ЗАТВЕРДЖЕНО

Науково-методичною радою
Державного університету
«Житомирська політехніка»

протокол від _09_ _11__ 2020 р.
№_4_

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
для проведення практичних занять з навчальної дисципліни «Захист інформації в телекомунікаційних системах»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 172 «Телекомунікації та радіотехніка»
освітньо-професійна програма «Телекомунікації та радіотехніка»
факультет інформаційно-комп'ютерних технологій
кафедра біомедичної інженерії та телекомунікацій

Схвалено на засіданні кафедри біомедичної інженерії та телекомунікацій
31 серпня 2020 р., протокол № 9

Завідувач кафедри
_____ Тетяна НІКІТЧУК

Розробник: к.т.н., доц. кафедри біомедичної інженерії та телекомунікацій
ДУБИНА Олександр

Житомир
2021 – 2022 н.р.

Вступ

Методичні рекомендації призначені для проведення практичних робіт з навчальної дисципліни «Захист інформації в телекомунікаційних системах».

Дисципліна складається з двох змістовних модулів: сучасні загрози мережевої безпеки, комплексна політика безпеки.

Під час проведення занять кожний студент повинен самостійно провести дослідження у відповідності до поставленого завдання на апаратних засобах, скласти звіт у письмовому вигляді і захистити його у викладача.

Практична робота № 1

БАЗОВІ ШИФРИ. ЧАСТОТНИЙ КРИПТОАНАЛІЗ

Мета роботи: ознайомитися з базовими шифрами. Розглянути методику частотного криптоаналізу.

Використовуване програмне забезпечення: середа розробки GNU Octave.

1.1 Теоретичні відомості

В криптографії здавна використовувались два види шифрів: заміна та перестановка. Історичним прикладом шифру заміни є шифр Цезаря. Його сутність така: в строку виписується алфавіт, після чого під ним виписується той же алфавіт з циклічним зсувом на 3 букви вліво.

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЄЮЯ
ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЄЮЯАБВ

При зашифруванні буква відкритого тексту замінюється на букву, що знаходиться під нею в нижній строчці. Наприклад: РИМ – УЛП. Ключем в шифрі Цезаря є величина здвигу нижньої строки.

1.1.1 Шифр простої заміни

Подальший розвиток шифру Цезаря є очевидним: нижня строчка може бути записана з випадковим порядком букв. Такий шифр носить назву шифру простої заміни. Ключем такого шифру є порядок розташування букв в нижній строчці, так звана «таблиця заміни». Якщо в шифрі Цезаря існує тільки 33 варіанта ключів, то в шифрі простої заміни їх вже 33! (33 факторіал).

1.1.2 Квадрат Полібія

Одна з відомих модифікацій шифру простої заміни – квадрат Полібія. Візьмемо алфавіт з 32 букв. Виберемо ключ – будь-яке слово, в якому немає однакових букв. Запишемо його в перші клітинки квадрата розміром, наприклад, 4×8. В останні клітинки запишемо алфавіт за віднятком тих букв, що зустрічаються в ключі. Для зашифрування букви повідомлення замінюються на букви, що стоять *під* ними в квадраті Полібія. Наприклад:

Ключ – «**САВКОМ**».

Повідомлення – «**НЕЛЬЗЯ ПОМОЧЬ ТОМУ, КТО НЕ ЖЕЛАЕТ СЛУШАТЬ СОВЕТОВ**».

На рис. 1.1 представлено Квадрат Полібія для ключа «**САВКОМ**».

С	**А**	**В**	**К**
О	**М**	Б	Г
Д	Є	Ж	З
И	И	Л	Н
П	Р	Т	У
Ф	Х	Ц	Ч
Ш	Щ	І	І
Ь	Е	Ю	Я

Рисунок 1.1 – Квадрат Полібія

Зашифроване повідомлення:

«**УЙТМНКФАВАЪМЦАВЧГЦАУЙЛЙТЕЙЦБТЧЬЕЦМБАДЙЦАД**».

Для розшифрування букви шифротексту замінюються на ті букви, що стоять *над* ними в квадраті Полібія.

1.1.3 Шифр перестановки

Оберемо ціле додатне число, наприклад, 5. Створимо випадкову підстановку:

$$\begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,2\,5\,1\,4 \end{pmatrix}$$

Зашифруємо фразу:

«БАЖАЄШ БАГАТО ЗНАТИ, ТРЕБА МЕНШЕ СПАТИ».

