Zarządzanie routerem CISCO

Routery Cisco podobnie jak to się ma z normalnymi komputerami są wyposażone w **procesor**, **płytę główną** a także **pamięć** a ich działaniem steruje **system operacyjny**. Systemem odpowiedzialnym za pracę routera jest **IOS** (ang. Internetwork Operation System). Więc jak widzisz czytelniku router ma wiele cech wspólnych z normalnym komputerem i tak należy go traktować jako komputer, który realizuje specyficzne czynności takie jak routing czy np. przetwarzania list ACL (zezwól/zabroń bądź przepuść/zablokuj – zasady odnoszące się do ruchu sieciowego)

Wyróżniamy następujące typy pamięci:

-
- **ROM** (ang. Read Only Memory) – pamięć tylko do odczytu w której znajdują się instrukcje rozruchowe wraz z programem bootującym czy tzw. miniIOS (okrojony system IOS, zawierający tylko podstawowe komendy),
- **RAM** (ang. Random Access Memory) – w pamięci tej przechowywane są informacje o bieżącej konfiguracji urządzenia (ang. running config), które jeśli nie zostaną zapisane są tracone w przypadku ponownego uruchomienia routera. Do pamięci RAM kopiowany jest również system operacyjny a dodatkowo w pamięci przechowywana jest **tablica routingu** (informacja o dostępnych sieciach – sieci bezpośrednio podłączone oraz sieci zdalne). Część pamięci wydzielona jest na **buforowanie pakietów** (miejsce w którym okresowo są zapisywane pakiety odebrane z jednego interfejsu przed przekazaniem go do innego) oraz na **bufor ARP** (pamięć przeznaczona na zapisywanie powiązań adres MAC – adres IP),
- **NVRAM** (ang. Nonvolatile Random Access Memory) – pamięć trwała, to na niej przechowywana jest konfiguracja początkowa routera (ang. startup config),
- **flash** – pamięć zawierająca system IOS, umożliwia dokonanie aktualizacji systemu.

Pracą routera Cisco steruje system operacyjny Cisco IOS. Cała procedura zarządzania routerem sprowadza się do wpisania odpowiednich poleceń za pomocą klawiatury w tzw. **trybie tekstowym** (ang. command-line interface). Możliwe jest skorzystanie z trybu graficznego wykorzystując do tego narzędzie **Cisco SDM** (ang. Cisco Security

Device Manager) ale wiąże się to z dodatkową konfiguracją routera a tak naprawdę tylko poprzez poznanie poleceń uzyskasz wiedzę o tym jak dany router działa i jak jest skonfigurowany. Tak naprawdę nie zniechęcam Cię czytelniku do wykorzystania tego sposobu konfiguracji routera lecz w pewnych sytuacjach łatwiej jest użyć linii poleceń zaś w innych środowiska graficznego (tworzenie ACL, Zone Based Firewall).

Każde urządzenie sieciowe posiada interfejsy. Interfejs routera umożliwia fizyczne połączenia go z innym urządzeniem.

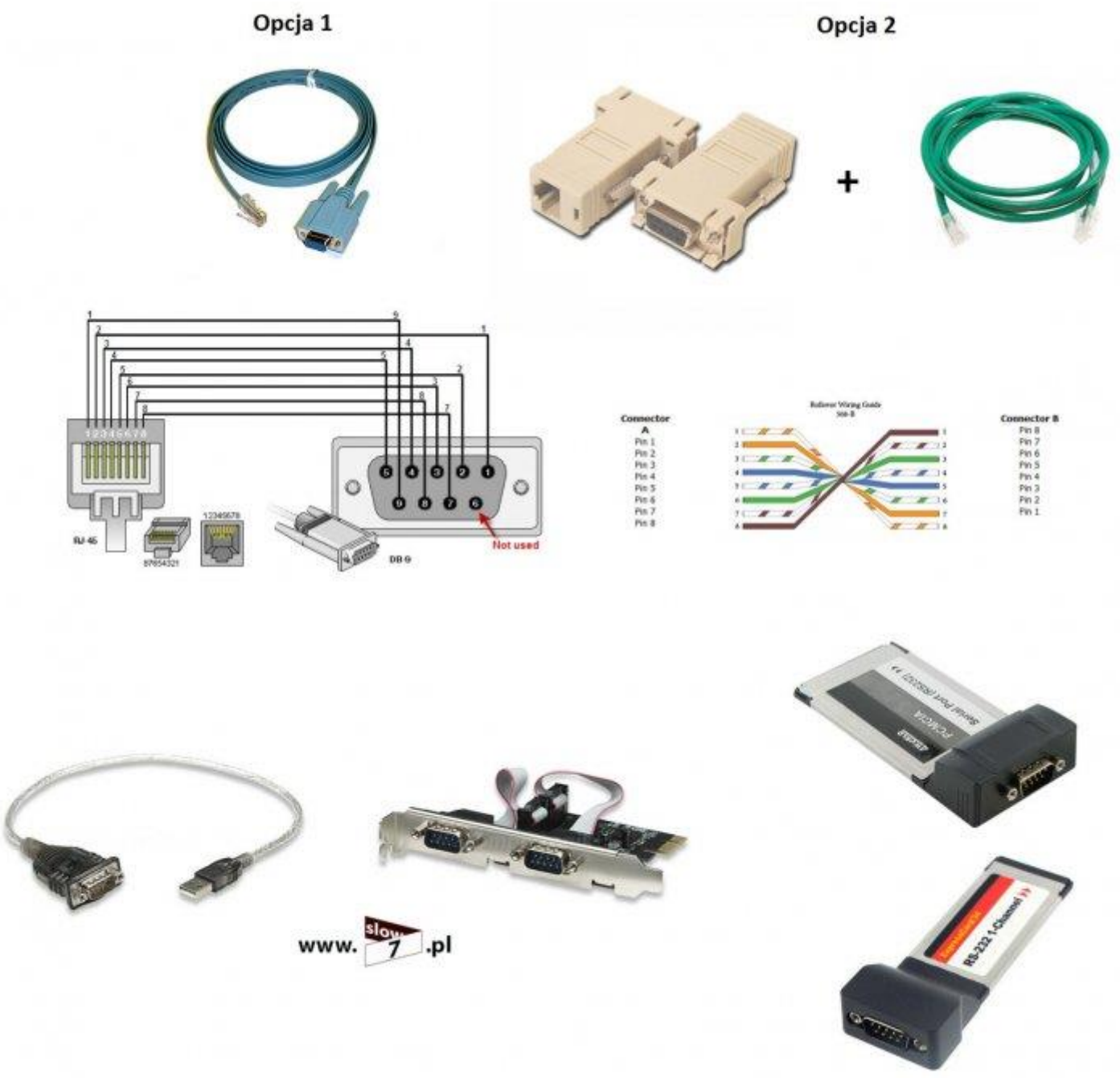
Każdy router Cisco wyposażony jest w interfejsy, które są zamontowane fabrycznie. Ich rodzaj i ilość zależy od konkretnego modelu routera. Dodatkowo budowa routerów Cisco opiera się na koncepcji modułowej, oznacza to że podstawowe funkcje routera mogą zostać rozszerzone poprzez zakup dodatkowych modułów, które to wzbogacają startowe możliwości urządzenia. Moduły te to tzw. karty WIC (ang. WAN Interface Card). Oczywiście router musi mieć możliwość ich zamontowania. Ilość kart, które można dołożyć do routera zależy również od konkretnego modelu urządzenia. Karta WIC jest modułem, który może przybrać różne kształty i postać a oferowana funkcja zależna jest od twoich potrzeb i potrzeb sieci a i niestety bardzo często o budżetu ponieważ niektóre moduły potrafią być naprawdę drogie.

Porty (interfejsy) z którymi najczęściej będziesz miał do czynienia to:

interfejsy ethernet służące do podłączenia kabla miedzianego, jak i światłowodowego. Uzależniony typ zależny jest od użytej technologii w sieci. Interfejsy jakie spotkasz będą zróżnicowane również pod względem oferowanej prędkości, spotkasz interfejsy standardu ethernet, fast ethernet oraz gigabit ethernet.

interfejsy szeregowe (ang. serial)umożliwiają np. łączenie sieci LAN za pomocą różnych technologii WAN.

port konsoli, oznaczony jako **CONSOLE**, podstawowy port umożliwiający konfigurację routera. Do podłączenia z routerem niezbędny jest przewód zakończony z jednej strony wtykiem RJ45 a z drugiej wtykiem DB9 (tzw. COM). Odpowiedni przewód najczęściej dostarczany jest razem z routerem choć niestety czasem się zdarza w szczególności gdy sprzęt kupujemy z drugiej ręki, że o odpowiednie okablowanie musimy zadbać sami. Możliwe jest zastosowanie przejściówek tj. adapter DB9-RJ45 plus tzw. **przewód odwrócony** (ang. rollover). Czasem większym problemem jest brak odpowiedniego złącza w komputerze ponieważ ten typ złącza (COM) jest już rzadko spotykany w nowych konstrukcjach płyt głównych. Ale i na to jest rada ponieważ można kupić adapter USB-COM lub skorzystać z kart rozszerzeń (laptopy) PCMCIA bądź ExpresCard. W przypadku komputerów stacjonarnych dozwolony jest zakup dodatkowej karty rozszerzeń na której będzie znajdować się potrzebne nam złącze. Karty rozszerzeń do działania wykorzystują interfejs PCI bądź PCI-e.



źródło: https://learningnetwork.cisco.com/thread/62578

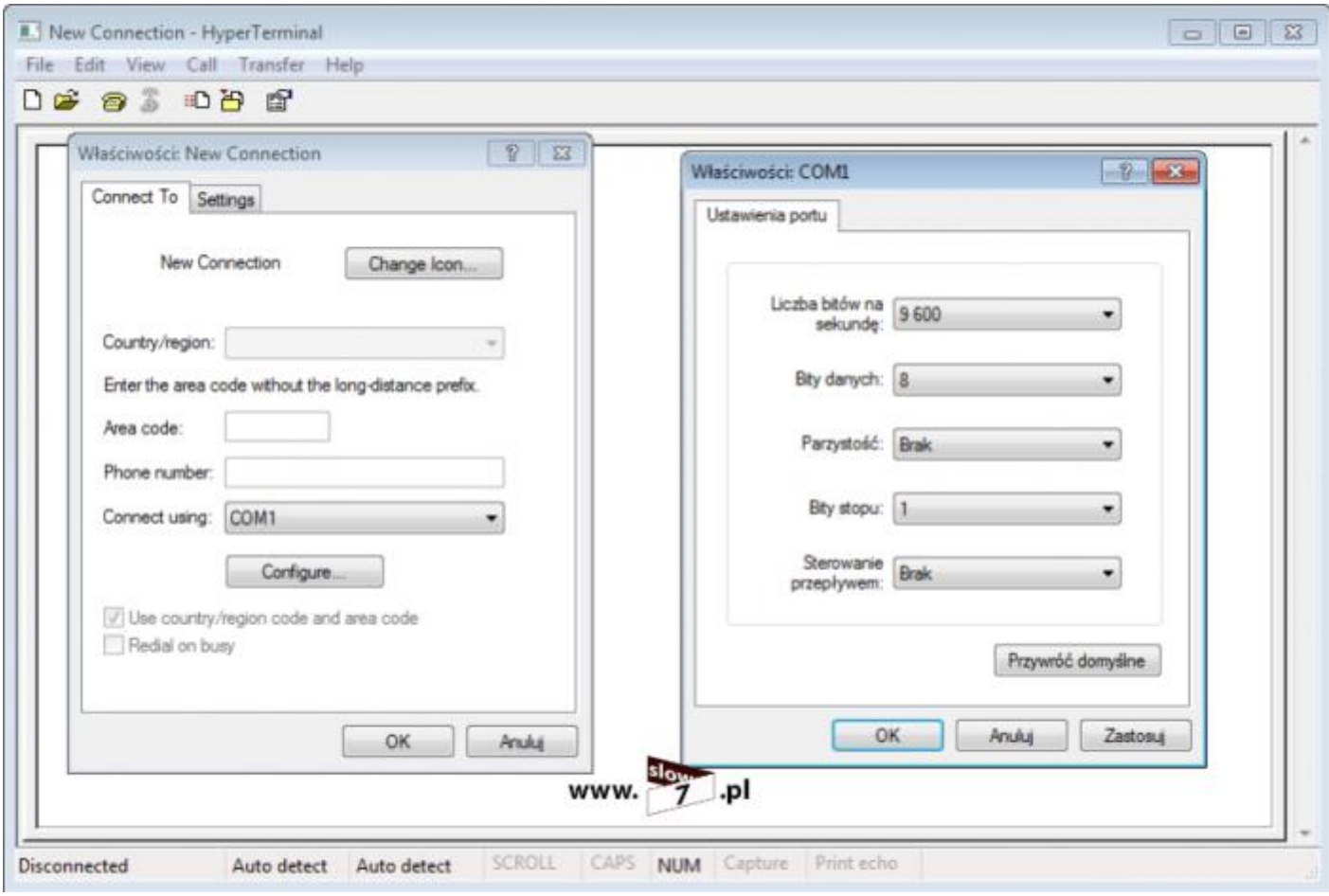
https://www.sonicwall.com/us/en/support/2213.html

Do konfiguracji routera wykorzystujemy program tzw. emulator terminalu. Do wyboru mamy windowsowy **HyperTerminal**bądź aplikację **PuTTY** lub **Tera Term**.

port AUX(ang. auxiliary)- podobnie jak to się ma z interfejsem konsolowym jest portem zarządzania routera. Z potem tym najczęściej łączy się modem celem wdzwonienia się do routera przez łącza telekomunikacyjne. Obecnie port AUX jest rzadko stosowany.

Gdy konfigurujemy router po raz pierwszy jedynym dostępnym sposobem jest skorzystanie z portu oznaczonego jako **CONSOLE**. Łączymy komputer jednym z sposobów podanych powyżej i uruchamiamy wybrany emulator terminali.
W przypadku gdy korzystasz z **HyperTerminal** kliknij menu **Start** i wybierz **Uruchom**. W oknie **Uruchamianie** wpisz **hypertrm** i naciśnij klawisz Enter. Program ten niestety dostępny jest standardowo tylko w systemie Windows XP i starszych. Microsoft w nowszych systemach tj. Vista, Windows 7 oraz Windows 8 aplikacji tej nie umieścił. Można temu szybko zaradzić (pod warunkiem, że mamy dostęp do Windows XP) kopiując poniższe pliki:
C:\Program Files\Windows NT\hypertrm.exe
C:\Windows\system32\hypertrm.dll
Program bez problemu uruchamia się w nowszych wersjach systemu Windows.
Korzystając z programu **HyperTerminal** (zresztą z pozostałych również) należy go odpowiednio skonfigurować. Oczywiście konfiguracja odnosi się do portu COM do którego podłączony jest router. Opcje, które należy podać to:

-
- Liczba bitów na sekundę (ang. Speed): 9600
- Bity danych (ang. Data bits): 8
- Parzystość (ang. Parity): brak
- Bity stopu (ang. Stop bits): 1
- Sterowanie przepływem (ang. Flow controlo): brak



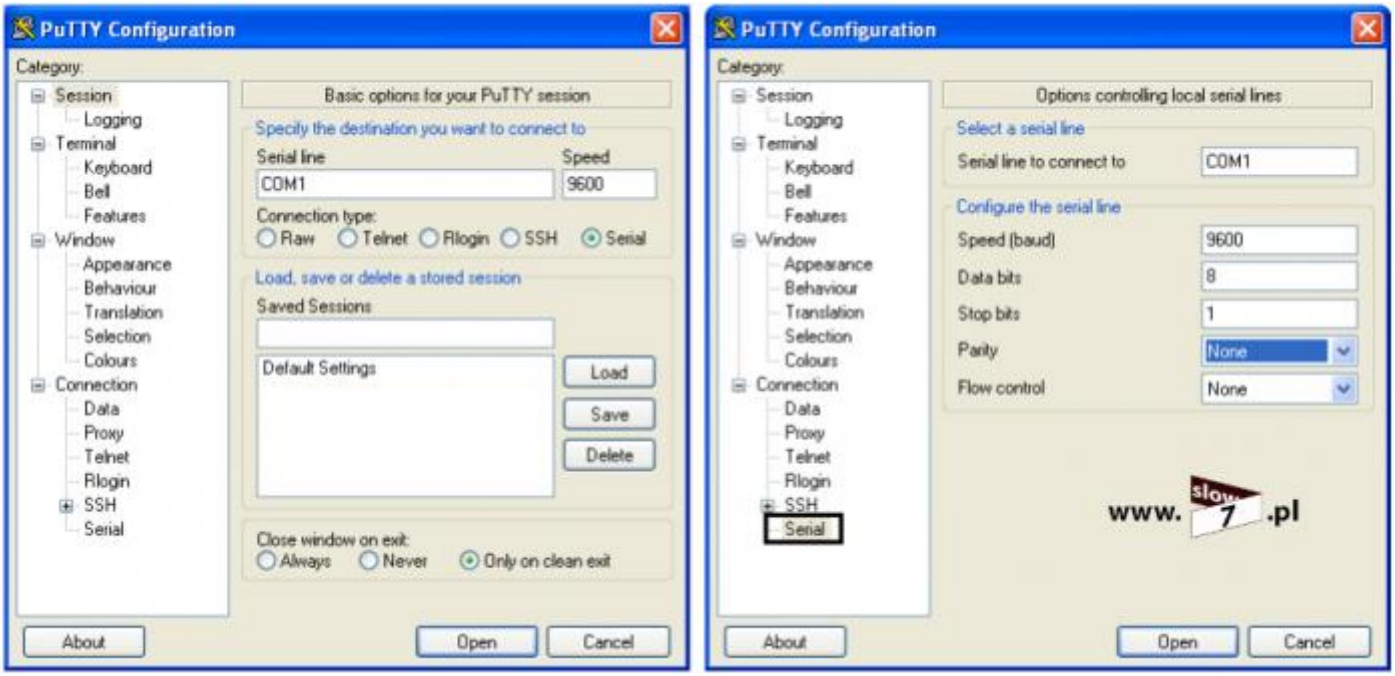
Po konfiguracji będzie można uzyskać połączenie z routerem.

