Тема 6. Налаштування засобів віддаленого доступу та адміністрування

Мета роботи: ознайомитися з особливостями функціонування протоколів та засобів віддаленого доступу та адміністрування 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 або 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 використовувати засоби, які базуються на протоколі SSH.

Протокол віддаленого доступу Telnet

Telnet (TELecommunication NETwork, телекомунікаційна мережа) – протокол, який був розроблений одним із перших для стеку TCP/IP.

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 використовує порт 23. Клієнт Telnet для організації обміну обирає вільний порт із діапазону динамічних портів системи.

Клієнт Telnet може бути налаштований 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.

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

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 в 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.

Для аутентифікації сервера у SSH використовується протокол аутентифікації сторін на основі алгоритмів електронно-цифрового підпису RSA або DSA. Для аутентифікації клієнта також може використовуватися 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.

Широкого використання протокол SSH набув для віддаленого доступу та адміністрування мережевих пристроїв. Більшість виробників мережевого обладнання включають реалізації SSH-серверів та клієнтів у мережеві операційні системи комутаторів, маршрутизаторів та інших пристроїв і саме цей протокол рекомендують використовувати.

Налаштування 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 налаштування SSH-сервера є створення локального користувача з зазначенням відповідного рівня привілеїв та пароля.

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

Команди налаштування протоколів віддаленого доступу

Команди login, password, username призначені для налаштування параметрів аутентифікації для певного мережевого підключення, команди групи

transport призначені для дозволу/заборони віддалених підключень до/з пристрою з використанням різних мережевих протоколів.

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;

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.

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 налаштування віддаленого підключення за протоколом Telnet із входом без паролю (без аутентифікації) наведений на рис. 6.1. Слід зазначити, що в 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
```

Рисунок 6.1 – Налаштування віддаленого безпарольного доступу Telnet

Сценарій налаштування віддаленого підключення за протоколом Telnet до маршрутизатора Cisco з використанням засобів локальної аутентифікації на базі механізму паролів наведений на рис. 6.2. В даному сценарії використані паролі типу 7 (шифр Віженера).

```
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
```

Рисунок 6.2 – Налаштування віддаленого парольного доступу Telnet

Сценарій налаштування віддаленого підключення за протоколом Telnet до маршрутизатора Cisco з використанням засобів локальної аутентифікації на базі механізму користувачів наведений на рис. 6.3. В даному сценарії використані паролі типу 5 (шифрування MD5).

```
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
```

Рисунок 6.3 – Налаштування віддаленого доступу Telnet з аутентифікацією

Команда ip ssh version призначена для визначення 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 використовуються 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 налаштування функціонування протоколу SSH на пристроях Cisco можна досягнути в разі використання різних команд.

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 (біт), 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 налаштування віддаленого підключення за протоколом SSH до маршрутизатора Cisco з використанням імені пристрою та імені домену і з

використанням засобів локальної аутентифікації на базі механізму користувачів наведений на рис. 6.4. В цьому сценарії використані 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
```

Рисунок 6.4 – Налаштування віддаленого доступу за протоколом SSH

Типи паролів Cisco IOS

На пристроях Cisco існує можливість налаштувати безпечний доступ для всіх видів підключень та певних режимів Cisco IOS із використанням парольного захисту. Для забезпечення парольного захисту на пристроях Cisco передбачено наступні 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 та 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.
2. Пароль типу 7.
3. Пароль типу 5.

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. Паролі даного типу доволі легко розшифровуються, тому рекомендується використовувати паролі типу 5 (шифрування MD5), які мають найвищий рівень безпеки.

Налаштування парольного доступу на пристроях Cisco

Для налаштування доступу по лініях до пристрою Cisco використовуються команди password та login. Використання цих команд передбачає те, що паролі є звичайними (відкритими). Для налаштування 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 з 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 паролю 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 |
    [encryption-type] encrypted-password-string},
```

де level – службова конструкція, яка зазначає рівень привілеїв паролю.

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

password-string – текстовий рядок паролю;

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 |
    [encryption-type] 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 налаштування доступу до комутатора з використанням механізму паролів наведено на рис. 6.5 (встановлюється пароль на вхід для консольного підключення та пароль на перехід до привілейованого режиму). Паролі зберігаються у файлі конфігурації у відкритому вигляді.

Сценарій налаштування доступу до комутатора з використанням механізму користувачів та паролів типу 7 наведено на рис. 6.6 (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 використання механізму користувачів для консольного підключення; здійснюється операція шифрування звичайних відкритих паролів з метою отримання паролів типу 7).

