

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

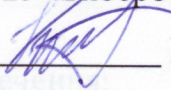
до випускної кваліфікаційної роботи магістра
на тему: «Методи та засоби захисту xPON-мережі
регіонального інтернет-провайдера»

затверджена Наказом університету від 6 жовтня 2025 р. №566/с

Термін здачі студентом закінченої роботи 25 грудня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
Об'єкт дослідження – мережа доступу регіонального інтернет-провайдера на
основі технологій xPON

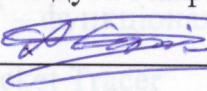
Виконав: студент 2-го курсу групи КБм-24-1
спеціальності 125 «Кібербезпека та захист інформації»

 Володимир КОРЖОВСЬКИЙ

Керівник: Старший викладач кафедри КІ та КБ

 Наталія ЩУР

Рецензент: Завідувач кафедри КІ та КБ, к.т.н., Доцент

 Андрій ЄФІМЕНКО

Житомир – 2025

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека»

Розділ	Консультант	Відомості про прийняв
1	Ольга ДЯЧУК	
2	Ольга ДЯЧУК	
3	Ольга ДЯЧУК	

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

Андрій Єфіменко

6 жовтня 2025 р.

Студент
Керівник

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Коржовський Володимир Васильович

Тема роботи: «Методи та засоби захисту xPON-мережі регіонального інтернет-провайдера»

затверджена Наказом університету від 6 жовтня 2025 р. №566/с

Термін здачі студентом закінченої роботи 25 грудня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єкт дослідження – мережа доступу регіонального інтернет-провайдера на основі технологій xPON.

Предмет дослідження – методи та засоби забезпечення інформаційної безпеки xPON-мережі доступу.

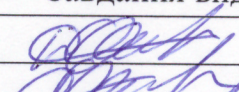
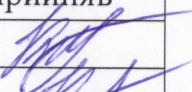
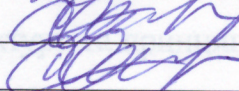
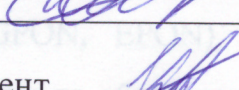
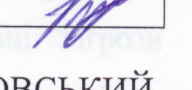
Обладнання та програмне забезпечення:

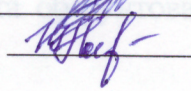
1. Маршрутизатор Cisco 2911 (аналог OLT)
2. Комутатори Cisco Catalyst 2960 (аналог вузлів доступу)
3. Абонентські вузли (ONU/ONT – функціональні аналоги)
4. Мережевий емулятор Cisco Packet Tracer

Студент
Керівник

Володимир КОРЖОВСЬКИЙ
Наталія ЦУР

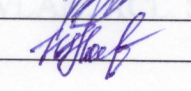
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Ольга.ДЯЧУК		6.10.25 
2	Ольга.ДЯЧУК		6.10.25 
3	Ольга.ДЯЧУК		6.10.25 

Студент  Володимир КОРЖОВСЬКИЙ
Керівник  Наталія ЩУР

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів проекту	Примітки
1	Аналіз отриманого завдання та уточнення поставлених завдань	3.05.2025	
2	Аналіз літературних джерел	5.11.2025	
3	Аналіз об'єкта дослідження	7.11.2025	
4	Постановка задачі дослідження	10.11.2025	
5	Розробка структурної моделі	14.11.2025	
6	Розрахунок параметрів адресації	17.11.2025	
7	Вибір технології для реалізації	19.11.2025	
8	Розробка структурної моделі xPON-мережі	22.11.2025	
9	Налаштування мережі	5.12.2025	
10	Налаштування та захист xPON-мережі доступу	11.12.2025	
11	Перевірка працездатності	13.12.2025	
12	Оформлення пояснювальної записки	14.12.2025	
13	Оформлення презентації	16.12.2025	
14	Захист кваліфікаційної роботи		

Студент  Володимир КОРЖОВСЬКИЙ
Керівник  Наталія ЩУР

АНОТАЦІЯ

Пояснювальна записка до випускної кваліфікаційної роботи бакалавра на тему «Методи та засоби захисту xPON-мережі регіонального інтернет-провайдера» складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

У роботі розглянуто архітектуру та принципи функціонування мереж доступу на основі технологій xPON (GPON, EPON), проаналізовано основні загрози інформаційній безпеці таких мереж та обґрунтовано вибір ефективних методів їх нейтралізації.

У першому розділі наведено теоретичні основи побудови xPON-мереж, розглянуто принципи роботи оптичних мереж доступу та сучасні підходи до забезпечення їх захисту.

У другому розділі виконано проєктування захищеної xPON-мережі регіонального інтернет-провайдера, визначено структуру мережі, методи сегментації трафіку та політики безпеки.

У третьому розділі здійснено практичну реалізацію та тестування розробленої моделі мережі з використанням програмного середовища Cisco Packet Tracer, включаючи налаштування VLAN, DHCP, списків контролю доступу та захищеного керування мережею.

У висновках наведено результати виконаної роботи та оцінено ефективність застосованих методів і засобів захисту xPON-мережі доступу.

У додатках представлено схеми мережі та конфігураційні файли мережевого обладнання.

КЛЮЧОВІ СЛОВА:

xPON, GPON, EPON, CISCO, OLT, ONU, МЕРЕЖА ДОСТУПУ, ІНФОРМАЦІЙНА БЕЗПЕКА, DHCP, VLAN, ACL, SSH.

ANNOTATION

The explanatory note to the bachelor's qualification work entitled "Methods and Means of Securing an xPON Network of a Regional Internet Provider" consists of an introduction, three chapters, conclusions, a list of references, and appendices.

The paper considers the architecture and principles of operation of access networks based on xPON technologies (GPON, EPON), analyzes the main information security threats inherent in such networks, and substantiates effective methods for their mitigation.

The first chapter presents the theoretical foundations of xPON network construction and modern approaches to ensuring their security.

The second chapter focuses on the design of a secure xPON access network for a regional Internet provider, including network structure development and traffic segmentation mechanisms.

The third chapter describes the practical implementation and testing of the designed network model using the Cisco Packet Tracer simulation environment, including the configuration of VLANs, DHCP, access control lists, and secure network management.

The conclusions summarize the results obtained and assess the effectiveness of the proposed security methods.

The appendices contain network topology diagrams and configuration files of the network equipment.

KEYWORDS:

XPON, GPON, EPON, CISCO, OLT, ONU, ACCESS NETWORK, INFORMATION SECURITY, DHCP, VLAN, ACL, SSH.

ЗМІСТ

ВСТУП	7
РОЗДІЛ 1 ТЕХНОЛОГІЇ xPON ТА ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ МЕРЕЖ ДОСТУПУ	8
1.1 Технології PON, GPON, XPON, EPON	8
1.1.2 Види PON та їх особливості.....	9
1.2. Загрози та методи захисту в мережах xPON	16
1.2.1 Аналіз основних загроз безпеці xPON-мереж	16
1.2.2 Несанкціонований доступ до мережі	16
1.2.3 Перехоплення трафіку в пасивних оптичних мережах	17
1.2.4 Атаки типу DoS та DDoS.....	17
1.2.5 Вразливості протоколів і систем керування.....	18
1.2.6 Фізичні загрози елементам мережі	18
1.2.7 Узагальнювальна таблиця загроз і методів захисту	19
ВИСНОВКИ ДО РОЗДІЛУ 1	20
РОЗДІЛ 2. МЕТОДИ ЗАХИСТУ	21
2.1 Криптографічні методи захисту.....	21
2.2 Автентифікація та контроль доступу	23
2.3 Сегментація та ізоляція трафіку	25
2.4 Моніторинг та виявлення аномалій	27
2.5 Фізичний захист елементів мережі.....	29
2.6 Засоби захисту на різних рівнях мережі	33
ВИСНОВКИ ДО РОЗДІЛУ 2	35
РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДІВ ЗАХИСТУ МЕРЕЖІ ДОСТУПУ В CISCO PACKET TRACER	36
3.1 Мета та завдання практичної реалізації.....	36
3.2 Опис топології та план адресації	36
3.3 Реалізація сегментації трафіку за допомогою VLAN.....	37
3.4 Міжвланова маршрутизація.....	38
3.5 Налаштування динамічної адресації DHCP	39
3.6 Контроль доступу та ізоляція абонентів (ACL)	40
3.7 Захищене керування мережею (SSH, MGMT VLAN)	40
3.8 Тестування та аналіз результатів.....	41
ВИСНОВКИ ДО РОЗДІЛУ 3	48
ВИСНОВОК	49
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	51
ДОДАТКИ	52

ВСТУП

Актуальність теми виникає у необхідності забезпечення надійного захисту xPON-мереж регіональних інтернет-провайдерів, що є основою сучасної телекомунікаційної інфраструктури. Розвиток мережевих технологій, зокрема GPON, EPON та XPON, вимагає постійного вдосконалення методів захисту для запобігання несанкціонованому доступу, перехопленню даних та іншим загрозам.

Мета роботи полягає у дослідженні та розробці комплексу методів і засобів захисту xPON-мереж регіонального інтернет-провайдера з метою підвищення рівня інформаційної безпеки, забезпечення конфіденційності, цілісності та доступності даних, а також запобігання несанкціонованому доступу й іншим актуальним загрозам у процесі експлуатації мереж GPON, EPON та XPON.

Об'єктом дослідження є процеси проектування, налаштування та тестування захищених xPON-мереж регіонального інтернет-провайдера.

Предметом дослідження є методи, засоби та технології захисту інформації в xPON-мережах, зокрема використання криптографічних протоколів та механізмів контролю доступу.

Методом дослідження є розробка ефективних методів та засобів захисту xPON-мережі регіонального інтернет-провайдера.

Завдання дослідження:

1. Аналіз сучасних загроз для xPON-мереж.
2. Вивчення криптографічних та організаційних методів захисту.
3. Розробка рекомендацій щодо впровадження захисних механізмів.
4. Тестування ефективності запропонованих рішень.

Практичне значення роботи відбувається у можливості впровадження розроблених методів захисту для підвищення безпеки та надійності мережевих регіональних провайдерів.

РОЗДІЛ 1 ТЕХНОЛОГІЇ xPON ТА ЗАГРОЗИ ІНФОРМАЦІЙНИЙ БЕЗПЕЦІ МЕРЕЖ ДОСТУПУ

1.1 Технології PON, GPON, XPON, EPON

У сучасному світі високошвидкісний доступ до Інтернету є критичним для бізнесу, навчання, розваг та зв'язку. Однією з найсучасніших та найефективніших технологій для забезпечення цього доступу є пасивні оптичні мережі (PON). У цій статті ми розглянемо, що такі PON, GPON, XPON, EPON, як вони працюють, їх історію, різновиди, які найпоширеніші в Україні, необхідне обладнання, переваги цієї технології, зокрема в умовах відключення електроживлення, та порівнюємо використання маршрутизатора з підтримкою оптики з традиційним маршрутизатором разом з медіаконвертором.

Історія розвитку PON

Пасивні оптичні мережі (PON) почали розроблятися в 1990-х роках як рішення для підвищення ефективності та зниження витрат на широкосмуговий доступ. Ідея полягала в тому, щоб використовувати оптичні волокна для передачі даних від оператора центрального офісу до кінцевого користувача без активних компонентів між ними. Це дозволило знизити витрати на обслуговування та підвищити надійність мережі.

У 2000 році Міжнародний союз електрозв'язку (ITU) стандартизував перший варіант PON — BPON (Broadband PON), який забезпечив швидкість передачі даних до 622 Мбіт/с. З розвитком технологій з'явилися нові досконалі версії, такі як GPON (Gigabit PON), EPON (Ethernet PON) та інші.

