Sieci komputerowe

Wykład 10 — Zarządzanie urządzeniami sieciowymi

Marta Szarmach
Zakład Telekomunikacji Morskiej
Wydział Elektryczny
Uniwersytet Morski w Gdyni

05.2022

Plan prezentacji

1. Dostęp do urządzeń sieciowych

Dostęp zdalny (telnet i SSH) oraz lokalny (linia konsolowa)

1. Dostęp do urządzeń sieciowych

Definicja

Jako **dostęp do urządzeń sieciowych** rozumiemy uzyskanie możliwości operowania na CLI urządzenia (np. wydawania komend ciscowemu IOSowi) w celu konfiguracji danego urządzenia lub sprawdzenia jego stanu.

Dostęp może być realizowany lokalnie (łączymy się kablem bezpośrednio z konfigurowanym urządzeniem) lub zdalnie, z wykorzystaniem infrastruktury sieciowej (licząc się z tym, że o ile jest to sposób wygodniejszy, to jednocześnie mniej bezpieczny).

1. Dostęp do urządzeń sieciowych

Rodzaje dostępu:

Dostęp lokalny

- Wymaga fizycznej obecności przy urządzeniu
- Realizowany przy użyciu **portu konsolowego** i dedykowanego kabla
- Możliwość skonfigurowania urządzenia fabrycznie nowego

Dostęp zdalny

- Dostęp z innego miejsca (np. z biura) poprzez sieć
- Realizowany przez **telnet** albo **SSH**
- Urządzenie sieciowe musi być już wstępnie skonfigurowane (adres IP i włączony interfejs)

1.1 Dostęp do urządzeń sieciowych. Port konsolowy

Cechy dostępu poprzez port konsolowy:

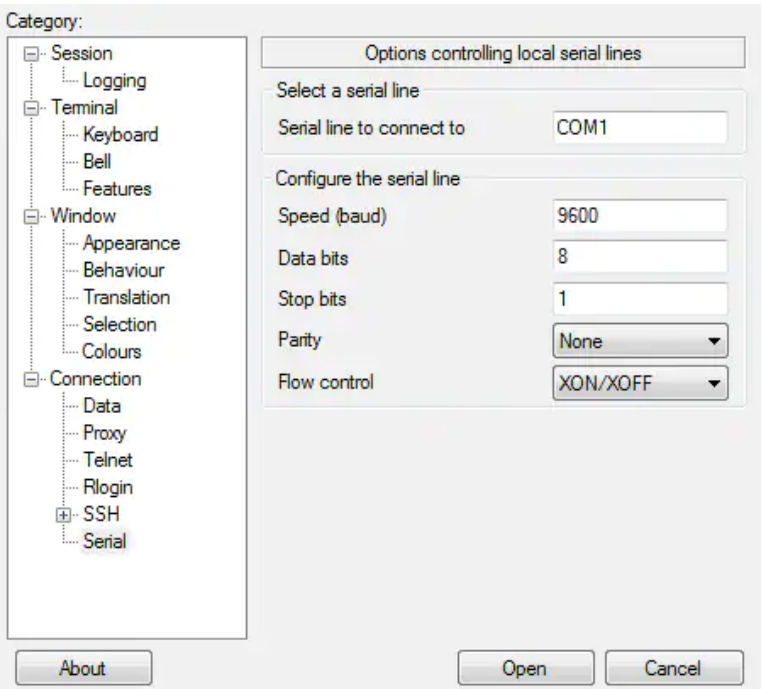
- Wymaga fizycznej obecności przy urządzeniu — musimy podłączyć się kablem konsolowym jednym końcem do portu konsolowego urządzenia, a drugim do portu szeregowego (ewentualnie portu USB przez przejściówkę) do naszego komputera, wyposażonego we właściwy terminal (np. PuTTY).
- Urządzenie konfigurowane nie wymaga żadnej wcześniejszej konfiguracji — jest to jedyny sposób na skonfigurowanie nowych urządzeń, z fabrycznymi ustawieniami.
- Dostęp może (i powinien) być chroniony hasłem (*line con 0 password*).

