Практична робота 5

НАЛАШТУВАННЯ ЗАСОБІВ ВІДДАЛЕНОГО ДОСТУПУ ТА АДМІНІСТРУВАННЯ

Мета заняття: ознайомитися з особливостями функціонування протоколів та засобів віддаленого доступу та адміністрування; отримати практичні навички налагодження, моніторингу та діагностування засобів віддаленого доступу та адміністрування сучасних ОС; дослідити можливості Cisco IOS з організації, налагодження та функціонування незахищених та захищених віддалених мережевих підключень на базі протоколів Telnet та SSH.

Теоретичні відомості

Протоколи віддаленого доступу

Надзвичайно важливим питанням системного та мережевого адміністрування є забезпечення постійного доступу до комунікаційних пристроїв та кінцевих вузлів мережі. Виконання цього завдання у сучасних мережах забезпечують так звані протоколи віддаленого доступу. Протокол віддаленого доступу забезпечує доступ адміністратора/користувача з одного вузла до іншого через існуючу мережеву інфраструктуру. Як правило, такі протоколи побудовані за клієнт-серверною схемою. До протоколів віддаленого доступу належать протоколи:

– Telnet (TELecommunication NETwork);

– SSH (Secure SHell);

– RLOGIN (Remote LOGIN);

– RDP (Remote Desktop Protocol);

– RFB (Remote FrameBuffer).

Для цих протоколів розроблено ряд інструментальних засобів для реалізації віддаленого доступу – програм-серверів та програм термінальних клієнтів. У багатьох ОС термінальні клієнти є вбудованими. Більшість із вищеперерахованих протоколів (зокрема, Telnet та SSH) орієнтовані на використання інтерфейсу командного рядка, лише деякі (зокрема, RDP) – на використання графічних засобів. Найбільш поширеними протоколами сьогодні є протоколи віддаленого доступу Telnet та SSH. Протокол Telnet є недостатньо захищеним, тому у практиці адміністрування рекомендується застосовувати засоби, які базуються на протоколі SSH.

Протокол віддаленого доступу Telnet

Telnet (TELecommunication NETwork, телекомунікаційна мережа) – протокол, який був розроблений одним із перших у стеку TCP/IP. Перші згадки про нього з'явились у стандарті RFC-15 «Network Subsystem for Time Sharing Hosts», що був випущений у 1969 р. До 1983 р., коли було випущено основну специфікацію протоколу RFC-854 «Telnet Protocol Specification», розроблено та опубліковано понад 20 стандартів RFC, які покращували і розширювали можливості протоколу. Останній стандарт, який має відношення до протоколу Telnet – це стандарт RFC-5198 «Unicode Format for Network Interchange», випущений у 2008 р.

Необхідність розробки протоколу Telnet була зумовлена потребою спрощення підключення до віддалених вузлів та пристроїв різних типів. У повсякденній діяльності використовується велика кількість різнотипних комп'ютерів, кожен із яких потребує сумісного обладнання для введення-виведення інформації, і це є проблемою.

Ситуацію ускладнює і те, що на цих комп'ютерах використовуються різні ОС, різні таблиці кодування та різне програмне забезпечення. Тому виникла потреба у службі емуляції термінала, яка б замінила спеціалізовані пристрої та

програми однією службою. Це було реалізовано за рахунок концепції віртуального термінала (NVT, Network Virtual Terminal). Віртуальний термінал отримує дані, які вводяться у клієнтській системі, і перекладає їх на «універсальну мову». Отримані дані перекладаються з «універсальної мови» на спеціалізовану мову, яка сприймається вузлом. Це дає змогу будь-якому спеціалізованому клієнтові взаємодіяти з будь-яким спеціалізованим сервером.

Telnet є клієнт-серверним протоколом. Належить цей протокол до прикладного рівня моделі OSI та прикладного рівня стеку TCP/IP. Для передачі своїх повідомлень Telnet використовує засоби надійного транспортного протоколу TCP. Саме TCP забезпечує стабільний і надійний зв'язок. За замовчуванням сервер Telnet застосовує порт 23. Клієнт Telnet для організації обміну обирає вільний порт із діапазону динамічних портів системи.

Клієнт Telnet може бути налагоджений на підключення до іншого порту сервера, на якому працює інша служба. Це дозволяє використовувати клієнт Telnet для передачі команд та отримання відповідей на команди конкретним службам додатків та для потреб діагностики.

Telnet може працювати у наступних режимах:

– напівдуплексний режим;

– посимвольний режим;

– рядковий режим;

– локальний режим.

