Міністерство освіти і науки України
Кам’янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра комп’ютерних наук

Дипломна робота
бакалавра
з теми: “ПОБУДОВА ТА МОДЕРНІЗАЦІЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ УНІВЕРСИТЕТУ”

Виконав: студент 4 курсу KN1-B18 групи
спеціальності 122 Комп’ютерні науки
Козаков Віталій Вікторович
Керівник: Понеділок Вадим Віталійович,
старший викладач кафедри комп’ютерних
наук, кандидат технічних наук

Кам’янець-Подільський – 2022

ЗМІСТ

Вступ

Сучасний інформаційний світ важко уявити без такого поняття, як комп'ютерна мережа, щоб користувачі по всьому світу обмінювалися інформацією і не тільки прості користувачі, а й великі компанії передавали дані, які могли бути захищені, то для цього потрібну побудувати надійну мережу, або локальну, якщо діапазон не великий, а глобальну для обміну даними між країнами і навіть континентами. Тому принципи побудуви комп'ютерної мережі зараз як не як актуальні, оскільки потрібно знати усі технології побудови, обладнання для побудови і забезпечення стабільного зв'язку і види цього обладнання та як обрати надійне, щоб можна було побудувати мережі під власні задачі.

Актуальність теми: в наш час дуже широко використовується поняття комп'ютерної мережі та її побудови, так як багато користувачів, компаній хочуть мати свою мережу для передачі даних і обміну інформацією, починаючи від малих відстаней до обміну між континентиами і тому щоб побудувати мережу треба знати технології і використовувати самі оптимальні під власні потреби і так, щоб канал передачі даних був надійно захищеним. Для прикладу було взято опис та модернізацію технології, що застосовується в мережі нашого університету, оскільки мережа побудована і вона зберігається в центрі інформаційних технологій.

Метою роботи: є аналіз стану розвитку сучасних технологій та типових рішень, що застосовуються при проектуванні та побудові телекомунікаційних мереж; огляд апаратного та програмного забезпечення; підбір та реалізація базових мережевих технологій, які дозволять ефективно обслуговувати, експлуатувати та масштабувати телекомунікаційні мережі.

Об'єктом даної роботи: є опис та модернізація комп'ютерної мережі університету, який включає в себе огляд технологій, які використовувалися у побудові мережі та використовуються зараз, технології захисту. А також тип мережі і апаратне забезпечення, яке підключене до мережі та використовується при побудови мережі університету.

Предметом дослідження: є комп'ютерна мережа університету та її концептуальна схема, а також сайт де вона зберігається і доступи до них.

Завданням дипломної роботи: є огляд і опис, і дослідження та аналіз стану розвитку усіх видів локальних і глобальних мереж, опис технологій і обладнання, яке використовується при побудові та практично описати і розробити конфігурацію з використанням даних технологій на прикладі мережі нашого університету.

Структура роботи: дипломна робота включає в себе вступ, 4 основних розділі, висновок і список використаних джерел.

Огляд технологій локальних мереж

Для початку, щоб приступити до огляду технологій локальних мереж потрібно вияснити, що це є і що вона собою являє. Локальна комп'ютерна мережа є об'єднанням певного числа комп'ютерів на відносно невеликій території, тобто це є мережа для обмеженого кола користувачів, що об'єднує комп'ютери в одному приміщені або рамках одного підприємства. За допомогою локальної мережі один комп'ютер отримує доступ до ресурсів іншого, таких, як дані та периферійні пристрої. Основними характеристиками локальної мережі є зазвичай більша швидкість обміну даними, менше географічне покриття та відсутність потреби використовувати запозичену телекомунікаційну лінію зв'язку у порівнянні із глобальною комп'ютерною мережею.

До основи технологій побудови локальних мереж можна виділити два пункти: топологія та технологія побудови. У локальних і глобальних мережах застосовують різні технології та топології, вибір яких залежить від багатьох факторів, серед яких:

- *Вимоги до пропускної здатності мережі і швидкості;*
- *Розташування вузлів, відстані і умови прокладки комунікацій;*
- *Вимоги надійності та конфіденційності зв'язку;*
- *Обмеження на вартість апаратури і комунікацій.*

Першим таким критерієм є топологія мережі, що характеризує властивості мереж, які не залежить від їх розмірів, відображає структуру, утворену вузлами мережі і безліччю каналів, що їх зв'язує. При цьому не враховується продуктивність і принцип роботи цих вузлів, їх типи і довжина каналів. З погляду фізичного розташування функціональних компонентів мережі і методу доступу до середовища передачі можна виділити чотири базові топології: "загальна шина", "зірка", "кільце", "чарункова".

Мережа з топологією “загальна шина” - мережа, ядром якої є моноканал. Моноканальна мережа утворюється підключенням групи абонентських систем до моноканалу.

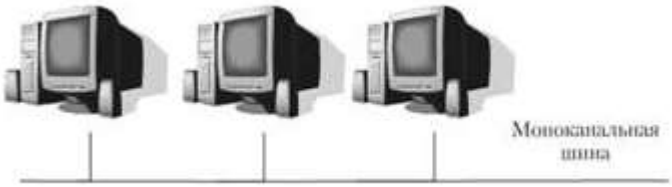

Рис. 1.1. Схема мережі з топологією “загальна шина”

Серед основних переваг шинної топології можна виділити:

- *надійно працює у невеликих мережах, проста у використанні і зрозуміла;*
- *вимагає менше кабелю для з’єднання комп’ютерів і тому дешевше, ніж інші схеми кабельних з’єднань;*
- *її топологією легко розширити;*
- *менша протяжність кабелів і більш висока надійність, оскільки вихід з ладу одного вузла не порушує працездатності мережі в цілому.*

Серед недоліків наступні:

- *обрив основного кабелю призводить до виходу всієї мережі з ладу;*
- *інтенсивний мережевий трафік значно знижує продуктивність такої мережі;*
- *інформація в системі на фізичному рівні слабо захищена, оскільки повідомлення, що посилаються одним комп'ютером іншому, в принципі можуть бути прийняті і на будь-якому іншому комп'ютері.*

Мережа з топологією “зірка” – являє собою деревоподібну мережу, в якій є рівно один проміжний вузол. Як центральної частини виступає ***мультиплексор***, який являє собою пристрій, що перетворює кілька сигналів входу в окремий сигнал виводу; при цьому зберігається можливість відновлення всіх сигналів введення або також можливе використання ***концентратора***, він в свою чергу дозволяє засобу передачі даних обслуговувати більшу кількість джерел даних по меншому числу каналів

передачі даних, який повністю управляє ЕОМ, підключеними до нього. Мережа має один центральний вузол від якого розходяться променями станції з периферійними пристроями на кінцях. У такій мережі всі станції безпосередньо пов'язані з центральним комп'ютером, який керує потоком повідомлень у мережі, і повідомлення від однієї станції до іншої можна передавати тільки через центральний комп'ютер.

Рис. 1.2. Схема мережі з топологією "зірка"

Розширювати зіркоподібну топологію можна шляхом підключення замість одного з комп'ютерів ще одного концентратора і приєднання до нього додаткових машин. Так створюється гібридна зіркоподібна мережа.

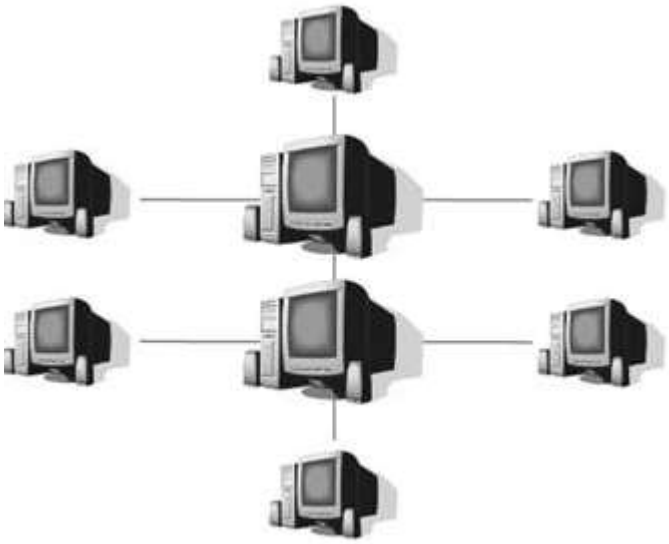

Рис. 1.3. Схема гібридної зіркоподібної мережі

Що до переваг використання топології зірка, то слід зазначити такі пункти:

- *така мережа допускає просту модифікацію і додавання комп'ютерів, не порушуючи решти її частини;*
- *центральний комп'ютер зіркоподібною топологією зручно використовувати для діагностики;*
- *відмова одного комп'ютера не завжди приводить до зупинки всієї мережі;*
- *в одній мережі допускається застосування декількох типів кабелів;*

До недоліків мережі можна віднести:

- *при відмові центрального комп'ютера стає непрацездатною вся мережа;*
- *зазвичай використовується великі по протяжності кабелі і, отже, такі мережі обходяться дорожче, ніж мережі з іншою топологією*.

Мережа з топологією "кільце" - мережа, в якій кожен вузол пов'язаний з двома іншими. Ця мережа є підсистемою старшої мережі. У ній кожна станція виступає в ролі центрального комп'ютера і прямо пов'язана з двома сусідніми

Рис. 1.4. Схема мережі з топологією " кільце"

До переваг мережі з кільцевою топологією:

- *оскільки всім комп'ютерам надається рівний доступ до маркера, ніхто з них не зможе монополізувати мережу;*
- *більш висока надійність системи при розривах кабелів, так як до кожного комп'ютера є два шляхи доступу;*
- *спільне використання мережі забезпечує поступове зниження її продуктивності у випадку збільшення числа користувачів і перевантаження.*

Серед недоліків слід зазначити:

- *велика протяжність кабелю;*
- *слабка захищеність інформації;*
- *невисока швидкодія в порівнянні з топологією "зірка".*

Комірчана топологія – мережа, в якій є безпосередні з'єднання між усіма вузлами мережі. Ця мережа характеризується наявністю надлишкових зв'язків між пристроями. Для великої кількості пристроїв така схема виявляється неприйнятною.

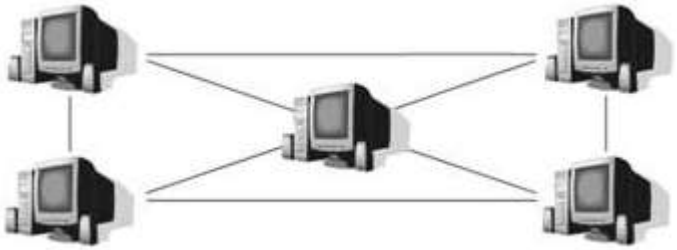

Рис. 1.5. Сема мережі з комірчастою топологією

Мережа гібридної топології застосовується для з'єднання декількох мереж між собою, кожна з яких може мати різну топологію, або для створення конгломератів локальних, регіональних і глобальних обчислювальних мереж. Топологія реальної мережі може повторювати одну з наведених вище або включати їх комбінацію.

Важливим елементом для побудови локальних мереж крім топології вважається і вибір технології, яка буде використовуватися при побудові мережі. На даний час існує багато технологій і нижче я опишу які є.

Технологія Token Ring

Token Ring — це технологія локальних мереж з маркерним методом доступу. Технологія Token Ring була розроблена компанією IBM в 1984 р., а потім передана як проект стандарту до комітету IEEE 802, який прийняв у 1985 р. стандарт 802.5. Компанія IBM використовує технологію Token Ring як основну мережну технологію для побудови локальних мереж на основі комп'ютерів різних класів — мейнфреймів, міні-комп'ютерів і персональних комп'ютерів. Мережі Token Ring працюють із двома бітовими швидкостями

— 4 і 16 Мбіт/с. Мережі Token Ring, що працюють зі швидкістю 16 Мбіт/с, мають деякі вдосконалення в алгоритмі доступу порівняно зі стандартом 4 Мбіт/с.

У мережі Token Ring кільце утворюється відрізками кабелю, що з'єднують сусідні станції. Таким чином, кожна станція зв'язана зі попередньою і наступною станцією й може безпосередньо обмінюватися даними тільки з ними. Для забезпечення доступу станцій до фізичного середовища кільцем циркулюється кадр спеціального формату й призначення — маркер. У мережі Token Ring будь-яка станція завжди безпосередньо отримує дані тільки від однієї станції — тієї, яка є попередньою в кільці. Така станція називається *найближчим активним сусідом, розташованим вище за потоком даних* (Nearest Active Upstream Neighbor, NAUN). Передачу ж даних станція завжди здійснює своєму найближчому сусідові вниз за потоком даних.

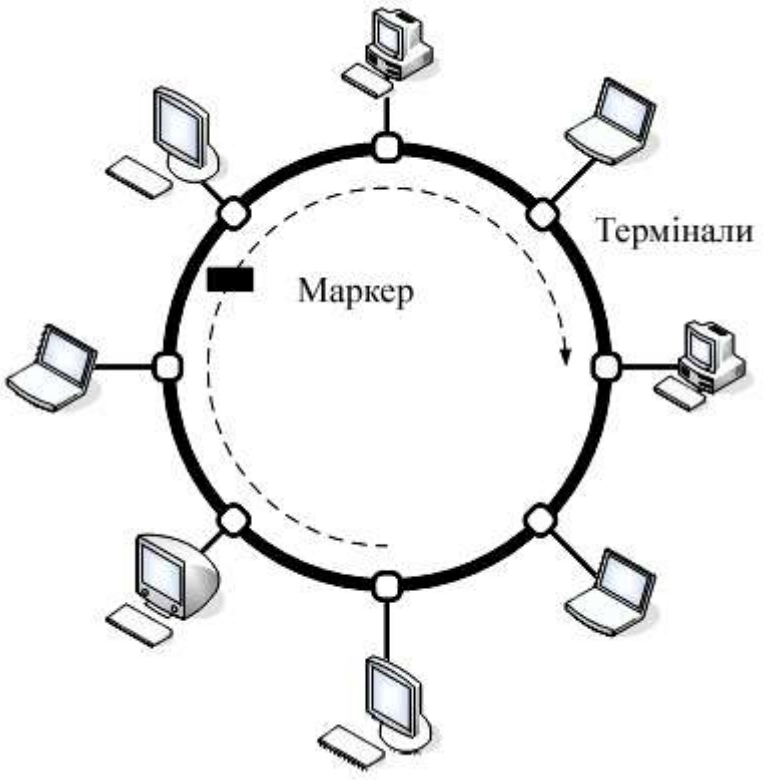

Рис. 1.6. Технологія Token Ring

Отримавши маркер, станція аналізує його й за відсутності в неї даних для передачі забезпечує його просування до наступної станції. Станція, що має дані для передачі, при отриманні маркера вилучає його з кільця, що дає їй право доступу до фізичного середовища й передачі своїх даних. Потім ця станція видає в кільце кадр даних встановленого формату послідовно по бітах. Передані дані проходять по кільцю завжди в одному напрямку від однієї станції до іншої. Кадр має адресу призначення й адресу джерела.

Усі станції кільця ретранслюють кадр побітово, як повторювачі. Якщо кадр проходить через станцію призначення, то, розпізнавши свою адресу, ця станція копіює кадр у свій внутрішній буфер і вставляє в кадр ознаку підтвердження прийому. Станція, що видала кадр даних у кільце, при зворотньому його одержанні з підтвердженням прийому вилучає цей кадр із кільця й передає в мережу новий маркер для забезпечення можливості іншим станціям мережі передавати дані. На сьогодні технологія повністю витиснута технологією Ethernet.

Технологія Ethernet

Технологія Ethernet набула найбільшого поширення зі всіх технологій локальних мереж. Технологію було розроблено фірмою Xerox у 1972 р. Проект виявився досить вдалим і в 1980 р. його підтримали найбільші фірми DEC й Intel. Об’єднання цих фірм назвали DIX за першими буквами їхніх назв. У 1985 р. мережа Ethernet стала міжнародним стандартом, її прийняли найбільші міжнародні організації зі стандартів: комітет 802 IEEE (Institute of Electrical and Electronic Engineers) і ECMA (European Computer Manufacturers Association). Стандарт отримав назву IEEE 802.3. Щодо основних характеристик, які використовуються у стандарті IEEE 802.3: топологія – шина, середовище передавання – коаксіальний кабель, швидкість передачі – 10 Мбіт/с, максимальна довжина – 5 км, максимальна кількість абонентів – до 1024, довжина сегмента мережі – до 500м, кількість абонентів на одному сегменті – до 100, метод доступу — carrier-sense-multiply-access with collision

detection (CSMA/CD). Характеристики цього стандарту використовуються у мережах, які побудовані використовуючи технологію Ethernet.

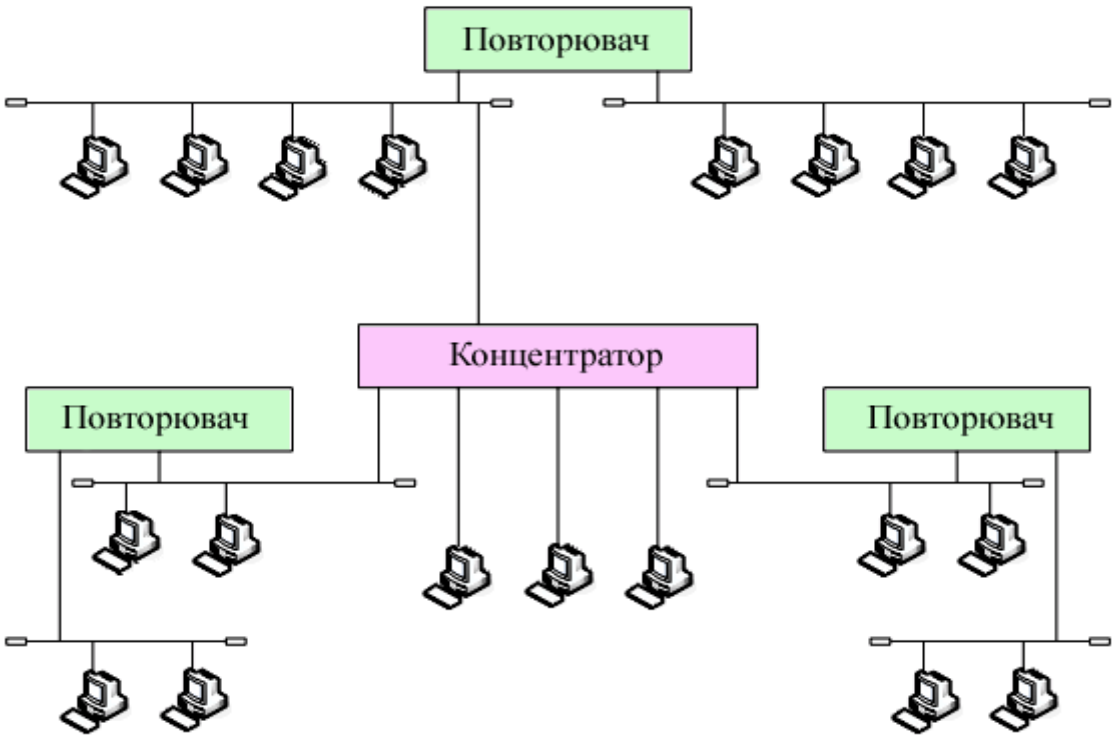

Рис. 1.7. Технологія Ethernet

Коаксіальний кабель використовується для шинних сегментів, а кручена пара й оптоволоконний кабель — для променів пасивної зірки для приєднання до концентратора одиночних комп'ютерів та інших концентраторів. У топології неприпустима поява петель. Це призведе до повної непрацездатності мережі. Фактично виходить, що абоненти з'єднані у фізичну шинну, оскільки сигнал від кожного з них поширюється відразу в усі сторони й не повертається назад, як у кільцевій топології. Максимальна довжина кабелю всієї мережі в цілому теоретично може сягати 6,5 км, але практично не перевищує 2,5 км.