1.1 Dostęp do urządzeń sieciowych. Port konsolowy

Przykładowy port i kabel konsolowy:

1.1 Dostęp do urządzeń sieciowych. Port konsolowy

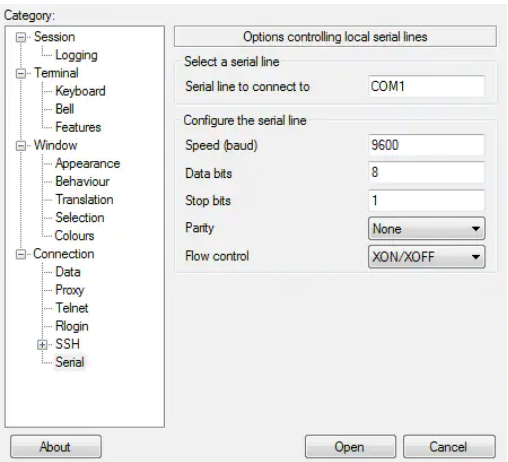
Dostęp przez port szeregowy z poziomu dowolnego terminala (np. PuTTY) — wymagane zdefiniowanie wymaganych parametrów



Grafiki: cisco.com

1.1 Dostęp do urządzeń sieciowych. Port konsolowy

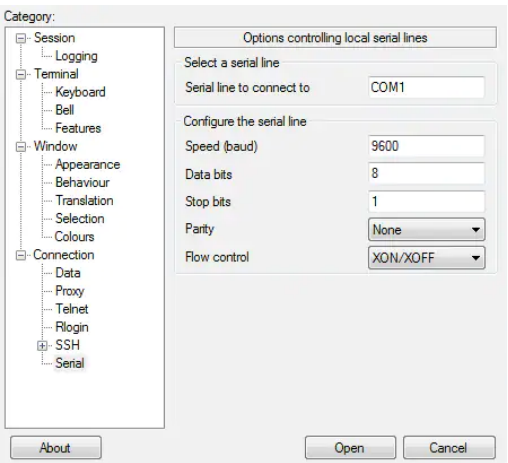
Parametry do skonfigurowania podczas otwierania połączenia szeregowego:



- **Nazwa otwartego portu szeregowego** (np. COM1) — do znalezienia w Menedżerze Urządzeń
- **Prędkość transmisji** (*baud rate/speed*) — właściwie ilość zmian sygnału w medium transmisyjnym w jednostce czasu (domyślnie 9600)
- **Wielkość ramki danych** (*data bits*) — domyślnie 8
- **Ilość bitów stopu** (*stop bits*) — sygnał zakończenia ramki, domyślnie 1

1.1 Dostęp do urządzeń sieciowych. Port konsolowy

Parametry do skonfigurowania podczas otwierania połączenia szeregowego:



- **Rodzaj parzystości** (*parity*) — służy do sprawdzania poprawności przesłanych danych; wymusza uzupełnianie ramki tak, by przesłany bajt był liczbą parzystą (*even*) lub nieparzystą (*odd*)
- **Kontrola przepływu** (*flow control*) — pozwala odbiornikowi na wysłanie informacji zwrotnej do nadajnika o zwolnieniu transmisji (np. poprzez linie CTS (*Clear To Send*) i RTS (*Ready To Send*)).

1.2 Dostęp do urządzeń sieciowych. Telnet

Cechy protokołu telnet:

- Umożliwia zdalny dostęp do CLI urządzenia sieciowego.
- Wykorzystuje model klient-serwer.
- Działa na porcie 23 TCP.
- Dane wymieniane w ramach protokołu telnet nie są szyfrowane — stwarza to pewną lukę w bezpieczeństwie, gdyż dane te (np. komendy wydawane urządzeniom, konfigurowane hasła) przesyłane są jawnym tekstem i można je podsłuchać.
- Jedynym zabezpieczeniem jest możliwość logowania się (urządzenie, do którego uzyskuje się dostęp, może prosić o podanie hasła).

