ВІДЗИВ НАУКОВОГО КЕРІВНИКА НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ

Студента Черняка Іллі Олександровича
представлену на здобуття освітнього ступеня бакалавр
зі спеціальності 123 «Комп'ютерна інженерія»

1. Робота виконана на тему „Проект підсистеми резервування каналів зв'язку організації".

2. Актуальність роботи зумовлена потребою у розробці та впровадженні у практику діяльності організацій рішень щодо забезпечення надійності, продуктивності, доступності, безперебійності доступу до ресурсів комп'ютерних мереж.

3. Основний зміст пояснювальної записки роботи викладено на 89 сторінках тексту, записка містить 6 таблиць, 106 ілюстрацій, 33 сторінки додатків. Список використаних літературних джерел налічує 24 найменування. Невід'ємною складовою роботи є реалізований у середовищі моделювання EVE-NG проект мережі на базі обладнання фірми Cisco з використанням можливостей міжмережних екранів Cisco ASA та адаптивного менеджера пристроїв безпеки ASDM.

4. Пояснювальна записка складається з вступу, трьох розділів основного тексту, висновків, списку використаної літератури, додатків.

Розділ 1 присвячений аналізу принципів, моделей, протоколів та технологій резервування та балансування комп'ютерних мереж, зокрема, у розділі розглянуто: поняття балансування трафіку в мережі, організація резервування каналів зв'язку, основні поняття, протоколи, принципи функціонування резервування в мережах організацій. У цьому ж розділі наведено огляд основних технологій резервування каналів зв'язку, що застосовуються в сучасних мережах.

Розділ 2 присвячений питанням проектування комп'ютерної мережі організації з резервування каналів зв'язку, зокрема, у ньому здійснено проектування топології мережі, розроблено схему адресації мережі, розроблено підсистему резервування для даної мережі. У розділі також описаний та обґрунтований вибір мережевого обладнання для проекті, проаналізовані та обрані основні методи для резервування.

Розділ 3 присвячений питанням налаштування обладнання для розробленого проекту мережі. У розділі наведено опис процесу налагодження та тестування побудованої мережі. Також у цьому розділі здійснено перевірку функціоналу підсистеми резервування мережі організації.

5. Висновки містять сумарні результати проведеної роботи.

6. Список використаних літературних джерел має відповідний для даного виду робіт обсяг, є правильно оформленим та повністю опрацьованим у ході виконання роботи.

7. Додатки містять змодельовану схему мережі, лістинги конфігураційних файлів налагоджених пристроїв.

8. Таблиці та ілюстрації оформлені якісно, є інформативними та наведені у відповідних місцях роботи.

9. Якість оформлення роботи є високою.

10. Виявлені на етапі попереднього захисту недоліки оформлення пояснювальної записки та презентації усунені. Рекомендації стосовно покращення проекту враховані.

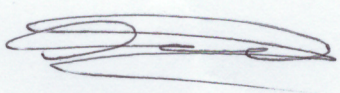
11. Ставлення студента до виконання випускної кваліфікаційної роботи – відповідальне.

12. У цілому при написанні випускної кваліфікаційної роботи студент Черняк І.О. виявив здібності до оволодіння знаннями, уміннями і навичками з таких дисциплін, як «Операційні системи», «Комп'ютерні мережі», «Захист інформації в інформаційно-комунікаційних системах», «Адміністрування комп'ютерних систем та мереж», «Хмарні технології». Також студент Черняк І.О. показав вміння підібрати необхідну літературу та інші інформаційні джерела, проаналізувати їх, виконати постановку задачі на розробку, розробити проект мережі організації з резервуванням каналів зв'язку, обрати відповідний інструментарій, створити закінчений цілісний продукт (у вигляді змодельованого проекту) і оформити свої розробки та напрацювання як випускну кваліфікаційну роботу.

Випускна кваліфікаційна робота студента Черняк І.О. написана на високому рівні та може бути допущена до захисту в Екзаменаційній комісії.

Пропонована оцінка – «відмінно».

Науковий керівник
к.т.н., завідувач кафедри КІ та КБ
15 червня 2020 року



А.А. Єфіменко

РЕЦЕНЗІЯ
на кваліфікаційну роботу
студента 4 курсу групи КІ-2 спеціальності 123 «Комп'ютерна інженерія»
факультету інформаційно-комп'ютерних технологій
Державного університету «Житомирська політехніка»
Черняка Іллі Олександровича
на тему: „ Проект підсистеми резервування каналів зв'язку організації "

Кваліфікаційна робота студента Черняка І.О. „Проект підсистеми резервування каналів зв'язку організації " присвячена актуальній тематиці – розробці та впровадженні у практику діяльності організації високонадійних та високопродуктнивних комп'ютерних мереж.

Робота містить реалізований у середовищі моделювання EVE-NG проект мережі на базі обладнання фірми Cisco та пояснювальну записку наступного складу: вступ, три розділи основного тексту, висновки, список використаної літератури, два додатки.

Перший розділ присвячений аналізу принципів, моделей, протоколів та технологій резервування та балансування комп'ютерних мереж. У розділі розглянуто поняття балансування трафіку в мережі, принципи організації резервування каналів зв'язку, протоколи резервування каналів зв'язку. У цьому ж розділі наведено огляд основних сучасних технологій резервування каналів зв'язку.

Другий розділ присвячений питанням проектування комп'ютерної мережі організації з використанням резервування каналів, зокрема, у ньому здійснено проектування топології мережі, розроблено схему адресації мережі, розроблено підсистему резервування для побудованої мережі, обгрунтований вибір мережевого обладнання та визначені основні методи для резервування.

Третій розділ присвячений питанням налаштування обладнання для розробленого проекту мережі. У розділі наведено опис процесу налагодження та тестування побудованої мережі. Також у цьому розділі здійснено перевірку функціоналу підсистеми резервування в мережі організації.

Зміст роботи відповідає поставленому завданню. У цілому кваліфікаційна робота виконана на високому рівні. Тема роботи розкрита повністю. Студентом продемонстровані грунтовні фахові компетентності, що отримані як під час навчання, так і у процесі виконання роботи. Матеріал пояснювальної записки викладено технічно грамотно. Ілюстративний матеріал (рисунки, таблиці), що наведений у роботі, оформлений якісно і наведений у відповідних місцях. Оформлення роботи у цілому відповідає вимогам стандартів. Проект мережі реалізовано у середовищі моделювання EVE-NG з використанням обладнання фірми Cisco. Його функціонал відповідає заявленому.

Позитивною стороною є те, що отримані результати мають практичну цінність – розроблені рішення та сценарії налагодження можуть бути використанні при практичній організації резервних калів. Недоліками роботи є наступні:

– деяка неструктурованість роботи – винесення частини теоретичного матеріалу (щодо IP SLA, EMM) у розділ 2;

– наявність деяких відхилень від вимог щодо оформлення пояснювальної записки (наприклад, сторінки 19, 21, 22);

– занадто деталізований опис процесів налагодження та тестування підсистеми резервування каналів зв'язку (розділи 3.2, 3.3.).

Зазначені недоліки у цілому не впливають на високу якість і актуальність роботи.

У цілому кваліфікаційна робота студента Черняка І.О. „Проект підсистеми резервування каналів зв'язку організації" відповідає вимогам рівня вищої освіти «бакалавр» спеціальності 123 «Комп'ютерна інженерія» і рекомендується до захисту в ЕК.

Пропонована оцінка роботи – «відмінно».

Рецензент,
Завідувач кафедри комп'ютерних наук,
к.т.н., доцент
16 червня 2020 р.



І.І. Сугоняк,

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 резервування каналів зв’язку організації»

Виконав студент 4-го курсу, групи КІ-2
спеціальності 123 «Комп’ютерна інженерія»
_____ Черняк І.О.
Керівник, завідувач кафедри КІ та КБ, к.т.н.
_____ Єфіменко А. А.
Рецензент, завідувач кафедри КН, к.т.н., доцент
_____ Сугоняк І. І.

Житомир–2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки
Єфіменко А. А.
«06» квітня 2020 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу

Студента **Черняка Іллі Олександровича**
Тема роботи: **Проект підсистеми резервування каналів зв'язку організації**
Затверджена Наказом університету від **«06» квітня 2020 р. № 98с**
Термін здачі студентом закінченої роботи **- 1 червня 2020 р.**

Вихідні дані для роботи:

1. Фізична топологія мережі організації
2. Міжмережний екран Cisco ASA
3. Маршрутизатори Cisco 7200
4. Комутатори Cisco Catalist 2960
5. Операційні системи Cisco IOS, Windows 10 Server, Windows 10
6. Графічний симулятор мереж EVE-NG

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А. А.	6.04.2020	6.04.2020
2	Єфіменко А. А.	20.04.2020	20.04.2020
3	Єфіменко А. А.	11.05.2020	11.05.2020

Керівник _____ Єфіменко А. А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2020 – 7 квітня 2020	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо підсистеми резервування каналів зв'язку організації	8 квітня 2020 – 11 квітня 2020	Виконано
3	Аналіз технологій резервування каналів зв'язку організації	12 квітня 2020 – 16 квітня 2020	Виконано
4	Аналіз можливостей мережного обладнання Cisco для організації підсистеми резервування каналів зв'язку організації	17 квітня 2020 – 19 квітня 2020	Виконано
5	Розробка загального проекту мережі організації	20 квітня 2020 – 24 квітня 2020	Виконано
6	Проектування підсистеми резервування каналів зв'язку організації та вибір обладнання для її реалізації	25 квітня 2020 – 30 квітня 2020	Виконано
7	Розробка підсистеми резервування каналів зв'язку організації	1 травня 2020 – 4 травня 2020	Виконано
8	Проектування та розробка тестів для підсистеми резервування	5 травня 2020 – 9 травня 2020	Виконано
9	Базове налагодження пристроїв мережі організації	10 травня 2020 – 13 травня 2020	Виконано
10	Налагодження підсистеми резервування каналів зв'язку організації	14 травня 2020 – 18 травня 2020	Виконано
11	Тестування роботи підсистеми резервування	19 травня 2020 – 22 травня 2020	Виконано
12	Аналіз результатів тестування	23 травня 2020 – 24 травня 2020	Виконано
13	Написання пояснювальної записки	25 травня 2020 – 29 травня 2020	Виконано
14	Підготовка презентації та виступу	30 травня 2020 – 31 травня 2020	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	4 червня 2020 – 8 червня 2020	Виконано
16	Захист	13 червня 2020	Виконано

Студент _____ Черняк І. О.

Керівник _____ Єфіменко А. А.

РЕФЕРАТ

Кваліфікаційна робота складається з проекту підсистеми резервування каналів зв'язку організації та пояснювальної записки до нього. Пояснювальна записка до роботи містить 90 сторінок, 106 ілюстрацій та 6 таблиць.

Метою роботи є розробка проекту підсистеми резервування каналів зв'язку організації.

В роботі визначено основні завдання на розробку підсистеми, яка забезпечить постійний та надійний зв'язок між офісами та в мережах офісів, доступ до мережі Internet без перебоїв. Також в роботі проаналізовано різні методи для резервування каналів зв'язку та обґрунтовано актуальність даної системи з описом сфери її використання та її можливостями. Обґрунтовано вибір обладнання для вирішення поставленої задачі. Розроблені, сформовані та налагоджені загальний проект мережі організації, проект підсистеми резервування каналів зв'язку. Показано найчастіші сценарії роботи системи резервування, загальна топологія мережі організації, описано серії обладнання, які варто використовувати в даній мережі та налаштування всіх основних пристроїв і сервісів в мережі з їх подальшим тестуванням та перевіркою працездатності. Також наводяться результати тестування підсистеми резервування каналів зв'язку організації та їх аналіз.

КЛЮЧОВІ СЛОВА: МЕРЕЖА ОРГАНІЗАЦІЇ, РЕЗЕРВУВАННЯ, ПРОВАЙДЕР СЕРВІСУ ІНТЕРНЕТ, ВІДДАЛЕНИЙ ДОСТУП, АГРЕГАЦІЯ, МІЖМЕРЕЖЕВІ ЕКРАНИ, ПІДСИСТЕМА РЕЗЕРВУВАННЯ КАНАЛІВ ЗВ'ЯЗКУ.

ABSTRACT

The qualification work consists of the project of the subsystem of reservation of communication channels of the organization and the explanatory note to it. The explanatory note to the work contains 90 pages, 106 illustrations and 6 tables.

The purpose of the work is to develop a project of the subsystem of reservation of communication channels of the organization.

The paper identifies the main tasks for the development of a subsystem that will provide a constant and reliable connection between offices and office networks, access to the Internet without interruption. Also, the paper analyzes various methods for redundancy of communication channels and substantiates the relevance of this system with a description of its scope and capabilities. The choice of equipment for solving the problem is substantiated. Developed, formed and adjusted the general project of the organization's network, the project of the subsystem of communication channels reservation. The most common scenarios of the backup system, the general topology of the organization's network, describes the series of equipment that should be used in this network and settings of all major devices and services in the network with their further testing and verification. The results of testing the organization's communication channel reservation subsystem and their analysis are also presented.

KEY WORDS: ORGANIZATION NETWORK, RESERVATION, INTERNET SERVICE PROVIDER, REMOTE ACCESS, AGGREGATION, SCREEN DISPLAY SCREENS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 7
ВСТУП 8
РОЗДІЛ 1. ОРГАНІЗАЦІЯ РОБОТИ ПІДСИСТЕМИ РЕЗЕРВУВАННЯ КАНАЛІВ 10
1.1. Організація балансування каналів в сучасних мережах 10
1.2. Організація резервування каналів зв'язку в сучасних мережах 13
1.3. Протоколи резервування каналів 14
РОЗДІЛ 2. ПРОЕКТ ПІДСИСТЕМИ РЕЗЕРВУВАННЯ, БАЛАНСУВАННЯ ТА ЗАХИСТУ МЕРЕЖІ ОРГАНІЗАЦІЇ 25
2.1. Проект мережі організації 25
2.2. Проект підсистеми резервування 32
2.3. Cisco IOS IP SLA та EEM 36
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ РЕЗЕРВУВАННЯ КАНАЛІВ 45
3.1. Базове налагодження пристроїв мережі 45
3.2. Налагодження підсистеми резервування каналів 54
3.3. Тестування підсистеми резервування каналів зв'язку та перевірка роботи мережі та налаштованих сервісів 75
3.4. Аналіз результатів тестування 88
ВИСНОВКИ 89
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 91
ДОДАТКИ 94

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACL – Access Control List

OSI – Open Systems Interconnection

TCP – Transmission Control Protocol

WAN – Wide Area Network

IP – Internet Protocol

LAN – Local Area Network

MAC – Media Access Control

NAT – Network Address Translation

ASA – Adaptive Security Appliances

ASDM – Adaptive Security Device Manager

IEEE – Institute of Electrical and Electronics Engineers

SLA – Service-level agreement (Угода про рівень обслуговування)

QoS – Quality of service

EEM – Embedded event manager

LSA – Link State Algorithm

ОС – операційна система

МЕ – міжмережний екран

ВСТУП

Актуальність теми. Постійний доступ до мережі Інтернет є невід'ємною частиною нашого життя, зараз просто неможливо уявити світ без можливостей, які нам надає Інтернет, будь то звичайна перевірка електронної пошта або інші інтернет сервіси для поглинання контенту. Все це призводить до неминучого збільшення кількості користувачів, трафіку, з'єднань і каналів зв'язку. І кожного разу, коли в нас виникають перебої в доступі до тих чи інших сервісів, ми занепокоюємося через це, так як не можемо, наприклад, отримати доступ до сервера з картинками котиків, чи те, що може навіть налякати нас, коли не буде доступу до серверів інтернет банка в потрібний час.

Тому актуальність даної теми є дуже високою, і полягає вона в резервуванні зв'язку між різними пристроями в мережі: будь це мобільний телефон чи великий центр обробки даних. Всі вони потребують резервних каналів зв'язку для отримання доступу до потрібних даних і файлів.

Метою випускної роботи є розробка проекту підсистеми резервування каналів зв'язку організації. Дана мета обумовлює собою наступні задачі для вирішення проблеми:

- аналіз основних способів для резервування каналів зв'язку;
- розробка способів для реалізації резервування в поставлених умовах;
- вибір засобів для реалізації резервування;
- розробка мережі з можливістю подальшого розширення;
- вибір технічного забезпечення для реалізації мережі;
- реалізація підсистеми резервування каналів зв'язку організації.

Об'єктом дослідження є процес стабільної та відлагодженої роботи різних методів і способів резервування каналів зв'язку для забезпечення безперебійного доступу до потрібного вузлу мережі.

Предметом дослідження є методи і засоби використання підсистеми резервування каналів зв'язку організації.

В процесі виконання кваліфікаційної роботи був розроблений проект організації, в якому була проаналізована підсистема резервування каналів

зв’язку. При цьому були використані МЕ, система для збору інформації про продуктивність мережі в режимі реального часу IP SLA та вмонтований менеджер подій EEM.

РОЗДІЛ 1. ОРГАНІЗАЦІЯ РОБОТИ ПІДСИСТЕМИ РЕЗЕРВУВАННЯ КАНАЛІВ

1.1. Організація балансування каналів в сучасних мережах

Обмін інформацією в сучасному світі є невід'ємною складовою життя суспільства XXI століття, через різке збільшення кількості інформації. Тепер неможливо уявити світ без можливостей, які нам надає мережа Інтернет, будь то звичайна пошукова система чи електронна пошта або інші інтернет сервіси для поглинання контенту. Через введення карантину у всьому світі, збільшення трафіку в глобальній мережі може призвести до різних наслідків. Не лише проблем з завантаженням фото котиків та обривів з'єднання під час перегляду потокового відео, але й затримці в роботі таких потрібних в даний час інтернет банків. Все це сприяє тому, що кількість інформації в глобальній мережі з кожним днем лише збільшується. І збільшення трафіку потребує модернізації мережі, як апаратної частини, так і каналів зв'язку, їх резервування та балансування для отримання стабільного доступу до потрібних сервісів та надійної їх роботи в будь-якій ситуації.

В наш час значної популярності здобули сервіси стрімінгового потоку відео такі як: Netflix, YouTube, Twitch, Mixer та інші. Вони генерують сотні і тисячі теребайт трафіку в мережі, і в той же час потребують канали передачі данних з найменшою затримкою та великою надійністю при їх передачі, тому будь-який збій мережі може спричинити порушення в роботі сервісів, що призводить до великих матеріальних збитків. Вони ж, в свою чергу, є відчутними як для сервісів, так і для його клієнтів. Щоб запобігти цьому, потрібно організувати балансування навантаження на каналах їх резервування та захист.

Балансування навантаження - це процес розподілу мережевого трафіку на декілька серверів. Це гарантує, що жоден сервер та канал зв'язку не має надто великого попиту. Рівномірно розподіляючи трафік, балансування навантаження покращує роботу. Це також збільшує доступність програм та веб-сайтів для

користувачів. Сучасні мережі не можуть працювати без балансування навантаження. З часом балансування завантаження додали додаткові можливості, включаючи безпеку та застосування.

Оскільки організація задовольняє попит на свої програми, балансування навантаження вирішує, які сервери та канали можуть обробляти та пропускати цей трафік. Це підтримує хороший досвід роботи користувачів.

Балансори завантаження керують потоком інформації між сервером і пристроєм кінцевої точки (ПК, ноутбук, планшет або смартфон). Сервер може бути локальним, у центрі обробки даних або у загальнодоступній хмарі. Сервер також може бути фізичним або віртуалізованим. Балансир навантаження допомагає серверам ефективно переміщувати дані, оптимізує використання ресурсів доставки додатків та запобігає перевантаженню сервера і канала передачі. Балансори завантаження проводять постійні перевірки стану сервера і каналів, щоб переконатися, що вони можуть обробляти запити. При необхідності балансир навантаження видаляє сервери з проблемами з пулу або перенаправляє трафік на інші канали, поки вони не будуть відновлені. Деякі балансири навантажень навіть запускають створення нових віртуалізованих серверів прикладних програм, щоб впоратися зі збільшенням попиту.

Існує безліч методів балансування навантаження, в яких використовуються різні алгоритми, найкраще придатні для конкретної ситуації.

- Найменший спосіб підключення - спрямовує трафік до сервера з найменшими активними з'єднаннями. Найкорисніше, коли трафік нерівномірно розподілений між серверами, які мають велику кількість стійких з'єднань.
- Метод найменшого часу відгуку - спрямовує трафік на сервер з найменшими активними з'єднаннями та найменшим середнім часом відгуку.
- Метод Round Robin - обертає сервери, спрямовуючи трафік на перший доступний сервер, а потім переміщує цей сервер до нижньої частини

черги. Найбільш корисно, коли сервери мають однакові характеристики та не існує багато стійких з'єднань.

– IP Hash - IP-адреса клієнта визначає, який сервер отримує запит.

Балансування навантаження стало необхідністю, оскільки додатки стають складнішими, зростає попит користувачів і збільшується обсяг трафіку. Балансування навантаження дозволяє організаціям створювати гнучкі мережі, які можуть відповідати новим викликам, не загрожуючи безпеці, сервісу чи продуктивності.

Традиційно балансири навантажень складаються з апаратного обладнання. Однак вони все більше набувають програмного забезпечення. Ось чому балансири навантажень є важливою частиною цифрової стратегії організації.

Досвід упровадження та експлуатації у великих мережах фірмового протоколу резервування шлюзу Cisco Systems Inc. HSRP та відкритого протоколу IETF VRRP показав, що, з одного боку, ці протоколи повністю забезпечували виконання своєї головної функції – резервування шлюзу, а з іншого боку, мали значні проблеми при реалізації допоміжної функції – балансування (розподілу) наванта-ження. Розподіл навантаження як у протоколі HSRP, так і у протоколі VRRP можна організувати лише за статичною схемою, яка пе-редбачає ручне налагодження пристроїв на основі виміряних або передбачуваних об’ємів трафіка. Але відомо, що інформаційні по-токи у будь-якій комп’ютерній мережі змінюються динамічно, без певних закономірностей. Це означає, що статичне балансування на-вантаження не відповідає реальному стану передачі трафіка між вузлами. Тому виникла необхідніть у розробці спеціалізованого протоколу, який повинен:

– виконувати балансування навантаження без попередніх руч-них змін конфігурацій кінцевих вузлів мережі;

– виконувати балансування навантаження за алгоритмом, який обрано адміністратором, з урахуванням можливостей резервуючого пристрою та його поточного завантаження запитами від кінцевих вузлів мережі;

– забезпечувати розподіл навантаження тільки між тими з резер-вуючих пристроїв, які мають достатній пріоритет і своєчасно підт-верджують свою працездатність.[19]

Тим самим балансування навантаження в мережі може бути простим на ефективним з усіх точок зору.

1.2. Організація резервування каналів зв’язку в сучасних мережах

Використання наземної мережевої інфраструктури пов'язане з ризиками перебоїв в якості і навіть тимчасовою втратою зв'язку. Чим глибше корпоративна система комунікацій інтегрована в бізнес-процеси, тим вище в разі виникнення проблем з нею загроза для всього бізнесу.

Будь-яка наземна телекомунікаційна мережа, будь то надійно захований під землю оптичний кабель, встановлене в дата-центрі активне мережеве обладнання або система радіопередавальних пристроїв, може стати жертвою вандалізму або форс-мажорних обставин, наприклад, пожежі або природних катаклізмів. Передбачити такі моменти неможливо, але для багатьох організацій несподівані простої в роботі, викликані втратою зв'язку, можуть стати причиною серйозних фінансових втрат або інших небажаних наслідків, аж до повної зупинки діяльності. В умовах високо конкурентного ринкового середовища збої в роботі телекомунікацій негативно впливають на імідж компаній, лояльність клієнтів і є серйозною загрозою для успішного розвитку бізнесу.

Щоб підвищити рівень доступності Інтернету в офісі, можна використовувати резервний канал від другого провайдера, тим самим забезпечивши резервування доступу в Інтернет.

Сучасні маршрутизатори дозволяють налаштувати автоматичне підключення другого каналу Інтернет в разі непрацездатності першого, а також розподіляти трафік між каналами, забезпечивши балансування навантаження.

Раніше проведення другого каналу Інтернет в офіс і купівля обладнання, яке могло б забезпечити резервування, були досить дорогими, і цим могли

користуватися лише великі компанії. Однак часи змінюються, і зараз все це по кишені і малому, і, тим більше, середньому бізнесу.

У разі проблем з підключенням другого наземного Інтернет-каналу в офіс, можна скористатися послугами провайдерів, що надають доступ в Інтернет по радіорелейному зв'язку: WiMAX або LTE. В останньому випадку досить придбати недорогий LTE-модем у оператора стільникового зв'язку.

У деяких випадках використання радіоканалу для резервування є навіть більш надійним варіантом, так як кабелі наземних каналів можуть проходити по одній і тій же каналізації і, як наслідок, зростають ризики їх одночасного ушкодження.

Якщо у компанії є філії, то, щоб підвищити рівень доступності мережі центрального офісу та IT-сервісів, що надаються їм, можна налаштувати відмовостійкий VPN-тунель між центральним офісом і філіями, з можливістю резервування каналів або балансування навантаження.

Ідея резервування каналів і резервних ліній зв'язку так само стара, як і сама технологія Ethernet в промислових комунікаціях. Проблема в тому, що ця ідея суперечить «природі» Ethernet, що не передбачає замкнутих контурів в мережі, тим самим забороняючи резервні канали передачі мережевого трафіку. Однак надійність, яка забезпечується дублюванням каналів передачі даних, була і залишається базовою вимогою у багатьох системах автоматизації. Тому для використання мереж Ethernet в промислової автоматизації необхідні спеціальні протоколи, які нівелюють протиріччя між стандартними протоколами Ethernet і резервними каналами передачі трафіку.

1.3. Протоколи резервування каналів

Першим таким протоколом, що застосовувався ще в офісних мережах, був STP, розроблений інститутом IEEE та опублікований в стандарті 802.1D в 1990 році. Резервування ліній зв'язку стало можливо на базі практично будь-якого керованого комутатора, але час відновлення зв'язку за алгоритмом, закладеному

в STP, складає десятки секунд. Наступні протоколи резервування, що розвивають принципи і механізми, описані в стандарті IEEE 802.1D, працюють набагато швидше і краще відповідають специфічним вимогам промислової середовища.

Сенс резервування каналів передачі даних. Дублювання каналів передачі даних здійснюється з метою виключення таких вузлів, відмова яких здатна вивести з ладу всю систему. Так, наприклад, якщо виробнича дільниця підключена до загальної системи передачі даних через єдиний комутатор, то відмова цього комутатора призведе до зупинки всієї ділянки і спричинить, відповідно, серйозні, в тому числі фінансові наслідки. Якщо ж даний комутатор дубльований іншим комутатором, то відмова першого призводить до фактичного повернення мережі до первісного стану без резервування. Резервування дозволяє системі залишатися працездатною на період ремонту вузла, що вийшов з ладу.

Резервовані мережеві структури використовуються для двох цілей:

– регулювання навантаження на мережу - додавання резервного каналу зв'язку збільшує сумарну пропускну здатність початкового з'єднання, для цієї мети використовується протокол агрегування каналів LACP ;
– підвищення стійкості до збоїв - резервні канали зв'язку між вузлами мережі дозволяють системі перемикатися на запасні лінії зв'язку в разі відмови основної.

Незважаючи на те, що друга мета може бути досягнута в рамках першої, пріоритет найчастіше віддається підвищенню стійкості до збоїв. У промислових мережах обсяги переданої інформації менше, ніж, наприклад, в офісних мережах, зате вимоги до надійності їх доставки вище. На гарантовану доставку даних в заданий проміжок часу орієнтовані промислові протоколи зв'язку і мережеві технології. Апаратні збої, звичайно, виключити не можна, але можна зробити їх наслідки найменш відчутними для організації.

Одне з ключових вимог для промислових мереж Ethernet - відсутність петель або замкнутих маршрутів в топології, тобто між одержувачем і відправником кадру даних повинен бути єдиний шлях його доставки. Поява

замкнутого маршруту в мережі викличе лавиноподібне зростання трафіку і, отже, перевантаження мережі, тому в традиційних мережах Ethernet уникають виникнення таких петель. У промислових мережах задача протоколів резервування - це моніторинг дубльованих каналів зв'язку з метою недопущення колізій і перерозподіл трафіку в аварійних ситуаціях. Протокол резервування повинен гарантувати логічне існування тільки одного шляху доставки повідомлення в конкретний момент часу при наявності декількох фізичних шляхів. З існуючих прокладених каналів зв'язку один вибирається основним, інші чекають в резерві.

Такий принцип був вперше застосований в протоколі STP, який відстежував стан каналів зв'язку і при виявленні обривів направляв трафік з відмовленого каналу на резервний. Це означає, що зв'язок втрачається на деякий час, поки обрив виявиться, а новий канал передачі даних буде активований. Залежно від розмірів мережі і складності її топології, час відновлення зв'язку може бути різним і заздалегідь його визначити не можна.

На основі протоколу STP можна сформулювати основні вимоги до протоколів резервування Ethernet в промисловому середовищі:

- Певний час відновлення мережі: період часу від моменту розриву основного з'єднання до відновлення зв'язку з резервного з'єднанню повинен бути менше певної допустимої величини.
- Вимоги до мережі: для протоколу повинні бути визначені - допустима топологія мережі, максимальна кількість вузлів (комутаторів), типи з'єднань та ін.
- Протокол повинен базуватися на стандартизованому методі або алгоритмі. Тільки так можна гарантувати сумісність з мережевим устаткуванням та іншими мережевими протоколами.

Перша вимога традиційно для промислових мереж, що працюють в реальному часі. Протокол резервування може бути задіяний, якщо максимально можливий час відновлення задовольняє вимогам процесу або програми, для якого мережа передачі даних використовується.

Технології та рішення: RSTP / MSTP.

В останні роки згаданий протокол STP був витіснений своїм більш швидким послідовником - протоколом RSTP (Rapid Spanning Tree Protocol), описаним у стандарті IEEE 802.1D-2004. Даний протокол підтримує безліч різних топологій і базується на тому, що з кожного мережного підключення виділяється деревоподібна структура, так що між будь-якими двома вузлами мережі в кожний момент часу існує єдиний маршрут передачі даних. Всі з'єднання, які не ввійшли в активне «дерево», вважаються резервними і не активні до зміни топології. Протокол базується на мостових з'єднаннях (BPDU - Bridge Protocol Data Units), серед яких вибирається кореневий міст (з'єднання комутатор-комутатор). Все інше «дерево» будується від нього. Будь-яка зміна в активному «дереві» означає зміну в складі BPDU з розсилкою спеціального BPDU-кадру по вузлах мережі, після чого ті активують резервні маршрути для трафіку. В протокол вбудовано захист від перевантаження мережі даними кадрами, які можуть привести до збільшення часу відновлення.

Протокол RSTP підтримує велику кількість вузлів і забезпечує час відновлення зв'язку близько 1 секунди. Цей час багато в чому залежить від місця виникнення обриву зв'язку в мережі, тому не може бути чітко визначений заздалегідь.

Даний істотний недолік можна обійти, якщо обмежити топологію мережі кільцевою структурою. Тим самим можна домогтися дотримання часу відновлення мережі близько 100 мс і менше.

MSTP - нова ітерація описаного протоколу резервованих «дерев», і працює вона за тим же принципом. Якщо RSTP працює незалежно від віртуальних мереж VLAN, то структури MSTP, навпаки, існують в складі віртуальної мережі і таким чином забезпечують більше зручностей і варіацій в плані можливих топологій і розподілу навантаження. Обидва протоколи сумісні між собою і можуть бути реалізовані всередині однієї мережі.

Резервування кільця. Кільцева топологія зручна насамперед тим, що з нею досягається певний і гарантований час відновлення зв'язку після збою, що

враховує кількість комутаторів в кільці. Стандарт IEC 62439-1 описує приклад розрахунку часу відновлення для кільця, а також додаткові обмеження (наприклад, RSTP не може бути налаштований на портах комутатора, не задіяних в кільці). Однак RSTP не розроблений для кільцевого резервування, тому поступається спеціалізованим протоколам типу MRP. У комутаторах Hirschmann реалізована підтримка обох протоколів, і, хоча приписів щодо їх спільного застосування немає, використовувати в цьому випадку краще MRP.

MRP - стандартизоване резервоване кільце.

Протокол MRP був спеціально розроблений для промислового застосування. Він описаний в стандарті IEC 62439-2 для промислових мереж Ethernet з високим ступенем доступності. MRP підтримує тільки кільцеву топологію мережі з кількістю комутаторів не більше 50, гарантуючи заздалегідь певний час відновлення зв'язку в разі виникнення збою. Час відновлення залежить від обраних параметрів протоколу MRP і може складати від 10 до 500мс, причому максимальний час можна встановити заздалегідь. Наприклад, при максимальному часу відновлення, що дорівнює 200 мс, типове значення складе 50-60 мс при середньому завантаженні мережі.

Протокол передбачає об'єднання в кільце групи комутаторів, один з яких бере на себе роль ведучого (MRM - Media Redundancy Manager). Він контролює цілісність кільця, передаючи по кільцю тестові кадри даних в одну сторону і отримуючи їх по ланцюжку з іншого боку. Для запобігання колізій всі дані, крім тестових кадрів, блокуються на одному з двох кільцевих портів MRM-комутатора, утворюючи фактично лінійну топологію мережі. Якщо ведучий комутатор не отримує тестові кадри, це означає розрив кільця, в такому випадку він розблокує друге з'єднання, відновивши передачу даних.

Решта комутатори в кільці грають роль клієнтів (MRC - Media Redundancy Clients) і передають тестові кадри по ланцюжку з одного кільцевого порту в інший. Також відомі комутатори передають головному інформацію про зміну стану їх портів. Якщо MRM-комутатор отримав повідомлення від MRC-комутатора про відмову його кільцевого порту раніше, ніж недорахувався

тестових кадрів, то він керується цим попередженням і активує заблоковане з'єднання. Такий підхід забезпечує найменший можливий час відновлення зв’язку в мережі.

PRP - паралельне резервування.

Незважаючи на швидкість роботи MRP і його універсальність для широкого кола завдань, існують додатки, де неприпустимо навіть мінімальний час відновлення мережі. Для таких додатків необхідний зовсім новий підхід до питання високої доступності мережі. В основі цього підходу - існування мінімум двох одночасно активних сполук між двомя вузлами мережі таким чином, що відправник інформації посилає кадри даних синхронно з двох Ethernet- каналів. Одержувач за допомогою протоколу резервування приймає перший кадр даних і відхиляє другий. Якщо другий кадр даних не отримано, адресат робить висновок про обрив зв'язку у відповідному каналі.

Даний механізм резервування реалізований в протоколі PRP (Parallel Redundancy Protocol), описаному в стандарті IEC 62439-3. PRP використовує дві паралельні мережі передачі даних з довільною топологією, не обмеженої ні кільцями, ні іншими структурами.[23] Більш того, в двох паралельних мережах може не бути резервування зовсім, а можуть застосовуватися протоколи MRP і RSTP. Таким чином, принципова перевага PRP полягає в його «безшовному» резервуванні з відсутністю навіть малого часу перемикання з основного на резервний канал зв'язку. Високий рівень доступності мережі з паралельним резервуванням дотримується за умови, що обидві підмережі, об'єднані PRP, не можуть відмовити одночасно.

Протокол PRP реалізується на кінцевих пристроях (рис. 1.1). Комутатори мережі працюють незалежно від даного протоколу і, відповідно, не повинні мати ніякої спеціальної апаратної або програмної підтримки.

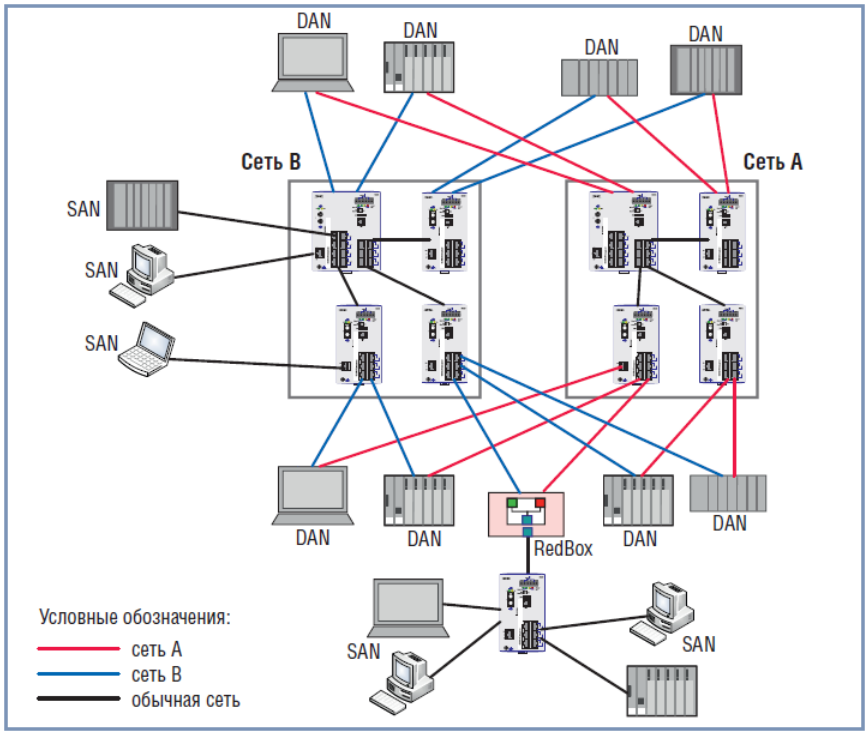


Рис. 1.1. Реалізація PRP на кінцевих пристроях

Кінцеві пристрої з підтримкою PRP (DANP -Double AttachedNode for PRP) мають два мережевих інтерфейси і підключаються до двох незалежних мереж. При цьому мережі можуть мати різну топологію, середовище і швидкість передачі. До мережі можуть підключатися і звичайні кінцеві пристрої з одним мережевим інтерфейсом (SAN - Single Attached Node). Також можуть використовуватися кінцеві пристрої типу DANP в ролі проксі-серверів (так звані RedBox - скорочення від Redundancy Box), до яких підключені декілька SAN-пристроїв. Від SAN-пристрою не потрібно ніякої спеціальної підтримки PRP. Цю можливість зручно застосовувати на практиці, користуючись тим, що в мережах з високою доступністю наявність паралельного резервування критично не для всіх пристроїв, тому кінцеві пристрої за ступенем важливості можна розділити на типи: DANP і SAN і з'єднати, використовуючи дубльований або єдиний канал зв'язку відповідно. Кінцеві пристрої з можливістю паралельного резервування типу DANP повинні контролювати дубльовані кадри Ethernet. Отримавши дані для передачі в мережу, пристрій, що реалізує протокол PRP, посилає їх по двом мережним інтерфейсам одночасно. Таким чином, два кадри Ethernet відправляються з незалежних мереж до одного одержувача і, з огляду на різну

топологію і пропускну здатність обох мереж, доходять до адресата з різною затримкою. Перший отриманий одержувачем кадр приймається і передається на верхній рівень, другий - відкидається. В результаті мережевий додаток, що використовує отримані дані, не "відчуває" різниці між резервованим з PRP і звичайним Ethernet-інтерфейсом.