1.1.2 Види PON та їх особливості



Рисунок 1.1.1 B-PON (широкопasmовий PON)

B-PON була першою стандартизованою технологією PON і забезпечувала швидкість передачі даних до 622 Мбіт/с на користувача. Вона використовувала ATM (Asynchronous Transfer Mode) для мультиплексування даних, що дозволяло передавати різні типи трафіку (дані, голос, відео).



Рисунок 1.1.2 G-PON (гігабітний PON)

G-PON став наступним кроком у розвитку PON і був стандартизований ITU в 2003 році (G.984). Вона значно підвищила швидкість передачі даних — до 2,5 Гбіт/с на користувача. G-PON використовує технології TDM (Time Division Multiplexing) і WDM (Wavelength Division Multiplexing) для більш ефективного використання пропускної здатності.



Рисунок 1.1.3 EPON (Ethernet PON)

EPON, стандартизований IEEE в 2004 році, використовує Ethernet для передачі даних і забезпечує швидкість до 1 Гбіт/с на користувача. EPON є популярною технологією в багатьох країнах за допомогою простої інтеграції з існуючими Ethernet-мережами.



Рисунок 1.1.4 XG-PON та XGS-PON

XG-PON (10G-PON) і XGS-PON (10G Symmetric PON) — це вдосконалені версії GPON, які забезпечують швидкість до 10 Гбіт/с на користувача. XG-PON дозволяє асиметричну передачу даних (10 Гбіт/с вниз, 2,5 Гбіт/с зверху), тоді як XGS-PON забезпечує симетричну швидкість передачі даних (10 Гбіт/с в обидві сторони).

NG-PON2 (PON 2 наступного покоління)

NG-PON2 — це найсучасніша версія PON, яка підтримує швидкість до 40 Гбіт/с за допомогою використання технології TWDM (Time and Wavelength

Division Multiplexing). NG-PON2 забезпечує високу гнучкість і надійність за рахунок можливості використання кількох хвильових довжин для передачі даних.

Механіка роботи PON

PON задає оптичне волокно для передачі даних від оператора центрального офісу до кінцевого користувача. Основна особливість PON полягає в тому, що між цими точками немає активних компонентів, які потребують електроживлення. Знижує витрати на обслуговування та надійність мережі.

Основні компоненти PON

1. OLT (Optical Line Terminal) — Оптичний лінійний термінал

Розташування: Центральний офіс провайдера (CO — Central Office).

Функції:

- Керує всією мережею PON, включаючи ініціалізацію, автентифікацію та управління абонентами.
- Перетворює вхідні електричні сигнали з мережі провайдера в оптичні сигнали для передачі по волокну.
- Виконує мультиплексування трафіку: об'єднує дані для кількох абонентів в один потік (в напрямку downstream) і розділяє зворотний трафік (upstream).
- Забезпечує управління смугою пропускання (Dynamic Bandwidth Allocation, DBA) для ефективного розподілу ресурсів між абонентами.

Кількість портів: Зазвичай має кілька PON-портів, кожен з яких обслуговує до 64 або 128 абонентів через розгалужувачі.

2. ONT/ONU (Optical Network Terminal / Unit) — Абонентський термінал

Розташування: У приміщенні абонента (ONT) або поблизу (ONU).

Функції:

- Приймає оптичний сигнал від OLT через розгалужувач і перетворює його в електричний для підключення до локальної мережі (LAN), Wi-Fi-роутера, IPTV, VoIP тощо.

- У зворотному напрямку перетворює електричні сигнали в оптичні для передачі до OLT.

- Може мати кілька портів: Ethernet, POTS (телефонія), RF (телебачення).

Різниця між ONT і ONU:

- ONT — термінал, встановлений безпосередньо в будинку користувача.

- ONU — може бути встановлений на відстані від користувача, наприклад, у підвалі або на стовпі, і підключений до користувача через Ethernet або інші технології.

3. Пасивні оптичні розгалужувачі (splitters)

Тип: Повністю пасивні пристрої, які не потребують електроживлення.

Функції:

- Розділяють оптичний сигнал від одного волокна на кілька напрямків (наприклад, 1:8, 1:16, 1:32, 1:64).

- Працюють в обох напрямках: downstream (від OLT до ONT) і upstream (від ONT до OLT).

Переваги:

- Зменшення кількості активного обладнання в полі.

- Зниження витрат на обслуговування та енергоспоживання.

Розміщення: У вуличних шафах, колодязях, на стовпах або в будівлях.

Ці три компоненти формують архітектуру PON, яка забезпечує високошвидкісний, надійний і масштабований доступ до Інтернету без потреби в активних елементах між провайдером і користувачем.

Обладнання для впровадження PON

Для впровадження PON в житлових будинках або офісах використовує таке обладнання:

1. OLT: Встановлюється на центральних вузлах зв'язку провайдера. деякі це багатопортові пристрої, які можуть обслуговувати всіх абонентів.



Рисунок 1.1.4 OLT (Optical Line Terminal)

2. ONT/ONU: Встановлюються у кінцевих користувачів. Вони можуть мати різну кількість портів для підключення комп'ютерів, телефонів та інших пристроїв.



Рисунок 1.1.5 ONU (Optical Network Unit)

3. Оптичні розгалужувачі: Встановлюються у під'їздах багатоквартирних будинків або всередині офісних будівель для розподілу сигналу.



Рисунок 1.1.6 Пасивний розгалужувач

Переваги PON в умовах відключення електроживлення:

Однією з найбільших переваг PON є його здатність працювати в умовах відключення електроживлення. Завдяки вільним активним компонентам між центральним офісом оператора та кінцевим користувачем, мережа залишається працездатною навіть при будь-якій електроенергії. Це особливо важливо в Україні, де відключення електроживлення може бути частиною явищем.

1. Надійність: Відсутність активних компонентів знижує ризик виникнення технічних проблем.

2. Економія енергії: Пасивні компоненти не потребують електроживлення, що знижує витрати на енергопостачання.

3. Підвищена безпека: Менша кількість активних компонентів зменшує ризик кібератаки.

Використання маршрутизатора з підтримкою оптики

При використанні технології PON, кінцеві користувачі можуть вибрати між двома варіантами підключення: маршрутизатор з підтримкою оптики або звичайний маршрутизатор разом з медіаконвертором.

Маршрутизатор з підтримкою оптики (наприклад, GPON-роутер) має вбудований оптичний модуль, який дозволяє підключити оптичне волокно разом до пристрою. Це має кілька переваг:

1. Простота установки: Наявність додаткових пристроїв (медіаконверторів) спрощує процес установки.

2. Менше місця: Один пристрій займає менше місць та виглядає більш точно.

3. Підвищена надійність: Менша кількість компонентів знижує ризик відмови.



Рисунок 1.1.5 Звичайний маршрутизатор з медіаконвертором

Звичайний маршрутизатор з медіаконвертором передбачає використання окремого пристрою для перетворення оптичного сигналу в електричний. це хоче також працювати, але має свої недоліки:

1. Складність установки: додатковий пристрій потребує окремого налаштування та підключення.

2. Більше місць: Два пристрої займають більше місць та виглядають менш акуратно.

3. Знижена надійність: Додатковий пристрій — це ще одна точка можливого відмови.

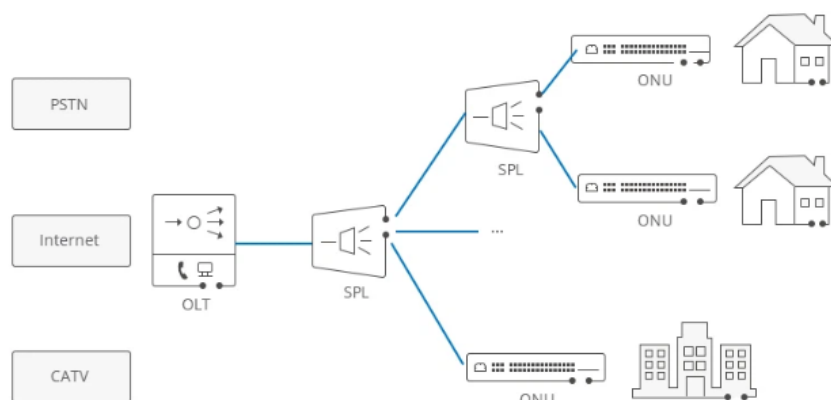


Рисунок 1.1.6 Типова топологія PON: OLT → сплітери → ONU → абоненти

Технології PON, GPON, XPON, EPON є критично важливими для забезпечення сучасного високошвидкісного доступу до Інтернету. Вони забезпечують високу швидкість, надійність та ефективність передачі даних, що робить їх ідеальними для використання в умовах відключення електроживлення. Вибір між маршрутизатором з підтримкою оптики та звичайним маршрутизатором з медіаконвертором залежить від конкретних умов та потреб користувача, але перший варіант має значні переваги в простоті встановлення та надійності.

Україна активно впроваджує ці технології, що сприяють розвитку інформаційної інфраструктури країни та забезпечують доступ до високоякісних інтернет-послуг для населення та бізнесу.

1.2. Загрози та методи захисту в мережах xPON

1.2.1 Аналіз основних загроз безпеці xPON-мереж

Мережі доступу на основі технологій xPON (GPON, EPON) широко застосовуються в сучасних телекомунікаційних системах завдяки високій пропускній здатності, масштабованості та економічній ефективності. Водночас особливості їх архітектури формують низку загроз інформаційній безпеці, що потребують системного аналізу та впровадження комплексних заходів захисту.

До основних загроз належать несанкціонований доступ до мережі, перехоплення трафіку, атаки типу DoS/DDoS, вразливості протоколів керування, а також фізичні загрози елементам інфраструктури.

1.2.2 Несанкціонований доступ до мережі

У процесі функціонування xPON-мереж кожен абонентський термінал (ONU/ONT) проходить процедуру автентифікації на стороні оптичного лінійного терміналу (OLT). Недостатній рівень контролю або помилки конфігурації можуть призвести до підключення сторонніх пристроїв із підробленими ідентифікаторами.

Наслідками несанкціонованого доступу є нецільове використання ресурсів мережі, створення внутрішніх векторів атак, порушення конфіденційності та цілісності інформації, а також фінансові втрати оператора.

Для зменшення ризиків застосовуються такі заходи:

- автентифікація ONU за серійним номером або MAC-адресою;
- використання інфраструктури відкритих ключів (PKI);
- застосування списків контролю доступу (ACL);
- централізований моніторинг підключених пристроїв.

1.2.3 Перехоплення трафіку в пасивних оптичних мережах

Архітектура PON передбачає спільне використання оптичного середовища, у якому сигнал від OLT передається через пасивні сплітери до кількох абонентів. За відсутності належного криптографічного захисту це створює потенційну можливість перехоплення інформації.

Наслідками таких загроз можуть бути витік конфіденційних даних, компрометація персональної або корпоративної інформації та прослуховування голосового трафіку.

Для захисту від перехоплення застосовуються:

- AES-шифрування, передбачене стандартами GPON;
- використання захищених протоколів IPSec і TLS;
- логічна сегментація трафіку;
- використання VPN-рішень у навчальних і тестових середовищах.

1.2.4 Атаки типу DoS та DDoS

Атаки типу DoS і DDoS спрямовані на перевантаження мережевих елементів або каналів зв'язку шляхом надсилання великої кількості запитів. У результаті легітимні користувачі не можуть отримати доступ до сервісів.

Наслідками таких атак є зниження продуктивності мережі, порушення доступності послуг, недотримання SLA та фінансові збитки.