1.2 Dostęp do urządzeń sieciowych. Telnet

Konfiguracja telnetu na urządzeniach Cisco

Aby uruchomić dostęp przez telnet na urządzeniu Cisco, wystarczy skonfigurować hasło na liniach wirtualnych vty (oraz hasło do trybu uprzywilejowanego, jeśli chcemy mieć dostęp do trybów wyższych niż użytkownika):

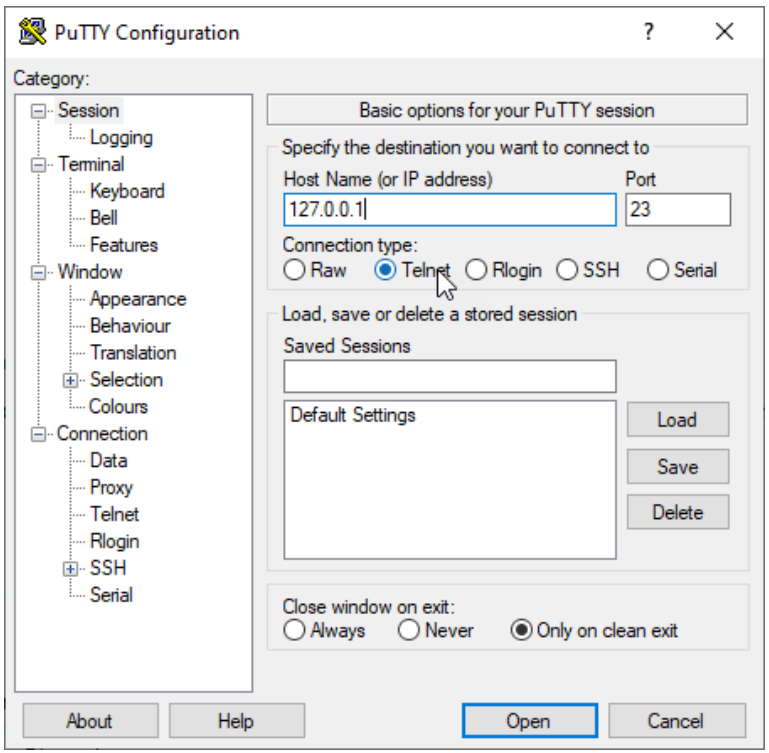
```
Router(config)#enable secret hasło
Router(config)#line vty 0 4
Router(config-line)#password hasło
Router(config-line)#login
```

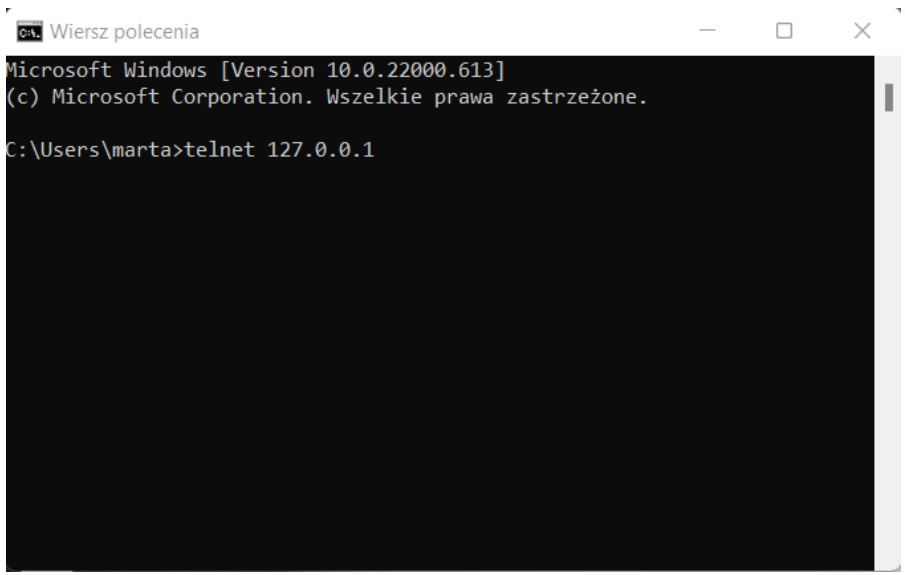
oraz nadać adres IP na interfejsie i go podnieść:

```
Router(config)#interface nazwa_interfejsu
Router(config-if)#ip address adres_IP maska_sieciowa
Router(config-if)#no shutdown
```