Ідентифікація дублюючих кадрів здійснюється за спеціальним контрольним маркером - RCT (Redundancy Control Trailer), поміщеним в Ethernet-кадр PRP-пристроєм. На додаток до ідентифікатора підмережі і призначених для користувача даних в кадр поміщається 32-бітове поле, що включає номер послідовності PRP. За цим номером кінцевий пристрій ідентифікує кадр і або передає його на верхній рівень, або видаляє. RCT-маркер знаходиться в кінці блоку даних, тому такий формат Ethernet-даних зчитується як DANP, так і SAN пристроями. Ця властивість дозволяє мережевим пристроям обмінюватися інформацією за відсутності резервування.

Вцілому протокол PRP дозволяє створити мережу з високим ступенем доступності, довільною топологією, але вимагає значно більших витрат на обладнання, інфраструктуру і мережеві компоненти.

HSR - безшовне резервування.

Протокол HSR (High-availability Seamless Redundancy) - подальший розвиток ідеї паралельного резервування. Однак якщо у випадку з PRP йшлося про резервування мережі, то HSR - це протокол резервування з'єднань. HSR, як і PRP, описаний в стандарті IEC 62439-3. Але на відміну від PRP протокол HSR розроблений для кільцевої топології мережі. Як і PRP, він використовує два мережевих порта у кінцевого пристрою для підключення до мережі, але ланцюжком, замкнутої в кільце.

Формат кадру даних у протоколі HSR аналогічний PRP. Ідентифікатор HSR схожий на поле RCT: включає розмір призначених для користувача даних, тип порту відправника (1-й або 2-й порт) і номер послідовності. Однак якщо ідентифікатор протоколу PRP йде всередині стандартного Ethernet-кадру, то у випадку з HSR ідентифікатор протоколу йде на початку. Тому HSR-пристрої

розпізнають дані на льоту і швидше їх обробляють, передаючи з першого на другий інтерфейс по ланцюжку. При цьому кожний кінцевий пристрій пропускає через себе всі кадри даних, читає заголовки і відбирає собі кадри зі своєю адресою одержувача, а також широкомовні повідомлення. Для запобігання циркуляції по колу широкомовних повідомлень пристрій-відправник видаляє повідомлення, які пройшли повне коло по мережі.

Відміну від мережі з паралельним резервуванням, в HSR-кільце не можна включити стандартний пристрій з одним мережевим інтерфейсом - кільце не буде замкнено і формат даних з HSR-заголовком не розпізнає. Аналіз кадру даних на другому рівні OSI з ідентифікатором PRP (він знаходиться в полі додаткової інформації) можливий і звичайним пристроєм - воно просто пропустить поле з RCT. Формат даних cHSR-заголовком виходить нестандартний, і кінцевий пристрій без підтримки HSR-протоколу його не розпізнає. Проте, в цьому випадку можна використовувати посередника RedBox, який включається в HSR-кільце і має додаткові підключення до кінцевих пристроїв поза кільцем.

Стандартні пристрої «не розуміють» HSR-дані, проте самі HSR-пристрої «розуміють» стандартний формат даних. Це необхідно для конфігурації і діагностики вузлів кільця. При цьому стандартні кадри даних не проходять по колу, як HSR-дані, а пересилаються безпосередньо між станцією управління і пристроєм.

HSR-кільце починає роботу в штатному режимі тільки після відключення станції управління і замикання ланцюга. HSR-кільця можна з'єднувати між собою двома 4-портовими пристроями, так званими QuadBox. Пристрої дублюють один одного, тому загальна мережа також залишається резервованою.

Що стосується часу відновлення, то тут HSR-протокол поводиться аналогічно PRP: кадри даних одночасно розсилаються по двох портах в обох напрямках по кільцю, в разі збою, одна з черг даних досягне одержувача. Такий

підхід гарантує резервування з нульовим часом відновлення і в той же час не вимагає додаткової мережевої структури.

З недоліків HSR можна відзначити обмежену гнучкість (тільки кільцева топологія), дворазовий обсяг трафіку, що передається по мережі з дублюванням кадрів даних, складність реалізації (спеціальний FPGA-чіп в кожному пристрої, синхронізація по протоколу IEEE 1588).

На практиці не існує ні ідеальної мережевої топології, ні ідеального протоколу резервування, що задовольняє всім вимогам промислових мереж. Правильний вибір топології мережі і протоколу резервування залежить від багатьох факторів, таких як фізичні вимоги до розташування мережевих компонентів.

Протокол HSR є новим (стандарт IEC 62439-3 прийнятий в березні 2016 року) і перспективним. Серед основних сфер його застосування слід зазначити АСУ в енергетиці. Він навіть буде включений в другу версію стандарту для електричних підстанцій IEC 61850. Протокол HSR буде забезпечувати функціонування мережі Ethernet в реальному часі разом з протоколом синхронізації годин IEEE 1587. [6]

Для підвищення надійності і гнучкості мережі протоколи резервування можна комбінувати між собою. Наприклад в мережі зі змішаною топологією, із застосуванням паралельного і кільцевого резервування. Можна зробити прогноз, що в майбутньому протоколи PRP і HSR (їх подальші ітерації) витіснять існуючі протоколи кільцевого і паралельного резервування.

Впровадженням протоколів PRP iHSR в реальні рішення займаються провідні світові розробники мережевого обладнання, такі як Siemens, Hirschmann (Belden), ZHAW. Також над ідеями паралельного резервування працюють компанії CISCO, RuggedCom. Перші мікросхеми FPGA виробництва компаній Altera і Xilinx з реалізацією цих протоколів існують з середини 2010 року. Механізми протоколів HSR і PRP були успішно протестовані з емуляцією на програмному рівні. Про функціонування в реальному часі з програмною реалізацією, звичайно, мова не йде, зате можна позитивно оцінити їх

працездатність у великих мережах, взаємодія з іншими протоколами резервування другого рівня OSI, GOOSE-повідомленнями протоколу IEC / IEC 61850.

На даному етапі розвитку промислового мережевого обладнання одним з найбільш передових комутаторів другого і третього рівнів OSI є Hirschmann MACH 1000 (торгова марка компанії Belden). Комутатори цієї серії відповідають найжорсткішим промисловим вимогам: функціонування в реальному часі (протокол IEEE 1588), підтримка технологій резервування RSTP, MRP, LACP, а також найбільш швидкого варіанту кільцевого резервування - Fast HIPER-Ring з дубльованим з'єднанням кілець. Крім того, MACH 1000 відповідає стандарту МЕК 61850-3, може функціонувати в широкому температурному діапазоні -40 ... + 85 ° С і в умовах сильних електромагнітних завад. Серія MACH 1000 є перспективною і буде служити базою для інтеграції протоколів резервування PRP і HSR. На жаль віртуальних версій даних комутаторів та способів їх віртуалізації зараз немає, через це для прикладу будуть використовуватися більш прості їх аналоги від компанії Cisco.[13]

РОЗДІЛ 2. ПРОЕКТ ПІДСИСТЕМИ РЕЗЕРВУВАННЯ, БАЛАНСУВАННЯ ТА ЗАХИСТУ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1. Проект мережі організації

В даній роботі була розглянута мережа організації, що представлена трьома офісами, різними за складом та призначенням. Кожна з філій має можливість розширити кількість офісів та пристроїв за рахунок підключення до вільних портів комутатора та можливості відтворення його копій в мережі.

Для підключення пристроїв мережі між собою використовуються високошвидкісні порти FastEthernet/GigabitEthernet, інтерфейси представлені нижче можуть змінюватися в залежності від пристрою та каналу зв'язку і представлені в таблиці є лише прикладом для реальної мережі.

Детальну топологію з'єднань можна побачити в табл. 2.1-2.3.

Таблиця 2.1

Параметри інтерфейсів пристроїв першого офісу

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Міжмережний екран MAIN_OFFICE	Gi0/0	Комутатор AD_SW	E0/2
	Gi0/1	Інтернет провайдер ISP_1	Gi0/0
	Gi0/2	Інтернет провайдер ISP_2	Gi0/0
	Gi0/5	Роутер OFFICE_R	Fa0/0
	Gi0/6	Робоча станція ADMIN	E0
	Mngm0/0	Робоча станція Conf_netbook	E0
Роутер OFFICE_R	Fa0/0	Міжмережний екран MAIN_OFFICE	Gi0/5
	Fa1/1	Комутатор OFFICE	E0/0
	Fa2/0	Комутатор MARKETING_OFFICE	E0/0
Комутатор OFFICE	E0/0	Роутер OFFICE_R	Fa1/0
	E0/1	Робоча станція OFFICE_PC_1	E0
	E0/2	Робоча станція OFFICE_PC_2	E0
	E0/3	Робоча станція OFFICE_PC_3	E0
Комутатор MARKETING_OFFICE	E0/0	Роутер OFFICE_R	Fa2/0
	E0/1	Робоча станція MARKETING _PC_1	E0
	E0/2	Робоча станція MARKETING _PC_1	E0

Продовження таблиці 2.1

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Комутатор AD_SW	E0/1	Міжмережний екран MAIN_OFFICE	Gi0/0
	E0/2	Windows server AD Win_S	E0
Робоча станція MARKETING _PC_1	E0	Комутатор MARKETING_OFFICE	E0/1
Робоча станція MARKETING _PC_2	E0	Комутатор MARKETING_OFFICE	E0/2
Робоча станція OFFICE_PC_1	E0	Комутатор Switch1-1	E0/1
Робоча станція OFFICE_PC_2	E0	Комутатор Switch1-1	E0/2
Робоча станція OFFICE_PC_3	E0	Комутатор Switch1-1	E0/3
Робоча станція ADMIN	E0	Міжмережний екран MAIN_OFFICE	Gi0/6
Робоча станція Conf_netbook	E0	Міжмережний екран MAIN_OFFICE	Mngm0/0
Windows server AD Win_S	E0	Комутатор AD_SW	E0/1

Таблиця 2.2

Параметри інтерфейсів пристроїв другого офісу

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Міжмережний екран SMALL_OFFICE	Gi0/0	Інтернет провайдер ISP_1	Gi0/0
	Gi0/1	Інтернет провайдер ISP_2	Gi0/0
	Gi0/2	Комутатор S_O_SW	E0/0
	Gi0/3	Маршрутизатор DB_R	E1/2
Комутатор S_O_SW	E0/0	Міжмережний екран SMALL_OFFICE	Gi0/2
	E0/2	Робоча станція VPC20	E0
	E0/3	Робоча станція VPC21	E0
	E0/1	Комутатор SW_BOOKKEEPER	E0/0
Комутатор SW_BOOKKEEPER	E0/0	Комутатор S_O_SW	E0/1
	Fa0/1	Робоча станція VPC18	E0
	Fa0/2	Робоча станція VPC19	E0
Робоча станція WS18	E0	Комутатор SW_BOOKKEEPER	Fa0/1
Робоча станція WS19	E0	Комутатор SW_BOOKKEEPER	Fa0/2
Робоча станція WS20	E0	Комутатор S_O_SW	Fa0/2
Робоча станція WS21	E0	Комутатор S_O_SW	Fa0/3

Таблиця 2.3

Параметри інтерфейсів пристроїв третього офісу

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Маршрутизатор DB_R	E1/0	Маршрутизатор HOME	Fa2/0
	E1/1	Інтернет провайдер ISP_2	Gi0/0
	E1/2	Міжмережний екран SMALL_OFFICE	Gi0/3
	E1/3	Комутатор DATABASE_OFFICE	E0/0
	E1/4	Комутатор DATABASE_OFFICE	E0/1
	E1/5	Інтернет провайдер ISP_1	Gi0/0
Комутатор DATABASE_OFFICE	E0/0	Маршрутизатор DB_R	E1/3
	E0/1	Маршрутизатор DB_R	E1/4
	E0/2	Міжмережний екран ASA_Active	Gi0/0
	E0/3	Міжмережний екран Active_Failover	Gi0/0
Міжмережний екран ASA_Active	Gi0/0	Комутатор DATABASE_OFFICE	E0/2
	Gi0/1	Комутатор INSIDE_DB_NETWORK	E0/0
	Gi0/2	Міжмережний екран Active_Failover	Gi0/2
Міжмережний екран Active_Failover	Gi0/0	Комутатор DATABASE_OFFICE	E0/3
	Gi0/1	Комутатор INSIDE_DB_NETWORK	E0/1
	Gi0/2	Міжмережний екран ASA_Active	Gi0/2
Комутатор INSIDE_DB_NETWORK	E0/0	Міжмережний екран ASA_Active	Gi0/1
	E0/1	Міжмережний екран Active_Failover	Gi0/1
	E0/2	Комутатор DB_WORKER	E0/0
Комутатор DB_WORKER	E0/0	Комутатор INSIDE_DB_NETWORK	E0/2
	E1/0	Комутатор INSIDE_DB_NETWORK	E0/3
	E0/1	Робоча станція DB_WORKER28	E0
	E0/2	Робоча станція DB_WORKER29	E0
	E0/3	Робоча станція DB_WORKER30	E0
Робоча станція DB_WORKER28	E0	Комутатор DB_WORKER	E0/1
Робоча станція DB_WORKER29	E0	Комутатор DB_WORKER	E0/2
Робоча станція DB_WORKER30	E0	Комутатор DB_WORKER	E0/3

Для забезпечення функціонування мережі представленої в проекті було обрано оптимальні маршрутизатори і комутатори компанії Cisco, котрі мають адаптованість під модернізацію модулями для подальшого розширення мережі.

Так як мережа розробляється в симуляторі, то конкретні моделі пристроїв назвати важко, в деяких випадках, навіть неможливо, так, як ми використовуємо віртуалізовані ресурси. Тому нижче охарактеризовані серії пристроїв, які були використані для побудови мережі.

Маршрутизація мережі реалізована маршрутизаторами Cisco 7200 Series є самими поширеними та універсальними рішеннями для великих компаній, через це багато хто довірив свій мережевий інтерфейс цим пристроям. Дана серія маршрутизаторів має модульну структуру і можливості розширення кількості інтерфейсів, тому активно використовується не тільки великими компаніями.

Володіючи високою продуктивністю, маршрутизатори здатні відправляти дані в мультипотоку, тим самим, такий тип передачі сприяє підвищенню швидкості обміну інформацією між вузлами мережі. Це досягається за рахунок мережевого процесора Cisco 7200 NPE-G2. Цей процесор допомагає створити мережну платформу, здатну не тільки швидко та якісно передавати дані, але також і справлятися із завантаженістю на каналах передачі. У разі її виникнення вмикається магістральна передача, яка допомагає справитися з завантаженістю відправивши надлишок пакетів протягом короткого періоду часу. Також на вибір даних пристроїв впливає широкий набір підтримуваних з'єднань, легкість в обслуговуванні і управлінні, та збільшена масштабованість і гнучкість завдяки новим модулям.

Cisco 7200 Series має ряд переваг, до яких відносять велику кількість віртуальних приватних мереж до 5000 на базі IPsec, модулі швидкої передачі відео та даних модульну архітектуру та форм-фактор 3U .[17]

Cisco ASA - це лінійка модульних багатофункціональних пристроїв захисту, вона є апаратним фаєрволом з інспекцією сесій зі збереженням стану (stateful inspection). ASA вміє працювати в двох режимах:

– routed (режим маршрутизатора, за замовчуванням)

– transparent (прозорий міжмережевий екран, коли ASA працює як міст з фільтрацією)

У своїй роботі Cisco ASA використовує не загальну операційну систему, а свою власну, інтегровану в пристрій. Ця ОС, схожа на Cisco IOS, з самого початку розроблялася з розрахунком на високу продуктивність і безпеку, пристрій здатний аналізувати до 500 000 з'єднань одночасно.

Cisco ASA - фаейрвол, який використовує динамічну фільтрацію, яка здійснюється з використанням алгоритму ASA - Adaptive Security Algorithm. Він багато разів безпечніше і надійніше статичної фільтрації і прикладних фаейрволов proxy. ASA контролює трафік, ізолюючи сегменти мережі, підключені до фаейрволу.

Всі інтерфейси отримують певний рівень безпеки, який змінюється від 0 до 100. Виходячи з цих даних, ASA змінює свою поведінку, забороняючи і дозволяючи ті чи інші з’єднання. Списки доступу можуть застосовуватися для заборони трафіку з високим рівнем довіри на більш низький, і навпаки.

ASA зберігає всі дані про сесії в мережі, передаючи її в таблицю стану, використовуючи потім ці дані для контролю всього трафіку, який проходить через фаейрвол. Трафік проходить аналіз, і, якщо інформація не відповідає очікуваним вимогам, з'єднання скидається. Іншими словами, безпека базується на з'єднанні, а не на пакеті, як це буває при статичній пакетній фільтрації, що практично повністю виключає можливість злому мережі методом hijack(привіт повідомленнями).

Починаючи з сьомої версії ОС, Cisco ASA здатне підтримувати технологію Security Context - віртуальних фаейрволів. З її допомогою можна встановити на одному пристрої кілька окремо працюючих фаейрволів - з різними інтерфейсами, конфігурацією, політикою безпеки та іншими параметрами.

Для комутації мережі доречно використовувати сімейство комутаторів Cisco Catalyst 2960-X, хоча це не є обов’язково. Комутатори Циско Catalyst є провідними продуктами серед комутаторів другого рівня. Їх використання

дозволяє упростити експлуатацію IT-інфраструктури, підвищити рівень безпеки бізнес-процесів, забезпечити стійку роботу мережі.

Для забезпечення функціонування мережі, перш за все було виконано розрахунок параметрів IP-адресації. Розраховуючи параметри IP-адресації, особлива увага була приділена економії IP-адрес, так, як наша організація використовуватиме протокол IPv4, хоча в майбутньому краще модернізувати мережу для подвійного стеку, а також приділити увагу можливості подальшого розширення внутрішньої мережі організації. Внутрішня адресація офісів в мережі буде налагоджена за рахунок протоколу динамічної конфігурації вузла – Dynamic Host Configuration Protocol (DHCP). Детальні параметри адресації мереж кожного з офісів оремо представлені в табл. 2.4-2.6.

Таблиця 2.4

Параметри адресації мережі першого офісу

Підмережа/ Пристрій	Інтерфейс/ Адаптер/Шлюз	IP-адреса	Маска підмережі	Пре-фікс
Міжмережний екран MAIN_OFFICE	Gi0/0	48.214.24.1	255.255.255.0	/24
	Gi0/1	10.0.0.1	255.255.255.0	/24
	Gi0/2	20.0.0.1	255.255.255.0	/24
	Gi0/5	192.2.24.1	255.255.255.252	/30
	Gi0/6	214.2.24.1	255.255.255.252	/30
	Mngm0/0	1.1.1.1	255.255.255.252	/30
Маршрутизатор OFFICE_R	Fa0/0	192.2.24.2	255.255.255.252	/30
	Fa1/0	192.168.0.1	255.255.255.0	/24
	Fa2/0	192.168.1.1	255.255.255.0	/24
Комутатор AD_SW	Vlan1	48.214.24.2	255.255.255.0	/24
Комутатор OFFICE	Vlan1	192.168.0.2	255.255.255.0	/24
Комутатор MARKETING_OFFICE	Vlan1	192.168.1.2	255.255.255.0	/24
Windows server AD Win_S	E0	48.214.24.70	255.255.255.0	/24
Робоча станція ADMIN	E0	214.2.24.2	255.255.255.252	/30
Робоча станція MARKETING _PC_1	E0	DHCP		
Робоча станція MARKETING _PC_2	E0			
Робоча станція OFFICE_PC_1	E0			
Робоча станція OFFICE_PC_2	E0			
Робоча станція OFFICE_PC_3	E0			

Таблиця 2.5

Параметри адресації мережі другого офісу

Підмережа/ Пристрій	Інтерфейс/ Адаптер/Шлюз	IP-адреса	Маска підмережі	Пре-фікс
Міжмережний екран SMALL_OFFICE	Gi0/0	10.0.0.2	255.255.255.0	/24
	Gi0/1	20.0.0.2	255.255.255.0	/24
	Gi0/2	192.168.4.1	255.255.255.0	/24
	Gi0/3	192.2.24.6	255.255.255.252	/30
Комутатор S_O_SW	Vlan 1	192.168.4.2	255.255.255.0	/24
	E0/1	192.168.3.1	255.255.255.252	/30
Комутатор SW_BOOKKEEPER	Vlan1	192.168.3.2	255.255.255.0	/24
Робоча станція WS20	E0	194.168.4.3	255.255.255.0	/24
Робоча станція WS21	E0	194.168.4.4	255.255.255.0	/24
Робоча станція WS19	E0	DHCP		
Робоча станція WS18	E0			

Таблиця 2.6

Параметри адресації мережі третього офісу

Підмережа/ Пристрій	Інтерфейс/ Адаптер/Шлюз	IP-адреса	Маска підмережі	Пре-фікс
Маршрутизатор DB_R	E1/0	195.2.3.1	255.255.255.128	/25
	E1/1	20.0.0.3	255.255.255.0	/24
	E1/2	192.2.24.5	255.255.255.252	/30
	E1/3	Agregation link		
	E2/0			
	E0/0	10.0.0.3	255.255.255.0	/24
Комутатор DATABASE_OFFICE	Vlan1	10.10.10.5	255.255.255.128	/25
Міжмережний екран ASA_Active	Gig0/0	10.10.10.2	255.255.255.0	/24
	Gig0/1	192.168.5.1	255.255.255.0	/24
	Gig0/2	Synchronization channel		
		172.2.24.1	255.255.255.252	/30
Міжмережний екран Active_Failover	Gig0/0	10.10.11.2	255.255.255.0	/24
	Gig0/1	192.168.5.2	255.255.255.0	/24
	Gig0/2	Synchronization channel		
		172.2.24.2	255.255.255.252	/30
Комутатор INSIDE_DB_NETWORK	Vlan 1	192.168.5.3	255.255.255.0	/24
Комутатор DB_WORKER	Vlan 1	192.168.5.4	255.255.255.0	/24
Робоча станція DB_WORKER28	E0	DHCP		
Робоча станція DB_WORKER29	E0			
Робоча станція DB_WORKER30	E0			

2.2. Проект підсистеми резервування

Мережу з трьома офісами та віддаленим доступом, для роботи під час надзвичайних ситуацій обрано не випадково. В ній можна проаналізувати найчастіше використовувані типи резервування, особливості мереж сучасних організацій та використати нові типи резервування та балансування, які не були доступні для таких організацій ще декілька років тому.

Основна частина резервування в такій мережі організації, це використання в мережі декілька провайдерів, та прокладення додаткових маршрутів зв'язку для можливості продовження роботи під час НП на лініях зв'язку провайдерів інтернету, також особливу увагу треба приділити обладнанню та його розміщенню в організації. Так, як деяке обладнання потребує особливих умов експлуатації, наприклад серверна кімната з віртуальними робочими машинами та сервером Windows 10 Server потребує контролю вологи та температури в приміщенні, для більш стабільної та довгої роботи з хорошою тривалістю роботи (uptime). Також все мережеве обладнання бажано розмістити в серверних стійках або шафах для обмеження доступу до нього. Ще треба звернути увагу на лінії зв'язку, які проходять всередині приміщень, всі вони повинні бути прокладені в кабель каналах, для зменшення ризиків пошкодження та несанкційованого доступу до мережі.

Ще одна частина резервування в такій мережі- це використання так званих standby пристроїв, або очікуючих пристроїв, які будуть резервувати найбільш потрібну частину мережі і в деяких випадках допомагати збільшити пропускну здатність каналів мережі. Хоча цей спосіб є доволі накладним, так, як для реалізації треба 2 пристрої, які будуть працювати або, як active/standby або active/active failover в ASA Firewall.



Рис. 2.1. Cisco ASA 5500 Series Firewalls

Контроль з'єднань між вузлами мережі забезпечує вбудований мережевий екран з механізмами інспекції пакетів з урахуванням стану протоколу (stateful inspection firewall) на рівнях 2-7, який дозволяє відстежувати стан всіх мережевих комунікацій і допомагає запобігти несанкціонованому доступу до мережі.

ASA 5500 дозволяє організувати віддалений доступ до мережі за допомогою VPN на основі технологій IPSec і SSL сертифікатів. Ці технології є хорошим способом організації віддаленого доступу до мережі з важливою інформацією при передачі її через публічні мережі, такі як Інтернет.

ASA 5500 може функціонувати в режимі transparent mode тобто прозорому режимі, при цьому вона не буде видимим вузлом мережі, і буде аналізувати трафік, який йде до користувачів, забезпечуючи необхідний рівень захисту і в разі потреби відправляти «ненадійні» пакети на додатковий аналіз для подальшої модерації трафіку.

Шляхом реалізації на одному апаратному пристрої декількох віртуальних фаерволів Cisco ASAv можна забезпечити більш складну і стійку мережу, яка в свою чергу збільшить гнучкість налаштувань мережі організації та в деяких

випадках зменшить фінансові затрати на апаратне забезпечення мережі та модернізацію, так як потрібно буде лише купити ліцензію на використання більш нової версії програмного забезпечення Cisco ASAv.

Розширити функціональність ASA можна за допомогою апаратних модулів та карт для захисту від вторгнень (AIP-SSM) і захисту контенту (CSC-SSM). Модуль AIP-SSM містить базу сигнатур мережевих атак, тим самим аналізуючи трафік в мережі він порівнює сигнатури і може блокувати небажаний трафік або атаки. Модуль CSC-SSM призначений для захисту від широкого спектру атак на кінцеві пристрої і шкідливого програмного забезпечення, містить у своєму складі антивірус, захист від шпигунських програм, фільтр URL-посилань, механізми захисту від фішингу та дозволяє захистити недосвідчених користувачів інтернету від типових атак на кінцеві пристрої та офіси.[15]

В нашій мережі буде використовуватись аварійне перемикання, тобто 2 пристроя Cisco ASA один з яких буде активний та постійно буде передавати дані, а другий буде резервуючим та перемикання буде проводитись при проблемах з каналами зв’язку або проблемами в роботі самого пристрою. В нашій мережі краще використати режим active/active failover, але, нажаль, реалізація даного режиму роботи потребує реального обладнання, і ми не можемо реалізувати це в проекті мережі організації через обмеження середовища EVE-NG та GNS3.

В данній підсистемі резервування каналів також можна використовувати агрегування каналів- це дозволяє об'єднати кілька фізичних каналів в один логічний. Так, як при обриві з’єднання одного каналу буде доступний інший канал передачі, ми можемо об’єднувати багато фізичних каналів, кожен з яких може бути прокладений іншим шляхом для забезпечення більшої надійності мережі.

Для маршрутизації в мережі обрано маршрутизатори серії 7200 від корпорації Cisco. Вони мають великий набір сервісів, які забезпечують не лише маршрутизацію, а й допомагають налаштувати роботу мережі за багатьма параметрами.



Рис. 2.2. Маршрутизатор Cisco серії 7200

Для комутації вузлів в мережі були обрані 2 типа комутаторів серії Catalist від компанії Cisco. Це комутатор 2 рівня Cisco Catalyst 2960-X та багаторівневий комутатор Cisco Catalyst 3560.

Комутатори Cisco Catalyst серії 2960-X пропонують цілий ряд можливостей забезпечення безпеки для обмеження доступу в мережу і зниження числа загроз, а також пропонують ряд можливостей резервування і відмовостійкості для забезпечення безперебійної роботи і постійної доступності мережі.



Рис. 2.3. Комутатор Cisco Catalyst серії 2960-X

Комутатори Cisco Catalyst серії 2960-X забезпечують інтелектуальне управління трафіком, підтримуючи безперебійну роботу. Гнучкі механізми маркування, класифікації та планування забезпечують найвищу продуктивність при передачі даних, голосового і відеотрафіка на швидкості, що відповідають провідному підключенню.[18]



Рис. 2.3. Стек комутаторів Cisco Catalyst серії 3560

Комутатори третього рівня моделі OSI обрані для даної мережі через свої особливості швидкісної роботи та зниження затримки мережі, оскільки пакет не повинен створювати додаткові переходи, щоб пройти через маршрутизатор та спрощене усунення помилок, оскільки виправлення помилок у шарі L2 є складним. Ще одною перевагою роботи з будь-яким L3-комутатором є те, що він продуктивніше будь-якого маршрутизатора (продуктивність в мільйонах пакетів в секунду у комутаторів проти тисяч пакетів в секунду у маршрутизаторів).[16]

2.3. Cisco IOS IP SLA та EEM

Cisco IP SLA є функціональною програмою в Cisco IOS, яка надає користувачеві можливість аналізувати рівень обслуговування IP для додатків і сервісних служб. Для цього IP SLA використовує метод активного тестування за рахунок безперервної генерації трафіку надійним і передбачуваним методом. Активне тестування дозволяє проводити вимірювання ключових показників

якості мережі передачі даних на базі протоколу IP. З Cisco IP SLA оператори зв'язку можуть вимірювати і контролювати SLA послуг, що надаються, а їхні клієнти в реальному часі отримувати інформацію про відповідність рівня сервісів SLA. Cisco IP SLA дозволяє:

– виконувати оцінку параметрів продуктивності мережевого з'єднання;
– перевіряти рівень якості сервісів (QoS) на відповідність SLA;
– допомагати у виявленні і локалізації несправностей мережевим інженерам.

Cisco IOS IP SLA додає тестові пакети в активне з'єднання для вимірювання продуктивності між рознесеними вузлами зв'язку або розподіленими мережевими маршрутами. Цей процес імітує мережеві дані та IP-сервіси і збирає інформацію про продуктивність мережі в реальному часі. Також Cisco IOS IP SLA забезпечує генерацію і аналіз трафіку між пристроями Cisco IOS або між пристроєм Cisco IOS і віддаленим IP-пристроєм, наприклад, мережевим сервером додатків. Результати вимірювань IP SLA тестами можуть бути використані для пошуку несправностей, аналізу проблем і проектування мережевої топології.

Залежно від специфіки IP SLA тесту, різна статистика продуктивності мережі зберігається всередині пристрою Cisco, а доступ до неї можна отримати за допомогою інтерфейсу командного рядка або по протоколу SNMP. Пакет IP SLA має конфігуруються параметри IP і варіанти рівня додатків, такі як джерело і призначення IP адреси, UDP, напрямок VPN і URL.[3]

Оскільки Cisco IP SLA забезпечує вимір і оцінку показників якості мережевого з'єднання на рівнях L3-L4 і не залежить від рівня L2, то існує можливість конфігурувати IP SLA вимірювання поверх різнорідних мереж, що дозволяє більш точно визначити показники якості, які впливають на сервіси кінцевих користувачів .

IP SLA збирає такі показники продуктивності IP з'єднання:

– Затримка (двостороння і одностороння)
– Варіація затримки (Джиттер) (за напрямками)

– Втрата пакетів (за напрямками)
– Послідовність пакетів (за напрямками)
– Шлях (за ділянку маршруту між двома точками)
– З'єднання (за напрямками)
– Час завантаження сайту або сервісу

Використання IP SLA дає наступні переваги:

– Моніторинг SLA (вимір і оцінку відповідності)
– Моніторинг мережевої продуктивності
– Вимірювання джиттера, часу відгуку, втрати пакетів на мережі
– Надає безперервні, надійні і обґрунтовані вимірювання
– Оцінка стану мережевих IP-сервісів, для визначення достатності якості наявних для користувача сервісів (QoS)
– Моніторинг доступності прикордонних мереж для активної перевірки і тестування з'єднання мережевих ресурсів (наприклад, показує доступність в мережі файл-сервера, що використовується для зберігання критичних даних віддаленого сховища)
– Пошук і усунення несправних сегментів мережі за допомогою точних і надійних вимірювань, які оперативно виявляють проблеми і економлять час на локалізацію несправностей.

IP SLA можна використовувати для моніторингу продуктивності між будь-якими областями в мережі - ядром, агрегацією і доступом - без необхідності установки апаратного вимірювального зонда. IP SLA використовує генерований тестовий трафік для вимірювання мережевої продуктивності між двома мережевими пристроями. На схемі показано, як працює IP SLA, коли перший пристрій відправляє згенерований пакет кінцевому пристрою. Після того, як кінцевий пристрій отримує пакет, в залежності від типу IP SLA вимірювання, воно відправляє тестовий пакет назад джерелу з часовою міткою для калькуляції мережевих показників. IP SLA виконує мережеві вимірювання від відправляючого пристрою до одержувача в мережі, використовуючи обраний протокол, наприклад UDP.

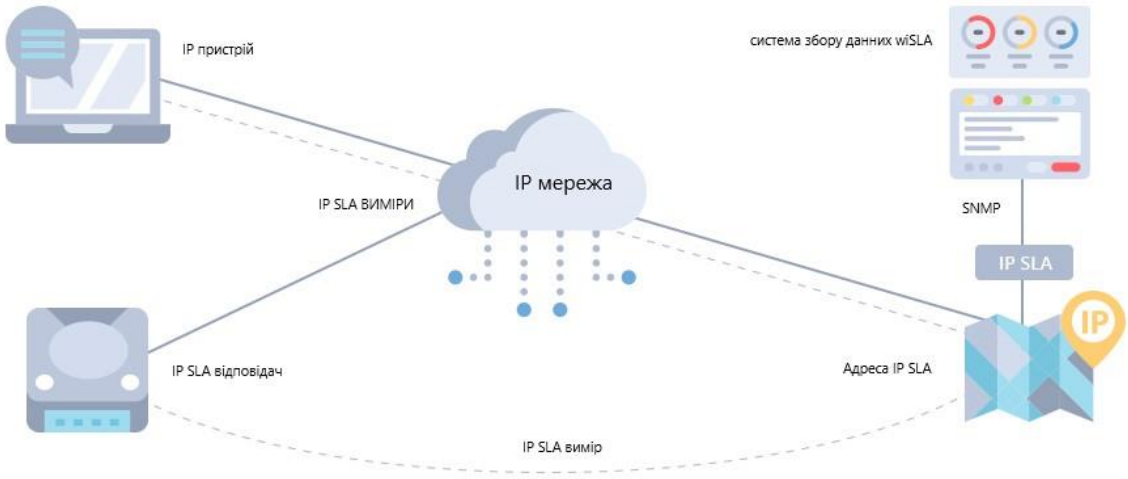


Рисунок 2.4. Приклад роботи IP SLA

Щоб почати вимірювання мережевої продуктивності за допомогою IP SLA, необхідно виконати наступні кроки:

- Включити IP SLA респондери на кінцевому пристрої, якщо потрібно
- Конфігурувати відповідний тип тесту IP SLA вимірювання на вихідному пристрої
- Конфігурувати порогові значення, якщо потрібно
- Запланувати початок тесту і визначити час його проведення
- Відобразити й інтерпретувати результати операції, використовуючи Cisco IOS CLI або SNMP, використовуючи систему управління мережею (Network Management System) або систему моніторингу SLA (SLA Management System).

IP SLA респондери або відповідачі є вбудованим компонентом IP SLA в мережеве обладнання Cisco, що дозволяє системі очікувати і відповідати на тестові пакети запитів IP SLA. Респондер надає точні вимірювання без потреби в спеціальних апаратних вимірювачах. Респондер використовує протокол контролю Cisco IP SLA, який забезпечує роботу механізму, що визначає порт для прослуховування і відповіді IP SLA.

На схемі вище показано, де встановлено пристрій Cisco з активованим IP SLA респондером в мережі. Респондери IP SLA очікує на певному порту так зване контрольне повідомлення по протоколу управління від генератора IP SLA

тестів з вихідного пристрою. Після отримання контрольного повідомлення, IP SLA включає певний UDP або TCP порт на певний час. У цей проміжок часу респондер приймає запити і відповідає на них. Ця операція відключає порт після відповіді на пакет IP SLA, або коли закінчується визначений час. З метою додаткового захисту для контрольного повідомлення є MD5 шифрування.

Процес обробки комутаторами і маршрутизаторами тестових пакетів може зайняти десятки мілісекунд через діяльність інших високо пріоритетних процесів. Ця затримка впливає на час відгуку, тому що відповідь тестового пакета може перебувати в черзі, чекаючи обробки. У такій ситуації час відгуку не завжди може надавати точні результати вимірювань мережевої затримки. IP SLA дозволяє мінімізувати час обробки пакетів на вихідному пристрої, так само як на пристрої відповідачі, на якому використовується респондер, для того, щоб максимально точно визначити час кругової затримки.

Ввімкнений IP SLA респондер дозволяє кінцевому пристрою при отриманні пакету на інтерфейс проставляти тимчасові мітки на рівні переривання, ігноруючи час обробки. Додавання тимчасової позначки зроблено з гранулярністю мілісекунди.

На схемі продемонстровано, як працює респондер. Отримані 4 тимчасові мітки дозволяють обчислити час кругової затримки. На крайовому пристрої, з активованою функцією IP SLA респондери, мітка часу 2 вирахувана з мітки 3 для визначення витраченого на обробку тестового пакета часу, як позначено дельтою. Це значення дельти віднімається від часу повної кругової затримки. Зверніть увагу, що такий же принцип застосовується IP SLA на вихідному маршрутизаторі, де мітка часу входу 4 також ставиться на рівні переривання, щоб забезпечити більшу точність.

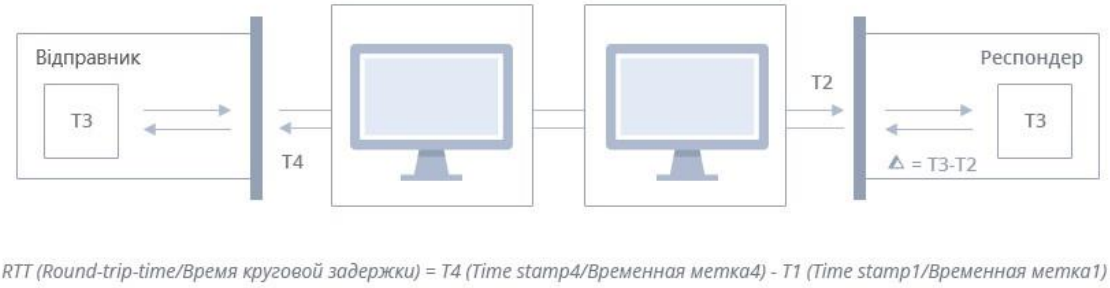


Рис. 2.5. Схема роботи респондера

Щоб підтримувати високий рівень виконання SLA, Ви повинні володіти інструментами, які негайно сповіщають вас про будь-які можливі порушення, або правила які змінюють поведінку пристроїв в мережі при виникненні певної події. IP SLA може відправляти повідомлення про мережеві події за допомогою SNMP-пток, які можуть ініціюватися наступними подіями:

- Втрата зв'язку
- Перевищення часу очікування відповіді
- Граничні значення кругової затримки
- Середнє порогове значення джиттера
- Одностороння втрата пакета
- односторонній джиттер
- Зниження якості передачі мови (Односторонній MOS (Mean opinion score))
- Одностороння затримка

Порушення порогових значень може також ініціювати IP SLA тест для подальшого аналізу. Наприклад, збільшення частоти відправки пакетів або ICMP, або джиттер можуть стати тригером початку тесту для усунення несправностей. Також тригер може перемикати канали зв’язку на резервні.

Вбудований менеджер подій Cisco або Cisco EEM - це програмний компонент Cisco IOS, IOS-XR та NX-OS, що забезпечує виявлення подій у мережі в режимі реального часу та автоматизацію роботи на борту.

