МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

Квасниця Роман Васильович

Мультисервісна комп'ютерна мережа гуртожитку ТНЕУ/ Multi-computer network dormitory of TNEU

Спеціальність: 123 – Комп'ютерна інженерія
Освітньо-професійна програма – Комп'ютерна інженерія

Випускна кваліфікаційна робота

Виконав: студент групи КСМ-43/2
Квасниця Роман Васильович
_____

Науковий керівник:
Вовкодав О.В.
_____

Випускну кваліфікаційну роботу
допущено до захисту:

"___" _____ 20___ р.

Завідувач кафедри
О. М. Березький

ТЕРНОПІЛЬ - 2019

РЕЗЮМЕ

Дипломний проект містить 100 сторінок пояснюючої записки, 27 рисунків, 8 таблиць, 5 додатоків. Обсяг графічного матеріалу 2 аркуші формату А3.

Метою дипломного проекту є розроблення проекту безпровідної мережі навчального закладу з роумінгом на прикладі навчального корпусу №3 ТНЕУ. Структурована кабельна система відповідає прийнятим міжнародним стандартам (ANSI/TIA/EIA-568-A і ISO/IEC11801).

Проектом передбачається забезпечення навчального корпусу не просто безпровідною мережею на основі Wi-Fi, а мережею, в якій буде повноцінно працювати роумінг. Було проаналізовано вже існуючу безпровідну мережу корпусу, виявлено її недоліки (недостатня кількість Wi-Fi точок доступу) та запропоновано шляхи вирішення проблеми. В роботі досліджені основні, та найбільш популярні засоби діагностика і управління Wi-Fi мереж, а саме – Orion NPM SolarWinds та AP Maneger. AP Maneger використовують для управління безпровідною мережею в ТНЕУ. Також нами описана система моніторингу, як засобу виявлення помилок в роботі Wi-Fi в режимі онлайн на прикладі ПЗ Nagios та Zabbix.

У проекті надані необхідні розрахунки й креслення, специфікація устаткування й матеріалів, необхідних для побудови безпровідної мережі з роумінгом. Крім того подані вимоги по монтажу, рекомендації з адміністрування, обслуговування й експлуатації системи.

Ключові слова: СТРУКТУРОВАНА КАБЕЛЬНА СИСТЕМА, NAGIOS, ZABBIX

RESUME

The diploma project contains 100 pages of explanatory note, 27 figures, 8 tables, 5 appendices. Volume of graphic material 2 sheets of A3 format.

The purpose of the diploma project is to develop a project of a wireless network of an educational institution with roaming on the example of the educational building №3 TNEU. The structured cabling system complies with accepted international standards (ANSI / TIA / EIA-568-A and ISO / IEC11801).

The project envisages providing the educational building not just with a wireless network based on Wi-Fi, but with a network in which roaming will fully work. The existing wireless network of the building was analyzed, its shortcomings were revealed (insufficient number of Wi-Fi access points) and ways to solve the problem were suggested. The main and most popular means of diagnostics and management of Wi-Fi networks, namely - Orion NPM SolarWinds and AP Maneger are investigated in the work. AP Maneger is used to control the wireless network in TNEU. We also describe the monitoring system as a means of detecting errors in the operation of Wi-Fi online on the example of Nagios and Zabbix software.

The project provides the necessary calculations and drawings, specifications of equipment and materials needed to build a wireless network with roaming. In addition, there are requirements for installation, recommendations for administration, maintenance and operation of the system.

Keywords: STRUCTURED CABLE SYSTEM, NAGIOS, ZABBIX

ЗМІСТ

					ДП.КСМ.07417/12.00.00.000.*ПЗ*		
Зм.	*Арк.*	*№ докум.*	*Підпис*	*Дат*			
Розробив		*Вітюк А.Ю.*			*Безпровідна мережа навчального закладу з роумінгом*.	*Літ.*	*Арк.* 8 / 85
Перевірив		*Романець І.Є.*				*н*	
Консульт.		*Сапожник Г.В.*				*ТНЕУ.ФКІТ.КСМз*-41	
Н.Контр.		*Карачка А.Ф.*					
Затверд.		*Саченко А.О.*					

ВСТУП

З бурхливим розвитком телекомунікації у сучасному світі суспільство неухильно йде до ускладнення взаємозв'язку між різними ланками виробництва, збільшення інформаційних потоків у технічній, науковій, політичній, культурній, побутовій та інших сферах суспільної діяльності. Сьогодні, очевидно, що жоден процес у житті сучасного суспільства не може відбуватися без обміну інформації, для своєчасної передачі якої використовуються різні засоби й системи зв'язку.

У цей час розвиток мультисервісних мереж відбувається в напрямку росту ринку мультисервісних послуг, впровадження нових телекомунікаційних і інформаційних технологій, їх конвергенції.

Широкосмугове підключення до Інтернету стало однією з найбільш успішних мультисервісних послуг не дуже давно, але всього за кілька років кількість користувачів виросла до 200 млн., більшість із них поки обмежуються доступом в Інтернет з комп'ютера або ноутбука.

Сучасний розвиток комп’ютерних мереж характеризується їхньою конвергенцією. Раніше ізольовані локальні мережі об’єднувались за допомогою глобальних мереж. Актуальною стає задача побудови універсальних мереж, що здібні однаково ефективно надавати послуги різних типів.

Одне з найважливіших напрямків цифрування - модернізація мереж зв'язку загального користування на основі концепції NGN (Next Generation Network) - мереж зв'язку наступного покоління. Перспективна архітектура мереж нового покоління (NGN) припускає створення мультисервісної мережі з винесенням функціональності послуг в граничні вузли мережі, створення спеціальної підсистеми керування послугами у вигляді окремої мережевої підсистеми, а також розширення номенклатури інтерфейсів для підключення устаткування постачальників послуг. Мультисервісні мережі можуть бути

створені як новий клас мереж зі забезпеченням можливості взаємодії з існуючими мережами.

Сутність мережі нового покоління полягає у переході від багатоплатформності до простої та ефективної мережі, розробленої спеціально для того, щоб надавати всі види послуг. З погляду технології перехід від традиційної мережі до мережі нового покоління є переходом від окремого існування мережі з комутацією каналів і мережі з комутацією пакетів до мультисервісних мереж, що здібні функціонувати як в першому, так і в другому режимах комутації. У результаті можна одержати мережі, що пристосовані до всіх видів послуг. Цими мережами буде набагато легше керувати, і водночас контроль за якістю послуг великою мірою перейде до самих клієнтів.

Мережа зв’язку наступного покоління (NGN) - концепція побудови мереж зв'язку, що забезпечують надання необмеженого набору послуг з гнучкими можливостями по їх управлінню і створенню нових послуг за рахунок уніфікації мережевих рішень, яка припускає реалізацію універсальної транспортної мережі з розподіленою комутацією, винесення функцій надання послуг у кінцеві мережеві вузли і інтеграцію з традиційними мережами зв'язку. Під терміном "мережу наступного покоління" (NGN) розуміють концепцію побудови мереж зв'язку, які забезпечують надання необмеженого набору послуг з гнучкими можливостями щодо їх управління, персоналізації та створенню нових послуг за рахунок уніфікації мережевих рішень. До складу NGN входить універсальна транспортна платформа з розподіленою комутацією.

Мультисервісна мережа - мережа зв'язку, яка побудована відповідно з концепцією мережі зв'язку наступного покоління, що забезпечує надання необмеженого набору послуг.

На сьогоднішній день розвиток інфокомунікаційних послуг здійснюється, в основному, в рамках комп'ютерної мережі Інтернет, доступ до послуг якої виконується через традиційні мережі зв'язку. Проте у ряді випадків послуги Інтернет, зважаючи на обмежені можливості її транспортної інфраструктури не

відповідають сучасним вимогам, що пред'являються до послуг інформаційного суспільства. У зв'язку з цим розвиток інфокомунікаційних послуг вимагає рішення задач ефективного управлінні інформаційними ресурсами з одночасним розширенням функціональності мереж зв'язку. У свою чергу, це стимулює процес інтеграції Інтернет і мереж зв'язку.

Мультисервісні мережі наступного покоління мають переваги над мережами традиційної архітектури, оскільки можуть використати єдину транспортну інфраструктуру для передачі всіх типів трафіку і ефективно її використовувати завдяки статистичному мультиплексуванню. Інтеграція трафіку різнорідних даних і мови дозволяє добитися якісного підвищення ефективності інформаційної підтримки управління підприємством, при цьому використовування інтегрованого транспортного середовища дозволяє понизити витрати на створення і експлуатацію мережі. Мультисервісна мережа використовує єдиний канал для передачі даних різних типів, дозволяє зменшити різноманітність типів устаткування, застосовувати єдині стандарти, технології і централізований управляти комунікаційним середовищем.

Метою даної дипломної роботи є розробка та проектування мультисервісної мережі, використовуючи на рівні доступу різних технологій, надання по одному каналу послуг високошвидкісного доступу до мережі Internet та IP телефонії, а також системи відеоспостереження та доступу до безпровідної мережі. Також метою даної роботи є поглиблене дослідження безпровідних і провідних технологій у мультисервісних мережах, для використання їх на рівні доступу.

Для забезпечення стабільного функціонування мережі мережа повинна мати надійні кабельні з'єднання, правильну топологію, грамотно обрані місця розташування устаткування. У даній роботі пророблені всі аспекти для створення якісної, сучасної мультисервісної мережі в місці, які в даний момент мають практичну реалізацію та будуть використовуватись в ННЦІТ ТНЕУ.

1 ОСНОВНІ ПАРАМИТРИ І ХАРАКТЕРИСТИКИ МУЛЬТИСЕРВІСНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Сучасний розвиток комп'ютерних мереж характеризується їхньою конвергенцією. Раніше ізольовані локальні мережі об'єднуються за допомогою глобальних мереж. Актуальною стає задача побудови універсальних мереж, що здібні однаково ефективно надавати послуги різних типів. Перспективна архітектура мереж нового покоління (NGN) припускає створення мультисервісної мережі з винесенням функціональності послуг в граничні вузли мережі, створення спеціальної підсистеми керування послугами у вигляді окремої мережевої підсистеми, а також розширення номенклатури інтерфейсів для підключення устаткування постачальників послуг. Сутність мережі нового покоління полягає у переході від багатоплатформності до простої та ефективної мережі, розробленої спеціально для того, щоб надавати всі види послуг. З погляду технології перехід від традиційної мережі до мережі нового покоління є переходом від окремого існування мережі з комутацією каналів і мережі з комутацією пакетів до мультисервісних мереж, що здібні функціонувати як в першому, так і в другому режимах комутації. У результаті можна одержати мережі, що пристосовані до всіх видів послуг. Цими мережами буде набагато легше керувати, і водночас контроль за якістю послуг великою мірою перейде до самих клієнтів.

Метою даної роботи є розгляд властивостей мультисервісної мережі, її структури і архітектури керування. У роботі вирішується задача аналізу стану переходу від сучасних комп'ютерних мереж до мереж нового покоління. В дослідженні застосуються наступні терміни:

Мережа зв'язку наступного покоління (NGN) - концепція побудови мереж зв'язку, що забезпечують надання необмеженого набору послуг з гнучкими можливостями по їх управлінню і створенню нових послуг за рахунок уніфікації мережевих рішень, яка припускає реалізацію універсальної

транспортної мережі з розподіленою комутацією, винесення функцій надання послуг у кінцеві мережеві вузли і інтеграцію з традиційними мережами зв'язку.

Мультисервісна мережа - мережа зв'язку, яка побудована відповідно з концепцією мережі зв'язку наступного покоління, що забезпечує надання необмеженого набору послуг.

Мультипротокольна мережа – транспортна мережа зв'язку, що входить до складу мультисервісної мережі та забезпечує перенесення різних видів інформації з використанням різних протоколів передачі.

Мережа доступу (Access Network – AN) – мережа зв'язку, що забезпечує підключення термінальних пристроїв користувача до кінцевого вузла мультипротокольної мережі.

На сьогоднішній день розвиток інфокомунікаційних послуг здійснюється, в основному, в рамках комп'ютерної мережі Інтернет, доступ до послуг якої виконується через традиційні мережі зв'язку. Проте у ряді випадків послуги Інтернет, зважаючи на обмежені можливості її транспортної інфраструктури не відповідають сучасним вимогам, що пред'являються до послуг інформаційного суспільства. У зв'язку з цим розвиток інфокомунікаційних послуг вимагає рішення задач ефективного управлінні інформаційними ресурсами з одночасним розширенням функціональності мереж зв'язку. У свою чергу, це стимулює процес інтеграції Інтернет і мереж зв'язку.

1.1 Основні концепція мультисервісних комп’ютерних мереж

До основних технологічних особливостей, що відрізняють інфокомунікаційні послуги від послуг традиційних мереж зв'язку, можна віднести наступні:

- інфокомунікаційні послуги виявляються на верхніх рівнях моделі OSI, тоді як послуги зв'язку надаються на третьому, мережевому рівні;

- більшість інфокомунікаційних послуг припускає наявність клієнтської та серверної частин; клієнтська частина реалізується в устаткуванні користувача, а серверна – на спеціальному виділеному вузлі мережі, що називається вузлом служб;

- інфокомунікаційні послуги, як правило, припускають передачу мультимедійної інформації, яка характеризується високими швидкостями передачі і несиметричністю вхідного і вихідного інформаційних потоків; - для надання інфокомунікаційних послуг часто необхідні складні багатоточкові конфігурації з'єднань;

- для інфокомунікаційних послуг характерна різноманітність прикладних протоколів і можливостей по керуванню послугами з боку користувача;

- для ідентифікації абонентів інфокомунікаційних послуг може використовуватися додаткова адресація в рамках даної інфокомунікаційної послуги.

Більшість інфокомунікаційних послуг є „додатками", тобто їхня функціональність розподілена між устаткуванням постачальника послуги і кінцевим устаткуванням користувача. Як наслідок, функції кінцевого устаткування також повинні бути віднесені до складу інфокомунікаційної послуги, що необхідно враховувати при їх регламентації.

До інфокомунікаційних послуг пред'являються наступні вимоги:

- мобільність послуг;

- можливість гнучкого і швидкого створення нових послуг;

- гарантована якість послуг.

Великий вплив на вимоги до інфокомунікаційних послуг надає процес конвергенції, що призводить до того, що інфокомунікаційні послуги стають доступними користувачам незалежно від способів доступу. Беручи до уваги

розглянуті особливості інфокомунікаційних послуг, можуть бути визначені наступні вимоги до перспективних мереж зв'язку:

- „мультісервісність”, під якою розуміється незалежність технологій надання послуг від транспортних технологій;

- „широкосмуговість”, під якою розуміється можливість гнучкої і динамічної зміни швидкості передачі інформації в широкому діапазоні у залежності від поточних потреб користувача;

- „мультімедійність”, під якою розуміється здатність мережі передавати багатокомпонентну інформацію (мова, дані відео, аудіо) з необхідною синхронізацією цих компонент у реальному часі та використовуванням складних конфігурацій з'єднань;

- „інтелектуальність”, під якою розуміється можливість керування послугою, викликом і з'єднанням з боку користувача або постачальника послуг;
- „інваріантність доступу”, під якою розуміється можливість організації доступу до послуг незалежно від використовуваної технології;

- „багатооператорність”, під якою розуміється можливість участі декількох операторів в процесі надання послуги та розділення їхньої відповідальності відповідно до області діяльності.

Існуючі мережі зв'язку загального користування з комутацією каналів і комутацією пакетів у даний час не відповідають перерахованим вище вимогам. Обмежені можливості традиційних мереж є стримуючим чинником на шляху впровадження нових інфокомунікаційних послуг. Нарощування об'ємів надаються інфокомунікаційних послуг може негативно позначитися на показниках якості обслуговування викликів базових послуг існуючих мереж зв'язку. Все це вимушує враховувати наявність інфокомунікаційних послуг при плануванні способів розвитку традиційних мереж зв'язку в напрямі створення мультисервісних мереж.

NGN характеризується такими фундаментальними аспектами [1]:

– пакетна передача;

– розділення функцій постачальника послуг та оператора телекомунікацій;

– підтримка широкого спектру послуг, прикладень і технологій: зв’язок у реальному часі, потокова передача, зв’язок не у реальному часі, мультимедіа-послуги;

– широкосмуговий зв’язок з потрібною наскрізною якістю і прозорими з’єднаннями;

– взаємодія з існуючими мережами через відкриті інтерфейси;

– рухливість абонента;

– необмежений доступ користувача до послуг різних провайдерів;

– єдині характеристики для однієї і тієї ж послуги, що надається різними провайдерами;

– конвергенція фіксованого і рухомого зв’язку.

Базовим принципом концепції NGN є відділення друг від друга функцій перенесення і комутації, функцій керування викликом і функцій керування послугами.

Функціональна модель мереж NGN, що представлена на **рисунку 1**, має три рівня:

– транспортний рівень;

– рівень керування комутацією і передачею інформації;

– рівень керування послугами.

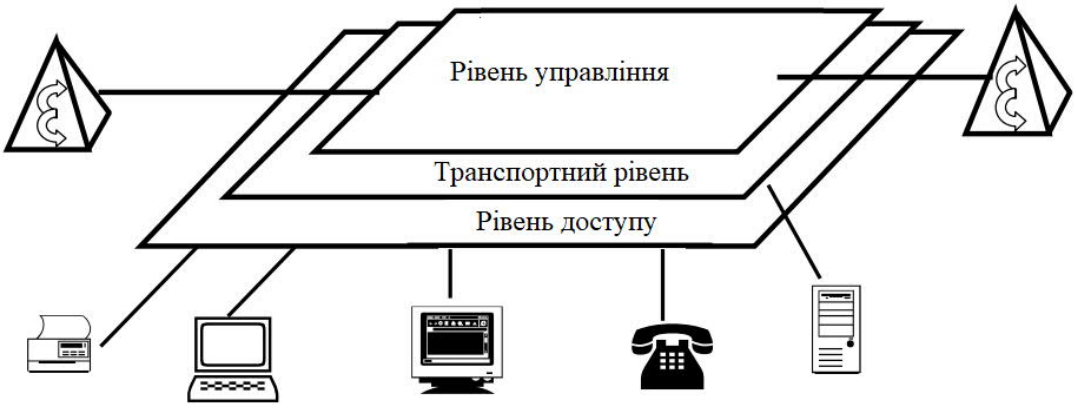

Рисунок 1.1- Функціональна модель мереж NGN

Задачею транспортного рівня є комутація і прозора передача інформації користувача. Задачею рівня керування комутацією і передачею є обробка інформації сигналізації, маршрутизація викликів і керування потоками. Рівень керування послугами має функції керування логікою послуг і додатків і є розподіленим обчислювальним середовищем.

Він забезпечує:

- надання інфокомунікаційних послуг;
- керування послугами;
- створення і впровадження нових послуг;
- взаємодію різних послуг.

Даний рівень дозволяє реалізувати специфіку послуг і застосовувати одну і ту ж програму логіки послуги незалежно від типу транспортної мережі (IP, ATM, FR і т. ін.) і способу доступу. Наявність цього рівня дозволяє також додавати до мережі будь-які нові послуги без втручання у функціонування інших рівнів.

Рівень керування послугами може включати множину незалежних підсистем („мереж послуг”), що базуються на різних технологіях, що мають своїх абонентів і використовують свої, внутрішні системи адресації.

1.2 Особливості архітектури мультисервісних комп’ютерних мереж.

З розвитком інфокомунікаційних послуг стали досить популярними обговорення різних варіантів архітектури NGN, які в рамках єдиної інфраструктури поєднують мережі ТфЗК, мобільного зв’язку, ресурси мережі Інтернет тощо. Відмінною рисою моделі NGN, запропонованої сектором стандартизації електрозв’язку ITU-T, є функціональний розподіл на два рівні: послуг і транспортний рисунок 1.2. Рівень послуг реалізує прикладні функції,

пов’язані із вимогами щодо послуг, наприклад, з організації передачі мови, відеозображення або їхні комбінації. Транспортний рівень забезпечує виконання функції доставки інформації будь-якого типу між будь-якими двома географічно рознесеними терміналами. У загальному випадку на транспортному рівні може використовуватися довільна технологія комутації пакетів. Однак ITU-T вважає, що технологія IP є кращою для організації транспорту в NGN, оскільки має найбільшу повноту для реалізації завдань мереж наступного покоління.

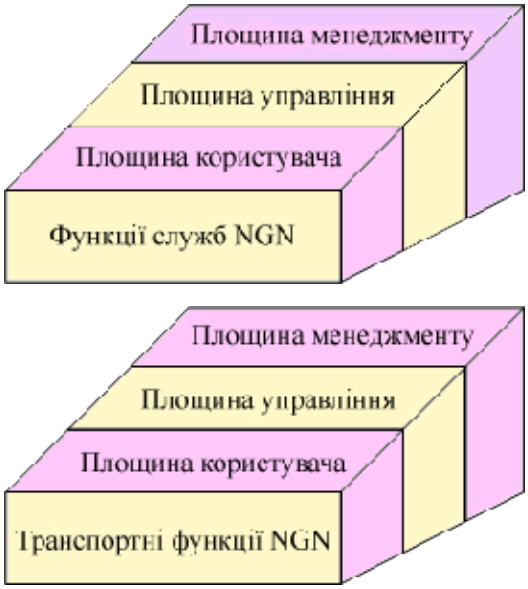

Рис. 1.2 - Розподіл функцій транспорту й служб в архітектурі NGN

Незважаючи на рекомендації ITU-T, на практиці нині найбільшого поширення набула чотирирівнева архітектура NGN, у якій рівень послуг і транспортний рівень в свою чергу зазнали подальшої декомпозиції на такі рівні (рис. 1.3):

- рівень управління послугами (четвертий рівень);
- рівень мережного контролю й управління (третій рівень);
- транспортний рівень (другий рівень);
- рівень доступу (перший рівень);

– термінальне обладнання (нульовий рівень).