Основними методами протидії є:

- застосування механізмів QoS;
- використання IDS/IPS-систем;

- обмеження швидкості передавання трафіку (rate limiting);
- фільтрація трафіку за допомогою ACL;
- постійний моніторинг мережевої активності.

1.2.5 Вразливості протоколів і систем керування

Використання застарілих або незахищених протоколів керування створює умови для реалізації атак типу man-in-the-middle та компрометації облікових даних.

Наслідками таких уразливостей можуть бути несанкціонований доступ до систем керування, зміна конфігурацій і порушення стабільності роботи мережі.

Для зниження ризиків необхідно:

- використовувати сучасні криптографічні алгоритми (AES-256, SHA-2);
- застосовувати захищені протоколи керування (SSH замість Telnet);
- регулярно оновлювати програмне забезпечення;
- здійснювати аудит конфігурацій;
- обмежувати доступ до керуючих інтерфейсів.

1.2.6 Фізичні загрози елементам мережі

Фізичний доступ до оптичних кабелів, муфт, сплітерів і телекомунікаційних шаф може призвести до пошкодження обладнання або підключення сторонніх пристроїв.

Основні фізичні загрози:

- Несанкціонований доступ до обладнання: Відкриті або слабо захищені телекомунікаційні шафи, муфти чи розгалужувачі можуть стати об'єктом втручання злоумисників.
- Пошкодження оптичного кабелю: Механічні пошкодження під час будівельних робіт, вандалізм або природні фактори (повені, зсуви, грози) можуть призвести до обриву або деградації сигналу.
- Підключення сторонніх пристроїв: У разі доступу до волокна можливе встановлення несанкціонованих пристроїв для перехоплення трафіку (наприклад, оптичних сплітерів або відгалужувачів).

– Крадіжка обладнання: Металеві частини шаф, кабелі або навіть активне обладнання можуть бути викрадені з метою наживи.

Наслідки:

- Переривання зв'язку для великої кількості абонентів.
 - Зниження надійності мережі через часті збої або деградацію сигналу.
 - Фінансові втрати на ремонт, заміну обладнання та компенсацію клієнтам.
 - Порушення конфіденційності у разі перехоплення трафіку.
- Для забезпечення фізичної безпеки застосовуються:
- контроль доступу до вузлів зв'язку;
 - використання антивандальних шаф і герметичних муфт;
 - впровадження систем відеоспостереження;
 - регулярний технічний огляд інфраструктури.

1.2.7 Узагальнювальна таблиця загроз і методів захисту

Таблиця 1.2.1 – Загрози, наслідки та методи захисту в xPON-мережах

Загроза	Наслідки	Методи захисту
Несанкціонований доступ	Незаконне використання ресурсів, витік даних	MAC/Serial-автентифікація, PKI, ACL, централізований контроль
Перехоплення трафіку	Компрометація інформації, прослуховування	AES (GPON), IPSec, TLS, VPN
DoS/DDoS-атаки	Відмова в обслуговуванні, деградація сервісів	QoS, IDS/IPS, rate limiting, ACL
Вразливості протоколів	MITM-атаки, компрометація керування	SSH, AES-256, SHA-2, оновлення ПЗ
Фізичні загрози	Пошкодження мережі, сторонні підключення	Контроль доступу, захисні шафи, відеоспостереження

ВИСНОВКИ ДО РОЗДІЛУ 1

Технології пасивних оптичних мереж PON, зокрема GPON, xPON та EPON, є ключовою основою сучасних систем широкосмугового доступу до мережі Інтернет. Вони забезпечують високу пропускну здатність, надійність і ефективність передавання даних, що робить їх придатними для використання як у побутовому, так і в корпоративному середовищі, зокрема в умовах нестабільного електроживлення. Вибір між маршрутизатором із вбудованою оптичною підтримкою та рішенням на основі медіаконвертора залежить від конкретних умов експлуатації, однак інтегровані оптичні маршрутизатори мають переваги з точки зору спрощення інсталяції, зменшення кількості вузлів та підвищення загальної надійності мережі.

Також було проаналізовано основні загрози інформаційній безпеці мереж доступу, побудованих на основі технологій xPON. Встановлено, що через особливості архітектури такі мережі можуть бути вразливими до несанкціонованого доступу, перехоплення трафіку, атак типу DoS/DDoS, експлуатації вразливостей протоколів керування та фізичних впливів на елементи інфраструктури. Забезпечення належного рівня безпеки можливе лише за умови комплексного підходу, який поєднує криптографічні, програмні, організаційні та фізичні засоби захисту.

Застосування сучасних алгоритмів шифрування, захищених протоколів керування, механізмів контролю доступу, систем моніторингу та виявлення атак дає змогу суттєво підвищити надійність, стійкість і безпечність функціонування xPON-мереж. У сукупності це забезпечує дотримання основних принципів інформаційної безпеки — конфіденційності, цілісності та доступності даних — і створює передумови для подальшого розвитку телекомунікаційної інфраструктури, зокрема в Україні.

РОЗДІЛ 2. МЕТОДИ ЗАХИСТУ

2.1 Криптографічні методи захисту

Типи шифрування у xPON (симетричні та асиметричні)

У xPON-мережах криптографічний захист є фундаментальним засобом забезпечення конфіденційності та цілісності даних. Основні типи шифрування:

- **Симетричне шифрування (AES):** Найбільш поширене у GPON/EPON. Один і той самий ключ використовується для шифрування і дешифрування даних між OLT та ONU. AES-128, AES-192, AES-256 — вибір залежить від вимог до продуктивності та рівня безпеки. AES-128 забезпечує оптимальний баланс між швидкістю та захистом, тому використовується у більшості комерційних рішень.
- **Асиметричне шифрування (RSA, ECC):** Застосовується для захисту управлінських каналів, автентифікації, обміну ключами. Перевага — відсутність необхідності передавати секретний ключ, але обмеження — висока обчислювальна складність, що не завжди прийнятна для масових пристроїв ONU/ONT.

Симетричні алгоритми (AES) реалізуються апаратно або програмно, забезпечуючи шифрування трафіку на рівні GEM-фреймів (GPON Encapsulation Method) або Ethernet-кадрів (EPON). Асиметричні — використовуються для PKI, TLS/IPsec, захисту управлінських протоколів.

Таблиця 2.1.2. Порівняння типів шифрування у xPON

Тип шифрування	Застосування	Переваги	Недоліки
AES-128/192/256	Трафік даних	Висока швидкість, стандарт FIPS, апаратна підтримка	Не захищає обмін ключами
RSA/ECC	Управління, автентифікація	Відсутність передачі секретного ключа	Висока обчислювальна складність, обмежена продуктивність

Симетричне шифрування є основою для захисту масового трафіку, а асиметричне — для управлінських операцій, автентифікації та PKI.

Управління ключами — критичний процес, що включає генерацію, розподіл, зберігання та оновлення криптографічних ключів. У xPON-мережах ключі AES генеруються для кожної ONU під час реєстрації, передаються OLT через захищені канали (наприклад, OMCI, PLOAM), періодично оновлюються для забезпечення forward secrecy.

Сучасні системи KMS (Key Management System) — Cosmian KMS, HSM (Hardware Security Module), PKI — дозволяють централізовано керувати життєвим циклом ключів, інтегруватися з SIEM, підтримувати стандарти FIPS 140-3, KMIP, PKCS#12, а також забезпечувати постквантову криптографію.

Ключові аспекти KMS у PON:

- **Генерація ключів:** Використання апаратних генераторів випадкових чисел, унікальних для кожної ONU.
- **Розподіл ключів:** Передача через OMCI або PLOAM, використання pre-shared keys для захисту від MITM-атак.
- **Оновлення ключів:** Періодична зміна (наприклад, щогодини/щодня), фрагментація ключа для підвищення надійності.
- **Зберігання:** Ключі не повинні зберігатися у відкритому вигляді на пристроях, використання HSM для захисту.

Таблиця 2.1.2 Функції KMS у PON

Функція	Опис	Приклад реалізації
Генерація	Випадковий ключ AES для кожної ONU	Cosmian KMS, HSM
Розподіл	OMCI, PLOAM, pre-shared key	OMCI, Altiplano Controller
Оновлення	Періодична зміна ключа	OLT ініціює key switch
Зберігання	Захищене сховище, HSM	PKCS#12, FIPS 140-3

Ефективне управління ключами — запорука стійкості криптографічного захисту у xPON.

TLS/IPsec — протоколи захисту управлінських та сервісних каналів у мережах xPON. TLS використовується для захисту Web-інтерфейсів управління OLT/ONU, REST API, SNMP, а IPsec — для тунелювання трафіку між вузлами мережі, особливо у мультисервісних архітектурах.

Особливості застосування:

- **TLS:** Шифрує HTTP/HTTPS трафік, забезпечує автентичність та цілісність даних. Вимагає коректної роботи PKI, сертифікатів, оновлення СА.
- **IPsec:** Використовується для захисту міжмережевого трафіку, VPN, з'єднань між OLT, маршрутизаторами, серверами. Може бути обмежений продуктивністю ONU/ONT, складністю налаштування.

Обмеження:

- Не всі ONU/ONT підтримують апаратне прискорення TLS/IPsec.
- Самопідписані сертифікати (self-signed) не рекомендуються для продуктивних середовищ.
- Висока складність інтеграції з PKI, необхідність регулярного оновлення сертифікатів.
- IPsec може впливати на продуктивність при великій кількості абонентів.

Практика: Вендори (Cisco, Huawei, ZTE, Nokia) рекомендують використовувати легітимні сертифікати, централізоване управління PKI, апаратне прискорення шифрування, а TLS/IPsec — для захисту критичних каналів управління, а не масового трафіку.

2.2 Автентифікація та контроль доступу

Типи автентифікації ONU (LOID, SN, 802.1X, DHCP option)

Автентифікація ONU — ключовий етап захисту xPON-мережі, що запобігає підключенню несанкціонованих пристроїв. Основні типи:

- **LOID (Logical Identifier):** Унікальний логічний ідентифікатор ONU, що задається оператором. OLT перевіряє LOID та check code, забезпечуючи гнучкість при зміні фізичного розташування ONU.
- **SN (Serial Number):** Заводський серійний номер ONU, жорстко прив'язаний до пристрою. Висока надійність, але низька гнучкість при заміні пристрою.

- **802.1X:** Протокол автентифікації на каналному рівні, використовує RADIUS сервер, підтримує MAC, Web-Auth, MAB. Дозволяє централізовано керувати доступом, автоматично призначати VLAN.
- **DHCP Option:** Використання опцій DHCP (наприклад, Option 82) для автентифікації та профілювання пристроїв, прив'язка IP-MAC-порт.

Таблиця 2.2.1. Порівняння типів автентифікації ONU

Тип автентифікації	Переваги	Недоліки	Сценарії використання
LOID	Гнучкість, централізоване управління	Можливість дублювання LOID	Міграція абонентів, корпоративні мережі
SN	Висока надійність, унікальність	Складність заміни ONU	Високий рівень безпеки, критичні об'єкти
802.1X	Централізований контроль, VLAN	Вимагає клієнта, складність налаштування	Корпоративні мережі, Wi-Fi, IoT
DHCP Option	Автоматизація, профілювання	Вразливість до DHCP-атак	Масові підключення, IoT

Вендори підтримують комбіновані режими автентифікації, що дозволяє гнучко налаштовувати політики доступу.