Для цього доповнимо фразу до довжини кратної 5 випадковими символами та розіб’ємо на групи по 5 букв.

БАЖАЄ ШБАГА ТОЗНА ТИТРЕ БАМЕН ШЕСПА ТИВСЕ

Букви кожної групи переставимо згідно обраної підстановки.

Отриманий текст запишемо без пропусків.

«ААБЄЖГБШААНОТАЗРИТЕТЕАБНМПЕШАССИТЕВ»

При розшифруванні текст розбивається на групи по 5 букв і букви переставляються в зворотному порядку. Ключом шифру є степінь підстановки (тут 5) і порядок розташування чисел в нижньому рядку підстановки.

1.1.4 Шифр Тритемія

В XV столітті абат Тритемій (Германія) запропонував шифр на основі “таблиці Тритемія”. Для російського алфавіту вона має наступний вигляд:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЄЮЯ
БВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯА
ВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБ
ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВ
ДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГ
ЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГД
ЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕ
ЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁ
ЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖ
ИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗ
ЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИ
КЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙ
ЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙК
МНОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛ
НОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМ
ОПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМН
ПРСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНО
РСТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОП
СТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПР
ТУФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРС
УФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТ
ФХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУ
ХЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФ
ЦЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХ
ЧШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦ
ШЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧ
ЩЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШ
ЫЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩ
ЪЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫ
ЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪ
ЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬ
ЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭ
ЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮ

Рисунок 1.2 – Таблиця Тритемія для російського алфавіту

Тут перша строчка є одночасно і строчкою букв відкритого тексту. Перша буква тексту шифрується по першій строчці, друга – по другій і т.д. Після останньої строчки знову повертаємось до першої. Наприклад, слово "**КРИПТОГРАФИЯ**" зміниться на "**КСКТЦУИЧЗЭТЙ**". Однак, в такому варіанті, в шифрі Тритемія був відсутній ключ. В подальшому удосконалення шифру пішли по двом шляхам:

- введення випадкового порядку розташування букв алфавіту;
- застосування більш складного порядку вибору строк таблиці при шифруванні (по ключу).

1.1.5 Частотний крипто аналіз

Частотний криптоаналіз базується на застосуванні статистики для аналізу текстової інформації. Текст складається із слів, слова із літер. Кількість літер в кожній мові обмежена. Важливими характеристиками тексту є повторюваність літер, пар літер (біграм) і , взагалі, m-грам, поєднання літер друг с другом, чередування голосних і приголосних і т.д. Всі ці характеристики є достатньо стійкими і можуть бути використані для аналізу шифртекстів. В табл. 1.1 та 1.2 приведені однобуквені ймовірності англійської та російської мов.

Таблиця 1.1 - Однобуквені ймовірності англійської мови

Літера	Імовірність	Літера	Імовірність
A	0.0856	N	0.0707
B	0.0139	0	0.0797

C	0.0279	P	0.0199
D	0.0378	Q	0.0012
E	0.1304	R	0.0677
F	0.0289	S	0.0607
G	0.0199	T	0.1045
H	0.0528	U	0.0249
I	0.0627	V	0.0092
J	0.0013	W	0.0149
K	0.0042	X	0.0017
L	0.0339	Y	0.0199
M	0.0249	Z	0.0008

Таблиця 1.2 - Однобуквені ймовірності російської мови

Літера	**Імовірність**	**Літера**	**Імовірність**	**Літера**	**Імовірність**
А	0,062	К	0,028	Ф	0,002
Б	0,014	Л	0,035	Х	0,009
В	0,038	М	0,026	Ц	0,004
Г	0,013	Н	0,053	Ч	0,012
Д	0,025	О	0,090	Ш	0,006
Е	0,072	П	0,023	Щ	0,003
Ж	0,007	Р	0,040	Ы	0,016
З	0,016	С	0,045	Ь,Ъ	0,014
И	0,062	Т	0,053	Э	0,003
И	0,010	У	0,021	Ю	0,006
				Я	0,018

Процес криптоанализу можна представити наступним чином. Криптоаналітик підраховує частоти букв в шифротексті. Далі він бере в шифртексті символ, що зустрічається найбільш часто, и припускає, що це пробіл. Потім бере наступний символ, що зустрічається найбільш часто, и припускає, що це Е (для англійскої мови), и т.д. Шляхом проб і помилок такий метод може привести до рішення задачі. Крім того, при підставленні букв замість символів аналізованого шифртексту криптоаналітик враховує частоти появи сполучень із двох букв (діаграм), трьох букв (триграмм) і т.д.