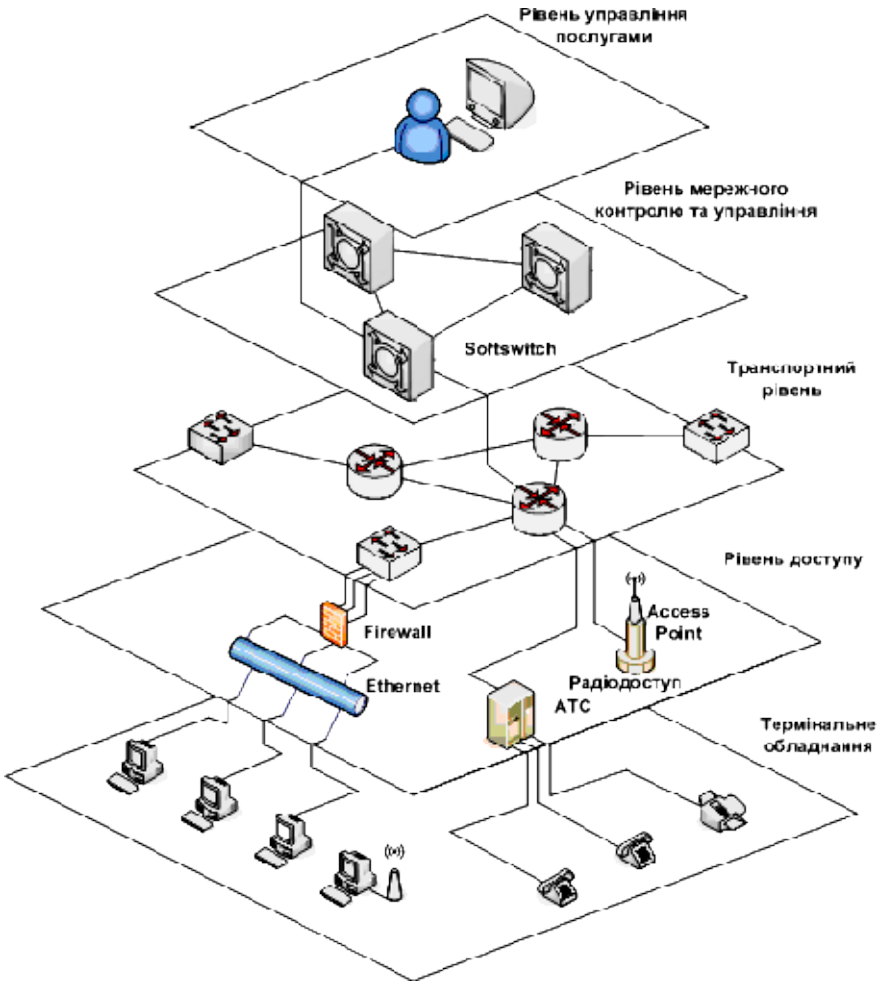

Рисунок 1.3. - Чотирирівнева архітектура мережі наступного покоління

Рівень управління послугами виконує функції управління логікою послуг і аплікацій й являє собою розподілене обчислювальне середовище, що забезпечує:

- надання (підтримку) інфокомунікаційних послуг;
- безпосередньо управління послугами;
- створення й упровадження нових послуг;
- взаємодію різних послуг.

Цей рівень має реалізувати специфіку послуг і застосовувати одну й ту саму програму логіки послуг незалежно від типу транспортної мережі й способу доступу. Наявність цього рівня забезпечить також можливість

введення на транспортній мережі нових послуг без втручання у функціонування інших рівнів.

Традиційна модель NGN (див. рис. 2.3.2) передбачає, що платформи для надання послуг підключаються до мережі зв'язку за допомогою стандартних інтерфейсів ЗКС № 7, SIP, Parlay, H.323. Однак при впровадженні послуг NGS різні рівні функціональної моделі можуть зливатися (рис. 1.3).

Рисунок 1.4 - Функціональна модель мережі NGN, адаптована для надання послуг NGS

Операторам зв'язку потрібні механізми, що забезпечують можливість швидко й гнучко розгортати, а також змінювати послуги залежно від індивідуальних потреб користувачів. Такі механізми передбачені відкритою сервісною архітектурою OSA (Open Services Access) — основною концепцією майбутнього розвитку мереж зв'язку щодо впровадження й надання нових додаткових послуг. При створенні систем на основі OSA мають бути такі ключові елементи:

- відкрите середовище для створення послуг;
- відкрита платформа управління послугами.

Рівень управління послугами відповідає за надання кінцевому користувачеві інформаційних послуг, і від того, наскільки ці послуги зацікавлять його, залежить подальший розвиток мережі. Сервери, що забезпечують надання послуг, можуть перебувати як усередині, так і за межами самої мережі (веб-сервери, сервери, що належать ASP-провайдерам). Важливою складовою рівня управління послугами також є інформаційні центри або

центри управління послугами (data centers, services control point) — це власні інформаційні ресурси мережі, на основі яких здійснюється обслуговування користувачів. У таких центрах може зберігатися інформація двох типів:

– інформація користувача, тобто ті дані, які безпосередньо цікавлять користувачів мережі;

– допоміжна службова інформація, яка дозволяє надавати користувачам додаткові послуги.

Прикладом інформаційних ресурсів першого типу можуть служити веб-портали, на яких розташована різноманітна довідкова інформація й новини, інформація електронних магазинів тощо. Раніше в телефонних мережах роль таких центрів відігравали служби екстреного виклику (наприклад, міліції, швидкої допомоги) і довідкові служби різних організацій і підприємств — вокзалів, аеропортів, магазинів тощо. У телевізійних мережах такими центрами були телестудії, які поставляли «живу» картинку або ж відтворювали раніше записані сюжети або фільми.

До ресурсів другого типу належать, наприклад, різні системи автентифікації й авторизації користувачів, за допомогою яких організація, що володіє мережею, перевіряє права користувачів на одержання тих або інших послуг; системи білінгу, які в комерційних мережах підраховують плату за надані послуги; бази даних облікової інформації користувачів, які зберігають імена й паролі, а також переліки послуг, на які підписаний кожний користувач.

Концепція NGN багато в чому спирається на технічні рішення, які вже розроблені міжнародними організаціями зі стандартизації. Так, взаємодію серверів у процесі надання послуг передбачається здійснювати на базі протоколів, специфікованих IETF (MEGACO), ETSI (TIPHON), Форумом 3GPP2 тощо. Для управління послугами використовуватимуться протоколи H.323, SIP і підходи, застосовувані в інтелектуальних мережах зв’язку.

Рівень мережного контролю й управління має забезпечувати обробку інформації сигналізації, маршрутизації викликів і управління потоками. Цей

рівень підтримує логіку управління, яка необхідна для обробки й маршрутизації трафіка. Функція встановлення з'єднання реалізується на рівні елементів базової мережі під зовнішнім управлінням обладнання програмного комутатора (Softswitch). Виключенням є АТС із функціями контролера шлюзів (Media Gateway Controller, MGC), які самі виконують комутацію на рівні елемента транспортної мережі. У разі використання на мережі декількох Softswitch вони взаємодіють за допомогою відповідних протоколів (як правило, сімейство SIP-T) і забезпечують спільне управління встановленням з'єднання.

Softswitch має здійснювати:

– обробку всіх видів сигналізації, які використовуються у його домені;

– зберігання й управління даними користувачів, що підключені до його домену безпосередньо або через обладнання шлюзів доступу;

– взаємодію із серверами аплікацій для надання розширеного списку послуг користувачам мережі.

Завдання транспортного рівня — забезпечення прозорої передачі інформації користувача шляхом її комутації та маршрутизації. У NGN оператори отримають можливість нарощувати обсяги послуг, що у свою чергу приведе до росту вимог щодо надійності та продуктивності мереж транспортного рівня. Причому надійність виходить на перше місце, оскільки NGN мають забезпечувати передачу різнорідного трафіка, у тому числі чутливого до затримок, що раніше передавався за допомогою класичних систем передачі з часовим поділом каналів ієрархій SDH або PDH. У деяких випадках новітні транспортні мережі замінюватимуть собою частину інфраструктури існуючих традиційних мереж зв'язку.

ITU-T визначає такі вимоги до можливостей транспортного рівня:

– підтримка з'єднань у реальному часі й з'єднань, не чутливих до затримок;

– підтримка різних моделей з'єднань: «точка — точка», «точка — багатоточка», «багатоточка — багатоточка», «багатоточка — точка»;

– гарантовані рівні продуктивності, надійності, доступності, масштабованості.

Особливістю інфраструктури NGN є використання універсальної транспортної мережі, що базується на технологіях саме пакетної комутації. Сьогодні при виборі технологічної основи транспортної мережі перспективною вважається технологія IP, або її розвиток MPLS, оскільки:

– використання технологій IP/MPLS у середовищі Ethernet дозволяє підвищити масштабованість і якість обслуговування до рівня, необхідного для транспортних мереж;

– кількість аплікацій, які використовують протокол IP, зростатиме, відповідно частка IP-трафіка збільшуватиметься, і, як наслідок, неминучі проблеми технології ATM, пов’язані з додатковими накладними витратами пропускної здатності при передачі IP-трафіка, внаслідок чого відбувається збільшення вартості реалізації мережних рішень на базі ATM.

До рівня доступу належать:

– шлюзи;

– вузли агрегування доступу;

– мережі доступу (МД), тобто мережі електрозв’язку, які забезпечують підключення термінальних пристроїв користувачів до приграничного вузла транспортної мережі.

Для організації рівня доступу можуть використовуватися різні середовища передачі. Це може бути мідна пара, коаксіальний кабель, волоконно-оптичний кабель, радіоканал, супутникові канали або будь-яка їхня комбінація.

Мережа доступу, як і NGN у цілому, може складатися з декількох рівнів. Комутатори, установлені у вузлах нижнього рівня, мультиплексують інформацію, що надходить по численних абонентських каналах (що часто називаються абонентськими закінченнями, local loop), і передають її комутаторам верхнього рівня, щоб ті, у свою чергу, передали її комутаторам

транспортного рівня. Кількість рівнів мережі доступу залежить від її розміру; невелика мережа доступу може складатися з одного рівня, а велика — із двох-трьох. Наступні рівні здійснюють подальшу концентрацію трафіка, збираючи його й мультиплексуючи в більш швидкісні канали.

Доступ до ресурсів транспортної мережі здійснюється через граничні вузли, до яких підключається обладнання мережі доступу або здійснюється зв'язок з існуючими мережами. В останньому випадку граничний вузол виконує функції міжмережного шлюзу. Одним з найважливіших критеріїв вибору технології транспортної мережі є її несуперечність існуючим транспортним і комутаційним структурам, тобто здатність забезпечити підтримку традиційних видів сервісу. При проектуванні структури транспортної мережі й локалізації її вузлів необхідно враховувати не тільки потенційні можливості концентраторів і комутаторів у них, але й продуктивність вузлів агрегування інформаційних сервісів (рис. 1.5).

Рисунок 1.5 - Взаємодія рівнів транспорту й доступу

Логіка агрегування доступу керується обмеженнями продуктивності комутатора транспортної мережі. Як правило, кожний вузол агрегування доступу обслуговує до 10000 абонентських закінчень. Виходячи з цього, вузли агрегування доступу об'єднуються за територіальною ознакою, вузли транспортної мережі закріплюються за відповідними мережами доступу,

замикаючи відповідний трафік на себе. Однак забезпечення надійності послуг вимагає резервного з'єднання хоча б із ще одним вузлом магістральної мережі. Це забезпечить для кожного вузла агрегування доступ мінімум до двох точок входу до транспортної мережі, що, з одного боку гарантує безперебійність надання послуг навіть у разі фізичного розриву одного із з'єднань, а з іншого — можливість перерозподілу абонентського навантаження по вузлах транспортної мережі. Залежно від характеру абонентів роль вузла абонентського доступу може взяти на себе вузол агрегування доступу (це характерно для мереж телефонії з комутаторами на 10000 номерів). Вузол абонентського доступу може виконувати функції вузла агрегування та шлюзувати різнорідний трафік у мультисервісне середовище (така ситуація частіше зустрічається в мережах пакетної комутації).

Можна відзначити, що з розвитком технологій зв'язку стає усе проблематичніше провести чітку межу між транспортним рівнем і рівнем доступу. Так, наприклад, цифровий абонентський мультиплексор доступу (DSLAM) може бути віднесений і до того, і до іншого рівня.

Рівень термінального обладнання включає різні типи кінцевих (термінальних) вузлів, мережі терміналів — обладнання, встановленого у користувачів (абонентів, клієнтів), за допомогою яких користувач використовує через мережі доступу ресурс транспортного рівня. У комп'ютерній мережі кінцевими вузлами є комп'ютери, телефонній — телефонні апарати, а телевізійній або радіомережі — відповідні теле- і радіоприймачі.

1.3 Структура мультисервісної комп'ютерної мережі гуртожитку.

Мультисервісними називаються мережі, в яких для передачі різних типів трафіку використовується один канал. Мультисервісні мережі надають

споживачам безліч різних послуг на єдиній технологічній основі — за принципом конвергенції послуг.

Отже, мультисервісна мережа — це єдина мережа, що здатна передавати різні типи трафіку: голос, відео і дані. Основною передумовою появи і розвитку мультисервісних мереж є прагнення зменшення вартості передачі даних, підтримка складних, насичених мультимедіа, прикладних програм і розширення функціональних можливостей мережевого обладнання. Мультисервісні мережі передачі даних дозволяють клієнтам реалізувати такі важливі функції:

– якісна передача даних;

– висока масштабованість;

– ефективне використання смуги пропускання існуючих магістральних каналів зв'язку;

– побудова безпечної схеми передачі даних;

– впровадження єдиної системи управління діяльністю всіх відділів і філій;

– організація системи резервування каналів передачі даних і доступу до Інтернет;

– управління інформаційними ресурсами та централізований моніторинг;

– створення єдиної телефонної мережі з єдиним адресним простором (об'єднана передача відео, голосу і даних для територіально розподілених організацій);

– введення нових корпоративних сервісів і додатків;

– здійснення єдиної адміністративно-технічної політики в області інформаційного обміну;

– виключення дублювання функцій та підвищення продуктивності праці співробітників;

– скорочення витрат на всі канали зв'язку;

– збільшення конкурентоспроможності організації;

– підвищення продуктивності праці співробітників.

Мультисервісні мережі бувають різних масштабів, залежно від завдань, які потрібно виконувати на основі Ethernet або MPLS.

В даний час побудова мультисервісних мереж з інтеграцією різних послуг є одним з найбільш перспективних напрямків розвитку мереж. Основне завдання мультисервісних мереж полягає в забезпеченні співіснування та взаємодії різнорідних комунікаційних підсистем в єдиній транспортній середовищі, коли для передачі звичайного трафіку (даних) і трафіку реального часу (голосу та відео) використовується єдина інфраструктура.

Мультисервісна мережа - це єдина мережа, здатна передавати голос, відеозображення і дані. Основним стимулом появи і розвитку мультисервісних мереж є прагнення зменшити вартість володіння, підтримати складні, насичені мультимедіа прикладні програми і розширити функціональні можливості мережевого обладнання.

Основна відмінність мереж наступного покоління від традиційних мереж в тому, що вся інформація, що циркулює в мережі, розбита на дві складові. Це сигнальна інформація, що забезпечує комутацію абонентів та надання послуг, і безпосередньо для користувача дані, що містять корисну навантаження, призначену абоненту (голос, відео, дані). Шляхи проходження сигнальних повідомлень і користувальницької навантаження можуть не збігатися. Мережі NGN базуються на інтернет технологіях включають у себе IP протокол і технологію MPLS

1.3.1. Локальна мережа (Lan)

Локальна мережа комп’ютерів — спільне приєднання декількох окремих комп’ютерів (робочих станцій) до одного каналу передачі даних. У сучасній технічній літературі для позначення використовується англійська абревіатура LAN (Local Area Network). Мережа об’єднує весь парк комп’ютерів (усіх

користувачів) в один інформаційний простір, який має такі властивості: 1) доступність даних для будь-якого користувача мережі, що дозволяє розв'язувати багато завдань оперативно і з більшою ефективністю, тому що з'являється можливість контролювати роботу впродовж усього терміну її виконання, погоджувати та поєднувати її результати; 2) достовірність і надійність зберігання інформації, що досягається завдяки високій перешкодостійкості системи, які, в свою чергу, забезпечують ефективність резервування та організацію архівного зберігання даних; 3) спрощений пошук необхідної інформації за допомогою об'єднаного архіву; 4) стандартизація документообігу відповідно до загальних вимог; 5) забезпечення доступу авторизованого користувача згідно з його правами доступу. Для забезпечення роботи мережі все її обладнання має працювати за певними стандартами і правилами. Найбільш поширеним є стандарт Ethernet. На сьогодні він використовується більше ніж у 5 млн мереж, в яких задіяно більше 50 млн комп'ютерів. Правила, що дозволяють здійснювати передачу неспотвореної інформації від одного комп'ютера до іншого, а також досягти сумісності комп'ютерів, мережевих програм та обладнання різних користувачів, зумовлені у протоколі передачі даних. Протоколів існує багато, оскільки кожен із них описує певний бік роботи мережі. Об'єднані в мережу комп'ютери створюють організовану систему, яка функціонує в режимі «клієнт — сервер». У будь-який час два комп'ютери, що взаємодіють у мережі, виступають один як запитувач — клієнт, інший — як сервер, який повинен забезпечити клієнта певним сервісом — набором послуг. У різних мережах сервер має змогу виконувати найрізноманітніші завдання. Це може бути і поштовий сервер, сервер бази даних, сервер доступу до глобальної мережі Інтернет, сервер друку, який забезпечує доступ до принтерів у мережі.

Локальна мережа комп'ютерів характеризується конкретною топологією, під якою розуміють конфігурацію графа, вершинами (або вузлами) якого є комп'ютерні мережі чи інше спорядження, а ребрами — фізичні зв'язки між

ними. Поряд із відомими топологіями обчислювальних мереж «кільце», «зірка», «шина» на практиці використовують і комбіновану структуру — деревоподібну. Топологія «кільце» в мережах Ethernet не використовується. Фізичні зв’язки між комп’ютерами в мережі зазвичай реалізують за допомогою оптично-волоконного кабеля. На сьогодні використовують і бездротові мережі WLAN (Wireless Local Area Network — бездротова локальна мережа), які працюють за допомогою модемів за протоколом Wi-Fi (Wireless Fidelity — бездротова точність).

1.3.2. Безпровідна мережа (Wi-Fi)

Технологія Wi-Fi – це безпровідний аналог стандарту Ethernet, на основі якого сьогодні побудована велика частина офісних комп'ютерних мереж. Він був зареєстрований в 1999 році і став справжнім відкриттям для менеджерів, торгових агентів, співробітників складів, основним робочим інструментом яких є ноутбук або інший мобільний комп'ютер.

Wi-Fi - скорочення від англійського Wireless Fidelity, що означає стандарт бездротового (радіо) зв'язку, який об'єднує декілька протоколів та має офіційне найменування IEEE 802.11 (від Institute of Electrical and Electronic Engineers - міжнародної організації, що займається розробкою стандартів у галузі електронних технологій). Найбільш відомим та поширеним на сьогоднішній день є протокол IEEE 802.11b (зазвичай під скороченням Wi-Fi мають на увазі саме його), що визначає функціонування бездротових мереж, в яких для передачі даних використовується діапазон частот від 2,4 до 2.4835 гігагерца і забезпечується максимальна швидкість 11 Мбіт/сек. Максимальна дальність передачі сигналу у такій мережі складає 100 метрів, однак на відкритій місцевості вона може досягати й більших значень (до 300-400 м).

Крім 802.11b існують ще бездротовий стандарт 802.11a, який використовує частоту 5 Ггц та забезпечує максимальну швидкість 54 Мбіт/с, а також 802.11g, що працює на частоті 2,4 Ггц і теж забезпечує 54 Мбіт/с. Однак,

через меншу дальність, значно більшу обчислювальну складність алгоритмів і високе енергоспоживання ці технології поки не набули великого поширення. Крім того, в даний час ведеться розробка стандарту 802.11n, який у найближчому майбутньому зможе забезпечити швидкість до 320 Мбіт/с.

Подібно традиційним провідним технологіям, Wi-Fi забезпечує доступ до серверів, що зберігають бази даних або програмні додатки, дозволяє вийти в Інтернет, роздруковувати файли і т. д. Але при цьому комп'ютер, з якого зчитується інформація, не потрібно підключати до комп'ютерної розетки. Досить розмістити його в радіусі 300 м від так званої точки доступу (access point) - Wi-Fi-пристрою, що виконує приблизно ті ж функції, що звичайна офісна АТС. У цьому випадку інформація буде передаватися за допомогою радіохвиль в частотному діапазоні 2,4-2,483 ГГц.

Таким чином, Wi-Fi-технологія дозволяє вирішити три важливих завдання:

– спростити спілкування з мобільним комп'ютером;

– забезпечити комфортні умови для роботи діловим партнерам, які прийшли в офіс зі своїм ноутбуком;

– створити локальну мережу в приміщеннях, де прокладка кабелю неможлива або надмірно дорога.

Крім цього, саме існування мережі Wi-Fi - важливий штрих до портрета фірми. Він так само працює на її корпоративний імідж, як шкіряні крісла в переговорній і красиво видані інформаційні буклети.

Бездротова технологія може стати як основою IT-системи компанії, так і доповненням до вже існуючої кабельної мережі.

Ядром бездротової мережі Wi-Fi є так звана точка доступу (Access Point), яка підключається до якоїсь наземної мережевої інфраструктури (наприклад, офісної Ethernet-мережі) та забезпечує передачу радіосигналу. Зазвичай, точка доступу складається із приймача, передавача, інтерфейсу для підключення до дротової мережі та програмного забезпечення для обробки даних. Після підключення навколо точки доступу формується територія радіусом 50-100

метрів (її називають хот-спотом або зоною Wi-Fi), на якій можна користуватися бездротовою мережею.

Для того щоб підключитися до точки доступу та відчути всі переваги бездротової мережі, власнику ноутбуку або іншого мобільного пристрою, оснащеного Wi-Fi адаптером, необхідно просто потрапити в радіус її дії. Усі дії із визначення пристрою та налаштування мережі більшість ОС проводять автоматично. Якщо користувач потрапляє одночасно в кілька Wi-Fi зон, то відбувається підключення до точки доступу, що забезпечує найпотужніший сигнал. Час від часу проводиться перевірка наявності інших точок доступу, і в разі, якщо сигнал від нової точки сильніший, пристрій перепідключається до неї, налаштовуючись абсолютно прозоро і непомітно для власника.

Одним з головних достоїнств будь-якої Wi-Fi мережі є можливість доступу до Інтернету для всіх її користувачів, яка забезпечується або прямим підключенням точки доступу до інтернет-каналу, або підключенням до неї будь-якого сервера, під’єднаного до Інтернет. В обох випадках мобільному користувачеві не потрібно нічого самостійно настроювати - досить запустити браузер і набрати адресу будь-якого інтернет-сайту.

Також декілька пристроїв з підтримкою Wi-Fi можуть з'єднуватися один з одним безпосередньо (зв'язок пристрій-пристрій), тобто без використання спеціальної точки доступу, утворюючи щось на кшталт локальної мережі, в якій можна обмінюватися файлами, але в цьому випадку обмежується число видимих станцій.

У випадку з пристроями без вбудованої підтримки **технології Wi-Fi** (наприклад, із звичайними домашніми або офісними комп'ютерами) потрібно буде придбати спеціальну карту, що підтримує цей стандарт.

Багато експертів вважають, що революція Wi-Fi почалася з ініціативи звичайних приватних користувачів. Людям сподобалося ділитися підключенням до мережі за допомогою нової бездротової технології. Для позначення безкоштовних Wi-Fi точок була розроблена система умовних

знаків, які наносилися крейдою на стіни будинків, біля яких можна було вийти в Інтернет. Спочатку ці дії викликали негативну реакцію мобільних і інтернет-операторів, але незабаром Wi-Fi провайдери стали мирно уживатися з приватними мережами.

1.3.3. IP-телефонія

IP-телефонія — це технологія, що дозволяє використовувати будь-яку IP-мережу як засіб організації та ведення телефонних розмов, передачі відео зображень та факсів у режимі реального часу.