EEM дозволяє автоматизувати завдання, виконувати незначні вдосконалення та створювати обхідні шляхи, а також полегшує життя

операторам мережі шляхом відстеження та класифікації подій, що відбуваються на мережевому пристрої та надаючи варіанти дій для цих подій. EEM використовує детектори подій та дії для надання сповіщень про ці події.

IOS Embedded Event Manager підтримує понад 20 детекторів подій, які добре інтегровані з різними компонентами програмного забезпечення Cisco IOS для запуску дій у відповідь на мережеві події. Ними можуть бути:

- SNMP - моніторинг SNMP-об'єктів, подій та повідомлень (SNMP-пастки) пристрою
- Syslog - відповідає на різні повідомлення syslog, дозволяючи узгоджувати регулярні вирази змісту повідомлення
- Counter(s) - моніторинг та реагування на лічильники інтерфейсів при встановленні межпорогових параметрів
- CLI - скринінг вводу CLI для відповідності регулярного вираження або коли вводиться спеціальний символ синтаксичного аналізу, наприклад Tab або "?" (знак питання)
- Таймери - зворотний відлік, сторожовий та CRON
- IP-події SLA та NetFlow
- Маршрутизація - Коли запис інформації про маршрут змінюється в Базі інформації про маршрутизацію (RIB)
- RPC - надає можливість викликати політики EEM поза маршрутизатором через зашифроване з'єднання за допомогою SSH. Детектор подій RPC використовує кодування даних простого об'єктного протоколу доступу (SOAP) для обміну повідомленнями на основі XML. Цей детектор подій може використовуватися для запуску політик EEM, а потім отримання виводу у відповіді у форматі SOAP XML
- OIR (онлайн-вставлення та вилучення) - коли карту видалено або вставлено
- Ресурс - коли вбудований менеджер ресурсів (ERM) повідомляє про подію.
- Enhanced Object Tracking Event Detector (EOT) або розширений детектор подій відстеження об'єктів - коли стан відстежуваного об'єкта змінюється

– Інша політика EEM - Інша політика EEM може публікувати подію.
– None - Цей детектор подій повинен протестувати скрипт / аплет EEM за допомогою команди «event manager run»

Діями EEM можуть бути:

– Виконання команди CLI (інтерфейс командного рядка Cisco IOS).
– Генерування події CNS для обробки вгору за допомогою пристроїв Cisco CNS.
– Встановлення або зміна названого лічильника.
– Перехід на вторинний процесор у надмірній конфігурації обладнання.
– Запит системної інформації, коли відбувається подія.
– Надсилання короткого електронного повідомлення.
– Ручне управління політикою EEM.
– Публікація події, що стосується додатків.
– Перезавантаження програмного забезпечення Cisco IOS.
– Генерування лову SNMP.
– Створення пріоритетних повідомлень системного журналу.
– Читання стану відстежуваного об’єкта.
– Встановлення стану відстежуваного об'єкта.

Ось три основні механізми політики в рамках Cisco EEM:

1. Еплементи EEM - підтримуються з EEM версії 1.0, ці політики визначені та визначені в конфігурації пристрою та розроблені для того, щоб забезпечити простий інтерфейс у функції EEM Cisco.

   У межах конфігурації аплетів дозволена лише одна команда конфігурації подій, або до шести подій з кореляцією, оскільки EEM 2.4 та багаторазові дії дозволені.

   Використовуйте команду: покажіть політику менеджера подій, зареєстровану для відображення списку зареєстрованих аплетів.
2. TCL-скрипти - підтримуються з EEM версії 2.0, ці політики визначаються в окремих файлах, що зберігаються локально на пристрої та задаються (реєструються) шляхом додавання єдиної команди конфігурації.

Tcl дозволяє здійснювати більш складні політики, а деякі функції EEM, такі як абоненти таймерів, на даний момент підтримуються лише в EEM Tcl.

3. Політика оболонки IOS.sh - підтримується з EEM версії 3.2, ці політики визначаються в окремих файлах, що зберігаються локально на пристрої та задаються (реєструються) шляхом додавання єдиної команди конфігурації. Політики оболонки використовують функцію оболонки IOS. Підтримка політики оболонок обмежена деякими платформами комутації.[5]

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ РЕЗЕРВУВАННЯ КАНАЛІВ

3.1. Базове налагодження пристроїв мережі

В даному пункті розглянуто базові налаштування пристроїв мережі. Для зручності налаштування та подальшої експлуатації були змінені стандартні імена пристроїв в мережі (рис. 3.1).

AD_SW

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname AD_server_SW
AD_server_SW(config)#
```

Рис. 3.1. Налаштування імені пристрою

Також для полегшення подальшої експлуатації мережі адміністратором були додані банери з основною інформацією про пристрій(рис. 3.2).

```
AD_server_SW(config)#banner motd ?
  LINE  c banner-text c, where 'c' is a delimiting character

AD_server_SW(config)#$dows AD server. DC to WinServer and Main office ASA"
```

Рис. 3.2. Налаштування повідомлення привітання для користувача

У фрагменті (рис. 3.3) було налаштовано статичну адресу інтерфейса для маршрутизації MAIN_OFFICE.

MAIN_OFFICE

```
ASA-MAIN-OFFICE(config-if)# ip addr 48.214.24.1 255.255.255.0
ASA-MAIN-OFFICE(config-if)# no sh
ASA-MAIN-OFFICE(config-if)# exi
ASA-MAIN-OFFICE(config)# int gig0/1
ASA-MAIN-OFFICE(config-if)# ip addr 10.0.0.1 255.255.255.0
ASA-MAIN-OFFICE(config-if)# no sh
ASA-MAIN-OFFICE(config-if)# exi
ASA-MAIN-OFFICE(config)# int gig0/2
ASA-MAIN-OFFICE(config-if)# ip addr 20.0.0.1 255.255.255.0
ASA-MAIN-OFFICE(config-if)# no sh
ASA-MAIN-OFFICE(config-if)# exi
```

Рис. 3.3. Налаштування статичної IP-адреси

Також для зручності віддаленого керування були налаштовані IP-адреси інтерфейсу Vlan1 на кожному з комутаторів (рис. 3.4).

```
AD_server_SW(config)#int vlan 1
AD_server_SW(config-if)#ip addr 48.214.24.2 255.255.255.0
AD_server_SW(config-if)#no sh
AD_server_SW(config-if)#
*Jun  2 07:12:23.518: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Jun  2 07:12:24.527: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, cha
nged state to up
```

Рис. 3.4. Налаштування статичної IP-адреси для інтерфейсу Vlan1

На маршрутизаторі OFFICE_R, багаторівневих комутаторів INSIDE_DB_NETWORK та S_O_SW також на ME, які мають пряме підключення до офісних підмереж було налаштовано протокол динамічної конфігурації вузла DHCP (рис. 3.5-3.7).

```
OFFICE_ROUTER(config)#ip dhcp excluded-address 192.168.0.2
OFFICE_ROUTER(config)#ip dhcp excluded-address 192.168.1.2
OFFICE_ROUTER(config)#ip dhco pool marketing_office
                          ^
% Invalid input detected at '^' marker.

OFFICE_ROUTER(config)#ip dhcp pool marketing_office
OFFICE_ROUTER(dhcp-config)#network 192.168.1.1 255.255.255.0
OFFICE_ROUTER(dhcp-config)#default router 192.168.1.1
```

Рис. 3.5. Налаштування DHCP на маршрутизаторі

```
Secon_office_SW(config)#ip dhcp excluded-address 192.168.3.1
Secon_office_SW(config)#ip dhcp excluded-address 192.168.3.2
Secon_office_SW(config)#ip dhcp pool Bookkepper_oddice_pool_DHCP
Secon_office_SW(dhcp-config)#network 192.168.3.0 255.255.255.0
Secon_office_SW(dhcp-config)#def
Secon_office_SW(dhcp-config)#default-router 192.168.3.1
```

Рис. 3.6. Налаштування DHCP на багаторівневих комутаторах

```
SMALL-OFFICE(config)# dhcpd addres 192.168.4.3-192.168.4.254 inside
SMALL-OFFICE(config)# dhcpd enable inside
```

Рис. 3.7. Налаштування DHCP на ME

Також для наступного налаштування резервування за допомогою міжмережевих екранів було налаштовано інтерфейс синхронізації між ASA_Active та Active_Failover (рис. 3.8-3.9).

```
ASA-Active(config)# int gig0/2
ASA-Active(config-if)# description STATE Failover Interface
ASA-Active(config-if)# no nameif
ASA-Active(config-if)# no security-level
ASA-Active(config-if)# no ip addr
ASA-Active(config-if)# no sh
```

Рис. 3.8. Налаштування інтерфейсу синхронізації ASA_Active

```
ASA-active-failover(config)# int gi0/2
ASA-active-failover(config-if)# description STATE Failover Interface
ASA-active-failover(config-if)# no nameif
ASA-active-failover(config-if)# no secu
ASA-active-failover(config-if)# no security-level
ASA-active-failover(config-if)# no ip addr
ASA-active-failover(config-if)# no sh
```

Рис. 3.9. Налаштування інтерфейсу синхронізації ASA Active_Failover

Також на всіх пристроях було налаштовано SSH для подальшого адміністрування та створені користувачі з різними рівнями доступу.

```
ASA-MAIN-OFFICE(config)# username admin password admin privilege 15
ASA-MAIN-OFFICE(config)# username user pass
ASA-MAIN-OFFICE(config)# username user password cisco priv
ASA-MAIN-OFFICE(config)# username user password cisco privilege 4
```

Рис. 3.10. Створення користувачів з різними рівнями доступу

```
Database_router(config)#crypto key generate rsa modulus 2048
The name for the keys will be: Database_router.diploma

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

Database_router(config)#
*Jun  8 12:13:37.131: %SSH-5-ENABLED: SSH 1.99 has been enabled
Database_router(config)#ip ssh version 2
Database_router(config)#line vty 0 4
Database_router(config-line)#login local
Database_router(config-line)#transport input ssh
Database_router(config-line)#transport output ssh
```

Рис. 3.11. Налаштування SSH v2 для віддаленого доступу на маршрутизаторі

```
ASA-MAIN-OFFICE(config)# domain-name diploma
ASA-MAIN-OFFICE(config)# cryp key gen rsa mod 2048
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...
ASA-MAIN-OFFICE(config)# ssh 214.2.24.0 255.255.255.0 admin
```

Рис. 3.12. Налаштування SSH v2 для віддаленого доступу на ME

Для маршрутизації та обміну даними офісів між собою через мережу інтернет були створені VPN тунелі. Ми використали протокол IPsec.

```
Database_router(config)#crypto ipsec transform-set TS esp-3des esp-sha-hmac co$
Database_router(cfg-crypto-trans)#crypto ipsec profile A
Database_router(ipsec-profile)#set transform-set TS
```

Рис. 3.13. Налаштування ISAKMP на DB_R

```
HOME(config)#int tunnel0
HOME(config-if)#ip addr 1
*Jun  8 12:50:21.307: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, c
hanged state to down0
HOME(config-if)#ip addr 100.0.0.2 255.255.255.252
HOME(config-if)#tunnel source 10.0.0.4
HOME(config-if)#tunnel destination 10.0.0.3
HOME(config-if)#no sh
*Jun  8 12:50:57.067: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, c
hanged state to up
```

Рис. 3.14. Налаштування інтерфейса Tunnel0 на HOME

```
Database_router(config)#int tunnel 0
Database_router(config-if)#ip addr 100.0.0.1 255.255.255.252
Database_router(config-if)#tunnel source 10.0.0.3
Database_router(config-if)#tunnel destination 10.0.0.4
Database_router(config-if)#no sh
Database_router(config-if)#exi
Database_router(config)#do ping 100.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/17/52 ms
```

Рис. 3.15. Налаштування інтерфейса Tunnel0 на DB_R

Для подальшої конфігурації тунелів та налаштувань на мережевих екранах було ввімкнено доступ через графічну оболонку ASA ASDM.

```
SMALL-OFFICE(config)# http server enable
SMALL-OFFICE(config)# http 192.168.0.0 255.255.255.0 config
```

Рис. 3.16. Ввімкнння http server на мережевому екрані для доступу через графічний інтерфейс

В даному випадку ми будемо використовувати графічний інтерфейс не лише для налаштувань, а й для моніторингу системи за допомогою систем моніторингу та логування, які є в мережевих екранах Cisco ASA.

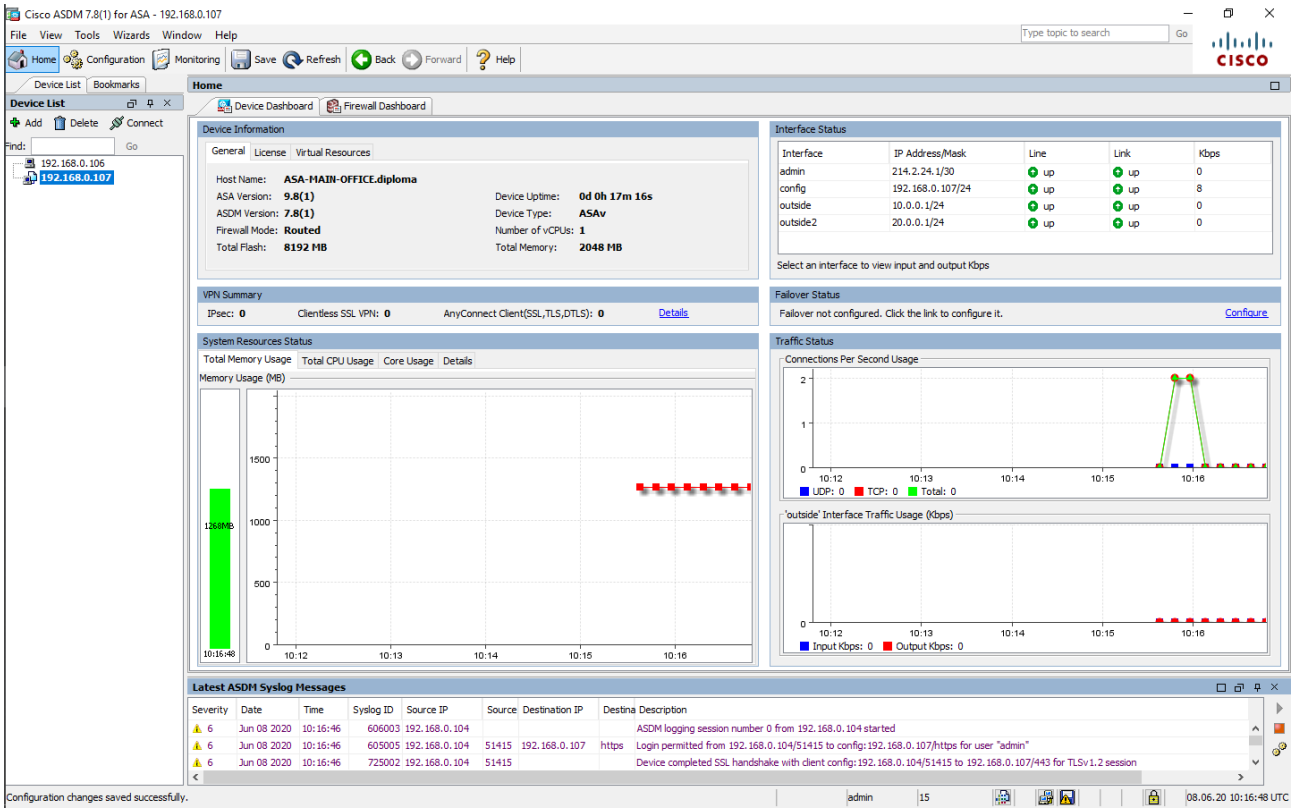


Рис. 3.17. Графічний інтерфейс Cisco ASA ASDM (домашня сторінка)

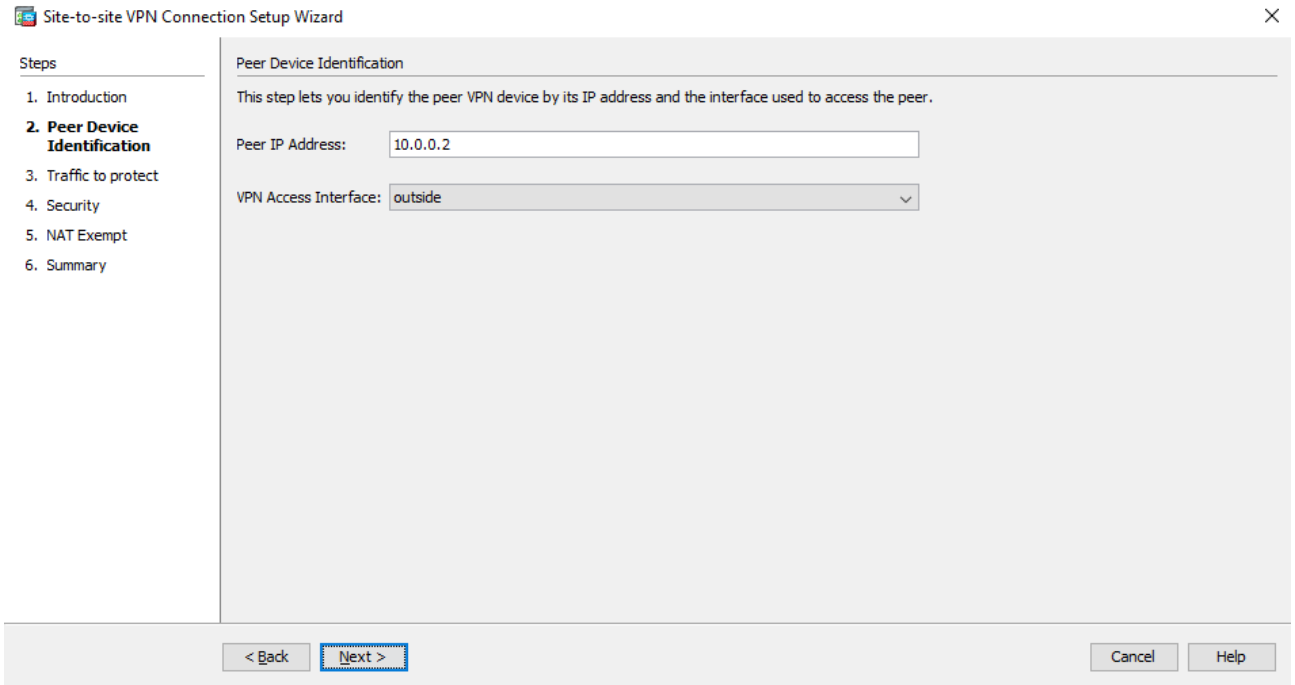


Рис. 3.18. Налаштування VPN тенуля для зв’язку між офісами

Так як мережевий екран Cisco ASA має свої особливості в налаштуванні VPN тунелів, він потребує переліку локальних та віддалених мереж для змінення

правил роботи пропускання трафіку, ці підмережі матимуть доступ до тунелю в будь-якому випадку налаштувань ME.

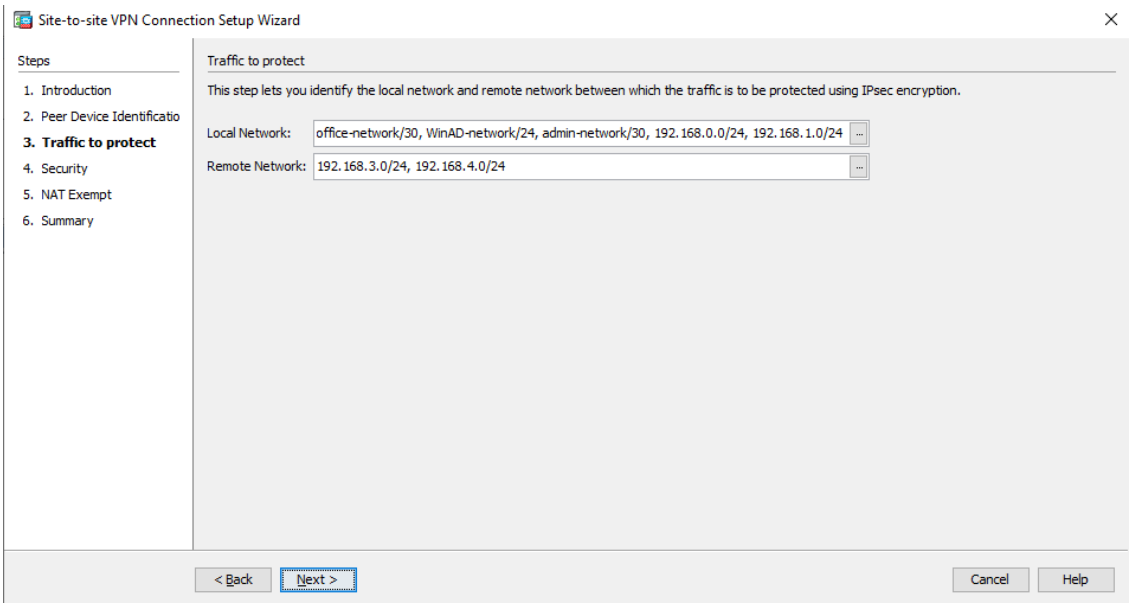


Рис. 3.19. Вибір підмереж для доступу до VPN тунеля

Pre-shared key - це рядок символів, який використовується як ключ автентифікації. Можна використовувати загальнодоступні ключі для автентифікації VPN від сайту до сайту та для сторонніх VPN-клієнтів. В нашому випадку ми згенеруємо ключ ,який буде унікальним для доступу до VPN тунля.

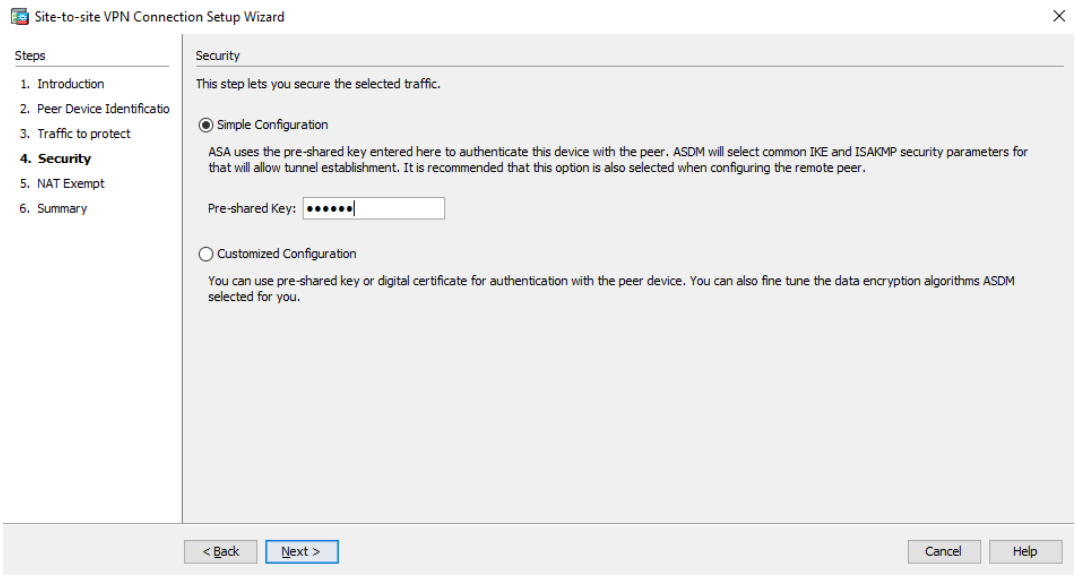


Рис. 3.20. Введення унікального ключа для захисту тунеля

Звільнення даного інтерфейса від трансляції NAT зменшить навантаження на мережу та зробить підмережу даного інтерфейса доступним з інших офісів нашої організації.

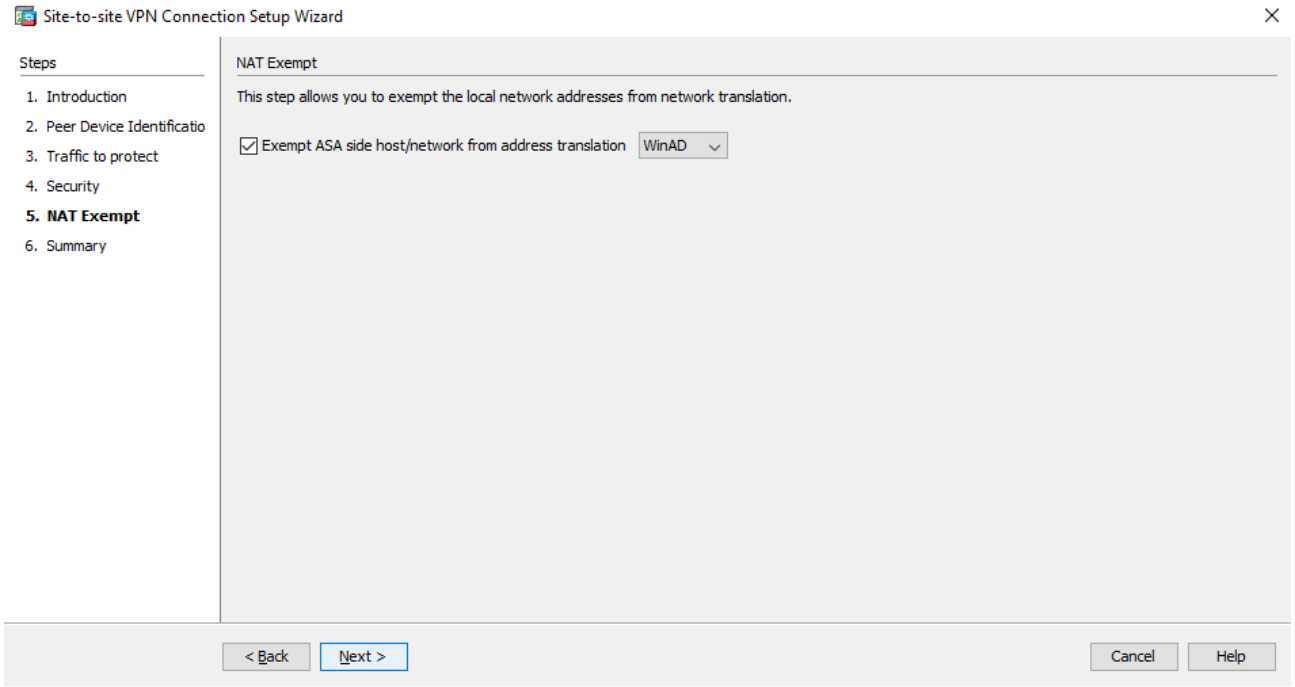


Рис. 3.21. Звільнення інтерфейсу від трансляції NAT

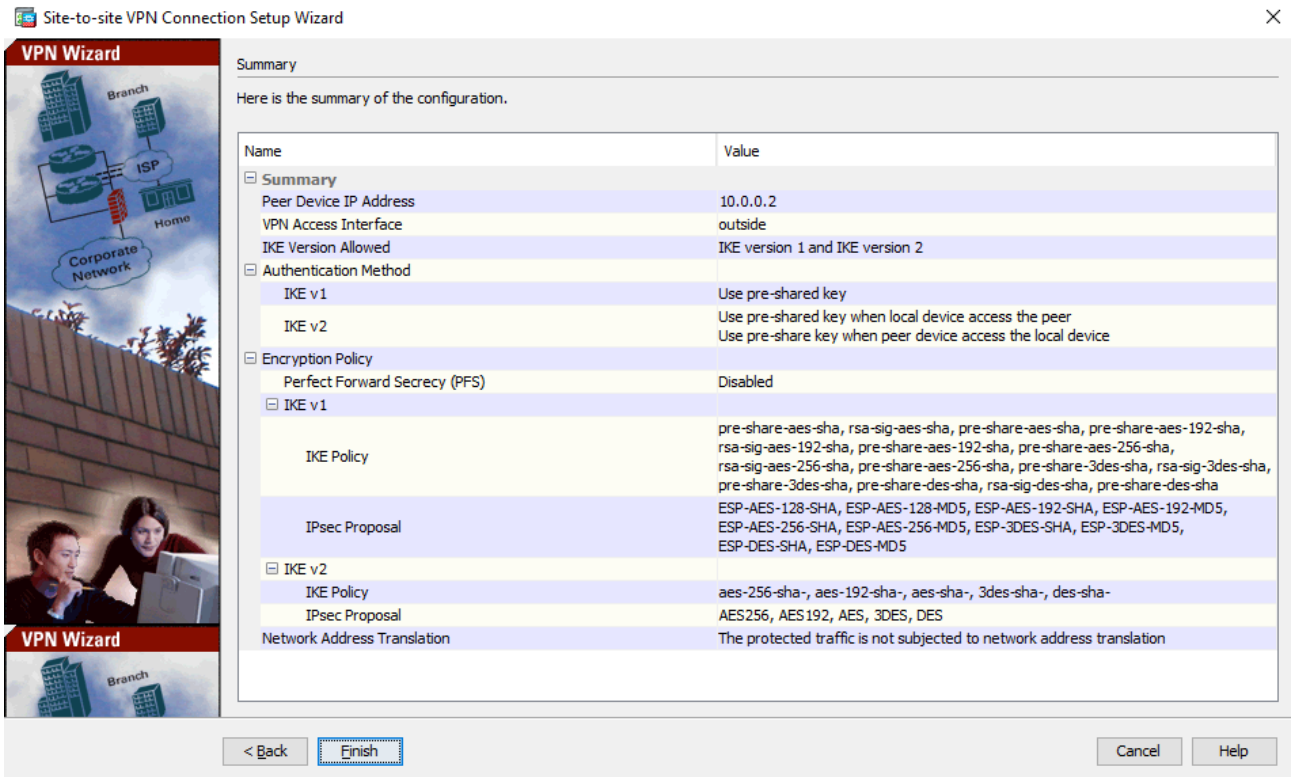


Рис. 3.22. Перевірка налаштувань тунеля перед збереженням

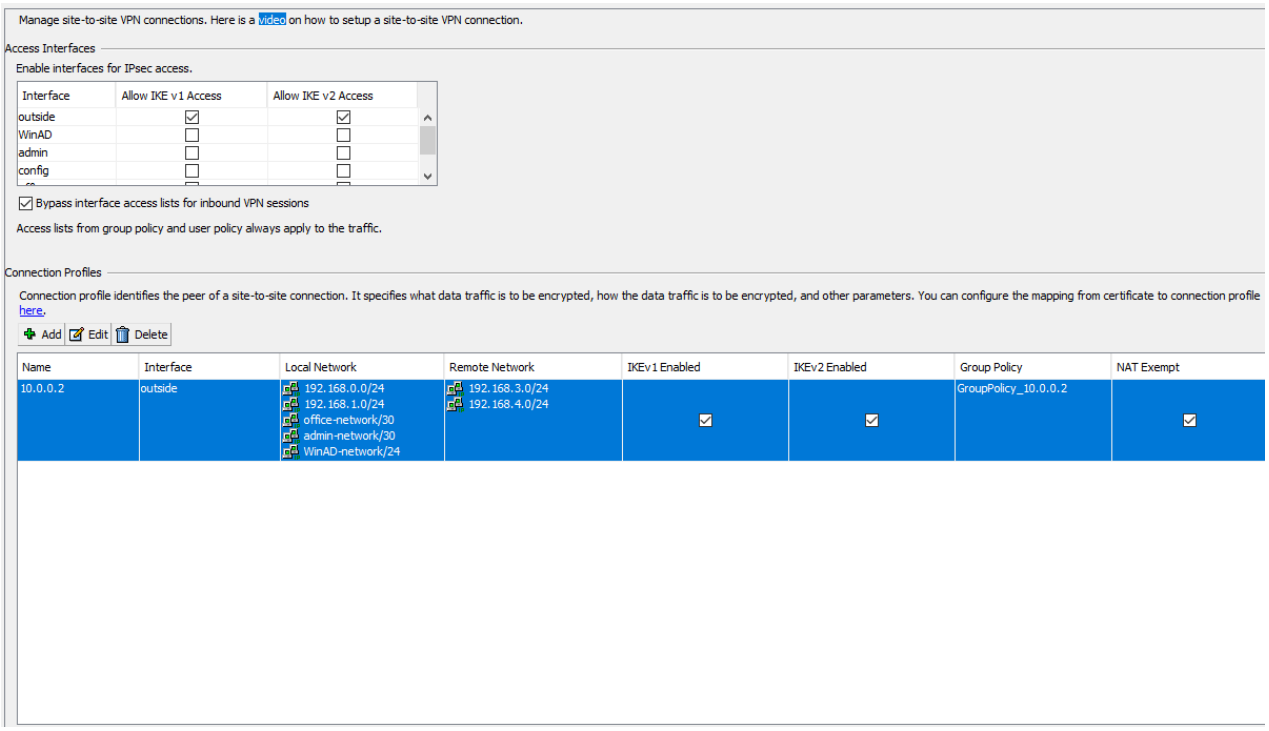


Рис. 3.23. Налаштований тунель

Так як більшість офісів має декілька підмереж ,які потребують доступу до глобальної мережі Інтернет було налаштовано PAT. Port Address Translation (PAT) - це розширення трансляції мережевих адрес Network Address Translation (NAT), що дозволяє відображати декілька пристроїв з різних підмереж у локальній мережі на одну загальну IP-адресу для збереження IP-адрес.

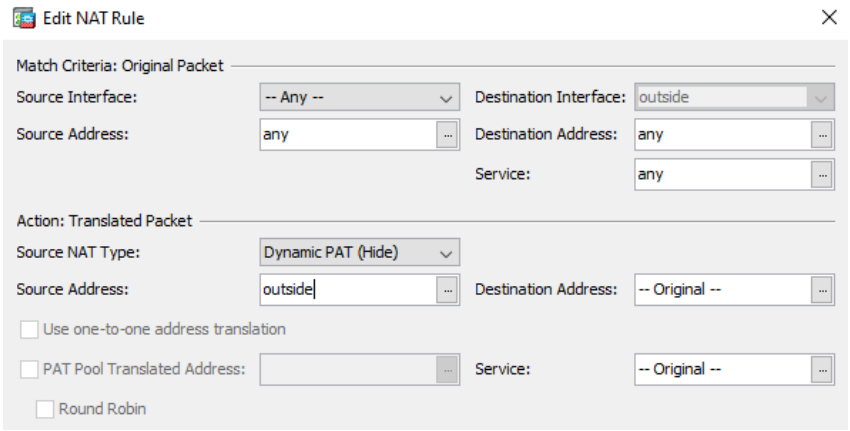


Рис. 3.24. Налаштування PAT

PAT схожий до переадресації портів, за винятком того, що вхідний пакет з портом призначення (зовнішній порт) переводиться на інший порт призначення (внутрішній порт). Постачальник Інтернет-послуг (ISP) присвоює єдину IP-

адресу крайовому пристрою. Коли комп'ютер входить в Інтернет, цей пристрій призначає клієнту номер порту, який додається до внутрішньої IP-адреси, надаючи комп'ютеру унікальну IP-адресу.

Для маршрутизації в мережі було використано протокол OSPF з редистрибуцією статичних маршрутів.

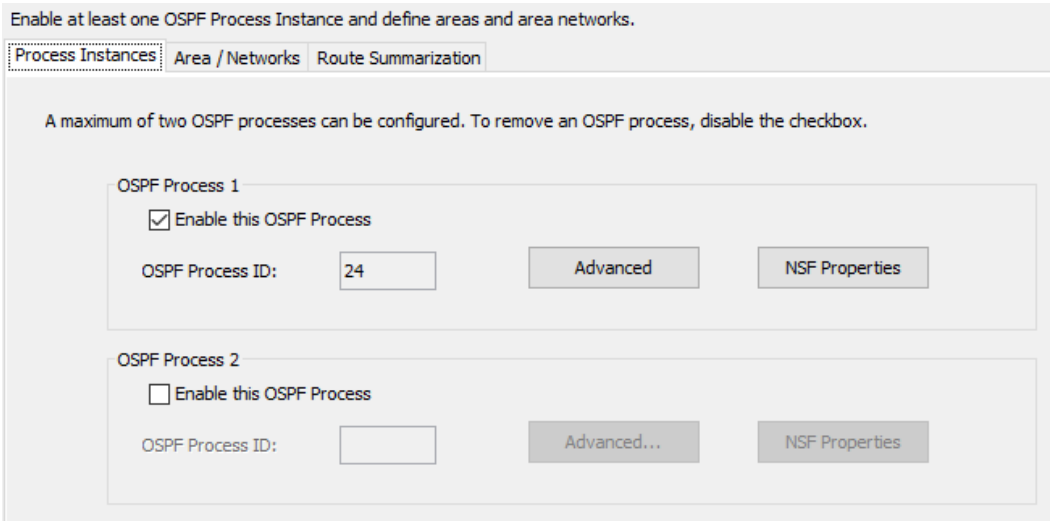


Рис. 3.25. Ввімкнення протоколу динамічної маршрутизації OSPF

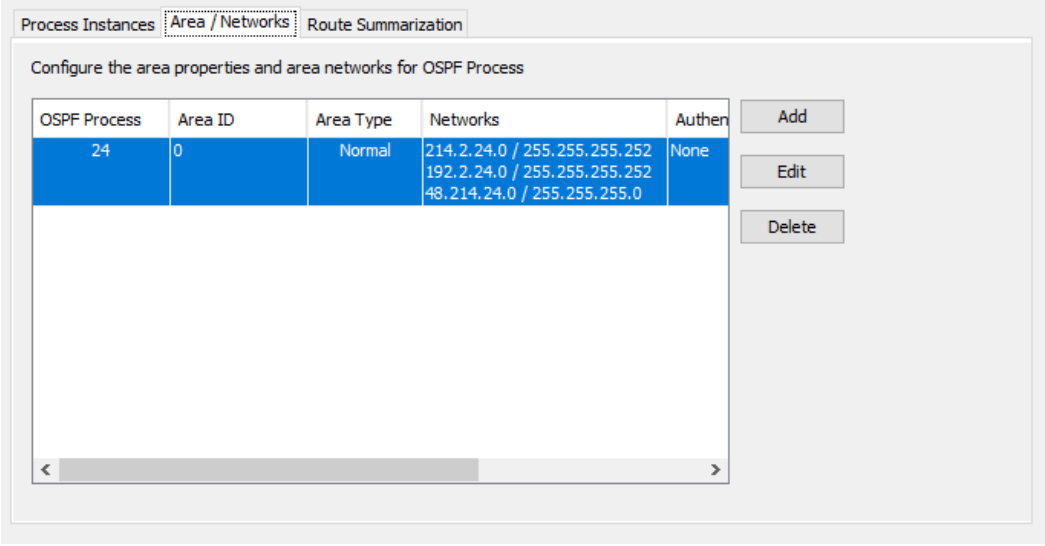


Рис. 3.26. Додавання підмереж для маршрутизації OSPF

Для того щоб резервні статичні маршрути працювали правильно їх треба додати в маршрутизацію OSPF за допомогою редистрибуції.

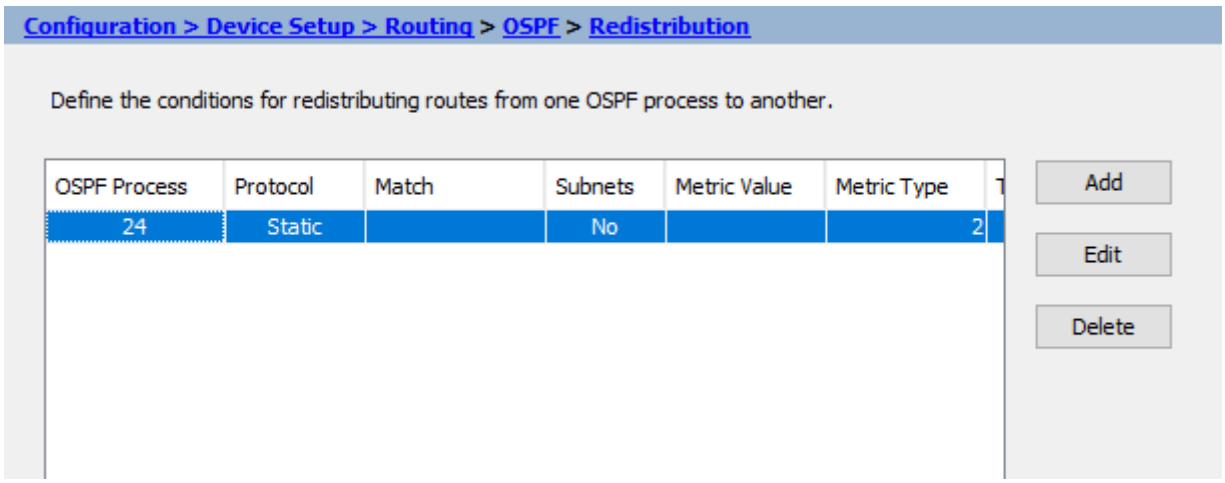


Рис. 3.27. Ввімкнення редистрибуції статичних маршрутів з OSPF

3.2. Налагодження підсистеми резервування каналів

Основною частиною мережі є ME, які використовуються для підвищення рівня захисту мережі, через це ми можемо використати одну з можливостей мережевих екранів Cisco ASA для резервування каналів зв'язку, а саме резервування Cisco Standby. Є багато режимів резервування в ASA. Найпоширенішими є Active/Standby та Active/Active failover. В нашому випадку краще було використати режим Active/Active failover, який був обраний найкращим через те, що ми не лише резервуємо канали, а також балансуємо навантаження в мережі, так, як будемо одночасно передавати дані через дві фізичні лінії, але, нажаль, під час тестування було виявлено, що даний режим неможливо ввімкнути на віртуалізованому обладнанні, так, як в даний час відсутній доступ до реального обладнання.

Через це було обрано другий режим Active/Standby в якому один мережевий екран працює постійно, поки є з'єднання з заданим нодом в мережі. А другий пристрій буде вмикатися лише при відсутності з'єднання в першого, тим самим резервуючи канал зв'язку. Ще одною особливістю є те що деякі Cisco ASA не мають можливості перемикання станів Active/Standby за станом каналу, тоді потрібно буде зробити додаткові налаштування та за допомогою вмонтованого менеджеру подій та SLA монітору створити подію, щоб

мережевий екран після втрати з’єднання перезавантажувався тим самим передаючи активну роль резервуючому пристрою.

