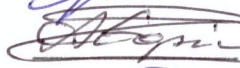


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

Пояснювальна записка

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту мережі
регіонального Інтернет-провайдера побудованої на базі
протоколу BGP»

Виконала студентка 4-го курсу, групи КБ-1
спеціальності 125 «Кібербезпека»

		Колощук М.С.
Керівник		Єфіменко А.А.
Рецензент		Россінський Ю.М.

Житомир – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

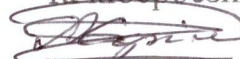
Спеціальність 125 «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії

та кібербезпеки

 Єфіменко А. А.

«12» квітня 2021 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студентки **Колощук Марії Сергіївни**

Тема роботи: **Проект підсистеми захисту мережі регіонального інтернет-провайдера побудованої на базі протоколу BGP**

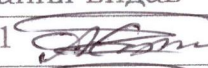
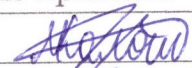
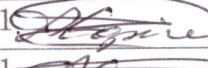
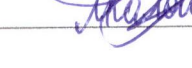
Затверджена Наказом університету від «12» квітня 2021 р. № 134/С

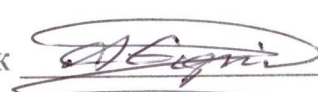
Термін здачі студентом закінченої роботи – «18» червня 2021р.

Вихідні дані для роботи:

1. Логічна топологія мережі
2. Маршрутизатори Cisco
3. Віртуальна машина vRIN
4. Графічний симулятор мереж GNS3

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	2.03.21 	2.03.21 
2	Єфіменко А.А.	6.04.21 	6.04.21 
3	Єфіменко А.А.	4.05.21 	4.05.21 

Керівник  Єфіменко А.А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка задачі. Пошук, огляд та аналіз аналогічних розробок. Формулювання технічного завдання. Опрацювання літературних джерел.	2 березня 2021 – 5 квітня 2021	Виконано
2	Проектування структури системи	6 квітня 2021 – 12 квітня 2021	Виконано
3	Налаштування мережі	13 квітня 2021 – 26 квітня 2021	Виконано
4	Тестування мережі	27 квітня 2021 – 4 травня 2021	Виконано
5	Захист	23 червня 2021	

Студент

Керівник

Колощук М.С.

Єфіменко А.А.

РЕФЕРАТ

Випускна кваліфікаційна робота бакалавра складається з проекту захищеної мережі Інтернет-провайдера та пояснювальної записки. Пояснювальна записка до випускної роботи містить 44 сторінки, 40 ілюстрацій та 1 таблицю.

Метою роботи є розробка проекту підсистеми захисту мережі регіонального Інтернет-провайдера побудованої на базі протоколу BGP.

В роботі визначено основні завдання на розробку мережі, проаналізовано інформацію яка буде використана для проектування мережі регіонального Інтернет-провайдера. Представлено сценарії налаштування мереж, опис протоколів та топологій, які будуть використані протягом всієї роботи. Також наводиться результати тестування мережі.

КЛЮЧОВІ СЛОВА: МЕРЕЖА, ЗАХИСТ, НАЛАШТУВАННЯ, ПРОТОКОЛ, ТОПОЛОГІЯ, ІНТЕРНЕТ-ПРОВАЙДЕР.

					КІК.КР.Б -125-08-ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту мережі регіонального інтернет-провайдера побудованої на базі протоколу BGP		
Розроб.		М. С. Колошук		23.06.11			
Керівник		А. А. Єфіменко		23.06.11			
н. контр.		Росінський Ю.М.		23.06.11			
Зав. каф.		А. А. Єфіменко		23.06.11	Пояснювальна записка		

Літ.	Арк.	Аркушів
	4	71

Житомирська політехніка,
 група КБ-1

ABSTRACT

The bachelor's thesis consists of a project of a secure network of the Internet provider and an explanatory note. The explanatory note to the thesis contains 44 pages, 40 illustrations and 1 table.

The purpose of the work is to develop a project of the subsystem of network protection of the regional Internet provider built on the basis of the BGP protocol.

The main tasks for network designing are defined in the work, the information which will be used for designing of a network of the regional Internet provider is analyzed. Network configuration scenarios, descriptions of protocols and topologies that will be used throughout the work are presented. The results of network testing are also given.

KEYWORDS: NETWORK, PROTECTION, SETTINGS, PROTOCOL, TOPOLOGY, INTERNET ISP.

					KIK.KP.Б -125-08-ПЗ	
						5

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ФУНКЦІОНУВАННЯ ТА БЕЗПЕКИ ПРОТОКОЛУ BGP.....	10
1.1. ЗАГАЛЬНІ ПРИНЦИПИ ПОБУДОВИ МЕРЕЖІ ІНТЕРНЕТ	10
1.2. ПРИНЦИПИ ФУНКЦІОНУВАННЯ ПРОТОКОЛУ BGP	13
1.3. ПРОБЛЕМИ БЕЗПЕКИ ПРОТОКОЛУ BGP	18
1.4. АНАЛІЗ МЕТОДІВ ІНСТРУМЕНТІВ ПРОВЕДЕННЯ АТАК НА ПРОТОКОЛ BGP	20
РОЗДІЛ 2. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ РЕГІОНАЛЬНОГО ІНТЕРНЕТ-ПРОВАЙДЕРА.....	22
2.1. РОЗРОБКА ПРОЕКТУ ЗАГАЛЬНОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ІНТЕРНЕТ- ПРОВАЙДЕРА	22
2.2. РОЗРОБКА СХЕМИ АДРЕСАЦІЇ МЕРЕЖІ ІНТЕРНЕТ-ПРОВАЙДЕРА	26
2.3. РОЗРОБКА ПІДСИСТЕМИ ЗАХИСТУ	31
РОЗДІЛ 3. ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ МЕРЕЖІ ТА ПІДСИСТЕМИ ЗАХИСТУ	33
3.1. ВИБІР ОБЛАДНАННЯ ТА ПЗ ПРИСТРІЙ В МЕРЕЖІ.....	33
3.2. БАЗОВЕ НАЛАШТУВАННЯ ПРИСТРОЇВ МЕРЕЖІ	34
3.3. НАЛАШТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ	39
3.4. ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ	41
ВИСНОВКИ.....	44
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	45
ДОДАТКИ.....	47

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

BGP – Border Gateway Protocol.

AS – Автономна система.

TCP – Transmission Control Protocol.

RFC – Request for Comments.

IGP – Interior Gateway Protocols.

RIR – Regional Internet Registry.

IP – Internet Protocol.

ACL – Access Control List.

ICANN – Internet Corporation for Assigned Names and Numbers

IPsec - IP Security.

VPN - Virtual Private Network

WAN – Wide Area Network

LAN – Local Area Network

OSPF – Open Shortest Path First

ВСТУП

Інтернет - це глобальна комп'ютерна мережа, що охоплює весь світ. На сьогоднішній день Інтернет має близько 15 мільйонів абонентів у понад 150 країнах світу. Розмір мережі щомісяця збільшується на 7-10%. Інтернет утворює своєрідне ядро, яке пов'язує різні інформаційні мережі, що належать різним установам по всьому світу, одне з одним.

Якщо раніше мережа використовувалась виключно як засіб передачі файлів та повідомлень електронної пошти, то сьогодні вирішуються більш складні проблеми розподіленого доступу до ресурсів. Близько двох років тому були створені оболонки, які підтримують функції мережевого пошуку та доступу до розподілених інформаційних ресурсів, електронних архівів.

Інтернет, який колись служив виключно для дослідницьких та освітніх груп, інтереси яких поширювалися на доступ до суперкомп'ютерів, стає все більш популярним у світі бізнесу.

Компанії спокушає швидкість, дешеве глобальне підключення, простота співпраці, доступне програмне забезпечення та унікальна Інтернет-база даних. Вони розглядають глобальну мережу як додаткову до своїх власних локальних мереж.

Інтернет та безпека інформації несумісні за самою природою Інтернету. Вона народилася як суто корпоративна мережа, однак на даний момент, використовуючи єдиний стек протоколів TCP / IP та єдиний адресний простір, вона об'єднує не лише корпоративні та відомчі мережі (освітні, державні, комерційні, військові тощо), які за визначенням мережі з обмеженим доступом, але також звичайні користувачі, які мають можливість отримати прямий доступ до Інтернету зі своїх домашніх комп'ютерів за допомогою модемів та телефонної мережі загального користування.

Як відомо, чим легше отримати доступ до Інтернету, тим гірша його інформаційна безпека, отже, ми можемо твердо сказати, що початкова простота доступу до Інтернету гірша за крадіжку, оскільки користувач може навіть не

знати, що він скопіював файли та програми, не кажучи вже про можливість пошкодження та коригування.

Плата за користування Інтернетом - це загальне зниження інформаційної безпеки.

Безпека даних - одна з головних проблем в Інтернеті. З'являється все більше і більше страшних історій про те, як комп'ютерні хакери, використовуючи дедалі складніші техніки, проникають у бази даних інших людей. Звичайно, нічого з цього не сприяє популярності Інтернету в ділових колах. Сама думка про те, що деякі хулігани або, що ще гірше, конкуренти зможуть отримати доступ до архівів комерційних даних, змушує керівників корпорацій відмовлятися від використання відкритих інформаційних систем. Експерти стверджують, що подібні побоювання є безпідставними, оскільки компанії, які мають доступ як до відкритих, так і до приватних мереж, мають майже рівні шанси стати жертвами комп'ютерного терору.

Метою випускної роботи є проектування захищеної мережі Інтернет-провайдера.

Встановлена мета обумовлює наступні завдання:

- проведення аналізу роботи протоколу BGP;
- визначення архітектури та загальної структури мережі;
- обґрунтування та вибір засобів реалізації мережі;
- розробка захищеної мережі Інтернет-провайдера;
- базове налаштування мережі та налаштування захисту мережі;
- тестування та перевірка налаштування мережі.

Об'єктом дослідження є процес проектування мережі.

Предметом дослідження є використання рушія GNS3 для проектування захищеної мережі Інтернет-провайдера.

В роботі було використано протокол BGP.

Розроблена система може бути використана для реалізації в реальному житті.

Пояснювальна записка до випускної роботи містить 58 сторінок, 37 ілюстрацій та 1 таблиця, список літературних джерел містить 21 найменування.

					КІК.КР.Б -125-08-ПЗ	
						9

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ФУНКЦІОНУВАННЯ ТА БЕЗПЕКИ ПРОТОКОЛУ BGP

Загальні принципи побудови мережі Інтернет

Інтернет - це глобальна мережа, що складається з безлічі автономних мереж, об'єднаних між собою на добровільних засадах. Він працює без центрального керівного органу. Технічна підтримка та стандартизація основних протоколів (IPv4 та IPv6) - це діяльність Інженерної групи Інтернету (IETF), некомерційної організації, що складається з вільно пов'язаних міжнародних учасників, з якими може співпрацювати будь-який бажаючий, вносячи свій технічний досвід. Для забезпечення сумісності основного простору імен Інтернету адмініструються Інтернет-корпорацією з присвоєння імен і номерів. (ICANN). ICANN управляється міжнародною радою директорів, що складається з представників технічних, ділових, академічних та інших некомерційних спільнот Інтернету. ICANN координує присвоєння унікальних ідентифікаторів для використання в Інтернеті, включаючи доменні імена, IP-адреси, номери портів додатків в транспортних протоколах і багато інших параметрів. Глобально уніфікований простір імен необхідний для підтримки глобального охоплення Інтернету.

Регіональні інтернет-реєстри (RIR) були створені для п'яти регіонів світу. Інформаційний центр Африканської мережі (AfriNIC) для Африки, американський реєстр для Internet Numbers (ARIN) для Північної Америки, Азіатсько-Тихоокеанський мережевий інформаційний центр (APNIC) для Азії і Тихоокеанського регіону, Інтернет - адреса реєстру (LACNIC) для Латинської Америки і Карибського басейну Réseaux IP Européens, Мережевий координаційний центр (RIPE NCC) для Європи, Близького Сходу і Центральної Азії. Було доручено призначати блоки IP-адрес та інші параметри Інтернету місцевим реєстрам, таким як провайдери Інтернет-послуг, з певного пулу адрес, виділеного для кожного регіону.

Комунікаційна інфраструктура Інтернету складається з його апаратних компонентів і системи програмних рівнів, які управляють різними аспектами

архітектури. Як і будь-яка комп'ютерна мережа, Інтернет фізично складається з маршрутизаторів, носіїв, ретрансляторів, модемів і т. д. Як приклад міжмережевої взаємодії, деякі з вузлів не обов'язково є інтернет-обладнанням як таким. Інтернет-пакети переносяться іншими повноцінними мережевими протоколами, при цьому Інтернет діє як однорідний мережевий стандарт, який працює на різнопрофільному обладнанні, причому пакети направляються до місця призначення за допомогою IP-маршрутизаторів.

Інтернет-провайдери (ISP) встановлюють всесвітнє з'єднання між різними мережами на різних рівнях. Кінцеві користувачі, які виходять в Інтернет тільки тоді, коли це необхідно для виконання функції або отримання інформації, представляють нижню частину ієрархії маршрутизації. На вершині ієрархії маршрутизації знаходяться мережі рівня 1, великі телекомунікаційні компанії, які обмінюються трафіком один з одним через високошвидкісні оптоволоконні кабелі – регулюються угодами про піринг. Мережі 2 рівня і нижче купують інтернет-трафік у постачальників, та беруть участь в пірингу. Інтернет-провайдер може користуватись послугами провайдера 1 рівня для підключення або реалізувати множинної адресації для досягнення балансування навантаження.

