МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітня програма: «Комп'ютерна інженерія»
Група: 2БКС-27

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

здобувача освіти денної форми навчання
БКС.27.09.000.КРБ

ВОРОБЕЙ ВІКТОР ЄВГЕНОВИЧ

м. Одеса
2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: **«Комп'ютерна інженерія»**

Група: **2БКС-27**

ПОЯСНЮВАЛЬНА ЗАПИСКА

До кваліфікаційної роботи бакалавра на тему:

« Проектування інформаційної безпеки в мультисервісній мережі »

Проектний матеріал складається з пояснювальної записки на 74 сторінках та графічного (презентаційного) матеріалу на 12 аркушах (слайдах)

Виконавець _____ (Воробей В.Є)

Керівник проекту _____ (Кунуп Т.В.)

Консультанти:

з охорони праці _____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Завідувачка кафедри _____ (Іванова Л.В.)

Завідувач відділення _____ (Скорнякова О.В.)

Захист «20» 06 2023 р. Протокол ДКК № 1

Оцінка ЕК 4 (добре)

Секретар ДКК _____

АНОТАЦІЯ

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

ABSTRACT

Next-generation multi-service networks have advantages over traditional architecture networks because they can use a single transport infrastructure to carry all types of traffic and use it efficiently through statistical multiplexing. The integration of the traffic of disparate data and language makes it possible to achieve a qualitative increase in the efficiency of the information support of enterprise management, while the use of an integrated transport environment allows to reduce the costs of creating and operating the network. Multi-service networks, which use a single channel for data transmission of various types, make it possible to reduce the variety of types of equipment, apply uniform standards, technologies and centrally manage the communication environment.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Кафедра *комп'ютерної інженерії*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР *Беркань І.В.*

" " 202 р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

Здобувачеві (здобувачці) освіти Воробея Віктора Євгеньєвича

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Проектування інформаційної безпеки в мультисервісній мережі

затверджена наказом по коледжу від "17" 10 2022 р. № 285-А2-ОД

2. Термін здачі кваліфікаційної роботи 20.06.2023р.

3. Вихідні дані до роботи

Обгрунтування технології проектування. Мережеві атаки та методи їх протидії. Технології цілостності та конфеденційності.Схема мережі. Програмного забезпечення Sniffer для реалізації проекту

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Аналіз існуючих технологій проектування; Обгрунтування вибору Формування вимог до інформаційної безпеки мережі; Проектування інформаційної безпеки; Безпека на 2 рівні; Безпека на 3 рівні; Розділ охорони праці. Висновок. Перелік використаних інформацій.

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

1. Схема мережі; 2. Безпека на 2 рівні;
3. Безпека на 3 рівні;
4. Додаткова конфігурація прилада;
5. Схема атаки через двойну інкапсуляцію;
6. CBAC-відкриття тимчасових дир»;
7. Вікно програми Sniffer.

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів роботи, що стосується їх

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний	*Кунуп Т.В.*		
Охорона праці	*Чорновол В.І.*		
Нормоконтроль	*Нетрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання

Керівник роботи Кунуп Т.В.

(підпис)

Завдання прийняв до виконання Воробей В.Є.

(підпис)

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Передмова	4.05.2023	Виконав
2.	Аналітичний огляд існуючих рішень	8.05.2023	Виконав
3.	Вимоги до мережевих атак	10.05.2023	Виконав
4.	Методи протидії їх захисту	15.05.2023	Виконав
5.	Технології цілостності та конфеденційності	17.05.2023	Виконав
6.	Розділ охорони праці	22.05.2023	Виконав
7.	Проетування безпеки на 2 та 3 рівнях	23.05.2023	Виконав
8.	Перелік літератури. Висновок	26.05.2023	Виконав
9.	Оформлення пояснювальної записки	28.05.2023	Виконав
10.	Оформлення графічної частини	31.05.2023	Виконав
11.	Малий захист кваліфікаційної роботи	15.06.2023	
12.	Захист кваліфікаційної роботи	24.06.2023	

Виконавець Воробей В.Є

(підпис)

Керівник роботи Кунуп Т.В.

(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 27. 09 000. 00 КРБ	*Кваліфікаційна робота бакалавра*		
А4			*БКС 27. 09 000. 00 КРБ ПЗ*	*Пояснювальна записка*	*1*	

Зм.	Арк.	№ докум.	Підпис	Дата	*БКС 26. 09. 000. 00 КРБ*		
Розробив		Ворбей В.Є.			*Проектування інформаційної безпеки в мультисервісній мережі*	Літ.	Аркуш 4 / Арку
Перевірив		Кунуп Т..В				Н Д П	
Н. Контр.		Петрашова В.І..				*ВСП "ОТФК ОНТУ" гр.БКС-27*	
Затверд.		Кривченко Ю.В.					

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: **«Комп'ютерна інженерія»**

Група: **2БКС-27**

ПОЯСНЮВАЛЬНА ЗАПИСКА

До кваліфікаційної роботи бакалавра на тему:

« Проектування інформаційної безпеки в мультисервісній мережі »

Проектний матеріал складається з пояснювальної записки на 77 сторінках та графічного (презентаційного) матеріалу на 12 аркушах (слайдах)

Виконавець _____ (Воробей В.Є)

Керівник проекту_____ (Кунуп Т.В.)

Консультанти:

з охорони праці_____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Завідувачка кафедри _____ (Іванова Л.В.)

Завідувач відділення _____ (Скорнякова О.В.)

Захист «____»_____ 202____ р. Протокол ДКК №_____

Оцінка ЕК _____

Секретар ДКК _____

ЗМІСТ

ВСТУП

За останні роки ми стали свідками все більш швидкої інтеграції комп'ютерів і телефонії як обладнання, так і мереж. Старі оператори загальнодоступних мереж спостерігали зменшення трафіку телефонії в своїх телекомунікаційних мережах з комутацією загального користування, в основному через все більшу популярність мобільних телефонів та рух послуг з телефонних мереж до загально доступного Інтернету.

Оператори мультисервісних мереж пропонують широкий спектр послуг, який включає як традиційні телефонні послуги, такі як голосовий зв'язок, передачу факсів і SMS-повідомлень, так і нові цифрові послуги, такі як відеоконференції, потокове відео, онлайн-ігри і передачу даних високої швидкості.

Розвиток мультисервісних мереж базується на концепції наступного покоління мереж (Next Generation Networks, NGN), яка передбачає перехід від традиційних аналогових мереж до цифрових пакетних мереж. NGN забезпечує інтеграцію різних типів комунікації (голос, дані, відео) і використовує Інтернет-протокол (IP) для передачі і керування трафіком.

Мультисервісні мережі мають декілька переваг. Вони дозволяють операторам ефективно використовувати мережеві ресурси, забезпечуючи одночасну передачу різних видів трафіку. Крім того, вони забезпечують гнучкість і масштабованість, що дозволяє операторам швидко впроваджувати нові послуги і збільшувати пропускну здатність мережі при необхідності.

У світі, де комп'ютери і телефонія стають все більш інтегрованими, мультисервісні мережі грають важливу роль у забезпеченні широкого спектру комунікаційних послуг, задовольняючи потреби клієнтів у зв'язку і передачі даних різного виду.

Організаційна конвергенція, що полягає у централізації мережевих, телекомунікаційних та інформаційних служб під керуванням вищого рівня менеджменту.

1.ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Опис функціонування мультисервісних мереж

Мультисервісні мережі є самостійним класом мереж, що базуються на концепції NGN. Вони надають широкий спектр послуг, включаючи як традиційні, так і нові послуги. Регламентація мультисервісних мереж здійснюється на основі нормативно-технічної бази, яка враховує особливості інтеграції різних послуг і системно-технічних рішень в рамках однієї мережі.

Мультисервісні мережі забезпечують доставку різних послуг на єдиній технологічній основі, використовуючи принцип конвергенції послуг. Пакетні мережі, зокрема ті, що використовують транспорт MPLS-TP, ефективно передають голос, відео та інші дані.

Мультисервісна мережа використовує один канал для передачі різних типів трафіку. Побудова мультисервісних мереж включає такі аспекти:

Конвергенція завантаження мережі, що передбачає передачу різних типів трафіку у єдиному форматі представлення даних.

Конвергенція протоколів, що передбачає перехід від багатьох наявних мережевих протоколів до загального протоколу.

Фізична конвергенція, яка дозволяє передавати різні типи трафіку у рамках єдиної мережевої інфраструктури.

Конвергенція пристроїв, що передбачає побудову мережевих пристроїв, які можуть підтримувати різнотипний трафік у єдиній системі.

Конвергенція додатків, що полягає у інтеграції різних функцій у рамках єдиного програмного засобу.

Конвергенція технологій, що передбачає створення єдиної загальної технологічної бази для будівництва мереж зв'язку, яка задовольняє вимогам регіональних мереж зв'язку і локальних обчислювальних мереж.

Організаційна конвергенція, що полягає у централізації мережевих, телекомунікаційних та інформаційних служб під керуванням вищого рівня

менеджменту.

Таким чином, мультисервісні мережі забезпечують інтеграцію різних послуг і типів трафіку на єдиній інфраструктурі, що сприяє ефективній та масштабованій доставці комунікаційних послуг.

Конвергенція включає об'єднання двох напрямків - комутацію каналів (передачу голосу) і комутацію пакетів (передачу даних). Ця нова концепція інтегрованої широкосмугової мережі розвивалася останні кілька років під назвою Мережі наступного покоління (NGN). NGN описує архітектурні еволюції в телекомунікаційному ядрі та мережах доступу і зазвичай базується на Інтернет-протоколі. Це дозволяє інтегрувати та ефективно передавати кілька сервісів, таких як голос, відео та дані, в одній інфраструктурі.

Перспективна архітектура NGN передбачає створення мультисервісної мережі, де функціональність послуг розташовується у граничних вузлах мережі, є окрема мережева підсистема для керування послугами і розширена номенклатура інтерфейсів для підключення устаткування постачальників послуг. Сутність NGN полягає у переході від багатоплатформеності до простої та ефективної мережі, спеціально розробленої для надання всіх видів послуг.

Технологічно, перехід від традиційної мережі до NGN означає перехід від окремих мереж з комутацією каналів і пакетної комутації до мультисервісних мереж, які можуть працювати в обох режимах комутації. Це дозволяє створити мережі, що підтримують всі види послуг. Керування такими мережами стає більш простим, а контроль за якістю послуг переходить до самого користувача.

1.2 Особливості побудови мультисервісних мереж

Мультисервісна мережа (МСМ) є мережею зв'язку, побудованою згідно з концепцією мережі зв'язку наступного покоління, яка забезпечує надання широкого набору послуг. Головною метою МСМ є зниження вартості володіння, підтримка складних мультимедійних застосунків і розширення функціональних можливостей мережевого обладнання.

Мультисервісні мережі є окремим класом мереж, побудованих на базі концепції NGN, і можуть надавати широкий спектр як традиційних, так і нових послуг.

Зараз спостерігається швидкий ріст обсягів інфокомунікаційних послуг, що вказує на їх перевагу у мережах зв'язку у найближчому майбутньому. Хоча розвиток інфокомунікаційних послуг в основному здійснюється через комп'ютерну мережу Інтернет, доступ до цих послуг здійснюється через традиційні мережі зв'язку. Однак, у деяких випадках Інтернет-послуги не відповідають сучасним вимогам інформаційного суспільства через обмежені можливості транспортної інфраструктури. Тому розвиток інфокомунікаційних послуг вимагає ефективного управління інформаційними ресурсами та розширення функціональності мереж зв'язку. Це спонукає до інтеграції Інтернету і мереж зв'язку.

Основні технологічні особливості інфокомунікаційних послуг, які відрізняють їх від послуг традиційних мереж зв'язку, включають наступне:
Інфокомунікаційні послуги працюють на верхніх рівнях моделі OSI, тоді як послуги зв'язку надаються на мережевому рівні.

Більшість інфокомунікаційних послуг вимагають наявності клієнтської та серверної частини. Клієнтська частина реалізується на устаткуванні користувача, а серверна - на спеціальному вузлі мережі, відомому як вузол служб.

Інфокомунікаційні послуги включають передачу мультимедійної інформації з високою швидкістю передачі та несиметричністю вхідних і вихідних потоків даних.

Для надання інфокомунікаційних послуг потрібні складні конфігурації з'єднань.

Інфокомунікаційні послуги характеризуються різноманітністю прикладних протоколів та можливостей керування послугами з боку користувача.

Для ідентифікації абонентів інфокомунікаційних послуг може

використовуватися додаткова адресація в межах цих послуг.

Інфокомунікаційні послуги представляють собою додатки, у яких функціональність розподілена між постачальником послуг та кінцевими користувачами. Тому функції кінцевого устаткування також включаються до складу інфокомунікаційних послуг і повинні враховуватися при їх регламентації.

Інфокомунікаційні послуги повинні відповідати наступним вимогам:

Мобільність послуг.

Гнучкість та швидкість створення нових послуг.

Гарантована якість послуг.

Існуючі мережі зв'язку, які використовують комутацію каналів або комутацію пакетів, не відповідають вимогам мультисервісних мереж. Обмежені можливості традиційних мереж є перешкодою для впровадження нових інфокомунікаційних послуг. Збільшення обсягів, що передаються в інфокомунікаційних послугах, може негативно вплинути на якість обслуговування базових послуг існуючих мереж зв'язку. Врахування наявності інфокомунікаційних послуг є необхідним при розробці стратегій розвитку традиційних мереж в напрямку мультисервісних мереж.

При реалізації мультисервісних мереж зазвичай вирішуються чотири технічні питання:

Пропускна здатність.

Затримка.

Розсинхронізація.

Управління.

Зростаючий попит на широкосмуговий передачі даних та доступ до Інтернету в умовах жорсткої конкуренції змушує постачальників послуг розширювати свій спектр послуг і знижувати витрати на інфраструктуру. Тому потрібна платформа, яка може запропонувати комплексне рішення для надання широкого спектру послуг, таких як ATM, Frame Relay, Інтернет, IP, голосові та відео передачі з гарантованою якістю обслуговування (QoS) та високою

доступністю. Клієнти отримують доступ до надійних і доступних послуг від одного постачальника, можуть змінювати свої пакети послуг та оплачувати єдиний рахунок.

При проектуванні мультисервісних мереж потрібний інший підхід. Доставка відео та голосу повинна здійснюватися в реальному часі з пріоритетом під час перевантажень мережі. Однак мережева індустрія раніше не була орієнтована на мережі реального часу, і дані передавалися відповідно до можливостей мережі в конкретні проміжки часу.

1.3 Структура мультисервісної мережі

Структура мультисервісної мережі складається з декількох основних компонентів. Універсальна транспортна мережа є основою цієї мережі і включає наступні елементи:

Транзитні вузли: ці вузли виконують функції перенесення і комутації даних у мультисервісній мережі.

Кінцеві вузли: ці вузли забезпечують доступ абонентів до мультисервісної мережі.

Контролери сигналізації: ці контролери виконують функції обробки інформації про сигналізацію, керування викликами і з'єднаннями в мережі.

Шлюзи: ці елементи дозволяють здійснити підключення до традиційних мереж зв'язку.

Транспортна мережа призначена для забезпечення послуг перенесення даних. Інфокомунікаційні послуги використовують вузли служб (SN) і/або вузли керування послугами (SCP) для своєї реалізації. Вузли SN є устаткуванням постачальників послуг, які функціонують як сервери додатків для інфокомунікаційних послуг. Клієнтська частина цих послуг реалізується на кінцевому устаткуванні користувача. Вузли SCP відповідають за керування логікою і атрибутами послуг. Коли декілька вузлів служб або вузлів керування послугами працюють разом для надання однієї і тієї ж послуги, вони утворюють

платформу керування послугами.

Побудова мультисервісних мереж передбачає дворівневу архітектуру, яка складається з регіонального та магістрального рівнів. Це дозволяє впроваджувати інфокомунікаційні послуги та розв'язувати завдання, пов'язані зі структурною надійністю та контролем якості послуг. На регіональному рівні мультисервісна мережа забезпечує підключення абонентів, надання транспортних та інфокомунікаційних послуг, а також взаємодію з аналогічними послугами в інших регіональних мережах. На магістральному рівні мультисервісна мережа забезпечує перенесення даних для взаємодії між мультисервісними регіональними мережами і передачу навантаження всіх існуючих мереж.

Рисунок 1. 1. Архітектура NGN

Мережа доступу включає абонентські лінії, вузли доступу і системи передачі. Вона призначена для організації підключення користувачів до ресурсів регіональних мереж. Для доступу до послуг NGN використовуються

інтегровані мережі доступу, які підключені до кінцевих вузлів мультисервісної мережі і забезпечують підключення користувачів до цієї мережі, а також до традиційних мереж. Крім того, традиційні мережі можуть бути використані, і їх абоненти можуть отримувати доступ до мультисервісної мережі через вузли, які підключені до шлюзів (Media Gateway).

1.4 Проектування мультисервісної мереж

Побудова мультисервісних мереж (МСМ) з інтеграцією різних послуг є одним з найбільш перспективних напрямків розвитку мереж зв'язку. МСМ вирішує проблеми конвергенції інформаційних і телекомунікаційних технологій.

Основне завдання МСМ полягає у забезпеченні співіснування і взаємодії різнорідних комунікаційних підсистем в єдиному транспортному середовищі. Це означає, що для передачі різних типів трафіку, таких як дані, голос і відео, використовується одна інфраструктура. МСМ використовує єдиний канал зв'язку для передачі різних типів трафіку, що дозволяє провайдерам зменшити різноманітність обладнання, застосовувати єдині стандарти і кабельну систему, централізовано керувати комунікаційним середовищем та розширити спектр послуг.

Для споживачів (абонентів) використання МСМ забезпечує зручність управління набором послуг, роботу з єдиним провайдером, широкий спектр сервісів та інші переваги.

При проектуванні МСМ розробники стикаються з деякими труднощами. По-перше, необхідно забезпечити адаптацію нових технологій під існуючу інфраструктуру оператора або поступову модернізацію інфраструктури. По-друге, мультисервісна мережа повинна підтримувати різні рівні якості обслуговування (QoS) для різнорідного трафіку. Третя проблема полягає в різнорідності середовища передачі даних і забезпеченні певної якості обслуговування незалежно від використовуваної технології доступу.