Напівдуплексний режим вважається застарілим і у сучасних системах не застосовується. У посимвольному режимі кожен введений символ відразу ж передається вузлу для обробки, а потім повертається клієнтові. У низькошвидкісних мережах це створює затримки. У багатьох реалізаціях згаданий режим застосовується за замовчуванням. У рядковому режимі текст команди спочатку виводиться на екран, і лише закінчені рядки передаються

віддаленому вузлу для обробки. У локальному режимі обробка символів проводиться у локальній системі під контролем віддаленої системи.

Протокол віддаленого доступу SSH

Протокол SSH (Secure SHell, «безпечна оболонка») – це мережевий протокол віддаленого доступу, який дає змогу здійснювати віддалене керування операційною системою будь-якого мережевого пристрою і безпечно передавати у незахищеному середовищі повідомлення будь-якого іншого мережевого протоколу (наприклад, здійснювати тунелювання TCP-з'єднань для передачі файлів). За функціональністю схожий на протоколи Telnet, але на відміну від нього, шифрує весь трафік, що передається, зокрема і паролі. Крім шифрування може також здійснювати стиснення даних. Протокол SSH, як і решта протоколів віддаленого керування, побудований із використанням клієнт-серверного підходу. SSH-клієнти та SSH-сервери доступні для більшості мережевих операційних систем.

Протокол SSH належить до прикладного рівня моделі OSI та прикладного рівня стеку TCP/IP. Для організації інформаційного обміну SSH-сервер використовує порт 22 TCP. Існує дві версії протоколу: SSH-1 (1995 р.) та SSH-2 (1996 р.). Версія SSH-2 є більш безпечною у порівнянні з SSH-1, тому набула більшого поширення. Сьогодні, коли йде мова про протокол SSH, то мається на увазі саме SSH-2.

Як стандарт мереж TCP/IP протокол SSH був затверджений IETF у 2000 р.

Архітектурно у протоколі SSH виділяють три рівні:

– транспортний рівень (Transport Layer);

– рівень аутентифікації користувача (Authentication Layer);

– рівень з'єднання (Connection Layer).

Протокол транспортного рівня забезпечує аутентифікацію сервера, конфіденційність і цілісність даних з гарною естафетною передачею. Додатково

може підтримуватися стиснення даних. Протокол аутентифікації користувача дає змогу серверу аутентифікувати клієнта. Протокол з'єднання мультиплексує шифрований тунель, створюючи в ньому кілька логічних каналів.

Для аутентифікації сервера у SSH використовується протокол аутентифікації сторін на основі алгоритмів електронно-цифрового підпису RSA або DSA. Для аутентифікації клієнта також може використуватися електронний цифровий підпис RSA або DSA, але допускається також аутентифікація за допомогою пароля (режим зворотної сумісності з Telnet) і навіть за IP-адресою вузла (режим зворотної сумісності з rlogin). Аутентифікація за паролем найбільш поширена і безпечна, оскільки пароль передається по зашифрованому віртуальному каналу. Аутентифікація за IP-адресою небезпечна, цю можливість, як правило, відключають. Для створення загального секрету (сеансового ключа) використовується алгоритм Діффі-Хеллмана. Для шифрування переданих даних використовується симетричне шифрування, алгоритми IDEA, AES, Blowfish, DES або 3DES. Цілісність передачі даних перевіряється за допомогою CRC32 у протоколі SSH версії 1 та за допомогою HMAC-SHA1/HMAC-MD5 у протоколі SSH версії 2. У протоколі SSH також можливе застосовування функції стиснення даних, що передаються. З цією метою використовується алгоритм LempelZiv (LZ77), який забезпечує рівень стиснення, аналогічний архіватору ZIP. Стиснення у SSH активується лише за запитом клієнта і на практиці застосовується досить рідко.

На базі протоколу SSH розроблено і функціонує ряд інших протоколів. Зокрема, SFTP (SSH File Transfer Protocol), SCP (Secure CoPy), FISH (Files Transferred over Shell Protocol), Rsync.

Широкого використання протокол SSH набув для віддаленого доступу та адміністрування мережевих пристроїв. Більшість виробників мережевого обладнання (в т.ч. Cisco, Juniper, Vyatta, Huawei та ін.) включають реалізації SSH-

серверів та клієнтів у мережеві операційні системи комутаторів, маршрутизаторів та інших пристроїв і саме цей протокол рекомендують використовувати.

Серверні та клієнтські засоби організації віддаленого доступу до мережевих пристроїв із використанням протоколів Telnet та SSH

Як відомо, протокол віддаленого доступу Telnet працює з використанням клієнт-серверного підходу. У більшості сучасних ОС наявні серверні та клієнтські програмні модулі, які забезпечують роботу цього протоколу. У деяких ОС згадані модулі є невід'ємними їх частинами та активуються за замовчуванням під час початкового встановлення системи, в інших ОС – потрібне виконання певних додаткових дій щодо їх встановлення та активації. У більшості ОС існує можливість встановлення і використання Telnet-серверів та Telnet-клієнтів сторонніх виробників. Як правило, і серверні, і клієнтські додатки протоколу Telnet використовують інтерфейс командного рядка.