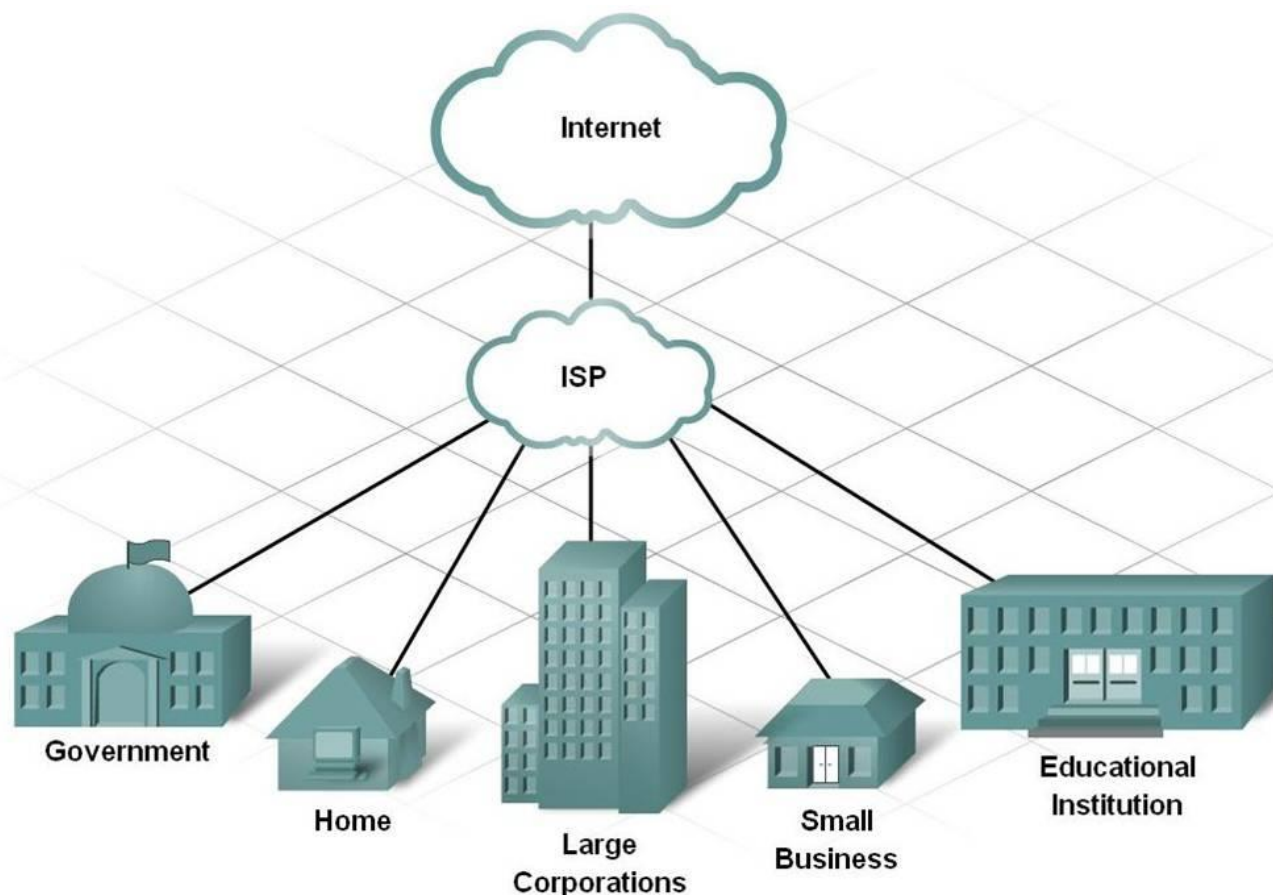


Рисунок 1.1. – Представлення роботи ISP

Звичайні методи доступу користувачів до Інтернету включають комутоване з'єднання з комп'ютерним модемом по телефонних каналах, широкосмуговий зв'язок по коаксіальному кабелю, оптоволоконному чи мідному кабелю, Wi-Fi, супутникову та стільникову технологію (наприклад, 3G, 4G, 5G). Доступ в Інтернет часто можна отримати з комп'ютерів в бібліотеках та Інтернет-кафе. Точки доступу до Інтернету є в багатьох громадських місцях, таких як зали аеропортів і кафе. У багатьох готелях також є громадські точки доступу, які зазвичай платні. Ці точки доступу широко доступні для різних цілей, таких як бронювання квитків, банківські перекази або онлайн-оплата. Wi-Fi забезпечує мобільний доступ в Інтернет через локальні комп'ютерні мережі. До точки доступу відносяться Wi-Fi в кафе, куди користувачам необхідно підключити свої бездротові пристрої, такі як ноутбук або мобільний пристрій. Ці послуги можуть бути безкоштовними для всіх або безкоштовними тільки для клієнтів.

Принципи функціонування протоколу BGP

Протокол граничного шлюзу (BGP) - це поштова служба Інтернету. Коли хтось кидає лист в поштову скриньку, поштова служба обробляє цей лист і вибирає швидкий і ефективний маршрут для доставки цього листа адресата. Так само, коли хтось відправляє дані через Інтернет, BGP відповідає за моніторинг всіх доступних шляхів, за якими можуть переміщуватись дані, і вибір найкращого маршруту, що зазвичай означає переміщення між автономними системами.

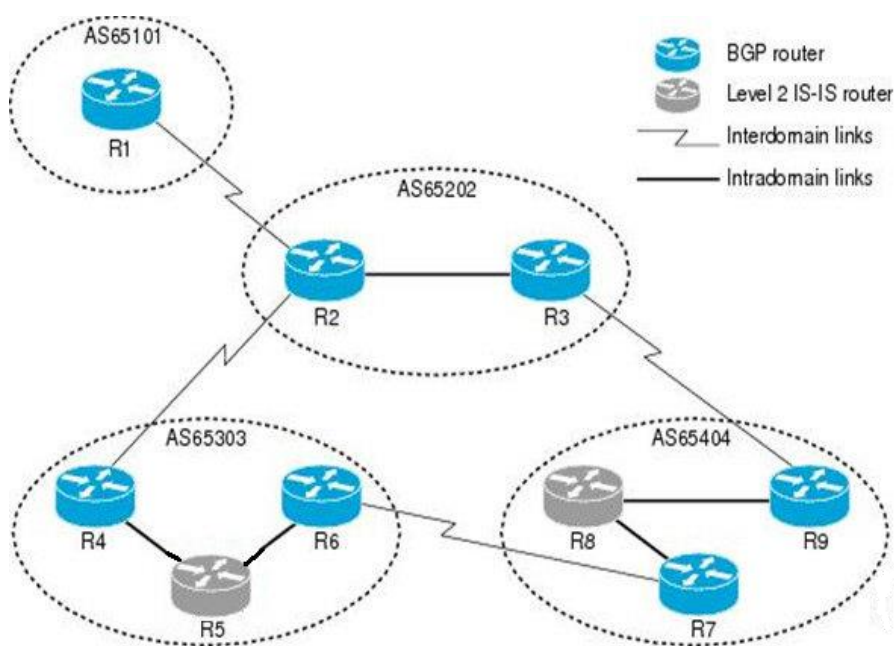


Рисунок 1.2. – Представлення роботи протоколу BGP

Протокол BGP, визначений у стандарті RFC 1771, дозволяє створювати ефективну міждоменну маршрутизацію між автономними системами (AS). AS - це набір маршрутизаторів під єдиним технічним управлінням. Маршрутизатор в AS можуть використовувати кілька протоколів внутрішнього шлюзу (IGP) для обміну маршрутною інформацією всередині AS. Маршрутизатор може використовувати протокол зовнішнього шлюзу для маршрутизації пакетів за межі AS.

BGP використовує TCP в якості транспортного протоколу на порту 179. Два маршрутизатора BGP утворюють TCP-з'єднання між собою. Ці маршрутизатори є одноранговими маршрутизаторами. Однорангові

маршрутизатори обмінюються повідомленнями, щоб відкрити і підтвердити параметри з'єднання.

Маршрутизатор BGP обмінюються інформацією про доступність мережі. Ця інформація в основному вказує на повні шляхи, які повинен пройти пакет, щоб досягти мережі призначення. Шляхи - це номери AS BGP. Ця інформація допомагає в побудові графа автономних систем. Графік також показує, де застосовувати політики маршрутизації, щоб накласти деякі обмеження на маршрутизацію.

Будь-які два маршрутизатора, які утворюють TCP-з'єднання для обміну інформацією маршрутизації BGP, є «одноранговими вузлами» або «сусідами».

1. Однорангові вузли BGP спочатку обмінюються повними таблицями маршрутизації BGP.
2. Після цього обміну однорангові вузли відправляють інкрементні оновлення по мірі зміни таблиці маршрутизації.
3. BGP зберігає номер версії таблиці BGP.
4. Номер версії однаковий для всіх вузлів BGP.
5. Номер версії змінюється щоразу, коли BGP оновлює таблицю зі змінами маршрутної інформації.
6. Відправка пакетів KEEPALIVE гарантує, що з'єднання між однорангових вузлів BGP жваво.
7. Пакети повідомлень відправляються у відповідь на помилки або особливі умови [1].

Формат заголовка повідомлення в BGP є поле маркера завдовжки 16 байт, за яким слідує поле довжини (2 байта), поле типу (1 байт). На рисунку 1.3. представлений формат заголовка повідомлення протоколу BGP.

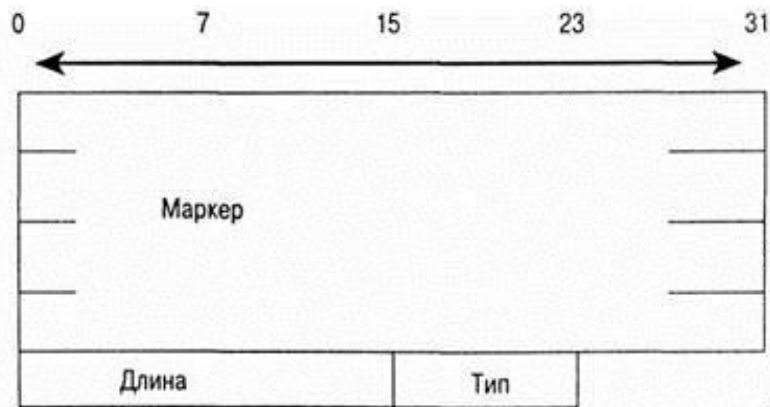


Рисунок 1.3. - Формат BGP-повідомлень про зміни маршрутів

Залежно від типу повідомлення в протоколі BGP за заголовком може слідувати або не слідувати блок даних. Так, наприклад, повідомлення KEEPALIVE складаються тільки з заголовку і даних не передають.

Поле маркера завдовжки 16 байт використовується для аутентифікації вхідних повідомлень BGP або для детектування втрати синхронізації між двома взаємодіючими по BGP маршрутизаторами.

Поле маркера буває двох форматів:

- Якщо надіслано повідомлення типу OPEN або в ньому відсутня інформація про аутентифікацію, то в поле маркера всі позиції позначаються 1.
- В іншому випадку значення поля маркера обчислюється відповідно до застосованих механізмів аутентифікації.

Поле розміром 2 байти використовується для відображення повної довжини повідомлення BGP, включаючи заголовок. Найменша довжина повідомлення BGP становить 19 байт ($16 + 2 + 1$), а найбільша - 4096 байт.

Поле типу розміром 1 байт визначає тип повідомлення. Можливі такі значення:

- OPEN (Відкриття з'єднання).
- UPDATE (Оновлення маршрутної інформації).
- NOTIFICATION (Повідомлення про помилку).
- KEEPALIVE (Перевірка стану з'єднання) [13].

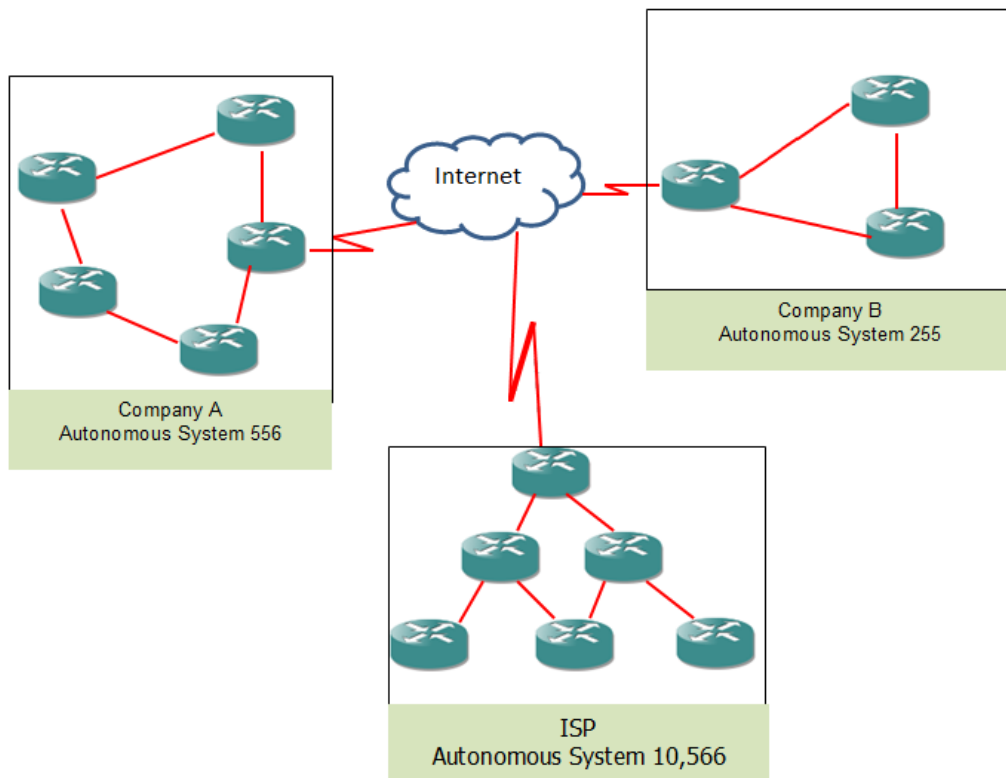


Рисунок 1.4. - Клієнти або корпоративні мережі, що підключаються через BGP

З накопиченням практичного досвіду BGP зросло усвідомлення його слабких місць та недоліків. BGP містить загальні технічні специфікації та стандарти Інтернету, інформаційні файли. Існує розуміння того, що BGP є єдиним інструментом маршрутизації між автономними системами та повинна забезпечувати якомога більшу доступність, в тому числі, у разі нападу або збої.

