переглядає таблицю. Якщо в таблиці присутній новий шлях або повідомлення про більш короткому маршруті, або відбулися зміни довжин шляху, ці зміни фіксуються одержувачем у своїй маршрутній таблиці.

Алгоритм побудови таблиці маршрутів

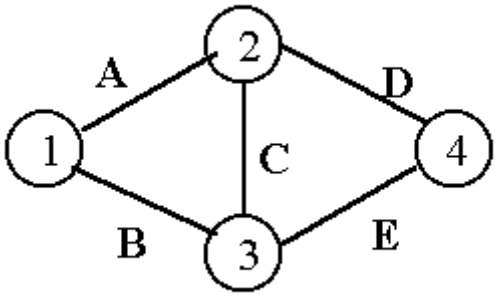
В цьому розділі для простоти будемо називати таблицею маршрутів таблицю, що є результатом діяльності протоколу RIP, як описано вище, тобто складається з рядків з полями "Мережа", "Відстань", "Наступний маршрутизатор". Записувати рядок у таблиці маршрутів будемо наступним чином: A = 2 -> (3). Це означає, що відстань від даного маршрутизатора до мережі A дорівнює 2, а дейтаграми, в мережу A, треба пересилати маршрутизатору (3).

Вектором відстаней називається набір пар ("Мережа", "Відстань до цієї мережі"), витягнутий з таблиці маршрутів. Кожну таку пару ми назвемо елементом вектора відстаней. Ми будемо записувати вектор відстаней у вигляді (A = 2, B = 1): це означає, що відстань від даного маршрутизатора до мережі A дорівнює 2, до мережі B - 1. Відстань до мережі, до якої маршрутизатор підключений безпосередньо, приймемо рівним 1.

Кожен маршрутизатор, на якому працює модуль RIP, періодично широкомовно поширює свій вектор відстаней. Вектор поширюється через всі інтерфейси маршрутизатора, підключені до мереж, що входять в RIP-систему. Кожен маршрутизатор також періодично отримує вектори відстаней від інших маршрутизаторів. Відстані в цих векторах збільшуються на 1, після чого порівнюються з даними в таблиці маршрутів, і, якщо відстань до якоїсь з мереж в отриманому векторі виявляється менше, ніж зазначено в таблиці, значення з таблиці заміщується новим (меншим) значенням, а адреса маршрутизатора, який надіслав вектор з цим значенням, записується в поле "Наступний маршрутизатор" в цьому рядку таблиці. Після цього вектор відстаней, що розсилається даними маршрутизатором, відповідно зміниться.

Приклад побудови таблиці маршрутів

Розглянемо цей процес на прикладі наступної мережі.



Приклад RIP-системи

Тут (1), (2), (3), (4) - маршрутизатори, A, B, C, D, E - мережі. Хости в мережах не показані за непотрібністю. Ми будемо стежити за формуванням таблиці маршрутів у вузлі (1). У початковий момент часу (наприклад, після подачі живлення на маршрутизатори) таблиця маршрутів у вузлі (1) виглядає наступним чином (тому вузол (1) знає тільки про ті мережі, до яких підключений безпосередньо):

A = 1 -> (1)

B = 1 -> (1)

Отже, вузол (1) розсилає в мережі A і B вектор відстаней (A = 1, B = 1).

Аналогічно вузол (2) розсилає в мережі A, C, D вектор (A = 1, C = 1, D = 1). Вузол (1) отримує цей вектор з мережі A, збільшує відстані на 1 (A = 2, C = 2, D = 2) і порівнює з даними в своїй таблиці маршрутів. Нова відстань до мережі A виявляється більше, ніж уже внесена в таблицю (A = 1), отже, нове значення ігнорується. Оскільки мережі C і D зовсім не фігурують в його таблиці маршрутів, вони туди вносяться. У вузлі (1) маємо:

A = 1 -> (1)

B = 1 -> (1)

C = 2 -> (2)

D = 2 -> (2)

Вузол (4) в свою чергу розсилає вектор (D = 1, E = 1) в мережі D і E. Вузол (2) отримує цей вектор з мережі D, збільшує відстані на 1, після чого додає собі в таблицю дані про мережу E (E = 2 -> (4)). Раніше з вузла (1) він отримав інформацію про мережу B і додав собі в таблицю рядок B = 2 -> (1). Вузол (2) розсилає в мережі A, C, D свій оновлений вектор відстаней (A = 1, B = 2, C = 1, D = 1, E = 2).

Вузол (1) отримує цей вектор від (2) з мережі A, збільшує відстані на 1: (A = 2, B = 3, C = 2, D = 2, E = 3) і зауважує, що всі зазначені відстані, крім відстані до мережі E, більше або дорівнюють значенням, наявними в його таблиці. Мережа E в таблиці вузла (1) відсутня, отже, вона туди вноситься, і у вузлі (1) ми отримуємо:

A = 1 -> (1)

B = 1 -> (1)

C = 2 -> (2)

D = 2 -> (2)

E = 3 -> (2)

Далі маршрутизатор (3), раніше не працював з якихось причин, розсилає в мережі B, C, E свій вектор (B = 1, C = 1, E = 1). Вузол (1) отримує цей вектор з мережі B, збільшує відстані на 1 і виявляє, що відстань E = 2 менше наявної в таблиці E = 3, отже запис про мережу E в таблиці замінюється на E = 2 -> (3). Інші елементи отримані від (3) вектора не викликають поновлення таблиці.

Підсумкова таблиця маршрутів маршрутизатора (1):

A = 1 -> (1)

B = 1 -> (1)

C = 2 -> (2)

D = 2 -> (2)

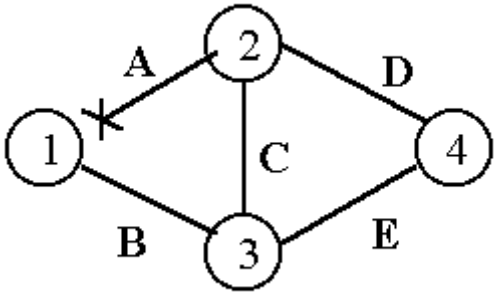
E = 2 -> (3)

На цьому алгоритм сходиться, тобто при незмінній топології системи ніякі вектори відстаней, одержувані маршрутизатором (1), більше не внесуть змін до таблиці маршрутів. Аналогічним чином алгоритм складання таблиці маршрутів працює і сходиться на інших маршрутизаторах. Зазначимо, що незважаючи на те, що таблиці маршрутів побудовані, вектори відстаней продовжують періодично широкомовно розсилатися кожним маршрутизатором. Це потрібно для оперативного реагування на раптові зміни топології системи.

Очевидно, що вид побудованої таблиці маршрутів може залежати від порядку отримання маршрутизатором векторів відстаней. Наприклад, якби вузол (1) отримав вектор від вузла (3) раніше, ніж від вузла (2), то дейтаграми в мережу З посилалися б від (1) через (3).

Зміна стану RIP-системи

З'ясуємо, що відбувається у випадку, коли стан системи несподівано змінюється, наприклад, маршрутизатор (1) відключається від мережі А.



Вузол (1) виявляє своє від'єднання від мережі А і змінює таблицю маршрутів, встановлюючи нескінченну відстань до всіх мереж, раніше досяжних через маршрутизатори, підключені до мережі А (тобто (2)). У протоколі RIP значення нескінченності дорівнює 16.

A = 16 -> (1)

B = 1 -> (1)

C = 16 -> (2)

D = 16 -> (2)

E = 2 -> (3)

Вектор відстаней, побудований на підставі цієї таблиці, розсилається в мережу B, щоб маршрутизатори, надсилаючи свої дані через (1) недосяжні мережі, якщо такі маршрутизатори існують, відповідно змінили свої маршрутні таблиці. Припустимо, у вузлі (3) була наступна таблиця маршрутів:

A = 2 -> (2)

B = 1 -> (3)

C = 1 -> (3)

D = 2 -> (4)

E = 1 -> (3)

Вузол (3) періодично і широкомовно розсилає в мережі B, C, E свій вектор відстаней (A = 2, B = 1, C = 1, D = 2, E = 1). Вузол (1) отримує цей вектор, збільшує відстані на 1: (A = 3, B = 2, C = 2, D = 3, E = 2) і зауважує, що відстані A = 3, C = 2 і D = 3 менше нескінченності отже, відповідні записи таблиці маршрутів модифікуються і вона приймає вигляд:

A = 3 -> (3)

B = 1 -> (1)

C = 2 -> (3)

D = 3 -> (3)

E = 2 -> (3)

Таким чином, вузол (1) побудував маршрути в обхід пошкодженої ділянки і відновив досяжність всіх мереж.

Протокол RIP повинен бути здатний обробляти три типи помилок: 1. Циклічні маршрути. Так як в протоколі немає механізмів виявлення замкнутих маршрутів, необхідно або сліпо вірити партнерам, або вживати заходів для блокування такої можливості.

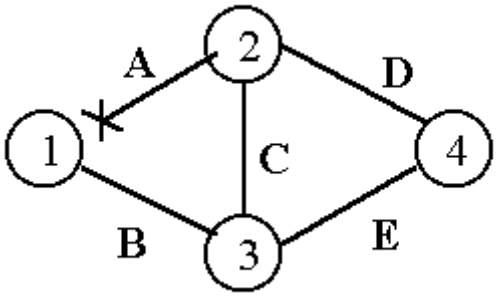
2. Для придушення нестабільностей RIP повинен використовувати мале значення максимально можливого числа кроків (<16).

3. Повільне поширення маршрутної інформації з мережі створює проблеми при динамічній зміні маршрутної ситуації (система не встигає за змінами). Мале граничне значення метрики поліпшує збіжність, але не усуває проблему.

Невідповідність маршрутної таблиці реальній ситуації типово не тільки для RIP, але характерно для всіх протоколів, що базуються на векторі відстані, де інформаційні повідомлення актуалізації несуть в собі тільки пари кодів: адреса місця призначення і відстань до нього.

Зациклення

На жаль, поведінка дистанційно-векторних протоколів (і зокрема, протоколу RIP) при зміні топології системи не завжди коректна і передбачувана. Розглянемо вищеописану ситуацію з від'єднанням вузла (1) від мережі A.



Зміна стану RIP-системи

Ми припускали, що вузол (3) не відправляв дейтаграми через вузол (1) (і, отже, зміна таблиці маршрутів у вузлі (1) не вплинула на таблицю вузла (3)). Припустимо тепер, що (3) відправляв дейтаграми в мережу A через (1), тобто таблиця у вузлі (3) мала вигляд:

A = 2 -> (1)

B = 1 -> (3)

C = 1 -> (3)

D = 2 -> (4)

E = 1 -> (3)

Після від'єднання (1) від мережі A вузол (3) отримує від (1) вектор (A = 16, B = 1, C = 16, D = 16, E = 2). Проаналізувавши цей вектор, (3) робить висновок, що всі зазначені в ньому відстані більше значень, що містяться в його маршрутної таблиці, на підставі чого цей вектор вузлом (3) ігнорується. У свою чергу вузол (3) розсилає в мережі B, C, E вектор (A = 2, B = 1, C = 1, D = 2, E = 1). Вузол (1) отримує цей вектор, збільшує відстані на 1: (A = 3, B = 2, C = 2, D = 3, E = 2) і зауважує, що відстані A = 3, C = 2 і D = 3 менше нескінченності, отже, відповідні записи таблиці маршрутів у вузлі (1) модифікуються і вона приймає вигляд:

A = 3 -> (3)

B = 1 -> (1)

C = 2 -> (3)

D = 3 -> (3)

E = 2 -> (3)

Очевидно, після цього вміст таблиць вузлів (1) і (3) стабілізується. Розглянемо тепер записи про досягнення мережі A в таблицях маршрутизаторів (1) і (3).

У вузлі (1): A = 3 -> (3)

У вузлі (3): A = 2 -> (1)

Таким чином, виникло зациклення: дані, адресовані в мережу A, будуть пересилатися між вузлами (1) і (3) до тих пір, поки не закінчиться час життя дейтаграм і вони не будуть знищені. Для того, щоб уникнути зациклення, в алгоритм розсилки векторів відстаней вносяться такі доповнення.

1. Якщо дейтаграми, адресовані в мережу X, надсилаються через маршрутизатор G, що знаходиться в мережі N, то у векторі відстаней, розісланому в мережі N, відстань до мережі X не вказується. У нашому прикладі вузол (3) буде розсилати в мережі B вектор (B = 1, C = 1, D = 2, E = 1). Елемент A = 2 не буде включений в цей вектор, тому що дейтаграми в мережу A відправляються вузлом (3) через вузол (1), а вузол (1) знаходиться в мережі B. При розсилці вузлом (3) вектора відстаней в інші мережі елемент A = 1 буде вказано (але не будуть вказані якісь інші елементи).

2. Якщо маршрутизатор G оголошує нову відстань до мережі X, то ця відстань вноситься в таблиці маршрутів вузлів, які відправляють дейтаграми в мережу X через G, незалежно від того, більше вона чи менше вже внесеної в таблиці відстані.

У нашому прикладі це означає, що якщо в маршрутній таблиці вузла (3) записано A = 1 -> (1) і (3) отримує від (1) вектор з елементом A = 16, то незважаючи на те, що 1 менше нескінченності, вузол (3) модифікує запис в таблиці: A = 16 -> (1).

Очевидно, що при виконанні вищевказаних умов, зациклення, розглянутого в прикладі, не утворюється і будуються коректні маршрути. Однак таким чином усуваються далеко не всі випадки зациклення.

Існує модифікація доповнення 1, що дозволяє ліквідувати складніші особливі ситуації, в тому числі, деякі випадки рахунку до нескінченності (див. також наступний пункт):

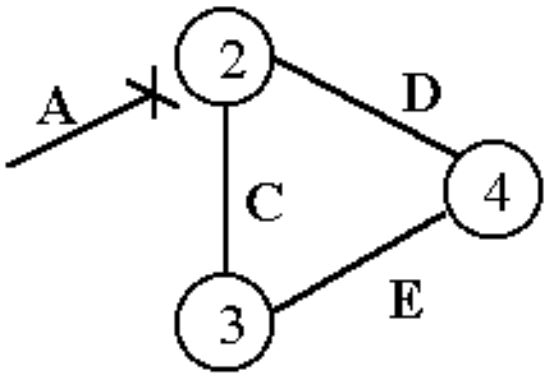
1A. Якщо дейтаграми, адресовані в мережу X, надсилаються через маршрутизатор G, що знаходиться в мережі N, то у векторі відстаней, розісланому в мережі N, відстань до мережі X покладається рівним нескінченності.

Універсальним методом виключення помилок при маршрутизації є використання достатньо великої витримки, перед тим як використовувати

інформацію про зміну маршрутів. В цьому випадку до моменту зміни маршруту ця інформація стане доступною всім учасникам процесу маршрутизації. Але всі перелічені методи і деякі інші відомі алгоритми, вирішуючи одну проблему, часто вносять інші. Багато з цих методів можуть за певних умов викликати лавину широкомовних повідомлень, що також дезорганізує мережу. Саме мала швидкість встановлення маршрутів в RIP (та інших протоколах, орієнтованих на вектор відстані) і є причиною їх поступового витіснення іншими протоколами.

Рахунок до нескінченності

Розглянемо наступну систему мереж:



Приклад RIP-системи (ілюстрація рахунку до нескінченності)

Спочатку мережа A була приєднана до вузла (2), але в якийсь момент часу сталася аварія і мережа A виявилася ізольованою.

До моменту аварії маршрутизатори мали такі записи щодо мережі A:

Вузол (2) A = 1 -> (2)

Вузол (3) A = 2 -> (2)

Вузол (4) A = 2 -> (2)

Негайно після аварії запис в таблиці маршрутів вузла A змінюється на A = 16 -> (2), це говорить про те, що мережа A недосяжна, а точніше, що мережа A через вузол (2) недосяжна. Вектор відстаней, що розсилається з (2), з елементом

A = 16 досягає вузла (3), але з якоїсь причини затримується на шляху в (4). Згідно з доповненнями до алгоритму розсилки векторів відстаней, наведених у попередньому пункті, вузол (3) вносить в свою таблицю запис A = 16 -> (2) і розсилає вектор з елементом A = 16. В цей момент вузол (4), до якого повідомлення від вузла (2) про недосяжність мережі A ще не дійшло, розсилає в мережі E свій вектор з елементом A = 2. Вузол (3) отримує цей вектор, додає до відстані 1 і зауважує, що воно менше записаного в таблиці (нескінченність), отже, у таблиці маршрутів вузла (3) з'являється запис A = 3 -> (4). Вектор відстаней з елементом A = 3 розсилається вузлом (3) в мережі C і досягає вузла (2). Вузол (2), керуючись тими ж міркуваннями, що й вузол (3) раніше, модифікує свою таблицю: A = 4 -> (3). Приблизно в цей час вузол (4) отримує нарешті вектор A = 16, відправлений після аварії вузлом (2), але слідом за цим з вузла (2) приходить вектор A = 4, який вузол (2) розсилає в мережі D. Оскільки (4) відправляє дейтаграми в мережу A через (2), він зобов'язаний реагувати на будь-які оголошення вузлом (2) відстані до мережі A. Тому в таблиці вузла (4) з'являється A = 5 -> (2).

Відповідний вектор від вузла (4) з елементом A = 5 досягає по мережі E вузол (3), у таблиці маршрутів якого зазначено, що дейтаграми в мережу A він відправляє через (4). Отже, вузол (3) зобов'язаний реагувати на будь-які оголошення вузлом (4) відстані до мережі A. Тому в таблиці вузла (3) з'являється A = 6 -> (4). Вектор від вузла (3) з елементом A = 6 досягає по мережі C вузол (2), в таблиці маршрутів якого зазначено, що дейтаграми в мережу A він відправляє через (3). Отже, вузол (2) зобов'язаний реагувати на будь-які оголошення вузлом (3) відстані до мережі A. Тому в таблиці вузла (2) з'являється A = 7 -> (3).

Далі все повторюється по колу до тих пір, поки відстань до A не стане рівною нескінченності в таблицях всіх трьох маршрутизаторів. Незважаючи на це протягом "рахунку до нескінченності" мережа A вважається досяжною,

оскільки відстань до неї вважається кінцевою, і всі дейтаграми, адресовані в мережу А, відправляються маршрутизаторами згідно їх таблиць, тобто по колу, що не можна визнати розумною і коректної маршрутизацією.

Існують і більш складні ситуації, коли виникає необхідність "рахунку до нескінченності". Щоб зменшити негативний ефект цього явища, значення нескінченності не повинно бути велике. У протоколі RIP воно дорівнює 16, що в свою чергу обмежує розмір RIP-системи.

Реалізація протоколу RIP

Існують дві версії протоколу RIP: RIP-1 і RIP-2. Версія 2 має деякі удосконалення, як то: можливість маршрутизації мереж за моделлю CIDR (крім адреси мережі передається і маска), підтримка мультікастінга, можливість використання аутентифікації RIP-повідомлень і ін.

Типи і формат повідомлень

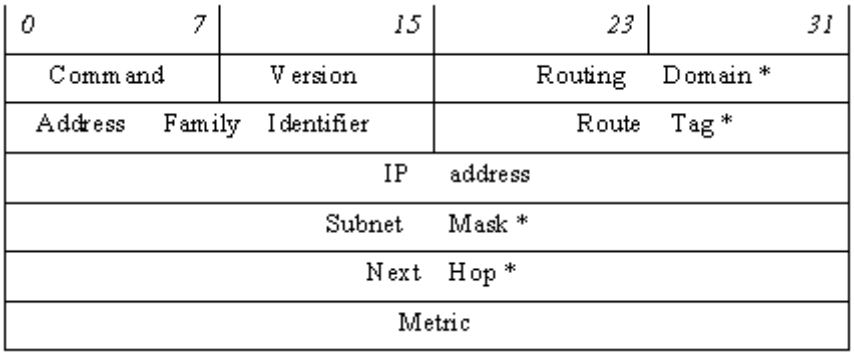
У протоколі RIP є два типу повідомлень, якими обмінюються маршрутизатори:

• відповідь (response) - розсилка вектора відстаней;

• запит (request) - маршрутизатор (наприклад, після свого завантаження) запитує у сусідів їх маршрутні таблиці або дані про певний маршрут.

Обмін повідомленнями відбувається по порту 520 UDP.

Формат повідомлень обох типів однаковий:



Поля, помічені знаком *, відносяться до версії 2; в повідомленнях RIP-1 ці поля повинні бути обнулені.

Повідомлення RIP складається з 32-бітного слова, що визначає тип повідомлення і версію протоколу (плюс "Routing Domain" у версії 2), за яким слідує набір з одного і більше елементів вектора відстаней. Кожен елемент вектора відстаней займає 5 слів (20 октетів) (від початку поля "Address Family Identifier" до кінця поля "Metric" включно). Максимальне число елементів вектора - 25, якщо вектор довше, він може розбиватися на кілька повідомлень.

Поле "Command" визначає тип повідомлення: 1 - request, 2 - response; поле "Version" - версію протоколу (1 або 2).

Поле "Address Family Identifier" містить значення 2, яке позначає сімейство адрес IP, інші значення не визначені. Поля "IP address" і "Metric" містять адресу мережі і відстань до неї.

Додатково до полів версії 1 у другій версії визначені наступні.

"Routing Domain" - ідентифікатор RIP-системи, до якої належить дане повідомлення; часто - номер автономної системи. Використовується, коли до одного фізичного каналу підключені маршрутизатори з декількох автономних систем, в кожній автономній системі підтримується своя таблиця маршрутів. Оскільки повідомлення RIP розсилаються всім маршрутизаторам, підключеним до мережі, потрібно розрізняти повідомлення, пов'язані з "своєю" і "чужою" автономною системою.

"Route Tag" - використовується як мітка для зовнішніх маршрутів при роботі з протоколами зовнішньої маршрутизації.

"Subnet Mask" - маска мережі, адреса якої міститься в полі IP address. RIP-1 працює тільки з класової моделлю адрес.

"Next Hop" - адреса наступного маршрутизатора для даного маршруту, якщо він відрізняється від адреси маршрутизатора, що послав це повідомлення. Це поле використовується, коли до одного фізичного каналу підключені

маршрутизатори з декількох автономних систем і, отже, деякі маршрутизатори "чужої" автономної системи фізично можуть бути досягнуті безпосередньо, минаючи прикордонний (логічно підключений до обох автономних систем) маршрутизатор. Про це прикордонний маршрутизатор і оголошує в полі "Next Hop".

Адреса 0.0.0.0 в повідомленні типу "відповідь" позначає маршрут, що веде за межі RIP-системи. У повідомленні типу "запит" ця адреса означає запит інформації про всіх маршрути (повного вектора відстаней). Вказівка в повідомленні типу "запит" адреси конкретної мережі означає запит елемента вектора відстаней тільки для цієї мережі - такий режим використовується зазвичай тільки в налагоджувальних цілях.

Аутентифікація може проводитися протоколом RIP-2 для обробки тільки тих повідомлень, які містять правильний аутентифікаційні код. При роботі в такому режимі перший 20-октетний елемент вектора відстаней, наступний безпосередньо за першим 32-бітним словом RIP-повідомлення, є сегментом аутентифікації. Він визначається за значенням поля "Address Family Identifier", рівному в цьому випадку 0xFFFF. Наступні 2 октету цього елемента визначають тип аутентифікації, а інші 16 октетів містять аутентифікаційний код. Таким чином, в RIP-повідомленні з аутентифікацією може передаватися не 25, а тільки 24 елемента вектора відстаней, які слідують за сегментом аутентифікації. До теперішнього моменту надійного алгоритму аутентифікації для протоколу RIP не розроблено; стандартом визначена тільки аутентифікація за допомогою звичайного пароля (значення поля "Тип" дорівнює 2).

Робота протоколу RIP

Для кожного запису в таблиці маршрутів існує час життя, контрольоване таймером. Якщо для будь-якої конкретної мережі, внесеної в таблицю маршрутів, протягом 180 с. не отриманий вектор відстаней, що підтверджує або

встановлює нову відстань до даної мережі, то мережа буде відзначена як недосяжна (відстань дорівнює нескінченності). Через певний час модуль RIP виробляє "збірку сміття" - видаляє з таблиці маршрутів всі мережі, відстань до яких нескінченна.

При отриманні повідомлення типу "відповідь" для кожного елемента вектора відстаней, що міститься в ньому, модуль RIP виконує наступні дії:

• перевіряє коректність адреси мережі і маски, зазначених у повідомленні;

• перевіряє, чи не перевищує метрика (відстань до мережі) нескінченності;

• некоректний елемент ігнорується;

• якщо метрика менше нескінченності, вона збільшується на 1;

• проводиться пошук мережі, зазначеної в розглянутому елементі вектора відстаней, у таблиці маршрутів;

• якщо запис про таку мережу в таблиці маршрутів відсутній і метрика в отриманому елементі вектора менше нескінченності, мережа вноситься в таблицю маршрутів із зазначеною метрикою; в поле "Наступний маршрутизатор" заноситься адреса маршрутизатора, який надіслав повідомлення; запускається таймер для цього запису в таблиці;

• якщо шуканий запис присутній в таблиці з метрикою більше, ніж оголошена в отриманому векторі, в таблицю вносяться нові метрика і, відповідно, адреса наступного маршрутизатора; таймер для цього запису перезапускається;

• якщо шуканий запис присутній в таблиці і відправником отриманого вектора був маршрутизатор, зазначений в полі "Наступний маршрутизатор" цього запису, то таймер для цього запису перезапускається, більше того, якщо при цьому метрика в таблиці відрізняється від метрики в отриманому векторі відстаней, в таблицю вноситься значення метрики з отриманого вектора;

• у всіх інших випадках розглянутий елемент вектора відстаней ігнорується.

Повідомлення типу "відповідь" розсилаються модулем RIP кожні 30 с по широкомовній або мультікастінговій (тільки RIP-2) адресі; розсилання "відповіді" може відбуватися також поза графіком, якщо маршрутна таблиця була змінена (triggered response). Стандарт вимагає, щоб triggered response розсилався не негайно після зміни таблиці маршрутів, а через випадковий інтервал тривалістю від 1 до 5 с. Цей захід дозволяє дещо понизити навантаження на мережу.

У кожну з мереж, підключених до маршрутизатора, розсилається свій власний вектор відстаней, побудований з урахуванням доповнення 1 (1A), сформульованого вище. Там, де це можливо, адреси мереж агрегуються (узагальнюються), тобто декілька підмереж з сусідніми адресами об'єднуються під одною, більш загальною адресою з відповідною зміною маски.

У разі triggered response надсилається інформація тільки про ті мережі, записи про які були змінені.

Інформація про мережі з нескінченною метрикою надсилається тільки в тому випадку, якщо вона була недавно змінена.

При отриманні повідомлення типу "запит" з адресою 0.0.0.0 маршрутизатор розсилає в відповідну мережу звичайне повідомлення типу відповідь. При отриманні запиту з будь-яким іншим значенням у полі (полях) "IP Address" надсилається відповідь, що містить інформацію тільки про мережі, які вказані. Така відповідь посилається на адресу маршрутизатора що її запросив (не широкомовно), при цьому додаток 1 (1A) не враховується.

Конфігурування RIP

Загальний порядок дій при конфігуруванні модуля RIP наступний:

1. Вказати, які мережі, підключені до маршрутизатора, будуть включені в RIP-систему;
2. Вказати "nonbroadcast networks", тобто мережі зі статичної маршрутизацією (наприклад, тупикові мережі, приєднані до зовнішнього світу через єдиний шлюз), куди не потрібно розсилати вектори відстаней;
3. Вказати "permanent routes" - статичні маршрути, наприклад, маршрут за замовчуванням за межі автономної системи.

Протокол RIP дуже простий і до сих пір продовжує використовуватися в системах з простою топологією, але має недоліки, які не дозволяють застосовувати його у великих і складних системах.

По-перше, мале значення нескінченності (через ефект "рахунок до нескінченності") обмежує розмір RIP-системи чотирнадцятьма проміжними маршрутизаторами в будь-якому напрямку. Крім того, з тієї ж причини вельми скрутно використання складних метрик, що враховують не просто кількість проміжних маршрутизаторів, але і швидкість і якість каналу зв'язку (чим гірше (повільніше) канал, тим більше метрика).

По-друге, саме явище рахунку до нескінченності викликає збої в маршрутизації.

По-третє, широкомовна розсилка векторів відстаней кожні 30 секунд погіршує пропускну здатність мережі.

По-четверте, час сходження алгоритму при створенні маршрутних таблиць досить велика (в порівнянні з протоколами стану зв'язків).

По-п'яте, незважаючи на те, що кожен маршрутизатор починає періодичну розсилку своїх векторів, взагалі кажучи, у випадковий момент часу (наприклад, після включення), через деякий час в системі спостерігається ефект синхронізації маршрутизаторів, схожий з ефектом синхронізації оплесків. Всі маршрутизатори розсилають свої вектора в один і той же момент часу, що

призводить до великих піків трафіку і відмов в маршрутизації дейтаграм під час обробки великої кількості одночасно отриманих векторів.

Протокол RIP описаний в RFC-1058 (версія 1) і RFC-1388 (версія 2).

У цій лабораторній роботі ви побудуєте мережу, що використовує RIP як протокол маршрутизації. Ви проаналізуєте таблиці маршрутизації, що зберігаються в маршрутизаторах, і поспостерігати, як RIP реагує на обриви зв'язків.