Program **HyperTerminal** można wykorzystać również do zestawienia połączenia telnetowego. Program nie obsługuje połączeń szyfrowanych SSH.

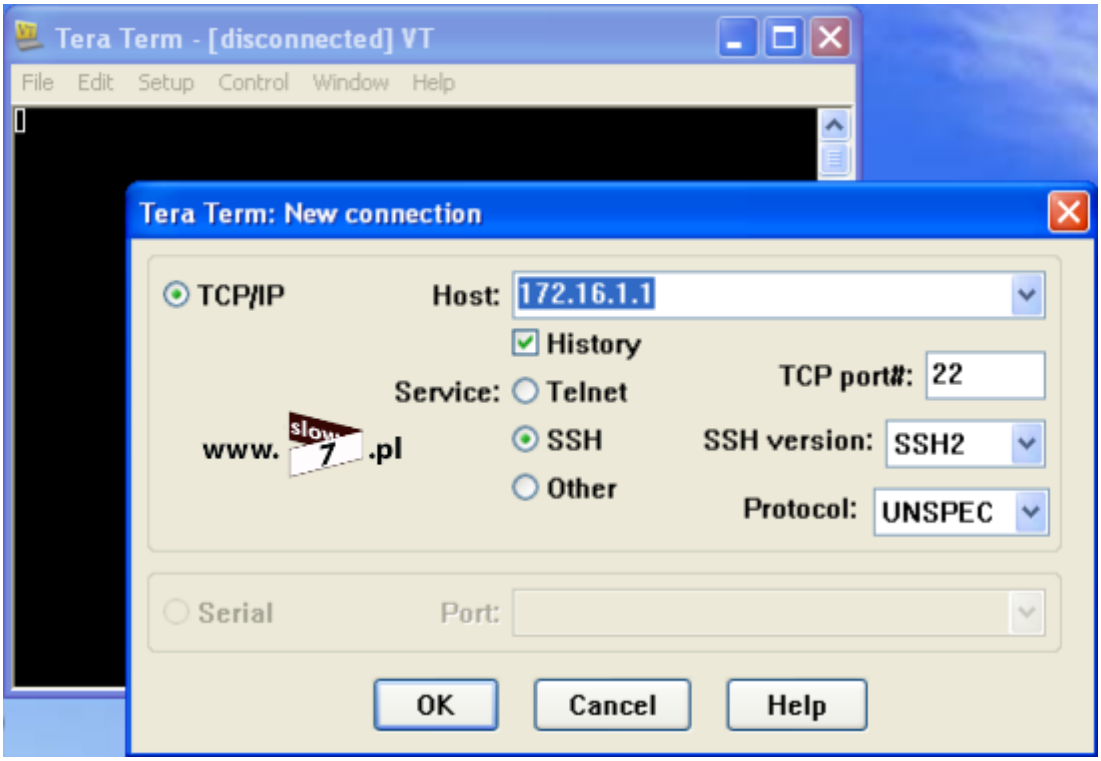
Drugim programem, który możemy użyć do uzyskania połączenia z routerem celem jego konfiguracji jest **PuTTY**. Program jest darmowy i możemy go pobrać z stąd: http://www.chiark.greenend.org.uk/~sgtatham/putty/

PuTTy jest klientem usług Telnet, SSH i Rlogin, działa pod systemami operacyjnymi Microsoft Windows oraz Unix/Linux.

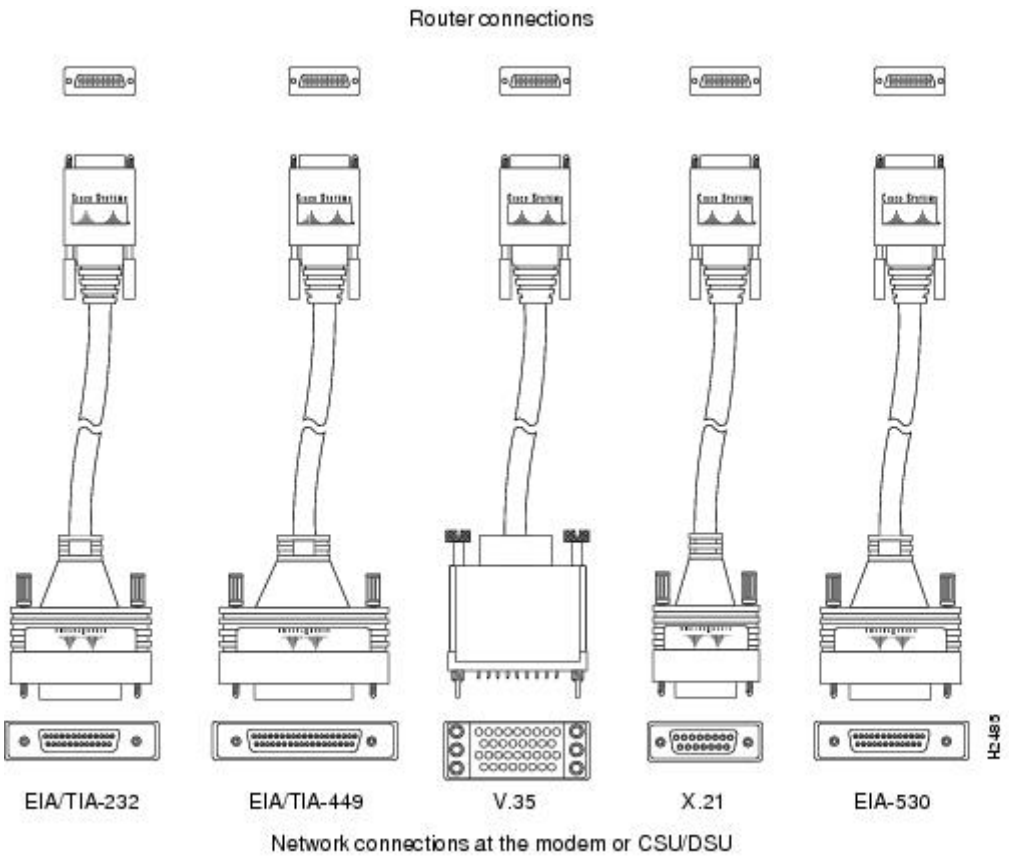
Konfiguracja sprowadza się do ustawienia opcji podanych już przy okazji konfigurowania programu **HyperTerminal** oraz wybraniu portu COM.



Kolejnym programem, który możemy użyć by zestawić połączenie z routerem jest **Tera Term**. Jest to darmowy, prosty program do obsługi połączeń modemowych oraz telnetowych. Program możemy pobrać np. z tej strony:http://logmett.com/index.php?/download/tera-term-480-freeware.html



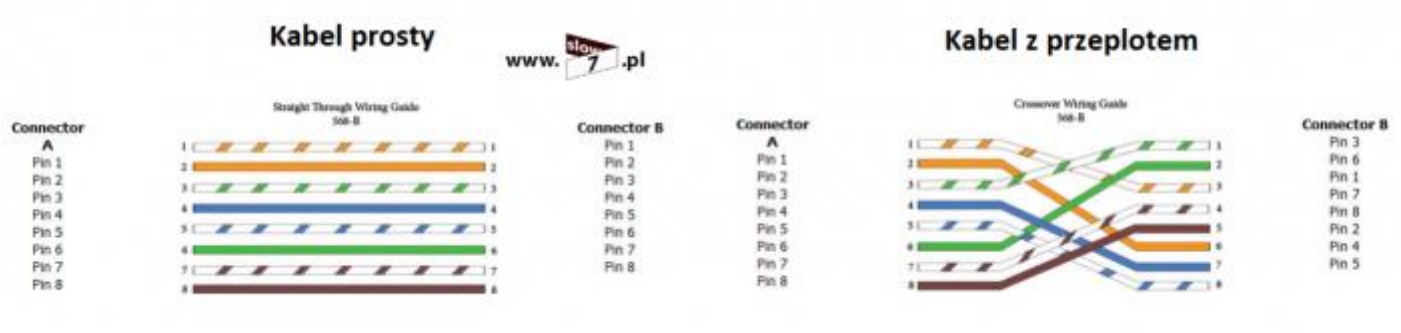
Routery Cisco jak już zostało wspomniane posiadają również złącza szeregowe, które mogą być użyte do podłączenia naszego routera z siecią WAN. Natomiast w laboratorium tego typu połączenia zestawiane pomiędzy routerami najczęściej symulują połączenia WAN. Aby wykorzystać tego typu złącza niezbędne jest dobranie odpowiedniego typu kabla a jak widać na rysunku poniżej router może obsługiwać różne typy złączy.



źródło: http://www.cisco.com/en/US/docs/wireless/mwr_1941/hardware_install/1941_hardware_install/guide/cablspec.html

Najczęściej stosowane są standardy EIA/TIA-232, EIA/TIA-449, V.35, X.21, EIA-530 i wszystkie te standardy reprezentowane przez odpowiednie złącza są łączone z portem DB-60 znajdującym się w routerze. Tak więc port ten może obsługiwać pięć różnych standardów okablowania. W nowych urządzeniach spotkamy się z interfejsem smart serial. Interfejs ten jest znacznie mniejszy od już zaprezentowanych i jednocześnie umożliwia zestawienia łącza o wyższej przepustowości.

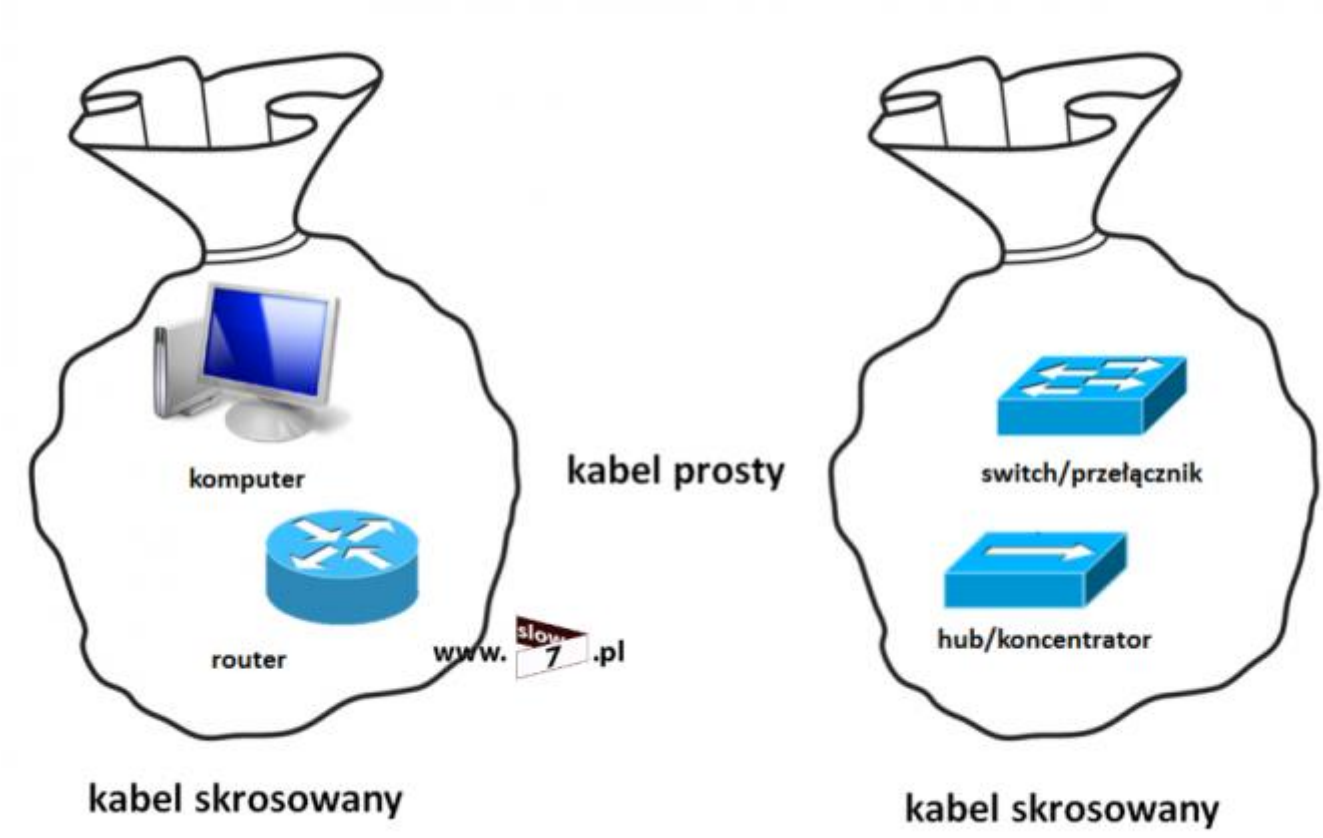
Jak już jesteśmy przy okablowaniu to warto jeszcze przypomnieć o zasadzie łączenia ze sobą różnych urządzeń sieciowych czyli kiedy użyć kabla prostego (ang. straight cable) a kiedy kabla z przeplotem (ang. crossover cable)?



Źródło: https://learningnetwork.cisco.com/thread/62578

Jak wiesz czytelniku to super a jeśli pytanie to sprawiło Ci trudność to już śpieszę z pomocą.

Wyobraź sobie dwa worki w jednym worku znajduje się komputer i router w następnym hub i switch. By łatwo zapamiętać jakiego kabla użyć, zastosuj o to taką zasadę: **w ramach jednego worka użyj kabla skrosowanego (z przeplotem) natomiast jeżeli będziesz łączył urządzenia, które znajdują się w różnych workach kabla prostego (be przeplotu)**.



Tak więc **kabel prosty** użyj w następujących połączeniach:

-

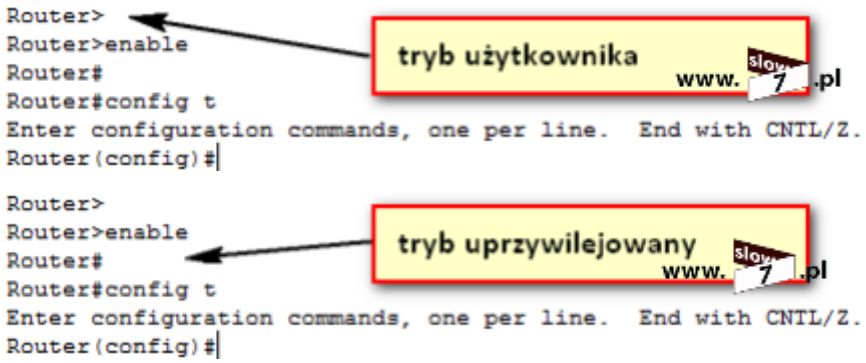
- komputer – przełącznik,
- komputer – hub
- router – przełącznik,
- router – koncentrator

  natomiast **kabel skrosowany** w połączeniach poniżej:

-

- komputer – komputer
- router – router
- komputer – router
- przełącznik – przełącznik
- koncentrator – koncentrator
- przełącznik - koncentrator

Podczas pracy z systemem IOS rozróżniamy różne tryby pracy routera. Każdy z trybów od pozostałych można rozróżnić po znaku gotowości (prompt), w zależności od ustalonego symbolu/składni wiemy, w którym miejscu systemu IOS się znajdujemy. Wykorzystywane tryby zależą od tego co aktualnie konfigurujemy ale możemy wyróżnić trzy z którymi będziemy mieli do czynienia najczęściej. Należą do nich **tryb użytkownika** (ang. user exec mode), **tryb uprzywilejowany** (ang. privileged mode) oraz **tryb konfiguracji** (ang. configuration mode).
Dla początkujących pewna uwaga - **dane polecenie jest dostępne i wykonywane w odpowiadającym mu trybie urządzenia**, więc gdy coś Ci nie wychodzi sprawdź czy polecenie, które wydajesz jest wydawane w odpowiednim trybie.



Tryb użytkownika ograniczony jest jedynie do przeglądania konfiguracji routera oraz monitorowania jego stanu. Zmiana konfiguracji routera w tym trybie jest niemożliwa. Tryb ten oznaczony jest znakiem **>**.

Drugi z dostępnych trybów to **tryb uprzywilejowany,** tryb ten identyfikowany jest przez znak gotowości **#**. Umożliwia pełną konfigurację routera a także przegląd wszystkich jego ustawień. Ze względu na możliwość zmiany sposobu działania routera przejście do tego trybu najczęściej jest zabezpieczone hasłem. Z tego trybu możliwy jest bezpośredni dostęp do **trybu konfiguracji routera**.

Tryb konfiguracji globalnej jest trybem służącym do konfigurowania podstawowych parametrów routera. W trybie tym mamy możliwość na zmianę takich parametrów jak: adresy IP dostępnych interfejsów routera, konfiguracja routingu statycznego i dynamicznego oraz wiele innych parametrów. Tryb ten rozpoznajemy po słowie **config** ujętym w nawiasie.