Отже, відповідно до таких вимог, для збільшення доступності, більшість розширень BGP, направлені для зменшення складності управління та налаштування маршрутних таблиць BGP, які найбільш схильні до несподіваних збоїв, і беручи до уваги дедалі складнішу топологію мережі та стратегію розподілу, нестабільність маршрутизації також може бути зменшена.

Іншими аспектами безпеки, тема яких піднімається в RFC, можна назвати цілісність та правильність інформації щодо маршрутизації. Існує три наступні групи «відсутностей», які впливають на роботу протоколу.

1. Відсутність аутентифікації повідомлень BGP, що не забезпечують цілісність, аутентифікацію та динамічну перевірку даних BGP в повідомленнях BGP: повідомлення BGP можуть бути підроблені, змінені, видалені або ретрансльовані випадково вузлом чи навіть навмисно сторонньою особою.

2. Відсутність перевірки повноважень мережесих (префіксних) оголошень: будь-який BGP користувач може оголосити маршрут до будь-якого префіксу.

3. Відсутність перевірки аутентичності шляху автономної системи і атрибутів шляху: сам шлях і його окремі атрибути можуть бути змінені під час стрибків оголошення [4].

Сусіди BGP, називаються одноранговими вузлами, встановлюються між маршрутизаторами шляхом ручного налаштування для створення сеансу TCP на порту 179. Вузол BGP відправляє 19-байтові повідомлення KEEPALIVE кожні 60 секунд [5] для підтримки з'єднання [6]. Серед протоколів маршрутизації BGP унікальний тим, що використовує TCP в якості транспортного протоколу.

Коли BGP працює між двома одноранговими вузлами в одній і тій же автономній системі (AS), він називається внутрішнім BGP (i-BGP або протокол внутрішнього граничного шлюзу). Коли він працює між різними автономними системами, він називається External BGP (eBGP або протокол зовнішнього граничного шлюзу). Маршрутизатор на кордоні однієї AS, що обмінюються інформацією з іншого AS, називаються граничними (граничними маршрутизаторами) або просто одноранговими вузлами eBGP і зазвичай підключаються безпосередньо, до однорангових вузлів i-BGP можуть бути взаємопов'язані через інші проміжні маршрутизатори. Інші топології розгортання також можливі, наприклад, запуск пірінгу eBGP всередині тунелю VPN, що дозволяє двом віддаленим сайтам обмінюватися маршрутною інформацією безпечним і ізольованим чином.

Основна відмінність пірінгу iBGP і eBGP полягає в тому, як маршрути отримані від одного однорангового вузла, поширюються на інші однорангові вузли. Наприклад, нові маршрути, отримані від однорангового вузла eBGP, зазвичай перерозподіляються всім одноранговим вузлам iBGP, а також всім іншим одноранговим вузлам eBGP (якщо на маршрутизаторі включений транзитний режим). Однак, якщо нові маршрути вивчаються в пірінгу iBGP, вони повторно оголошуються тільки всім одноранговим вузлам eBGP. Ці

правила поширення маршруту фактично вимагають, щоб всі однорангові вузли iBGP всередині AS були з'єднані між собою в повну сітку.

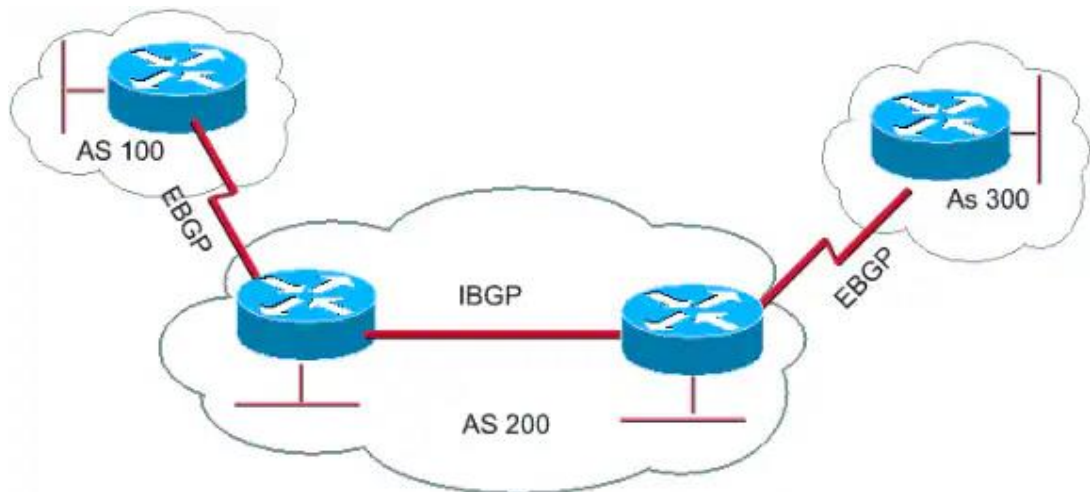


Рисунок 1.5. - Принципи роботи пірингу iBGP і eBGP

Відслідковувати маршрути, можна контролювати за допомогою механізму карт маршрутів. Цей механізм складається з набору правил. Кожне правило описує для маршрутів, що відповідають певним критеріям, які дії слід зробити. Дія може полягати в відкиданні маршруту або в зміні деяких атрибутів маршруту перед його вставкою в таблицю маршрутизації.

Проблеми безпеки протоколу BGP

Проблема з BGP полягає в тому, що протокол не включає безпосередньо механізми безпеки і в основному заснований на довірі між операторами мережі, що вони надійно захищають свої системи і надсилатимуть коректні дані. Однак трапляються помилки і можуть виникнути проблеми, якщо зловмисники намагаються вплинути на таблиці маршрутизації, що використовуються BGP.

Наступні класи загроз представляють класи противників, які розглядаються як такі, що мають відношення до цього середовища:

- Оператори мережі
- Хакери
- Злочинці
- Реєстри
- Держава

Оператори мережі

Оператор мережі може представляти загрозу. Оператор може змусити маршрутизатори BGP, які він контролює, відправляти повідомлення про оновлення з неточною інформацією про маршрутизацію, наприклад, викликати потік трафіку по шляхах, які є економічно вигідними для оператора. Такі оновлення можуть вплинути на потік трафіку через шляхи, які в іншому випадку будуть відхилені як менш вигідні іншими операторами мережі. Оскільки оператор контролює маршрутизатори BGP у своїй мережі, він може змінювати їх роботу довільними способами.

Хакери

Хакер може взяти під свій контроль комп'ютери управління мережею та маршрутизатори, керовані операторами. У таких випадках хакери могли б виступати в ролі зловмисних операторів мережі. Передбачається, що хакери, як правило, не мають можливості здійснювати атаки на більшість каналів між мережами (посилання, що використовуються для передачі BGP та абонентського трафіку). Хакер може бути завербований злочинцями або державами для дії від їх імені.

Злочинці

Злочинці можуть переконати (за допомогою погроз або вимагання) оператора мережі виступити в ролі оператора-шахрая і таким чином мати можливість здійснювати широкий спектр атак. Злочинці можуть переконати співробітників оператора телекомунікацій дозволити атаки на трафік між маршрутизаторами. Зловмисники також можуть маніпулювати маршрутом, щоб приховати джерела спаму, DoS-атаки або інші злочинні дії.

Реєстри

Співробітники реєстру можуть маніпулювати вмістом сховища або керувати сертифікатами, які вони видають. Ці дії можуть негативно вплинути на оператора мережі або клієнта оператора мережі.

Держава

Держава може контролювати одного або декількох мережевих операторів, які працюють в країні та змусити їх діяти як неправдиві. Держава має технічно активну можливість прослуховування (наприклад, на її території), яка дозволяє їй здійснювати атаки на міжмережний трафік. Цю можливість може спричинити контроль або вплив на постачальника телекомунікаційних послуг, що працює в межах країни. Він має можливість атакувати та контролювати маршрутизатори або керувати мережевими обладнанням операторів в інших країнах. Держава може контролювати реєстр (наприклад, RIR), який функціонує на її території, і може змусити цей реєстр діяти неправомірно.

Аналіз методів інструментів проведення атак на протокол BGP

Щоб захиститись атак типу "зловмисник в середині" і запобігти штучне додавання незаконних маршрутів в таблиці в злочинних цілях. Використовуючи кілька функцій безпеки в BGP, можна значно знизити вразливість BGP для атак зловмисників.

Методи захисту від атак типу "зловмисник в середині"

- MESSAGE DIGEST v5
- Ефективна політика маршрутів

MESSAGE DIGEST v5

Налаштування ключа Message Digest на сусідніх маршрутизаторах дозволяє аутентифікувати BGP повідомлення, виходячи з дійсного джерела. Хеш-ключ MD5 важко зламати і майже неможливо підробити в реальному часі за допомогою сучасних технологій. Увімкнений MD5 в повідомленнях про маршрути BGP. Маршрутизатори повинні бути попередньо налаштовані з правильними значеннями хешу та ключів, однак це робить мережу набагато безпечнішою від зловмисного використання маршруту, оскільки ключі ніколи не передаються по мережі.

Ефективна політика маршрутів

Встановлення політики маршруту значно допомагає подолати зовнішні загрози на додаток до запобігання навантаження, циклів маршрутизації та інших аномалій мережі.

1. Створення фільтрів входу та виходу.
2. Блокувати адреси, які не можна маршрутизувати (Loopback та приватні адреси).
3. Блокувати IP-адреси спеціального / експериментального використання.
4. Блокувати відомих порушників проблем:
 - Блокувати будь-які пакети, що отримують IP-адреси поза межами мережі.
 - Адреси домашніх комутованих, кабельних і DSL-модемів.
 - Деякі іноземні адреси в певних країнах.
5. Налаштовані нульові маршрути у мережі, які скидають трафік, спрямований на недосяжні пункти призначення, у сегмент бітів.

Найкращим варіантом захисту сеансу BGP є:

1. Налаштована ефективна політика маршрутів (наприклад: карти маршрутів Cisco).
2. Списки вхідних та вихідних префіксів, фільтри маршрутів.
3. Встановлені обмеження на максимальну кількість префіксів BGP, прийнятих від кожного партнера.
4. Використання ключів MD5.
5. Налаштування демпфірування маршруту належним чином.
6. Обмеження на максимальну кількість префіксів, прийнятих від кожного однорангового вузла.
7. Додати нульові маршрути в стратегічно розподілених місцях, щоб поганий трафік скидався, як тільки він входить в мережу [7].

РОЗДІЛ 2. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ РЕГІОНАЛЬНОГО ІНТЕРНЕТ-ПРОВАЙДЕРА

2.1. Розробка проекту загальної мережевої інфраструктури Інтернет-провайдера

Серед топологій виділяють такі види:

- Шлюз VPN типу "мережа - мережа" для RAS з BGP на корпоративному сайті ребра
- Сторонній шлюз з BGP на границі сайту підприємства
- Кілька корпоративних сайтів, що підключаються до хмарного центру обробки даних CSP
- Окремі кінцеві точки для BGP і VPN

Шлюз VPN типу "мережа - мережа" для RAS з BGP на корпоративному сайті ребра

У цій топології представлений сайт підприємства, підключений до CSP. Топологія маршрутизації підприємства включає внутрішній маршрутизатор, шлюз RAS сервера Windows Server 2016, налаштований для підключень VPN типу "мережа - мережа" з CSP, і пристрій з граничним брандмауером. Шлюз RAS перериває підключення S2S VPN і BGP.

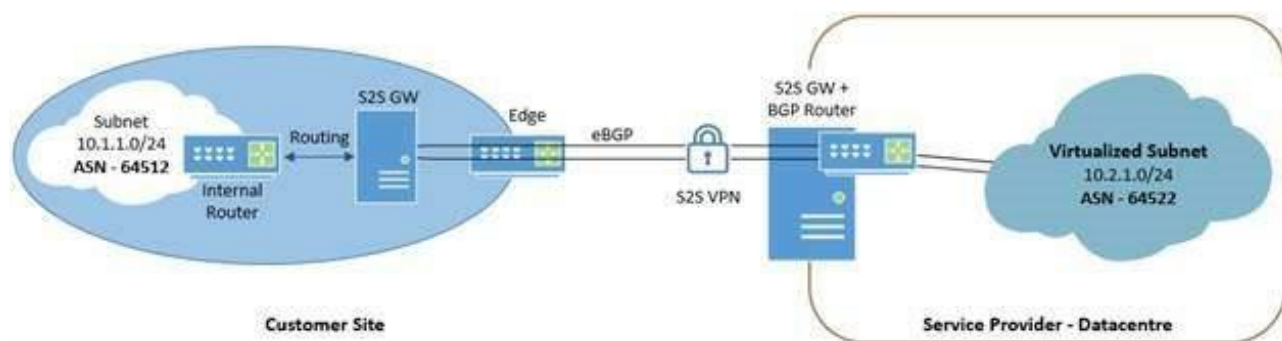


Рисунок 2.1. – Шлюз VPN типу "мережа - мережа" для RAS

Обидва сайти підключаються по протоколу eBGP, який дозволяє передавати дані між маршрутизаторами з підтримкою BGP в окремих автономних системах. Для цього необхідно, щоб у підприємства і CSP були окремі номери автономних систем (ASN), що є невід'ємним параметром протоколу BGP.