Сертифікати та PKI (Public Key Infrastructure) — основа для автентифікації пристроїв, захисту управлінських каналів, реалізації TLS/IPsec. Сертифікати видаються СА (Certificate Authority), містять унікальні ідентифікатори ONU/OLT, підписуються приватним ключем СА, перевіряються OLT/контролером.

Функції PKI у xPON:

- **Верифікація ідентичності ONU/OLT:** Сертифікат підтверджує справжність пристрою.
- **Шифрування управлінських каналів:** TLS/IPsec, SNMPv3, HTTPS.

- **Централізоване управління сертифікатами:** Відкликання, оновлення, аудит.
- **Підтримка електронного підпису:** Перевірка авторства та цілісності повідомлень.

Механізми авторизації та профілювання абонентів

Авторизація — визначення прав доступу абонента до сервісів, VLAN, QoS, SLA. **Профілювання** — збір інформації про тип пристрою, трафік, поведінку, автоматичне призначення політик.

Механізми:

- **Role Based Access Control (RBAC):** Призначення ролей (адміністратор, користувач, гість), CRUD-права на конфігурацію OLT/ONU.
- **SLA профілі:** Гарантована/максимальна швидкість, пріоритет трафіку, політики QoS.
- **VLAN, QoS, ACL:** Автоматичне призначення VLAN, класу сервісу, списків доступу на основі профілю абонента.
- **DHCP Option 82, RADIUS, SNMP:** Профілювання пристроїв, автоматичне призначення політик.

2.3 Сегментація та ізоляція трафіку

У пасивних оптичних мережах (xPON) логічна сегментація трафіку є критично важливою для забезпечення безпеки, керованості та якості обслуговування. Основними інструментами для цього є VLAN, QoS та мікросегментація.

VLAN (Virtual Local Area Network)

VLAN дозволяє логічно розділити трафік у межах однієї фізичної інфраструктури, ізолюючи абонентів і сервіси.

Типи VLAN:

- **Access VLAN** — виділяється для одного абонента або сервісу. Забезпечує базову ізоляцію.

- Trunk VLAN — транспортує трафік кількох VLAN між комутаторами або між OLT і ядром мережі. Використовує тегування 802.1Q.

- Q-in-Q (802.1ad) — Додавання другого VLAN-тега для тунелювання трафіку клієнта через мережу провайдера. Дозволяє ізолювати трафік різних клієнтів, підтримувати мультисервісність, прозорість для клієнта.

Тегування VLAN (stacking). Дозволяє провайдеру інкапсулювати трафік клієнта у власний VLAN:

- C-Tag (Customer Tag) — внутрішній тег клієнта.
- S-Tag (Service Tag) — зовнішній тег провайдера.
- Push/Pop — операції додавання або видалення тегів на пристроях

OLT/ONU.

Призначення:

- Ізоляція трафіку між абонентами.
- Підтримка мультисервісності (інтернет, IPTV, VoIP).
- Прозорість для корпоративних клієнтів (L2 VPN).

QoS (Quality of Service) — забезпечує контроль над розподілом пропускної здатності, пріоритетами та виконанням SLA для різних типів трафіку.

Основні механізми:

- CoS (Class of Service): Значення 0–7 у VLAN-тегу, визначає пріоритет трафіку.
- T-CONT (Transmission Container): GPON-специфічна одиниця, що асоціюється з ONU. Кожен T-CONT має тип (1–5), який визначає рівень гарантій.
- DBA (Dynamic Bandwidth Allocation):
- SR DBA (Status Reporting): ONU повідомляє про потребу в смузі.
- NSR DBA (Non-Status Reporting): OLT оцінює потребу на основі історії трафіку.

Алгоритми та політики:

- WRR (Weighted Round Robin): Зважене чергування.
- SP (Strict Priority): Жорсткий пріоритет для критичного трафіку.

- FIFO (First In, First Out): Простий, але менш ефективний метод.

SLA-профілі: Визначають гарантовану та максимальну швидкість, затримки, втрати.

Policy-Based QoS: Призначення політик на основі VLAN, MAC, IP, порту або сервісного профілю.

Мікросегментація — це глибший рівень ізоляції, який дозволяє контролювати трафік на рівні окремого пристрою, абонента або сервісу, що особливо важливо для реалізації Zero Trust-архітектури.

Механізми:

- VLAN per subscriber/service: Кожен абонент або сервіс отримує унікальну VLAN.
- ACL (Access Control Lists): Фільтрація трафіку за MAC, IP, портами.
- Port Security: Обмеження доступу до порту ONU за MAC-адресою.
- Policy-Based VLAN/QoS: Динамічне призначення VLAN і QoS на основі профілю абонента.
- VEIP (Virtual Ethernet Interface Point), UNI (User Network Interface): Гнучке розділення сервісів між портами ONU, що дозволяє реалізувати мультисервісність і ізоляцію.

Ці механізми дозволяють провайдерам створювати масштабовані, безпечні та керовані мережі, адаптовані до потреб як масових абонентів, так і корпоративних клієнтів.

2.4 Моніторинг та виявлення аномалій

IDS (Intrusion Detection System), IPS (Intrusion Prevention System) — системи виявлення та запобігання атак у xPON-мережах. IDS аналізує трафік, виявляє аномалії, IPS — блокує підозрілий трафік у реальному часі.

Розміщення:

- Периметр мережі: IDS для моніторингу вхідного/вихідного трафіку.
- Сегментні межі: IDS/IPS для контролю між VLAN, сервісами, абонентами.

- Хостові агенти: HIDS/HIPS на критичних серверах, OLT, контролерах.

Методи:

- Сигнатурний аналіз: Виявлення відомих атак за шаблонами.
- Аномалійний аналіз: Виявлення відхилень від нормального трафіку, ML, поведінковий аналіз.
- NBA (Network Behavior Analysis): Аналіз потоків, виявлення DoS/DDoS, lateral movement.

SIEM (Security Information and Event Management) — централізована платформа для збору, кореляції, аналізу логів з OLT, ONU, маршрутизаторів, комутаторів, серверів.

Функції SIEM:

- Збір логів: SNMP, Syslog, REST API, SNMPv3, централізоване сховище.
- Кореляція подій: Виявлення складних атак, ланцюгів інцидентів.
- Аналіз аномалій: ML, UEBA (User and Entity Behavior Analytics), поведінковий аналіз.
- Інцидент-менеджмент: Автоматичне реагування, SLA, аудит, звітність.

Методи виявлення аномалій: сигнатури, ML, поведінковий аналіз:

- **Сигнатурний аналіз:** Виявлення атак за відомими шаблонами (Snort, Suricata).
- **ML (Machine Learning):** Класифікація трафіку, виявлення невідомих атак, кластеризація, KNN, SVM, нейронні мережі.
- **Поведінковий аналіз:** Виявлення відхилень у поведінці користувачів, пристроїв, сервісів, UEBA.

Приклади інцидентів та кейси реагування

Інциденти:

- DoS/DDoS атаки на OLT через ін'єкцію оптичного сигналу.

- Компрометація ONU/ONT через вразливості прошивки (CVE-2025-34049: OS command injection у OptiLink ONT1GEW GPON).
- Атаки на DHCP, ARP, VLAN (DHCP starvation, ARP-spoofing, VLAN hopping).
- Фізичне підслуховування оптичної лінії (fiber tapping), виявлення через моніторинг потужності, підвищення затухання, сповіщення SIEM.
- Внутрішні атаки через компрометацію MAC/IP, несанкціоноване підключення ONU.

Кейси реагування:

- Автоматичне блокування порту, VLAN, MAC/IP через ACL, Portsecurity.
- Відключення ONU/ONT, оновлення прошивки, secure boot.
- Аудит логів, кореляція подій у SIEM, автоматичне сповіщення адміністраторів.
- Відновлення сервісу через резервний OLT (Type B dual-homing protection).
- Аналіз впливу інциденту через GIS, MITRE ATT&CK, оцінка ризику, планування контрзаходів.

2.5 Фізичний захист елементів мережі

Фізичний захист — перша лінія оборони від фізичних атак, саботажу, несанкціонованого доступу.

Рішення:

- **Металеві шафи, корпуси:** Захист від вологи, пилу, температури, механічних впливів, монтаж у 19" стійку, гаряча заміна модулів.



Рисунок 2.5.1 Металева шафа

- **Біометричний/електронний контроль доступу:** RFID, BioLock, централізоване управління, аудит доступу, відповідність PCI DSS, HIPAA, FISMA.
- **Відеоспостереження, сигналізація:** Контроль доступу, сповіщення про несанкціоновані дії.
- **Інвентаризація, маркування:** Ведення обліку обладнання, стану, конфігурації, автоматичне сповіщення про зміни.

Захист оптичних ліній від фізичного підслуховування та несанкціонованого доступу

Оптичні волокна мають високу стійкість до електромагнітних перешкод, що робить їх ідеальними для захищеного передавання даних. Проте вони залишаються вразливими до фізичного підслуховування (fiber tapping) — процесу, коли зломисник отримує доступ до оптичного сигналу без розриву лінії.

Загроза: фізичне підслуховування (fiber tapping)

Принцип дії: Зловмисник використовує спеціальні пристрої (наприклад, оптичні відгалужувачі або вигини волокна), щоб зчитати частину світлового сигналу без помітного впливу на якість зв'язку.

Складність виявлення: Через пасивність методу втручання часто не викликає помітного зниження потужності сигналу, особливо при використанні високоякісного обладнання.

Технічні методи захисту:

1. Моніторинг потужності та оптичних параметрів

Принцип: Постійне вимірювання рівня оптичного сигналу, затухання, відбиття, розсіювання.

Інструменти:

OTDR (Optical Time Domain Reflectometer): Виявляє аномалії, мікрозгинання, втрати.

SIEM-інтеграція: Автоматичне сповіщення про підозрілі зміни потужності або патернів сигналу.

Перевага: Можливість раннього виявлення втручання.

2. Оптичні сенсори та волоконно-оптичні системи виявлення вторгнень (FIDS)

Принцип: Виявлення механічних впливів — вібрацій, згинів, натягу, зміни температури.

Інтеграція з:

- SIEM: Для кореляції подій безпеки.
- GIS: Для географічної локалізації інциденту.

Застосування: Критична інфраструктура, військові об'єкти, дата-центри.

3. Шифрування трафіку

Мета: Навіть якщо трафік буде перехоплено, його неможливо буде дешифрувати без ключа.

Технології:

- AES (Advanced Encryption Standard): Симетричне шифрування на рівні L2/L3.

- TLS/IPsec: Шифрування на рівні транспортного або мережевого протоколу.

- MACsec (IEEE 802.1AE): Шифрування на рівні канального рівня (L2), актуальне для корпоративних мереж.

4. PDS (Protective Distribution System)

Призначення: Фізичний захист каналів зв'язку відповідно до військових стандартів (наприклад, NSTISSI 7003).

Компоненти:

- Армовані кабелі, металеві гофровані труби.
- Захищені кабельні канали з контролем доступу.
- Системи виявлення відкриття або пошкодження оболонки.

Організаційні заходи безпеки

Централізоване управління доступом

Функції:

- Ведення журналів доступу до обладнання.
- Аудит змін конфігурацій.
- Автоматичне сповіщення про несанкціоновані дії.
- Інструменти: AAA-сервери, RADIUS/TACACS+, інтеграція з SIEM.

Інвентаризація обладнання

Мета: Контроль за фізичним станом і розташуванням обладнання.

Методи:

- Ведення актуального реєстру пристроїв, кабелів, муфт.
- Використання SNMP, NetConf/YANG для автоматичного оновлення даних.
- Інтеграція з системами моніторингу (Zabbix, PRTG, SolarWinds).