1.2 Завдання на лабораторну роботу

1.2.1 Розробити програми шифрування та розшифрування наступними шифрами:

- шифр простої заміни;
- квадрат Полібія;
- шифр перестановки;
- шифр Тритемія з вибором строк по ключу;

(У якості ключа або сова, що аналізується, використовувати власне ім’я.)

1.2.2 Виконати частотний криптоаналіз отриманих зашифрованих текстів.

1.3 Зміст звіту

1.3.1Титульний лист, тема і мета роботи.
1.3.2Відповіді на контрольні питання.
1.3.3Тексти програм.
1.3.4Обране повідомлення для шифрування.
1.3.5Обраний ключ.
1.3.6Зашифроване повідомлення.
1.3.7Розшифроване повідомлення.
1.3.8Результати проведення частотного криптоаналізу.

1.4 Контрольні питання

1.4.1Опишіть шифр Полібія.
1.4.2Опишіть шифр простої заміни.
1.4.3Опишіть шифр Тритемія.
1.4.4Опишіть шифр перестановки.
1.4.5Чи є шифр Полібія шифром простої заміни?
1.4.6Як залежить стійкість шифру від довжини ключа?
1.4.7Опишіть метод частотного криптоанализу.
1.4.8В яких випадках можна застосовувати метод частотного криптоанализу?

Практична робота № 2
КРИПТОГРАФІЯ З ВІДКРИТИМ КЛЮЧЕМ . ФУНКЦІЯ ҐЕШУВАННЯ

Мета роботи: ознайомитися з найпростішою функцією ґешування та схемами електронного цифрового підпису RSA та ElGamal.

Використовуване програмне забезпечення: пакети математичних обчислень MathCad і середа розробки GNU Octave.

3.1 Теоретичні відомості

3.1.1 Асиметричні криптосистеми

Ефективними системами криптографічного захисту даних є *асиметричні криптосистеми*. В таких системах для зашифрування даних використовується один ключ, а для розшифрування – інший. Причому ключі пов'язані між собою певним математичним співвідношенням, що робить можливим процес адекватного розшифрування. Концепція таких криптосистем основана на застосуванні однонаправлених функцій з секретом, що дозволяє легко отримати відкритий ключ із секретного, але не навпаки.

Двухключова криптографія використовується в двух схемах: *цифрового підпису* і *спрямованого шифрування*. В першому випадку повідомлення підписується закритим ключем і будь-яка особа може упевнитися в його дійсності за допомогою відкритого ключа. В схемі спрямованого шифрування, навпаки, повідомлення зашифровується на відкритому ключі отримувача. Розшифрувати повідомлення має можливість тільки сам отримувач за допомогою свого секретного ключа.

В протоколах цифрового підпису застосовується так звана «ґеш- функція».

Ґеш-функцією називається перетворення *H*, що переводить повідомлення M довільної довжини у повідомлення *H(M)* фіксованої довжини. Ґеш-функція повинна задовольняти таким вимогам:

- не вище чим поліноміальна складність обчислення значення ґеш-функції;
- не нижче чим експоненціальна складність визначення повідомлення *Mi* по відомому значенню *H(Mi)*;
- практична захищеність від колізій, коли можна знайти *Mi* та *Mj*, такі, що *H(Mi)=H(Mj)*, з імовірністю не вище чим *Pk*, де *Pk* завідомо задане значення.

3.1.2 Алгоритм RSA в схемі спрямованого шифрування

Алгоритм RSA запропонували у 1978 р. три автора Р.Райвест, А.Шамір, А.Адлеман. Стійкість алгоритму базується на складності факторизації великих чисел і трудності обчислення дискретних логарифмів.