Фізичні специфікації технології Ethernet на сьогодні містять такі середовища передачі даних:

- *10Base-5 — коаксіальний кабель діаметром 0,5 дюйма, який називають «товстим» коаксіалом. Має хвильовий опір 50 Ом. Максимальна довжина сегмента — 500 м (без повторювачів);*

- *10Base-2 — коаксіальний кабель діаметром 0,25 дюйма, який називають «тонким» коаксіалом. Має також хвильовий опір 50 Ом. Максимальна довжина сегмента — 185 м (без повторювачів);*
- *10Base-T — кабель на основі неекранованої крученої пари (Unshielded Twisted Pair, UTP), який створює зіркоподібну топологію з концентратором. Відстань між концентратором і кінцевим вузлом може бути не більше 100 м;*
- *10Base-F — оптоволоконний кабель, який використовується в топологіях, аналогічних стандарту на крученій парі. Є кілька варіантів цієї специфікації — FOIRL, 10Base-FL, 10Base-FB.*

Число 10 позначає бітову швидкість передачі даних цих стандартів — 10 Мбіт/с, а слово Base — метод передачі на одній базовій частоті 10 МГц (на відміну від стандартів, які використовують кілька носійних частот і називаються broadband — широкосмуговими).

Для передачі інформації мережею двійковий потік кодується лінійним манчестерським кодом. Для доступу до мережі використовується метод CSMA/CD. У мережі використовується пакети змінної довжини. Довжина кадру Ethernet має бути не менше 512 бітових інтервалів, або 51,2 мкс. В Ethernet підтримується індивідуальне, групове й широкомовне розсилання кадрів. Класичний Ethernet зараз витиснутий більш швидкими модифікаціями Fast Ethernet й Gigabit Ethernet, але ці технології підтримують сумісність «вниз».

Технологія Fast Ethernet

У 1992 р. група виробників мережного обладнання, включаючи таких лідерів технології Ethernet, як SynOptics, 3Com і ряд інших, утворила некомерційне об’єднання Fast Ethernet Alliance для розробки стандарту нової технології, яка повинна була забезпечити різке підвищення продуктивності при максимально можливому збереженні особливостей технології Ethernet. У комітеті 802 інституту IEEE у цей же час була сформована дослідницька група для вивчення технічного потенціалу нових високошвидкісних

технологій. За період з кінця 1992 р. і до кінця 1993 р. група IEEE вивчила 100-мегабітові рішення, запропоновані різними виробниками. Восени 1995 р. комітет IEEE 802.3 прийняв специфікацію Fast Ethernet як стандарт 802.3u, який не є самостійним стандартом, а являє собою доповнення до існуючого стандарту 802.3.

Офіційний стандарт 802.3 установив три різних специфікації для середовища передачі Fast Ethernet:

- *100Base-TX для двопарного кабелю на неекранованій крученій парі UTP категорії 5 або екранованій крученій парі STP типу 1;*
- *100Base-T4 для чотирьохпарного кабелю на неекранованій крученій парі UTP категорії 3, 4 або 5;*
- *100Base-FX для багатомодового оптоволоконного кабелю із двома волокнами.*

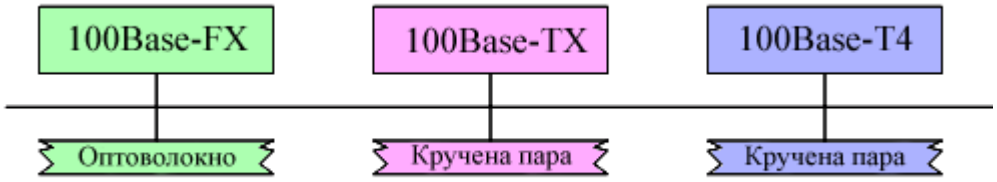

Рис. 1.8 Специфікації технології Fast Ethernet

Специфікація 100Base-FX визначає роботу протоколу Fast Ethernet за багатомодовим оптоволокном у напівдуплексному й дуплексному режимах.

У ***специфікації 100Base-TX*** як середовище передачі даних використовується кручена пара UTP категорії 5 або STP типу 1.

Специфікація 100Base-T4 з'явилася пізніше інших специфікацій фізичного рівня Fast Ethernet. Для роботи використовується кабель UTP категорії 3, що містить чотири пари.

Технологія Gigabit Ethernet

Улітку 1996 р. було оголошено про створення групи 802.3z для розробки протоколу, у максимальному ступені подібного Ethernet, але з бітовою швидкістю 1000 Мбіт/с. Технологія отримала назву Gigabit Ethernet. Стандарт 802.3z був остаточно прийнятий у 1998 р. Роботи з реалізації

Gigabit Ethernet на крученій парі категорії 5 були передані проблемній групі 802.3ab через складність забезпечення гігабітної швидкості на цьому типі кабелю, який був створений для підтримки швидкостей 100 Мбіт/с. Проблемна група 802.3ab успішно впоралася зі своїм завданням, і версія Gigabit Ethernet для крученої пари категорії 5 також була прийнята.

Для багатомодового оптоволокна стандарт 802.3z визначає специфікації 1000Base-SX і 1000Base-LX. У першому випадку використовується довжина хвилі 850 нм (S — Short Wavelength), а в другому — 1300 нм (L — Long Wavelength). Специфікація 1000Base-SX може використовувати тільки багатомодовий кабель, при цьому його максимальна довжина складає близько 500 м.

Для специфікації 1000Base-LX як джерело випромінювання завжди застосовується напівпровідниковий лазерний діод з довжиною хвилі 1300 нм. Специфікація 1000Base-LX може працювати як із багатомодовим (максимальна відстань до 500 м), так і з одномодовим кабелем (максимальна відстань залежить від потужності передавача і якості кабелю й може сягати декількох десятків кілометрів). Лінійний код, застосовуваний для цих специфікацій — 8B/10B.

Специфікація також визначає роботу Gigabit Ethernet по крученій парі категорії 5. Кожна пара кабелю категорії 5 має гарантовану смугу пропускання до 100 МГц. Для передачі даних по такому кабелю зі швидкістю 1000 Мбіт/с було вирішено організувати паралельну передачу одночасно за всіма чотирма парами кабелю. Це відразу знизило швидкість передачі даних по кожній парі до 250 Мбіт/с. Для кодування даних був застосований код PAM5, у якому 5 рівнів потенціалу: –2, –1, 0, +1, +2. Тому за один такт по одній парі передається 2,322 бітів інформації (log25). Отже, для досягнення швидкості 250 Мбіт/с тактову частоту 250 МГц можна зменшити в 2,322 рази. Розробники стандарту вирішили використати трохи вищу частоту, а саме 125 МГц. При цій тактовій частоті код PAM5 має спектр вужче, ніж 100 МГц, і може бути переданий без викривлень по кабелю категорії 5.

Технологія FDDI

Технологія Fiber Distributed Data Interface (FDDI) — перша технологія локальних мереж, яка використала як середовище передачі даних оптоволоконний кабель. Спроби застосування світла як середовища, яке несе інформацію, були давно — ще в 1880 р. Олександр Белл запатентував пристрій, який передавав мову на відстань до 200 метрів за допомогою дзеркала, що вібрувало синхронно зі звуковими хвилями й модулювало відбите світло.

Нині більшість мережних технологій підтримують оптоволоконні кабелі, як одного з варіантів фізичного рівня, але FDDI залишається найбільш відпрацьованою високошвидкісною технологією, стандарти на яку пройшли перевірку часом й устоялися, так що обладнання різних виробників показує високий ступінь сумісності.

Технологія FDDI багато в чому ґрунтується на технології Token Ring, розвиваючи й удосконалюючи її основні ідеї. Розроблювачі технології FDDI ставили перед собою як найбільш пріоритетні такі цілі:

- *підвищити бітову швидкість передачі даних до 100 Мбіт/с;*
- *підвищити відмовостійкість мережі за рахунок стандартних процедур відновлення її після відмов різного роду — пошкодження кабелю, некоректної роботи вузла, концентратора, виникнення високого рівня завад на лінії тощо;*
- *максимально ефективно використати потенційну пропускну здатність мережі як для асинхроного, так і для синхроного трафіку.*

Мережа FDDI будується на основі двох оптоволоконних кілець, які утворюють основний і резервний шляхи передачі даних між вузлами мережі. Використання двох кілець — це основний спосіб підвищення відмовостійкості в мережі FDDI, і вузли, які хочуть ним скористатися, мають бути підключені до обох кілець. У нормальному режимі роботи мережі, дані проходять через всі вузли й всі ділянки кабелю первинного (Primary) кільця,

тому цей режим названий режимом Thru — «наскрізним» або «транзитним». Вторинне кільце (Secondary) у цьому режимі не використовується.

У випадку якого-небудь виду відмови, коли частина первинного кільця не може передавати дані (наприклад, обрив кабелю або відмова вузла), первинне кільце поєднується із вторинним (рис. 1.4.16), створюючи знову єдине кільце. Цей режим роботи мережі називається Wrap, тобто «згортання» кілець. Операція згортання проводиться силами концентраторів й/або мережних адаптерів FDDI. Для спрощення цієї процедури дані по первинному кільцю завжди передаються проти годинникової стрілки, а по вторинному — за годинниковою. Тому при створенні загального кільця із двох кілець, передавачі станцій як і раніше залишаються підключеними до приймачів сусідніх станцій, що дозволяє правильно передавати й приймати інформацію сусідніми станціями.

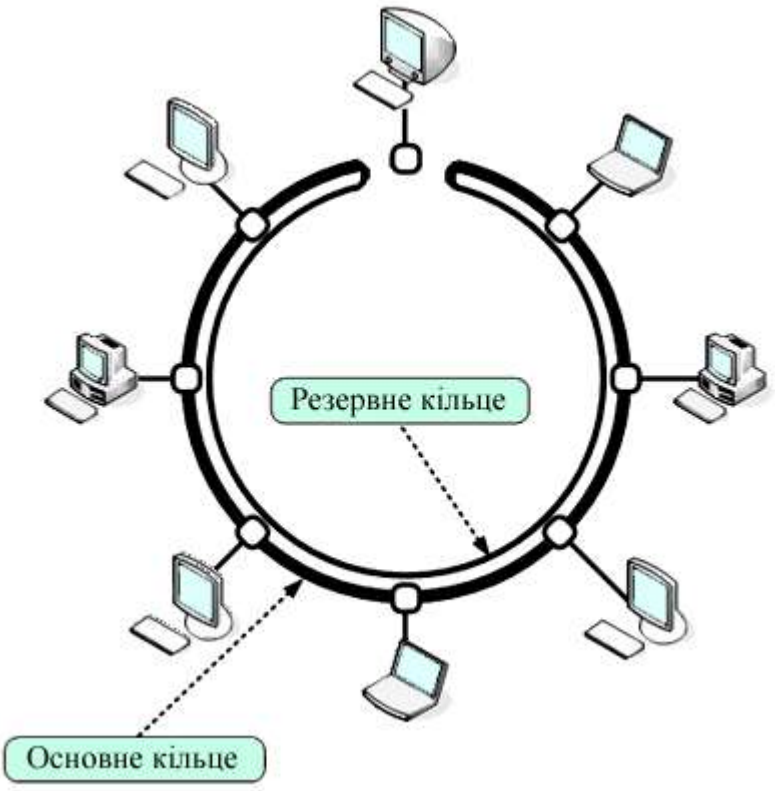

Рис. 1.9. Технологія FDDI

У стандартах FDDI багато уваги приділяється різним процедурам, які дозволяють визначити наявність відмови в мережі, а потім зробити необхідну в таких випадках реконфігурацію. Мережа FDDI може повністю

відновлювати свою працездатність у разі одиничних відмов її елементів. При множинних відмовах мережа розпадається на декілька незв’язаних мереж.

Кільця в мережах FDDI розглядаються як загальне середовище передачі, тому для неї визначений спеціальний метод доступу. Цей метод дуже близький до методу доступу мереж Token Ring і також називається методом маркерного (або токенного) кільця — token ring. Станція може почати передачу своїх власних кадрів даних тільки в тому разі, якщо вона отримала від попередньої станції спеціальний кадр — токен доступу. Після цього вона може передавати свої кадри, якщо вони в неї є, протягом часу, який називається часом утримання токена — Token Holding Time (THT). Після часу THT станція зобов’язана завершити передачу свого чергового кадру й передати токен доступу наступній станції. Якщо ж у момент прийняття токена в станції немає кадрів для передачі мережею, то вона негайно транслює токен наступній станції. У мережі FDDI у кожної станції є попередній сусід (upstream neighbor) і наступний сусід (downstream neighbor), які визначаються її фізичними зв’язками й напрямком передачі інформації.

Огляд сучасного обладнання для побудови мереж

Для побудови комп’ютерної локальної мережі використовується два види обладнання: основне (активне) та другорядне (неактивне). До активного обладнання відносять: маршутизатор, комутатор та сервер, концентратори, мережеві адаптери, репітери, ретранслятори, медіаконвертори, IP-камери, точки доступу WI-FI. До неактивного відносять зв’язуючи елементи, а саме оптоволокно та інші.

Маршутизатор, або в простонароді роутер— електронний пристрій, що використовується для поєднання двох або більше мереж і керує процесом маршрутизації, тобто на підставі інформації про топологію мережі та певних правил приймає рішення про пересилання пакетів мережевого рівня, а саме рівень 3 “моделі OSI” між різними сегментами мережі.

Для звичайного користувача маршрутизатор насамперед є мережевим пристроєм, який підключається між локальною мережею й інтернетом. Часто маршрутизатор не обмежується простим пересиланням даних між інтерфейсами, а також виконує й інші функції: захищає локальну мережу від зовнішніх загроз, обмежує доступ користувачів локальної мережі до ресурсів інтернету, роздає IP-адреси, шифрує трафік і багато іншого.

Маршрутизатор є окремою підстанцією, яка приймає сигнали і передає їх певним пристроям. Частіше всього у вигляді останніх є комп'ютери, однак це не обов'язково. Справа в тому, що до інтернету за допомогою роботи маршрутизатора можуть підключатися камери, принтери, розумна техніка, також холодильники і кондиціонери. По суті, роутер пов'язує всі пристрої, які до нього підключені, і сервер, який забезпечує приймання сигналу і роботу інтернету. Говорячи про те, що це - маршрутизатор, потрібно визначитися з принципом його роботи.

Маршрутизатори працюють на мережевому рівні моделі OSI: можуть пересилати пакети з однієї мережі до іншої. Для того, щоб надіслати пакети в

потрібному напрямку, маршрутизатор використовує таблицю маршутизації, яка зберігається у його пам'яті. Таблиця маршутизації може складатися засобами статичної або динамічної маршутизації. Крім того, маршрутизатори можуть здійснювати трансляцію адреси відправника й одержувача, фільтрацію транзитного потоку даних на основі певних правил з метою обмеження доступу, шифрування та дешифрування даних що передаються. Маршрутизатори не можуть здійснювати передачу широкомовних повідомлень, таких як ARP-запит. Маршрутизатором може виступати як спеціалізований пристрій, так і звичайний комп'ютер, що виконує функції простого маршрутизатора.

Зазвичай маршрутизатор використовує адресу одержувача, вказану в пакетах даних, і визначає за таблицею маршрутизації шлях, за яким слід передати дані. Якщо в таблиці маршрутизації для адреси немає описаного маршруту, пакет відкидається.

Таблиця маршрутизації містить інформацію, на основі якої маршрутизатор приймає рішення про подальшу пересилку пакетів. Таблиця складається з деякого числа записів — маршрутів, в кожному з яких міститься адреса мережі одержувача, адреса наступного вузла, якому слід передавати пакети і певна вага запису, — метрика. Метрики записів в таблиці грають роль в обчисленні найкоротших маршрутів до різних одержувачів.

Для передачі даних шляхом маршрутизатора використовують статичну та динамічну маршрутизацію:

- *статична маршрутизація — коли записи в таблиці вводяться і змінюються вручну. Такий спосіб вимагає втручання адміністратора щоразу, коли відбуваються зміни в топології мережі. З іншого боку, він є найстабільнішим і таким, що вимагає мінімуму апаратних ресурсів маршрутизатора для обслуговування таблиці;*
- *динамічна маршрутизація — коли записи в таблиці оновлюються автоматично за допомогою одного або кількох протоколів маршрутизації — RIP, OSPF, EIGRP, IS-IS, BGP, і ін. Крім того,*

маршрутизатор будує таблицю оптимальних шляхів до мереж призначення на основі різних критеріїв — кількості проміжних вузлів, пропускної спроможності каналів, затримки передачі даних тощо. Критерії обчислення оптимальних маршрутів найчастіше залежать від протоколу маршрутизації, а також задаються конфігурацією маршрутизатора. Такий спосіб побудови таблиці дозволяє автоматично тримати таблицю маршрутизації в актуальному стані і обчислювати оптимальні маршрути на основі поточної топології мережі. Проте динамічна маршрутизація надає додаткове навантаження на пристрої, а висока нестабільність мережі може приводити до ситуацій, коли маршрутизатори не встигають синхронізувати свої таблиці, що приводить до суперечливих відомостей про топологію мережі в різних її частинах і втраті передаваних даних.

Необхідно зауважити, що однією з функцій роутера можна назвати роботу з протоколом DHCP. Завдяки йому спосіб роботи з даними набагато легше. Кожен пристрій, що підключається до такої техніки, має IP-адресу. Він є тимчасовим, а не постійним.

Класифікація маршрутизаторів

На даний момент є декілька класифікацій роутерів. Найбільш основними вважаються поділу за сферою застосування і за способом підключення.

За способом підключення

Пристрої можуть підключатися або дротовим або ***бездротовим*** способом до інтернету або ж до великої мережі. Розведення мережі за іншими приладами здійснюється підключенням за допомогою бездротової мережі, тобто Wi-Fi, або за рахунок оптоволоконного кабелю. В домашніх умовах часто використовуються варіанти проводового підключення маршрутизатора, а для комп'ютерів використовують бездротову технологію.

Рис. 2.1. Бездротовий маршрутизатор

Налаштування маршрутизатора ***проводового*** типу буде максимально простою. Як правило, такі пристрої купуються для роботи з мережами, де буде підключено два або три комп'ютера. Нерідко, залежно від моделі, можна підключити до 8 пристроїв. Як вже було написано вище, завдяки проводовому способу здійснити настройку можна буде максимально легко і просто. Та й впринципі не дуже важко навіть із інструкцією у більшості підприємств таких типу офіс стоїть дротовий маршрутизатор, який запезпечує стабільний сигнал і передачу даних усім абонентам, які під’єднані.

Рис. 2.2. Дротовий маршрутизатор

Ще одним цікавим пристроєм є Wi-Fi-роутер. Він може передавати дані як за допомогою кабелю, так і без нього. Тобто це такий собі аналог дротового та бездротового маршрутизатора, але навідміну від них працює, як і з тим, так і з тим. Як правило, настільні комп'ютери підключаються тільки за допомогою дротяного способу, а от побутові пристрої підтримують як такий, так і звичайний спосіб, по повітрю. Дуже все просто у мене в квартирі також використовується Wi-Fi-роутер куди за допомогою кабелю підключені настільні комп’ютери, а також можливо по повітрю ловити сигнал інтернету на мобільні пристрої та планшети і ще безліч інших.

