МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«Графічний інтерфейс консольного серверу»

Завідувач випускаючої кафедри — **Довбиш А.С.**

Керівник роботи — **Великодний Д.В.**

Студента групи ІН – 71 — **Громенко Д.В.**

СУМИ 2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних наук

Затверджую_____

Зав. кафедри Довбиш А.С.

"_____" _____2021 р.

ЗАВДАННЯ
до випускної роботи

Студента четвертого курсу, групи ІН-71 спеціальності "Комп'ютерні науки" денної форми навчання Громенко Дар'ї Валеріївни.

Тема: «Графічний інтерфейс консольного серверу»

Затверджена наказом по СумДУ

№_____ от _____2021 р.

Зміст пояснювальної записки: 1) огляд та аналіз існуючих аналогів; 2) постановка завдання й формулювання завдань дослідження; 3) огляд технологій для реалізації завдання; 4) налаштування консольного серверу; 5) аналіз результату.

Дата видачі завдання "_____"_____2021 р.

Керівник випускної роботи _____ Великодний Д.В.

Завдання прийняв до виконання _____ Громенко Д.В.

РЕФЕРАТ

Записка: 50 стор., 28 рис., 0 табл., 0 додатків, 13 джерел.

Об’єкт дослідження — консольний сервер.

Мета роботи — налаштування консольного серверу для віддаленого доступу до обладнання Cisco.

Методи дослідження — метод комп’ютерного моделювання.

Результати — У рамках роботи було створено схему налаштування консольного серверу за допомогою симулятору мережі передачі даних Cisco Packet Tracer, яка б максимально відтворювала реальне налашування консольного серверу. На основі створеної схеми здійснено підключення та налаштування мережі віддаленого доступу з використанням консольного серверу на реальному обладнанні Cisco.

КОНСОЛЬНИЙ СЕРВЕР, ВІДДАЛЕНИЙ ДОСТУП, SSH, TELNET, DIAL-UP, CISCO PACKET TRACER.

ЗМІСТ

ВСТУП

ІТ- фахівцям був завжди потрібен зручний доступ до робочих серверів, мережевих пристроїв і додатків у будь-який час і у будь-якому місці. Проблеми, викликані збоєм пристроїв, атаками з метою порушення нормального обслуговування користувачів, мережевими вторгненнями і шкідливим ПО, а також природними катастрофами, ставлять функціонування центру обробки даних(ЦОД) під загрозу. Необхідність в надійному мережевому управлінні нарівні із забезпеченням безпеки стала для адміністраторів мереж пріоритетним завданням. Довгий час подібні завдання вирішувалися за допомогою ресурсоємних рішень, стаючи економічно невигідними навіть для великих організацій з єдиним ядром ЦОД. Але з появою доступних рішень на основі видаленого управління по IP ситуація кардинально змінилася.

Виникає питання: чи завжди модернізація засобів видаленого управління зручна і вигідна і як вона вплине на ІТ- інфраструктуру в цілому? Відповісти на першу частину питання можна тільки після інвентаризації і оптимізації облаштувань управління на базі IP. При належному підході до цього завдання будь-які доповнення, починаючи від використання IP KVM- перемикачів(від англ. keyboard video mouse - клавіатура, відео, миша) і закінчуючи готовими промисловими рішеннями, будуть виправданими і правомірними. На другу частину питання відповісти ще простіше. Вигода від застосування новинок в області видаленого управління очевидна. По-перше, заміна старих KVM-перемикачів на нові облаштування управління на базі IP - така заміна кардинальним чином позначиться на оперативності рішення завдань. По-друге, впровадження пристроїв і рішень, що комбінують функціональні можливості KVM- перемикачів і систем видаленого доступу. В усіх цих випадках керівники ІТ-підрозділів отримають значну економію бюджету, а адміністратори мереж підвищать ефективність своєї роботи, а також отримають видалений доступ без збоїв.

Використання комбінованих облаштувань управління по IP довело, що вони є надійнішим рішенням, ніж програмний видалений доступ, для якого потрібен агент на кожному цільовому сервері. Програмний видалений доступ обмежений в можливостях і забезпечує додаткове навантаження на CPU. Апаратне поєднання KVM-перемикача з облаштуванням IP-доступу надає видаленому користувачеві прямий доступ до сотень серверів без навантаження на CPU. Воно також забезпечує повноцінний контроль від ГІП(графічний інтерфейс користувача - від англ. graphical user interface, GUI) додатків до усунення несправностей на рівні BIOS, обслуговування і перезавантаження. Не менш важливо і те, що ці рішення забезпечують доступ по окремому мережевому інтерфейсу, тому сервери залишаються доступними навіть при вимкненні основної мережі. Подібні можливості важливі для IT- фахівців, особливо коли їм необхідно реагувати на несподіваний технічний збій.

Serial Console Servers, SCS(чи console access server, або console management server - сервери управління консолями) допоможуть значно понизити витрати підприємства. Ефективне управління IT-периферією за допомогою цих пристроїв істотно скоротить час простою мережі.

У рамках даної роботи потрібно виконати налаштування віддаленого доступу з використанням Console Servers за домопомогою симулятора Cisco Packet Tracer та після на реальному обладнанні, проаналізувати методи підключення, розглянувши всі переваги та недоліки кожного для найякіснішого проведення побудови мережі віддаленого доступу.

1 ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

1.1 Віддалений доступ

Віддалений доступ - це дуже широке поняття, яке включає різні типи і варіанти взаємодії комп'ютерів, мереж і додатків. Існує величезна кількість схем взаємодії, які можна називати віддаленим доступом, їх спільною рисою є використання глобальних каналів та мереж при взаємодії. Крім того, для віддаленого доступу, як правило, характерна асиметрична взаємодія, тоді з одного боку є центральна велика мережа або центральний комп'ютер, а з іншої - окремий віддалений термінал, комп'ютер або невелика мережа, якій необхідно отримати доступ до інформаційних ресурсів центральної мережі. Останні роки кількість підприємств з територіально розподіленими корпоративними мережами значно збільшилася. Тому для сучасних засобів віддаленого доступу дуже важлива хороша масштабованість і підтримка великої кількості видалених клієнтів [1].

Ще нещодавно для віддаленого управління корпоративними мережами застосовувалися фірмові рішення, що відрізняються використанням власних протоколів передачі даних по телефонним мережам і власними методами аутентифікації віддалених користувачів, а також оригінальними засобами надання ресурсів центральній мережі. Це викликало деякі проблеми і при з'єднання двох мереж, що мали раніше різну конфігурацію засобів управління мережею, і при підготовці фахівців, і в інших ситуаціях. Зараз в системах управління працює все більше стандартних компонентів: протокол передачі даних PPP; надання інформаційних ресурсів видаленим користувачам за допомогою служби WWW або тих же сервісів, які працюють і в локальній мережі. Цей процес полегшує взаємодію серверів видаленого доступу з клієнтами і мережевими операційними системами [2].

Основні зусилля операторів телекомунікаційних сервісів сьогодні спрямовані на подолання обмежень аналогових модемів. Крім того, передача інформації через мережу Інтернет є небезпечним.

Підключення корпоративної мережі до Internet виправдано у тому випадку, якщо вам потрібний доступ до відповідних послуг. Використати Internet як середовище передачі даних варто тільки тоді, коли інші способи недоступні і коли фінансові міркування переважують вимоги надійності і безпеки.

Однією з найширше обговорюваних проблем віддаленого адміністрування є саме безпека. Якщо допускається можливість віддаленого управління вашою мережею, незважаючи на те, яка технологія була застосована, з'являється ряд проблем, які пов'язані із забезпеченням безпеки інформації, що передається по мережі.

Які небезпеки можуть погрожувати приватній мережі при використанні тієї або іншої технології передачі даних? Передусім це перехоплення інформації при передачі. Тут можуть допомогти засоби шифрування, які вирішують проблему лише частково, оскільки застосовані в основному до пошти і передачі файлів. Рішення ж, що дозволяють з прийнятною швидкістю шифрувати інформацію в реальному часі, поки малодоступні і дорогі. Є засіб захисту від несанкціонованого доступу до мережі – Firewall (міжмережевий екран). Проте, будь-який захист можна взламати, особливо якщо отримана інформація окупає вартість взлому. Отже, Internet не може стати основою для систем, в яких потрібно надійність і закритість, застосовувати можна лише в крайньому випадку і при використанні усіх заходів захисту, включаючи міжмережеві екрани, шифрування каналу і VPN.

Перші три види віддаленого доступу часто об'єднують поняттям індивідуального доступу, а схеми доступу "мережу-мережу" іноді ділять на два класи - ROBO(RegionalOffice/BranchOffice) і SOHO(SmallOffice/ HomeOffice). Клас ROBO відповідає випадку підключення до центральної мережі мереж

середніх розмірів - мереж регіональних підрозділів підприємства, а класу SOHO - випадку віддаленого доступу мереж невеликих офісів і домашніх мереж [3].

Особливе місце серед усіх видів видаленого доступу до комп'ютера займає спосіб, при якому користувач дістає можливість віддалено працювати з комп'ютером так само, як якби він управляв ним за допомогою локально підключеного терміналу. За допомогою даного режиму можна встановити програми на віддаленому комп'ютері та бачити результати їх виконання. При цьому такий спосіб доступу прийнято розділяти на термінальний доступ і на видалене управління. Хоча це близькі режими роботи, але в описі продуктів видаленого доступу їх не прийнято об'єднувати в один клас. Частіше за все під терміном «термінальний доступ» розуміють символьний режим роботи з віддаленими розрахованими на багато користувачів ОС - UNIX, VAXVMS, ОС мейнфреймів IBM. У клас віддаленого управління включають програми емуляції графічного екрану ОС персональних комп'ютерів.

Багато виробників операційних систем передбачили у своїх стеках протоколів засоби термінального доступу користувачів до комп'ютерів по мережі. Вони дозволяють користувачеві, працюючому за комп'ютером, підключеним до мережі, перетворити екран свого монітора на емулятор терміналу іншого комп'ютера, також підключеного до мережі. Протокол Telnet стека TCP/IP – найпопулярший засіб такого типу, що з'явився у рамках операційної системи UNIX і відтоді нерозривно з нею пов'язаного [4].

На відміну від систем термінального доступу, засоби підтримки режиму видаленого вузла (remote node) роблять машину повноправною ланкою локальної мережі. Це досягається за рахунок того, що на видаленому комп'ютері працює той же стек протоколів, що і в комп'ютерах центральної локальної мережі, за винятком протоколів канального і фізичного рівня. На цьому рівні замість традиційних протоколів Ethernet або 26 Token Ring працюють модемні протоколи (фізичний рівень) і канальні протоколи з'єднань "точка-точка", такі як SLIP, HDLC і PPP. Ці протоколи використовуються для передачі по телефонним

мережам пакетів мережевого і інших протоколів верхніх рівнів. Таким чином, здійснюється повноцінний зв'язок видаленого вузла з іншими вузлами мережі [2].

1.2 Out-of-band management

Внутрішньосмуговий і позасмуговий трафік управління пов'язаний з площиною управління. Є два основні способи управління мережею:

- внутрішньосмугове управління мережею (In-band network management);
- позасмугове управління (Out - of - band management).

Внутрішньосмугове управління відноситься до управління через саму мережу з використанням підключення Telnet / SSH до маршрутизатора або за допомогою інструментів на основі SNMP (Simple Network Management Protocol (простий протокол мережевого управління) - стандартний інтернет-протокол для управління пристроями в IP-мережах на основі архітектури TCP/UDP). Внутрішньосмуговий - це звичайний спосіб управління мережею, при якому фактичний трафік даних / виробництва і управління може використати один і той же шлях для зв'язку з різними елементами. Для великих або критично важливих для бізнесу мереж внутрішньосмугового управління мережею недостатньо. Якщо мережа не працює, це впливає на доступність мережевого пристрою, і це великий ризик для організації і її бізнесу. Нам потрібний альтернативний або вторинний шлях доступу, щоб обійти проблему або отримати доступ до джерела проблеми - по суті, це те, що забезпечує Out-of-Band Management(OOB)(рис.1.1).