Технології, які використовувалися раніше для інтеграції різнорідного трафіку, включають ISDN (Integrated Services Digital Network), FR (Frame Relay) і ATM (Asynchronous Transfer Mode).

Хоча сьогодні ці технології можуть вважатися застарілими, багато основних принципів і технічних рішень, що були вперше використані в них, залишаються актуальними й досі. Сучасні мультисервісні мережі будуються на основі цих принципів і рішень.

Мережа зв'язку наступного покоління (NGN) є концепцією побудови мережі, що надає необмежений набір послуг з гнучкими можливостями управління і створення нових послуг. Це досягається шляхом уніфікації мережевих рішень, використання розподіленої комутації, винесення функцій надання послуг у кінцеві мережеві вузли і інтеграції з традиційними мережами зв'язку.

NGN, яка реалізується Міжнародним союзом електрозв'язку (МСЕ), має особливості безперебійної доступності та комплексного страхування якості. Вона керує робочими графіками операторів мережі та постачальників послуг. Метою NGN є забезпечення функціональної сумісності та мобільності всіх елементів мережі, зберігаючи концепцію поділу між мережевим транспортом, обслуговуванням і додатками. Однією з привабливих особливостей NGN є поділ функцій мережевого транспорту та управління, що забезпечує уніфіковані, протокольні, незалежні від технологій функції управління транспортом.

Рекомендація МСЕ описує концепцію та ознаки NGN в п'яти областях:

NGN є пакетною мережею, яка може надавати будь-які види телекомунікаційних послуг.

Мережа може використовувати різні широкосмугові і транспортні технології, засновані на якості обслуговування.

Функції послуг в NGN не залежать від базових технологій транспорту.

Мережа забезпечує безперешкодний доступ з точки зору постачальників мережевих послуг і користувачів.

NGN забезпечує загальну мобільність, що забезпечує постійне і повсюдне надання послуг користувачам.

Функціональна архітектура NGN була розроблена для задоволення вимог і підтримки очікуваних послуг. Вона включає функції рівня обслуговування і функції транспортного рівня. Основними орієнтирами є мережевий інтерфейс користувача (UNI), міжмережевий інтерфейс (NNI) і прикладний мережевий інтерфейс (Application Network Interface). Дворівнева архітектура мультисервісної мережі представлена на рисунку 1.

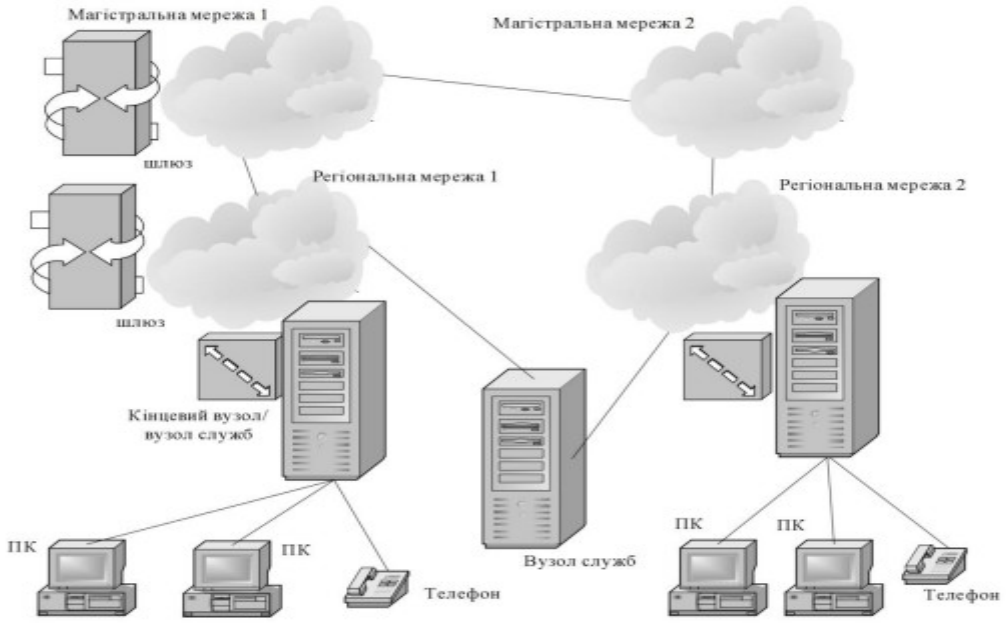


Рисунок 1.2. Дворівнева архітектура мультисервісної мережі

У розумінні NGN, різниця між інтерфейсами UNI і NNI вказує на те, що інтерфейси для клієнтів та інших мереж будуть відрізнятися. Ця розбіжність відображає зміну у концепції Інтернету, де всі компоненти розглядаються як однакові будівельні блоки. Основна ідея Інтернету полягає в тому, що будь-які компоненти можуть бути поєднані в будь-якій комбінації. Однак NGN відрізняється від цього підходу. Найменше, UNI і NNI мають відмінності щодо можливостей, масштабу, ролі та відповідальності між клієнтською та мережевою стороною. Інша вагома причина акценту на зовнішніх інтерфейсах, таких як UNI і NNI, полягає в тому, що внутрішні інтерфейси всередині NGN

можуть бути різними від UNI і NNI. Це дозволяє операторам мережі будувати гнучкіші мережі, забезпечуючи відповідність ключовим зовнішнім інтерфейсам. На межах UNI і NNI в NGN також є можливість захисту від зловмисних атак або несподіваного поведінки з боку клієнтів або інших мереж, зберігаючи при цьому обслуговування звичайних клієнтів.

Транспортний рівень в NGN відповідає за передачу даних і управління та експлуатаційну підтримку транспортних ресурсів для передачі цих даних між термінальними пристроями. Взаємодія між додатками та елементами мережі NGN здійснюється через прикладний мережевий інтерфейс (ANI). Мережевий інтерфейс користувача (UNI) забезпечує взаємодію функцій кінцевого користувача та елементів мережі NGN. Міжмережевий інтерфейс (NNI) забезпечує взаємодію мережі NGN з іншими мережами. З огляду на передачу різноманітного трафіку, включаючи трафік, чутливий до затримок, важливими є вимоги до високої надійності обладнання вузлів, підтримки функцій управління трафіком та хорошої масштабованості.

Усередині NGN, транспортний рівень забезпечує передачу IP-пакетів, дозволяючи функціям контролю мережевих підключень (NACF) керувати терміналами, а функціям управління ресурсами та доступом (RACF) реалізовувати управління ресурсами IP. Рівень обслуговування забезпечує сервісний контроль. Розмежування рівнів обслуговування та транспорту забезпечує гнучкість в різних аспектах. Наприклад, обладнання може бути незалежним від обладнання на іншому рівні, що дозволяє гнучкіше відповідати потребам кожного компонента. Нові сервісні можливості можуть бути реалізовані шляхом впровадження нових серверів, залишаючи транспортне обладнання незмінним. Навіть якщо новий сервіс не стає популярним, транспортний рівень все одно може бути використаний для інших послуг. Незалежність міграції є ще одним аспектом, де транспортні засоби можуть бути оновлені або замінені новими технологіями без впливу на засоби обслуговування. В крайньому випадку, загальний транспортний рівень може бути використаний різними роздрібними відділами однієї і тієї ж групи

постачальників. Цей розподіл або модульність є унікальною особливістю архітектури NGN.

1.5 Функції транспортного рівня

Функції транспортного рівня в рамках NGN забезпечують з'єднання для всіх компонентів та фізично розділених функцій, а також підтримку передачі мультимедійних файлів, контрольної і керуючої інформації.

Основні функції транспортного рівня включають:

Функції доступу до мережі: вони забезпечують доступ кінцевих користувачів до мережі, збирають та оцінюють трафік, отриманий від користувачів. Також вони відповідають за управління якістю обслуговування, включаючи управління ємністю буфера, планування черг, фільтрацію та класифікацію трафіку, маркування та виконання політик щодо формування трафіку.

Функції граничного маршрутизатора: вони обробляють дані та трафік, які надходять з різних мереж доступу і зливають їх в один потік на кордоні домену NGN. Ці функції включають підтримку QoS та контроль трафіку.

Функції транзитного маршрутизатора: вони забезпечують переміщення інформації через мережу NGN і надають засоби для поділу трафіку з урахуванням вимог до якості обслуговування. Ці функції надають механізми QoS, пов'язані з трафіком користувача, включаючи керування буфером, розміром черги, плануванням, фільтрацією пакетів, класифікацією трафіку, маркуванням, виконанням політик, контролем точок доступу та можливостями брандмауера.

Функції шлюзу: вони забезпечують взаємодію між функціями кінцевого користувача та/або іншими мережами, включаючи мережі NGN та існуючі мережі, такі як PSTN/ISDN, Інтернет тощо.

Функції обробки медіанних: вони надають медіаресурси, необхідні для надання послуг, таких як генерація тональних сигналів і перетворення кодів.

Функції управління транспортним рівнем: вони включають функції контролю доступу до ресурсів (RACF) та функції контролю здійснення підключення до мережі (NACF).

Функції контролю доступу до ресурсів дозволяють представляти інфраструктуру транспортної мережі для функцій управління послугами (SCF) у абстрактному вигляді, звільняючи провайдерів від деталей, таких як топологія мережі, інтерфейс підключення, використання ресурсів, механізми QoS. Вони контролюють ресурси мережі на основі заданої політики, резервують ресурси, взаємодіють з функціями маршрутизатора для контролю фільтрації пакетів, класифікації трафіку, маркування, визначення політики, пріоритетів тощо.

Функції контролю здійснення підключення до мережі реєструють користувача на рівні доступу та ініціалізують необхідні для доступу до послуг NGN функції користувача. Вони також ідентифікують транспортний рівень, керують адресним простором мережі, аутентифікують користувачів.

Функції управління послугами (Service Management Functions) в контексті транспортного рівня включають низку завдань і функцій, спрямованих на керування та надання послуг у мережі.

1.6 Функкції управління послугами

Основні функції управління послугами на транспортному рівні включають:

Планування послуг: Ця функція відповідає за визначення, проектування та планування різних типів послуг, які будуть надаватись у мережі. Вона включає в себе визначення вимог до послуг, вибір відповідних технологій та ресурсів, розробку моделей та сценаріїв послуг.

Активація послуг: Ця функція забезпечує процес активації та запуску послуг у мережі. Вона включає встановлення з'єднань, конфігурацію необхідних ресурсів, ініціалізацію функцій та сервісів, необхідних для надання послуг.

Моніторинг та керування послугами: Ця функція відповідає за постійний моніторинг та керування наданими послугами у реальному часі. Вона включає в себе збір статистики та метрик про використання послуг, контроль якості обслуговування, виявлення та вирішення проблем, а також налаштування та оптимізацію ресурсів для покращення якості та ефективності послуг.

Управління збереженням та відновленням послуг: Ця функція включає в себе резервування, збереження та відновлення послуг у випадку виникнення аварій, збоїв або втрати з'єднання. Вона забезпечує надійність та безперебійність надання послуг шляхом резервування та реплікації ресурсів та даних.

Управління життєвим циклом послуг: Ця функція охоплює усі етапи життєвого циклу послуг, включаючи планування, розробку, впровадження, експлуатацію, підтримку та відмову від послуг. Вона забезпечує ефективне керування та управління послугами протягом усього їх існування у мережі.

Функції управління послугами на транспортному рівні грають важливу роль у забезпеченні якості та надійності послуг, ефективного використання ресурсів та задоволення потреб користувачів у мережі.

1.7 Функції кінцевого користувача

Функції кінцевого користувача відносяться до компонентів транспортної мережі, що забезпечують взаємодію та надання послуг для кінцевих користувачів. Основні функції кінцевого користувача включають:

З'єднання з мережею: Кінцевий користувач має можливість підключитися до транспортної мережі, використовуючи різні засоби доступу, такі як Ethernet, Wi-Fi, дротові або бездротові з'єднання. Ця функція забезпечує фізичне підключення користувача до мережі.

Аутентифікація та ідентифікація: Кінцевий користувач проходить процес аутентифікації для підтвердження своєї ідентичності та отримання доступу до мережевих ресурсів. Це може включати введення облікових даних, паролів,

використання біометричних методів або інших форм ідентифікації.

Надання послуг: Кінцевий користувач має можливість користуватися різними послугами транспортної мережі, такими як доступ до Інтернету, голосова телефонія, відеозв'язок, передача даних тощо. Він може взаємодіяти з цими послугами за допомогою відповідного програмного забезпечення або пристроїв, які підтримують ці функції.

Керування настройками: Кінцевий користувач може налаштовувати різні параметри та параметри зв'язку, що стосуються його підключення до мережі. Це може включати настройку мережевих протоколів, налаштування безпеки, управління брандмауером та інші опції, які дозволяють користувачеві контролювати своє з'єднання.

Управління ресурсами: Кінцевий користувач може керувати своїми мережевими ресурсами, такими як пропускна здатність, використання мережевих пристроїв, обмеження швидкості передачі даних тощо. Ця функція дозволяє користувачеві ефективно використовувати доступні ресурси та контролювати їх використання.

Функції кінцевого користувача спрямовані на забезпечення зручності, безпеки та ефективності використання транспортної мережі користувачами. Вони дозволяють кінцевим користувачам отримувати доступ до послуг та взаємодіяти з мережевим середовищем зручним та ефективним способом.

Так, підтримка управління є фундаментальною для роботи в мережі наступного покоління (Next Generation Network, NGN). Функції управління дозволяють керувати та контролювати NGN з метою забезпечення якості, безпеки і надійності наданих послуг.

Функції управління розподілені по різних функціональних модулях (Functional Entity, FE) та взаємодіють з мережевими елементами управління і елементами управління послугами. Вони застосовуються як на рівні транспортної мережі, так і на рівні послуг NGN. Основні області, які охоплюються цими функціями, включають:

Управління вихідними налаштуваннями: Ця функція дозволяє

налаштовувати параметри транспортної мережі та послуг NGN. Вона охоплює налаштування маршрутизації, пропускної здатності, якості обслуговування та інші параметри, що впливають на роботу мережі.

Управління конфігураціями: Ця функція включає керування конфігураціями мережевих пристроїв та програмного забезпечення, встановленими на них. Вона забезпечує контроль за налаштуванням, змінами та оновленнями конфігураційних параметрів.

Управління обліковими записами користувачів: Ця функція дозволяє провайдерам послуг NGN керувати обліковими записами своїх користувачів. Вона включає створення, налаштування, видалення та керування обліковими записами, а також наданням прав доступу до різних послуг та ресурсів.

Управління продуктивністю: Ця функція відповідає за моніторинг та оптимізацію продуктивності мережі та послуг NGN. Вона включає збір та аналіз даних про використання ресурсів, навантаження мережі, якість обслуговування та інші параметри продуктивності.

Управління безпекою: Ця функція забезпечує захист мережі та послуг NGN від потенційних загроз безпеці. Вона включає контроль доступу, аутентифікацію, шифрування, виявлення вторгнень та інші заходи для забезпечення безпеки мережі та даних користувачів.

Функції управління обліковими записами користувачів дозволяють провайдерам послуг NGN забезпечувати своїх користувачів замовленими послугами. Це включає створення та налаштування облікових записів, управління послугами, тарифними планами, забезпечення безпеки та надання підтримки користувачам.

1.8 Концепції мережі наступного покоління NGN

Концепція мережі наступного покоління (Next Generation Network, NGN) відноситься до архітектури телекомунікаційних мереж, яка спрямована на забезпечення передачі голосу, даних та інших послуг за допомогою

інтегрованої IP-мережі. NGN є еволюційним кроком у розвитку мережі з метою покращення якості обслуговування, зниження вартості та надання нових послуг.

Основні концепції NGN включають наступне:

Інтегрована IP-мережа: NGN базується на протоколі Internet Protocol (IP) та використовує його як основний механізм передачі даних. Це дозволяє об'єднати різні типи трафіку (голос, відео, дані) у єдину мережу і передавати їх за допомогою спільних протоколів.

Розподілені функції: NGN розділяє функції мережі на різні модулі, які можуть розташовуватись в різних фізичних місцях. Це дозволяє більш гнучко розгортати та керувати мережевими ресурсами та послугами.

Орієнтованість на послуги: NGN спрямована на надання різноманітних послуг, які можуть бути доступні з будь-якого пристрою та з будь-якого місця. Це означає, що користувачі можуть отримувати послуги голосової комунікації, відеозв'язку, мультимедіа, передачі даних тощо через одну IP-мережу.

Відкритий інтерфейс: NGN надає стандартизовані відкриті інтерфейси для взаємодії між різними системами, компонентами та провайдерами послуг. Це сприяє легкій інтеграції нових технологій та додатків у мережу.

Підтримка мобільності: NGN розроблена з урахуванням мобільності користувачів. Вона дозволяє забезпечити послуги та зберігати стан користувача незалежно від його фізичного місцезнаходження або пристрою, з якого він користується.

Гнучкість і масштабованість: NGN надає гнучкість та масштабованість для підтримки зростаючих потреб мережі. Вона дозволяє змінювати конфігурацію мережі та розширювати її місткість залежно від вимог і обсягу трафіку.

Концепція NGN забезпечує платформу для розвитку нових телекомунікаційних послуг, покращення якості зв'язку та підвищення ефективності мережі. Вона є основою для еволюції традиційних телекомунікаційних мереж у сучасну інтегровану IP-мережу.

ISDN (Integrated Services Digital Network) - це міжнародний стандарт

телекомунікаційних мереж, що був розроблений для передачі голосу, даних та інших послуг через цифрові канали зв'язку.

ISDN забезпечує інтеграцію різних послуг, таких як телефонні розмови, передача факсів, доступ до Інтернету, відеоконференції та інші, за допомогою цифрових комунікаційних каналів. Він використовує цифрову передачу даних, що дозволяє отримувати високу якість зв'язку та швидку передачу інформації.

Основні характеристики ISDN:

Цифрові канали: ISDN використовує цифрові канали для передачі голосу та даних. Це дозволяє отримувати більшу якість зв'язку, менші шуми та спотворення, а також використовувати широкосмугові послуги.

Канал зв'язку B (Bearer): Цифровий канал B використовується для передачі голосу та даних. Він має пропускну здатність 64 Кбіт/с і може бути комутований (постійний) або сполучений (виклик на вимогу).