Алгоритм RSA використовується в моделі взаємної недовіри. Її сутність полягає в тім, що кожен користувач генерує ключі сам собі. Особистий ключ залишає в себе і забезпечує його строгу конфіденційність. Відкритий ключ розсилає всім користувачам, з якими він зв'язаний. Він також забезпечує цілісність і дійсність відкритих ключів. Таким чином, будь-хто може надіслати йому повідомлення, зашифроване на відомому відкритому ключі, яке може прочитати тільки сам користувач, бо тільки він володіє відповідним секретним ключем.

3.1.3 Використовуючи відкритий $e = 7$ і закритий $d = 3$ ключі та модуль $n = 33$ схеми RSA, сформуйте та перевірте цифровий підпис для повідомлення.

«ВЫДАТЬ _ СТО _ ГРН _ ГЛБУХ _ [ФАМИЛИЯ]»,

Цифровий підпис представте в двійковому виді.

Сформуйте та перевірте цифровий підпис зформованого ґеш- образа за допомогою схеми ElGamal.

3.1.4 Для заданого повідомлення в двійковому виді,

00101011 10001000 11100001 10111010 00000000

01101000 01000000 11000100 10101101 01101001

01110011 01000000 01001000 00110100 00000101

01001100 00001100 10101001 00111010 00011001

- відокремліть повідомлення і цифровий підпис, створений за допомогою алгоритму RSA (5 біт);
- повідомлення і цифровий підпис представте у десятковому виді;
- за допомогою відкритого ключа $e = 17$ і модуля $n = 33$ розшифруйте цифровий підпис;
- сформуйте ґеш-образ відокремленого повідомлення;
- перевірте коректність поставленого підпису, порівнявши результати двох попередніх пунктів;
- прочитайте повідомлення.

3.2 Зміст звіту

3.2.1Титульний лист, тема і мета роботи.

3.2.2Відповіді на контрольні питання.

3.2.3Опис алгоритмів RSA та ElGamal.
3.2.4Тексти програм
3.2.5Результати розрахунків.

3.3 Контрольні питання

3.3.1Поняття криптографії з відкритим ключем.
3.3.2Поняття ґеш-функції. Її властивості.
3.3.3Модель взаємної недовіри.
3.3.4Загальна схема формування та перевірки цифрового підпису.
3.3.5Загальна схема спрямованого шифрування.
3.3.6Схема цифрового підпису RSA.
3.3.7Доказати математично коректність алгоритму RSA.
3.3.8Схема цифрового підпису ElGamal.
3.3.9Доказати математично коректність алгоритму ElGamal. 3.4.10Від чого захищає цифровий підпис? Яким чином?

Практична робота № 3

ЗАХИСТ КОМУТАТОРІВ І МАРШРУТИЗАТОРІВ

Мета роботи: Навчитися ставити парольний захист на комутатор і маршрутизатор на різні режими роботи.

Робота з програмним забезпеченням: CPT.

1. Теоретичні відомості

Мережеві пристрої можуть працювати в режимах, які поділяються на три великі категорії.

Перша і основна категорія-це передача даних (площину даних, data plane). Це режим роботи комутатора з передачі кадрів, що генеруються пристроями, підключеними до комутатора. Іншими словами, передача даних є основним режимом роботи комутатора.

По-друге, управління передачею даних відноситься до налаштувань і процесам, які керують і змінюють вибір, зроблений передає рівнем комутатора. Системний адміністратор може контролювати, які інтерфейси включені і відключені, які порти працюють з якою швидкістю, як сполучна дерево блокує деякі порти, щоб запобігти цикли, і так далі. Так само важливою частиною є управління пристроєм, здійснюване через площину спостереження (management plane). Площина спостереження - це управління самим пристроєм, а не управління тим, що робить пристрій.

Захист комутатора через CLI

За замовчуванням комутатор Cisco Catalyst дозволяє будь-якому користувачеві підключитися до консольного порту, отримати доступ до призначеного для користувача режиму, а потім перейти в привілейований режим без будь-якого захисту. Ці настройки задані в мережевих пристроях Cisco за замовчуванням і, якщо у вас є фізичний доступ до пристрою, то ви спокійно можете підключитися до пристрою через консольний порт або USB, використовуючи відповідний кабель і відповідно виробляти різні настройки.

Однак не завжди є фізичний доступ до комутатора і тоді необхідно мати доступ до пристроїв для віддаленого управління, і першим кроком в цьому процесі є забезпечення безпеки комутатора так, щоб тільки відповідні користувачі могли отримати доступ до інтерфейсу командного рядка комутатора (CLI).