1.2 Dostęp do urządzeń sieciowych. Telnet

Dostęp przez telnet — z poziomu dowolnego terminala (np. PuTTY) lub windowsowego Wiersza polecenia:





Grafika: blog.octanetworks.com

1.3 Dostęp do urządzeń sieciowych. SSH

Cechy protokołu SSH (ang. *Secure Shell*):

- Umożliwia zdalny dostęp do CLI urządzenia sieciowego.
- Wykorzystuje model klient-serwer.
- Działa na porcie 22 TCP.
- Dane wymieniane w ramach protokołu SSH są szyfrowane — SSH jest więc udoskonaloną wersją telnetu. Do szyfrowania używany jest algorytm **RSA** (asymetryczny — kluczem publicznym dane są szyfrowane, a prywatnym odszyfrowane). Do bezpiecznej wymiany kluczy używany jest algorytm **Diffiego-Hellmana**, bazujący na trudności w rozkładzie dużych liczb na czynniki.

1.3 Dostęp do urządzeń sieciowych. SSH

Konfiguracja SSH na urządzeniach Cisco:

- Ustawienie nazwy urządzenia, domeny i hasła do trybu uprzywilejowanego (obowiązkowo):

```
Router(config)#hostname R1
R1(config)#ip domain-name example.com
R1(config)#enable secret hasło
```

- Wygenerowanie klucza RSA (np. 1024-bitowego):

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

- Stworzenie konta użytkownika:

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

1.3 Dostęp do urządzeń sieciowych. SSH

Konfiguracja SSH na urządzeniach Cisco:

- Skonfigurowanie adresu IP na interfejsie, podniesienie interfejsu (ethernetowego, vlan1)
- (Opcjonalne) Wymuszenie na linii vty logowania z lokalnej bazy użytkowników i przyjmowania tylko ruchu SSH:

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

Logowanie z Wiersza polecenia przez SSH:

```
ssh -l user docelowy_adres_IP
```

2. Pliki na urządzeniach sieciowych

Pliki konfiguracyjne i obraz systemu

2.1 Pliki na urządzeniach sieciowych. Pliki konfiguracyjne

Pliki konfiguracyjne na urządzeniach Cisco:

Running-config

- Zawiera konfigurację bieżącą (aktualnie działającą)
- Przechowywany w pamięci ulotnej RAM
- Tracony w momencie utraty zasilania/wyłączenia urządzenia (o ile nie przekopiowano jego zawartości do *startup-config*)

Startup-config

- Zawiera konfigurację, która ma być wdrożona wraz z uruchomieniem systemu
- Przechowywany w pamięci nieulotnej NVRAM
- Należy pamiętać o zaktualizowaniu pliku *startup-config* po wprowadzeniu zmian w konfiguracji

2.1 Pliki na urządzeniach sieciowych. Pliki konfiguracyjne

Zapisywanie konfiguracji bieżącej:

- Do *startup-config*:

```
Switch#copy running-config startup-config
```

- Na serwer TFTP:

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

- Z serwera TFTP:

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

- Przy zapisywaniu do/z serwera TFTP należy sprecyzować adres IP serwera oraz nazwę pliku (kreator prowadzi przez kolejne kroki)
- Na urządzeniu, na które wysyłany jest plik, musi być zainstalowane oprogramowanie tworzące serwer TFTP (np. tftpd32)

2.2 Pliki na urządzeniach sieciowych. Obraz systemu

Obraz systemu Cisco IOS:

- Przechowywany w pamięci nieulotnej flash
- System jest (domyślnie) bootowany podczas startu urządzenia właśnie z obrazu systemu
- Aktualizacja systemu odbywa się poprzez podmianę pliku z obrazem