Podczas korzystania z konsoli można posiłkować się następującymi skrótami klawiaturowymi (niektóre skróty zależne są od użytego oprogramowania):

Tab - kończy jednoznaczne polecenie,

Ctrl+R - ponownie wyświetla linię,

Ctrl+Z - wychodzi z dowolnego trybu konfiguracji do trybu uprzywilejowanego,

Ctrl+N lub strzałka w górę - poprzednie polecenie,

Ctrl+P lub strzałka w dół - następne polecenie,

Ctrl+Shift+6 - przerywa wykonywane, bieżące polecenie (czasem trzeba wcisnąć dwukrotnie),

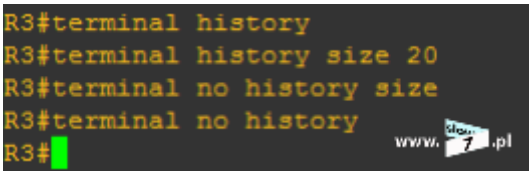
Ctrl+C - przerywa polecenie i opuszcza tryb konfiguracyjny,

Ctrl+A - przenosi na początek linii,

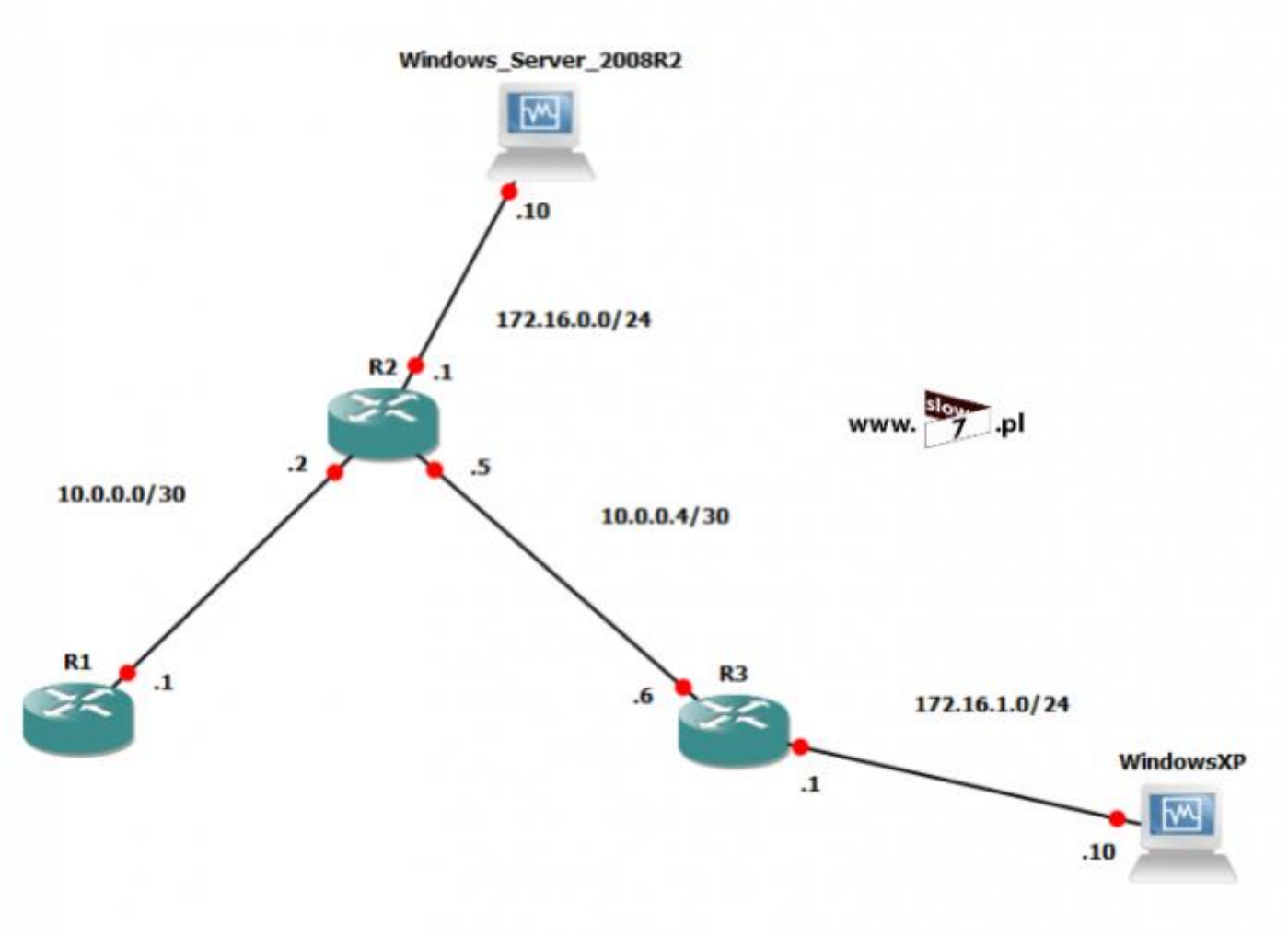
Ctrl+E - przenosi na koniec linii,

Ctrl-D - kasuje bieżący znak (zamiast przycisku Delete).

Możemy również sterować pracą samego terminala czyli ilością zapamiętywanych poleceń. Historia wpisywanych poleceń jest domyślnie włączona. Jakby z jakiegoś powodu udogodnienie te było wyłączone to można je uaktywnić za pomocą polecenia**terminal history**. Zmiana ilości zapamiętanych poleceń następuje za pomocą komendy -
terminal history size <ilość_poleceń>, wartości dozwolone od 0 do 256. Powrót do wartości domyślnych (10 ostatnich poleceń) następuje po wydaniu polecenia - **terminal no history size** natomiast wyłączenie historii wpisywanych poleceń**terminal no history**. Wszystkie polecenia wydajemy w trybie uprzywilejowanym.

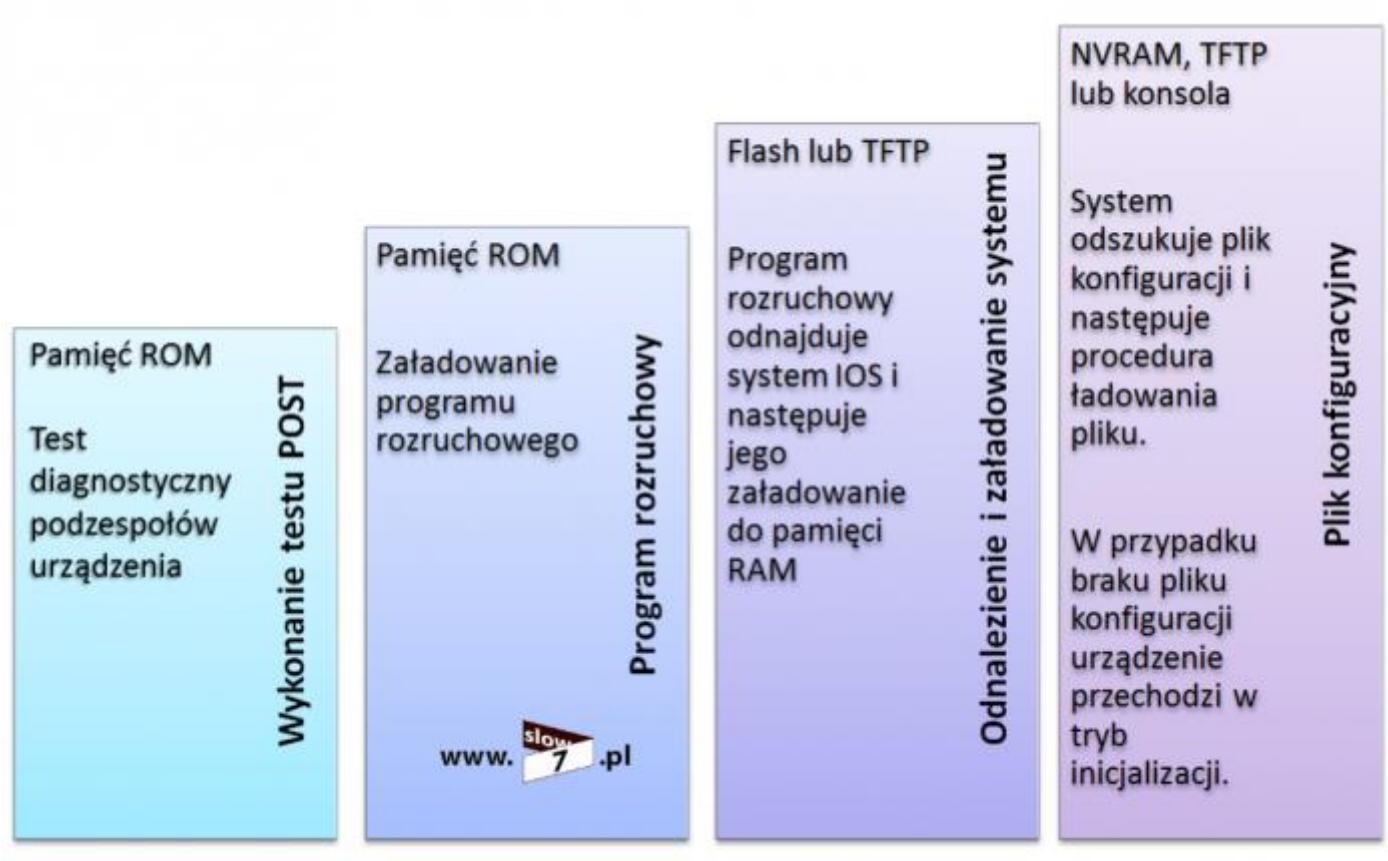


Celem szczegółowego omówienia wybranych opcji konfiguracji routera wprowadźmy następującą topologię sieci:



Sekwencja uruchomieniowa routera przebiega podobnie jak w przypadku normalnego komputera. Pierwszą czynnością jest zainicjalizowanie testu **POST** (ang. Power-On Self Test). Celem testu jest sprawdzenie wszystkich komponentów routera. Sprawdzane są następujące podzespoły: procesor, pamięć RAM, interfejsy.

Po przejściu testu **POST** router ładuje system IOS. Po załadowaniu IOS, router przechodzi do wczytania konfiguracji startowej routera, która najczęściej znajduje się w pamięci NVRAM (standardowe ustawienia choć możliwa jest zmiana lokalizacji pliku lokalizacji startowej). Jeśli plik konfiguracji jest odnaleziony następuje proces konfiguracji routera według danych zawartych w pliku konfiguracyjnym. Tak więc **konfiguracja startowa** (ang. startup-config) zapisana w pamięci NVRAM routera (choć może również być pobrana z serwera TFTP), ładowana jest podczas startu urządzenia. Schemat procesu startu można przedstawić za pomocą poniższego schematu.



W pliku konfiguracji startowej znajdują się m.in. takie informacje jak: adresy interfejsów, hasła, informacje o routingu a także inne bardziej szczegółowe ustawienia. Podczas rozruch zawartość pliku zostaje skopiowana tworząc tzw. **konfigurację bieżącą**(ang. running-config). Wprowadzając jakiekolwiek zmiany wprowadzamy je do **konfiguracji bieżącej** a ustawienia te obowiązują do momentu w którym router jest włączony. Jeśli nastąpi np. zanik napięcia i nastąpi ponowne uruchomienie routera,**konfiguracja bieżąca** jest kasowana i następuje ponowne załadowanie **konfiguracji startowej**. Dlatego jeśli wprowadzamy jakiekolwiek zmiany i chcemy by obowiązywały one z każdym uruchomieniem routera nie zapomnijmy zapisać bieżących ustawień. Do utworzenia pliku konfiguracji startowej służy polecenie: **copy running-config startup-config** (dawniej – **write memory**).

Jeśli z jakiś powodów spotkamy się z informacją o niemożliwości zapisania pliku konfiguracyjnego w pamięci NVRAM, to jest to najprawdopodobniej oznaka w której rozmiar zapisywanego pliku jest większy niż rozmiar dostępnej pamięci. W takim przypadku możemy zdecydować się na włączenie kompresji pliku konfiguracyjnego. Włączenie kompresji dokonujemy w **trybie konfiguracji globalnej** poprzez wydanie polecenia – **service compress-config**.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#service compress-config
R1(config)#exit
R1#
*Mar  1 00:24:49.019: %SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 988 bytes to 640 bytes[OK]
R1#
```

Jeżeli chcemy wykonać ponowny rozruch routera wydajemy polecenie - **reload**
Nazwę routera zmieniamy w **trybie konfiguracji** wydając polecenie **hostname <nazwa_routera>**. Nazwa routera używana jest przez serwer DNS celem odwzorowania jej na adres IP.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname routerTEST
routerTEST(config)#
```

Ustawienie czasu i daty dokonuje się w **trybie uprzywilejowanym** za pomocą polecenia **clock set <gg:mm:ss> <dzień> <miesiąc> <rok>**

```
routerTEST#clock set 10:59:00 30 December 2013
routerTEST#
*Dec 30 10:59:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:22:37 UTC Fri Mar 1 2002 to 10:59:00 UTC M
on Dec 30 2013, configured from console by console.
routerTEST#show clock
10:59:55.863 UTC Mon Dec 30 2013
routerTEST#
```

Czas na routerze może być synchronizowany za pomocą serwera czasu NTP (ang. Network Time Protocol). Serwer czasu może być uruchomiony w naszej sieci lub można skorzystać z serwerów czasu dostępnych w Internecie. W naszym przykładzie router R2 jest źródłem czasu dla pozostałych urządzeń. Celem ustawienia źródła synchronizacji czasu wydajemy polecenie **ntp server <adres_serwera_synchronizacji>** -oczywiście można podać kilka źródeł z których czas będzie zynchronizowany.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp server 10.0.0.2
R1(config)#end
R1#
.Jan  5 17:14:06.675: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

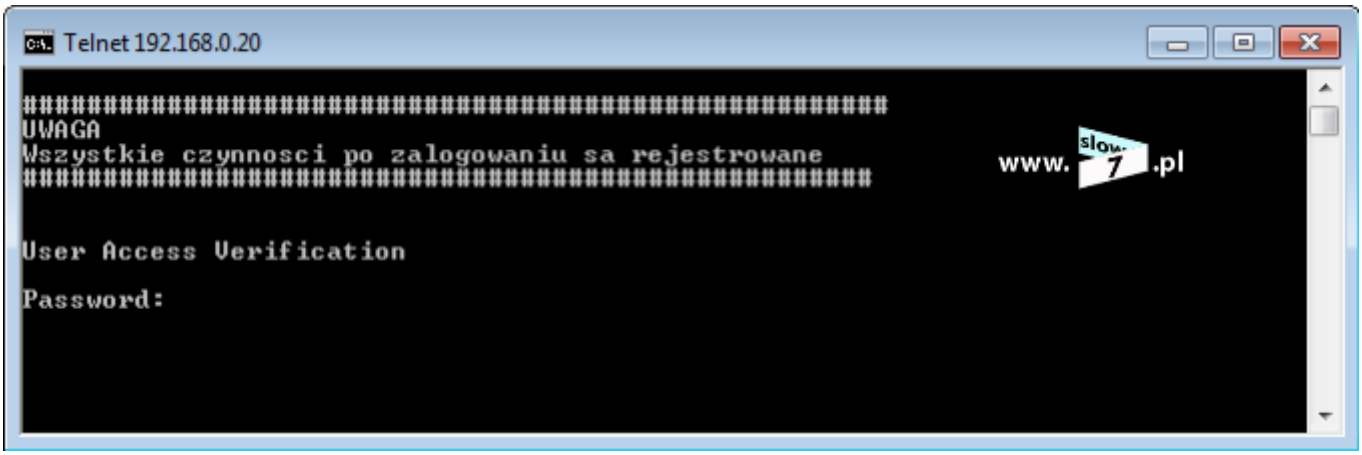
Stan synchronizacji z serwerem czasu sprawdzamy za pomocą polecenia - **show ntp associations**.

```
R1#show ntp associations
      address         ref clock       st  when  poll reach  delay  offset    disp
*~10.0.0.2       .LOCL.           1     0    64  377    12.0    5.91    13.2
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
R1#
```

Nie we wszystkich urządzeniach CISCO została zaimplementowana obsługa czasu realizowana dzięki protokołowi NTP. Jeśli urządzenie nie obsługuje protokołu NTP to najprawdopodobniej poradzi sobie z protokołem SNTP (ang. Simple Network Time Protocol) będącym podzbiorem standardu NTP. Aby włączyć protokół SNTP wydaj polecenie - **sntp server <adres_serwera_synchronizacji>**.
Konfiguracja routera umożliwia ustawienie szeregu bannerów powitalnych. Konfiguracja polega na użyciu polecenia **banner <rodzaj_ustawianego_banneru> <znak_początku/końca edycji>**. Polecenie wydajemy w **trybie konfiguracji globalnej**. Znak początku/końca edycji banneru dobieramy dowolnie a znak ten informuje router o zakończeniu tworzenia banera. Cały tekst banneru zawarty jest pomiędzy wybranym symbolem. Wybranego znaku nie używamy w tekście tworzonego banneru, ponieważ użycie go spowoduje zakończenie edycji.
Pierwszym bannerem, który możemy ustawić jest tzw. **banner MOTD** (ang. Message of the Day). Baner ustawiamy poleceniem**banner motd <znak_początku/końca edycji>**.

```
routerTEST#config t
Enter configuration commands, one per line.  End with CNTL/Z.
routerTEST(config)#banner motd %
Enter TEXT message.  End with the character '%'.
##########################################################
UWAGA
Wszystkie czynnosci po zalogowaniu sa rejestrowane
##########################################################
%
routerTEST(config)#
```

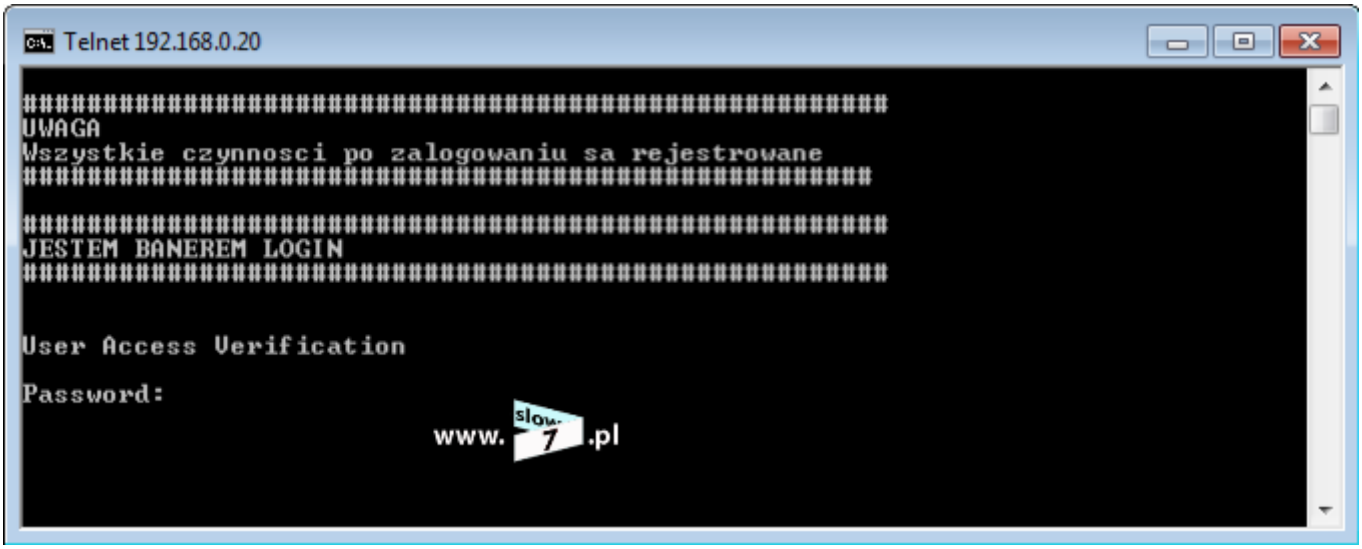
Banner ten pojawia się zaraz po nawiązaniu połączenia z routerem (poniżej przykład nawiązania połączenia z wykorzystaniem sesji telnet) a głównym celem stosowania banneru jest poinformowanie próbujących zalogować się użytkowników o konsekwencjach prawnych towarzyszących temu procesowi.