Канал керування D (Delta): Канал керування D використовується для передачі сигналів керування, які необхідні для встановлення, управління та закінчення з'єднання. Він має пропускну здатність 16 Кбіт/с і використовується для сигналізації між абонентською лінією та комутаційним обладнанням.

Широкий спектр послуг: ISDN підтримує різноманітні послуги, такі як голосові дзвінки, передача факсів, передача даних, відеоконференції, доступ до Інтернету тощо. Він забезпечує інтеграцію цих послуг та їх одночасне використання.

Ідентифікація абонентів: ISDN надає можливість ідентифікувати абонентів та керувати доступом до послуг. Це дозволяє забезпечити безпеку та контроль над використанням мережі.

ISDN був популярним у 90-х роках, але з появою більш швидких та потужних технологій, таких як DSL та кабельний Інтернет, він поступово витіснився. Проте, деякі оператори та організації все ще використовують ISDN для підтримки деяких послуг та підключення до традиційних телефонних мереж.

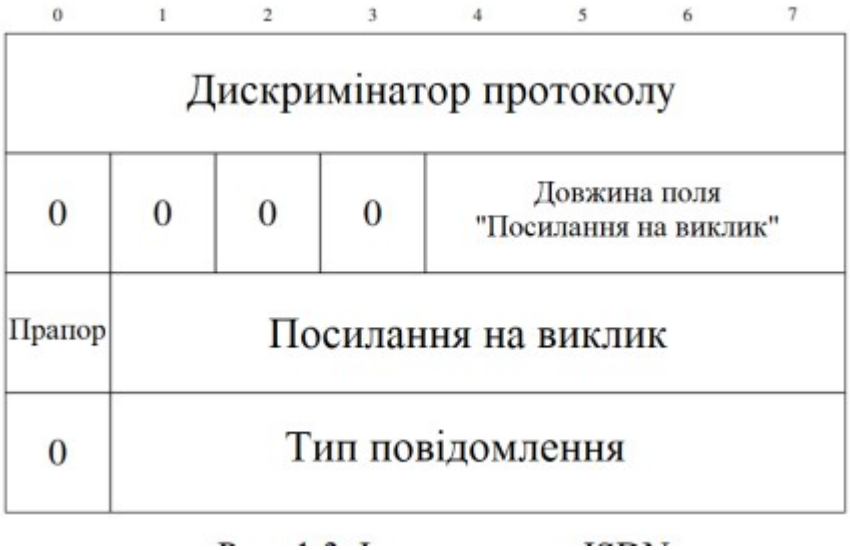


Рисунок 1.3. Формат кадру ISDN

Основні компоненти мультисервісної мережі включають:

Ядро мережі: Ядро мережі є центральним елементом мультисервісної мережі. Воно забезпечує комутацію трафіку, маршрутизацію, керування ресурсами та інші функції, що необхідні для передачі даних різних типів послуг.

Інфраструктура доступу: Інфраструктура доступу включає в себе різноманітні технології, такі як DSL, кабельний доступ, бездротовий доступ, оптоволоконні мережі та інші. Вона забезпечує підключення користувачів до мережі і передачу трафіку між користувачем і ядром мережі.

Периферія (межа мережі): Периферія мережі включає мережеві вузли, такі як комутатори, маршрутизатори, файрволи, сервери, апаратне та програмне забезпечення, що використовується для обробки, передачі та управління послугами в мережі.

Мультисервісна мережа надає можливість надавати різноманітні послуги, такі як голосова телефонія, передача даних, відеоконференції, потокове відео, інтернет-послуги та інші, використовуючи спільну інфраструктуру та оптимальні ресурси мережі. Це дозволяє ефективно використовувати мережеві ресурси, забезпечувати високу якість обслуговування та задовольняти потреби різних типів користувачів.

1.9 Якість обслуговування (QoS) в мережах NGN

QoS (Quality of Service) відіграє важливу роль у мережах зв'язку наступного покоління, оскільки вони стикаються з різнорідним мультимедійним трафіком, який має особливі вимоги до якості обслуговування. QoS дозволяє надавати різні рівні обслуговування для різних типів трафіку або потоків руху. Це база для пропонування різних класів обслуговування різним сегментам користувачів, що в свою чергу визначає різні рівні ціноутворення, що відповідають різним рівням CoS (Class of Service) та QoS.

QoS має велике значення для розгортання послуг реального часу, таких як голосова телефонія або відеоконференції, а також для послуг передачі даних. Вона включає в себе визначення вимог до пропускної здатності мережі, контроль пріоритету користувачів, контроль втрати пакетів або кадрів, а також контроль затримок, як затримок транзиту (що відбуваються від однієї кінцевої точки до іншої), так і варіацій затримки трафіку (тобто джиттеру).

Характеристики QoS включають визначення допустимих затримок та еластичності для конкретного додатка. Вони можуть також враховувати стійкість до затримок та еластичність у відношенні до програм та користувачів, а також, можливо, до сценаріїв часу, дня тижня тощо.

Для забезпечення QoS необхідно мати можливість надавати різні рівні обслуговування, включаючи наявність достатньої пропускної здатності, керування затримками від кінця до кінця, контроль відхилень затримок та втрати пакетів, які відповідають вимогам конкретних програм. Також важливим аспектом QoS є відносний пріоритет різних потоків трафіку. Крім того, QoS пов'язаний з контролем дотримання політики та виконання правил для керування потоками трафіку.

Забезпечення високої якості обслуговування (QoS) є ключовим аспектом при плануванні, розгортанні та управлінні мультисервісними мережами, оскільки воно дозволяє задовольняти вимоги різних типів трафіку та

забезпечувати високий рівень задоволення користувачів.

Інженерна рада інтернету (The Internet Engineering Task Force - IETF) є організацією, яка займається розробкою та стандартизацією протоколів та технологій Інтернету. В контексті QoS (Quality of Service), IETF пропонує різні моделі та протоколи для вирішення проблеми відсутності QoS в Інтернеті.

Перша запропонована модель - Integrated Service (IntServ) - надає суворі гарантії QoS, але масштабується погано для великих мереж. Інша модель - Differentiated Services (DiffServ) - розв'язує цю проблему шляхом забезпечення QoS для агрегованих потоків трафіку, класифікованих у обмежений набір класів обслуговування.

Є два способи реалізації QoS: явний QoS і неявний QoS. Явний QoS означає, що програма вибирає необхідні параметри QoS, тоді як неявний QoS означає, що менеджер мережі контролює ці параметри.

Багатопротокольна комутація по мітках (MPLS) є ще одним рішенням, яке забезпечує підтримку QoS шляхом можливостей проектування трафіку на мережевому рівні.

Проте, DiffServ відіграє центральну роль у забезпеченні QoS, оскільки він пропонує масштабованість на мережевому рівні і є незалежним від конкретних технологій доступу або протоколів вищого рівня.

Щодо маршрутизації з урахуванням QoS, використовуються різні протоколи, такі як OSPF (Open Shortest Path First) або RIP (Routing Information Protocol). Однак, з конвергенцією мереж передачі даних та телекомунікацій навколо NGN (Next Generation Network), проблеми з маршрутизацією QoS стають складнішими для вирішення. Це пов'язано з існуванням трафіку з різними обмеженнями QoS в одній мережі, складністю отримання актуальної інформації про стан мережі та управлінням ресурсами мережі для різних рівнів обслуговування.

Узагалі, вирішення проблеми QoS в Інтернеті вимагає комплексного підходу, поєднуючи різні моделі, протоколи та технології для забезпечення потрібного рівня обслуговування для різних типів трафіку та вимог

користувачів.

ATM QoS

ATM (Asynchronous Transfer Mode) QoS (Quality of Service) відноситься до набору технологій, які використовуються для забезпечення якості обслуговування в мережах ATM. ATM є комутованою мережевою технологією, де дані передаються у вигляді маленьких пакетів, відомих як "клітини". З метою забезпечення передачі даних з вимогами до якості обслуговування, ATM QoS використовує різні механізми та параметри.

Основні елементи ATM QoS включають:

Traffic Shaping (формування трафіку): Цей механізм дозволяє регулювати розподіл трафіку, контролюючи швидкість передачі даних. Це дозволяє уникнути перевантаження мережі та забезпечити стабільну передачу даних.

Traffic Policing (контроль трафіку): Цей механізм перевіряє, чи відповідає трафік певним параметрам якості обслуговування, таким як максимальна швидкість передачі або максимальне затримку. Якщо трафік не задовольняє встановлені параметри, він може бути відкинутий або оброблений з низьким пріоритетом.

Virtual Channels (віртуальні канали): ATM дозволяє створювати віртуальні канали, які можуть мати різні параметри QoS. Це дозволяє розділити трафік на окремі потоки з різними пріоритетами і параметрами обслуговування.

Quality of Service Classes (класи якості обслуговування): ATM визначає різні класи якості обслуговування, такі як Constant Bit Rate (CBR), Variable Bit Rate (VBR), Available Bit Rate (ABR) і Unspecified Bit Rate (UBR). Кожен клас має свої характеристики та параметри QoS, що дозволяють встановлювати пріоритети для різних типів трафіку.

Cell Loss Priority (пріоритет втрати клітин): Кождій клітині ATM можна призначити пріоритет втрати. Це дозволяє пріоритезувати передачу клітин залежно від їх важливості. Клітини з вищим пріоритетом мають меншу ймовірність бути відкинутими при перевантаженні мережі.

ATM QoS використовується для забезпечення гарантованої передачі даних в

мережах ATM, особливо у вимогливих застосунках, таких як голосова та відео комутація. Він дозволяє контролювати трафік, забезпечувати високу якість обслуговування та підтримувати надійну передачу даних в ATM мережах.

MPLS (Multiprotocol Label Switching) - це протокол-агностична технологія мережі, яка використовується для ефективного пересилання пакетів та інженерії трафіку. Вона забезпечує гнучке та масштабоване рішення для пересилання пакетів даних по мережі IP за допомогою міток (labels), а не традиційного маршрутизаційного підходу на основі IP-адрес призначення.

Основні аспекти MPLS:

Маркування пакетів: MPLS працює шляхом призначення мітки (label) кожному пакету даних при вході в мережу MPLS. Ця мітка містить інформацію, що визначає шлях пересилання та обробку пакета. Мітки додаються до заголовка пакета, утворюючи стек міток MPLS.

Розподіл міток: MPLS використовує протоколи розподілу міток, такі як LDP (Label Distribution Protocol) або RSVP-TE (Resource Reservation Protocol - Traffic Engineering), для розподілу міток по мережі. Протоколи розподілу міток встановлюють зв'язки між вузлами мережі, що дозволяє обмінюватися пакетами з мітками.

Маршрутизатори з переключенням міток (LSR): LSR - це ключові елементи в мережі MPLS. Вони отримують пакети, перевіряють мітку в заголовку пакета та приймають рішення про пересилання на основі цієї мітки. LSR можуть виконувати операції заміни, додавання та видалення міток, щоб пересилати пакети по маршрутах з переключенням міток MPLS (LSP).

Інженерія трафіку: MPLS дозволяє операторам мережі контролювати потік трафіку та оптимізувати ресурси мережі за допомогою технік інженерії трафіку. Шляхи пересилання трафіку можуть бути спрямовані по конкретним шляхам, щоб уникнути перенавантаження, зменшити затримки та покращити продуктивність мережі загалом.

Підтримка якості обслуговування (QoS): MPLS надає вбудовані можливості QoS, дозволяючи розрізняти та пріоритизувати трафік на основі

міток MPLS. Можна визначити різні класи обслуговування та пов'язати з ними параметри QoS для забезпечення належної обробки різних типів трафіку.

Підтримка VPN: MPLS може бути використана для створення віртуальних приватних мереж (VPN) за допомогою міток MPLS для відокремлення та ізоляції трафіку між різними користувачами VPN. VPN на основі MPLS забезпечують безпечне та масштабоване підключення для підприємств та постачальників послуг.

MPLS була широко прийнята в мережах постачальників послуг, оскільки вона пропонує ефективне пересилання, можливості інженерії трафіку та підтримку QoS. Вона дозволяє створювати приватні мережі, підтримує інтеграцію різних технологій мереж та покращує продуктивність мережі. Однак останнім часом MPLS зазнає конкуренції з боку нових технологій, таких як Segment Routing та рішень з програмним визначенням мережі (SDN).

1.10 Проектування інформаційної безпеки в мультисервісної мережі

Проектування інформаційної безпеки в мультисервісних мережах є важливим завданням, оскільки ці мережі передають різноманітний трафік, включаючи конфіденційні дані, голосову та відеоінформацію, електронну пошту, транзакції тощо. Забезпечення безпеки в таких мережах передбачає використання комплексного підходу та впровадження заходів безпеки на різних рівнях.

1.10.1 Аспекти проектування інформаційної безпеки в мультисервісних мережах

Основні аспекти проектування інформаційної безпеки в мультисервісних мережах включають:

Аутентифікація та авторизація: Це важливі механізми, які дозволяють ідентифікувати користувачів та пристрої, перевіряти їх права доступу та

надавати адекватні дозволи. Це може бути досягнуто за допомогою протоколів аутентифікації, таких як RADIUS або TACACS+, та засобів управління доступом, таких як списки контролю доступу (ACL) або рішення для управління ідентифікацією та доступом (IAM).

Шифрування: Важливий аспект безпеки включає шифрування конфіденційних даних, щоб запобігти їх незаконному доступу під час передачі через мережу. Використання протоколів шифрування, таких як SSL/TLS, IPsec або SSH, може забезпечити захист від перехоплення та несанкціонованого доступу до інформації.

Виявлення та запобігання вторгнень: Це включає використання систем виявлення вторгнень (IDS) та систем запобігання вторгнень (IPS), які моніторять мережу на предмет незвичайної активності, атак або вразливостей. Вони допомагають виявити й запобігти можливим загрозам для безпеки.

Захист мережевих пристроїв: Комутатори, маршрутизатори, мережеві фаєри та інші мережеві пристрої є цільовими об'єктами атак. Забезпечення їх безпеки передбачає використання сильних паролів, оновлення програмного забезпечення з патчами безпеки, обмеження доступу до пристроїв та моніторинг їх стану.

Резервне копіювання та відновлення: Забезпечення належного резервного копіювання та відновлення даних є важливим елементом проектування інформаційної безпеки. Це дозволяє відновити мережу в разі випадкового видалення даних, вірусних атак або інших непередбачуваних подій.

Навчання та свідомість користувачів: Одним з найважливіших елементів проектування інформаційної безпеки є навчання користувачів про загрози та процедури безпеки. Це включає проведення навчальних програм, організацію свідомості про безпеку та впровадження політик безпеки, які вимагають від користувачів дотримуватися встановлених правил та процедур.

Проектування інформаційної безпеки в мультисервісних мережах вимагає комплексного підходу та постійного оновлення, оскільки загрози безпеці постійно змінюються. Важливо розробляти і впроваджувати політики безпеки,

використовувати передові технології шифрування та виявлення вторгнень, а також навчати користувачів про процедури безпеки для забезпечення безпеки мультисервісних мереж. Спроектуємо інформаційну безпеку для мережі пресцентра. Схема проектуємої мережі представлена на рисунку

Схема проектуємої мережі. Обладнання. Адресація.

Вимоги до мережі пресцетра

1. 30 стаціонарних робочих станцій
2. проводна і радіо телефонний зв'язок
3. организація радіо мережі (WiFi) для подключення користуваяів з ноутбуками
4. створення резервних кабельних подключень для ноутбуків на випадок конфлікта обладнання або відсутність мережевих карт 802.11.
5. простота і удобство підключення нових хостів
6. надійність мережі

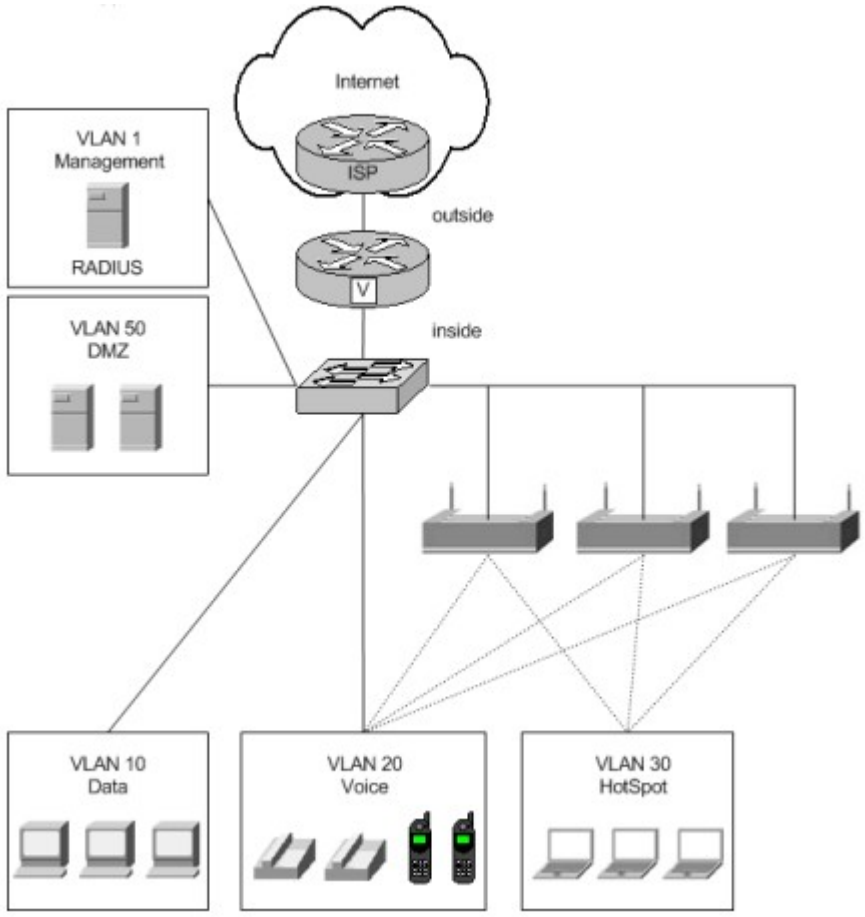


Рисунок 1.4. Схема проектуємої мережі

Була розроблена мережа відповідно до вимог, яка представлена на малюнку.

У цій мережі маршрутизатор виконує функції маршрутизації трафіку між VLAN-ами, керує встановленням з'єднання для телефонних дзвінків, виступає в ролі міжмережевого екрана та фаєрволлу для внутрішнього та зовнішнього трафіку.