При відправленні або отриманні електронної пошти відбувається передача «пакета» інформації через мережу Інтернет. Аналогічним чином працює й IP-телефонія. Створення «пакетів» — перетворення аналогових (зокрема, звукових) сигналів у цифрові, їх стискання, передачу мережею Internet і зворотне перетворення в аналогові відбувається завдяки існуванню протоколу передачі даних через Інтернет (IP — Internet Protocol), звідси і назва «IP-телефонія».

Дедалі ширшим стає застосування Internet мережі. І якщо ще 15 років тому аналітики заперечували можливість передачі голосу через Internet, то сьогодні їхні погляди повністю змінилися. Наприклад, згідно з прогнозом дослідницької фірми Analysys у 2003 році на Internet-телефонію буде припадати 36% всіх міжнародних переговорів. Чим же викликано такий бурхливий розвиток нещодавно нікому невідомої технології? Справа в тому, що використання IP-телефонії дозволяє в кілька разів зменшити витрати на послуги зв'язку (не лише голосового, бо насправді технологія дозволяє передавати і факси, і мультимедіа). Очікується, що ціни на телефонні послуги через Internet і звичайні телефонні мережі зрівняються в найближчі 3-5 років.

Основною перевагою IP-телефонії є нижча вартість міжміських і міжнародних переговорів у порівнянні з традиційною телефонією за рахунок

цифрування і наступної компресії (стиснення) голосового потоку, що дозволяє знизити собівартість послуги.

Друге — нижча вартість кінцевого устаткування. На шляху проходження пакетів інформації з голосовим сигналом не використовується дороге устаткування, що стало вже традиційним для міжнародної та міжміської телефонії. У цій високоякісній технології використовуються відносно недорогі комутатори-маршрутизатори

У традиційній телефонії використовується принцип встановлення з'єднання, що має назву комутація каналів. Це означає, що під час зв'язку відбувається тимчасове з'єднання, якому виділяється весь канал зв'язку, незалежно від його завантаженості. Перевагою такого типу зв'язку є дуже не значний час затримки.

Під час передачі інформації через Internet відбувається зв'язок з комутацією пакетів. Це означає, що вся інформація розбивається на пакети, кожен з яких передається окремо від вузла до вузла без попереднього зв'язку між початковим та кінцевим пунктом. Кожен вузол мережі, через який передається IP-пакет повинен аналізувати цей пакет (тип, адреса відправлення і призначення, контроль цілісності та інші параметри). Через те, що таких вузлів можуть бути десятки, кожен з них повинен проводити аналіз, і, крім того, зв‘язок між ними часто не найкращий, виникають великі, непередбачені затримки в мережі. Також затримка може виникати під час стиснення та відновлення голосового сигналу. Людське ж вухо починає сприймати уривчастість мови навіть при затримці 150 мс. Ось чому Internet не є ідеальним середовищем для комунікацій в реальному часі.

Але якщо розглянути передачу інформації в Internet (локальній мережі, LAN), то ситуація буде дещо кращою. Тут все обладнання знаходиться під контролем однієї компанії, яка може конфігурувати його за власним бажанням. Наприклад, можна проставити вищий приорітет проходження голосових IP-

пакетів, порівняно з іншою інформацією, для якої час затримки не є критичним. Це забезпечить якіснішу передачу мови.

1.3.4. Система відеоспостереження.

Відеоспостереження (англ. Video surveillance) — система передавання інформації з відеокамер, телевізійних камер на обмежену кількість моніторів та/або записуваних пристроїв.

Відмінність систем відеоспостереження від телевізійного мовлення полягає у тому, що сигнал не передається у відкритому режимі. Системи відеоспостереження часто використовуються для спостереження у місцях, які потребують постійного нагляду, таких як банки, банкомати, казино, вокзали, аеропорти, військові об'єкти та звичайні крамниці тощо.

На промислових об'єктах камери спостереження можуть використовуватись для централізованого стеження за виробничим процесом, або, у разі наявності середовища, небезпечного для людини . Системи відеоспостереження можуть знімати безперервно, або вмикатись лише за заданою подією. Досконаліші системи стеження, з використанням відео реєстраторів, дозволяють створювати записи, які зберігатимуться роками, з різною якістю та з додатковими можливостями (такими як виявлення рухів та оповіщення через електронну пошту).

Відеоспостереження за громадськими місцями, особливо поширене у Великій Британії, де оцінна кількість камер до населення, найбільша серед країн світу.Використання відеоспостереження підсилило дебати про баланс між захистом приватності та безпекою.

Водночас, системи відеоспостереження підрозділяються на дротові та бездротові.

Система відеоспостереження може бути як з простою структурою, яка складається лише з однієї камери, зображення з якої, передається у прямому ефірі на один монітор, а також у вигляді складної системи з декількома

камерами і різними системами для зберігання й вивчення зображення або відео — матеріалу. Система може контролюватися персоналом оператора або постачальника послуг, чи працювати після установки, у повністю автоматичному режимі. У цілком автоматизованих системах, в яких, наприклад, живе зображення не враховується, шляхом відбору проб, можуть проводитися функціональні перевірки та доступні зображення, лише за потреби.

Спочатку власне, аналогові системи передавання, було побудовано з використанням: коаксіального кабелю, дротом за технологією крученої пари або волокно-оптичної системи.

Протягом декількох останніх років, початку XXI століття, відбувається перехід у напрямку цифрових систем відеоспостереження. Вони доступні у декількох варіантах. По-перше, аналогові камери приєднано до комп'ютера, який відцифровує сигнал відповідною картою, що уможливлює проходження мережею, аналогових сигналів. Такі гібридні системи є, в основному там, де аналогові камери вже наявні, і потрібні великі зусилля на заміну кабельної розводки. По-друге, є винятково цифрові версії. Вони використовують лише IP-камери, відеозображення з яких, передаються приватною або публічною мережею IP до центральної станції відеоспостереження задля перегляду і/або запису. Передавання відео, здійснюється винятково комерційними IT-системами (маршрутизатори, комутатори та інше). Головним завданням у цьому разі, є надійне та безпечне передавання інформації. Цифрові технології, мають як переваги (якість зображення), так і новий набір проблем (пам'ять і вимоги до пропускної здатності, а також різноманітність форматів та методів стиснення відео).

Цифрові системи відеоспостереження, дозволяють оператору дуже гнучко вибирати, за яких обставин і в якій формі (зображення низької або високої роздільної здатності, відео зі звуком) здійснюється запис. Камери, навіть, можна використати як давачі руху, тобто розпочати запис після відстеження події на певній ділянці. Це дозволяє зменшити вимоги до

обсягу пам'яті та часу. Головне завдання на даному відрізку, уникнути помилкових спрацювань від руху комах, пташиного польоту або, навіть, змін умов освітлення. Інтеграція інших джерел сигналів, наприклад, систем охоронної сигналізації, також можлива.

Сонячне або штучне світло, що падає крізь вікно або двері, може значно погіршити зображення камери. Програмне забезпечення у камерах або системі запису, може протидіяти цій проблемі обмеженням балансу білого й індивідуального налаштування експозиції.

Завдяки різним можливостям збору, обробки та запису сигналу, станом на початок 2010 років, не існує технологічного стандарту для систем відеоспостереження. Залежно від застосування і розташування, треба лише враховувати правові норми конкретної країни та дотримуватися їх під час вибору й установки.

Засоби управління та моніторингу мультисервісних комп’ютерних мереж

Все різноманіття пристроїв, які транслюють і комутують трафік даних, перетворюють інформацію, закладену в пакети, в стандартну телефонну сигналізацію і з'єднання, сполучають цифрові мережі різної природи, термінують на собі різні види трафіку, управляється з одного потужного ядра. Це третій рівень NGN - керуючий.

Даний рівень часто пов'язують з таким поняттям, як SoftSwitch. Основна функція третього рівня NGN - управління з'єднанням абонента А з абонентом Б. Займається цим спеціалізований сервер, або «сервер з'єднань» - по термінології SoftSwitch. Велика потужність і продуктивність подібних серверів - важлива умова безперебійної роботи мережі. Крім того, при проектуванні SoftSwitch враховують специфічні фактори IP-мереж - це необхідність забезпечення параметрів якості обслуговування (QoS) мережі VoIP, поділ маршрутів потоків голосу і даних, управління маршрутизацією за наявності досить строкатого спектру пристроїв: маршрутизаторів, конверторів сигналізації, прикордонних

контролерів, шлюзів, проксі-серверів, абонентських терміналів,і контролерів абонентського доступу різної природи.

Головна перевага XDSL-технологій полягає в можливості одночасного надання по одній мідній парі як телефонного зв'язку, так і високошвидкісної передачі даних.

Одна з найбільш економічних технологій DSL - асиметрична ADSL. Однак пропускна здатність лінії ADSL знижується зі збільшенням відстані, а також внаслідок дефектів кабелів або установки схем корекції.

Як головного технологічного конкурента ADSL фахівці розглядають симетричний доступ SHDSL, який використовує більш ефективний лінійний код і займає вузьку смугу частот при будь-якій швидкості. Більш того, спектральна щільність сигналу SHDSL має форму, що забезпечує його майже ідеальну сумісність з сигналами ADSL, що є надзвичайно важливою обставиною для забезпечення стійкої роботи в умовах широкого впровадження технологій XDSL в майбутньому.

1.4 Переваги та недоліки технології Wi-Fi

Технологія Wi-Fi розвивається і широко застосовується в усьому світі останнім часом дуже стрімко. Технологія безпровідної мережі Wi-Fi має великий потенціал. Як і у будь-який інший технології, поряд із плюсами є й мінуси. Переваги технології Wi-Fi. Основною перевагою в застосуванні технології Wi-Fi є відсутності проводів. Wi-Fi - це радіозв'язок, який може об'єднувати між собою кілька пристроїв.

Технологія Wi-Fi є особливо корисною в тих випадках, коли прокладка кабелів не є доцільною або взагалі неприпустима. Наприклад, її часто використовують в залах конференцій та виставок. Це ідеальне рішення для

будівель, які вважаються архітектурними пам'ятками історії, так як там виключається можливість проводки кабелів.

Безпровідні мережі знайшли широке застосування при підключенні різних пристроїв не лише між собою, але і до мережі Інтернет. Практично усі сучасні ноутбуки, планшети і деякі мобільні телефони мають таку можливість. Це дуже зручно та дозволяє підключитися до Інтернету практично скрізь, а не тільки там, де прокладені мережеві кабелі. Сьогодні можна увійти в Інтернет, наприклад, перебуваючи в парку на прогулянці, в кафе, чи столові, або в залі очікування аеропорту, чи автовокзалі. Основною потребою є те, що поблизу має бути доступна точка Wi-Fi [31].

Ще однією перевагою бездротової технології Wi-Fi можна вважати простоту створення мережі. Щоб підключити новий пристрій до мережі досить просто включити функцію Wi-Fi в пристрої і провести нескладну настройку. У випадках з дротяними технологіями необхідно тягнути провід до самого пристрою, тому багато сучасних офісів переходять на цю технологію мережі.

Стандартизація технології Wi-Fi дозволяє підключатися до мережі в будь-якій країні світу. Все обладнання, що працює з технологією Wi-Fi сертифіковане та дозволяє досягати високої сумісності.

Технологія Wireless Fidelity дозволяє розгорнути мережу без прокладки мережевого кабелю, що зменшує вартість прокладки і розширення мережі. Місця, де не можна прокласти кабель, наприклад, поза приміщеннями і в будівлях, що мають історичну цінність, можуть обслуговуватися безпровідними мережами. Також технологія дозволяє мати доступ до мережі мобільним пристроям. Wi-Fi пристрої широко поширені на ринку та гарантується сумісність устаткування завдяки обов'язковій сертифікації устаткування з логотипом Wi-Fi. Випромінювання від Wi-Fi пристроїв у момент передачі даних у 100 разів менше, ніж від мобільного телефону. Технологія Wi-Fi - це набір глобальних стандартів. На відміну від мобільних телефонів, Wi-Fi пристрій може працювати в різних країнах по всьому світу [33].

Недоліки Wi-Fi. На якість безпровідної мережі великий вплив має навколишнє середовище. Мережа дуже чутлива до електромагнітних випромінювань, що створюються побутовими приладами, та іншою технікою. Дія електромагнітних хвиль в першу чергу впливає на швидкості передачі даних в мережі.

Незважаючи на стандартизацію, багато пристроїв від різних виробників мають неповну сумісність, що знову ж впливає на швидкість та якість зв'язку.

Частотні діапазони роботи Wi-Fi і експлуатаційні обмеження в країнах світу неоднакові. У європейських країнах дозволено два додаткові канали, які заборонені в США. У Японії є ще один канал у верхній частці діапазону, а інші країни, наприклад - Іспанія, забороняють використання низькочастотних каналів. Деякі країни, наприклад Росія, Білорусь і Італія, вимагають реєстрації всіх мереж приміщень, що працюють зовні, або вимагають реєстрації Wi-Fi оператора [30].

В Росії точки доступу, а також адаптери Wi-Fi, що перевищує 20 дБм (100 мВт), підлягають обов'язковій реєстрації.

Мережі Wi-Fi на деяких стандартах шифрування дуже просто зламати зловмисникові, так найпопулярніший стандарт шифрування WEP може бути відносно легко зламаний навіть при правильній конфігурації, тобто через слабку стійкість алгоритму. Незважаючи на те, що нові пристрої підтримують досконаліший протокол шифрування даних WPA і WPA2, багато старих точок доступу не підтримують його і вимагають заміни. В червні 2004 року ухвалення стандарту IEEE 802.11i (WPA-2) зробило доступною безпечнішу схему, яка доступна в новому устаткуванні. Обидві схеми вимагають стійкіший пароль, ніж ті, які зазвичай призначаються користувачами мережі. Багато установ використовують додаткове шифрування для захисту від проникнення. Прикладом додаткового шифрування є VPN - віртуальна приватна мережа [29].

1.1 Безпека безпровідних Wi-Fi мереж

Як і будь яка комп'ютерна мережа, Wi-Fi – є джерелом підвищеного ризику несанкціонованого доступу. Проникнути в безпровідну мережу значно простіше, ніж в звичайну, адже зловмиснику не потрібно підключатися до проводів, а досить лише опинитися в зоні сигналу мережі [39].

Звичайний користувач може за кілька хвилин налаштувати домашню мережу, але, не маючи базових знань про ці технології та забезпечення безпеки в локальній мережі, він стає легкою мішенню для того, хто хоче проникнути в його мережу. Дехто може сказати, що йому нема чого приховувати на своєму комп'ютері, але він не усвідомлює того факту, що зловмисник може використати його комп'ютер для здійснення своїх dos атак. Після цього до нашого користувача можуть завітати представники державних органів, яким він буде довго пояснювати, що уявлення не має про те, що сталось. Для захисту свого Wi-Fi підключення потрібно:

– змінити стандартний пароль і IP адресу точки доступу;

– можна відключити трансляцію ID мережі, це допоможе приховати вашу мережу. Виявити її зможе тільки та людина, яка знає її ID назву;

– необхідно включати фільтрацію по MAC-адресі;

– використовувати надійне шифрування даних (WPA,WPA-2).

У бездротовій мережі, налаштуванням якої не було приділено належної уваги, зловмисник може отримати:

– доступ до ресурсів і дисків користувачів Wi-Fi-мережі, та через неї - і до ресурсів мережі;

– перехват трафіку та витяг з нього конфіденційної інформації;

– спотворення проходить в мережі інформації;

– перехоплення Інтернет трафіку;

– атака на комп'ютери користувачів і сервери мережі;

– створення фіктивної точки доступу;

– розсилка спаму

– протиправна діяльність від імені вашої мережі.

Існують такі технологій захисту Wi-Fi мереж.

WEP-шифрування (Wired Equivalent Privacy).

Аналог шифрування трафіку в провідних мережах. В WEP-шифруванні використовується симетричний потоковий шифр RC4 (Rivest Cipher 4), який досить швидко працює. На сьогодні WEP і RC4 не вважаються криптостійкими, а існують два основних протоколи WEP - 40-бітний WEP (довжина ключа 64 біта, 24 з яких - це вектор ініціалізації, який передається відкритим текстом); та 104-бітний WEP (довжина ключа 128 біт, 24 з яких - це теж вектор ініціалізації). Вектор ініціалізації використовується алгоритмом RC4. Збільшення довжини ключа не призводить до збільшення надійності самого алгоритму.

TKIP-шифрування (Temporal Key Integrity Protocol).

Використовується той же симетричний потоковий шифр RC4, як і WEP-шифруванні, але є більш криптостійким. Вектор ініціалізації становить 48 біт. В TKIP-шифруванні враховані основні атаки на WEP. Також тут використовується протокол Message Integrity Check для перевірки цілісності повідомлення, який блокує станцію на 1 хвилину, якщо послані протягом 1 хвилини два повідомлення не пройшли перевірку на цілісності. З урахуванням всіх удосконалень шифрування TKIP все одно не вважається криптостійким.

CKIP-шифрування (Cisco Key Integrity Protocol).

Дуже схожий з протоколом TKIP. Протокол створений компанією Cisco та використовується CMIC (Cisco Message Integrity Check) для перевірки цілісності повідомлень [5].

WPA шифрування (Wi-Fi Protected Access).

Тут взаміну уразливого RC4, використовується криптостійкий алгоритм шифрування AES (Advanced Encryption Standard). Також можливим є використання EAP (Extensible Authentication Protocol) - розширюваний протокол автентифікації. Доступними є два режими WPA шифрування: Pre-

Shared Key (WPA-PSK) - кожен вузол вводить пароль для доступу до мережі; Enterprise - перевірка здійснюється серверами RADIUS;

WPA-2-шифрування (IEEE 802.11i).

Протокол був прийнятий у 2004 році. З 2006 року шифрування WPA-2 повинно підтримувати все вироблене Wi-Fi обладнання. В даному протоколі застосовується RSN (Robust Security Network) - мережа з підвищеною безпекою. Спочатку в WPA2 використовувався протокол CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). Протокол блочного шифрування з кодом автентичності повідомлення та режимом зчеплення блоків і лічильника. Основою WPA2 є алгоритм AES. Для сумісності зі старим обладнанням здійснюється підтримка TKIP і EAP (Extensible Authentication Protocol) з деякими його оновленнями. Як і в WPA в WPA2 є два режими роботи: Pre-Shared Key і Enterprise [22].

VPNT (Virtual Private Network). Технологія віртуальних приватних мереж VPN була заснована компанією Intel. Розроблялась вона для захищеного підключення клієнтів до мережі через загальнодоступні Інтернет канали. VPN працює за допомогою так званих безпечних «тунелів» від користувача до вузла доступу, або сервера. VPN спочатку не був розрахований для роботи з Wi-Fi мережами, він придатний для всіх типів мереж. Для шифрування трафіку в VPN найчастіше застосовується протокол IPSEC, та рідше – PPTP. або L2TP. Можуть бути використаними такі алгоритми, як DES, Triple DES, AES та Md5. VPN підтримується на багатьма операційними системами (Windows, Linux, Solaris) як програмними, так і апаратними засобами. Варто відзначити високу надійність технології віртуальних приватних мереж – на сьогодні ще не зафіксовано випадків злому VPN мережі. Найчастіше технологію VPN рекомендують застосовувати у великих корпоративних мережах. Для домашнього користування установка і налаштування VPN є дуже громіздкою і трудомісткою. Мінусом VPN є те, що при застосуванні технології доведеться пожертвувати близько 35% пропускної спроможності Інтернет каналу.

Багато великих провайдерів пропонують свої послуги з організації VPN-мереж для бізнес-клієнтів. До VPN належать:

– IPSec (IP security) - часто використовується поверх IPv4;

– PPTP (point-to-point tunneling protocol) - розроблявся декількома компаніями, серед яких і Microsoft;

– PPPoE (PPP (Point-to-Point Protocol) over Ethernet) - мережевий протокол передачі кадрів PPP через Ethernet;

– L2TP (Layer 2 Tunnelling Protocol) - протокол тунелювання другого рівня, що використовується в продуктах компаній Cisco і Microsoft;

– L2TPv3 (Layer 2 Tunnelling Protocol version 3);

– OpenVPN SSL VPN з відкритим вихідним кодом, підтримує режими PPP, bridge, point-to-point та multi-client server [37].

2 ЗАСОБИ УПРАВЛІННЯ ТА МОНІТОРИНГУ БЕЗПРОВІДНОЇ МЕРЕЖІ

Системи аналізу та моніторингу безпровідних мереж дозволяють уникнути маси проблем ще на етапі проектування і прокладання бездротової мережі стандарту 802.11a/b/g/n, а також швидко і своєчасно вирішувати виникаючі проблеми з продуктивністю, виявленням джерел перешкод, безпекою та інше [18].

На етапі проектування системи аналізу та моніторингу безпровідних мереж дозволяють :

– здійснювати візуалізацію зон дії бездротових точок доступу для забезпечення надійного покриття;

– визначати оптимальні місця установки бездротових точок доступу, як при прокладанні мережі, так і при модернізації вже існуючої;

– моделювати будівельні матеріали приміщень, перешкод, що впливають на загасання Wi-Fi сигналу;

– моделювати зміни в параметрах точок доступу;

– прогнозувати продуктивність Wi-Fi мережі;

– тестувати продуктивність і можливість підключення до бездротової мережі [15].

У процесі експлуатації Wi-Fi мережі системи аналізу та моніторингу дозволяють:

– в реальному часі видавати докладну інформацію, включаючи: назву мереж, MAC адреса клієнтів, типи шифрування, дані про рівні сигналу, рівні перешкод в каналах та інше;

– проводити аналіз продуктивності Wi-Fi мережі;

– вести моніторинг інтерференції між каналами;

– проводити аналіз радіочастотного спектру для пошуку несправностей Wi-Fi мереж;

– визначати місцезнаходження пристроїв , що створюють перешкоди;

– ідентифікувати неавторизовані пристрої (обладнання зловмисників, які підключилися або намагаються підключитися до мережі) і визначати їх місцезнаходження;

– вести безперервний аналіз трафіку на предмет загроз і автоматично блокувати неавторизовані та підозрілі пристрої в мережі.

На сьогодні найпопулярнішими системами аналізу та моніторингу Wi-Fi мереж є аналізатори, що представляють собою комплекси апаратного та програмного забезпечення.

2.1 Діагностика і управління Wi-Fi мереж

Для діагностики безпровідних мереж використовують безліч програмних засобів. В роботі проаналізуємо найбільш популярні на сьогодні продукти ORION NPM SolarWinds та AP Manager.