МЕТОДИЧНІ ВКАЗІВКИ

Створення нового проекту

1. Запустіть ***OPNET IT Guru Academic Edition*** ➔ Виберіть ***New*** з меню ***File***.
2. Виберіть ***Project*** і натисніть ***OK*** ➔ Назвіть проект <ваші_ініціали> ***_RIP***, і сценарій ***NO_Failure*** ➔ Натисніть ***OK.***
3. У діалоговому вікні ***Startup Wizard: Initial Topology*** переконайтеся, що вибрано ***Create Empty Scenario*** ➔ Натисніть ***Next*** ➔ Виберіть ***Campus*** з ***Network Scale list*** ➔Натисніть ***Next*** три рази ➔Натисніть ***OK.***

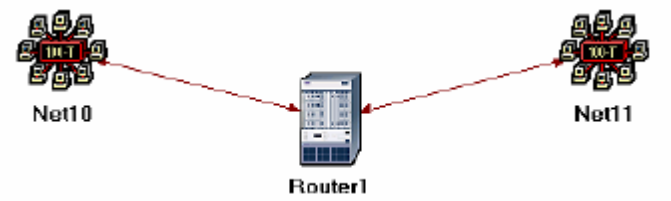
Створення та конфігурування мережі

Модель вузлів ***ethernet4_slip8_gtwy*** являє собою IP-орієнтований шлюз, що підтримує чотири інтерфейси ***Ethernet*** концентраторів і вісім послідовних інтерфейсів. IP-пакети, що приходять на кожен інтерфейс, маршрутизуються на відповідний вихідний інтерфейс, грунтуючись на IP-адресі одержувача. ***Routing Information Protocol*** (***RIP***) або ***Open Shortest Path First*** (***OSPF***) протокол можуть використовуватися для динамічного автоматичного створення таблиць маршрутизації шлюзу і вибору шляхів адаптивним методом.

Ініціалізація мережі

1. Діалогове вікно ***Object Palette*** має бути на робочому просторі вашого проекту. Якщо воно не там, відкрийте його натисканням  . Переконайтеся, що ***internet_toolbox*** обран з меню, що випадає в палітрі об'єктів.
2. Додайте на робочий простір наступні об'єкти з палітри: один маршрутизатор ***ethernet4_slip8_gtwy*** і два об'єкти ***100BaseT_LAN***.

   Для того, щоб додати об'єкт з палітри, натисніть на його іконку в палітрі об'єктів ➔ Перемістіть миша на робочий простір ➔Натисніть ЛКМ, щоб помістити об'єкт на робочий простір ➔ Натисніть ПКМ для того, щоб припинити створення об'єктів цього типу.
3. Використовуйте двонаправлені з'єднання ***100BaseT*** для з'єднання об'єктів, які ви тільки що додали, в наступну фігуру:



Перейменуйте об'єкти, як показано на малюнку (ПКМ на вузлі ➔ ***Set Name***).

4. Закрийте діалогове вікно ***Object Palette***.
5. Збережіть проект.

Конфігурація маршрутизатора

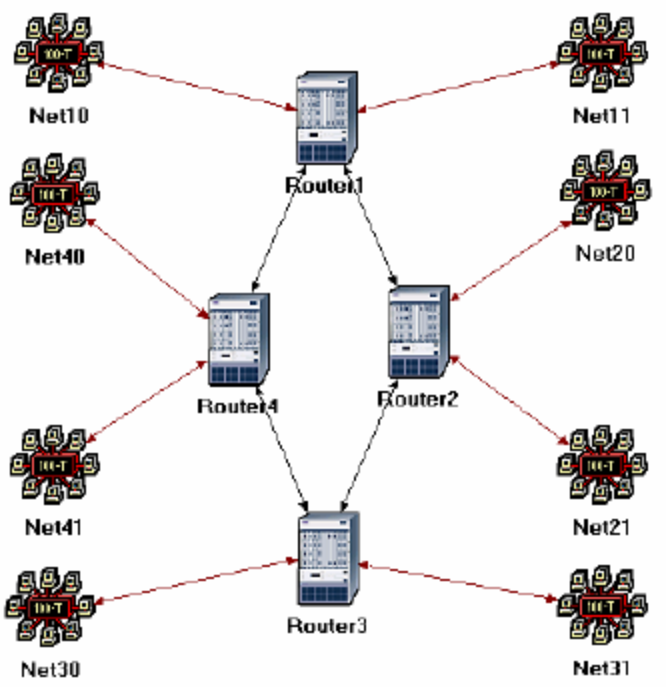
1. ПКМ на ***Router1*** ➔ ***Edit Attributes*** ➔ Розгорніть ***IP Routing Parameters*** і встановіть наступне:

   Routing Table Export = ***Once at End of Simulation***. Це змусить маршрутизатор зберегти свою таблицю маршрутизації в лог при закінченні моделювання.
2. Натисніть ***OK*** і збережіть проект.

   Додавання мереж, що залишилися:

   ! Швидкість передачі даних для з'єднання PPP_DS3: 44.736 Mbps.

3. Виділіть і виберіть (використовуючи ***shift*** і ЛКМ) всі п'ять об'єктів, які знаходяться на вашому робочому просторі (один маршрутизатор, дві мережі і два з'єднання).
4. Натисніть ***Ctrl + C*** для копіювання та натисніть ***Ctrl + V***, щоб вставити їх.
5. Повторіть крок 2 три рази, щоб створити 3 копії об'єктів, і збудуйте їх, як показано на малюнку. Змініть назви об’єктів.



6. З'єднайте маршрутизатори, як на малюнку, використовуючи з'єднання ***PPP_DS3***.

Вибір статистики

RIP traffic (***RIP***-трафік) - це загальна кількість трафіку оновлень ***RIP*** (в bits) відправлених / отриманих в секунду усіма вузлами, що використовують ***RIP*** як протокол маршрутизації через ***IP***-інтерфейси вузла.

Total Number of Updates (Загальна кількість оновлень) - кількість оновлень таблиці маршрутизації на даному сайті (наприклад, в результаті додавання нового шляху, видалення існуючого шляху, і т.д.).

Для дослідження продуктивності протоколу RIP, ми зберемо такі статистичні дані:

1. Клацніть ПКМ в будь-якому місці робочого простору і виберіть ***Choose Individual Statistics*** з контекстного меню.
2. У діалоговому вікні ***Choose Results*** виберіть наступну статистику:
    a. ***Global Statistics ➔ RIP ➔ Traffic Sent (bits / sec).***
    b. ***Global Statistics ➔ RIP ➔ Traffic Received (bits / sec).***
    c. ***Nodes Statistics ➔ Route Table ➔ Total Number of Updates.***
3. Натисніть ***OK*** і збережіть проект.

Конфігурація та моделювання

Auto Addressed (Авто адресація) означає, що ***IP***-інтерфейси отримають ***IP***-адреси автоматично під час моделювання. Клас адрес (наприклад, A, B, або C) визначається на основі кількості вузлів в мережі, що розробляється. Маска підмережі, пов'язана з інтерфейсом - маска за замовчуванням для даного класу.

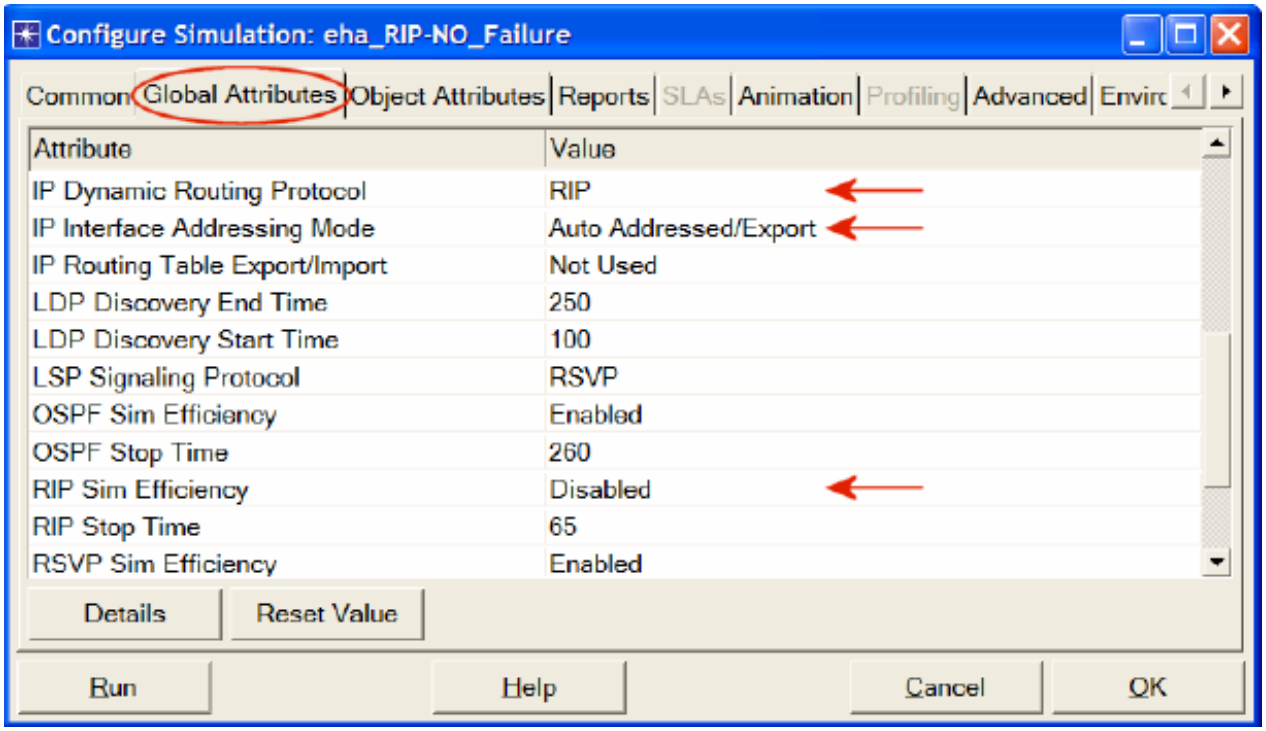
Export (Експорт) змусить систему експортувати роздані інтерфейсам IP-адреси в файл (назва файлу: <ім'я_мережі> - ip_addresses.gdf), який буде збережений в основній директорії моделі.

Тут нам необхідно конфігурувати декілька параметрів моделювання:

1. Натисніть на  і з'явиться вікно ***Configure Simulation***.
2. Визначте на ***10.0*** хвилин.
3. Натисніть на закладці ***Global Attributes*** і змініть наступні атрибути:
    a. ***IP Dynamic Routing Protocol*** = ***RIP***. Це встановить ***RIP*** як протокол маршрутизації для всіх маршрутизаторів.
    b. ***IP Interface Addressing Mode*** = ***Auto Addressed / Export***.
    c. ***RIP Sim Efficiency*** = ***Disabled***. Якщо цей атрибут дозволений, ***RIP*** зупиниться після "***RIP Stop Time***." Але він повинен продовжувати

оновлювати таблиці в разі будь-якої зміни в мережі (як ми побачимо в наступному сценарії).

4. Натисніть ***OK*** і збережіть проект.



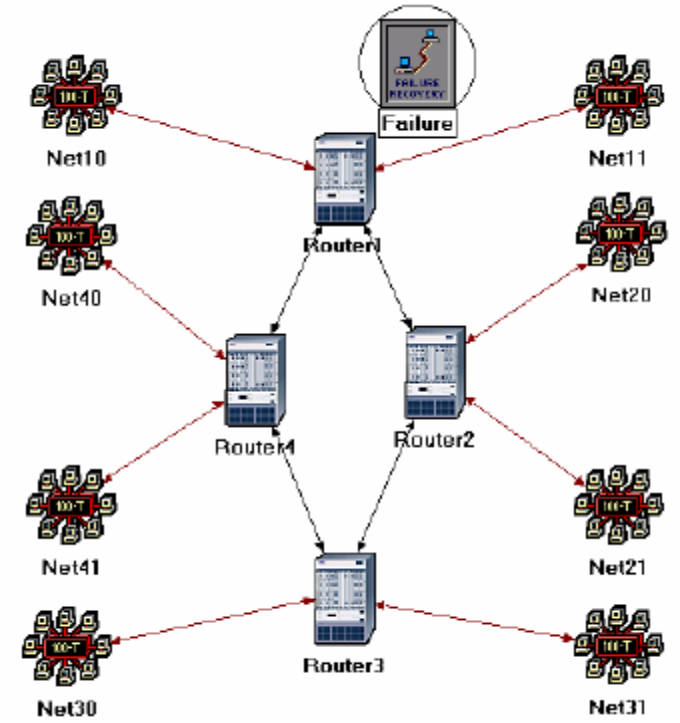
Дублювання сценарію

У мережі, яку ми тільки що створили, маршрутизатори побудують свої маршрутні таблиці, і їм не треба буде оновлювати їх надалі, тому що ми не моделюємо обриви зв'язків та відмови вузлів. У цьому сценарії ми промоделюємо відмови і зможемо порівняти поведінку маршрутизаторів в обох випадках.

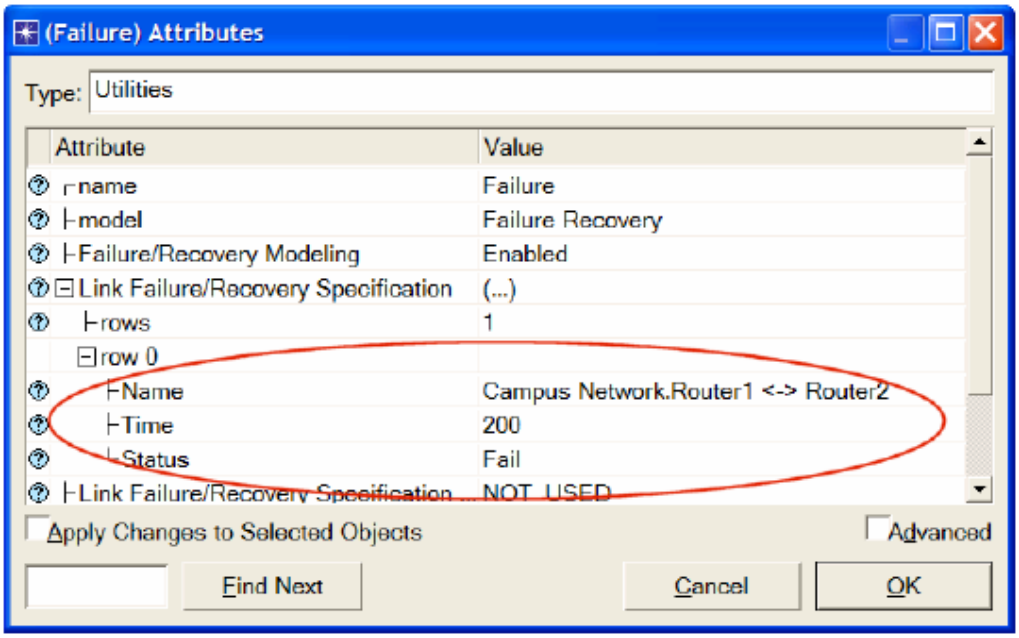
1. Виберіть ***Duplicate Scenario*** з меню ***Scenarios*** і назвіть його ***Failure*** ➔натисніть ***OK***.

2. Відкрийте ***Object Palette*** натисканням  . Виберіть палітру ***Utilities*** з випадаючого меню.

3. Додайте об'єкт ***Failure Recovery*** на ваш робочий простір і назвіть його ***Failure***, як показано ➔ Закрийте ***Object Palette***.



4. ПКМ на об'єкті ***Failure*** ➔ ***Edit Attributes*** ➔ Розгорніть ***Link Failure/Recovery Specification*** ➔Встановіть ***rows*** на ***1*** ➔ Встановіть атрибути доданого рядка, ***row 0***, як показано:



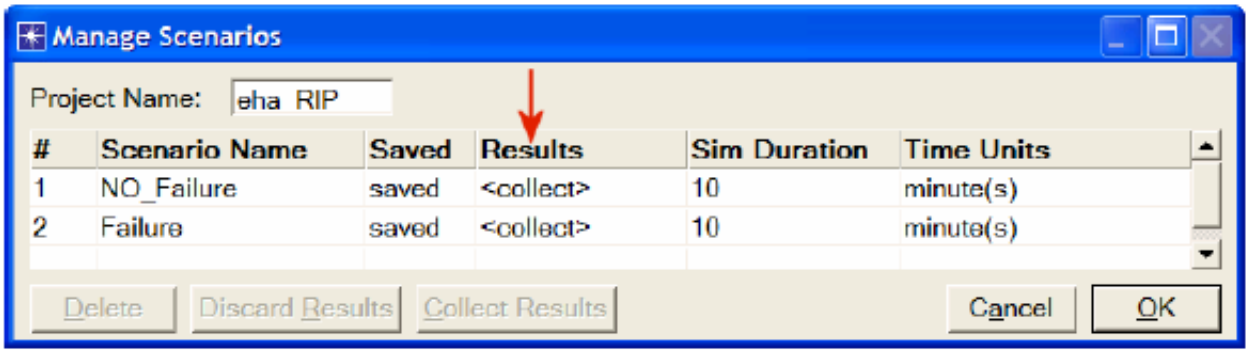
Це «упустить» з'єднання ***Router1 - Router2*** на 200й секунді моделювання.

5. Натисніть ***OK*** і збережіть проект.

Запуск моделювання

Для запуску моделювання обох сценаріїв одночасно:

1. Відкрийте меню ***Scenarios*** ➔ Виберіть ***Manage Scenarios***.
2. Змініть значення під стовпцем ***Results*** на <collect> (або <recollect>) для обох сценаріїв. Порівняйте з наступною картинкою:



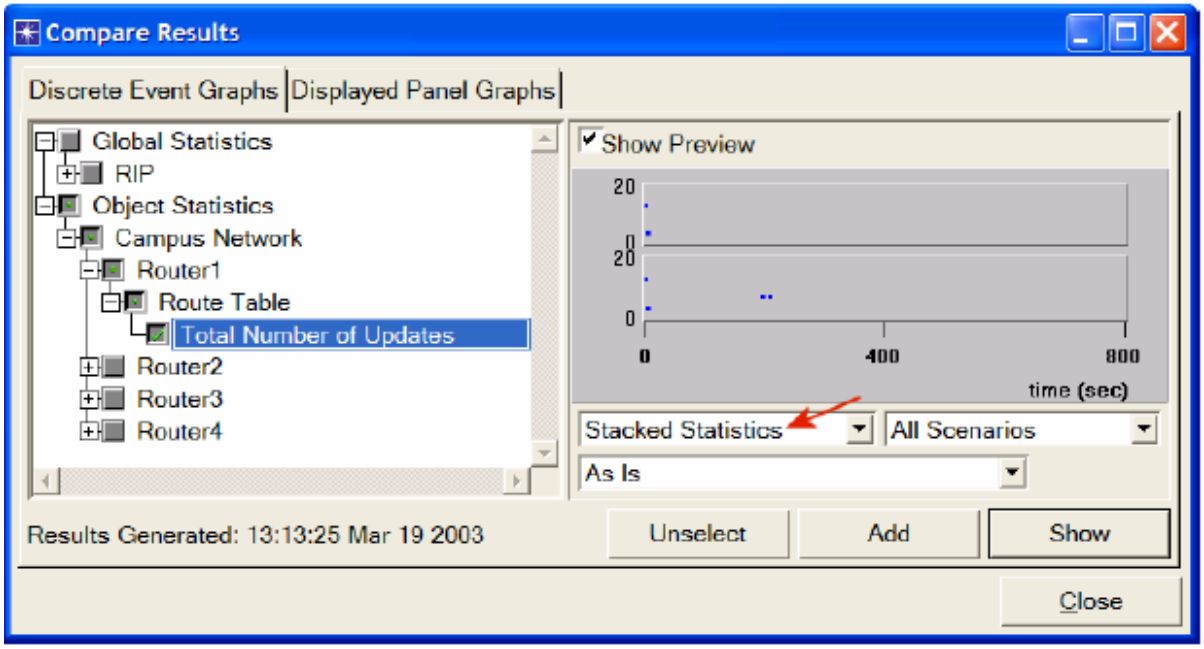
3. Натисніть ***OK*** для запуску двох сеансів моделювання. В залежності від продуктивності вашого процесора, моделювання може зайняти кілька секунд.
4. Після завершення двох сеансів моделювання, для кожного сценарію, натисніть ***Close*** ➔ Збережіть ваш проект.

Показ результатів

Порівняйте кількість оновлень:

1. Виберіть ***Compare Results*** з меню ***Results***.
2. Змініть меню, що випадає в нижній правій частині ***Compare Results*** на ***Stacked Statistics***, як показано.
3. Виберіть статистику ***Total Number of Updates*** для ***Router1*** і натисніть ***Show***.
4. Ви повинні отримає два графіки, по одному для кожного сценарію. ПКМ на кожному графіку і виберіть ***Draw Style*** ➔ ***Bar***.

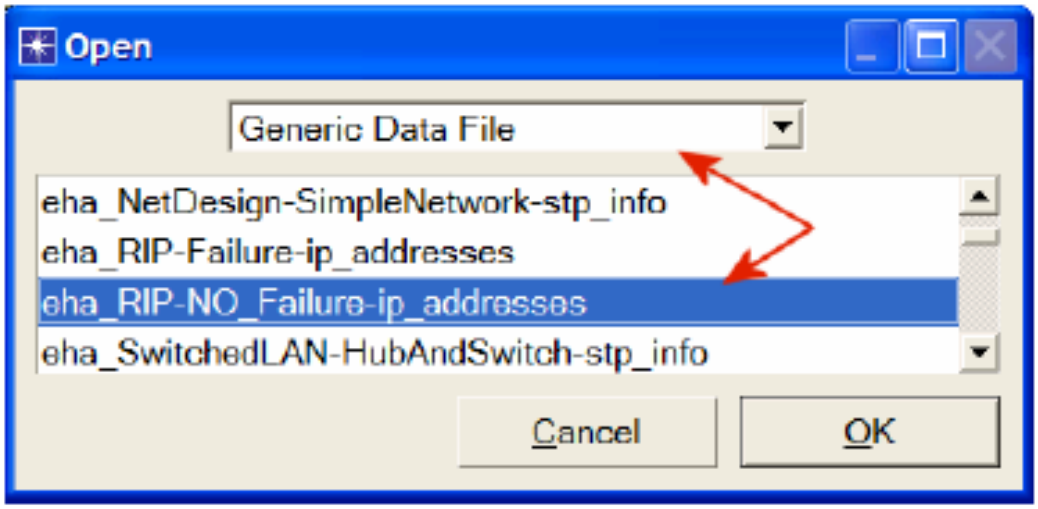
5. Результуючі графіки повинні показати наступне (ви можете збільшити графік, виділивши область, що вас цікавить):



Отримання IP-адрес інтерфейсів

Перед тим, як перевірити вміст таблиць маршрутизації, ми повинні визначити IP-адреси всіх інтерфейсів в нашій мережі. Нагадуємо, що ці IP-адреси автоматично роздаються в процесі моделювання, і ми встановили атрибут ***IP Interface Addressing Mode*** на експортування цієї інформації в файл.

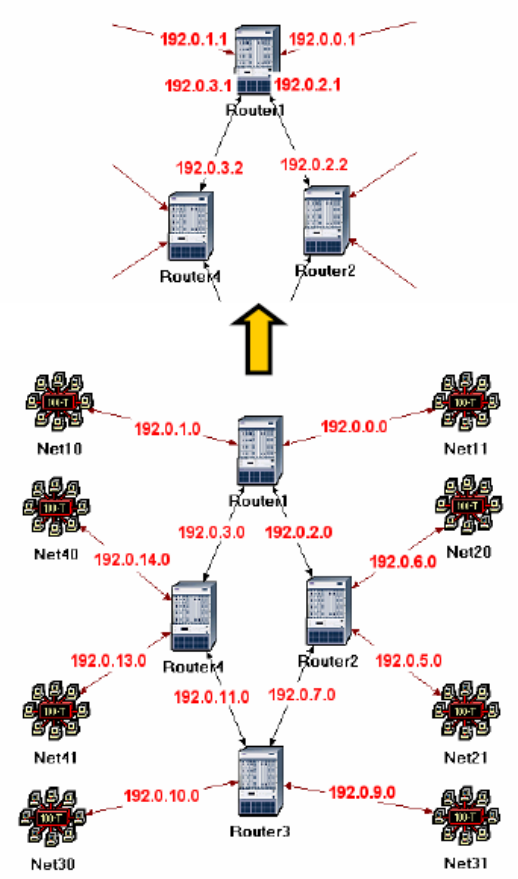
1. З меню ***File*** виберіть ***Model Files*** ➔ ***Refresh Model Directories***. Це змусить ***OPNET IT Guru*** знайти папки моделі та оновити файли.
2. З меню ***File*** виберіть ***Open*** ➔ З випадного меню виберіть ***Generic Data File*** ➔ Виберіть файл <ваші ініціали> _RIP-NO_Failure-ip_addresses (файл, створений для сценарію ***Failure*** повинен містити аналогічну інформацію) ➔ Натисніть ***OK***.



3. Малюнок являє собою частину вмісту файлу gdf. Він показує IP-адреси, встановлені для інтерфейсу ***Router1*** в нашій мережі. Наприклад, інтерфейс ***Router1***, приєднаний до ***Net11*** має IP-адресу 192.0.0.1 (Зауваження: ваші результати, в залежності від розташування вузлів, можуть відрізнятися). ***Subnet Mask***, пов'язана з цим інтерфейсом, показує, що адреса підмережі, до якої підключено інтерфейс, 192.0.0.0 (тобто, логічне і IP-адреса інтерфейсу і маска підмережі).

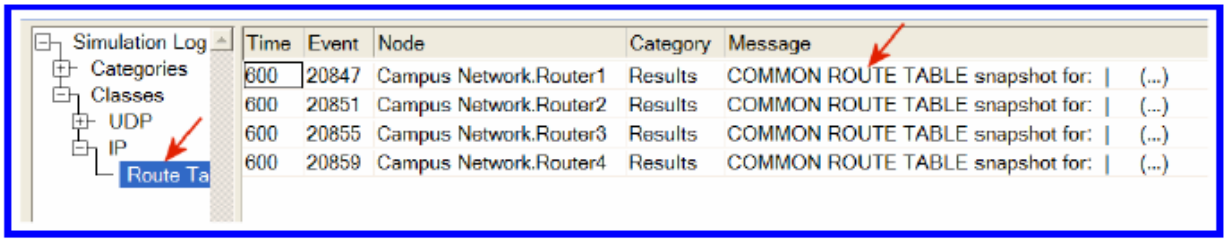
```
Node Name: Campus Network.Router1
 Iface Name          Iface Index   IP Address       Subnet Mask      Connected Link
 ----------          -----------   ---------------  ---------------  ----------------
 IF0                       0       192.0.0.1        255.255.255.0    Campus Network.Net11 <-> Router1
 IF1                       1       192.0.1.1        255.255.255.0    Campus Network.Net10 <-> Router1
 IF10                     10       192.0.2.1        255.255.255.0    Campus Network.Router1 <-> Router2
 IF11                     11       192.0.3.1        255.255.255.0    Campus Network.Router4 <-> Router1
 Loopback                 12       192.0.4.1        255.255.255.0    Not connected to any link.
```

4. Роздрукуйте план мережі, яку ви реалізували в цій лабораторній роботі. На цьому плані, використовуючи інформацію з gdf-файлу, надпишіть IP-адреси, асоційовані з ***Router1*** і адреси, асоційовані з кожною підмережею, як зазначено на наступних двох малюнках (Зауваження: ваші результати, в залежності від розташування вузлів, можуть відрізнятися)



Порівняння вмісту таблиць маршрутизації

1. Для перевірки вмісту таблиць маршрутизації ***Router1*** для обох сценаріїв: Відкрийте меню ***Results*** ➔ ***Open Simulation Log*** ➔ Розгорніть меню зліва, як показано нижче ➔ Клікніть на поле ***COMMON ROUTE TABLE***.



2. Повторіть попередній крок для обох сценаріїв. Наступний малюнок - частина вмісту таблиці маршрутизації ***Router1*** (Зауваження: ваші результати, в залежності від розташування вузлів, можуть відрізнятися):

Таблиця маршрутизації Router1 (сценарій *NO_Failure*):

Router name: Campus Network.Router1
at time: 600.00 seconds

ROUTE TABLE contents:

Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol
192.0.0.0	255.255.255.0	192.0.0.1	IF0	0	Direct
192.0.1.0	255.255.255.0	192.0.1.1	IF1	0	Direct
192.0.2.0	255.255.255.0	192.0.2.1	IF10	0	Direct
192.0.3.0	255.255.255.0	192.0.3.1	IF11	0	Direct
192.0.4.0	255.255.255.0	192.0.4.1	Loopback	0	Direct
192.0.5.0	255.255.255.0	192.0.2.2	IF10	1	RIP
192.0.6.0	255.255.255.0	192.0.2.2	IF10	1	RIP
192.0.7.0	255.255.255.0	192.0.2.2	IF10	1	RIP
192.0.8.0	255.255.255.0	192.0.2.2	IF10	1	RIP
192.0.11.0	255.255.255.0	192.0.3.2	IF11	1	RIP
192.0.13.0	255.255.255.0	192.0.3.2	IF11	1	RIP
192.0.14.0	255.255.255.0	192.0.3.2	IF11	1	RIP
192.0.15.0	255.255.255.0	192.0.3.2	IF11	1	RIP
192.0.9.0	255.255.255.0	192.0.2.2	IF10	2	RIP
192.0.10.0	255.255.255.0	192.0.2.2	IF10	2	RIP
192.0.12.0	255.255.255.0	192.0.2.2	IF10	2	RIP

Loopback interface (Інтерфейс зворотнього зв'язку) дозволяє клієнту і серверу на одному вузлі з'єднуватися один з одним, використовуючи ***TCP / IP***.

Таблиця маршрутизації Router1 (сценарій Failure):

Router name: Campus Network.Router1
at time: 600.00 seconds

ROUTE TABLE contents:

Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol
192.0.0.0	255.255.255.0	192.0.0.1	IF0	0	Direct
192.0.1.0	255.255.255.0	192.0.1.1	IF1	0	Direct
192.0.2.0	255.255.255.0	192.0.2.1	IF10	0	Direct
192.0.3.0	255.255.255.0	192.0.3.1	IF11	0	Direct
192.0.4.0	255.255.255.0	192.0.4.1	Loopback	0	Direct
192.0.11.0	255.255.255.0	192.0.3.2	IF11	1	RIP
192.0.13.0	255.255.255.0	192.0.3.2	IF11	1	RIP
192.0.14.0	255.255.255.0	192.0.3.2	IF11	1	RIP
192.0.15.0	255.255.255.0	192.0.3.2	IF11	1	RIP
192.0.5.0	255.255.255.0	192.0.3.2	IF11	3	RIP
192.0.6.0	255.255.255.0	192.0.3.2	IF11	3	RIP
192.0.7.0	255.255.255.0	192.0.3.2	IF11	2	RIP
192.0.8.0	255.255.255.0	192.0.3.2	IF11	3	RIP
192.0.9.0	255.255.255.0	192.0.3.2	IF11	2	RIP
192.0.10.0	255.255.255.0	192.0.3.2	IF11	2	RIP
192.0.12.0	255.255.255.0	192.0.3.2	IF11	2	RIP

КОНТРОЛЬНІ ЗАПИТАННЯ

1) Отримайте і проаналізуйте статистику по відправленому трафіку ***RIP*** для обох сценаріїв. Переконайтеся, що стиль відображення для графіків - ***Bar***.