```
ASA-Active(config)# failover
ASA-Active(config)# failover lan unit primary
ASA-Active(config)# failover lan interface STATE Gi0/2
INFO: Non-failover interface config is cleared on GigabitEthernet0/2 and its sub-interfaces
ASA-Active(config)# failover lan interface STATE Gi0/2
ASA-Active(config)# failover polltime unit 1 holdtime 3
ASA-Active(config)# failover link STATE Gi0/2
ASA-Active(config)# failover int ip STATE 172.2.24.1 255.255.255.252 standby 1$
```

Рис. 3.28. Налаштування активного пристрою

```
ASA-active-failover(config)# failover
ASA-active-failover(config)# failover lan unit secondary
ASA-active-failover(config)# failover lan interface STATE Gi0/2
ASA-active-failover(config)# failover polltime unit 1 holdtime 3
ASA-active-failover(config)# failover link STATE Gi0/2
ASA-active-failover(config)# failover int ip STATE 172.2.24.1 255.255.255.252 $
```

Рис. 3.29. Налаштування резервуючого пристрою

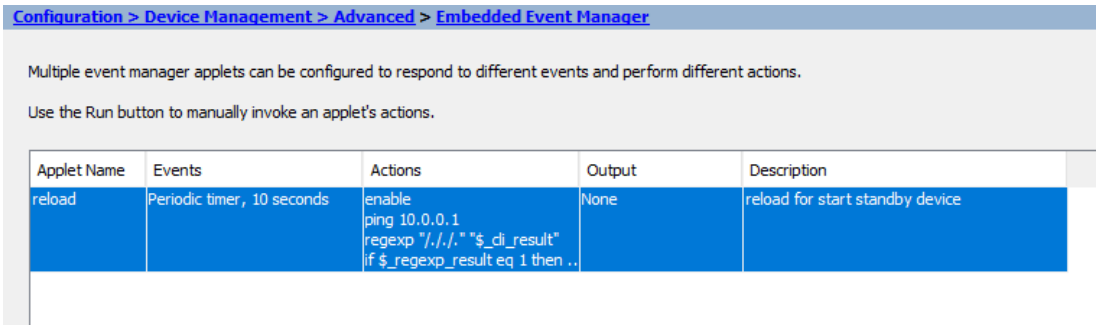


Рис. 3.30. Налаштування менеджера подій для перезавантаження

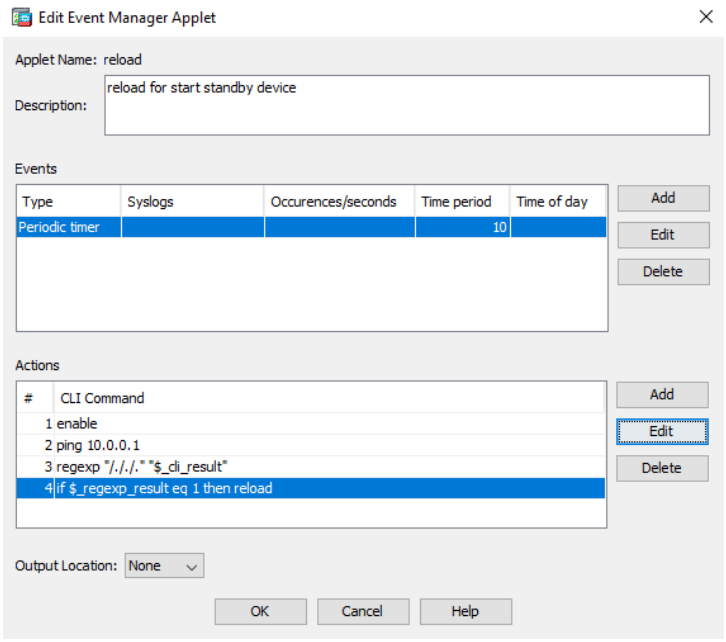


Рис. 3.31. Розширені налаштування EEM applet

Подальші налаштування пристроїв проводиться лише на ME з роллю active так, як пристрій з роллю standby буде копіювати конфігурацію після кожного збереженні автоматично.

Наступним кроком резервування каналів є агрегація. Так як зазвичай резервування каналів намагаються зробити 2 другому рівні моделі OSI, використовуючи агрегацію каналів так як це більш простий в налаштуванні та експлуатації варіант.

PAgP це один із динамічних протоколів агрегації каналів, цей протокол є пропріетарним протоколом розробленим компанією Cisco для своїх комутаторів і маршрутизаторів.

```
Database_router(config)#int range e1/3,e2/0
Database_router(config-if-range)#sh
Database_router(config-if-range)#channel
*Jun  8 16:04:55.915: %LINK-5-CHANGED: Interface Ethernet1/3, changed state to a
dministratively down
*Jun  8 16:04:55.915: %LINK-5-CHANGED: Interface Ethernet2/0, changed state to a
dministratively down
*Jun  8 16:04:56.917: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
3, changed state to down
*Jun  8 16:04:56.917: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/
0, changed state to down
Database_router(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

Database_router(config-if-range)#
```

Рис. 3.32. Налаштування PAgP на Database_router

```
DB_Office(config)#int range e0/0,e0/1
DB_Office(config-if-range)#channel-group 1 mode auto
Creating a port-channel interface Port-channel 1

DB_Office(config-if-range)#
*Jun  8 16:07:35.294: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to down
*Jun  8 16:07:35.294: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to down
```

Рис. 3.33. Налаштування PAgP на комутаторі DB_Office