Під час розробки протоколу Telnet проблемам захисту інформації не приділяли достатньої уваги, тому сеанси інформаційного обміну, які організовані за даним протоколом, не є захищеними від дій зловмисників. З метою підвищення рівня інформаційної безпеки засобами даного протоколу не рекомендується користуватися у відкритих (незахищених) мережевих середовищах. Як виняток, можливе використання Telnet у захищених сегментах мереж.

Основною альтернативою використанню протоколу Telnet, яка забезпечує високий рівень захисту інформаційного обміну в ході організації віддаленого доступу як у відкритих, так і у захищених мережевих середовищах, сьогодні є протокол SSH. Цей протокол, як і протокол Telnet, працює з використанням клієнт-серверного підходу. На жаль, у багатьох мережевих ОС відсутні вбудовані програмні модулі, які забезпечують його роботу.

На ринку програмного забезпечення наявна велика кількість як комерційних, так і вільнорозповсюджуваних SSH-серверів та SSH-клієнтів для

різних ОС. Деякі з них орієнтовані на використання лише в певних ОС, деякі є кросплатформними. Найбільш поширеними SSH-серверами є OpenSSH, Bitvise SSH Server (WinSSHD), CopSSH, Dropbear, freeSSHd SSH Server, GoAnywhere Services, lsh, MobaSSH SSH Server, Pragma Fortress SSH Server, Tectia SSH Serve.

Найбільш поширеними SSH-клієнтами є OpenSSH, PuTTY, SecureCRT та інші. Узагальнена інформація про вбудовані серверні та клієнтські засоби організації віддаленого доступу сучасних мережевих ОС наведена у табл. 1.

Таблиця 1 – Вбудовані серверні та клієнтські засоби організації віддаленого доступу

Операційна система	Telnet		SSH	
	Сервер	Клієнт	Сервер	Клієнт
Windows	+*	+*	–	–
macOS	+*	+*	+	+
Linux	+	+	+	+
Cisco IOS	+	+	+	+
Juniper JunOS	+	+	+	+

* необхідні додаткові дії щодо встановлення та активації сервера та клієнта в системі

Порядок налагодження сервера та клієнта протоколу Telnet на обладнанні Cisco

Налагодження функціонування Telnet-сервера на пристроях Cisco для забезпечення організації віддаленого доступу може здійснюватися з використанням трьох підходів:

– безпарольний вхід;

– вхід із використанням паролів на мережеві підключення;

– вхід із використанням механізму користувачів.

Для безпарольного входу порядок виконання етапів налагодження є таким:

1. Обрати мережеве підключення для подальшої активації віддаленого доступу за протоколом Telnet (обов’язково).

2. Відключити використання аутентифікації для входу в систему для обраного мережевого підключення (обов’язково).

3. Активувати можливість Telnet-підключення для відповідного мережевого підключення (обов’язково).

4. Налагодити додаткові параметри (тайм-аути, системні повідомлення тощо) для відповідного мережевого підключення (необов’язково).

Для входу з використанням паролів на мережеві підключення порядок виконання етапів налагодження є наступним:

1. Обрати мережеве підключення для подальшої активації віддаленого доступу за протоколом Telnet (обов’язково).

2. Створити пароль входу для відповідного мережевого підключення та паролі на командні режими (обов’язково).

3. Активувати використання парольної аутентифікації для відповідного мережевого підключення (обов’язково).

4. Активувати можливість Telnet-підключення для відповідного мережевого підключення (обов’язково).

5. Налагодити додаткові параметри (тайм-аути, системні повідомлення тощо) для відповідного мережевого підключення (необов’язково).

Для входу з використанням механізму користувачів порядок виконання етапів налагодження є наступним:

1. Створити локального користувача із зазначенням відповідного рівня привілеїв та пароля (обов’язково).

2. Обрати мережеве підключення для подальшої активації віддаленого доступу за протоколом Telnet (обов’язково).

3. Активувати використання парольної аутентифікації з використанням локальної бази користувачів для відповідного мережевого підключення (обов’язково).

4. Активувати можливість Telnet-підключення для відповідного мережевого підключення (обов’язково).

5. Налагодити додаткові параметри (тайм-аути, системні повідомлення тощо) для відповідного мережевого підключення (необов’язково).

Для організації звичайного підключення для Telnet-клієнта не потрібно проводити налагодження параметрів. За потреби організації специфічного складного підключення існує можливість налагодження певних специфічних параметрів, наприклад, інтерфейсу виходу підключення на маршрутизаторі.