Рис. 2.3. Wi-Fi-роутер

Маршрутизатори або роутери розділяють на три класи:

- ***нижній*** *(пристрої даного типу використовують для побудови мережі окремих офісів та будинку, вони зазвичай мають два порти глобальної мережі та чотири локальної);*
- ***середній*** *(клас який має на увазі об'єднання невеликої мережі для підприємства середнього розміру, такі пристрої працюють з 8 портами локальної мережі, і з трьома глобальної);*
- ***верхній*** *(пристрій, який поєднує великі організації і підприємства).*

Для того щоб мережа працювала надійно і безперебійно перед її побудовою і використанням маршрутизатора, проводять аналіз враховуючі усі аспекти мережі. Бездротовий маршрутизатор, як і дротовий, потрібно вміти вибирати. Заздалегідь необхідно обговорити з постачальником інтернету пристрій, який йому необхідно. Потрібно зауважити, що деякі фірми не підтримують роботу маршрутизаторів TP-Link або інших. Буває таке, що замість доступу в мережу людина отримує тільки витрачені гроші на маршрутизатор, який не підійшов. Якщо йдеться про промислове використання, то допускається поєднання відразу декількох пристроїв. Відмінно з таким завданням буде справлятися маршрутизатор TP-Link. Подібний пристрій буде мати більш складний маршрут і максимально захищену передачу інформації. Найчастіше таке вимагається тільки при роботі в офісі. Для домашнього пристрою буде цілком достатньо одного маршрутизатора простого типу.

Кожен клієнт який використовує для власних потреб чи потреб компанії має бути впевнений у захисті його даних від зловмисників і хакерів. До системи безпеки відносять:

- ***Firewall*** — деякі адреси або порти можуть бути закриті повністю, ні один пакет ніколи не потрапить і не покине мережу при правильному налаштуванні цієї підсистеми;
- ***VPN*** — віртуальні приватні мережі. При цьому всередині (а точніше, «поверхньо») мережі формується віртуальний зашифрований сегмент,

який має власну систему адресації. Чужі комп'ютери не зможуть відправити шкідливі пакети при такій організації трафіку;

- ***NAT*** — трансляція мережевих адрес. Роутер змінює заголовок пакета таким чином, щоб приховати подробиці внутрішньої організації мережі від зовнішніх спостерігачів.

Що ж стосується виробників маршрутизаторів та Wi-Fi-роутерів, то слід виділити 3 потужний компанії: **TP-Link, ASUS, D-Link.**

Компанія TP-Link має солідний стаж роботи – понад 20 років. Спочатку їхня продукція була націлена виключно на внутрішній ринок Китаю. Однак в 2005 році ситуація змінилася і товари бренду стали доступні на міжнародній арені.

На даний момент виробник входить до переліку компаній-лідерів в сфері створення техніки класу SOHO (для невеликих офісів, домашнього вжитку). Маршрутизатор – один з основних товарів, які виробляє бренд, ще в асортименті є, наприклад, смартфони і мережеві адаптери.

Серед основних плюсів роутерів TP-Link варто виділити:

- **Вибір девайсів на будь-який смак,** продукції бренду покупці знайдуть гаджети з 3-ма різними видами підключення: ADSL (підключення за допомогою телефонної лінії), 3G (бездротовий інтернет), Ethernet. Перші відрізняються невисокою вартістю і максимальною швидкістю до 300 Мбіт/с. Другі – мобільністю і можливістю підключення в будь-якому місці. Треті – наявністю 2-5 антен, включаючи змінні, що позитивно позначається на дальності і швидкості передачі інформації;
- **Різноманіття корисних опцій,** підібрати апарати, в яких є функція батьківського контролю (обмеження доступу), гостьова мережа (організація окремого доступу), дистанційне керування (налаштування, увімкнення/вимикання апарату через Інтернет) та інші;
- **Оригінальний дизайн**, компактні за розмірами і радують користувачів нетривіальним зовнішнім виглядом: можна вибрати білі, чорні, сріблясті, сині агрегати з гладкою або рифленою поверхнею. Форма корпусу – від

стандартного прямокутника до незвичайних конструкцій з вигнутою поверхнею.

Ціновий розбір в асортименті даного бренду досить великий, можна підібрати недорогі девайси з мінімум опцій або придбати більш функціональні агрегати, ціна яких вище середнього. Я власне використовую в себе дома роутер саме цієї фірми, він є надійний і не дуже дорогий, забезпечує безперебійну роботу.

ASUS є Тайванським брендом успішно підкорює світові вершини в сфері IT-технологій. На його виробничому рахунку величезна кількість суперсучасних гаджетів: смартфонів, ноутбуків, планшетів і іншого. Кожен девайс обладнаний за останнім словом техніки, не виняток і роутери ASUS.

Виробник випускає маршрутизатори, в яких є:

- фірмовий веб-інтерфейс – дозволяє в швидкісному режимі налаштувати інтернет-коннект і швидко налагодити параметри роботи техніки;
- утиліта AirPlayer – служить для трансляції мультимедіа з підключеного до роутера USB-диска на мобільний девайс;
- батьківський контроль – обмеження доступу до веб-сторінок, а також створення розкладу для входу в інтернет;
- технологія захисту – AiProtection забезпечує надійну охорону від стороннього втручання, проникнення вірусів в мережу цифрових девайсів, підключених до маршрутизатора;
- підключення принтера, USB-накопичувача – можна підключити до апарату зовнішній HDD, модем і використовувати їх в якості загальнодоступного мережевого ресурсу.

В асортименті бренду є як простенькі агрегати для будинку, так і потужні бездротові гаджети для використання в бізнес-цілях. Окрема лінійка присвячена ігровим девайсів (двох, трьохдіапазонним). Крім надшвидкісної роботи в них є потужний чіпсет, передбачена можливість об'єднати кілька маршрутизаторів в одну домашню мережу, широка область покриття.

Компанія D-Link утворена понад 30 років тому і входить до переліку провідних світових виробників мережевих приладів. Родина бренду – Тайвань. Продукція фірми радує покупців доступністю цін і довговічністю роботи.

Виготовлення маршрутизаторів – тільки один з витоків діяльності D-Link. Компанія також спеціалізується на створенні «цифрових» будинків, випуск ПК, ноутов, TV та іншого сучасного обладнання. ***В роутерах D-Link безліч оригінальних технічних рішень. Ось деякі з них:***

- Функція Beamforming – технологія обробляє, формує і підтримує високу швидкість передачі сигналу у важких місцях, наприклад, при проході крізь товсті стіни. Прилад «відчуває», де сигнал втрачається і коригує свою роботу відповідно;
- Установка пріоритетів – це стосується, наприклад, онлайн розваг: щоб нічого не заважало грі, потрібно присвоїти їй в налаштуваннях апарата максимальне значення. В цьому випадку ніякі оновлення ОС або антивіруса не вплинуть на пропускну здатність пристрою;
- 3-діапазоний зв'язок – реалізований в геймерських апаратах. Пропускна здатність в них досягає 3-5 Гбіт/с. Цього достатньо для онлайн-розваг, перегляду якісного відео і інших завдань без гальм і провалів в швидкості.

Комутатор або перемикач - це пристрій, що дозволяє з'єднувати кілька ділянок комп'ютерної мережі. Дане обладнання є свого роду багатопортовим мостом між комп'ютерами в мережі. Відмінною рисою комутатора є можливість передавати пакети даних конкретному одержувачу, що оптимізує роботу мережі, знижуючи навантаження, підвищуючи безпеку. Завдяки можливості "думати" комутатори витіснили концентратори (хаби) і активно використовуються в побудові мереж.

Можливість адресної відправки пакетів досягається шляхом фіксації індивідуальних MAC-адрес підключених комп'ютерів в спеціальній таблиці, яка заповнюється в міру використання світча користувачами і зверненнями до мережі. У міру отримання інформації про підключені пристрої, комутатор

"розуміє" куди відправляти отримані пакети, що істотно підвищує продуктивність.

При обрані, який саме вам потрібен комутатор слід визначити критерії вибору, які необхідні вам для нормальної роботи комутатора, для початку треба визначити кількість абонентів, які буде підключено до мережі, для домашньої мережі підійде простий 5-ти або 8-ми портовий комутатор. Для розгортання мережі в офісі варто подбати про наявність резерву, так як може знадобитися вільний порт під мережевий принтер або інше обладнання. Більшість комутаторів використовують порти зі швидкістю 100 Мбіт/с. Порти (1000 Мбіт/с) можуть бути актуальні для мереж підприємств і фірм. Такі порти використовуються для підключення серверів, або іншого комунікаційного устаткування для отримання високошвидкісного з'єднання. Тому при покупці і виборі комутатора слід враховувати наступні характеристики такі як: кількість і тип портів; швидкість портів (10/100/1000 Мбіт/сек); наявність можливості управління (керований/некерований); виробник устаткування; додаткові можливості і характеристики

Рис. 2.4. Типовий комутатор виробництва фірми 3Com

Комутатор працює наступним чином, візьмемо наприкладі вузла А. Всі кадри, які виходять від вузла А і мають в заголовку адресу, одержує клієнт в сегменті Бета (наприклад, R), надходять в перший порт комутатора другого

рівня, а потім він виходить з другого порту, щоб бути переданим в вузол R. Такий процес має назву «ретрансляція», по англійські – forwarding. Кадр виходить ретранслювати в тому випадку, якщо він був прийнятий одним портом комутатора 2-го рівня і переданий через інший порт пристрою.

Кадр, який виходить з вузла А і має адресу одержувача пункту В, надходить і на місце призначення, і на комутатор другого рівня, але той визначає, що вузли мають один сегмент, і не передає його. Цей процес називається фільтрацією, тобто, якщо комутатор отримує кадр, але не передає його, то він називається відфільтрованим.

Логічно, що якщо у визначенні маршрутизатора йдеться про роботу пристрою на швидкості каналу, то називати його повільним немає сенсу, адже його продуктивність в даному випадку залежить безпосередньо від каналу зв’язку.

Ретрансляція кадрів з сегмента ЛВС в інший комутатор може здійснюватися за допомогою таких способів комутації, як:

- Наскрізна комутація (Cute-Through);
- Наскрізна комутація модифікована (Interim Cute-Through);
- Проміжна буферизация або накопичення з подальшою ретрансляцією (Store-and-Forward);
- Комутація гібридного типу.

Не варто говорити, що у кожного типу комутації є і свої плюси, і вагомі недоліки.

Для технології комутації другого рівня характерні висока продуктивність, що дозволяє створювати складні мережі широкомовних областей-доменів.

Комутатори мають свою кваліфікацію, на даний момент існує чотири види мережевих комутаторів: некеровані комутатори, керовані комутатори, інтелектуальні комутатори і керовані комутатори підприємства. Кожен тип має свої сильні і слабкі сторони, які необхідно враховувати.

Некерований комутатор є найдешевшим варіантом і зазвичай використовується в невеликому офісі або на підприємстві. Вони виконують основні функції управління потоком даних між загальним принтером і декількома комп'ютерами. Вони можуть бути настільними або змонтованими в стійку.

Керований комутатор має користувальницький інтерфейс або програмне забезпечення, яке дозволяє користувачам змінювати налаштування комутатора. Існує кілька способів поновлення мережевого комутатора – від послідовної консолі до інтернет-додатків. Пристрій такого типу вимагає, щоб знаючий користувач в міру необхідності коригував налащтування.

Інтелектуальний комутатор – це проміжний продукт, який встановлюється між некерованим і керованим комутатором. Інтерфейс є веб-інтерфейсом і має найпопулярніші налаштування за замовчуванням. Коригування одного налаштування призводить до автоматичного налаштування відповідного пункту.

Керований підприємством мережевий комутатор має широкий діапазон налаштувань, що дозволяє використовувати його у великій компанії або організації. Вони зазвичай управляються мережевими фахівцями і постійно контролюються. Ці пристрої абсолютно необхідні для управління комп'ютерною мережею. Вони функціонують як система управління трафіком в мережі, направляючи пакети даних в правильний пункт призначення. Вони використовуються для підключення периферійних пристроїв до мережі і забезпечення максимальної економічної ефективності і можливості спільного використання ресурсів.

Якщо взяти найпопулярніші виробники комутаторів, то найбільшим попитом зокрема в Україні користується такі фірми TP-link, Ubiquiti, D-link, Zyxel, Mikrotik, 2e, Netis, HP, Linksys.

Сервер – це потужний комп’ютер призначений для зберігання інформації і запезпечення доступа до неї з віддалених клієнтський пристроїв. Тип даних, які зберігаються на сервері, залежить від його виду і призначення.

.Простими словами – це спеціальний комп’ютер, який служить тому щоб та чи інша інформаційна мережа могла повноціно функціонувати.

З терміном "сервер" нерозривно пов'язаний інший термін - "клієнт". Так називається персональний комп'ютер, мобільний або інший пристрій, що знаходиться в одній мережі з сервером, що спрямовує на нього ті чи інші запити і отримує необхідну інформацію.

Ця машина в залежності від її типу та призначення може виконувати різні корисні функції:

• зберігати інформацію одного чи кількох сайтів. Так працюють сервери інтернет-провайдерів, які надають послуги хостингу;

• координувати взаємодію багатьох комп'ютерів, що знаходяться в одній мережі. Класичний приклад – ігрові сервери;

• використовуватись для зберігання корпоративних даних та доступу працівників до них. Один із можливих прикладів — сервер у центральному офісі компанії, на якому зберігається та регулярно оновлюється бухгалтерська база даних.

Це лише деякі з поширених способів використання серверів. Нижче ми розглянемо існуючі види цих машин і детальніше розкриємо питання їх застосування.

Будь-який сервер незалежно від його типу та призначення є комп'ютером. Саме тому він має на борту класичні комп'ютерні комплектуючі:

- материнську плату, яка відіграє роль основи системи;
- один чи кілька центральних процесорів;
- певний обсяг оперативної пам'яті;
- систему зберігання даних, що складається з накопичувачів тієї чи іншої типу.

«Залізо» сервера за принципової схожості з комплектуючими стандартного комп'ютера має і власну специфіку. Вона пов'язана з тим, що основні завдання серверного обладнання - зберігання, інтенсивна обробка та швидка передача великих обсягів даних. Щоб вони успішно виконувалися, сервери оснащують:

- високопродуктивними багатоядерними процесорами;
- великий обсяг оперативної пам'яті з контролем помилок;
- ємними та швидкісними жорсткими дисками та твердотілими накопичувачами.

Існує багато типів серверів, які використовуються спеціалістами для власної роботи і вони пібираються під конкретну роботу.

Web-сервер

Це найпопулярніший з усіх серверів. На web-серверах зберігається текстовий, графічний, відео та інший контент, з якого складаються інтернет-сайти. Відвідувач надсилає запит, використовуючи для цього браузер персонального комп'ютера або мобільного пристрою, що відіграє роль клієнта. Web-сервер дає відповідь у форматі HTTP та надсилає клієнту дані. В результаті відвідувач бачить на екрані сайт, що його цікавить, переходить по сторінках, відправляє через форми дані - словом, взаємодіє з web-сервером.

Ігровий сервер

Ця машина забезпечує взаємодію гравців, що запускають ту саму гру в режимі мультиплеєра і одночасно перебувають у віртуальному світі. Дуже багато в світі ігор і кожна ігрова платформа має свою машину тобто сервер. У всіх випадках мова йде саме про ігрові сервери, причому у випадку з відомими іграми вони є дуже потужними, адже їм доводиться витримувати чималі навантаження.

Відеосервер

Даний сервер використовується для зберігання відеороликів, фільмів, кліпів і так далі. Користувач, звертаючись до відеосервера зі свого пристрою,

отримує можливість дивитися відео, не завантажуючи його і не витрачаючи власний дисковий простір. Найбільший відеосервер це YouTube.

Серевер локальної мережі

Так називається сервер, до якого організований обмежений доступ, наприклад, усередині корпоративної мережі, розгорнутої на підприємстві. Завдяки її наявності співробітники, перебуваючи на різних (і нерідко дуже віддалених) робочих місцях, можуть одночасно використовувати інформацію, наприклад, бухгалтерську базу даних тай різні інші бази даних, та інформацію про сервер та його особливості. Такий сервер дозволяє спілкуватися з робочих питань, відстежувати виконання доручень, вирішувати багато інших завдань.

Поштовий сервер

Застосовується для зберігання електронної пошти, надсилання листів, фільтрації спаму, сортування електронних листів за категоріями, вирішення інших завдань, пов'язаних з використанням e-mail. Серед найбільш відомих сервісів, що дозволяють скористатися поштовими серверами - Mail, Yandex, Gmail, інші. Таку можливість дають і хостинг-провайдери, які виготовляють електронні скриньки на персональних доменах користувачів.

FTP-сервер

Використовується для зберігання файлів та віддаленого доступу до них по FTP – File Transfer Protocol. Залежно від призначення та масштабу сервера доступ може бути реалізований як через Інтернет, так і через локальну мережу. Якщо у випадку з web-сервером користувачі працюють у браузерах, то в даному випадку найзручніше використовувати спеціалізовані програми для передачі файлів - наприклад, Filezilla.

DNS-сервер

DNS-сервер напряму зв’язаний із IP-адресою, що являє собою набір кількох груп цифр, розділених точками. Знаючи його, можна відкрити сайт, завантажити файли, вирішити інші завдання, пов'язані з доступом до сервера. Є проблеми: набір цифр набагато складніше запам'ятати, до того ж, він зміниться при переїзді сайту на інший хостинг. Вони вирішуються за допомогою доменних імен - простіше кажучи, звичних кожній адресі веб-сайтів. Зв'язок між IP-адресами та доменними іменами забезпечують DNS-сервери. Вони потрібні для автоматичного визначення згаданих вище наборів цифр під час введення користувачами адрес сайтів.

VPN-сервер

Це обладнання забезпечує роботу віртуальної мережі, яка дозволяє зашифрувати та захистити персональні дані користувачів. Останні можуть користуватися загальнодоступним каналом зв'язку, тобто Інтернетом, проте завдяки серверу VPN залишатися при цьому всередині захищеної приватної мережі.

Проксі-сервер

Однією з функцій цього серверного обладнання є кешування (збереження на локальному диску) інформації, отриманої з Інтернету. При повторному зверненні проксі-сервер віддає збережені дані користувачеві, роблячи непотрібним черговий вихід у всесвітню мережу та заощаджуючи трафік.

У комп’ютерній мережі університу, задіяні у роботі сервери двох типів такі, як **Windows Server** та **CentOS**. Ці сервери складають основу і безпеку мережі університета імені Івана Огієнка.

Windows Server — лінійка серверних операційних систем компанії Microsoft.

Формально не входять до продуктової лінійки, як такі, що мають іншу торгову марку, однак є попередніми версіями серверних ОС сімейства NT, за цей час вийшло безліч версій і ось які, і роки їх випуску:

- Windows NT 3.1 Advanced Server (27 липня 1993)
- Windows NT 3.5 Server (21 вересня 1994)
- Windows NT 3.51 Server (30 травня 1995)
- Windows NT 4.0 Server (серпень 1996)
- Windows 2000 Server (лютий 2000)
- Windows .NET Server (2002)
- Лінійка складається з наступних версій[2][3]:
- Windows Server 2003 (Квітень 2003)
- Windows Server 2003 R2 (Грудень 2005)
- Windows Server 2008 (лютий 2008)
- Windows Server 2008 R2 (Жовтень 2009)
- Windows HPC Server 2008 (Вересень 2010)
- Windows Server 2012 (вересень 2012)
- Windows Server 2012 R2 (Жовтень 2013)
- Windows Server 2016 (вересень 2016)
- Windows Server 2019 (Жовтень 2018)
- Windows Server 2022 (серпень 2021)

Microsoft також випустила Windows Small Business Server, версія для малих підприємств. Ці версії включають серверну операційну систему разом з набором інших програмних продуктів компанії.

CentOS (***C****ommunity* ***ENT****erprise* ***O****perating* ***S****ystem*) — вільно доступний дистрибутив Linux, на основі якого формується комерційний дистрибутив Red Hat Enterprise Linux компанії Red Hat. У минулому (до версії 8 включно) метою проєкту було складання 100 % двійково сумісного з RHEL дистрибутиву. Підтримка CentOS 8 припинилася 31 грудня 2021 року; користувачам запропоновано перейти на безперервно оновлювану редакцію CentOS Stream або на альтернативні дистрибутиви, що використовують формат пакунків RPM.

Основними інструментами керування пакунками у CentOS є yum (у CentOS 7 і раніших версіях) і dnf (починаючи з CentOS 8).