```
Database_router(config-if-range)#no sh
Database_router(config-if-range)#
*Jun  8 16:08:11.835: %LINK-3-UPDOWN: Interface Ethernet1/3, changed state to up
*Jun  8 16:08:11.835: %LINK-3-UPDOWN: Interface Ethernet2/0, changed state to up
*Jun  8 16:08:12.838: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
3, changed state to up
*Jun  8 16:08:12.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/
0, changed state to up
Database_router(config-if-range)#
*Jun  8 16:08:15.627: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-chann
el1, changed state to up
```

Рис. 3.34. Ввімкнення PAgP на Database_router

Агрегація каналів LACP дозволяє агрегувати до 16 каналів зв'язку, 8 з яких будуть активними, а всі інші працюватимуть в standby режимі, тим самим резервуючи канали зв'язку. Цей протокол на відміну від PAgP є стандартним протоколом і може бути налаштований на комутаторах будь-якого вендору.

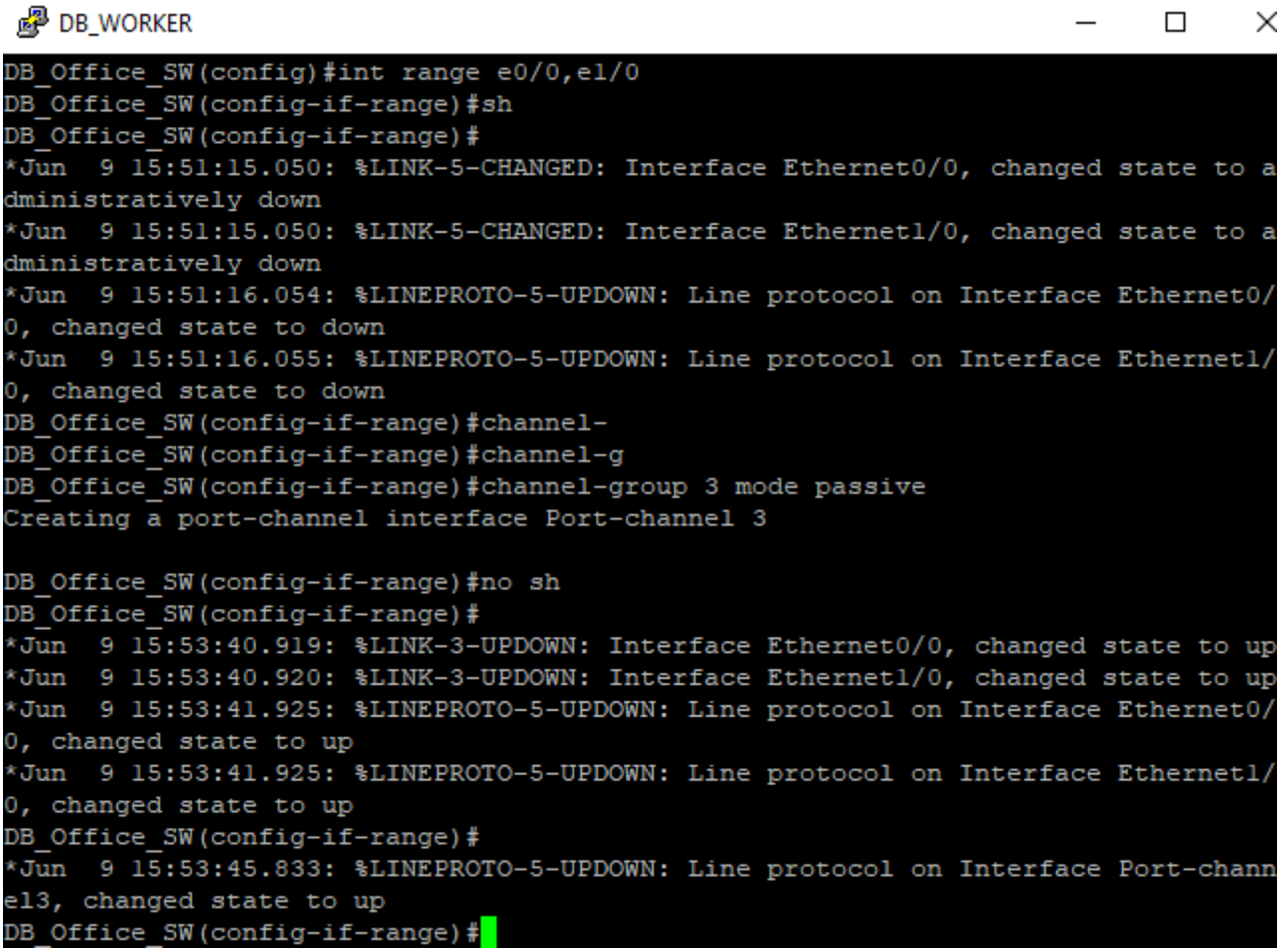


Рис. 3.35. Ввімкнення LACP на DB_WORKER

Хоч цей протокол і має великий недолік для мереж, які потребують низьких затримок, так як в ньому є доволі велика затримка при ввімкненні агрегованого каналу та при збереженні налаштувань, хоча він досі використовується для резервування каналів зв'язку.

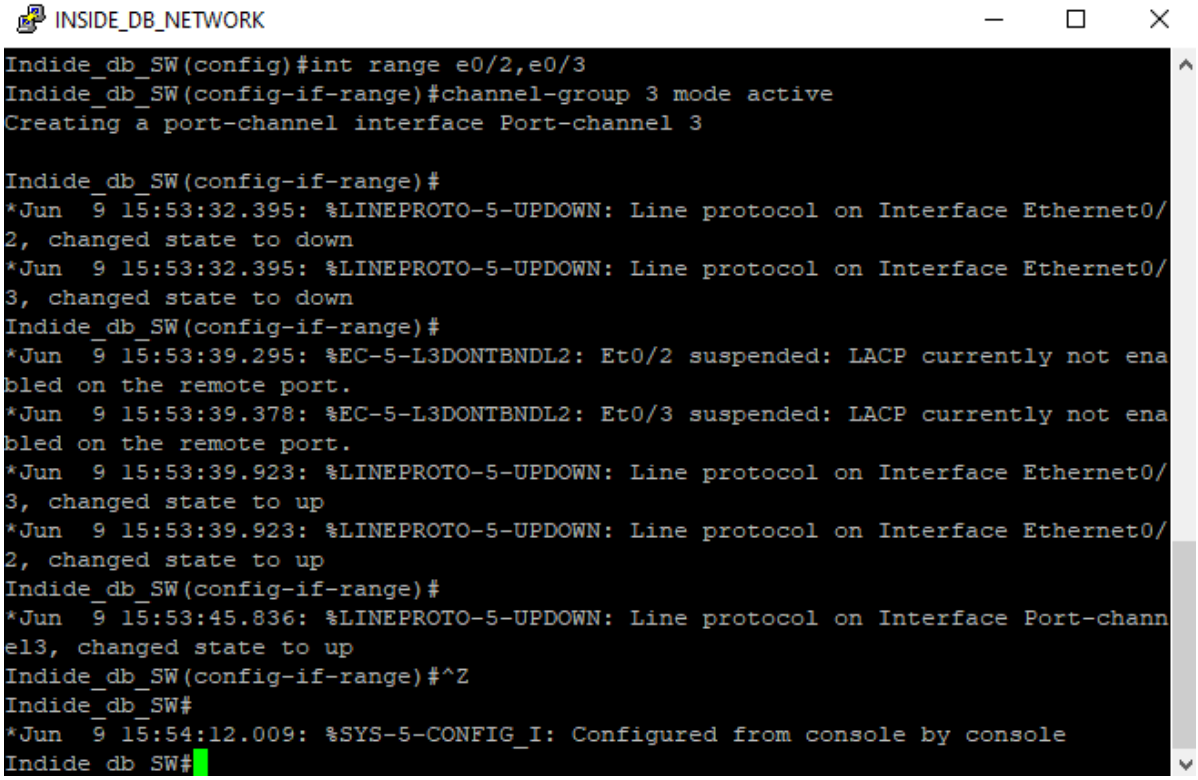


Рис. 3.36. Ввімкнення LACP на INSIDE_DB_NETWORK

Для підключення резервних маршрутів до другого провайдера інтернету, зазвичай використовують протоколи динамічної маршрутизації засновані LSA. Тим самим, маючи 2 маршрути, ми можемо змінити ціну переходу, щоб означити основний та резервний маршрут. В той же час, не завжди просто означити ці маршрути, через те ,на мою думку, краще використати більш надійні способи. В нашому випадку, ми будемо використовувати статичні маршрути з використанням трекінгу IP SLA.

Для правильної роботи Cisco рекомендує налаштовувати 2 маршрути, один з яких буде прив’язаний до SLA моніторингу за допомогою трека, другий маршрут буде звичайним статичним маршрутом з більшою метрикою.

Interface	Name	Zone	Route Map	State	Security Level	IP Address	Subnet Mask Prefix Length	Secondary VLAN	Redundant	Group	Type
GigabitEthernet0/0	WinAD			Enabled	100	48.214.24.1	255.255.255.0		No		Hardware
GigabitEthernet0/1	outside			Enabled	0	10.0.0.1	255.255.255.0		No		Hardware
GigabitEthernet0/2	backup			Enabled	0	20.0.0.1	255.255.255.0		No		Hardware
GigabitEthernet0/3				Disabled					No		Hardware
GigabitEthernet0/4				Disabled					No		Hardware
GigabitEthernet0/5	office			Enabled	100	192.2.24.1	255.255.255.252		No		Hardware
GigabitEthernet0/6	admin			Enabled	50	214.2.24.1	255.255.255.252		No		Hardware
Management0/0	config			Enabled	0	192.168.0.106 (DHCP)	255.255.255.0 (D...		No		Hardware

Рис. 3.37. Налаштовані інтерфейси на мережевому екрані основного офіса

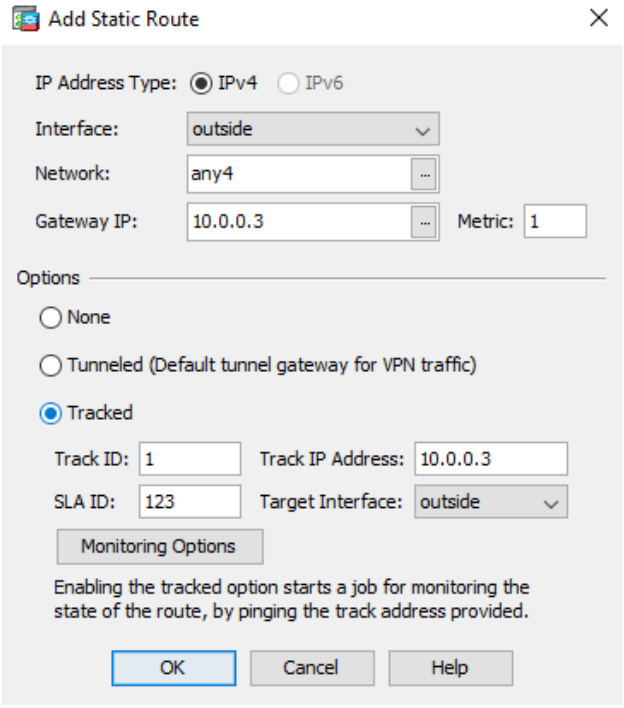


Рис. 3.38. Створення статичного основного маршрута для доступу до першого інтернет провайдера

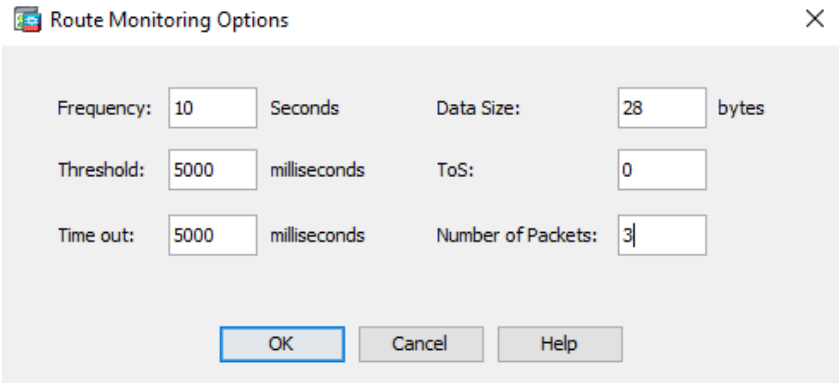


Рис. 3.39. Налаштування монітору для перевірки з’єднання

Головні налаштування для нас - це частота відправки повідомлень та кількість пакетів, які ми відправляємо. Так як, ми можемо виставити завелику частоту відправки, тим самим порушивши стабільну роботу мережі на довший чим, це допустимо, час. Також кількість пакетів обрана не випадково, відповідь від стандартних для всіх систем 5 пакетів буде довша майже в 2 рази, а 1 пакет може загубитися навіть в повністю нормально функціонуючій мережі, тим самим за допомогою серії експериментів, я отримав результат, який найбільше підходить до даних умов використання мережі.

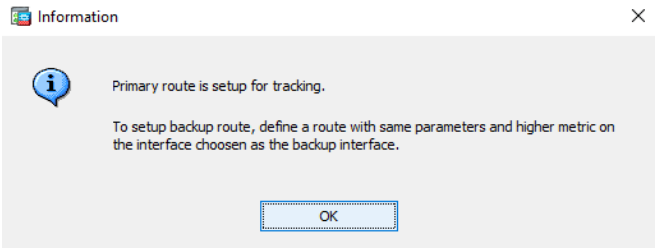


Рис. 3.40. Повідомлення після налаштування маршрута з монітором

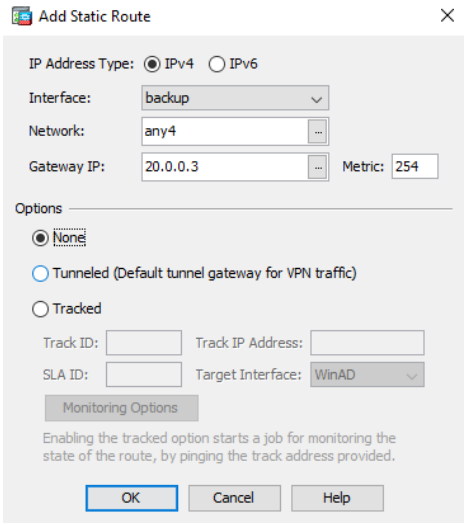


Рис. 3.41. Налаштування резервного маршруту з більшою метрикою

Принцип роботи даного типу налаштувань дуже простий, за допомогою SLA монітору, ми відслідковуємо наступний перехід або доступність потрібного нам пристрою в мережі, при втраті зв'язку між ними системою буде автоматично видалено статичний маршрут з траком, який був зв'язаний з ним, коли монітор, в нашому випадку, при відправці 3 пакетів кожні 10 секунд не отримає відповіді від обраного пристрою для перевірки з'єднання .

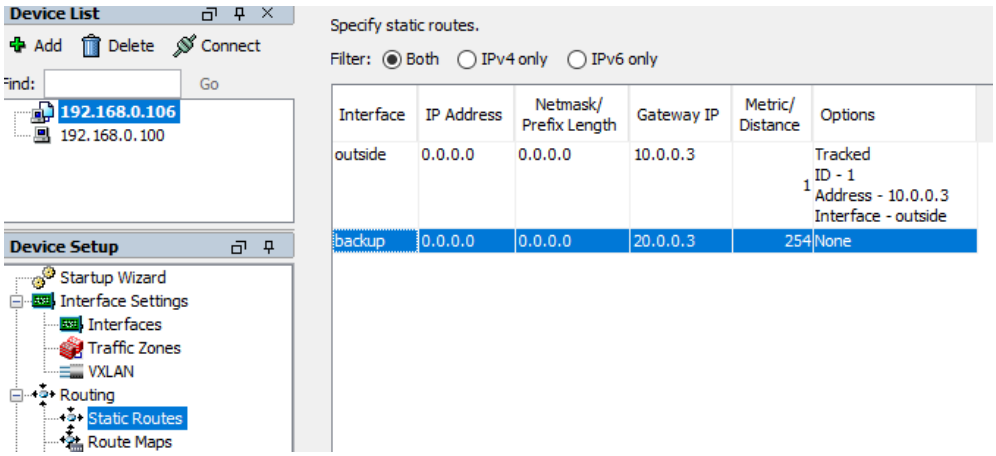


Рис. 3.42. Налаштовані основний та резервний маршрути для доступу до мережі інтернет.

Через ситуацію з пандемією більшість компаній почали переходити на віддалену роботу, тим самим вони почали використовувати найпоширенішу схему організації віддаленої роботи- це використання Access VPN + Remote Desktop. Ця схема є найпоширенішою через простоту реалізації та мінімальньні витрати на її реалізацію.

Я реалізував цю схему за допомогою Cisco AnyConnect VPN та віддаленого робочого столу операційної системи Windows.

Першим кроком буде налаштування AnyConnect в даному випадку ми будемо налаштовувати його на міжмережному екрані Cisco ASA так як така можливість уже інтегрована в даний пристрій.

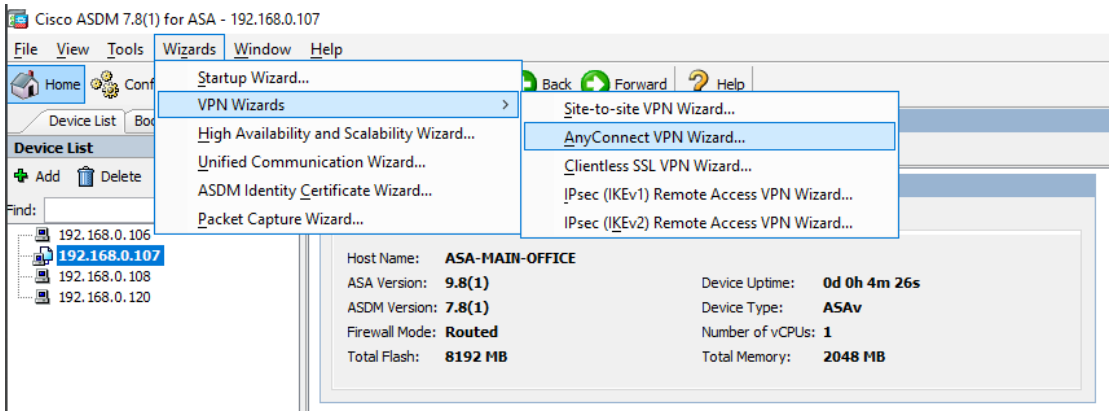


Рис. 3.43. Запуск майстра налаштувань AnyConnect

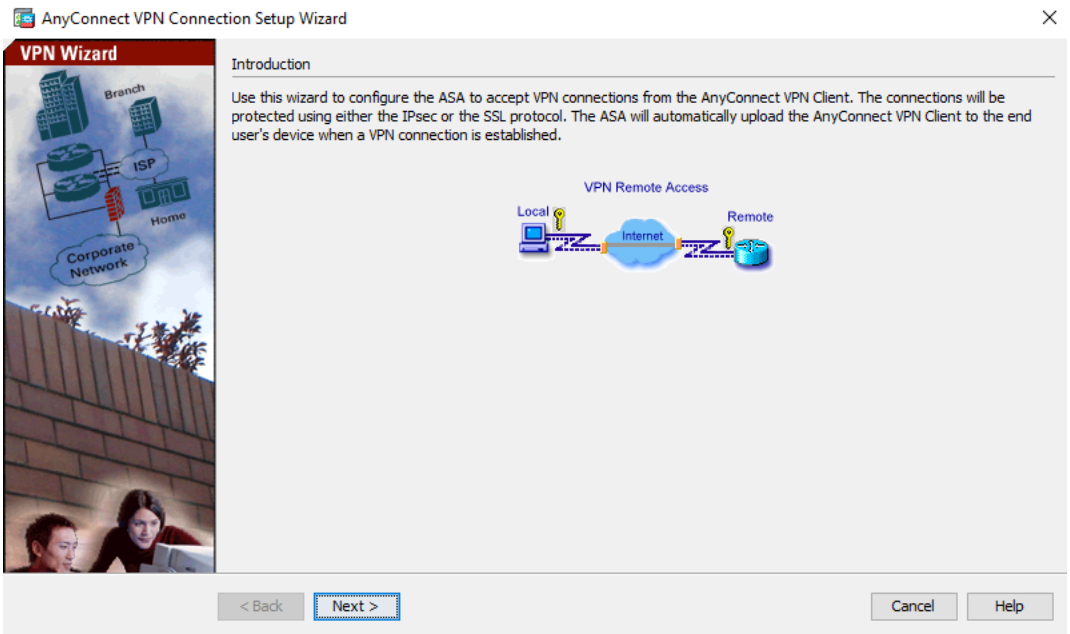


Рис. 3.44. Введення в налаштування

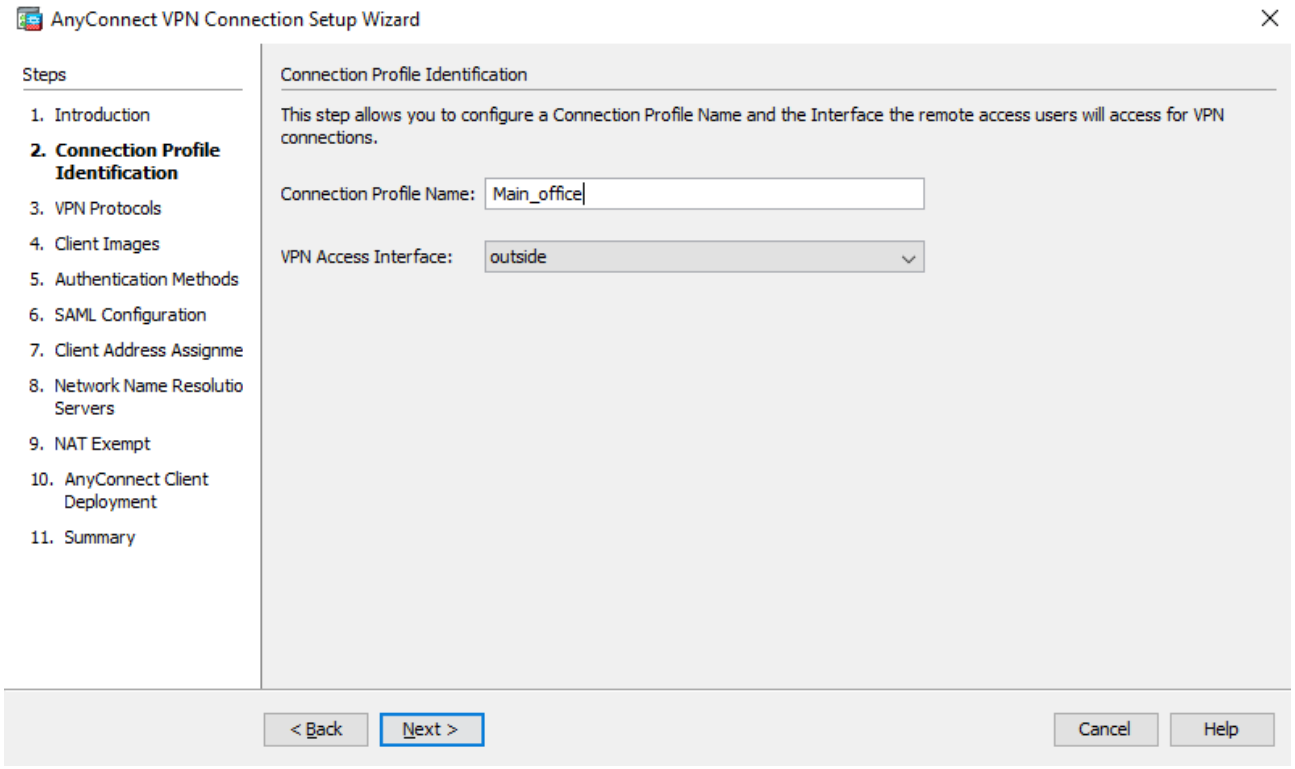


Рис. 3.45. Створення профілю та вибір інтерфейса для підключення

Так, як у нас немає створених сертифікатів для віддалених клієнтів, ми створимо самопідписний сертифікат за допомогою менеджера сертифікатів.

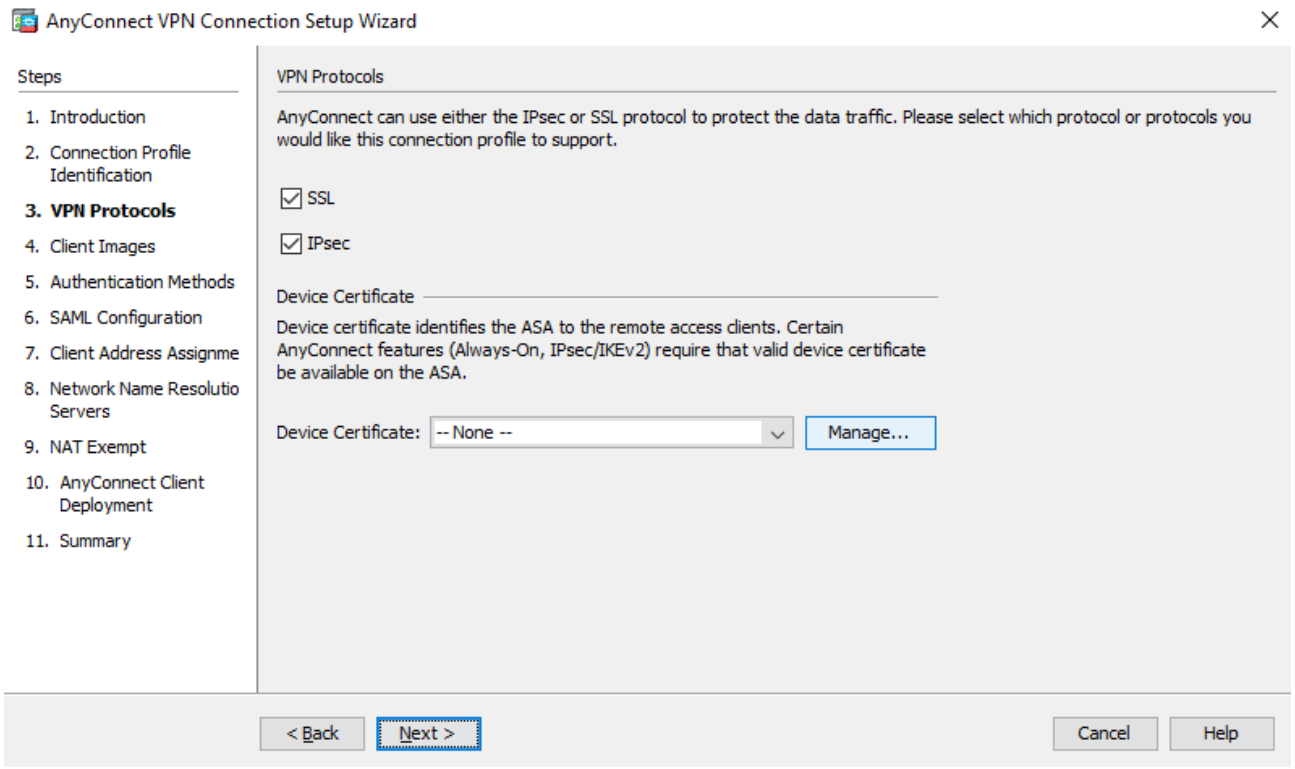


Рис. 3.46. Вибір сертифіката та VPN протоколів

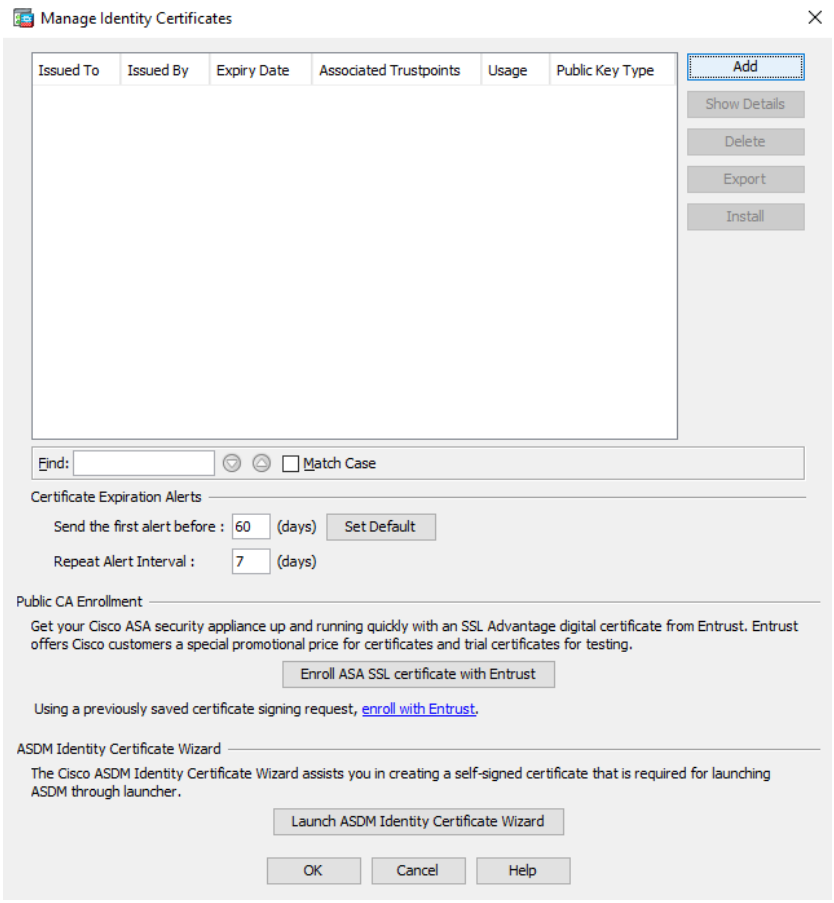


Рис. 3.47. Менеджер сертифікатів

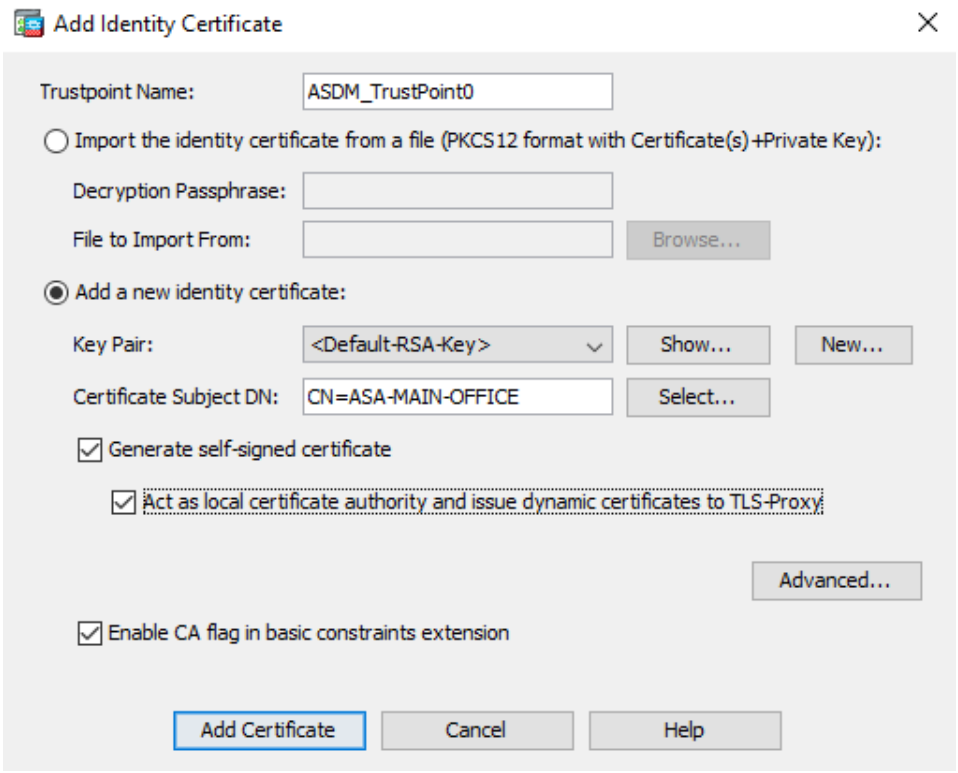


Рис. 3.48. Створення самопідписного сертифікату

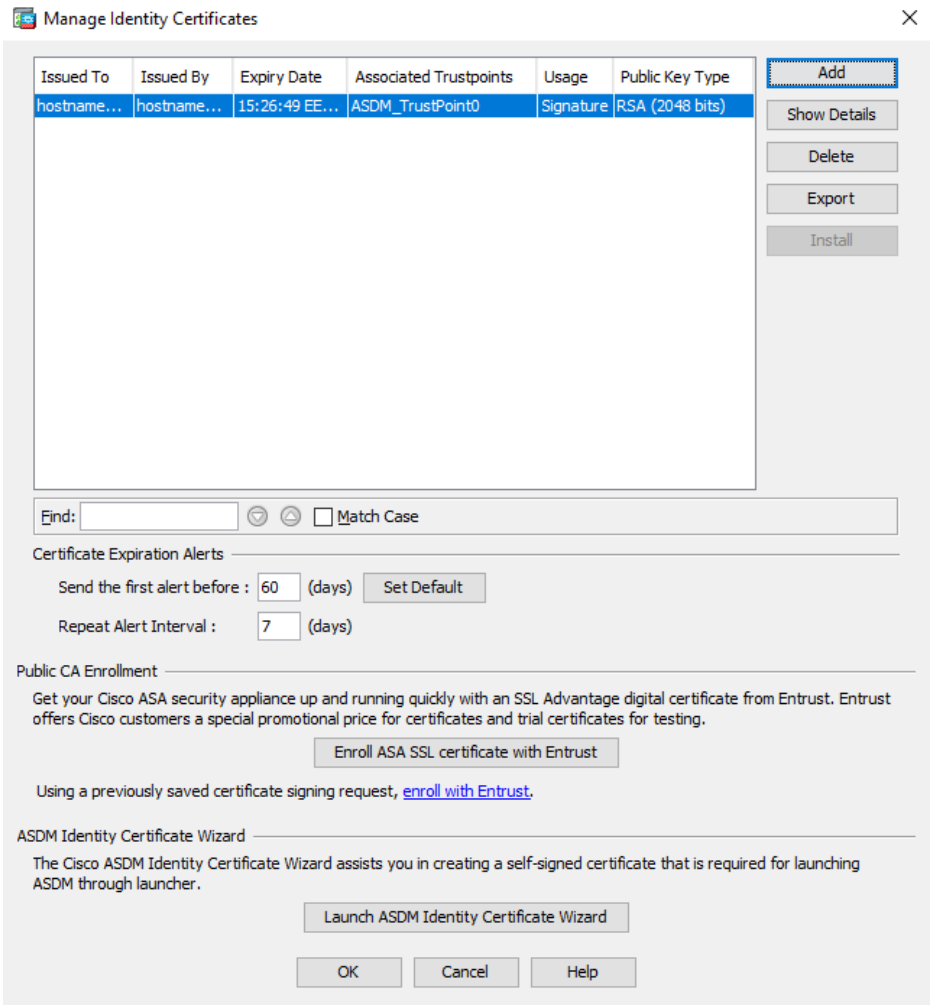


Рис. 3.49. Вибір сертифікату, який був створений на попередньому зображенні

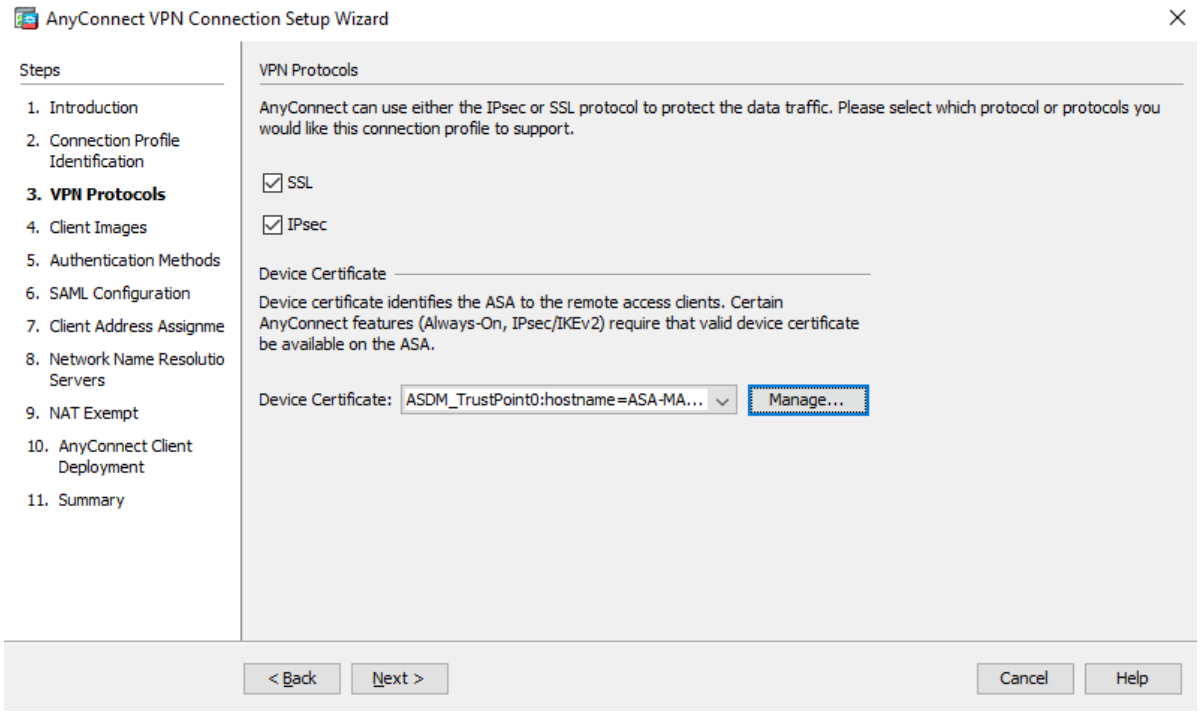


Рис. 3.50. Вибір сертифіката та протоколів VPN

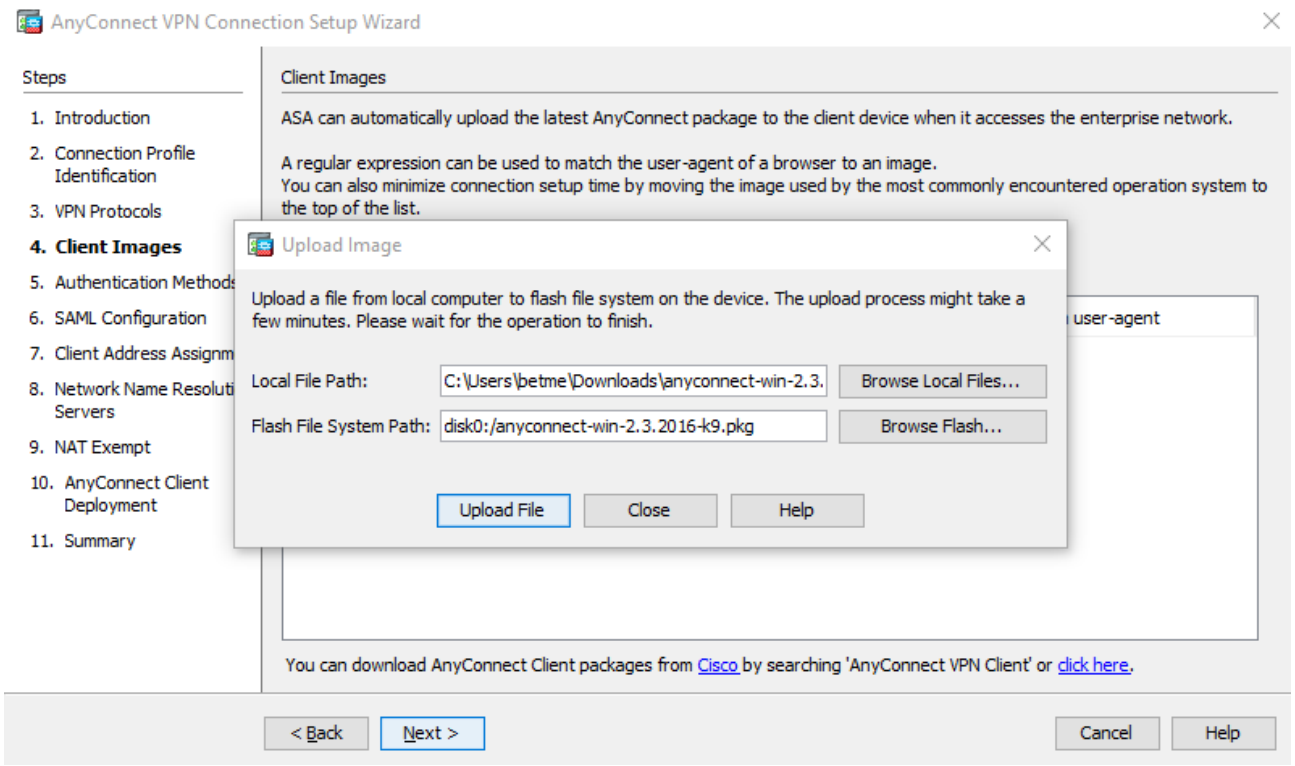


Рис. 3.51. Завантаження образу клієнта для операційної системи Windows

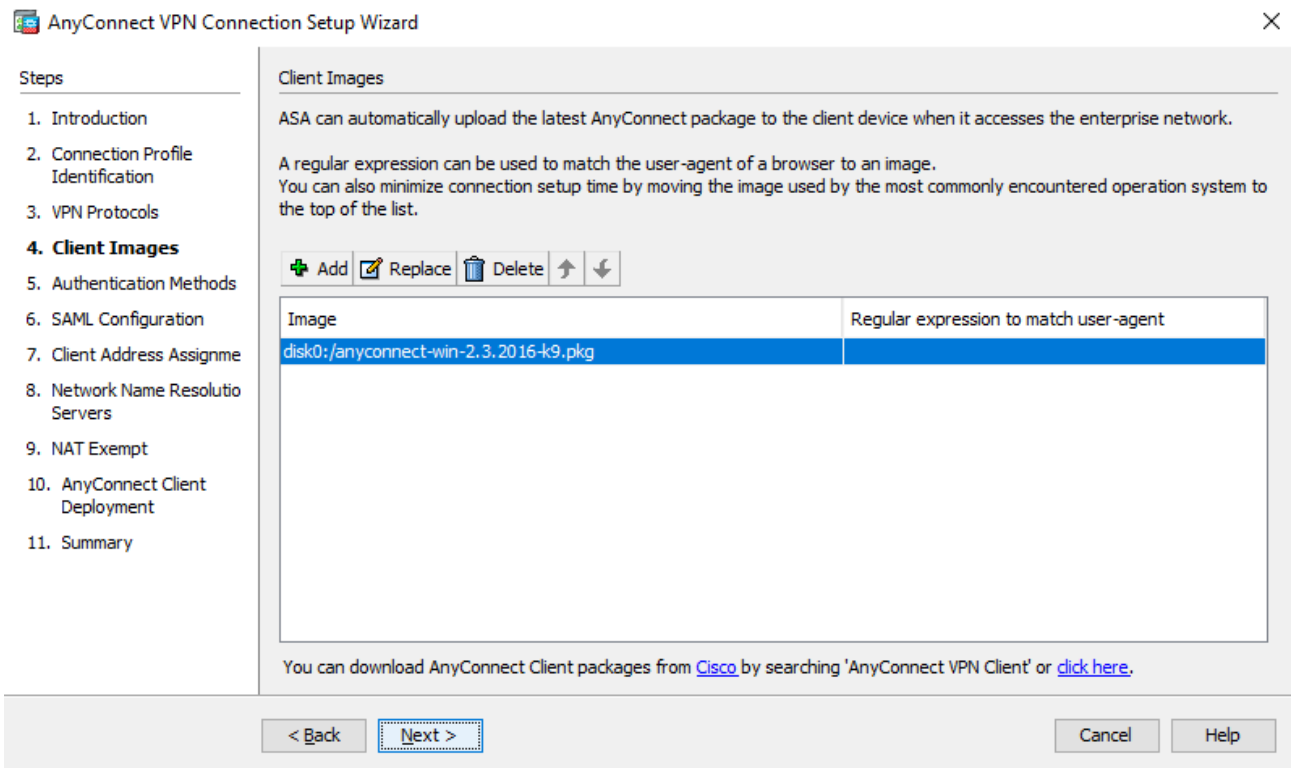


Рис. 3.52. Вибір завантаженого образу для підключення клієнтів

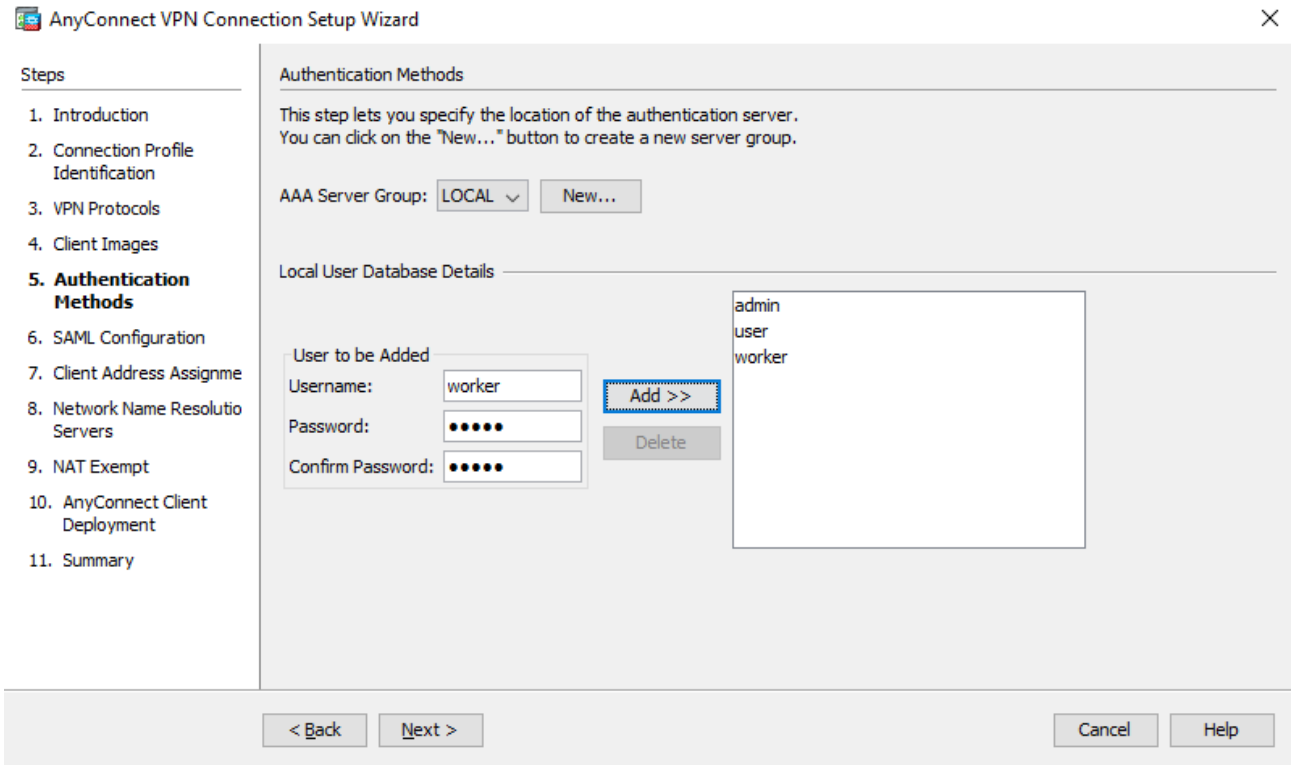


Рис. 3.53. Додавання користувачів до локального серверу AAA

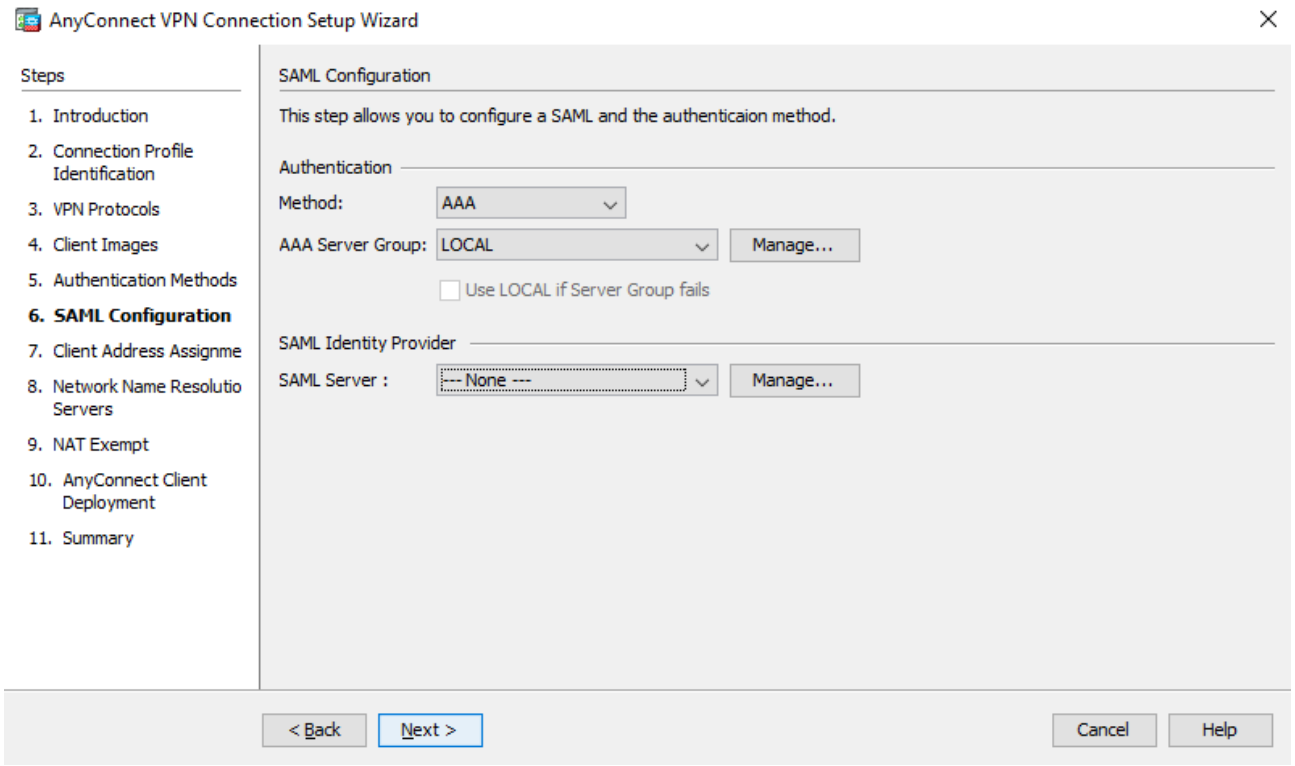


Рис. 3.54. Вибір методу автентифікації

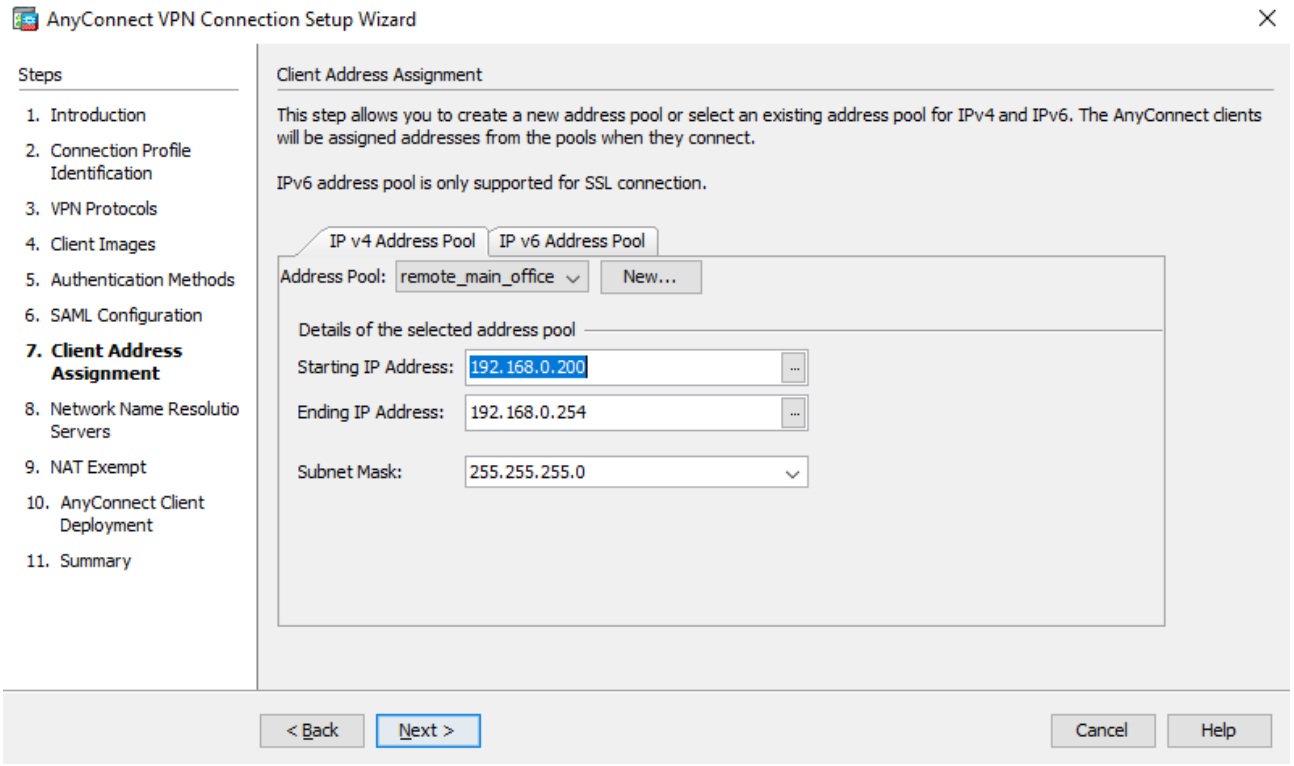


Рис. 3.55. Створення пулу адрес для віддалених клієнтів

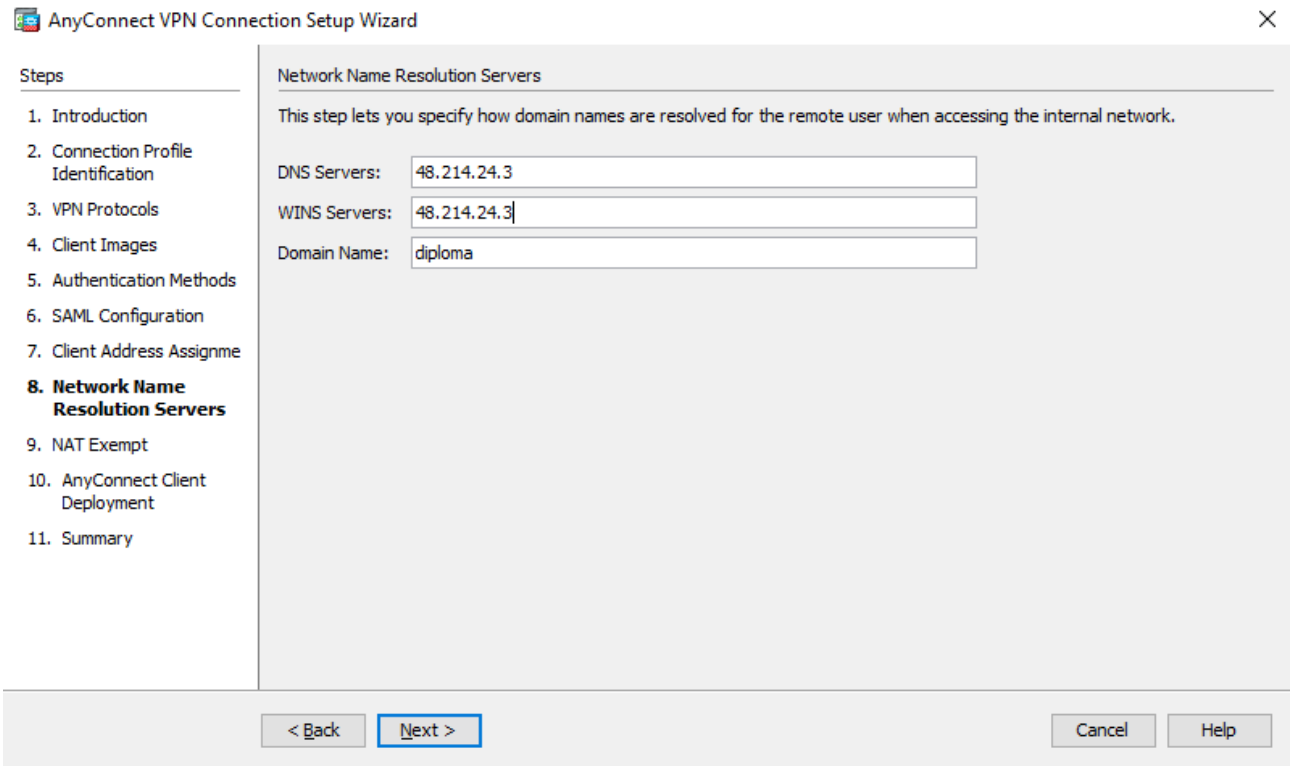


Рис. 3.56. Додавання адрес DNS і WinAD серверів та редагування доменного імені

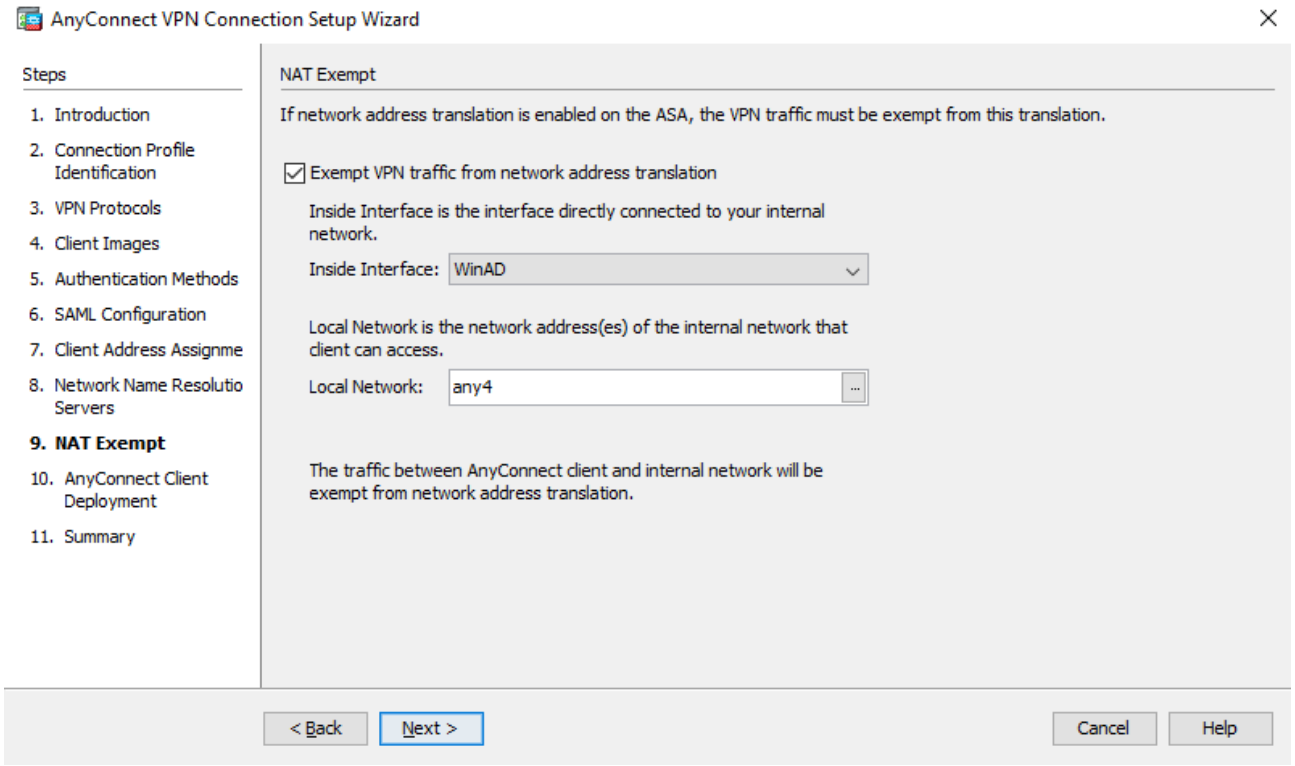


Рис. 3.57. Налаштування NAT для віртуальної мережі

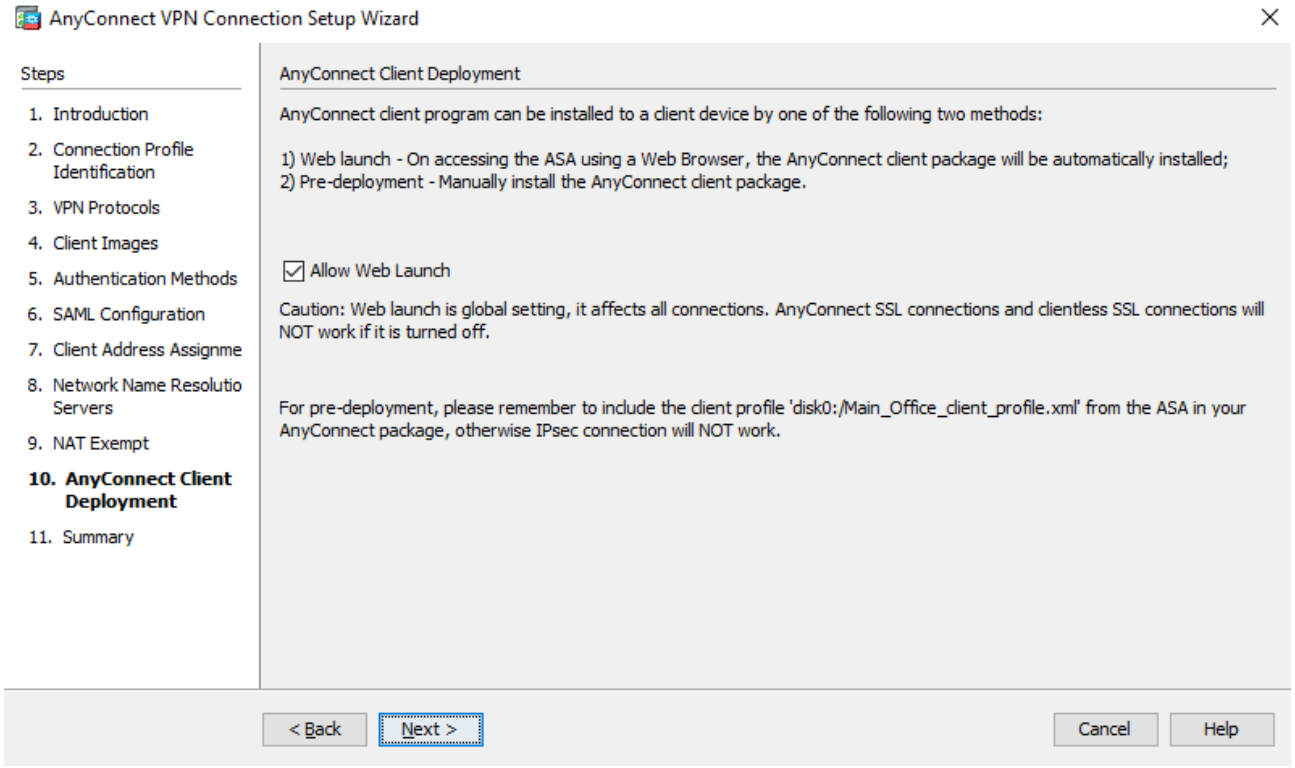


Рис. 3.58. Ввімкнення веб інтерфейсу для завантаження Cisco AnyConnect Secure Mobility Client

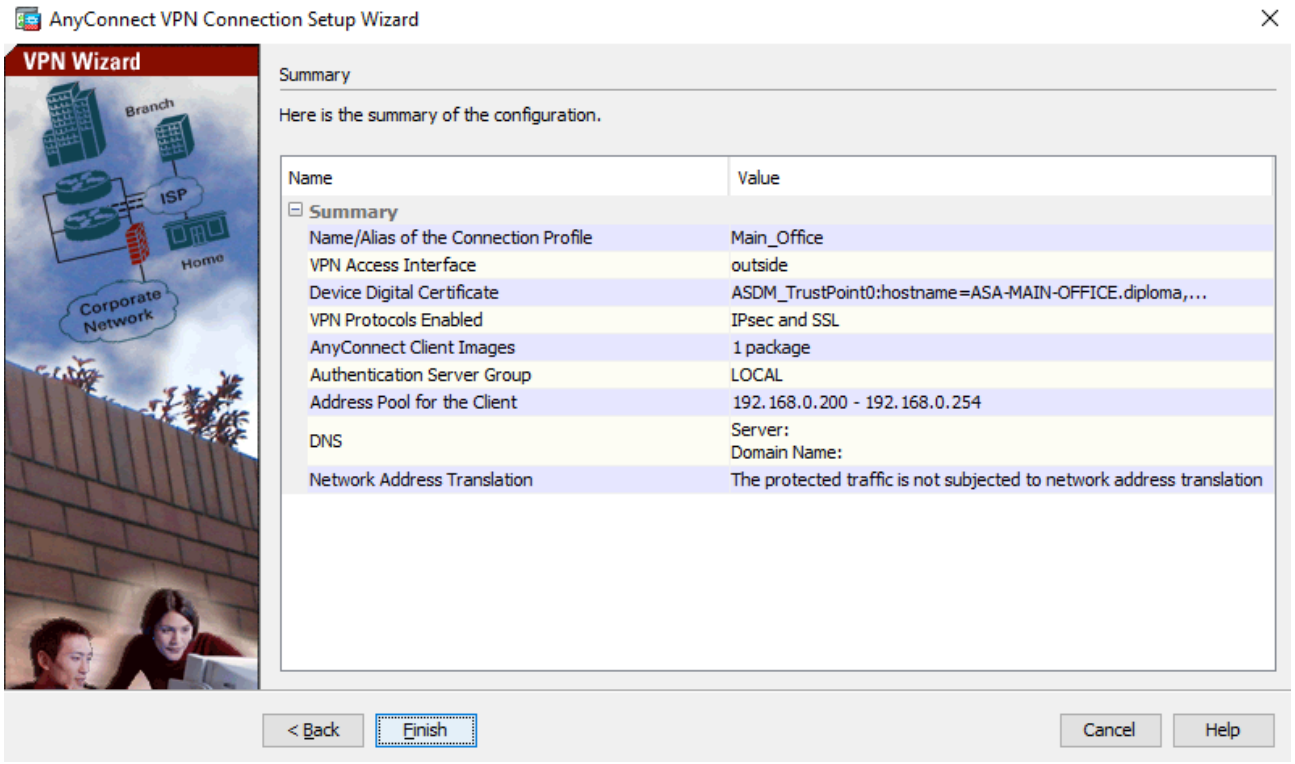


Рис. 3.59. Перевірка налаштувань перед збереженням

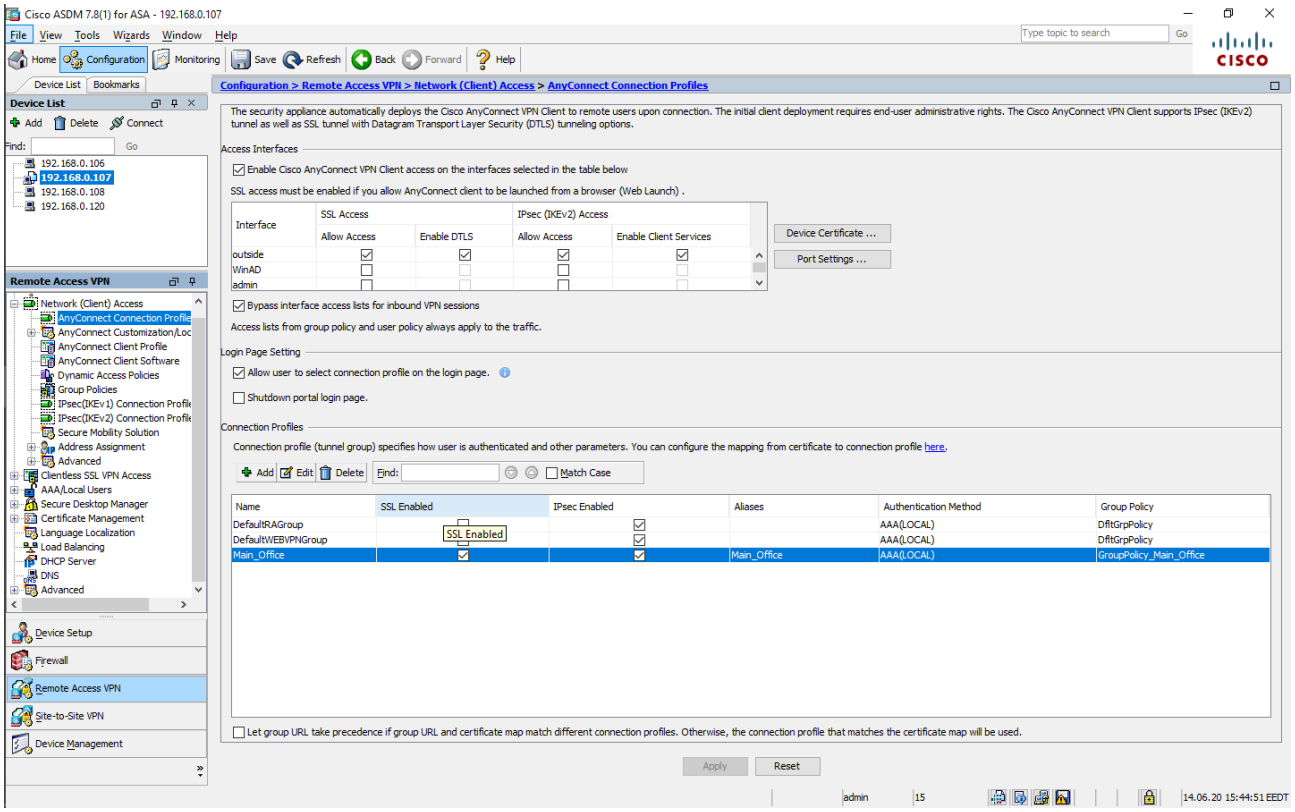


Рис. 3.60. Перевірка збережених налаштувань

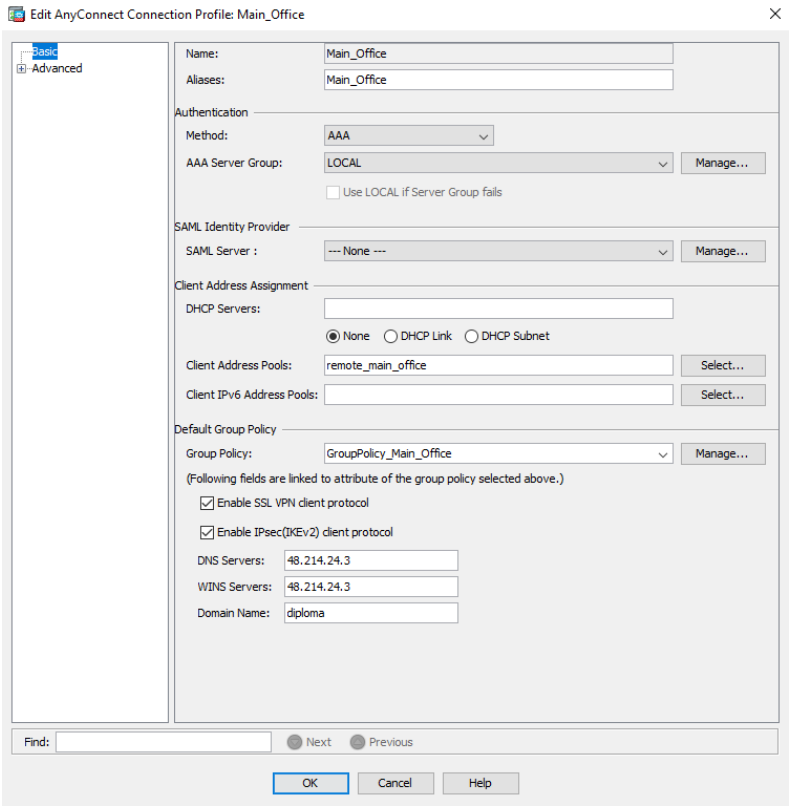


Рис. 3.61. Перевірка профілю підключення

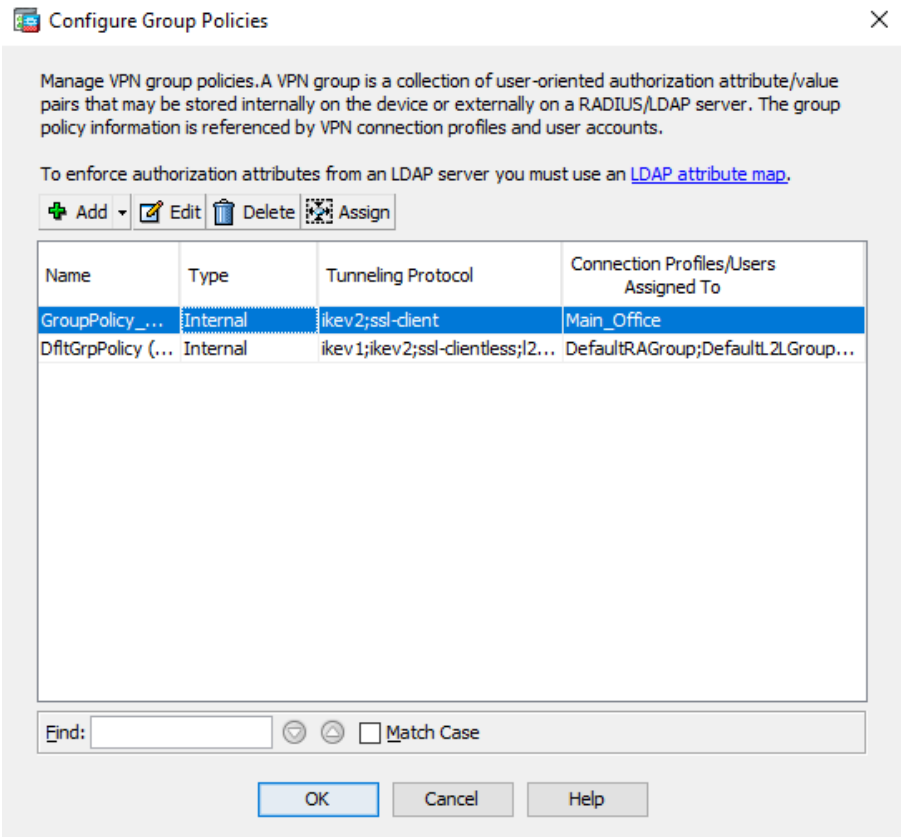


Рис. 3.62. Налаштування групової політики

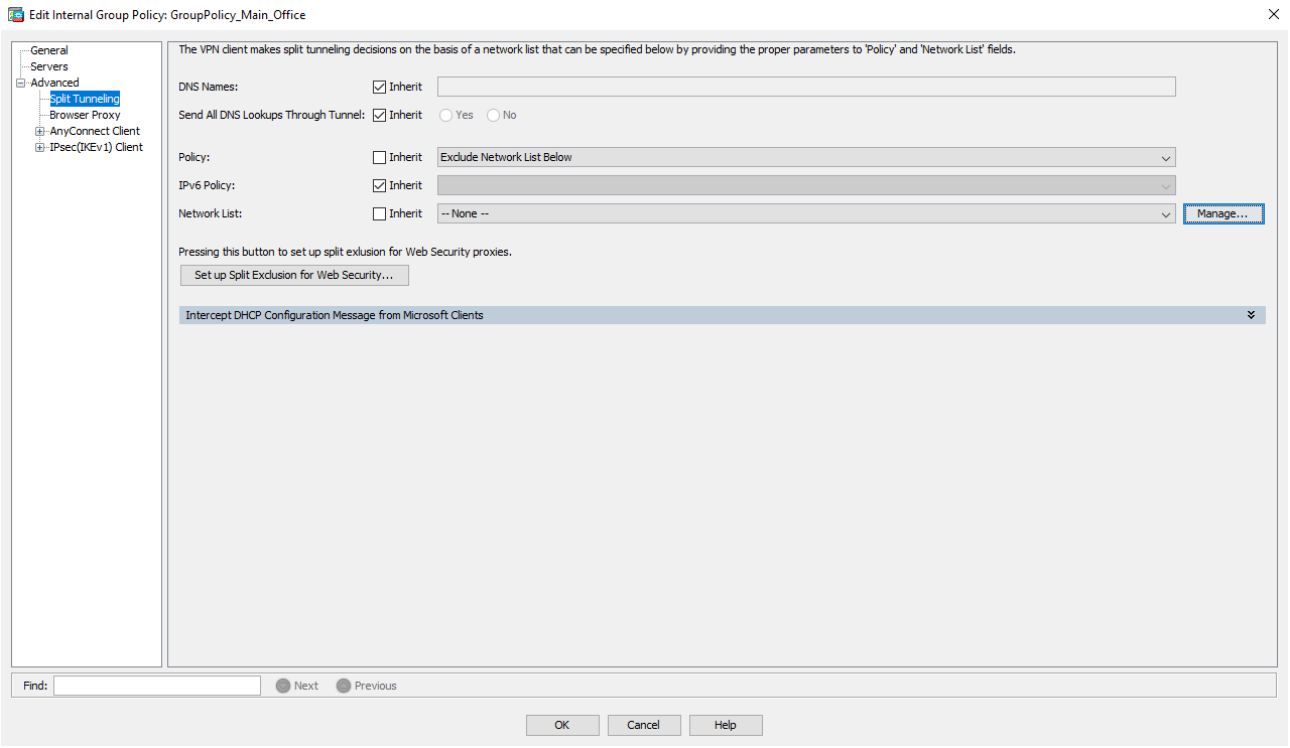


Рис. 3.63. Налаштування правил Split Tunel

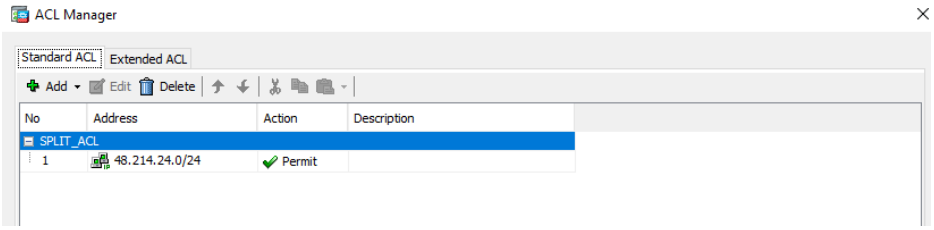


Рис. 3.64. Налаштування списку доступу

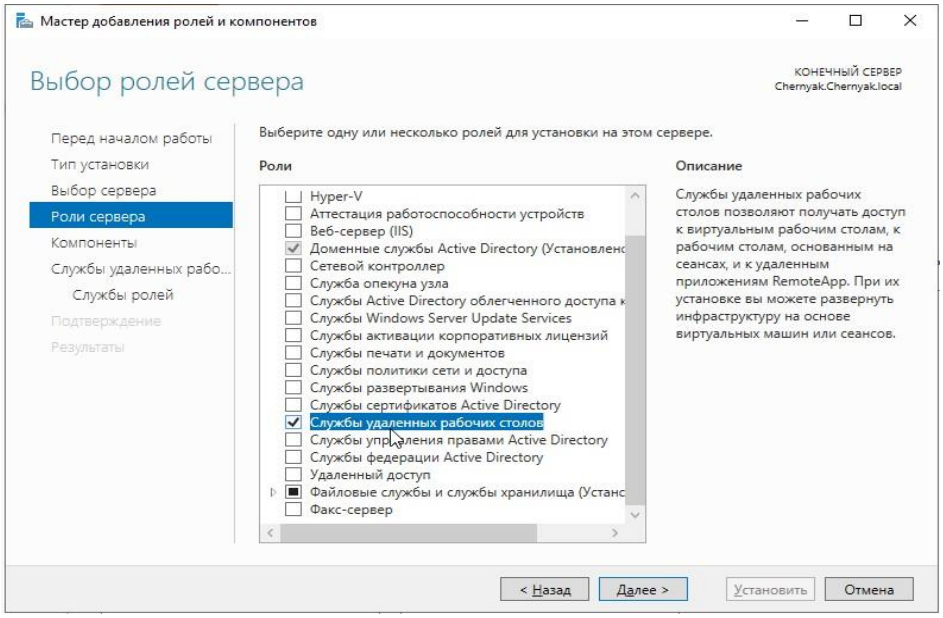


Рис. 3.65. Встановлення служби віддалених робочих столів

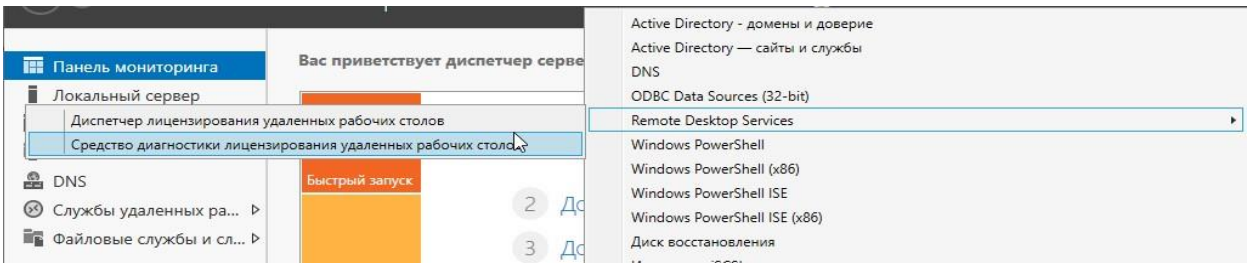


Рис. 3.66. Перевірка наявності служби віддалених робочих столів

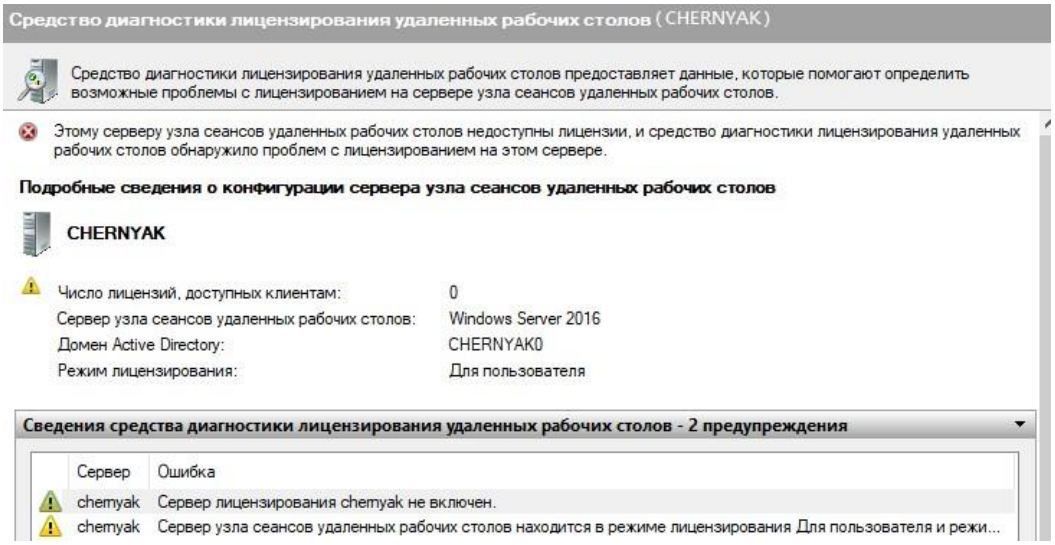


Рис. 3.67. Активація сервера ліцензій віддалений робочих столів

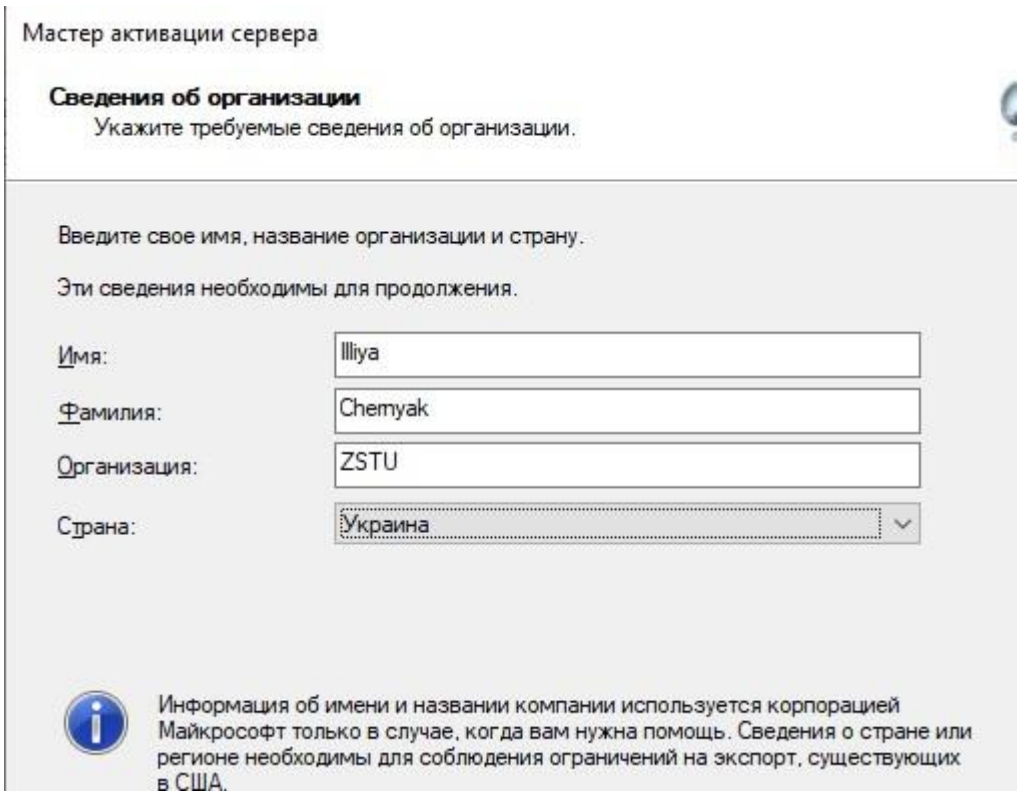


Рис. 3.68. Активація сервера ліцензій віддалений робочих столів

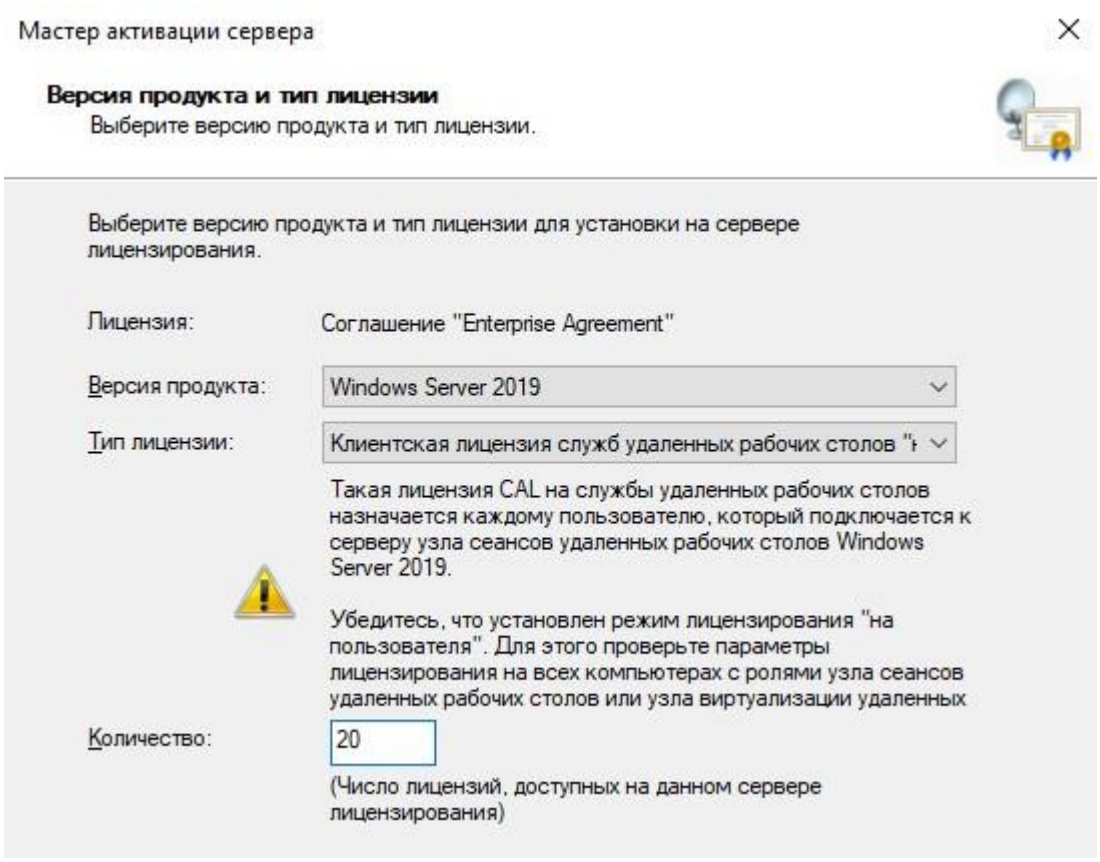


Рис. 3.69. Параметри активації

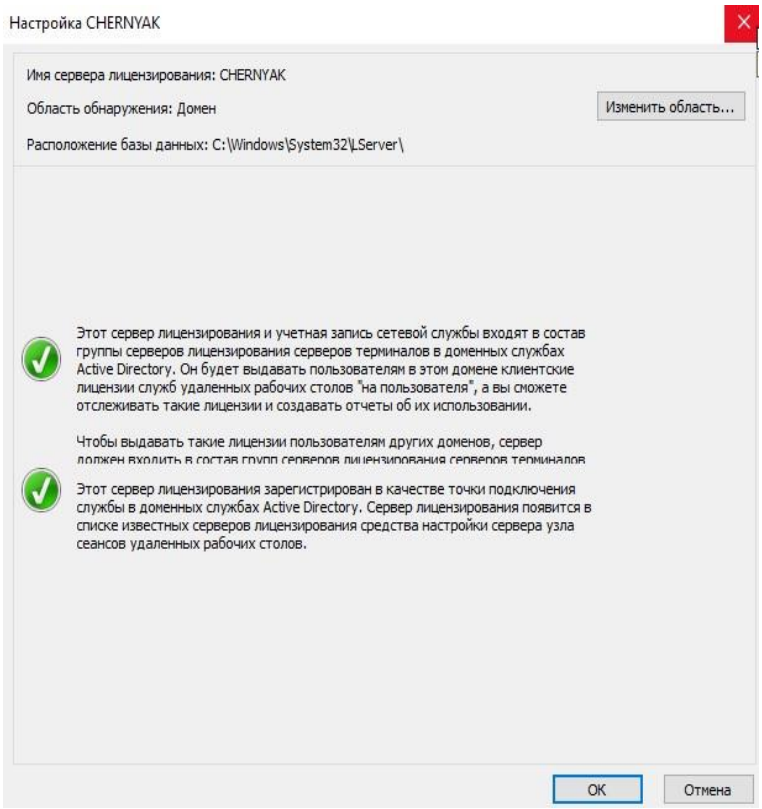


Рис. 3.70. Додавання в групу

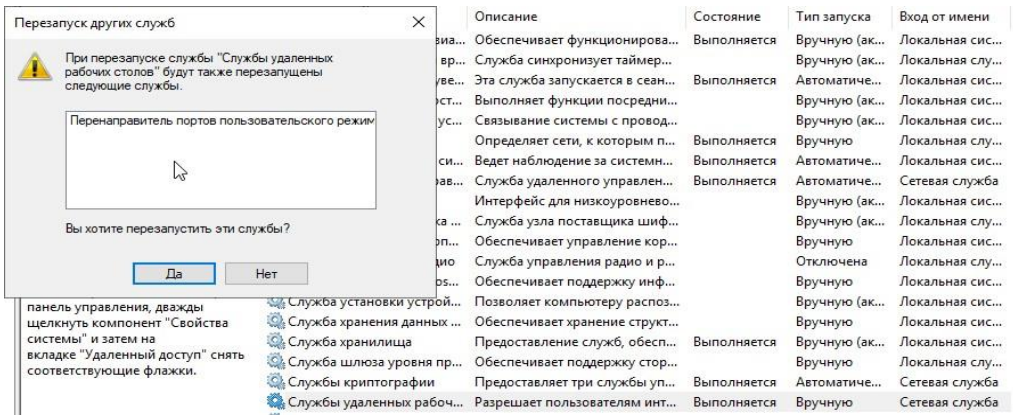


Рис. 3.71. Перезапуск служби

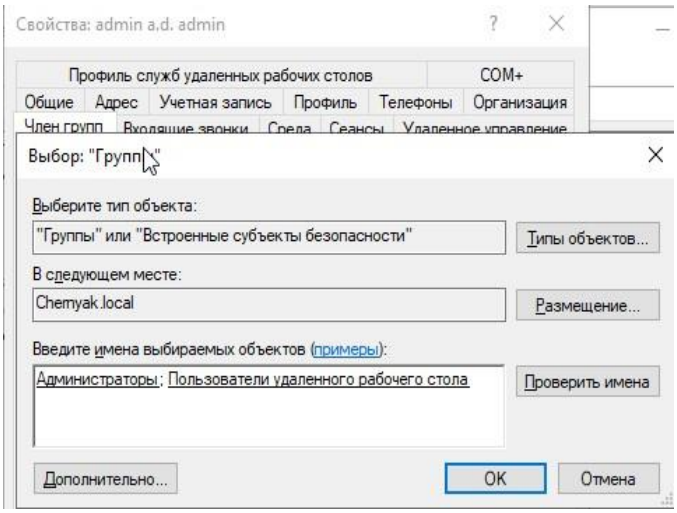


Рис. 3.72. Створення користувача та додання до відповідних груп

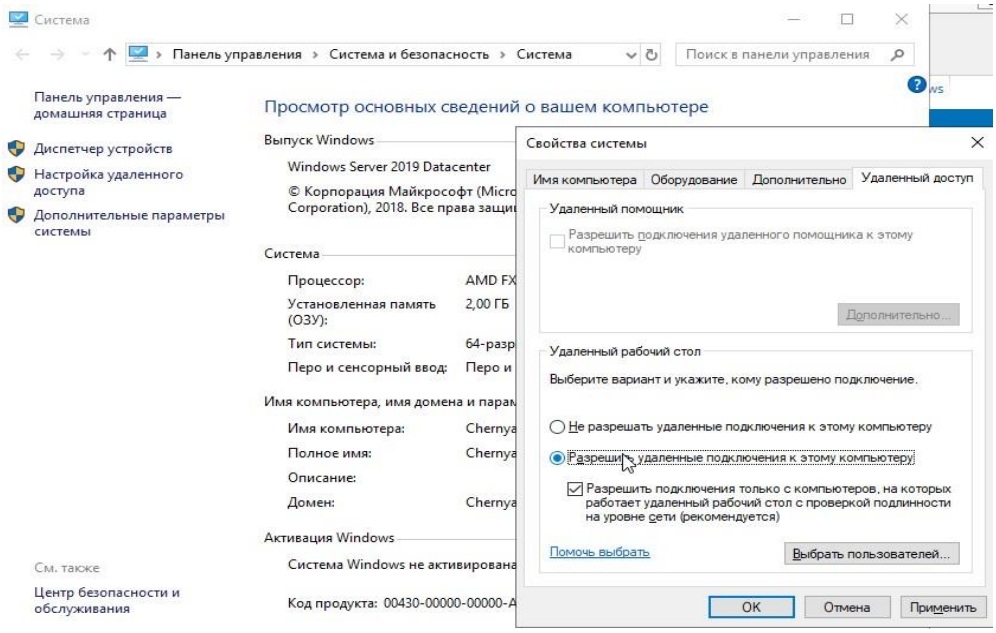


Рис. 3.73. Налаштування віддаленого доступу до робочої станції

3.3. Тестування підсистеми резервування каналів зв’язку та перевірка роботи мережі та налаштованих сервісів

Після налаштувань головного та резревуючого пристрою та збереження налаштувань їх треба завантажити в потрібній послідовності, щоб основний пристрій завантажився першим, а пристрій, який повинен бути в режимі standby другим, тим самим після завантаження другого пристрою, ми побачимо повідомлення про те, що в мережі знайдено активний пристрій.

