Instrukcja laboratoryjna z przedmiotu: Sieci komputerowe

Ćwiczenie 11: Zarządzanie urządzeniami sieciowymi. Telnet/SSH, port konsolowy i obsługa plików

Marta Szarmach
Zakład Telekomunikacji Morskiej
Wydział Elektryczny
Uniwersytet Morski w Gdyni

05.2022

I. Wprowadzenie

Zarządzanie urządzeniami sieciowymi obejmuje zarówno konfigurację urządzeń (tak, aby działały zgodnie z założeniem) czy sprawdzanie ich stanu, jak i dbanie o wykonywanie kopii zapasowych właściwych plików, np. z konfiguracją urządzenia czy obrazem systemu.

Przy zarządzaniu urządzeniami sieciowymi kluczowe jest uzyskanie dostępu do urządzenia, tj. do jego wiersza polecenia, tak, by móc wydawać mu komendy. W większości urządzeń sieciowych (nie tylko producenta Cisco) dostęp realizowany jest na kilka sposobów:

- Lokalnie, z wykorzystaniem **portu konsolowego** oraz dedykowanego kabla konsolowego — umożliwia konfigurowanie nawet fabrycznie nowych urządzeń (nieskonfigurowanych wcześniej), lecz wymaga fizycznej obecności przy urządzeniu (podłączenia się doń kablem konsolowym). Zazwyczaj połączenie to jest połączeniem szeregowym, otwieranym na komputerze administratora za pomocą specjalnego terminala (oprogramowania takiego jak PuTTY czy HyperTerminal). Ciekawostka: w wielu firmach kable konsolowe od urządzeń z szafy rackowej wpięte są w **serwer terminali**, który stanowi centralny punkt dostępu do urządzeń.
- Zdalnie, z wykorzystaniem sieci — sposób wygodniejszy, gdyż umożliwia połączenie się z urządzeniami z dowolnego miejsca w sieci (przykładowo, urządzenia sieciowe stoją w serwerowni, a administrator łączy

się z nimi, siedząc przy swoim biurku). Niestety, z uwagi na to, że połączenie odbywa się poprzez zwykłą „współdzieloną" infrastrukturę sieciową, jest to sposób mniej bezpieczny niż połączenie konsolowe (ruch ten można podsłuchać). Ponadto, sposób ten wymaga wcześniejszej konfiguracji urządzeń (przykładowo, ustawienia haseł dostępu czy kluczy szyfrujących, adresów IP), dlatego nie przydaje się przy konfiguracji urządzenia fabrycznie nowego. Połączenie można zrealizować za pomocą dwóch protokołów:

  - **telnet** — na porcie 23 TCP; połączenie nie jest szyfrowane,
  - **SSH** (ang. *Secure Shell*) — na porcie 22 TCP; połączenie jest szyfrowane, do szyfrowania używany jest algorytm **RSA** (asymetryczny — kluczem publicznym dane są szyfrowane, a prywatnym odszyfrowane), a do bezpiecznej wymiany kluczy używany jest algorytm **Diffiego-Hellmana**, bazujący na trudności w rozkładzie dużych liczb na czynniki.

Inną ważną rzeczą, o której powinniśmy pamiętać jako administratorzy sieciowi, jest robienie kopii zapasowej plików ważnych z punktu widzenia działania urządzeń: plików z konfiguracją urządzenia oraz z obrazem systemu operacyjnego urządzenia (np. Cisco IOSa).

- **Plik z konfiguracją bieżącą** (running-config) zawiera aktualną konfigurację urządzenia i jest przechowywany w ulotnej pamięci RAM. Jest tracony w wyniku wyłączenia urządzenia czy utraty zasilania, o ile nie zostanie przekopiowany do **pliku z konfiguracją startową** (*startup-config*), który umieszczony jest w nieulotnej pamięci NVRAM; konfiguracja startowa jest wdrażana domyślnie przy każdym uruchomianiu urządzenia.

- **Obraz systemu IOS** przechowywany jest w pamięci nieulotnej flash jako plik .bin, .tar lub .pie. To z tego pliku bootowany jest system podczas startu urządzenia. Aktualizacja systemu odbywa się poprzez podmianę pliku z obrazem.