Banner LOGIN pojawia się po MOTD lecz przed zalogowaniem. Polecenie, które ustawia ten typ banneru to:
banner login <znak_początku/końca edycji>.

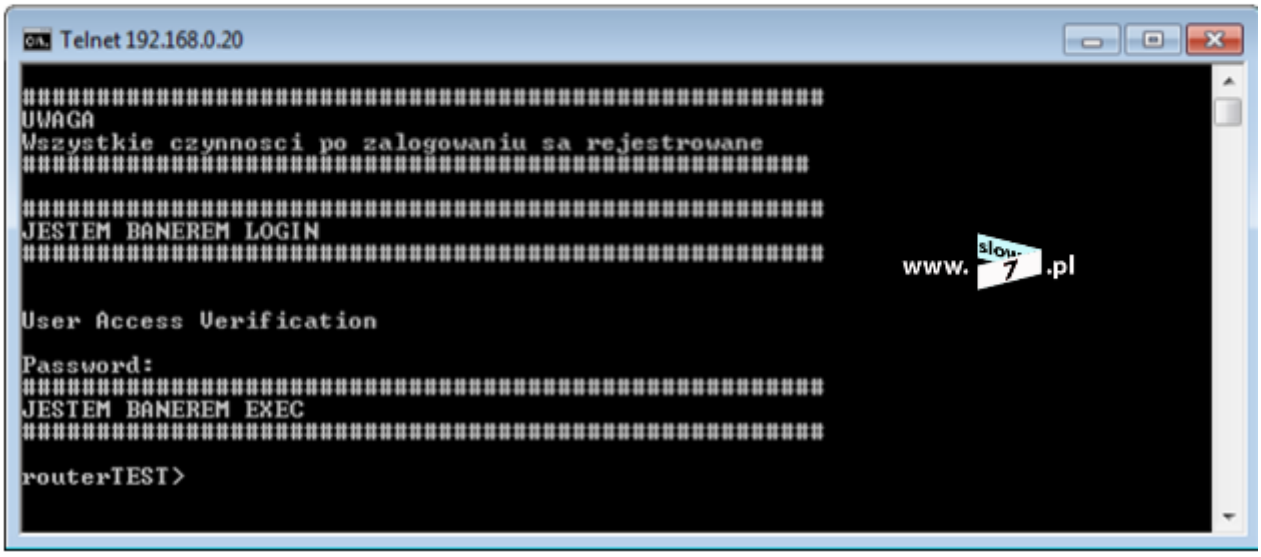
```
routerTEST#config t
Enter configuration commands, one per line.  End with CNTL/Z.
routerTEST(config)#banner login %
Enter TEXT message.  End with the character '%'.
##########################################################
JESTEM BANEREM LOGIN
##########################################################
%
routerTEST(config)#
```

Poniżej przykład włączenia banneru MOTD i LOGIN.



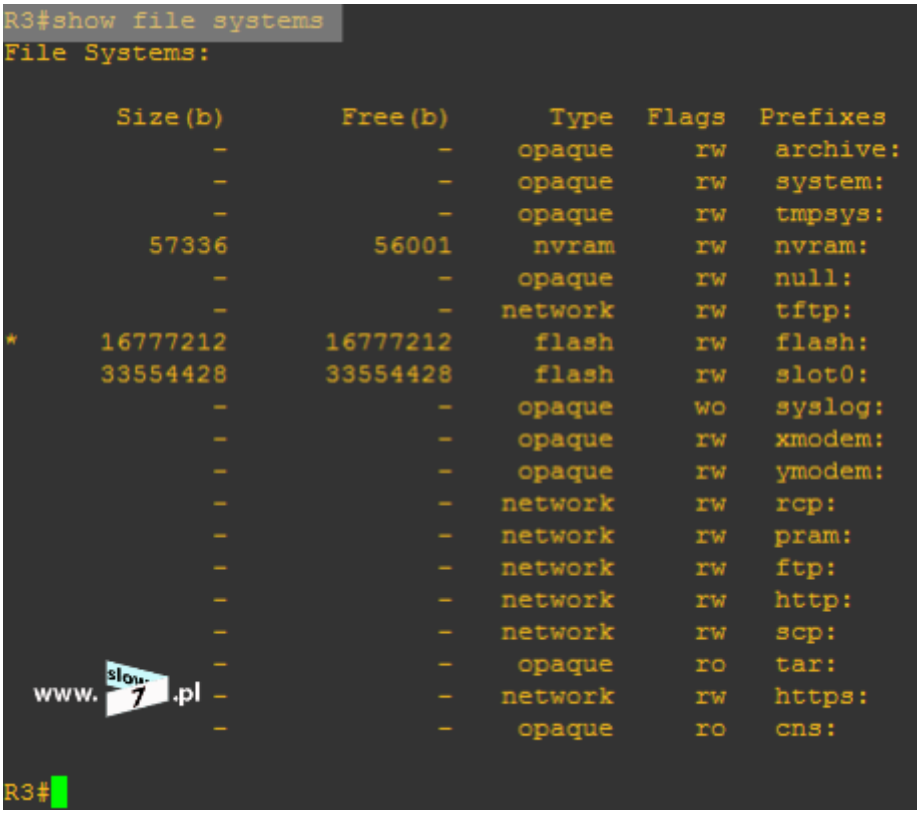
Banner EXEC jest trzecim typem ekranu informacyjnego, który możemy skonfigurować. Konfiguracja baneru składa się do wydania polecenia **banner exec <znak_początku/końca edycji>**. Banner ten pojawia się po poprawnym zalogowaniu się do routera.

```
routerTEST#config t
Enter configuration commands, one per line.  End with CNTL/Z.
routerTEST(config)#banner exec %
Enter TEXT message.  End with the character '%'.
##########################################################
JESTEM BANEREM EXEC
##########################################################
%
routerTEST(config)#
```



Banner usuwamy za pomocą polecenia: **no banner <motd | login | exec>**

Każdy router Cisco posiada pewną ilość miejsca, które jest przeznaczone na pliki systemu IOS (flash) oraz zapis konfiguracji (NVRAM). Dodatkowo pamięć możemy rozszerzyć poprzez dodanie dodatkowych kart flash (karta CF), ilość tych kart zależna jest od modelu routera ale najczęściej przyjmuje wartość od jednej do dwóch kart.
System routera został wyposażony w polecenia, które są odpowiedzialne za zarządzanie systemem plików routera oraz za zarządzanie plikami. Jedną z komend, która pozwala nam na poznanie ilości i typu zainstalowanej pamięci jest polecenie – **show file systems**.



Jak widać po powyższym zrzucie router dysponuje 55 kB pamięci NVRAM, 16 MB pamięci flash oraz 32 MB dodatkowej pamięci, która jest zamontowana w slot0.
Informacje o ilości dostępnego miejsca uzyskamy również po wydaniu polecenia – **show version**

```
Cisco 3725 (R7000) processor (revision 0.1) with 124928K/6144K bytes of memory.
Processor board ID FTX0945W0MY
R7000 CPU at 240MHz, Implementation 39, Rev 2.1, 256KB L2, 512KB L3 Cache
2 FastEthernet interfaces
DRAM configuration is 64 bits wide with parity enabled.
55K bytes of NVRAM.
16384K bytes of ATA System CompactFlash (Read/Write)
```

Polecenie **show version** dodatkowo zdradzi nam informacje o: wersji systemu IOS, interfejsach, położeniu systemu IOS, procesorze, ilości pamięci RAM, NVRAM oraz flash czy informacja o rejestrze konfiguracji.

Dokupienie kart CF i pozyskane w ten sposób dodatkowe miejsce możemy przeznaczyć np. na zapisanie konfiguracji routera. Po wydaniu komendy: **copy running-config slot0:** i podaniu nazwy pliku, kopia konfiguracji zostaje zapisana na karcie (zwróć uwagę na pytanie – **Erase slot0: before copying?**). Polecenie: **show <nośnik>** ukarze namstrukturę plików/katalogówzapisanych na danym nośniku.

```
R3#copy running-config slot0:
Destination filename [r3-confg]?
Erase slot0: before copying? [confirm]
Erasing the slot0 filesystem will remove all files! Continue? [confirm]
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Erase of slot0: complete
Verifying checksum...  OK (0xB24A)
875 bytes copied in 2.204 secs (397 bytes/sec)
R3#show slot0:

Slot0 CompactFlash directory:
File  Length   Name/status
  1   875      r3-confg
[940 bytes used, 33553488 available, 33554428 total]
32768K bytes of ATA Slot0 CompactFlash (Read/Write)
```

Na dodanej karcie (oczywiście jeśli mamy taką potrzebę) możemy wykonać proces partycjonowania. Proces ten polega na wydaniu polecenia: **partition <ilość_partycji> <rozmiar_partycji>**. Polecenie te w zależności od wersji oprogramowania jak i modelu routera wydajemy w trybie uprzywilejowanym bądź trybie konfiguracji. W przykładzie karta o pojemności 32 MB została podzielona na dwie partycje po 16 MB.

```
R3#partition slot0: 2 16 16
Partitioning will destroy all data in "slot0:".  Continue? [confirm]

Primary Partition created...Size 16 MB
Extended Partition created...Size 16 MB

Drive communication & 1st Sector Write OK...

Extended Partition entry 1 created...Size 16 MB
Extended Partition Table 1 Write OK...

Partition of slot0: complete
R3#
```


Utworzone partycje będą widoczne po wydaniu już znanego nam polecenia: **show file systems**

```
R3#show file systems
File Systems:

      Size(b)       Free(b)      Type  Flags  Prefixes
           -             -    opaque     rw   archive:
           -             -    opaque     rw   system:
           -             -    opaque     rw   tmpsys:
       57336         56001     nvram     rw   nvram:
           -             -    opaque     rw   null:
           -             -   network     rw   tftp:
*   16777212      16777212     flash     rw   flash:
           -             -      disk     rw   slot0:
           -             -    opaque     wo   syslog:
           -             -    opaque     rw   xmodem:
           -             -    opaque     rw   ymodem:
           -             -   network     rw   rcp:
           -             -   network     rw   pram:
           -             -   network     rw   ftp:
           -             -   network     rw   http:
           -             -   network     rw   scp:
           -             -    opaque     ro   tar:
           -             -   network     rw   https:
           -             -    opaque     ro   cns:
           -             -      disk     rw   slot0:0:
           -             -      disk     rw   slot0:1:
```


Próba wyświetlenia zawartości partycji (polecenie **show slo0:<numer_partycji>:** - pisane łącznie) zakończy się informacją o braku wykonania formatowania. Proces formatowania rozpoczyna się po wydaniu komendy – **format <miejsce_docelowe>**.

```
R3#show slot0:0:
Unformatted Partition, please format it.

R3#show slot0:1:
Unformatted Partition, please format it.

R3#format slot0:0:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "slot0:0:".  Continue? [confirm]
Writing Monlib sectors....
Monlib write complete

Format: All system sectors written. OK...

Format: Total sectors in formatted partition: 32736
Format: Total bytes in formatted partition: 16760832
Format: Operation completed successfully.

Format of slot0:0: complete
R3#format slot0:1:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "slot0:1:".  Continue? [confirm]
Format: All system sectors written. OK...

Format: Total sectors in formatted partition: 32736
Format: Total bytes in formatted partition: 16760832
Format: Operation completed successfully.

Format of slot0:1: complete
R3#
```

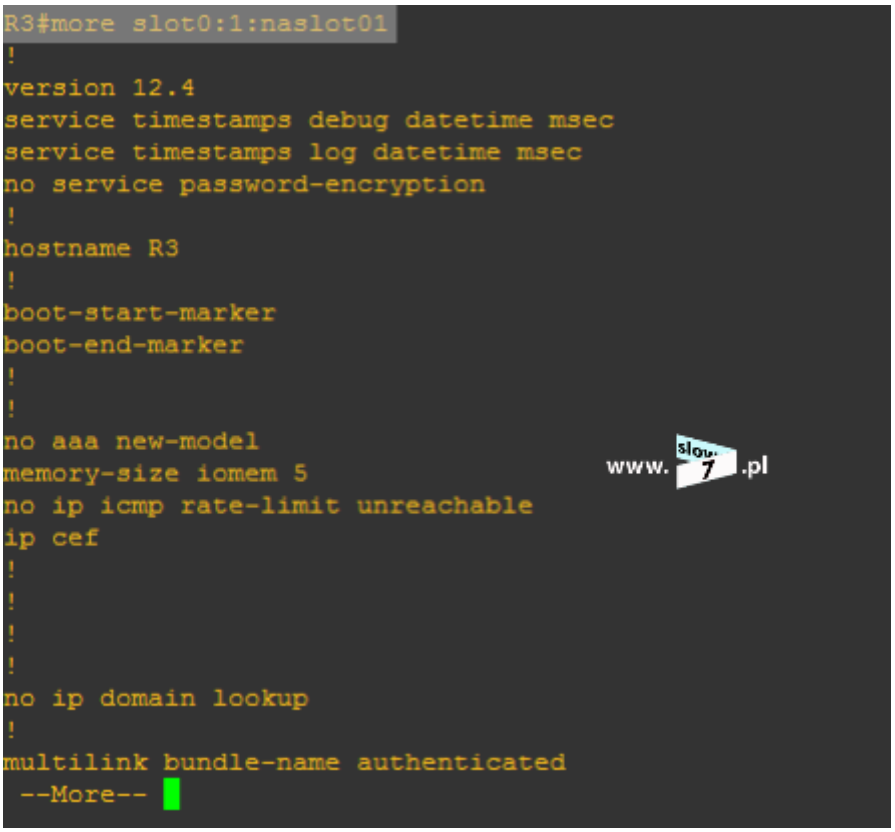

Po wydaniu polecenia **show file systems** uzyskamy informację o wielkości utworzonych partycji oraz ilości dostępnego miejsca.

```
R3#show file systems
File Systems:

     Size(b)       Free(b)      Type  Flags  Prefixes
           -             -    opaque     rw   archive:
           -             -    opaque     rw   system:
           -             -    opaque     rw   tmpsys:
       57336         56001     nvram     rw   nvram:
           -             -    opaque     rw   null:
           -             -   network     rw   tftp:
*   16777212      16777212     flash     rw   flash:
    16566272      16566272      disk     rw   slot0:#
           -             -    opaque     wo   syslog:
           -             -    opaque     rw   xmodem:
           -             -    opaque     rw   ymodem:
           -             -   network     rw   rcp:
           -             -   network     rw   pram:
           -             -   network     rw   ftp:
           -             -   network     rw   http:
           -             -   network     rw   scp:
           -             -    opaque     ro   tar:
           -             -   network     rw   https:
           -             -    opaque     ro   cns:
    16566272      16566272      disk     rw   slot0:0:#
    16703488      16703488      disk     rw   slot0:1:#
```

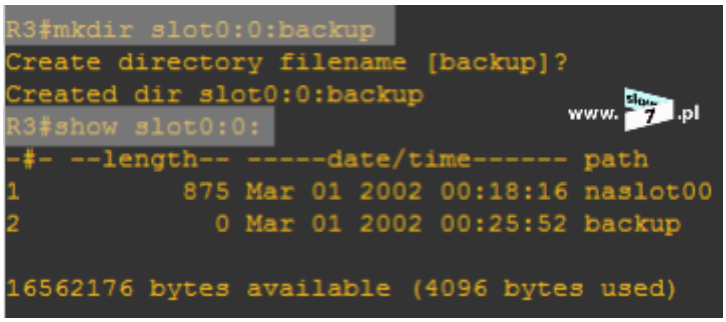

Po wykonaniu formatowania będzie możliwy zapis na partycjach. Poniżej została wykonana kopia konfiguracji routera na obu utworzonych partycjach (dwa pliki **naslot00** oraz **naslot01**).

```
R3#copy running-config slot0:0:
Destination filename [running-config]? naslot00

875 bytes copied in 1.488 secs (588 bytes/sec)
R3#copy running-config slot0:1:
Destination filename [running-config]? naslot01

875 bytes copied in 1.540 secs (568 bytes/sec)
R3#show slot0:0:
-#- --length-- -----date/time------ path
1           875 Mar 01 2002 00:18:16 naslot00

16564224 bytes available (2048 bytes used)

R3#show slot0:1:
-#- --length-- -----date/time------ path
1           875 Mar 01 2002 00:18:26 naslot01

16701440 bytes available (2048 bytes used)
```

Pokazanie zawartości pliku odbywa się za pomocą polecenia – **more <lokalizacja_pliku>**



Do utworzenia katalogu służy polecenie: **mkdir <ścieżka_katalogu>**



Przejście do danego katalogu umożliwi nam polecenie cd <ścieżka_katalogu> natomiast do wyświetlenia zawartości katalogu służy polecenie **dir**.

```
R3#cd slot0:0:backup
R3#dir
Directory of slot0:0:/backup/

No files in directory

16566272 bytes total (16562176 bytes free)
R3#
```

Kasowanie pliku odbywa się za pomocą polecenia **delete <ścieżka_kasowanego_pliku>**

```
R3#cd slot0:0:
R3#dir
Directory of slot0:0:/

    1  -rw-         875   Mar 1 2002 00:18:16 +00:00  naslot00
    2  drw-           0   Mar 1 2002 00:25:52 +00:00  backup

16566272 bytes total (16562176 bytes free)
R3#delete naslot00
Delete filename [naslot00]?
Delete slot0:0:/naslot00? [confirm]
R3#dir
Directory of slot0:0:/

    2  drw-           0   Mar 1 2002 00:25:52 +00:00  backup

16566272 bytes total (16564224 bytes free)
R3#
```

Uważny czytający na pewno dostrzeże analogię do systemu DOS jak i wiersza poleceń systemu Windows. Użyte polecenia w systemie IOS są tożsame z wymienionymi systemami operacyjnymi. Choć należy tu dodać, że nie wszystkie są one dostępne w każdym modelu routera a tak naprawdę zależne są od typu zastosowanego **systemu plików**. Cisco stosuje trzy różne **systemy plików** a oznacza je jako systemy plików klasy A, klasy B i klasy C.