У цьому сценарії протокол BGP працює описаним нижче чином.

1. Кінцевий пристрій сайту підприємства визначає маршрути віртуалізованій підмережі (10.2.1.0/24), розміщеної в хмарі, за допомогою BGP. Цей пристрій також оголошує локальні маршрути підмережі (10.1.1.0/24) в багато клієнтський шлюз RAS постачальника служби віддаленого доступу.

2. Кінцевий маршрутизатор клієнта визначає внутрішні локальні маршрути одним із зазначених нижче способів:

- Кінцевий пристрій використовує протокол BGP з внутрішнім маршрутизатором і визначає внутрішні маршрути (в прикладі це 10.1.1.0/24). Тим часом внутрішній маршрутизатор дізнається внутрішні маршрути (наприклад, 10.2.1.0/24) від кінцевого пристрою і повинен надати ці маршрути іншим локальним маршрутизаторам за допомогою протоколу IGP, такого як OSPF або RIP.

- У кінцевому пристрої можна налаштувати статичні маршрути або інтерфейси для вибору маршрутів, які повинні оголошуватися за допомогою BGP. Кінцевий пристрій також повідомляє зовнішні маршрути іншим локальним маршрутизаторам за допомогою IGP.

Сторонній шлюз з BGP на границі сайту підприємства

У цій топології представлений сайт підприємства, який використовує сторонній кінцевий маршрутизатор для підключення до CSP. Кінцевий маршрутизатор також служить шлюзом для міжсайтових підключень VPN.

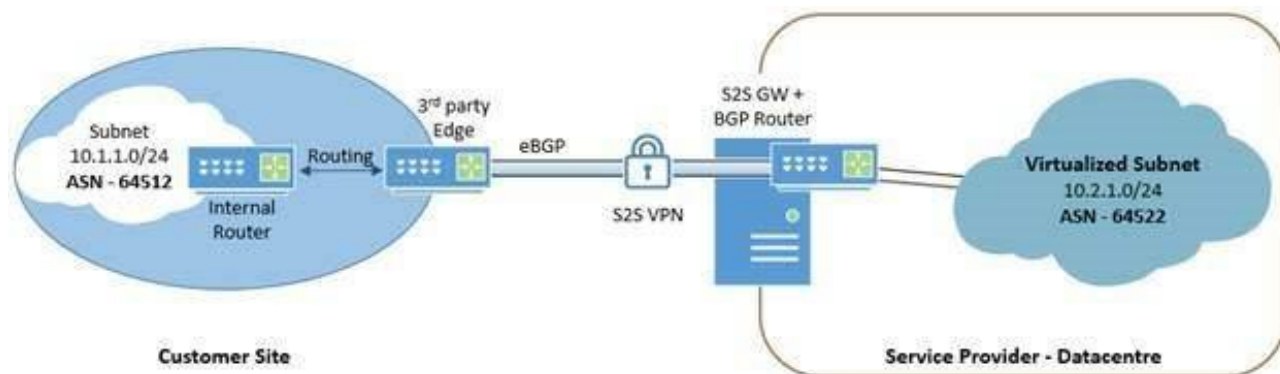


Рисунок 2.2. – Сторонній шлюз з BGP на границі сайту підприємства

Кінцевий маршрутизатор підприємства визначає внутрішні локальні маршрути одним із зазначених нижче способів:

1. Кінцевий пристрій використовує протокол BGP з внутрішнім маршрутизатором і визначає внутрішні маршрути (в прикладі це 10.1.1.0/24).
2. Кінцевий пристрій реалізує протокол IGP і безпосередньо бере участь у внутрішній маршрутизації.

Кілька корпоративних сайтів, що підключаються до хмарного центру обробки даних CSP

У цій топології представлено кілька сайтів підприємства, які використовують сторонні шлюзи для підключення до CSP. Сторонні прикордонні пристрої виступають в ролі шлюзів для міжсайтових підключень VPN і в ролі маршрутизаторів BGP.

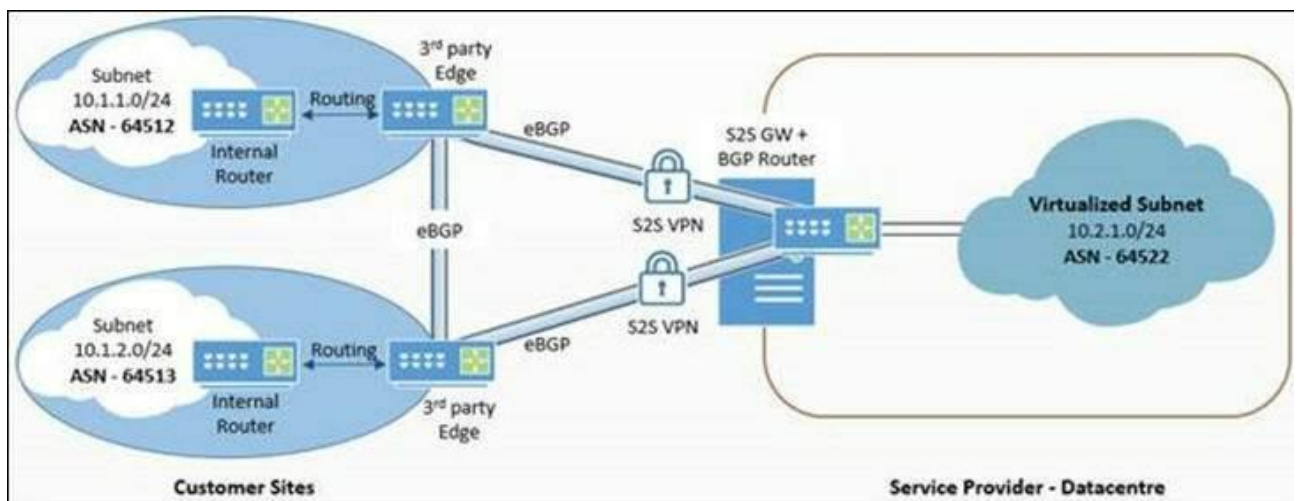


Рисунок 2.3. – Представлення роботи технології

Кінцевий маршрутизатори клієнта визначають внутрішні локальні маршрути одним із зазначених нижче способів.

Кінцевий пристрій використовує протокол BGP з внутрішнім маршрутизатором і визначає внутрішні маршрути (в прикладі це 10.1.1.0/24).

- Кінцевий пристрій реалізує протокол IGP і безпосередньо бере участь у внутрішній маршрутизації.
- Кожен сайт підприємства дізнається маршрути від іншого сайту за допомогою прямого підключення eBGP.

Кожен сайт підприємства отримує відомості про маршрути в розміщеній мережі безпосередньо і від іншого сайту підприємства, а потім вибирає оптимальний маршрут на основі його вартості.

Якщо маршрутизатор BGP на корпоративному сайті 1 не може підключитися до маршрутизатора BGP корпоративного сайту 2 через збій підключення, маршрутизатор BGP сайту 1 динамічно починає вивчати маршрути до мережі корпоративного сайту 2 від маршрутизатора BGP постачальника служб шифрування, а трафік перенаправляється з сайту 1 на сайт 2 через маршрутизатор BGP Windows Server на CSP.

Окремі кінцеві точки для BGP і VPN

У цій топології представлено підприємство, в якому в якості кінцевої точки BGP і кінцевої точки міжсайтових підключень VPN використовуються два різних маршрутизатора. VPN-підключення типу "мережа - мережа" завершується на шлюзі RAS Windows Server 2016, а BGP завершується на внутрішньому маршрутизаторі. На стороні постачальника служб шифрування CSP перериває підключення VPN і BGP до шлюзу RAS. У такій конфігурації обладнання внутрішнього стороннього маршрутизатора має підтримувати повторне поширення маршрутів IGP в BGP, а також повторне розповсюдження маршрутів BGP в IGP.

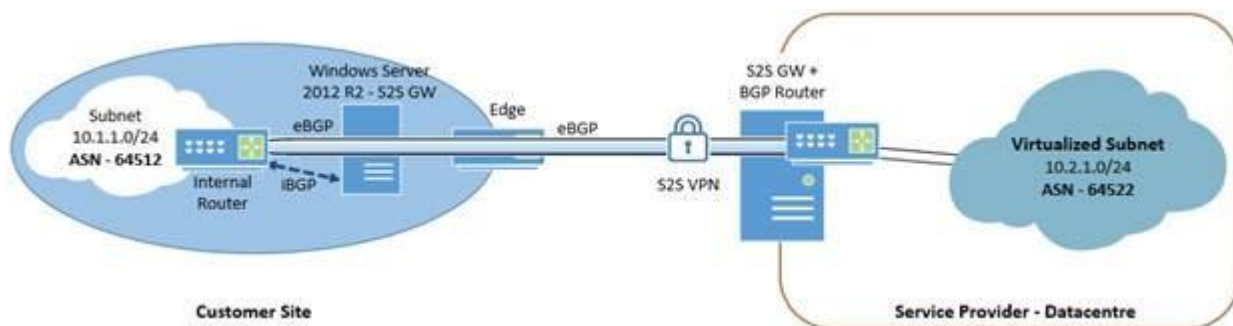


Рисунок 2.4. – Представлення роботи технології

Внутрішній маршрутизатор визначає маршрути пакетів одним із зазначених нижче способів:

- BGP.
- Протокол IGP, наприклад OSPF або RIP.
- Налаштування статичних маршрутів.

При використанні будь-якого протоколу IGP на сайті підприємства внутрішній маршрутизатор повинен повторно поширювати маршрути IGP в BGP, а також повторно поширювати маршрути BGP в IGP для забезпечення

зв'язку між віртуальними мережами CSP і локальними підмережами підприємства.

В цій топології корпоративний шлюз RAS використовує VPN-підключення типу "мережа - мережа" з шлюзом RAS CSP, який надає корпоративний шлюз RAS з маршрутами до шлюзу CSP. Потім внутрішній маршрутизатор підприємства дізнається цей маршрут до шлюзу CSP. Внутрішній маршрутизатор підприємства може встановити сеанс пірингу з маршрутизатором BGP шлюзу віддаленого доступу CSP.

З цього моменту внутрішній маршрутизатор підприємства і шлюз RAS обмінюються відомостями про маршрутизацію. А корпоративний маршрутизатор BGP для RAS вивчає маршрути CSP і корпоративні маршрути, щоб фізично маршрутизувати пакети між мережами [15].

З вище перечилених топологій нам ближче за вибором 1 тополюія. В нашій регіональній мережі є дві автономні системи в одній з яких знаходяться чотири мережі провайдерів. Тому доречно вибрати топологію типу "мережа - мережа".

2.2. Розробка схеми адресації мережі Інтернет-провайдера

Існує багато видів мереж: за розмірами, за призначенням, для того щоб вибрати, яку саме мережу нам потрібно використовувати для створення проекту, потрібно проаналізувати параметри всіх мереж і вибрати, яка підходить для досліджень.

Nanonetwork або нанорозмірних мережа - набір з'єднаних між собою наномашини (пристрої декількох сот нанометрів або кілька мікрометрів самої більший за розміром), які здатні виконувати тільки дуже прості завдання, такі як обчислення, зберігання даних, зондування і приведення в дію. Наномережі, як очікується, розширять можливості окремих наномашин як з точки зору складності, так і діапазону операцій, дозволяючи їм координувати, спільно використовувати і об'єднувати інформацію. Наномережі відкривають нові можливості застосування нанотехнологій в біомедицині, екологічні дослідження, військові технології, промислові і споживчі товари. Зв'язок в наномасштабі визначена в IEEE P1906.1 [17].