W łatwy sposób z poziomu CLI urządzeń Cisco (z trybu uprzywilejowanego) można wysłać wymienione pliki na komputer, o ile uruchomiony jest na nim przykładowo serwer TFTP (np. dzięki oprogramowaniu tftpd32).

II. Cel ćwiczenia

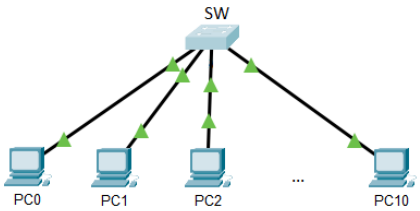
Celem niniejszego ćwiczenia jest zapoznanie się z podstawowymi czynnościami niezbędnymi do zarządzania urządzeniami sieciowymi, takimi jak:

- umiejętnością połączenia się z urządzeniem zarówno lokalnie (przez port konsolowy, także z wykorzystaniem serwera terminali), jak i zdalnie (przez telnet oraz SSH),
- przygotowaniem urządzeń sieciowych (producenta Cisco) do obsługi ruchu telnet i SSH,
- obserwacją przechwyconego ruchu telnet,
- wykonaniem kopii zapasowej plików istotnych z punktu widzenia działania urządzenia: plików konfiguracyjnych oraz obrazu systemu.

III. Stanowisko laboratoryjne

Do wykonania pierwszej części ćwiczenia niezbędne jest stanowisko laboratoryjne składające się z komputera klasy PC z zainstalowanym programem Cisco Packet Tracer.

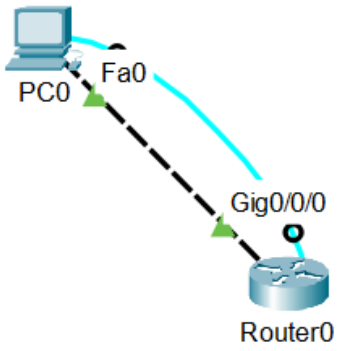
Kolejna część ćwiczenia wymaga użycia niewielkiej sieci komputerowej, składającej się z komputerów klasy PC (z zainstalowanym oprogramowaniem tftpd32 oraz Wireshark) podłączonych do przełącznika sieciowego Cisco. Ponadto, w drugiej części ćwiczenia potrzebujemy serwera terminali, do którego podłączone są portami szeregowymi kable konsolowe wszystkich urządzeń z laboratorium.



IV. Przebieg ćwiczenia

1 Konfiguracja połączenia zdalnego i konsolowego w programie Packet Tracer

1.1 Stwórz w programie Packet Tracer projekt prostej sieci.



a) Otwórz program Cisco Packet Tracer. Przeciągnij na obszar projektu dwa urządzenia: komputer klasy PC (z sekcji *End Devices*) oraz router, np. 2911 (z sekcji *Network Devices* ⇒ *Routers*).

b) Połącz oba urządzenia ze sobą. Z sekcji *Connections* wybierz kabel z przeplotem i jeden koniec kabla umieść w porcie ethernetowym kompuera PC0, a drugi w porcie routera (np. GigabitEthernet 0/0).

c) Dokonaj wstępnej konfiguracji komputera: kliknij w komputer PC0, przejdź do zakładki *Desktop* i wybierz *IP Configuration*, po czym ustaw na nim statyczny prywatny adres IP (np. 192.168.0.100 z maską 255.255.255.0).