2) Опишіть і поясніть вплив падіння з'єднання між ***Router1*** і ***Router2*** на таблиці маршрутизації.

3) Створіть ще один сценарій як дублікат сценарію ***Failure***. Назвіть новий сценарій ***3_Recover***. У цьому сценарії поставте відновлення з'єднання ***Router1*** - ***Router2*** через 400 секунд. Згенеруйте і проаналізуйте графік, що показує ефект цього відновлення на ***Total Number of Updates*** таблиці маршрутизації ***Router1***. Перевірте вміст таблиці маршрутизації ***Router1***. Порівняйте її з відповідними таблицями сценаріїв ***NO_Failure*** і ***Failure scenarios***.

ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ

Підготуйте звіт, виконаний за рекомендаціями до лабораторної роботи. Звіт повинен включати відповіді на вищезгадані питання, а також графіки, які Ви отримали при моделюванні сценаріїв. Проаналізуйте результати, які Ви отримали і порівняйте ці результати з очікуваними. Включіть до звіту будь-які аномалії або незрозумілу з Вашої точки зору поведінку.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

− RIP: IETF RFC number 2453 (www.ietf.org/rfc.html).

Лабораторна робота №8

TCP - ПРОТОКОЛ УПРАВЛІННЯ ПЕРЕДАЧЕЮ

Мета робота. Продемонструвати алгоритми з управління перевантаженням, вбудованих в протокол TCP. Представити ряд сценаріїв для

моделювання вищевказаних алгоритмів. Порівняти продуктивність алгоритмів за допомогою аналізу результатів моделювання.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Інтернет протокол TCP гарантує надійність і правильну доставку потоку байтів. Він включає в себе механізм управління потоком для потоків байтів, який дозволяє одержувачеві встановлювати кількість даних, які відправник зможе відіслати за виділений час. До того ж в TCP реалізований дуже тонко настроєний механізм по контролю за перевантаженням. Сенс механізму полягає у визначенні швидкості відправки протоколом TCP даних з тим, щоб відправник не перевантажував мережу.

Суть контролю перевантаження в протоколі TCP полягає в тому, щоб для кожного джерела визначити яка пропускна здатність мережі, так щоб знати скільки пакетів можна вільно пересилати. Для цього в кожному з'єднанні створюється змінна ***congestion window*** (вікно перевантаження), яка використовується джерелом для визначення допустимої кількості даних, що пересилаються в заданий проміжок часу. Протокол TCP використовує механізм ***additive increase / multiplicative decrease***, який призначений для зменшення вікна перевантаження коли рівень перевантаження зростає і, відповідно, збільшує вікно перевантаження, коли рівень перевантаження зменшується. Протокол TCP сприймає час простою, як сигнал про перевантаження. Кожен раз, коли відбувається затримка, джерело зменшує значення вікна перевантаження в два рази. Це зменшення відноситься до механізму мультиплікативного зменшення. Розмір вікна перевантаження не може бути менше розміру одного пакета (максимальний розмір сегмента TCP - MSS). Кожен раз, коли джерело успішно відправляє число пакетів, рівне значенню вікна перевантаження, то до значення

вікна перевантаження додається значення, еквівалентне одному пакету, це – механізм адитивного збільшення.

Протокол TCP використовує механізм повільного старту для збільшення вікна перевантаження «швидше», ніж холодний старт в TCP з'єднаннях. Цей механізм збільшує вікно перевантаження експоненціально, а не лінійно. Нарешті, в TCP використовується механізм швидкої повторної пересилки і швидкого відновлення.

Швидка повторна передача - евристична величина, яка в деяких випадках викликає повторну передачу обірваного пакета. При чому робиться це швидше, ніж за допомогою використання звичайного механізму затримки.

У цій роботі необхідно налаштувати мережу, яка використовує TCP в якості наскрізного протоколу обміну і проаналізувати розмір вікна перевантаження при різних механізмах.

МЕТОДИЧНІ ВКАЗІВКИ

Створення нового проекту

Створіть Новий Проект.

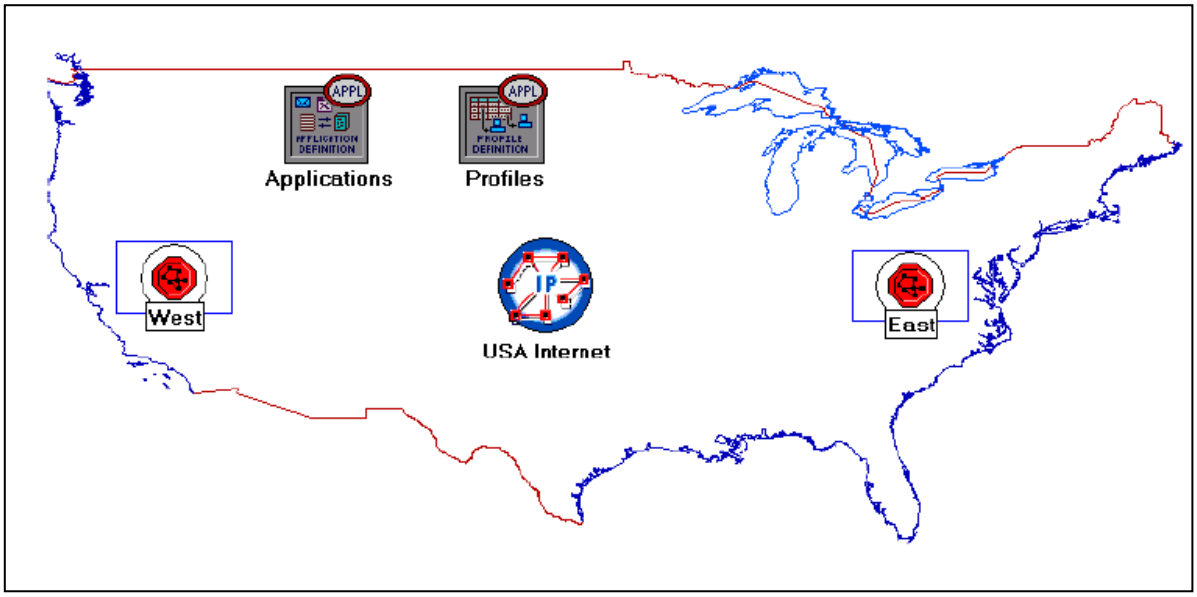
1. Запустіть ***OPNET IT Guru Academic Edition***, виберіть ***New*** в меню ***File***.
2. Виберіть ***Project*** і клацніть ***OK***. Назвіть проект <назва> _TCP, і сценарій ***No_Drop***. Клацніть ***OK***.
3. В ***Startup Wizard: Initial Topology*** діалоговому вікні, переконайтеся в тому, що виділено ***Create Empty Scenario***, клацніть ***Next***, виберіть ***Choose From Maps*** в списку ***Network Scale***, клацніть ***Next***, виберіть ***USA*** зі списку ***Map List***, двічі клацніть ***Next*** два рази, і клацніть ***OK***.

Створення та налагодження мережі

Ініціалізація мережі

1. Діалогове вікно ***Object Palette*** має знаходитися вгорі робочого простору. Якщо його там немає, відкрийте його. Переконайтеся, що пункт ***internet_toolbox*** вибраний з випадного меню на панелі об'єктів.
2. Додайте в робочий простір проекту наступні об'єкти з панелі: ***Application Config***, ***Profile Config***, ***ip32_Cloud***, і дві підмережі. Для того, щоб додати об'єкт з панелі потрібно клацнути по значку об'єкта на панелі, пересуньте курсор миші в робочий простір. Клацніть, щоб перемістити об'єкт у потрібне положення. ПКМ щоб завершити створення об'єктів цього типу.
3. Закрийте робочий простір.
4. Змініть назву об'єктів, як це показано нижче, і збережіть проект:

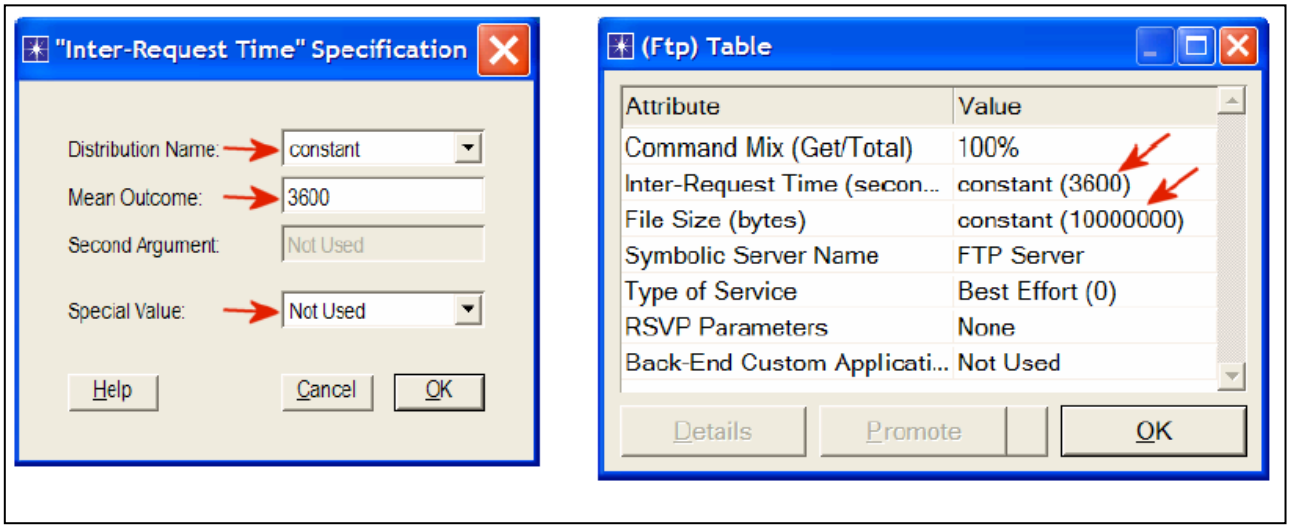
Модель вершин ***ip32_cloud*** відображає ***IP*** хмари, які підтримуються аж до 32 розрядної лінії послідовної передачі в масштабі передаваємих даних, через які може бути змодельований ***IP*** трафік. ***IP*** пакети, які прибувають на інтерфейс будь-якої хмари, будуть маршрутизироватися відповідно до інтерфейсів виведення , які найбільш підходять, заснованому на їх IP адреспх призначення. Протокол ***RIP*** або ***OSPF*** може використовуватися для автоматичного або динамічного створення таблиць маршрутизації хмар і для вибору маршрутизації адаптивним способом. Такфй хмарі потрібна фіксована кількість часу для маршрутизації кожного пакета, що визначається ***Packet Latency*** атрибутом кожної вершини.



Конфігурування додатків

1. ПКМ по вершині ***Applications***, потім ***Edit Attributes***, потім розкриваємо ***Application Definitions***. Встановлюємо значення атрибута ***rows*** рівним 1. ***Expand the new row*** - називаємо рядок ***FTP_Application***.

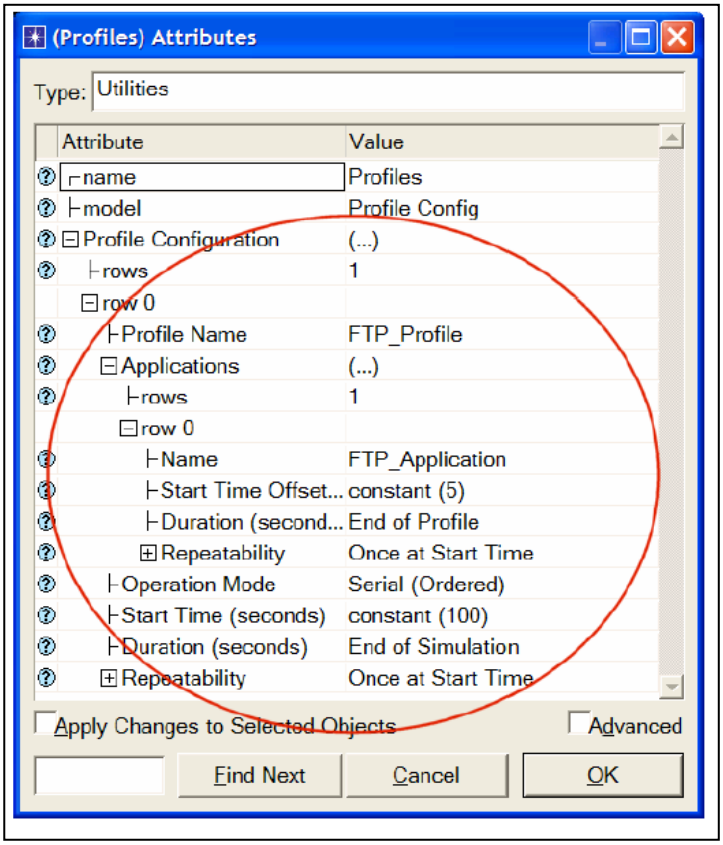
   Розкриваємо ієрархію ***Description*** - редагуємо рядок ***FTP*** так як показано (для редагування зазначених параметрів необхідно встановити параметр ***Special Value*** в ***Not Used***):



2. Двічі натискаємо ***OK*** і зберігаємо проект.

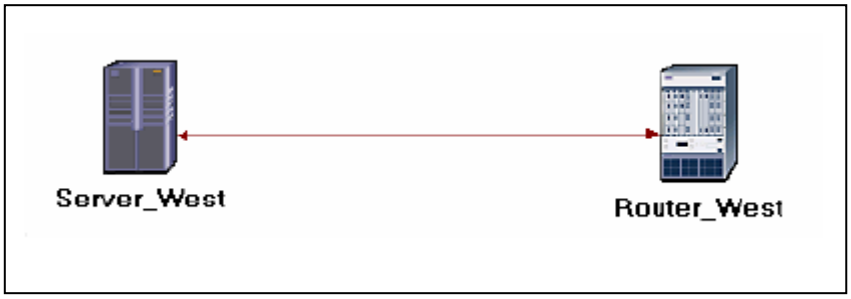
Конфігурування профілів

ПКМ по вершині ***Profiles-Edit Attributes*** - розтягуємо атрибут ***Profile Configuration*** і присвоюємо ***rows*** значення 1. Називаємо і встановлюємо атрибути ***row*** 0 - Клацаємо ***OK***.



Налаштування підмережі *West Subnet*

1. Подвійний клацання по вершині підмережі ***West***. З'являється вільний простір, що показує, що в підмережі немає ніяких об'єктів.
2. Відкриваємо панель об'єктів, виділяємо елемент ***internet_toolbox*** в випадаючому меню.
3. Додаємо в підмережу такі об'єкти: один ***ethernet_server***, один ***ethernet4_slip8_gtwy*** маршрутизатор і підключаємо їх двонаправленим з'єднанню ***100_BaseT*** - Закриваємо панель – Змінюємо назву об'єктів так, як показано нижче.

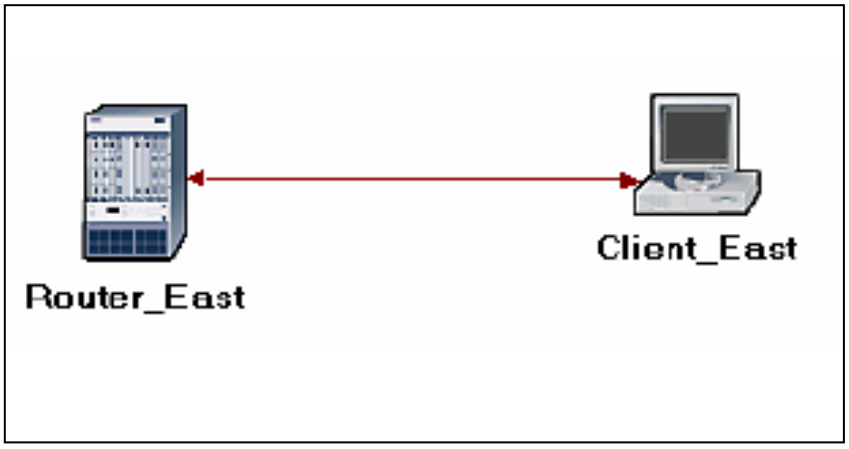


4. ПКМ по вершині ***Server_West*** - ***Edit Attributes***:
   - Редагуємо ***Application: Supported Services*** - Надаємо ***rows*** значення 1 - Встановлюємо ***Name*** в ***FTP_Application*** - Натискаємо ***OK***.
   - Редагуємо значення атрибута ***Server Address*** і пишемо ***Server_West***.
   - Розширюємо ієрархію ***TCP Parameters*** - Надаємо ***Fast Retransmit*** і ***Fast Recovery*** значення ***Disabled***.
5. Натискаємо ***OK*** і зберігаємо проект.

На даному етапі настройка підмережі ***West*** закінчена. Для того, щоб піднятися на вищий рівень проекту нажмітекнопку ***Go to next higher level***.

Налаштування підмережі *East*

1. Подвійне клацання на вершині підмережі ***East***. З'являється вільний простір, що показує, що в підмережі немає ніяких об'єктів.
2. Відкриваємо панель об'єктів, виділяємо елемент ***internet_toolbox*** в випадаючому меню.
3. Додаємо в підмережу такі об'єкти: один ***ethernet_wkstn***, один маршрутизатор ***ethernet4_slip8_gtwy*** і підключаємо їх двонаправленим з'єднанню ***100_BaseT*** - Закриваємо панель - Перейменовуємо об'єкти так, як показано.

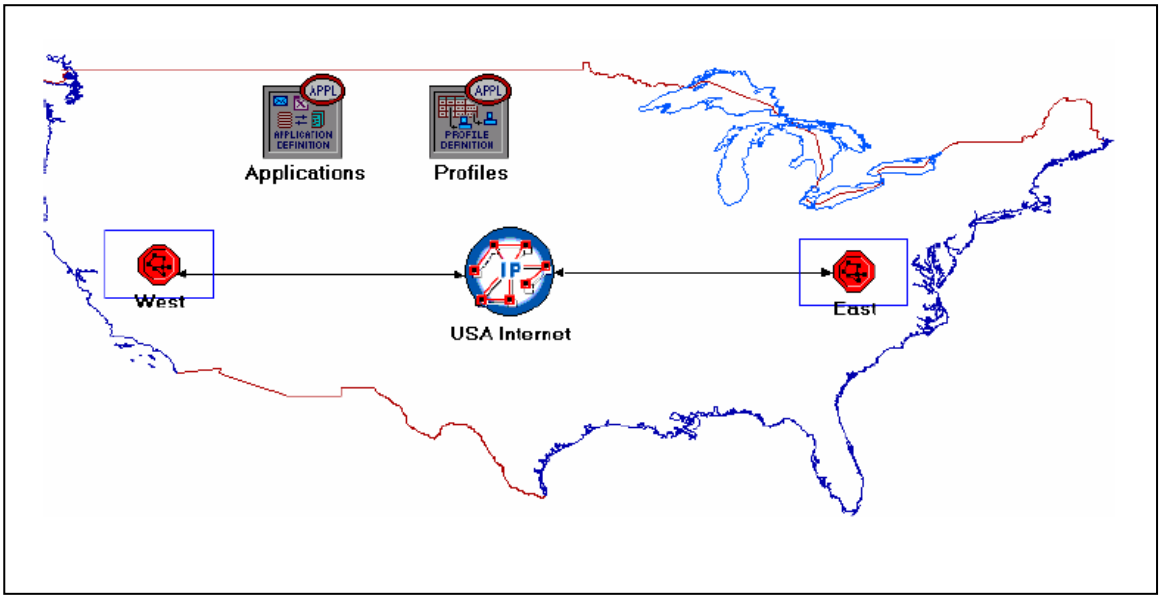


4. ПКМ по вершині ***Client_East - Edit Attributes***:
   - Розширюємо ієрархію ***Application***: ***Supported Profiles*** - присвоюємо ***rows*** 1 - розширюємо ієрархію ***row*** 0 - встановлюємо ***Profile Name*** в ***FTP_Profile***.
   - ii.Атрібуту ***Client Address*** присвоюємо значення ***Client_ East***.
   - iii.Редагуємо атрибути ***Application***: ***Destination Preferences*** так як показано нижче:

   Встановлюємо ***rows*** в 1 - Встановлюємо ***Symbolic Name*** в ***FTP Server*** - Редагуємо ***Actual Name*** - Встановлюємо ***rows*** в 1 - У новому рядку колонки ***Name*** присвоюємо значення ***Server_West***.
5. Тричі натискаємо ***OK*** і зберігаємо проект.
6. Налаштування підмережі ***East*** закінчено. Для того, щоб повернутися в простір проекту потрібно натиснути кнопку ***Go to next higher level***.

Підключення підмереж до хмари *IP Cloud:*

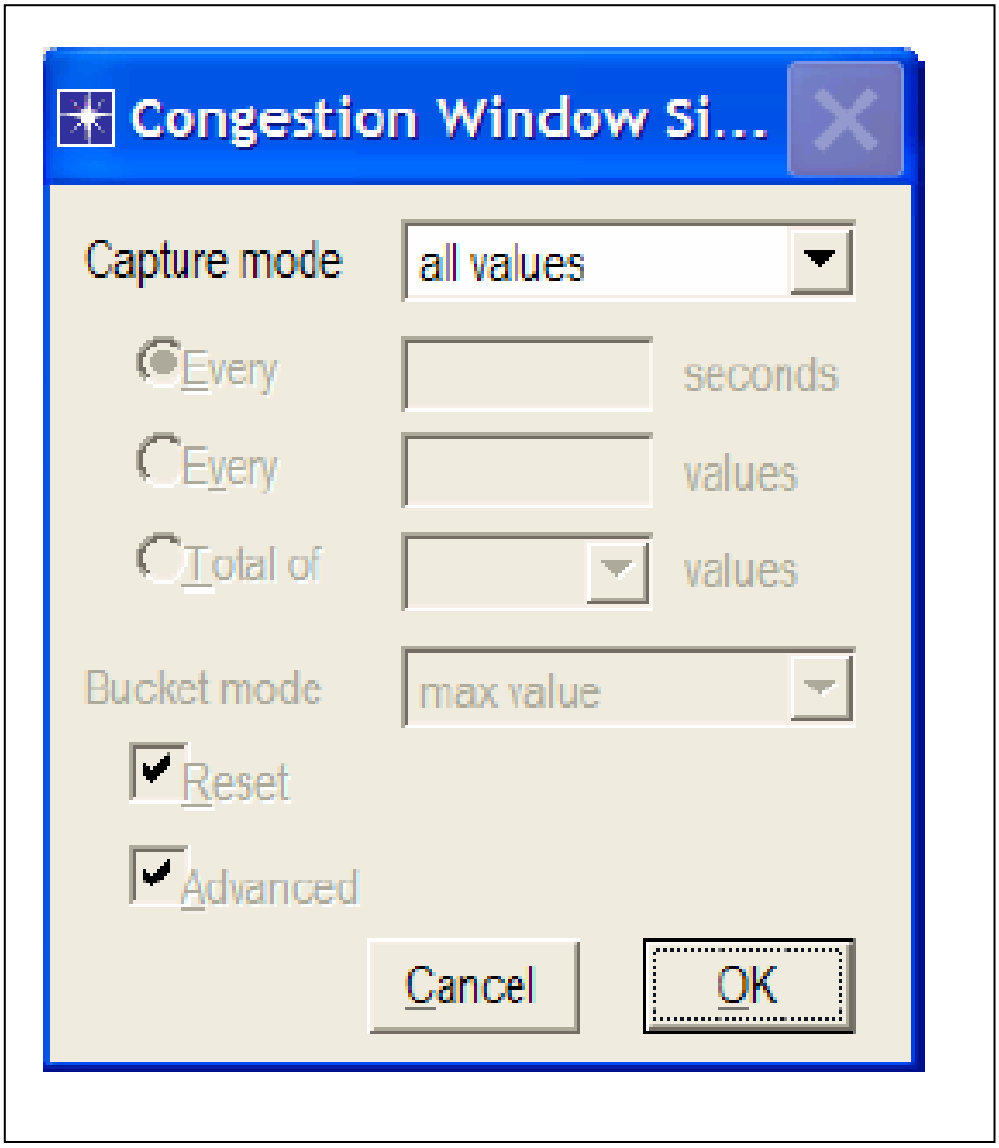
1. Відкриваємо панель об'єктів.
2. Використовуючи два двонаправлених з'єднання ***PPP_DS3***, підключаємо підмережі ***West*** і ***East*** до ***IP Cloud***.
3. З'явиться випадаюче діалогове меню, в якому необхідно підтвердити, що ви хочете підключити підмережі до ***IP Cloud***. Перевірте, чи вибрали ви "***routers***".
4. Закриваємо панель.



Вибір статистики

1. ПКМ по ***Server_West*** в підмережі ***West*** - вибираємо ***Choose Individual Statistics*** з випадаючого меню.
2. У діалоговому вікні ***Choose Results*** вибираємо таку статистику:

   TCP Connection - Congestion Window Size (bytes) і ***Sent Segment Sequence Number***.
3. ПКМ ***no Congestion Window Size (bytes)*** - Вибираємо ***Change Collection Mode*** - У діалоговому вікні виділяємо ***Advanced*** - У випадаючому меню присвоюємо ***Capture mode*** значення ***all values*** - Натискаємо ***OK***.



4. ПКМ по ***Sent Segment Sequence Number*** - Вибираємо ***Change Collection Mode*** - У діалоговому вікні вибираємо ***Advanced*** - У випадаючому меню присвоюємо ***Capture mode*** значення ***all values***.
5. Двічі натискаємо ***OK*** і зберігаємо проект.
6. Натискаємо кнопку ***Go to next higher level***.

Налаштування моделювання

Необхідно налаштувати тривалість моделювання:

1. Повинно з'явитися вікно ***Configure Simulation***.
2. Встановлюємо тривалість рівну 10.0 ***minutes***.

3. Натискаємо ***OK*** і зберігаємо проект.

OPNET надає такі моделі:

All values-збирає всі дані статистики.

Sample-збирає дані відповідно до встановленого користувачем тимчасового інтервалу або числом дискретизації. Наприклад, якщо часовий інтервал дорівнює 10, то дані будуть записуватися кожні 10 секунд. Якщо число дискретизації дорівнює 10, то буде записуватися кожен 10-й відлік даних. Інші дані будуть втрачені.

Bucket-збирає всі дані в заданому часовому інтервалі або числі дискретизації в «корзину даних», і генерує результат у кожному кошику. Встановлено за замовчування.

Створення копії сценарію

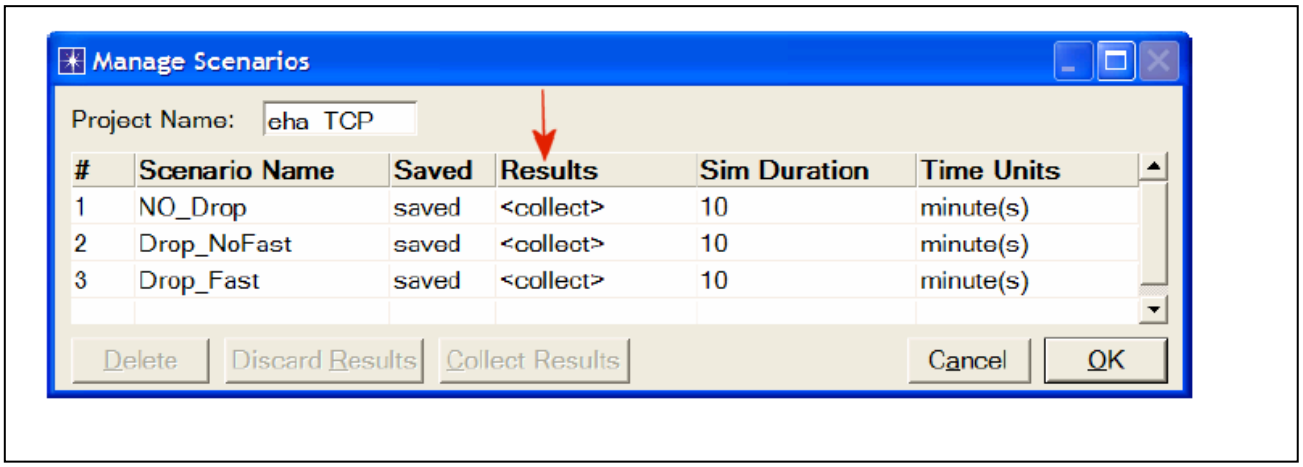
Ми створили і налаштували мережу, але в ній немає бракованих пакетів. Ми також вимкнули можливість швидкої повторної пересилки і швидкого відновлення ***TCP***. Для того, щоб проаналізувати ефект бракованих пакетів і технології контролю перевантаження ми створимо два додаткові сценарія.

1. Вибираємо ***Duplicate Scenario*** в меню ***Scenarios*** і називаємо його ***Drop_NoFast*** - Натискаємо ***OK***.
2. У новому сценарії ПКМ по ***IP Cloud*** - ***Edit Attributes*** - Надаємо значення 0.05% атрибуту ***Packet Discard Ratio***.
3. Натискаємо ***OK*** і зберігаємо проект.
4. Перебуваючи в сценарії ***Drop_NoFast*** вибираємо ***Duplicate Scenario*** з меню ***Scenarios*** і називаємо його ***Drop_Fast***.
5. У сценарії ***Drop_Fast*** ПКМ по ***Server_ West***, який знаходиться в підмережі ***West*** - ***Edit Attributes*** - Розширюємо ієрархію ***TCP Parameters*** - Включаємо ***Fast Retransmit*** - Надаємо атрибуту ***Fast Recovery*** значення ***Reno***.
6. Натискаємо ***OK*** і зберігаємо проект.