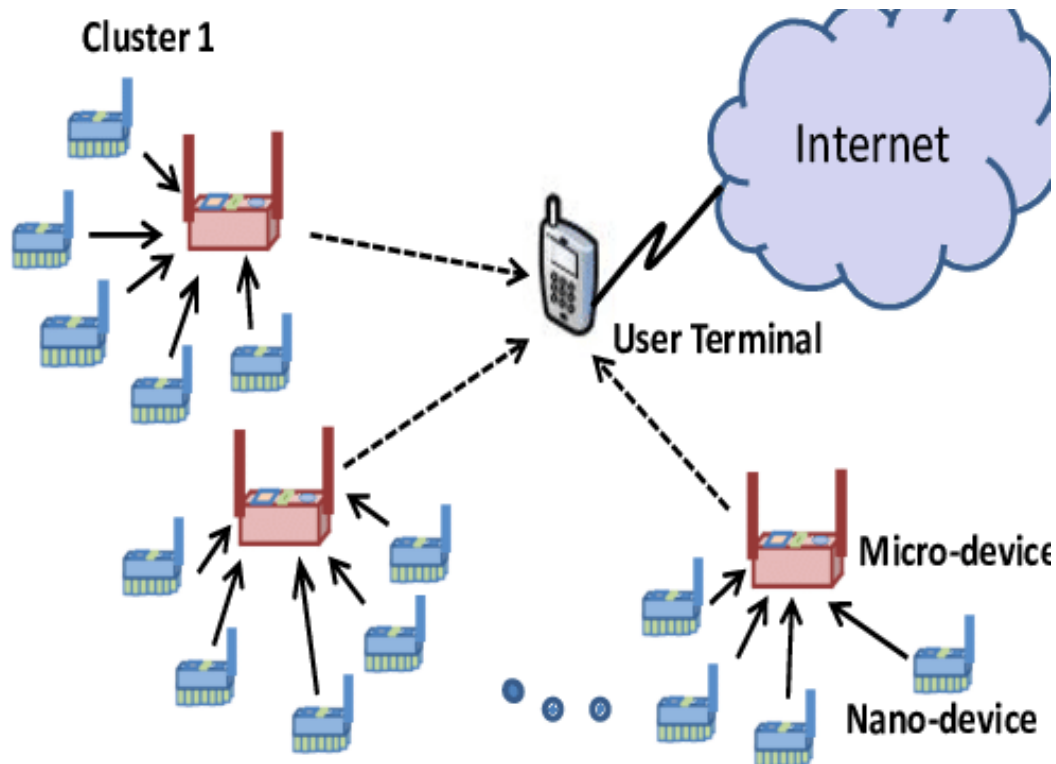


Рисунок 2.5. – Представлення наномережі

Персональна мережа (PAN) є комп'ютерною мережею для з'єднання електронних пристроїв в робочому просторі окремої людини. PAN забезпечує передачу даних між такими пристроями, як комп'ютери, смартфони, планшети і персональні цифрові помічники. PAN можуть використовуватися для зв'язку між самими персональними пристроями або для підключення до мережі більш високого рівня і Інтернету, де один головний пристрій відіграє роль шлюзу.

PAN може бути бездротовим або передаватися через провідні інтерфейси, такі як USB [18].



Рисунок 2.6. – Представлення персональної мережі

Локальна мережа (LAN) являє собою комп'ютерну мережу, яка з'єднує між комп'ютерами в межах обмеженої області, такі як місця проживання, школи, лабораторію, університетське містечко або офісний центр. Навпаки, глобальна мережа (WAN) не тільки покриває більшу відстань, але також зазвичай включає в себе орендовані телекомунікаційні канали.

Ethernet і Wi-Fi - дві найбільш поширені технології, застосовані в локальних мережах. Історичні мережеві технології включають ARCNET, Token Ring і AppleTalk [19].



Рисунок 2.7. – Представлення локальної мережі

Міська мережа (MAN) - це комп'ютерна мережа, яка взаємопов'язує користувачів з комп'ютерними ресурсами в географічному регіоні, розміром із мегаполіс. Термін MAN застосовується до об'єднання локальних обчислювальних мереж в місті в єдину велику мережу, яка потім може також пропонувати ефективне з'єднання з глобальною мережею. Цей термін також використовується для опису взаємозв'язку кількох локальних мереж в мегаполісі за допомогою використання двоточкових з'єднань між ними [20].

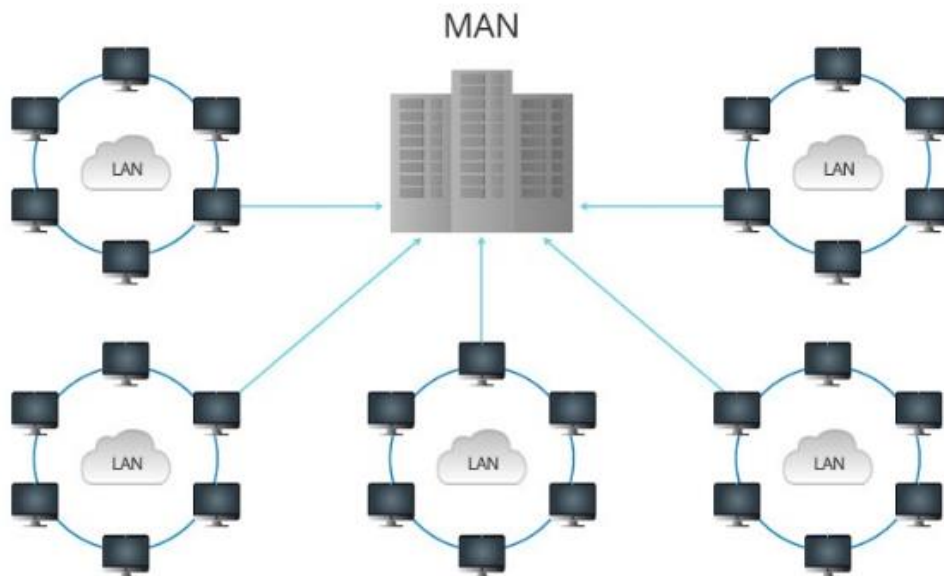


Рисунок 2.8. – Представлення міської мережі

Глобальна мережа (WAN) є телекомунікаційною мережею, яка поширюється на велику область для об'єднання комп'ютерних мереж. Глобальні мережі часто створюються з використанням орендованих телекомунікаційних каналів.

Підприємства, а також школи та державні установи використовують глобальні мережі для передачі даних співробітникам, студентам, клієнтам, покупцям і постачальникам з різних місць по всьому світу. По суті, цей спосіб зв'язку дозволяє бізнесу ефективно виконувати свої повсякденні функції незалежно від місця розташування. Інтернет може розглядатися як WAN.

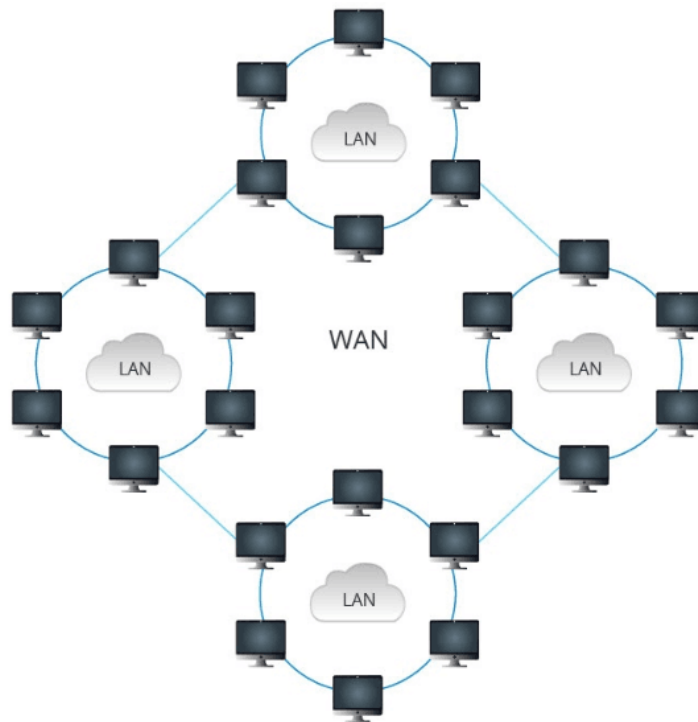


Рисунок 2.9. – Представлення глобальної мережі

При порівнянні всіх вище представлених мереж для подальшого дослідження нам підходить глобальна мережа (WAN). По масштабам вона підходить для представлення регіонального Інтернет-провайдера [19].

2.3. Розробка підсистеми захисту

Серед видів захисту протоколу BGP виділяють такі види:

- Захист користувача BGP
- Захист BGP-сесій
- Префіксна фільтрація

Захист користувача BGP

Вузол BGP захищений від спроб порушити BGP-сесію. Цей захист повинен бути досягнуто за допомогою контролю доступу. Список (ACL), який відкидає всі пакети, спрямовані на TCP-порт 179 на локальний пристрій і отримано з адреси, яка невідома або не дозволена щоб стати сусідом BGP. Стандартний захист, яку повинен пропонувати TCP, не завжди достатньо, тому що злочинці іноді запускаються в програмному забезпеченні рівня управління. За відсутності списків контролю доступу можна атакувати динамік BGP, просто відправивши великий обсяг запитів на підключення до нього.

Якщо підтримується, ACL, що відноситься до площини управління маршрутизатора. Слід використовувати ACL, щоб уникнути конфігурацію фільтрів для даних пакетів, що проходять через маршрутизатор, отже, не досягає рівня управління. Якщо обладнання не може цього зробити, інтерфейси ACL можуть використовуватися для блокування пакетів адресований локальному роутеру.

Деякі маршрутизатори автоматично програмують ACL по протоколу BGP. На інших пристроях ACL повинен бути налаштований і підтримуватись вручну або за допомогою скриптів.

На додаток до фільтрації може бути налаштована обмеження швидкості для прийняття трафіку BGP. Трафік BGP з обмеженням швидкості складається тільки з визначеної кількості біт в секунду. Це захищає BGP площину управління маршрутизатором в разі перевищення кількості трафіку BGP

Захист BGP-сесій

Атаки на сеанси TCP, які використовує BGP (також відомі як сеанси BGP), наприклад, відправка підроблених пакетів TCP RST може порушити пірінг BGP. Після успішної атаки з підміною ARP (або іншої подібної спроби злому) атака по центру, зловмисник може впровадити пакети в потік TCP.

Недоліком захисту TCP-сесії є додаткова настройка. і накладні витрати на управління для підтримки аутентифікації інформації (наприклад, паролі MD5). Захист TCP-сесій використовується BGP, навіть якщо пірінг встановлено через загальні мережі, де можливий спуфінг, але операторам рекомендується враховувати компроміси і застосовувати TCP захист сеансу там, де це необхідно.

Префіксна фільтрація

Основний аспект захисту BGP полягає у контролі префіксів, які отримуються та рекламуються на пірінгах BGP. Префікси, якими обмінюються між рівнем BGP, контролюються за допомогою вхідних та вихідних фільтрів, які можуть відповідати префіксам IP-адреси [14].

РОЗДІЛ 3. ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ МЕРЕЖІ ТА ПІДСИСТЕМИ ЗАХИСТУ

3.1. Вибір обладнання та ПЗ пристрій в мережі

Маршрутизатор повинен містити достатню кількість портів, забезпечувати легке розширення мережі, забезпечувати необхідну швидкість передачі даних та швидкість їх обробки.

Нам потрібен маршрутизатор який би підтримував технології FastEthernet та протокол RIPv2, OSPF та BGP, та містив додаткові функції налаштування. Для заданих критеріїв підходить маршрутизатор Cisco Systems CISCO 7200, рисунок 3.1.



Рисунок 3.1. – Маршрутизатор Cisco Systems CISCO 7200

Серія маршрутизаторів Cisco 7200 розроблена як агрегує пристрій для сервіс-провайдерів і ідеально підходить в якості центрального маршрутизатора (core) або в якості прикордонного маршрутизатора ISP-компаній. Даний маршрутизатор дозволяє обробляти дані, голос, відео з піковою швидкістю 1000000 пакетів в секунду. Як більшість маршрутизаторів Cisco Systems, серія Cisco 7200VXR являється модульною (модулі сумісні з обладнанням серій Cisco 7100, 7400 і 7500); в основне шасі встановлюються модулі з підтримкою різних технологій (модулі портів LAN, WAN, Multichannel і ISDN портів, модулі цифрових голосових портів, SONET / ATM, Mainframe Channel Connection). Устаткування серії Cisco 7200 гарантує високу надійність, відмовостійкість,

підтримку величезного спектру середовищ передачі даних. З метою забезпечення відмовостійкості системи в маршрутизаторах серії Cisco 7200 передбачена можливість підключення двох джерел живлення, а також можливість заміни модулів в гарячому режимі без виключення обладнання.

Для того щоб порівняти налаштування на різних маршрутизаторах та наблизити нашу мережу до реалій нам потрібен ще один маршрутизатор який би підтримував технології FastEthernet та протокол RIPv2, OSPF та BGP, та містив додаткові функції налаштування. Для того щоб порівняти налаштування в різних випадках, виберемо декілька серій маршрутизаторів. Щоб побачити чи якісь відмінності в налаштуваннях. Маршрутизатор Cisco Systems CISCO 7200, рисунок 3.2, оптимальний варіант для великої мережі підприємства чи офісу.



Рисунок 3.2. – Маршрутизатор Cisco Systems CISCO 3725

Cisco 3725. Протокол каналу передачі даних: Ethernet, ATM, ISDN, HSSI, Fast Ethernet, X.25. Архітектура процесора: MIPS, Оперативна пам'ять: 256 МБ. Східний живлення: 135 Вт Требуванія к питанию: 100/240 В переменного тока (50/60 Гц), Скорость передачи данных (макс.): 0,1 Гбіт / с.

3.2. Базове налаштування пристроїв мережі

Під час проектування мережі була розроблена мережа регіонального Інтернет-провайдера.