```
ASA-active-failover> .

        Detected an Active mate
Beginning configuration replication from mate.
WARNING: Disabling auto import may affect Smart Licensing
WARNING: Local user database is empty and there are still 'aaa' commands for 'LO
CAL'.
Creating trustpoint "_SmartCallHome_ServerCA" and installing certificate...

Trustpoint CA certificate accepted.

WARNING: Trustpoint _SmartCallHome_ServerCA is already authenticated.
End configuration replication from mate.
```

Рис. 3.74. Ввімкнення резервуючого пристроя в мережі

Після втрати зв’язку спрацьовує дія в EEM, яка перезавантажує головний пристрій, тим самим передаючи роль основного пристрою резервному.

Для тесту ми відімкнемо порт комутатора, який безпосередньо підключений до основного пристрою, тим самим перевіримо, чи спрацьовує резервування в автоматичному режимі за допомогою налаштованого менеджера подій.

Active_Failover

```
WARNING: Trustpoint _SmartCallHome_ServerCA is already authenticated.
End configuration replication from mate.

Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.

        Switching to Active

ASA-Active>
```

Рис. 3.75. Перемикання в активний режим резервуючого пристроя

Резервування спрацьовує, швидкість спрацювання доволі висока, так як по суті, ми має 2 ввімкнутих пристрої і резервний має скопійовану конфігурацію з основного пристою, тим самим перемикання проходить дуже швидко.

Інший способів резервування, який був налаштований в даній мережі, - це IP SLA static track. Для перевірки роботи основного та резервного статичних маршрутів, ми також будемо вимикати та вмикати інтерфейси.

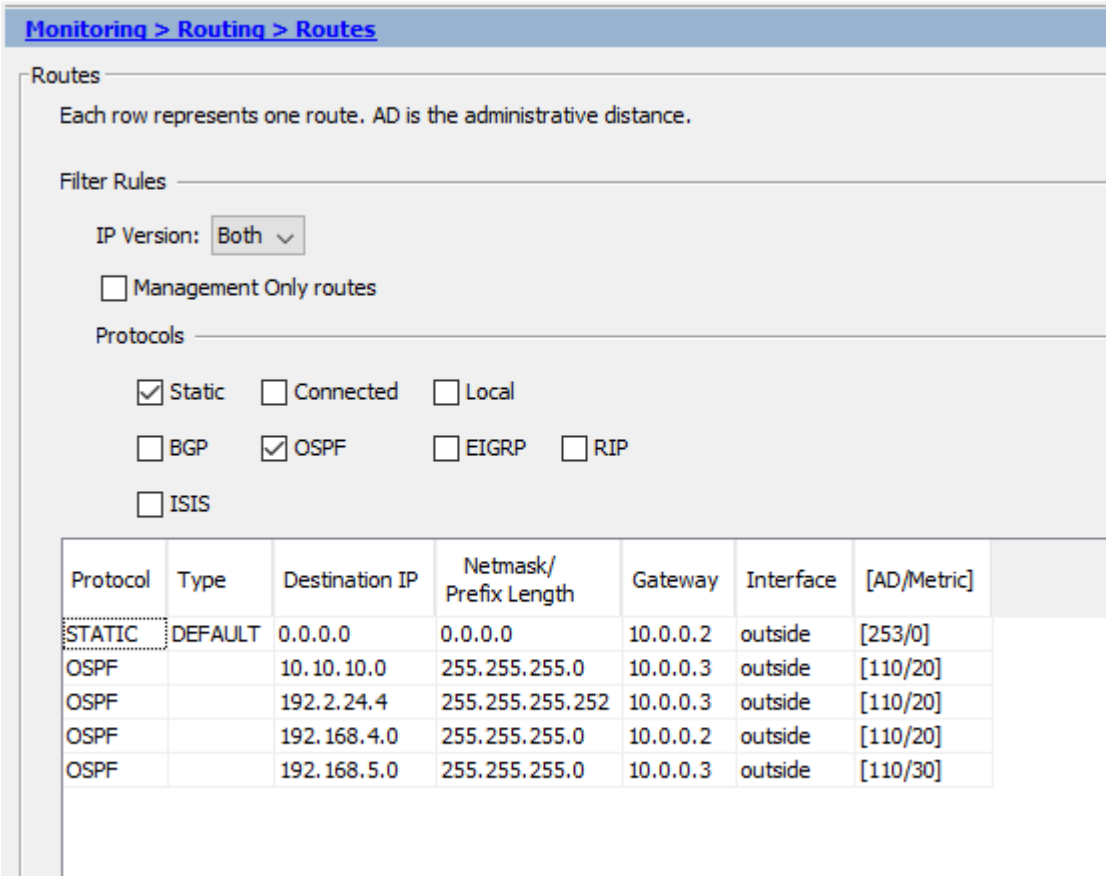


Рис. 3.76. Перевірка роботи основного статичного маршрута для доступу в інтернет до вимкнення інтерфейсу

Для перевірки вимкнемо інтерфейс, доступність до якого перевіряється за допомогою SLA монітору.

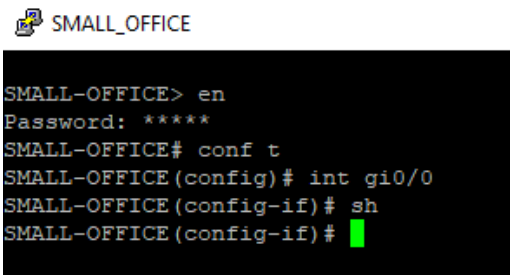
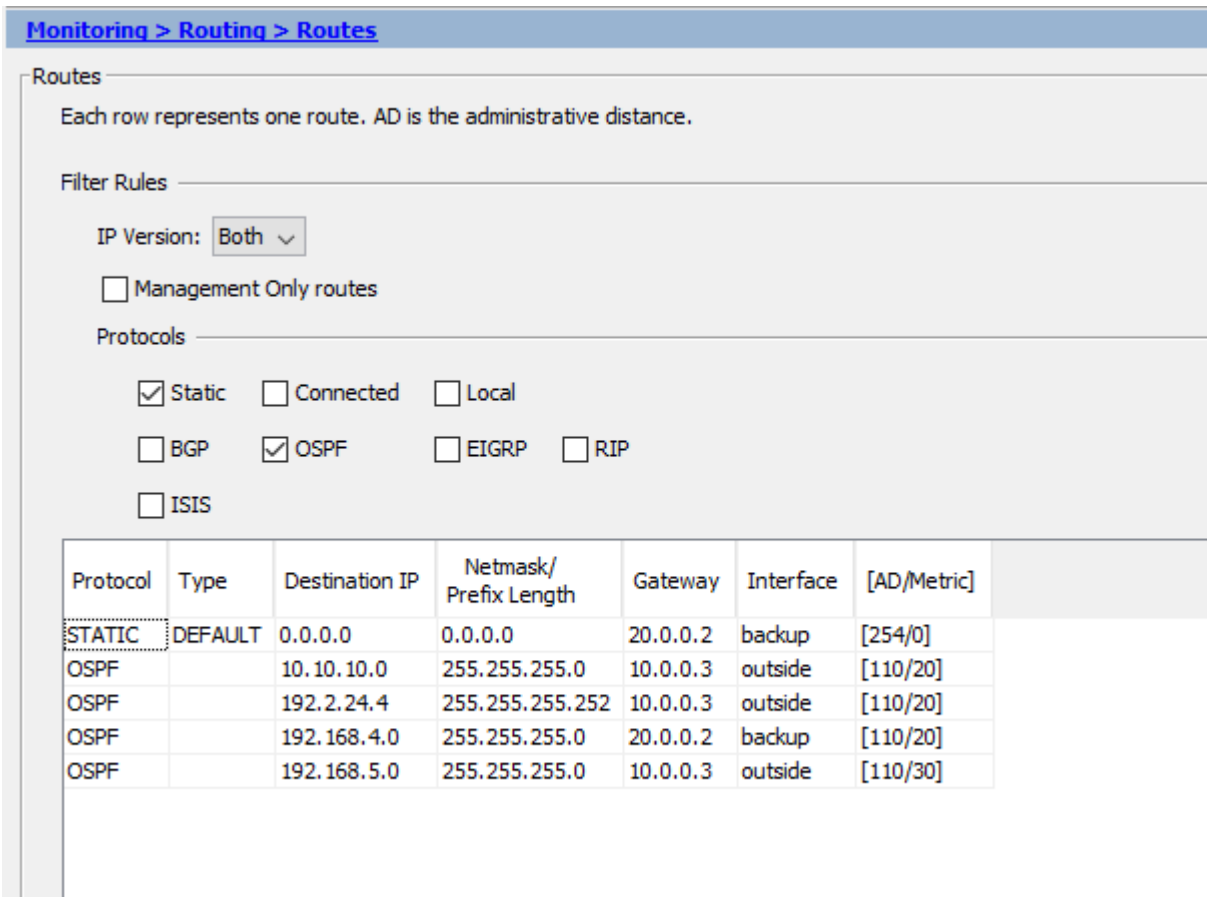


Рис. 3.77. Вимкнення інтерфейсу для моніторингу

Як ми бачимо, результатом вимкнення інтерфейсу, доступ до якого перевірявся SLA, видалення основного маршруту з таблиці маршрутизації та заміна його резервним маршрутом з більшою метрикою.



Protocol	Type	Destination IP	Netmask/ Prefix Length	Gateway	Interface	[AD/Metric]
STATIC	DEFAULT	0.0.0.0	0.0.0.0	20.0.0.2	backup	[254/0]
OSPF		10.10.10.0	255.255.255.0	10.0.0.3	outside	[110/20]
OSPF		192.2.24.4	255.255.255.252	10.0.0.3	outside	[110/20]
OSPF		192.168.4.0	255.255.255.0	20.0.0.2	backup	[110/20]
OSPF		192.168.5.0	255.255.255.0	10.0.0.3	outside	[110/30]

Рис. 3.78. Результат роботи SLA + track для резервного маршруту

Для перевірки повернення основного маршруту після відновлення з’єднання, ми знову ввімкнемо інтерфейс,, який моніториться.

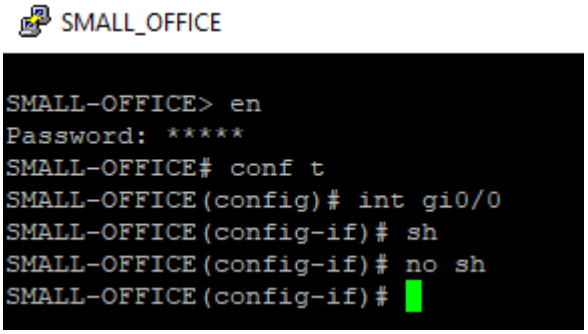


Рис. 3.79. Ввімкнення інтерфейсу для моніторингу

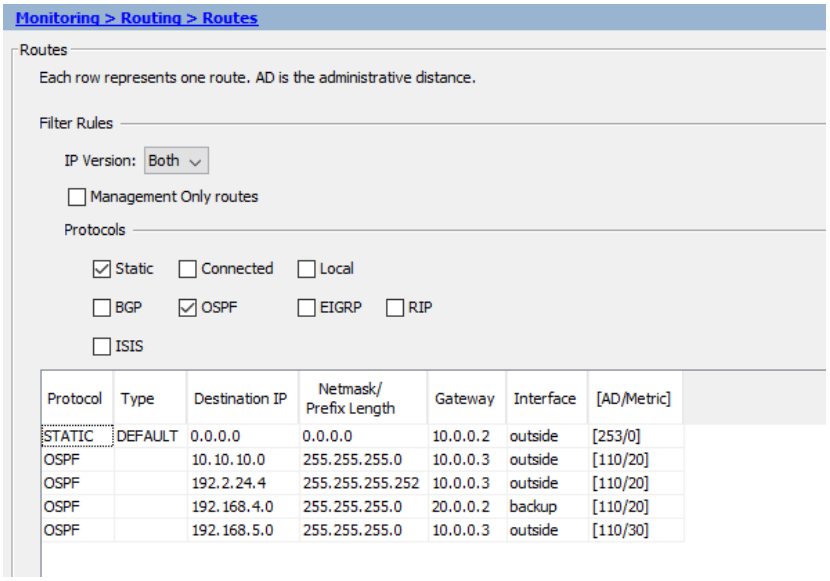


Рис. 3.78. Результат роботи SLA + track для резервного маршруту після відновлення з’єднання

Тим самим, ми бачимо стабільну роботу даного типу резервування, перевіримо доступність пристроїв в мережі інтернет під час перемикання за допомогою icmp пакетів, які будуть відправлятися для тестування.

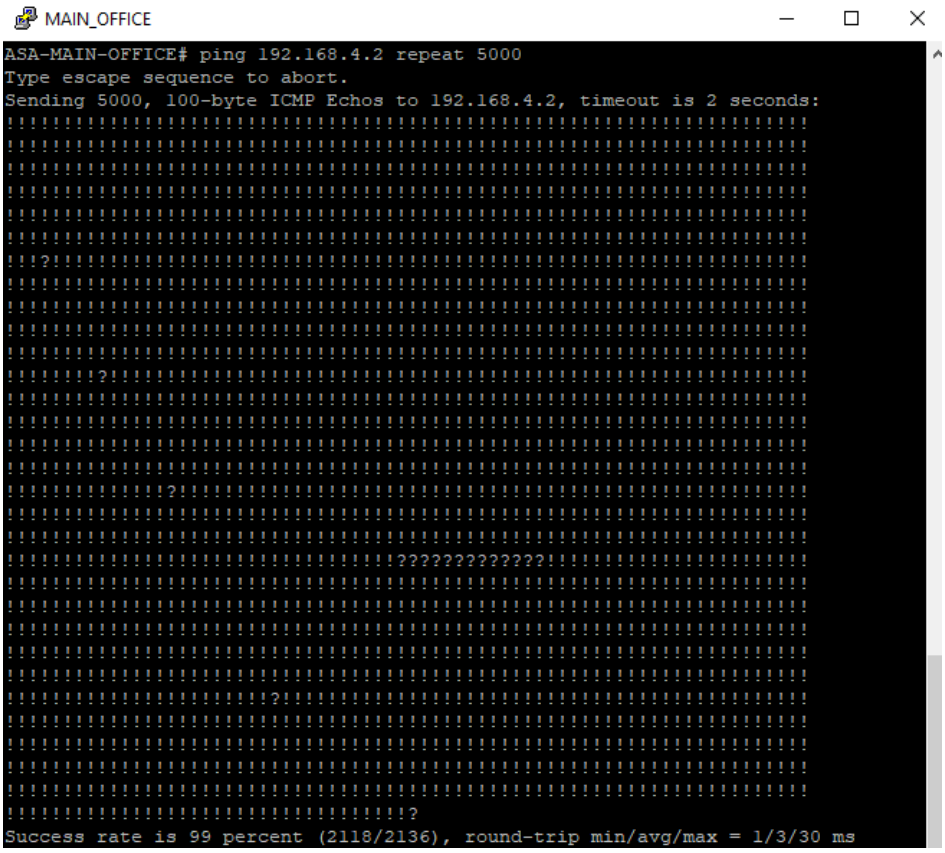


Рис. 3.79. Перевірка затримки перемикання на резервний маршрут

З рисунка вище, ми бачимо, що затримка в перемиканні на резервний маршрут є невеликою, 13 пакетів icmp, що складає приблизно 0,4 секунди.

Наступною частиною резервування каналів є протоколи агрегації каналів, в нашому випадку- це протоколи PAgP між пристроями DB_R і DATABASE_OFFICE та протокол LACP між пристроями INSIDE_DB_NETWORK і DB_WORKER. На рисунках нижче, ми можемо побачити, чи працює налаштована агрегація та в якому вона режимі.

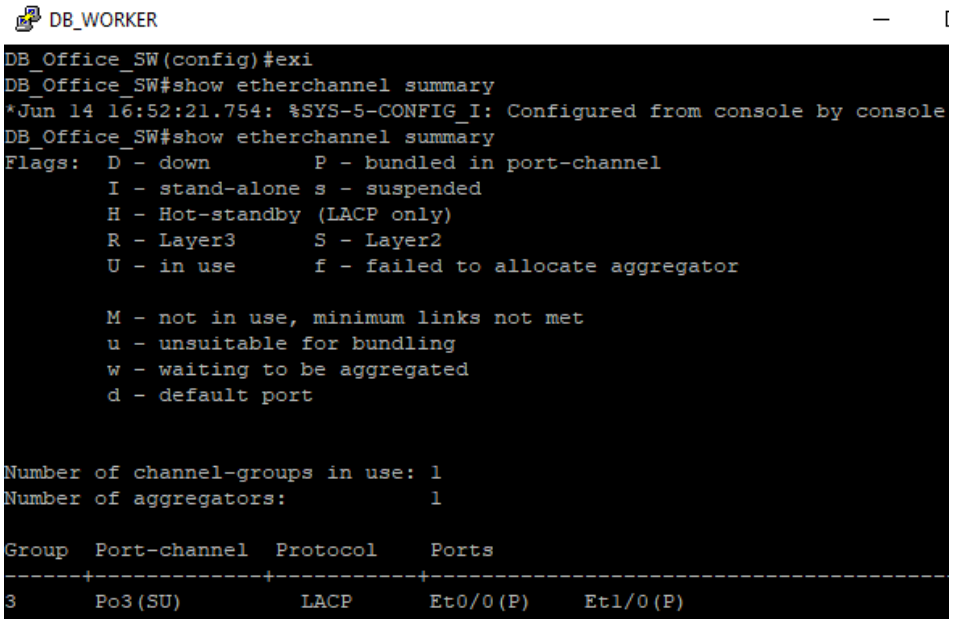


Рис. 3.80. Перевірка роботи та протоколу агрегування на DB_WORKER

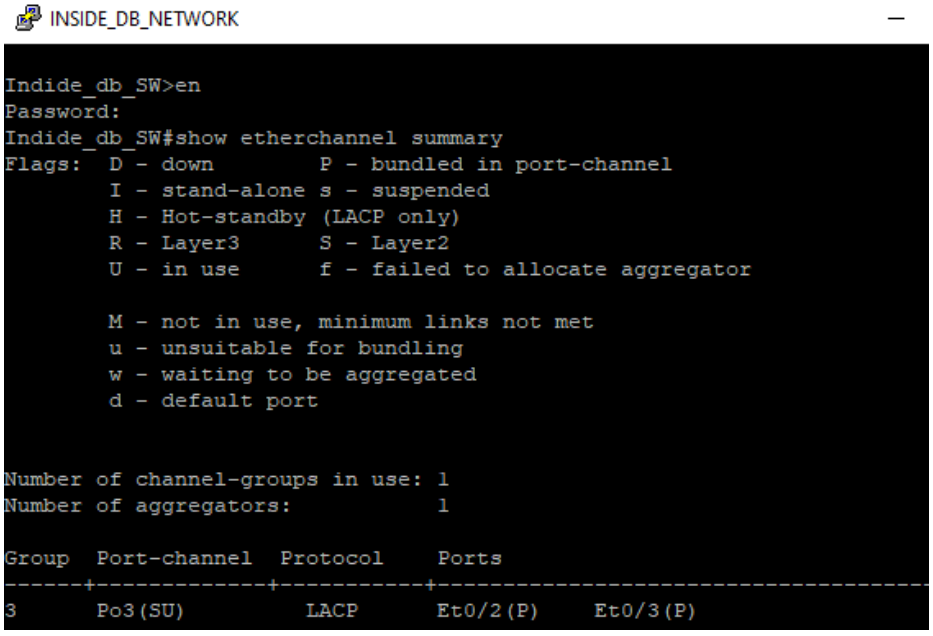


Рис. 3.81. Перевірка роботи та протоколу агрегування на NSIDE_DB_NETWORK

INSIDE_DB_NETWORK