Запуск моделювання

Для виконання одночасного моделювання трьох сценаріїв:

1. Меню ***Scenarios*** - Вибираємо ***Manage Scenarios***.
2. У колонці ***Results*** змінюємо значення на <collect> (або <recollect>) для трьох сценаріїв. Порівнюємо з малюнком:



3.Для запуску трьох сценаріїв натискаємо ***OK***. В залежності від швидкості процесора на моделювання може знадобитися до декількох хвилин.

4. По завершенню моделювання для кожного сценарію потрібно натиснути ***Close*** - Зберігаємо проект.

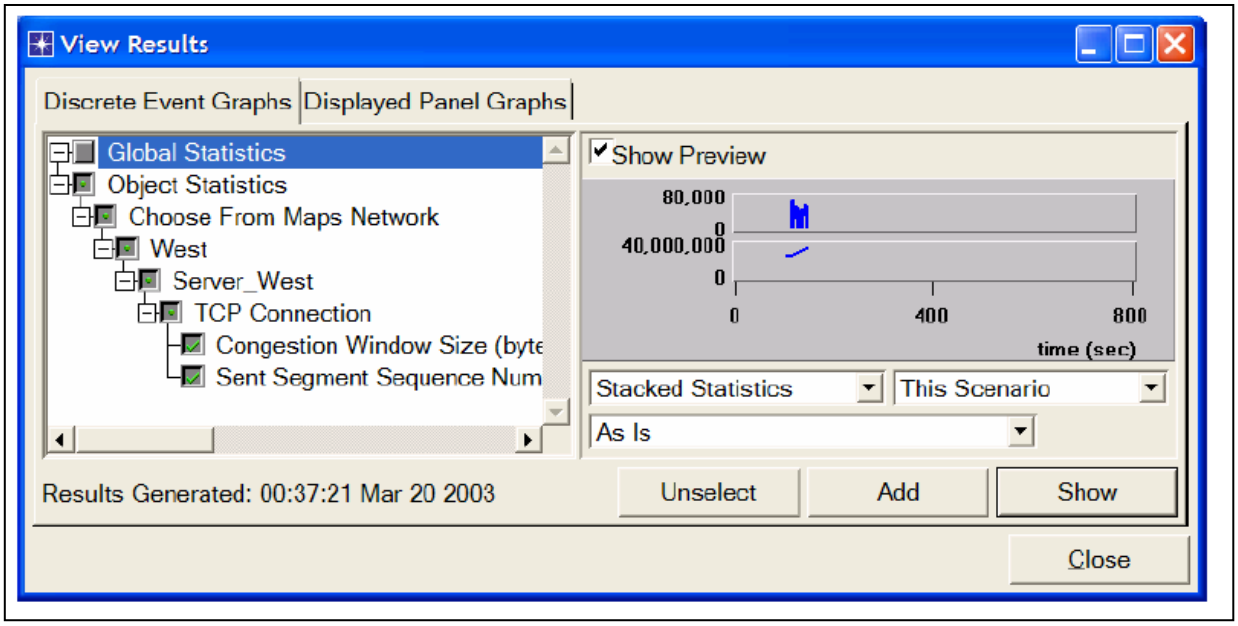
За допомогою технології швидкої повторної пересилки протокол ***TCP*** надає можливість пересилки втрачених сегментів ще до того, як відбудеться спрацьовування таймера повторної пересилки. Після пересилання втраченого сегмента виконується уникнання перевантаження, але не повільний старт. Це і є алгоритм швидкого відновлення. Як правило алгоритми швидкої повторної пересилки і швидкого відновлення виконуються разом (RFC 2001).

Перегляд результатів

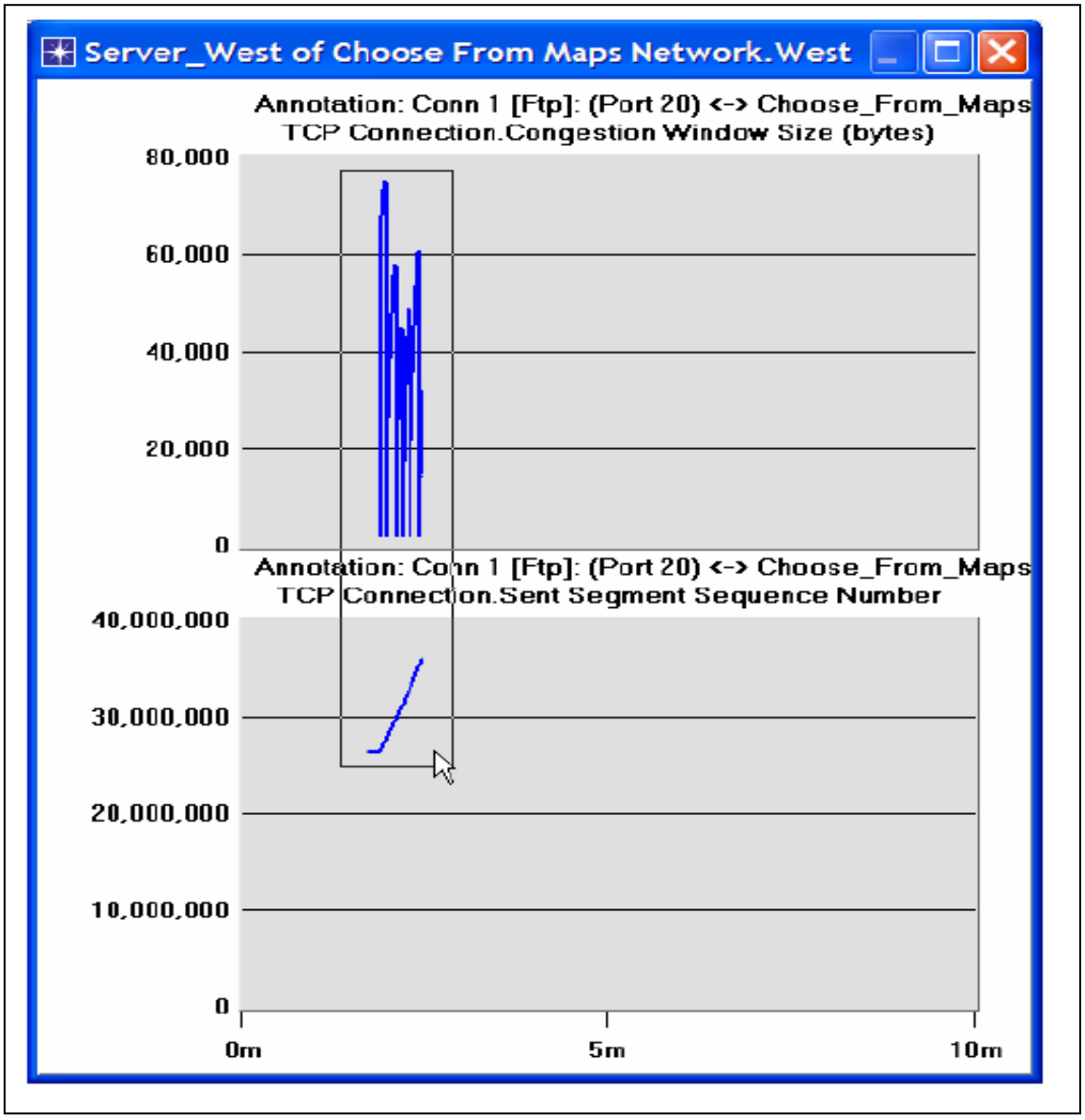
Для перегляду та аналізу результатів:

1. Переходимо до сценарію ***Drop_NoFast*** (другий за рахунком) і вибираємо ***View Results*** в меню ***Results***.

2. На все вікно розтягуємо ієрархію ***Object Statistics*** і вибираємо такі результати: ***Congestion Window Size*** (***bytes***) і ***Sent Segment Sequence Number***.

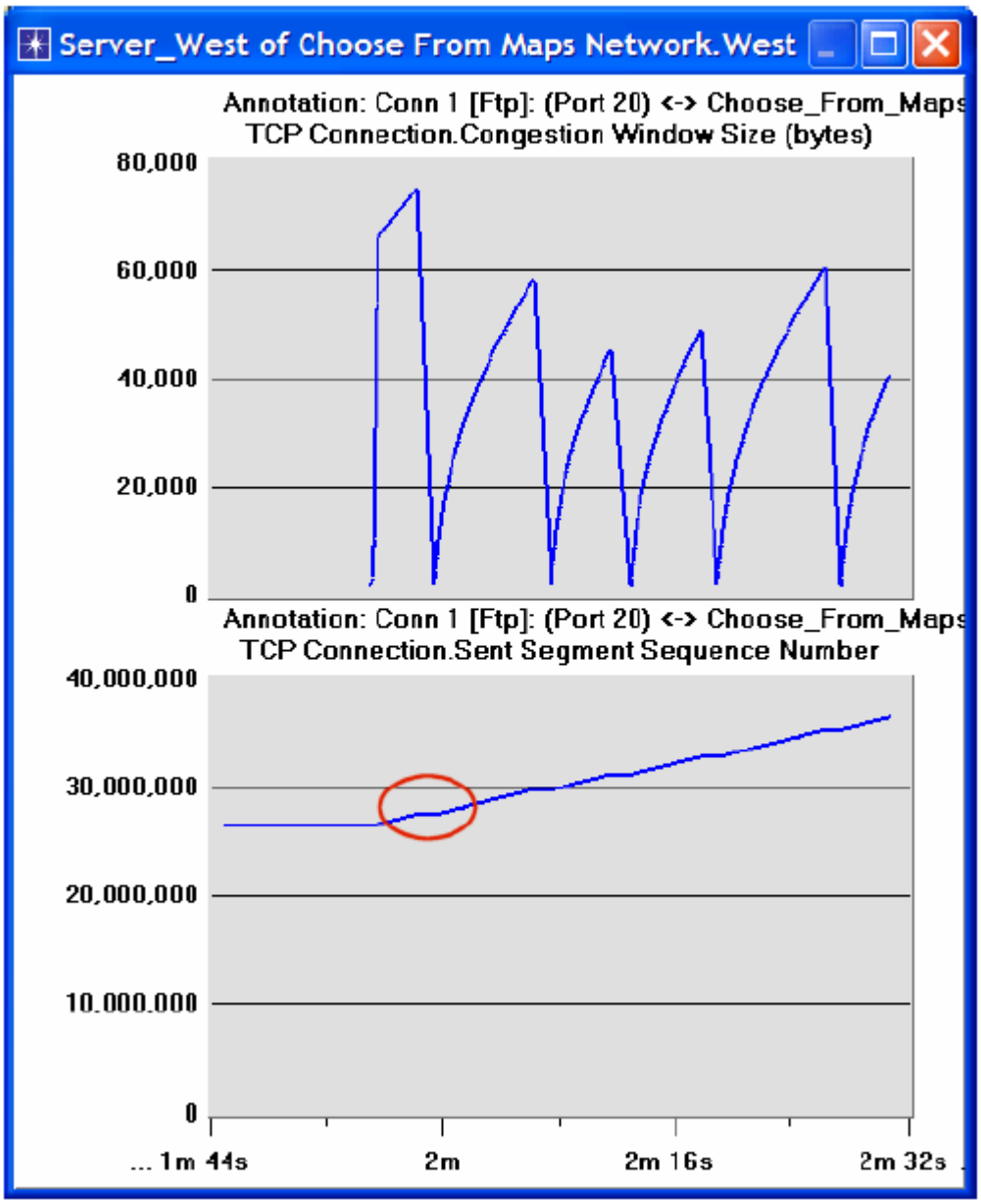


3. Клацніть Show. Результуючий графік буде мати вигляд:



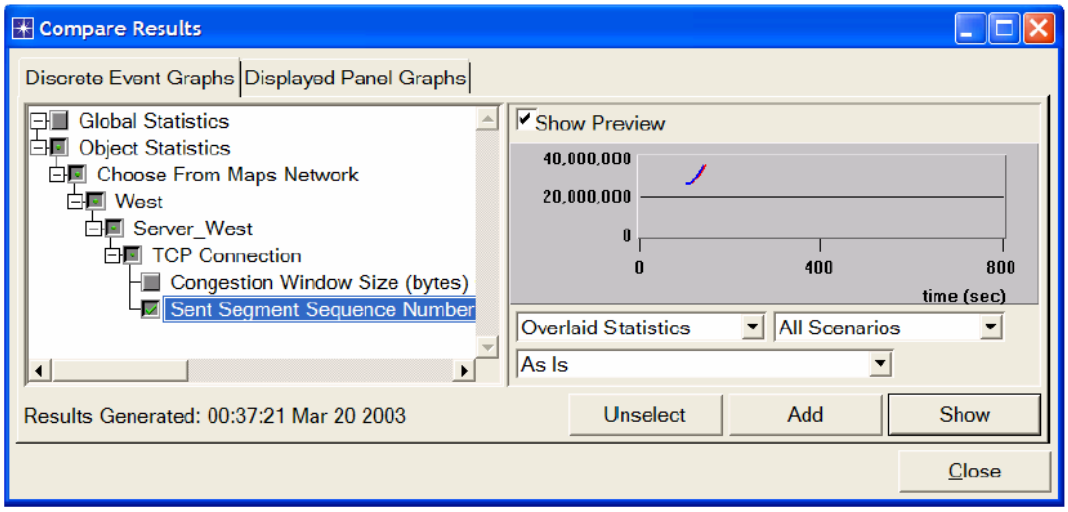
Для того щоб переключити сценарій потрібно вибрати ***Switch tP Scenario*** з меню або просто натиснути ***Ctrl*** + <номер сценарію>.

4. Для того, щоб збільшити деталі графіка потрібно затиснути кнопку миші і намалювати прямокутник.
5. Графік перемалюють і відобразять те, що показано нижче:
6. Зверніть увагу, що ***Segment Sequence Number*** майже плоский у вікні перевантаження.

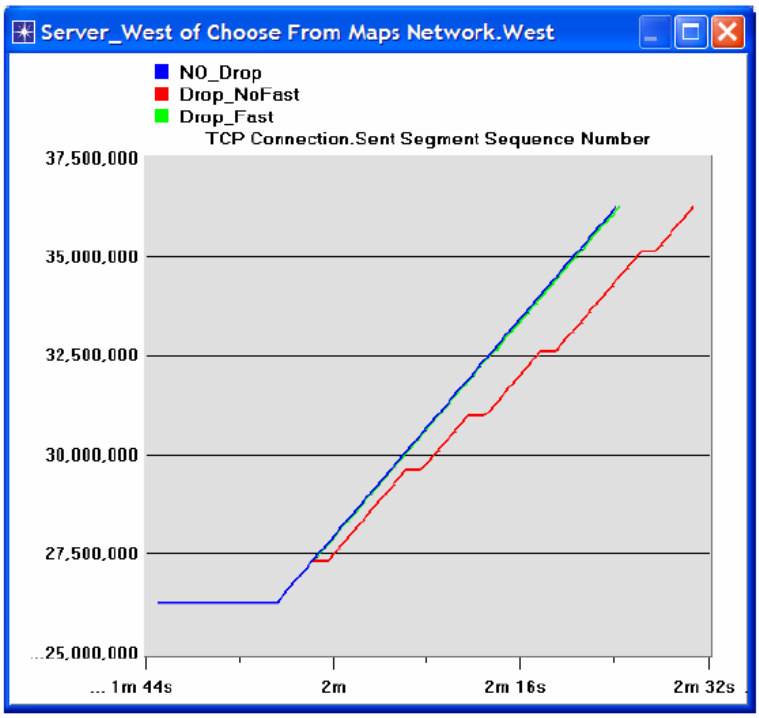


Зверніть увагу, що ***Segment Sequence Number*** у вікні перевантаження майже плоский.

7. Закриваємо діалогове вікно ***Close the View Results*** і вибираємо ***Compare Results*** з меню ***Result***.
8. Розтягуємо на все вікно ієрархію ***Object Statistics*** і вибираємо такий результат: ***Sent Segment Sequence Number***.



9. Клацніть ***Show***. Після збільшення результуючий граф повинен бути схожий на граф, вказаний нижче.



КОНТРОЛЬНІ ЗАПИТАННЯ

1) Чому ***Segment Sequence Number*** залишається незмінним (відображається на графіку горизонтальними лініями) при зміні вікна перевантаження?

2) Проаналізуйте графік, на якому порівнюється значення ***Segment Sequence*** трьох сценаріїв. Чому значення сценарію ***Drop_NoFast*** зростає повільніше всього?

3) Для сценарію ***Drop_NoFast*** отримаєте графік, що містить порівняння ***Sent Segment Sequence Number*** з ***Received Segment ACK Number*** для ***Server_West***. Поясніть отримані результати.

Підказка:

Переконайтеся, що для статистики ***Segment ACK Number*** параметрам ***Capture mode*** і ***Received*** присвоєно значення ***all values***.

4) Створіть інший сценарій, як дуплікат сценарію ***Drop_Fast***. Назвіть новий сценарій ***Q4_Drop_Fast_Buffer***. У новому сценарії змініть атрибути вершини ***Client_East*** і надайте значення 65535 його атрибуту ***Receiver Buffer*** (***bytes***) (один з ***TCP Parameters***). Побудуйте графік, на якому буде показано ***Congestion Window Size*** (***bytes***) для ***Server_West***, на який впливаємо збільшенням буфера одержувача (порівняти графік розміру вікна перевантаження для сценарію ***Drop_Fast*** з відповідним графіком для сценарію ***Q4_Drop_Fast_Buffer***).

ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ

Підготуйте звіт, виконаний за рекомендаціями до лабораторної роботи. Звіт повинен включати відповіді на вищезгадані питання, а також графіки, які Ви отримали при моделюванні сценаріїв. Проаналізуйте результати, які Ви отримали і порівняйте ці результати з очікуваними. Включіть до звіту будь-які аномалії або незрозумілу з Вашої точки зору поведінку.

Лабораторна робота №9

ДИСЦИПЛІНИ ЧЕРГ. ЧЕРГОВІСТЬ ПЕРЕДАЧІ І СКИДАННЯ ПАКЕТІВ

Мета роботи. Розглянути ефективність різних дисциплін черг в доставці пакетів і затримки різних служб.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Як складова механізмів розташування ресурсів, кожен роутер повинен забезпечувати деяку дисципліну обслуговування черг, яка обумовлює, як пакети будуть буферізовати поки очікують передачі. Для контролю за тим, які пакети будуть передані, а які - відкладені (в буфер), можуть бути використані різні дисципліни черг. Тип дисципліни також впливає на час, який пакет проводить в черзі. Найбільш поширені дисципліни - перший увійшов перший вийшов (FIFO), за пріоритетом (PQ), справедливі вагові черги (WFQ).

Ідея черги FIFO полягає в тому, що перший пакет, що прибув в роутер, буде переданий також першим (тобто передача в порядку прибуття). Враховуючи, що розмір буфера кінцевий, то прибуття пакета, коли черга (буфер) сповнена, призводить до відкидання пакета. Це відбувається без урахування того, наскільки важливий пакет і частиною якого потоку він є.

Черга PQ - всього лише варіація базової дисципліни FIFO. Ідея полягає у видачі пріоритету кожному пакету. Він може зберігатися, наприклад, в полі типу служби the IP Type of Service (ToS). Роутери реалізують множинні FIFO-черги, по одній для кожного класу пріоритету. Усередині кожного окремо взятого пріоритету пакети впорядковані за дисципліною FIFO. Така організація призводить до просування високопріоритетних пакетів вперед у черзі.

Дисципліна справедливої черги (FQ) забезпечує окремі черги для кожного поточного потоку під управлінням роутера. Роутер може обслуговувати ці черги циклічно. WFQ також припускає наявність ваги у кожного потоку (черги). Ця вага дозволяє ефективно контролювати яку частину пропускної здатності отримає кожен потік. Ми можемо використовувати біти поля ToS в заголовку IP для вказівки ваги.

У цій лабораторної роботи ви будете налаштовувати мережу, яка підтримує три програми: FTP, відео та VoIP. Ви вивчіте як вибір дисципліни черги в роутері впливає на виконання програм та використання мережевих ресурсів.

МЕТОДИЧНІ ВКАЗІВКИ

Створення нового проекту

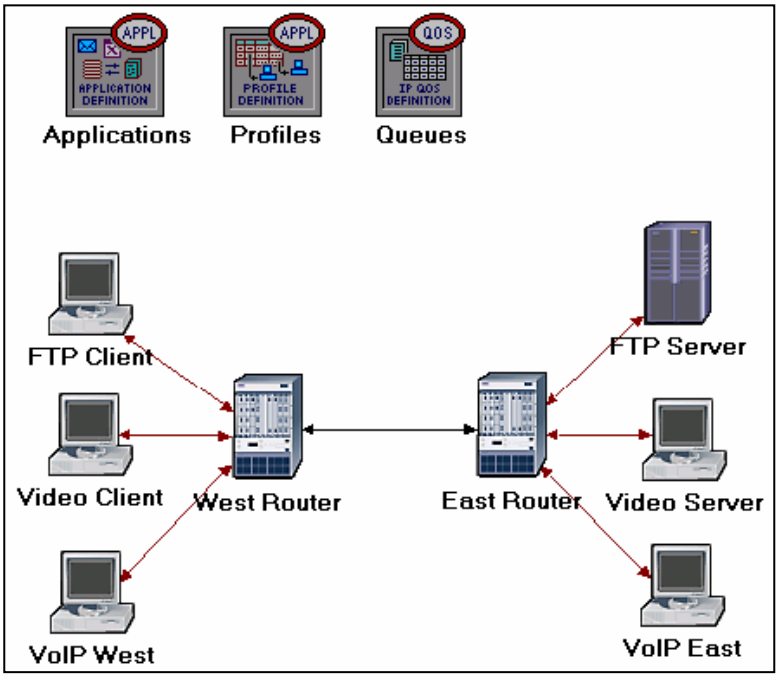
1. Запустіть ***OPNET IT Guru Academic Edition*** і виберете пункт ***New*** в меню ***File***.
2. Виберіть ***Project*** і натисніть ***OK***. Ім'я проекту - <ваші ініціали> _Queues, сценарій - ***FIFO***. Підтвердіть натисканням ***OK.***
3. У діалоговому вікні ***Startup Wizar***d: ***Initial Topology*** переконайтеся, що вибрано пункт ***Create Empty Scenario***. Натисніть ***Next***. Потім виберете ***Campus*** зі списку ***Network Scale***. Натисніть ***Next*** тричі і потім ***OK.***

Створення та конфігурування мережі

Ініціалізація мережі:

1. Діалогове вікно ***Object Palette*** має бути вгорі простору вашого проекту. Якщо його там немає, відкрийте натисканням  . Переконайтеся, що пункт ***internet_toolbox*** обраний у спадному меню діалогового вікна.

2. Додайте в проект наступні об'єкти з палітри: ***Application Config***, ***Profile Config***, ***QoS Attribute Config***, п'ять ***ethernet_wkstn***, один ***ethernet_server*** і два ***ethernet4_slip8_gtwy*** роутера.
3. З'єднайте обидва роутера разом двунаправленим зв'язком ***PPP_DS1***.
4. З'єднайте робочі станції і сервер з роутерами, використовуючи двонаправлений зв'язок ***10Base_T*** як показано на малюнку.
5. Змініть назву доданим об'єктам, як показано щоб потім зберегти проект.



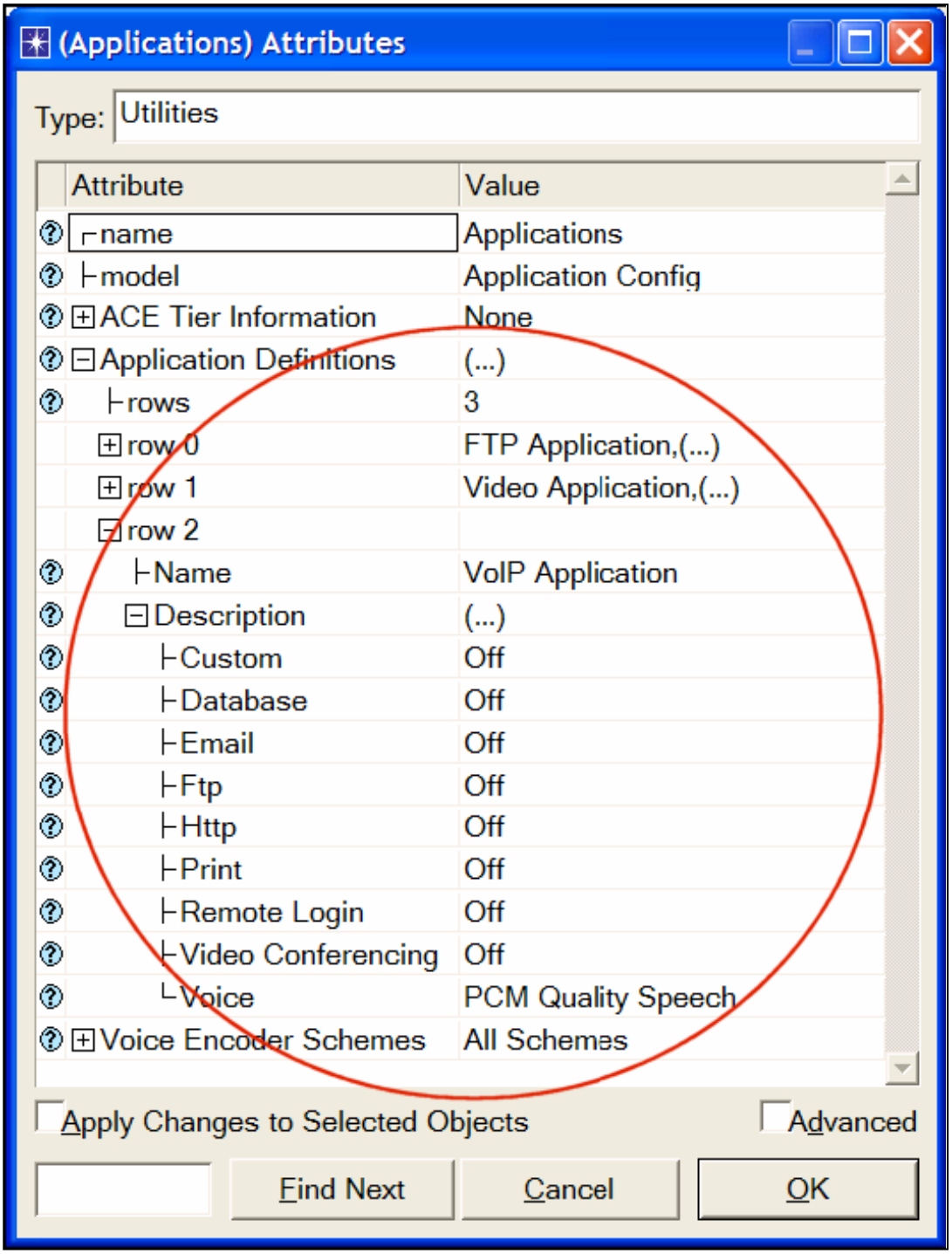
Налаштування програми

1. ПКМ по вузлу ***Applications*** => ***Edit Attributes*** => Розширте ієрархію ***Application Definitions*** => Встановіть ***rows*** на 3 => Назвіть їх: ***FTP Application***, ***Video Application*** і ***VoIP Application***.
   а) Переходьте на ***FTP Application*** => Розширте ієрархію ***Description*** => Призначте ***High Load*** на ***FTP*** => Натисніть на значення ***High Load*** і виберіть ***Edit*** з випадаючого меню => Призначте ***Constant*** (***10***) в ***Inter-Request Time*** => Призначте ***Constant*** (***1000000***) в ***File Size***. Залиште ***Type of Service*** (***ToS***) як ***Best Effort*** (***0***).

b) Тепер перейдіть на ***Video Application*** => Розширте ієрархію ***Description*** => Призначте ***Low Resolution Video*** на ***Video Conferencing*** => Натисніть на значення ***Low Resolution Video*** і виберіть ***Edit*** => Змініть значення поля ***Type of Service*** (З'явиться вікно ***Configure TOS / DSCP***) => З випадного меню підтвердіть ***Streaming Multimedia*** (***4***) в ***ToS*** => Натисніть ***OK*** двічі.

c) Переходьте на ***VolP Application*** => Розширте ієрархію ***Description*** => Призначте ***PCM Quality Speech*** в ***Voice*** => Якщо ви зміните це, то побачите, що ***ToS*** призначений в ***Interactive Voice*** (***6***). ***Type of Servic***е (***ToS***) призначений в ***IP*** пакетах. Він являє собою сесію атрибутів, які дозволяють пакети, якщо відповідний сервіс знаходиться в IP черги. Доставка Best-effort означає, що доставка пакетів спробує бути зроблена, але не гарантована. ***PCM*** (***Pulse Code Modulation***) це процедура, яка використовується для перекладу голосу в цифрову форму, перед тим як доставити його в мережу.

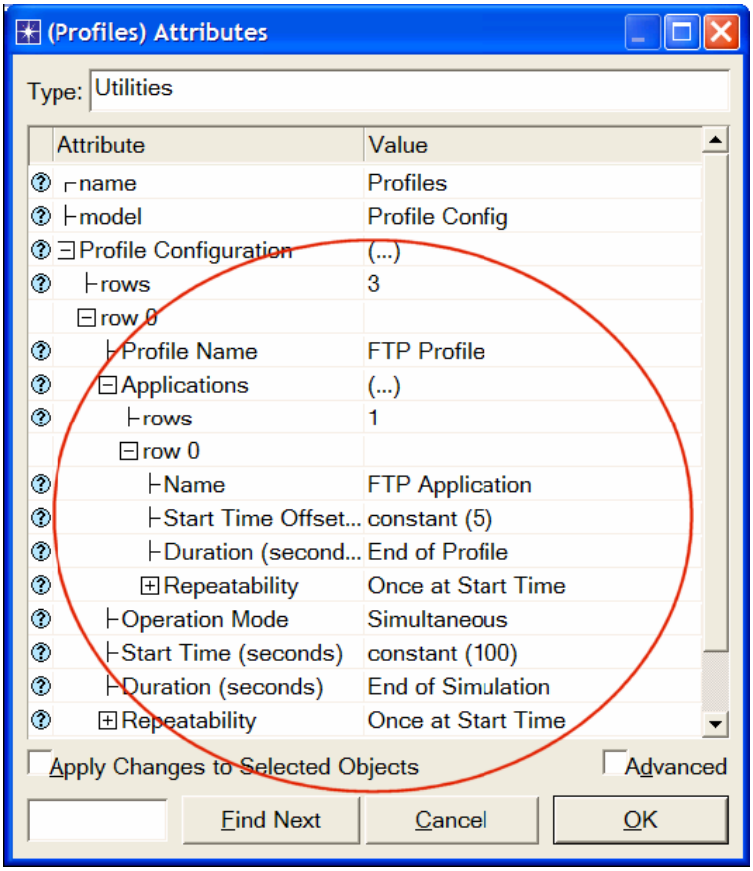
2. Натисніть ***OK*** а потім збережіть свій проект.