SolarWinds - найбільший розробник рішень для управління мережами підприємств та установ. Основні продукти SolarWinds - системи мережевого управління, а також діагностики мереж і виявлення помилок в роботі мережевих пристроїв. Продукти SolarWinds використовують більше 90 тис. компаній, у тому числі MasterCard, Microsoft, Siemens, Nokia, Гарвардський університет, НАСА, державний департамент і міністерство оборони США. Одним з таких продуктів є Orion Network Performance Monitor (NPM) - потужний, але досить простий у використанні продукт, що надає важливу інформацію, яка необхідна для збереження контролю над мережею. Orion NPM дозволяє швидко виявляти, діагностувати і вирішувати проблеми продуктивності мережі і простої до того, як до вас почнуть надходити скарги на недоступність мережі. Orion NPM – це найпростіший у використанні та

обслуговуванні продукт. Це означає, що можна витрачати свій час на управління мережею, а не на підтримку програмного забезпечення для управління мережею. Крім того програма дозволяє відразу приступити до моніторингу, а не заповнювати технічні завдання для безлічі позицій [10].

Основні функції Orion NPM :

– моніторинг і аналіз докладної статистики мережевої продуктивності для маршрутизаторів, комутаторів, бездротових точок доступу, серверів і будь-яких інших пристроїв з підтримкою SNMP в режимі реального часу (рисунок 2.1).

– моніторинг серверів VMware і автоматичне відстеження продуктивності віртуальних машин за допомогою vCenter.

– безпроблемний моніторинг як віртуальних комутаторів Cisco Nexus 1000V, так і фізичних серверів;

– моніторинг проблем продуктивності VSAN і оптоволоконного каналу з повідомленнями на основі порогових значень в реальному часі і звітами про працездатність VSAN (рисунок 2.2);

– періодична перевірка змін у мережі, запити на моніторинг нових пристроїв, надання можливостей перегляду мережевих карт і динамічне відображення зв'язків між пристроями;

– розширення можливостей управління за допомогою аналізу трафіку NetFlow, моніторингу SLA IP, управління IP-адресами та управління конфігурацією мережі та моніторингу продуктивності додатків і сервера;

– графічне відображення мережі і можливість візуального відстеження статистики продуктивності в реальному часі з використанням динамічних карт мереж (рисунок 2.3);

– мониторинг EnergyWise для зменшення енергоспоживання пристроїв, підключених до мережі від пристроїв Power over Ethernet (PoE) (рисунок 2.4) [21].

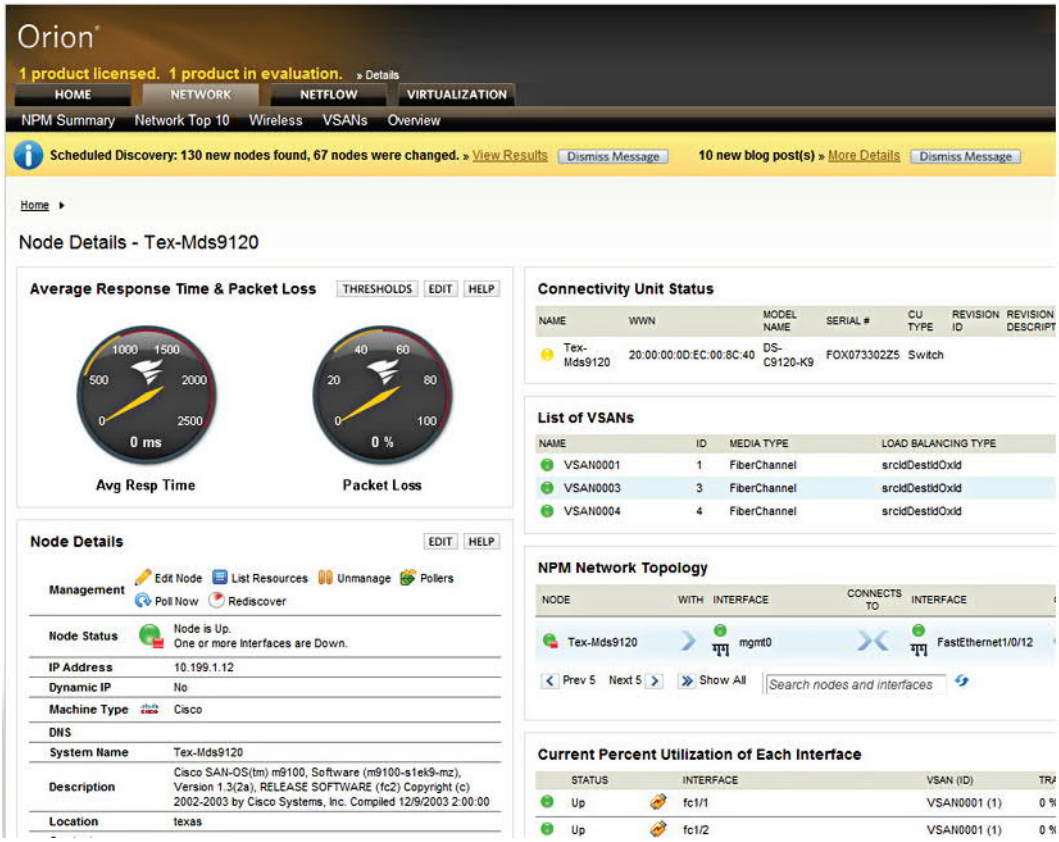

Рисунок 2.1 - Моніторинг мережі в ORION NPM SolarWinds.

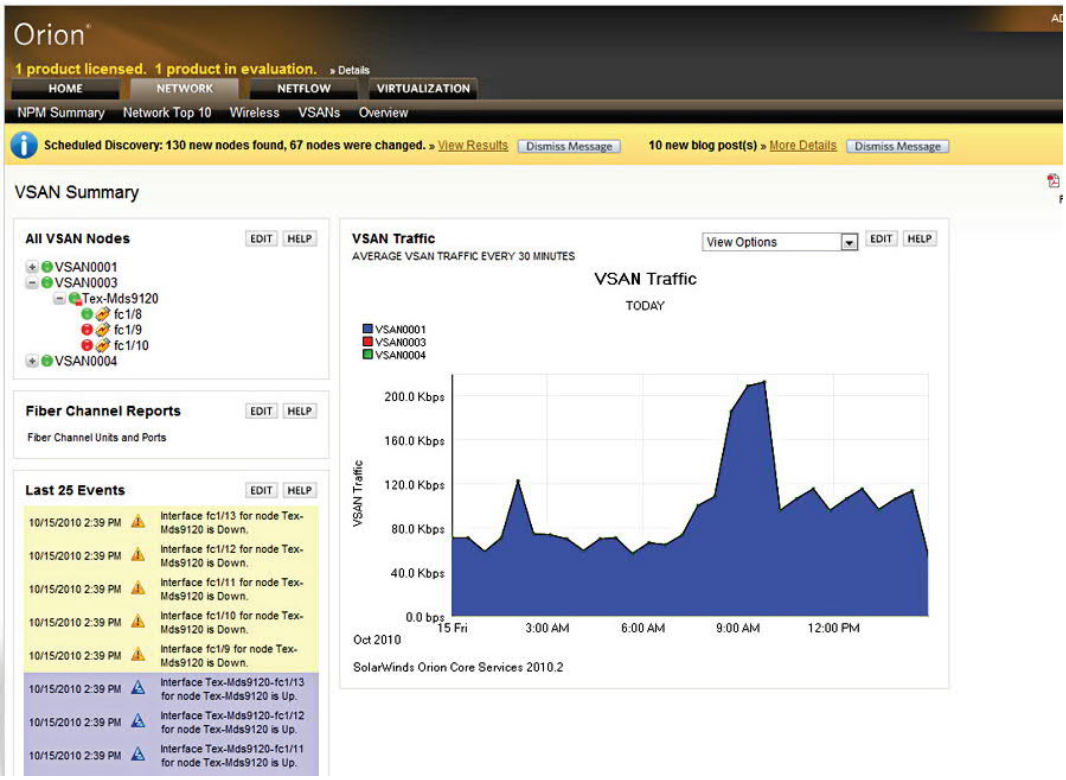

Рисунок 2.2 - Моніторинг проблем продуктивності в ORION SolarWinds.

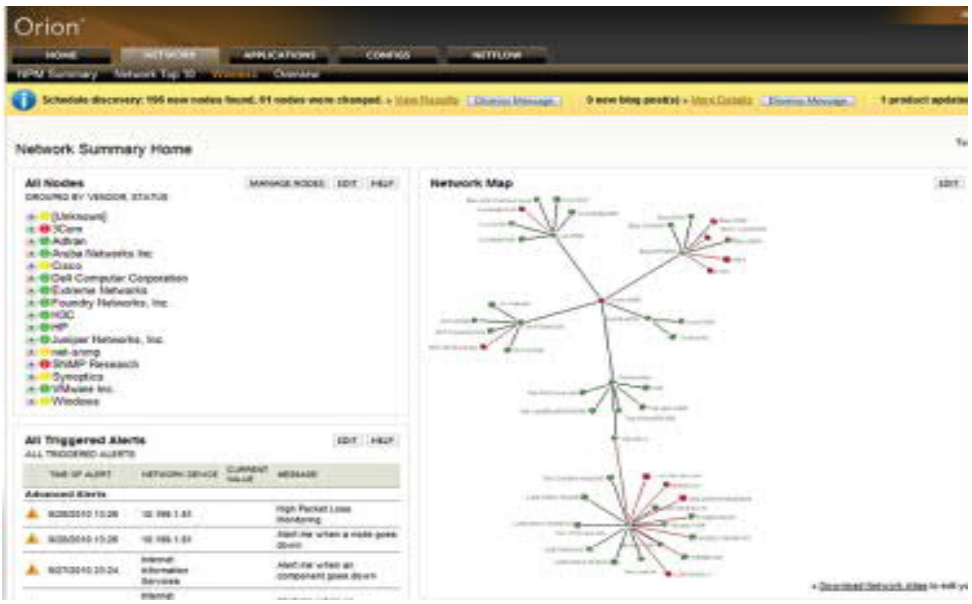

Рисунок 2.3 - Графічне відображення мережі в ORION SolarWinds.

Рисунок 2.4 - Мониторинг енергоспоживання пристроїв в ORION SolarWinds.

Окрім плюсів в роботі в ORION NPM SolarWinds є і один дуже суттєвий мінус. Продукт є платним. Для забезпечення стабільної роботи по моніторингу мережі в ТНЕУ потрібно заплатити від 2-2,5 тис. доларів, щоб отримати ліцензійний продукт. Так, як дуже дорого продукт неможливо використати в наших цілях. В ТНЕУ використовують безкоштовний продукт AP Manager.

Програма APM призначена для настройки і адміністрування точок доступу DWL2100AP, DWL3200AP, BlueBox, та інших. З її допомогою можна змінити основні настройки AP (точки доступу), провести пошук доступних мереж, а також виміряти рівень і якість сигналу. У програмі також реалізований інтерфейс telnet для доступу до AP з допомогою командного рядка [4].

Програма дуже зручна у використанні, за допомогою AP Manager непотрібно кожного разу згадувати IP-адрес роутера та його пароль, для входу. Це не дуже зручно і забиратиме багато часу, адже таких точок доступу в університеті близько 28 шт. (рисунок 2.5).

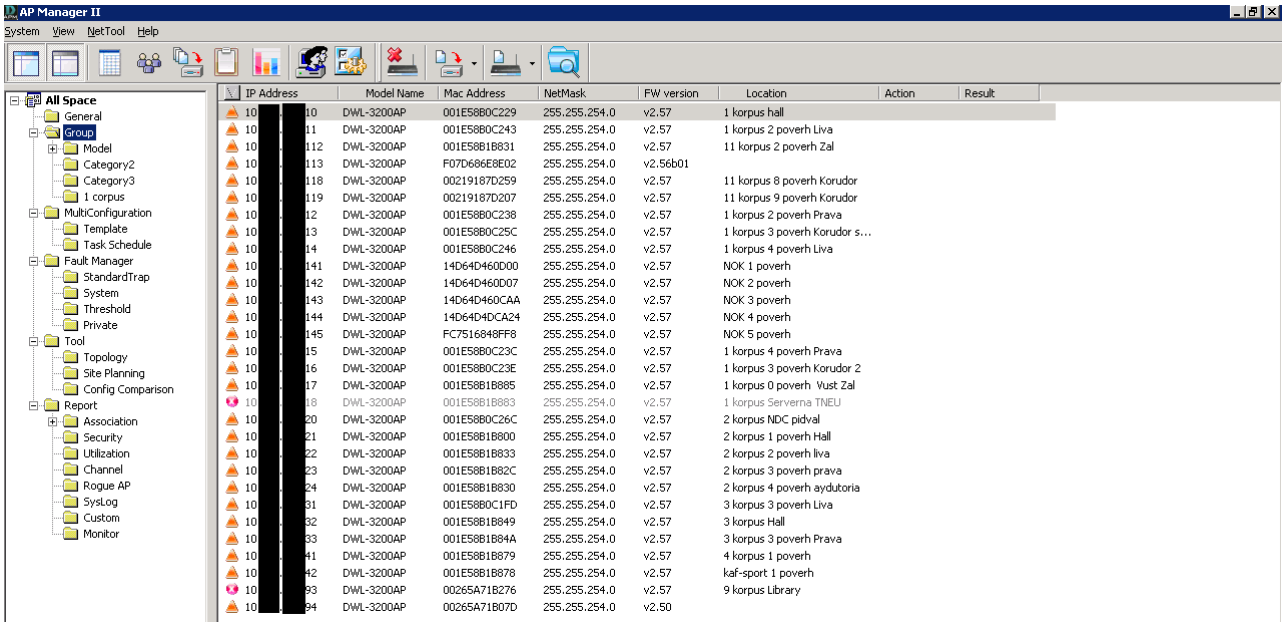

Рисунок 2.5 – Безпровідні точки доступу ТНЕУ в AP Manager.

IP Address – 10._._.31, де цифра 31 означає, що це точка доступу знаходиться в 3 корпусі на 1 поверсі.

NetMask – 255.255.254.0 – одинакова для всіх Wi-Fi роутерів в ТНЕУ.

Mac Address - це унікальний ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж. Адреси в кожному з просторів теоретично мають бути глобально унікальними. Тобто кожна точка доступу має свою унікальну Mac Address (наприклад, 01-23-45-67-89-AB)

Model Name – назва (ім’я) роутера. Всі точка доступу DWL-3200AP фірми D-Link, FW Version – версія прошивки роутера.

Для коректної роботи безпровідної мережі з роумінгом всі точки доступу повинні бути налаштовані в однин канал (рисунок 2.6). Видно, що всі 28 точок налаштовані в 10 каналі.

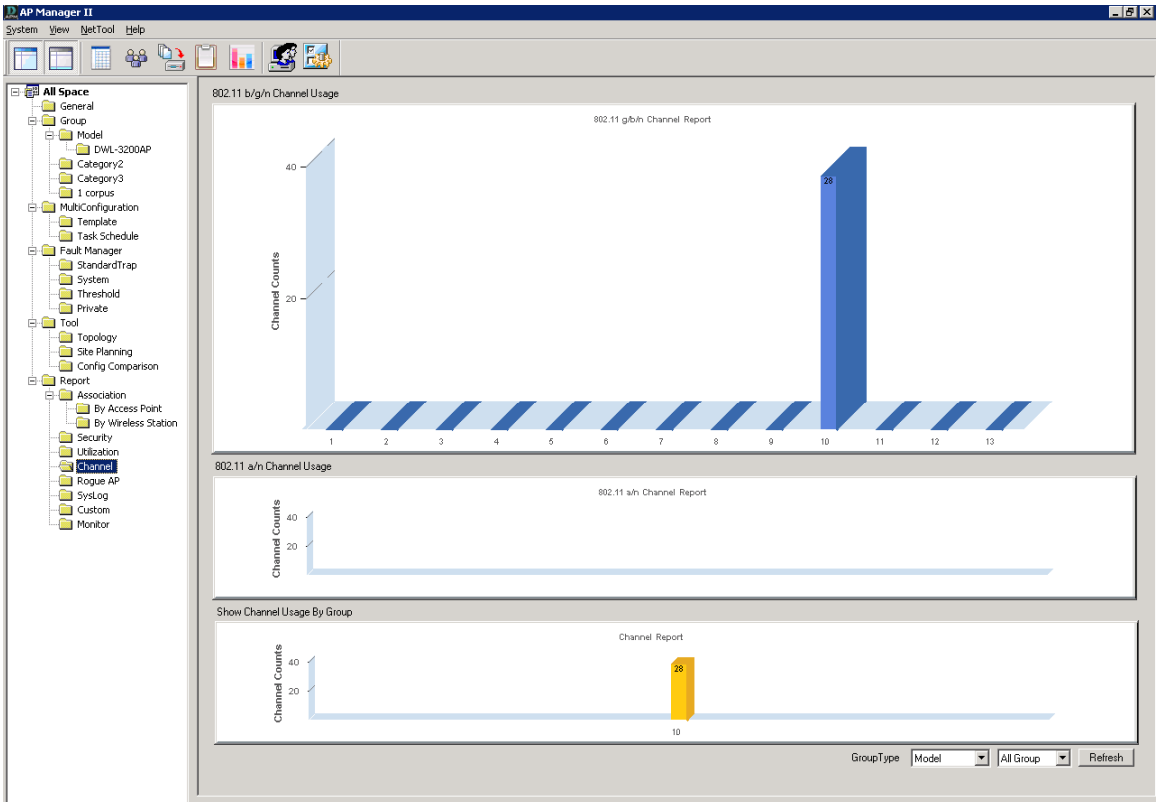

Рисунок 2.6 - Канал роботи безпровідних точок доступу ТНЕУ в AP Manager.

Також слід пам’ятати про захист Wi-Fi роутера Security Level (рисунок 2.7) - WEP, WPA чи WPA-2. Було проаналізовані всі протоколи безпеки бездротових мереж та вибрано – WPA-2 Personal, що відповідає рівню «6» в AP Manager ver 2, як видно, що на всіх 28 точок використано саме його.

У режимі WPA-2 Personal з введеної відкритим текстом фрази генерується 256 - розрядний ключ PSK (PreShared Key). Ключ PSK спільно з ідентифікатором SSID (Service Set Identifier) використовуються для генерації тимчасових сеансових ключів PTK, (Pairwise Transient Key) для взаємодії бездротових пристроїв. Як і статичному протоколу WEP, протоколу WPA-2

Personal притаманне певні проблеми, пов'язані з необхідністю розподілу та підтримки ключів на бездротових пристроях мережі, що робить його більш відповідним для застосування в невеликих мережах [2].

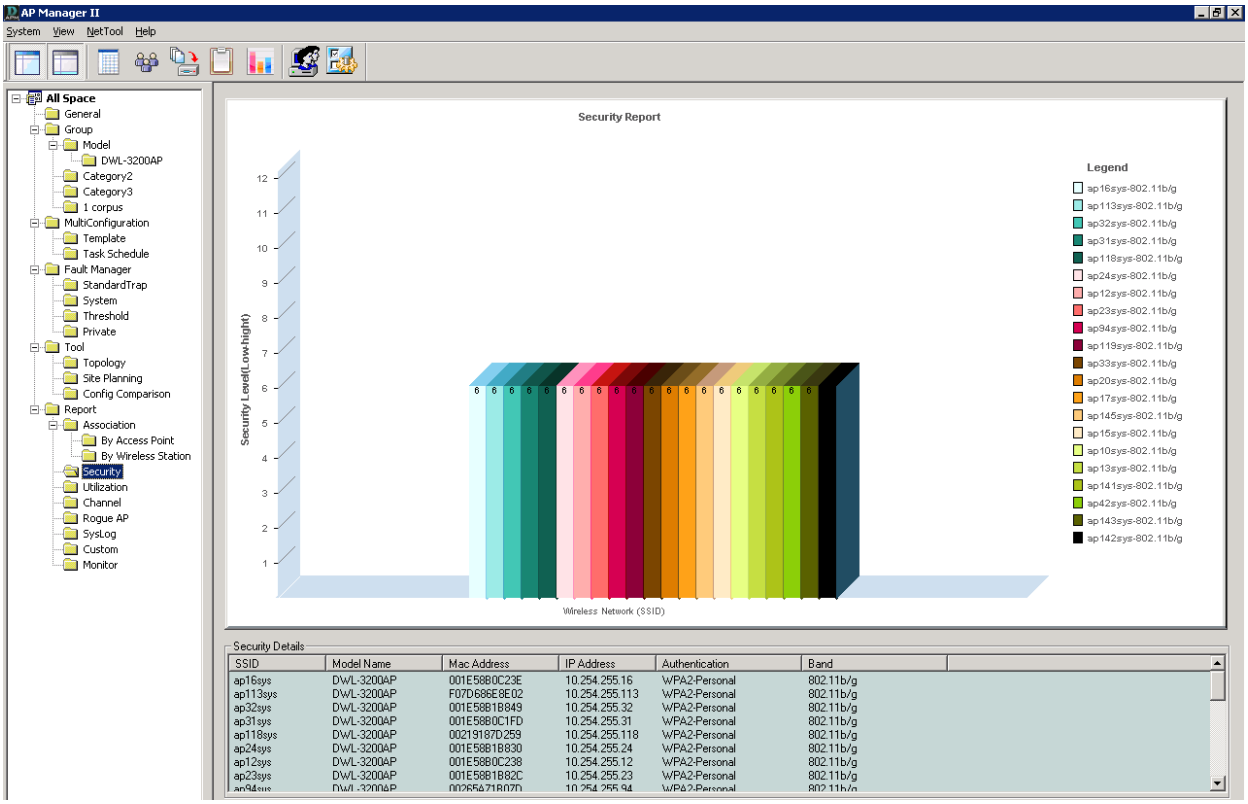

Рисунок 2.7 - Протокол безпеки бездротових мереж WPA-2 Pers. в AP Manager.

2.2 Система моніторингу, як засіб виявлення помилок в роботі безпровідної мережі в режимі онлайн.

Система моніторингу повинна виявляти помилки, та зміни в роботі Wi-Fi мережі в режимі онлайн. При винекленні неполадки адміністратору мережі повинно приходити сповіщення у вигляді листа на електронну пошту, дзвінка, чи смс повідомлення на мобільний телефон з відповідним текстом помилки. Одними з найпопулярніших програм для моніторигу є: Nagios та Zabbix.

Nagios - програма моніторингу комп'ютерних систем і мереж. Призначена для спостереження, контролю стану обчислювальних вузлів і служб, оповіщення адміністратора, якщо якісь із служб припиняють (або відновлюють) свою роботу [1].

Nagios спочатку була створена під ім'ям Netsaint, розроблена Етаном Ґалстадом. Він же підтримує і розвиває систему сьогодні, спільно з командою розробників, які займаються як офіційними, так і неофіційними плагінами. Спочатку Nagios була розроблена для роботи під Linux, але вона також добре працює і під іншими ОС, такими як Solaris, FreeBSD, AIX і HP-UX.

Згідно з офіційним FAQ Етана Ґалстада на сайті Nagios, NAGIOS це рекурсивний акронім Nagios Ain't Gonna Insist On Sainthood, розшифровка якого в перекладі звучить так: «Nagios не збирається наполягати на святості». Це камінь в город програми, що послужила основою для Nagios, Netsaint.