CentOS придатний для використання базованих на X Window стільницях, однак більш звично використовувати його, як серверну операційну систему для веб-хостингу. Багато великих хостингових компаній використовують CentOS разом із cPanel Control Panel для забезпечення стабільної роботи для своїх веб-застосунків.

Оптоволокно – кабель, який складаєься з тоненьких проводків, які один від одного відділяються спецальним покриттям, це є нашвидший спосіб передачі даних по мережі інтернет в світі. Кожний провід передає світло, а світло передає дані по мережі. Він передає дані не тільки інтернет-з'єднання, а й стаціонарний телефон, але зараз в 2022 році стаціонарний телефон вже є рідкістю ніж 15-20 років тому, зараз дуже рідко можна знайти стаціонарний телефон, а також оптоволокно передає сигнал телебачення, це воно також популярне, але зараз телебачення відійшло на другий план, а інтернет вийшов на перший.

Основними елементами є те, що оптоволокно маючи оптичні промені всередені таких волокон, які проходять через кременевий сердечник кожного волокна. Вони здатні переносити дані на великі відстані, можливо налаштувати з'єднання не тільки якогось окремого міста чи села, а й великих країн та континетів.

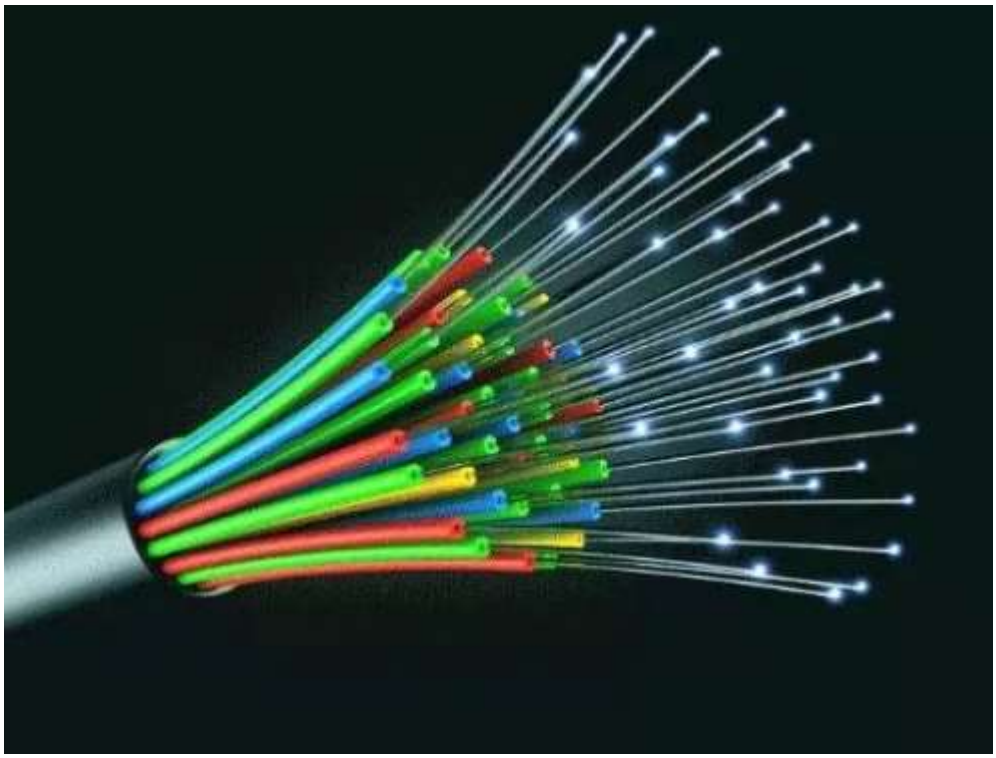

Рис. 2.5. Оптоволокно

Серед основних переваг використання оптоволокна наступні:

- Саме оптоволокно є довговічним матеріалом, який має високий рівень пропускної можливості, саме це відповідає за високу швидкість передачі даних;
- Оптоволокно є безпечним варіантом передачі даних, оскільки програмне запезпечення виявляє моментом факт несанкціонованого доступу до даних мережі;
- Оптоволокно добре захищає від перещкод та є добрим шумоподавлювачем;
- Оптоволокно має хорошу швидкість передачі даних навідміну від інших, особливо файли, аудіо та відео;
- Підключення оптоволокна дозволяє організувати систему для ряду додаткових опцій, до прикладу, для встановки системи відеонагляду або охоронних пристроїв.

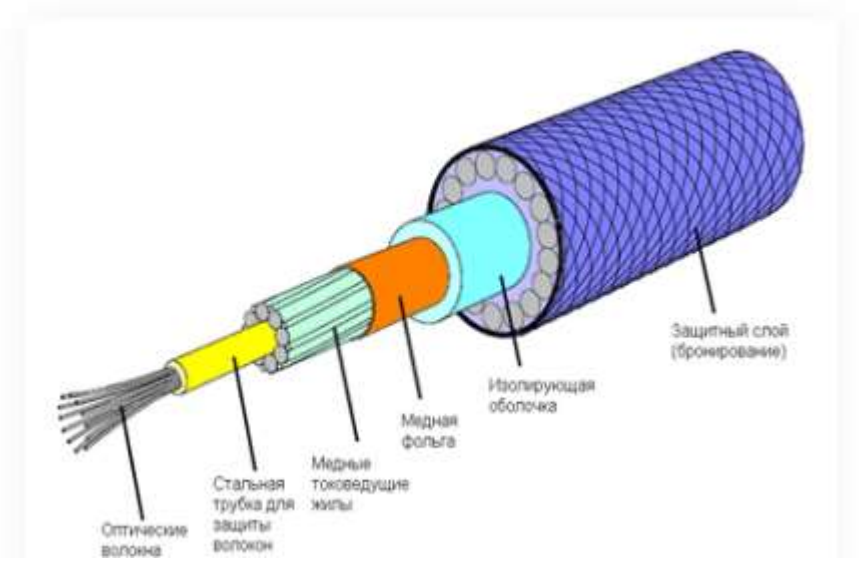

Рис. 2.6. Схема побудови кабелю оптоволокна

Концептуальний огляд мережі

Технологія VLAN

VLAN (Virtual Local Area Network, віртуальна локальна мережа) - це функція в роутерах та комутаторах, що дозволяє на одному фізичному мережному інтерфейсі (Ethernet, Wi-Fi інтерфейсі) створити кілька віртуальних локальних мереж. VLAN використовують для створення логічної топології мережі, яка не залежить від фізичної топології.

VLAN дуже популярна мережа і спектр її використання все більше розширюється на підприємствах чи учбових закладах використовують різні технології застосування технології VLAN, зокрема:

- ***Об'єднання в єдину мережу комп'ютерів, підключених до різних комутаторів.***

Допустимо, у вас є комп'ютери, які підключені до різних світильників, але їх потрібно об'єднати в одну мережу. Одні комп'ютери ми об'єднаємо у віртуальну локальну мережу VLAN 1, а інші — у мережу VLAN 2. Завдяки функції VLAN комп'ютери в кожній віртуальній мережі будуть працювати, немов підключені до одного й того ж комутатора. Комп'ютери з різних віртуальних мереж VLAN 1 та VLAN 2 будуть невидимі один для одного.

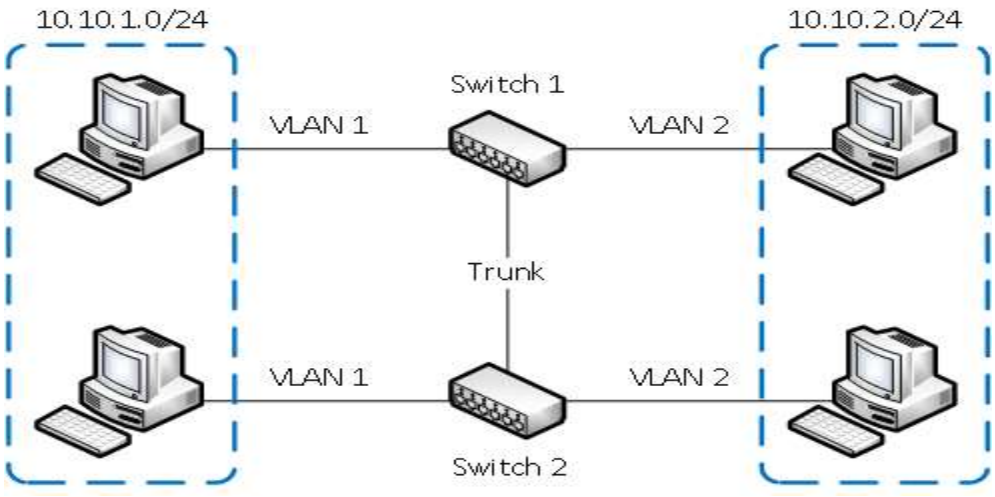

Рис. 3.1. Об’єднання в єдину мережу комп’ютерів, підключених до різних комутаторів

- ***Поділ у різні підмережі комп'ютерів, підключених до одного комутатора.***

На Рис 3.2 комп'ютери фізично підключені до одного комутатора, але розділені в різні віртуальні мережі VLAN 1 та VLAN 2. Комп'ютери з різних віртуальних підмереж будуть невидимі один для одного.

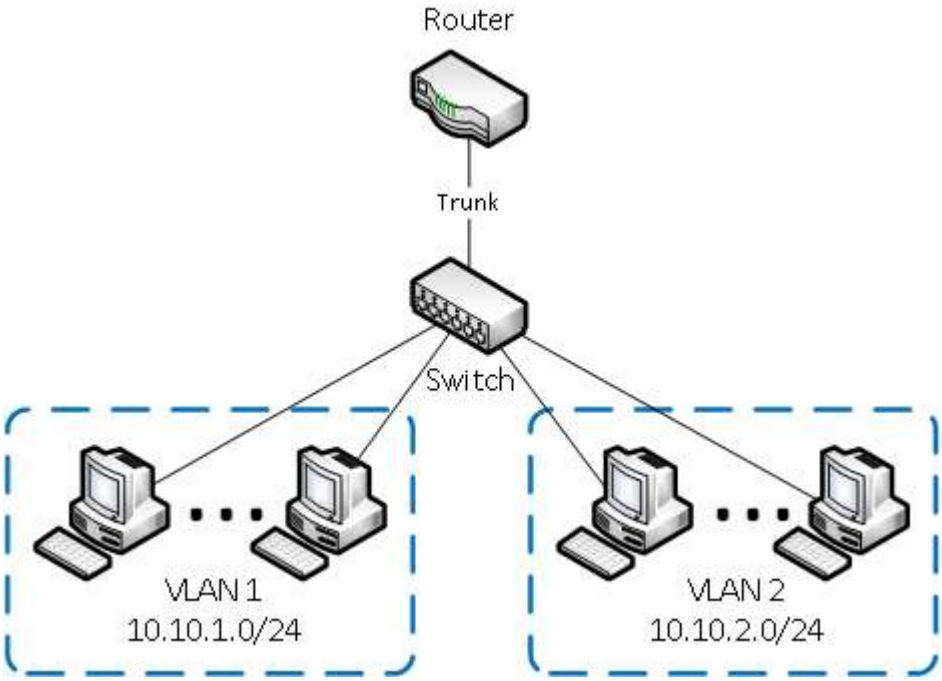

Рис. 3.2. Поділ у різні підмережі комп'ютерів, підключених до одного комутатора

- ***Поділ гостьової Wi-Fi мережі та Wi-Fi мережі підприємства.***

На Рис 3.3 показано поділ фізично одна Wi-Fi точка доступу. На точці створено дві віртуальні Wi-Fi точки з назвами HotSpot та Office. До HotSpot будуть підключатися Wi-Fi гостьові ноутбуки для доступу до інтернету, а до Office - ноутбуки підприємства. З метою безпеки необхідно, щоб гостьові ноутбуки не мали доступу до мережі підприємства. Для цього комп'ютери підприємства та віртуальна Wi-Fi точка Office об'єднані у віртуальну локальну мережу VLAN 1, а гостьові ноутбуки будуть знаходитись у віртуальній мережі VLAN 2. Гостьові ноутбуки з мережі VLAN 2 не матимуть доступу до мережі підприємства VLAN 1.

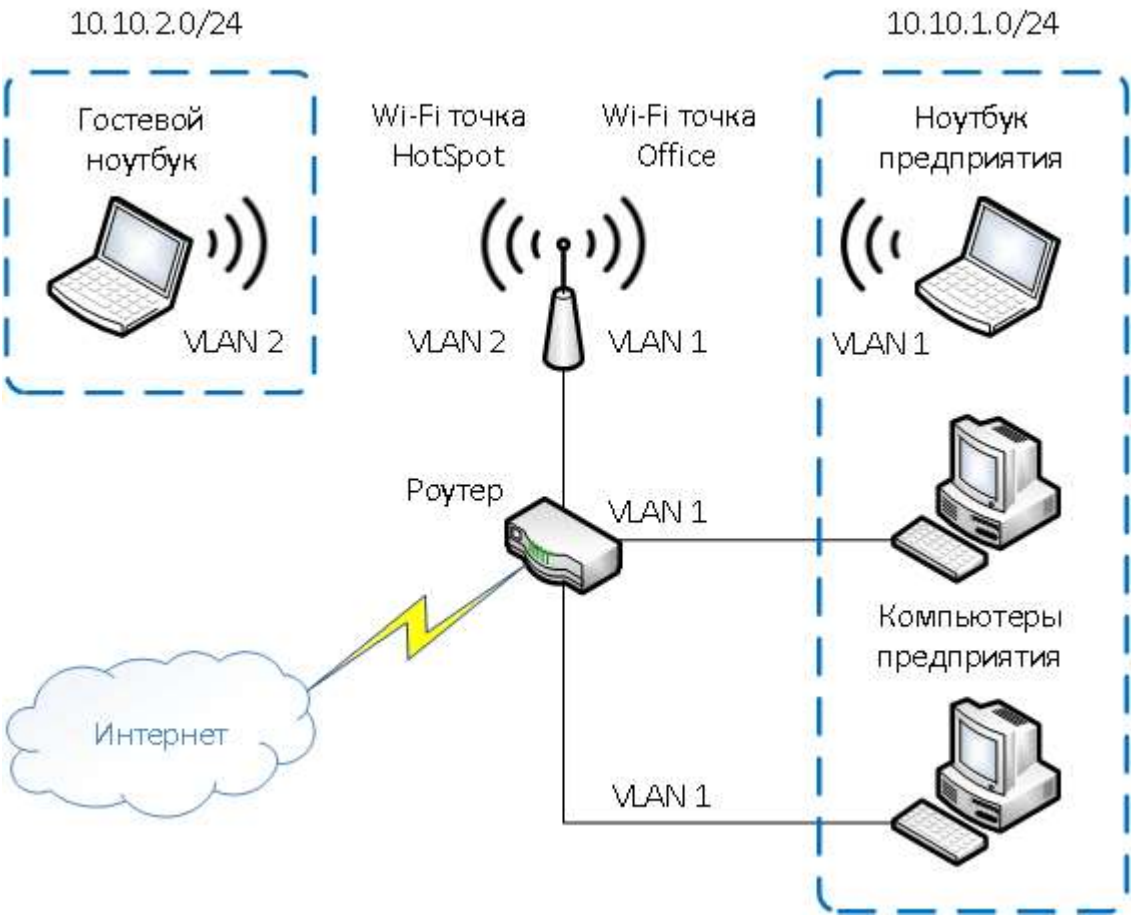

Рис. 3.3. Поділ гостьової Wi-Fi мережі та Wi-Fi мережі підприємства

Серед основних переваг за що обирають клієнти VLAN це:

- ***Гнучкий поділ пристроїв на групи*** (як правило, одному VLAN відповідає одна підмережа, а комп'ютери, що знаходяться в різних VLAN, будуть ізольовані один від одного. Це дає можливість з'єднувати в одну мережу комп'ютери, що підключені до різних комутаторів);
- ***Зменшення широкомовного трафіку в мережі*** (кожен VLAN є окремим широкомовним доменом. Широкомовний трафік не транслюватиметься між різними VLAN. Якщо на різних комутаторах налаштувати той самий VLAN, то порти різних комутаторів утворюватимуть один широкомовний домен);
- ***Збільшення безпеки та керованості мережі*** (у мережі, розбитій на віртуальні підмережі, зручно застосовувати політики та правила безпеки для кожного VLAN. Політика буде застосована до цілої підмережі, а не до окремого пристрою);

- ***Зменшення кількості обладнання та мережевого кабелю*** (для створення нової віртуальної локальної мережі не потрібно купувати комутатор і прокладати мережевий кабель. Однак, потрібно використовувати більш дорогі керовані комутатори з підтримкою VLAN).
- ***Гнучка побудова мережі*** — VLAN дозволяє сегментувати локальну мережу на підмережі за функціональною ознакою незалежно від територіального розташування пристроїв. Тобто, пристрої однієї підмережі VLAN можуть бути підключені до різних комутаторів, віддалених один від одного. І навпаки, до одного комутатора можуть бути підключені пристрої, що належать до різних підмереж VLAN.
- ***Збільшення продуктивності*** – VLAN поділяє підсіть на окремі широкомовні домени. Це означає, що широкомовні повідомлення будуть отримувати лише пристрої, що знаходяться в одній мережі VLAN. Побудова системи з використанням технології VLAN дозволяє зменшити широкомовний трафік усередині мережі, тим самим знижується навантаження на мережні пристрої та покращується продуктивність системи загалом.
- ***Покращення безпеки*** – пристрої з різних підмереж VLAN не можуть спілкуватися один з одним, що зменшує шанси на несанкціонований доступ до пристроїв системи. Зв'язок між різними підмережами можливий лише через маршрутизатор. Крім того, використання маршрутизатора дозволяє налаштувати політику безпеки, яку можуть застосовувати відразу до всієї групи пристроїв, що належать до однієї підмережі.

Сам принцип роботи технології VLAN працює наступним чинном, кожна VLAN-підмережа має свій ідентифікатор, за яким визначається належність тієї чи іншої підмережі. Інформація про ідентифікатор міститься в тезі, який додається в тіло Ethernet-фрейму мережі, в якій введено розділення на підмережі VLAN.

Найпоширеніший стандарт, який описує процедуру тегування трафіку, – це відкритий стандарт 802.1 Q. Крім нього є пропрієтарні протоколи, але менш популярні.

Технологія Inter VLAN-routimg

Inter VLAN-routing — це сегменти мережі в комутованій локальній мережі. Технологія Inter VLAN-routing відноситься до переміщення пакетів по мережі між хостами в різних сегментах мережі.

Inter VLAN-routing полегшують сегментацію мережі, що, у свою чергу, покращує продуктивність мережі та робить її більш гнучкою, оскільки вони є логічними з'єднаннями.

Inter VLAN-routing діють як окрема підмережа в мережі. Щоб переміщувати пакети з однієї VLAN мережі в іншу та дозволяти зв'язок між хостами.

Методи маршрутизації між Inter VLAN-routing це досить компоненті технології. У цьому методі використовується кілька інтерфейсів маршрутизатора, кожен з яких підключається до порту комутатора в різних VLAN. Ці інтерфейси використовуються як шлюзи за замовчуванням, які потребують додаткового кабелю, коли мережу потрібно розширити. А отже, додавання додаткових мережевих кабелів та покращення інфраструктури є дорожчим.

У цьому методі, на відміну від застарілої маршрутизації, один фізичний порт інтерфейсу використовується для маршрутизації трафіку між сегментами мережі. Адміністратору мережі не потрібно створювати окремі інтерфейси VLAN, як-от fa0/1 до fa0/10.

Натомість усі інтерфейси від 1 до 10 створюються за допомогою одного інтерфейсу. Цей метод простий у реалізації та використовується для малих і середніх мереж.

Перемикач рівня 3 за допомогою комутованого віртуального інтерфейсу (SVI)

На даний момент цей метод маршрутизації між VLAN, який використовує комутатор 3-го рівня/багатошаровий і комутовані віртуальні інтерфейси (SVI), є найбільш переважним.