Маркування та фізичний контроль

Маркування: Кабелі, муфти, шафи мають бути чітко промарковані з унікальними ідентифікаторами.

Контроль: Регулярна перевірка на предмет несанкціонованих змін або підключень.

Навчання персоналу

Цілі:

- Підвищення обізнаності про загрози фізичного доступу.
- Навчання реагуванню на інциденти (SOC playbooks).
- Проведення регулярних аудитів дій персоналу.

Комплексне поєднання технічних і організаційних заходів дозволяє значно знизити ризики, пов'язані з фізичним підслуховуванням оптичних ліній.

2.6 Засоби захисту на різних рівнях мережі

Захист на рівні OLT: управління, шифрування, ACL, профілі

OLT (Optical Line Terminal) — центральний елемент xPON, відповідає за управління, шифрування, розподіл пропускної здатності, ACL, профілі сервісів.

Засоби захисту:

- **Управління ключами, шифрування AES:** Генерація, розподіл, оновлення ключів для кожної ONU.
- **ACL, MAC/IP фільтрація:** Блокування несанкціонованих підключень, контроль доступу.
- **SLA, VLAN, QoS:** Призначення політик, ізоляція трафіку, гарантія сервісу.
- **802.1X, DHCP Relay, PPPoE:** Автентифікація, централізоване управління доступом.
- **Оновлення прошивки, аудит:** Захист від вразливостей, контроль версій, автоматичне реагування.

Захист на рівні ONU/ONT: локальні механізми, прошивки, secure boot

ONU/ONT (Optical Network Unit/Terminal) — абонентський пристрій, відповідає за локальні механізми захисту, оновлення прошивки, secure boot.

Засоби захисту:

- **Локальні ACL, VLAN, QoS:** Ізоляція трафіку, контроль доступу.
- **Оновлення прошивки, secure boot:** Захист від компрометації, BootHole, rootkit, контроль цілісності.

- **MAC/IP фільтрація, Portsecurity:** Блокування несанкціонованих підключень.

- **Віддалене вимкнення лазера, Reset ONU:** Реагування на інциденти, блокування компрометованих пристроїв.

Захист на мережевому рівні: маршрутизатори, брандмауери, VPN

Мережевий рівень — маршрутизатори, брандмауери, VPN, edge firewalls, SDN, хмарні сервіси.

Засоби захисту:

- **Edge firewall, IPS/IDS:** Захист периметру, сегментів, сервісів, інтеграція з SIEM.

- **VPN, IPsec, TLS:** Захист міжмережевого трафіку, тунелювання, шифрування.

- **SDN, хмарні сервіси:** Гнучке управління політиками, автоматичне реагування, інтеграція з SIEM, SNMP.

- **ACL, VLAN, QoS:** Ізоляція трафіку, контроль доступу, гарантія сервісу.

Організаційні заходи — політики безпеки, SLA, оновлення, інцидент-менеджмент, аудит, навчання.

Методи:

- **Політики безпеки:** Визначення вимог, контроль виконання, аудит.

- **SLA:** Гарантія сервісу, контроль якості, автоматичне реагування на порушення.

- **Оновлення прошивки, патч-менеджмент:** Захист від вразливостей, аудит, автоматичне оновлення.

- **Інцидент-менеджмент:** Виявлення, реагування, аудит, навчання персоналу, інтеграція з SIEM, SNMP.

ВИСНОВКИ ДО РОЗДІЛУ 2

Захист мереж xPON — багаторівневий процес, що охоплює криптографічні алгоритми, автентифікацію, сегментацію, моніторинг, фізичний захист, організаційні політики та інцидент-менеджмент. Сучасні рішення вендорів, стандарти ITU-T, IEEE, ETSI, інструменти моніторингу (PMon, Zabbix, SIEM), ML-методи, централізоване управління ключами та сертифікатами, мікросегментація, автоматичне реагування — забезпечують високий рівень безпеки, гнучкість, масштабованість та відповідність нормативним вимогам.

Ефективність заходів захисту визначається не лише технічними рішеннями, а й організаційними політиками, навчанням персоналу, регулярним аудитом, інтеграцією з SIEM, SNMP, ML, автоматичним реагуванням на інциденти. Впровадження сучасних підходів, регулярний аудит, оптимізація політик, навчання — запорука стійкості xPON-мереж до сучасних кіберзагроз.

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДІВ ЗАХИСТУ МЕРЕЖІ ДОСТУПУ В CISCO PACKET TRACER

3.1 Мета та завдання практичної реалізації

У зв'язку з тим, що програмне середовище **Cisco Packet Tracer** не підтримує безпосереднє моделювання реальних елементів xPON-мереж, таких як OLT, ONU/ONT та протоколи керування оптичним доступом, у даній роботі застосовано підхід **функціонального відображення xPON-мережі на Ethernet-інфраструктуру**.

Сутність даного підходу полягає в тому, що логічні функції та принципи роботи мережі доступу xPON моделюються за допомогою еквівалентних за функціональним призначенням елементів Ethernet-мережі. Зокрема, маршрутизатор Cisco використовується як **функціональний аналог OLT**, комутатор рівня доступу — як **аналог оптичного сплітера**, а кінцеві абонентські вузли — як **аналог ONU/ONT**.

При цьому основна увага приділяється не фізичному рівню передавання оптичного сигналу, а **реалізації та дослідженню методів і засобів захисту мережі доступу**, зокрема сегментації абонентського трафіку, ізоляції абонентів між собою, контролю доступу, захищеного керування мережею та автоматичної видачі мережевих параметрів.

Використання Ethernet-інфраструктури як моделі дозволяє коректно відобразити **логічну архітектуру xPON-мережі**, принципи централізованого керування та механізми інформаційної безпеки, що є достатнім для досягнення мети випускної кваліфікаційної роботи в умовах обмежень програмного середовища Cisco Packet Tracer.

3.2 Опис топології та план адресації

Модель мережі складається з маршрутизатора (OLT-аналог), комутатора доступу, трьох абонентських вузлів (ONU1–ONU3) та окремого адміністративного вузла (Admin-PC). Логічна сегментація реалізована за допомогою VLAN.

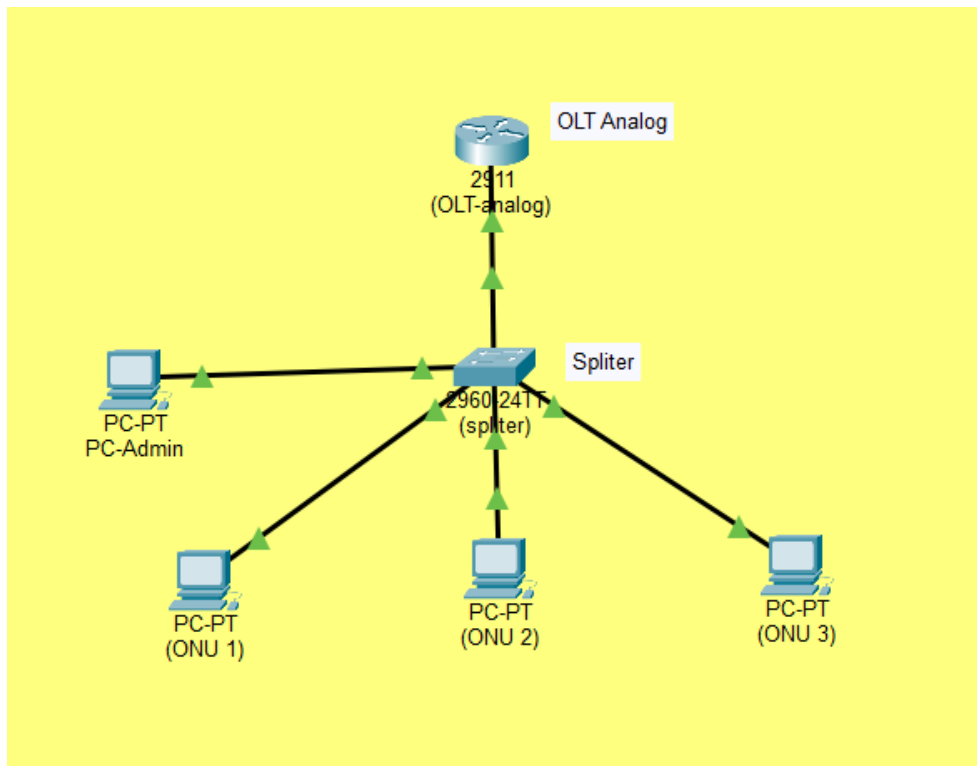


Рисунок 3.2.1 Модель мережі

Для адресації використовується приватний IP-діапазон 10.10.0.0/16 з поділом на окремі підмережі: VLAN 10 – 10.10.10.0/24, VLAN 20 – 10.10.20.0/24, VLAN 30 – 10.10.30.0/24. Абонентські вузли отримують мережеві параметри автоматично за допомогою DHCP.

3.3 Реалізація сегментації трафіку за допомогою VLAN

Сегментація трафіку є базовим механізмом ізоляції абонентів у мережах доступу. У межах моделі кожному абоненту відповідає окремий VLAN, що знижує ризик перехоплення трафіку.

```

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name ONU1
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name ONU2
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name ONU3
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name MGMT
Switch(config-vlan)#exit
Switch(config)#in fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#in fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#in fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#in fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 99
Switch(config-if)#exit
Switch(config)#in fa0/24
Switch(config-if)#exit
Switch(config)#in gi0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access trunk
Switch#

% Invalid input detected at '^' marker.

Switch(config-if)#switchport mode trunk
Switch(config-if)#end
Switch#

```

Рисунок 3.3.1 Реалізація сегментації трафіку за допомогою VLAN

3.4 Міжвланова маршрутизація

Для забезпечення доступу вузлів до відповідних шлюзів на маршрутизаторі налаштовано підінтерфейси з інкапсуляцією IEEE 802.1Q.

```

%LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
OLT(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
OLT(config-if)#in g0/0.10
OLT(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.10, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up
OLT(config-subif)#encapsulation dot1Q 10
OLT(config-subif)#ip address 10.10.10.1 255.255.255.0
OLT(config-subif)#exit
OLT(config)#in g0/0.20
OLT(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.20, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up
OLT(config-subif)#encapsulation dot1Q 20
OLT(config-subif)#ip address 10.10.20.1 255.255.255.0
OLT(config-subif)#exit
OLT(config)#in g0/0.30
OLT(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.30, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up
OLT(config-subif)#encapsulation dot1Q 30
OLT(config-subif)#ip address 10.10.30.1 255.255.255.0
OLT(config-subif)#exit
OLT(config)#in g0/0.99
OLT(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.99, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.99, changed state to up
OLT(config-subif)#encapsulation dot1Q 99
OLT(config-subif)#ip address 10.10.99.1 255.255.255.0
OLT(config-subif)#end
OLT#