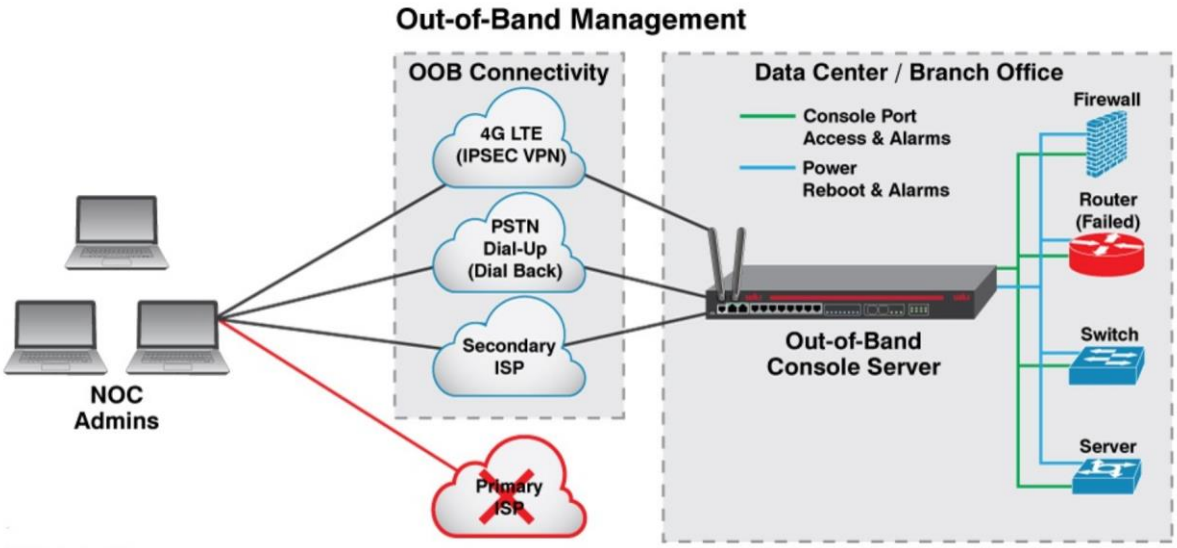


Рисунок 1.1 — Out-of-Band Management

OOBM працює в "площині управління", яка відокремлена від "площини даних", використованої трафіком даних на комутаторі і трафіком внутрішньосмугового управління. Тому коли основна мережа стає недоступною або пристрої виходять з ладу, Out-of-Band Management забезпечує видалений доступ, моніторинг і управління IT-інфраструктурою через вторинне і безпечне з'єднання з використанням супутникового, Ethernet або видаленого доступу.

Використання портативного комп'ютера і програмного забезпечення емуляції терміналу - один з найбільш поширених способів зв’язку з послідовним console port. Коли адміністратор мережі використовує послідовне кабельне з'єднання з консольним портом позасмугового управління, він може підключатися до елементів в стійці для діставання кореневого доступу до параметрів управління і контролю. Аналогічним чином вторинна IP- мережа також може бути підключена безпосередньо до диспетчера консолі з двома Ethernet-портів, щоб адміністратори могли видалено підключатися один до одного. Коли кількість мережевих елементів, що вимагають управління, починає рости, традиційні засоби зв'язку RS-232 стають громіздкими і вимагають багато часу. Консольний сервер позасмугового управління - це економічне і зручне рішення для спрощення цього важливого засобу підключення до мережі [5].

Основною перевагою інтерфейсу позасмугового управління є його доступність, коли мережа не працює, пристрій вимкнений, знаходиться в сплячому режимі, гібернації або недоступно з інших причин. OOBM можна використати для видаленого перезавантаження пристроїв, що вийшли з ладу, і управління відключеними пристроями. Основна ідея полягає забезпеченні цілодобової безвідмовної роботи вашої мережі, забезпечивши постійний доступ до критично важливих IT-активів, таких як телекомунікаційні пристрої, міжмережеві екрани, маршрутизатори, комутатори, сервери, живлення, сховище і збої в роботі і час простою зводяться до мінімуму, забезпечуючи кращу видимість фізичного середовища і фізичного стану устаткування. Це забезпечує безперервність бізнесу за рахунок збільшення часу безвідмовної роботи і підвищення ефективності.

Тож які ще причини, через які підприємству потрібний альтернативний спосіб доступу до свого устаткування? Причин декілька.

Безпека: кількість порушень збільшується, і вони є загрозою для організацій в усіх галузях. Якщо усі порти адміністрування або управління підключені до виробничої мережі і відбувається атака, вони можуть спробувати отримати доступ до вашої IT-інфраструктури. Тоді як, якщо порт підключений до системи позасмугового управління, локальна мережа не може отримати доступ до яких-небудь консолей адміністрування на цьому устаткуванні. Оскільки він розділяє призначений для користувача і управлінський трафік, інженери можуть заблокувати частини мережі, обмежити доступ і захистити площину управління.

Безперервність бізнесу: позасмугове управління гарантує, що технічну інформацію не треба відправляти на місце, а виправлення можна буде виконувати віддалено. У поєднанні з 4G LTE підприємства отримують безпечний альтернативний шлях доступу, а перемикання на віддалений зв'язок при відмові забезпечує смугу пропускання, необхідну для забезпечення продовження роботи процесів під час збою.

Підприємства постійно звертаються до IT-фахівців, щоб скоротити витрати і при цьому забезпечити постійну доступність мережі. Первинні витрати, понесені під час розгортання позасмугового управління, окупляться після розгортання. Організації матимуть кращу доступність і надійність за невелику частину вартості ліній POTS.

Перевагами Out - of - Band Management є:

- доступ-SSH до інфраструктури через LTE, Ethernet або комутоване з'єднання при збоях інтернет-провайдера або пристрою;
- provisioning - налаштування конфігурацій через порти управління, ZTP і автоматизацію;
- моніторинг - реєструйте і отримуйте повідомлення при зміні стану підключення, живлення, довкілля, безпеки або конфігурації;
- усунення збоїв;
- стійке виправлення і автоматизація. Ведення системного журналу і локального аудиту;
- управління - включення/виключення/перезавантаження і налаштування портів управління.

Є три основні способи позасмугового управління. Вибір правильного методу залежить від ваших цілей.

Одним з традиційних методів позасмугового управління є підключення модему до консольного порту мережевого пристрою. У цього методу є декілька очевидних обмежень. Для цього вимагається, щоб у вас була телефонна лінія і модем для кожного керованого пристрою, тому воно погано масштабується. Ви можете увійти до системи тільки на декількох пристроях одночасно. А захищати модемні лінії украй складно. Навіть якщо у вас є ідентифікатори користувачів і надійні паролі на кожному пристрої, будь-хто, хто може вгадати або наштовхнутися на ваш телефонний номер модему, може, принаймні,

перешкодити вам отримати до нього доступ, просто підключивши телефонну лінію.

В деяких випадках люди можуть фізично вимикати модем, коли він не використовується. Хтось на видаленому сайті повинен включити його, щоб дозволити доступ. Виключення модему вирішує проблему безпеки, але ще більше ускладнює доступ до нього, коли він вам потрібний.

Крім того, модеми і телефонні лінії дуже повільні.

Консольний сервер - це пристрій з множиною низькошвидкісних асинхронних послідовних інтерфейсів. Потім ви підключаєте ці послідовні інтерфейси до різних мережевих пристроїв у віддаленому місці. Це особливо корисно, коли треба управляти великою кількістю пристроїв. Сам консольний сервер може бути спеціалізованим пристроєм або просто маршрутизатором (наприклад, Cisco 3925) з парою низькошвидкісних асинхронних послідовних модулів високої щільності.

Доступ до сервера консолі зазвичай здійснюється через окрему мережу, хоча ви можете також легко підключити модем до сервера терміналів і підключитися до нього по телефонній лінії. З'єднання Ethernet - найпоширеніший метод. Зазвичай кожному порту дається номер порту TCP. Ви використовуєте Telnet з IP-адресою термінального сервера по номеру порту, який відповідає певному підключенню консолі пристрою.

І ще одним спосіб є окрема мережа управління (Separate management network). Прийом з розміщенням інтерфейсів управління в іншій мережі полягає в тому, щоб зробити ці інтерфейси недоступними з основної мережі. Кращий спосіб створити інтерфейс позасмугового управління на міжмережевому екрані Cisco ASA - використати для управління окремий віртуальний контекст міжмережевого екрану. Проте у разі брандмауера ви також можете скористатися перевагами більшого контролю над списками контролю доступу (ACL), щоб просто заблокувати трафік управління (SNMP, Telnet, SSH) від використання інтерфейсів в основній мережі.

Списки контролю доступу не є ідеальним рішенням, оскільки таблиця маршрутизації брандмауера включає маршрути як до основної мережі, так і до мережі зовнішнього управління. Таким чином, можуть виникнути ситуації, коли буде складно відокремити трафік управління від виробничої мережі.

1.3 Консольний сервер

Завдання видаленого управління через IP- мережі можна вирішити за допомогою консольного сервера. Видалене консольне управління надає адміністраторам систем можливість ефективної установки і конфігурації мережевих пристроїв через TCP/IP Ethernet або через модемне з'єднання [6].

Консольний сервер - це спеціалізований мережевий комп'ютер з одним мережевим Ethernet портом і великою кількостю послідовних портів, які забезпечують управління з одного центрального комп'ютера, використовуючого TCP/IP мережу та можливості послідовного доступу до консольних портів різних пристроїв. З використанням Telnet через Ethernet LAN/WAN з'єднання досягається централізованим консольним контролем. Модемне з'єднання використовується як запасний варіант управління, коли пряме управління через Ethernet мережу неможливо. Управляючий комп'ютер зв'язується через модем з модемом, підключеним до консольного порту пристрою [7].

Він використовується для підключення пристроїв з послідовним інтерфейсом до мережі Ethernet, щоб відповідати найвимогливішим потребам при застосуванні в промислових системах управління, збору даних, моніторингу довкілля і системах видаленого управління потужностями і устаткуванням. Можливі різні режими роботи включаючи Real COM Port, TCP сервер/клієнт, UDP сервер/клієнт, Serial Tunnel і Virtual Modem. Це допомагає змінити можливості застарілих пристроїв з послідовним інтерфейсом з метою отримання переваг TCP/IP-мережі, що дозволяє здійснювати видалений доступ, налаштування і управління цими пристроями з будь-якої точки світу через Інтернет.

Консольний (термінальний) сервер призначений для видаленого управління різними пристроями через інтерфейс RS-232 (V.24/V.28).

Консольний порт з інтерфейсом RS-232 є універсальним засобом управління різними пристроями, такими як телефонні станції, модеми, мультиплексори, різні датчики і тому подібне, але нині все більше значення приймає видалене управління устаткуванням через IP- мережі.

Консольне управління використовує консольні порти великої кількості різних мережевих пристроїв для різних установок і функцій управління цими пристроями. І хоча ця можливість відома вже починаючи з 1970 років, це є найбільш ефективним шляхом управління, особливо при використанні гнучкого консольного сервера.

Консольні сервери об'єднують у собі функціонал сучасних технологій для забезпечення управління і безпечного доступу до пристроїв з послідовним інтерфейсом, використовуваних в центрах обробки даних. Консольний сервер дозволяє отримати як внутрішній так і зовнішній видалений доступ до послідовної консолі серверів і мережевих пристроїв, використовуючи безпосередньо Telnet/SSH-клієнт або додаток для перегляду. Консольні сервери є повним рішенням по безпечному видаленому доступу і управлінню пристроями з послідовним інтерфейсом. Політика прав доступу дозволяє налаштувати права індивідуально для кожного порту. Шифрування забезпечує надійне збереження данних, що передаються. Логірування дій і сповіщення про події допомагає прискорити вирішення спірних питань і понизити ризики. Розширені налаштування безпеки забезпечать її відповідність з внутрішньою політикою безпеки підприємства.

Out-of-Band тип доступу до пристроїв дозволяє здійснювати управління і діагностику на рівні завантажувача/BIOS, що неможливо у великій кількості випадків. До таких випадків відносяться відмови від програмного забезпечення і мережевих інтерфейсів, помилки конфігурації і інші аварійні ситуації, коли

штатний "ln-band" доступ, наприклад, по протоколах Telenet/SSH/VNC відсутній або ускладнений.

Коли мережевий адміністратор використовує послідовний консольний сервер, щоб забезпечити зовнішнє управління підключенням до віддаленого сайту, ряд інших інструментів може використовуватися спільно з консольним сервером для підвищення рівня управління і контролю. Мережеві контроллери живлення часто використовуються в тандемі з сервером послідовної консолі, щоб дозволити мережевому адміністратору управляти живленням мережевого елементу. Можливість отримати доступ до консольного сервера через позасмуговий сеанс (SSH або Dial-Up) і перезавантажити або управляти живленням певних елементів на сайті - зручний спосіб доповнити повний контроль над корпоративною глобальною мережею. Окрім контроллерів живлення, до сервера послідовної консолі також можуть бути підключені інші інструменти мережевого середовища, такі як реєстратори даних і датчики довкілля.

Режими роботи:

- підключення через COM порт (serial - based applications with a COM/TTY port driver): за допомогою спеціального драйвера на ПК створюється "віртуальний" COM, який пов'язаний з апаратним COM портом сервера послідовних інтерфейсів. Існують драйвера для ОС Windows і Linux;
- підключення по TCP сокету (Raw TCP socket): підключення по TCP сокету між сервером послідовних інтерфейсів і іншим пристроєм (режим TCP Client - TCP Server). Можливе підключення точка-точка або точка-безліч пристроїв;
- підключення по UDP сокету (Raw UDP socket): підключення по UDP сокету між сервером послідовних інтерфейсів і іншим пристроєм. Можливе підключення точка-точка або точка-безліч пристроїв;
- консольне підключення (Reverse Telnet, Reverse SSH): використовується Telnet або SSH для доступу до пристрою з послідовним портом. На ПК має

бути запущений Telnet або SSH клієнт для підключення до сервера послідовних інтерфейсів;

– послідовний тунель через два сервери: можливо організувати кидок COM портів через два сервери сполучених по Ethernet і налагоджених один на одного, один виступає в ролі TCP Client, а інший TCP Server;
– режим віртуального модему (Virtual modem): дозволяє пристроям, що підтримують роботу тільки через модем, передавати дані по Ethernet за допомогою AT команд [8].