За звичайного використання для Telnet-клієнта немає необхідності виконувати налагодження параметрів підключення. За потреби можливе використання великої кількості специфічних параметрів підключення (наприклад, тип терміналу, перевірка достовірності, інтерфейс виходу для маршрутизатора). Перелік параметрів мо жна визначити з довідки системи. Налагодження параметрів здійснюється безпосередньо у командному рядку під час організації сеансу. Слід зазначити, що за допомогою Telnet-клієнта можна підключатися не лише до Telnet-сервера, а й до серверів та складових інших мережевих протоколів стеку TCP/IP (зокрема, поштових протоколів SMTP, POP3, протоколу маршрутизації BGP і т.д.).

Порядок налагодження сервера та клієнта протоколу SSH на обладнанні Cisco

Налагодження функціонування SSH-сервера на пристроях Cisco для забезпечення віддаленого доступу може здійснюватися з використанням двох підходів:

– з використанням імені пристрою та імені домену;

– з використанням ключових пар RSA (без використання імені пристрою та імені домену).

Слід зазначити, що одним із обов’язкових попередніх етапів налагодження SSH-сервера є створення локального користувача з зазначенням відповідного рівня привілеїв та пароля.

Для підходу з використанням імені пристрою та імені домену порядок виконання етапів налагодження є таким:

1. Задати ім’я пристрою (обов’язково).

2. Задати ім’я домену (обов’язково).

3. Згенерувати SSH-ключ (ключову пару RSA), який буде використовуватися у процесі роботи (обов’язково).

4. Налагодити додаткові параметри SSH-сервера: версію протоколу, час тайм-ауту, кількість спроб аутентифікації та ін. (необов’язково).

5. Обрати мережеве (мережеві) підключення для подальшої активації віддаленого доступу за протоколом SSH (обов’язково).

6. Активувати використання локальної бази даних користувачів для обраного мережевого підключення (обов’язково).

7. Активувати можливість SSH-підключення для відповідного мережевого підключення (обов’язково).

8. Налагодити додаткові параметри (тайм-аути, системні повідомлення тощо) для відповідного мережевого підключення (необов’язково).

Для підходу з використанням ключових пар RSA (без використання імені пристрою та імені домену) порядок виконання етапів налагодження є таким:

1. Створити ключову пару RSA, яка буде використовуватися у процесі роботи (обов’язково).

2. Згенерувати ключову пару RSA із зазначенням довжини ключа (обов’язково).

3. Налагодити додаткові параметри SSH-сервера: версію протоколу, час тайм-ауту, кількість спроб аутентифікації та ін. (необов’язково).

4. Обрати мережеве підключення для подальшої активації віддаленого доступу за протоколом SSH (обов’язково).

5. Активувати використання локальної бази даних користувачів для обраного мережевого підключення (обов’язково).

6. Активувати можливість SSH-підключення для відповідного мережевого підключення (обов’язково).

7. Налагодити додаткові параметри (тайм-аути, системні повідомлення тощо) для відповідного мережевого підключення (необов’язково).

За звичайного використання для SSH-клієнта не потрібно виконувати налагодження параметрів підключення. Специфічні параметри підключення встановлюються за рахунок використання ключів в командному рядку клієнта.

Загальні команди налагодження функціонування протоколів віддаленого доступу на пристроях Cisco

Для налагодження функціонування протоколів віддаленого доступу (зокрема, Telnet та SSH) на пристроях Cisco використовуються як деякі загальні для всіх протоколів команди, так і характерні лише для певного протоколу команди. До загальних команд належать такі команди: ***password***, ***username***, ***login***, ***transport***, ***rotary***, ***autocommand***, ***security authentication*** та похідні від них команди.

Команди ***login***, ***password***, ***username*** призначені для налагодження параметрів аутентифікації для певного мережевого підключення, команди групи ***transport*** призначені для дозволу/заборони віддалених підключень до/з пристрою з використанням різних мережевих протоколів. Команда ***rotary*** відповідає за налагодження нестандар тних портів для підключень. Команда autocommand дає можливість налагодити виконання певної команди режиму користувача після підключення. Для керування сеансами мережевих протоколів можуть використовуватися як певні комбінації клавіш (для призупинення сесії

Ctrl+Shift+6, ***x***), так і певні команди (повернення до сеансу – команда ***resume***, завершення сеансу – команда ***disconnect***).