W tabeli poniżej zebrano zastosowane systemy plików w zależności od modelu urządzenia (źródło: D. Hucaby, S. McQuerry – „Cisco Field Manual: Router Configuration”; K. Dooley, I. Brown – „Cisco IOS Cookbook”)

Typ routera	System plików
7000(RSP)	klasa A

7500(RSP2,4,8)	klasa A
12000	klasa A
LS1010	klasa A
Catalyst 6500 series	klasa A
1003	klasa B
1004	klasa B
1005	klasa B
1600	klasa B
1700	klasa B
2500	klasa B
2600	klasa B
3600*	klasa B
4000	klasa B
AS5200	klasa B
AS5300	klasa B
AS5800	klasa C
MC3810	klasa C
7100	klasa C
7200	klasa C

* - routery serii 3600 standardowo korzystają z systemu plików B lecz od wersji IOS 12.2(4)T dodano obsługę systemu plików klasy C

W drugiej zaś tabeli zebrałem dostępne polecenia, które dotyczą zarządzania plikami wraz z ich opisem oraz rodzajem systemu plików
(źródło: http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/frf006.html).

Polecenie	**System plików**	**Uwagi**
cd	wszystkie	zmiana katalogu
copy	wszystkie	kopiowanie plików
delete	wszystkie	kasowanie plików, zaznaczenie jako usunięte lecz bez fizycznego usunięcia
dir	wszystkie	wyświetlenie zawartości katalogu
erase	wszystkie	czyszczenie całej pamięci
format	A i C	formatowanie
fsck	C	sprawdzenie systemu plików
mkdir	C	tworzenie katalogu
more	wszystkie	wyświetlenie zawartości pliku

pwd	wszystkie	pokazuje lokalizację w której się aktualnie znajdujemy
rename	C	zmiana nazwy pliku
rmdir	C	kasowanie katalogu
squeeze	A	trwałe usunięcie plików zaznaczonych wcześniej za pomocą polecenia delete
undelete	A	przywrócenie plików zaznaczonych jako usunięte
verify	wszystkie	wyliczenie sumy kontrolnej pliku i sprawdzenie otrzymanej wartości z wartością zapisaną w danych obrazu

Do całkowitego skasowania nośnika wykorzystaj polecenie **erase <wybrany_nośnik>**.

```
R3#erase slot0:
Erasing the slot0 filesystem will remove all files! Continue? [confirm]
Current DOS File System flash card in slot0: will be formatted into Low End File System
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Erase of slot0: complete
R3#show slot0:

Slot0 CompactFlash directory:
No files in Slot0 CompactFlash
[0 bytes used, 33554428 available, 33554428 total]
32768K bytes of ATA Slot0 CompactFlash (Read/Write)
```

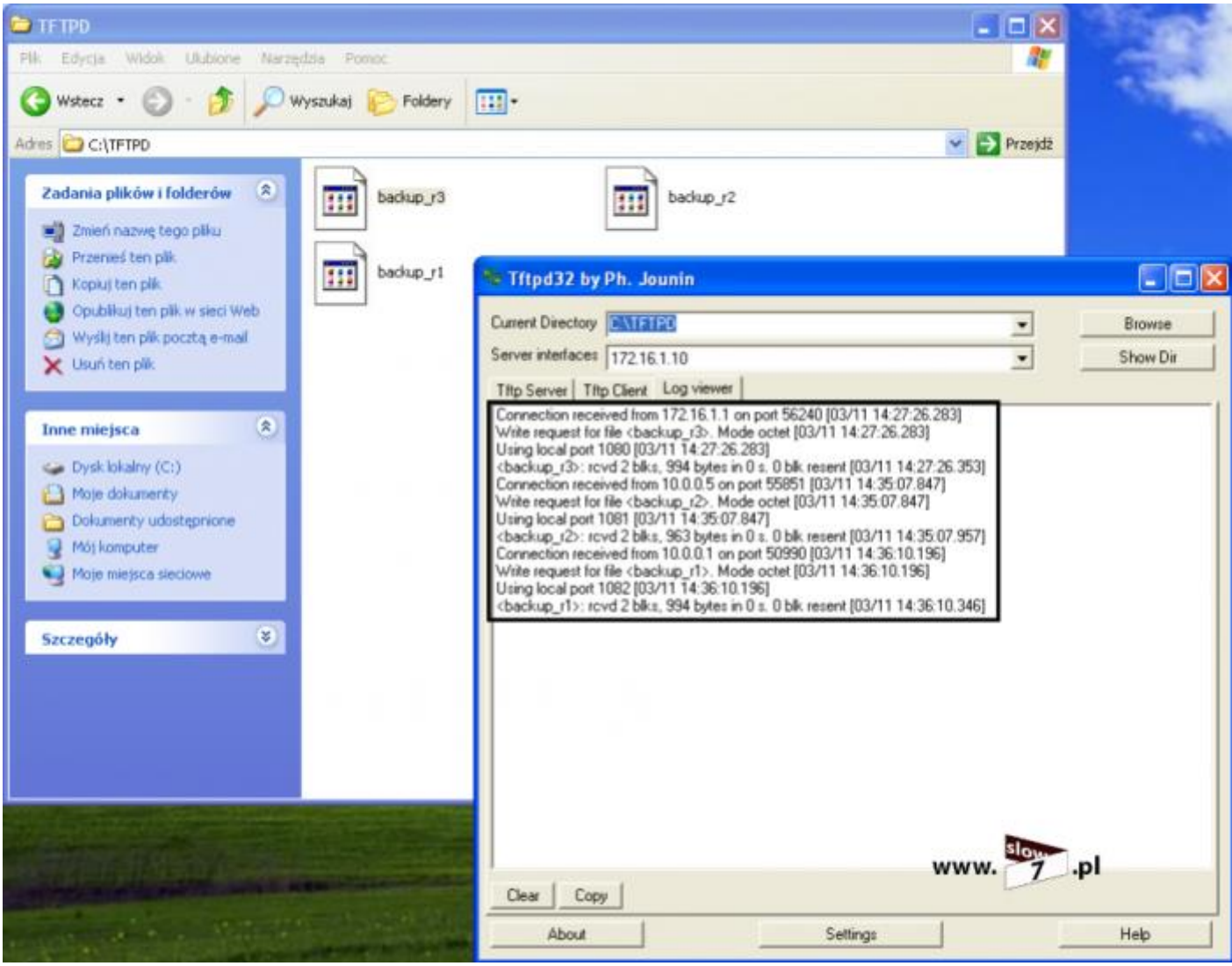
Aby wymazać konfigurację routera użyj polecenia **erase nvram** (w starszych urządzeniach **write erase**).

Warto wiedzieć, że celem wykonania kopii ustawień routera, jego konfigurację można zapisać na zewnętrznym serwerze **TFTP**(ang. Trivial File Transfer Protocol). **TFTP** jest prostym protokołem wykorzystywanym do przesyłania plików. Bazuje on na protokole UDP, jest bardziej „ubogim” bratem protokołu FTP – ponieważ nie może wyświetlać katalogów, ani uwierzytelniać użytkowników, a jego głównym zadaniem jak już zostało wspomniane jest odczyt i zapis plików na komputerze zdalnym. Celem wykonania kopii konfiguracji routera wydajemy polecenie: **copy running-config <tftp://adres_serwera/nazwa_pliku>>.**

Poniżej pokazano przykład wykonania kopii konfiguracji routera R3, plik konfiguracji bieżącej został zapisany na serwerze 172.16.1.10.

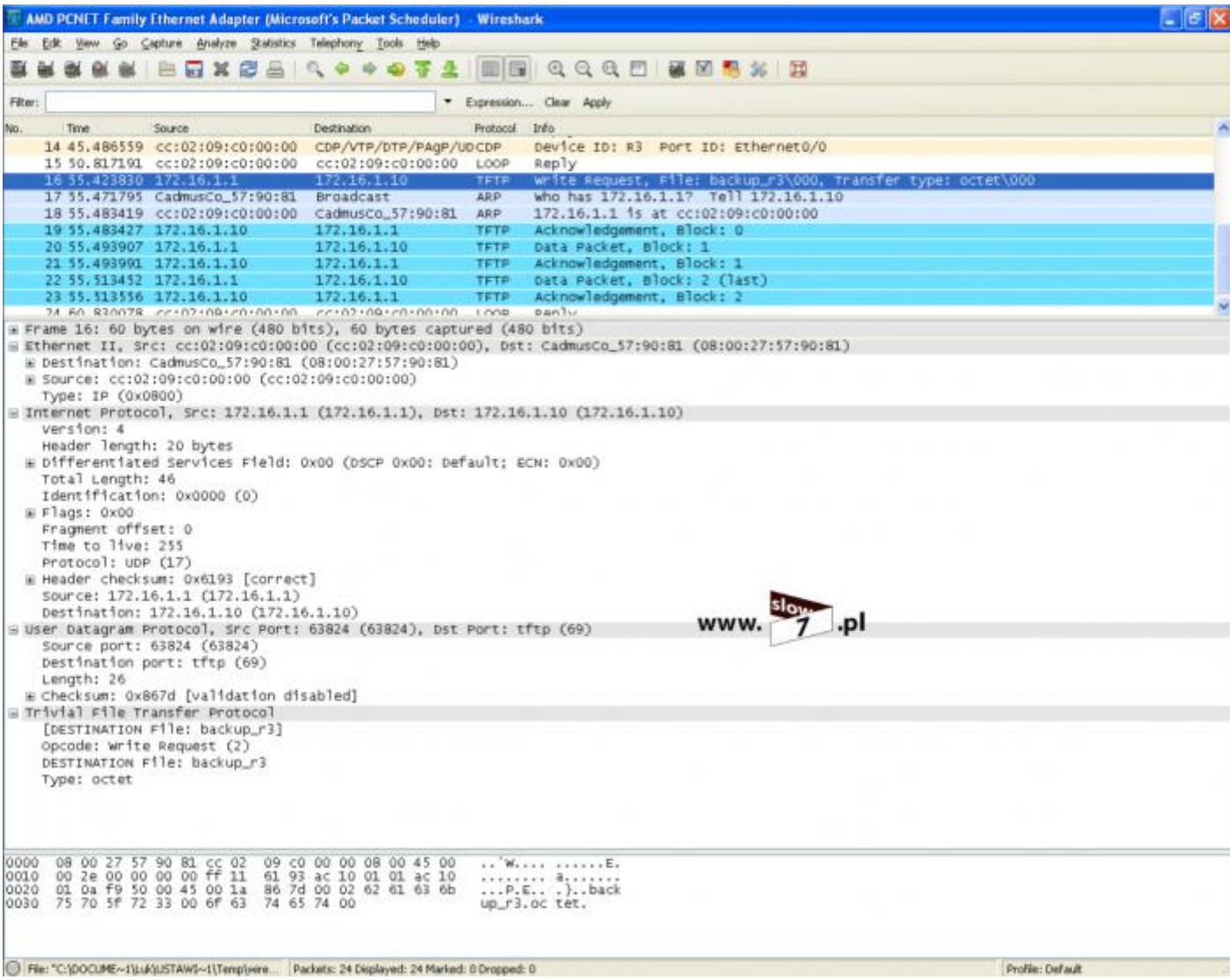
```
R3#copy running-config tftp://172.16.1.10/backup_r3
Address or name of remote host [172.16.1.10]?
Destination filename [backup_r3]?
!!
994 bytes copied in 0.672 secs (1479 bytes/sec)
R3#
```

Jak widać poniżej została również wykonana kopia ustawień routerów R1 oraz R2.



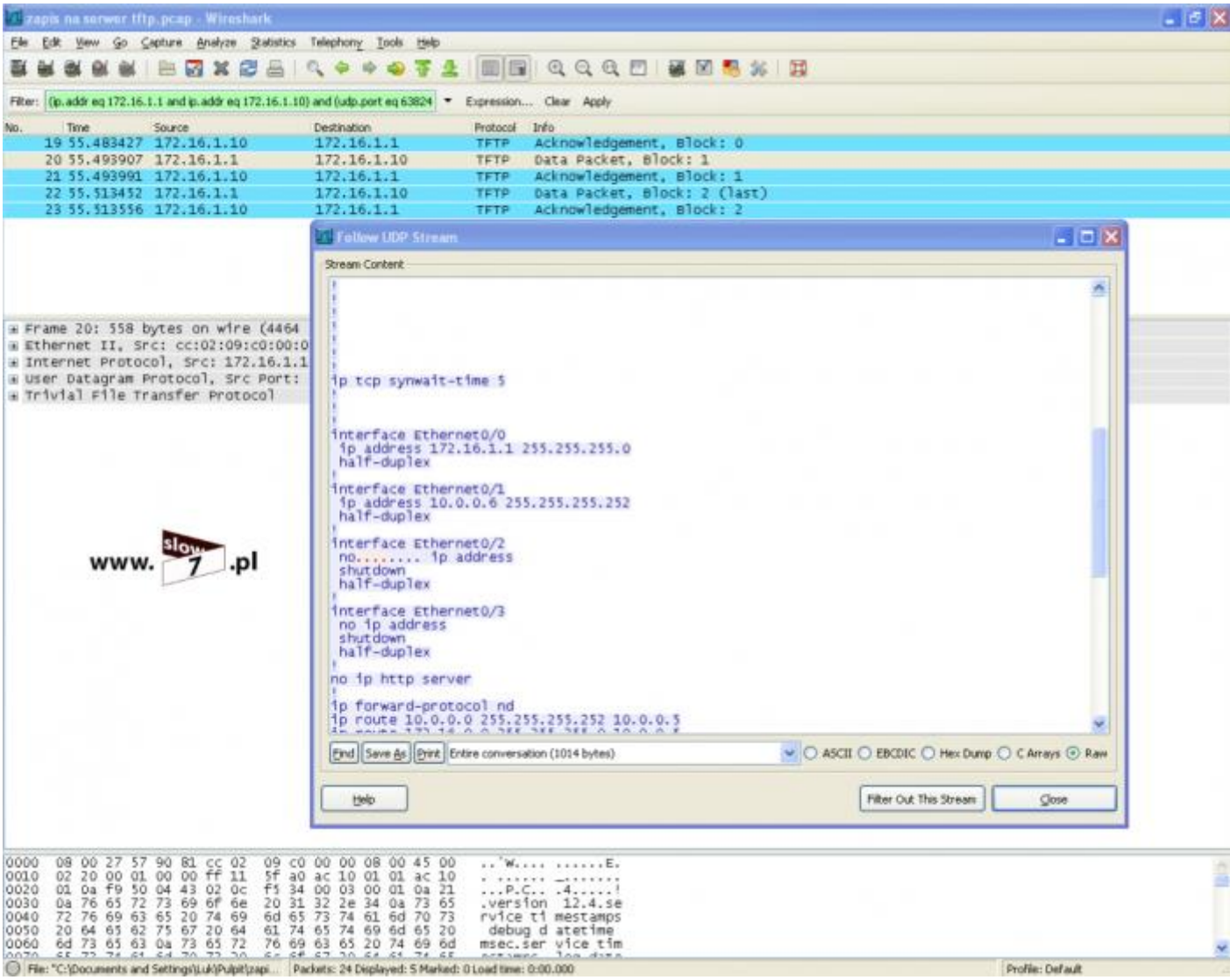
Jako serwer TFTP posłużył darmowy program **Tftpd32**. Program ten możesz pobrać z tej strony: http://tftpd32.jounin.net/

Proces przesyłania pliku kopii routera można również podejrzeć z poziomu przechwyconych pakietów. Jak widać proces zapisu pliku rozpoczyna się od wysłania pakietu **write request** na adres serwera 172.16.1.10. Pakiet **write request** jest datagramem UDP korzystającym z portu 69 (port używany tylko w celu inicjalizacji procesu zapisu/odczytu).