На рисунку 1.2 зображені найпопулярніші варіанти налаштування віддаленого доступу за допомогою консольного серверу:

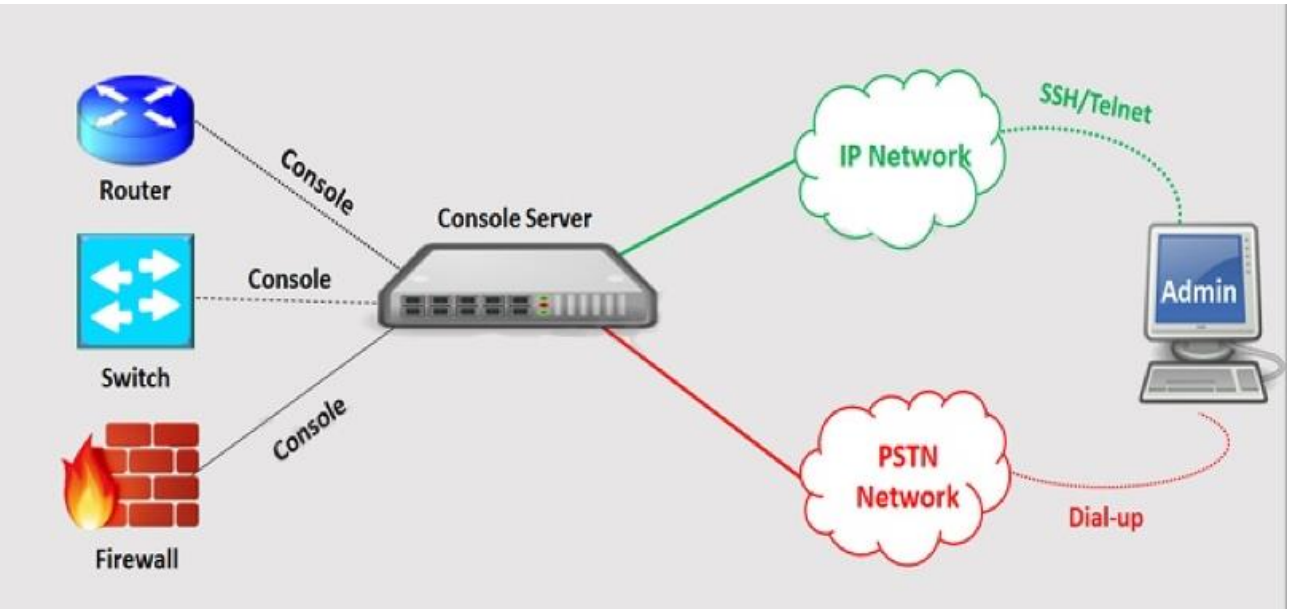


Рисунок 1.2 — схема віддаленого доступу з використанням консольного серверу

1.4 Telnet protocol

Telnet - це один з протоколів, який використовується як в Інтернеті, так і в локальній мережі. Іншими словами, Telnet - це протокол, який використовується для доступу до терміналів, серверів чи видаленого комп'ютера. З'єднання встановлюється через Інтернет за допомогою протоколу TCP / IP. Telnet часто називають TN (рис.1.3) [9].

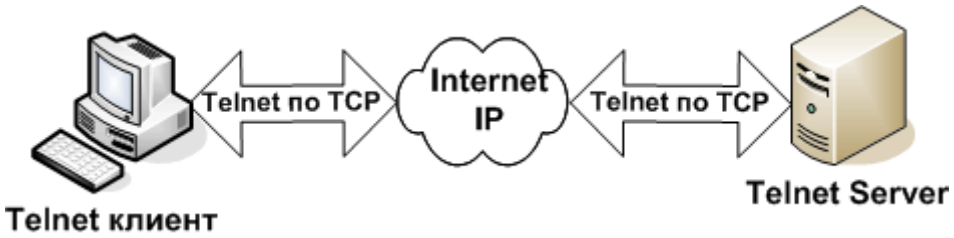


Рисунок 1.3 — TN з використанням протоколу TCP/IP

Уперше він був задуманий ще в 1969 році IETF(Internet Engineering Task Force). Telnet розшифровується як Teletype Network.

Telnet спеціально розроблений для видаленого доступу до сервера, де ми можемо управляти усією архітектурою клієнт/сервер. Для використання Telnet пристрій повинен підтримуватися командами. Деякі пристрої можуть не підтримуватися, і тому ми не можемо виконати команду на цих пристроях. Для мереж TCP/IP, таких як Інтернет, Telnet є програмою емуляції терміналу. Програмне забезпечення Telnet запускається, зв'язуючи мережевий сервер з вашим персональний комп'ютером. Той факт, що він перетворить усі дані в простий текст, вважається уразливим. Це означає, що якщо користувач підкоючиться до мережі, ви можете записати своє ім'я користувача і пароль під час передачі. Це дозволяє користувачеві отримати віддалений доступ до облікового запису або комп'ютера. Наприклад, для віддаленого управління своїми файлами споживач може підключитися до головного комп'ютера через Telnet.

Він робить доступним користувачам інтерактивну і двонаправлену текстову систему повідомлень, що використовує ефективне термінальне з'єднання. Призначені для користувача дані розміщуються в смузі з інформацією telnet, що управляє, над TCP. Це допомагає виконувати деякі функції видалено. Користувач приєднується до сервера не лише по протоколу TCP, це означає, що, як і на іншій стороні, з'єднання також встановлюється з використанням імені хоста telnet [10].

Синтактис: telnet hostname port.

Нині як віртуальний термінал, так і емулятори терміналу можуть використовуватися для telnet.

Нижче описані деякі з переваг.

- він доступний для безлічі різних операційних систем;
- з його допомогою можна виконати елементи конфігурації мережевого устаткування;
- доступ до видалених комп'ютерів: тобто воно дає згоду на віддалений доступ до іншого комп'ютера;
- це допомагає дуже швидко заощадити багато часу, встановити з'єднання і виконати завдання на різних комп'ютерах;
- конфігурація маршрутизатора: тут дуже просто розв'язати проблему, оскільки для передачі використовується простий текст. Отже, передача даних здійснюється з великим доступом і меншим об'ємом передачі;
- універсальність: його можна гнучко розгорнути на будь-якому з комп'ютерів. Навіть Різні ОС можуть підключатися один до одного незалежно від їх версії і часу випуску;
- він робить доступним користувачам інтерактивну і двонаправлену текстову систему повідомлень, за допомогою термінального з'єднання, що перевищує 8 байт. Призначені для користувача дані покриваються довгою смугою з інформацією telnet, що управляє, над TCP. Це допомагає виконувати деякі функції віддалено.

Telnet в основному відправляє усі повідомлення у вигляді звичайного тексту. Це означає, що немає спеціального механізму безпеки. Таким чином, це не вважається безпечним, і люди не вважають за краще відправляти свої особисті дані через Telnet. Це один з найбільших недоліків Telnet. Більше того, проводить не належну аутентифікацію. Іншими словами, ми не можемо гарантувати, що дані просто передаються між двома хостами і немає перехоплення посередині. Отже, це ще одна проблема, яка виникає, коли йдеться про безпеку Telnet. Проте

зараз у багатьох сервісах і додатках існують поліпшені заходи, щоб зробити їх безпечнішими. Тому у багатьох застосуваннях Secure Shell(SSH) замінює Telnet.

1.5 SSH protocol

Створено в 1995 Tatu Ylönen, протокол SSH, відомий також як Secure Shell or Secure Socket Shell, - мережевий протокол, який дає системним адміністраторам безпечний шлях звернутися до видалених активів по незабезпеченій мережі. SSH забезпечує пароль або ключову засновану ідентифікацію і кодує з'єднання між двома мережевими кінцевими точками. Це - безпечна альтернатива протоколам (як наприклад telnet, дистанційна реєстрація) законного логіна і ненадійним transfer методам (як наприклад FTP) файлу. На додаток до забезпечення стійкого шифрування, SSH широко використовується адміністраторами мережі, щоб управляти системами і додатками віддалено, доставляють частини програмного забезпечення, або виконують команди і переміщають файли [11].

Інтерактивне використання - це коли хтось на зразок системного адміністратора використовує SSH для видаленого управління і налаштування комп'ютера, мережевого устаткування і різних інших хостов. Це означає, що адміністраторам не треба вручну управляти і налаштовувати кожен окремий пристрій, що економить час, гроші і знижує вірогідність людської помилки [6].

Протокол SSH будувався в серверах Unix і Linux, щоб дозволити безпечні з'єднання між системами. Протокол SSH використовує архітектуру клієнт-сервер, в якій пристрій використовує клієнтське програмне забезпечення для виконання команд на сервері. Ось узагальнена версія того, як встановлюється SSH-з'єднання. По-перше, системний адміністратор використовує клієнтський додаток SSH на своєму пристрої (хост A), щоб ініціювати з'єднання з серверним додатком SSH (хост B). Потім два хоста погоджують, які алгоритми шифрування використати для зв'язку, встановлюють ключ шифрування для сеансу, аутентифікують сервер, і системний адміністратор відправляє свої облікові дані,

такі як ім'я користувача і пароль, на сервер. Аутентифікація сервера і клієнта - важливий елемент в підтримці конфіденційності і цілісності SSH- з'єднання [12].

Клієнт SSH ініціює connection setup процес і користується ключовою криптографією, щоб перевірити ідентичність сервера SSH. Після setup-фази, протокол SSH користується сильною симетричною схемою шифрування і алгоритмами хешування, щоб гарантувати конфіденційність і цілісність даних, це обмінюється між клієнтом і сервером.

На рисунку 1.4 нижче представлена спрощена схема з'єднання:

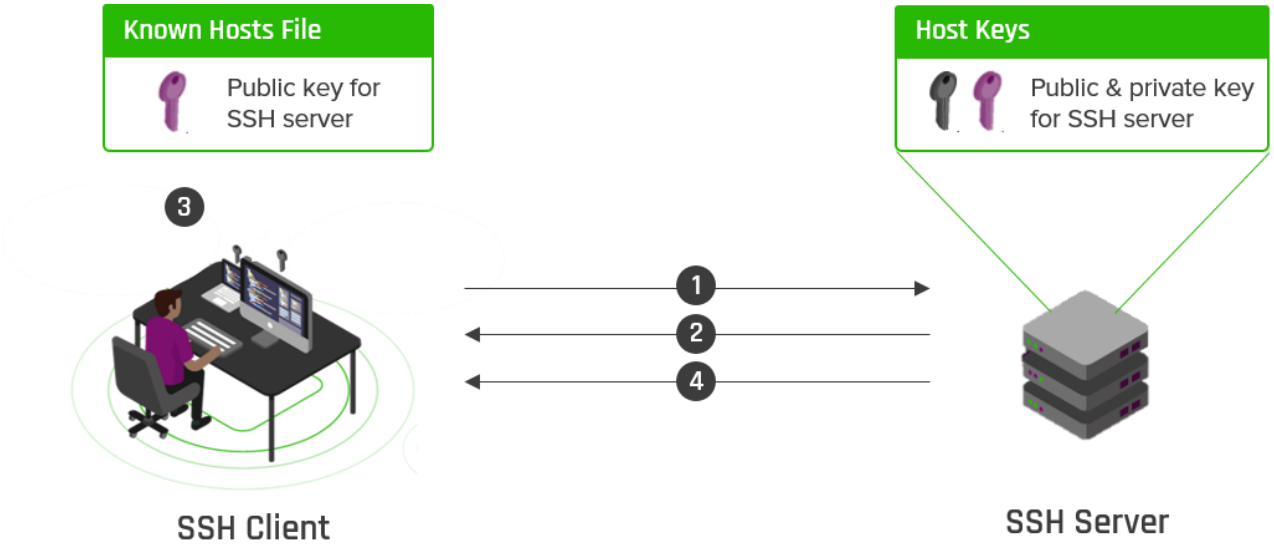


Рисунок 1.4 — робота SSH протоколу

1. Клієнт ініціює з'єднання з SSH- сервером.
2. Сервер відправляє клієнтові свій відкритий ключ.
3. Відкритий ключ сервера зберігається у файлі відомих хостів клієнта.
4. Клієнт і сервер погоджують параметри з'єднання і встановлюють з'єднання.

З'єднання SSH в основному використовується для захисту різних типів зв'язку між локальним комп'ютером і видаленим хостом, у тому числі:

- Безпечний видалений доступ до ресурсів
- Видалене виконання команд
- Доставка патчів і оновлень програмного забезпечення
- Інтерактивна і автоматична передача файлів

Окрім створення безпечного каналу між локальними і видаленими комп'ютерами, протокол SSH використовується для управління критично важливою корпоративною інфраструктурою, такою як маршрутизатори, серверне устаткування, платформи віртуалізації і операційні системи.

1.6 Різниця між SSH і Telnet

Telnet був першим протоколом інтернет-додатків, який використовувався для створення і підтримки термінального сеансу на видаленому хості.