Налаштування парольного доступу до комутатора Cisco

Захист CLI включає захист доступу в привілейований режим, оскільки з цього режиму зловмисник може перезавантажити комутатор або змінити конфігурацію.

Захист призначеного для користувача режиму також важлива, оскільки зловмисники можуть бачити настройки комутатора, отримати настройки мережі і знаходити нові способи атаки на мережу.

Особливо важливо, щоб всі протоколи віддаленого доступу і управління, щоб IP-налаштування комутатора були налаштовані і працювали.

Для того, щоб отримати віддалений доступ по протоколах Telnet і Secure Shell (SSH) до комутатора, необхідно на комутаторі налаштувати IP-адресацію.

Захист призначеного для користувача і привілейованого режиму за допомогою простих паролів.

Отримати повний доступ до комутатора Cisco можна тільки через консольний порт.

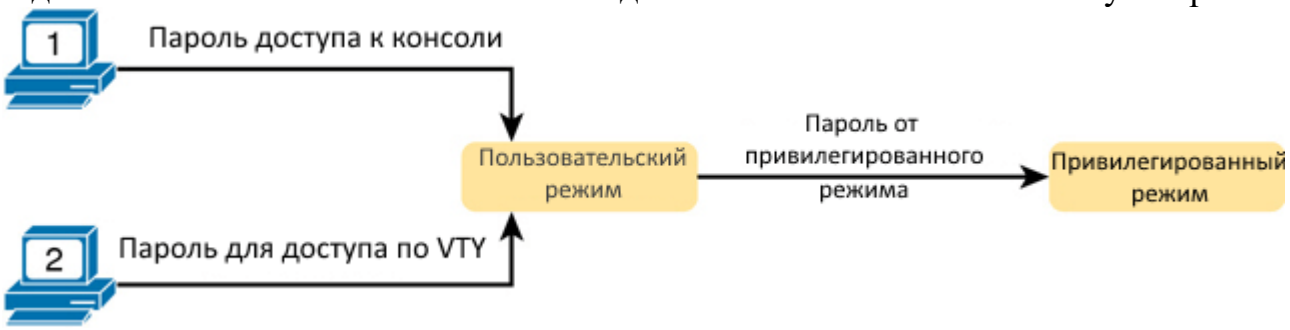
В цьому випадку, налаштування за замовчуванням, дозволяють отримати доступ спочатку до режиму користувача, а потім можна перейти в привілейований режим без використання паролів.

А ось по протоколам віддаленого доступу Telnet або SSH отримати доступ навіть до режиму користувача неможливо.

Налаштування за замовчуванням йдуть у зовсім нового комутатора, але у виробничому середовищі необхідно забезпечити безпечний доступ через консоль, а також включити віддалений вхід через Telnet і / або SSH, щоб була можливість підключатися до всіх комутаторів в локальній мережі.

Можна організувати доступ до мережного обладнання з використанням одного загального пароля.

Цей метод дозволяє підключитися до обладнання, використовуючи тільки пароль - без введення імені користувача - з одним паролем для входу через консольний порт і іншим паролем для входу по протоколу Telnet. Користувачі, які підключаються через консольний порт, повинні ввести пароль консолі, який був попередньо налаштований в режимі конфігурації. Користувачі, які підключаються через протокол Telnet, повинні ввести пароль від Telnet, також званий паролем vty, так званий, тому що це режим конфігурації термінальних ліній (vty). На малюнку 1 представлені варіанти використання паролів з точки зору користувача, що підключається до комутатора.