Базова функціональність системи реалізована у ядрі Nagios Core з відкритим сирцевим кодом, він ключає базовий рушій моніторингу та веб-інтерфейс для відстеження стану інфраструктури. Nagios Core є основою для серії комерційних продуктів. Комерційні надбудови надають такі можливості, як інтерфейс для конфігурації, підтримку SNMP Traps, мобільний застосунок, засоби моніторингу бізнес-процесів, графіки зміни продуктивності, підтримка зберігання даних в СУБД, аудит логів, додаткові звіти тощо. Тим не менш, багато з розширених можливостей можна отримати безплатно завдяки величезній колекції плагінів і таким доповненням/надбудовам, як Opsview, Monarch, Nconf, NCPL, Centreon, NagVis тощо [7].

Програма Nagios забезпечує :

– моніторинг мережевих служб (SMTP, POP3, HTTP, NNTP, ICMP, SNMP);

– моніторинг стану хостів (завантаження процесора, використання диска, системні логи) у більшості мережевих операційних систем;

– підтримку віддаленого моніторингу через шифровані тунелі SSH або SSL;

– просту архітектуру модулів розширень, що дозволяє, використовуючи будь-яку мову програмування за вибором (Shell, C++, Perl, Python, PHP, C# та інші), легко розробляти свої власні способи перевірки служб;

– паралельну перевірку служб;

– можливість визначати ієрархії хостів мережі за допомогою «батьківських» хостів, дозволяє виявляти і розрізняти хости, які вийшли з ладу, і ті, які недоступні;

– відправку оповіщень у разі виникнення проблем зі службою або хостом (за допомогою пошти, пейджера, смс, або будь-яким іншим способом, визначеним користувачем через модуль системи);

– можливість визначати обробники подій, що відбулися зі службами або хостами для активного вирішення проблем;

– автоматичну ротація лог-файлів;

– можливість організації спільної роботи декількох систем моніторингу з метою підвищення надійності і створення розподіленої системи моніторингу;

– включення в себе утиліту Nagiostats, яка виводить загальне зведення по всім хостам, за якими ведеться моніторинг (рисунок 2.8).

Іншою системою для моніторингу безпровідної мережі є Zabbix.

Zabbix - вільна система моніторингу та відстеження статусів різноманітних сервісів комп'ютерної мережі, серверів та мережевого обладнання, написана Олексієм Владишевим [38].

Для зберігання даних використовується MySQL, PostgreSQL, SQLite, або Oracle. Веб-інтерфейс написаний на PHP. Zabbix підтримує кілька видів моніторингу:

Simple checks - може перевіряти доступність і реакцію стандартних сервісів, таких як SMTP або HTTP без встановлення будь-якого програмного забезпечення на спостережуваному хості.

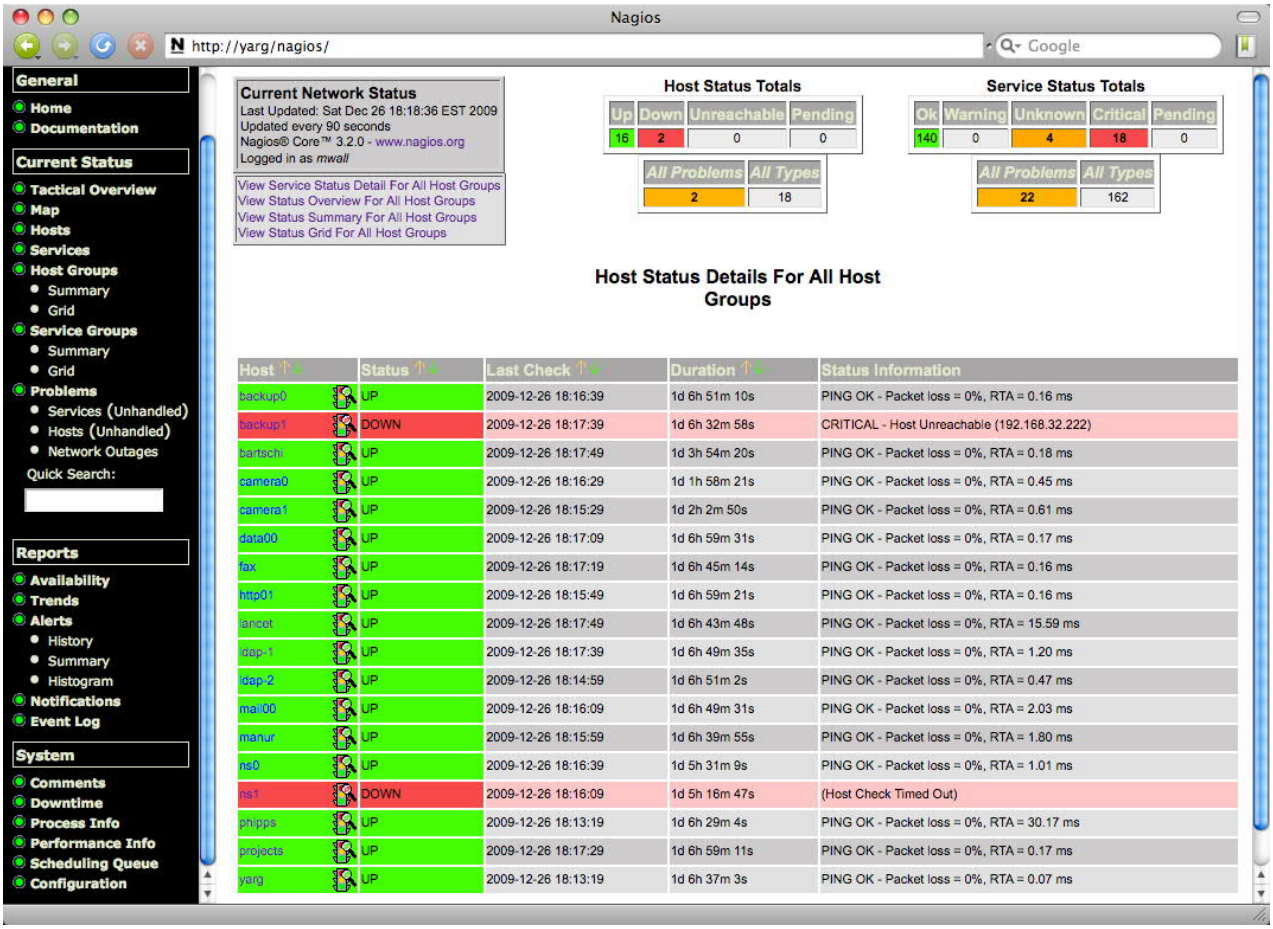

Рисунок 2.8 – Моніторинг безпровідної мережі в Nagios.

Zabbix agent - може бути встановлений на UNIX-подібних або Windows хостах для отримання даних про навантаження процесора, використання мережі, дисковому просторі і т. д.

External check - виконання зовнішніх програм. Zabbix також підтримує моніторинг через SNMP.

Zabbix складається з:

– власне сервера моніторингу, який виконує періодичне одержання даних, обробку, аналіз і запуск скриптів оповіщення;

– бази даних (MySQL , PostgreSQL , SQLite або Oracle);

– web інтерфейсу на PHP;

– агента - демона, який запускається на що відслідковуються об'єктах і надає дані серверу.

Моніторинг можна проводити не тільки за допомогою нього, а й по SNMP (версій 1, 2, 3), запуском зовнішніх скриптів, що видають дані та кілька видів зумовлених вбудованих перевірок, таких як ping, запит по http , ssh , ftp і інших протоколах, а так само виміру часу відповіді цих сервісів.

Zabbix по даними будь-якого параметра зможе побудувати графік зміни за будь-який проміжок часу з максимальною роздільною здатністю (рисунок 2.9) [14].

Рисунок 2.9 – Графік зміни стану безпровідної мережі в Zabbix.

Для відображення логічної структури мережі можна створювати карти мережі, що відображають саме розташування вузлів мережі та зв'язків між ними. Природно, стан вузлів (доступний чи ні) відображається і на карті (рисунок 2.10).

Zabbix - досить велика і потужна і система, з набором функцій, які дозволяють ще більше спростити спостереження за мережею.

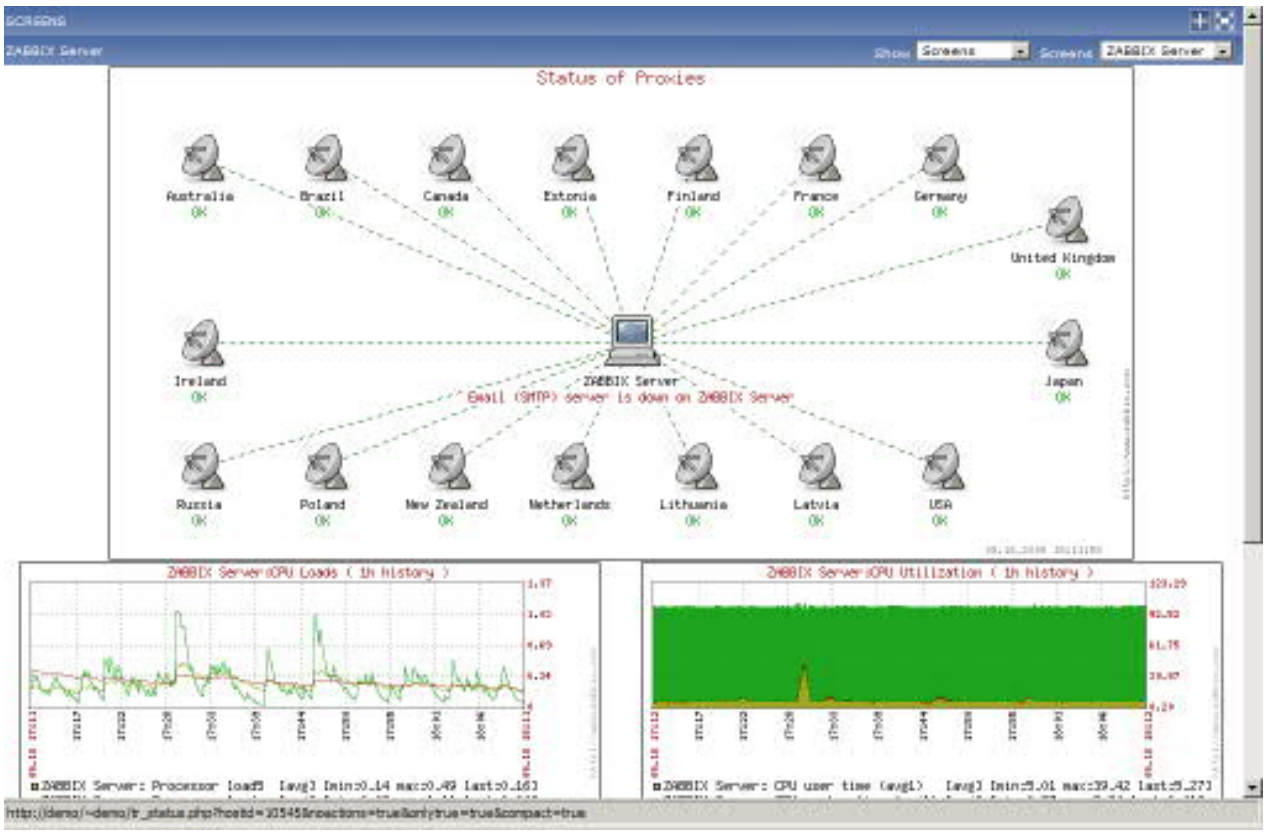

Рисунок 2.10 – Карта стану вузлів безпровідної мережі в Zabbix.

Програма Zabbix забезпечує :

– розподілений моніторинг аж до 1000 вузлів. Конфігурація молодших вузлів повністю контролюється старшими вузлами , що знаходяться на більш високому рівні ієрархії;

– сценарії на основі моніторингу;

– автоматичне виявлення помилок;

– централізований моніторинг лог файлів;

– веб інтерфейс для адміністрування та налаштування;

– звітність по моніторингу мережі;

– SLA моніторинг;

– підтримку високопродуктивних агентів для всіх платформ;

– комплексну реакція на подій;

– підтримку SNMP v 1, 2, 3;

– підтримку SNMP трапів;

– підтримку IPMI;

– підтримку моніторингу JMX додатків;

– підтримку виконання запитів в різні бази даних;

– розширення за рахунок виконання зовнішніх скриптів;

– гнучка система шаблонів і груп;

– можливість створювати карти мереж;

– автоматичне виявлення помилок за діапазоном IP-адрес, доступним сервісам і SNMP перевірку;

– автоматичний моніторинг виявлених пристроїв;

– автоматичне видалення відсутніх хостів;

– розподіл за групами та шаблонами залежно від кінцевого результату.

2.3 Система проектування безпровідної мережі

Існує багато різних систем для проектування чи то локальної, чи бездротової мережі. В роботі ж ми розглянемо Експерт СКС та NetCracker Professional.

Експерт СКС - дозволяє в повному обсязі автоматизувати всі етапи проектування СКС як цілісної системи. Надасть допомогу в коректному застосуванні обладнання і технології відомих виробників. Комплексний підхід до проектування та параметризації дозволить у декілька разів швидше розробляти проекти комп’ютерних систем, істотно підвищити якість виконуваних робіт, контролювати інсталяції та впровадження.

У кілька разів збільшить швидкість розробки проектів, а зміни в діючий проект зможуть бути внесені миттєво з перерахунком всіх результатів. Всю роботу по контролю, що раніше робили вручну: пояснювальні записки, специфікації, кабельні журнали, відомості ресурсів, відомості норм (робіт),

креслення шаф, креслення схем будівель, відомості кабелів і кабельних каналів система формує автоматично.

Експерт СКС включає в себе:

– графічну САПР оболонку;

Повний функціонал для проектування вихідних архітектурних, та інших схем. Підготовлений заздалегідь план можна імпортувати як через стандартні векторні файли обміну (*.dxf , *.wmf , та інші) так і використовуючи сканований файл.

– інтелектуальну підсистему проектування СКС;

Проектування СКС будь-якого виду на вихідному плані. Розстановка робочих місць і шаф (точкових елементів), прокладання трас і кабелів (в т.ч. автотрасування), вкладання коробів, розподіл підключень, формування міжповерхових переходів і переходів між будівлями. Підсистема компоновки шаф дозволяє у візуальному режимі проектувати розподільні шафи .

– базу даних стандартних виробів відомих виробників;

Надає можливість знаходити, компонувати і розставляти складальні вузли на робочому плані. Закладена в базі інформація включає багато технічних даних і цін.

– менеджер проекту - деревоподібну ієрархію розробленої СКС.

Надає можливість навігації і коректування готової структурованої кабельної системи . Дозволяє формувати проекти з будь-якою кількістю рівнів вкладеності. Включає підсистему конфігурацій підключень для контролю і зміни підключень, сформованих в проекті.

Модуль випуску розрахункових документів включає випуск графічної документації (плани і креслення), і текстових розрахункових документів (відомості, специфікації, журнали, тощо). Приклад проекту бездротової мережі в «Експерт- СКС» зображено на рисунку 2.11 [40].

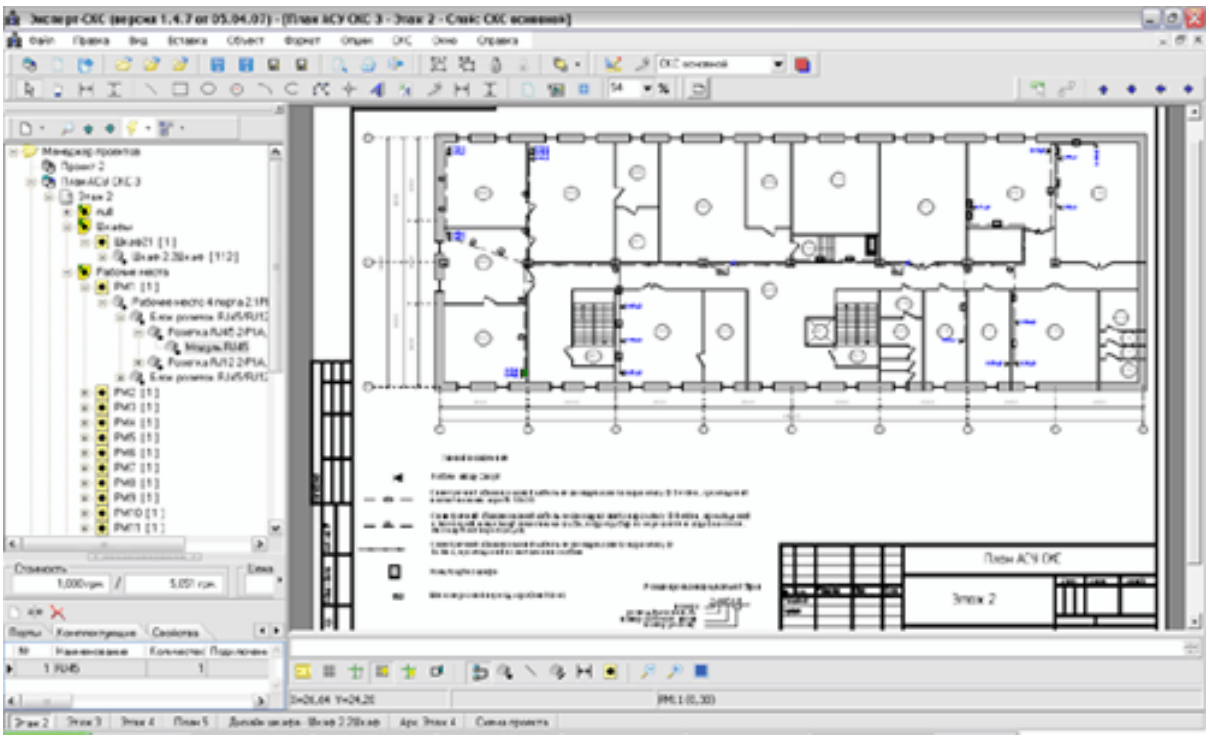

Рисунок 2.11 – Приклад проекту бездротової мережі в «Експерт- СКС».

Іншою системою для проектування КС є NetCracker. Система являє собою CASE - засоби автоматизованого проектування, моделювання та аналізу комп'ютерних мереж. Дозволяє провести експерименти, результати яких можуть бути використані для обґрунтування вибору типу мережі, середовищ передачі, мережевих компонент обладнання та програмно-математичного забезпечення.

Програмні засоби NetCracker дозволяють виконати збір відповідних даних про існуючої мережі без зупину її роботи, створити проект цієї мережі і виконати необхідні експерименти для визначення граничних характеристик, можливості розширення, зміни топології і модифікації мережного обладнання з метою подальшого її вдосконалення та розвитку [8].

За допомогою NetCracker можна проектувати комп'ютерні мережі різного масштабу (рисунок 2.13) і призначення: від локальних мереж, що нараховують кілька десятків комп'ютерів, до міждержавних глобальних мереж, побудованих з використанням супутникового зв'язку. У складі програмного забезпечення NetCracker є потужна база даних мережевих пристроїв провідних

виробників: робочих станцій, серверів, середовищ передачі, мережевих адаптерів, повторювачів, мостів, комутаторів, маршрутизаторів, використовуваних для різних типів мереж і мережевих технологій .

NetCracker дозволяє розробляти багаторівневі проекти із заданою проектувальником ступенем деталізації; при цьому має досить зручний інтерфейс і засоби швидкого перегляду всіх рівнів проекту. Для реалізацій функцій імітаційного моделювання у складі NetCracker передбачені засоби візуального контролю заданих параметрів; засоби накопичення статистичної інформації та формування звітної документації про проведені роботи [9].

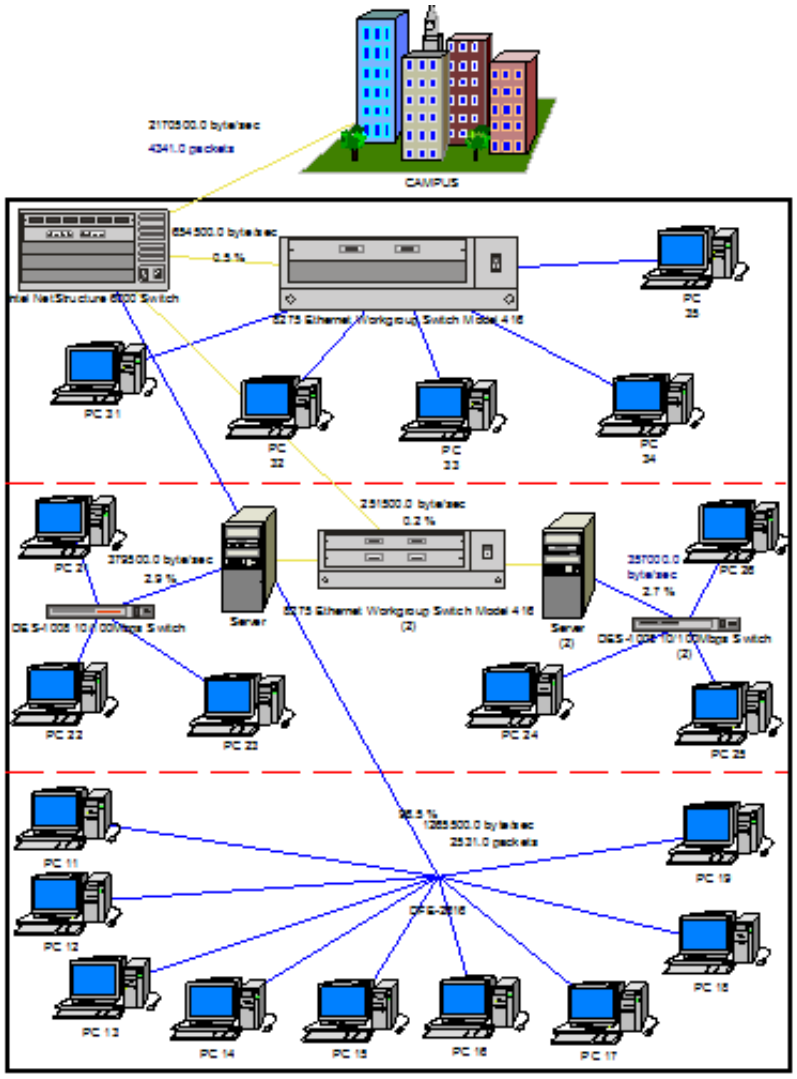

Рисунок 2.12 - Проектування комп'ютерні мережі в NetCracker.

3 ПРОЕКТУВАННЯ БЕЗПРОВІДНОЇ МЕРЕЖІ З РОУМІНГОМ НА ПРИКЛАДІ НАВЧАЛЬНОГО КОРПУСУ №3 ТНЕУ

3.1 Схема підключення Інтернет у ТНЕУ

Для стабільної роботи мережі Інтернет в університеті виділено 3 канали. Це BitterNet (100 Мбіт/с), Datagroup (150 Мбіт/с), UarNet (150 Мбіт/с). Канали прокладені оптоволокном, до головного сервера в корпусі №1 ТНЕУ (рисунок 3.1), від якого вже мережа розгалужується по всіх корпусах, гуртожитках, та філіях університету.