І SSH, і Telnet мають однакову функціональність. Проте, основна відмінність полягає в тому, що протокол SSH захищений криптографією з відкритим ключем, яка аутентифікує кінцеву точку при налаштуванні сеансу терміналу. З іншого боку, в Telnet не передбачена аутентифікація для користувача, що робить її менш безпечною.

SSH відправляє зашифровані дані, а Telnet відправляє дані у вигляді звичайного тексту.

Із-за високої безпеки SSH є переважним протоколом для загальнодоступних мереж, а із-за меншої безпеки Telnet підходить для приватних мереж.

За умовчанням SSH працює на порту 22, але його можна змінити, тоді як Telnet використовує порт номер 23, спеціально розроблений для локальної мережі.

1.7 Dial-up

Dial-up (комутоване з'єднання)- інтернет-з'єднання, що встановлюється за допомогою телефонних ліній [13].

Dial-up з'єднання встановлюється, коли два та більше одиниць обладнання зв'язку використовують комутовану телефонну мережу загального користування (PSTN) для підключення до постачальника послуг Інтернету (ISP), корпоративної мережі або промислової мережі за допомогою аналогового

телефонного модему. Модеми комутованого доступу підтримують швидкості в діапазоні від 300 біт/з (біт в секунду) до 56 кбит/з (кілобіт в секунду). Де б у вас не було комутоване з'єднання, на окремі комутовані виклики "відповідає" сервер видаленого доступу [13].

Віддалений доступ - це можливість зв'язуватися з комп'ютером або мережею, що знаходиться на деякій відстані, через dial-up. Цей термін спочатку використовувався для опису підключення користувачів до Інтернету з використанням комутованого з'єднання по традиційним телефонним лініям POTS або ISDN. Протоколи віртуальної приватної мережі (VPN) зазвичай використовуються для захисту цих приватних з'єднань. Віддалений доступ по телефонній лінії все ще використовується сьогодні як резервна копія широкосмугових підключень. Сьогодні більшість комутованих підключень видаленого доступу використовуються для пристроїв в точках продажів (POS), таких як термінали для кредитних карт, лічильники і квиткові автомати, обладнані модемами для комутованого доступу. Сервери видаленого доступу по телефонній лінії (RAS) також як і раніше поширені в таких промислових комунікаційних застосуваннях, як віддалене управління, міжмашинні мережі і Інтернет речей (IoT).

Сервер віддаленого доступу – це обчислювальний пристрій, працюючий на програмному забезпеченні віддаленого доступу, який відповідає на вхідні модемні дзвінки видаленого доступу. Сервер віддаленого доступу, який іноді називають комунікаційним сервером, використовує технологію протоколу точка-точка через Ethernet (PPPoE) для встановлення надійного комутованого з'єднання. RAS встановлюється на території компанії і підключається до внутрішньої мережі і систем. Віддалені користувачі і машини можуть встановити VPN-з'єднання з RAS за допомогою комутованого PPPoE для доступу до Інтернету або приватної мережі.

Коли шляхи внутрішньосмугового управління мережею не можуть надати адміністраторам необхідні засоби для управління видаленим мережевим

устаткуванням, стратегія позасмугового управління видаленим доступом є цінним доповненням до арсеналу будь-якого мережевого адміністратора, у якого є розподілені елементи глобальної мережі.

Впровадження позасмугового управління дозволяє мережевому адміністраторові мати повний контроль над усіма елементами в глобальній мережі, навіть коли стратегії внутрішньосмугового управління і управління на основі IP терплять невдачу. Консольні сервери з внутрішніми модемами комутованого доступу забезпечують комплексну стратегію позасмугового управління. Це може бути потужним інструментом в арсеналі будь-якого адміністратора, якому потрібна надійна стратегія віддаленого управління. На рис.1.5 наведено приклад підключення dial-up через загальнодоступну PSTN.

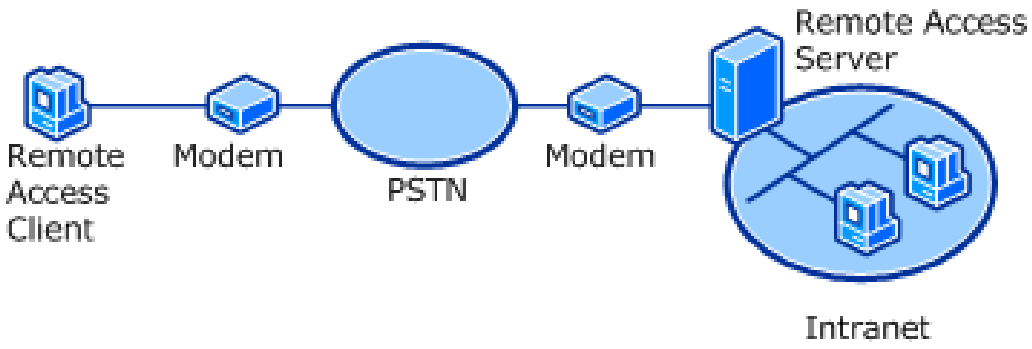


Рисунок 1.5 — Dial-UP через PSTN

Дозвіл доступу до сервера послідовної консолі через модемне з'єднання через загальнодоступну PSTN представляє деякі важливі аспекти безпеки. Багато консольних серверів включають вбудовані модеми для видаленого управління з'єднаннями. Сторонні протоколи аутентифікації (Radius, LDAP) можуть бути реалізовані через консольний сервер, щоб гарантувати аутентифікацію будь-якого користувача віддаленого доступу. Повнофункціональний консольний сервер також включатиме функції безпеки зворотного виклику і журнали аудиту усіх комутованих з'єднань. Неприпустиме блокування спроби з повідомленням - ще одна корисна функція, що допомагає забезпечити безпеку комутованого

з'єднання. Локальна перевірка достовірності також може бути включена в сервер послідовної консолі для перевірки достовірності видаленого доступу під час збоїв мережі, що може вплинути на можливість внутрішньосмугової перевірки достовірності користувачів**.**

Ще одно важливе міркування при виборі віддаленого консольного сервера з внутрішнім модемом - це рівень доступності для підключень, що входять. Повнофункціональний консольний сервер матиме декілька засобів забезпечення доступності внутрішнього модему для сеансів управління, що входять. Функції доступності модему повинні включати таймери стеження і періодичну ініціалізацію модему.

Відповідний послідовний консольний сервер, використовуваний для комутованих підключень до видалених сайтів, повинен включати декілька методів перевірки достовірності усередині і поза діапазоном. Доступність модему має первинне значення, тому мікропрограмне забезпечення сервера консолі повинне використати декілька схем скидання і ініціалізації модему, щоб гарантувати доступність модему. Журнал аудиту і ведення журналу корисні для адміністраторів, що надають віддалений доступ декільком групам управління.

1.8 Постановка задачі

Проаналізувавши літературні відомості з книжкових та електронних ресурсів, мету дипломної роботи можна сформувати наступним чином: необхідно виконати налаштування консольного серверу для віддаленого доступу до обладнення Cisco за допомогою протоколу SSH.

Для загального розуміння конфігурації створити схему за допомогою симулятору мережі передачі данних Cisco Packet Tracer, яка б максимально відтворювала реальне налашування консольного серверу.

На основі створеної схеми здійснити підключення та налаштування мережі віддаленого доступу з використанням консольного серверу на реальному обладнанні Cisco.

Постановка задачі:

1. Налаштування консольного серверу за допомогою програмного додатку Cisco Packet Tracer.

2.Налаштування консольного серверу за допомогою реального обладнання Cisco.

2 ВИБІР МЕТОДУ РІШЕННЯ

2.1 Конфігурація мережі з використанням симулятора Cisco Packet Tracer

Cisco Packet Tracer - це кроссплатформенный інструмент мережевого моделювання, що дозволяє упорядковувати вузли і сполучні лінії, а також імітувати комп'ютерні мережі. Cisco Packet Tracer - одна з найкорисніших програм візуального моделювання для мережевих сертифікатів, наприклад CCNA. За допомогою цього інструменту можна експериментувати з поведінкою мережі. Таким чином, знайти відповіді на широке коло питань і досліджувати різні сценарії для досягнення кращих результатів. Оскільки Cisco Packet Tracer є важливою частиною мережевої академії, вона надає студентам великий досвід навчання. Крім того, він пропонує декілька можливостей візуалізації, моделювання, оцінки, спільної роботи і розробки, щоб полегшити безпроблемне навчання і викладання складних концепцій IT. Програма є моделлю інтерфейсу командного рядка, в якому ви можете перетягувати мережеві пристрої на власний розсуд. Це допоможе вам зрозуміти поведінку мережі і, можливо, виявити нові мережеві ідеї.

Перевагами Cisco Packet Tracer є забезпечення реалістичного середовища навчання з симуляцією і візуалізацією, яка доповнює класну кімнату, устаткування, включаючи можливість бачити внутрішні процеси в реальному часі, які зазвичай приховані на реальному пристрої. Також забезпечує розраховану на багато користувачів співпрацю в реальному часі. Дане програмне забезпечення дозволяє вивчати концепції, проводити експерименти і перевіряти своє розуміння побудови, розробки та налаштування мережі. Мережеві пристрої відображаються в пакетному трасувальнику так, як вони виглядають в реальності, а студент може взаємодіяти з різними мережевими пристроями, налаштування конфігурацій шляхом їх включення і виключення і т. д. Трасування пакетів також має зручний графічний інтерфейс і інтерфейс

командного рядка, інтерфейси, з якими легко працювати і що не вимагають будь-який досвід або знання. Ще одна важлива особливість пакетного трасувальника полягає в тому, що він може підтримувати декілька мов, і ця платформа незалежна. Це програмне забезпечення з відкритим початковим кодом. Packet Tracer також допомагає зрозуміти концепцію логічного усунення несправностей і також можна використати для тематичних досліджень.

Робочі простори: є два типи робочого простору. Логічний робочий простір: дозволяє користувачам створювати логічні мережеві топології і різні пристрої можна перетягувати в логічну робочу область. Фізичний робочий простір: дозволяє користувачеві створювати мережу так, як вона виглядала б у реальному світі, і можливість географічного представництва, де різні мережеві пристрої можуть відображатися як підключені на різні локації міста. Режими: є два типи режимів. Режим реального часу: пристрої в мережі поводяться, працюють і виглядають як справжні пристрої. Режим моделювання: в цьому режимі можна бачити і контролювати інтервали часу, щоб дізнатися, як усувати збої в мережі.

Мережеві пристрої: існують різні мережеві пристрої, які можна використати для створення різних мереж лабораторних сценаріїв. Наприклад, маршрутизатори, комутатори, хаби, безпровідні пристрої, Connections, End Devices, емулятори WAN, Custom Made Devices, Multi-user Connection, персональні комп'ютери, ноутбуки, сервери, принтери, IP-телефонія, VOIP пристрої, аналогові телефони, телевізори, безпровідні планшети та інше. Для підключення різних мережевих пристроїв до трасувальника пакетів можна використати різні типи кабелів: консольний кабель, прямий мідний кабель, мідний перехресний кабель, оптоволоконний кабель, телефонний кабель, коаксіальний кабель, послідовний DTE, послідовний DCE і вісімковий кабель.

На ПК ми можемо додати модуль виходячи з вимог, включити правила брандмауера, призначити IP-адресу IPV4 і IPV6, шлюз за умовчанням і маску підмережі до інтерфейсу. Створення комутованого з'єднання – ще одна особливість Cisco Packet Tracer. Використовуючи програмне забезпечення

терміналу ми можемо отримати доступ до інтерфейсу командного рядка маршрутизатора за допомогою консольного кабелю. Ми можемо проводити різні діагностичні тести за допомогою командного рядка; також ми можемо використати веб-браузер, безпровідне з'єднання, VPN, генератор трафіку, Cisco Ip Communicator, електронну пошту, PPPoE Dialer, текстовий редактор та т.д.

Ми також можемо використати наступні служби на сервері HTTP, DHCP, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, FIREWALL, IPV6 FIREWALL і протестувати ці служби з клієнтської машини. Packet Tracer має зручний Режим CLI, де користувач може вводити різні команди для налаштування різних мережевих пристроїв.

2.2 Конфігурація мережі на базі роутерів Cisco

Cisco Systems, Inc. займається розробкою, виробництвом і продажем мережевих продуктів і послуг на основі Інтернет-протоколу, пов'язаних з індустрією зв'язку і інформаційних технологій. Фірма працює в наступних географічних сегментах: Америка, Європа, Близький Схід і Африка і APJC. Його продукція включає наступні категорії:

- комутатори;
- маршрутизатори;
- безпровідні мережі;
- інтерфейси;
- модулі управління мережею;
- оптичні мережі;
- точки доступу;
- зовнішні і промислові точки доступу;
- міжмережеві екрани нового покоління;
- розширений захист від шкідливих програм;
- клієнти безпеки VPN;

– електронна пошта і веб-безпека.