```
Indide_db_SW#sh etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 3
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po3    (Primary Aggregator)

------------

Age of the Port-channel   = 0d:00h:12m:29s
Logical slot/port   = 16/0          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Et0/2    Active             0
  0     00     Et0/3    Active             0

Time since last port bundled:    0d:00h:12m:18s    Et0/3
```

Рис. 3.82. Перевірка роботи агрегованого канала на NSIDE_DB_NETWORK

DB_WORKER

```
DB_Office_SW#sh etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 3
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po3    (Primary Aggregator)

------------

Age of the Port-channel   = 0d:00h:13m:39s
Logical slot/port   = 16/0          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Et0/0    Passive            0
  0     00     Et1/0    Passive            0

Time since last port bundled:    0d:00h:13m:10s    Et1/0
Time since last port Un-bundled: 0d:00h:13m:13s    Et1/0
```

Рис. 3.83. Перевірка роботи агрегованого канала на DB_WORKER

Наступним кроком- це перевірка роботи агрегованого канала при втраті з’єднання одного з каналів зв’язку, для цього ми відімкнемо один з портів, якій використовується в агрегованому каналі.

Під час відімкнення було втрачено 1 пакет при перемиканні агрегованого каналу, через це ми можемо сказати, що затримка для відновлення зв’язку є мінімальною, яка навіть не вплине на роботу мережі в цілому.

DB_WORKER

```
DB_Office_SW#sh etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 3
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po3    (Primary Aggregator)

------------

Age of the Port-channel   = 0d:01h:18m:00s
Logical slot/port   = 16/0          Number of ports = 1
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Et0/0    Passive            0

Time since last port bundled:    0d:00h:01m:01s    Et1/0
Time since last port Un-bundled: 0d:00h:00m:41s    Et1/0
```

Рис. 3.84. Перевірка роботи агрегованого канала на DB_WORKER

DB_WORKER28

```
192.168.5.4 icmp_seq=14995 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=14996 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=14997 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=14998 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=14999 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=15000 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=15001 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=15002 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=15003 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=15004 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=15005 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=15006 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=15007 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=15008 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=15009 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=15010 ttl=64 time=0.001 ms
192.168.5.4 icmp_seq=15011 ttl=64 time=0.001 ms
```

Рис. 3.85. Відправка тестових пакетів для тестування резервування за допомогою агрегованого каналу

```
*Jun 14 18:00:36.114: %EC-5-L3DONTBNDL2: Et0/3 suspended: LACP currently not ena
bled on the remote port.
```

Рис. 3.86. Повідомлення що агрегація відімкнута на одному з портів через вимкнення порту на іншому пристрої

Наступний тип резервування- це пропрієтарний протокол PAgP розроблений Cisco

DB_R

```
Database_router#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1
------------

Age of the Port-channel   = 0d:00h:02m:17s
Logical slot/port   = 16/0          Number of ports = 2
GC                  = 0x00010001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   PAgP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Et1/3    Desirable-Sl       0
  0     00     Et2/0    Desirable-Sl       0

Time since last port bundled:    0d:00h:01m:35s    Et2/0
```

Рис. 3.87. Перевірка роботи та протоколу агрегування на DB_R

DATABASE_OFFICE

```
DB_Office#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1
------------

Age of the Port-channel   = 0d:00h:01m:18s
Logical slot/port   = 16/0          Number of ports = 2
GC                  = 0x00010001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   PAgP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Et0/0    Automatic-Sl       0
  0     00     Et0/1    Automatic-Sl       0

Time since last port bundled:    0d:00h:01m:09s    Et0/1
```

Рис. 3.88. Перевірка роботи та протоколу агрегування на DATABASE_OFFICE

```
DB_Office#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1
------------

Age of the Port-channel   = 0d:00h:23m:04s
Logical slot/port   = 16/0          Number of ports = 1
GC                  = 0x00010001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   PAgP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Et0/0    Automatic-S1       0

Time since last port bundled:    0d:00h:22m:54s    Et0/1
Time since last port Un-bundled: 0d:00h:00m:16s    Et0/1
```

Рис. 3.89. Перевірка роботи протоколу агрегування на DB_R при вимкнені одного з інтерфейсів

При використанні протоколів агрегації каналів дуже просто резервувати будь-яке з'єднання типу точка-точка, і ми маємо можливість прокласти 15 резервних каналів для збільшення надійності передачі і резервування.

Наступна частина, яка частково може відноситися не лише до віддаленої роботи а й до резервування, - це віддалений доступ до мережі основного офісу організації та підключення до віддаленого робочого столу.

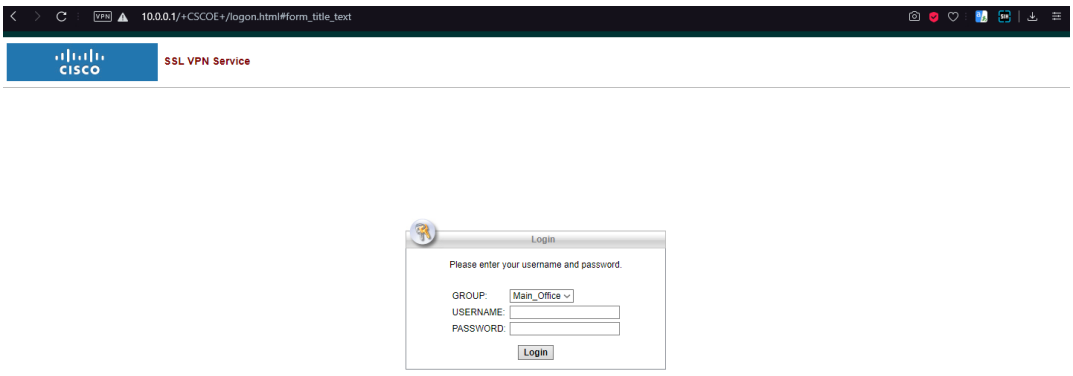


Рис. 3.90. Підключення до веб інтерфейсу користувача для авторизації і подальшого завантаження клієнта



Рис. 3.91. Підключення до веб інтерфейсу користувача для завантаження клієнта

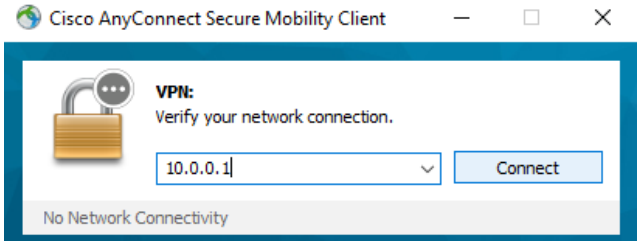


Рис. 3.92. Підключення до мережі організації

Так як сертифікат є самопідписним, ми отримуємо повідомлення про це, і нам потрібно погодитися з цим, для успішного підключення до сервера.

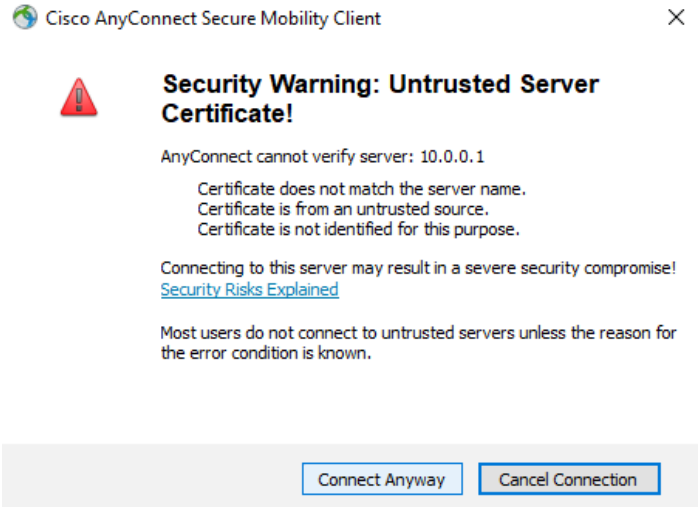


Рис. 3.93. Підтвердження підключення так як сертифікат самопідписний

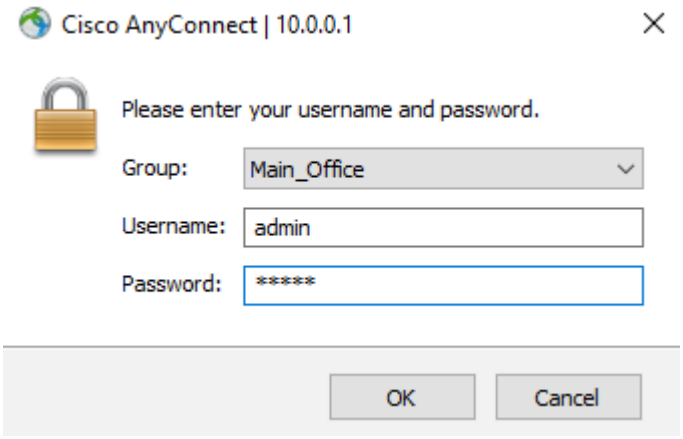


Рис. 3.94. Введення даних авторизації

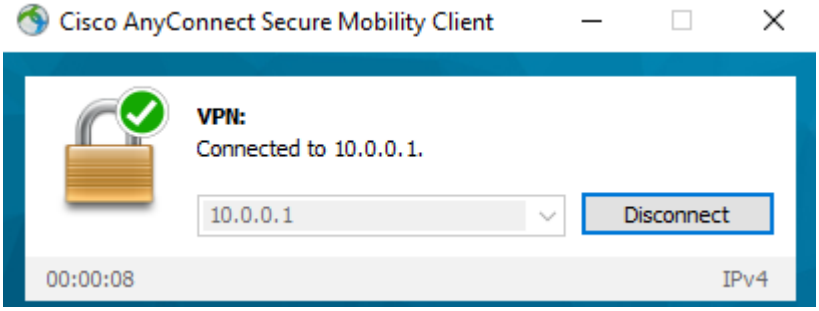


Рис. 3.95. Успішне підключення до мережі організації

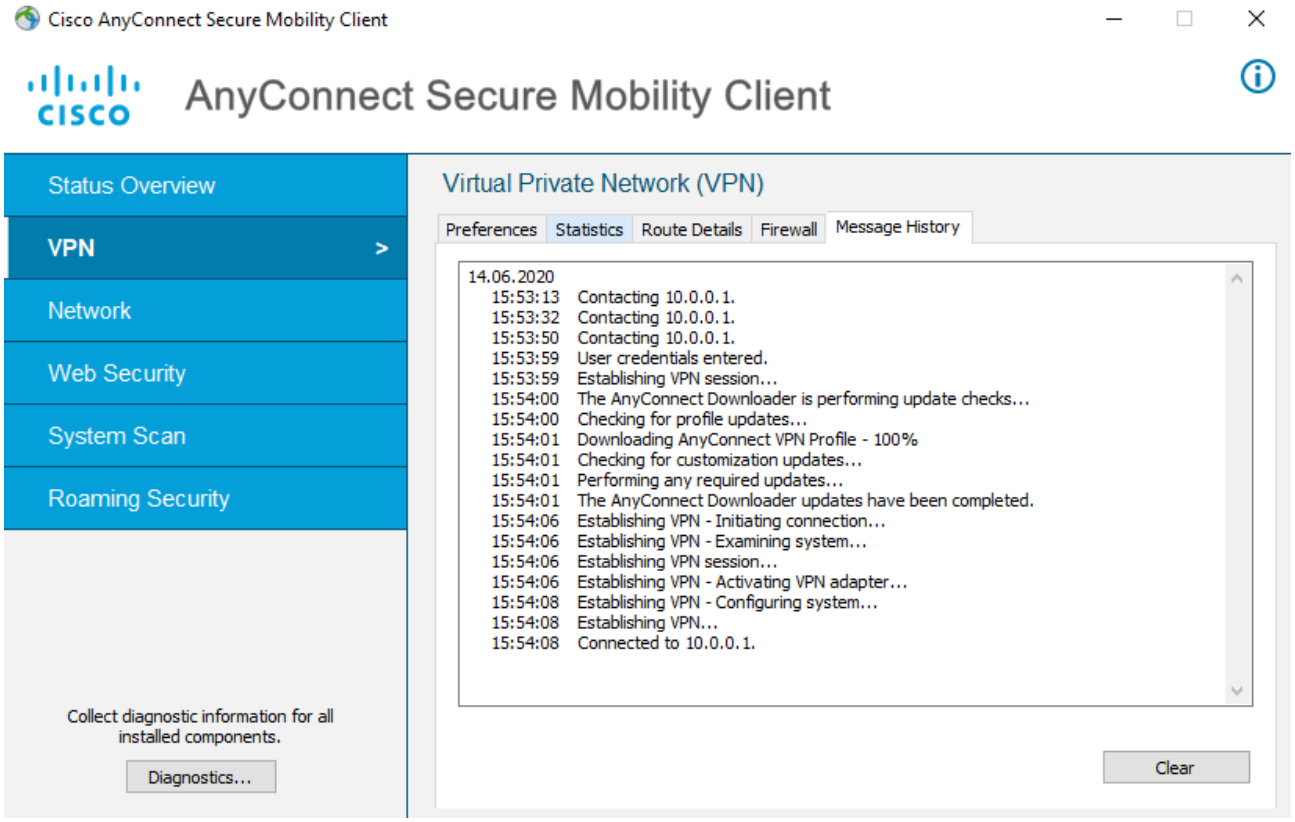


Рис. 3.96. Перевірка інформації про VPN підключення до мережі організації

Наступна частина організації віддаленої роботи - це перевірка підключення до віддаленого робочого столу, так як це допоможе працівникам продовжити роботу з своїх робочих станцій або створити новий віртуальний робочий стіл на сервері для початку роботи.

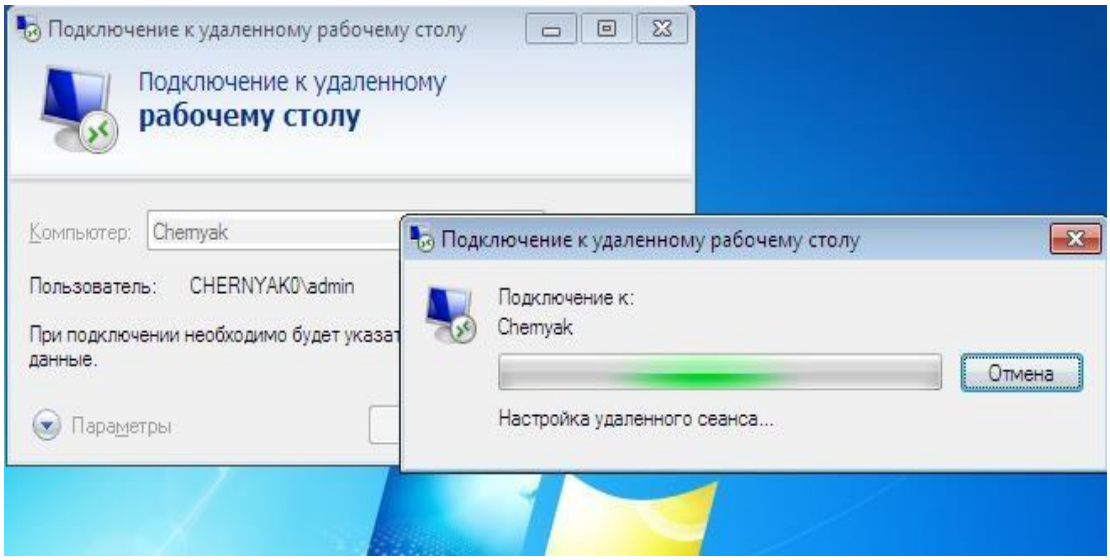


Рис. 3.97. Підключення до сервера з робочої станції

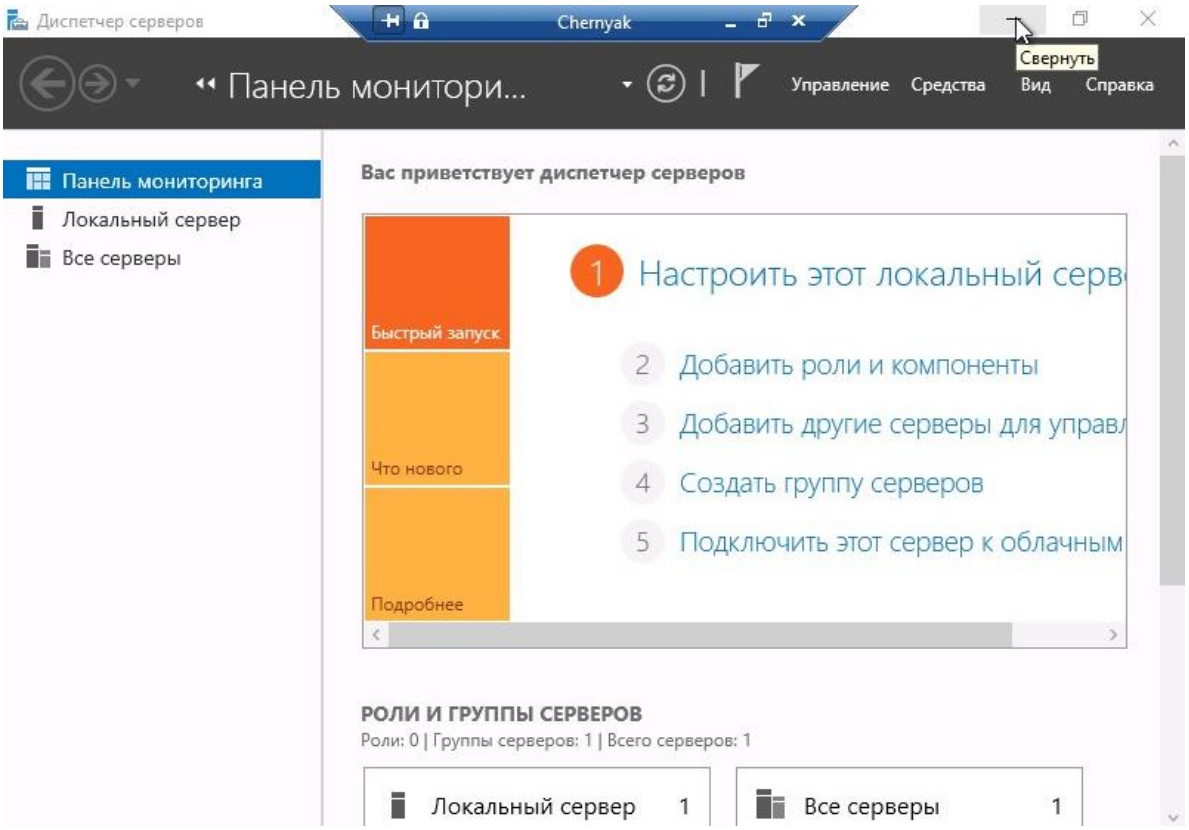


Рис. 3.98. Результат підключення (успішно)

Іншою стороною роботи з віддаленими робочими столами є спрощення віддаленого адміністрування за допомогою підключення з сервера до потрібних робочих станцій.

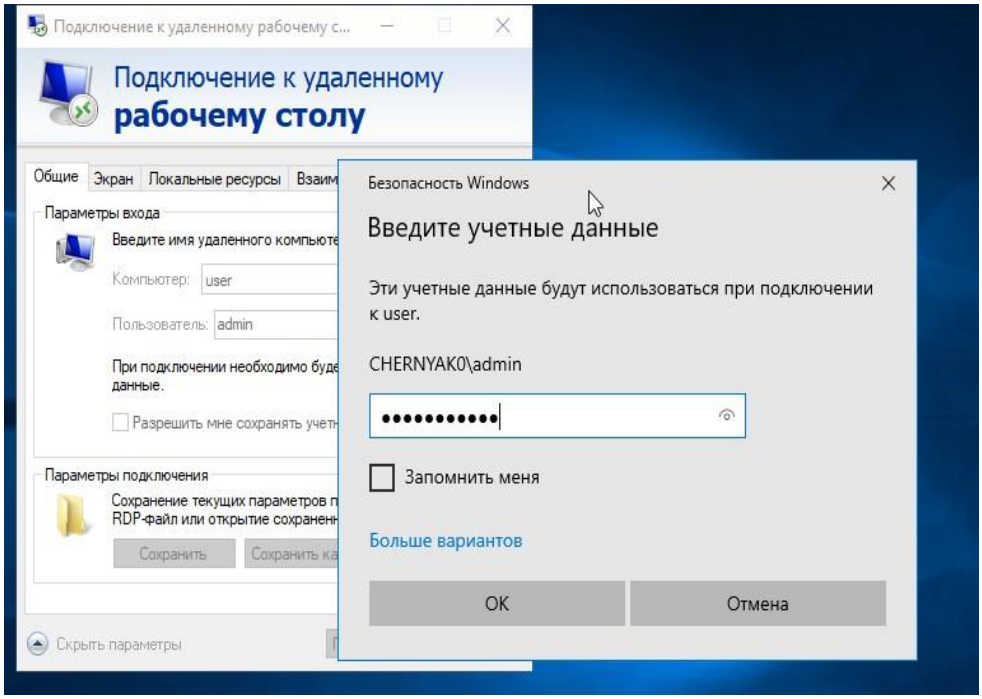


Рис. 3.99. Підключення до робочої станції з сервера



Рис. 3.100. Результат підключення (успішно)

3.4. Аналіз результатів тестування

Нажаль не всі заплановані методи резервування каналів зв’язку були реалізовані в даній мережі через особливості віртуалізованого обладнання, а саме резервування за допомогою Cisco ASA firewall в режимі active/ active failover було замінене більш простим типом, який не балансує навантаження та має велику вартість, напевно це є великим недоліком в резервування каналів, але при необхідності, все ж про такий спосіб резервування також не потрібно забувати. Найпростіше і найдешевше для організації - це використання агрегованих каналів для резервування внутрішніх каналів зв’язку в межах організації.

Для резервування каналів, які дають доступ до мережі Інтернет можна також використовувати і інші типи резервування, наприклад, використання протоколів динамічної маршрутизації, які можуть автоматично знаходить новий шлях на основі інформації про стан каналу, але в такому випадку вам потрібно або розміщувати своє обладнання в провайдера інтернет сервісів або використовувати той самий протокол маршрутизації, що може бути незручним для адміністрування вашої мережі. Через це, на мою думку, використання IP SLA монітору для перевірки доступності пристрою через порт, який ми обрали та створення треку в статичному маршруті, є більш простим та стабільним для мережі невеликої організації, хоча і не таким поширеним, як інші варіанти, які використовують протоколи динамічної маршрутизації, наприклад BGP.

Також велику увагу треба звернути на час відновлення зв’язку між пристроями в реальній мережі, цей час може трішки змінитися в ту чи іншу сторону, але це не буде суттєвим недоліком, і слід додати, що дана мережа і захищена від обривів, вона, нажаль, не є ідеальною з точки зору дизайну мереж вцілому, та повинна мати трішки іншу конфігурацію внутрішнього мережного пристрою з більш тонкими налаштуваннями політик доступу та чітким розмежуванням рівнів мережі.

ВИСНОВКИ

В даній кваліфікаційній роботі було проаналізовані основні засоби резервування каналів звязку та описані ті, які використовуються в даному проекті. Була розроблена топологія мережі, обране обладнання, яке має можливість підтримувати усі необхідні для проекту технології та протоколи.

Також була розглянута тема балансування навантаження трафіку в мережах організацій як побічна частина резервування каналів. Розглянуто реалізацію резервування доступу до мережі Інтернет за допомогою протоколів IP SLA та EEM. Це допомогло уникнути використання протоколів динамічної маршрутизації, які могли б ускладнити адміністрування даної топології. Були проаналізовані протоколи резервування каналів зв’язку та обрані найбільш придатні до використання в даній мережі.

Крім того було проаналізовано та обрано технічні та програмні засоби для реалізації фізичної топології даної організації. Проаналізовано вибір апаратного забезпечення для локальних та глобальної мережі.

Також важливу роль в данній роботі була приділена використанню графічного інтерфейсу для управління мережевих екранів ASDM. Показані його функціональні можливості в налаштуванні, адмініструванні та моніторингу ресурсів мережі. Мережа була побудована з можливістю розширення топології за рахунок додаткових офісів та філій, тим самим підготовлена для розширення мережі організації в майбутньому.

В мережі також налаштований VPN Cisco AnyConnect який допомагає організувати віддалену роботу підключившись до мережі основного офісу і отримавши доступ для віддаленого підключення тим самим офіс може функціонувати в період карантину.

В якості модернізації даного проекту можна використовувати також способи резервування каналів за допомогою бездротового зв'язку. Нажаль ці способи недоступні для їх реалізації в рамках графічних емуляторів. Дане рішення може стати одною з найважливіших модернізацій в сфері резервування даного проекту. Якщо враховувати випадки, коли наша філія або офіс може

знаходитись на дуже великій відстані, на яку не доцільно проводити додаткові фізичні лінії, то слід розглядати варіанти резервування за допомогою супутникового зв'язку або з використанням високошвидкісних стільникових каналів. Також одним з варіантів є модернізація за допомогою радіоканалів. Всі вищеперераховані методи можуть позитивно відобразитисьна працездатності мережі організації за рахунок збільшення кількості резервних каналів, що виведе відмовостійкість на новий рівень.

Реалізована мережа є повністю готовим макетом реальної реалізації проекту мережі організації з резервуванням каналів зв’язку. Конфігурації наведені в додатках можуть бути застосовані для налаштування реального обладнання мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Купер Дж. Архитектура корпоративных сетей. / Джон Купер. – Москва: NETSKILLS.RU, 2014. – 125 с. – (NETSKILLS.RU).
2. EVE-NG documentation [Електронний ресурс] – Режим доступу до ресурсу: https://www.eve-ng.net/index.php/documentation/
3. IP SLAs Configuration Guide. How to use Cisco IOS IP Service Level Agreements [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/xe-16/sla-xe-16-book.html
4. DUAL WAN ON CISCO ASA [Електронний ресурс] – Режим доступу до ресурсу: https://deltaconfig.com/dual-wan-on-cisco-asa/
5. IP SLA + Embedded Event Manager [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/72447/
6. IEEE Standards [Електронний ресурс] – Режим доступу до ресурсу: https://standards.ieee.org
7. Варианты использования Cisco EEM [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/91879/
8. Configure the ASA for Redundant or Backup ISP Links [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118962-configure-asa-00.html
9. Агрегирование каналов Cisco [Електронний ресурс] – Режим доступу до ресурсу: https://bogachev.biz/2015/06/28/agregirovanie-kanalov-cisco/#:~:text=Агрегирование%20каналов%20Cisco,пропускную%20способность%20и%20надежность%20канала.
10. Компьютерные сети /Таненбаум Э. С., Уэзеролл Д. – Санкт-Петербург: Питер, 2014. – 960 с. – (Питер).

11. Построение удаленного доступа к корпоративной сети на базе Cisco Systems [Електронний ресурс] – Режим доступу до ресурсу: http://www.cisco-lan.ru/corporate_multi_service_networks/remote_access_to_corporate_networks.php
12. Active Directory Domain Services [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
13. Иван Л. Концепция паралельного и кольцевого резервирования / Лопухов Иван. // Современные технологии автоматизации. – 2012. – №1. – С. 18–25.
14. ASA Security Device Manager (ASDM) [Електронний ресурс] – Режим доступу до ресурсу: https://geek-university.com/ccna-security/asa-security-device-manager-asdm-installation/
15. Cisco ASA 5500 Series Adaptive Security Appliances Data Sheet [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/data_sheet_c78-345385.html
16. Cisco Catalyst 3560 Series Switches [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/switches/catalyst-3560-series-switches/index.html
17. Cisco 7200 Series Routers [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/routers/7200-series-routers/index.html
18. Cisco Catalyst 2960-X Series Switches [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/switches/catalyst-2960-x-series-switches/series.html
19. Налагодження та дослідження роботи протоколу динамічного резервування шлюзу та балансування навантаження glbp у мережі на базі обладнання cisco [Електронний ресурс] – Режим доступу до ресурсу:

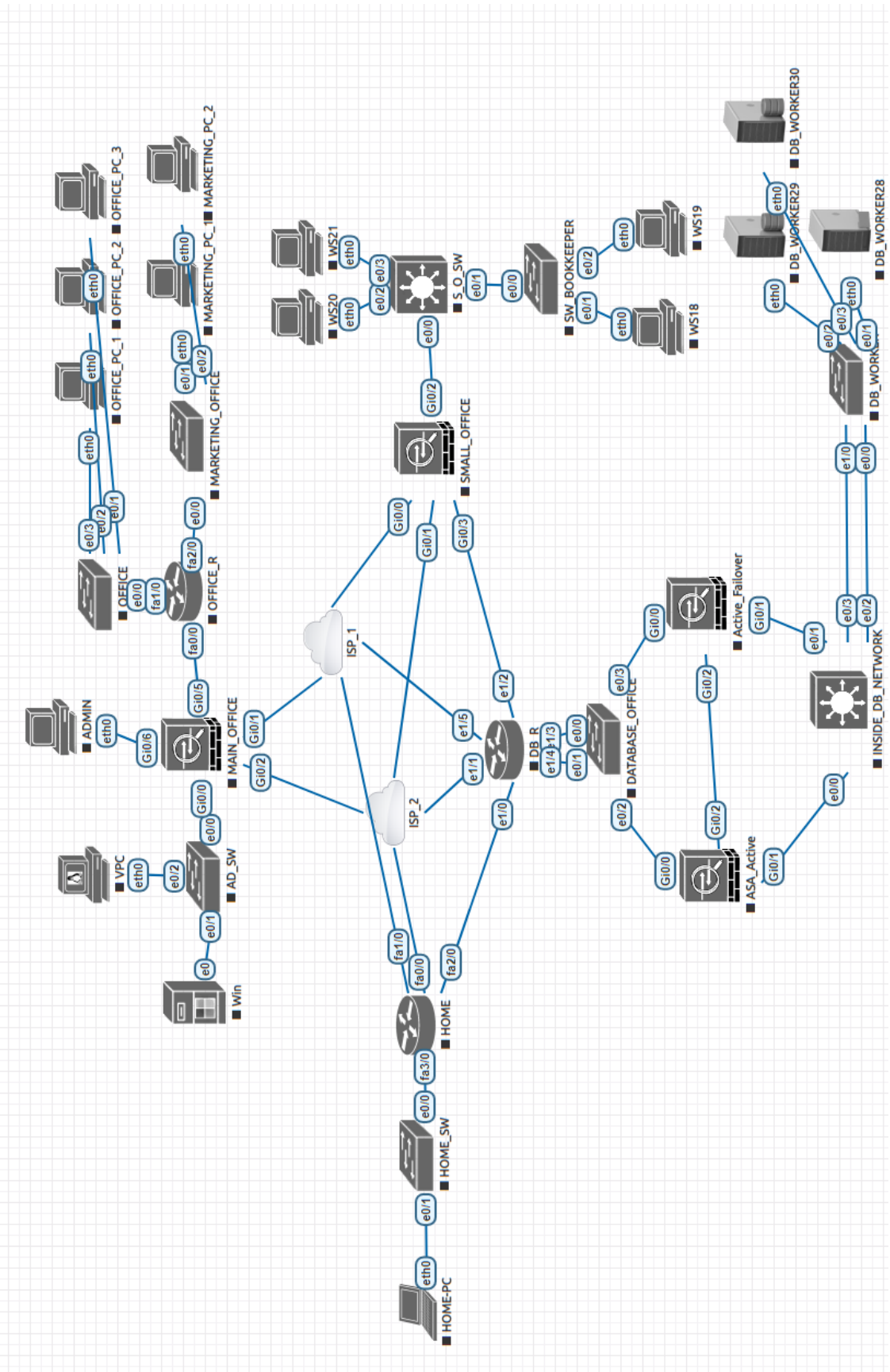
https://learn.ztu.edu.ua/pluginfile.php/60583/mod_resource/content/1/KM_KIKB_LR-31-2019-2020_KI-3_KB-2-1_KB-2-2_KBK-19-1.pdf

20. Failover режим на Cisco ASA [Електронний ресурс] – Режим доступу до ресурсу: http://ithelp21.ru/nastroyka-failover-rezhima-na-cisco-asa/
21. Курс Cisco DESGN 3.0 [Електронний ресурс] – Режим доступу до ресурсу: https://www.atraining.ru/cisco-desgn/
22. CISCO FIREWALLS [Електронний ресурс] – Режим доступу до ресурсу: http://www.firewall.cx/cisco-technical-knowledgebase/cisco-firewalls.html
23. INTERNATIONAL STANDARD [Електронний ресурс] – Режим доступу до ресурсу: https://webstore.iec.ch
24. Cisco ASA Anyconnect Remote Access VPN [Електронний ресурс] – Режим доступу до ресурсу: https://networklessons.com/cisco/asa-firewall/cisco-asa-anyconnect-remote-access-vpn

ДОДАТКИ

Додаток А

Топологія мережі проекту



Додаток Б

Лістинги конфігураційних файлів пристроїв мережі

Комутатор AD_SW