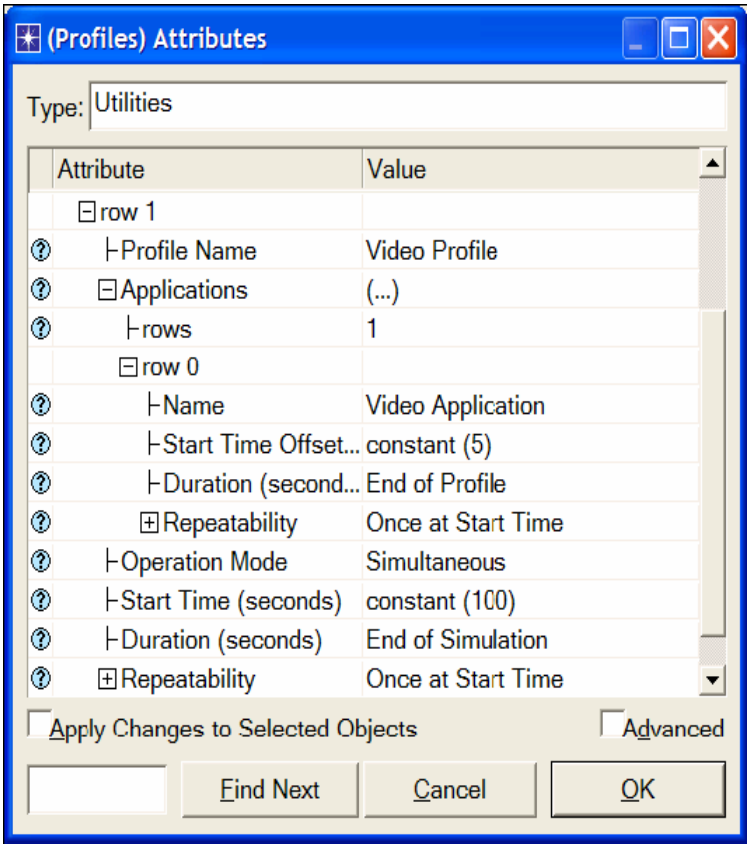
Налаштування профілів

1. ПКМ на ***Profile*** => ***Edit Attributes*** => Розширте ієрархію ***Profile Configuration*** => Встановіть ***rows*** в ***3***.

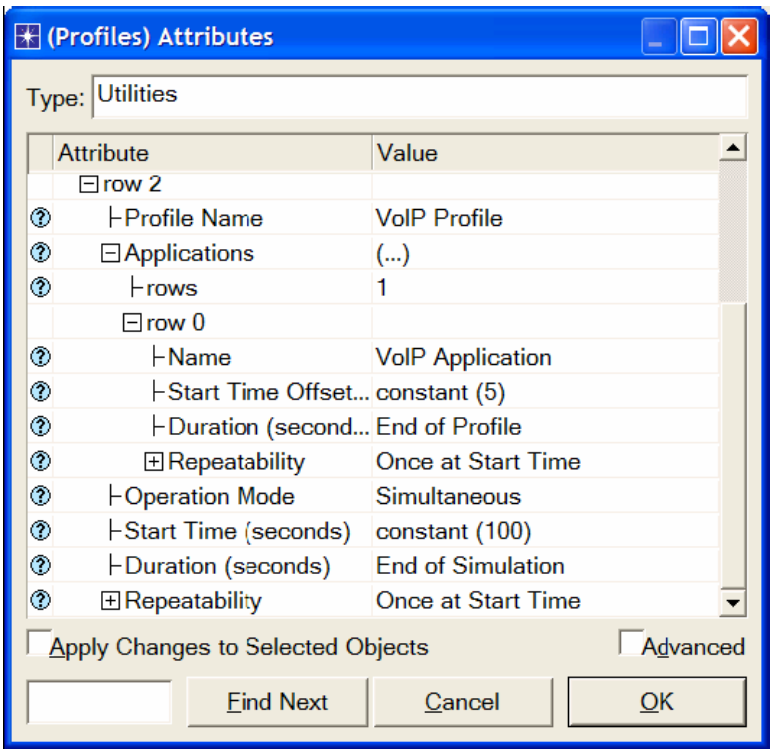
а) Проіменуйте і встановіть атрибути row 0, як показано на малюнку:



б) Проіменуйте і встановіть атрибути ***row*** 1, як показано на малюнку:



в) Проіменуйте і встановіть атрибути ***row*** 2, як показано на малюнку:



2. Натисніть ***OK*** і збережіть свій проект.

Налаштування черг

Ми не будемо змінювати наші налаштування черг, які встановлені в нашому об'єкті ***Queues***. Це рекомендується, якщо ви перевіряєте конфігурацію профілів ***FIFO***, ***PQ*** і ***WFQ***.

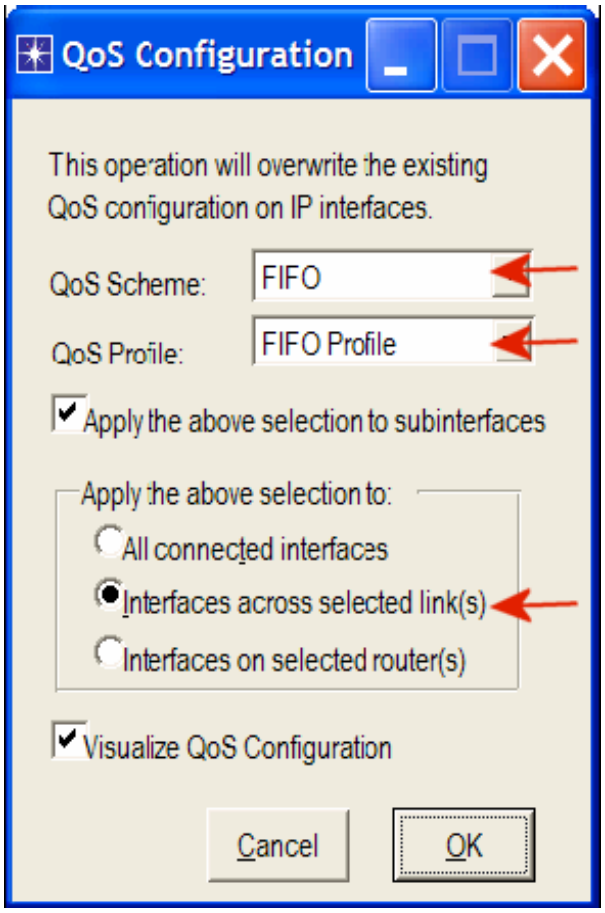
Налаштування робочої станції і серверів

1. Натисніть ПКМ на ***FTP Client*** => ***Edit Attributes*** => Розширте ієрархію ***Application: Supported Profiles*** => встановіть ***row*** в 1 => Встановіть ***Profile Name*** як ***FTP Profile*** => Натисніть ***OK***.
2. Натисніть правою кнопкою на ***Video Client*** => ***Edit Attributes*** => Розширте ієрархію ***Application: Supported Profiles*** => встановіть ***row*** в 1 => Встановіть ***Profile Name*** як ***Video Profile*** => Натисніть ***OK***.
3. Натисніть ПКМ на ***VoIP West*** => ***Edit Attributes***.
   а) Розширте ієрархію ***Application: Supported Profiles*** => встановіть ***row*** в 1=> Встановіть ***Profile Name*** як ***VoIP Profile***.
   б) Змініть значення ***Application: Supported Services*** => встановіть ***row*** в 1 => Встановіть ***Service Name*** як ***VoIP Application*** => Натисніть ***OK*** двічі.
4. Натисніть ПКМ на ***VoIP East*** => ***Edit Attributes***.
   а) Розширте ієрархію ***Application: Supported Profiles*** => встановіть ***row*** в 1 => Встановіть ***Profile Name*** як ***VoIP Profile***.
   б) Змініть значення ***Application: Supported Services*** => встановіть ***row*** в 1=> Встановіть ***Service Name*** як ***VoIP Application*** => Натисніть ***OK*** двічі.
5. Натисніть ПКМ на ***FTP Server*** => ***Edit Attributes*** => Змініть значення ***Application:*** Supported Services => встановіть ***row*** в 1 => Встановіть ***Service Name*** як ***FTP Application*** => Натисніть ***OK*** двічі.

6. Натисніть ПКМ на ***Video Server*** => ***Edit Attributes*** => Змініть значення ***Application: Supported Services*** => встановіть ***row*** в 1 => Встановіть ***Service Name*** як ***Video Application*** => Натисніть ***OK*** двічі.
7. Збережіть свій проект.

Налаштування роутерів

1. Натисніть на посилання з'єднання роутерів ***East*** та ***West***, щоб вибрати їх => З меню ***Protocols*** виберіть => ***IP*** => ***QoS*** => ***Configure QoS.***
2. Переконайтеся, що встановили вибрані об'єкти в ***shown*** в діалоговому вікні ***QoS Configuration*** => Натисніть ***OK***.



Примітка: Якщо опція ***Visualize QoS Configuration*** включена, то використовується посилання, засноване на кольорі схеми ***QoS*** (блакитна для ***FIFO***).

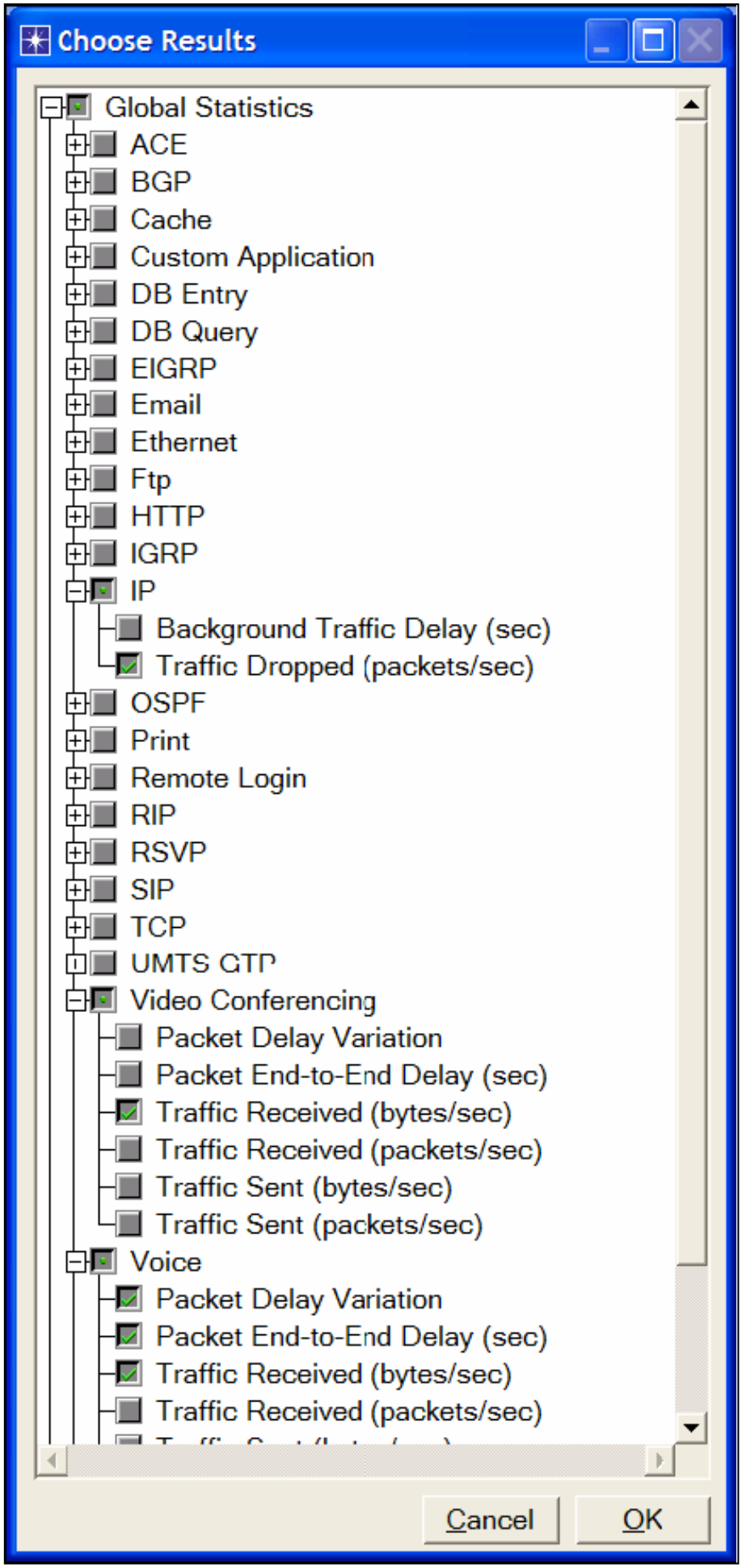
3. Збережіть свій проект.

Виберіть статистику

Щоб тестувати виконання програм визначених у мережі, ми зберемо одну з багатьох доступних статистик наступним чином:

1. ПКМ в будь-якому місці робочої області проекту та виберіть ***Choose Individual Statistics*** із спливаючого меню.

2. У діалоговому вікні ***Choose Results***, виберіть таку загальну статистику:


Choose Results
Global Statistics
ACE
BGP
Cache
Custom Application
DB Entry
DB Query
EIGRP
Email
Ethernet
Ftp
HTTP
IGRP
IP
Background Traffic Delay (sec)
Traffic Dropped (packets/sec)
OSPF
Print
Remote Login
RIP
RSVP
SIP
TCP
UMTS GTP
Video Conferencing
Packet Delay Variation
Packet End-to-End Delay (sec)
Traffic Received (bytes/sec)
Traffic Received (packets/sec)
Traffic Sent (bytes/sec)
Traffic Sent (packets/sec)
Voice
Packet Delay Variation
Packet End-to-End Delay (sec)
Traffic Received (bytes/sec)
Traffic Received (packets/sec)
Cancel
OK

3. Клацніть ОК для того, щоб зберегти ваш проект.

Конфігурація моделювання

Тут нам потрібно конфігурувати тривалість моделювання:

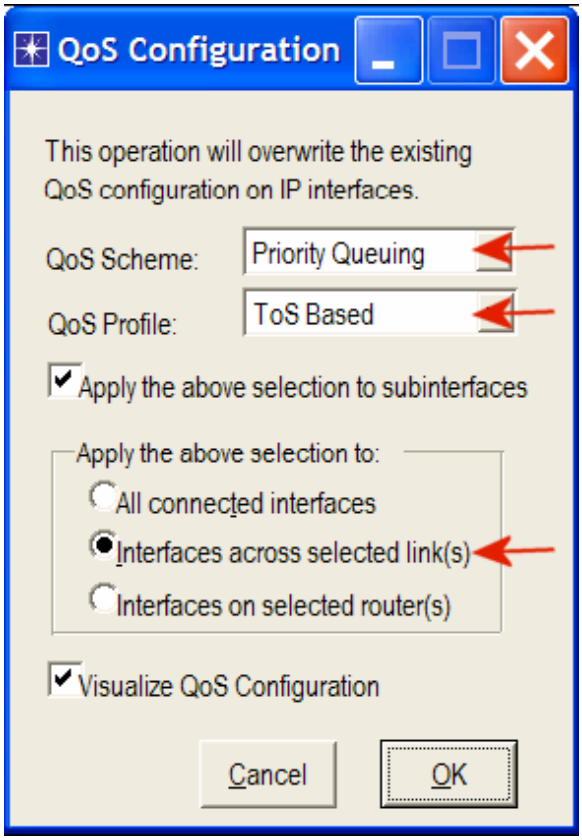
1. Клацніть на  , повинно з'явитися вікно ***Configure Simulation***.
2. Визначте в ***150*** секунд.
3. Клацніть ***OK***, щоб потім зберегти ваш проект.

Дублювання сценарію

У мережі, що ми тільки що створили, ми використовували організацію черги дисципліни ***FIFO*** в маршрутизаторах. Щоб аналізувати ефект іншої організації черги дисциплін, ми створимо 2 нових сценарія, для тестування дисциплін ***PQ*** і ***WFQ***.

А. Виберіть ***Duplicate Scenario*** з меню ***Scenarios*** і дайте йому ім'я ***PQ*** ⇒ Клікніть ***OK***.

1. Клацніть на з'єднанні ***East*** і ***West*** маршрутизаторів щоб вибрати їх ⇒ з меню ***Protocols*** виберіть ***IP → QoS → Configure QoS***.
2. Переконайтеся, що вибрані пункти відповідають показаному діалоговому вікну, ***QoS Configuration*** ⇒ Клікніть ***OK***.



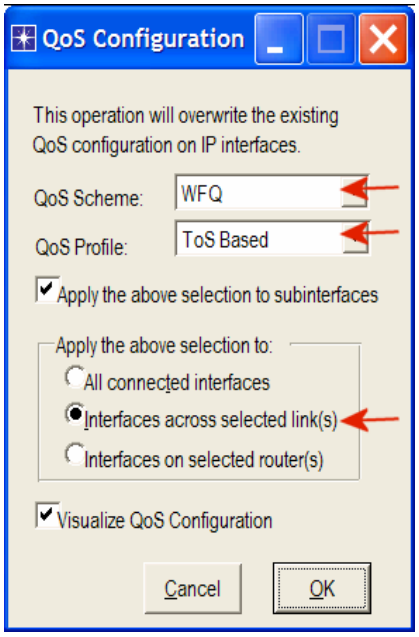
Примітка: оскільки прапорець ***Visualize QoS Configuration*** буде відмічен, зв'язок буде пофарбован на основі використовуваної схеми ***QoS*** (помаранчевий для пріоритетної організації черги).

3. Збережіть ваш проект.

В. Виберіть ***Duplicate Scenario*** з меню ***Scenarios*** і дайте йому ім'я ***WFQ*** ⇒ Клікніть ***OK.***

4. Клацніть на з'єднанні ***East*** і ***West*** маршрутизаторів, щоб вибрати їх ⇒ З меню ***Protocols*** виберіть ***IP → QoS → Configure QoS***.

5. Переконайтеся, що вибрані пункти відповідають показаному діалоговому вікну, ***QoS Configuration*** ⇒ Клікніть ***OK***.



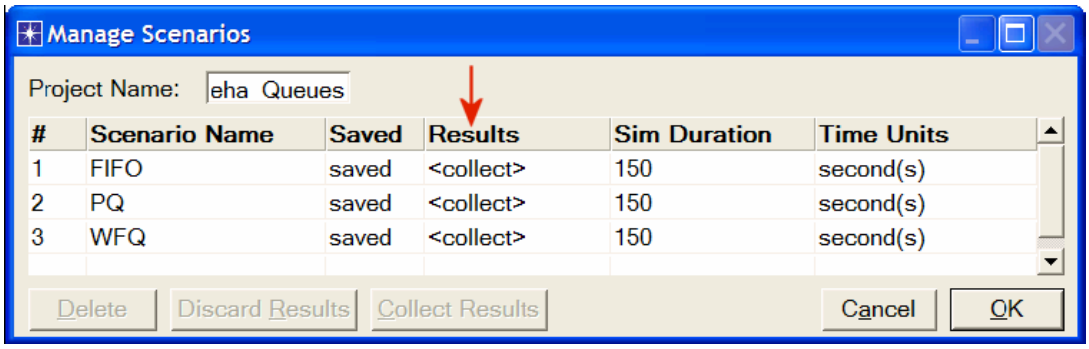
Примітка: Оскільки прапорець ***Visualize QoS Configuration*** буде відмічен, зв'язок буде пофарбована на основі використовуваної схеми ***QoS*** (зелена для ***WFQ***).

3. Збережіть ваш проект.

Запуск моделювання

Для запуску моделювання для трьох сценаріїв одночасно:

1. Ідіть в меню ***Scenarios*** ⇒ Виберіть ***Manage Scenarios***.
2. Змініть величини під колонкою ***Results*** для трьох сценаріїв. Порівняйте з наступною формою.



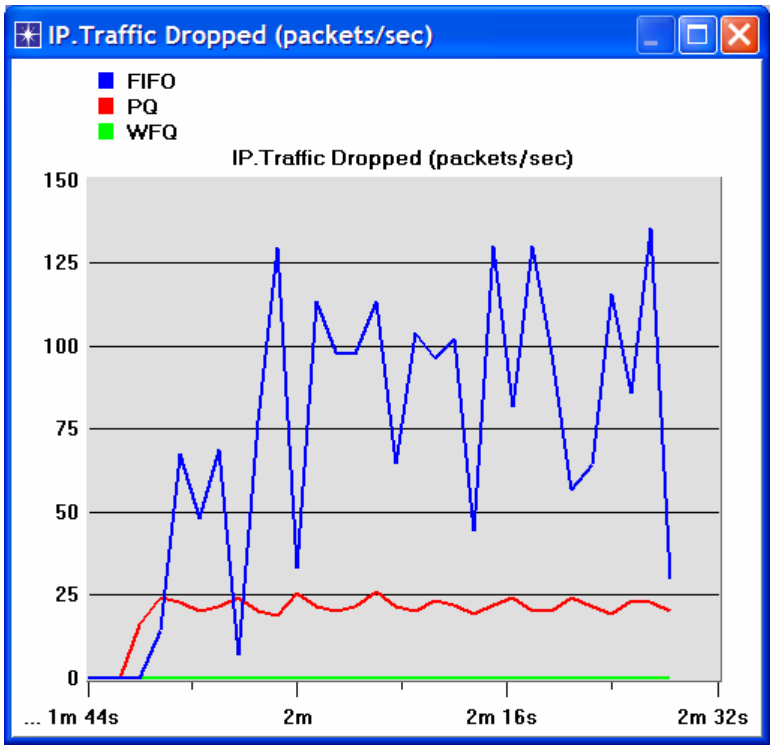
3. Клацніть ***OK*** щоб запустити три сценарії. В залежності від швидкості вашого процесора, буде потрібно декілька хвилин для завершення.
4. Після того, як моделювання завершитися трьома запусками для кожного сценарію, клікніть ***Close***.
5. Збережіть ваш проект.

Зауваження: Фактичні результати базово трохи поміняються у фактичному вузлі, що позиціонується в проекті.

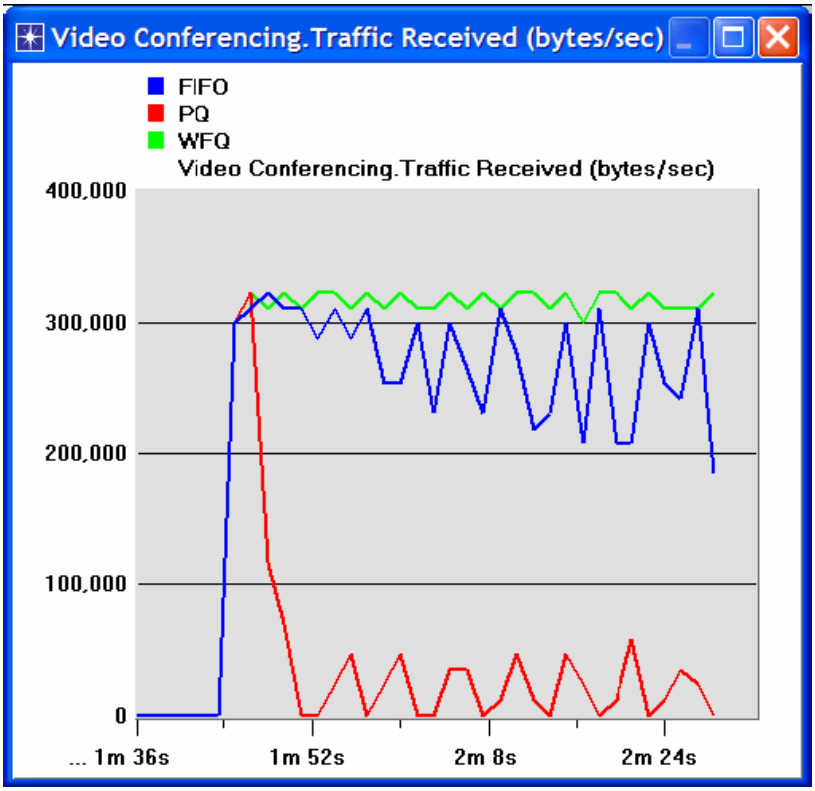
Відображення результатів

Для того, щоб показати і проаналізувати результати:

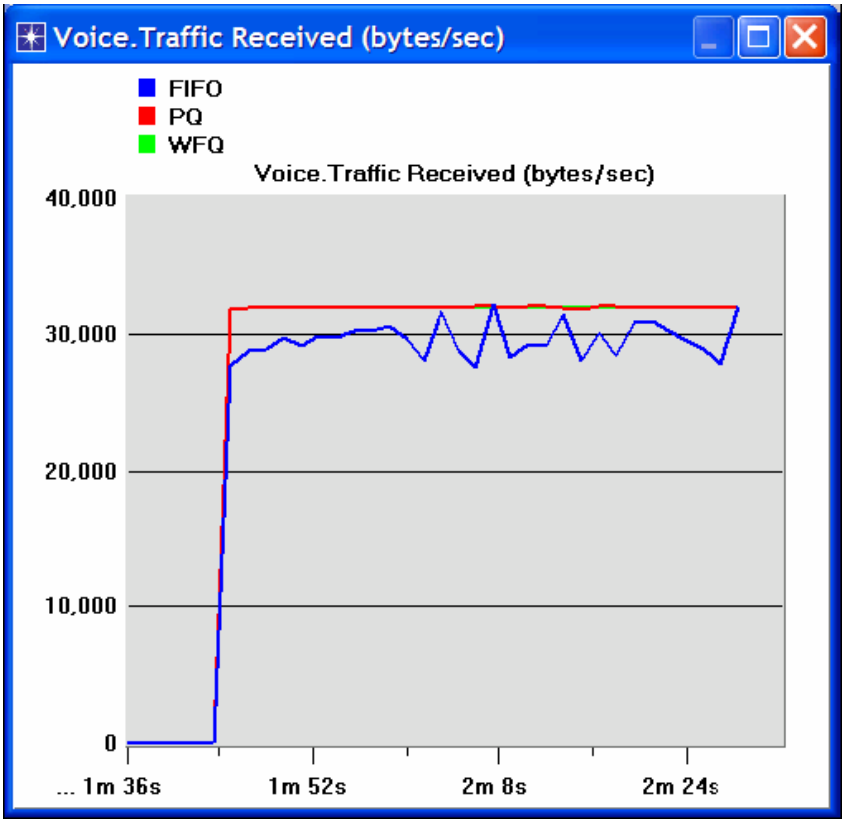
1. Виберіть ***Compare Results*** з меню ***Results***.
2. Виберіть ***IP Traffic Dropped*** та натисніть ***Show***. Результуючий графік повинен нагадувати той нижній. Увага: показаний графік - це результат зміни масштабу області вставки на оригінальному графіку.



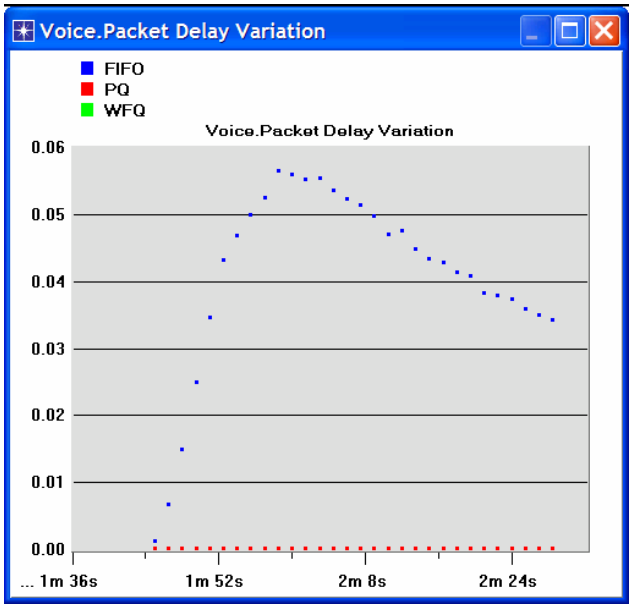
Побудуйте графік для ***Video Conferencing Traffic Received***.

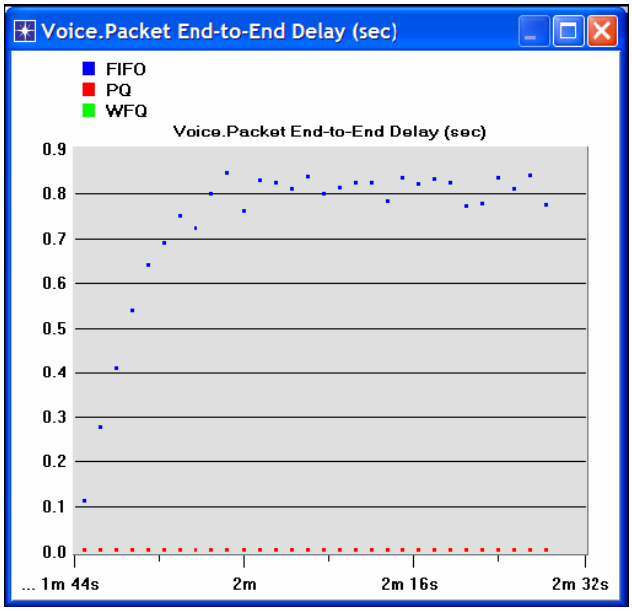


Побудуйте графік для ***Voice Traffic Received***.