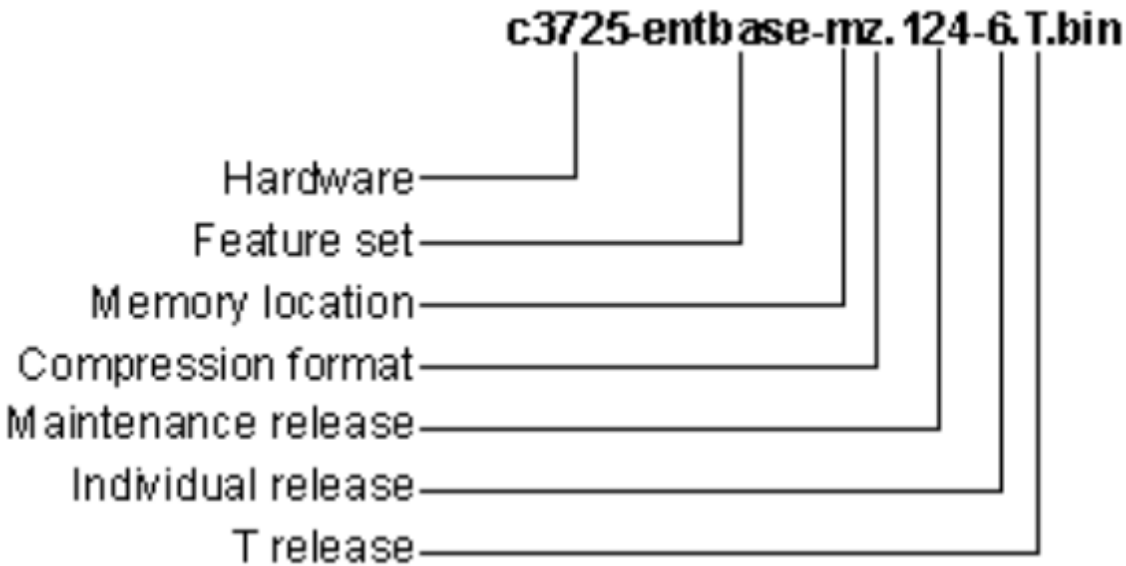
```
Router#dir flash:
Directory of flash:/

    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)
```

2.2 Pliki na urządzeniach sieciowych. Obraz systemu

Obraz systemu Cisco IOS — informacje zawarte w nazwie plików:



Grafika: cisco.com

2.2 Pliki na urządzeniach sieciowych. Obraz systemu

Zapisywanie obrazu systemu:

- Na serwer TFTP (zachowanie kopii zapasowej):

```
Switch#copy flash: tftp:
```

- Z serwera TFTP (np. w celu aktualizacji):

```
Switch#copy tftp: flash:
```

- Wskazujemy adres serwera TFTP oraz plik ze specyficzną nazwą oraz rozszerzeniem .bin, .tar lub .pie
- Podejrzenie zawartości pamięci flash komendą dir:

```
Switch#dir flash:
```

3. Protokół SNMP

Struktura systemu, baza MIB, komunikaty

3.1 Protokół SNMP. Definicja i rola

Definicja

Protokół SNMP (ang. *Simple Network Management Protocol*) jest protokołem umożliwiającym zarządzanie urządzeniami sieciowymi z jednego, centralnego punktu — odczytywanie informacji o ich stanie czy też wpływanie na ich działanie.

- Wykorzystuje port 161 (zazwyczaj UDP) oraz 162 (do wysłania komunikatów typu Trap)
- Wymieniane mogą być dane dotyczące m.in.: temperatury podzespołów, wielkości ruchu sieciowego, ilości błędów, zajętości pamięci i wiele innych, ale też tablic routingu, tablic MAC adresów.