Dane przesyłane są jawnie czyli nie jest użyte żadne szyfrowanie. Przechwycenie transmisji TFTP powoduje zdobycie przez atakującego całej konfiguracji routera a co za tym idzie atakujący ma bardzo cenne informacje dające mu wgląd w sposób działania

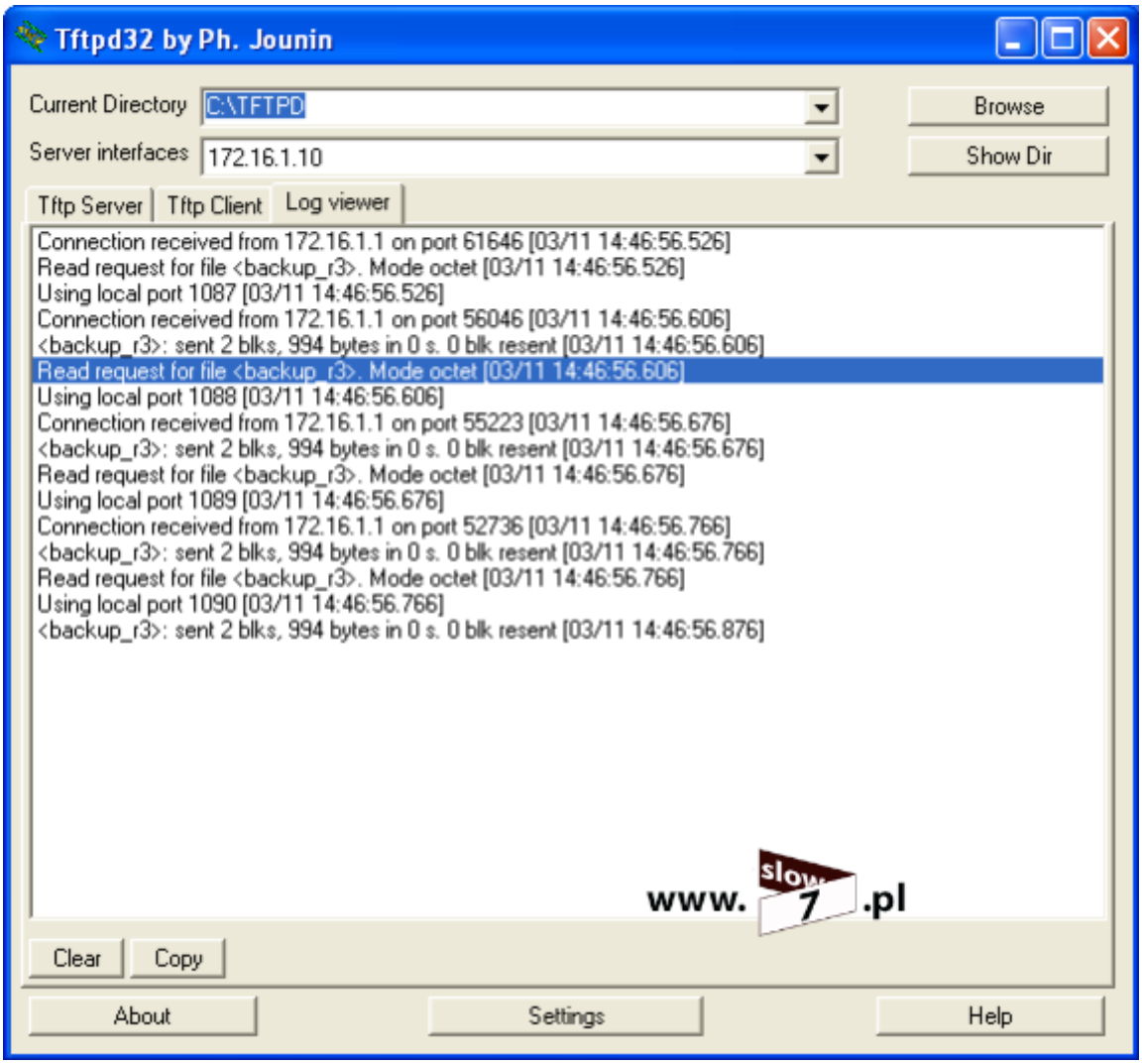
naszej sieci – użyta adresacja, informacje dotyczące routingu a nawet hasła dostępu do routera (zapisane jawnie lub hashe haseł).
Poniżej przykład przechwyconej transmisji (przykład powyżej kopia wysłana z routera R3 do serwera TFTP).



Proces odwrotny czyli kopiowanie pliku konfiguracji z serwera TFTP odbywa się po wydaniu polecenia:
copy <tftp://adres_serwera/nazwa_pliku> running-config>. Poniżej na rysunku przykład przywrócenia konfiguracji z wcześniej wykonanej kopii. Kierunek kopiowania pliku to: z serwera TFTP (172.16.1.10) do routera R3 (172.16.1.1).

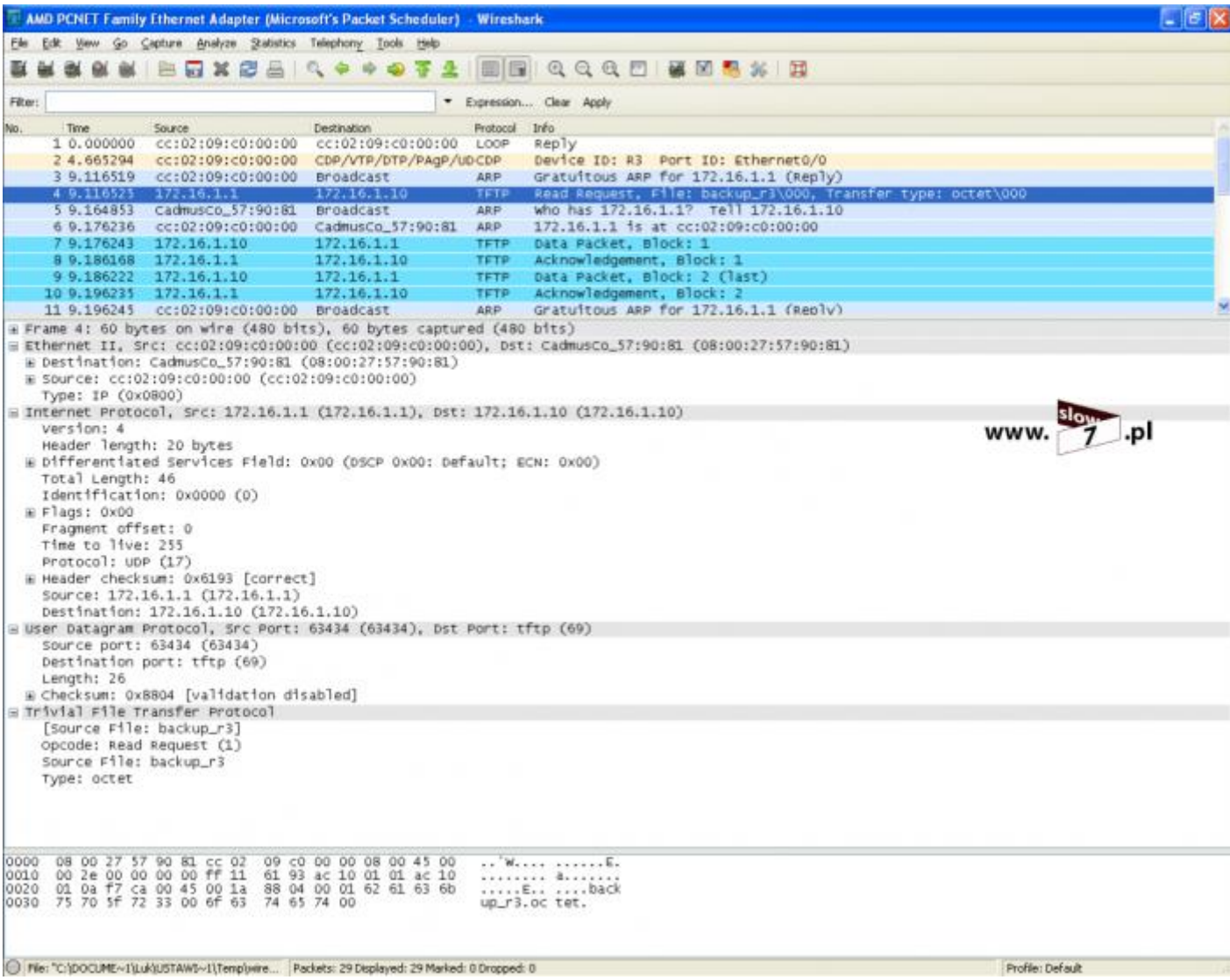
```
R3#copy tftp://172.16.1.10/backup_r3 running-config
Destination filename [running-config]?
Accessing tftp://172.16.1.10/backup_r3...
Loading backup_r3 from 172.16.1.10 (via Ethernet0/0): !
[OK - 994 bytes]

994 bytes copied in 0.516 secs (1926 bytes/sec)
R3#
*Mar  1 01:33:13.963: %SYS-5-CONFIG_I: Configured from tftp://172.16.1.10/backup_r3 by console
R3#
```

Proces transferu pliku można również zaobserwować przeglądając logi serwera TFTP.

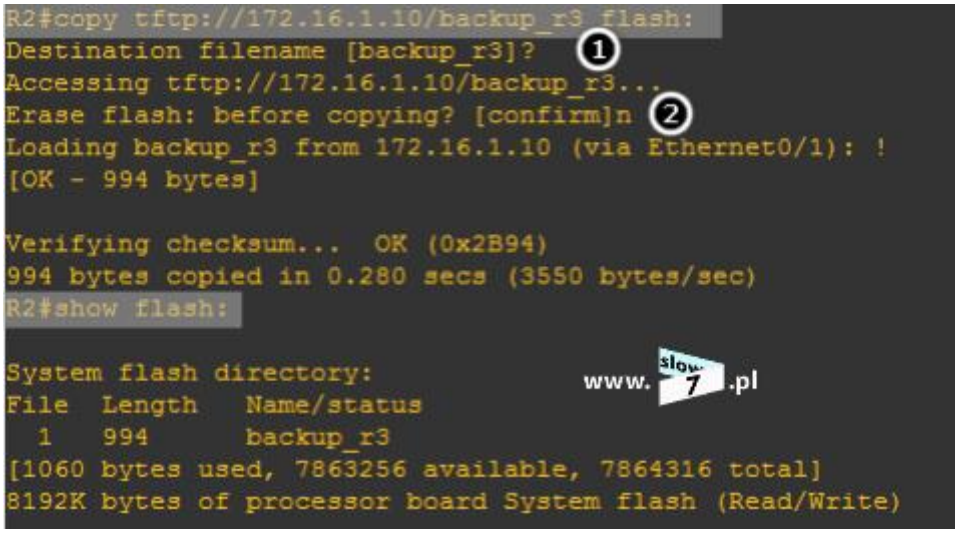


Kopiowanie jest również widoczne w oknie **Wireshark** w procesie sniffingu pakietów. Po bliższym zapoznaniu się z zawartością przechwyconych pakietów można zaobserwować,

że pakiet **read request** wysłany jest z adresu IP 172.16.1.1 (router R3) na adres IP serwera TFTP 172.16.1.10 i jest to datagram UDP o porcie docelowym 69.



Tak naprawdę aby skorzystać z TFTP wcale nie musimy mieć dedykowanego serwera ponieważ rolę serwera może pełnić każdy inny router Cisco. Przeanalizujmy oto taką sytuację: serwer TFTP 172.16.1.10 jest niedostępny ponieważ uległ on awarii a trzeba przywrócić konfigurację routera R3, która na skutek błędu administratora została wykasowana. Administrator sieci był na tyle przewidujący, że umieścił kopię konfiguracji routerów również w pamięci flash routera R2. Celem jest więc przywrócenie konfiguracji routera R3 z kopii pliku znajdującego na routerze R2.
Kopia konfiguracji routera R3 na routerze R2 została wykonana za pomocą polecenia:
copy <tftp://adres_serwera/nazwa_pliku> flash:



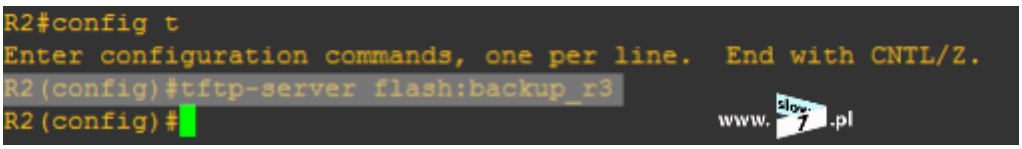
Podczas wykonywania tego polecenia musimy podać:

1.

1. nazwa pliku docelowego, kliknięcie Enter powoduje przyjęcie nazwy domyślnej,
2. pytanie o uprzednie skasowanie pamięci flash, jeśli zatwierdzimy zawartość pamięci zostaje skasowana a następnie kopiowany jest plik z lokalizacji zdalnej.

Zawartość pamięci flash sprawdzamy za pomocą polecenia: **show flash**

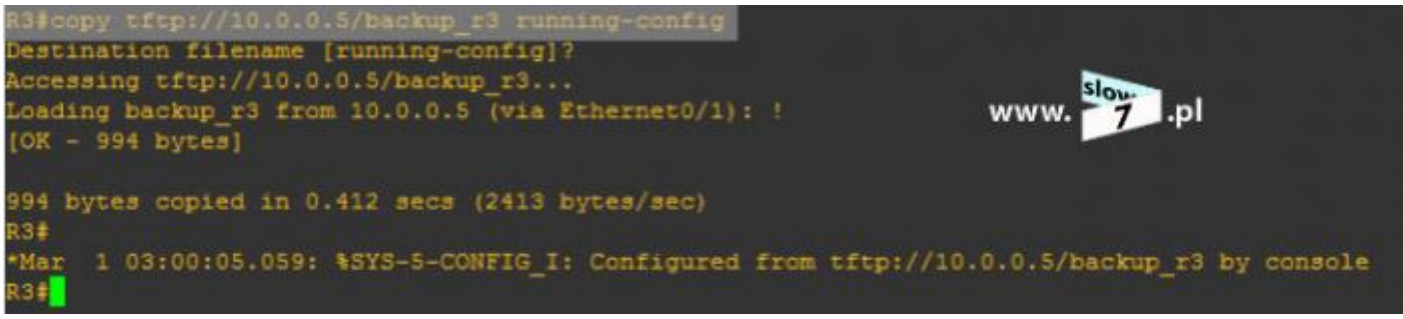
Aby móc wykonać zadanie naszym pierwszym krokiem jest uruchomienie usługi serwera TFTP na routerze R2. Aby to wykonać w trybie **konfiguracji globalnej** wydaj polecenie: **tftp-server <lokalizacja_pliku_który_chcemy_udostępnić>**



Plik backup_r3 zawierający konfigurację routera R3 został udostępniony, można go skopiować na inne urządzenie.

Proces kopiowania wykonujemy znanym już nam poleceniem:

copy <tftp://adres_serwera/nazwa_pliku> running-config.

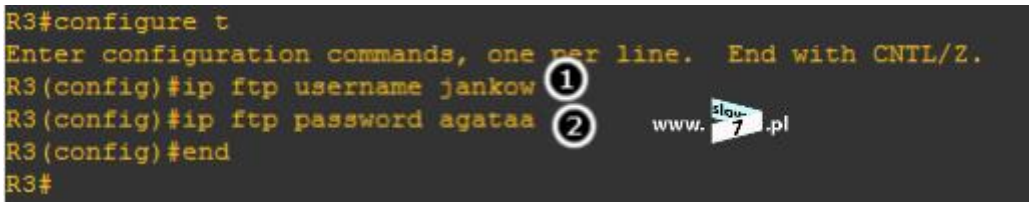


Oprócz protokołu TFTP do wykonania kopii konfiguracji (choć nie tylko) możemy użyć również protokołu FTP.
Protokół FTP (ang. File Transfer Protocol) jest protokołem transferu plików typu klient-serwer. Do działania w przeciwieństwie do TFTP wykorzystuje bardziej pewny protokół TCP zapewniając w ten sposób pewne dostarczenie pliku. Protokół ten umożliwia uwierzytelnienie.

Opis podstawowych poleceń protokołu FTP umieściłem tu: http://www.slow7.pl/windows-7/102-nie-samym-gui-czlowiek-zyje-rzecz-o-cmd?showall=&start=3

Dane niezbędne i wykorzystywane przez protokół FTP czyli nazwę użytkownika i hasło możemy zapisać w pamięci routera (tryb konfiguracji globalnej):

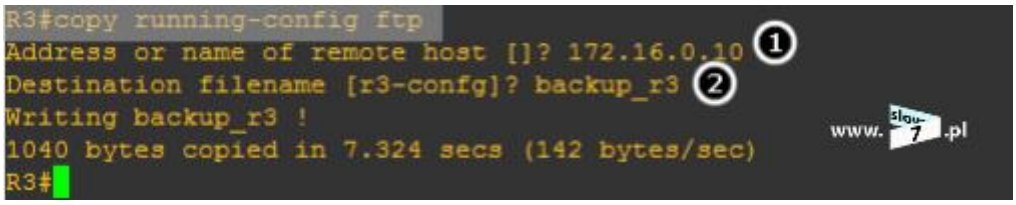
1.
1. podanie nazwy użytkownika FTP – **ip ftp username <nazwa_użytkownika>,**
2. hasło użytkownika FTP **– ip ftp password <hasło_użytkownika>**.