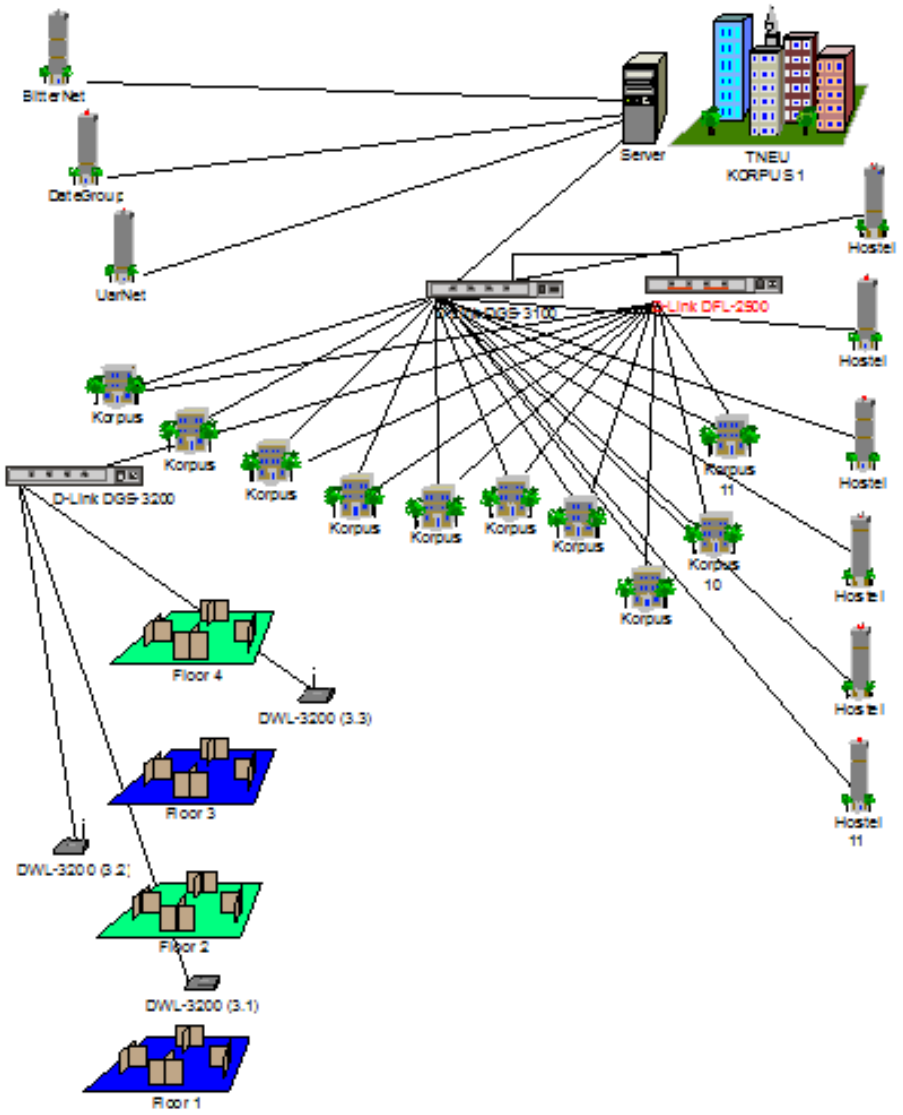

Рисунок 3.1 - Схема підключення Інтернет у ТНЕУ.

Канал Datagroup – основний Інтернет канал в університеті, до якого мають доступ як викладачі так і студенти університету (лабораторії, відділи, центри). Підключення до мережі відбувається через прокосі-сервер - сервер (комп'ютерна система або програма) в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі (через посередництво проксі-сервера) запити до мережевих сервісів. Спочатку клієнт з'єднується з проксі-сервером і запитує який-небудь ресурс (наприклад, e-mail), розташований на іншому сервері. Потім proxy сервер або підключається до вказаного сервера і отримує ресурс у нього, або повертає ресурс з власного кешу (у випадках, якщо proxy має свій кеш). У деяких випадках запит клієнта або відповідь сервера може бути змінена проксі-сервером з певною метою. Також proxy сервер дозволяє захищати клієнтський комп'ютер від деяких мережевих атак. Кожен користувач мережі має свій логін і пароль для входу (рисунок 3.2), ведеться статистика по кожному з користувачів (рисунок 3.3).

Рисунок 3.2 – Користувач proxy серверу.

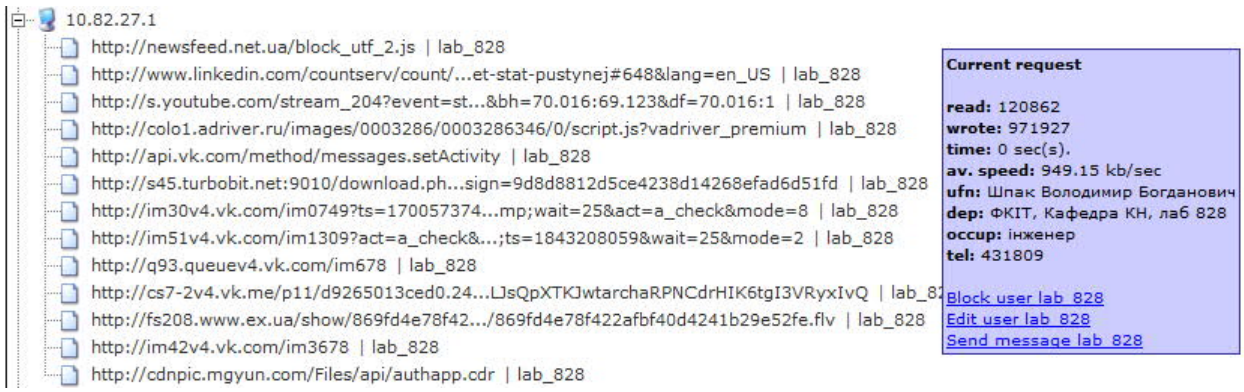

Рисунок 3.3 – Статистика роботи користувача lab_828.

Канал UarNet є резерним каналом, при виході з ладу основного, робота мережі не припиняються, а автоматично переходять в режим роботи з провайдером UarNet. Канал BitterNet використовується для Wi-Fi мережі по університету. Інтернет трафік проходить через міжмережевий екран (фаєрвол) D-Link DFL-2500 (рисунок 3.4).

Рисунок 3.4 - Міжмережевий екран D-Link DFL-2500.

Фаєрвол – пристрій або набір пристроїв, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати через proxy весь комп'ютерний трафік між областями різної безпеки згідно з набором правил.

Фаєрвол може бути у вигляді окремого приладу (маршрутизатор або роутер), або програмного забезпечення, що встановлюється на персональний комп'ютер чи проксі-сервер. Простий та дешевий фаєрвол може не мати такої

гнучкої системи налаштувань правил фільтрації пакетів та трансляції адрес вхідного та вихідного трафіку [3].

В залежності від активних з'єднань, що відслідковуються, фаєрволи розділяють на:

– stateless (проста фільтрація);
– stateful (фільтрація з урахуванням контексту).

Для того щоб задовольнити вимогам широкого кола користувачів, існує три типи фаєрволів: мережного рівня, прикладного рівня і рівня з'єднання. Кожен з цих трьох типів використовує свій, відмінний від інших підхід до захисту мережі.

Від фаєрволу, мережа розводиться до головних комутаторі (DES-1210, DES-3100, DES-3200,) корпусів та гуртожитків по оптоволоконному кабелю. І вже від так званих «розумних» свічів, мережа розводиться до свічів (DES-1008, DES-1024 та інші) та Wi-Fi точок доступу - D-Link DWL-3200 (рисунок 3.4) і до ПК, ноутбуків, планшетних комп'ютерів, смартфонів та інше.

Рисунок 3.5 - D-Link DWL-3200.

Безпровідні Wi-Fi адаптери D-Link DWL-3200 (Додаток Е) підключаються в мережу за допомогою PoE (рисунок 3.6). Power over Ethernet - технологія, що дозволяє передавати віддаленого пристрою електричну енергію разом з даними, через стандартну виту пару в мережі Ethernet. Дана технологія

призначається для IP-телефонії, точок доступу бездротових мереж, IP-камер, мережевих концентраторів та інших пристроїв, до яких небажано або неможливо проводити окремий електричний кабель [20].

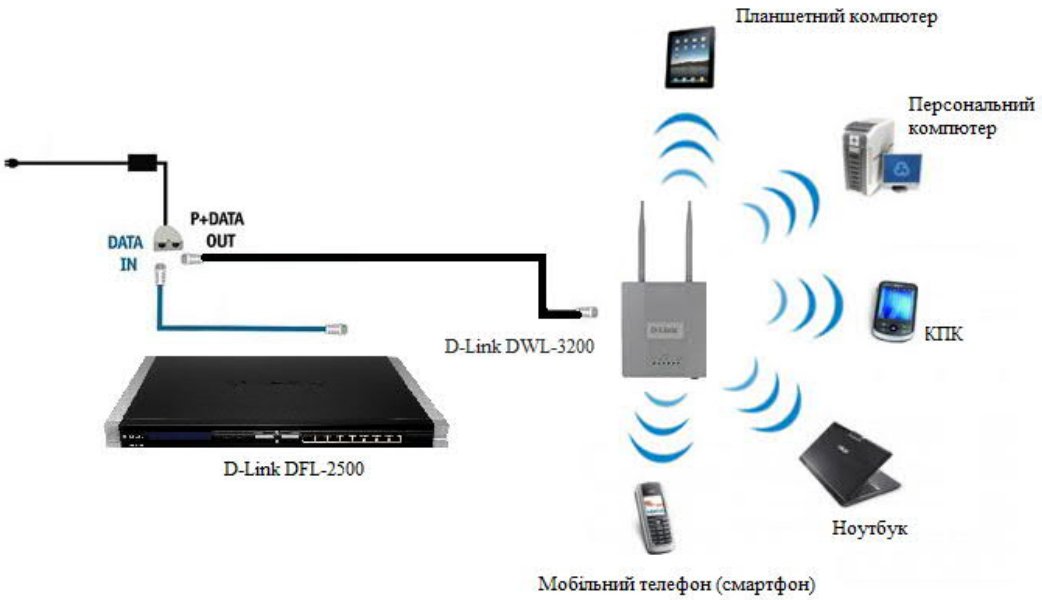

Рисунок 3.6 – Підключення D-Link DWL-3200 по PoE.

3.2 Налаштування Wi-Fi роутерів у VLAN

VLAN (від англ. Virtual Local Area Network) - логічна («віртуальна») локальна комп'ютерна мережа, що має ті ж властивості, що й фізична локальна мережа. Простіше кажучи, VLAN - це логічний канал всередині фізичного [12].

Дана технологія дозволяє виконувати два протилежні завдання:

1) групувати пристрої на канальному рівні (тобто пристрої, що знаходяться в одному VLAN), хоча фізично при цьому вони можуть бути підключені до різних мережевих комутаторів (розташованим, наприклад, географічно віддалено);

2) розмежовувати пристрої (знаходяться в різних VLAN), підключені до одного комутатора.

Інакше кажучи, VLAN дозволяють створювати окремі широкомовні домени. Мережа будь-якого великого підприємства, чи установи не може функціонувати без застосування VLAN.

Застосування даної технології дає нам такі переваги:

– угруповання пристроїв (наприклад, серверів) по функціоналу;

– зменшення кількості широкомовного трафіку в мережі, тому що кожен VLAN - це окремий широкомовний домен;

– збільшення безпеки і керованості мережі (як наслідок перших двох переваг) [16].

Простий приклад: припустимо, є хости, включені в комутатор, який, у свою чергу, приєднаний до маршрутизатора (рисунок 3.7) . Припустимо, у нас є дві локальні мережі, з'єднані одним комутатором і виходять в Інтернет через один роутер. Якщо не розмежувати мережі по VLAN, то, по-перше, мережевий шторм в одній мережі буде впливати на другу мережу, по-друге, з кожної мережі можна буде «виловлювати» трафік іншої мережі. Тепер же, розбивши мережу на VLAN, ми фактично отримали дві окремі мережі, пов'язані між собою роутером, тобто L3 (мережевим рівнем) . Весь трафік проходить з однієї мережі в іншу через роутер, а доступ тепер працює тільки на рівні L3, що значно полегшує роботу адміністратора [32].

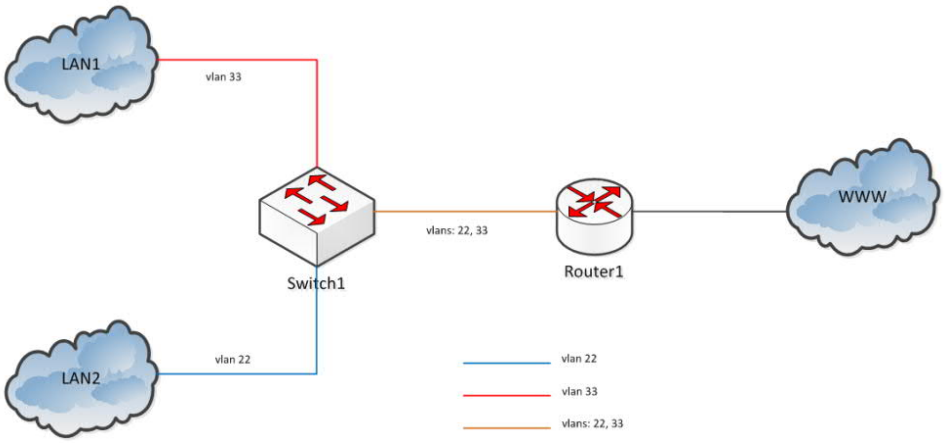

Рисунок 3.7 – Приклад мережі VLAN.

Процес додавання мітки VLAN (він же тег) до фреймів трафіку - тегування.

Як правило, кінцеві хости не тегують трафік (наприклад, комп'ютери користувачів). Цим займаються комутатори, що стоять в мережі. Більш того, кінцеві хости і не підозрюють про те, що вони знаходяться в такому-то VLAN. Строго кажучи, трафік в різних VLAN чимось особливим не відрізняється.

Якщо через порт комутатора може прийти трафік різних VLAN, то комутатор повинен його якось розрізняти. Для цього кожен кадр повинен бути позначений міткою .

Найбільшого поширення набула технологія, описана у специфікації IEEE 802.1Q. Також існую і інші пропрієтарні протоколи (специфікації).

802.1Q - це відкритий стандарт, що описує процедуру тегування трафіку.

Для цього в тіло фрейма поміщається тег (рисунок 3.8), що містить інформацію про приналежність до VLAN. Так тег поміщається в тіло, а не в заголовок фрейма, пристрої, які не підтримують VLAN, пропускають трафік прозоро, тобто без урахування його прив'язки до VLAN [27].

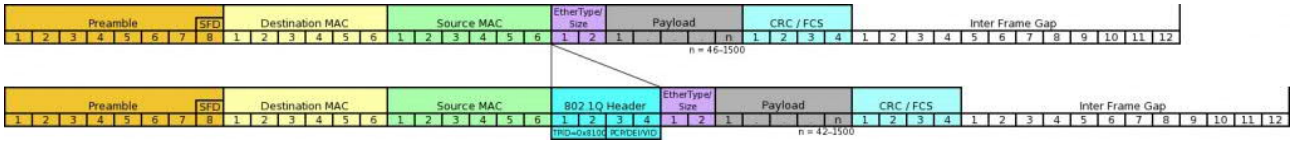

Рисунок 3.8 – Тег, що містить інформацію про приналежність до VLAN.

Розмір мітки (тега) всього 4 байт. Складається з 4-х полів (рисунок 3.9) :

– Tag Protocol Identifier (TPID, ідентифікатор протоколу тегування);

Розмір поля - 16 біт. Вказує на те, який протокол використовується для тегування. Для 802.1Q використовується значення 0×8100.

– Priority (Пріоритет);

Розмір поля - 3 біта. Використовується стандартом IEEE 802.1p для задання пріорітету переданого трафіку.

– Canonical Format Indicator (CFI, індикатор канонічного формату);

Розмір поля - 1 біт. Вказує на формат MAC - адреси . 0 - канонічній, 1 - не канонічній. CFI використовується для сумісності між мережами Ethernet и Token Ring.

– VLAN Identifier (VID, ідентифікатор VLAN).

Розмір поля - 12 біт. Вказує на те, якому VLAN належить фрейм . Діапазон можливих значення - від 0 до 4095 .

Рисунок 3.9 – Розмір тега, що містить інформацію про приналежність до VLAN

Якщо трафік тегується, або навпаки - мітка забирається, то контрольна сума кадру перераховується (CRC).

Стандарт 802.1q також передбачає позначення VLAN трафіку, що йде без тега, тобто не тегований. Цей VLAN називається нативним VLAN, за замовчуванням це - VLAN 1. Це дозволяє вважати тегований трафік, який в реальності тегованим не був.

802.1ad - це відкритий стандарт (аналогічно 802.1q), що описує подвійний тег (рисунок 3.10). Також відомий як Q-in-Q, або Stacked VLANs. Основна відмінність від попереднього стандарту - це наявність двох VLAN - зовнішнього і внутрішнього, що дозволяє розбивати мережа не на 4095 VLAN, а на 4095x4095.

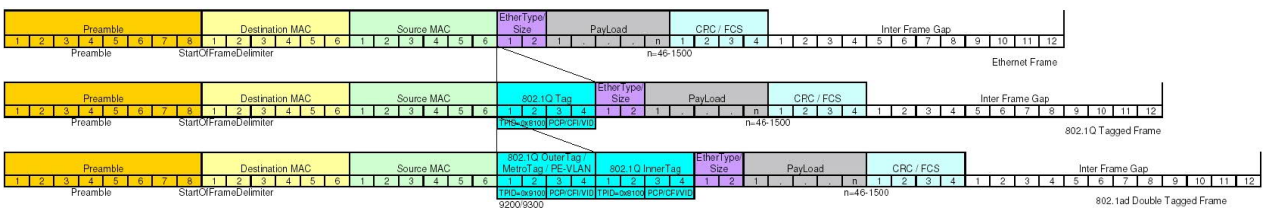

Рисунок 3.10 – Відкритий стандарт 802.1ad, що описує подвійний тег.

Так само наявність двох міток дозволяє організовувати більш гнучкі і складні мережі оператора. Також бувають випадки, коли операторові потрібно організувати L2 з'єднання для двох різних клієнтів в двох різних містах, але клієнти посилають трафік з одним і тим же тегом (рисунок 3.11).

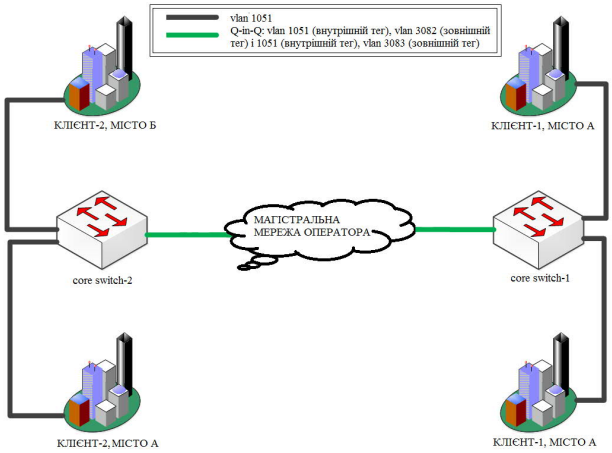

Рисунок 3.10 - З'єднання для двох різних клієнтів в двох різних містах.

Клієнт - 1 і клієнт - 2 мають філії в місті А і Б, де є мережа одного провайдера. Обом клієнтам необхідно пов'язати свої філії в двох різних містах. Крім того, для своїх потреб кожен клієнт тегує трафік 1051 VLAN. Відповідно, якщо провайдер буде пропускати трафік обох клієнтів через себе в одному єдиному VLAN, помилка в роботі одного клієнта може відобразитися на роботі другого клієнта. Більш того, трафік одного клієнта зможе перехопити інший клієнт. Для того, щоб ізолювати трафік клієнтів, оператору (адміністратору) найпростіше використовувати Q-in-Q. Додавши додатковий тег до кожного окремого клієнта (наприклад, 3083 до клієнта - 1 і 3082 до клієнта - 2), оператор ізолює клієнтів один від одного, і клієнтам вже не доведеться міняти тег.

Залежно від виконуваної операції з VLAN порти комутатора діляться на два види :

– тегований (trunk порт) - порт , який пропускає трафік тільки з певним тегом;

– не тегований (access порт) - входячи в даний порт, не тегований трафік в тег.

Існує два підходи для призначення порту в певний VLAN:

– статичне призначення - коли приналежність порту VLAN задається адміністратором;

– динамічне призначення - коли приналежність порту VLAN визначається в ході роботи комутатора за допомогою процедур, описаних в спеціальних стандартах, таких, наприклад, як 802.1X .

Для розуміння процесу комутації з VLAN розглянемо таблиці комутації без використанні VLAN і з використанням VLAN. Таблиця 3.1 виглядає наступним чином:

Таблиця 3.1 – Комутація без використання VLAN

ПОРТ	MAC-адрес
1	A
2	B
2	C

Якщо ж комутатор підтримує VLAN, то таблиця 3.2 комутації буде виглядати таким чином:

Таблиця 3.2 – Комутація з використанням VLAN

ПОРТ	VLAN	MAC-адрес
1	345	A
2	879	B
3	default	C

В таблиці 3.2 значенні default - Native VLAN (нативний VLAN).

Існує кілька протоколів, які працюють з VLAN, а саме:

– GVRP - протокол, що працює на канальному рівні, робота якого зводитися до обміну інформації про наявні VLAN;

– MSTP - протокол, модифікація протоколу STP, що дозволяє будувати «дерево» з урахуванням різних VLAN;

– LLDP - протокол для обміну описової інформацією про мережу, окрім інформації про VLAN, а також поширює інформацію і про інші налаштування [36].

Отже, VLAN розділятиме безпровідну мережу від загально університетської мережі, тобто зловмисник, який зможе зламати Wi-Fi (отримає доступ до роутера) буде ізольованим від 1С бухгалтерії, та не зможе отримати доступ до інших важливих серверів (як то документообіг та інше).

3.3 Реалізація безпровідної мережі навчального закладу з роумінгом

Для реалізація безпровідної мережі та здобуття навичок по проектуванні горизонтальної і вертикальної кабельної системи було змодельовано відповідну Wi-Fi Lan за допомогою програми NET CRACKER 4.1.

Завданням роботи є схематична побудова 5-ох поверхової будівлі корпусу №3, та розвід магістральної та вертикальної кабельної системи, а також проектування горизонтальної кабельної системи кожного поверху будівлі.

Від головного свіча корпусу №1 мережа прокладена до шаф правого і лівого крила корпусу №3, для прокладення використаний оптичний кабель, який підтримує канал в 1 гігабіт (рисунок 3.11). Від свіча правого каналу мережа розгалужена по всьому правому крилі корпусу, підключені кафедри, бібліотека, читальний зал, лінгафонний кабінет, АТС, банкомат, і 4 Wi-Fi точки доступу, які розташовані на 2,3,4,5 поверхах. Від свіча лівого крила мережа проведена до архіву, деканату, комп’ютерної лабораторії, та кафедр, а також 3 Wi-Fi точки доступу на 1,2 і 4 поверху корпусу.