3.2 Protokół SNMP. Struktura

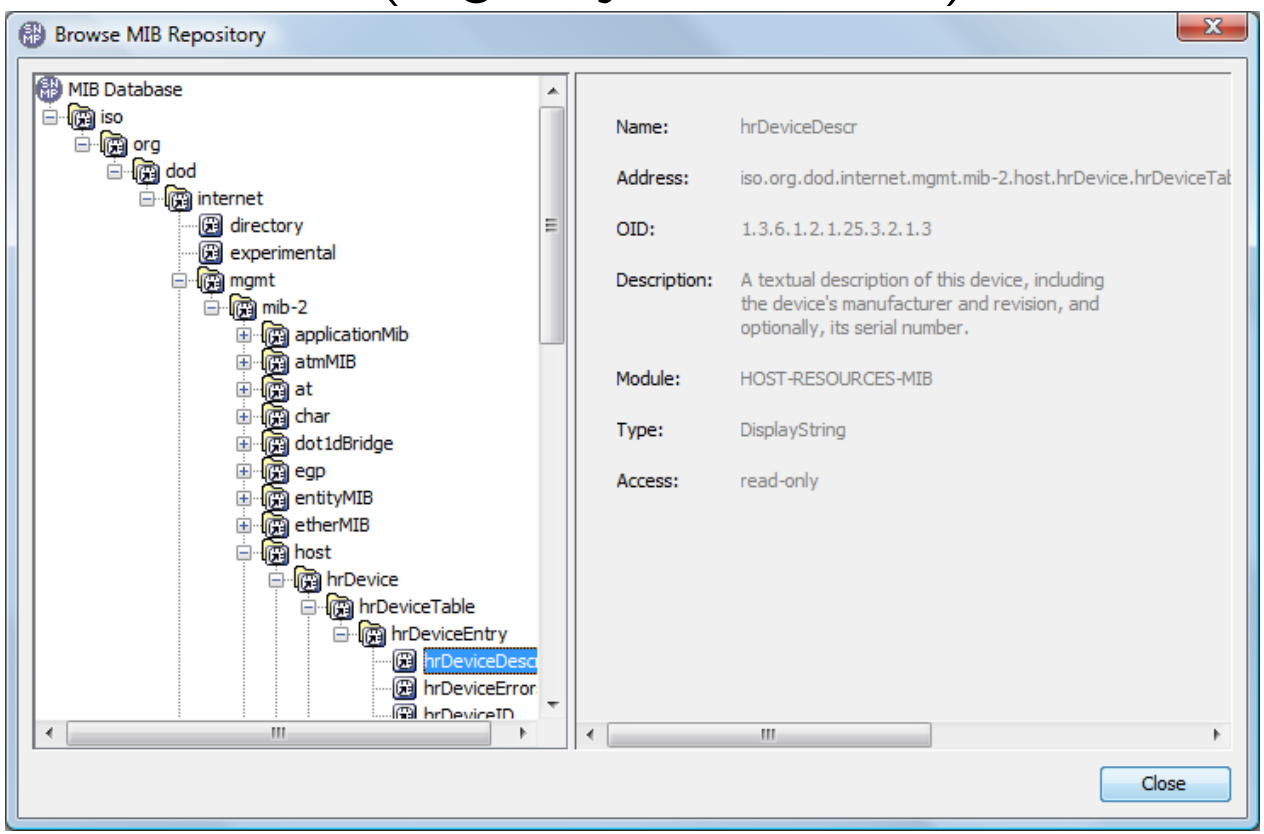
Budowa systemu bazującego na SNMP:

- SNMP wykorzystuje model klient-serwer: urządzenie administratora jest **managerem**, a na każdym urządzeniu zarządzanym jest zainstalowany **agent**.
- Przy próbie odczytu danych z agenta manager posługuje się hasłem odczytu (*public community string*), a przy próbie zapisu używany jest *private community string*.
- Agenci tworzą na zarządzanych urządzeniach bazę MIB (ang. *Management Information Base*), w której zapisywane są informacje o stanie urządzenia.

3.2 Protokół SNMP. Struktura

Budowa systemu bazującego na SNMP:

- Baza MIB ma hierarchiczną strukturę. Obiekty w bazie są pogrupowane w drzewo, do każdego prowadzi określona identyfikatorem OID (ang. *Object Identifier*) ścieżka.



Grafika: netiq.com

3.3 Protokół SNMP. Komunikaty

Rodzaje komunikatów w ramach SNMP — od agenta:

- **Response** — odpowiedź na żądanie managera
- **Trap** — informacja o zmianie stanu urządzenia (a'la przerwanie)

Rodzaje komunikatów w ramach SNMP — od managera:

- **Get** — zapytanie o wartość konkretnego obiektu z bazy MIB
- **GetNext** — zapytanie o wartość następnego obiektu niż ostatnio wywołany
- **GetBulk** — zapytanie o wartości w kilku obiektach
- **Set** — ustawienie wartości w danym obiekcie
- **Inform** — Trap wysłany pomiędzy managerami