```
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
```

Рисунок 6.5 – Налаштування доступу з використанням паролів

```
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
```

Рисунок 6.6 – Налаштування доступу з використанням користувачів та паролів

Для підвищення рівня безпеки комутатора рекомендується замість паролів типу 7 використовувати паролі типу 5. В такому разі краще використовувати наведений на рис. 6.7 модифікований сценарій налаштування 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
```

Рисунок 6.7 – Використання паролів типу 5

Хід роботи

1. В середовищі Cisco Packet Tracer створити проект мережі (рис. 6.8). При побудові звернути увагу на вибір моделей маршрутизаторів, мережевих модулів та плат, а також мережевих з'єднань. На схемі канали зв'язку підмереж показані в загальному вигляді, при побудові підмережі вибрати довільний тип кабелю та технології. Для побудованої мережі заповнити описову таблицю, аналогічну табл. 6.1.

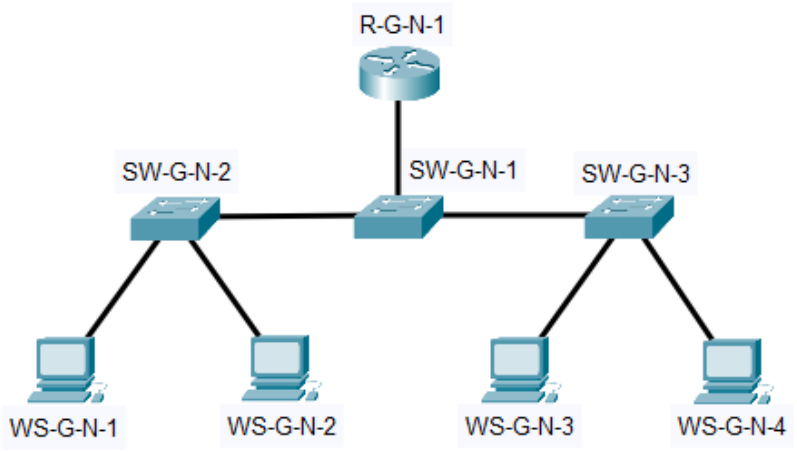

Рисунок 6.1 – Проект локальної мережі

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

Таблиця 6.1 – Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Комутатор SW-1	Gi0/1	Сервер Serv-A-1	Gi0
	Fa0/1	Робоча станція WS-A-1	Fa0
	Fa0/24	Робоча станція WS-A-2	Fa0
Сервер Serv-A-1	Gi0	Комутатор SW-1	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.

3. Розробити схему адресації пристроїв мережі. Для цього скористатися даними таблиці А.13. Результати навести у вигляді таблиці, аналогічної табл. 6.2.

Таблиця 6.2 – 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 налаштування віддаленого доступу до маршрутизатора згідно з даними таблиці А.13. Перевірити наявність віддаленого підключення до маршрутизатора з робочих станцій.

6. Оформити звіт до практичної роботи, який повинен обов’язково містити: назву дисципліни, номер роботи, прізвище та ім’я студента, що її виконав, номер варіанту завдання, скріншоти основних етапів виконання завдання (побудова схеми мережі, налаштування пристроїв, перевірка зв’язку між пристроями, перевірка встановлення віддаленого доступу) та короткі текстові пояснення до них, таблиці інтерфейсів пристроїв, адресації мережі.

Контрольні запитання

1. Поняття та призначення протоколів віддаленого доступу.
2. Загальна характеристика протоколів Telnet та SSH.
3. Сфера застосування протоколів Telnet та SSH.
4. Характеристика рівня безпеки протоколів Telnet та SSH.
5. Основні команди налаштування протоколу Telnet на пристроях Cisco.

Основні команди налаштування протоколу SSH на пристроях Cisco