Побудуйте графіки для ***Voice Packet End-to-end Delay*** і ***Voice Packet Delay variation***.





Додаткова інформація: IETF RFC номер 2474 (www.ietf.org / rfc.html)

КОНТРОЛЬНІ ЗАПИТАННЯ

1) Проаналізуйте отримані графіки ***Voice Packet End-to-End Delay*** і ***Voice Packet Delay Variation*** і спробуйте порівняти їх. Порівняйте три дисципліни черг і поясніть їх на прикладі роботи трьох додатків.
2) У здійсненому проекті редагуйте об'єкт ***Queues*** і перевірте профілі, призначені для ***FIFO***, ***PQ*** і ***WFQ*** дисциплін. Для кожного профілю дайте відповідь на наступні питання:
   а) скільки черг пов'язано з кожною дисципліною?
   б) в даній роботі ми використовуємо параметр ***ToS*** для завдання пріоритету і ваги для ***PQ*** і ***WFQ*** відповідно. Які ще параметри можуть бути використані для завдання пріоритету або ваги?

в) як конфігуруються черги в ***PQ*** щоб зберегти різні значення ***ToS***?

г) як конфігуруються черги в ***WFQ*** щоб зберегти різні значення ***ToS***?

3) Для всіх сценаріїв оберіть "***queuing delay***» - статистику для зв'язку, який з'єднує ***East Router*** і ***West Router***. Поверніться в режим моделювання та згенеруйте графіки щоб порівняти затримки в чергах для всіх дисциплін. Проаналізуйте їх.

Попередження: при виборі «***queuing*** delay» статистика в ієрархічному вигляді.

ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ

Підготуйте звіт, виконаний за рекомендаціями до лабораторної роботи. Звіт повинен включати відповіді на вищезгадані питання, а також графіки, які Ви отримали при моделюванні сценаріїв. Проаналізуйте результати, які Ви отримали і порівняйте ці результати з очікуваними. Включіть до звіту будь-які аномалії або незрозумілу з Вашої точки зору поведінку.

Лабораторна робота №10

БРАНДМАУЕРИ І VPN.
МЕРЕЖЕВА БЕЗПЕКА ТА ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ

Мета роботи. Вивчити роль брандмауерів і віртуальних приватних мереж (***VPN***) в забезпеченні безпеки в загальнодоступних мережах типу Інтернет.

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Зазвичай комп'ютерні мережі являють собою розділяємий ресурс, який використовується багатьма програмами для різних цілей. Іноді передача даних між процесами, являються конфіденційними, і користувачі додатків бажають, щоб інші не змогли їх прочитати.

Брандмауер - це спеціально запрограмований маршрутизатор, що знаходиться між вузлом і рештою мережі. Маршрутизатор він у тому сенсі, що приєднаний до двох або більше фізичних мереж, і пересилає пакети з однієї мережі в іншу, але крім цього він фільтрує пакеті, що проходять через нього. Брандмауер дозволяє системному адміністратору зосередити політику безпеки в одному місці. Брандмауери, засновані на фільтрах, - найпростіший і найбільш широко використовуваний клас брандмауерів. Вони конфігуруються таблицею адрес, яка описує пакети, які потрібно і не потрібно пропускати.

VPN - приклад контрольованої зв'язку через публічну мережу типу Інтернет. VPN використовує ідею IP-тунелювання (IP tunnel) - віртуального з'єднання «точка-точка» між парою вузлів, фактично розділених довільною кількістю мереж. Для створення маршрутизатором біля входу в тунель віртуального з'єднання задається IP-адреса маршрутизатора на іншому кінці тунелю. Коли маршрутизатор на вході хоче послати пакет через VPN, він інкапсулює його в IP-датаграму. Адреса одержувача в IP-заголовку - це адреса маршрутизатора на дальньому кінці тунелю, а в якості адреси відправника вказана адреса маршрутизатора, що здійснив інкапсуляцію.

У цій лабораторній роботі ви налаштуєте мережу, в якій користувачі з різними правами здійснюють доступ до серверів через Інтернет. Ви вивчите, як брандмауери та VPN забезпечують безпеку серверів, що підтримують доступ користувачів з відповідними правами.

Політика безпеки брандмауерів

Основи і мета

Поза комп'ютерної галузі брандмауером (firewall) називається стіна, зроблена з негорючих матеріалів і перешкоджає поширенню пожежі. У сфері комп'ютерних мереж брандмауер являє собою бар'єр, що захищає від фігуральної пожежі - спроб зловмисників вторгнутися в мережу, для того щоб скопіювати, змінити або стерти інформацію або щоб скористатися смугою пропускання, пам'яттю або обчислювальною потужністю працюючих у цій мережі комп'ютерів. Брандмауер встановлюється на кордоні мережі, що захищається, і фільтрує всі вхідні і вихідні дані, пропускаючи тільки авторизовані пакети.

Брандмауер є набором компонентів, налаштованих таким чином, щоб реалізувати певну політику контролю зовнішнього доступу до вашої мережі. Зазвичай брандмауери захищають внутрішню мережу компанії від "вторгнень" з Internet, проте вони можуть використовуватися і для захисту від "нападів", наприклад, з корпоративної інтрамережі, до якої підключена і ваша мережа. Як і в разі реалізації будь-якого іншого механізму мережевого захисту, організація, що виробляє конкретну політику безпеки, крім усього іншого, повинна визначити тип трафіку TCP / IP, який буде сприйматися брандмауером як "авторизований". Наприклад, необхідно вирішити, чи буде обмежений доступ користувачів до певних служб на базі TCP / IP, і якщо буде, то до якої міри. Вироблення політики безпеки допоможе зрозуміти, які компоненти брандмауера вам необхідні і як їх настроїти, щоб забезпечити ті обмеження доступу, які ви задали.

Робота всіх брандмауерів заснована на використанні інформації різних рівнів моделі OSI (таблиця 1). Модель OSI, розроблена Міжнародною організацією по стандартизації (International Standards Organization - ISO), визначає сім рівнів, на яких комп'ютерні системи взаємодіють одина з одною, -

починаючи з рівня фізичного середовища передачі даних і закінчуючи рівнем прикладних програм, що використовуються для комунікацій. У загальному випадку, чим вище рівень моделі OSI, на якому брандмауер фільтрує пакети, тим вище і забезпечуваний ним рівень захисту.

Таблиця 1 - Брандмауери і моделі OSI.

Рівень моделі OSI	**Протоколи Internet**	**Категорія брандмауера**
Прикладний	Telnet, FTP, DNS, NFS, PING, SMTP, HTTP	Шлюз прикладного рівня, брандмауер експертного рівня
Подання даних		
Сеансовий	TCP	Шлюз сеансового рівня
Транспортний	TCP	
Мережевий	IP	Брандмауер з фільтрацією пакетів
Канальний		
Фізичний		

Основна функція брандмауера - централізація управління доступом. Якщо видалені користувачі можуть отримати доступ до внутрішніх мереж в обхід брандмауера, його ефективність близька до нуля. Наприклад, якщо менеджер, що знаходиться у відрядженні, має модем, приєднаний до його ПЕОМ в офісі, то він може додзвонитися до свого комп'ютера з відрядження, а так як ця ПЕОМ також знаходиться у внутрішній захищеній мережі, то атакуючий, що має можливість встановити комутоване з'єднання з цієї ПЕОМ, може обійти захист брандмауера. Якщо користувач має підключення до Інтернету у якого-небудь провайдера Інтернету, і часто з'єднується з Інтернетом з своєї робочої машини за допомогою модему, то він або вона встановлюють небезпечне з'єднання з Інтернетом, в обхід захисту брандмауера.

Брандмауери часто можуть бути використані для захисту сегментів інтранета організації, але цей документ в-основному буде описувати проблеми, пов'язані з Інтернетом. Більш детальна інформація про брандмауери міститься в

"NIST Special Publication 800-10" Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls. "

Брандмауери забезпечують декілька типів захисту:

• Вони можуть блокувати небажаний трафік
• Вони можуть направляти вхідний трафік тільки до надійних внутрішніх систем
• Вони можуть приховати уразливі системи, які не можна убезпечити від атак з Інтернету іншим способом.
• Вони можуть протоколювати трафік в і з внутрішньої мережі
• Вони можуть приховувати інформацію, таку як імена систем, топологію мережі, типи мережних пристроїв і внутрішні ідентифікатори користувачів, від Інтернету
• Вони можуть забезпечити більш надійну аутентифікацію, ніж та, яку представляють стандартні додатки.

Кожна з цих функцій буде описана далі.

Як і для будь-якого засобу захисту, потрібні певні компроміси між зручністю роботи і безпекою. Прозорість - це видимість брандмауера як внутрішнім користувачам, так і зовнішнім, що здійснюють взаємодію через брандмауер. Брандмауер прозорий для користувачів, якщо він не заважає їм отримати доступ до мережі. Зазвичай брандмауери конфігуруються так, щоб бути прозорими для внутрішніх користувачів мережі (які посилають пакети назовні за брандмауер), і з іншого боку брандмауер конфігурується так, щоб бути непрозорим для зовнішніх користувачів, що намагаються отримати доступ до внутрішньої мережі ззовні. Це зазвичай забезпечує високий рівень безпеки і не заважає внутрішнім користувачам.

Аутентифікація

Брандмауери на основі маршрутизаторів не забезпечують аутентифікації користувачів. Брандмауери, до складу яких входять проксі-сервера, забезпечують такі типи аутентифікації:

Ім'я / пароль

Це найгірший варіант, так як ця інформація може бути перехоплена в мережі або отримана шляхом підглядання за її введенням за спини і ще тисячею інших способів.

Одноразові паролі

Вони використовують програми або спеціальні пристрої для генерації нового пароля для кожного сеансу. Це означає, що старі паролі не можуть бути повторно використані, якщо вони були перехоплені в мережі або вкрадені іншим способом.

Електронні сертифікати

Вони використовують шифрування з відкритими ключами

Аналіз можливостей маршрутизації і проксі-серверів

У гарній політиці має бути написано, чи може брандмауер маршрутизувати пакети або вони повинні передаватися з допомогою проксі-серверів. Тривіальним випадком брандмауера є маршрутизатор, який може виступати в ролі пристрою для фільтрації пакетів. Все, що він може - тільки маршрутизувати пакети. А прикладні шлюзи навпаки не можуть бути налаштовані для маршрутизації трафіку між внутрішнім і зовнішнім інтерфейсами брандмауера, так як це може привести до обходу засобів захисту. Всі з'єднання між зовнішніми і внутрішніми хостами повинні проходити через прикладні шлюзи (проксі-сервера).

Маршрутизація джерела

Це механізм маршрутизації, за допомогою якого шлях до машини-одержувача пакета визначається відправником, а не посередником маршрутизатором. Маршрутизація джерела в основному використовується для усунення проблем у мережах, але також може бути використана для атаки на хост. Якщо атакуючий знає, що ваш хост довіряє якому-небудь іншому хосту, то маршрутизація джерела може бути використана для створення враження, що пакети атакуючого приходять від довіреного хоста. Тому через таку загрозу безпеки маршрутизатори з фільтрацією пакетів зазвичай конфігуруються так, щоб відкидати пакети з опцією маршрутизації джерела. Тому сайт, який бажає уникнути проблем з маршрутизацією джерела, зазвичай розробляє політику, в якій їх маршрутизація заборонена.

Фальсифікація IP-адреси

Це має місце, коли атакуючий маскує свою машину під хост в мережі об'єкта атаки (тобто намагається змусити ціль атаки думати, що пакети приходять від довіреної машини у внутрішній мережі). Політика щодо маршрутизації пакетів повинна бути чіткою, щоб можна було коректно побудувати обробку пакетів, якщо є проблеми з безпекою. Необхідно об'єднати аутентифікацію на основі адреси відправника з іншими способами, щоб захистити вашу мережу від атак подібного роду.

Типи брандмауерів

Існує кілька різних реалізацій брандмауерів, які можуть бути створені різними шляхами.

Шлюзи з фільтрацією пакетів

Брандмауери з фільтрацією пакетів використовують маршрутизатори з правилами фільтрації пакетів для надання або заборони доступу на основі адреси відправника, адреси одержувача і порту. Вони забезпечують мінімальну

безпеку за низьку ціну, і це може виявитися прийнятним для середовища з низьким ризиком. Вони є швидкими, гнучкими і прозорими. Правила фільтрації часто нелегко адмініструвати, але є ряд засобів для спрощення завдання створення і підтримки правил.

Шлюзи з фільтрацією мають свої недоліки, включаючи такі:

• Адреси і порти відправника і одержувача, що містяться в заголовку IP-пакета, - єдина інформація, доступна маршрутизатору при ухваленні рішення про те, дозволяти чи забороняти доступ трафіку у внутрішню мережу.

• Вони не захищають від фальсифікації IP-і DNS-адрес.

• Атакуючий отримає доступ до всіх хостів у внутрішній мережі після того, як йому було надано доступ брандмауером.

• Посилена аутентифікація користувача не підтримується деякими шлюзами з фільтрацією пакетів.

• У них практично відсутні кошти протоколювання доступу до мережі

Прикладний шлюз використовує програми (звані проксі-серверами), що запускаються на брандмауері. Ці проксі-сервера приймають запити ззовні, аналізують їх і передають безпечні запити внутрішнім хостам, які надають відповідні послуги. Прикладні шлюзи можуть забезпечувати такі функції, як аутентифікація користувачів і протоколювання їх дій.

Так як прикладний шлюз вважається безпечним типом брандмауера, ця конфігурація має ряд переваг з точки зору сайту з середнім рівнем ризику:

• Брандмауер може бути налаштований як єдиний хост, видимий із зовнішньої мережі, що буде вимагати проходити всі з'єднання із зовнішньою мережею через нього.

• Використання проксі-серверів для різних сервісів запобігає прямий доступ до цих сервісів, захищаючи організацію від небезпечних чи погано сконфігурованих внутрішніх хостів

• За допомогою прикладних шлюзів може бути реалізована посилена автентифікація.

• Проксі-сервера можуть забезпечувати детальне протоколювання на прикладному рівні

Брандмауери прикладного рівня повинні конфігуруватися так, щоб весь вихідний трафік здавався вихідним від брандмауера (тобто щоб тільки брандмауер було видно зовнішніх мереж). Таким чином буде заборонений прямий доступ до внутрішніх мереж. Усі вхідні запити різних мережевих сервісів, таких як Telnet, FTP, HTTP, RLOGIN, і т.д., незалежно від того, який внутрішній хост запитується, повинні проходити через відповідний проксі-сервер на брандмауері.

Прикладні шлюзи вимагають проксі-сервера для кожного сервісу, такого як FTP, HTTP і т.д., підтримуваного брандмауером. Коли потрібний сервіс не підтримується проксі, в організації є три варіанти дій:

• Відмовитись від використання цього сервісу, поки виробник брандмауера не розробить для нього безпечний проксі-сервер - це кращий підхід, оскільки багато нових сервісів мають велике число вразливих місць.

• Розробити свій проксі - це досить складна задача і повинна вирішуватися тільки технічними організаціями, що мають відповідних фахівців.

• Пропустити сервіс через брандмауер - використання того, що зазвичай називається "заглушками", більшість брандмауерів з прикладними шлюзами дозволяє пропускати більшість сервісів через брандмауер з мінімальною фільтрацією пакетів. Це може обмежити число вразливих місць, але привести до компрометації систем за брандмауерів.

Низький ризик

Коли для вхідних інтернетівських сервісів немає проксі-сервера, але потрібно пропускати його через брандмауер, адміністратор брандмауера повинен використовувати конфігурацію або "латочку", яка дозволить використовувати необхідний сервіс. Коли проксі-сервер розробляється виробником, то "латочка" повинна бути відключена.

Середній-високий

Усі вхідні інтернетівські сервіси повинні оброблятися проксі-сервером на брандмауері. Якщо потрібне використання нового сервісу, то його використання має бути заборонено до тих пір, поки виробник брандмауера не розробить для нього проксі-сервер і він не буде протестований адміністратором брандмауера. Тільки за спеціальним дозволом керівництва можна розробляти свій проксі-сервер або закуповувати його в інших виробників.

Гібридні або складні шлюзи

Гібридні шлюзи об'єднують в собі два описаних вище типу брандмауера і реалізують їх послідовно, а не паралельно. Якщо вони з'єднані послідовно, то загальна безпека збільшується, з іншого боку, якщо їх використовувати паралельно, то загальна безпека системи буде рівна найменш безпечному з використовуваних методів. В середовищах з середнім і високим ризиком, гібридні шлюзи можуть виявитися ідеальною реалізацією брандмауера.

Архітектури брандмауера

Брандмауери можуть бути налаштовані у вигляді однієї з декількох архітектур, що забезпечує різні рівні безпеки при різних витратах на установку і підтримку працездатності. Організації повинні проаналізувати свій профіль ризику і вибрати відповідну архітектуру. Наступні розділи описують типові архітектури брандмауера і приводять приклади політик безпеки для них.

Хост, підключений до двох сегментів мережі

Це такий хост, який має більше одного інтерфейсу з мережею, причому кожен інтерфейс з мережею підключений фізично до окремого сегменту мережі. Найпоширенішим прикладом є хост, підключений до двох сегментів.

Брандмауер на основі хоста, підключеного до двох сегментах мережі

Це брандмауер з двома мережевими платами, кожна з яких підключена до окремої мережі. Наприклад, одна мережева плата сполучена з зовнішньою або небезпечною мережею, а інша - з внутрішньою або безпечною мережею. У цій конфігурації ключовим принципом забезпечення безпеки є заборона прямої маршрутизації трафіку з недовіреною мережі в довірену - брандмауер завжди повинен бути при цьому посередником.

Маршрутизація повинна бути відключена на брандмауері такого типу, щоб IP-пакети з однієї мережі не могли пройти в іншу мережу.

Примітка перекладача: Така конфігурація, напевно, є однією з найдешевших і розповсюджених при комутованому підключенні ЛОМ організації до Інтернету. Береться машина, на яку встановлюється FreeBSD, і на ній забороняється маршрутизація, крім того відповідним чином конфігурується вбудований в ядро пакетний фільтр (ipfw).

Екранований хост

При архітектурі типу екранований хост використовується хост (званий хостом-бастіоном), з яким може встановити з'єднання будь-який зовнішній хост, але заборонений доступ до всіх інших внутрішніх, менш безпечних хостів. Для цього фільтруючий маршрутизатор конфігурується так, що всі з'єднання з внутрішньою мережею із зовнішніх мереж направляються до хосту-бастіону.

Якщо шлюз з пакетною фільтрацією встановлений, то хост-бастіон повинен бути налаштований так, щоб всі з'єднання із зовнішніх мереж

проходили через нього, щоб запобігти пряме з'єднання між мережею організації та Інтернетом.

Екранована під мережа

Архітектура екранованої мережі по суті збігається з архітектурою екранованого хоста, але додає ще одну лінію захисту, за допомогою створення мережі, в якій знаходиться хост-бастіон, відділений від внутрішньої мережі.

Екранована підмережа повинна впроваджуватися за допомогою додавання мережі-периметра для того, щоб відокремити внутрішню мережу від зовнішньої. Це гарантує, що навіть при успіху атаки на хост-бастіон, атакуючий не зможе пройти далі мережі-периметра через те, що між внутрішньою мережею і мережею-периметром знаходиться ще один маршрутизатор, що екранує.

Інтранет

Хоча брандмауери зазвичай містяться між мережею і зовнішньої небезпечною мережею, у великих організаціях або компаніях брандмауери часто використовуються для створення різних підмереж в мережі, часто званої інтранет. Брандмауери в интранеті розміщуються для ізоляції окремої підмережі від решти корпоративної мережі. Причиною цього може бути те, що доступ до цієї мережі потрібний тільки для деяких співробітників, і цей доступ повинен контролюватися брандмауерами і надаватися тільки в тому обсязі, який потрібен для виконання обов'язків співробітника. Прикладом може бути брандмауер для фінансового відділу або бухгалтерії в організації.

Рішення використовувати брандмауер звичайно грунтується на необхідності надавати доступ до деякої інформації деяким, але не всім внутрішнім користувачам, або на необхідності забезпечити хороший облік доступу та використання конфіденційної і критичної інформації.

Для всіх систем організації, на яких розміщені критичні програми або які надають доступ до критичної або конфіденційної інформації, повинні використовуватися внутрішні брандмауери та фільтрувальні маршрутизатори для забезпечення суворого контролю доступу та аудіювання. Ці засоби захисту повинні використовуватися для поділу внутрішньої мережі організації заради реалізації політик управління доступом, розроблених власниками інформації (або відповідальними за неї).

Адміністрування брандмауера

Брандмауер, як і будь-який інший мережевий пристрій, повинен кимось управлятися. Політика безпеки повинна визначати, хто відповідає за управління брандмауером.

Повинні бути призначені два адміністратори брандмауера (основний і заступник) відповідальним за інформаційну безпеку (або будь-ким з керівництва) і вони повинні відповідати за працездатність брандмауера. Основний адміністратор повинен робити зміни в конфігурації брандмауера, а його заступник повинен виробляти будь-які дії тільки в відсутність основного, щоб не виникало суперечливих установок.

Кожен адміністратор брандмауера повинен повідомити свій домашній номер телефону, номер пейджера, стільникового телефону або іншу інформацію, необхідну для того, щоб зв'язатися з ним в будь-який час.

Кваліфікація адміністратора брандмауера

Зазвичай рекомендується мати двох досвідчених людей для щоденного адміністрування брандмауера. При такій організації адміністрування брандмауер буде працювати практично без збоїв. Інформація про кожного адміністратора повинна бути обов'язково в письмовому вигляді, щоб швидко зв'язатися з ними при виникненні проблем.

Безпека сайту важлива для повсякденної діяльності організації. Тому потрібно, щоб адміністратор брандмауера по-справжньому розумів принципи мережевих технологій та їх реалізації. Наприклад, так як більшість брандмауерів зроблено для роботи з TCP / IP, необхідне серйозне розуміння всіх особливостей цього протоколу. Більш докладно про знання і навички, необхідні для технічних фахівців, дивіться в розділі "Адміністрування ЛВС".

Людина, призначена адміністратором брандмауера, повинна мати великий досвід роботи з мережевими технологіями, щоб брандмауер був правильно налаштований і був коректно адміністрований. Адміністратор брандмауера повинен періодично відвідувати курси по брандмауерам та теорії і практиці мережевої безпеки або іншим способом підтримувати високий професійний рівень.

Віддалене адміністрування брандмауера

Брандмауери - перша лінія оборони, видима для атакуючого. Так як брандмауери в загальному випадку важко атакувати безпосередньо через їх призначення, атакуючі часто намагаються отримати логін адміністратора на брандмауері. Імена і паролі адміністративних логінів повинні бути серйозно захищені.

Найкращим методом захисту від такої форми атаки є серйозна фізична безпека самого брандмауера і адміністрування брандмауера тільки з локального терміналу. Але в повсякденному житті часто потрібна деяка форма видаленого доступу для виконання деяких операцій з адміністрування брандмауера. У будь-якому випадку віддалений доступ до брандмауера по небезпечним мережам повинен здійснюватися з використанням посиленої аутентифікації. Крім того, для запобігання перехоплення сеансів повинно використовуватися наскрізне шифрування всього трафіку віддаленого з'єднання з брандмауером.

Низький ризик

При будь якому віддаленому доступу по небезпечним мережам для адміністрування брандмауера повинена використовуватися посилена аутентифікація, така як одноразові паролі і смарт-карти.

Середній ризик

Кращим методом адміністрування брандмауера є робота з локального терміналу. Фізичний доступ до терміналу брандмауера повинен бути дозволений тільки адміністраторові брандмауера і адміністраторові архівних копій.

Коли потрібен віддалений доступ для адміністрування брандмауера, він повинен здійснюватися тільки з інших хостів внутрішньої мережі організації. Такий внутрішній віддалений доступ вимагає посиленої аутентифікації, такий як одноразові паролі і смарт-карти. Віддалений доступ по небезпечним мережам, таким як Інтернет, вимагає використання крізного шифрування всього трафіку з'єднання і посиленої аутентифікації.

Високий ризик

Все адміністрування брандмауера повинно здійснюватися тільки з локального терміналу - робота з брандмауером шляхом віддаленого доступу заборонена. Фізичний доступ до терміналу брандмауера дозволений тільки адміністраторові брандмауера і адміністраторові архівних копій.

Зареєстровані користувачі

Брандмауери ніколи не повинні використовуватися як сервера загального призначення. Єдиними зареєстрованими користувачами на брандмауері можуть бути тільки адміністратор брандмауера і адміністратор архівних копій. Крім того, тільки ці адміністратори повинні мати привілеї для модифікації завантажувальних модулів програм на ньому.

ільки адміністратор брандмауера і адміністратори архівних копій повинні мати логіни на брандмауері організації. Будь-яка модифікація

системних програм на брандмауері повинна здійснюватися адміністратором або адміністратором архівних копій з дозволу відповідального за мережеві сервіси (або начальника відділу автоматизації).

Архівні копії брандмауера

Для забезпечення можливості відновлення після збою або стихійного лиха, брандмауер, як і будь-який інший мережевий хост, повинен мати політику щодо створення архівних копій. Для всіх файлів даних, а також системних файлів конфігурації повинен бути певний план створення архівних копій.

Для брандмауера (його системних програм, конфігураційних файлів, баз даних і т.д.) повинні створюватися щоденні, щотижневі та щомісячні архівні копії, щоб у разі збою можна було відновити дані і файли конфігурації. Архівні копії повинні зберігатися в безпечному місці на носії, з якого можна тільки зчитати інформацію, щоб їх випадково не затерли, яке має бути замкнено, щоб носії були доступні тільки відповідним співробітникам.

Іншою альтернативою буде мати запасний брандмауер, сконфігурований як основний, і підтримуваний в холодному резерві, щоб у разі збою основного, запасний міг бути включений і використаний замість нього, поки основний брандмауер відновлюється.

Довірчі взаємозв'язки в мережі

Комерційні мережі часто вимагають взаємодії з іншими комерційними мережами. Такі сполуки можуть здійснюватися по виділених лініях, приватним глобальним мережам, або громадським глобальним мережам, таким як Інтернет. Наприклад, багато урядів штатів використовують виділені лінії для з'єднання з регіональними офісами в штаті. Багато компаній використовують комерційні глобальні мережі для зв'язку своїх офісів в країні.

Сегменти мереж, що беруть участь в передачі даних, можуть перебувати під управлінням різних організацій, у яких можуть бути різні політики безпеки.

За своєю природою мережі такі, що загальна мережева безпека дорівнює безпеці найменш безпечної ділянки мережі. Коли мережі об'єднуються, повинні бути визначені взаємозв'язки довіри, щоб уникнути зменшення безпеки всіх інших мереж.

Надійні мережі визначаються як мережі, у яких є однакова політика безпеки або в яких використовуються такі програмно-апаратні засоби безпеки та організаційні заходи, які забезпечують однаковий стандартний набір сервісів безпеки. Ненадійні мережі - це ті мережі, де не реалізован стандартний набір сервісів безпеки, або де рівень безпеки є нестабільним або невідомим. Найбезпечнішою політикою є дозволяти з'єднання тільки з надійними мережами. Але бізнес може зажадати тимчасового з'єднання з діловими партнерами або віддаленими сайтами, при якому будуть використовуватися ненадійні мережі.

Високий ризик

Всі з'єднання мережі організації з зовнішніми мережами повинні бути затверджені відповідальним за мережеві сервіси і знаходитися під його контролем. Повинні дозволятися з'єднання тільки з тими зовнішніми мережами, для яких був проведений аналіз і встановлено, що в них є необхідні програмно-апаратні засоби безпеки і застосовуються необхідні організаційні заходи. Всі з'єднання до затверджених мереж повинні проходити через брандмауери організації.

Середній ризик - низький ризик

Всі з'єднання мережі організації з зовнішніми мережами повинні бути затверджені відповідальним за мережеві сервіси. Всі з'єднання з затвердженими зовнішніми мережами повинні проходити через брандмауер організації.

Щоб зменшити шкоду від такого великого уразливого місця, всі з'єднання з зовнішніми мережами і логіни користувачів, що працюють з ними, повинні періодично перевірятися, і видалятися, якщо вони більше не потрібні.

Системні журнали з'єднань із зовнішніми мережами повинні проглядатися щотижня. Всі логіни, які використовують такі сполуки, які більше не використовуються протягом місяця, повинні бути відключені. Відповідальний за мережеві сервіси повинен опитувати начальників відділів кожен квартал на предмет необхідності таких сполук. Якщо з'єднання з тією чи іншою мережею більше не потрібно, і відповідальний за мережеві сервіси сповіщений про це, всі логіни і параметри, пов'язані з цим з'єднанням, повинні бути вилучені протягом одного робочого дня.

Віртуальні приватні мережі (VPN)

Віртуальні приватні мережі дозволяють надійній мережі взаємодіяти з іншою надійної мережею по небезпечній мережі, такій як Інтернет. Оскільки деякі брандмауери мають можливості створення VPN, необхідно визначити політику для створення VPN.

Будь-яке з'єднання між брандмауерами з суспільних глобальних мереж має використовувати механізм шифрованих віртуальних приватних мереж для забезпечення конфіденційності та цілісності даних, переданих по глобальних мережах. Всі VPN-з'єднання повинні бути затверджені відповідальним за мережеві сервіси і знаходитися під його контролем. Також мають бути створені відповідні кошти розподілу та адміністрування ключів шифрування перед початком експлуатації VPN. VPN на основі брандмауерів можуть бути створені у вигляді декількох різних конфігурацій. Служби VPN дозволяють створити канал контрольованого шифрованого зв'язку з Internet, гарантуючи конфіденційність пакетів, що передаються з цього каналу. Таким чином, компанії отримують можливість створювати захищені приватні мережі, з'єднані

через Internet. В VPN використовується спеціальний метод шифрування, заснований на 40-бітній реалізації криптографічного алгоритму RC2.