```

Рисунок 3.4.1 Міжвланова маршрутизація

3.5 Налаштування динамічної адресації DHCP

Для автоматичної видачі мережевих параметрів абонентам та адміністративному вузлу DHCP-сервер реалізовано на маршрутизаторі з використанням окремих пулів для кожного VLAN.

```

OLT#
OLT#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OLT(config)#ip dhcp excluded-address 10.10.10.1 10.10.10.20
OLT(config)#ip dhcp excluded-address 10.10.20.1 10.10.20.20
OLT(config)#ip dhcp excluded-address 10.10.30.1 10.10.30.20
OLT(config)#ip dhcp excluded-address 10.10.99.1 10.10.99.20
OLT(config)#
OLT(config)#ip dhcp pool VLAN10_ONU1
OLT(dhcp-config)#network 10.10.10.0 255.255.255.0
OLT(dhcp-config)#default-router 10.10.10.1
OLT(dhcp-config)#exit
OLT(config)#ip dhcp pool VLAN20_ONU2
OLT(dhcp-config)#network 10.10.20.0 255.255.255.0
OLT(dhcp-config)#default-router 10.10.20.1
OLT(dhcp-config)#exit
OLT(config)#ip dhcp pool VLAN30_ONU3
OLT(dhcp-config)#network 10.10.30.0 255.255.255.0
OLT(dhcp-config)#default-router 10.10.30.1
OLT(dhcp-config)#exit
OLT(config)#ip dhcp pool VLAN99_MGMT
OLT(dhcp-config)#network 10.10.99.0 255.255.255.0
OLT(dhcp-config)#default-router 10.10.99.1
OLT(dhcp-config)#end
OLT#

```

Рисунок 3.5.1 Налаштування динамічної адресації DHCP

3.6 Контроль доступу та ізоляція абонентів (ACL)

Для запобігання взаємодії абонентів між собою та захисту керуючого доступу застосовано списки контролю доступу.

```

OLT#conf t
Enter configuration commands, one per line. End with CNTL/Z.
OLT(config)#access-list 100 deny ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255
OLT(config)#access-list 100 deny ip 10.10.10.0 0.0.0.255 10.10.30.0 0.0.0.255
OLT(config)#access-list 100 deny ip 10.10.20.0 0.0.0.255 10.10.10.0 0.0.0.255
OLT(config)#access-list 100 deny ip 10.10.20.0 0.0.0.255 10.10.30.0 0.0.0.255
OLT(config)#access-list 100 deny ip 10.10.30.0 0.0.0.255 10.10.10.0 0.0.0.255
OLT(config)#access-list 100 deny ip 10.10.30.0 0.0.0.255 10.10.20.0 0.0.0.255
OLT(config)#access-list 100 permit ip any any
OLT(config)#
OLT(config)#in g0/0
OLT(config-if)#ip access-group 100 in
OLT(config-if)#

```

Рисунок 3.6.1 Контроль доступу та ізоляція абонентів (ACL)

3.7 Захищене керування мережею (SSH, MGMT VLAN)

Захищене керування маршрутизатором дозволене лише з керуючого сегмента VLAN 99. Для цього налаштовано доступ за протоколом SSH та обмежено підключення за допомогою ACL.

```

OLT# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
OLT(config)#ip domain-name xpon.local
OLT(config)#crypto key generate rsa

OLT(config)#crypto key generate rsa
% You already have RSA keys defined named OLT.xpon.local .
% Do you really want to replace them? [yes/no]: no
OLT(config)#username admin secret admin123
OLT(config)#
OLT(config)#ip access-list standard MGMT_SSH_ONLY
OLT(config-std-nacl)# permit 10.10.99.0 0.0.0.255
OLT(config-std-nacl)#deny any
OLT(config-std-nacl)#
OLT(config-std-nacl)#line vty 0 4
OLT(config-line)#login local
OLT(config-line)#transport input ssh
OLT(config-line)#access-class MGMT_SSH_ONLY in
OLT(config-line)#end
OLT#
%SYS-5-CONFIG_I: Configured from console by console

OLT#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
OLT#

```

Рисунок 3.7.1 Захищене керування мережею (SSH, MGMT VLAN)

3.8 Тестування та аналіз результатів

У процесі тестування перевірено отримання IP-адрес через DHCP, доступність шлюзів, блокування трафіку між абонентськими VLAN, а також можливість керування маршрутизатором виключно з MGMT VLAN. Результати підтвердили ефективність реалізованих методів захисту.

Перевірка роботи DHCP

Мета тестування – перевірка коректності автоматичної видачі IP-адрес абонентським та керуючим вузлам.

Пристрої: ONU1, ONU2, ONU3 (PC-PT), Admin-PC, маршрутизатор (OLT-analog).

Команди (маршрутизатор, OLT-analog):

```
show ip dhcp binding
```

```
show ip dhcp pool
```

Очікуваний результат: вузли отримують IP-адреси з відповідних VLAN-підмереж.

Фактичний результат: DHCP працює коректно, IP-адреси видані успішно.

```
OLT#show ip dhcp binding
IP address      Client-ID/      Lease expiration      Type
                Hardware address
10.10.10.21     0004.9A88.89D9   --                     Automatic
10.10.20.21     00E0.F9B4.690C   --                     Automatic
10.10.30.21     0001.42A9.4A33   --                     Automatic
10.10.99.21     0001.6332.D32A   --                     Automatic
OLT#show ip dhcp pool

Pool VLAN10_ONU1 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next)    : 0 / 0
Total addresses              : 254
Leased addresses             : 1
Excluded addresses          : 4
Pending event                : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
10.10.10.1         10.10.10.1 - 10.10.10.254   1 / 4 / 254

Pool VLAN20_ONU2 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next)    : 0 / 0
Total addresses              : 254
Leased addresses             : 1
Excluded addresses          : 4
Pending event                : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
10.10.20.1         10.10.20.1 - 10.10.20.254   1 / 4 / 254

Pool VLAN30_ONU3 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next)    : 0 / 0
Total addresses              : 254
Leased addresses             : 1
Excluded addresses          : 4
Pending event                : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
10.10.30.1         10.10.30.1 - 10.10.30.254   1 / 4 / 254

Pool VLAN99_MGMT :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next)    : 0 / 0
Total addresses              : 254
Leased addresses             : 1
Excluded addresses          : 4
Pending event                : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
10.10.99.1         10.10.99.1 - 10.10.99.254   1 / 4 / 254
OLT#
```

Рисунок 3.8.1 – Результат виконання команди show ip dhcp binding

Перевірка доступності шлюзів VLAN

Мета тестування – перевірка доступності шлюзу за замовчуванням для кожного VLAN.

Пристрої: ONU1, ONU2, ONU3 (PC-PT).

Команди (абонентські вузли – PC-PT):

ping 10.10.10.1 (ONU1)

ping 10.10.20.1 (ONU2)

ping 10.10.30.1 (ONU3)

Очікуваний результат: ICMP-запити до власного шлюзу проходять успішно.

Фактичний результат: доступ до шлюзів забезпечено.

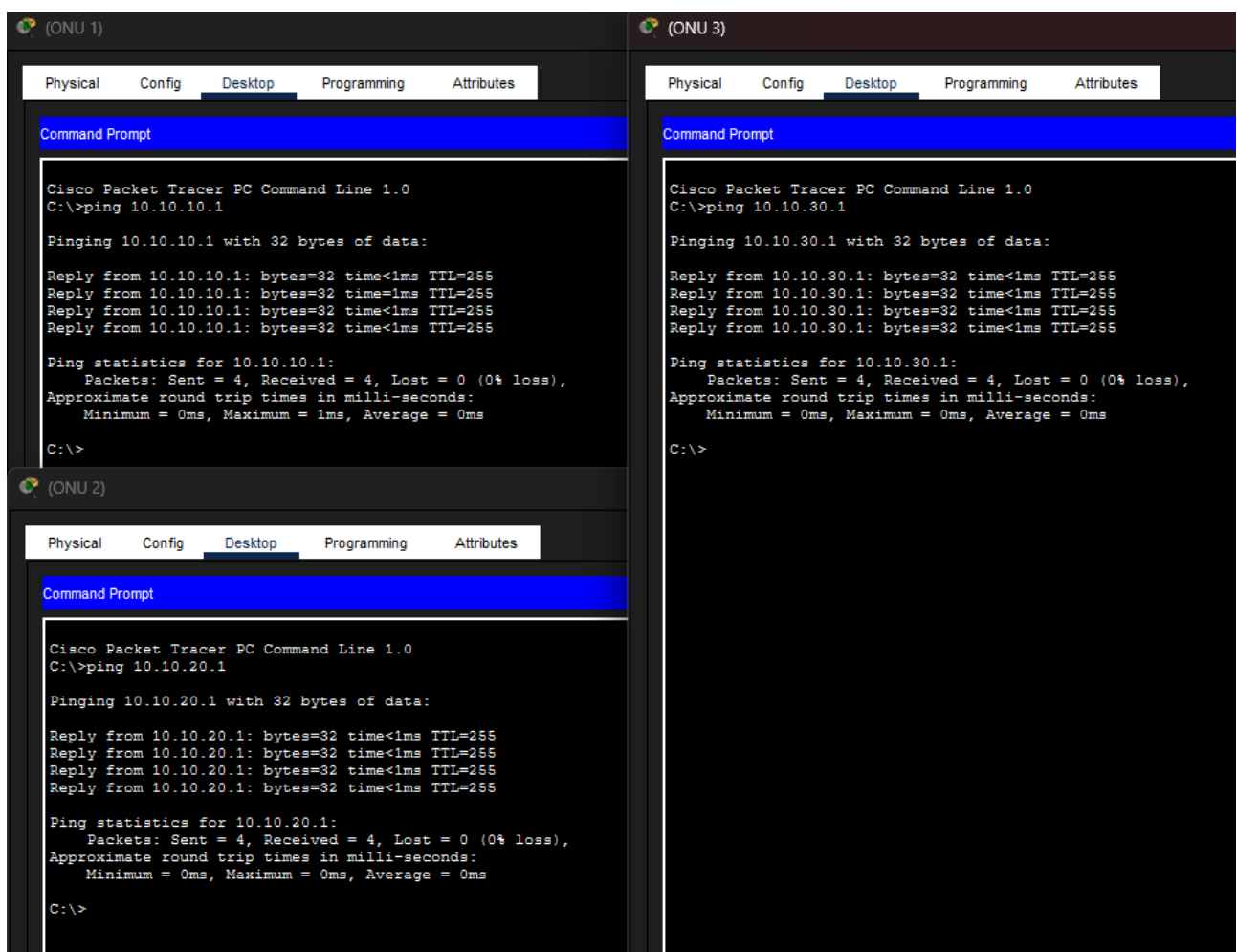


Рисунок 3.8.2 – Перевірка доступності шлюзу VLAN

Перевірка ізоляції абонентських вузлів

Мета тестування:

Оцінити можливість ізоляції абонентських вузлів між собою та проаналізувати особливості реалізації даного механізму в умовах моделювання xPON-мережі в середовищі Cisco Packet Tracer.

Пристрої:

- ONU1, ONU2, ONU3 (PC-PT)
- Комутатор доступу (аналог оптичного сплітера)
- Маршрутизатор (OLT-analog)

Порядок виконання тестування:

1. З абонентського вузла ONU1 виконано ICMP-запити до IP-адрес абонентських вузлів ONU2 та ONU3.
2. Аналогічні перевірки виконано з інших абонентських вузлів.
3. Проаналізовано шлях проходження трафіку та місце застосування механізмів контролю доступу.

Команди (абонентські вузли – PC-PT):

ping 10.10.20.x

ping 10.10.30.x

Команди (маршрутизатор, OLT-analog):

show access-lists 100

Очікуваний результат:

У реальних xPON-мережах прямий обмін трафіком між абонентськими вузлами відсутній, оскільки ізоляція ONU реалізується на фізичному та протокольному рівнях OLT.

Фактичний результат:

У процесі тестування встановлено, що в умовах моделювання в середовищі Cisco Packet Tracer абонентські вузли можуть здійснювати обмін трафіком між собою. Це пояснюється тим, що всі абонентські пристрої підключені до одного комутатора доступу та взаємодіють на канальному рівні (L2), минаючи маршрутизатор. У зв'язку з цим списки контролю доступу, налаштовані на маршрутизаторі, не застосовуються до такого трафіку.