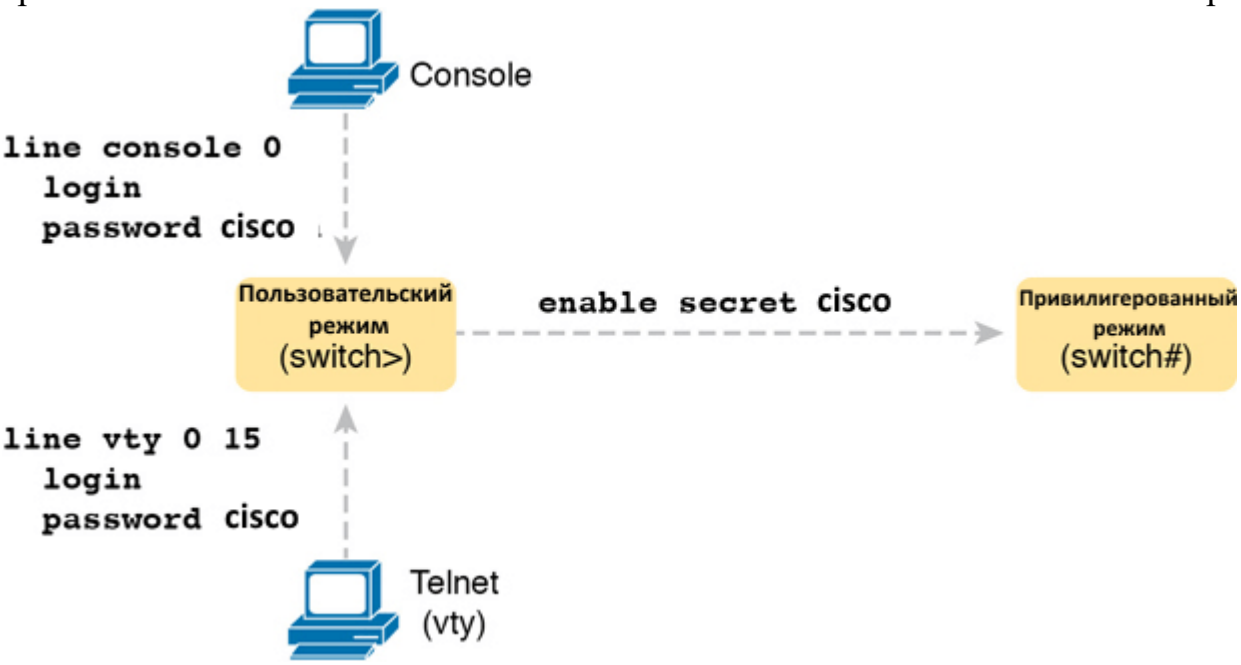


Як видно з малюнка 1, на комутаторах Cisco стоїть захист привілейованого режиму (enable) за допомогою ще одного загального пароля, що задається командою enable password. Системний адміністратор, який підключається до CLI комутатора потрапляє в режим користувача і далі, вводить команду enable.

Ця команда запитує у користувача пароль входу в привілейований режим; якщо користувач вводить правильний пароль, IOS переміщує користувача в привілейований режим.

Щоб налаштувати загальні паролі для консолі, Telnet і привілейованого режиму (enable), необхідно ввести кілька команд. На рис. 2 показаний порядок завдання всіх

трьох паролів.



На рисунку показані два ПК, які намагаються отримати доступ до режиму управління пристроєм. Один з ПК підключений за допомогою консольного кабелю, що з'єднується через лінію console 0, а інший за допомогою Telnet, що з'єднується через термінальну лінію vty 0 15. Обидва комп'ютери не мають Логінов, пароль для консолі і Telnet -cisco. Призначений для користувача режим отримує доступ до привілейованого режиму (enable) за допомогою введення команди "enable secret cisco". Для настройки цих паролів не треба докладати багато зусиль. Все робиться легко. По-перше, конфігурація консолі і пароля vty встановлює пароль на основі контексту: для консолі (рядок con 0) і для ліній vty для пароля Telnet (рядок vty 0 15). Потім в режимі консолі і режимі vty, відповідно вводимо команди:

login

password <пароль задається користувачем>

Налаштований пароль привілейованого режиму, показаний в правій частині малюнка, застосовується до всіх користувачів, незалежно від того, підключаються вони до призначеного для користувача режиму через консоль, Telnet або іншим чином. Команда для настройки enable password є командою глобальної конфігурації: enable secret <пароль користувача>.

У старих версіях, для завдання пароля на привілейований режим, використовувалася команда password. В сучасних IOS застосовується два режими завдання пароля: password і secret.

Рекомендується використовувати команду secret, так як вона найбільш безпечна в порівнянні з password.