Комутатор забезпечує підключення точок прийому, таких як робочі станції та IP-телефони, організує віртуальні локальні мережі (VLAN), надає функції QoS (Quality of Service) та забезпечує безпеку на рівні портів.

Точки прийому відповідають за підключення пристроїв доступу, таких як робочі станції та IP-телефони, і також надають функції QoS та безпеки.

Для реалізації необхідної функціональності вирішено використовувати наступне обладнання:

маршрутизатор Cisco 2811 Integrated Services Router,

комутатор Cisco 2960 Catalyst Switch та точки прийому Cisco Aironet 1231 Access Point. Розглянемо кожен з них.

Cisco 2811 Router:

Забезпечує продуктивність різних послуг, таких як голос і безпека, на високій швидкості передачі даних.

Має продвинуту модульність та загальну продуктивність системи.

Підтримує понад 90 різних модулів.

Має 2 інтегрованих порти 10/100 Fast Ethernet.

Опціонально підтримує технологію PoE (Power over Ethernet) для живлення пристроїв через Ethernet.

Вбудована функція шифрування.

Підтримує SDM (Security Device Manager) для зручного керування.

Може підтримувати до 1500 VPN тунелів з використанням модуля AIM-EPII-PLUS.

Забезпечує антивірусний захист з використанням NAC (Network Admission

Control).

Має функції виявлення та запобігання вторгненням (IPS - Intrusion Preventing System).

Має функції програмного міжмережевого екрану (IOS Firewall).

Підтримує аналогові та цифрові голосові дзвінки.

Опціонально підтримує голосову пошту.

Опціонально підтримує Cisco CME (CallManager Express) для локальної обробки дзвінків (до 36 IP-телефонів).

Опціонально підтримує SRST (Survivable Remote Site Telephony) для локальної підтримки голосових дзвінків (до 36 IP-телефонів).

Cisco 2960 Catalyst Switch:

Має вбудовані заходи безпеки, включаючи NAC (Network Admission Control). Підтримує QoS (Quality of Service). Має 48 вбудованих портів 10/100 Fast Ethernet. 2 інтегрованих порти Gigabit Ethernet

Cisco Aironet 1231 Access Point:

підтримка стандартів IEEE 802.11a/b/g

підтримка живлення через Ethernet

підтримка засобів управління

інтегровані функції безпеки

Таблиця 1 Адресація мережі

Номер	Назва	Адрес	Опис
VLAN 1	Management	192.168.0.0/24	Керуючий доступ до обладнання виробляється тільки з Management VLAN, тут розташовується RADIUS сервер.
VLAN 10	Data	192.168.10.0/24	Мережа для стаціонарних робочих станцій по кабельним підключенням
VLAN 20	Voice	192.168.10.0/24	Мережа для голосового трафіку (кабельні та радіор IP-телефони)
VLAN 30	HotSpot	192.168.20.0/24	Мережа гарячого бездротового доступу для відвідувачів із ноутбуками
VLAN 40	Unused	192.168.30.0/24	VLAN для портів комутатора, що не використовуються. (як складовий компонент системи безпеки
VLAN	DMZ	-	Мережа гарячого бездротового доступу для відвідувачів із ноутбуками
VLAN	Unused	217.80.159.0/29	Мережа для серверів публічного доступу (у зокрема, Proxy-сервер)

1.10.2 Забезпечення аутентифікації доступу користувачів до обладнання

1. AAA та захищений доступ до обладнання

Для забезпечення аутентифікації доступу користувачів до обладнання, авторизації їх прав та аудиту дій, необхідно налаштовувати пристрої спеціальним чином.

Існує декілька способів реалізації механізму AAA:

Перший спосіб передбачає встановлення окремого сервера ACS (access control server) у мережі управління, через який пристрої здійснюють функції аутентифікації, авторизації та аудиту.

Другий спосіб полягає у запуску локального сервера ACS на одному з пристроїв, таких як маршрутизатор, комутатор або точка доступу. Через цей локальний сервер пристрої виконують функції аутентифікації, авторизації та аудиту.

Третій спосіб передбачає, що кожен пристрій має власну локальну базу даних для реалізації механізму AAA. Аутентифікація, авторизація та аудит виконуються незалежно на кожному пристрої з урахуванням його власної бази даних.

AAA на основі локальної БД.

Для впровадження даної технології необхідно виконати наступні кроки:

1. Включити AAA на пристрої: Налаштувати пристрій таким чином, щоб він підтримував механізм AAA (аутентифікацію, авторизацію, аудит). Це може здійснюватися через налаштування відповідних параметрів на пристрої.
2. Додати користувальницький обліковий запис: Створити обліковий запис користувача з відповідними параметрами, такими як ім'я, пароль і рівень привілеїв. Цей обліковий запис буде використовуватися для аутентифікації користувачів.

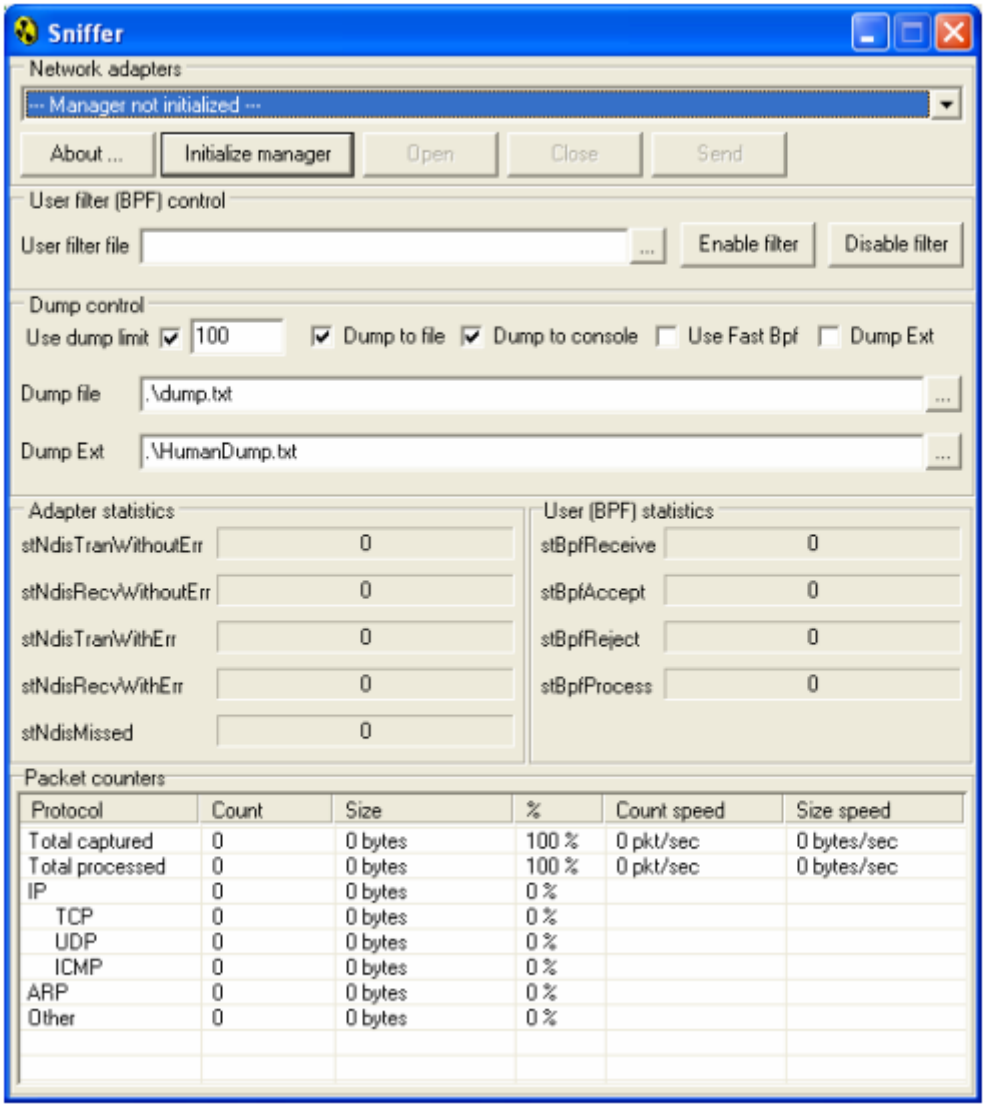


Рисунок 1.5. Головне вікно програми Sniffer.

3. Створити списки AAA: Створити списки, які визначають правила для аутентифікації, авторизації та аудиту. У цих списках визначаються параметри, такі як методи аутентифікації, правила доступу та журналізація.
4. Застосувати списки AAA: Налаштувати пристрій таким чином, щоб він застосовував визначені списки AAA у відповідних місцях.

Наприклад, встановити список AAA для конкретного інтерфейсу або для доступу до певних ресурсів.

5. Виконання цих кроків дозволить налаштувати механізм AAA і забезпечити аутентифікацію, авторизацію та аудит дій користувачів на

пристрої.

```
Router#conf terminal
Router(config)#aaa new-model
Router(config)#username test privilege 15 secret test
Router(config)#aaa authentication login logina1 local
uter(config)#aaa authorization exec execa2 local
Router(config)#line vty 0 4 34
Router(config-line)#login authentication logina1
Router(config-line)#authorization exec execa2
```

AAA з окремим ACS сервером

Для реалізації цієї технології необхідно виконати наступні кроки:

1. Встановлюємо і налаштовуємо ACS сервер:
2. Установлюємо спеціальний сервер для контролю доступу (ACS server) в мережі. Проводимо необхідну настройку сервера згідно вимог технології.
3. Створюємо облікові записи користувачів:
4. Створити облікові записи для користувачів, які будуть мати доступ до мережі. Для кожного облікового запису вказати ім'я користувача, пароль та необхідні привілеї.
5. Увімкнути AAA на пристроях: Налаштовуємо пристрої (маршрутизатори, комутатори, точки доступу) таким чином, щоб вони підтримували механізм AAA. Включаємо AAA на кожному пристрої за допомогою відповідних налаштувань.
6. Налаштовуємо адресу ACS сервера: Вказати адресу ACS сервера (або серверів), до якого пристрої будуть звертатися для здійснення процедур аутентифікації, авторизації та аудиту. Налаштовуємо на пристроях з'єднання з ACS сервером.
7. Створити листи AAA: Створити на пристроях листи, які визначатимуть

правила для аутентифікації, авторизації та аудиту. В цих листах визначаються параметри, такі як методи аутентифікації, правила доступу та журналізація.

8. Застосувати листи AAA:

Налаштовуємо пристрої таким чином, щоб вони застосовували визначені листи AAA у відповідних місцях.

Наприклад, встановити лист AAA для конкретного інтерфейсу або для доступу до певних ресурсів.

Виконання цих кроків дозволить реалізувати технологію AAA і забезпечити контроль доступу, авторизацію та аудит дій користувачів у мережі.

```
Router#conf terminal Router(config)#aaa new-model
Router(config)#radius-server host 192.168.5.100 key test
Router(config)#username test privilege 15 secret test
Router(config)#aaa authentication login logina1 group radius
Router(config)#aaa authorization exec execa2 group radius
Router(config)#aaa accounting exec execa3 wait-start group radius
Router(config)#line vty 0 4
Router(config-line)#login authentication logina1
```

Далі AAA с ACS сервером, запускаємо на окремому пристороюю (маршрутизаторі, точці доступу).

Для впровадження цієї технології необхідно виконати такі кроки:

1. Вмикаємо RADIUS-сервер на пристроях.
2. В налаштуваннях RADIUS-сервера додайте всі NAS (Network Access Server), які будуть користуватися його послугами, разом з відповідними ключами доступу.

(Опціонально) Створюємо групи користувачів.

Створіть облікові записи користувачів та розподіліть їх по групах.

В налаштуваннях AAA на всіх NAS використовуйте адресу раніше створеного RADIUS-сервера як ACS-сервер.

Створіть листи AAA.

Застосуйте листи AAA.

Початок форми

AP1# configure terminal AP1(config)# radius-server local

AP1(config-radsrv)# nas 192.168.0.252 key test

AP1(config-radsrv)# nas 192.168.0.251 key test

AP1(config-radsrv)# nas 192.168.0.250 key test

AP1(config-radsrv)# group voicegroup

AP1(config-radsrv-group)# vlan 20

AP1(config-radsrv-group)# ssid voice

AP1(config-radsrv-group)# reauthentication time 1800 35

AP1(config-radsrv-group)# group hotspotgroup

AP1(config-radsrv-group)# vlan 30

AP1(config-radsrv-group)# ssid hotspot

AP1(config-radsrv-group)# reauthentication time 1800

AP1(config-radsrv-group)# exit

AP1(config-radsrv)# user test password test group voicegroup

AP1(config)# radius-server host 192.168.0.252 key test

Для реализации данної технології необхідно :

1. Включити 802.1x глобально на коммутаторі

2. Произвести настройку усіх інтерфейсов, де необхідимо виставити режим роботи, таймери і опції.

3. Створити лист аутентифікації через 802.1x

Switch(config)# aaa authentication dot1x dot1xa1 group radius

Switch(config)# dot1x system-auth-control

witch(config-if)# dot1x port-control auto

Switch(config-if)# dot1x multi-hosts

Switch(config-if)# dot1x reauthentication

Switch(config-if)# dot1x timeout reauth-period 60

Switch(config-if)# dot1x timeout quiet-period 60

Switch(config-if)# dot1x max-reauth-req 5

Проте, з метою зниження адміністративних зусиль при підключенні нових користувачів і для забезпечення зручності користування мережею та простоти підключення, було відмовлено від даної технології.

Доступ до обладнання тоді здійснюється лише через Management мережу. Використання відкритих засобів взаємодії, таких як HTTP і Telnet, заборонено. На всіх пристроях вимикається HTTP сервер.

Router#conf terminal

Router(config)#no ip http server

Дозволяється лише використання захищеного сервера за протоколом S-HTTP. I

настроюється автентифікація доступу.

Router(config)#ip http secure-server

Router(config)#ip http authentication local

Замість Telnet використовується протокол SSH. Для цього встановлюється SSH як єдиний транспортний протокол по лініях, тим самим відключаючи Telnet. При цьому налаштовується аутентифікація доступу через SSH, що забезпечує безпеку під час з'єднання з обладнанням.

Router(config)#line vty 0 4

Router(config-line)#transport input ssh

Router(config-line)#login authentication logina1

Для закриття мережі управління від зовнішнього доступу і обмеження передачі пакетів в цю мережу необхідно додати наступні фільтруючі правила:

Заборонити всім вхідним пакетам з інших мереж проникати до мережі управління:

Вихідне IP-адресування: <IP-адреси_інших_мереж>

Порт назначення: <порти_протоколів_інших_мереж>

Дія: Заборонити

Заборонити вихідним пакетам з мережі управління виходити до інших

мереж:

Вихідне IP-адресування: <IP-адреси_мереж_управління>

Порт призначення: <порти_протоколів_інших_мереж>

Дія: Заборонити

Ці фільтруючі правила дозволять створити захист на межі мережі управління, обмежуючи комунікацію з іншими мережами та забезпечуючи безпеку та ізоляцію мережі управління. Будь ласка, зверніть увагу, що конкретні IP-адреси та порти потрібно налаштувати згідно з вашою мережною інфраструктурою та вимогами безпеки.

Router(config)#access-list 101 permit ip 192.168.0.0 0.0.0.255 192.168.0.0 0.0.0.255
Router(config)#access-list 101 deny ip 192.168.0.0 0.0.0.255 any
Router(config)#access-list 101 deny ip any 192.168.0.0 0.0.0.255

При підключенні пристроїв (комутаторів, маршрутизаторів, точок доступу) до мережі керування, необхідно враховувати такі важливі аспекти:
Усі пристрої повинні бути приєднані до відповідного VLAN, який відповідає мережі керування. Цей VLAN повинен бути налаштований на всіх транкових з'єднаннях, від комутатора до маршрутизатора та точок доступу.

Необхідно виключити порти комутатора з мережі керування, згідно з принципом безпеки на 2-му рівні. Це означає, що порти, що приєднані до пристроїв керування, не повинні бути членами мережі керування VLAN, але вони повинні бути налаштовані для передачі трафіку, необхідного для управління та конфігурації пристроїв.

Заборонити висвітлення мережі керування в ефір на точках доступу. Це означає, що точки доступу не повинні мати SSID, який пов'язаний з мережею керування.

У мережі керування, через її компактність, не були використані динамічні протоколи маршрутизації. Замість цього, на маршрутизаторі було налаштовано статичний маршрут за замовчуванням до інтерфейсу провайдера.

Важливо запобігати отриманню динамічних оновлень маршрутної

інформації про мережу керування. Це можна досягти шляхом налаштування динамічних протоколів маршрутизації таким чином, що вони не оголошують мережу керування як частину маршрутної інформації.

Враховуючи ці рекомендації, можна створити безпечну і ефективну мережу керування, яка буде захищена від зовнішнього доступу та небажаних мережевих оновлень.

1.10.3 Проектування інформаційної безпеки на 2му рівні

Безпека на 2-му рівні мережі включає в себе ряд заходів для захисту від атак, зокрема від спуфінгу MAC-адрес і атаки на посередництво в комутованому середовищі. Ось деякі рекомендації для налаштування комутаторів 2-го та 3-го рівнів з метою забезпечення безпеки:

Використовуйте функції, такі як Port Security, щоб обмежити кількість MAC-адрес, які можуть бути нав'язані на порт комутатора. Це запобігає атакам з використанням спуфінгу MAC-адрес.

Встановіть список дозволених MAC-адрес (MAC Whitelist), які можуть бути прийняті на порті комутатора. Це допомагає уникнути прийняття небажаних MAC-адрес і зменшує ризик атаки спуфінгом.

Використовуйте функцію DHCP Snooping для перевірки валідності DHCP-пакетів, які надходять на порти комутатора. Це допомагає запобігти атакам, пов'язаним зі спуфінгом DHCP.

Налаштуйте функцію Dynamic ARP Inspection (DAI), яка перевіряє правильність ARP-запитів та ARP-відповідей на портах комутатора. Це ускладнює атаки, пов'язані зі спуфінгом ARP.