Синтаксис команди ***transport input*** (режим конфігурування лінії):

```
transport input {value | values},
```

де **value** – параметр, який може набувати значень **all**, **lapb-ta**, **lat**, **mop**, **none**, **pad**, **rlogin**, **ssh**, **telnet**, **udptn**, **v120**; залежно від версії IOS можливі й інші значення;

values – рядок параметрів, що формується із значень **lapb-ta**, **lat**, **mop**, **pad**, **rlogin**, **ssh**, **telnet**, **udptn**, **v120**;

all – всі протоколи;

lapb-ta – термінальний адаптер протоколу LAPB;

lat – протокол DEC LAT;

mop – протокол DEC MOP Remote Console Protocol;

none – жоден із протоколів;

pad – протокол X.3 PAD;

rlogin – протокол Rlogin;

ssh – протокол SSH;

telnet – протокол Telnet;

udptn – асинхронний UDPTN через UDP протокол;

v120 – Асинхронне підключення через ISDN.

Синтаксис команди ***transport output*** (режим конфігурування лінії):

```
transport output {value | values}.
```

Параметри команди аналогічні параметрам попередньої команди.

Синтаксис команди ***transport preffered*** (режим конфігурування лінії):

```
transport preffered value.
```

Параметр команди аналогічний параметру **value** попередньої команди, за винятком значення **all**.

Cisco VTY – віртуальний інтерфейс, за допомогою якого можна забезпечити віддалений доступ до пристрою. Обладнання Cisco підтримує не менше 16 одночасних підключень по віртуальному інтерфейсу.

VTY – це лінія віртуального терміналу маршрутизатора, що використовується виключно для керування внутрішніми з'єднаннями Telnet, SSH та rlogin з маршрутизатором. Вони є віртуальними, функцією програмного забезпечення – немає обладнання, пов'язаного з ними. Вони відображаються в конфігураціях як vty 0 4.

Сценарій налагодження віддаленого підключення за протоколом Telnet із входом без пароля (без аутентифікації) наведений нижче. Слід зазначити, що у даному сценарії передбачено прямий перехід у привілейований режим за рахунок встановлення найвищого рівня привілеїв:

```
Router(config)#line vty 0 4
Router(config-line)#no login
Router(config-line)#transport input telnet
Router(config-line)#privilege level 15
Router(config-line)#exit
```

Сценарій налагодження віддаленого підключення за протоколом Telnet до маршрутизатора Cisco з використанням засобів локальної аутентифікації на базі механізму паролів на вхід до відповідних командних режимів пристрою наведений нижче. У даному сценарії застосовані паролі типу 7:

```
Router(config)#service password-encryption
Router(config)#enable password adminpass2
Router(config)#line vty 0 4
Router(config-line)#password adminpass1
Router(config-line)#login
Router(config-line)#transport input telnet
Router(config-line)#exit
```

Сценарій налагодження віддаленого підключення за протоколом Telnet до маршрутизатора Cisco з використанням засобів локальної аутентифікації на базі механізму користувачів наведений нижче. У даному сценарії застосовані паролі типу 5:

```
Router(config)#username admin privilege 15 secret adminpass
Router(config)#enable secret adminpass2
Router(config)#line vty 0 4
Router(config-line)#login local
Router(config-line)#transport input telnet
Router(config-line)#exit
```

Команди налагодження функціонування протоколу SSH

Команда ***ip ssh authentication-retries*** призначена для встановлення кількості спроб аутентифікації, після якої SSH-клієнтові забороняється доступ. Команда ***ip ssh time-out*** використовується для обмеження часу відповіді SSH-клієнта (SSH-сервер перериває з'єднання, якщо дані не передаються протягом часу очікування). Команда ***ip ssh version*** призначена для вказування версії протоколу SSH, що буде використовуватися у процесі роботи. За замовчуванням на пристроях Cisco активовано використання протоколу SSH версії 1. Відміна дії більшості команд ***ip ssh*** виконується формою ***no***.

Для роботи з ключами використовуються команди групи ***crypto key***. Для генерації ключів застосовуються команди ***crypto key generate***, ***crypto key generate rsa general-keys modulus***. Для видалення ключів призначені команди ***crypto key zeroize***, ***crypto key zeroize rsa***.

Слід звернути увагу, що однакового результату у процесі налагодження функціонування протоколу SSH на пристроях Cisco можна досягнути у разі використання різних команд. Детальний опис дії команд можна знайти в документації виробника.

Синтаксис команди ***ip ssh authentication-retries*** (режим глобального конфігурування):

```
ip ssh authentication-retries retries-value,
```

де **retries-value** – значення максимальної кількості спроб аутентифікації підряд, число з діапазону 0…5; за замовчуванням встановлюється 3 спроби.

Синтаксис команди ***ip ssh time-out*** (режим глобального конфігурування):

```
ip ssh time-out seconds,
```

де **seconds** – значення інтервалу часу очікування відповіді клієнта (с), число з діапазону 1 ... 120; за замовчуванням встановлюється 120 с.