Для правильного налаштування захисту комутатора Cisco паролями необхідно слідувати по кроках, зазначеним нижче:

Крок 1. Задайте пароль на привілейований режим командою enable secret password-value

Крок 2. Задайте пароль на доступ по консолі

1. Використовуйте команду line con 0 для входу режим конфігурації консолі;

2. Використовуйте команду password password-value для завдання пароля на консольний режим;

3. Використовуйте команду login для запиту пароля при вході по консолі;

Крок 3. Задайте пароль на термінальні підключення vty (Telnet)

1. Використовуйте команду line vty 0 15 для входу режим конфігурації термінальних ліній. В даному прикладі налаштування будуть застосовані до всіх 16 термінальним лініях;

2. Використовуйте команду password password -value для завдання пароля на режим vty;

3. Використовуйте команду login для запиту пароля при вході по Telnet

У прикладі 2 показаний процес налаштування, відповідно до описаних вище кроків, а також установка пароля enable secret. Рядки, які починаються з! - це рядки коментарів. Вони призначені для коментування призначення команд.

! Enter global configuration mode, set the enable password, and also set the hostname (just because it makes sense to do so)

Switch # configure terminal
Switch (config) # enable secret cisco
Switch # (config) # line console 0
Switch # (config-line) # password cisco
Switch # (config-line) # login
Switch # (config-line) # exit
Switch # (config) # line vty 0 15
Switch # (config-line) # password cisco
Switch # (config-line) # login
Switch # (config-line) # end
Switch #

2. Завдання на практичну роботу.

1. Створити в CPT локальну мережу, що складається з 1 комутатора, 1 маршрутизатора і 4 комп'ютерів.

2. Створити таблицю IP адрес.

3. Налаштувати IP адресацію пристроїв мережі.

4. Встановити паролі на призначений для користувача і привілейований режим комутатора, використовуючи консольний з'єднання.

5. Установити паролі на призначений для користувача і привілейований режим комутатора, використовуючи консольний з'єднання.

6. В якості пароля користувача режиму використовувати власне ім'я.

7. В якості пароля привілейованого режиму використовувати власне прізвище.

8. Провести перевірку отриманих налаштувань.

9. Зберегти файл.

Практична робота № 4

НАСТРОЙКА РІВНЯ ПРИВІЛЕЇВ

Мета роботи: Навчитися налаштування рівня привілеїв.
Робота з програмним забезпеченням: CPT.

1. Теоретичні відомості

За замовчуванням командний інтерфейс CISCO має два рівні доступу:

1. User EXEC mode - 1-й рівень. Є доступ до деякої інформації про пристрій, наприклад, можна подивитися статус мережевих інтерфейсів, маршрути в таблиці маршрутизації і т.д. Але змінити конфігурацію не можна.

2. Privileged EXEC mode - 15-й рівень. Найвищий. Всі права.

Можна настроїти права на виконання певних команд для кожного рівня від 0-го (самого обмеженого) до 15 (найвищого). Таким чином, можна надати певному користувачеві обмежені права на зміну конфігурації пристрою (наприклад, змінювати тільки настройки access-list, або настройки мережевого інтерфейсу), або тільки на перегляд конфігурації і т.д.

Для цього необхідно виконати наступні кроки:

1. Зайти в режим конфігурації:

configure terminal

2. Створити користувача з якимось рівнем привілеїв від 2 до 14:

username userstring privilege level secret [encryption-type] passwordstring
username - команда створення користувача
userstring - ім'я користувача
privilege level - рівень привілеїв
secret [encryption-type]:
secret 0 - пароль вводиться в відкритому вигляді, зберігається в зашифрованому вигляді
secret 5 - пароль вводиться в зашифрованому вигляді, зберігається в зашифрованому вигляді
secret - пароль вводиться і зберігається у відкритому вигляді
passwordstring - пароль користувача

3. Вказати які команди можна виконувати на даному рівні привілеїв

privilege mode [all] level level command
privilege - команда для завдання рівня привілеїв команд
mode - режим конфігурації (EXEC, interface, line і т.д.)
all - означає можливість виконання всіх команд починаються на «command»
level - рівень привілеїв
command - виконання якої команди дозволено на рівні привілеїв level

4. Визначити пароль для цього рівня привілеїв

enable secret level level [encryption-type] passwordstring
Сенс параметрів аналогічний параметрам в команді username
5.сохранилось конфігурацію
do copy running-config startup-config

2. Завдання на практичну роботу.