Для налаштування я використовувала обладнання:

– Маршрутиразор Cisco 2900 Series

Cisco серії 2900 пропонують підвищений рівень інтеграції послуг з голосом, відео, безпекою, послуги безпровідного зв'язку, мобільності і передачі даних, що дозволяють підвищити ефективність і скоротити витрати. Маршрутизатори з інтегрованими сервісами Cisco серії 2900 скорочують початкові капітальні витрати за рахунок розділення доставки програмного забезпечення і устаткування за допомогою додаткових сервісних модулів. Крім того, здатний активувати безліч функцій Cisco IOS і що дозволяє швидко розгортати нові сервіси. Cisco серії 2900 знижує витрати на розгортання і збільшує гнучкість. Платформа також пропонує підтримку багатьох існуючих модулів ISR. Архітектура Cisco 2900 включає джерела живлення з більш високим ККД, інтелектуальне управління живленням і повну підтримку Cisco EnergyWise в майбутньому. Cisco серії 2900 пропонує значні поліпшення продуктивності в порівнянні з ISR попереднього покоління. В цілому, Cisco 2900 Series пропонує безпрецедентну економію на сукупній вартості володіння і гнучкість мережі за рахунок інтелектуальної інтеграції безпеки, безпровідного зв'язку, уніфікованих комунікацій і сервісів додатків.

– Маршрутиразор Cisco 1941 Series

Він пропонує підвищений рівень інтеграції послуг з послугами даних, безпеки, безпровідного зв'язку і мобільності, що дозволяє підвищити ефективність і скоротити витрати. Cisco Services Ready Engine (SRE) забезпечує нову операційну модель, яка дозволяє понизити капітальні витрати (CapEx) і розгорнути різні сервіси додатків в міру необхідності в одному інтегрованому модулі обчислювальних сервісів. Cisco серії 1900 забезпечує розгортання в середовищах високошвидкісної глобальної мережі з одночасними послугами до 25 Мбіт/с. Мульти-гігабітная матриця забезпечує зв'язок між модулями з високою пропускною спроможністю без зниження продуктивності

маршрутизації. Розроблені для задоволення бізнес-вимог замовників, Cisco 1941 Series з модульною архітектурою пропонує діапазон продуктивності модульних інтерфейсів і послуг у міру зростання потреб вашої мережі. Модульні інтерфейси забезпечують підвищену пропускну спроможність, різноманітність варіантів підключення і відмовостійкість мережі. Cisco 1900 Series пропонує інтелектуальне управління живленням і дозволяє замовникові управляти живленням модулів залежно від часу доби. Інтеграція послуг і модульність на єдиній платформі, що виконує безліч функцій, оптимізує споживання сировини і енергії. Гнучкість платформи і постійний розвиток апаратних і програмних можливостей подовжують життєвий цикл продукту, знижуючи усі аспекти сукупної вартості володіння, включаючи використання матеріалів і енергії. Кожна платформа оснащена високоефективними джерелами живлення. Повторне використання широкого набору існуючих модулів, підтримуваних початковими маршрутизаторами з інтегрованими сервісами, забезпечує нижчу вартість володіння.

– Switch Cisco Catalyst 3560-CG Series

Cisco Catalyst компактні перемикачі, які легко розширюють інтелектуальну, повністю керовану інфраструктуру дротяної комутації Cisco Catalyst, включаючи наскрізний IP і мережеві сервіси без меж з одним кабелем Ethernet або оптоволокном. Підтримка розширеної безпеки і послуг, включаючи голосовий зв'язок, відео і послуги Cisco Borderless Network, до видалених кінцевих точок. Наскрізне живлення через Ethernet (PoE) дозволяє компактному комутатору отримувати живлення від комутаційної шафи і передати його кінцевим пристроям. Привабливий, компактний форм-фактор підходять для обмеженого простору, де може бути прокладені декілька кабелів. Простота розгортання, управління і розширення мережі без петель.

3 ІНФОРМАЦІЙНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ

3.1 Налаштування консольного серверу за допомогою програмного додатку Cisco Packet Tracer

Для реалізації налаштування консольного серверу у програмному додатку Cisco Packet Tracer я використала дане обладнання:

– PC (персональний компьютер с IP-адресою 192.168.0.100);

– Router 2901 (с IP-адресою 192.168.0.1), який буде виступати у ролі серверу (рис.3.1);

Перед підключенням та налаштуванням потрібно вставити картку HWIC-8A.

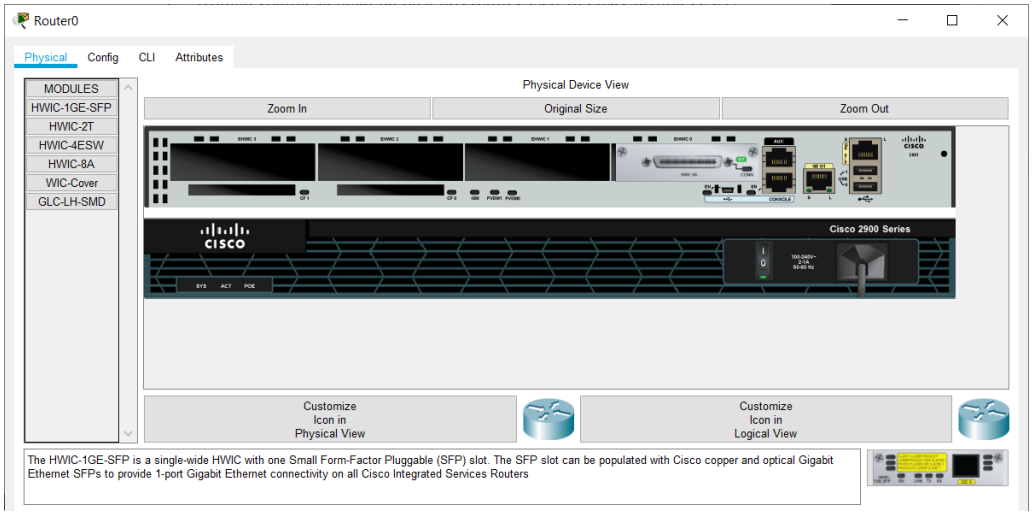


Рисунок 3.1 — вид фізичного пристрою Router 2901

– Switch 2960, який буде виступати першим віддаленим пристроєм (рис.3.2);

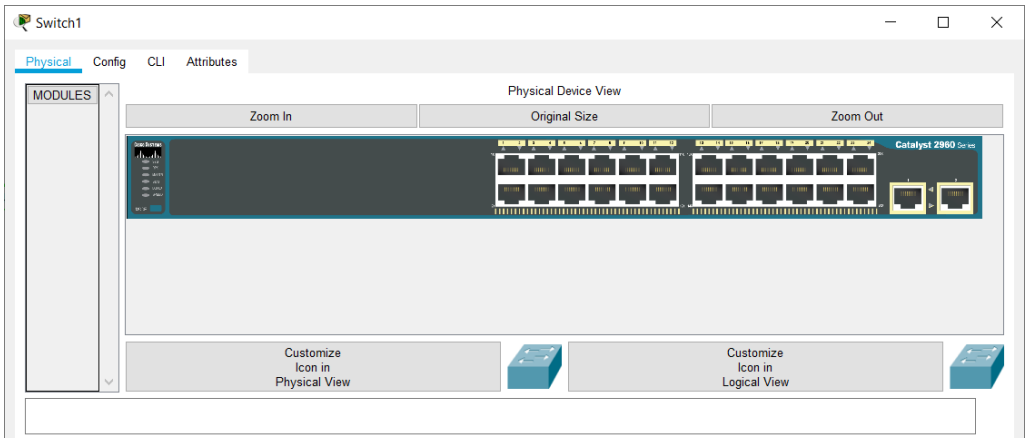


Рисунок 3.2 — вид фізичного пристрою Switch 2960

– Router 1941, який буде виступати другим віддаленим пристроєм (рис.3.3).

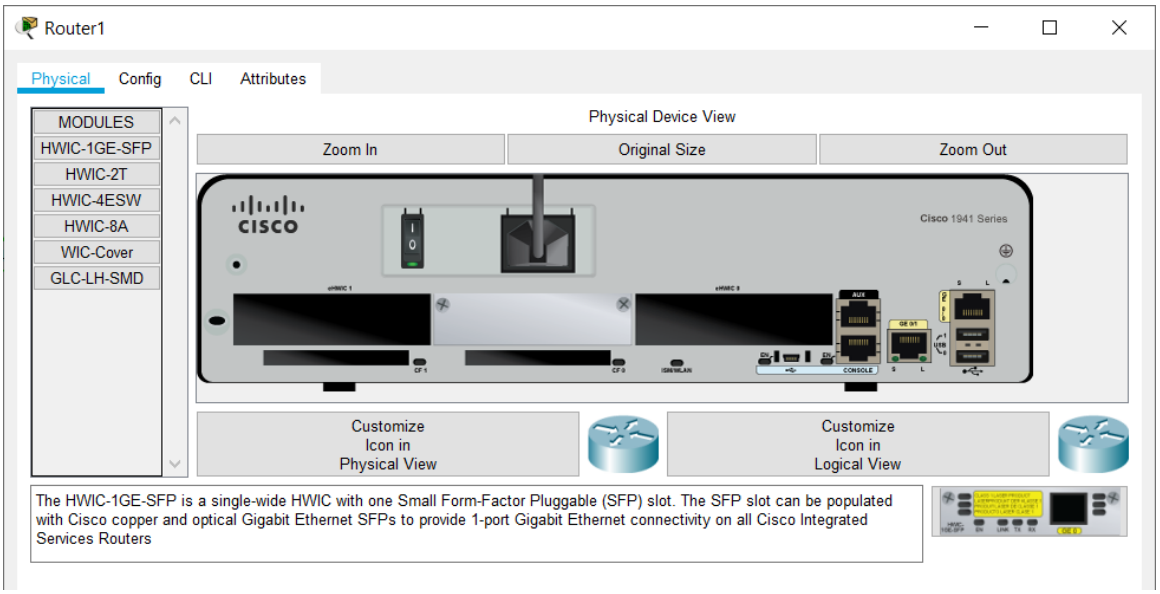


Рисунок 3.3 — вид фізичного пристрою Router 1941

У результаті підключення пристроїв я отримала наступну схему, яка зображена на рисунку 3.4 :

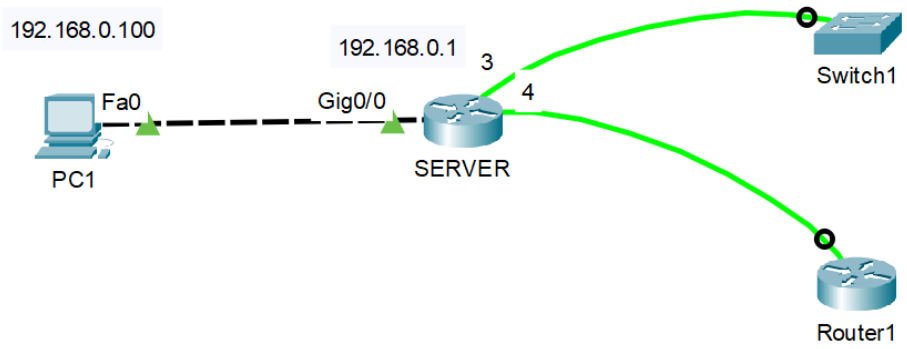


Рисунок 3.4 — схема налаштування консольного серверу у програмному додатку Cisco Packet Tracer

Прописавши команди (рис.3.5) успішно налаштувала SERVER для віддаленого доступу з PC1 до Router1 та Switch1 за допомогою протоколу SSH.

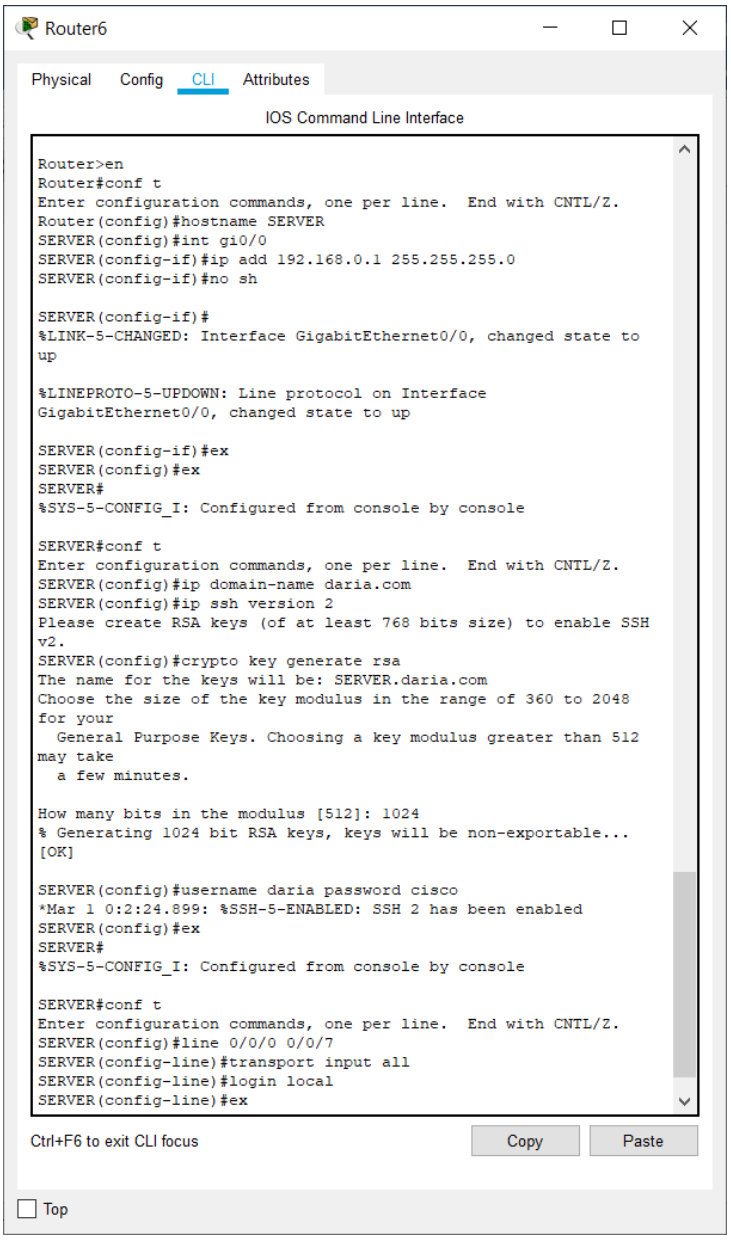


Рисунок 3.5 — командий рядок інтерфейсу SERVER

Зайшовши до командного рядку PC перевірила правильність налаштування віддаленого доступу спочатку під’єднавшись до 3 лінії (рис.3.6) за допомогою команди:

ssh –l daria:3 192.168.0.1

Password: cisco

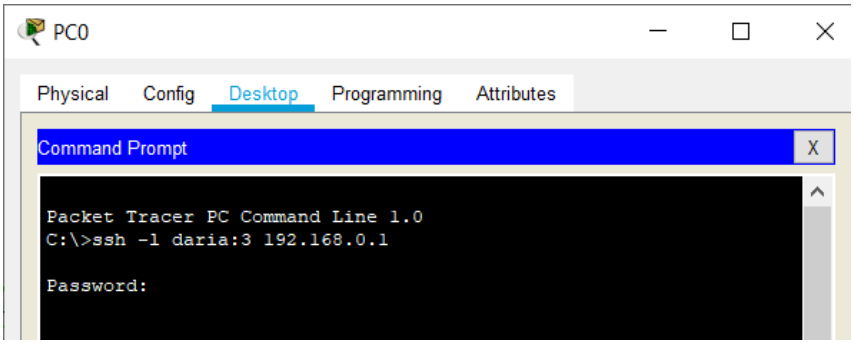


Рисунок 3.6 — перевірка підключення до Switch у командному рядку PC

У результаті отримала доступ до Switch через PC (рис.3.7). Отже, виконали все правильно.

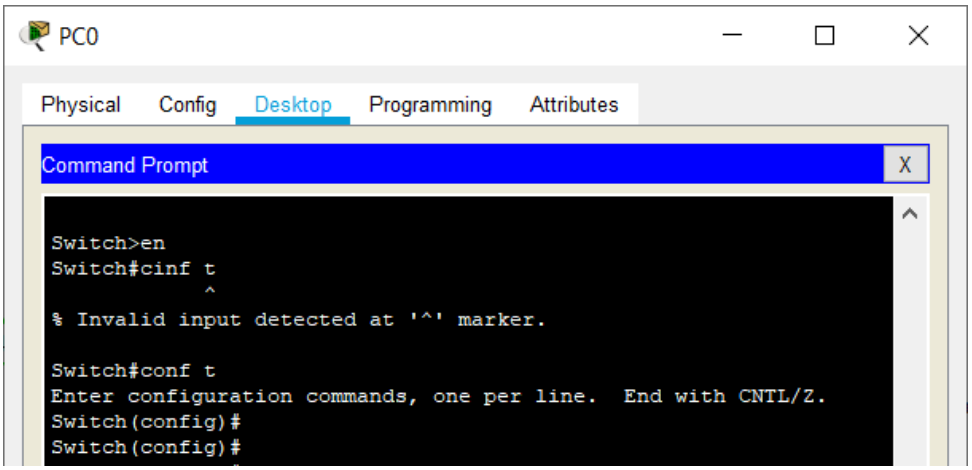


Рисунок 3.7 — віддалений доступ до Switch з командного рядка PC

Повторила перевірку з 4 лінією, та у результаті отримала доступ до Router (рис.3.8-3.9).

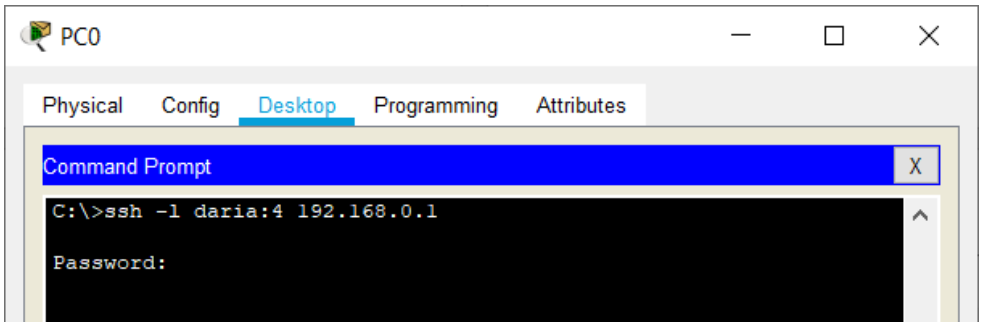


Рисунок 3.8 — перевірка підключення до Router у командному рядку PC

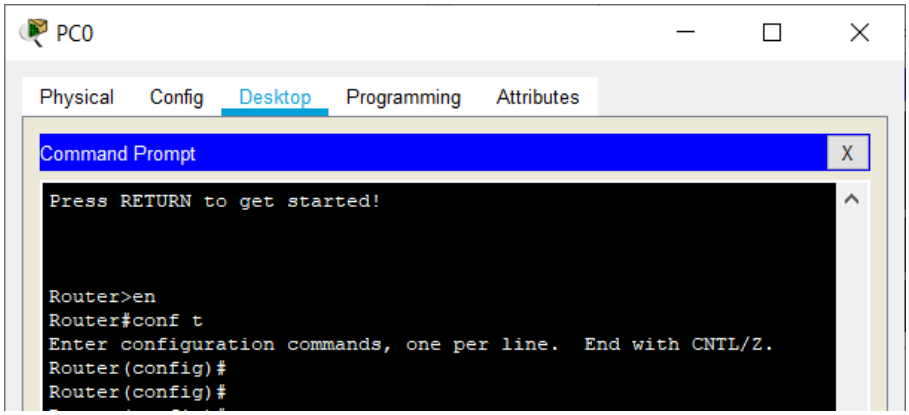


Рисунок 3.9 — віддалений доступ до Switch з командного рядка PC

3.1 Налаштування консольного серверу за допомогою реального обладнання Cisco

Для налаштування я використовувала обладнання:

- Маршрутиразор Cisco 2900 Series (рис.3.10-3.11);
- Маршрутиразор Cisco 1941 Series (рис.3.12-3.13);
- Switch Cisco Catalyst 3560-CG Series (рис.3.12-3.13);
- PC (рис.3.14).

Рисунок 3.10 — Cisco 2900 Series

Рисунок 3.11 — Cisco 2900 Series

Рисунок 3.12 — Cisco 1941 Series та Switch Cisco Catalyst 3560-CG Series

Рисунок 3.13 — Cisco 1941 Series та Switch Cisco Catalyst 3560-CG Series

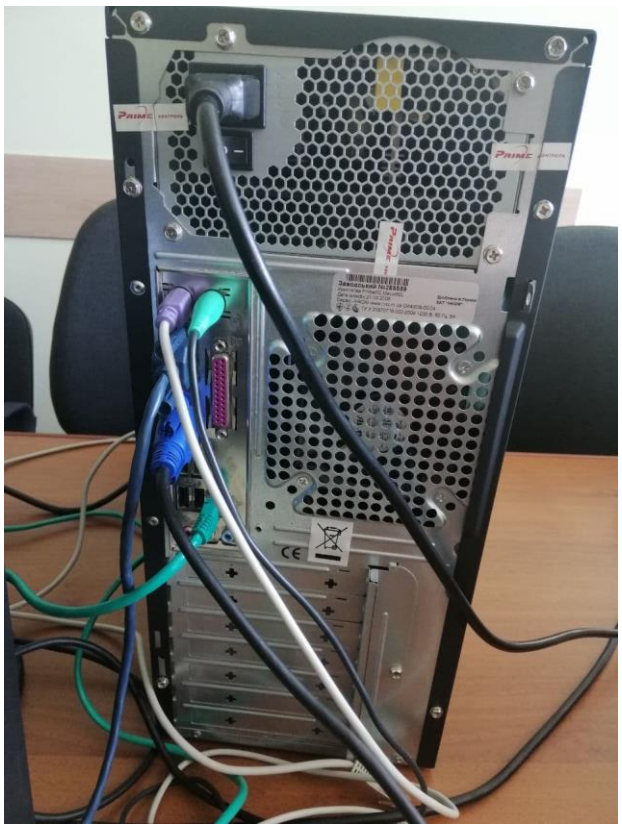


Рисунок 3.14 — PC

Для зв'язку з сервером на PC я використовувала Putty. Це безкоштовна програма для підключення до сервера через безпечне з'єднання SSH, Telnet, TCP або rlogin. Тобто, це тільки своєрідна оболонка, що відповідає за відображення: робота виконується на стороні віддаленого вузла. Вона застосовується для

передачі команд серверу. Відбувається це приблизно за наступною схемою: ви підключаєтеся до сервера за допомогою налагодженої Putty, вводите в рядок команду, сервер її виконує.

Для початкового налаштування протоколу SSH у PuTTY Configuration обрала Connection type: Serial (рис.3.15). Тобто з'єднання здійснюється через консольний кабель.

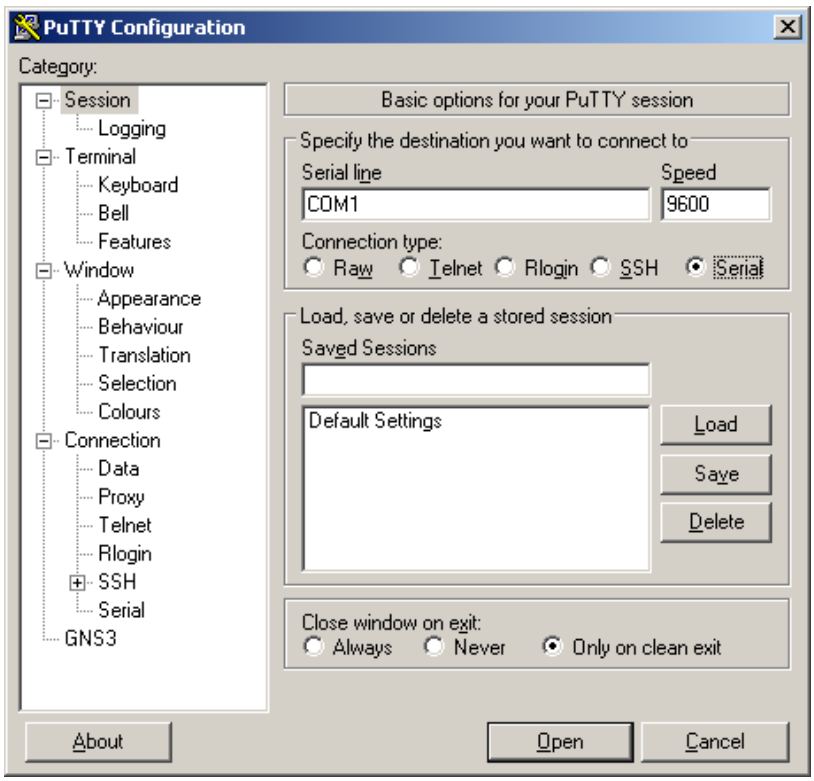


Рисунок 3.15 — початкове налаштування протоколу SSH у PuTTY Configuration

Вхід до привілейованого режиму роутеру:

Router>en

Вхід до режиму конфігурації:

Router#conf t

Команда для задання ім’я роутеру(у нашому випадку «SERVER»):

Router(config)#hostname SERVER

Конфігурація порту gi0/0, до якого підключений PC:

SERVER(config)#int gi0/0

SERVER(config-if)#ip add 192.168.0.1 255.255.255.0

Команда для вмикання інтерфейсу:

SERVER(config-if)#no sh

Вихід з режиму конфігурації:

SERVER(config-if)#ex

SERVER(config)#exit

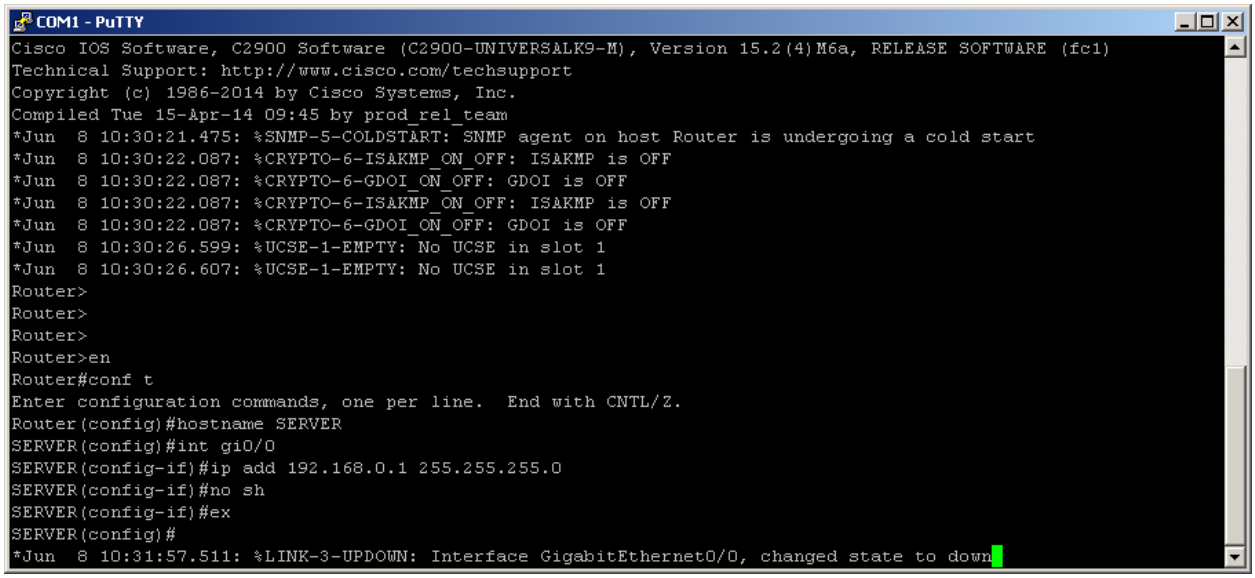


Рисунок 3.16 — командний рядок PuTTY

Налаштування параметри, які будуть необхідні для генерації ключа протокола SSH (рис.3.17):

Команда для встановлення поточних дату та час:

SERVER#clock set 15:00:00 15 May 2021

Вхід до режиму конфігурації:

SERVER#configure terminal

Команда, яка задаєму назву домену (у моєму випадку daria.ua):

SERVER(config)#ip domain name daria.ua

Генерація RSA ключ для протоколу SSH (вказуємо значення 1024):

SERVER(config)#crypto key generate rsa

Команда для задання версії SSH:

SERVER(config)#ip ssh version 2

Команда, де прописується кількість спроб підключення по протоколу SSH:

SERVER(config)#ip ssh authentication-retries 2

Зберігання паролів у зашифрованому вигляді:

SERVER(config)#service password-encryption

Вмикання протокол AAA:

SERVER(config)#aaa new-model

Створення користувача daria з максимальним рівнем привилегій (15) та паролем cisco:

SERVER(config)#username daria privilege 15 secret cisco

Задання паролю для привілейованого режиму:

SERVER(config)#enable secret cisco

Команда для доступу по протоколу SSH тільки з певної мережі:

SERVER(config)#access-list 23 permit 192.168.0.0 0.0.0.255

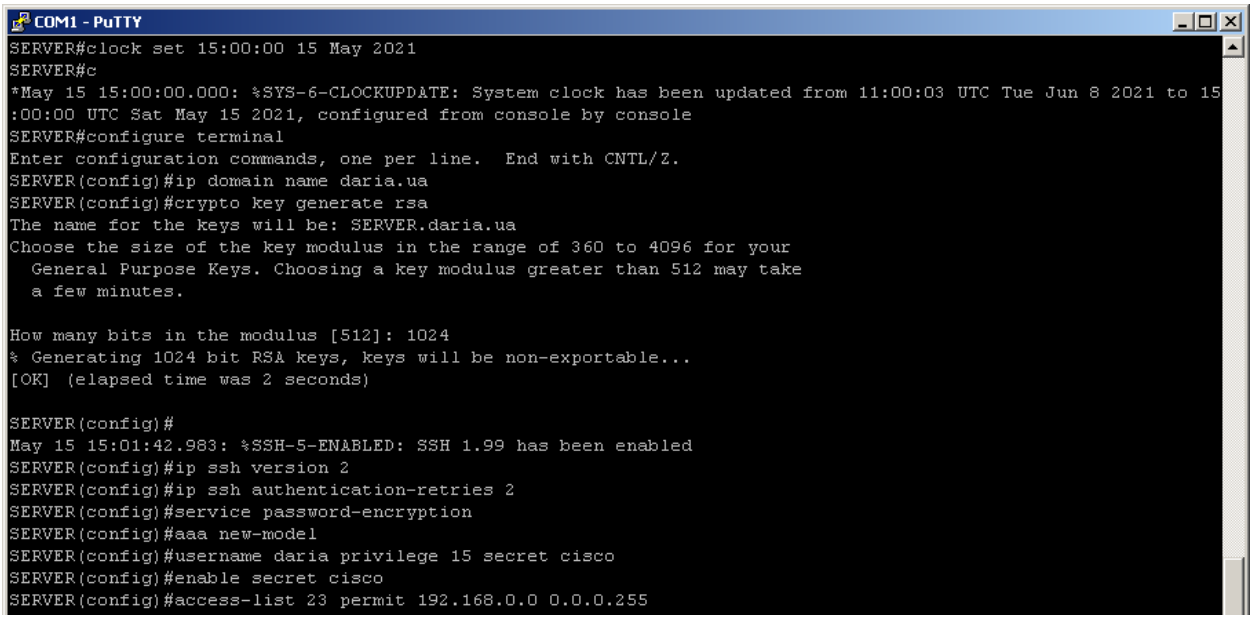


Рисунок 3.17 – командний рядок PuTTY

Вхід до режиму конфігурації термінальної лінії:

SERVER(config)#line vty 0 15

Команда, яка дозволяє доступ лише по протоколу SSH:

SERVER(config-line)#transport input ssh

Команда logging synchronous для того, щоб марштуризатор чекав завершення поточної команди та виводу звіту про виконання на екран. Вона необхідна, бо за замовченням журнальні повідомлення можуть виводитися в незалежності від того вводить користувач будь-які команди чи ні, перериваючи виконання поточних.

SERVER(config-line)#logging synchronous

Команда, яка дозволяє заходити одразу до привілейованого режиму:

SERVER(config-line)#privilege level 15

Команда, що вмикає автоматичне закриття сесії SSH через 30 хвилин:

SERVER(config-line)#exec-timeout 30 0

Команда, яка прив'язує групу доступу до термінальної лінії:

SERVER(config-line)#access-class 23 in

Вихід з режиму конфігурації:

SERVER(config-line)#end

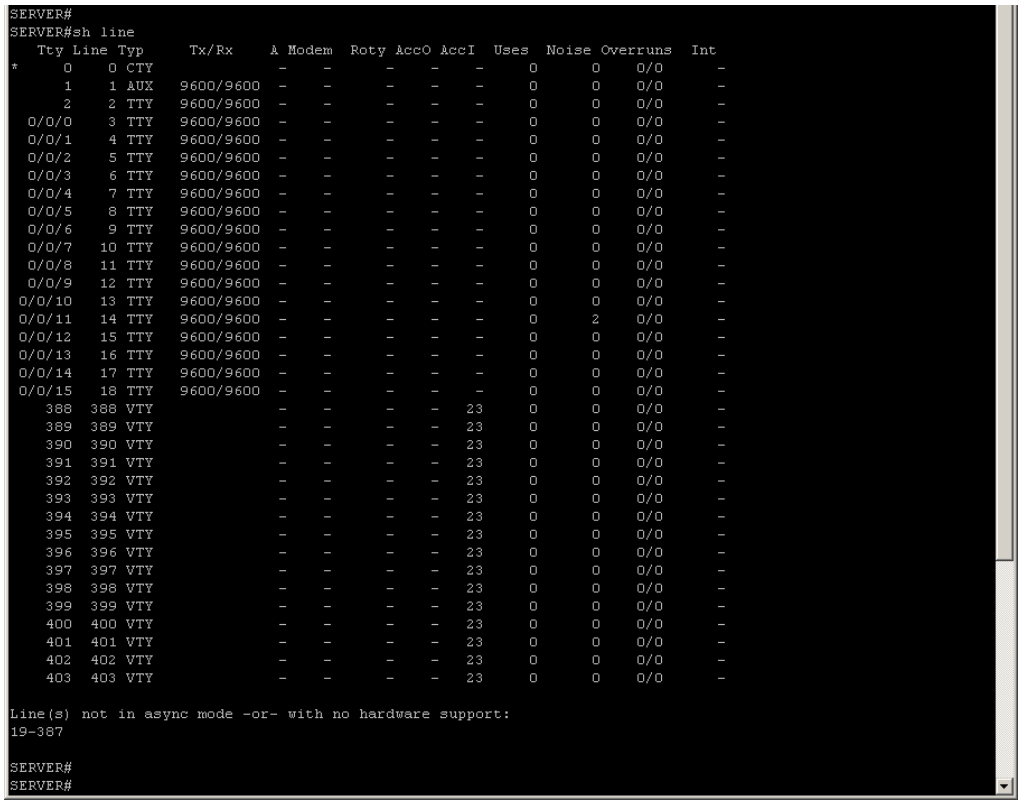
Збереження:

SERVER#copy running-config srartup-config

Рисунок 3.18 – командний рядок PuTTY

Команда, яка показує інформацію про лінії-інтерфейси:

SERVER#sh line



```
SERVER#
SERVER#sh line
   Tty Line Typ     Tx/Rx    A Modem  Roty AccO AccI  Uses  Noise Overruns  Int
*     0    0 CTY              -    -      -    -    -     0      0    0/0      -
      1    1 AUX    9600/9600 -    -      -    -    -     0      0    0/0      -
      2    2 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
  0/0/0    3 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
  0/0/1    4 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
  0/0/2    5 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
  0/0/3    6 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
  0/0/4    7 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
  0/0/5    8 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
  0/0/6    9 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
  0/0/7   10 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
  0/0/8   11 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
  0/0/9   12 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
 0/0/10   13 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
 0/0/11   14 TTY    9600/9600 -    -      -    -    -     0      2    0/0      -
 0/0/12   15 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
 0/0/13   16 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
 0/0/14   17 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
 0/0/15   18 TTY    9600/9600 -    -      -    -    -     0      0    0/0      -
   388  388 VTY              -    -      -    -   23     0      0    0/0      -
   389  389 VTY              -    -      -    -   23     0      0    0/0      -
   390  390 VTY              -    -      -    -   23     0      0    0/0      -
   391  391 VTY              -    -      -    -   23     0      0    0/0      -
   392  392 VTY              -    -      -    -   23     0      0    0/0      -
   393  393 VTY              -    -      -    -   23     0      0    0/0      -
   394  394 VTY              -    -      -    -   23     0      0    0/0      -
   395  395 VTY              -    -      -    -   23     0      0    0/0      -
   396  396 VTY              -    -      -    -   23     0      0    0/0      -
   397  397 VTY              -    -      -    -   23     0      0    0/0      -
   398  398 VTY              -    -      -    -   23     0      0    0/0      -
   399  399 VTY              -    -      -    -   23     0      0    0/0      -
   400  400 VTY              -    -      -    -   23     0      0    0/0      -
   401  401 VTY              -    -      -    -   23     0      0    0/0      -
   402  402 VTY              -    -      -    -   23     0      0    0/0      -
   403  403 VTY              -    -      -    -   23     0      0    0/0      -

Line(s) not in async mode -or- with no hardware support:
19-387

SERVER#
SERVER#
```

Рисунок 3.19 – командний рядок PuTTY

З рисунку 3.19 бачимо, що маємо інтерфейси з 0 по 15. Наші роутери знаходяться під номерами 4 та 5, тому звертатися по протоколу SSH потрібно вказуючи саме їх.

Вхід до режиму конфігурації:

SERVER#conf t

Команда, що відкриває інтерфейси з 0 по 7:

SERVER(config)#line 0/0/0 0/0/7

Команда для управління того, які протоколи може підтримувати маршрутизатор на своїх vty-лініях (у нашому випадку усі, як Telnet, так і SSH):

SERVER(config-line)#transport input all

Команда для перевірки логіну і паролю при вході:

SERVER(config-line)#login local

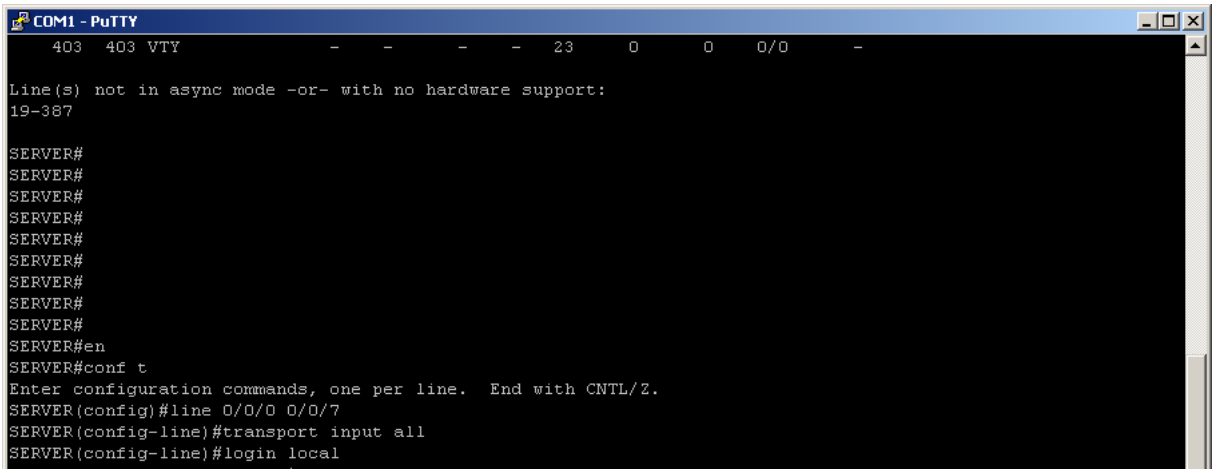


Рисунок 3.20 – командний рядок PuTTY

Для подального віддаленого доступу до обладнання по протоколу SSH у PuTTY Configuration потрібно було обрати Connection type: SSH та прописати IP address нашого серверу, через який і буде здійснюватися доступ, тобто 192.168.0.1. (рис.3.21).