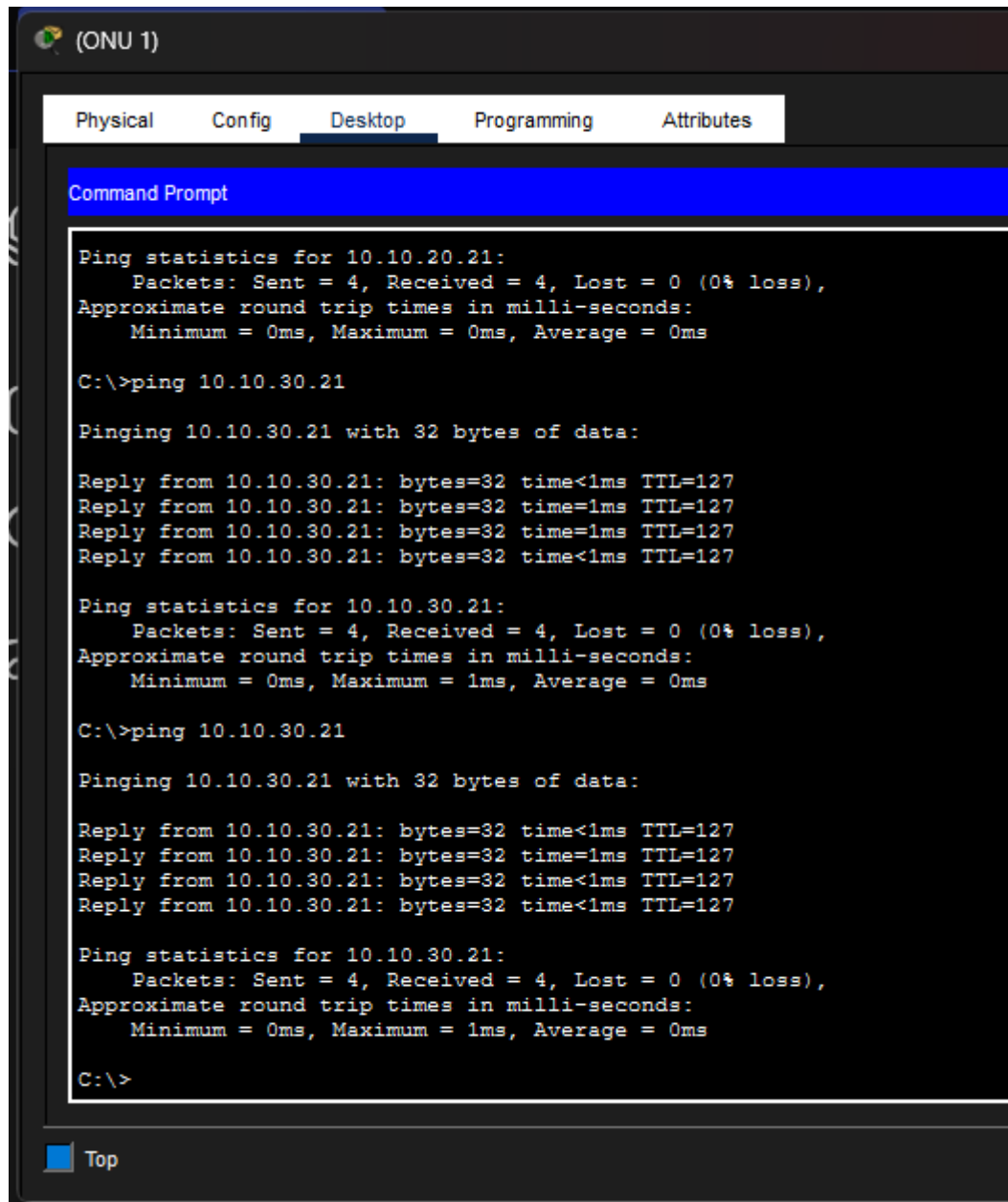


Рисунок 3.8.3 – Обмін ICMP-трафіком між абонентськими вузлами в умовах моделювання

Примітка до даної перевірки

Слід зазначити, що в реальних xPON-мережах ізоляція абонентів забезпечується апаратними та протокольними механізмами OLT, які виключають можливість прямої взаємодії між ONU. У середовищі Cisco Packet Tracer така функціональність відсутня, тому модель мережі доступу реалізує логічну архітектуру xPON та дозволяє досліджувати методи захисту на рівнях

сегментації, контролю доступу та керування мережею, що є достатнім для досягнення мети даної випускної кваліфікаційної роботи.

Перевірка захищеного керування мережею (SSH)

Мета тестування – перевірка доступу до керування маршрутизатором лише з MGMT VLAN.

Пристрої: Admin-PC, ONU1, маршрутизатор (OLT-analog).

Команди (Admin-PC):

```
ssh -l admin 10.10.99.1
```

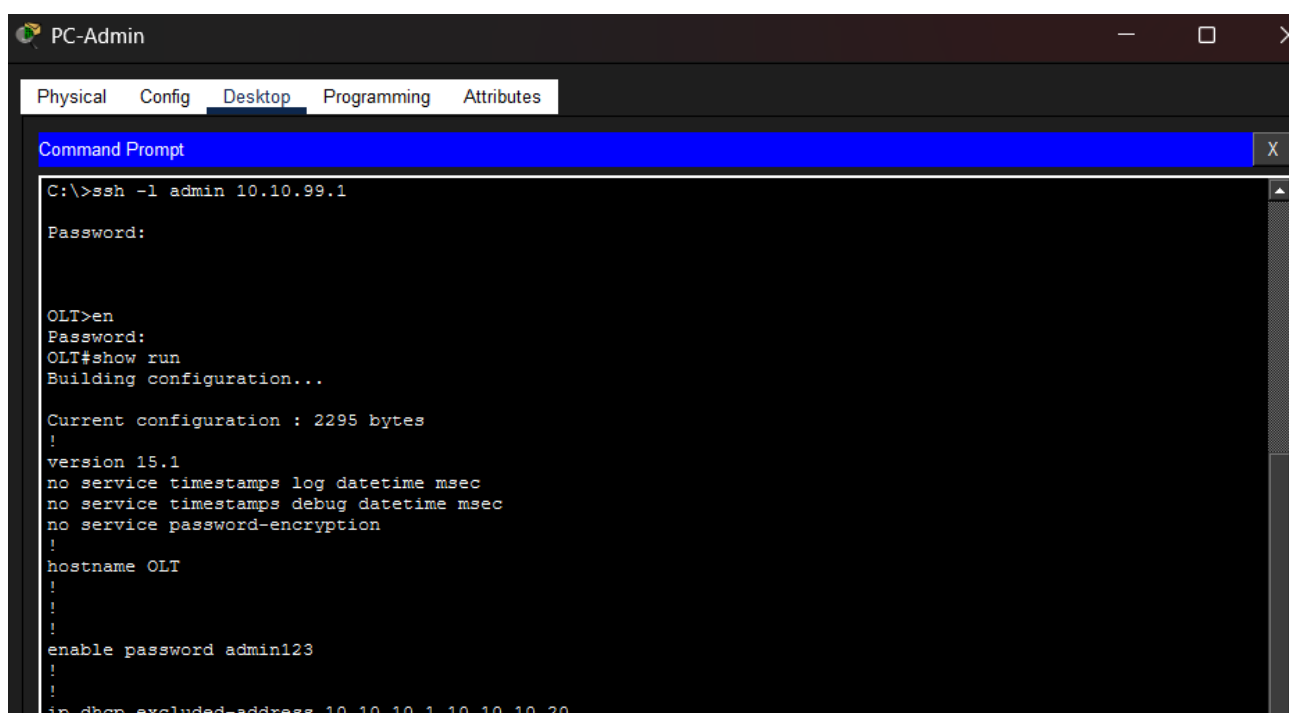
Команди (маршрутизатор, OLT-analog):

```
show ssh
```

```
show run | section line vty
```

Очікуваний результат: SSH-доступ дозволений з MGMT VLAN і заборонений з абонентських VLAN.

Фактичний результат: доступ відповідає налаштуванням політик безпеки.



```
PC-Admin
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ssh -l admin 10.10.99.1
Password:

OLT>en
Password:
OLT#show run
Building configuration...

Current configuration : 2295 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname OLT
!
!
!
enable password admin123
!
!
!
ip dhcp excluded-address 10.10.10.1 10.10.10.20
```

Рисунок 3.8.4 – SSH-підключення з Admin-PC

```
(ONU 1)
Ping statistics for 10.10.30.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.10.30.21

Pinging 10.10.30.21 with 32 bytes of data:

Reply from 10.10.30.21: bytes=32 time<1ms TTL=127
Reply from 10.10.30.21: bytes=32 time=1ms TTL=127
Reply from 10.10.30.21: bytes=32 time<1ms TTL=127
Reply from 10.10.30.21: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.30.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ssh -l admin 10.10.10.1
% Connection refused by remote host
C:\>ssh -l admin 10.10.99.1
% Connection refused by remote host
C:\>
```

Рисунок 3.8.5 – Відмова SSH-підключення з абонентського VLAN

Результати тестування підтвердили працездатність змодельованої мережі та ефективність реалізованих методів захисту. Усі поставлені завдання практичної частини виконано.

ВИСНОВКИ ДО РОЗДІЛУ 3

У третьому розділі виконано практичну реалізацію моделі захищеної мережі доступу регіонального інтернет-провайдера з урахуванням особливостей та обмежень середовища моделювання Cisco Packet Tracer. Зважаючи на відсутність у програмному середовищі підтримки реальних елементів xPON-інфраструктури, застосовано підхід функціонального відображення, відповідно до якого основні компоненти xPON-мережі змодельовано на базі Ethernet-інфраструктури.

У процесі моделювання маршрутизатор Cisco використано як функціональний аналог OLT, комутатори доступу — як аналог пасивних оптичних сплітерів, а кінцеві вузли мережі — як аналоги абонентських терміналів ONU/ONT. Такий підхід дозволив коректно відтворити логіку роботи мережі доступу, принципи сегментації абонентського трафіку та механізми централізованого керування.

У межах практичної частини реалізовано базові засоби захисту мережі доступу, зокрема логічну сегментацію за допомогою VLAN, контроль міжмережевої взаємодії з використанням списків керування доступом (ACL), динамічну IP-адресацію, а також захищений доступ до керуючого сегмента мережі з використанням протоколу SSH. Проведене тестування підтвердило працездатність змодельованої мережі та ефективність застосованих механізмів захисту в межах обраної моделі.

Отримані результати свідчать, що навіть за умови обмежень програмного середовища можливо реалізувати коректну модель мережі доступу та проаналізувати ключові аспекти її захисту. Реалізовані в роботі рішення відповідають практикам, що застосовуються в реальних xPON-мережах, та можуть бути використані як основа для подальших досліджень і проектування захищених мереж доступу провайдерського рівня.

ВИСНОВОК

У магістерській кваліфікаційній роботі виконано комплексне дослідження методів та засобів захисту мереж доступу регіонального інтернет-провайдера, побудованих на основі технологій xPON. У межах роботи досягнуто поставленої мети та розв'язано всі визначені на початку дослідження завдання.

У першому розділі роботи проаналізовано архітектуру та принципи функціонування пасивних оптичних мереж xPON, зокрема технологій GPON, EPON та XG(S)-PON. Визначено їх ключові переваги, обмеження та особливості застосування в мережах доступу провайдерського рівня. Окрему увагу приділено аналізу актуальних загроз інформаційній безпеці xPON-мереж, таких як несанкціонований доступ, перехоплення трафіку, атаки типу DoS/DDoS, вразливості протоколів керування та фізичні загрози інфраструктурі.