SVI створюються для мереж Inter VLAN-routing, які існують на комутаторі, який виконує ту ж функцію для VLAN, що й маршрутизатор.

Комутатори рівня 3 дорогі, вони в першу чергу підходять для великих організаційних мереж.

Технологія ARP Inspection

Dynamic ARP Inspection – це є перевірка ARP-пакетів (протокол в комп'ютерній мережі, який призначений для знаходження MAC-адреси другого комп'ютера по відомому вже IP-адресу), яка використовується для відфільтрування несанкціоновани пакетів ARP. Це дозволяє запобігти багатьом видам атак зокрема, **"Третій лишній"**.

В цій схемі атак наступне. Наприклад два комп'ютери з'єднанні між собою в одну мережу за допомогою маршутизатора, в широкодіючому домені. І між ними вклюнюється інший комп'ютер, який знаходиться також в тому широкодіючому домені і буде перехоплювати ARP-запит для знаходження адреси одного з комп'ютерів, а також він може себе видавати за один із комп'ютерів логічного ланцюга і відправляти йому повідомлення від імені першого абонента та від імені другого абонента приймати повідомлення адресоване першим комп'ютером. В загальному можна сказати що обмін між першим і другим абонентом стається через посередника, тобто третього абонента.

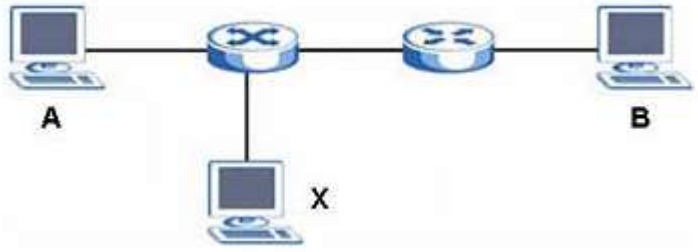

Рис. 3.4. Приклад атаки "Третій лишній"

Система ARP-Inspection діє наступним чинном, при знаходжені комутатором несанкціонованого ARP-пакета, нею автоматично створюється фільтр MAC-адрес, блокуючий трафік від MAC-адрес і мережі VLAN, від яких надійшов несанкціонований ARP-пакет. Період активності фільтру MAC-адрес на комутаторі можно налаштовувати. Дана технологія також ділить усі порти на ***довірені та недовірені***, але не залежить від аналогічної технології DHCP Snooping, тут навідміно від попередньої технології можна вказати швидкість з якою комутатор буде приймати. Довірені порти підключаються до самого комутатора, а не довірені підключаються до хоста. Але потрібно бути уважним і вміло аналізувати де можна довіряти комп'ютеру, а де ні, оскільки налаштування інтерфейсу як ненадійного, коли йому можна і слід довіряти, може призвести до втрати підключення. Він діє так, як і технологія DHCP Snooping, а саме пакети ARP, які надходять у довірений порт приймаються, а не приймаються лише ті у яких швидкість передачі пакетів досить висока та якщо інформація про відправник не співпадає ні з одною із діючих прив'язок.

Технологія Source guard

IP Source guard – одна з основних технологій, що забезпечує безпеку користувача та інформації, яку передає користувач ішому абоненту мережі. Не можна сказати, що вона є однією з основ, але вона є можна сказати додатковою технологією для захисту. Технологія виконує функцію захисту від підміни IP-адрес, та дозволяє відфільтровувати пакети DHCP і ARP в локальній мережі. IP-адреси використовується таблиця прив'язок Static Binding, яка дозволяє розрізняти санкціоновані та несанкціоновані DHCP- та ARP-пакети. При прив'язці використовуються такі атрибути для більш детальної ідентифікації: ***MAC-адреса, VLAN ID, IP-адреса, Номер порту***.

При отриманні комутатором DHCP або ARP здійснюється пошук відповідних MAC-адрес, ідентифікатора VLAN ID, IP-адреси та номера порту в таблиці прив'язок. За наявності прив'язки комутатор пересилає пакет. Якщо прив'язки не виявлено, пакет комутатором відкидається. Таблиця прив'язок

будується комутатором за допомогою відстеження пакетів DHCP, являє собою динамічна прив'язка та з урахуванням інформації, наданої адміністратором вручну, що являє собою статичну прив'язку.

Технологія DHCP Snooping

DHCP Snooping - це технологія безпеки другого рівня, призначена для захисту від атак з використанням протоколу DHCP. Для того щоб розібратися із технологією DHCP Snooping, спочатку розберемося із важливою технологію, DHCP-протокол, що є невід'ємною частиною цієї технології. ***DHCP*** — це є протокол прикладного уровня модели TCP/IP, який слугує для призначення IP-адреси клієнту. Наприклад, атаки з заміною DHCP-сервера в мережі або атаки DHCP starvation, що змушує DHCP-сервер видати все зловмиснику, що існує на сервері. DHCP Snooping запобігає несанкціонованим (шахрайським) DHCP-серверам, що пропонують IP-адреси DHCP-клієнтам. Функція DHCP Snooping забезпеує такі функції, як:

- захист клієнтів у мережі від отримання адреси від неавторизованого DHCP-сервера;
- регулювати, які повідомлення протоколу DHCP відкидати, які перенаправляти та на які порти;

Для правильної роботи DHCP snooping, необхідно вказати, які порти комутатора будуть довіреними (trusted), а які – недовіреними (untrusted або ненадійними):

- ***Ненадійні (Untrusted)*** – порти, до яких підключені клієнти. DHCP-відповіді, що надходять з цих портів, відкидаються комутатором. Для ненадійних портів виконується ряд перевірок повідомлень DHCP та створюється база даних прив'язки DHCP (DHCP snooping binding database);
- ***Довірені (Trusted)*** — порти комутатора, до яких підключено інший комутатор або DHCP-сервер. DHCP-пакети, отримані з довірених портів, не відкидаються.

За замовчуванням комутатор відкидає DHCP-пакет, який прийшов на ненадійний порт, якщо:

- *Надходить одне з повідомлень, яке надсилає DHCP-сервер (DHCPOFFER, DHCPACK, DHCPNAK або DHCPLEASEQUERY);*
- *Надходить повідомлення DHCPRELEASE або DHCPDECLINE, в якому міститься MAC-адреса з бази даних прив'язки DHCP, але інформація про інтерфейс у таблиці не співпадає з інтерфейсом, на якому було отримано пакет;*
- *У DHCP-пакеті, що прийшов, не збігаються MAC-адреса вказана в DHCP-запиті і MAC-адреса відправника;*

Щоб дізнатися, як працює DHCP Snooping, ми повинні зловити робочий механізм DHCP, який означає протокол динамічної конфігурації хоста. При включеному DHCP мережевий пристрій без IP-адреси буде "взаємодіяти" з DHCP-сервером через 4 етапи в такий спосіб.

На етапі підтвердження буде створено таблицю прив'язки DHCP відповідно до повідомлення DHCP ACK. Він записує MAC-адресу хоста, орендовану IP-адресу, час оренди, тип прив'язки, а також номер VLAN та інформацію про інтерфейс, пов'язану з хостом. Якщо наступний пакет DHCP, отриманий від ненадійного хоста, не співпадає з інформацією, його буде видалено.

Серед основних атак, які здатна попередити і запобігти технологія DHCP Snooping, є такі:

- *Спуфінгова атака DHCP* (спуфінг відбувається, коли зловмисник намагається відповісти на запити DHCP і намагається вказати себе (spoof), як стандартний шлюз або DNS-сервер, а отже ініціюючи атаку через посередника, але при цьому можливо, що вони можуть перехоплювати трафік від користувачів перед пересиланням на реальний шлюз або виконувати DDoS атаки, заповнюючи реальний DHCP сервер запитами на засмічення ресурсів IP-адрес);
- *DHCP Starvation* (виснаження ресурсів DHCP, зазвичай націлене на мережеві DHCP-сервери з метою заповнити авторизований DHCP-сервер повідомленнями DHCP REQUEST з використанням підроблених MAC-адрес джерела. Сервер буде відповідати на всі запити, не знаючи, що це атака зі виснаженням DHCP, призначаючи доступні IP-адреси, що призводить до виснаження пулу DHCP.

Технологія ACL

Ця технологія є однією із тих, які призначені для захисту прав користувача та захисту даних, які внесені в базу і даних під час листування. Якщо сказати науковою точкою зору то ACL (Access Control List) – є списком правил, який забороняє або дає дозвіл використання ресурсів мережі. Тобто дає дозвіл тим хто може отримувати доступ до об’єкту, а це в свою чергу різні програми, файли та інша інформація, а також дає доступ тим кому дозволено виконувати операцію у мережі, а кому ні. Простими словами це величезний механізм фільтрації.

Самі списки доступу поділяють на:

- ***Стандартні;***
- ***Розширені;***
- ***Динамічні;***
- ***Рефлексивні;***
- ***Почасові.***

Динамічні ACL: пакет, який дозволяє закривати доступ глобальної мережі, до прикладу, якщо системний адміністратор має закрити доступ до

всієї мережі, але він може зберегти доступ до неї окремим і невеликим групам людей. Тобто адіністратор виконує функцію і настройку списку правил з надання доступу користувачу. Він може закрити усю мережу, але доприкладу надати доступ 3 людям і вони зможуть мати і отримувати інформацію із мережі.

Даний список працює тільки на вхідні направлення, тобто тільки по прийому заявок на отримання доступу до інформації. Незважаючи на те що ця технологія працює із глобальною мережею, користуватися і отримувати доступ також можуть і користувачі локальної мережі, для необхідно використовувати мережевий протокол для реалізації текстового терміналу інтерфейсу по мережі – Telnet (teletype network). А усі решта користувачів можуть отримувати доступ через протокол HTTP.

Почасові ACL: цей лист надає користувачам доступ на деякий час, через певний період часу доступ знову закривається, і щоб знову зайти потрібно підключитися повторно.

Рефлексивні: це являє собою те, що через приватну мережу відкритий вузол, який відправляє TCP-запит в глобальну мережу і в той же час очікує TCP-відповіді. В цей момент канал має бути відкритим, щоб встановити з’єднання, якщо він буде закритим, то до нього неможливо буде підключитися і зловмисники зможуть проникнути в локальну мережу з метою крадіжки даних.

У підсумку можна сказати, що рефлексивні листи, не зможуть надати доступ користувачам, які хочуть підключитися із глобальної мережі до локальної, але можуть згенерувати групу абонентів, які зможуть отримувати відповіді.

Технологія Port Security

Дана технологія призначена для захисту комутатора від атаки, основною функцією є переповнення таблиці MAC-адрес. Дана технологія дозволяє зменшити кількість MAC-адрес, які може запам’ятати комутатор для даного порту до максимальної кількості, яку може отримати даний порт.

Порт з увікненою функцією Port Security буде запам’ятовувати MAC-адреси динаміно або статично і коли кількість MAC-адрес досягне ліміту, він перестає приймати далі MAC-адреси, таблиця не стане заповнюватися, бо досягнуто максимума. Тобто злодій не зможе посилати більше кадрів в поле MAC-адреси за для заповнення її, який після цієї атаки злодій зможе отримати усі кадри, оскільки вам комутор і пристрій не зможе їх приймати, їх буде приймати злочинець. Пристрої, які не занесені в таблицю не отримують доступ в інтернет через цей порт. Також дана функція виконує завдання по обмеженню кількості пристроїв за портом.

Можем навести приклад із картинки.

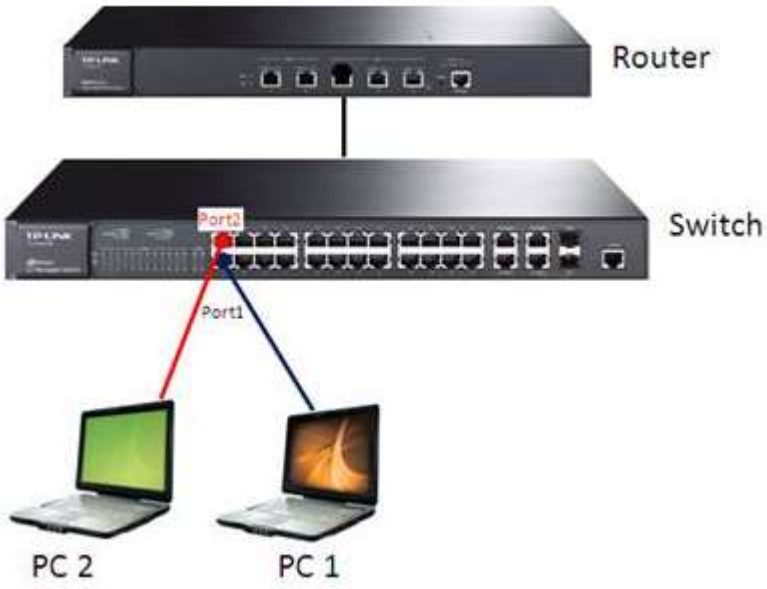

Рис. 3.5. Приклад роботи технології Port Security

До прикладу потрібно підключити комп’ютери в різні порти, де ті порти, куди підключаються, пристрої мають доступ до інтернету, і здатні отримувати MAC-адреси у тій максимальній кількості, якій можуть. Якщо ж комп’ютери підключені до інших портів, де невключена система Port Security, то доступ до мережі інтернет не буде. Тобто під час підключення до кожного порту, потрібно підключати дану функцію, за для безпечного користування.

Технологія IP Mac binding

IP Mac binding – технологія, яка дозволяє контролювати доступ комп'ютерів до мережі, будь-якої чи локальної, чи глобальної, на основі їх IP і MAC-адрес, а також тих портів комутаторів куди підключені самі пристрої.

Принцип дії дуже простий, адміністратор створює список усіх IP та MAC-адрес комп'ютерів разом з портами підключення комутатора, тобто заноситься в базу даних для даного комутатора усі IP та MAC-адреси користувачів. Якщо ж при спробі увійти в мережу, дані клієнта не співпадають, то він не отримує доступ у мережу, якщо співпадають то отримує, технологія IP-MAC-порт заблокує ті дані не співпадають з параметрами заздалегідь сконфігурованого запису. Нижче наведений малюнок, який показує наглядний приклад роботи даної функції.

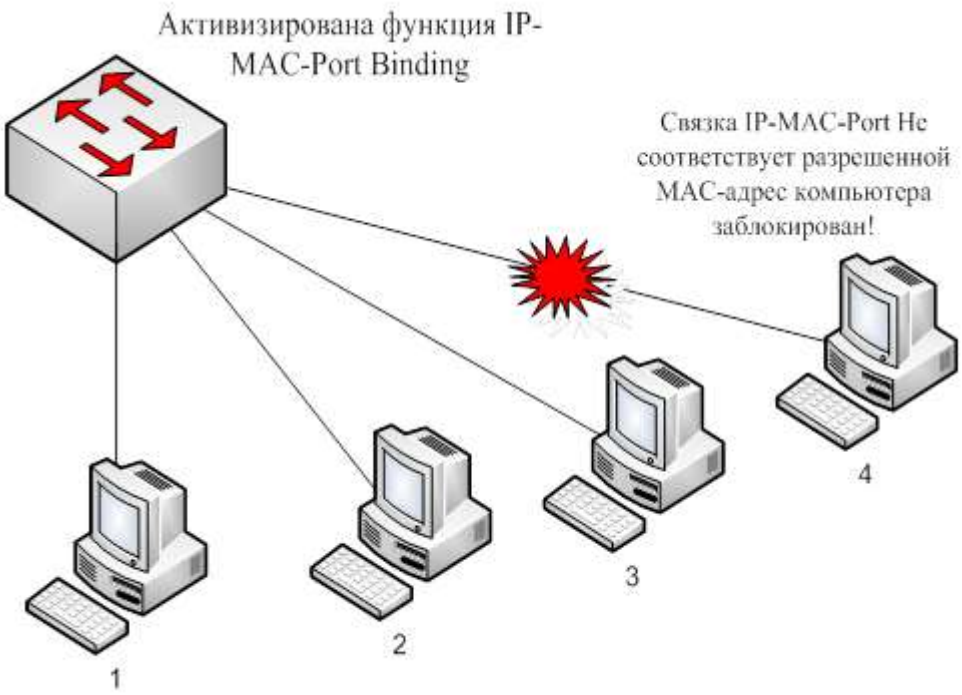

Рис. 3.6. Приклад роботи функції IP-MAC-Binding

Існує декілька режимів роботи функції IP-MAC-Binding серед них наступні:

- ***ARP-mode*** діє наступним чином, якщо в ARP-пакеті, що надходить на комутатор зв'язка IP-MAC не співпадає з тією конфігурацією, яка

занесена в список “відкинути”, якщо адреса співпадає то надходжений пакет надходить в список “дозволити”.

- ***ACL-mode*** в цьому режимі комутатор на основні створеного адміністратором списка тих кому дозволено мати доступ до мережі, створює правила ACL, тобто будь-який пакет, у якого IP та MAC адреси будуть відсутніми в списку адміністратора буде блокуватися, якщо функція не включена то правила ACL діяти не будуть.
- ***DHCP Snooping*** тут комутатор автоматично створює правильний список, але для того щоб сервер коректно працював потрібно підключити його до довіреного порту з виключеною функцією IP MAC Binding.
- ***Strict mode*** при роботі в цьому режимі порт перед тим, як передавати пакети даних, відправить їх на перевірку на ЦПУ для перевірки на те чи співпадають IP та MAC-адреси з тими, які занесені в білий список, тому передача даних не буде до тих пір поки не буде точно сказано чи вони довірені.
- ***Loose mode*** в цьому режимі порти автоматично відкриті, і вони закриваються чи заблоковуються, якщо через нього пройде недостовірний пакет, порт тільки здійснює перевірку пакетів ARP і IPBroadcast.

Технологія NAT

Дана технологія більш використовується не як захист, а як система, яка дозволяє і надає доступ користувачам до мережі.

Технологія NAT – це є технологія глобальної мережі, яка перетворює приватні адреси, які можна назвати зарезервованими в легальні IP-адреси.

Оскільки ми знаємо, що ***публічний IP-адрес***, який відноситься до глобальної мережі призначається мережевим інформаційним центром (NIC), та доступний для пошуку по всьому світу. А ***приватний IP-адрес***, він також називається внутрішнім адресом використовується виключно тільки у внутрішній організації.

Основний принцип роботи NAT полягає в тому, що коли IP-пакети, що передаються між хостом приватної мережі та хостом загальнодоступної

мережі, проходять через шлюз NAT, то вихідна IP-адреса, яка знаходяться у приватному IP, технологія NAT її конвертує в публічну IP-адресу. Шлюз функції NAT має 2 мережні порти, а IP-адреса порту загальнодоступної мережі є загальнодоступною IP-адресою з одноманітним призначенням до прикладу IP-адреса глобальної мережі дорівнює 202.204.65.2, а IP-адреса порту приватної мережі - зарезервована адреса, що дорівнює 192.168.1.1. Хост 192.168.1.2 у приватній мережі відправив 1 пакет IP на хост 166.111.80.200 до публічної мережі (Des = 166.111.80.200, Src = 192.168.1.2).

Серед основних переваг NAT це можливість перевести приватний IP в глобальний IP. Якщо брати недостатки то це насамперед неможливість встановити з’єднання з внутрішнім сервером.

Опис комп'ютерної мережі університету

Комп'ютерну мережу нашого університету ми можемо побачити через систему Zabbix, де і зберігається карта мережі головного корпусу К-ПНУ, а також схема мережі фізико-математичного корпусу К-ПНУ.

Zabbix.net — є вільна система моніторингу служб і станів комп'ютерної мережі. Zabbix.net складається з трьох базових компонентів: сервера для координації виконання перевірок, формування перевірочних запитів та накопичення статистики; агентів для здійснення перевірок на стороні зовнішніх хостів.

Для того, щоб описати комп'ютерну мережу університету, було отримано пароль і логін від входу в Zabbix.net. Після того, як було здійснено вхід в систему, відкривається таке вікно.