1.2 Utwórz połączenie konsolowe pomiędzy komputerem PC0 a routerem.

a) Z sekcji *Connections* wybierz kabel konsolowy (niebieski). Jeden koniec kabla umieść w porcie szeregowym RS232 komputera PC0, a drugi w porcie konsolowym routera.

b) Przejdź do karty Desktop komputera PC0 i otwórz na nim program *Terminal*. Jest to program, za pomocą którego połączysz się szeregowo z routerem przez port konsolowy. Sprawdź, czy wybrane są następujące ustawienia:

- Bits Per Second: 9600
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow control: None

Pamiętaj, że w normalnej sytuacji, po podłączeniu zarządzanego urządzenia przez port konsolowy do swojego komputera, należałoby sprawdzić w Menedżerze urządzeń, który port COM został otwarty.

c) Połącz się z routerem. Po wciśnięciu klawisza Enter powinieneś mieć dostęp do CLI urządzenia. Jako że router nie posiada na ten moment żadnej specyficznej konfiguracji, powinieneś uzyskać do niego dostęp bez podawania hasła.

d) Będąc już połączonym z routerem przez port konsolowy, dokonaj jego podstawowej konfiguracji: zmiany nazwy urządzenia, ustawienia haseł do trybu uprzywilejowanego, portu konsolowego i linii wirtualnych, bannera *message-of-the-day*, a także konfiguracji interfejsu, do którego dołączony jest komputer PC0 (pamiętając, by nadać mu adres IP z tej samej podsieci).

```
Router(config)#hostname R1
R1(config)#enable secret cisco
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#banner motd % Unauthorized access prohibited %
R1(config)#interface g0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

Jak widzisz, aby uzyskać dostęp do urządzenia przez port konsolowy, urządzenie nie musiało być wstępnie skonfigurowane — konfiguracji dokonałeś dopiero po uzyskaniu połączenia.

e) Przejdź do pulpitu (*Desktop*) komputera PC0, wybierz *Command Prompt* i wykonaj polecenie telnet na adres IP routera. Sprawdź, czy połączenie przy obecnej konfiguracji powiedzie się.

1.3 Skonfiguruj połączenie z routerem przez SSH.

Czas skonfigurować na routerze te rzeczy, których jeszcze nie skonfigurowaliśmy, a są wymagane do uruchomienia połączenia z routerem przez SSH.

a) Skonfiguruj nazwę domeny (np. example.com):

```
R1(config)#ip domain-name example.com
```

b) Stwórz konto użytkownika o nazwie *user* z hasłem *cisco*:

```
R1(config)#username user secret cisco
```

c) Wygeneruj 1024-bitowy klucz RSA:

```
R1(config)#crypto key generate rsa
...
How many bits in the modulus [512]: 1024
```

d) (Opcjonalnie) Wymuś na linii vty logowanie z lokalnej bazy użytkowników i przyjmowanie tylko ruchu SSH:

```
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
```

e) Przejdź do pulpitu (*Desktop*) komputera PC0, wybierz *Command Prompt* i sprawdź, czy połączenie SSH powiedzie się:

```
ssh -l user 192.168.0.1
```

2 Połączenie konsolowe w rzeczywistej sieci

2.1 Połącz się z laboratoryjnym switchem z wykorzystaniem serwera terminali.

W laboratorium istnieje serwer terminali — urządzenie, do którego schodzą się kable konsolowe z wszystkich urządzeń z szafy rackowej. Łącząc się z tym serwerem, możemy uzyskać dostęp do dowolnego uruchomionego urządzenia z laboratorium.

a) Utwórz połączenie pomiędzy rzeczywistym komputerem laboratoryjnym a serwerem terminali. Możesz zrobić to na 2 sposoby: albo wybierz *Start* $\Rightarrow$ *Programy* $\Rightarrow$ *LAB* $\Rightarrow$ *TS*, albo stelnetuj się (za pomocą Wiersza polecenia lub PuTTY) na adres 192.168.133.25.

b) Zaloguj się (zgodnie z instrukcją umieszczoną w banerze) jako użytkownik *user* z hasłem *cisco*. Przeczytaj instrukcję obsługi serwera terminali.

c) Pojedynczo, umawiając się z innymi kolegami z grupy, dokonaj za pomocą serwera terminali połączenia z przełącznikiem S3, wpisując jego nazwę w CLI serwera terminali (s3 lub S3).

d) Wciśnij Enter i poczekaj, aż uzyskasz połączenie z przełącznikiem. Możliwe, że będziesz musiał się do niego zalogować (hasło *cisco*).

e) Zobacz, że masz do niego pełny dostęp: przejdź do trybu uprzywilejowanego (z trybu użytkownika poleceniem *enable*, z trybu konfiguracyjnego poleceniem *end*) i wyświetl przykładowo tablicę MAC adresów poleceniem *show mac address-table*.

f) Będąc w trybie uprzywilejowanym, zamknij okno PuTTY z połączeniem z serwerem terminali, aby kolejna osoba mogła z niego skorzystać.

2.2 Połącz się z routerem przez port konsolowy w tradycyjny sposób — bez wykorzystania serwera terminali.

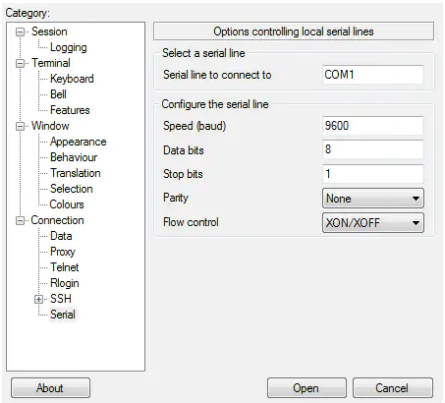
Przy każdym stanowisku do środkowego gniazda podłączony jest kabel, który wychodzi z portu szeregowego komputera. Drugi koniec tego kabla wyprowadzony jest na patch panelu w szafie rackowej — każde stanowisko ma na panelu swój port. Użyj go, aby połączyć się z laboratoryjnym routerem.

a) Poproś prowadzącego o skrętkę, po czym wepnij ją jednym końcem w port konsolowy wskazanego przez prowadzącego routera, a drugim — we wskazany port na patch panelu, do którego doprowadzony jest kabel z Twojego stanowiska.

b) Wróć do swojego komputera. Uruchom Menedżera urządzeń (*Start* ⇒ *Ustawienia* ⇒ *Panel sterowania* ⇒ *System* ⇒ *Sprzęt* ⇒ *Menedżer urządzeń*) i w sekcji Porty LPT i COM zobacz, jaki numer ma aktywny port COM.

c) Uruchom program PuTTY. W pierwszym oknie zaznacz opcję *Serial*, po czym wybierz z listy po lewej stronie *Serial* i doprezycuj parametry połączenia szeregowego:

- Serial line to connect to — właściwy port COM
- Speed: 9600
- Data bits: 8
- Stop bits: 1
- Parity: None
- Flow control: None



d) Otwórz połączenie i wciśnij Enter. Zobacz, że uzyskałeś dostęp do CLI urządzenia.

3 Obserwacja ruchu telnet

3.1 Połącz się z przełącznikiem laboratoryjnym za pomocą telnetu.

a) Przełącz się na kartę sieciową LAB, ustaw na niej właściwy adres IP z sieci 172.16.1.0/24.

b) Wejdź w Wiersz polecenia systemu Windows na swoim komputerze.

c) Stelnetuj się na laboratoryjny przełącznik sieciowy:

```
telnet 172.16.1.253
```

d) Zaloguj się na przełącznik, podając hasło *cisco*.

3.2 Przechwyć za pomocą programu Wireshark ruch telnet i przeanalizuj go.

a) Uruchom program Wireshark oraz przechwytywanie ruchu sieciowego (filtruj tak, by widoczny był tylko ruch telnet).

b) Przejdź do uruchomionego w poprzednim punkcie okna Wiersza polecenia z aktywnym połączeniem telnet z przełącznikiem. Przejdź do trybu uprzywilejowanego i wydaj jakiekolwiek polecenie (np. show running-config), aby wywołać ruch telnet.