У другому розділі систематизовано сучасні методи та засоби захисту xPON-мереж. Розглянуто криптографічні механізми забезпечення конфіденційності даних, методи автентифікації та контролю доступу, засоби сегментації й ізоляції трафіку, а також організаційні та фізичні заходи безпеки. Показано, що ефективний захист мереж доступу можливий лише за умови комплексного підходу, який поєднує технічні, програмні та адміністративні механізми.

У третьому розділі виконано практичну реалізацію моделі захищеної мережі доступу з урахуванням обмежень середовища моделювання Cisco Packet Tracer. Обґрунтовано застосування функціонального відображення елементів xPON-мережі на Ethernet-інфраструктуру, що дозволило відтворити логіку роботи мережі доступу, принципи централізованого керування та реалізувати базові механізми захисту. У процесі моделювання налаштовано сегментацію трафіку за допомогою VLAN, динамічну IP-адресацію, контроль міжмережевої взаємодії засобами ACL, а також захищений доступ до керуючого сегмента з використанням протоколу SSH. Проведено тестування працездатності мережі та підтверджено ефективність застосованих засобів захисту.

Отримані результати свідчать, що запропонована модель забезпечує необхідний рівень інформаційної безпеки мережі доступу та відповідає практикам, які застосовуються в реальних xPON-мережах регіональних інтернет-провайдерів. Хоча середовище Cisco Packet Tracer не дозволяє повною мірою змодельовати фізичний рівень пасивних оптичних мереж, реалізоване функціональне відображення є достатнім для аналізу архітектури, механізмів захисту та принципів експлуатації xPON-інфраструктури.

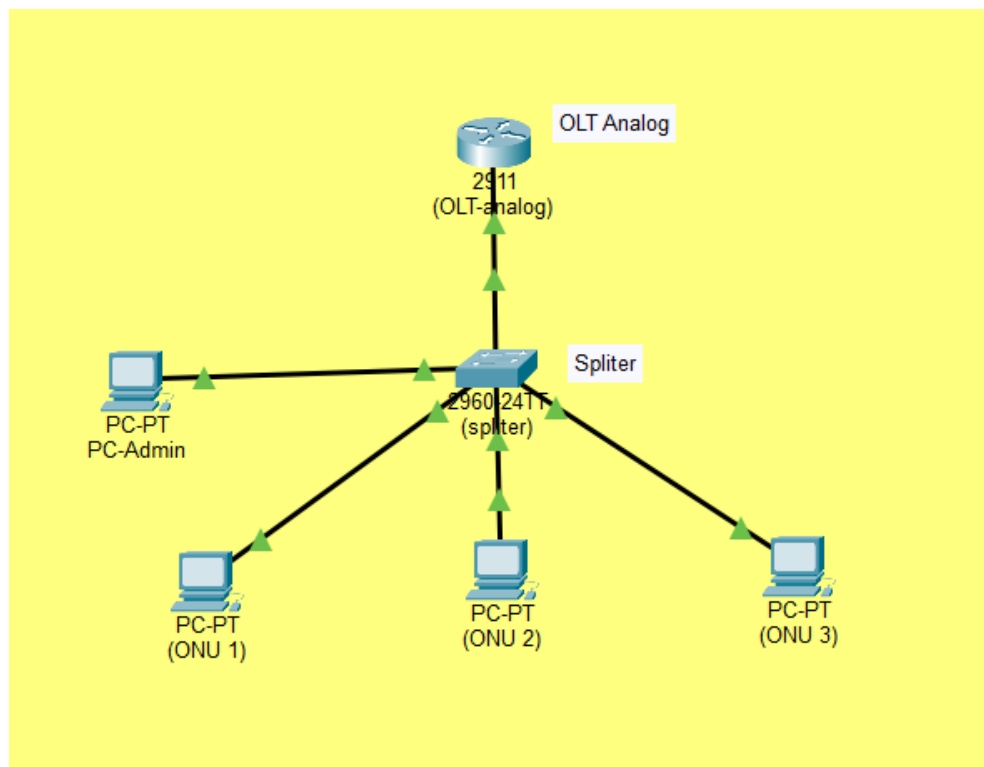
Практична цінність роботи полягає у можливості використання отриманих результатів під час проєктування, модернізації та експлуатації мереж доступу провайдерського рівня, а також у навчальному процесі для підготовки фахівців у галузі кібербезпеки та телекомунікацій. Напрямами подальших досліджень можуть бути поглиблений аналіз механізмів моніторингу та виявлення атак, а також моделювання xPON-мереж із використанням спеціалізованих середовищ або реального оптичного обладнання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ITU-T G.984. Gigabit-capable Passive Optical Networks (GPON). – International Telecommunication Union, Geneva.
2. ITU-T G.987. 10-Gigabit-capable Passive Optical Networks (XG-PON). – International Telecommunication Union, Geneva.
3. ITU-T G.9807.1. 10-Gigabit-capable symmetric passive optical network (XGS-PON). – International Telecommunication Union, Geneva.
4. IEEE 802.3ah. Ethernet in the First Mile (EFM). – IEEE Standards Association.
5. Зингеренко Ю. А. Пасивні оптичні мережі xPON. – СПб.: Університет ІТМО, 2020.
6. Катко В. Б., Михайленко Є. В., Котенко М. О. Пасивні оптичні мережі xPON. – Київ, 2006.
7. Stallings W. Cryptography and Network Security: Principles and Practice. – Pearson Education, 2017.
8. RFC 4301. Security Architecture for the Internet Protocol. – IETF.
9. NIST SP 800-53. Security and Privacy Controls for Information Systems and Organizations. – NIST, USA.
10. ETSI TS 103 645. Cyber Security for Consumer Internet of Things. – ETSI.
11. Cisco Networking Academy. CCNA: Enterprise Networking, Security, and Automation. – 2023. – URL: <https://www.netacad.com>
12. Cisco Catalyst 2960 Series Switches – Configuration Guide. – Cisco Systems, 2023. – URL: <https://www.cisco.com>
13. Cisco 2911 Integrated Services Router – Configuration Guide. – Cisco Systems, 2023. – URL: <https://www.cisco.com>
14. Cisco IOS DHCP Configuration Guide. – Cisco Systems, 2023. – URL: <https://www.cisco.com>
15. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2010.
16. Таненбаум Э. Компьютерные сети. – 5-е изд. – СПб.: Питер, 2012.
17. Азаров О. Д., Захарченко С. М., Кадук О. В. Комп'ютерні мережі. – Вінниця: ВНТУ, 2013.

ДОДАТКИ

Модель мережі



Технічні специфікації маршрутизатора Cisco 2911/K9

Код продукту	Cisco 2911/K9
Стелажні блоки	2RU
Інтерфейси	3 вбудованих порти 10/100/1000 Ethernet (тільки RJ-45)
Слот(и) розширення	1 слот для сервісного модуля
	1 слот для внутрішнього сервісного модуля
	2 слоти для вбудованого цифрового сигнального процесора (DSP)
	4 слоти для розширених високошвидкісних інтерфейсних плат WAN
ОПЕРАТИВНА ПАМ'ЯТЬ	512 МБ (встановлено) / 2 ГБ (макс.)
Флеш-пам'ять	256 МБ (встановлено) / 8 ГБ (макс.)
Розміри	43,8 см x 30,5 см x 8,9 см
Вага упаковки	16,15 кг

Технічні специфікації комутатора Cisco Catalyst 2960-24TTL

Код продукту	WS-C2960-24TT-L
Тип корпусу	Монтаж у стійку - 1U
Набір функцій	LAN Base
Інтерфейси висхідної лінії зв'язку	2 x 10/100/1000 TX uplink
Порти	24 x Ethernet 10/100 порти
Пропускна здатність	6,5 МПП
Ємність об'єднувальної плати	16 Гбіт/с
DRAM	16 МБ
Розміри	1,73 x 17,5 x 9,3 дюйма.
Вага упаковки	8,15 кг

Нижче представлені конфігураційні файли пристроїв мережі

!	no ipv6 cef	ip address 10.10.20.1
version 15.1	!	255.255.255.0
no service timestamps log	!	!
datetime msec	!	interface
no service timestamps	username admin secret 5	GigabitEthernet0/0.30
debug datetime msec	\$1\$mERr\$AFX/pZT1Lh7N	encapsulation dot1Q 30
no service password-	P3Dp3P/qq/	ip address 10.10.30.1
encryption	!	255.255.255.0
!	!	!
hostname OLT	license udi pid	interface
!	CISCO2911/K9 sn	GigabitEthernet0/0.99
!	FTX15248C2Z-	encapsulation dot1Q 99
!	!	ip address 10.10.99.1
enable password admin123	!	255.255.255.0
!	!	!
!	!	interface GigabitEthernet0/1
ip dhcp excluded-address	!	no ip address
10.10.10.1 10.10.10.20	!	duplex auto
ip dhcp excluded-address	!	speed auto
10.10.20.1 10.10.20.20	!	shutdown
ip dhcp excluded-address	!	!
10.10.30.1 10.10.30.20	!	interface GigabitEthernet0/2
ip dhcp excluded-address	!	no ip address
10.10.99.1 10.10.99.20	ip domain-name xpon.local	duplex auto
!	!	speed auto
ip dhcp pool	!	shutdown
VLAN10_ONU1	spanning-tree mode pvst	!
network 10.10.10.0	!	interface Vlan1
255.255.255.0	!	no ip address
default-router 10.10.10.1	!	shutdown
ip dhcp pool	!	!
VLAN20_ONU2	!	ip classless
network 10.10.20.0	!	!
255.255.255.0	interface GigabitEthernet0/0	ip flow-export version 9
default-router 10.10.20.1	no ip address	!
ip dhcp pool	ip access-group 100 in	!
VLAN30_ONU3	duplex auto	ip access-list standard
network 10.10.30.0	speed auto	MGMT_SSH_ONLY
255.255.255.0	!	permit 10.10.99.0 0.0.0.255
default-router 10.10.30.1	interface	deny any
ip dhcp pool	GigabitEthernet0/0.10	access-list 100 deny ip
VLAN99_MGMT	encapsulation dot1Q 10	10.10.10.0 0.0.0.255
network 10.10.99.0	ip address 10.10.10.1	10.10.20.0 0.0.0.255
255.255.255.0	255.255.255.0	access-list 100 deny ip
default-router 10.10.99.1	!	10.10.10.0 0.0.0.255
!	interface	10.10.30.0 0.0.0.255
!	GigabitEthernet0/0.20	access-list 100 deny ip
!	encapsulation dot1Q 20	10.10.20.0 0.0.0.255
ip cef		10.10.10.0 0.0.0.255

```

access-list 100 deny ip
10.10.20.0 0.0.0.255
10.10.30.0 0.0.0.255
access-list 100 deny ip
10.10.30.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 100 deny ip
10.10.30.0 0.0.0.255
10.10.20.0 0.0.0.255
access-list 100 permit ip
any any
!
!
!
!
!
logging 10.10.99.21
line con 0
!
line aux 0
!
line vty 0 4
access-class
MGMT_SSH_ONLY in
login local
transport input ssh
!
!
!
end

!
version 15.0
no service timestamps log
datetime msec
no service timestamps
debug datetime msec
no service password-
encryption
!
hostname Spliter
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend
system-id
!
interface FastEthernet0/1

switchport access vlan 10
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 99
switchport mode access
!
interface FastEthernet0/5
switchport mode access
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23

!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end

```