Синтаксис команди ***ip ssh version*** (режим глобального конфігурування):

```
ip ssh version version-number,
```

де **version-number** – номер версії протоколу, може набувати значень 1 або 2; якщо значення не встановлене, то функціонування протоколу здійснюється у змішаному режимі.

Синтаксис команди ***crypto key generate*** (режим глобального конфігурування):

```
crypto key generate.
```

Команда не має параметрів.

Синтаксис команди ***crypto key generate rsa general-keys modulus*** (режим глобального конфігурування):

```
crypto key generate rsa general-keys modulus
modulus-value,
```

де **modulus-value** – значення довжини ключа (бітів), число з діапазону 360 ... 2048; за замовчуванням генеруються ключі довжиною 512 біт.

Синтаксис команди ***crypto key zeroize*** (режим глобального конфігурування):

```
crypto key zeroize
```

Команда не має параметрів.

Синтаксис команди ***crypto key zeroize rsa*** (режим глобального конфігурування):

```
crypto key zeroize rsa keypair-name-string,
```

де **keypair-name-string** – текстовий рядок, який містить назву ключової пари RSA.

Сценарій налагодження віддаленого підключення за протоколом SSH до маршрутизатора Cisco з використанням імені пристрою та імені домену та з

використанням засобів локальної аутентифікації на базі механізму користувачів наведений нижче. У цьому сценарії застосовані паролі типу 5:

```
R-G-N(config)#username admin privilege 15 secret adminpass
R-G-N(config)#enable secret adminpass2
R-G-N(config)#ip domain-name mynet.net
R-G-N(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R-G-N.mynet.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:4:16.653: %SSH-5-ENABLED: SSH 1.99 has been enabled
R-G-N(config)#ip ssh version 2
R-G-N(config)#ip ssh time-out 60
R-G-N(config)#line vty 0 4
R-G-N(config-line)#login local
R-G-N(config-line)#transport input ssh
R-G-N(config-line)#exit
```

Типи паролів Cisco IOS

На пристроях Cisco існує можливість налагодити безпечний доступ для всіх видів підключень та певних режимів Cisco IOS із використанням парольного захисту. Для забезпечення парольного захисту на пристроях Cisco передбачено такі паролі:

1. Пароль ліній (пароль для входу в режим користувача).

2. Пароль входу у привілейований режим.

3. Паролі користувачів.

Перші два паролі встановлюються на пристрій у цілому й обмежують вхід до відповідних режимів. Паролі для користувачів можуть мати різний рівень привілеїв щодо виконання команд. Інформація про паролі та користувачів зберігається у конфігураційному файлі пристрою.

Для пристроїв Cisco використовуються три типи паролів:

1. Звичайний пароль (Plain-text password).

2. Пароль типу 7 (Type 7 password).

3. Пароль типу 5 (MD5 hash password).

Звичайні паролі встановлюються за замовчуванням і зберігаються у конфігураційному файлі пристрою у відкритому вигляді, що є загрозою безпеці.

Паролі типу 7 для підвищення рівня безпеки використовують шифрування за алгоритмом Віженера (Vigenere). Паролі даного типу доволі легко розшифровуються, тому рекомендується використовувати паролі типу 5, які мають найвищий рівень безпеки.

Налагодження парольного доступу на пристроях Cisco

Для налагодження доступу по лініях до пристрою Cisco використовуються команди ***password*** та ***login***. Застосування цих команд передбачає те, що паролі є звичайними (відкритими). Для налагодження парольного доступу до привілейованого режиму у пристроях Cisco передбачено команду ***enable password***. Якщо цю команду використати без параметрів, то пароль буде теж звичайним відкритим. Існує можливість використання цієї команди із встановленням шифрованого пароля типу 7. Для шифрування всіх паролів відразу (встановлення паролів типу 7) використовується команда ***service password-encryption***. Оскільки пароль даного типу вважається слабким, використовувати дану команду не рекомендується. Замість неї рекомендується використовувати команду ***enable secret***, яка активує використання шифрованих паролів типу 5. Існує можливість створення окремих користувачів із різними привілеями входу в різні режими на пристроях Cisco. Для цього використовується команда ***username***. Відміна дії всіх розглянутих команд здійснюється за допомогою службової конструкції ***no***.

Синтаксис команди ***password*** (режим конфігурування лінії):

```
password password-string,
```

де **password-string** – текстовий рядок пароля довжиною до 80 символів, який повинен починатися з літери.

Синтаксис команди ***login*** (режим конфігурування лінії):

```
login {local},
```

де local – службова конструкція, яка вказує, що для входу необхідно використовувати імена створених користувачів та їх паролі.