```
Switch>enable
Password: [cisco]
Switch#show runn
```

c) Przejdź do okna Wiresharka i zatrzymaj przechwytywanie ruchu sieciowego.

d) Przyjrzyj się przechwyconemu ruchowi, przede wszystkim ostatniej sekcji. Zauważ, jak wszystko, co wykonywałeś na przełączniku lub przełącznik Ci zwracał, wysyłane było jawnym tekstem.

4 Zarządzanie plikami na urządzeniach Cisco

Będąc połączonym z przełącznikiem laboratoryjnym przez telnet, dokonaj przesłania kopii zapasowej pliku z konfiguracją bieżącą oraz obrazu systemu na swój komputer z wykorzystaniem TFTP.

4.1 Zrób kopię zapasową pliku z konfiguracją bieżącą przełącznika na serwerze TFTP (na swoim komputerze).

a) Uruchom program tftpd32 (*Start* ⇒ *Programy* ⇒ *tftpd32*).

b) Wydaj przełącznikowi polecenie przekopiowania pliku z konfiguracją bieżącą (*running-config*) na serwer TFTP:

```
SW1#copy running-config tftp:
```

Doprecyzuj adres serwera TFTP, na który chcesz wysłać plik (podaj adres IP swojego komputera) oraz zostaw domyślną nazwę pliku po wysłaniu. Powinieneś zaobserwować, że plik pojawił się na pulpicie Twojego komputera.

4.2 Zmodyfikuj na komputerze w niewielki sposób konfigurację przełącznika i wgraj ją z powrotem na przełącznik.

a) Znajdź wysłany przed chwilą plik z konfiguracją bieżącą przełącznika na swoim komputerze i otwórz go za pomocą Notatnika. Zobacz, jak konfiguracja urządzenia zapisana jest w formie pliku tekstowego.

b) Znajdź linijkę określającą nazwę urządzenia (*hostname*) i zmodyfikuj ją, np. zmieniając nazwę na SW + numer stanowiska (SW1, SW2, ..., SW10).

c) Uruchom program tftpd32 (*Start* ⇒ *Programy* ⇒ *tftpd32*).

d) Po kolei każda osoba w grupie, w porozumieniu z innymi, niech wysyła zmodyfikowany plik z konfiguracją z serwera TFTP na przełącznik:

```
SW1#copy tftp: running-config
```

Ponownie należy doprecyzować adres IP serwera TFTP (swojego komputera) oraz nazwę pliku z konfiguracją. Zauważ, jak przy każdej zmianie nowa konfiguracja jest natychmiast wdrażana — widać to po zmianie nazwy urządzenia.

4.3 Zrób kopię zapasową obrazu systemu przełącznika na serwerze TFTP (na swoim komputerze).

a) Uruchom program tftpd32 (*Start* ⇒ *Programy* ⇒ *tftpd32*).

b) Wyświetl zawartość pamięci flash przełącznika, aby zobaczyć nazwę pliku z obrazem systemu:

```
SW1#dir flash:
```

```
Router#dir flash:
Directory of flash:/

  3  -rw-   486899872          <no date>  isr4300-universalk9.16.06.04.SPA.bin
  2  -rw-       28282          <no date>  sigdef-category.xml
  1  -rw-      227537          <no date>  sigdef-default.xml

3249049600 bytes total (2761893909 bytes free)
```

Poszukaj pliku o charakterystycznej nazwie, dużym rozmiarze i rozszerzeniu .bin.

c) Wydaj przełącznikowi polecenie przekopiowania pliku z obrazem systemu na serwer TFTP:

```
SW1#copy flash: tftp:
```

Doprecyzuj adres serwera TFTP, na który chcesz wysłać plik (podaj adres IP swojego komputera), a także nazwę pliku z obrazem systemu oraz zostaw domyślną nazwę pliku po wysłaniu. Powinieneś zaobserwować, że po pewnym czasie plik pojawił się na pulpicie Twojego komputera.

Gdybyś chciał wykonać tę operację w odwrotną stronę — przekopiować za pomocą TFTP obraz systemu IOS ze swojego komputera na przełącznik, przykładowo w celu jego aktualizacji, należałoby wydać komendę odwrotną: *copy tftp: flash:*

V. Pytania kontrolne

1. Wymień różnice pomiędzy dostępem do urządzeń sieciowych poprzez port konsolowy a poprzez telnet/SSH.
2. Wymień różnice pomiędzy protokołem telnet a SSH.
3. Wymień, w jakich obszarach pamięci w urządzeniach Cisco przechowywane są pliki z: konfiguracją bieżącą, konfiguracją startową, obrazem systemu.