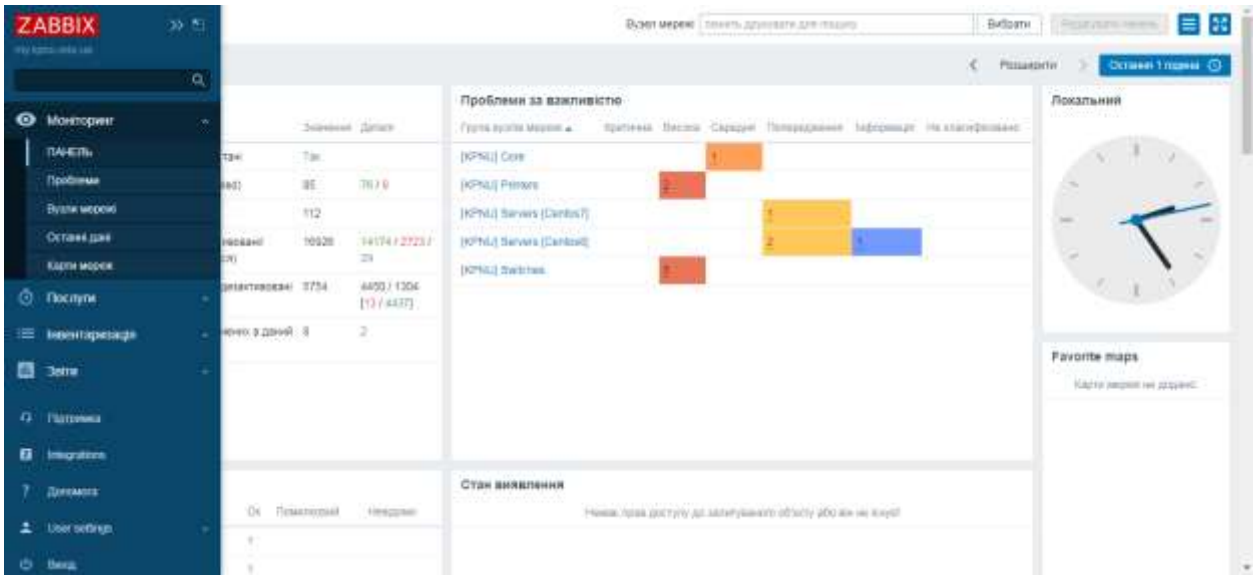

Рис. 4.1. Вікно при вході в систему Zabbix

Після того як увійшли в систему, відкривається зліва діалогове меню, тобто набір команд для виконання, і посередині бачимо стан мереж, стан оптоволокна та швидкість передачі сигналу. Нам потрібно знайти мережу нашого університету для цього ми з лівого боку відкриваємо команду ***“Моніторинг”*** і вибираємо ***“Карта мережі”***.

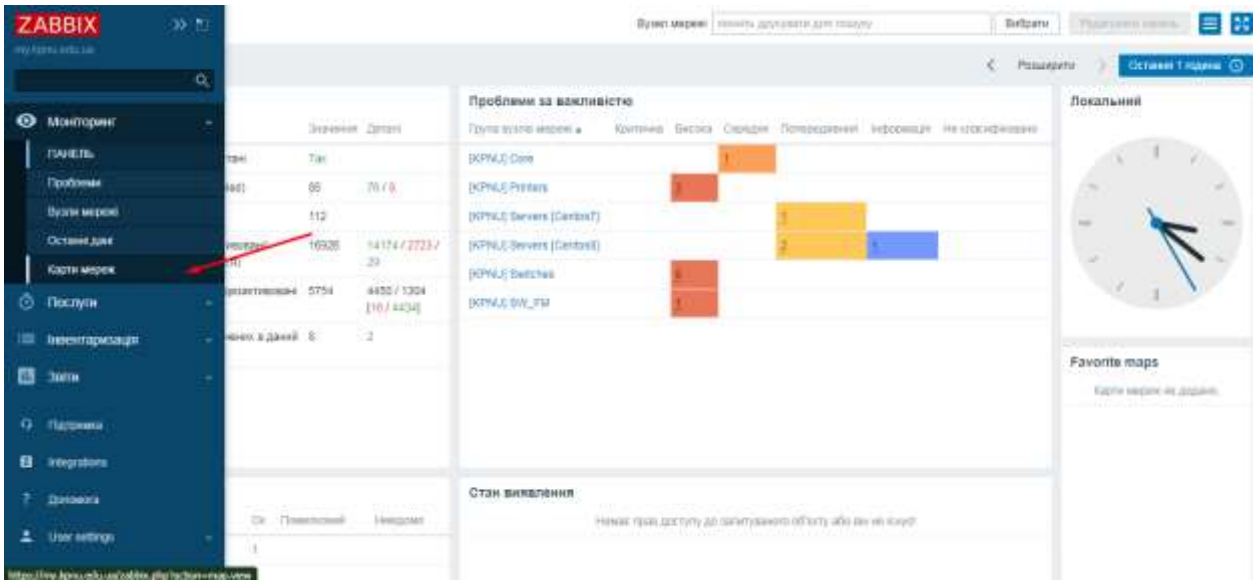

Рис. 4.2. Діалогове вікно

Після того потрібно, прописати назву мережі і її задіяти тоді і відкриється карта мережі. Мережа нашого університету має назву KPNU.

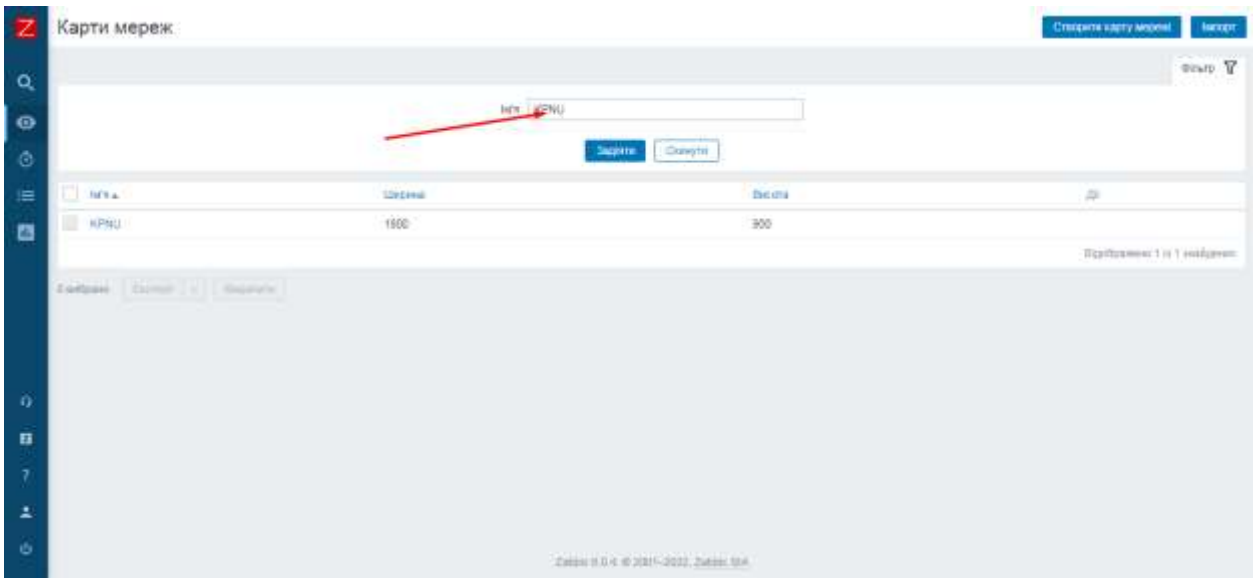

Рис. 4.3. Команда "Карта мережі"

Після того нам відкрилася карта мережі головного корпусу К-ПНУ, вона наведена нижче.

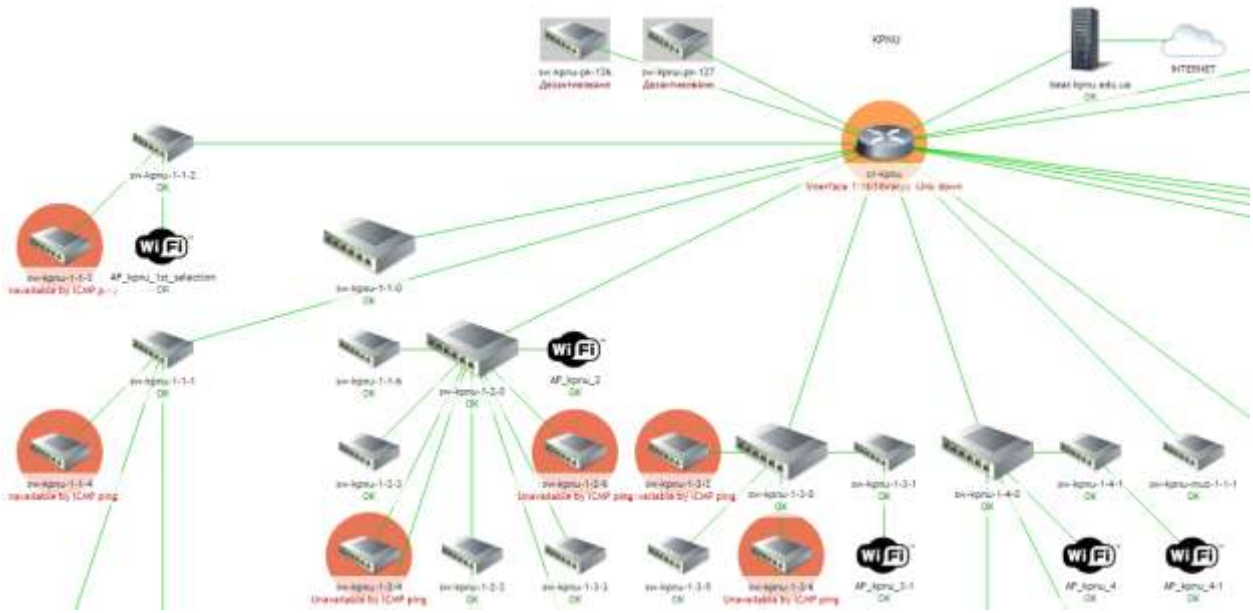

Рис. 4.4. Карта мережі К-ПНУ

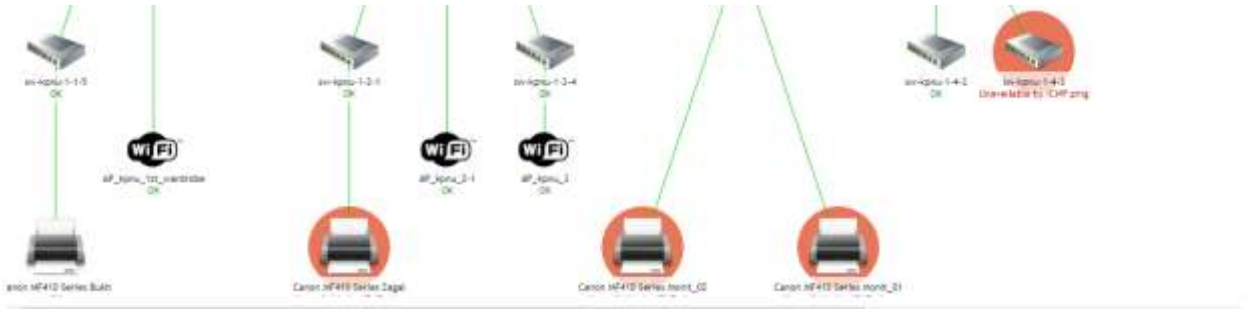

Рис. 4.5. Продовження карти мережі К-ПНУ

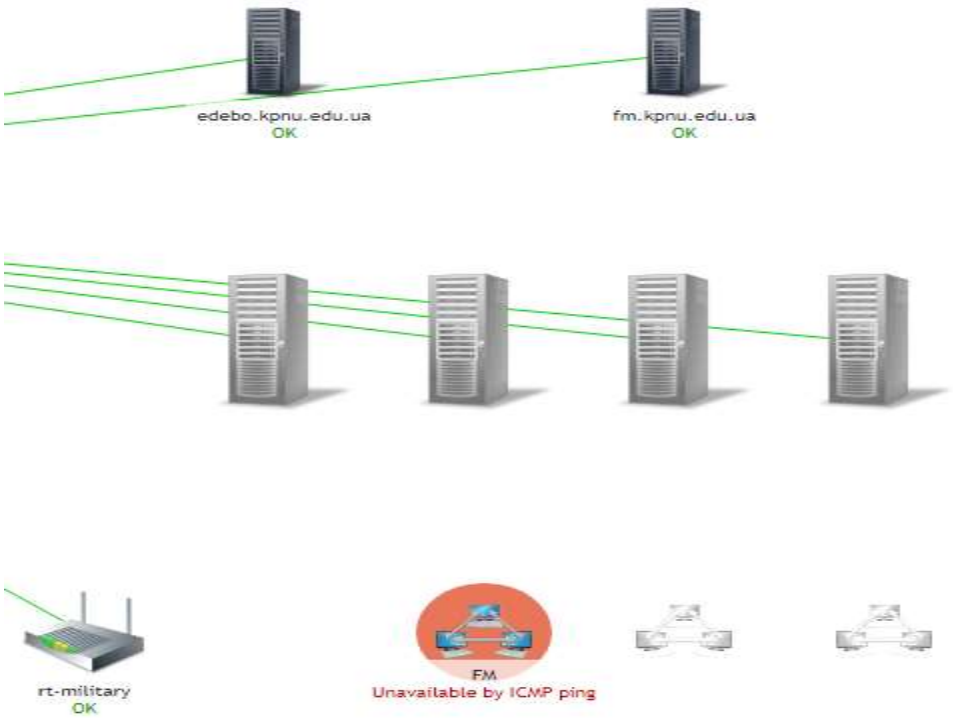

Рис. 4.6. Продовження карти мережі К-ПНУ

Дана мережа має топологію зірка, а використовується технологія Ethernet. ***До кожного комутатор під'єднані апаратні пристрої в основному комп'ютери, які знаходяться в лабораторіях і навчальних аудиторіях, але вони наданій карті не представлені, оскільки досить громісткою була б карта мережі і не зрозуміла, але, від кожного комутатора є зв'язок до комп'ютерів.***

Умовні позначки даної схеми:

 - комутор;

 - точка доступу до інтернета;

 - маршрутизатор;

 - принтер;

Для того, щоб подивитися фірму виробника усіх під’єднаних елементів до мережі, достатньо на карті мережі клікнути на елемент і вибрати в меню команду **Інвентаризація** і можемо побачити у **Апаратній конфігурації** модель і фірму виробника елементу.

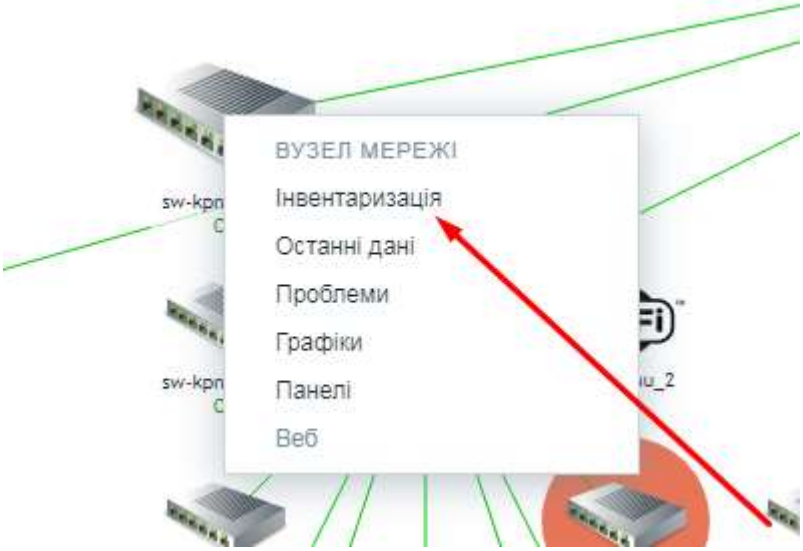

Рис. 4.7. Порядок, яка знайти модель і фірму виробника елементу мережі

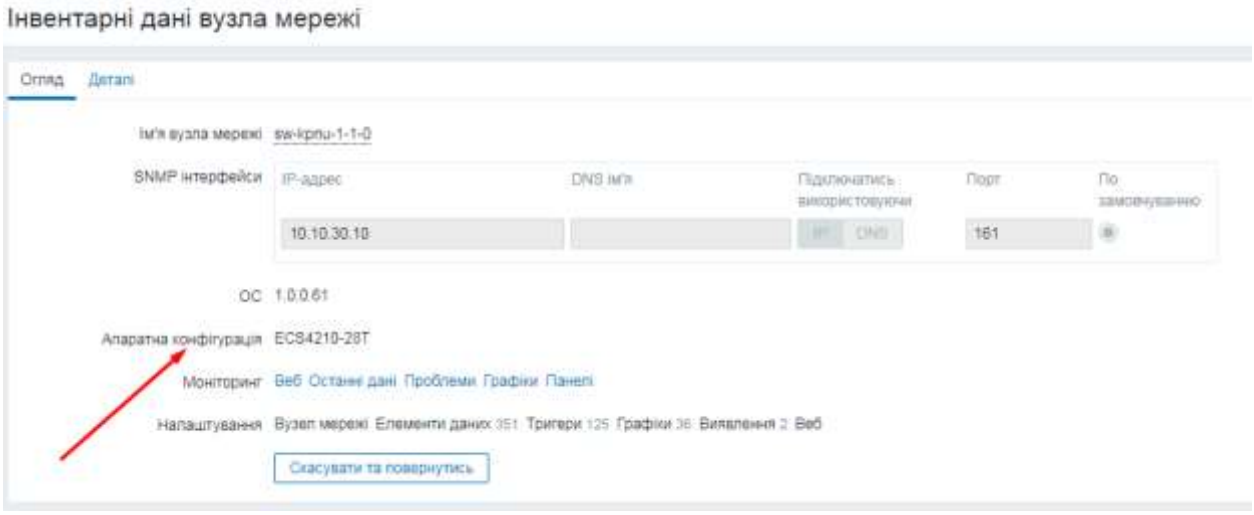

Рис. 4.8. Модель і фірма виробника елементу

У центральному корпусі є ядро (роутер), який передає дані по всій мережі, тобто саме від нього йде зв'язок до всіх пристроїв, що підключені до даної схеми, даний маршрутизатор має назву **cr-kpnu**. Даний маршрутизатор знаходиться в центрі інформаційних технологій.

Рис. 4.9. Маршрутизатор К-ПНУ(центральний корпус)

Тепер розберемо докладніше про кожну систему. Для даної системи ми будемо використовувати Рис. 4.4., 4.5., 4.6., а також окремі нарізки.

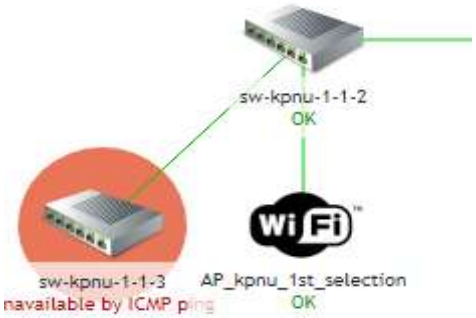

Рис. 4.10. ділянка № 1

Від центрального маршрутизатор **cr-kpnu** є зв'язок до комутатора sw-kpnu-1-1-2, в даній схемі цифри означають наступне:

- *1 цифра – корпус, в даному випадку 1 – центральний корпус;*

- *2 цифра – поверх в даному випадку 1 –перший поверх;*
- *3 цифра – порт підключення в даному випадку це 2 порт.*

Тобто можна бачити, що до маршрутизатора підключено комутатор, який знаходиться на першому поверсі і підключений до маршрутизатор на 2 порт, далі можемо бачити, що до даного світча підключений інший світч (**sw-kpnu-1-1-3**), який також знаходиться на першому поверсі, але підключений до **sw-kpnu-1-1-2** уже в 3 порт, і він знаходиться в червоному колі, що означає, що в даний момент він відключений. Також можна побачити, що до **sw-kpnu-1-1-2** підключена точка доступу Wi-Fi (AP_kpnu_1st_selection), це є інтернет з вільним доступом KPNU FREE, тобто студенти можуть вільно заходити на нього, знаходиться в першій секції.