Цей алгоритм забезпечує прийнятну продуктивність роботи на WAN-каналах і може виконуватися в симетричних мультипроцесорних системах, що дозволяє підвищити швидкість шифрування даних. Служби безпеки включають в себе фільтрацію пакетів, шлюз сеансового рівня, програму-посередника HTTP прикладного рівня і використовують технології трансляції адрес.

Віртуальні приватні мережі (Virtual Private Networks - VPN), що дозволяють передавати конфіденційну інформацію по мережах загального користування, виникли як альтернатива дорогим приватним мережам, що базувався на виділених каналах зв'язку. Останнім часом завдяки розвитку електронних форм ведення бізнесу, його глобалізації та збільшення числа мобільних і віддалених користувачів, яким необхідний безпечний доступ до корпоративної мережі, інтерес до них зріс. А найбільш обговорюваною технологією сьогодні є так звані Layer 2 VPN.

Треба сказати, що точного визначення VPN не існує, а множинність трактувань цього поняття дає кожній компанії можливість з повним правом заявляти, що саме її продукти реалізують справжні VPN. Однак для замовника не важливо, яким визначенням користуватися. Йому потрібна відповідна функціональність. Проте з наявних визначень можна вибрати найбільш загальне. Сутність віртуальних приватних мереж полягає у використанні публічної телекомунікаційної інфраструктури для забезпечення безпечного доступу віддалених філій і користувачів до основної мережі організації (Remote Access VPN) або для об'єднання географічно віддалених локальних мереж (LAN-to-LAN VPN).

Найбільш універсальним способом побудови VPN є використання технології тунелювання, або інкапсуляції. Ця технологія дозволяє передавати пакети однієї мережі (первинної) по каналах зв'язку іншої (вторинної). Для

цього пакет первинної мережі (дані і протоколи) инкапсулюється в пакет вторинної мережі і стає видно, як дані. Взагалі кажучи, інкапсуляція не передбачає кодування. Якщо для підвищення рівня безпеки воно необхідне, то повинно виконуватися засобами приватної мережі до процедури інкапсуляції.

Тунель можна представити як наскрізний віртуальний канал, що має початкову точку (ініціатор тунелю) і одну або більше кінцевих (термінаторів тунелю). Цими точками можуть бути комп'ютер віддаленого користувача, який працює як VPN-клієнт, маршрутизатор, шлюз або сервер доступу до мережі (Network Access Server - NAS). На обох кінцях необхідно встановити апаратне і програмне забезпечення (включаючи шифрування / дешифрування, якщо воно є), що працює у відповідності з тими протоколами, за допомогою яких був утворений тунель. Хоча термін "тунель" асоціюється з фіксованим шляхом, насправді для мереж з комутацією пакетів (Internet зокрема) це не так. Зашифровані і інкапсульовані пакети можуть використовувати різні маршрути між кінцевими точками. Основне призначення тунелю - забезпечити конфіденційність сесії. Це означає, що ніхто, крім отримувача, не розшифрує (в ідеалі) пакет, і чужі пакети не можуть потрапити в тунель, оскільки маршрутна інформація для VPN зберігається окремо від загальної.

Традиційно VPN (тунелювання та / або шифрування) організують на нижніх рівнях комунікаційного стека протоколів - канальному (Layer 2) і мережному (Layer 3). Відповідно до цього розрізняють віртуальні приватні мережі на рівні 2 (Layer 2 VPN) і на рівні 3 (Layer 3 VPN).

Для побудови тунелів на різних рівнях існують кілька протоколів. Типовим протоколом для Layer 2 VPN є L2F (Layer 2 Forwarding), запропонований Cisco, який інкапсулює пакети у фрейми Frame Relay або в осередку ATM. Для Layer 3 VPN найпоширенішим є протокол IPSec. Його сесію можна представити наступними етапами. Комп'ютер ініціює тунель, зв'язуючись з іншим комп'ютером і посилаючи йому свій сертифікат. У

відповідь ініціатор отримує сертифікат віддаленого комп'ютера. Потім машини починають обмін даними, використовуючи публічний і приватний ключі для їх шифрування і дешифрування, так само як і іншу інформацію, необхідну для успішної та безпечної передачі. Ще одним популярним протоколом цього рівня є Point-to-Point Tunneling Protocol (PPTP), розроблений компанією Microsoft і рядом інших. Він побудований на вершині протоколу PPP (Point-to-Point Protocol), який широко використовувався для доступу до Internet по телефонних комутованих каналах (dial-up). PPTP створює тунель, інкапсулює пакети PPP в IP-пакети.

Починаючи з 1996 р. протоколи L2F і PPTP конкурували між собою. В кінці 1997 р. компанії Cisco і Microsoft домовилися про розробку нового протоколу, що об'єднує достоїнства обох. Ця пропозиція отримала підтримку IETF, а протокол став називатися L2TP (Layer 2 Tunneling Protocol). Основна відмінність між L2TP і PPTP полягає в тому, що перший об'єднує дані і керуючу інформацію і працює через UDP, а не TCP. UDP є більш швидким протоколом і з меншими накладними витратами (і менш надійним), оскільки він не передає повторно загублені пакети, як це передбачається TCP. На противагу цьому PPTP роз'єднує керуючу інформацію і дані. Перша передається по протоколу TCP, тоді як потік даних - по протоколу GRE (Generic Routing Encapsulation) - менш поширеному стандарту для створення тунелю.

Розглянемо коротко, як працює протокол L2TP. Як згадувалося вище, L2TP є надбудовою над PPP. Останній визначає механізм інкапсуляції для передачі мультипротокольних пакетів по каналу рівня 2 (L2) точка - точка. У типовому випадку користувач приєднується по такому каналу (наприклад, по телефонній мережі, ISDN, ADSL і т. п.) до сервера доступу до мережі, і потім по цьому з'єднанню починає працювати протокол PPP. У такій конфігурації термінальна точка каналу L2 і кінцева точка (endpoint) сесії PPP перебувають на тому ж фізичному пристрої (в даному випадку NAS). L2TP розширює модель

PPP, дозволяючи кінцевим точкам каналу L2 і PPP розташовуватися на різних пристроях, які пов'язані між собою мережею з комутацією пакетів. Відповідно до L2TP користувач по каналу L2 приєднується до концентратора доступу (наприклад, до модемного пулу або мультиплексору доступу DSL), який потім по тунелю передає індивідуальні пакети NAS. Це дозволяє не виконувати фактичну обробку PPP-пакетів у термінальній точці каналу L2. Одне з очевидних переваг такого поділу полягає в тому, що канал L2 може мати термінальну крапку на локальному концентраторі, а не на віддаленому NAS, що обійшлося б істотно дорожче.

Для створення L2TP-тунелю використовують два пристрої: концентратор доступу L2TP (L2TP Access Concentrator - LAC) і мережевий сервер L2TP (L2TP Network Server - LNS). LAC є однією з кінцевих точок L2TP-тунелю. Він розташовується між віддаленою системою (користувачем або філією) і LNS. LAC приймає виклики від віддалених систем і інкапсулює PPP-фрейми в пакети L2TP. Потім він направляє їх по L2TP-тунелю на один або кілька LNS по мережі з комутацією пакетів (Internet, Frame Relay, ATM). LNS - друга кінцева точка тунелю, на цей раз з боку корпоративної мережі. Він є логічною кінцевою точкою PPP-сесії. LNS деінкапсулює L2TP-пакети, обробляє PPP-фрейми і направляє їх у корпоративну мережу.

Можливості віртуальних приватних мереж на рівні 2 значно розширюються за допомогою технології мультипротокольной комутації міток (MPLS). Вона дозволяє інкапсулювати за допомогою міток безпосередньо трафік рівня 2 (ATM, Frame Relay SONET і Ethernet) і передавати його по IP-мережі. Цим досягається використання єдиної інфраструктури для мереж L2 VPN і L3 VPN.

МЕТОДИЧНІ ВКАЗІВКИ

Створення нового проекту

1.Запустіть ***OPNET IT Guru Academic Edition*** → Виберіть ***New*** з меню ***File***.

2.Виберіть ***Project*** і натисніть ***OK*** → Назвіть проект <ваші_ініціали> _VPN, і сценарій ***NoFirewall*** → Натисніть ***OK***. Натисніть ***Quit*** на ***Startup Wizard***.

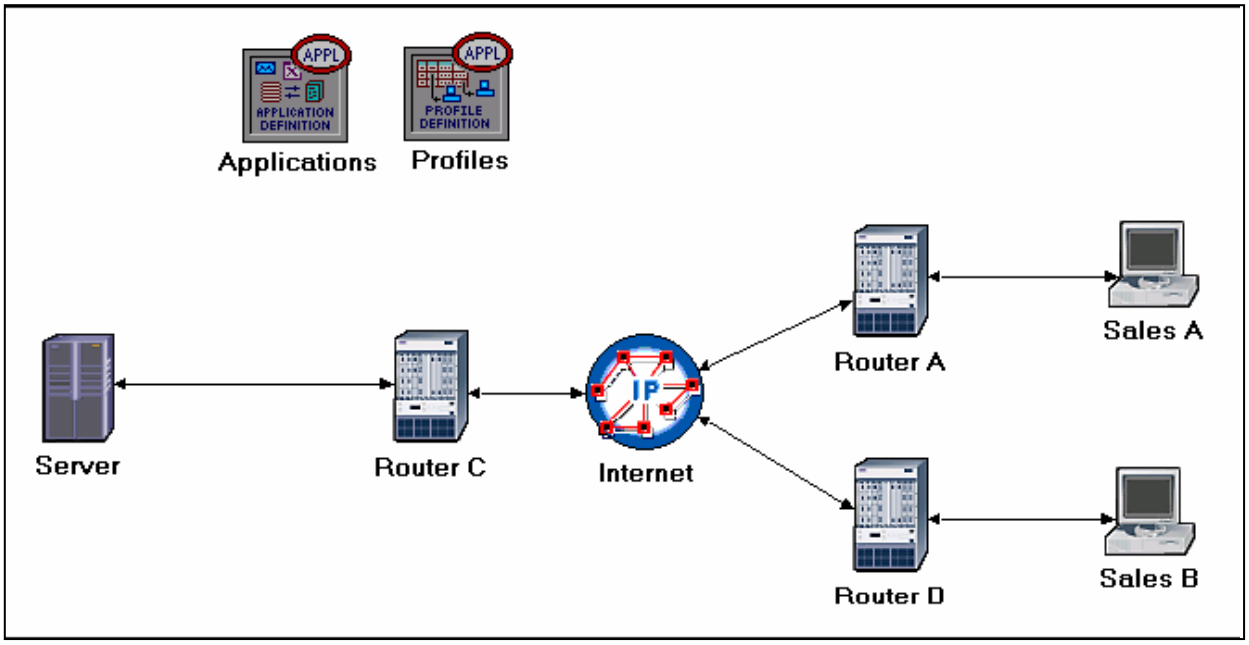
3. Для того, щоб прибрати підкладку з картою світу, виберіть меню ***View*** → ***Background*** → ***Set Border Map*** → Виберіть ***NONE*** з випадаючого меню → Натисніть ***OK***.

Створення та конфігурування мережі

ppp_server і ppp_wkstn підтримує одне базове SLIP (Serial Line Internet Protocol) з'єднання на обраній швидкості передачі даних. PPP DS1 з'єднує два вузли, що підтримують IP. Швидкість передачі даних - 1.544 Mbps.

Ініціалізація мережі

1. Діалогове вікно ***Object Palette*** має бути на робочому просторі вашого проекту. Якщо воно не там, відкрийте його натисканням  . Переконайтеся, що ***internet_toolbox*** обран з меню, що випадає в палітрі об'єктів.
2. Додайте на робочий простір наступні об'єкти з палітри: (зверніть увагу на малюнок нижче): ***Application Config***, ***Profile Config***, ***ip32_cloud***, один ***ppp_server***, три маршрутизатора ***ethernet4_slip8_gtwy***, і два хоста ***ppp_wkstn***. Для того, щоб додати об'єкт з палітри, натисніть на його іконку в палітрі об'єктів → Перемістіть миш на робочий простір → Натисніть ЛКМ, щоб помістити об'єкт на робочий простір → Натисніть ПКМ для того, щоб припинити створення об'єктів цього типу.
3. Змініть назву об'єкта, як показано на малюнку (Правою кнопкою на вузлі → ***Set Name***) і з'єднайте їх, використовуючи ***PPP DS1***, як показано нижче:



4. Збережіть проект.

Конфігурація вузлів

В установках Default є кілька прикладів конфігурацій додатків. Наприклад, "Web Browsing (Heavy HTTP1.1)" означає додаток для перегляду Інтернет-файлів, що виконує інтенсивний перегляд з використанням протоколу HTTP 1.1.

1. ПКМ на вузлі ***Applications*** → ***Edit Attributes*** → Призначте ***Default*** атрибуту ***Application Definitions*** → Натисніть ***OK***.
2. ПКМ на вузлі ***Profiles*** → ***Edit Attributes*** → Призначте ***Sample Profiles*** атрибуту ***Profile Configuration*** → Натисніть ***OK***.
3. ПКМ на вузлі ***Server*** → ***Edit Attributes*** → Призначте ***All*** атрибуту ***Application: Supported Services*** → Натисніть ***OK***.
4. ПКМ на вузлі ***Sales*** A → ***Select Similar Nodes*** (Переконайтеся, що вибрані і ***Sales A***, і ***Sales B***).
   a. ПКМ на вузлі ***Sales A*** → ***Edit Attributes*** → Встановвіть галочку на ***Apply Changes to Selected Objects***.

b. Розгорніть меню атрибута ***Application: Supported Profiles*** → Встановіть ***rows*** на 1 → Розкрийте підпункти ***row*** 0 → ***Profile Name*** = ***Sales Person*** (це один з "профілів-шаблонів", який ми сконфигурировали у вузлі ***Profiles***).

c. Натисніть ***OK***.

5. Збережіть проект

Вибір статистики

DQ Query Response Time міряється в проміжку від часу, коли система запитів до бази даних відправляє запит на сервер, до часу, коли вона отримує у відповідь пакет.

HTTP Page Response Time визначає час, необхідний для завантаження всієї сторінки з усіма включеними об'єктами.

1. ПКМ в будь-якому місці робочого простору і виберіть ***Choose Individual Statistics*** з контекстного меню.
2. У діалоговому вікні ***Choose Results*** виберіть наступну статистику:
   a. ***Global Statistics → DB Query → Response Time (sec)***.
   b. ***Global Statistics → HTTP → Page Response Time (seconds)***.
3. Натисніть ***OK***.
4. ПКМ на вузлі ***Sales A*** і виберіть ***Choose Individual Statistics*** із спливаючого меню.
5. У діалозі ***Choose Results*** виберіть наступну статистику:
   a. ***Client DB → Traffic Received (bytes / sec)***.
   b. ***Client Http → Traffic Received (bytes / sec)***.
6. Натисніть ***OK***.
7. ПКМ на вузлі ***Sales B*** і виберіть ***Choose Individual Statistics*** із спливаючого меню.
8. У діалозі ***Choose Results*** виберіть наступну статистику:

a. ***Client DB → Traffic Received (bytes / sec)***.

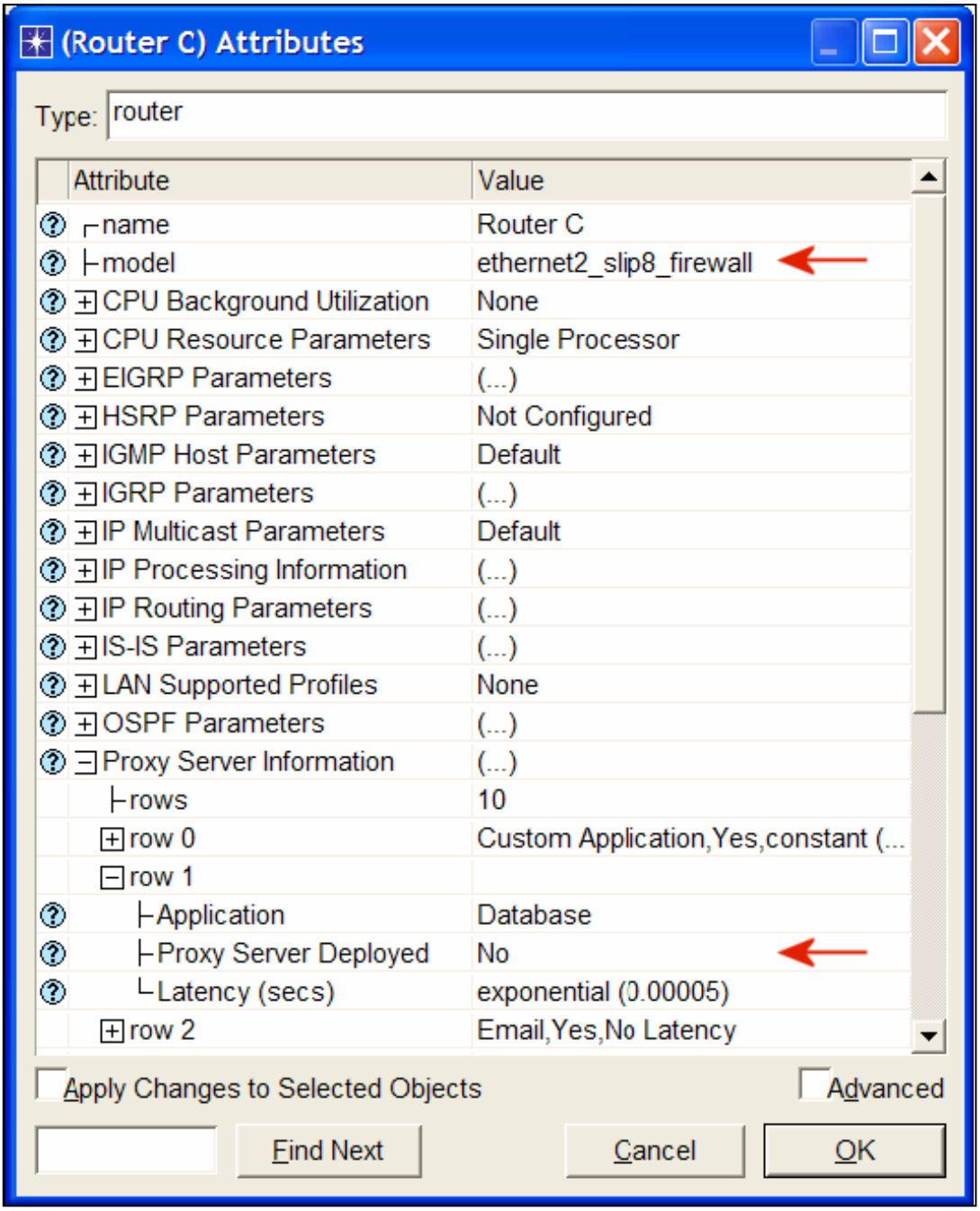
b. ***Client Http → Traffic Received (bytes / sec)***.

9. Натисніть ***OK*** і збережіть проект.

Сценарій з брандмауером

У мережі, яку ми тільки що створили, профіль ***Sales Person*** дозволяє обом точкам продажу отримувати доступ до бази даних, електронної пошти та Інтернет через сервер (перевірте ***Profile Configuration*** у вузлі ***Profiles***). Припустимо, нам необхідно захистити базу даних на сервері від зовнішнього доступу для всіх, включаючи продавців. Один з варіантів зробити це - замінити маршрутизатор ***C*** (***Router C***) брандмауером.

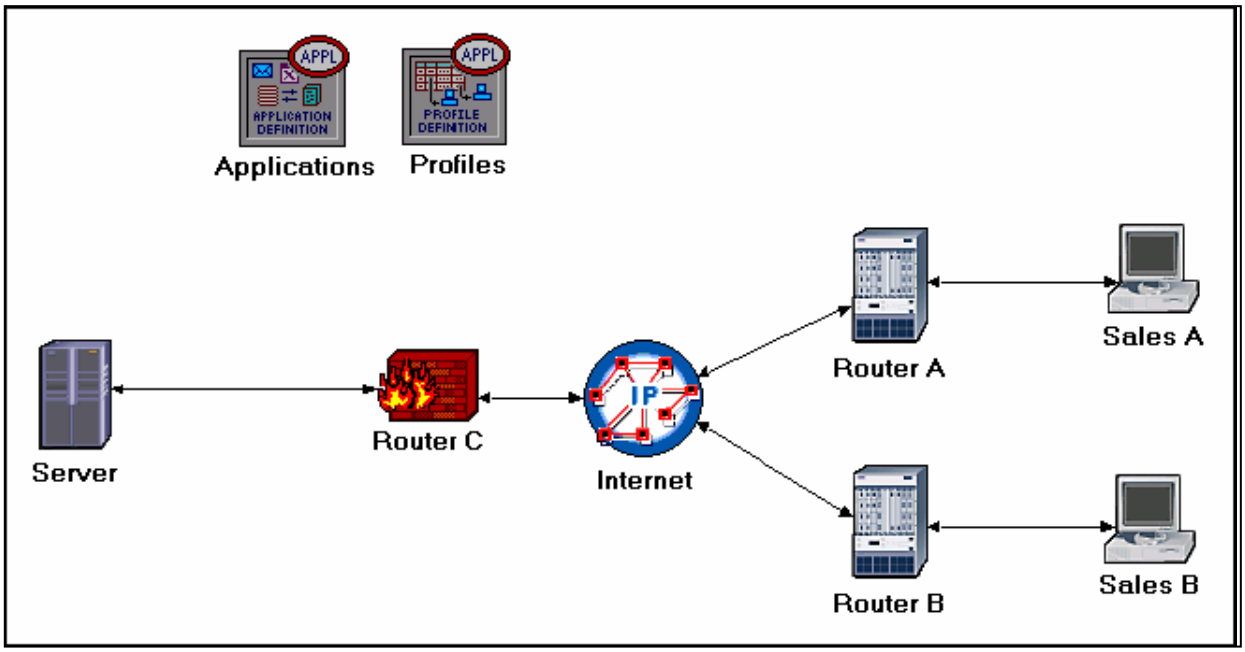
1. Виберіть ***Duplicate Scenario*** з меню ***Scenarios*** і назвіть його ***Firewall →*** Натисніть ***OK***.
2. У новому сценарії натиснітьПКМ на ***Router C → Edit Attributes***.
3. Встановіть атрибуту ***model*** параметр ***ethernet2_slip8_firewall***.
4. Розкрийте підпункти атрибута ***Proxy Server Information →*** Розкрийте підпункти ***row*** 1 в ієрархії ***Database application →*** Встановіть ***No*** для атрибута P***roxy Server Deployed***, як показано на малюнку:



5. Натисніть ***OK*** і збережіть проект.

Proxy Server Information - це таблиця, яка визначає конфігурацію проксі-серверів на брандмауері . Кожен рядок показує, який проксі-сервер встановлений для конкретного застосування і кількість додаткової затримки, доданої до пакетиу, що пересилає проксі-сервер.

Наша конфігурація брандмауера не дозволяє пов'язаному з базою даних трафіку проходити через брандмауер (такі пакети фільтруються). Таким чином, бази даних на сервері захищені від доступу ззовні. Ваш сценарій повинен бути схожий на показаний на малюнку:



Сценарій Firewall_VPN

У сценарії ***Firewall*** ми захистили базу даних від будь-якого доступу ззовні, використавши маршрутизатор-брандмауер. Припустимо, нам необхідно дозволити продавцям з ***Sales A*** доступ до бази даних на сервері. Але так як брандмауер фільтрує весь пов'язаний з базою трафік, незалежно від його джерела, ми розглянемо рішення на базі ***VPN***. Віртуальний тунель буде використовуватися ***Sales A*** для того, щоб відсилати запити до бази на сервер. Брандмауер не буде фільтрувати трафік, створений ***Sales A***, тому що ***IP***-пакети в тунелі будуть інкапсульовані всередині ***IP***-датаграм.

1. Перебуваючи в сценарії ***Firewall***, виберіть ***Duplicate Scenario*** з меню ***Scenarios*** і назвіть його ***Firewall_VPN*** → Натисніть ***OK.***
2. Видаліть з'єднання між ***Router C*** і ***Server.***

3. Відкрийте ***Object Palette***, натиснувши на  . Переконайтеся, що відкрита палітра ***internet_toolbox***.

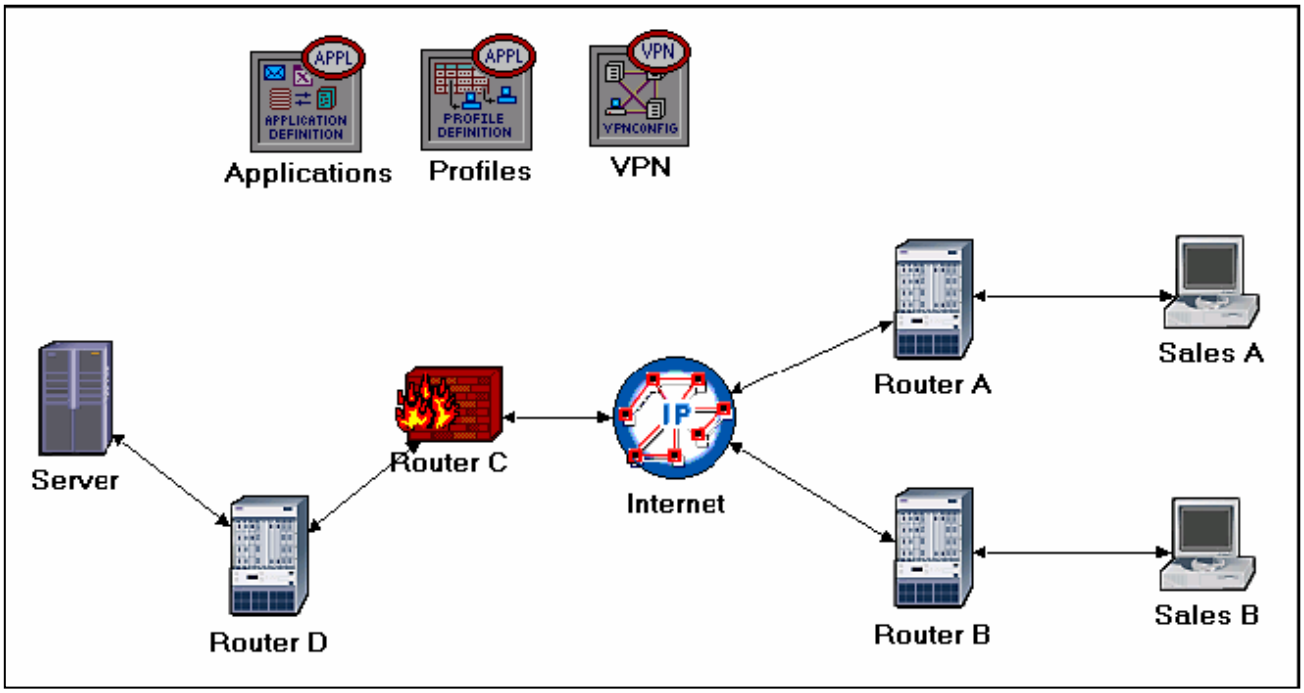
   I. Додайте на робочий простір ***ethernet4_slip8_gtwy*** і один ***IP VPN Config*** (місце розташування дивіться на малюнку внизу).

   II. З ***Object Palette***, використовуйте ***PPP DS1*** для з'єднання нового маршрутизатора з ***Router C*** (брандмауером) і ***Server***, як показано нижче.

   III. Закрийте ***Object Palette***.

4. Змініть назву об'єкта ***IP VPN Config*** в ***VPN***.

5. Змініть назву нового маршрутизатора на ***Router D***, як показано:



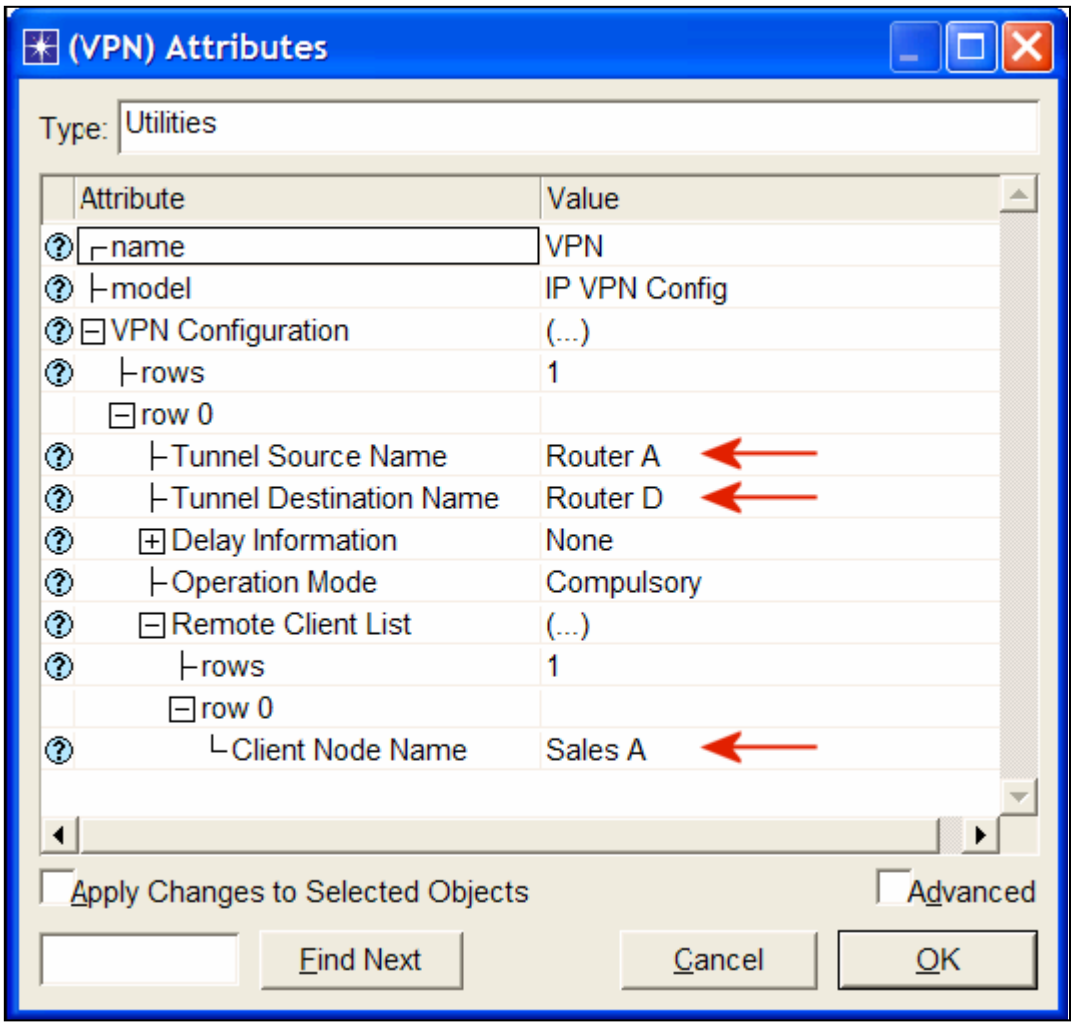
Конфігурація VPN

Натисніть ПКМ на вузлі ***VPN*** → ***Edit Attributes***.