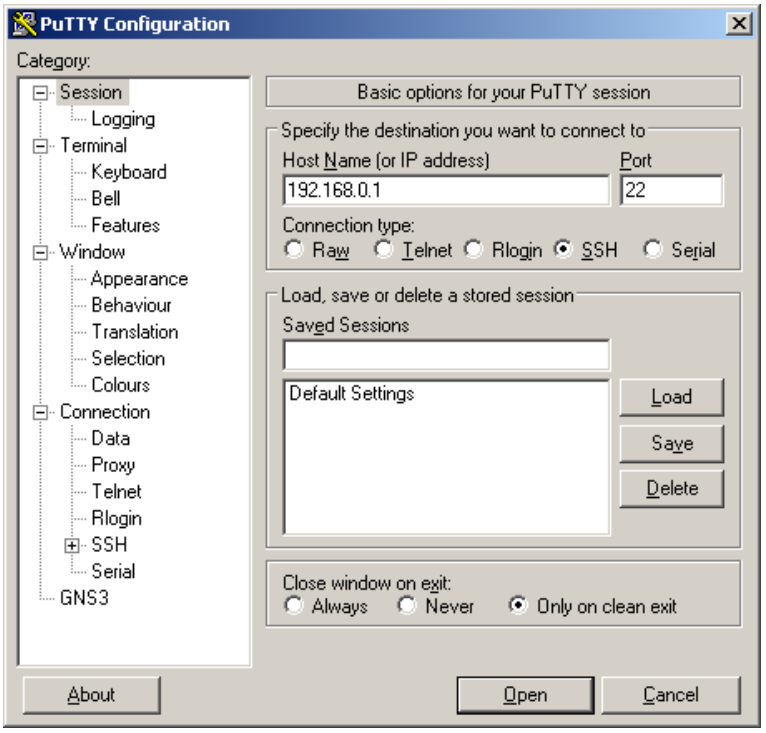


Рисунок 3.21 — PuTTY Configuration

У консолі прописала login, номер лінії, до якої підключений роутер та пароль:

login as: daria:4

password: cisco (при записі паролю він не відображається)

Якщо логін і пароль було введено правильно ми отримуємо доступ до Router (рис.3.22).

Вхід до привілейованого режиму роутеру:

Router>en

Вхід до режиму конфігурації:

Router#conf t

Команда для задання ім’я роутеру:

Router(config)#hostname Router4

Вихід з режиму конфігурації:

Router4(config)#ex

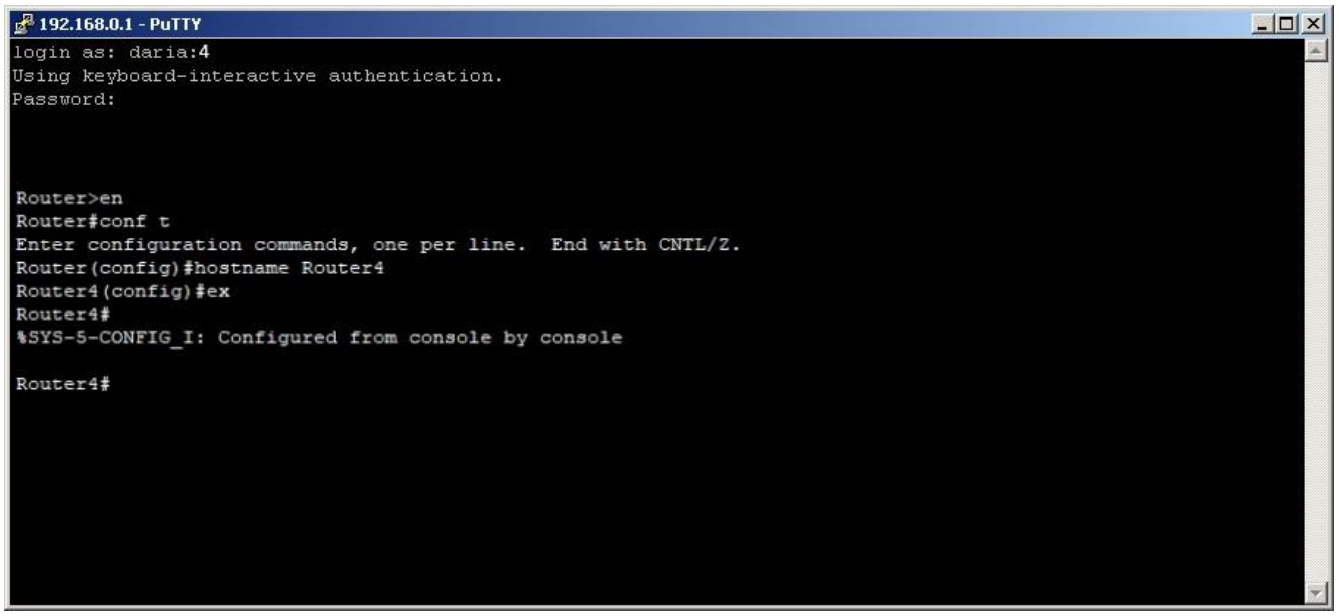


Рисунок 3.22 – командний рядок PuTTY

Так само отримала доступ до Switch (рис.3.23).

login as: daria:5

password: cisco

Вхід до привілейованого режиму роутеру:

Switch>en

Вхід до режиму конфігурації:

Switch#conf t

Команда для задання ім’я роутеру:

Router(config)#hostname Router5

Вихід з режиму конфігурації:

Router5(config)#ex

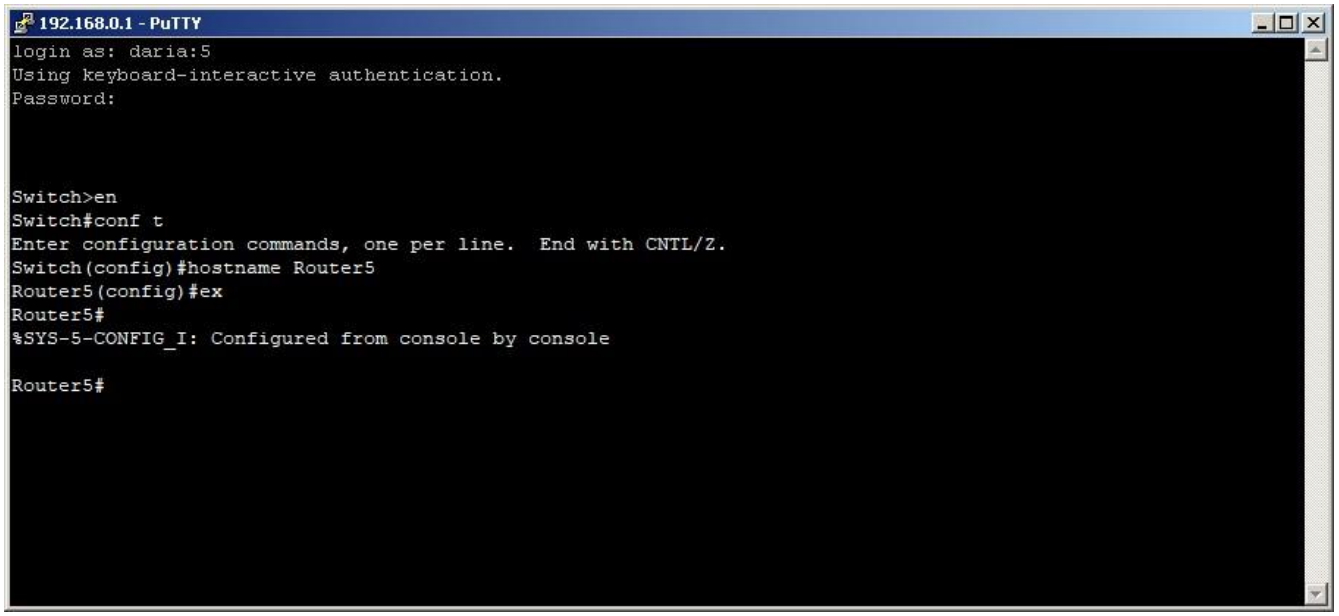


Рисунок 3.23 – командний рядок PuTTY

Для закриття сессії на роутері SERVER треба прописати наступні команди:

Вхід до привілейованого режиму роутеру:

SERVER>en

Команда, де вказано номер лінії, через яку підключені до роутеру по віддаленому доступу:

SERVER#clear line tty 4

Отже, у результаті перевірок роботи консольного серверу, можна дійти висновку, що налаштування проведені вірно, ми маємо віддалений доступ до Router та Switch з консольного рядка нашого PC.

ВИСНОВКИ

Висновки до випускої роботи можна сформувати наступним чином:

Проаналізувавши зібрану літературу, з’ясовано принцип роботи, методи підключення, налаштування віддаленого доступу у телекомунікаційних мережах.

Було виконане порівняння двох основних способів управління мережею:

- внутрішньосмугове управління мережею;
- позасмугове управління.

Проведено аналіз позитивних сторонін використання Out-of-band management та трьох основних способів управління.

Були з’ясовані принципи налаштування мережі віддаленого доступу з використанням консольного серверу.

Порівнявши 3 найпопулярніші методи консольного підключення, а саме SSH, Telnet та Dial-up, було встановлено, що для практичного використання на сьогоднішній день найбільше підійде SSH-протокол, саме через високий рівень надання безпеки він є переважним протоколом для загальнодоступних мереж.

Також було розглянуто основні переваги та можливості симулятору Cisco Packet Tracer та обладннання, яке використовувалось у подальшому.

У рамках роботи було створено схему налаштування консольного серверу за допомогою симулятору мережі передачі данних Cisco Packet Tracer, яка б максимально відтворювала реальне налашування консольного серверу.

На основі створеної схеми здійснено підключення та налаштування мережі віддаленого доступу з використанням консольного серверу на реальному обладнанні Cisco.

СПИСОК ЛІТЕРАТУРИ

1. Бабчук С. М. Мережеві інформаційні технології : конспект лекцій / С. М. Бабчук // Івано-Франківськ : ІФНТУНГ, 2016. - 73 с.

2. Способи здійснення віддаленого адміністрування. Знахідка для віддаленого адміністрування [Електронний ресурс].-Режим доступу: https://qipu.ru/uk/mobilnye-sovety/sposoby-osushchestvleniya-udalennogo-administrirovaniya-nahodka-dlya.html.

3. Основні інструменти адміністрування Windows. Що таке віддалене адміністрування? Способи здійснення віддаленого адміністрування [Електронний ресурс].-Режим доступу: https://school38vrn.ru/uk/osnovnye-instrumenty-administrirovaniya-windows-chto-takoe-udalennoe-administrirovanie-sposoby-osushche.html.

4. Кулаков О.Ю., Берест Р.Ю. Комп’ютерні мережі 1.Локальні комп’ютерні мережі. Методичні вказівки до комп’ютерного практикуму / Кулаков О.Ю., Берест Р.Ю. // Київ : НТУУ «КПІ», 2018. – 80 с.

5. Борян Л. О. КОМП'ЮТЕРИ ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ. Курс лекцій / Борян Л. О. // Миколаїв, 2019. – 106 с.

6. Олещенко Л. М. Організація компьютерних мереж. Конспект лекції / Олещенко Л. М. // Київ : КПІ ім. Ігоря Сікорського, 2018. – 140 с.

7. Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А. Навчальний посібник з дисципліни «Комп’ютерні мережі» / Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А.// Київ : Комппрінт, 2017. – 266 с.

8. Сервер послідовних інтерфейсів [Електронний ресурс].-Режим доступу: https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80_%D0%BF%D0%BE%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D1%85_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81%D0%BE%D0%B2.

9. Купін А. І., Музика І. О. Мережні інформаційні технології. Практикум / Купін А. І., Музика І. О. // Кривий Ріг : : Видавець ФО-П Чернявський Д. О., 2015. – 154 с.

10. Що таке Telnet [Електронний ресурс].-Режим доступу: https://uk.photo-555.com/2633878-what-is-telnet.

11. Майкл Лукас Майстерність SSH: OpenSSH, PuTTY, тунелі і ключі // Майкл Лукас / Tilted Windmill Press, 2018. – 145 с.

12. SSH [Електронний ресурс].-Режим доступу: https://ru.wikipedia.org/wiki/SSH.

13. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 302-305 с.