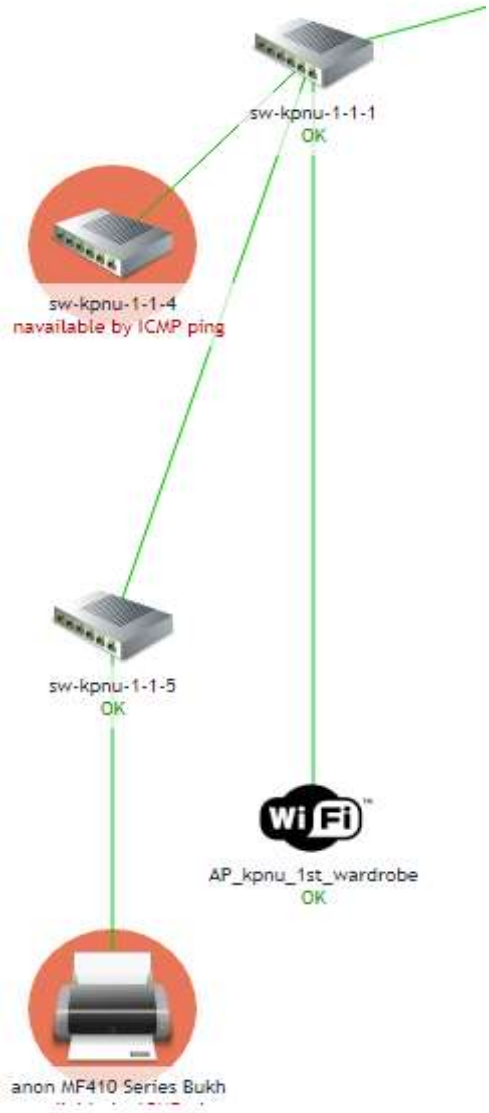

Рис. 4.11. ділянка № 2

Від центрального маршрутизатора **cr-kpnu** йде зв'язок до комутатора **sw-kpnu-1-1-1**, згідно нуменклатурою яка відома то цифри у цьому комутаторі означають, що даний комутатор знаходиться в 1 корпусі (головному), на 1 поверсі і підключений в 1 порт маршрутизатора. Від даного комутора є чотири зв'язки, перший це до іншого комутатора **sw-kpnu-1-1-4**, що знаходиться в оловному корпусі і на 1 поверсі і підключений в 4 порт **sw-kpnu-1-1-1**, але наданий момент він виведений в червоному кружечку і пише повідомлення “navalible by ICMP ping”, що означає, що є помилка при передачі даних, але це означає, що вони просто відключені. Далі бачимо, що до **sw-kpnu-1-1-1** підключений комутатор **sw-kpnu-1-1-5**, те саме означення цифр тільки те, що остання цифра означає що даний комутатор під'єднаний до 5 порту першого комутатора, від даного комутатора йде зв'язок на сканер або принтер **Canon MF410 Series Bukh**, але вданий момент він також є відключеним і обведений кружечком, це є сканер, який знаходиться на першому поверсі і є копіювальним центром, де студенти можуть скористатися ним. Також ми бачимо, що до даного комутатор **sw-kpnu-1-1-1** під’єднана точку доступу інтернету KPNU FREE (**AP_kpnu_1st_wardrobe**), яка знаходиться біля гардеробу на першому поверсі ЦК.

Важливий момент, є те що якщо лінія позначена зеленим і біля елемента мережі зеленим кольором пише ОК, то зв’язок є і працює.

Рис. 4.12. ділянка № 3

Даний комутатор **sw-kpnu-1-1-0** є єдиним у цій ділянці і він під’єднаний до основного маршрутизатора **cr-kpnu**. Він розшифровується так само, тобто знаходиться в центральному корпусі і на першому поверсі, але є один момент, цифра 0 означає, що він є вузловим комутатором і на

карті він позначається великим розміром у порівнянні з іншими комутаторами. Тобто до даних комутаторів під'єднуються інші комутатори, принтери, комп'ютери тощо, він виконує функцію хаба.

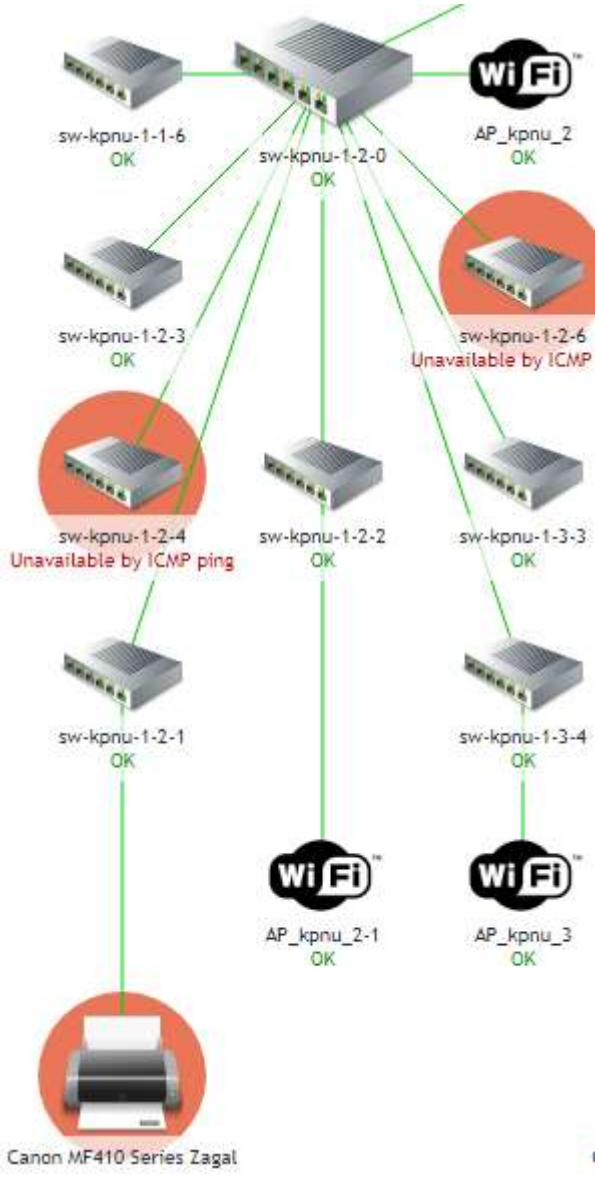

Рис. 4.13. ділянка № 4

До центрального маршрутизатора **cr-kpnu** під'єднаний вузловий комутатор **sw-kpnu-1-2-0**, який знаходиться в головному корпусі на другому поверсі. До цього вузлового комутатора на схемі під'єднані інші комутатори і пристрої, зокрема комутатор **sw-kpnu-1-1-6**, що є з'єднувальними між першим і другим поверхом, комутатор **sw-kpnu-1-2-3** знаходиться на другому поверсі і є одним, скоріше до нього під'єднанні комп'ютері однієї з навчальних аудиторій, також є комутатор **sw-kpnu-1-2-6** та **sw-kpnu-1-2-4**,

вони є одні і до них під’єднані окремі комп’ютери, але наданий момент вони виділенні червоним кружечком і протокол ICMP, видає помилку передачі даних, отже вони відключенні. Також до вузлового під’єднаний світч (**sw-kpnu-1-3-3**), що знаходиться уже на третьому поверсі ЦК, і є з’єднувальним між 2 і 3 поверхами, а також до вузлового під’єднана точка доступу Wi-Fi KPNU FREE (**AP_kpnu_2**), що знаходиться у першому крилі 2 поверху і забезпечує вільний інтернет для усіх студентів і не тільки. Далі ми можемо побачити, що від **sw-kpnu-1-2-0**, йде зв’язок до **sw-kpnu-1-2-1**, що знаходиться на 2 поверсі, а вже від нього йде зв’язок до сканера **Canon MF410 Series Zagal**, це є сканер який знаходиться в ректорскій і є відключеним, то немає зв’язку і цей комутатор також, отже і до нього підключені комп’ютери ректора і секретаря. Від маршрутного комутатора, також ми бачимо 2 зв’язки до **sw-kpnu-1-2-2**, а вже до нього під’єднані також інші пристрої і під’єднанна точка доступу Wi-Fi KPNU FREE (**AP_kpnu_2-1**), що знаодиться вже у 2 крилі 2 поверху і є вільною точкою доступу до інтернету, і до маршрутного також під’єднаний інший комутатор sw-kpnu-1-3-4, який знаодиться на 3 поверсі вже, до якого є доступ у інших пристроїв і зокрема з’єднанні також точка доступу Wi-Fi KPNU FREE (**AP_kpnu_3**), вільна точка доступу до інтернету, яка знаходиться в першому крилі на 3 поверсі.

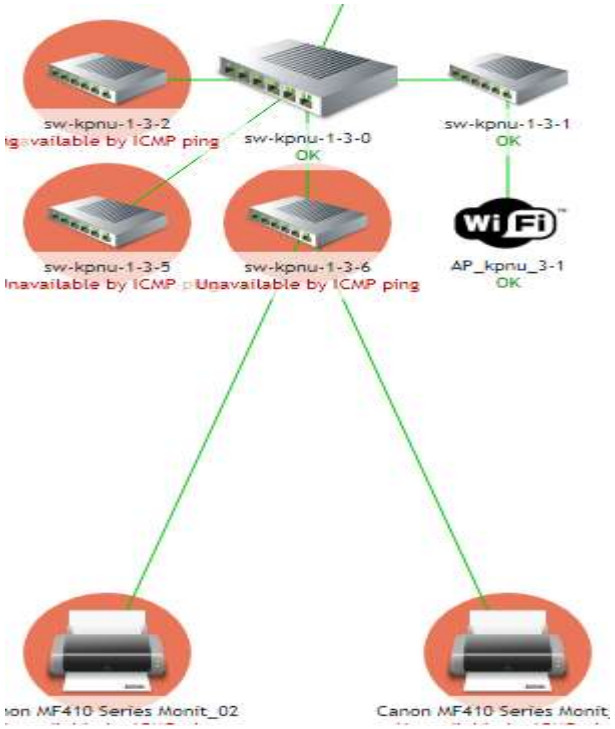

Рис. 4.15. ділянка № 5

До маршрутизатора **cr-kpnu** під'єднаний вузловий комутатор **sw-kpnu-1-3-0**, він знаходиться на 3 поверсі, до нього під’єднанні інші комутатори, які не є вузловими. Зокрема, комутатор **sw-kpnu-1-3-1**, до якого під’єднана точка доступу Wi-Fi KPNU FREE, яка знаходиться на 3 поверсі 2 крило, це є вільний доступ в інтернет для усіх користувачів. Також, до вузлового світча під’єднаний і комутатор **sw-kpnu-1-3-2** та **sw-kpnu-1-3-5**, вони є одиночними, від них не йде зв’язок до інши комутаторів, а тільки можливо до комп’ютерів, але на даний момент вони є відключеними і отже передача даних неможлива, знаходяться вони на 3 поверсі. Далі ми бачимо що до основного під’єднаний не маршрутний комутатор **sw-kpnu-1-3-6**, до якого під’єднано інші комп’ютери навчальний аудиторій, а також два сканера **Canon MF410 Series Monit_02**, **Canon MF410 Series Monit_01**, це два сканера, які знаходять на кафедрах, але дані принтери і комутатор до яких вони під’єднанні має зв’язок, але вони є відключені.

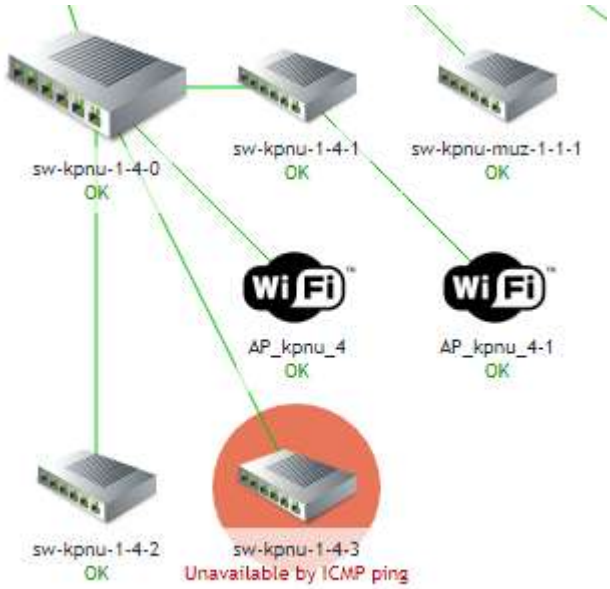

Рис. 4.16. ділянка № 6

До центрального маршрутизатора **cr-kpnu** під'єднано вузловий комутатор **sw-kpnu-1-4-0**, який знаходиться на 4 поверсі, до нього під'єднаний не мережевий комутатор **sw-kpnu-1-4-2**, до якого під'єднанні інші апаратні засоби, які знаходяться в лабораторіях, також до маршрутного під'єднаний світч **sw-kpnu-1-4-3**, який такий самий як і попередній, знаходиться на 4 поверсі і до нього підключене апаратне забезпечення аудиторій. Зі схеми ми можемо побачити, що до вузлового комутатора під'єднаний точка для доступу Wi-Fi KPNU FREE **AP_kpnu_4**, яка з'єднана на пряму з вузловим комутатором і забезпечує вільний доступ до інтернету у 1 крилі (ЦК) на 4 поверсі, а також з'єднанна інша точка доступу до вільного інтернету **AP_kpnu_4-1**, але з'єднанна з вузловим комутаторм іншим проміжним світчем, а саме **sw-kpnu-1-4-1**.

Рис. 4.17. ділянка № 7

До маршрутизатора окремо під'єднаний комутатор **sw-kpnu-muz-1-1-1**, даний комутатор знаходиться в музичному корпусі, що знаходиться по

вулиці Гагаріна, до даного комутатора під’єднуються інші апаратні засоби, що знаходяться в даному корпусі. .

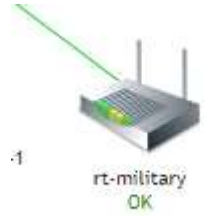

Рис. 4.18. ділянка № 8

До даного маршрутизатора **cr-kpnu**, під’єднаний роутер (**rt-military**), який роздає інтернет на військовий кафедрі.

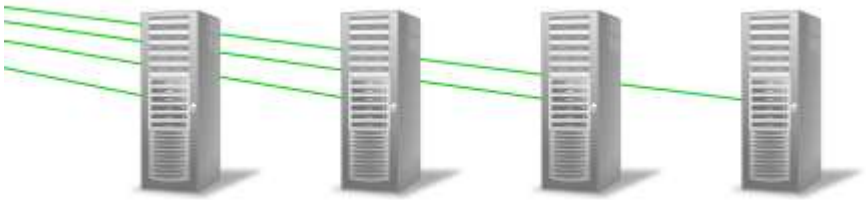

Рис. 4.19. ділянка № 9

Від маршрутизатора **cr-kpnu**, йдуть зв’язки на сервери на яких розташовані сайти, MOODLE, АСУ та інші програми.

Рис. 4.20. ділянка № 10

Дані комутатори знаходяться на першому поверсі центрального корпусу, до них під'єднуються усі апаратні пристрої, зокрема комп'ютери планшети та Wi-Fi роутери. Дані комутатори працюють в 126 та 127 аудиторії, а це є приймальна комісія. Тому вони наданий момент дезактивовані бо немає потреби в роботі, оскільки вони працюють тільки коли працює приймальна комісія тобто в кінці літку.

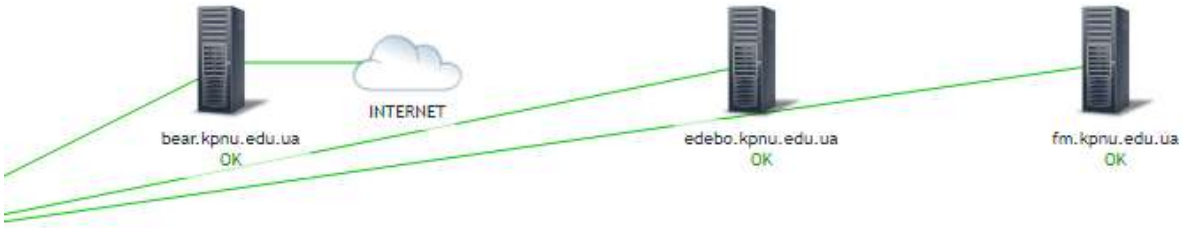

Рис. 4.21. ділянка № 11

Від маршрутизатора **cr-kpnu** йде зв'язок до серверів у яких зберігаються усі зв'язки зокрема окремих серверів edebo.kpnu.edu.ua та сервера **fm.kpnu.edu.ua.** А також ми можемо бачити сервер, який забезпечує інтернет-зв'язок **bear.kpnu.edu.ua** до якого під'єднаний інтернет провайдер, який забезпечує інтернет з'єднання в центральному корпусі університету. Даний сервер назвали Bear, що в перекладі на англійський означає Ведмедик в даному сервері використана технологія NAT, саме вона забезпечує доступ в інтернет.

Карта мережі фізико-математичного факультету К-ПНУ

Також в даній карті натиснувши на карту FM після того натискаємо на суб-карта, можна побачити мережеву карту фізико-математичного факультету К-ПНУ. При побудові даної схеми використовується головний комутатор від якого йде інший не вузловий, але він виконує функцію вузла і передає дані і має з'єднання з іншими комутаторами. Тому можна сказати, що при побудові мережі фізмату К-ПНУ, використовується топологія гібридна зірка, тобто із 2 центральними і більше центральними маршрутизаторами.