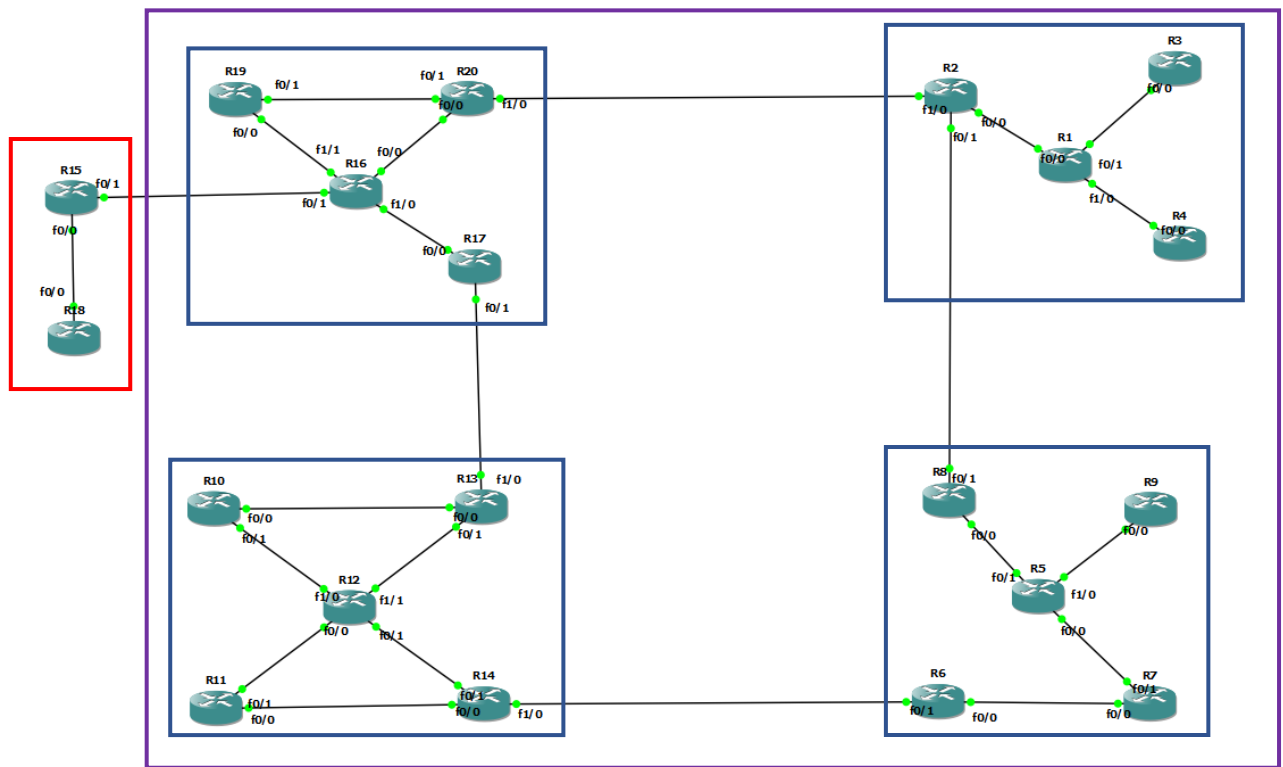


Рисунок 3.3. – Розроблена мережа регіонального Інтернет-провайдера

Мережа складається з 2 автономних систем. Одна з автономних систем складається з 4 мереж провайдера. 2 підмережі поєднуються за допомогою протоколу RIP, а інші 2 підмережі поєднуються протоколом OSPF.

Загалом використовують 20 маршрутизаторів. Проект складається із 23 підмережі. Таблиця підмереж представлена в додатку А.

Кожна з підмереж підключаються однотипно. За допомогою портів Fast Ethernet, маршрутизатори з'єднуються за допомогою витої пари.

Розрахунок IP-адрес для підмереж наведені в додатку А.

Спочатку налаштуємо адресацію маршрутизаторам. Нижче представлено базове налаштування мереж, налаштування представлені на рисунках 3.4 – 3.14. Повністю вся конфігурація представлена в додатку Б.

```

R1
interface FastEthernet0/0
ip address 100.13.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.14.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 100.15.8.2 255.255.255.252
duplex auto
speed auto
!

```

Рисунок 3.4. – Базове налаштування маршрутизатора R1

```

R1#conf ter
Enter configuration commands, one per
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 100.13.8.0
R1(config-router)#network 100.14.8.0
R1(config-router)#network 100.15.8.0
R1(config-router)#exit
R1(config)#exit
R1#
*Jun 19 10:27:45.495: %SYS-5-CONFIG_I:
R1#

```

Рисунок 3.5. – Базове налаштування протоколу RIP маршрутизатора R1

```

R2
!
interface FastEthernet0/0
ip address 100.13.8.1 255.255.255.252
duplex auto
speed auto

```

Рисунок 3.6. – Базове налаштування маршрутизатора R1

```

R2#conf ter
Enter configuration commands, one per
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 100.13.8.0
R2(config-router)#exit
R2(config)#exit

```

Рисунок 3.7. – Базове налаштування протоколу RIP маршрутизатора R4

```

R2#ping 100.15.8.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.15.8.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/251/852 ms
R2#

```

Рисунок 3.8. – Перевірка з'єднання між маршрутизаторами R2 та R4

 R5

```

interface FastEthernet0/0
ip address 100.18.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.16.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 100.17.8.2 255.255.255.252
duplex auto
speed auto
!

```

Рисунок 3.9. – Базове налаштування маршрутизатора R5

```

R5(config)#router ospf 1
R5(config-router)#network 100.16.8.0 0.0.0.3 area 20
R5(config-router)#
*Jun 19 12:39:50.751: %OSPF-5-ADJCHG: Process 1, Nbr 100.16.8.1 on FastEthernet0
/1 from LOADING to FULL, Loading Done
R5(config-router)#network 100.17.8.0 0.0.0.3 area 20
R5(config-router)#
*Jun 19 12:40:10.335: %OSPF-5-ADJCHG: Process 1, Nbr 100.17.8.1 on FastEthernet1
/0 from LOADING to FULL, Loading Done
R5(config-router)#network 100.18.8.0 0.0.0.3 area 20
R5(config-router)#exit
R5(config)#
*Jun 19 12:40:28.819: %OSPF-5-ADJCHG: Process 1, Nbr 100.19.8.2 on FastEthernet0
/0 from LOADING to FULL, Loading Done
R5(config)#

```

Рисунок 3.10. – Базове налаштування протоколу OSPF маршрутизатора R5

 R8

```

interface FastEthernet0/0
ip address 100.16.8.1 255.255.255.252
duplex auto
speed auto
!

```

Рисунок 3.11. – Базове налаштування маршрутизатора R8

 R8

```

old start
*Mar 1 00:00:39.467: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Mar 1 00:00:39.467: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
R8#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R8(config)#router ospf 1
R8(config-router)#network 100.16.8.0 0.0.0.3 area 20
R8(config-router)#exit
R8(config)#

```

Рисунок 3.12. – Базове налаштування протоколу OSPF маршрутизатора R8

```

R8#ping 100.17.8.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.17.8.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/324/1156 ms
R8#ping 100.19.8.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.19.8.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/204/448 ms
R8#tracer 100.19.8.1

Type escape sequence to abort.
Tracing the route to 100.19.8.1

 0 100.16.8.2 68 msec 48 msec 64 msec
 1 100.18.8.1 284 msec 72 msec 68 msec
 2 100.19.8.1 224 msec 276 msec 156 msec
R8#

```

Рисунок 3.13. – Перевірка з'єднання між маршрутизаторами R8 та R6, R9

```

R15
!
interface FastEthernet0/0
 ip address 100.4.8.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 100.5.8.1 255.255.255.252
 duplex auto
 speed auto

```

Рисунок 3.14. – Базове налаштування маршрутизатора R15

```

R15
!
router ospf 1
 log-adjacency-changes
 network 100.4.8.0 0.0.0.3 area 300
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 network 100.4.8.0 mask 255.255.255.252
 neighbor 100.5.8.2 remote-as 200
 neighbor 100.5.8.2 ebgp-multihop 100
 no auto-summary

```

Рисунок 3.15. – Базове налаштування протоколу OSPF та BGP на маршрутизаторі R15

```

R15#ping 100.3.8.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.3.8.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/57/124 ms

```

Рисунок 3.16. – Перевірка з'єднання між маршрутизаторами R15 та R6

3.3. Налаштування підсистеми захисту

Починаємо налаштовувати віддалений доступ до маршрутизаторів. Для віддаленого доступу використовуємо ssh v2, так-як він більш надійніший ніж telnet.

```

R16(config)#line con 0
R16(config-line)#exec-timeout 5 0
R16(config-line)#login local
R16(config-line)#logging synchronous
R16(config-line)#line aux 0
R16(config-line)#exec-timeout 5 0
R16(config-line)#login local
R16(config-line)#line vty 0 4
R16(config-line)#exec-timeout 5 0
R16(config-line)#privilege level 15
R16(config-line)#transport input ssh
R16(config-line)#login local
R16(config-line)#ip ssh version 2

```

Рисунок 3.17. – Налаштування захисту на маршрутизаторі R16

```

R20#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R20(config)#service password-encryption
R20(config)#security passwords min-length 10
R20(config)#enable secret cisco12345
R20(config)#ip domain name netsec.com
R20(config)#username user01 secret user01pass
R20(config)#username admin privilege 15 secret adminpasswd
R20(config)#crypto key generate rsa general modul 1024
The name for the keys will be: R20.netsec.com

```

Рисунок 3.18. – Створюємо користувачів та зашифруємо їх паролі на маршрутизаторі R20

Використаємо AutoSecure для налаштування базової безпеки . Відключимо такі сервіси як finger, PAD, tcrпні Small Servers, BOOTP, вбудований HTTP, CDP, NTP, механізм Source Routing і купу всього подібного.

```

R20#auto secure login
      --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: no
Enter the new enable password:
Confirm the enable password:
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 666

Maximum Login failures with the device: 10

Maximum time period for crossing the failed login attempts: 5

This is the configuration generated:

enable password 7 060506324F41584B5643475D
aaa new-model
aaa authentication login local_auth local
line con 0
  login authentication local_auth
  exec-timeout 5 0
  transport output telnet
line aux 0
  login authentication local_auth
  exec-timeout 10 0
  transport output telnet
line vty 0 4
  login authentication local_auth
  transport input telnet
login block-for 666 attempts 10 within 5
!
end

```

Рисунок 3.19. – Налаштування AutoSecure

3.4. Тестування підсистеми захисту

За допомогою віртуальної машини vRIN проводимо стрес-тест мережі Е. Віртуальну машину підключаємо до маршрутизатора R15, як зображено на рисунку 3.20.

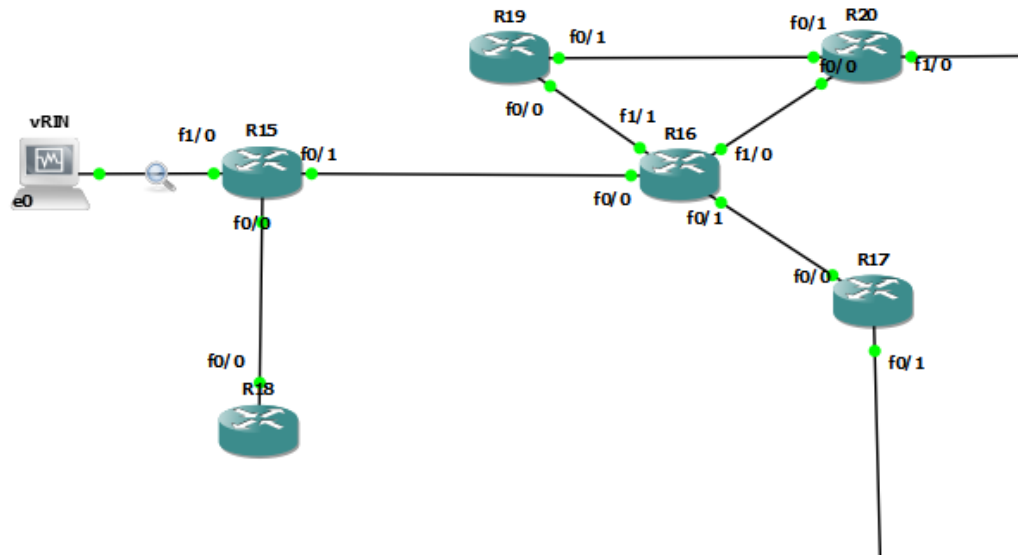


Рисунок 3.20. – Мережа регіонального провайдера з підключеною віртуальною машиною vRIN

Проводимо налаштування віртуальної машини та маршрутизатора R15.

```
interface Loopback0
 ip address 1.1.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 100.4.8.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 100.5.8.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 192.162.10.1 255.255.255.0
 duplex auto
 speed auto
```

Рисунок 3.21. – Налаштування IP-адрес на маршрутизаторі R15

```

router bgp 100
no synchronization
bgp router-id 1.1.1.1
bgp log-neighbor-changes
network 100.4.8.0 mask 255.255.255.252
neighbor 100.5.8.2 remote-as 200
neighbor 100.5.8.2 ebgp-multihop 100
neighbor 192.162.10.10 remote-as 30
no auto-summary

```

Рисунок 3.22. – Налаштування BGP на маршрутизаторі R15

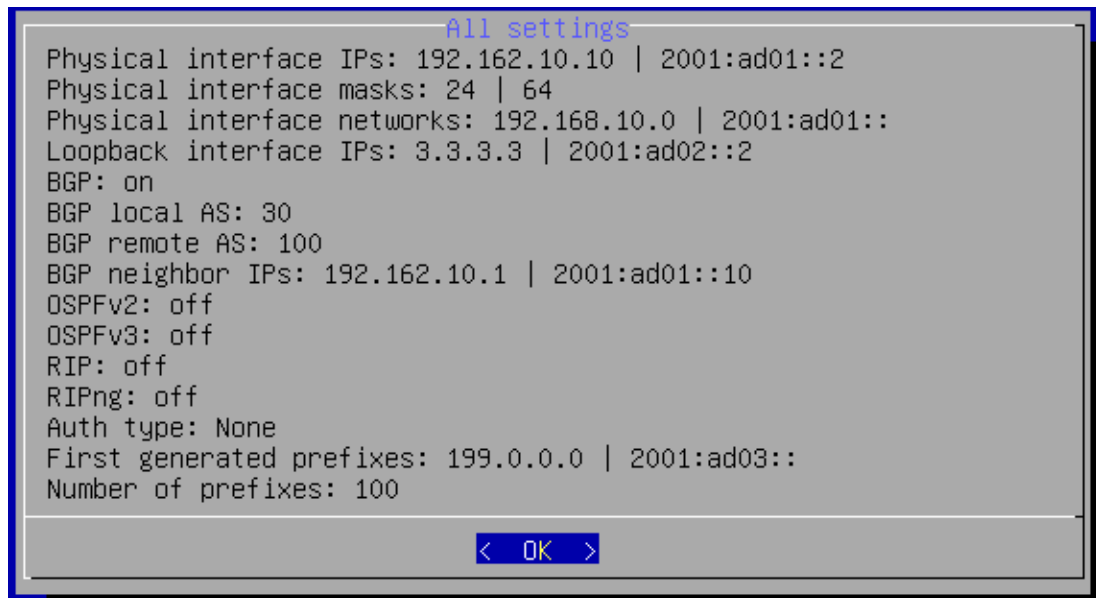


Рисунок 3.23. – Налаштування віртуальної машини vRIN

```

R15#ping 192.162.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.162.10.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/118/316 ms