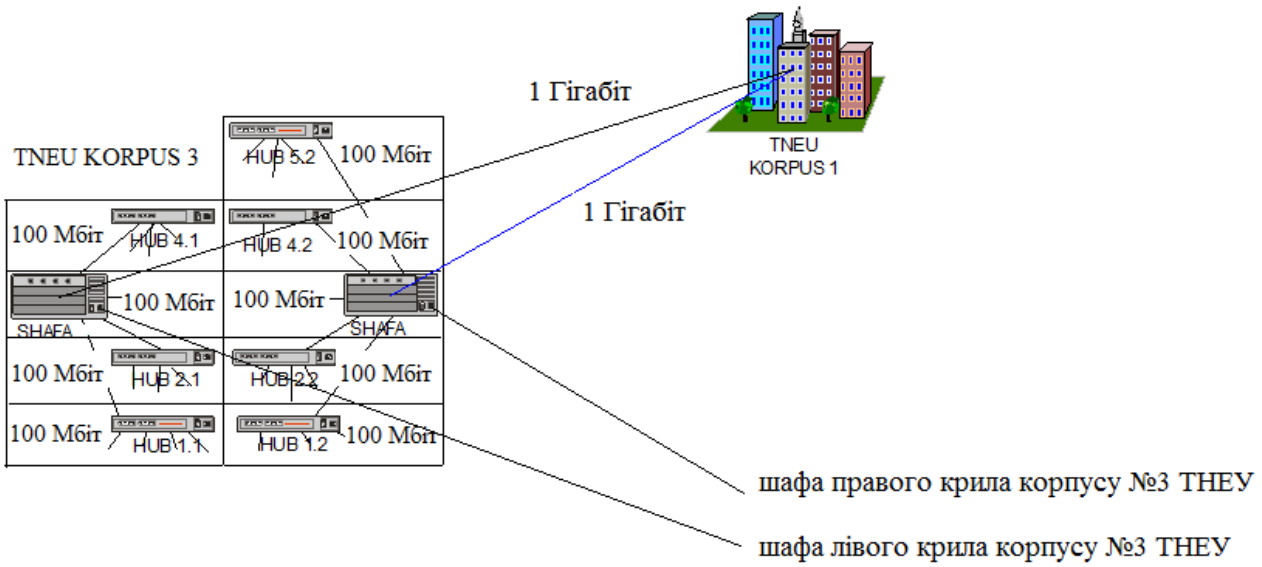

Рисунок 3.11 – Мережа правого і лівого крила корпусу №3 ТНЕУ

Мережа Wi-Fi розташована в іншому VLAN від загальноуніверситетської мережі та каналу до якого підключений банкомат, таким чином зменшується ризик мережі бути зламаною (рисунок 3.12).

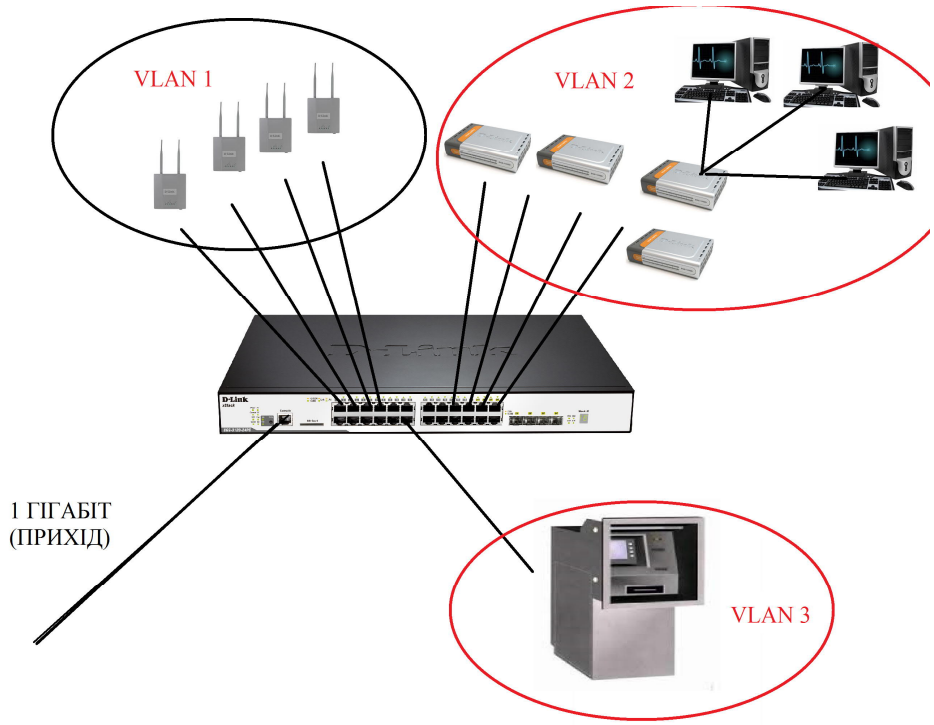

Рисунок 3.12 – Підмережі VLAN

Wi-Fi точки, які розташовані на 1-5 поверхах (Додаток А-Д) розташовані таким чином, що Wi-Fi зона перекриється все приміщення навчального корпусу.

Для нормального функціонування безпровідної мережі з роумінгом у навчальному корпусі №3 Тернопільського національного економічного університету нам потрібно 7 точок доступу D-Link DWL-3200 (рисунок 3.13) , які живляться від PoE (рисунок 3.13), це означає, що до Wi-Fi роутера нам прийдеться завести лише один кабель (вита пара) категорії 5е. Це значно зменшить затрати при монтажі бездротової мережі, але слід пам’ятати, що відстань від розетки живлення до точки доступу не повинна перевищувати 100 метрів. Ціна D-Link DWL-3200 - близько 100 $.

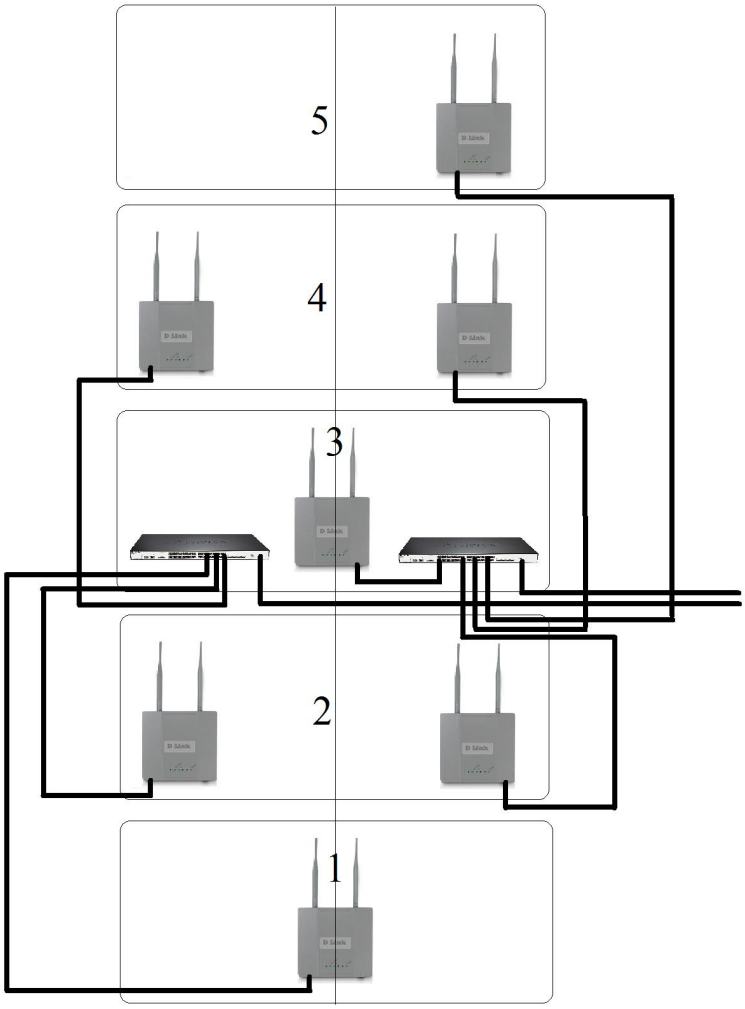

Рисунок 3.13 – Безпровідна мережа корпусу №3 ТНЕУ

Рисунок 3.14 – Адаптер Power over Ethernet

Для налаштування для налаштування точки доступ D-Link DWL-3200 потрібно підключитися за допомогою мережевого кабелю (пачкорд), або за допомогою Wi-Fi до мережі, яка по замовчуванні буде називатися dlink. Після підключення потрібно в браузері ввести IP адресу – 192.168.0.50, та Ім’я користувача – admin, значення комірки - Пароль залишаємо порожнім, як і вказано на рисунок 3.15.

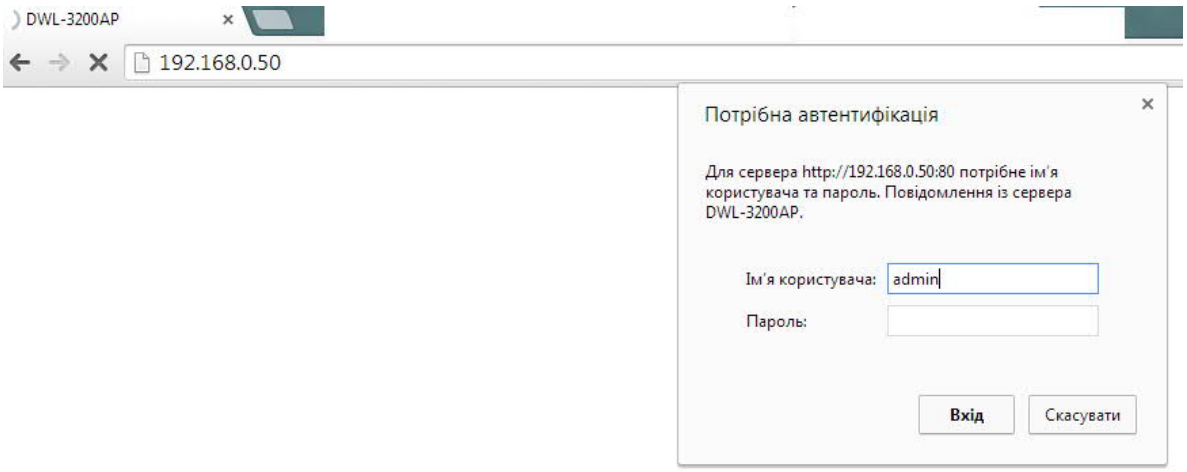

Рисунок 3.15 – Доступ до DWL-3200AP з браузер Google Chrome.

Після входу на точку доступу обов’язково потрібно замінити Ім’я користувача (логін) та Пароль, в необхідності і IP адресу. Для цього потрібно перейти в меню Basic Settings / Lan Settings (рисунок 3.16). Після збереження всіх налаштувань потрібних для роботи в режимі роумінгу точка запропонує перезавантажитися. Для роумінгу всі 7 точок доступу повинні називатися однаково (SSID - TNEU.EDU.UA) та працювати в одному (10) каналі, та бути

захищеними однаковим типом безпеки. Стан мережевого підключення TNEU.EDU.UA зображено на рисунку 3.18.

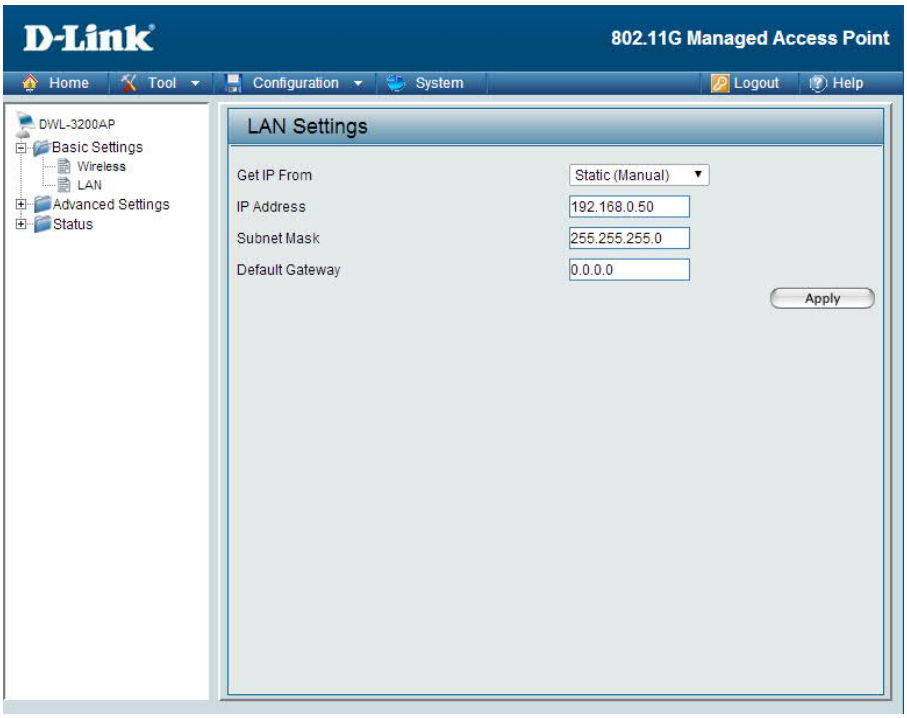

Рисунок 3.17 – Налаштування точки доступу DWL-3200AP.

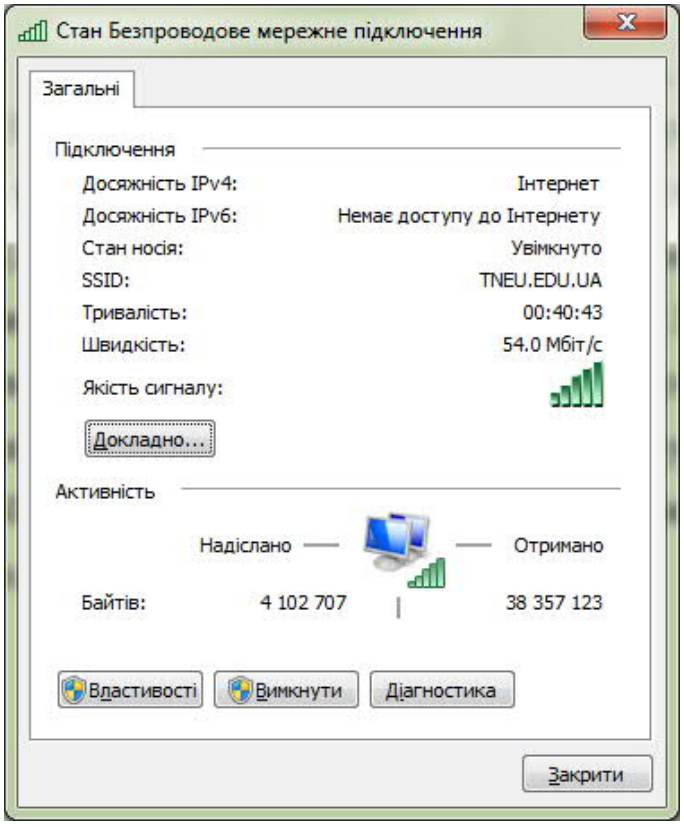

Рисунок 3.18 - Мережеве підключення TNEU.EDU.UA.

Для перевірки безпровідної мережі з роумінгом в приміщенні навчального корпусу №3 будо проведено дослід. Взявши ноутбук та запустивши в командній стрічці команду ping tneu.edu.ua –t, ми рухались від першого поверху до п’ятого.

Ping - службова програма, яка призначена для перевірки з'єднань в мережі на основі протокола TCP/IP [11].

Програма дозволяє відправляти запити протоколу ICMP зазначеному вузлу (www.tneu.edu.ua) мережі та фіксує відповіді на цей запит. Час між відправленням запиту та одержанням на нього відповіді дозволяє визначати затримки на маршруті і втрату пакетів.

Переглянувши статистику роботи службової програми (рисунок 3.19) ми побачили, що підключення жодного разу не пропало, тобто роумінг працює. Коли ми рухались по корпусі з зони дії однієї Wi-Fi в зону дії іншої з кращим рівнем сигналу, наш ноутбук автоматично перемикався в до іншої точки доступу. Це означає, що всі точки Wi-Fi доступу працюють коректно. Отже робота виконана правильно.

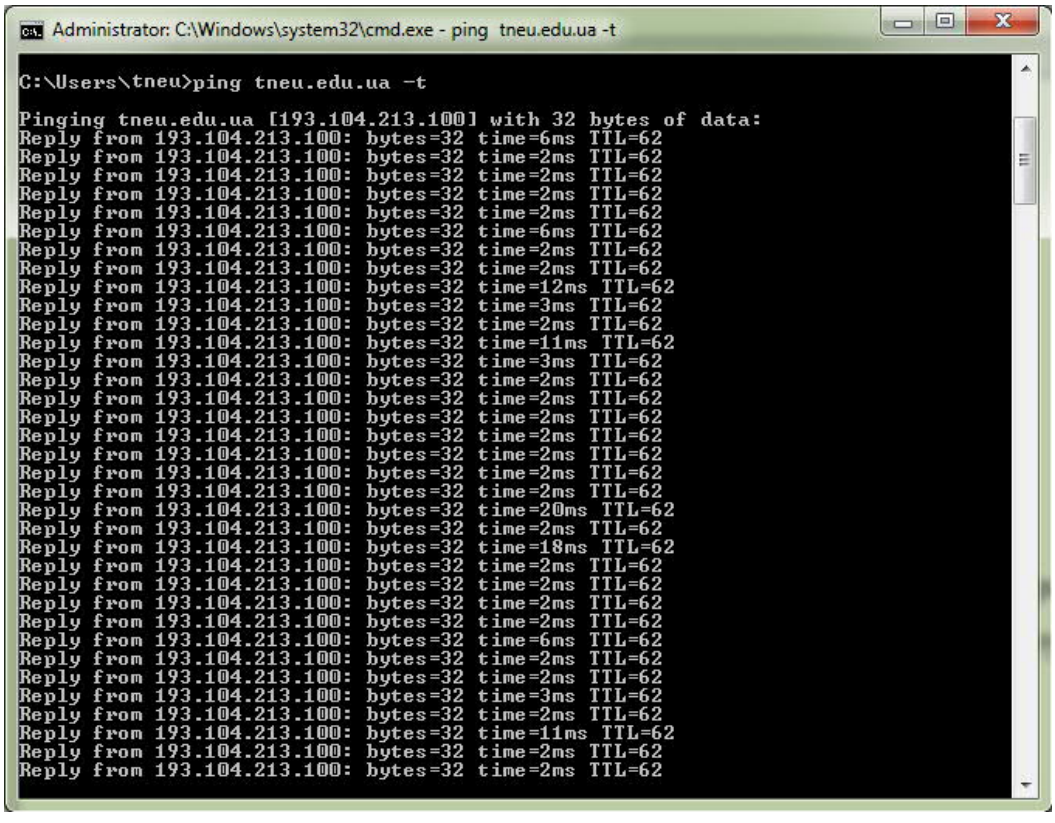

Рисунок 3.19 - Статистика роботи службової програми Ping.

4 ОХОРОНА ПРАЦІ

Питання охорони праці людини необхідно вирішувати на всіх стадіях трудового процесу незалежно від виду професійної діяльності.

Забезпечення безпечних і здорових умов праці в значній мірі залежить від правильної оцінки небезпечних, шкідливих виробничих факторів. Однакові по складності зміни в організмі людини можуть бути викликані різними причинами. Це можуть бути фактори виробничого середовища, надмірне фізичне і розумове навантаження, нервово-емоційна напруга, а також різне сполучення цих причин.

У даному розділі вирішується питання охорони праці програміста на стадії розробки ним програмного комплексу, призначеного для контролю готових виробів на наявність дефектів, діагностики й ідентифікації дефектів працюючого устаткування за допомогою дослідження їхніх спектральних графіків.

4.1 Аналіз небезпечних і шкідливих факторів

4.1.1 Організація робочого місця

Приміщення, в якому працює програміст, має загальну площу 40м^2, висоту стелі 3,5м. У приміщенні знаходиться 10 робочих місць з ПК. Кожне робоче місце обладнане робочим столом площею 1,2м^2, стільцем та персональним комп'ютером, що складається з монітора, системного блоку, клавіатури та миші. Слід відзначити, що площа одного робочого місця оператора ПК не повинна бути меншою за 6м^2, а об'єм не менший за 20м^3, тобто площі та об'єму даного приміщення не вистачає для розташування 10 робочих місць операторів ПК.

Аналіз умов праці показує, що у приміщенні лабораторії на програміста можуть негативно впливати наступні фізичні та психофізіологічні фактори:

– підвищена або знижена температура повітря робочої зони;

– підвищена або знижена вологість повітря;

– недостатня освітленість робочого місця;

– підвищений рівень шуму на робочому місці;

– підвищена іонізація повітря;

– підвищений рівень електромагнітних випромінювань;

– нервово-психічні;

– фізичні перевантаження.

4.1.2 Мікроклімат робочої зони програміста

Робота програміста (інженера-програміста) за енерговитратами відноситься до категорії легких робіт Іа, Іб, тому повинні дотримуватися наступні вимоги згідно ДСН 3.3.6.042-99:

– оптимальна температура повітря 22°С (допустима температура 20-24°С);

– оптимальна відносна вологість - 40-60% (допустима вологість - не більш 75%);

– швидкість руху повітря не більш 0,1 м/с.

Виміряні за допомогою приладів (психрометр Августа) температура та вологість у лабораторії відповідають вказаним у таблиці для теплого періоду року.

Розташовані у приміщенні 10 персональних комп’ютерів являються джерелами тепловиділень, крім того для підтримання у приміщенні в холодний період року оптимальних параметрів мікроклімату використовуються нагріті поверхні опалювальної системи. Нормованим показником ІЧВ являється гранично допустима густина потоку енергії Іг.д, Вт/м^2, яка встановлюється в залежності від площі опромінюваної поверхні тіла людини (Sопр). Нормовані рівні складають: Іг.д =35 Вт/м^2 при Sопр > 50%; Іг.д =70 Вт/м^2 при Sопр ~ 25-50%; Іг.д =100 Вт/м^2 при Sопр < 25%.

4.1.3 Освітлення робочого місця

Нормованим параметром природного освітлення згідно ДБН В.2.5-28-2006 являється коефіцієнт природного освітлення (КПО). КПО встановлюється в залежності від розряду виконуваних зорових робіт. Робота програміста відноситься до робіт середньої точності (IV розряд зорових робіт, мінімальний розмір об'єкту розрізнення складає 0,5 - 1,0мм), для яких при використанні бокового освітлення КПО=1,5%. Для штучного освітлення нормованим параметром виступає Емін - мінімальний рівень освітленості, та Кп - коефіцієнт пульсації світлового потоку, який не повинний бути більшим ніж 20%. Мінімальна освітленість встановлюється в залежності від розряду виконуваних зорових робіт. Для IV розряду зорових робіт вона складає 300-500 лк.

Перевірка освітленості робочого місця програміста в лабораторії на кафедрі ЕОМ на відповідність розряду зорової роботи

За даними вимірювань (люксметр Ю-116) рівень природної освітленості поверхні, де розташований ПК програміста, складає 200 лк при освітленості тієї же поверхні відкритим небосхилом в 20000 лк, тобто КПО = 1%, що не відповідає нормативному КПО.