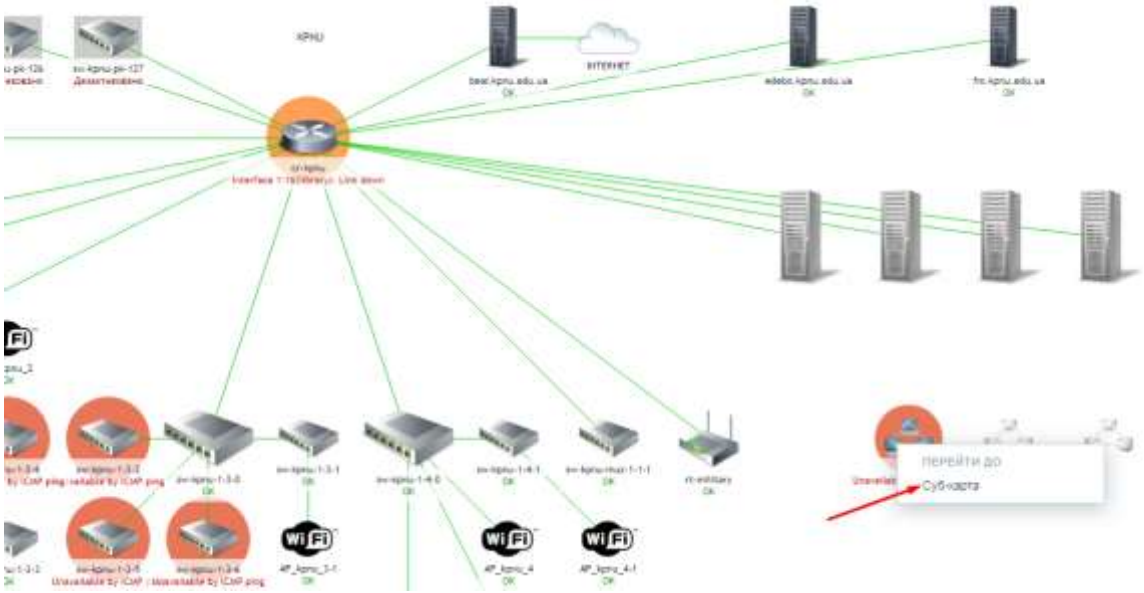

Рис. 4.22. Як зайти на карту мережі фізмату

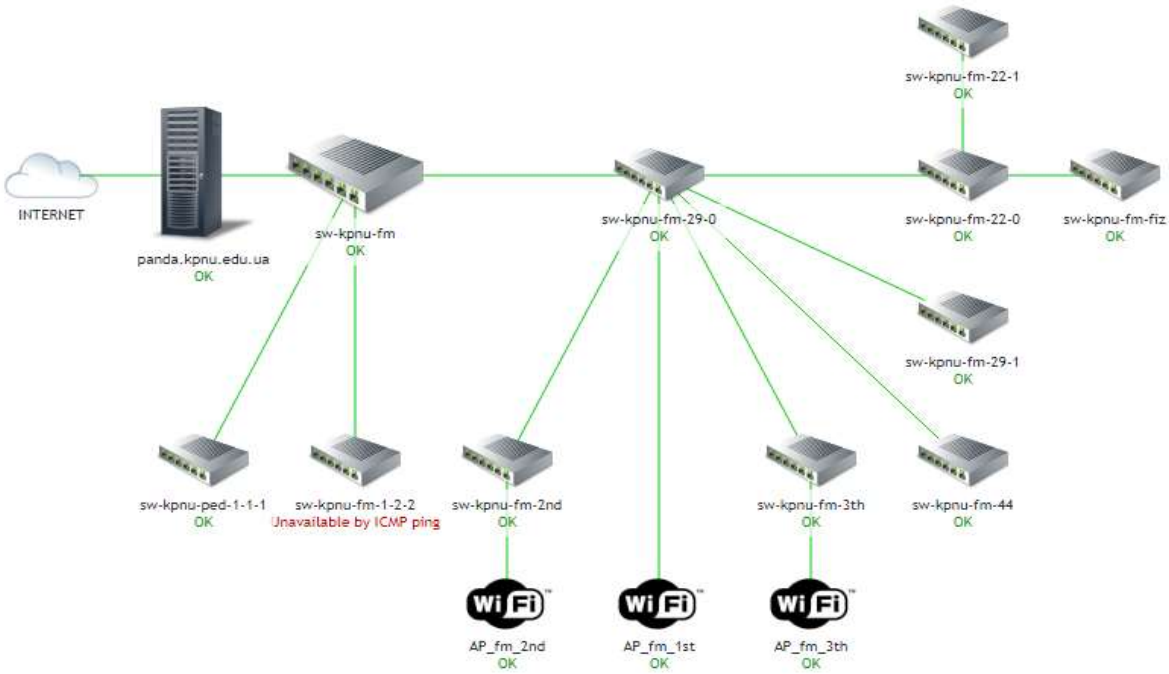

Рис. 4.23. Карта мережі фізмату

В даній схемі можна побачити вузловий комутатор **sw-kpnu-fm** від якого розгалужується уся мережа. Від неї йде доступ до сервера із назвою Panda, у мережі він позначається (panda.kpnu.edu.ua), даний сервер використовує технологію NAT через неї є доступ у мережу Інтернет, від даного вузлового комутатора йде зв’язок до комутатора **sw-kpnu-ped-1-1-1,**

до даного комутатора під'єднанні комп'ютери і інші апаратні засоби аудиторій педагогічного корпусу, також від нього йде зв’язок до світча sw-kpnu-fm-1-2-2, це є комутатор на 2 поверсі фізмату, але наданий момент він є відключеним. Також ми бачимо, що від вузлового світча sw-kpnu-fm, йде з’єднання на інший не маршрутний комутатор (sw-kpnu-fm-29-0), але який виконує роль транспортного, знаходиться в 29 аудиторії від відходять інші комутатори аудиторії 22, оскільки там серверна (sw-kpnu-fm-22-1, sw-kpnu-fm-22-0, sw-kpnu-fm-fiz), також від даного комутатора йде зв’язок на інші комутатори зокрема лабораторії обчислюваної техніка, яка знаходиться на 4 поверсі в 44 аудиторії (sw-kpnu-fm-44), також до комутатора sw-kpnu-fm-29-0 під’єднаний sw-kpnu-fm-3th до якого під’єднана точка доступу Wi-Fi KPNU FREE (AP_fm_3th), це є вільна точка доступу до інтернет, яка знаходиться на 3 поверсі, а також вона дає вільний доступ до мережі на 4 поверсі, а також через інший комутатор, який знаходиться на 2 поверсі і має назву sw-kpnu-fm-2th, і до даного світча під’єднана точка доступу в інтернет KPNU FREE (AP_fm_2th), а вільна точка доступу на першому поверсі напряму під’єднана до комутатора sw-kpnu-fm-29-0 і має назву AP_fm_1th).

Окремі порти та їх опис

Перший на огляді у буде **порт 17** даної мережі, до якого підключений ректор, завдяки інформаційному коду, який дав мені керівник дипломної роботи можемо розглянути основні функції і можливості даного порта і зв’язку та описати технології, які використовуються тут.

Інформація про **17 порт**.

```
Vty-0#sh run int e 1/17
interface ethernet 1/17
 spanning-tree loopback-detection trap
 description rektor
 port security max-mac-count 2
 port security
 switchport multicast packet-rate 64
```

```
 switchport unknown-unicast packet-rate 64
 rate-limit input bits-per-second 128
 no rate-limit input
 rate-limit output bits-per-second 128
 no rate-limit output
 switchport allowed vlan add 40 untagged
 switchport ingress-filtering
 switchport native vlan 40
 switchport allowed vlan remove 1
 switchport mode access
 spanning-tree bpdu-guard
 spanning-tree bpdu-guard auto-recovery
 ip source-guard sip-mac
 ip source-guard max-binding 2
 qos map trust-mode dscp
 ip igmp query-drop
 loopback-detection
!
```

Даний порт використовує технологію Ethernet, яка є найпопулярніша та дія за принципом посилає сигнал і не обов’язково отримувати відповідь і за будь-яких пошкоджень кабелю працювати не буде.

spanning-tree loopback-detection trap, це означає що в даному порті використовується система Loopback Detection, яка забезпечує захист від петель, замикання дроту, підключення до іншого комутатора та інше. Суть наступна з одного порта йде передача пакетів протоколу циклу з портів на яких увімкнено захист від циклу. Коли комутатор надсилає пакет протоколу циклу, а потім отримує той самий пакет, він вимикає порт, який отримав пакет. Loopback Detection працює незалежно від STP. Після виявлення циклу порт, який отримав цикли, переводиться в стан вимкнення. Пастка

надсилається, і подія реєструється. Менеджери мережі можуть визначити інтервал виявлення, який встановлює інтервал часу між LBD-пакетами.

description rektor це є назва самого порта, що означає що даний зв’язок йде до комп’ютера ректора.

port security max-mac-count 2

port security

Це означає, що даний порт використовує технологію Port Security, тобто захист від перевантаження порту MAC адресами, тут стоїть цифра 2 яка означає, що даний порт приймає дві MAC адреси комп’ютерів, який знаходиться в ректора у кабінеті та у разі неполадки він може під’єднатися до мережі і даного порту з ноутбука.

switchport multicast packet-rate 64, це є функція передачі даних де копії пакетів надсилаються окремій групі користувачів, але потрібна зворотня відповідь у даному випадку, надсилання йде ректору, який має дати зворотню відповідь на прийняття, rate це пороговий рівень, або ж скільки кілобіт на секуднду у даному випадку це 64.

switchport unknown-unicast packet-rate 64, це означає йде передача даних від невідомих користувачів, але потрібна зворотня відповідь, і швидкість передачі (rate) становить 64 кілобіт за секунду.

rate-limit input bits-per-second 128, функція, яка забезпечує ліміт для вхідних даних у порт за секунду, в нашому випадку це 128 кілобіт, тобто даний порт здатний прийняти за секунду 128 кілобіт.

no rate-limit input, дана функція каже, що немає обмеження на кількість переселання інформації, але вона буде мати пропускну здатність 128.

rate-limit output bits-per-second 128, функція, яка забезпечує ліміт для вихідних даних з порту за секунду у нашому випадку це 128 кілобіт, тобто даний порт здатний відправити за секунду 128 кілобіт.

no rate-limit output, дана функція забезпечує безперервний потік вихідних даних, але вона має випускну здатність 128.

switchport allowed vlan add 40 untagged, функція технології VLAN, із можливістю додавання до 40 можливих користувачів, але вона є закритою, це є системною мережею VLAN 40 для даного порту.

switchport ingress-filtering, функція, яка вільтрує і захищає мережу від незаконного проникнення, а також різні спроби хакерських атак. Тобто коли хтось намагався увійти в систему одразу адміністраторам видає сигнал про несанкціоновану спробу доступу.

switchport native vlan 40, функція, яка відповідає за VLAN даного порту, створення мережі, означає нумерацію і тип самого VLAN, тобто мережевий трафік із зворотнюю відповідю від самого користувача на чиє ім’я зареєсрована мережа, в нашому випадку це ректор.

switchport allowed vlan remove 1, дозволяє із мережі VLAN видаляти користувача, починаючи від одного, тобто адміністратор може в будь-який момент від мережі відключити одну MAC-адресу, видаляє членство порта із мережі VLAN 1.

spanning-tree bpdu-guard, дана функція використовує BPDU, це блок повідомлень протоколу Spanning Tree (STP), який описує атрибути порту комутатора, такі як MAC-адреса, пріоритет, які дозволяють комутарам брати участь у протоколі Spanning Tree Protocol для збору інформації один від одного. BPDU Guard — це функція, яка захищає топологію протоколу Layer 2 Spanning Tree Protocol (STP) від загроз, пов’язаних з BPDU, і призначена для захисту мережі комутації. Функція захисту BPDU має бути активована на портах, які не повинні отримувати BPDU від підключених пристроїв. Якщо ви використовуєте функцію PortFast протоколу Spanning Tree Protocol (STP) для налаштування портів комутатора, ви повинні підключатися до кінцевих пристроїв (робочих станцій, серверів, принтерів тощо).

spanning-tree bpdu-guard auto-recovery, це система є тією самою, що і попередня, але має підключений модуль до самовідновлення.

ip source-guard sip-mac, функція, яка захищає даний порт від підміни IP-адреси, тобто неможливо буде увійти в систему замінивши IP-адресу, вона є фіксованою і зарезервованою в мережі.

ip source-guard max-binding 2, це є система, яка зарезервувала в мережі лише дві IP-адреси, тобто IP-адресу комп'ютера ректора в кабінеті і особистого комп'ютера, тобто передача даних може здійснюватися тільки від цих IP-адрес.

qos map trust-mode dscp, даний сегмент використовується для того, що зменшити затримку передачі мультимедійних та голосових повідомлень, оскільки інші повідомлення йдуть без затримки, тобто щоб обмін між портом до якого підключений ректор і іншими довіреними користувачами.

ip igmp query-drop, функція, яка забезпечує встановлення багатоадресної передачі даних, від ректора до інших користувачів, а також здатна відкидувати запити, які не мають права приймати запит на передачу даних.

loopback-detection, дана функція створенна для того, щоб запобігти ушкодженню кабеля, а саме петлі, під'єднання кабелю до іншого комутатора, та інші з цим зв'язані причини і система попереджає менеджерів про проблему.

Порт 21, це порт, який є загального доступу в центральному корпусі, тобто порт до якого підключаються абсолютно усі користувачі і провидитися передача даних може між будь-якими користувачами, які підключилися до даної передачі даних.

Інформація про **21 порт**.

```
Vty-0#sh run int e 1/21
interface ethernet 1/21
no spanning-tree loopback-detection
description cr-kpnu
no switchport broadcast
switchport multicast packet-rate 64
```

switchport unknown-unicast packet-rate 64

ip arp inspection trust

ip arp inspection limit none

switchport allowed vlan add 1 untagged

switchport acceptable-frame-types tagged

switchport mode trunk

switchport allowed vlan add 1,20,22,30,40,50 tagged

spanning-tree spanning-disabled

ip dhcp snooping trust

interface ethernet 1/21, функція, яка забезпечує роботу технології Ethernet, яка підключена до маршрутизатора і до 21 порту.

no spanning-tree loopback-detection, до даного порту функція loopback-detection не використовується, тобто тут немає контролю за тим чи в той порт підключено чи ні, а також петель.

description cr-kpnu, це означає, що даний порт використовують для загального доступу по центральному корпусу.

no switchport broadcast, до даного порту не підключена система передаі даних Broadcast, яка забезпечує зв’язок усім, але без зворотнього зв’язку.

switchport multicast packet-rate 64, це є функція передачі даних де копії пакетів надсилаються окремій групі користувачів, але потрібна зворотня відповідь, у даному випадку надсилання йде усім користувачам, які мають доступ до даного порту, це зокрема бухгалтери та різні викладачі кафедр і так далі, і щоб розпочати обмін інформацією потрібно дати згоду (зворотню відповідь), rate це пороговий рівень, або ж скільки кілобіт на секуднду у даному випадку це 64, а також є там де 128.

switchport unknown-unicast packet-rate 64, це означає, що йде передача даних від невідомих користувачів, але потрібна зворотня відповідь, і швидкість передачі (rate) становить 64 кілобіт за секунду.

ip arp inspection trust, є функцією безпеки, яка відхиляє недійсні та шкідливі ARP-пакети. Ця функція запобігає класу атак «людина посередині», коли недружня станція перехоплює трафік для інших станцій, отруюючи кеші ARP своїх нічого не підозрюючих сусідів.

ip arp inspection limit none, дана функція не має обмеження для отримання запиту на передачу даних.

switchport allowed vlan add 1 untagged, означає що даний порт дозволяв трафіку VLAN 1, використовується для виходу із порту як нетегований, увесь порт який водить є нетеговий.

switchport acceptable-frame-types tagged, функція, яка забезпечує передачу даних, тобто можна кадри без тегів, або пріоритетність тегів.

switchport trunk mode, підключена до 21 порту дана функція, переводить інтерфейс у постійний режим транкингу та узгоджує перетворення сусіднього каналу в магістраль. Інтерфейс стає магістральним інтерфейсом, навіть якщо сусідній інтерфейс не є магістральним інтерфейсом.

switchport allowed vlan add 1, 20, 22, 30, 40, 50 tagged, функція встановлюється для порта використання тільки тегованого трафіка в мережах, VLAN 1, 20, 22, 30, 40, 50, трафік з цими помітками від 1, 20, 22, 30, 40, 50 пропускається.

spanning-tree spanning-disabled, функція, що забезпечує приведення мережі інтернет і всіх зв’язків до деревоподібної структури, але у даному випадку вона навпаки не дозволяє мережі перетворитися у дерево.

ip dhcp snooping trust, функція безпеки яка діє між брандамауром і ненайдійними хостами та серверами DHCP, ця функція надає користувачу IP адресу, і записує дану IP адресу в мережу даного порту і захищає від підміни IP адреси дану IP адресу. Тобто не дозволяє вхід в мережу несанкціонованих користувачів.

Висновки

Комп'ютерні мережі є основою обміну інформації між користувачами інформаційного середовища. Саме через мережу будується зв'язки між простими користувачами та цілими групами користувачів, а то і фірмами. Як локально так і глобально. Добре побудована мережа є запорукою надійного каналу передачі даних та їх захисту.

Результатом даної роботи є аналіз стану розвитку сучасних технологій , що застосовується при проектуванні та побудові телекомунікаційних мереж, здійснено огляд апаратного та програмного забезпечення, реалізовано використання базових мережевих технологій, які дозволяють ефективно обслуговувати, експлуатувати та масштабувати телекомунікаційні мережі.

Список використаних джерел

1. Принцип комунікації та технології локальних мереж - Комп'ютерні мережі: сайт URL: https://sites.google.com/site/komputernimerezi440/3

2. 1.4.4 Технології локальних мереж: сайт URL: https://www.znanius.com/3562.html

3. Принцип побудови локальних мереж, основні компоненти, їх призначення та функції. Топологія комп'ютерних мереж: сайт URL: https://stud.com.ua/50138/informatika/printsipi_pobudovi_lokalnih_merezh_osnovni_komponenti_priznachennya_funktsiyi

4. Принципи побудови і призначення комп'ютерних мереж – TDMUV: сайт URL: https://tdmuv.com/kafedra/internal/informatika/classes_stud/uk/nurse/and/03.%D0%9F%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF%D0%B8%20%D0%BF%D0%BE%D0%B1%D1%83%D0%B4%D0%BE%D0%B2%D0%B8%20%D1%96%20%D0%BF%D1%80%D0%B8%D0%B7%D0%BD%D0%B0%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%BA%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D1%85%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6.html

5. Що таке маршрутизатор і як він працює?: сайт URL: https://westelecom.ua/blog/222_cto-takoe-marsrutizator-i-kak-on-rabotaet.html

6. ЗНАЧЕННЯ МАРШРУТИЗАТОРА (ЩО ЦЕ, ПОНЯТТЯ ТА ВИЗНАЧЕННЯ) – ТЕХНОЛОГІЇ ТА ІННОВАЦІЇ – 2022: сайт URL: https://uk.encyclopedia-titanica.com/significado-de-router

7. Що таке маршрутизатор : сайт URL: https://a2os.org.ua/4231/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80/

8. Маршрутизатор – що це таке, особливості, характеристики і види : сайт URL: http://hi-news.pp.ua/tehnka-tehnologyi/9967-marshrutizator-scho-ce-take-osoblivost-harakteristiki-vidi.html

9. Маршрутизатор – Вікіпедія : сайт URL: https://uk.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80

10. Локальна мережа – Вікіпедія : сайт URL: https://uk.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0

11. Що таке (switch) або мережевий комутатор : сайт URL: https://nettech.ua/news/svitch-switch-setevoy-kommutator

12. Что это такое оптоволокно? – Как подключить оптоволоконный интернет : сайт URL: http://geek-nose.com/chto-eto-takoe-optovolokno/

13. Технология VLAN : сайт URL: https://moxa.ru/tehnologii/ethernet_network/tech-vlan/

14. VLAN | Курс “Компьютерные сети” – YouTube: сайт URL: https://www.youtube.com/watch?v=Ig4WoXWzhNc

15. Технология VLAN: особенности применения: сайт URL: https://www.smart-soft.ru/blog/tehnologija_vlan/

16. Understanding Inter-VLAN Routing | Engineering Education (EngEd) Program | Section: сайт URL: https://www.section.io/engineering-education/inter-vlan-routing/#what-is-inter-vlan-routing

17. Dynamic ARP Protection: сайт URL: http://xgu.ru/wiki/Dynamic_ARP_Protection

18. Настройка DHCP Option 82 і DHCP Snooping: сайт URL: https://www.raisecom.su/articles/53117/

19. Port Security: сайт URL: http://xgu.ru/wiki/Port_security

20. ACL – Википедия: сайт URL: https://ru.wikipedia.org/wiki/ACL

21. Access Control List (ACL): что это, для чего используется, види: сайт URL: https://itglobal.com/ru-ru/company/glossary/access-control-list/https://itglobal.com/ru-ru/company/glossary/access-control-list/

22. Access Control List: сайт URL: https://linkmeup.gitbook.io/sdsm/5.-acl-i-nat/00-access-control-list

23. Функция IP-MAC-Port-Binding, Функция Storm Control: сайт URL: https://studbooks.net/2215769/informatika/funktsiya_port_binding

24. Loopback Detection Settings: сайт URL: https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/350_550/index.html#page/tesla_350_550_olh/loopback_detection_over.html

25. Э. Таненбаум, Д. Уэзеролл Компьютерные сети. 5 издание., перевод Киев, Харьков, Самара, Минск, Москва, Санкт-Петербург: Питер, 2012. С. 17-21, С. 32-43, С. 305-324, С. 326-329, С. 469-488.