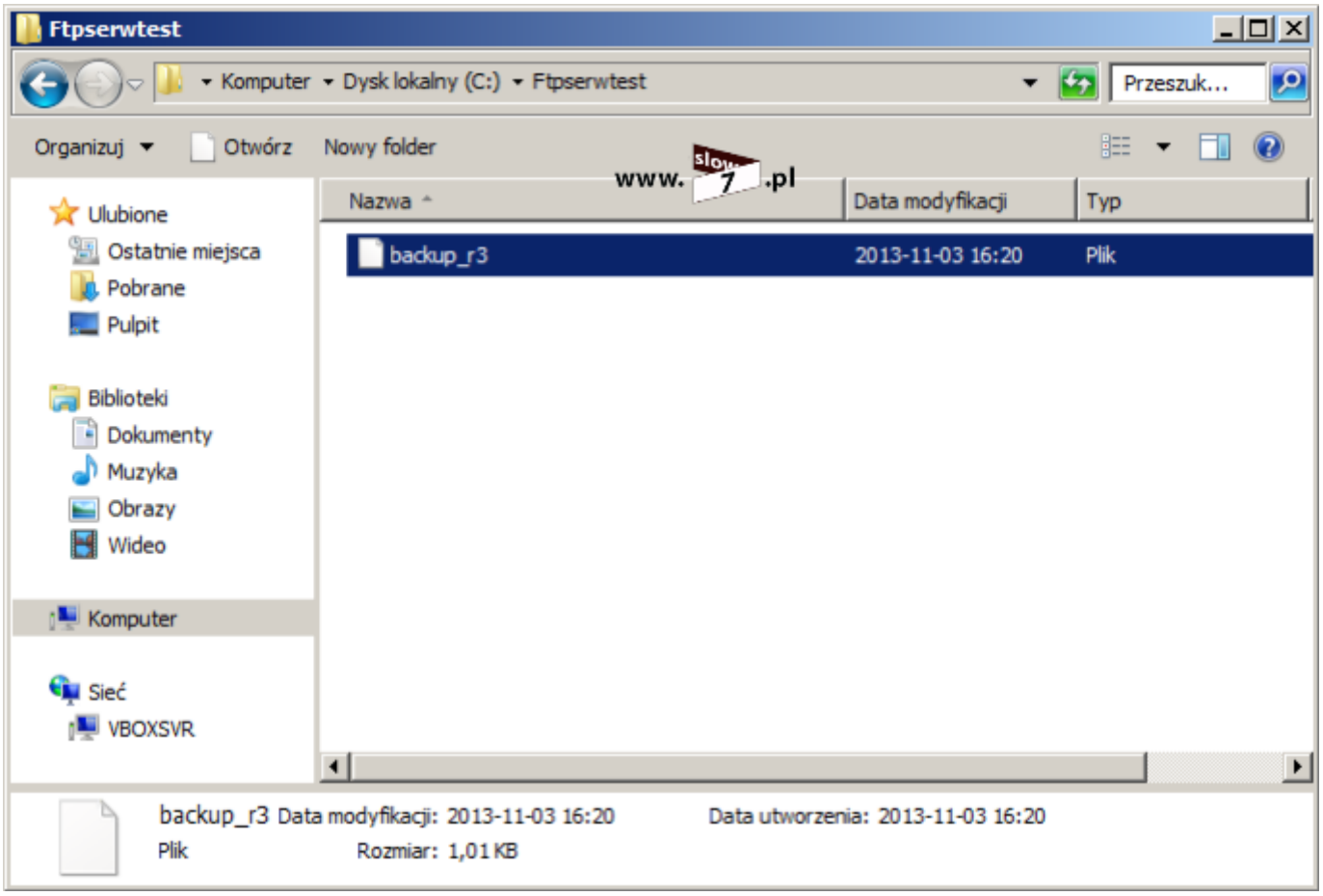
Wykonanie kopii konfiguracji (kopiowanie pliku na serwer FTP) odbywa się poprzez wydanie polecenia:
copy running-config ftp
Po wydaniu polecenia musimy dodatkowo określić:

1.

1. adres serwera FTP,
2. nazwa pliku docelowego.

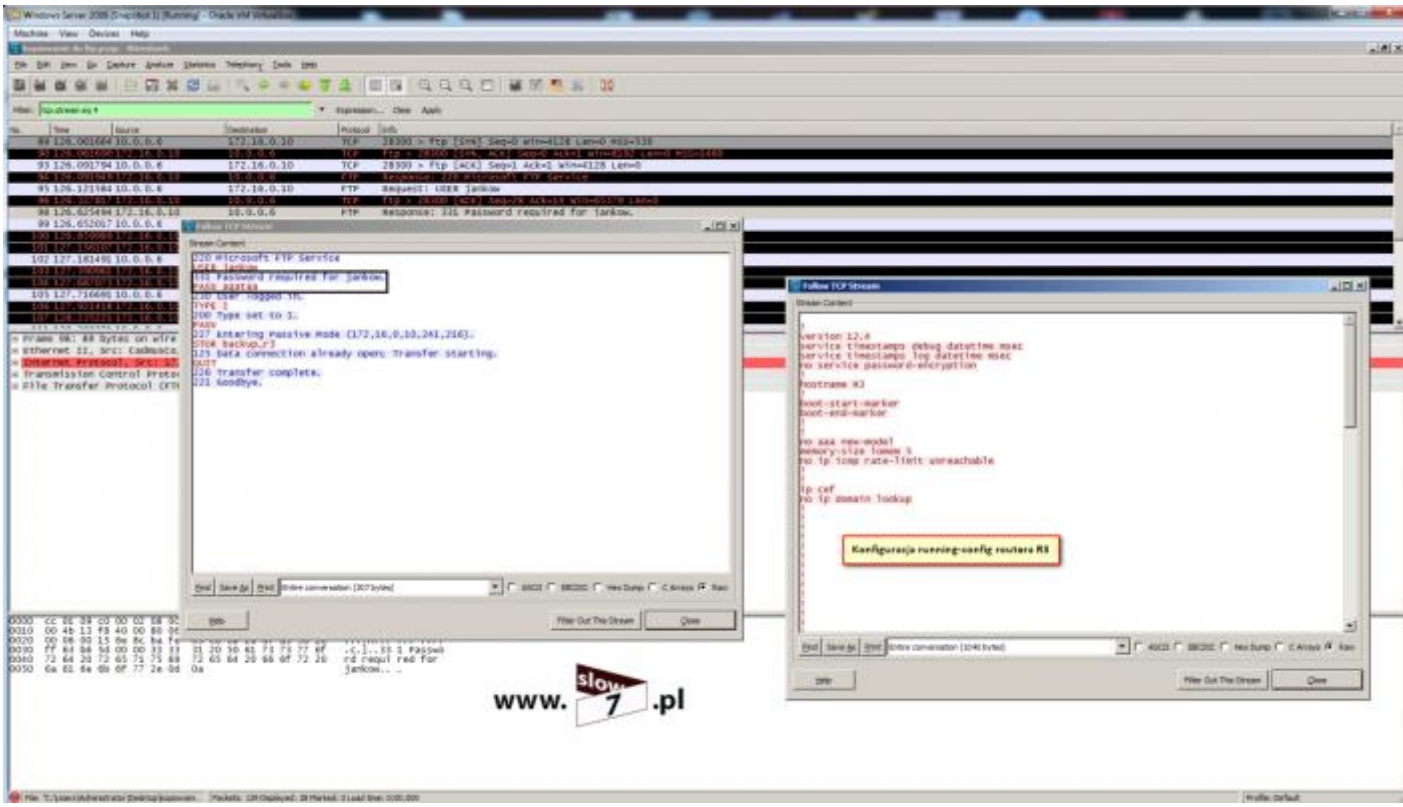


Po wykonaniu polecenia plik zostaje zapisany na serwerze FTP.

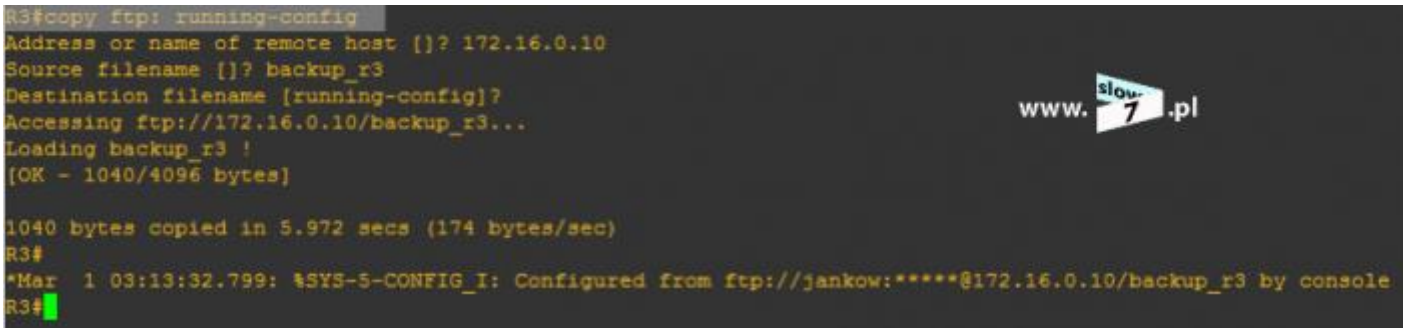


Pomimo tego, że protokół FTP daje nam możliwość skorzystania z uwierzytelnienia czyni go tylko nieznacznie bezpieczniejszym protokołem niż TFTP. Dzieje się tak ponieważ protokół ten również wszystkie informacje przesyła trybem otwartym.

Poniżej przechwycona sesja pomiędzy routerem R3 a serwerem FTP. Jak widać dane niezbędne do uwierzytelnienia oraz treść przesłanej informacji zostaje wyodrębniona z przechwyconych pakietów.



Oczywiście proces kopiowania z wykorzystaniem protokołu FTP może być przeprowadzony w obydwie strony, tak więc by przywrócić kopię konfiguracji z serwera FTP wydaj polecenie - **copy ftp: running-config**



Do przeprowadzenia całej operacji można również użyć znanego formatu URL. Dzięki formatowi URL określamy adres serwera, nazwę użytkownika i hasło. Tak więc polecenie przywracania kopii mogłoby być zapisane w ten sposób:

copy ftp://jankow:agataa@172.16.0.10/backup_r3 running-config

W podanym poleceniu dwukropek oddziela nazwę użytkownika od hasła, natomiast znak małpy wyznacza koniec informacji o użytkowniku i początek adresu serwera FTP. Znak ukośnika / używamy do określenia katalogu w którym znajduje się kopiowany plik.

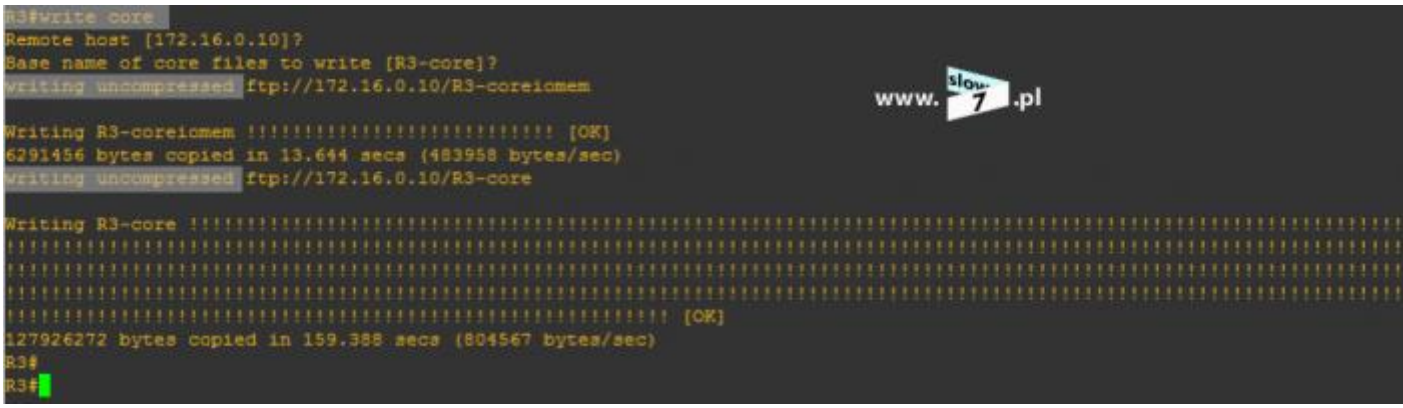
Serwer FTP można wykorzystać również do wykonania awaryjnego zrzutu pamięci routera w razie wystąpienia jakiegoś poważnego błędu działania. Zrzuty te mogą być pomocne w poznaniu przyczyn wystąpienia błędu, który przekłada się na nieprawidłowe funkcjonowanie urządzenia. Zrzut jest zapisem stanu routera przed wykonaniem restartu, tworzone są dwa pliki (domyślnie **nazwa_routera-core** – główna pamięć systemu oraz **nazwa_routera-coreiomem** – pamięć interfejsów wejścia-wyjścia), które ze względu na swoją objętość nie mogą być zapisane w pamięci trwałej urządzenia. Aby wykonać zrzut pamięci routera trzeba posłużyć się poleceniem **exception dump** wydanym w trybie konfiguracji routera.