Для штучного освітлення у приміщенні використовуються люмінесцентні лампи, які в порівнянні з лампами розжарювання мають ряд істотних переваг: за спектральним складом світла вони близькі до природного світла; мають підвищену світлову віддачу (у 2-5 разів вищу, ніж у ламп розжарювання); мають триваліший термін служби (до 10 тис. годин).

Розрахунок штучного освітлення проведемо для кімнати площею 40 м^2, ширина якої складає 5м, довжина - 8м, висота – 3,5м за методом коефіцієнта використання світлового потоку.

Для визначення потрібної кількості світильників, які повинні забезпечити нормований рівень освітленості, визначимо світловий потік, що падає на робочу поверхню за формулою:

$$F = \frac{ESKZ}{n}$$

де F - світловий потік, що розраховується, Лм;

E - нормована мінімальна освітленість, Лк; E = 300 Лк;

S - площа освітлюваного приміщення (у нашому випадку S=40м^2);

Z - відношення середньої освітленості до мінімальної (зазвичай приймається рівним 1,1... 1,2, в нашому випадку Z = 1,1);

К - коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників в процесі експлуатації (його значення залежить від типу приміщення і характеру робіт, що проводяться в ньому, в нашому випадку К = 1,5);

n - коефіцієнт використання світлового потоку, (виражається відношенням світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп, і обчислюється в долях одиниці; залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі, що характеризуються коефіцієнтами відбиття від стін (ρст.) і стелі (ρстелі), значення коефіцієнтів дорівнюють ρст = 40% і ρстелі=60%.

Обчислимо індекс приміщення за формулою:

$$i = \frac{S}{h(A+B)}$$

де S - площа приміщення,

S = 40м^2 ;

h-розрахункова висота підвісу,

h = 3,5м;

A - ширина приміщення,

A = 5м;

B - довжина приміщення,

B = 8м.

Підставивши значення отримаємо: i=0,879121.

Знаючи індекс приміщення, знаходимо n = 0,246154.

Підставимо всі значення у формулу для визначення світлового потоку.

$$F = \frac{300 \cdot 1{,}5 \cdot 40 \cdot 1{,}1}{0{,}246154} = 80437{,}5 Лм$$

Для освітлення використані люмінесцентні лампи типу ЛБ 40-1, світловий потік яких F = 4320 Лм.

$$N = \frac{F}{F_л}$$

де N - визначуване число ламп;

F - світловий потік,

F – 80437,5 Лм;

Fл - світловий потік однієї лампи,

Fл = 4320 Лм.

N=80437,5/4320=18,61979

В приміщенні використовуються світильники типу ЛПО. Кожен світильник комплектується трьома лампами. Тобто необхідно використовувати 7 світильників із 21 працюючими лампами в них (>18,6).

У лабораторії, де аналізувалось робоче місце програміста працює 15 ламп, тому рівень штучного освітлення не задовольняє санітарним нормам.

4.1.4 Вплив шуму на програміста

Як було вказано вище, в лабораторії знаходиться сім робочих місць з ПК, кожне з яких устатковане монітором, вінчестером в системному блоці, трьома вентиляторами системи охолоджування ПК та клавіатурою. Крім того поряд працює периферійна техніка. Таким чином у приміщенні мають місце шуми механічного і аеродинамічного походження, широкосмугові із аперіодичним підсиленням при роботі принтерів. Орієнтовні еквівалентні рівні звукового тиску джерел шуму, що діють на програміста на його робочому місці, представлені в таблиці 4.1. Допустимий еквівалентний рівень шуму для робочого місця програміста складає 50 дБА. Розрахуємо середній рівень шуму на робочому місці оператора при роботі всієї вказаної техніки.

Таблиця 4.1 - Рівні звукового тиску від різних джерел

Джерело шуму	Рівень шуму, дБА
жорсткий диск	45
вентилятор	45
принтер матричний	55
сканер	50

Рівень шуму, що виникає від декількох некогерентних джерел, що працюють одночасно, підраховується на підставі принципу енергетичного підсумовування рівня інтенсивності окремих джерел:

$$L = 10\lg \sum_{i=1}^{n} 10^{0,1L_i}$$

де Li - рівень звукового тиску і-го джерела шуму;

n — кількість джерел шуму.

Підставивши значення рівня звукового тиску для кожного виду устаткування у формулу, отримаємо:

$L= 10\lg(10^{4,5}+10^{4,5}+10^{5,5}+10^{5,0})=44,2$ дБ.

За наявності декількох джерел шуму з однаковим рівнем інтенсивності Li загальний рівень шуму визначають за формулою:

$L = L_i+10lgn.$

У нашому випадку таких джерел сім, отже загальний рівень шуму буде визначатися так:

$L=44,2+ 10_{lg}10 = 54,2$дБ.

Розраховане значення середнього рівня шуму перевищує гранично допустимий рівень шуму для робочого місця програміста, тобто слід передбачити заходи по зниженню рівня шуму.

4.1.5 Виробничі випромінювання

Допустимі значення параметрів неіонізуючих електромагнітних випромінювань від монітору комп'ютера представлені в таблиці 4.2. Нормованим параметром невикористаного рентгенівського випромінювання

виступає потужність експозиційної дози. На відстані 5 см від поверхні екрану монітору її рівень не повинен перевищувати 100 мкР/год. Максимальний рівень рентгенівського випромінювання на робочому місці програміста зазвичай не перевищує 20 мкР/год.

Таблиця 4.2 - Допустимі значення параметрів неіонізуючих електромагнітних випромінювань.

Найменування параметра	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50 см від поверхні монітора	10 В/м
Напруженість магнітної складової електромагнітного поля на відстані 50 см від поверхні монітора	0,3 А/м
Напруженість електростатичного поля не повинна перевищувати: – для дорослих користувачів – для дітей дошкільних установ і що вчаться середніх спеціальних і вищих учбових закладів	20 кВ

На відстані 5-10 см від екрана і корпуса монітора рівні напруженості можуть досягати 140 В/м по електричній складовій, що значно перевищує допустимі значення.

4.1.6 Електробезпека. Статична електрика

Приміщення лабораторії за небезпекою ураження електричним струмом можна віднести до 1 класу, тобто це приміщення без підвищеної небезпеки (сухе, без пилу, з нормальною температурою повітря, ізольованими підлогами і малим числом заземлених приладів).

На робочому місці програміста з всього устаткування металевим є лише корпус системного блоку комп’ютера, але тут використовуються системні

блоки, що відповідають стандартові фірми IBM, у яких крім робочої ізоляції передбачений елемент для заземлення і провід з жилою, що заземлює, для приєднання до джерела живлення.

Основні причини ураження людини електричним струмом на робочому місці:

– дотик до металевих частин (корпусу, периферії комп'ютера), що можуть виявитися під напругою в результаті ушкодження ізоляції;

– нерегламентоване використання електричних приладів;

– відсутність інструктажу співробітників з правил електробезпеки.

На протязі роботи на корпусі комп'ютера накопичується статична електрика. На відстані 5-10 см від екрана напруженість електростатичного поля складає 60-280 кВ/м, тобто в 10 разів перевищує норму 20 кВ/м.

4.1.7 Важкість та напруженість праці

Оцінка напруженості праці здійснювалась на підставі обліку всіх наявних значущих показників, які можуть перевищувати нормативні рівні.

Розподіл функцій за ступенем складності завдання - належить до класу 2 (обробка, виконання завдання та його перевірка). Характер виконуваної роботи - належить до класу 2 (робота за встановленим графіком з можливим його коректуванням у ході діяльності). Навантаження на зоровий аналізатор (при відстані від очей працюючого до об'єкта розрізнення не більше 0,5 м), при тривалості зосередженого спостереження (% часу зміни) - належить до класу 2 (5,0-1,1мм більше 50 % часу; 1,0-0,3мм до 50 % часу; менше 0,3 мм до 25 %). Спостереження за екранами відеотерміналів (годин на зміну) - належить до класу 3.2 (більше 4 годин). Монотонність праці. Кількість елементів (прийомів, необхідних для реалізації простого завдання або в операціях, які повторюються багаторазово) - належить до класу 3.1 (5-3 прийоми). Режим праці (фактична тривалість робочого дня (год.) - належить до класу 1 (6-7 годин). Наявність регламентованих перерв та їх тривалість - належить до класу 2 (перерви

регламентовані, недостатньої тривалості: від 3 % до 7 % часу зміни). Отже робоче місце за показниками напруженості трудового процесу відноситься до класу 3.1 - Шкідливий (напружена праця).

Важкість праці. Оцінка важкості праці здійснюється на підставі обліку всіх наявних значущих показників. При цьому спочатку встановлюється клас кожного із вимірюваних показників, а кінцева оцінка важкості праці встановлюється за показником, який має найвищий ступінь важкості.

Стереотипні робочі рухи (кількість за зміну): при локальному навантаженні (за участю м'язів кистей та пальців рук) - належить до класу 1 (до 20000). При загальному навантаженні (при роботі з переважною участю м'язів рук та плечового поясу) - належить до класу 1 (до 10000). Робоча поза Щ належить до класу 2 (періодичне перебування в незручній позі (робота з поворотом) тулуба, незручним розташуванням кінцівок та/або фіксованій позі (неможливість зміни розташування різних частин тіла відносно одна одної) до 25 % часу зміни.) Нахили корпуса (вимушені, більше 30), кількість за зміну - належить до класу 1 (до 50). Переміщення у просторі (переходи, обумовлені технологічним процесом протягом зміни), км: по горизонталі - належить до класу 1 (до 4). По вертикалі - належить до класу 1 (до 2). Отже робоче місце за показниками важкості трудового процесу відноситься до класу 2 - Допустимий, середнє фізичне навантаження.

4.2 Розробка заходів з охорони праці

4.2.1 Ергономіка та організація робочого місця

Після проведення аналізу робочого місця програміста в лабораторії було з'ясовано, що воно не відповідає встановленим вимогам. Також у результаті аналізу були виявлені порушення в організації безпосередньо самого робочого

місця програміста. У зв'язку з цим пропонується організувати робоче місце програміста наступним способом:

– висота над рівнем підлоги робочої поверхні, на якій працює програміст, повинна складати 720 мм. Бажано, щоб робочий стіл при необхідності можна було регулювати по висоті в межах 680-780 мм;

– оптимальний розмір поверхні столу 1600 х 1000 мм . Під столом повинен бути простір для ніг з розмірами по глибині 650 мм. Робочий стіл оператора повинен також мати підставку для ніг, розташовану під кутом 15^0 до поверхні столу. Довжина підставки - 400 мм, ширина -350 мм. Відстань клавіатури від краю столу повинна бути не більш 300 мм, що забезпечить програмісту зручну опору для передпліч. Відстань між очима й екраном монітору повинне складати 40-80см;

– робочий стілець програміста повинен бути оснащений підйомно-поворотним механізмом. Висота сидіння повинна регулюватися в межах 400-500 мм. Глибина сидіння повинна складати не менш 380 мм, а ширина - не менш 400 мм. Висота опорної поверхні спинки не менш 300 мм, ширина - не менш 380 мм. Кут нахилу спинки стільця до площини сидіння повинен змінюватися в межах 90 - 110 град.. Виходячи з результатів аналізу важкості та напруженості праці пропоную скоротити час роботи за комп'ютером, робити перерви, час яких повинен складати 50 хвилин при 8-ми годинній зміні.

4.2.2 Нормалізація повітря робочої зони

Для створення й автоматичної підтримки в лабораторії незалежно від зовнішніх умов оптимальних значень температури, вологості, чистоти і швидкості руху повітря, у холодний час року використовується водяне опалення, у теплий час року застосовується кондиціонер для охолодження повітря.

4.2.3 Виробниче освітлення

Під час аналізу освітлення на робочому місті програміста було встановлено, що воно не відповідає встановленим нормам, тому для

покращення умов праці рекомендуємо збільшити рівень загальної освітленості приміщення шляхом встановлення 6 додаткових ламп.

Також для підтримки запроектованого освітлення у чистому виді необхідно скласти графік, де передбачити очищення віконних блоків і світильників не менше 2 разів на рік.

4.2.4 Захист від виробничого шуму

Як міри по зниженню шуму можна запропонувати:

– облицювання стелі і стін звукопоглинаючим матеріалом (знижують шум на 6-8 дб);

– екранування робочого місця (постановкою перегородок, діафрагм);

– установка в комп'ютерних приміщеннях устаткування, що робить мінімальний шум;

– раціональне планування приміщення.

Для зменшення шуму в аналізованій лабораторії пропоную використовувати замість матричного принтера, що створює багато шуму, більш тихий - лазерний принтер.

4.2.5 Захист від електромагнітних полів

Для попередження впровадження небезпечної техніки всі дисплеї повинні бути сертифіковані.

4.2.6 Електробезпека

Електробезпечність у приміщенні лабораторії пропоную забезпечити наступними технічними способами і засобами захисту:

– для зменшення накопичення статичної електрики застосовувати зволожувачі і нейтралізатори, антистатичне покриття підлоги;

– забезпечити приєднання металевих корпусів устаткування до жили, що заземлює. Заземлення корпуса ПК забезпечити підведенням жили, що заземлює, до розеток. Опір заземлення 4 Ом, згідно (ПУЗ) для електроустановок з напругою до 1000 В.

Також організаційними заходами:

– своєчасне проведення інструктажів з техніки безпеки;

– по забороні використання непередбачених у лабораторії електричних приладів, таких як електричні чайники та обігрівачі.

4.3 Пожежна безпека

Ступінь вогнестійкості будинків приймається в залежності від їхнього призначення, категорії по вибухопожежній і пожежній небезпеці, по поверховості, площі поверху в межах пожежного відсіку згідно НАПБ Б.03.002-2007.

Будинок, у якому знаходиться лабораторія по пожежній небезпеці будівельних конструкцій відноситься до категорії К1 (мало пожежонебезпечні), оскільки тут присутні займисті (книги, документи, меблі, оргтехніка і т.д.) і важкогорючі речовини (сейфи, різне устаткування і т.д.), що при взаємодії з вогнем можуть горіти без вибуху.

По конструктивних характеристиках будинок можна віднести до будинків з несучими і огороджуючими конструкціями із природних або штучних кам'яних матеріалів, бетону або залізобетону, де для перекриттів допускається використання дерев'яних конструкцій, захищених штукатуркою або важкогорючими листовими, а також плитними матеріалами.

Отже, ступінь вогнестійкості будинку можна визначити як третю (III). Приміщення лабораторії по функціональній пожежній небезпеці відноситься до класу Ф 4.2 - вищі навчальні заклади, установи підвищення кваліфікації.

4.3.1 Причини виникнення пожежі

Пожежа в лабораторії, може привести до дуже несприятливих наслідків (втрата коштовної інформації, псування майна, загибель людей і т.д.), тому

необхідно: виявити й усунути всі причини виникнення пожежі; розробити план заходів для ліквідації пожежі в будинку; план евакуації людей з будинку.

Причинами виникнення пожежі можуть бути:

– несправності електропроводки, розеток і вимикачів які можуть привести до короткого замикання або пробою ізоляції;

– використання ушкоджених (несправних) електроприладів;

– використання в приміщенні електронагрівальних приладів з відкритими нагрівальними елементами;

– виникнення пожежі внаслідок влучення блискавки в будинок;

– загоряння будинку внаслідок зовнішніх впливів;

– неакуратне поводження з вогнем і недотримання мір пожежної безпеки.

ВИСНОВКИ

У рамках дипломного проекту був складений проект безпровідної мережі навчального закладу з роумінгом на прикладі навчального корпусу №3 ТНЕУ. Структурована кабельна система відповідає прийнятим міжнародним стандартам (ANSI/TIA/EIA-568-A і ISO/IEC11801).

Проектом передбачається забезпечення навчального корпусу не просто безпровідною мережею на основі Wi-Fi, а мережею, в якій буде повноцінно працювати роумінг. Було проаналізовано вже існуючу безпровідну мережу корпусу, виявлено її недоліки (недостатня кількість Wi-Fi точок доступу) та запропоновано шляхи вирішення проблеми. В роботі досліджені основні, та найбільш популярні засоби діагностика і управління Wi-Fi мереж, а саме – Orion NPM SolarWinds та AP Maneger. AP Maneger використовують для управління безпровідною мережею в ТНЕУ. Також нами описана система моніторингу, як засобу виявлення помилок в роботі Wi-Fi в режимі онлайн на прикладі ПЗ Negius та Zabbix.

Для побудови мережі також було проаналізовано основні параметри, характеристики, властивості, стандарти, переваги та недоліки технології Wi-Fi. Для одержання найбільш точних і ефективних результатів по роботі мережі її було змодельовано за допомогою програми NET CRACKER 4.1. Також досліджено і інші програмні засоби, як то – Експерт СКС, для проектування мереж, та визначили яке мережеве обладнання краще використати для повноцінної роботи мережі, та де найкраще розмістити точки доступу.

У проекті надані необхідні розрахунки й креслення, специфікація устаткування й матеріалів, необхідних для побудови безпровідної мережі з роумінгом. Крім того подані вимоги по монтажу, рекомендації з адміністрування, обслуговування й експлуатації системи.

Результати дипломного проектування будуть використані в ЦІТ ТНЕУ

(Додаток Є) для побудови безпровідної мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. About Nagios [Електронний ресурс]. – Режим доступу: http://www.nagios.org – Назва з екрану.

2. Alan Holt, Chi-Yu Huang. 802.11 Wireless Networks: Security and Analysis, Springer, 2010, 194-198 с.

3. Amitabh Mishra. Security and Quality of Service in Ad Hoc Wireless Networks, Cambridge press, 2008, 95-97с.

4. AP Manager [Електронний ресурс]. – Режим доступу: http://acowa.narod.ru/index/0-4 – Назва з екрану.

5. Cisco Press. Программа сетевой академии Cisco CCNA 3, Вильямс, 2007, 560 с

6. IEEE 802.11 [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/IEEE_802.11 – Назва з екрану.

7. Nagios [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Nagios – Назва з екрану.

8. NetCracker [Електронний ресурс]. – Режим доступу: http://www.netcracker.com/ukr – Назва з екрану.

9. NetCracker Technology [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/NetCracker_Technology – Назва з екрану.

10. Network Performance Monitor - SolarWinds [Електронний ресурс]. – Режим доступу: http://www.solarwinds.com/network-performance-monitor.aspx – Назва з екрану.

11. Ping [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Ping – Назва з екрану.

12. VLAN [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/VLAN – Назва з екрану.

13. Wi-Fi [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Wi-Fi – Назва з екрану.

14. Zabbix [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Zabbix – Назва з екрану.

15. Айвенс К. Компьютерные сети. Хитрости, СПб.: Питер, 2006, 98-103с.

16. Ватаманюк А. Беспроводная сеть своими руками, СПб.: Питер, 2006, 113-114с.

17. Владимиров А.А. Wi-фу: боевые приемы взлома и защиты беспроводных сетей, НТ Пресс, 2005, 464с.

18. Гейер Джим. Беспроводные сети. Первый шаг, Вильямс, 2005, 89с.

19. Гейер Джим. Реализация высокоскоростных беспроводных сетей, Вильямс, 2007, 33с.

20. Глушаков С. В. , Хачиров Т. С. Настраиваем сеть своими руками, Фолио, 2008, 45с.

21. Димарцио Дж.Ф. Маршрутизаторы. Пособие для самостоятельного изучения, Символ, 2003, 422 - 423с.

22. Захист в Wi-Fi мережах [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Захист_в_Wi-Fi_мережах – Назва з екрану.

23. Зорин М., Писарев Ю., Соловьев П. Радиооборудование диапазона 2,4 ГГц: задачи и возможности // PCWeek/Russian Edition.1999.№20-21.стр. 20.

24. Кенин А. Самоучитель системного администратора, 3-е издание – БХВ-Петербург, 2012, 312с.

25. Методичні вказівки до написання розділу “Охорона праці” в дипломних проектах з освітньо-кваліфікаційного рівня “Спеціаліст” для спеціальності 7.091501-Комп’ютерні системи та мережі / Г.В. Сапожник, Н.М.Васильків. - Тернопіль: ТАНГ, 2004. – 24 с.

26. Методичні рекомендації до виконання дипломного проекту з освітньо-кваліфікаційного рівня “Бакалавр” напряму підготовки 6.050102

«Комп'ютерна інженерія» фахового спрямування «Комп'ютерні системи та мережі» / О.М. Березький, Л.О.Дубчак, Р.Б. Трембач, Г.М. Мельник, Ю.М. Батько, С.В. Івасьєв / Під ред. О.М. Березького. Тернопіль: ТНЕУ, 2013.–65 с.

27. Молта Д., Фостер-Вебстер А. Тестируем оборудование для беспроводных ЛВС стандарта 802.11 // Сети и системы связи.1999.№7.стр. 34.

28. Павликевич М. Лекції для студентів спеціальності 7.092402 "Інформаційні мережі зв'язку" – Телекомунікаційні мережі – безпровідні локальні мережі (WLAN) - Львів, 2005, 9-10с.

29. Педжман Р., Джонатан Л. Основы построения беспроводных локальных сетей стандарта 802.11, СПб.:Вильямс, 2004. – 302 с.

30. Переваги та недоліки технології Wi-Fi [Електронний ресурс]. – Режим доступу: http://e-ogo.com.ua/perevagi-ta-nedoliki-texnologii-wi-fi – Назва з екрану.

31. Писарев Ю. Беспроводные сети: на пути к новым стандартам // PC Magazine/Russian Edition.1999.№ 10. стр. 176.

32. Поляк-Брагинский А.. Локальные сети. Модернизация и поиск неисправностей. - БХВ-Петербург, 2006, 567-568с.

33. Родичев Ю.А. Компьютерные сети - архитектура, технологии, защита, Универс-групп, 2006, 365 - 368с.

34. Росс. Джон. Wi-Fi. Беспроводные сети. Установка. Конфигурирование. – СПб.:НТ Пресс, 2006, 550с.

35. Столлингс В. Беспроводные линии связи и сети : пер. с англ. / В. Столлингс. - М. : Издательский дом «Вильямс», 2003, 640 с.

36. Сюваткин В.С., Есипенко В.И., Ковалев И.П., Сухоребров В.Г. Технология беспроводной связи. Основы теории, стандарты, применение, СПб.: БХВ-Петербург, 2005, 300-305с.

37. Технології Wi-Fi [Електронний ресурс]. – Режим доступу: http://www.wimagic.com.ua/uk – Назва з екрану.

38. Что такое Zabbix [Електронний ресурс]. – Режим доступу: http://www.zabbix.com/ru – Назва з екрану.

39. Щербаков В.Б., Ермаков С.А. Безопасность беспроводных сетей: стандарт IEEE 802.11, М: РадиоСофт, 2010, 29-34с.

40. Эксперт-СКС: Описание "Эксперт-СКС" [Електронний ресурс]. – Режим доступу: http://www.expertsoft.com.ua/scs/128 – Назва з екрану.