```

Рисунок 3.24. – Перевіряємо зв'язок між маршрутизатором R15 та віртуальною машиною vRIN

Після налаштування віртуальної машини перевіряємо маршрутизатор R15, як саме вплинула атака.

```

R15#show ip bgp
BGP table version is 106, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*> 3.3.3.3/32      192.162.10.10           0             0 30 i
*> 100.2.8.0/30    100.5.8.2               0             0 200 i
*> 100.3.8.0/30    100.5.8.2               0             0 200 i
*> 100.4.8.0/30    0.0.0.0                 0             32768 i
*> 100.6.8.0/30    100.5.8.2               0             0 200 i
*> 199.0.0.0/32    192.162.10.10           0             0 30 ?
*> 199.0.0.1/32    192.162.10.10           0             0 30 ?
*> 199.0.0.2/32    192.162.10.10           0             0 30 ?
*> 199.0.0.3/32    192.162.10.10           0             0 30 ?
*> 199.0.0.4/32    192.162.10.10           0             0 30 ?
*> 199.0.0.5/32    192.162.10.10           0             0 30 ?
*> 199.0.0.6/32    192.162.10.10           0             0 30 ?
*> 199.0.0.7/32    192.162.10.10           0             0 30 ?
*> 199.0.0.8/32    192.162.10.10           0             0 30 ?
*> 199.0.0.9/32    192.162.10.10           0             0 30 ?
*> 199.0.0.10/32   192.162.10.10           0             0 30 ?
*> 199.0.0.11/32   192.162.10.10           0             0 30 ?
*> 199.0.0.12/32   192.162.10.10           0             0 30 ?
*> 199.0.0.13/32   192.162.10.10           0             0 30 ?
*> 199.0.0.14/32   192.162.10.10           0             0 30 ?
*> 199.0.0.15/32   192.162.10.10           0             0 30 ?
*> 199.0.0.16/32   192.162.10.10           0             0 30 ?
*> 199.0.0.17/32   192.162.10.10           0             0 30 ?
*> 199.0.0.18/32   192.162.10.10           0             0 30 ?
*> 199.0.0.19/32   192.162.10.10           0             0 30 ?
*> 199.0.0.20/32   192.162.10.10           0             0 30 ?
*> 199.0.0.21/32   192.162.10.10           0             0 30 ?
*> 199.0.0.22/32   192.162.10.10           0             0 30 ?
*> 199.0.0.23/32   192.162.10.10           0             0 30 ?
*> 199.0.0.24/32   192.162.10.10           0             0 30 ?
*> 199.0.0.25/32   192.162.10.10           0             0 30 ?
*> 199.0.0.26/32   192.162.10.10           0             0 30 ?
*> 199.0.0.27/32   192.162.10.10           0             0 30 ?
*> 199.0.0.28/32   192.162.10.10           0             0 30 ?

```

Рисунок 3.25. – Результат атаки на маршрутизатор R15

Для того щоб захистити маршрутизатор від такої атаки застосовуємо списки доступу.

ВИСНОВКИ

BGP (Border Gateway Protocol) являється провідною технологією для з'єднання мереж в Інтернет просторі. Під час виконання випускної роботи бакалавра було спроектовано та реалізовано захищену мережу регіонального Інтернет-провайдера. Під час проектування розглянули структуру протоколу BGP, як він співпрацює з внутрішніми протоколами які використовуються для з'єднання мереж.

Розглянули види загроз які можуть втрутитись в справну роботу протоколу. Знайшли рішення для різних видів загроз які допоможуть захистити мережу від зовнішнього та внутрішнього втручання в мережу. Розібрали які є види топологій в протоколу BGP. І визначили з якою саме топологією будемо працювати впродовж всієї роботи. Розробили систему захисту яку будемо використовувати для забезпечення безпеки розробленої мережі регіонального Інтернет-провайдера.

Налаштували розроблену мережу. Провели стрес-тест, щоб подивитись як налагоджена мережа реагує на сторонній вплив на мережу.

В подальшому дана мережа може бути розширена шляхом налаштування додаткових маршрутизаторів. Завдяки обраній архітектурі масштабування мережі відбувається просто та швидко.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. BGP Case Studies [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html>.
2. What is BGP? | BGP routing explained [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cloudflare.com/learning/security/glossary/what-is-bgp/>.
3. BGP Keepalive Messages [Електронний ресурс] – Режим доступу до ресурсу: <https://www.inetdaemon.com/tutorials/internet/ip/routing/bgp/operation/messages/keepalives.shtml>.
4. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.: іл.
5. Войтенко Є. Д., Орлова М. М. Аналіз вразливості безпеки функціонування BGP та причин складності боротьби з ними Є. Д. Войтенко, М. М. Орлова – Ж.: "Луцьк", 2020. – 117-121 с.
6. BGP-4 Protocol Analysis [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc4274>.
7. Security and BGP [Електронний ресурс] – Режим доступу до ресурсу: <https://www.inetdaemon.com/tutorials/internet/ip/routing/bgp/security/index.shtml>.
8. Securing BGP [Електронний ресурс] – Режим доступу до ресурсу: <https://www.internetsociety.org/deploy360/securing-bgp/>.
9. Threat Model for BGP Path Security [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc7132>.
10. Основы протокола border gateway protocol (BGP) [Електронний ресурс] – Режим доступу до ресурсу: <https://wiki.merionet.ru/seti/35/osnovy-protokola-border-gateway-protocol-bgp/>.

11. Internet [Електронний ресурс] – Режим доступу до ресурсу:
<https://en.wikipedia.org/wiki/Internet>.
12. Протоколи міждоменої маршрутизації [Електронний ресурс] – Режим доступу до ресурсу: <https://ppt-online.org/30386>.
13. BGP Operations and Security [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc7454>.
14. Протокол BGP [Електронний ресурс] – Режим доступу до ресурсу:
<https://docs.microsoft.com/ru-ru/windows-server/remote/remote-access/bgp/border-gateway-protocol-bgp>.
15. Внешний протокол маршрутизации BGP [Електронний ресурс] – Режим доступу до ресурсу: <http://book.itep.ru/4/44/bgp44114.htm>.
16. Nanonetwork [Електронний ресурс] – Режим доступу до ресурсу:
<https://en.wikipedia.org/wiki/Nanonetwork>.
17. Personal area network [Електронний ресурс] – Режим доступу до ресурсу:
https://en.wikipedia.org/wiki/Personal_area_network.
18. Local area network [Електронний ресурс] – Режим доступу до ресурсу:
https://en.wikipedia.org/wiki/Local_area_network.
19. Wide area network [Електронний ресурс] – Режим доступу до ресурсу:
https://en.wikipedia.org/wiki/Wide_area_network.
20. Как настроить BGP с подключением к двум интернет-провайдерам [Електронний ресурс] – Режим доступу до ресурсу:
<https://blog.sedicomm.com/2020/09/25/kak-nastroit-bgp-s-podklyucheniem-k-dvum-internet-provayderam/>.
21. Как настроить перераспределение между OSPF и RIP [Електронний ресурс] – Режим доступу до ресурсу:
<https://blog.sedicomm.com/2020/01/25/kak-nastroit-pereraspredelenie-mezhdu-ospf-i-rip/>.

ДОДАТКИ

					КІК.КР.Б -125-08-ПЗ	
						47

Адресація підмереж

Таблиця А.1 - Паметри адресації мереж та вузлів

Підмережа	IP-адреса	Маска мережі	Шлюз по замовчуванню	Діапазон вільних адрес
Підмережа А	100.1.8.0	255.255.255.252	100.1.8.1	100.1.8.1-100.1.8.2
Підмережа В	100.2.8.0	255.255.255.252	100.2.8.1	100.2.8.1-100.2.8.2
Підмережа С	100.3.8.0	255.255.255.252	100.3.8.1	100.3.8.1-100.3.8.2
Підмережа D	100.4.8.0	255.255.255.252	100.4.8.1	100.4.8.1-100.4.8.2
Підмережа E	100.5.8.0	255.255.255.252	100.5.8.1	100.5.8.1-100.5.8.2
Підмережа F	100.6.8.0	255.255.255.252	100.6.8.1	100.6.8.1-100.6.8.2
Підмережа G	100.7.8.0	255.255.255.252	100.7.8.1	100.7.8.1-100.7.8.2
Підмережа H	100.8.8.0	255.255.255.252	100.8.8.1	100.8.8.1-100.8.8.2
Підмережа I	100.9.8.0	255.255.255.252	100.9.8.1	100.9.8.1-100.9.8.2
Підмережа J	100.10.8.0	255.255.255.252	100.10.8.1	100.10.8.1-100.10.8.2
Підмережа K	100.11.8.0	255.255.255.252	100.11.8.1	100.11.8.1-100.11.8.2
Підмережа L	100.12.8.0	255.255.255.252	100.12.8.1	100.12.8.1-100.12.8.2
Підмережа M	100.13.8.0	255.255.255.252	100.13.8.1	100.13.8.1-100.13.8.2

Продовження таблиці А.1

Підмережа N	100.14.8.0	255.255.255.252	100.14.8.1	100.14.8.1-100.14.8.2
Підмережа O	100.15.8.0	255.255.255.252	100.15.8.1	100.15.8.1-100.15.8.2
Підмережа P	100.16.8.0	255.255.255.252	100.16.8.1	100.16.8.1-100.16.8.2
Підмережа Q	100.17.8.0	255.255.255.252	100.17.8.1	100.17.8.1-100.17.8.2
Підмережа R	100.18.8.0	255.255.255.252	100.18.8.1	100.18.8.1-100.18.8.2
Підмережа S	100.19.8.0	255.255.255.252	100.19.8.1	100.19.8.1-100.19.8.2
Підмережа T	100.20.8.0	255.255.255.252	100.20.8.1	100.20.8.1-100.20.8.2
Підмережа U	100.21.8.0	255.255.255.252	100.21.8.1	100.21.8.1-100.21.8.2
Підмережа V	100.22.8.0	255.255.255.252	100.22.8.1	100.22.8.1-100.22.8.2
Підмережа W	100.23.8.0	255.255.255.252	100.23.8.1	100.23.8.1-100.23.8.2

Конфігураційні файли пристроїв спрєктованої мережі

Виведення конфігураційного файлу з кожного маршрутизатора

Конфігураційний файл маршрутизатора R1

```

R1#show configuration
Using 1902 out of 522232 bytes
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging message-counter syslog
enable secret 5
$1$utIL$9N8x62QHufQkiA0Ty9GsQ/
enable password 7
094F471A1A0A46405858517C
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
login block-for 666 attempts 10 within 5
no ipv6 cef
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$kie5$N8x62QHufQkiA0Ty9GsQ/
username admin privilege 15 secret 5
$1$R846$0Xs..WZ/vgLJTOC9rik7/
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.13.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.14.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 100.15.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
router rip
version 2
network 100.0.0.0
no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line aux 0

```

```

privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line vty 0 4
exec-timeout 5 0

```

```

privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R2

```

R2#show configuration
Using 2063 out of 57336 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5
$1$ruub$md4jNdnh.AO6arIFA8ppN/
enable password 7
05080F1C22431F5B4A514244
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
login block-for 666 attempts 10 within 5
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$vDuo$3jAg5BIXinMT8e62oSvxB.
username admin privilege 15 secret 5
$1$VIB/$5LKhf3AveV6x1Wtzi53SU.
archive
log config
logging enable

```

```

hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.13.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.22.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 100.20.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
redistribute rip subnets
network 100.20.8.0 0.0.0.3 area 10
network 100.22.8.0 0.0.0.3 area 20
!
router rip
version 2
redistribute ospf 1 metric 5
network 100.0.0.0
default-metric 5
no auto-summary
!
ip forward-protocol nd
!
no ip http server

```

```

no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line aux 0

```

```

privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R3

```

R3#show configuration
Using 1677 out of 57336 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5
$1$2FoT$5bwPoak.7aKxKCY5Yokzv1
enable password 7
13061E010803557878707D65
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
login block-for 666 attempts 10 within 5
!
multilink bundle-name authenticated
!

```

```

username user01 secret 5
$1$mhoL$VTPPcZPiPCKg8QvllgH5//
username admin privilege 15 secret 5
$1$HdF4$sgeBVj.ciXQlJt9hbVKOz0
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.14.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
router rip
version 2
network 100.0.0.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!