Синтаксис команди ***enable password*** (режим глобального конфігурування):

```
enable password [level level-value] {password-string |
    [encryptiontype] encrypted-password-string},
```

де **level** – службова конструкція, яка зазначає рівень привілеїв пароля.

level-value – значення рівня, число в межах від 0 до 15;

password-string – текстовий рядок пароля;

encryption-type – тип шифрування;

encrypted-password-string – зашифрований пароль, отриманий з іншого джерела шифрування.

Синтаксис команди ***enable secret*** (режим глобального конфігурування):

```
enable secret [level level-value] { password-string |
    [encryptiontype] encrypted-password-string }.
```

Параметри команди аналогічні параметрам попередньої команди.

Синтаксис команди ***username*** (режим глобального конфігурування):

```
username name {nopassword | password password-string |
 password encryption-type encrypted-password-string},
```

де **name** – текстове ім’я користувача;

nopassword – службова конструкція, яка вказує на те, що не потрібно використовувати пароль;

password – службова конструкція, яка вказує на використання пароля;

password-string – текстовий рядок пароля;

encryption-type – тип шифрування.

encrypted-password-string – зашифрований пароль, отриманий з іншого джерела шифрування.

Сценарій налагодження доступу до комутатора з використанням механізму паролів наведено нижче (встановлюється пароль на вхід для консольного

підключення та пароль на перехід до привілейованого режиму). Паролі зберігаються у файлі конфігурації у відкритому вигляді:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password mypass1
Router(config-line)#login
Router(config-line)#exit
Router(config)#enable password mypass2
Router(config)#exit
```

Сценарій налагодження доступу до комутатора з використанням механізму користувачів та паролів типу 7 наведено нижче (встановлюється пароль на вхід у привілейований режим; створюються користувач User1 з рівнем привілеїв 1 (за замовчуванням) та користувач Admin із максимальним рівнем привілеїв 15; відключається пароль на вхід для консольного підключення; активується застосування механізму користувачів для консольного підключення; здійснюється операція шифрування звичайних відкритих паролів із метою отримання паролів типу 7):

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#username User1 password mypass3
Router(config)#username Admin privilege 15 password mypass4
Router(config)#line console 0
Router(config-line)#no password
Router(config-line)#login local
Router(config-line)#exit
Router(config)#service password-encryption
Router(config)#exit
```

Для підвищення рівня безпеки комутатора рекомендується замість паролів типу 7 застосовувати паролі типу 5. У такому разі краще застосовувати наведений нижче модифікований сценарій налагодження доступу до комутатора:

```
Router(config)#enable secret mypass2
Router(config)#username User1 secret mypass3
Router(config)#username Admin privilege 15 secret mypass4
Router(config)#line console 0
Router(config-line)#login local
Router(config-line)#exit
```

Хід роботи

1. У середовищі програмного симулятора/емулятора створити проект мережі (рис. 1). При побудові звернути увагу на вибір моделей маршрутизаторів, мережевих модулів та плат, а також мережевих з'єднань. На схемі канали зв'язку підмереж показані у загальному вигляді, при побудові підмережі вибирати потрібний тип кабелю для відповідної технології. Для цього використовувати дані табл. 2. Для побудованої мережі заповнити описову таблицю (табл. 3).

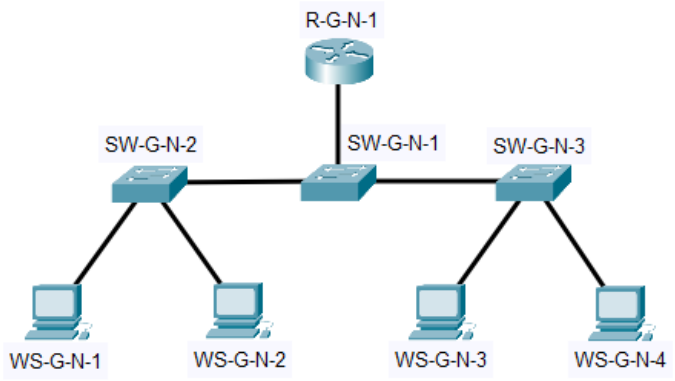

Рисунок 3 – Проект локальної мережі

Примітка: на схемі замість літери G вказати номер групи, замість N – номер варіанту