Використовуйте VLAN-и для логічного розділення трафіку в мережі. Це допомагає зменшити можливість атак на посередництво в комутованому середовищі.

Встановіть додаткові заходи безпеки, такі як BPDU Guard і Root Guard, для запобігання атакам, пов'язаним з маревою протоколу STP (Spanning Tree

Protocol).

Регулярно оновлюйте програмне забезпечення комутаторів, щоб користуватися останніми заходами безпеки та виправленнями помилок.

Ці заходи допоможуть забезпечити безпеку на 2-му рівні мережі та запобігти багатьом типам атак, пов'язаних зі спуфінгом та посередництвом.

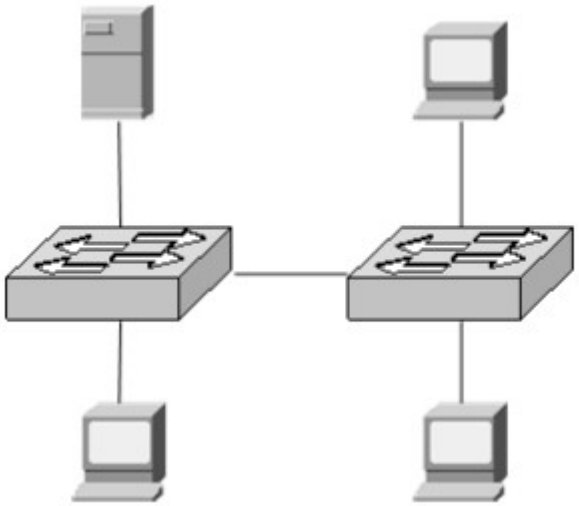


Рисунок1.6. Встановлення посередництва у комутованому середовищі**.**

Технологія port-security дійсно може бути використана для захисту від атак, пов'язаних із спуфінгом MAC-адрес. Основні можливості, які вона надає, включають:

Обмеження кількості вивчених MAC-адрес на певному інтерфейсі комутатора. За допомогою налаштувань port-security можна обмежити, скільки MAC-адрес може бути вивчено з певного порту. Це дозволяє уникнути перевантаження пам'яті комутатора та забезпечити контроль над MAC-адресами, які можуть бути пов'язані з певним портом.

Застосування штрафних санкцій за порушення. Порти комутатора можуть бути налаштовані на застосування штрафних санкцій, таких як вимкнення порту або видалення вивчених MAC-адрес, якщо порушені певні політики безпеки. Наприклад, якщо на порті вивчено більше MAC-адрес, ніж дозволено, можна застосувати штрафні заходи для запобігання атак.

Дозвіл лише певним станціям підключатися до порту. Можна

налаштувати комутатор таким чином, щоб він приймав тільки валідні MAC-адреси від певних станцій. Це забезпечує контроль над тим, хто може підключатися до порту комутатора і запобігає невповідомленому доступу до мережі.

Використання технології port-security разом з іншими заходами безпеки значно зменше ризики атак, пов'язаних зі спуфінгом MAC-адрес та забезпечити більшу безпеку в мережі.

Наведені альтернативні санкції дійсно можуть бути використані в рамках технології port-security. Конкретний вибір санкцій залежить від вимог і обмежень вашої мережі.

Переведення порту в стан errdisable є ефективним способом заблокувати порт, який порушує політику безпеки. Після блокування порту, він може бути відновлений адміністратором вручну або автоматично за допомогою механізму errdisable recovery. Проте, варто враховувати можливі наслідки таких блокувань і їх вплив на санкціоновані станції.

Блокування всіх пакетів з MAC адресами джерела, коли кількість вивчених MAC-адрес перевищує встановлений поріг, є альтернативним підходом. Це дозволяє дозволяє продовжувати роботу з дозволеними MAC-адресами, а блокувати неправильні адреси.

Встановлення "пастки" на пристрої збору лог-інформації може допомогти відслідковувати спроби атак та збирати відповідні дані для подальшого аналізу.

Таймер старіння вивчених MAC-адрес є важливим аспектом налаштування port-security. Його використання дозволяє автоматично видаляти MAC-адреси, які вже не активні, з пам'яті комутатора. Це забезпечує ефективне використання ресурсів комутатора і уникнення переповнення таблиці вивчених MAC-адрес.

Загалом, використання комбінації різних санкцій та налаштувань технології port-security дозволяє створити більш безпечне середовище мережі та ефективно захистити від спуфінг-атак.

Switch(config-if)#switchport port-security

Switch (config-if)#switchport port-security maximum 1

Switch(config-if)#switchport port-security violation protect

Switch (config-if)#switchport port-security aging static

Switch (config-if)#switchport port-security aging type inactivity

Switch (config-if)#switchport port-security aging time 1

Установки port-security на комутаторах стосуються лише портів доступу і не застосовуються до портів транків. Це дозволяє забезпечити гнучкість використання транків для передачі даних між комутаторами.

Щодо протоколу VTP (VLAN Trunking Protocol), для запобігання несанкціонованим змінам VLAN-інформації рекомендується аутентифікувати VTP-повідомлення. Це можна зробити шляхом налаштування пароля VTP для домену.

Пароль VTP, встановлений для домену, використовується для аутентифікації комутаторів, які намагаються надіслати або прийняти VTP-повідомлення. Тільки комутатори з вірним паролем VTP можуть активно взаємодіяти з іншими комутаторами у вказаному домені. Це допомагає запобігти несанкціонованим змінам VLAN-інформації і забезпечити контроль над VLAN-ами в мережі.

Важливо встановити однаковий пароль VTP на всіх комутаторах у домені і переконатися, що він застосовується на всіх портах транків, які використовуються для передачі VTP-повідомлень.

Застосування пароля VTP є важливим заходом безпеки, який допомагає запобігти несанкціонованим змінам VLAN-інформації і забезпечити централізований контроль над VLAN-ами у комутованій мережі.

Switch#vlan database

Switch(vlan-data)#vtp password test

Switch(vlan-data)#apply

відключення протоколу VTP і перехід комутатора в режим "прозорий" (transparent) є додатковим заходом безпеки, який може бути використаний для запобігання несанкціонованим змінам VLAN-інформації зі сторони

потенційних зловмисників.

У режимі "прозорий" комутатор може локально створювати, видаляти та модифікувати інформацію про VLAN-и, але не застосовує отримані оновлення VTP на свою базу даних. Замість цього, він просто пересилає отримані VTP-повідомлення далі до інших комутаторів.

Це означає, що комутатор, налаштований в режимі "прозорий", не приймає і не впливає на зміни, які здійснюються іншими серверами або клієнтами VTP. Він зберігає свою власну локальну копію VLAN-інформації, але не розповсюджує її далі по мережі.

Такий підхід забезпечує контроль над VLAN-ами на рівні комутатора і запобігає несанкціонованим змінам, які можуть бути внесені з інших комутаторів через протокол VTP. Це особливо корисно в середовищах, де існує ризик несанкціонованого доступу або зловживання привілеями.

Таким чином, переведення комутатора в режим "прозорий" є доброю практикою з точки зору безпеки, яка допомагає захистити мережу від можливих маніпуляцій з VLAN-інформацією.

Switch#vlan database

Switch(vlan-data)#vtp mode transparent

Так, атака на протокол DTP (Dynamic Trunking Protocol) може створювати серйозну загрозу безпеці в мережевому середовищі. DTP використовується для автоматичного встановлення транкових з'єднань між комутаторами. Зловмисник, який отримав доступ до магістралі (транка), може використовувати емуляцію DTP для отримання транкових з'єднань і маніпулювання мережевими даними.

Якщо зловмисник успішно емулює DTP протокол, він може отримати доступ до всієї інформації, що проходить через ту саму VLAN, до якої належить отриманий транк. Він також може маніпулювати VTP (VLAN Trunking Protocol) оновленнями, що може призвести до несанкціонованих змін у VLAN-інформації.

Крім того, зловмисник може використовувати техніку подвійної

інкапсуляції, додаючи два заголовки 802.1q до кадру. Це дозволяє йому бути посередником між різними VLAN-ами і отримувати доступ до мережевих даних, які пройшли через ці VLAN.

Для запобігання таким атакам рекомендується вживати наступні заходи безпеки:

Вимкнути DTP на транках і налаштувати їх як статичні транки (trunk) для певних портів, які повинні бути транками.

Використовувати безпечні режими (наприклад, "desirable" або "nonegotiate") для портів, які мають бути транками, і вимкнути автоматичний режим (auto) і динамічний режим (dynamic) на решті портів.

Встановити магістралі (транки) тільки на необхідних портах і виключити їх на непотрібних портах.

Використовувати налаштування аутентифікації (наприклад, 802.1X) для контролю доступу до мережевих пристроїв і встановлення транкових з'єднань.

Ці заходи допоможуть уникнути атак на протокол DTP та забезпечити безпеку транків і VLAN-інформації в мережі.

Для боротьби зі загрозами подвійної інкапсуляції і несанкціонованого доступу до інших VLAN-ів було прийнято рішення відключити адміністративно всі порти, Що не використовуються, та помістити їх в окрему VLAN з назвою "unused". Крім того, було налаштовано ці порти як порти доступу (access ports).

Цей підхід є ефективним способом зменшення ризику атак і недозволених доступів до інших VLAN-ів. Відключення адміністративно не використовуваних портів допомагає уникнути потенційних адміністративних помилок, які можуть призвести до небезпеки. Поміщення цих портів в окрему VLAN "unused" і налаштування їх як портів доступу забезпечує їх ізоляцію від інших VLAN-ів і обмежує можливості зловмисників впливати на мережевий трафік.

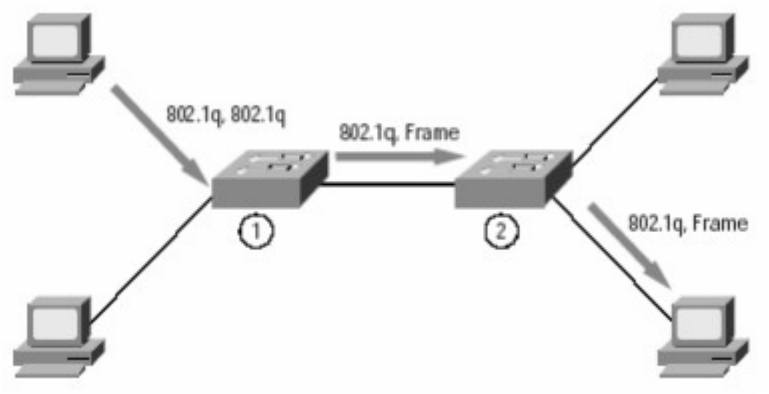


Рисунок 1.7. Атака через двойну інкапсуляцію

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 40

Switch(config-if)#shut

Всім портам доступу явно виставити режим access та визначити їх у правильну

VLAN. Також для них вимикається DTP.

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#switchport nonegotiate

Всі порти, що є магістральними, про всяк випадок визначаються

VLAN, що не використовується. Це робиться для страховки у разі переведення порту в режим

доступу адміністративно, коли адміністратор забуває визначити VLAN для нього.

Switch(config-if)#switchport access vlan 40

Багато небезпек несе у собі протокол 2-го рівня CDP, оскільки він повідомляє сусіднім пристроям багато приватної інформації.

Ось приклад виведення інформації про сусідні пристрої командою #show cdp neighbor

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
device1.cisco.com	Eth 0/1	122	T S	WS-C2900	2/11
device2.cisco.com	Eth 0/1	179	R	4500	Eth 0
device3.cisco.com	Eth 0/1	155	R	2500	Eth 0
device4.cisco.com	Eth 0/1	155	R	2509	Eth 0

Вивід команди #show cdp neighbors detail:

Device ID: device2.
cisco.com Entry address(es):
IP address: 171.68.162.134
Platform: cisco 4500, Capabilities:
Router Interface:
Ethernet0/1, Port ID (outgoing port):
Ethernet0 Holdtime :
156 sec Version :
Cisco Internetwork Operating System Software
IOS(tm) 4500 Software(C4500-J-M),Version 11.1(10.4),MAINTENANCE INTERIM SOFTWARE Copyright (c) 1986-1997 by Cisco Systems, Inc.
Compiled Mon 07-Apr-97 19:51 by dschwart

Така інформація не має потрапити до чужих рук. Для цього було прийнято рішення відключити CDP на всіх пристроях.
Switch(config)#no cdp run

Відключення STP (Spanning Tree Protocol) на VLAN-ах може бути одним зі способів захисту від атак, які спрямовані на маніпуляцію деревом STP та порушення працездатності мережі. Цей підхід використовується для уникнення можливості зловмисника стати коренем дерева STP та маніпулювати пріоритетами, що може спричинити відмову в роботі мережі (DoS атака).

Однак, перед відключенням STP на VLAN-ах потрібно ретельно оцінити його наслідки. STP виконує важливу роль в уникненні фізичних циклів у топології мережі та забезпечує надійність і збалансованість трафіку. Відключення STP може призвести до появи циклів і збільшення ризику виникнення петель та переповнення мережі.

Як альтернативу, можна розглянути використання інших методів захисту від атак на STP, таких як налаштування паролів для BPDU, обмеження доступу до протоколу STP на портах, використання PortFast для швидкого переходу портів в стан Forwarding, а також моніторинг та аудит конфігурацій STP.

Вибір заходів захисту повинен бути обгрунтованим і враховувати вимоги топології мережі, її надійності та особливості використання. Рекомендується провести аналіз ризиків і консультуватися з експертами з мережевої безпеки, щоб визначити найкращі практики та заходи захисту для конкретного середовища.

Switch(config)#no spanning-tree vlan 10

Switch(config)#no spanning-tree vlan 20

Switch(config)#no spanning-tree vlan 30

Switch(config)#no spanning-tree vlan 40

Switch(config)#no spanning-tree vlan 50

Механізм захисту STP з використанням bpdufilter дійсно може бути використаний для оголошення портів доступу як тупикових (англ. portfast). Коли порт налаштований як тупиковий, він вважається закінченим пунктом і не очікується наявність інших комутаторів за цим портом.

При налаштуванні bpdufilter на порті, він виконує функцію відкидання (відхилення) усіх Bridge Protocol Data Units (BPDU), які надходять через цей порт. BPDU є керівними повідомленнями STP, і вони використовуються для обміну інформацією між комутаторами для побудови та підтримки дерева STP.

Використання bpdufilter на портах доступу може бути корисним у випадках, коли на цих портах точно не повинно бути жодних інших

комутаторів і ви хочете запобігти потенційним проблемам, пов'язаним з неправильним розгортанням STP. Наприклад, якщо порт підключений до сервера або кінцевого пристрою, де використовується статична конфігурація VLAN і відсутність STP функціональності.

Проте, варто пам'ятати, що використання bpdufilter на портах доступу має потенційні ризики. Якщо на порт непередбачено підключається комутатор, це може призвести до появи петель або невірної роботи STP. Тому перед використанням bpdufilter рекомендується ретельно оцінити топологію мережі та ризики і проконсультуватися з експертами з мережевої безпеки.

Switch(config-if)#spanning-tree bpdufilter enable

1.10.4 Захист від атаки "DHCP голодування"

Для захисту від атаки "DHCP голодування" в даній мережі було прийнято рішення використовувати технологію DHCP Snooping. Ця технологія використовується для контролю і фільтрації DHCP-повідомлень, що проходять через комутатори, з метою запобігання неправомірному виділенню IP-адрес та наданню некоректних налаштувань користувачам.

Для використання DHCP Snooping необхідно виконати наступні кроки:

Увімкнути глобально DHCP Snooping на комутаторі.

Вказати VLAN, на якому буде застосовуватися DHCP Snooping.

Встановити додаткові опції, такі як перевірка MAC-адреси, для покращення безпеки.

Оголосити надійні та ненадійні (довірені та недовірені) інтерфейси.

Встановити пороги для кількості DHCP-повідомлень, які можуть пройти через кожен інтерфейс.

Ці заходи дозволять обмежити кількість DHCP-повідомлень, що проходять через кожний інтерфейс, а також визначити надійні інтерфейси, де дозволено проходити DHCP-повідомленням від DHCP-сервера.

Використання DHCP Snooping допомагає зменшити ризик атаки "DHCP

голодування" і забезпечує більшу безпеку в мережі, де використовується протокол DHCP для надання налаштувань користувачам.

ip dhcp snooping ip dhcp snooping vlan 20

ip dhcp snooping information option

ip dhcp snooping verify mac-address

! на інтерфейсі fast 0/1, до якого підключений маршрутизатор, який є DHCP сервером.

ip dhcp snooping trust ip dhcp snooping limit rate 200

! на любому інтерфейсі рівня доступа ip dhcp snooping limit rate 20

На випадок створення демілітаризованої зони було опрацьовано варіант створення приватних віртуальних локальних мереж (private VLAN).

Ми перерахували кроки, які відносяться до конфігурації приватних VLAN (Private VLANs), а не до DHCP Snooping. Приватні VLAN використовуються для ізоляції трафіку між пристроями в межах одного VLAN. Тому, якщо ви маєте намір налаштувати приватні VLAN, підпорядковані використанню DHCP Snooping, ось кроки, які ви можете виконати:

Створюємо приватні VLAN. Визначте первинну VLAN, яка буде використовуватись для сполучення зовнішнього світу і зв'язку з DHCP-сервером.

1.Проасоціюємо приватні VLAN з первинною VLAN.

2.Налаштуємо порти комутатора, до яких підключаються сервери, як тупикові порти (Private VLAN Host). Це забезпечить ізоляцію трафіку між серверами.

Тепер, що стосується DHCP Snooping, ось кроки, які потрібно виконати:

1.Микаємо DHCP Snooping глобально на комутаторі.

2.Вкажіть VLAN, на яких буде застосовуватися DHCP Snooping.

3.Налаштуємо додаткові опції, такі як перевірка MAC-адресів та виключення портів, де знаходяться DHCP-сервери (trusted interfaces).

4.Встановлюємо пороги для кількості DHCP-повідомлень на інтерфейсі, якщо це необхідно.

Ці кроки допоможуть застосувати технологію DHCP Snooping у мережі та захистити її від певних атак, пов'язаних з протоколом DHCP.

```
Switch(config)# vlan 51
Switch(config-vlan)# private-vlan isolated
Switch(config)# vlan 50
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 51
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 50 51
```

Так, для боротьби з проблемами широкомовних штормів рекомендується використовувати механізм storm control, який доступний на багатьох комутаторах, включаючи Cisco Catalyst Switch 2960.