```
Building configuration...
Current configuration : 995 bytes
! Last configuration change at 12:07:32 EET Mon Jun 15 2020
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname AD_server_SW
boot-start-marker
boot-end-marker
username admin privilege 15 password 0 admin
no aaa new-model
clock timezone EET 2 0
ip domain-name diploma
ip cef
no ipv6 cef
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
interface Ethernet0/0
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Vlan1
 ip address 48.214.24.2 255.255.255.0
ip forward-protocol nd
!
no ip http server
no ip http secure-server
control-plane
!
banner motd ^CDC to win AD server and Main_offcie cisco asa^C
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login local
 transport input ssh
 transport output ssh
!
End
```

Міжмережевий екран Main_office

```
: Saved
: Serial Number: 9ALK23L1P9R
: Hardware:   ASAv, 2048 MB RAM, CPU Pentium II 3608 MHz
:
ASA Version 9.8(1)
!
hostname ASA-MAIN-OFFICE
domain-name diploma
enable password $sha512$5000$NEHoK705ki/9p4JnWmfeqA==$DLNfjJfTxjBviY2c4j4L5g== pbkdf2
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names

!
interface GigabitEthernet0/0
 nameif WinAD
 security-level 20
 ip address 48.214.24.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0

 ip address 10.0.0.1 255.255.255.0
!
interface GigabitEthernet0/2
```

```
 nameif backup
 security-level 0
 ip address 20.0.0.1 255.255.255.0
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 nameif office
 security-level 100
 ip address 192.2.24.1 255.255.255.252
!
interface GigabitEthernet0/6
 nameif admin
 security-level 50
 ip address 214.2.24.1 255.255.255.252
!
interface Management0/0
 nameif config
 security-level 0
 ip address dhcp
!
banner motd "Main office border device (ASA) DC to AD_SW Gi0/0 |

ADMIN Gi0/6 | OFFICE_R Gi0/5 | Gi0/1 to ISP1 | Gi0/2 to ISP2"
ftp mode passive
clock timezone EEST 2
clock summer-time EEDT recurring last Sun Mar 3:00 last Sun Oct 4:00
dns server-group DefaultDNS
 domain-name diploma
same-security-traffic permit inter-interface
object network 10.0.0.3
 host 10.0.0.3
 description 10.0.0.3
object-group network DM_INLINE_NETWORK_1
 network-object 192.168.3.0 255.255.255.0
 network-object 192.168.4.0 255.255.255.0
 network-object host 10.0.0.2
 network-object host 20.0.0.2
object-group network DM_INLINE_NETWORK_2
 network-object host 10.0.0.2
 network-object 192.168.3.0 255.255.255.0
 network-object 192.168.4.0 255.255.255.0
 network-object host 20.0.0.2
access-list outside_access_in extended permit ip object-group DM_INLINE_NETWORK_1 any4
access-list backup_access_in extended permit ip object-group DM_INLINE_NETWORK_2 any
pager lines 23
logging enable
logging asdm informational
mtu WinAD 1500
mtu outside 1500
mtu backup 1500
mtu office 1500
mtu admin 1500
mtu config 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
nat (any,outside) source dynamic any interface
access-group outside_access_in in interface outside
access-group backup_access_in in interface backup
router ospf 24
 network 10.0.0.0 255.255.255.0 area 0
 network 20.0.0.0 255.255.255.0 area 0
 network 48.214.24.0 255.255.255.0 area 0
 network 192.2.24.0 255.255.255.252 area 0
 network 214.2.24.0 255.255.255.252 area 0
 area 0
```

log-adj-changes
redistribute static
!
route outside 0.0.0.0 0.0.0.0 10.0.0.2 253 track 1
route backup 0.0.0.0 0.0.0.0 20.0.0.2 254
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication login-history
http server enable
http 192.168.0.0 255.255.255.0 config
no snmp-server location
no snmp-server contact
sla monitor 123
type echo protocol ipIcmpEcho 10.0.0.2 interface outside
num-packets 3
frequency 10
sla monitor schedule 123 life forever start-time now
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set main esp-aes-256 esp-sha-hmac

```
 crypto ipsec ikev2 ipsec-proposal AES256
  protocol esp encryption aes-256
  protocol esp integrity sha-1 md5
 crypto ipsec ikev2 ipsec-proposal AES192
  protocol esp encryption aes-192
  protocol esp integrity sha-1 md5
 crypto ipsec ikev2 ipsec-proposal AES
  protocol esp encryption aes
  protocol esp integrity sha-1 md5
 crypto ipsec ikev2 ipsec-proposal 3DES
  protocol esp encryption 3des
  protocol esp integrity sha-1 md5
 crypto ipsec ikev2 ipsec-proposal DES
  protocol esp encryption des
  protocol esp integrity sha-1 md5
 crypto ipsec security-association pmtu-aging infinite
 crypto ca trustpoint _SmartCallHome_ServerCA
  no validation-usage
  crl configure
 crypto ca trustpool policy
  auto-import
 crypto ca certificate chain _SmartCallHome_ServerCA
  certificate ca 18dad19e267de8bb4a2158cdcc6b3b4a
   308204d3 308203bb a0030201 02021018 dad19e26 7de8bb4a 2158cdcc 6b3b4a30
   0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117
   30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b
   13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038 06035504
   0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d 20466f72
   20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504 03133c56
   65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043
   65727469 66696361 74696f6e 20417574 686f7269 7479202d 20473530 1e170d30
   36313130 38303030 3030305a 170d3336 30373136 32333539 35395a30 81ca310b
   30090603 55040613 02555331 17301506 0355040a 130e5665 72695369 676e2c20
   496e632e 311f301d 06035504 0b131656 65726953 69676e20 54727573 74204e65
   74776f72 6b313a30 38060355 040b1331 28632920 32303036 20566572 69536967
   6e2c2049 6e632e20 2d20466f 72206175 74686f72 697a6564 20757365 206f6e6c
   79314530 43060355 0403133c 56657269 5369676e 20436c61 73732033 20507562
   6c696320 5072696d 61727920 43657274 69666963 6174696f 6e204175 74686f72
   69747920 2d204735 30820122 300d0609 2a864886 f70d0101 01050003 82010f00
   3082010a 02820101 00af2408 08297a35 9e600caa e74b3b4e dc7cbc3c 451cbb2b
   e0fe2902 f95708a3 64851527 f5f1adc8 31895d22 e82aaaa6 42b38ff8 b955b7b1
   b74bb3fe 8f7e0757 ecef43db 66621561 cf600da4 d8def8e0 c362083d 5413eb49
   ca595485 26e52b8f 1b9febf5 a191c233 49d84363 6a524bd2 8fe87051 4dd18969
   7bc770f6 b3dc1274 db7b5d4b 56d396bf 1577a1b0 f4a225f2 af1c9267 18e5f406
   04ef90b9 e400e4dd 3ab519ff 02baf43c eee08beb 378becf4 d7acf2f6 f03dafdd
   75913319 1d1c40cb 74241921 93d914fe ac2a52c7 8fd50449 e48d6347 883c6983
   cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0 6773e314 087ee53f 9f73b833 0acf5d3f
   3487968a ee53e825 15020301 0001a381 b23081af 300f0603 551d1301 01ff0405
   30030101 ff300e06 03551d0f 0101ff04 04030201 06306d06 082b0601 05050701
   0c046130 5fa15da0 5b305930 57305516 09696d61 67652f67 69663021 301f3007
```

06052b0e 03021a04 148fe5d3 1a86ac8d 8e6bc3cf 806ad448 182c7b19 2e302516
23687474 703a2f2f 6c6f676f 2e766572 69736967 6e2e636f 6d2f7673 6c6f676f 2e676966 301d0603 551d0e04 1604147f d365a7c2 ddecbbf0 3009f343 39fa02af
33313330 0d06092a 864886f7 0d010105 05000382 01010093 244a305f 62cfd81a
982f3dea dc992dbd 77f6a579 2238ecc4 a7a07812 ad620e45 7064c5e7 97662d98
097e5faf d6cc2865 f201aa08 1a47def9 f97c925a 0869200d d93e6d6e 3c0d6ed8
e6069140 18b9f8c1 eddfdb41 aae09620 c9cd6415 3881c994 eea28429 0b136f8e
db0cdd25 02dba48b 1944d241 7a05694a 584f60ca 7e826a0b 02aa2517 39b5db7f
e784652a 958abd86 de5e8116 832d10cc defda882 2a6d281f 0d0bc4e5 e71a2619
e1f4116f 10b595fc e7420532 dbce9d51 5e28b69e 85d35bef a57d4540 728eb70e
6b0e06fb 33354871 b89d278b c4655f0d 86769c44 7af6955c f65d3208 33a454b6
183f685c f2424a85 3854835f d1e82cf2 ac11d6a8 ed636a
quit
crypto ikev2 policy 1
encryption aes-256
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 10
encryption aes-192
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 20
encryption aes
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 30
encryption 3des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 40
encryption des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev1 policy 1
authentication pre-share
encryption aes-256
hash sha
group 5
lifetime 3600
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
crypto ikev1 policy 20
authentication rsa-sig
encryption aes-256
hash sha
group 2
lifetime 86400
crypto ikev1 policy 40
authentication pre-share
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 50
authentication rsa-sig
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 70
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
crypto ikev1 policy 80
authentication rsa-sig
encryption aes
hash sha
group 2
lifetime 86400
crypto ikev1 policy 100

```
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
!
track 1 rtr 123 reachability
telnet timeout 5
ssh stricthostkeycheck
ssh 214.2.24.0 255.255.255.0 admin
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record
DfltAccessPolicy
username admin password
$sha512$5000$4YCJWCIz/fwEhj8FQpbotA=
=$r7G5TAeL7vATeSpGobj09A== pbkdf2
privilege 15
username user password
$sha512$5000$W3i1BMQJX2ix+ejtcYNrCg
==$eUhl1G775VTENUmkeOQsBw==
pbkdf2 privilege 4
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns
preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
  inspect http
policy-map type inspect dns
migrated_dns_map_2
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect dns
migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/servi
ces/DDCEService
  destination address email
callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
```

```
      subscribe-to-alert-group inventory
periodic monthly
      subscribe-to-alert-group configuration
periodic monthly
      subscribe-to-alert-group telemetry
periodic daily
     profile License
      destination address http
https://tools.cisco.com/its/service/oddce/servi
ces/DDCEService
      destination transport-method http
    event manager applet 10.10.10.1
     output none
    Cryptochecksum:6a46ae284e27b0829962
36ba4a10ef2a
    : end
    Маршрутизатор OFFICE_R
    Building configuration...

    Current configuration : 1885 bytes
    !
    upgrade fpd auto
    version 12.4
    service timestamps debug datetime msec
    service timestamps log datetime msec
    no service password-encryption
    !
    hostname OFFICE_ROUTER
    !
    boot-start-marker
    boot-end-marker
    !
    logging message-counter syslog
    enable password admin
    !
    no aaa new-model
    ip source-route
    ip cef
    !
    ip dhcp excluded-address 192.168.0.1
    ip dhcp excluded-address 192.168.1.1
    ip dhcp excluded-address 192.168.0.2
    ip dhcp excluded-address 192.168.1.2
    !
    ip dhcp pool Office
      network 192.168.0.0 255.255.255.0
      default-router 192.168.0.1
    !
    ip dhcp pool marketing_office
      network 192.168.1.0 255.255.255.0
    !
    ip domain name diploma
    no ipv6 cef
    !
    multilink bundle-name authenticated
    !
    username admin privilege 15 password 0
admin
    archive
     log config
      hidekeys
    !
    ip ssh version 2
    !
    interface FastEthernet0/0
     ip address 192.2.24.2 255.255.255.252
     duplex half
    !
    interface FastEthernet1/0
     ip address 192.168.0.1 255.255.255.0
     duplex half
    !
    interface FastEthernet2/0
     ip address 192.168.1.1 255.255.255.0
     duplex half
    !
    interface FastEthernet3/0
     no ip address
     shutdown
     duplex half
    !
    interface FastEthernet4/0
     no ip address
     shutdown
     duplex half
    !
    interface FastEthernet5/0
     no ip address
     shutdown
     duplex half
    !
    interface FastEthernet6/0
     no ip address
     shutdown
     duplex half
    !
    router ospf 24
     log-adjacency-changes
     network 192.2.24.0 0.0.0.3 area 0
     network 192.168.0.0 0.0.0.255 area 0
     network 192.168.1.0 0.0.0.255 area 0
    !
```

```
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
!
gatekeeper
 shutdown
!
banner motd ^CRouter for offices | fa0/0 DC to MAIN_OFFICE | fa1/0 DC to OFFICE switch | fa2/0 DC to MARKETING_OFFICE | DHCP ON Ff1/0 and fa2/0^C
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login local
 transport input ssh
 transport output ssh
!
End
```

Комутатор OFFICE

```
Current configuration : 997 bytes
!
! Last configuration change at 12:27:26 EET Mon Jun 15 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname OFFICE_SW
!
boot-start-marker
boot-end-marker
!
enable password admin
!
username admin privilege 15 password 0 admin
no aaa new-model
clock timezone EET 2 0
!
ip domain-name diploma
ip cef
no ipv6 cef
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
!
interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Vlan1
 ip address 192.168.0.2 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CFIRST OFFICE DC to OFFICE_R ^C
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login local
 transport input ssh
 transport output ssh
!
End
```

КомутаторMARKETING_OFFICE

```
Current configuration : 1007 bytes
!
! Last configuration change at 12:29:40 EET Mon Jun 15 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Marketing_office
```

```
!
boot-start-marker
boot-end-marker
!
enable password admin
!
username admin privilege 15 password 0 admin
no aaa new-model
clock timezone EET 2 0
!
ip domain-name diploma
ip cef
no ipv6 cef
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
!
interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CMarketing office DC to Office_r^C
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login local
 transport input ssh
 transport output ssh
!
End
Міжмережевий екран SMALL_OFFICE
: Saved

:
: Serial Number: 9AJXK2G3FDD
: Hardware:   ASAv, 2048 MB RAM, CPU Pentium II 3608 MHz
:
ASA Version 9.8(1)
!
hostname SMALL-OFFICE
enable password $sha512$5000$AFHGiTDkXcTqaCq7NiWC6w==$BJJQ4TeCRlCMGXHRMkXCLg== pbkdf2
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
!
license smart
 feature tier standard
 throughput level 2G
names

!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.0.0.2 255.255.255.0
!
interface GigabitEthernet0/1
 nameif backup
 security-level 0
 ip address 20.0.0.2 255.255.255.0
!
interface GigabitEthernet0/2
 nameif inside
 security-level 100
 ip address 192.168.4.1 255.255.255.0
!
interface GigabitEthernet0/3
```

```
 nameif 3office
 security-level 100
 ip address 192.2.24.6 255.255.255.252
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif config
 security-level 0
 ip address 192.168.0.120 255.255.255.0
!
banner motd "Second office| DC Gi0/0 ISP1 | Gi0/1 ISP2 | Gi0/3 DB_R | Gi0/2 S_O_SW"
ftp mode passive
same-security-traffic permit inter-interface
object-group network DM_INLINE_NETWORK_3
 network-object 192.168.0.0 255.255.255.0
 network-object 192.168.1.0 255.255.255.0
 network-object 192.2.24.0 255.255.255.252
 network-object 214.2.24.0 255.255.255.252
 network-object 48.214.24.0 255.255.255.252
 network-object host 10.0.0.1
 network-object host 20.0.0.1
access-list outside_access_in extended permit ip object-group DM_INLINE_NETWORK_3 any4
pager lines 23
logging enable
logging asdm informational
mtu outside 1500
mtu backup 1500
mtu inside 1500
mtu 3office 1500
mtu config 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
access-group outside_access_in in interface outside
router ospf 24
 network 10.0.0.0 255.255.255.0 area 0
 network 20.0.0.0 255.255.255.0 area 0
 network 192.168.4.0 255.255.255.0 area 0
 area 0
 log-adj-changes
 !
route outside 0.0.0.0 0.0.0.0 10.0.0.1 253 track 1
route backup 0.0.0.0 0.0.0.0 20.0.0.1 254
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication login-history
http server enable
http 0.0.0.0 0.0.0.0 config
http 192.168.0.0 255.255.255.0 config
no snmp-server location
no snmp-server contact
sla monitor 123
 type echo protocol ipIcmpEcho 10.0.0.1 interface outside
 num-packets 3
 frequency 10
```

sla monitor schedule 123 life forever start-time now
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set main esp-aes-256 esp-sha-hmac
crypto ipsec ikev2 ipsec-proposal DES
protocol esp encryption des
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
protocol esp encryption 3des
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
protocol esp encryption aes
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
protocol esp encryption aes-192
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca trustpool policy
auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
certificate ca 18dad19e267de8bb4a2158cdcc6b3b4a
308204d3 308203bb a0030201 02021018 dad19e26 7de8bb4a 2158cdcc 6b3b4a30
0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117

30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b

13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038 06035504

0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d 20466f72

20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504 03133c56

65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043

65727469 66696361 74696f6e 20417574 686f7269 7479202d 20473530 1e170d30

36313130 38303030 3030305a 170d3336 30373136 32333539 35395a30 81ca310b

30090603 55040613 02555331 17301506 0355040a 130e5665 72695369 676e2c20

496e632e 311f301d 06035504 0b131656 65726953 69676e20 54727573 74204e65

74776f72 6b313a30 38060355 040b1331 28632920 32303036 20566572 69536967

6e2c2049 6e632e20 2d20466f 72206175 74686f72 697a6564 20757365 206f6e6c

79314530 43060355 0403133c 56657269 5369676e 20436c61 73732033 20507562

6c696320 5072696d 61727920 43657274 69666963 6174696f 6e204175 74686f72

69747920 2d204735 30820122 300d0609 2a864886 f70d0101 01050003 82010f00

3082010a 02820101 00af2408 08297a35 9e600caa e74b3b4e dc7cbc3c 451cbb2b

e0fe2902 f95708a3 64851527 f5f1adc8 31895d22 e82aaaa6 42b38ff8 b955b7b1

b74bb3fe 8f7e0757 ecef43db 66621561 cf600da4 d8def8e0 c362083d 5413eb49

ca595485 26e52b8f 1b9febf5 a191c233 49d84363 6a524bd2 8fe87051 4dd18969

7bc770f6 b3dc1274 db7b5d4b 56d396bf 1577a1b0 f4a225f2 af1c9267 18e5f406

04ef90b9 e400e4dd 3ab519ff 02baf43c eee08beb 378becf4 d7acf2f6 f03dafdd

75913319 1d1c40cb 74241921 93d914fe ac2a52c7 8fd50449 e48d6347 883c6983

cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0 6773e314 087ee53f 9f73b833 0acf5d3f

3487968a ee53e825 15020301 0001a381 b23081af 300f0603 551d1301 01ff0405

30030101 ff300e06 03551d0f 0101ff04 04030201 06306d06 082b0601 05050701

0c046130 5fa15da0 5b305930 57305516 09696d61 67652f67 69663021 301f3007

06052b0e 03021a04 148fe5d3 1a86ac8d 8e6bc3cf 806ad448 182c7b19 2e302516

23687474 703a2f2f 6c6f676f 2e766572 69736967 6e2e636f 6d2f7673 6c6f676f

2e676966 301d0603 551d0e04 1604147f d365a7c2 ddecbbf0 3009f343 39fa02af

33313330 0d06092a 864886f7 0d010105 05000382 01010093 244a305f 62cfd81a

982f3dea dc992dbd 77f6a579 2238ecc4 a7a07812 ad620e45 7064c5e7 97662d98

097e5faf d6cc2865 f201aa08 1a47def9 f97c925a 0869200d d93e6d6e 3c0d6ed8

e6069140 18b9f8c1 eddfdb41 aae09620 c9cd6415 3881c994 eea28429 0b136f8e

db0cdd25 02dba48b 1944d241 7a05694a 584f60ca 7e826a0b 02aa2517 39b5db7f

e784652a 958abd86 de5e8116 832d10cc defda882 2a6d281f 0d0bc4e5 e71a2619

e1f4116f 10b595fc e7420532 dbce9d51 5e28b69e 85d35bef a57d4540 728eb70e

6b0e06fb 33354871 b89d278b c4655f0d 86769c44 7af6955c f65d3208 33a454b6

183f685c f2424a85 3854835f d1e82cf2 ac11d6a8 ed636a

quit

crypto ikev2 policy 1

encryption aes-256

integrity sha

group 5 2

prf sha

```
 lifetime seconds 86400
crypto ikev1 policy 1
 authentication pre-share
 encryption aes-256
 hash sha
 group 5
 lifetime 3600
!
track 1 rtr 123 reachability
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
management-access config
dhcpd address 192.168.4.3-192.168.4.254
inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record
DfltAccessPolicy
username admin password
$sha512$5000$myrt00Bn7nbQu+BPuLd1jg=
=$n3XHaRl1Ty5RjYd8FuW4sg== pbkdf2
privilege 15
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns
preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
policy-map type inspect dns
migrated_dns_map_2
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect dns
migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/servi
ces/DDCEService
  destination address email
callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory
periodic monthly
  subscribe-to-alert-group configuration
periodic monthly
  subscribe-to-alert-group telemetry
periodic daily
 profile License
  destination address http
https://tools.cisco.com/its/service/oddce/servi
ces/DDCEService
  destination transport-method http
Cryptochecksum:f473b160e024c288ba45
e8d0b780c84d
: end
Багаторівневий комутатор S_O_SW
Building configuration...

Current configuration : 1479 bytes
```

```
!
! Last configuration change at 12:01:30 EET Mon Jun 15 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Secon_office_SW
!
boot-start-marker
boot-end-marker
!
enable password admin
!
no aaa new-model
clock timezone EET 2 0
!
ip dhcp excluded-address 192.168.3.1
ip dhcp excluded-address 192.168.3.2
!
ip dhcp pool Bookkepper_oddice_pool_DHCP
 network 192.168.3.0 255.255.255.0
 default-router 192.168.3.1
!
ip cef
no ipv6 cef
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface Ethernet0/0
 switchport mode access
!
interface Ethernet0/1
 no switchport
 ip address 192.168.3.1 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 switchport mode access
!
interface Ethernet0/3
 switchport mode access
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Vlan1
 ip address 192.168.4.2 255.255.255.0
!
router ospf 24
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
banner motd ^CS_O_SW | DC to SMALL_OFFICE ASA e0/0 | DC e0/1 to BOOKKEEPER OFFICE| other interfacess devops office with main vlan ad switch dhcp^C
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
End

SW_BOOKKEEPER
Current configuration : 958 bytes
!
! Last configuration change at 12:35:34 EET Mon Jun 15 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW_BOOKKEEPER
!
boot-start-marker
boot-end-marker
!
```

```
enable password admin
!
username admin privilege 15 password 0 admin
no aaa new-model
clock timezone EET 2 0
!
ip domain-name diploma
ip cef
no ipv6 cef
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
!
interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Vlan1
 ip address 192.168.3.2 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login local
 transport input ssh
 transport output ssh
!
end
```

Маршрутизатор DB_R

```
Building configuration...

Current configuration : 1554 bytes
!
! Last configuration change at 13:40:07 UTC Mon Jun 15 2020
!
upgrade fpd auto
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Database_router
!
boot-start-marker
boot-end-marker
!
enable password admin
!
no aaa new-model
!
ip source-route
ip cef
!
ip domain name diploma
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
username admin privilege 15 password 0 admin
!
redundancy
!
ip ssh version 2
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
 !
interface Ethernet1/0
 description to home
 ip address 195.2.3.1 255.255.255.128
 duplex half
 !
interface Ethernet1/1
 description to_ISP2
 ip address 20.0.0.3 255.255.255.0
 duplex half
 !
```

```
interface Ethernet1/2
 description reserv lick to second office
 ip address 192.2.24.5 255.255.255.252
 duplex half
 !
interface Ethernet1/3
 ip address 10.10.11.1 255.255.255.0
 duplex half
 !
interface Ethernet1/4
 ip address 10.10.10.1 255.255.255.0
 duplex half
 !
interface Ethernet1/5
 no ip address
 shutdown
 duplex half
 !
interface Ethernet1/6
 no ip address
 shutdown
 duplex half
 !
interface Ethernet1/7
 no ip address
 shutdown
 duplex half
 !
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login local
 transport input ssh
 transport output ssh
!
End
```

Комутатор DATABASE_OFFICE

```
Building configuration...

Current configuration : 898 bytes
!
! Last configuration change at 12:42:41 EET Mon Jun 15 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname DB_Office
!
boot-start-marker
boot-end-marker
!
enable password admin
!
username admin privilege 15 password 0 admin
no aaa new-model
clock timezone EET 2 0
!
 --More--
*Jun 15 10:42:41.896: %SYS-5-CONFIG_I: Configured from console by console
!
ip domain-name diploma
ip cef
no ipv6 cef
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
!
interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
```

```
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login local
 transport input ssh
 transport output ssh
!
End

Міжмережевий екран ASA_Active
: Saved

:
: Serial Number: 9ADWG0WSGVQ
: Hardware:   ASAv, 2048 MB RAM, CPU
Pentium II 3608 MHz
:
ASA Version 9.8(1)
!
hostname ASA-Active
enable                          password
$sha512$5000$GLH7dJjX+VFIsO/SBs37OQ
==$tVbXARK2Z21vt2xKSMYMGA==
pbkdf2
names

!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.10.10.2 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.5.1 255.255.255.0
!
interface GigabitEthernet0/2
 description      LAN/STATE      Failover
Interface
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
pager lines 23
mtu outside 1500
mtu inside 1500
failover
failover lan unit primary
failover      lan      interface      STATE
GigabitEthernet0/2
failover polltime unit 1 holdtime 3
failover link STATE GigabitEthernet0/2
failover interface ip STATE 172.2.24.1
255.255.255.252 standby 172.2.24.2
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
router ospf 24
 network 10.10.10.0 255.255.255.0 area 0
 network 192.168.5.0 255.255.255.0 area 0
 log-adj-changes
!
```

timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication login-history
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca trustpool policy
auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
certificate ca 18dad19e267de8bb4a2158cdcc6b3b4a
308204d3 308203bb a0030201 02021018 dad19e26 7de8bb4a 2158cdcc 6b3b4a30
0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117
30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d 20466f72
20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504 03133c56
65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043
65727469 66696361 74696f6e 20417574 686f7269 7479202d 20473530 1e170d30
36313130 38303030 3030305a 170d3336 30373136 32333539 35395a30 81ca310b
30090603 55040613 02555331 17301506 0355040a 130e5665 72695369 676e2c20
496e632e 311f301d 06035504 0b131656 65726953 69676e20 54727573 74204e65
74776f72 6b313a30 38060355 040b1331 28632920 32303036 20566572 69536967
6e2c2049 6e632e20 2d20466f 72206175 74686f72 697a6564 20757365 206f6e6c
79314530 43060355 0403133c 56657269 5369676e 20436c61 73732033 20507562
6c696320 5072696d 61727920 43657274 69666963 6174696f 6e204175 74686f72
69747920 2d204735 30820122 300d0609 2a864886 f70d0101 01050003 82010f00
3082010a 02820101 00af2408 08297a35 9e600caa e74b3b4e dc7cbc3c 451cbb2b
e0fe2902 f95708a3 64851527 f5f1adc8 31895d22 e82aaaa6 42b38ff8 b955b7b1
b74bb3fe 8f7e0757 ecef43db 66621561 cf600da4 d8def8e0 c362083d 5413eb49
ca595485 26e52b8f 1b9febf5 a191c233 49d84363 6a524bd2 8fe87051 4dd18969
7bc770f6 b3dc1274 db7b5d4b 56d396bf 1577a1b0 f4a225f2 af1c9267 18e5f406
04ef90b9 e400e4dd 3ab519ff 02baf43c eee08beb 378becf4 d7acf2f6 f03dafdd
75913319 1d1c40cb 74241921 93d914fe ac2a52c7 8fd50449 e48d6347 883c6983
cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0 6773e314 087ee53f 9f73b833 0acf5d3f
3487968a ee53e825 15020301 0001a381 b23081af 300f0603 551d1301 01ff0405
30030101 ff300e06 03551d0f 0101ff04 04030201 06306d06 082b0601 05050701

```
        0c046130 5fa15da0 5b305930
57305516 09696d61 67652f67 69663021
301f3007
        06052b0e 03021a04 148fe5d3 1a86ac8d
8e6bc3cf 806ad448 182c7b19 2e302516
        23687474 703a2f2f 6c6f676f 2e766572
69736967 6e2e636f 6d2f7673 6c6f676f
        2e676966 301d0603 551d0e04
1604147f d365a7c2 ddecbbf0 3009f343
39fa02af
        33313330 0d06092a 864886f7
0d010105 05000382 01010093 244a305f
62cfd81a
        982f3dea dc992dbd 77f6a579 2238ecc4
a7a07812 ad620e45 7064c5e7 97662d98
        097e5faf d6cc2865 f201aa08 1a47def9
f97c925a 0869200d d93e6d6e 3c0d6ed8
        e6069140 18b9f8c1 eddfdb41 aae09620
c9cd6415 3881c994 eea28429 0b136f8e
        db0cdd25 02dba48b 1944d241
7a05694a 584f60ca 7e826a0b 02aa2517
39b5db7f
        e784652a 958abd86 de5e8116
832d10cc defda882 2a6d281f 0d0bc4e5
e71a2619
        e1f4116f 10b595fc e7420532 dbce9d51
5e28b69e 85d35bef a57d4540 728eb70e
        6b0e06fb 33354871 b89d278b c4655f0d
86769c44 7af6955c f65d3208 33a454b6
        183f685c f2424a85 3854835f d1e82cf2
ac11d6a8 ed636a
      quit
    telnet timeout 5
    ssh stricthostkeycheck
    ssh timeout 5
    ssh key-exchange group dh-group1-sha1
    console timeout 0
    dhcpd address 192.168.5.4-192.168.5.254
inside
    dhcpd enable inside
    !
    threat-detection basic-threat
    threat-detection statistics access-list
    no threat-detection statistics tcp-intercept
    dynamic-access-policy-record
DfltAccessPolicy
    !
    class-map inspection_default
     match default-inspection-traffic
    !
    !
    policy-map type inspect dns
preset_dns_map
     parameters
      message-length maximum client auto
      message-length maximum 512
      no tcp-inspection
    policy-map global_policy
     class inspection_default
      inspect dns preset_dns_map
      inspect ftp
      inspect h323 h225
      inspect h323 ras
      inspect rsh
      inspect rtsp
      inspect esmtp
      inspect sqlnet
      inspect skinny
      inspect sunrpc
      inspect xdmcp
      inspect sip
      inspect netbios
      inspect tftp
      inspect ip-options
    !
    service-policy global_policy global
    prompt hostname context
    no call-home reporting anonymous
    call-home
     profile CiscoTAC-1
      no active
      destination address http
https://tools.cisco.com/its/service/oddce/servi
ces/DDCEService
      destination address email
callhome@cisco.com
      destination transport-method http
      subscribe-to-alert-group diagnostic
      subscribe-to-alert-group environment
      subscribe-to-alert-group inventory
periodic monthly
      subscribe-to-alert-group configuration
periodic monthly
      subscribe-to-alert-group telemetry
periodic daily
     profile License
      destination address http
https://tools.cisco.com/its/service/oddce/servi
ces/DDCEService
      destination transport-method http
    Cryptochecksum:27efc71172bd3b31ae38
69d1bc86718d
```

: end

Міжмережевий екран Active_Failover
: Saved

:
: Serial Number: 9A61SS09GMW
: Hardware: ASAv, 2048 MB RAM, CPU Pentium II 3608 MHz
:
ASA Version 9.8(1)
!
hostname ASA-Active
enable password $sha512$5000$GLH7dJjX+VFIsO/SBs37OQ==$tVbXARK2Z21vt2xKSMYMGA== pbkdf2
names

!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.10.10.2 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.5.1 255.255.255.0
!
interface GigabitEthernet0/2
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
pager lines 23
mtu outside 1500
mtu inside 1500
failover
failover lan unit secondary
failover lan interface STATE GigabitEthernet0/2
failover polltime unit 1 holdtime 3
failover link STATE GigabitEthernet0/2
failover interface ip STATE 172.2.24.1 255.255.255.252 standby 172.2.24.2
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
router ospf 24
 network 10.10.10.0 255.255.255.0 area 0
 network 192.168.5.0 255.255.255.0 area 0
 log-adj-changes
!
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10

user-identity default-domain LOCAL
aaa authentication login-history
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca trustpool policy
auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
certificate ca 18dad19e267de8bb4a2158cdcc6b3b4a
308204d3 308203bb a0030201 02021018 dad19e26 7de8bb4a 2158cdcc 6b3b4a30
0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117
30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d 20466f72
20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504 03133c56
65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043
65727469 66696361 74696f6e 20417574 686f7269 7479202d 20473530 1e170d30
36313130 38303030 3030305a 170d3336 30373136 32333539 35395a30 81ca310b
30090603 55040613 02555331 17301506 0355040a 130e5665 72695369 676e2c20
496e632e 311f301d 06035504 0b131656 65726953 69676e20 54727573 74204e65
74776f72 6b313a30 38060355 040b1331 28632920 32303036 20566572 69536967
6e2c2049 6e632e20 2d20466f 72206175 74686f72 697a6564 20757365 206f6e6c
79314530 43060355 0403133c 56657269 5369676e 20436c61 73732033 20507562
6c696320 5072696d 61727920 43657274 69666963 6174696f 6e204175 74686f72
69747920 2d204735 30820122 300d0609 2a864886 f70d0101 01050003 82010f00
3082010a 02820101 00af2408 08297a35 9e600caa e74b3b4e dc7cbc3c 451cbb2b
e0fe2902 f95708a3 64851527 f5f1adc8 31895d22 e82aaaa6 42b38ff8 b955b7b1
b74bb3fe 8f7e0757 ecef43db 66621561 cf600da4 d8def8e0 c362083d 5413eb49
ca595485 26e52b8f 1b9febf5 a191c233 49d84363 6a524bd2 8fe87051 4dd18969
7bc770f6 b3dc1274 db7b5d4b 56d396bf 1577a1b0 f4a225f2 af1c9267 18e5f406
04ef90b9 e400e4dd 3ab519ff 02baf43c eee08beb 378becf4 d7acf2f6 f03dafdd
75913319 1d1c40cb 74241921 93d914fe ac2a52c7 8fd50449 e48d6347 883c6983
cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0 6773e314 087ee53f 9f73b833 0acf5d3f
3487968a ee53e825 15020301 0001a381 b23081af 300f0603 551d1301 01ff0405
30030101 ff300e06 03551d0f 0101ff04 04030201 06306d06 082b0601 05050701
0c046130 5fa15da0 5b305930 57305516 09696d61 67652f67 69663021 301f3007
06052b0e 03021a04 148fe5d3 1a86ac8d 8e6bc3cf 806ad448 182c7b19 2e302516
23687474 703a2f2f 6c6f676f 2e766572 69736967 6e2e636f 6d2f7673 6c6f676f
2e676966 301d0603 551d0e04 1604147f d365a7c2 ddecbbf0 3009f343 39fa02af
33313330 0d06092a 864886f7 0d010105 05000382 01010093 244a305f 62cfd81a

982f3dea dc992dbd 77f6a579 2238ecc4
a7a07812 ad620e45 7064c5e7 97662d98
097e5faf d6cc2865 f201aa08 1a47def9
f97c925a 0869200d d93e6d6e 3c0d6ed8
e6069140 18b9f8c1 eddfdb41 aae09620
c9cd6415 3881c994 eea28429 0b136f8e
db0cdd25 02dba48b 1944d241
7a05694a 584f60ca 7e826a0b 02aa2517
39b5db7f
e784652a 958abd86 de5e8116
832d10cc defda882 2a6d281f 0d0bc4e5
e71a2619
e1f4116f 10b595fc e7420532 dbce9d51
5e28b69e 85d35bef a57d4540 728eb70e
6b0e06fb 33354871 b89d278b c4655f0d
86769c44 7af6955c f65d3208 33a454b6
183f685c f2424a85 3854835f d1e82cf2
ac11d6a8 ed636a
quit
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd address 192.168.5.4-192.168.5.254
inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record
DfltAccessPolicy
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns
preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile License
destination address http
https://tools.cisco.com/its/service/oddce/servi
ces/DDCEService
destination transport-method http
profile CiscoTAC-1
no active
destination address http
https://tools.cisco.com/its/service/oddce/servi
ces/DDCEService
destination address email
callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory
periodic monthly
subscribe-to-alert-group configuration
periodic monthly
subscribe-to-alert-group telemetry
periodic daily
Cryptochecksum:51deb4c9924d3a4ee609
8eac3f0b5de9
: end
Багаторівневий комутатор
INSIDE_DB_NETWORK
Building configuration...

Current configuration : 1041 bytes
!
! Last configuration change at 12:36:50
EET Mon Jun 15 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec

```
no service password-encryption
service compress-config
!
hostname Indide_db_SW
!
boot-start-marker
boot-end-marker
!
enable password admin
!
username admin privilege 15 password 0 admin
no aaa new-model
clock timezone EET 2 0
!
ip domain-name diploma
ip cef
no ipv6 cef
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
!
interface Port-channel3
!
interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
 channel-group 3 mode active
!
interface Ethernet0/3
 channel-group 3 mode active
!
interface Vlan1
 ip address 192.168.5.2 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login local
 transport input ssh
 transport output ssh
!
End
```

Комутатор DB_WORKER

```
Building configuration...

Current configuration : 1083 bytes
!
! Last configuration change at 12:36:55 EET Mon Jun 15 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname DB_Office_SW
!
boot-start-marker
boot-end-marker
!
enable password admin
!
username admin privilege 15 password 0 admin
no aaa new-model
clock timezone EET 2 0
!
ip domain-name diploma
ip cef
no ipv6 cef
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
!
interface Port-channel3
!
interface Ethernet0/0
 channel-group 3 mode passive
!
interface Ethernet0/1
!
```

```
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
 channel-group 3 mode passive
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login local
 transport input ssh
 transport output ssh
!
end
```