I. Розкрийте підпункти меню ***VPN Configuration*** → Встановіть ***rows*** в 1 → Розкрийте підпункти ***row*** 0 → Відредагуйте значення ***Tunnel Source Name***, вписавши ***Router A*** → Відредагуйте значення ***Tunnel Destination Name***, вписавши ***Router D***.

II. Розкрийте підпункти меню ***Remote Client List*** → Встановіть ***rows*** в 1 → Розкрийте підпункти ***row*** 0 → відредагуйте значення ***Client Node Name***, вписавши ***Sales A***.

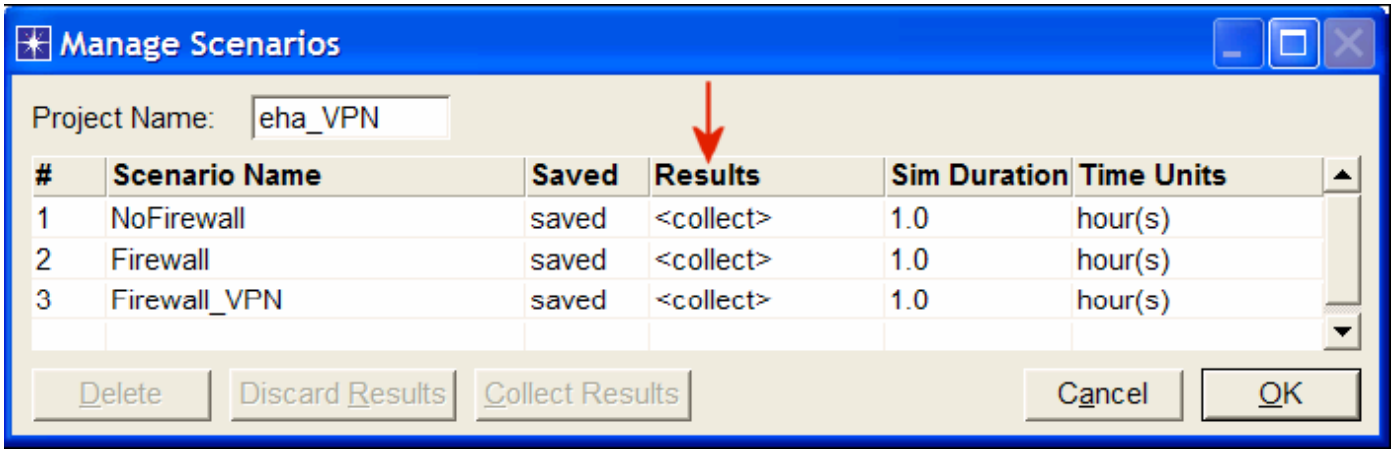
III. Натисніть ***OK*** і збережіть проект.



Запуск моделювання

Для запуску одночасного моделювання трьох сценаріїв:

1. Зайдіть в меню ***Scenarios*** → Виберіть ***Manage Scenarios***.
2. Змініть значення за стовпцем ***Results*** на <collect> (або <recollect>) для трьох сценаріїв. Збережіть значення за замовчуванням для ***Sim Duration*** (1:00).Порівняйте з наступним малюнком.

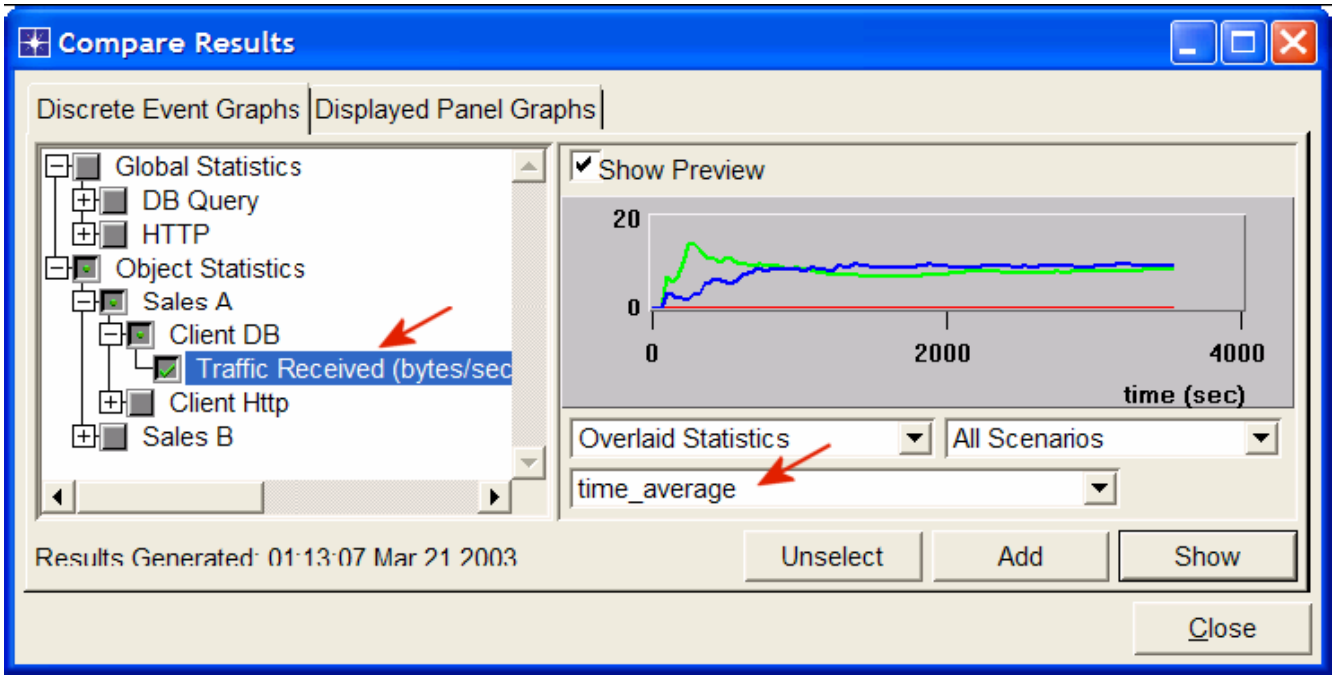


3. Натисніть ***OK*** для запуску трьох моделювань. В залежності від швидкості вашого процесора, це займе кілька хвилин.
4. Після закінчення трьох моделювань, для кожного сценарію, натисніть ***Close*** → Збережіть проект.

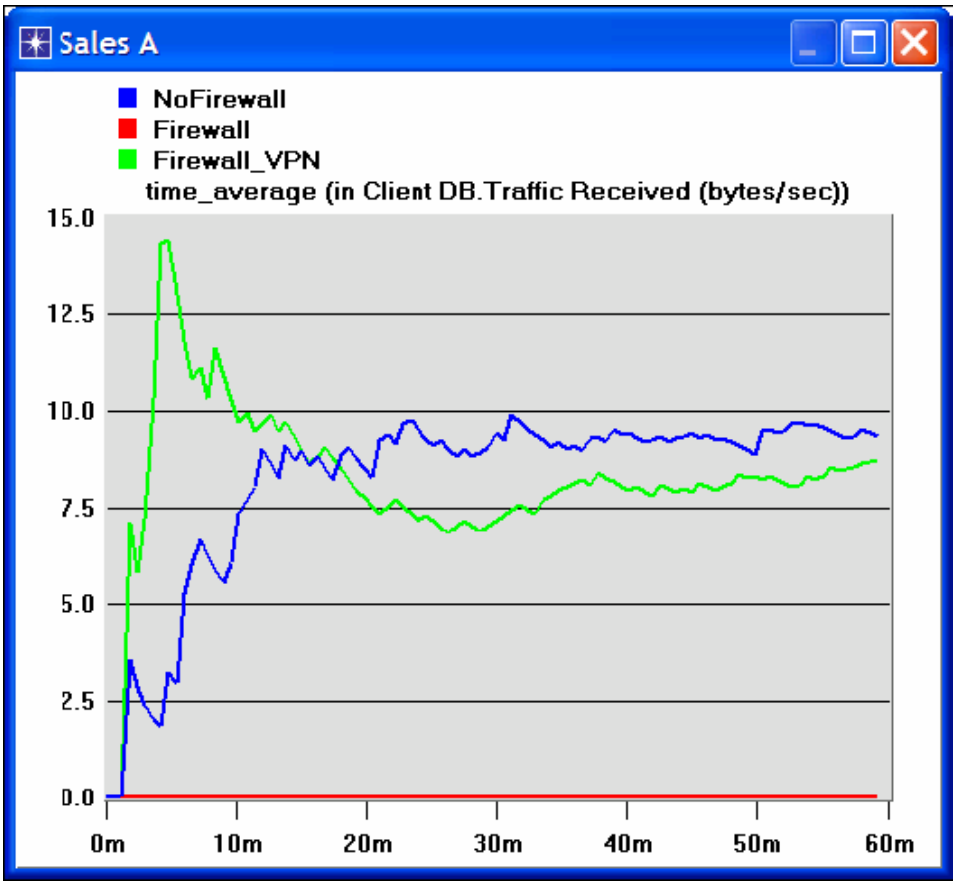
Перегляд результатів

Для перегляду та аналізу результатів:

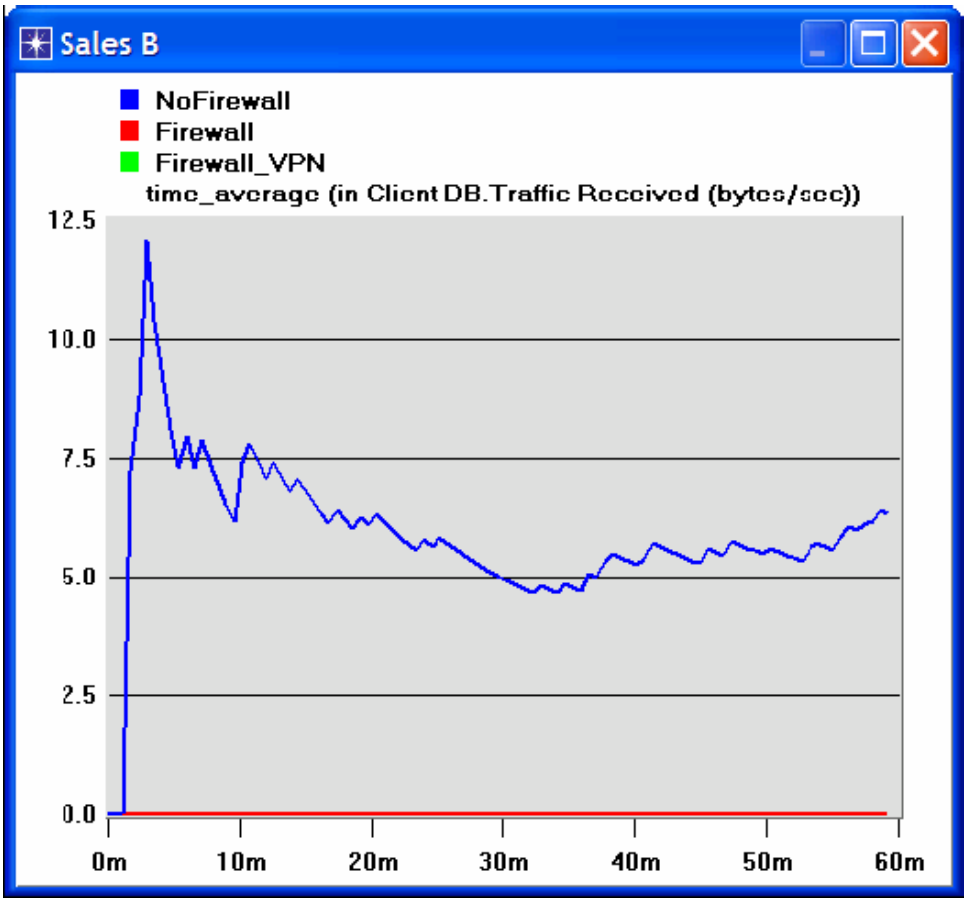
1. Виберіть ***Compare Results*** з меню ***Results***.
2. Розкрийте підпункти ***Sales A*** → Розкрийте підпункти ***Client DB***→Виберіть статистику ***Traffic Received***.
3. Змініть меню, що випадає в нижній центральній частині форми ***Compare Results*** з ***As Is*** на ***time_average***, як показано.



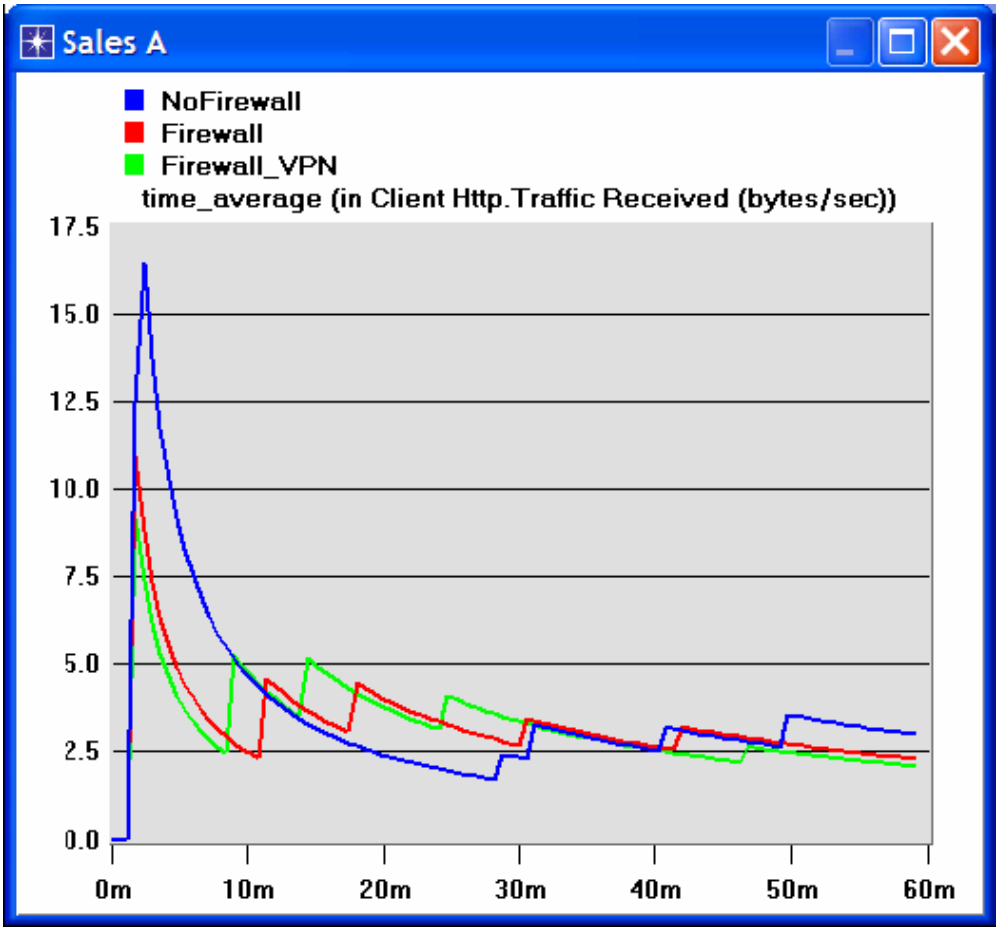
4. Натисніть ***Show*** і результуючий графік повинен нагадувати нижченаведений:

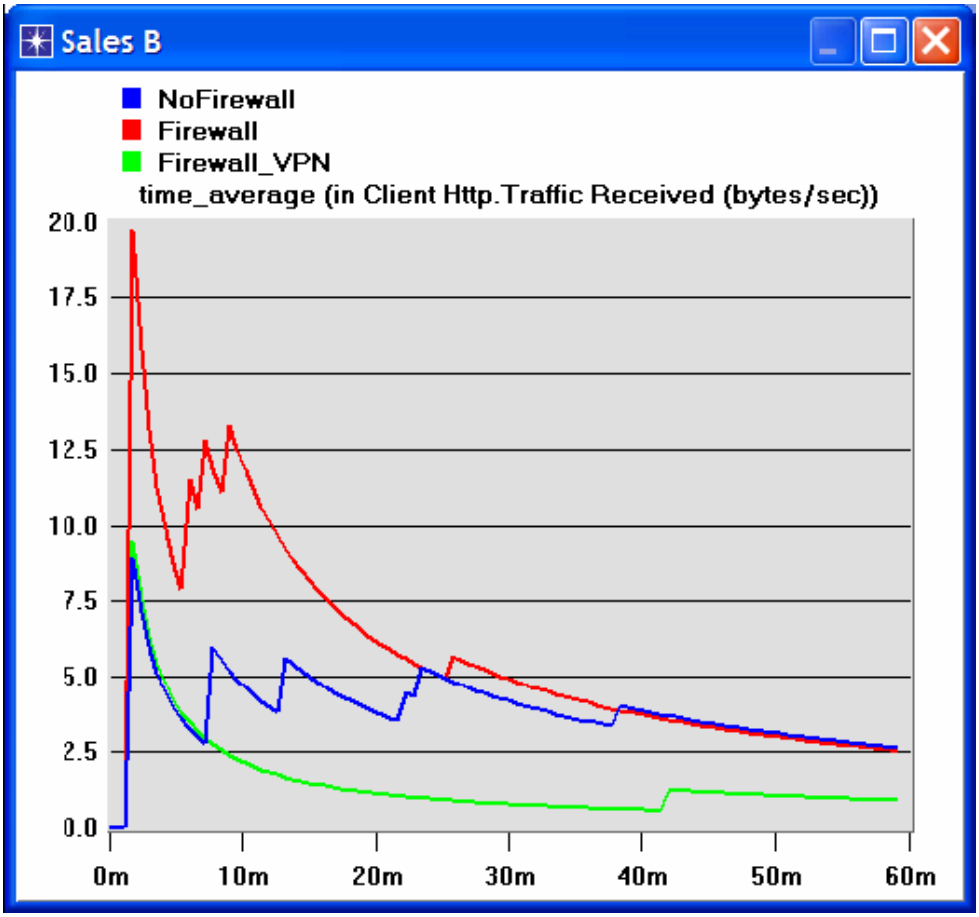


5. Створіть аналогічний попередньому графік для ***Sales B***:



6. Створіть ще два аналогічних графіка, що відображають трафік, отриманий ***Client Http*** для ***Sales A*** і ***Sales B***.


Sales A
NoFirewall
Firewall
Firewall_VPN
time_average (in Client Http.Traffic Received (bytes/sec))
17.5
15.0
12.5
10.0
7.5
5.0
2.5
0.0
0m
10m
20m
30m
40m
50m
60m



Зауваження: Результати можуть змінюватись, залежно від розташування вузлів.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Грунтуючись на отриманих графіках, поясніть вплив брандмауера, як і налаштованого VPN, на пов'язаний з базою даних трафік, запитаний Sales A і Sales B.
2. Порівняйте графіки, що ілюструють отриманий http-трафік, з трафіком, який ілюструє отриманий трафік від бази даних.
3. Згенеруйте і проаналізуйте графіки, що ілюструють вплив брандмауера і VPN на затримку завантаження http-сторінок і запитів до бази даних.

4. У сценарії ***Firewall_VPN*** ми сконфігурували вузол VPN так, що трафік від Sales A не блокувався брандмауером. Створіть копію сценарію ***Firewall_VPN*** і назвіть його ***Q4_DB_Web***. У цьому сценарії ми повинні налаштувати мережу так, що:

   a. Бази даних на сервері доступні тільки користувачам з ***Sales A***.

   b. Веб-сайти на сервері доступні тільки користувачам з ***Sales B***.

Включіть в ваш звіт схеми для нової конфігурації мережі, в тому числі і будь-які зміни, які ви внесли в атрибути існуючих або доданих вузлів. Згенеруйте необхідні графіки для ілюстрації того, як нова мережа задовольняє вищезазначеним вимогам.

ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ

Підготуйте звіт, виконаний за рекомендаціями до лабораторної роботи. Звіт повинен включати відповіді на вищезгадані питання, а також графіки, які Ви отримали при моделюванні сценаріїв. Проаналізуйте результати, які Ви отримали і порівняйте ці результати з очікуваними. Включіть до звіту будь-які аномалії або незрозумілу з Вашої точки зору поведінку.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРА

- Вплив швидкості Інтернет-з'єднання на продуктивність додатків: From the Protocols menu, select Methodologies ⇒ Capacity Planning.

- Virtual Private Networks: IETF RFC number 2685 (www.ietf.org / rfc.html).

Лабораторна робота №11

ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ МАСШТАБУ МАЛОГО МІСТА

Мета роботи: Отримати навички вибору мережної архітектури, методу доступу, топології, типу кабельної системи, операційних систем, додатків і протоколів для побудови комп'ютерної мережі масштабу малого міста. Розрахувати кількість необхідного мережевого обладнання, а також отримати навички формування підмереж з урахуванням особливостей географічного розташування локальної мережі.

ЗАВДАННЯ НА РОБОТУ

Побудувати макет локальної комп'ютерної мережі масштабу малого міста, самостійно обравши при цьому мережеве обладнання та компоненти. Для цього необхідно:

1. В залежності від географічного розташування обгрунтувати вибір мережевої архітектури для комп'ютерної мережі, метод доступу, топологію, тип кабельної системи, додатків, протоколів і т.д.
2. Вибрати мережеве обладнання - кількість серверів, комутаторів, маршрутизаторів тощо для заданої за варіантом кількості вузлів мережі.
3. Вручну розрахувати і встановити IP-адреси для всіх вузлів мережі і вибрати необхідний протокол маршрутизації.
4. Зібрати мережу в програмі моделювання OpNET.
5. Додати додаткові мережеві компоненти (якщо такі існують за варіантом).
6. Поставити необхідний трафік за варіантом.
7. Промоделювати і проаналізувати результати моделювання.

Дана лабораторна робота виконується індивідуально кожним студентом, номер варіанта визначається порядковим номером за списком групи, який знаходиться у викладача. Для порядкових номерів 21 і більше, номер варіанту розраховується по модулю 20 щодо порядкового номера за списком, наприклад: 25 mod 20 = 5.

ЗВІТ ДО ЛАБОРАТОРНОЇ РОБОТИ

Титульна сторінка протоколу обов'язково повинна містити прізвище, ім'я і варіант (порядковий номер за списком групи). У протоколі необхідно відобразити:

• ескіз мережі з зазначенням IP-адреси кожного з вузлів;

• результати моделювання (графіки), що відображають працездатність мережі;

• коротко описати причини вибору мережевого обладнання та архітектури комп'ютерної мережі;

• зробити висновки по роботі з урахуванням обраного обладнання та отриманих результатів.

ВАРІАНТИ

Загальне зауваження:

Якщо вказаний параметр «загальний» - це означає, що інформацію з даного вузла повинні отримувати всі абоненти міської мережі. Якщо вказаний параметр «приватний» - це означає, що інформацію з даного вузла повинні отримувати абоненти тільки в межах підмережі відділу.

Варіант № 1

Міська мережа 10×10 км (відстань між відділами не менше 2 км.), 3 відділи, 10 робочих станцій на відділ.

Параметри трафіку / сервера:

1 загальний Web-сервер (HTTP), 1 загальний E-mail сервер, 1 загальний FTP сервер.

Варіант № 2

Міська мережа 20×20 км (відстань між відділами не менше 4 км.), 4 відділу, 5 робочих станцій на відділ.

Параметри трафіку / сервера:

1* загальний сервер відеоконференцій, 2 приватних FTP сервера, 1 загальний E-mail сервер.

(**Високий пріоритет передачі даних, без затримок.*)

Варіант № 3

Міська мережа 5×5 км (відстань між відділами не менше 3 км.), 2 відділи, 7 робочих станцій на відділ. Віртуальна мережа (***VPN***) об'єднує машини відділів в єдину під мережу.

Параметри трафіку / сервера:

1 загальний DataBase сервер, 5 загальний E-mail серверів. Захищений вихід в інтернет.

Варіант № 4

Міська мережа 3×3 км (відстань між відділами не менше 300 м.), 3 відділи, 40 робочих станцій на відділ *

Параметри трафіку / сервера:

1 загальний FTP сервер (Heavy), 2 приватних E-mail сервера в різних відділах

** Примітка: організувати мережу без колізій і втрат*

Варіант № 5

Міська мережа 10х10 км (відстань між відділами не менше 200 м.), 10 відділів, 3 робочих станцій на відділ. У кожному з відділів стоїть приватний принтер

Параметри трафіку / сервера:

1 загальний DataBase сервер, 1 загальний E-mail сервер, 2 загальних FTP сервера

Варіант № 6

Міська мережа 2х2 км (відстань між відділами не менше 80 м.), 20 відділів, 7 робочих станцій на відділ

Параметри трафіку / сервера:

1 DataBase сервер, вхідний трафік - загальний, вихідні – приватний, 5 загальний E-mail серверів, 1 загальний FTP сервер Захищений вихід в інтернет

Варіант № 7

Міська мережа 50х50 км (відстань між відділами не менше 20 км.), 5 відділів, 20 робочих станцій на відділ в одному відділі для всіх робочих станцій організувати бездротову мережу.

Параметри трафіку / сервера:

2 загальний DataBase сервера (у різних відділах), 1 загальний E-mail сервер

Варіант № 8

Міська мережа 10х10 км (відстань між відділами не менше 1км.), 3 відділи, 20 робочих станцій на відділ

Параметри трафіку / сервера:

1 загальний сервер відео конференцій, 1 приватний сервер Voice, 3 загальних Web-сервера в кожному з відділів

Варіант № 9

Міська мережа 50х50 км (відстань між відділами не менше 30 км.), 3 відділи, 5 робочих станцій на відділ

Параметри трафіку / сервера:

3 приватних шлюза VoIP телефонії, 1 загальний FTP сервер. Захищений вихід в інтернет

Варіант № 10

Міська мережа 10х10 км (відстань між відділами не менше 1 км.), 6 відділів, 5 робочих станцій на відділ

Параметри трафіку / сервера:

У кожному з відділів забезпечити свої приватні сервера: HTTP, Voice, Video, FTP, E-mail, Database, 1 загальний захищений вихід в інтернет

Варіант № 11

Міська мережа 15х15 км (відстань між відділами не менше 1 км.), 10 відділів, 10 робочих станцій на відділ в одному відділі для всіх робочих станцій організувати бездротову мережу.

Параметри трафіку / сервера:

1 загальний Web-сервер (HTTP), 1 загальний FTP сервер, 1 загальний захищений вихід в інтернет

Варіант № 12

Міська мережа 2х2 км (відстань між відділами не менше 130м.), 4 відділа, 5 робочих станцій на відділ

Параметри трафіку / сервера:

1 загальний E-mail сервер, 2 загальних сервера Database

Організувати мережу, використовуючи по можливості найпростішого (дешевшого) обладнання

Варіант № 13

Міська мережа 20х20 км (відстань між відділами не менше 2 км.), 5 відділів, 10 робочих станцій на відділ

Параметри трафіку / сервера:

1 загальний DataBase сервер, 1 загальний FTP сервер (Heavy), 3 приватних шлюзу VoIP телефонії. Захищений вихід в інтернет

Варіант № 14

Міська мережа 5х5 км (відстань між відділами не менше 700 м.), 3 відділи, 10 робочих станцій на відділ. Віртуальна мережа (VPN) об'єднує машини відділів в єдину підмережу

Параметри трафіку / сервера:

1 загальний FTP сервер (Heavy), 2 загальних E-mail сервера

Варіант № 15

Міська мережа 10х10 км (відстань між відділами не менше 50 м.), 40 відділів, 2 робочих станцій на відділ

Параметри трафіку / сервера:

1 загальний DataBase сервер, 1 загальний E-mail сервер, 3 приватних FTP сервера. Захищений вихід в інтернет

Варіант № 16

Міська мережа 6х6 км (відстань між відділами не менше 750 м.), 6 відділів, 25 робочих станцій на відділ

Параметри трафіку / сервера:

10 загальних DataBase серверів, 1 загальний E-mail сервер, 2 приватних FTP сервера

Варіант № 17

Міська мережа 20х20 км (відстань між відділами не менше 1 км.), 9 відділів, 8 робочих станцій на відділ, в 2-ох відділах для всіх робочих станцій організувати бездротову мережу.

Параметри трафіку / сервера:

2 загальний DataBase сервера (у різних відділах), 1 приватний FTP сервер, 1 загальний E-mail сервер

Варіант № 18

Міська мережа 15х15 км (відстань між відділами не менше 3 км.), 5 відділів, 20 робочих станцій на відділ

Параметри трафіку / сервера:

1 загальний сервер відео конференцій, 1 приватний шлюз VoIP телефонії, 5 загальних Web-серверів в кожному з відділів

Варіант № 19

Міська мережа 10х10 км (відстань між відділами не менше 200 м.), 8 відділів, 5 робочих станцій на відділ.

Параметри трафіку / сервера:

3 приватних шлюза VoIP телефонії. 1 загальний FTP сервер. Захищений вихід в інтернет

Варіант № 20

Міська мережа 40х40 км (відстань між відділами не менше 10 км.), 3 відділи 15 робочих станцій на відділ .

Параметри трафіку / сервера:

У кожному з відділів забезпечити свої приватні сервера: HTTP, E-mail, Voice. 1 загальний FTP сервер. Захищений вихід в інтернет.