Щоб налаштувати storm control, виконуємо наступні кроки:

1.Вибераємо інтерфейс комутатора, на якому бажаєте використовувати storm control.

2.Вмикаємо storm control на вибраному інтерфейсі командою storm-control <рівень>.

<рівень> вказує процентний поріг, який ви хочете встановити для контролю над широкомовним трафіком.

Наприклад, storm-control 5.00 означає обмеження широкомовного трафіку до 5% пропускної здатності інтерфейсу.

Налаштуємо поведінку комутатора щодо обробки широкомовних кадрів, які перевищують заданий поріг. Це може включати фільтрацію (відкидання) широкомовних пакетів, переведення порту в стан errdisable або надсилання лог-повідомлень.

Налаштування поведінки може варіюватися залежно від моделі комутатора і його програмного забезпечення.

Встановлення обмежень на рівні 5% продуктивності дозволить контролювати і обмежувати широкомовний трафік, що може виникати через помилки або зловмисні дії. Рекомендується також розглянути додаткові заходи,

які можуть включати вимкнення портів або надсилання лог-повідомлень, для забезпечення відповідного управління широкомовним штормом та виявлення проблем.

Switch(config-if)# storm-control broadcast level 5

Проетування інформаційної безпеки на 3 рівні

На основі наданої інформації не вдалося відтворити конкретний приклад опису сигнатури. Однак, IPS (Intrusion Prevention System) є потужним механізмом захисту на рівні мережі, який виявляє та запобігає вторгненням у мережеве середовище.

Нижче наведені загальні кроки для конфігурації та застосування IPS на маршрутизаторах Cisco IOS:

Встановлення та налаштування сигнатур: IPS використовує сигнатури для виявлення конкретних видів атак. Сигнатури зазвичай зберігаються у файлі формату SDF (Signature Detection File). Ви можете вимкнути непотрібні сигнатури або налаштувати їх параметри за потреби.

Налаштування правил застосування:

Вибераємо, які інтерфейси маршрутизатора мають бути охоплені IPS і встановлюємо правила застосування IPS на цих інтерфейсах. Наприклад, можемо встановити IPS для перевірки всього трафіку, що проходить через інтерфейси WAN.

Налаштування дій при виявленні вторгнення: Встановіть, які дії мають бути вжиті при виявленні атаки. Це може включати надсилання тривоги на syslog сервер, відкидання пакетів, скидання з'єднання або блокування трафіку з IP-адреси атакуючого на певний час.

Налаштування логування та моніторингу: Визначте, які події IPS мають бути зареєстровані та які механізми моніторингу ви плануєте використовувати. SDEE (Security Device Event Exchange) є одним з механізмів для генерації лог-подій IPS.

Залежно від ваших потреб та конкретних вимог безпеки, ви можете налаштувати IPS таким чином, щоб він забезпечував найбільш ефективний захист мережі.

Так, ви можете скопіювати файл sdf з маршрутизатора на комп'ютер і змінити його для налаштування поведінки IPS під час виявлення атаки. Для цього ви можете використовувати протокол TFTP (Trivial File Transfer Protocol). Ось кілька кроків для обміну файлами між маршрутизатором та комп'ютером за допомогою TFTP:

Запустіть TFTP-сервер на комп'ютері: Встановіть та налаштуйте TFTP-сервер на комп'ютері, який буде служити для обміну файлами з маршрутизатором. Існують різні програми TFTP-серверів, які ви можете використовувати, наприклад, tftpd32, SolarWinds TFTP Server тощо.

Скопіюйте файл sdf з маршрутизатора на комп'ютер: На маршрутизаторі виконайте команду copy flash tftp та слідуйте інтерактивним підказкам. Введіть IP-адресу комп'ютера і ім'я файлу sdf, який ви хочете скопіювати. Ця команда перегонить файл sdf зі сховища (наприклад, флеш-пам'яті) маршрутизатора на комп'ютер через TFTP.

Змініть файл sdf на комп'ютері: Знайдіть скопійований файл sdf на комп'ютері та відкрийте його в текстовому редакторі. Здійсніть необхідні зміни в полі EventAction, яке контролює поведінку IPS під час виявлення атаки. Збережіть змінений файл sdf.

Скопіюйте змінений файл sdf на маршрутизатор: На маршрутизаторі виконайте команду copy tftp flash та слідуйте інтерактивним підказкам. Введіть IP-адресу комп'ютера та ім'я файлу sdf, який ви хочете скопіювати. Ця команда замінить існуючий файл sdf на маршрутизаторі новим файлом sdf, який ви змінили на комп'ютері.

Після цих кроків ви зможете використовувати змінений файл sdf для налаштування поведінки IPS на маршрутизаторі. Завжди бережіть оригінальний файл sdf, щоб у разі потреби повернутися до нього.

Для запуску системи IPS і виконання захисних заходів на маршрутизаторі

необхідно виконати такі кроки:

1.Завантаження файлу sdf в модуль IPS: Виконайте процедуру завантаження файлу sdf з комп'ютера на маршрутизатор у модуль IPS за допомогою протоколу TFTP, як описано в попередньому відповіді.

2.Створення іменованого правила IPS: Визначити іменоване правило IPS, в якому вказані умови, сигнатури або шаблони, які мають викривати потенційні атаки. Це може бути зроблено за допомогою відповідних команд або конфігураційного інтерфейсу маршрутизатора, залежно від версії IOS.

3.Увімкнення механізму SDEE та налаштування розмірів буферів повідомлень: Включаємо механізм SDEE (Security Device Event Exchange) для зберігання лог-подій, які будуть створюватися під час роботи IPS. Налаштуйте розміри буферів повідомлень, які визначають максимальну кількість повідомлень, які можуть бути збережені у буферах.

4. Застосування правила IPS на потрібних інтерфейсах та напрямках: Налаштуйте маршрутизатор таким чином, щоб правило IPS було застосовано на відповідних інтерфейсах, де потрібна захисту. Виберіть необхідні напрямки трафіку, на які слід застосувати правило IPS.

Ці кроки можуть відрізнятися залежно від конфігурації конкретного маршрутизатора та версії IOS, тому рекомендується вивчити документацію Cisco або консультуватися з фахівцями для точного налаштування системи IPS на вашому маршрутизаторі.

```
Router(config)#ip ips sdf location flash:128MB.sdf
Router(config)#ip ips name testIPS
Router(config)#ip ips notify SDEE
Router(config)#ip sdee messages 111
Router(config)#ip sdee alerts 555
Router(config)#interface fast 0/1
Router(config-if)#ip ips testIPS in 44
Router(config-if)#ip ips testIPS out
```

Для реалізації технології TCP intercept і захисту від атаки TCP SYN

FLOOD на маршрутизаторі необхідно виконати такі кроки:

1.Створити розширений список контролю доступу (ACL): Створіть ACL, в якому визначається трафік, який підлягає перехопленню. ACL визначатиме правила фільтрації для вхідного трафіку, що буде перевірятися TCP intercept.

2.Зв'язати ACL із технологією TCP Intercept: Виконайте налаштування, щоб пов'язати створений ACL із технологією TCP Intercept. Це забезпечить перехоплення трафіку, що відповідає умовам ACL.

3.Виставити режим роботи TCP intercept: Встановіть режим роботи TCP intercept на маршрутизаторі, який може бути "intercept" або "watch". Режим "intercept" спробує встановити з'єднання з хостом перед пересиланням запиту до сервера, відкидаючи небажані відповіді. Режим "watch" буде відстежувати статистику напіввідкритих з'єднань і може виконувати їхнє скидання за потреби.

4.Виставити режим відбору кандидатів на скидання: Налаштувати механізм відбору кандидатів на скидання з'єднань, який може бути "випадковим" або "найстарішим". Це визначає, які з'єднання будуть скинуті, якщо буде досягнуто захисний поріг.

5.Виставити захисні пороги: Встановіть захисні пороги, які визначають, коли механізм TCP intercept буде виконувати додаткові дії для захисту від атаки. Ці пороги можуть бути налаштовані, наприклад, для кількості напіввідкритих з'єднань або швидкості надходження пакетів SYN.

Ці кроки можуть варіюватися залежно від конфігурації конкретного маршрутизатора та версії IOS. Рекомендується ознайомитися з документацією Cisco або звернутися до фахівців для точного налаштування TCP intercept на нашому маршрутизаторі.

```
Router(config)#ip access-list 125
permit tcp any host 217.80.159.1
Router(config)#ip tcp intercept list 125
Router(config)#ip tcp intercept mode intercept
Router(config)#ip tcp intercept drop-mode old ! час, за який напіввідкрите
```

з'єднання має перейти у повне.

Router(config)#ip tcp intercept watch-timeout 30 ! інтервал неактивності з’єднання

ip tcp intercept connection-timeout 10

! кількість напіввідкритих сполук, за яких потрібно починати агресивне

! скидання ip tcp intercept max-incomplete high 100

! кількість напіввідкритих сполук, за яких потрібно починати агресивне

! скидання, при якому потрібно прекращати агресивне

! скидання ip tcp intercept max-incomplete low 20

! кількість напіввідкритих з'єднань за хвилину, коли потрібно починати агресивне

! скидання е ip tcp intercept one-minute high 50

! количество напіввідкритих з’єднань за хвилину, при якому потрібно прекратити

! агресивне очікування ip tcp intercept one-minute low

Для налаштування Reflexive ACL на прикордонному маршрутизаторі і фільтрації сесій потрібно виконати наступні кроки:

1. Створюємо іменований ACL для вихідного потоку: Створіть ACL, в якому визначається трафік, який підлягає фільтрації. В цьому ACL ми вказуєте правила, які будуть застосовуватись до вихідних пакетів.

2. Створюємо іменований ACL для вхідного потоку: Створюємо другий ACL, в якому вказуєте посилання на динамічний список, визначений в першому ACL. Цей другий ACL буде використовуватись для контролю вхідного трафіку, що відповідає на вихідні пакети.

3.Встановлюємо тайм-аут неактивності сесії: Визначте інтервал часу, протягом якого сесія вважатиметься активною. Якщо сесія неактивна протягом цього інтервалу, то тимчасові правила Reflexive ACL будуть видалені.

4.Застосуємо ACL на інтерфейсах: Налаштуємо інтерфейси маршрутизатора, на яких необхідно застосувати Reflexive ACL, і вкажіть, який

ACL застосовувати для контролю трафіку.

Ці кроки можуть варіюватися залежно від конфігурації маршрутизатора та версії IOS.

Рекомендується ознайомитися з документацією Cisco або звернутися до фахівців для точного налаштування Reflexive ACL на вашому маршрутизаторі.

```
ip access-list extended
OutBoundFilter permit tcp any any
reflect TCPtrafic ip access-list extended InBoundFilter evaluate TCPtrafic
! тут можуть розміщаватися інші дозвільні/заборонні правила
deny ip any any ip reflexive-list timeout 180
```

Технологія CBAC (Context-Based Access Control) є потужним механізмом захисту, який фільтрує TCP і UDP пакети на основі інформації рівня програми. Використовуючи CBAC, можна застосовувати додаткові рівні контролю інформації, що проходить через мережевий екран.

Основні особливості CBAC:

Фільтрація на рівні протоколу: CBAC базується на аналізі протоколів, таких як HTTP, SMTP, FTP, і т.д. Це дозволяє виявляти та блокувати нелегальні або небезпечні дії в мережі.

Підтримка двостороннього фільтрування: CBAC може проводити фільтрацію як в напрямку зовнішньої мережі в середину, так і в напрямку внутрішньої мережі на зовнішні ресурси. Це дозволяє контролювати трафік усередині мережі та забезпечувати безпеку з'єднань.

Динамічне створення ACL: CBAC автоматично створює тимчасові ACL для забезпечення проходження відповідей на вхідні з'єднання, які були ініційовані з внутрішньої мережі.

Виявлення небезпечних дій: CBAC використовує розуміння протоколів для виявлення небезпечних або нелегальних інструкцій, які можуть бути включені в пакети.

Підтримка додаткових заходів безпеки: CBAC може додатково

застосовувати заходи безпеки, такі як блокування певних протоколів або додаткові перевірки на основі аналізу вмісту пакетів.

Для налаштування CBAC необхідно налаштувати правила ACL та включити механізм CBAC на маршрутизаторі. Конкретні кроки залежать від виробника обладнання та версії програмного забезпечення, тому рекомендується ознайомитися з документацією виробника або звернутися до фахівців для правильного налаштування CBAC на вашому маршрутизаторі.

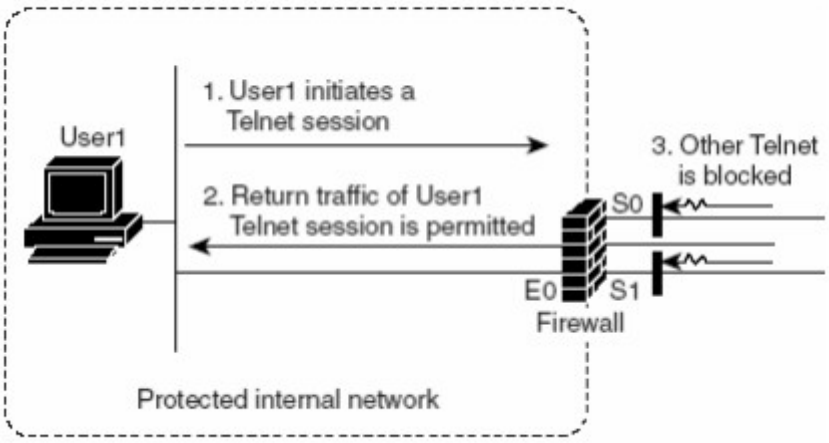


Рисунок1.8. CBAC – відкриття тимчасових зворотних дірок.

Механізм CBAC (Stateful Packet Inspection) схожий на Reflexive ACL, оскільки він відкриває зворотні дірки для вихідних з'єднань. Проте CBAC також надає додаткові можливості для виявлення атак та захисту системних ресурсів. Основні кроки для налаштування CBAC такі:

Встановлення глобальних таймерів та порогів: Визначте значення таймерів і порогів для виявлення атак і регулювання трафіку.

Створення іменованого інспекційного правила: Створіть правило, в якому вказані протоколи, що підлягають фільтрації та інспекції.

Створення списків контролю доступу: Створіть списки контролю доступу (ACL), в яких визначені правила для блокування певних пакетів або дозволу певних типів трафіку.

Застосування списків контролю доступу на інтерфейсах: Призначте ACL

для вхідних і вихідних інтерфейсів, щоб фільтрувати трафік, що проходить через мережевий пристрій.

Застосування інспекційного правила: Призначте створене інспекційне правило до відповідних інтерфейсів, щоб виконувати інспекцію пакетів, фільтрацію та виявлення атак.

У нашому випадку, ви вирішили налаштувати фільтрацію TCP, UDP, FTP, моніторинг фрагментованих пакетів та блокування Java з певних серверів. Тому вам необхідно створити відповідні списки контролю доступу та інспекційне правило, що відповідатимуть вашим потребам.

Важливо врахувати, що конкретні кроки налаштування можуть відрізнятися залежно від виробника обладнання та версії програмного забезпечення. Рекомендується ознайомитися з документацією виробника або звернутися до фахівців для налаштування CBAC на вашому мережевому пристрої.

```
ip inspect max-incomplete low 200
ip inspect max-incomplete high 400
ip inspect one-minute low 100
ip inspect one-minute high 400
ip inspect udp idle-time 20
ip inspect dns-timeout 6
ip inspect tcp idle-time 600
ip inspect tcp finwait-time 6
 inspect tcp synwait-time 18
 inspect tcp max-incomplete host 20 block-time 0
 ip inspect name testinspect ftp timeout 20
ip inspect name testinspect http java-list FriendlySites
ip inspect name testinspect tcp
ip inspect name testinspect udp
ip inspect name testinspect fragment maximum 20
ip access-list standart FriendlySites
! permit trafic from friendlySites
```

ermit 213.213.213.213

permit 217.80.217.40

! create an ACL to permit inspecting trafic to leave inside network access-list 101

permit tcp 192.168.0.0 0.0.255.255 any access-list 101

permit udp 192.168.0.0 0.0.255.255 any access-list 101

permit icmp any any access-list 101 deny ip any any

! create an ACL to deny inspecting trafic to enter inside network from outside access-list 111 deny tcp any 192.168.0.0 0.0.255.255 access-list 111

deny udp any 192.168.0.0 0.0.255.255 access-list 111 permit

ip any any … !

on outside interface ip access-group 111

in ip access-group 101 out ip inspect testinspect in

Однак не слід забувати, що CBAC має ті ж обмеження, що і Reflexive ACL

Відключення невикористовуваних служб та протоколів є важливою складовою безпечної конфігурації пристроїв. Нижче перераховані кроки для відключення деяких непотрібних служб та протоколів:

Відключення непотрібних TCP та UDP служб: Перегляньте список служб, які запущені на вашому пристрої, та відключіть ті, які не використовуються. Це можна зробити управлінням списком служб на операційній системі пристрою.

Відключення служби finger: Служба finger може надавати зайву інформацію про користувачів системи. Вимкніть цю службу або обмежте її доступ до необхідних користувачів.

Відключення протоколу BOOTP: Якщо протокол BOOTP не використовується у вашій мережі, відключіть його. Це можна зробити на налаштуваннях мережевого пристрою або маршрутизатора.

Відключення SNMP: SNMP (Simple Network Management Protocol) може бути вразливим до атак і використання для отримання неправомірного доступу. Якщо ви не використовуєте SNMP для моніторингу або керування пристроями,

вимкніть його.

Додатково рекомендується:

Оновлення програмного забезпечення: Періодично перевіряйте наявність оновлень для операційної системи та інших програмних компонентів пристрою. Встановлюйте всі необхідні патчі та оновлення для заповнення вразливостей.

Встановлення сильних паролів: Використовуйте складні паролі для доступу до пристроїв та інших облікових записів. Враховуйте рекомендації щодо довжини та складності паролів, а також вимагайте їх від користувачів.

Налаштування мережевої фільтрації: Використовуйте файрвол або інші засоби мережевої фільтрації для контролю трафіку, який входить і виходить з пристрою. Встановлюйте правила фільтрації, що відповідають вашим потребам та політиці безпеки.