Таблиця 2 – Варіанти завдання

Варіант	IP-адреса мережі	Префікс	Адреса шлюзу	Протокол доступу
1	191.G.N.0	/24	Перша IP-адреса діапазону	Telnet
2	192.G.N.0	/25	Остання IP-адреса діапазону	Telnet&Pwd
3	193.G.N.0	/26	Перша IP-адреса діапазону	Telnet&User
4	194.G.N.0	/27	Остання IP-адреса діапазону	SSHv1
5	195.G.N.0	/28	Перша IP-адреса діапазону	SSHv2
6	196.G.N.0	/24	Остання IP-адреса діапазону	Telnet
7	197.G.N.0	/25	Перша IP-адреса діапазону	Telnet&Pwd
8	198.G.N.0	/26	Остання IP-адреса діапазону	Telnet&User
9	199.G.N.0	/27	Перша IP-адреса діапазону	SSHv1
10	200.G.N.0	/28	Остання IP-адреса діапазону	SSHv2
11	201.G.N.0	/24	Перша IP-адреса діапазону	Telnet
12	202.G.N.0	/25	Остання IP-адреса діапазону	Telnet&Pwd

13	203.G.N.0	/26	Перша IP-адреса діапазону	Telnet&User
14	204.G.N.0	/27	Остання IP-адреса діапазону	SSHv1
15	205.G.N.0	/28	Перша IP-адреса діапазону	SSHv2
16	206.G.N.0	/24	Остання IP-адреса діапазону	Telnet
17	207.G.N.0	/25	Перша IP-адреса діапазону	Telnet&Pwd
18	208.G.N.0	/26	Остання IP-адреса діапазону	Telnet&User
19	209.G.N.0	/27	Перша IP-адреса діапазону	SSHv1
20	210.G.N.0	/28	Остання IP-адреса діапазону	SSHv2
21	211.G.N.0	/24	Перша IP-адреса діапазону	Telnet
22	212.G.N.0	/25	Остання IP-адреса діапазону	Telnet&Pwd
23	213.G.N.0	/26	Перша IP-адреса діапазону	Telnet&User
24	214.G.N.0	/27	Остання IP-адреса діапазону	SSHv1
25	215.G.N.0	/28	Перша IP-адреса діапазону	SSHv2
26	216.G.N.0	/24	Остання IP-адреса діапазону	Telnet
27	217.G.N.0	/25	Перша IP-адреса діапазону	Telnet&Pwd
28	218.G.N.0	/26	Остання IP-адреса діапазону	Telnet&User
29	219.G.N.0	/27	Перша IP-адреса діапазону	SSHv1
30	220.G.N.0	/28	Остання IP-адреса діапазону	SSHv2

Примітка: замість літери G вказати номер групи, замість N – номер варіанту. Позначення Telnet – підключення за протоколом Telnet з входом без паролю; Telnet&Pwd – підключення за протоколом Telnet із використанням засобів локальної аутентифікації на базі механізму паролів; Telnet&User – підключення за протоколом Telnet із використанням аутентифікації на базі механізму користувачів; SSHv1, SSHv2 – підключення за протоколом SSH відповідних версій із використанням засобів локальної аутентифікації на базі механізму користувачів.

Таблиця 3 – Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Комутатор SW-1 (Cisco 2960-24TT-L)	Console	Робоча станція WS-MGMT	RS-232 (USB)
	Gi0/1	Сервер Serv-A-1	Gi0
	Fa0/1	Робоча станція WS-A-1	Fa0
	Fa0/24	Робоча станція WS-A-2	Fa0
Робоча станція WS-MGMT	RS-232 (USB)	Комутатор SW-1 (Cisco 2960-24TT-L)	Console
Сервер Serv-A-1	Gi0		Gi0/1
Робоча станція WS-A-1	Fa0		Fa0/1
Робоча станція WS-A-2	Fa0		Fa0/24

2. Провести базове налаштування маршрутизаторів та комутаторів, мережевих інтерфейсів та з’єднань. Для цього використовувати дані табл. 2.

3. Розробити схему адресації пристроїв мережі. Для цього скористатися даними табл. 2. Результати навести у вигляді таблиці, яка аналогічна табл. 4.

Таблиця 4 – Параметри адресації мережі для прикладу

Мережа/Пристрій	Інтерфейс/Мережевий адаптер/Шлюз	IP-адреса	Маска	Префікс
Мережа А	–	195.10.1.0	255.255.255.0	/24
Маршрутизатор R-1	Інтерфейс Fa0/0	195.10.1.254	255.255.255.0	/24
	Інтерфейс Fa0/1	196.10.1.254	255.255.255.0	/24
Сервер Serv-1	Мережевий адаптер	195.10.1.253	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–
Робоча станція WS-A1	Мережевий адаптер	195.10.1.1	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–
Робоча станція WS-A2	Мережевий адаптер	196.10.1.1	255.255.255.0	/24
	Шлюз за замовчуванням	196.10.1.254	–	–

4. Провести налаштування параметрів IP-адресації пристроїв мережі у відповідності до даних п. 3. Перевірити наявність зв’язку між пристроями мережі.

5. Провести налагодження віддаленого доступу до маршрутизатора згідно з даними табл. 2. Перевірити наявність віддаленого підключення до маршрутизатора з робочих станцій.