1. Створити в CPT локальну мережу, що складається з 1 комутатора, 1 маршрутизатора і 4 комп'ютерів.
2. Створити таблицю IP адрес.
3. Налаштувати IP адресацію пристроїв мережі.

2.1 Налаштування рівня привілеїв 5:
• Використовуйте команду privilege exec level для надання доступу до команди ping.
• Увімкніть секретний пароль рівня 5 ІМЯ_5, який зашифрований за допомогою хешування algorithm-type scrypt.
• Створіть запис в локальній базі даних для користувача з ім'ям ПРІЗВИЩЕ з рівнем привілеїв 5, встановіть пароль ФАМІЛІЯ_5 і зашифруйте пароль за допомогою хешування type 9 (algorithm-type scrypt).

2.2. Налаштування рівня привілеїв 10:
• Використовуйте команду privilege exec level для дозволу доступу до команди reload.
• Дозвольте секретний пароль рівня 10 ІМЯ_10, який зашифрований за допомогою хешування algorithm-type scrypt.
• Створіть запис в локальній базі даних для користувача з ім'ям ПРІЗВИЩЕ з рівнем привілеїв 10, встановіть пароль ФАМІЛІЯ_10 і зашифруйте пароль за допомогою хешування type 9 (algorithm-type scrypt).

2.3. Налаштування рівня привілеїв 15:
• Дозвольте секретний пароль рівня 15 ІМЯ_123, який зашифрований за допомогою хешування algorithm-type scrypt.
• Створіть запис в локальній базі даних для користувача з ім'ям Admin з рівнем привілеїв 15, встановіть пароль ФАМІЛІЯ_123 і зашифруйте пароль за допомогою хешування type 9 (algorithm-type scrypt).
• Вийдіть з режиму конфігурації.

Практична робота № 5

НАСТРОЙКА ПРЕДСТАВЛЕНЬ З РІЗНИМИ ПРИВІЛЕЯМИ.

Мета роботи: Навчитися налаштування уявлень з різними привілеями.

Робота з програмним забезпеченням: CPT.

1. Теоретичні відомості

Перш ніж адміністратор зможе створити представлення, необхідно активувати AAA (аудентифікація, авторизація і облік) за допомогою команди aaa new-model. Щоб настроїти та відредагувати представлення, адміністратор повинен увійти в кореневе представлення за допомогою команди enable view в привілейованому режимі. Можна також використовувати команду enable view root. При появі запрошення введіть пароль enable secret.

Для створення і управління поданням необхідно виконати п'ять кроків.

Крок 1. Увімкніть AAA за допомогою команди aaa new-model в режимі глобальної конфігурації. Вийдіть з кореневого представлення і увійдіть в нього за допомогою команди enable view.

Крок 2. Створіть представлення за допомогою команди parser view view-name в режимі глобальної конфігурації. Таким чином включиться режим конфігурації представлення. Виключаючи кореневе представлення, діє максимальне обмеження - всього 15 подань.

Крок 3. Дайте поданням секретний пароль за допомогою команди secret encrypted-password в режимі конфігурації представлення.

Крок 4. Дайте команди заданого подання за допомогою команди commands parser-mode в режимі конфігурації представлення.

Крок 5. Вийдіть з режиму конфігурації уявлення, ввівши команду exit.

2. Завдання на практичну роботу.

1. Створити в CPT локальну мережу, що складається з 1 комутатора, 1 маршрутизатора і 4 комп'ютерів.
2. Створити таблицю IP адрес.
3. Налаштувати IP адресацію пристроїв мережі.

Увімкніть AAA.

Створіть представлення з ім'ям ФАМІЛІЯ_1.

- Дайте поданням пароль ІМ'Я.
- Дозвольте поданням використовувати всі команди введення EXEC, які починаються з show.
- Після конфігурації поверніться в режим глобальної конфігурації.

Створіть представлення з ім'ям ФАМІЛІЯ_2.

- Дайте поданням пароль ІМЯ_5.
- Дозвольте поданням використовувати команду ping.
- Після конфігурації поверніться в режим глобальної конфігурації.

Створіть представлення з ім'ям ФАМІЛІЯ_10.

- Дайте поданням пароль ІМЯ_10.
- Дозвольте поданням використовувати команду reload.
- Після конфігурації поверніться безпосередньо в привілейований режим.

Перевірте сконфігуровані уявлення за допомогою команди show running-config | section parser.