Використання шифрування: Застосовуйте шифрування для захищеного передавання даних по мережі, особливо в разі використання протоколів, таких як SSH (Secure Shell) або HTTPS (HTTP Secure).

Зазначені кроки є загальними рекомендаціями, і конкретні налаштування можуть відрізнятися в залежності від вашого пристрою та операційної системи. Рекомендується виконати аудит безпеки вашої мережі та пристроїв, щоб виявити всі можливі вразливості і прийняти відповідні заходи для їх усунення.

no service finger

no service pad no service tcp-small-servers

no service udp-small-servers

no snmp-server

no ip bootp server

Вимкнення маршрутизації на адресу джерела може бути корисним заходом для забезпечення додаткової безпеки вашої мережі. Це запобігає використання вашого пристрою як проміжного вузла для переадресації пакетів і збільшує контроль над шляхами передачі даних у вашій мережі. Щоб вимкнути маршрутизацію на адресу джерела, виконайте наступні кроки:

Зайдіть до налаштувань вашого маршрутизатора або комутатора за допомогою адміністративного доступу.

Знайдіть налаштування маршрутизації або рутизації.

Знайдіть опцію, пов'язану з маршрутизацією на адресу джерела або "source routing".

Вимкніть цю опцію або встановіть її в безпечне значення, яке не дозволяє використання маршрутизації на адресу джерела.

Збережіть зміни і перезавантажте пристрій, якщо це потрібно, для застосування нових налаштувань.

Важливо зауважити, що конкретний процес вимкнення маршрутизації на адресу джерела може варіюватися в залежності від виробника пристрою та використовуваної оперативної системи. Рекомендується звернутися до документації пристрою або сконсультуватися з постачальником послуг для отримання точних інструкцій щодо вимкнення маршрутизації на адресу джерела у вашому конкретному випадку.

service password encryption service tcp-keepalives-in

service tcp-keepalives-out

service timestamps debuf datetime localtime

show-timezone msec

service timestamps log datetime localtime show-timezone msec

service sequence-numbers

ip cef

Обов'язково слід налаштувати банери, що з'являються під час входу на пристрій.

banner # #

banner motd # #

banner login # #

Рекомендоване повідомлення для банеру, яке виводиться при доступі до системи, може мати наступний вигляд:

"Authorized access only! This system is proprietary to <назва компанії> Enterprise. Disconnect IMMEDIATELY if you are not an authorized user! Contact <адреса електронної пошти адміністратора> or call <номер телефону адміністратора>."

Щодо обмежень на паролі та обліку помилкових спроб аутентифікації, рекомендується виконати наступні кроки:

Встановити політику складних паролів: Вимагайте від користувачів використовувати паролі, які складаються з комбінації великих і малих літер, цифр та спеціальних символів. Задайте мінімальну довжину пароля, наприклад, 8 символів.

Вимкнути можливість використання слабких паролів: Забороніть використання очевидних або легко вгадуваних паролів, таких як "password", "123456" тощо.

Обмежити кількість невдалих спроб: Встановіть обмеження на кількість помилкових спроб аутентифікації перед тим, як облік можливих атак на пароль почне застосовуватись. При перевищенні цього обмеження можна застосовувати блокування акаунта на певний час.

Вести журнал помилкових спроб: Активуємо журналювання помилкових спроб аутентифікації, щоб відслідковувати спроби несанкціонованого доступу та виявляти потенційні атаки на паролі.

Моніторити журнали безпеки: Регулярно переглядайте журнали безпеки, щоб виявляти підозрілу активність або незвичайні спроби вторгнення.

Застосування цих рекомендацій допоможе підвищити рівень безпеки вашої системи та захистити її від несанкціонованого доступу.

security passwords min-length 8

security authentication failure rate 3 log

Настроїти параметри збору лог-інформації.

logging on logging 192.168.5.100 !

log-server logging console critical

logging trap debugging

logging buffered 32000

На інтерфейсній основі, додаткові кроки для покращення безпеки можуть включати:

Вимкнути спрямовані широкомовлення (Directed Broadcast): Це може запобігти можливості використання спрямованих широкомовних пакетів для виконання атак, таких як Smurf атаки або Distributed Denial of Service (DDoS) атаки.

Вимкнути proxy-arp: Це захистить від потенційних атак ARP-отрутизатора (ARP poisoning) або ARP-флуду (ARP flooding), які можуть спричинити перехоплення пакетів або перекривання мережевих з'єднань.

Вимкнути перенаправлення (IP forwarding): Якщо пристрій не є маршрутизатором, вимкнення функції перенаправлення може запобігти небажаним маршрутизаційним поведінкам та захистити внутрішню мережу від неправильно налаштованих маршрутів або перехоплення пакетів.

Включити опцію зворотної перевірки (RPF - Reverse Path Forwarding): Ця функція дозволяє перевіряти правильність шляху до пакетів, що надходять на вхідний інтерфейс, забезпечуючи, що пакети надходять через очікуваний шлях. Це може запобігти використанню атак типу IP-захоплення або дзеркальних атак, де пакети приходять з неправильного джерела.

Вимкнення непотрібних функцій та включення захисних механізмів на інтерфейсній основі допоможе зменшити поверхню атак та підвищити загальний рівень безпеки вашої мережі.

```
no ip directed-broadcast
no ip proxy-arp
no ip redirects
ip verify unicast reachable-via rx
```

Використання Reverse Path Forwarding (RPF) дійсно є важливим моментом для боротьби зі спуфінгом IP-адрес. RPF перевіряє, чи існує шлях до мережі, яка відповідає IP-адресі джерела, в таблиці маршрутизації і чи

відповідний інтерфейс отримав пакет. Якщо згідно з маршрутизуючою інформацією мережа джерела знаходиться за іншим інтерфейсом, пакет буде відкинуто.

Однак, хоча RPF може використовувати таблиці маршрутизації для перевірки, це може бути довгим процесом, оскільки вимагає врахування багатьох шляхів. Тому для поліпшення продуктивності може бути використана спеціальна база даних, створена за допомогою технології Cisco Express Forwarding (CEF). CEF забезпечує ефективну маршрутизацію, швидкий доступ до інформації про шляхи та використання кешу для прискорення перевірки RPF.

Таким чином, використання спеціальної бази даних, створеної технологією CEF, може покращити продуктивність і швидкість перевірки RPF, забезпечуючи ефективний захист від спуфінгу IP-адрес.

2 ОХОРОНА ПРАЦІ

Охорона праці на виробництві завжди була дуже важлива, отже саме завдяки рекомендаціям з охорони праці, персонал, який працює на підприємстві створює алгоритм виконання робочих завдань з чітким дотриманням рекомендацій. Основне завдання охорони праці – це створення та проведення заходів, спрямованих на захист життя, працездатності та здоров'я людини у процесі трудової діяльності.

При роботі з комп'ютером, як і в багатьох інших галузях, повинні враховуватись нормативи освітлення, температура, відносна вологість і сили вібрації. Але при роботі у приміщенні з комп'ютером найважливішим є дотримання правил пожежної безпеки, це вогнестійкість приміщення, також рівень звукового шуму, характеристики електромагнітних, ультрафіолетових та інфрачервоних полів.

Для аналізу охорони праці у дипломному проєкті досліджується безпека праці розробника веб-сторінок у офісному приміщені.

1.1 Аналіз та безпека умов праці працівника на робочому місці

Під час будь-якого виду роботи за комп'ютером, на працівника можуть мати дію небезпечні фактори виробничого середовища, а саме: фізичні та психофізіологічні небезпечні й шкідливі виробничі фактори.

Серед фізичних небезпечних факторів, найпоширеніші це підвищена температура повітря робочої зони, підвищений рівень шуму, знижена вологість повітря – це звичайні фактори, які виникають при роботі у приміщеннях з комп'ютерами, через їх роботу на робочому місті підіймається температура та знижається вологість повітря. Окрім цього, комп'ютер випромінює електростатичні та електромагнітні поля у діапазоні від 5 Гц до 2 кГц та від 2 до 400 кГц, тож робота за комп'ютером включає ще підвищений рівень електромагнітний випромінювання та підвищений рівень статичної електрики.

У офісних приміщеннях не завжди є достатня кількість природного освітлення у такому разі присутня велика кількість штучного освітлення, яке у свою чергу не завжди правильно налаштоване, з цього виникає, що світло може бути недостатньо яскравим або дуже яскравим.

Психофізіологічні виробничі небезпечні фактори поділяються на фізичні перевантаження та нервово-психічні перевантаження, при роботі з комп'ютером найчастіше друге. У нервово-психічних перевантаженнях програміст зазнає перенапругу аналізаторів та монотонність праці, інколи, ще й розмовну перенапругу, коли розробнику потрібно складати технічне завдання разом з клієнтом.

1.2 Розробка заходів з охорони праці

Виробниче освітлення

Штучне освітлення в приміщеннях з робочими місцями, обладнаними ВДТ має здійснюватися системою загального рівномірного освітлення. У виробничих та адміністративно-громадських приміщеннях, у разі переважної роботи з документами, допускається застосування системи комбінованого освітлення (крім системи загального освітлення, додатково встановлюються світильники місцевого освітлення).

Мікроклімат

При роботі у приміщеннях з великою кількістю комп'ютерів, приміщення з якими класифікуються як приміщення з підвищеною небезпекою електротравм, температура повітря влітку може становити більше 35 С, що погано впливає на здоров'я людини, тож у таких приміщеннях повітря повинне охолоджуватись та понижена вологість повітря повинна регулюватись спеціальним обладнанням.

Відповідно до норм ДСН 3.3.6.042-99 температура повітря в офісі повинна становити 22-25 С, вологість повітря 40-60%, швидкість руху повітря

не більше 0,1 м/с. Якщо ці норми перевищені, робочій день працівника повинен бути скорочений на 10%.

2.3 Організація робочого місця користувача ПК

Конструкція робочого місця користувача ПК й взаємне розташування всіх його елементів (сидіння, органи керування, засобу відображення інформації) відповідають антропометричним, фізіологічним і психологічним вимогам, а також характеру роботи. Конструкція робочих меблів повинна забезпечувати можливість індивідуального регулювання відповідно росту працюючих для підтримки зручної пози. Робочий стіл повинен бути пофарбований матовою фарбою. Дисплей розташований так, що його верхній край перебуває на рівні очей на відстані близько 70 см, що укладається в у припустимі рамки від 60 до 90 см. Частота мерехтіння екрана fмер=100 Гц, що відповідає умові fмер>70 Гц.

Робоче місце розташоване перпендикулярно віконним прорізам, це зроблено з тією метою, щоб виключити пряму й відбиту мерехтливість екрана від вікон і приладів штучного освітлення.

Згідно темі дипломного проекту робоче місце програміста укомплектовано пристроями з електромагнітним випромінюванням.

2.4 Пожежна безпека

Забезпечення пожежної безпеки на об’єкті праці є важливою частиною роботи по створенню безпечних та здорових умов праці.

Прохід до аварійних виходів повинен бути вільний, шириною не менше 1 метру, у разі великої кількості горючих відходів потрібно використовувати відведені сміттєзбірники. Електроприлади повинні використовуватися тільки для їхнього прямого призначення, а у разі пошкодження приладів, слід вимкнути їх живлення та привести до пожежобезпечного стану.

Первинні засоби пожежогасіння застосовуються для боротьби з пожежами на початковій стадії. До них належать: пожежні кран-комплекти,

вогнегасники, пожежний інвентар (резервуари з водою, ящики з піском, пожежні відра, лопати), а також різний переносний пожежний інструмент (кирки, сокири, багри, ломи і т. ін.).

Для гасіння пожеж промисловість випускає різні вогнегасники. Найбільшого поширення набули водопінні, водяні, газові (вуглекислотні) і порошкові. За ефективністю пожежогасіння гасіння, економічністю та іншими показниками більш перспективними вважаються порошкові вогнегасники.

Первинні засоби пожежогасіння розміщують на пожежних щитах, які встановлюють на виробничій території з розрахунку один щит на 5000 м2. Вони фарбуються у червоний колір.

Згідно Правил, на кожному поверсі будинку адміністративного призначення повинно знаходитися не менше двох вогнегасників з масою заряду вогнегасної речовини 5 кг і більше. Експлуатація вогнегасників без призначення відповідального за організацію цієї роботи не допускається.

Забороняється палити на підприємстві, крім спеціально виведених для цього місцях, забороняється зберігати легкозаймисті матеріали, такі як папір ближче ніж 1 метр від електрощитів, 0,15 м від приладів центрального водяного опалення та 0,6 м від сповіщувачів автоматичної пожежної сигналізації, також документація повинна зберігатися у спеціально відведених для цього шафах.

Для запобігання розповсюдження пожежі встановлюють протипожежні системи, які складаються з датчиків, звукових сповіщувачів, аварійних кнопок, приймально-контрольної панелі, яка виступає як аналізатор інформації, яку отримали датчики і відправляє ці данні на пульт пожежної охорони. Протипожежна сигналізація призначення для виявлення пожежі на початковому етапі.

Підприємство крім установки пожежної сигналізації на своєму об'єкті, має укласти договір на обслуговування даної системи з фірмою, що має на це ліцензію. В обслуговування входить проведення встановлених нормами регламентних робіт, а так само усунення несправностей в роботі системи.

Періодичність перевірки узгоджується з замовником, але повинна бути не рідше ніж один раз на місяць.

У разі, якщо пожежі не вдалось уникнути, необхідно:

1. терміново повідомити пожежну охорону по телефону 101, вказати при цьому адресу, кількість поверхів, місце виникнення пожежі, наявність людей, своє прізвище;
2. організувати евакуацію людей та матеріальних цінностей;
3. повідомити про виникнення пожежі адміністрацію та чергового (за його наявності);
4. вимкнути, у разі необхідності, струмоприймачі та вентиляцію;
5. розпочати гасіння пожежі наявними первинними засобами пожежогасіння;
6. організувати зустріч підрозділів пожежної охорони й надати їм консультаційну та іншу допомогу в процесі гасіння пожежі.

ВИСНОВКИ

В ході виконання кваліфікаційній роботи було здійснено глибокий аналіз існуючих підходів до забезпечення безпеки корпоративних мультисервісних мереж. Було розглянуто ряд передових технологій у цій галузі. Проведено тестування на обладнанні від фірм DLink та Cisco засобу атаки - агресивного генератора пакетів. Це важливий етап для перевірки стійкості мережі до потенційних атак.

Забезпечення безпеки мережі - це постійний процес, і рекомендується періодично оцінювати і оновлювати заходи безпеки з урахуванням змінених вимог та нових загроз. Також важливо відстежувати вразливості та патчі для обладнання та програмного забезпечення, щоб забезпечити найвищий рівень безпеки вашої мережі.

Під час реалізації КРБ були перевірені всі три механізми. Початково було використано окремий сервер ACS, розташований у мережі управління, як основний спосіб. Також, як альтернатива, одна з трьох точок доступу була налаштована як ACS для функцій AAA для користувачів мережі гарячого доступу - бездротового радіо доступу для відвідувачів з ноутбуками.

Проте ці варіанти було відкинуто з метою зменшення адміністративних зусиль при підключенні нових користувачів та забезпечення зручності користування мережею і простоти підключення.

В результаті були створені локальні бази даних для аутентифікації доступу до керування. Для аутентифікації підключення користувачів (чи то проводової мережі до комутатора, чи через бездротовий доступ до точок прийому), було використано протокол портової автентифікації.

У лабораторній конфігурації було проведено налаштування комутатора згідно вимог протоколу. Принцип протоколу полягає в тому, що комутатор блокує будь-які кадри, від користувача, який щойно підключився, до моменту успішної завершення автентифікації. Також передбачається можливість повторної аутентифікації та відстеження періоду мовчання хоста.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. SP: Cisco Certified Security Professional Certification All-in-One Exam Guide, Robert E. Larson, Lance Cockcroft, Osborn/McGraw-Hill, 2013
2. CCDP: Cisco Internetwork Design Study Guide, unknown author.
3. Routing TCP/IP (CCIE Professional Development, a detailed examination of interior routing protocols), Jeff Doyle, Cisco Press, 1998
4. Рішення компанії Cisco Systems по забеспеченню безпеки корпоративних мереж, М. Кадер, Cisco Press, 2004
5. Рішення Cisco для забеспечення інформаціоної безпеки, укладач А. Лукацкий, Cisco Press, 2015
6. 6. CCNP BCMSN Exam Certification Guide, David Hucaby (Building Cisco Multilayer Switching Networks), Osborne/McGraw-Hill, 2000
7. .«Адміністрування інформаційно-обчислювальних мереж», Н. Т. Кустов, навчальний посібник, Суми 2019
8. . Побудова виртуальних частних мереж (VPN) на базі технології MPLS, укладач М. Захватов, Cisco Press, 2004
9. . «Настройка маршрутизаторів», електроний ресурс, Белицкий Д. Ю.
10. “SAFE Layer 2 Security In-Depth”, Ido Dubrawsky, 2004, электронный ресурс на www.cisco.com.
11. “Побудова і аналіз мультисервисних мереж передачі даних, голоса і відео”, Кравченко А.В., електронний ресурс.

Додаток А. Слайди мультимедійної презентації

Слайд 1

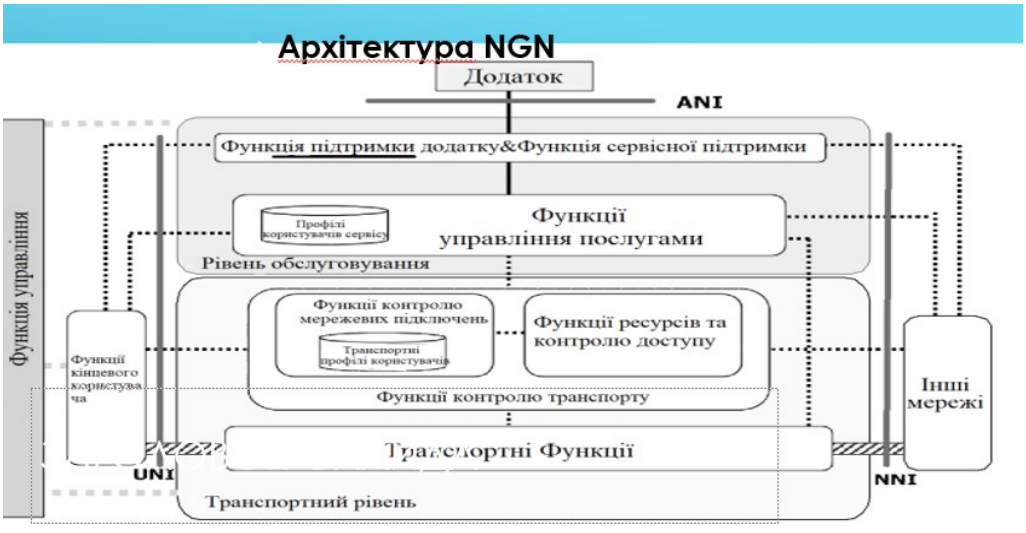
ПРОЕКТУВАННЯ ІФОРМАЦІЙНОЇ БЕЗПЕКИ В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ

Виконав: здобувач коледжу групи БКС-27
Воробей В.Є.
Керівник: к.т.н. Кунуп Т.В.