```

```

line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet

```

```

line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R4

```

R4#show configuration
Using 1677 out of 57336 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5
$1$cgYF$/q6Wes2Eh/es8jRiVe/pv0
enable password 7
121A0C0411045D56797F717E
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
login block-for 666 attempts 10 within 5
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$C00j$VWVRdelf/EFSdKJUdjGrv0
username admin privilege 15 secret 5
$1$gY52$u1DfU6eZ/7nxZmTUocLL71

```

```

archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.15.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
router rip
version 2
network 100.0.0.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet

```

```

line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line vty 0 4
exec-timeout 5 0

```

```

privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R5

```

R5#show configuration
Using 1989 out of 522232 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R5
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging message-counter syslog
enable secret 5
$1$DQjE$lfu7tzA.0hrmz0HiyGfRZ/
enable password 7
060506324F41584B5643475D
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
login block-for 666 attempts 10 within 5
no ipv6 cef
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$EkRE$kpBWwSkYFoLFpwICFZsPL.
username admin privilege 15 secret 5
$1$TWi5$Iu2gFpbRyRGoBp8QB2YmL.
archive
log config
logging enable

```

```

hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.18.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.16.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 100.17.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
network 100.16.8.0 0.0.0.3 area 20
network 100.17.8.0 0.0.0.3 area 20
network 100.18.8.0 0.0.0.3 area 20
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown

```

```

!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line aux 0
privilege level 15
logging synchronous

```

```

login authentication local_auth
transport output telnet
stopbits 1
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R6

```

R6#show configuration
Using 1658 out of 522232 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R6
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging message-counter syslog
enable secret 5
$1$lfIP$ss.40JKTxDio0IUxVRD/r1
enable password 7
045802150C2E1D1C5A4D5041
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
login block-for 666 attempts 10 within 5
no ipv6 cef
!
multilink bundle-name authenticated
!

```

```

username user01 secret 5
$1$biRN$KbXTpl8VYfsxMqhsNVfZH.
username admin privilege 15 secret 5
$1$v17N$SuvqdSDY5zjc6rgZJxkr81
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.19.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!
line con 0
exec-timeout 5 0

```

```

privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet

```

```

stopbits 1
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R7

```

R7#show configuration
Using 1726 out of 57336 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R7
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5
$1$TH/F$VqlPRcdtW5nDDCx6JM2AO0
enable password 7
01100F175804575D72181B5F
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
login block-for 666 attempts 10 within 5
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$/0bB$hpEU0MoBT0n.wXxBxbm7N/

```

```

username admin privilege 15 secret 5
$1$hWJI$9vH3XE4S97wm8mDDQs.ZI/
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.19.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.18.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 5 0

```

```

privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet

```

```

line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R8

```

R8#show configuration
Using 1712 out of 57336 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R8
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5
$1$TCyL$Zlqzj2F8zZbyQgwBYuMZK/
enable password 7
00071A1507545A545C751918
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
login block-for 666 attempts 10 within 5
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$FetE$w5tZkNKkI.7DJaZod/Wxw1
username admin privilege 15 secret 5
$1$Ffw8$qa.XJuezVLrKVbK.5oDKO.

```

```

archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.16.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous

```

```
login authentication local_auth
transport output telnet
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line vty 0 4
```

```
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end
```

Конфігураційний файл маршрутизатора R9

```
R9#show configuration
Using 1688 out of 57336 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R9
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5
$1$0XdV$3tmO2QlHa/yFjN543.Zww0
enable password 7
110A1016141D5A5E577E7E72
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
login block-for 666 attempts 10 within 5
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$IN3t$fo1seyYvRG98b8KjWERcx.
username admin privilege 15 secret 5
$1$hUdY$ldYZwmMY92dhLKBBNuBNU.
archive
```

```
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.17.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
banner motd ^C
Unauthorized access is strictly prohi^C
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line aux 0
privilege level 15
logging synchronous
```

```
login authentication local_auth
transport output telnet
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
```

```
transport input telnet
!
end
```

Конфігураційний файл маршрутизатора R10

```
R10#show configuration
Using 1785 out of 57336 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R10
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5
$1$5svr$k5vGeaSa0Qj4SujiZjkc//
enable password 7
00071A1507545A545C751918
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
login block-for 666 attempts 10 within 5
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$U8Eo$48MK7kwLD6EDwYueoM.jK1
username admin privilege 15 secret 5
$1$a8wU$WK6/gc/R/jQ1/ecGBL0LV.
archive
log config
logging enable
```

```
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.7.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.8.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
router rip
version 2
network 100.0.0.0
no auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
```

```

line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line vty 0 4
exec-timeout 5 0

```

```

privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R11

```

R11#show configuration
Using 1787 out of 57336 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R11
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5
$1$c038$YgQxt6ERWgJQ/.5WZw6fg.
enable password 7
0822455D0A165445415F5952
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
login block-for 666 attempts 10 within 5
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$aEv8$3x0GSUAER/p7axHNjzYHS1
username admin privilege 15 secret 5
$1$gJ06$VUxvbTA8FTQ2dlB2t6QPr.
archive
log config

```

```

logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.12.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.10.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
router rip
version 2
network 100.0.0.0
no auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous

```

```
login authentication local_auth
transport output telnet
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line vty 0 4
exec-timeout 5 0
```

```
privilege level 15
login authentication local_auth
transport input telnet
!
end
```

Конфігураційний файл маршрутизатора R12

```
R12#show configuration
Using 2071 out of 522232 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R12
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging message-counter syslog
enable secret 5
$1$dQhF$mCf3n3MN/LFm2FMM8vOHN/
enable password 7
02050D4808095E731F1A5C4F
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
login block-for 666 attempts 10 within 5
no ipv6 cef
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$fVfj$DCFoC2zybgrrILA2y41b./
```

```
username admin privilege 15 secret 5
$1$A/8A$qGF6uYq/UOPvAsdhKYWIo1
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.10.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.11.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 100.8.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 100.9.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
```

```

shutdown
duplex auto
speed auto
!
router rip
version 2
network 100.0.0.0
no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!
line con 0

```

```

exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R13

```

R13#show configuration
Using 2050 out of 522232 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R13
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging message-counter syslog
enable secret 5
$1$HuVd$ADRSgbbZ.MH2aFxdMFeYg/
enable password 7
00071A1507545A545C751918
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable

```

```

ip cef
!
no ip domain lookup
ip domain name netsec.com
login block-for 666 attempts 10 within 5
no ipv6 cef
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$btZW$/Vqt797c2EbWLkHbf64eI/
username admin privilege 15 secret 5
$1$!ADx$NhfixR5uVuRjkg14LK.GQ0
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.7.8.2 255.255.255.252
duplex auto
speed auto
!

```

```

interface FastEthernet0/1
ip address 100.9.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 100.21.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
redistribute rip subnets
network 100.21.8.0 0.0.0.3 area 10
!
router rip
version 2
redistribute ospf 1 metric 5
network 100.0.0.0
default-metric 5
no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R14

```

R14#show configuration
Using 2026 out of 522232 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R14
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging message-counter syslog
enable secret 5
$1$3YiR$rcgPJvx0AgUryLGptPKH30
enable password 7
094F471A1A0A46405858517C
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
login block-for 666 attempts 10 within 5
no ipv6 cef
!
multilink bundle-name authenticated

```

```

!
username user01 secret 5
$1$1/aD$yFPKjNugF3W3pI1K9fzoo/
username admin privilege 15 secret 5
$1$wqfi$UuH/WLd4Ya8Nj3a97g/c51
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.12.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.11.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 100.23.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
network 100.23.8.0 0.0.0.3 area 20
!

```

```

router rip
version 2
redistribute ospf 1 metric 5
network 100.0.0.0
default-metric 5
no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R15

```

R15#show configuration
Using 2297 out of 522232 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!

```

```

hostname R15
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging message-counter syslog
enable secret 5
$1$1hvO$w4XWoWm0/qIUytEw1E9CR.

```

```

enable password 7
030752180500701E1D5D4C53
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
login block-for 666 attempts 10 within 5
no ipv6 cef
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$j1gD$J5Bxn6uZCvB.p8hZ2h6PN1
username admin privilege 15 secret 5
$1$b.nq$OBpFJtv63ce.VOM3eARym0
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface FastEthernet0/0
ip address 100.4.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.5.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.162.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address

```

```

shutdown
duplex auto
speed auto
!
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
network 100.4.8.0 0.0.0.3 area 300
!
router bgp 100
no synchronization
bgp router-id 1.1.1.1
bgp log-neighbor-changes
network 100.4.8.0 mask 255.255.255.252
neighbor 100.5.8.2 remote-as 200
neighbor 100.5.8.2 ebgp-multihop 100
neighbor 192.162.10.10 remote-as 30
no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!
banner motd ^C
Unauthorized access is strictly prohi^C
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R16

```

R16#show configuration
Using 2329 out of 522232 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R16
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging message-counter syslog
enable secret 5
$1$WfZQ$fcjdT3s39pMdMNIv5m.eN.
enable password 7
05080F1C22431F5B4A514244
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
login block-for 666 attempts 10 within 5
no ipv6 cef
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$aWbp$mq47LTZF/A8a.uv0vIb2T/
username admin privilege 15 secret 5
$1$mouJ$0Ys2mpa/37RS1y/WsI8u5.
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2

```

```

!
interface Loopback0
ip address 2.2.2.2 255.255.255.0
!
interface FastEthernet0/0
ip address 100.5.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.6.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 100.3.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 100.2.8.2 255.255.255.252
duplex auto
speed auto
!
router ospf 1
router-id 2.2.2.2
log-adjacency-changes
network 100.2.8.0 0.0.0.3 area 10
network 100.3.8.0 0.0.0.3 area 10
network 100.6.8.0 0.0.0.3 area 10
!
router bgp 200
no synchronization
bgp router-id 2.2.2.2
bgp log-neighbor-changes
network 100.2.8.0 mask 255.255.255.252
network 100.3.8.0 mask 255.255.255.252
network 100.6.8.0 mask 255.255.255.252
neighbor 100.5.8.1 remote-as 100
no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown

```

```

!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line aux 0
privilege level 15
logging synchronous

```

```

login authentication local_auth
transport output telnet
stopbits 1
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R17

```

R17#show configuration
Using 1938 out of 522232 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R17
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
logging message-counter syslog
enable secret 5
$1$DCTd$Z8pTOsMYZ.R2K.fXreXva0
enable password 7
121A0C0411045D56797F717E
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
login block-for 666 attempts 10 within 5
no ipv6 cef
!
multilink bundle-name authenticated
!

```

```

username user01 secret 5
$1$bla4$PAR4XWvZTOFieQk8toYLH0
username admin privilege 15 secret 5
$1$Bbwf$VEWF.u3pR1l7sLGiieGJ2.
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.6.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.21.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes

```

```

network 100.6.8.0 0.0.0.3 area 10
network 100.21.8.0 0.0.0.3 area 10
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous

```

```

login authentication local_auth
transport output telnet
stopbits 1
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
stopbits 1
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R18

```

R18#show configuration
Using 1787 out of 57336 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R18
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5
$1$4g7x$17Kx/EPs29kJCzWAVOgLx/
enable password 7
060506324F41584B5643475D
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip domain name netsec.com
ip auth-proxy max-nodata-conns 3

```

```

ip admission max-nodata-conns 3
login block-for 666 attempts 10 within 5
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$AEhc$i5QgvNoxWMxbyAQw9S5yE/
username admin privilege 15 secret 5
$1$aXdm$Uy6rgTijVf6VuHF6F3KMK.
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.4.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/0

```

```

no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
network 100.4.8.0 0.0.0.3 area 300
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
no cdp log mismatch duplex
!
control-plane
!
```

```

line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end
```

Конфігураційний файл маршрутизатора R19

```

R19#show configuration
Using 1912 out of 57336 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R19
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5
$1$1Yok$yiGbT7LDrPqipaMmuwGQw/
enable password 7
104D000A061843595F507F7D
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
```

```

no ip domain lookup
ip domain name netsec.com
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
login block-for 666 attempts 10 within 5
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$ARwi$Aqeemas3sGiMX3zSvTf9M0
username admin privilege 15 secret 5
$1$LbM8$FjcZgusn0e55BILHnpoxD0
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.2.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.1.8.1 255.255.255.252
```

```

duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
network 100.1.8.0 0.0.0.3 area 10
network 100.2.8.0 0.0.0.3 area 10
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!

```

```

no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```

Конфігураційний файл маршрутизатора R20

```

R20#show configuration
Using 1980 out of 57336 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R20
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5
$1$CneE$NLj9Y.uqTdG3BHk5H0B0g0
enable password 7
060506324F41584B5643475D
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable

```

```

ip cef
!
no ip domain lookup
ip domain name netsec.com
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
login block-for 666 attempts 10 within 5
!
multilink bundle-name authenticated
!
username user01 secret 5
$1$XgoP$IvfcArSf2uK.iDBuEcM8r/
username admin privilege 15 secret 5
$1$RPtv$UKszDk2nDwD7vdDeJz3K1
archive
log config
logging enable
hidekeys
!
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
interface FastEthernet0/0
ip address 100.3.8.1 255.255.255.252

```

```

duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.1.8.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 100.20.8.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
redistribute rip
network 100.1.8.0 0.0.0.3 area 10
network 100.3.8.0 0.0.0.3 area 10
network 100.20.8.0 0.0.0.3 area 10
!
ip forward-protocol nd

```

```

!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line aux 0
privilege level 15
logging synchronous
login authentication local_auth
transport output telnet
line vty 0 4
exec-timeout 5 0
privilege level 15
login authentication local_auth
transport input telnet
!
end

```