Слайд 2

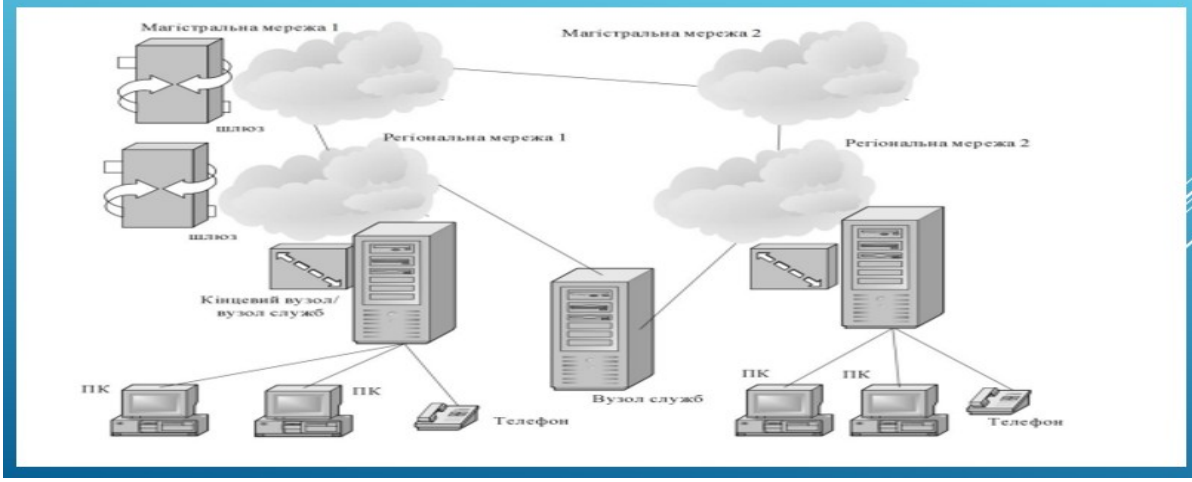
- Мультисервісні мережі є самостійним класом мереж, що базуються на концепції NGN. Вони надають широкий спектр послуг, включаючи як традиційні, так і нові послуги. Регламентація мультисервісних мереж здійснюється на основі нормативно-технічної бази, яка враховує особливості інтеграції різних послуг і системно-технічних рішень в рамках однієї мережі.
- Мультисервісні мережі забезпечують доставку різних послуг на єдиній технологічній основі, використовуючи принцип конвергенції послуг. Пакетні мережі, зокрема ті, що використовують транспорт MPLS-TP, ефективно передають голос, відео та ін

Слайд 3



Слайд 4

Дворівнева архітектура мультисервісної мережі



Слайд 5

Концепції мережі наступного покоління NGN

ІДНОСИТЬСЯ ДО АРХІТЕКТУРИ МЕРЕЖ, ЯКА СПРЯМОВАНА НА ЗАБЕЗПЕЧЕННЯ ПЕРЕДАЧІ ОЛОСУ, ДАНИХ ТА ІНШИХ ПОСЛУГ ЗА ДОПОМОГОЮ ІНТЕГРОВАНОЇ IP-МЕРЕЖІ. NGN Є ВОЛЮЦІЙНИМ КРОКОМ У РОЗВИТКУ МЕРЕЖІ З МЕТОЮ ПОКРАЩЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ, НИЖЕННЯ ВАРТОСТІ ТА НАДАННЯ НОВИХ ОСЛУГ.КОНЦЕПЦІЯ МЕРЕЖІ НАСТУПНОГО ОКОЛІННЯ

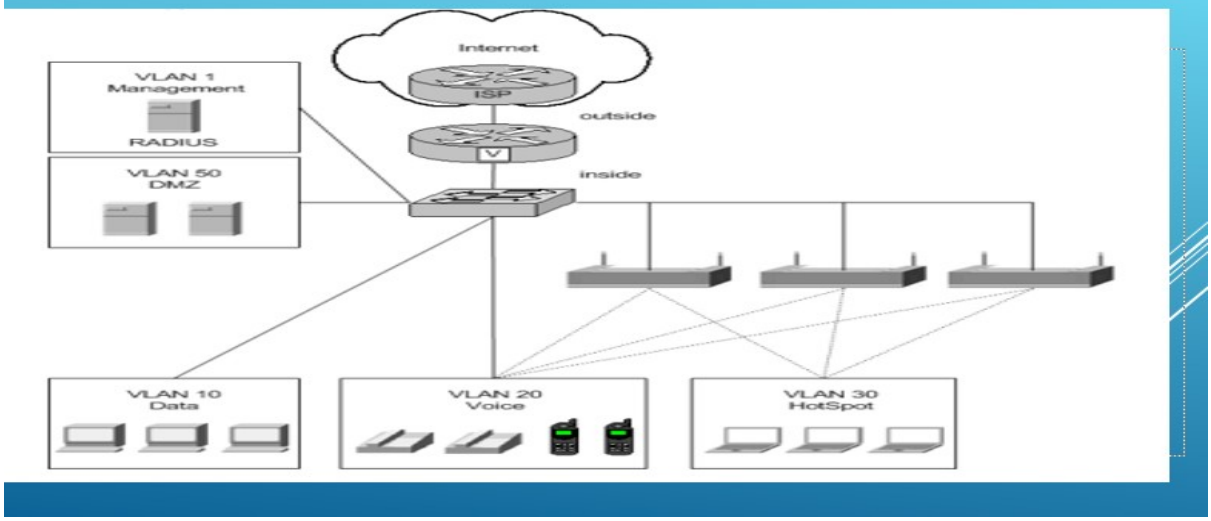
Слайд 6

▸Основні аспекти проектування інформаційної безпеки в мультисервісних мережах

1. АУТЕНТИФІКАЦІЯ ТА АВТОРИЗАЦІЯ
2. ШИФРУВАННЯ:
3. ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ
4. ЗАХИСТ МЕРЕЖЕВИХ ПРИСТРОЇВ
5. РЕЗЕРВНЕ КОПІЮВАННЯ ТА ВІДНОВЛЕННЯ
6. НАВЧАННЯ ТА СВІДОМІСТЬ КОРИСТУВАЧІВ

Слайд 7

▸Схема проектуємої мережі

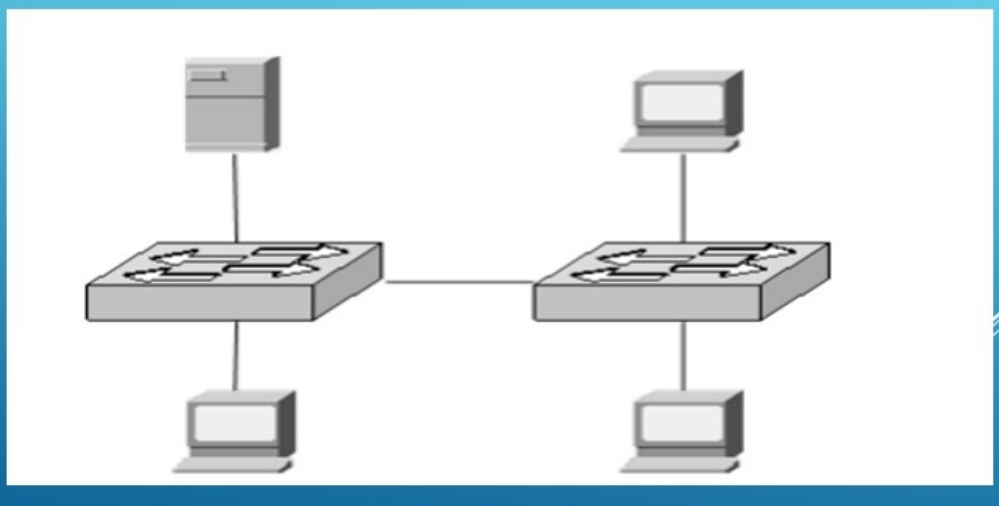


Слайд 8

ЗАБОРОНИТИ ВСІМ ВХІДНИМ ПАКЕТАМ З ІНШИХ МЕ
ПРОНИКАТИ ДО МЕРЕЖІ УПРАВЛІННЯ:
ВИХІДНЕ IP-АДРЕСУВАННЯ: <IP-АДРЕСИ_ІНШИХ_МЕР
ПОРТ НАЗНАЧЕННЯ:
<ПОРТИ_ПРОТОКОЛІВ_ІНШИХ_МЕРЕЖ>
ДІЯ: ЗАБОРОНИТИ
ЗАБОРОНИТИ ВИХІДНИМ ПАКЕТАМ З МЕРЕЖІ
УПРАВЛІННЯ ВИХОДИТИ ДО ІНШИХ МЕРЕЖ:
ВИХІДНЕ IP-АДРЕСУВАННЯ: <IP-
АДРЕСИ_МЕРЕЖ_УПРАВЛІННЯ>
ПОРТ ПРИЗНАЧЕННЯ:
<ПОРТИ_ПРОТОКОЛІВ_ІНШИХ_МЕРЕЖ>
ДІЯ: ЗАБОРОНИТИ

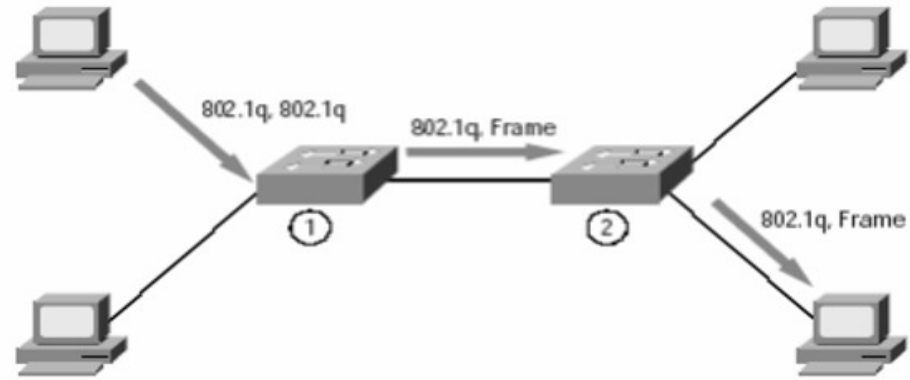
Слайд 9

Встановлення посередництва у комутованому середовищ



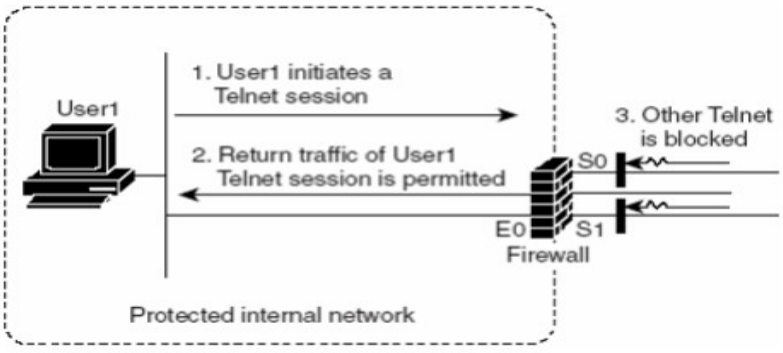
Слайд 10

Атака через двойну інкапсуляцію



Слайд 11

CBAC – відкриття тимчасових зворотних дірок



Слайд 12

ДЯКУЮ ЗА УВАГУ

UNICHECK
by Turnitin

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015632519

Дата перевірки:
17.06.2023 13:25:54 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
17.06.2023 13:27:07 EEST

ID користувача:
100011688

Назва документа: 2БКС-27 Воробей В.Є

Кількість сторінок: 71 Кількість слів: 15231 Кількість символів: 114237 Розмір файлу: 747.00 KB ID файлу: 1015279056

13.5%
Схожість

Найбільша схожість: 7.81% з Інтернет-джерелом (https://vdocuments.site/diplom-570e87549e498.html)

13.5% Джерела з Інтернету | 955 ..... Сторінка 73

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 6

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНГО ДИПЛОМНОГО ПРОЕКТА
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Воробей Віктор Євгенович,
здобувач освіти гр. 2БКС-27, та

Кунуп Тетяна Василівна,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускного дипломного проекту молодшого спеціаліста на тему:

«Проектування та реалізація інформаційної безпеки в мультисервісній мережі» (автор роботи – Воробей В.Є., керівник роботи – Кунуп Т.В.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2023 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Воробей В.Є. /

Керівник _____ / Кунуп Т.В. /

«15» 06 2023 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на кваліфікаційну роботу бакалавра
відділення комп'ютерних систем

Воробєя Віктора Євгеньевича

(прізвище, ім`я та по батькові)

Напрямку підготовки *123 «Комп'ютерна інженерія»*

Керівник кваліфікаційної роботи ***Кунуп Т.В.***

(прізвище, ім`я та по батькові)

Тема кваліфікаційної роботи ***«Проектування інформаційної безпеки в мультисервісних мережі»***

Обсяг пояснювальної записки 53 сторінок

Обсяг графічної (презентаційної) частини проекту 14 аркушів (слайдів)

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) заключення про ступінь відповідності виконаної роботи завданню

Представлена на рецензію випускна кваліфікаційна робота відповідає затвердженій темі та виконаний відповідно до технічного завдання. Випускна робота має актуальну тематику щодо аналізу та практичної реалізації інформаційної безпеки в мультисервісних мережах.

б) характеристика виконання кожного розділу роботи

Пояснювальна записка складається з технологічного розділу, розділу охорони праці та додатку. Технологічний розділ пояснювальної записки містить підрозділи, що поетапно охоплюють аналітичну частину, реалізацію суті роботи, дослідження ефективності прийнятих рішень. Розділ охорони праці містить загальну інформацію та вимоги до техніки безпеки оператора ЕОТ

в) оцінка якості виконання графічної (презентаційної) частини роботи і пояснювальної записки

Графічна частина складається з 12 слайдів мультимедійної презентації, виконаної у програмному продукті MS PowerPoint, які містять креслення та ілюстративні схеми, малюнкиі, передбачені технічним завданням. Пояснювальна записка виконана акуратно та у відповідності до норм оформлення документів. Якість виконання графічної частини роботи та пояснювальної записки висока, розробку виконано у повному обсязі

г) перелік позитивних якостей роботи

Проаналізовано саме актуальні методи забезпечення інформаційної безпеки та практично реалізовано;

У роботі виконано практичну реалізацію інформаційної безпеки в мультисервісних мережах

Розроблені рекомендації щодо її подальшої модернізації.

д) основні недоліки роботи

З тексту пояснювальної записки не дуже зрозуміло, які саме методи інформаційної безпеки рекомендовано;

У розділі охорони праці наведені відомі нормативні вимоги загального плану замість конкретних розрахунків освітлення приміщення, вентиляції, рівня шуму.

Оцінка розрахункової частини Відмінно

Оцінка графічної (презентаційної) частини Відмінно

Загальна оцінка Відмінно

Прізвище, ім'я та по батькові рецензента Василіу Євген Вікторович

Місце роботи і посада рецензента Державний університет інтелектуальних технологій і зв'язку, д.т.н., проф. кафедри КБ та ТЗІ, декан факультету інформаційних технологій та кібербезпеки

« 16 » червня 2023 р.

(підпис)

ПІДПИС ПОСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ КАДРІВ ДУІТЗ

ВІДДІЛ КАДРІВ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на кваліфікаційну роботу бакалавра здобувача (здобувачки) освіти відділення комп'ютерних систем

Воробея Віктора Євгеньєвича

(прізвище, ім`я та по батькові)

Спеціальність: 123 «Комп'ютерна інженерія»"

Освітня програма: «Комп'ютерна інженерія»

Тема дипломного проекту: Проектування та реалізація інформаційної безпеки в мультісервісній мережі

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки)

Кваліфікаційна робота виконано відповідно технічному завданню. Пояснювальна записка містить 51 сторінку. У пояснювальній записці виконано опис етапів розробки структури програми. Графічна частина складається з 12 слайдів мультимедійної презентації, які також містять креслення, передбачені технічним завданням. Якість виконання пояснювальної записки та графічної частини добра, розробку виконано в повному обсязі.

б) самостійність роботи над проектом:

Протягом всього строку роботи над кваліфікаційною роботою та переддипломної практики здобувач освіти Воробей В.Є. поступово та послідовно виконував всі етапи розробки. Всі роботи здобувач освіти виконував самостійно, з оглядом на рекомендації керівника

в) теоретична підготовка випускника (випускниці):

Здобувач освіти Воробей В.Є. під час роботи над кваліфікаційною роботою вивчив достатню кількість літературних джерел та матеріалів за даною тематикою. Вважаю, що теоретична підготовка здобувача добра і він готовий до захисту кваліфікаційної роботи

г) вміння розв'язувати виробничі та конструкторські питання

Під час роботи над кваліфікаційною роботою здобувач освіти Воробей В.Є. мав змогу самостійно приймати окремі рішення з реалізації інформаційної безпеки в мультисервісній мережі працювати над поставленим завданням, спроектував інформаційну безпеку в мультисервісній мережі.

Оцінка розрахункової частини Добре

Оцінка графічної частини Добре

Загальна оцінка Добре

Прізвище, ім'я, по батькові керівника дипломного проекту

Кунуп Тетяна Василівна

Місце роботи і посада керівника дипломного проекту

ВСП "Одеський технічний фаховий коледж ОНТУ", викладач спецдисциплін комісії комп'ютерних технологій та програмної інженерії, голова циклової комісії КТ та ПІ

Підпис

«___» 06 2023 р.