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip ftp username jankow 1
R3(config)#ip ftp password agataa 2
R3(config)#exception protocol ftp 3
R3(config)#exception region-size 65536 4
R3(config)#exception dump 172.16.0.10 5
R3(config)#end
R3#
*Mar  1 07:15:19.002: %SYS-5-CONFIG_I: Configured from console by console
R3#
```

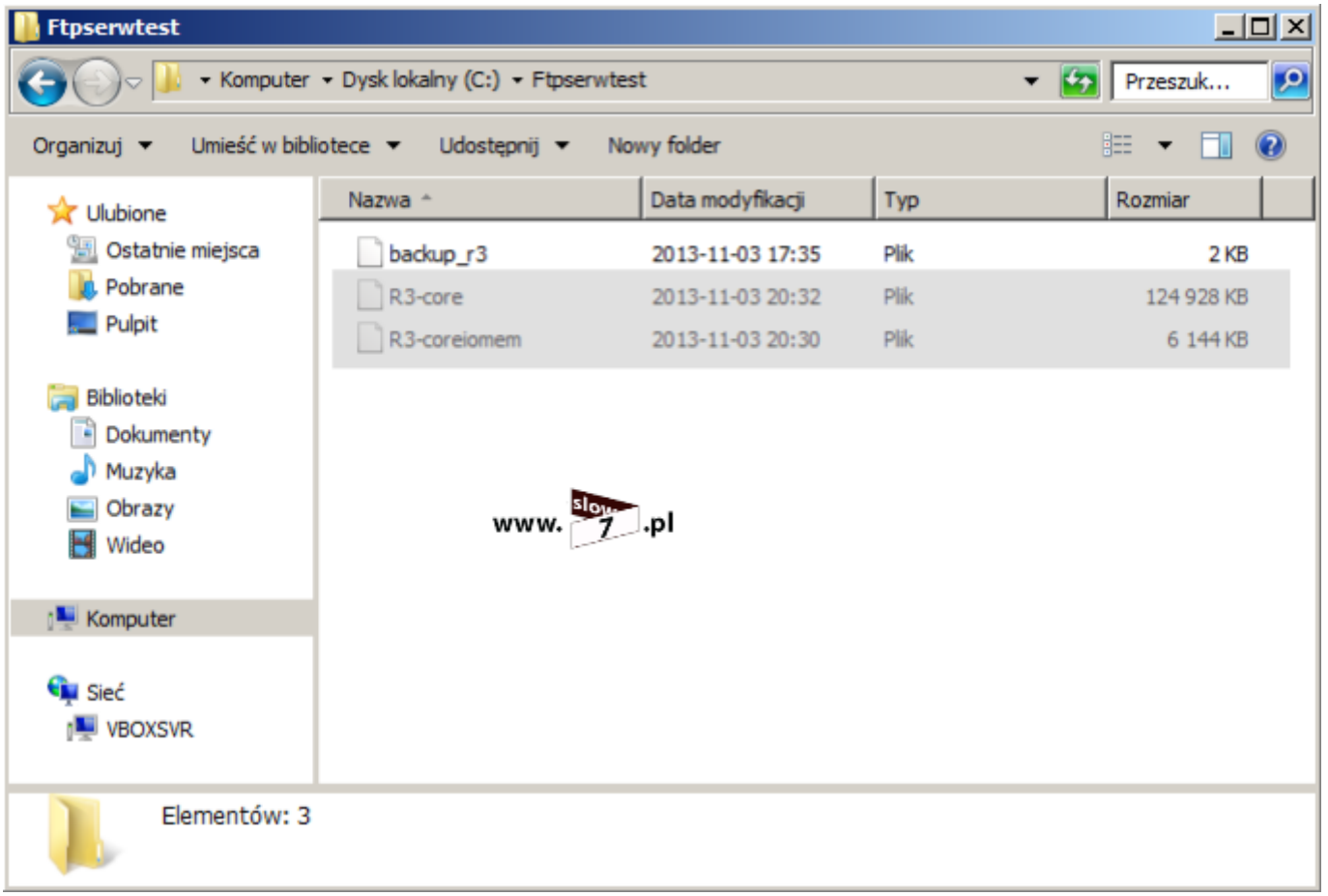

1.

1. określenie nazwy użytkownika FTP,
2. określenie hasła użytkownika FTP,
3. określenie protokołu odpowiedzialnego za transfer zrzutu (domyślnie: TFTP),
4. określenie obszaru pamięci, który będzie przeznaczony na utworzenie zrzutu (domyślnie: 16384 bajty),
5. adres serwera zrzutu.

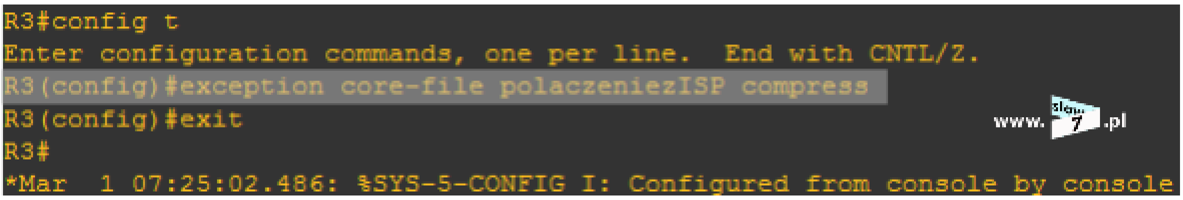
Po skonfigurowaniu wszystkich opcji, warto przeprowadzić test wprowadzonych ustawień, by wymusić na routerze wykonanie zrzutu pamięci wydaj polecenie **write core** (tryb uprzywilejowany).



Jak widać na zrzutach powyżej i poniżej proces przebiegł prawidłowo, router wykonał zrzut i zapisał pliki na serwerze FTP.

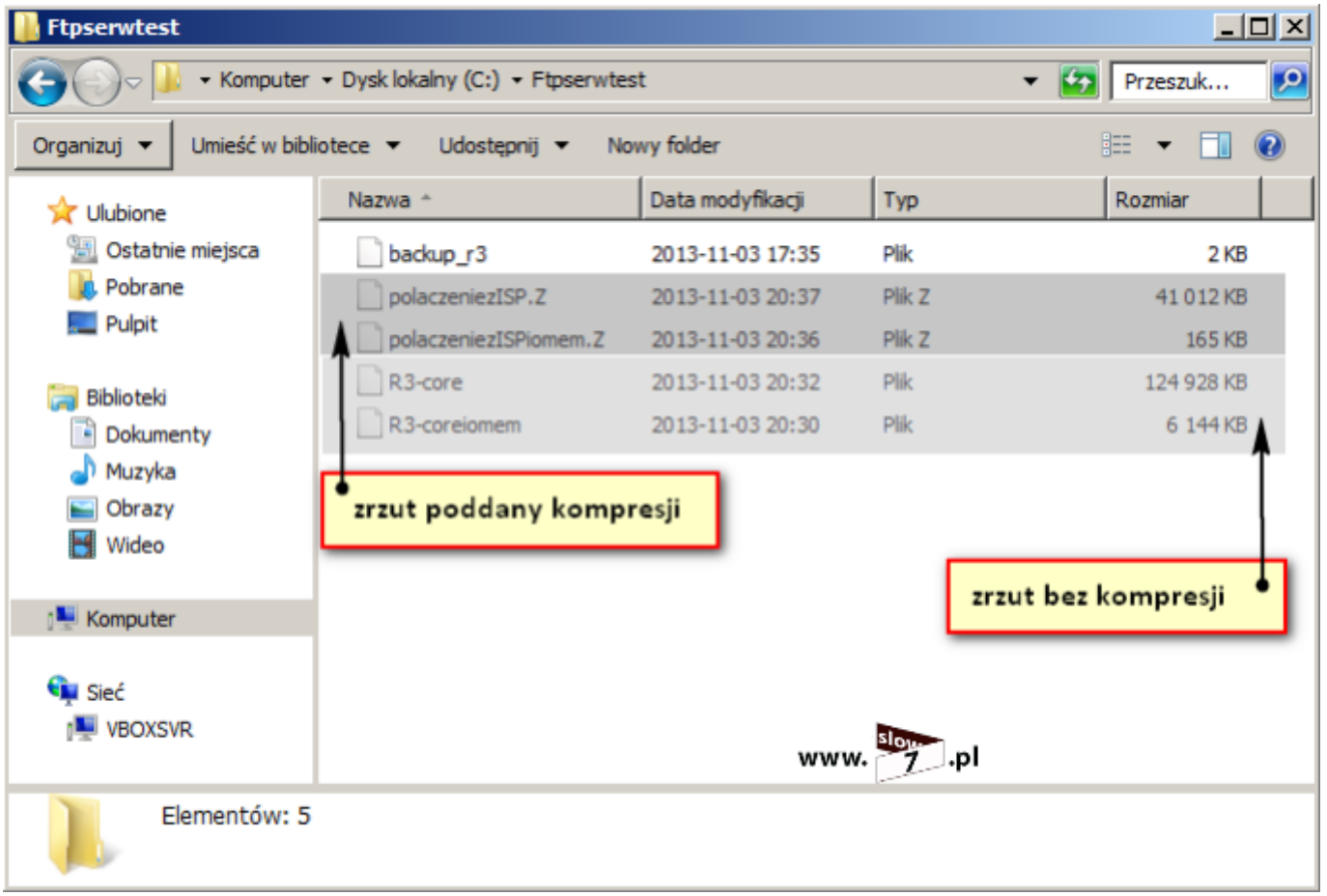


Analizując wymuszony proces zapisu zrzutu pamięci routera można zauważyć, że podane pliki nie są poddane kompresji (writing uncompressed). By wymusić na routerze wykonanie kompresji pliku przed jego przesłaniem należy wydać polecenie - **exception core-file <nazwa_pliku_zrzutu> compress**



By ponownie sprawdzić poprawność ustawień wydaj znane już Ci polecenie – **write core**

Porównując rozmiary utworzonych plików widać różnicę w ich rozmiarze.

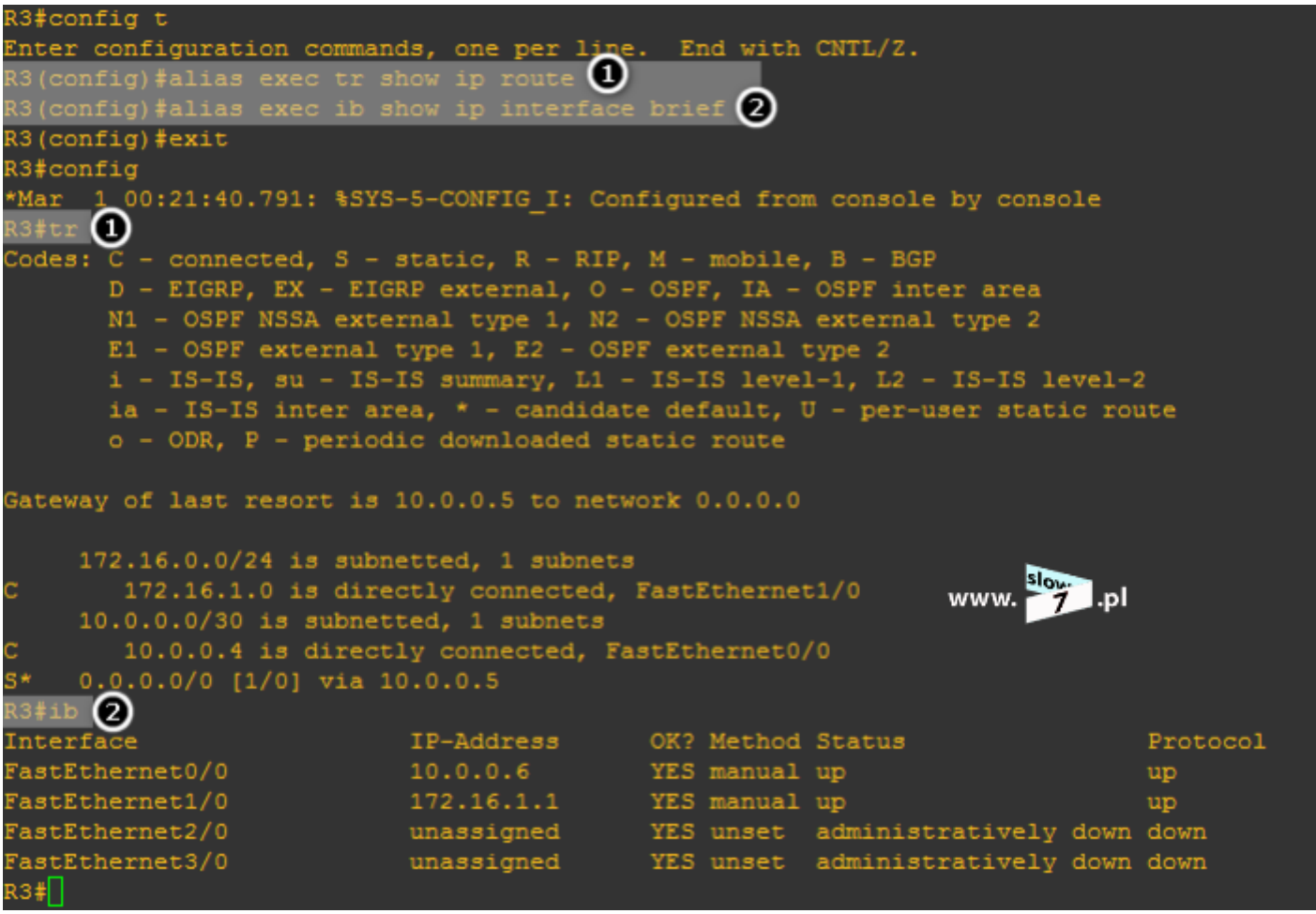


W codziennej pracy by przynajmniej trochę zautomatyzować i uprościć sobie pracę z routerem warto skorzystać z mechanizmu tworzenia aliasów poleceń. Alias upraszcza procedurę wprowadzani długich i skomplikowanych poleceń. Składnia polecenia tworzenia aliasu jest następująca: **alias exec <nazwa_aliasu> <polecenie_wykonane_po_wprowadzeniu_aliasu>**

Poniżej zostały utworzone dwa aliasy:

1.

1. alias **tr** (od tablica routingu), po wywołaniu aliasu zostaje wykonane polecenie: **show ip route**,
2. alias **ib** (od interface brief), po wywołaniu aliasu zostaje wykonane polecenie: **show ip interface brief**.



Przeważnie komunikując się z urządzeniami w naszej sieci używamy adresów IP, które tym urządzeniom są przypisane. Ale nic nie stoi na przeszkodzie by komunikować się za pośrednictwem nazw urządzeń. Czyli chodzi o to, by zamiast wpisywać **ping 10.0.0.1** celem sprawdzenia dostępności routera R1 wydać polecenie **ping r1**. Aby móc korzystać z tego typu poleceń (adres IP jest zastępowany nazwą urządzenia) możemy zdecydować się na jedno z dwóch rozwiązań:

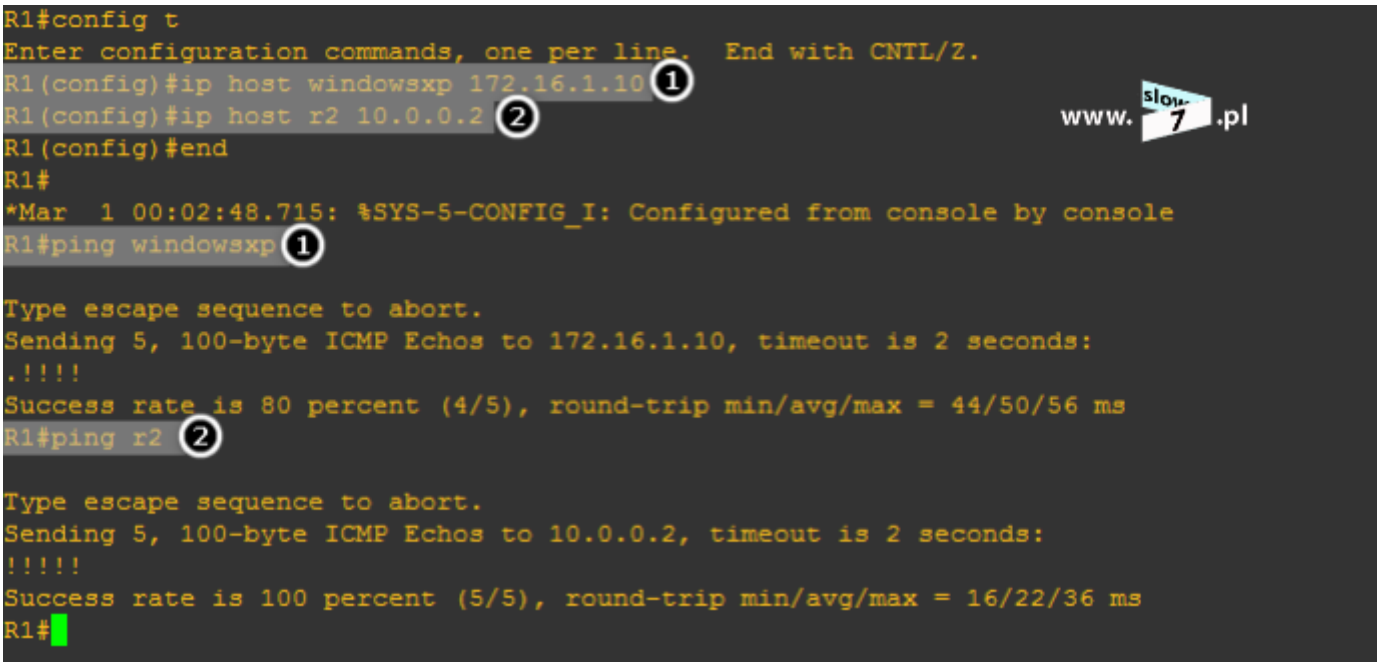
1.

1. **statyczna tablica nazw stacji** zapisana w konfiguracji routera,
2. **system nazw domenowych DNS**.

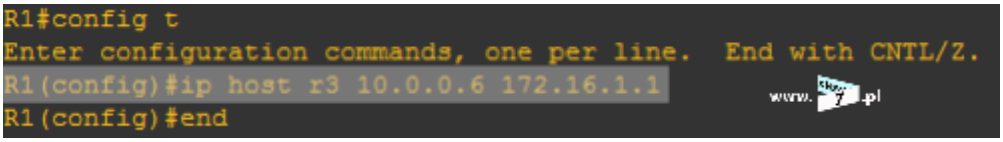
Pierwszy sposób polega na dodaniu statycznych wpisów, które wiążą nazwę z konkretnym adresem IP. Wadą tego rozwiązania jest lokalny charakter takiego wpisu. Oznacza to nic innego, że utworzony wpis na routerze R1 będzie dostępny tylko na tym urządzeniu.

Wpis do konfiguracji routera dodajemy za pomocą komendy - **ip host <nazwa_urządzenia> <adres_IP>**

Od tej pory możemy odwoływać się do nazwy urządzenia np. w poleceniu ping.



W naszym przykładzie np. router R3 posiada dwa adresy IP – pierwszy to 10.0.0.6 zaś drugi to 172.16.1.1, te dwa adresy mogą być użyte do utworzenia odwzorowania. Oba adresy będą wykorzystane w takiej kolejności w jakiej zostały podane w poleceniu konfiguracyjnym.



Przy tworzeniu tablicy nazw polecenie **ip host** pozwala także na zdefiniowanie konkretnych portów TCP. Poniżej zostało zdefiniowane powiązanie pomiędzy adresem 10.0.0.6 port 80 a nazwą www. Następnie nazwa ta została wykorzystana w poleceniu telnet. Następuje próba nawiązania połączenia z portem 80 pod adresem 10.0.0.6.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip host www 80 10.0.0.6
R1(config)#end
R1#t
*Mar  1 00:28:42.639: %SYS-5-CONFIG_I: Configured from console by console
R1#telnet www
Trying www (10.0.0.6, 80)...
% Connection refused by remote host
```

Tablicę nazw zdefiniowanych hostów poznamy po wydaniu polecenia - **show hosts**

```
R1#show hosts
Default domain is not set
Name/address lookup uses static mappings

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                      Port  Flags      Age Type   Address(es)
windowsxp                 None  (perm, OK)  1   IP    172.16.1.10
r2                        None  (perm, OK)  1   IP    10.0.0.2
r3                        None  (perm, OK)  1   IP    10.0.0.6
                                                      172.16.1.1
www                       80    (perm, OK)  1   IP    10.0.0.6
R1#
```

Aby wykasować wpis z tabeli nazw stacji wydaj polecenie **no ip host <nazwa_urządzenia> <adres_IP>**.

Drugim ze sposobów jest skorzystanie z **serwera DNS** (domyślnie włączone), który dla każdego podłączonego urządzenia (klienta) będzie rozwiązywał nazwy urządzeń tj. kojarzył w parę nazwa urządzenia – jego adres IP. Rozwiązanie drugie jest o tyle wygodniejsze gdyż serwer DNS może obsługiwać wielu klientów przez co dostęp do niego mogą mieć wszystkie urządzenia znajdujące się w sieci. Brak tu lokalnego tworzenia tablicy odwzorowań, tablica taka tworzona jest na serwerze DNS i dostępna dla wszystkich.
W przypadku braku serwera DNS (czasem odwzorowanie może być również wyłączone na samym routerze) próba uzyskania adresu urządzenia kończy się niepowodzeniem.

```
R1#ping serwtest

Translating "serwtest"
% Unrecognized host or address, or protocol not running.

R1#
```

W naszej testowej topologii rolę serwera DNS pełni komputer 172.16.0.10. Po włączeniu serwera i konfiguracji routera, serwer zaczyna rozwiązywać nazwy.
Konfiguracja routera sprowadza się do włączenia funkcji DNS na samym urządzeniu za pomocą komendy - **ip domain-lookup**(tryb konfiguracji routera) oraz określeniu adresu IP serwera – polecenie **ip name-server <adres_IP_serwera_DNS>** (można dodać wiele adresów IP różnych serwerów DNS). Opcjonalnie możemy podać nazwę domeny – **ip domain-name <nazwa_domeny>**.

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip domain-lookup
R3(config)#ip domain-name firma.local
R3(config)#ip name-server 172.16.0.10
R3(config)#exit
R3#p
*Mar  1 00:51:50.147: %SYS-5-CONFIG_I: Configured from console by console
R3#ping serwtest

Translating "serwtest"...domain server (172.16.0.10) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
R3#
```

Jak widać na przykładach poniżej i powyżej łączność z serwerem DNS jest zapewniona.

```
R3#ping r2

Translating "r2"...domain server (172.16.0.10) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/21/32 ms
R3#
```

Adresy odwzorowań uzyskane dzięki serwerowi DNS są dostępne po wydaniu polecenia: **show hosts**

```
R3#show hosts
Default domain is firma.local
Name/address lookup uses domain service
Name servers are 172.16.0.10

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                      Port  Flags      Age Type   Address(es)
xxx.firma.local           None  (temp, OK)  0   IP    172.16.1.10
r2.firma.local            None  (temp, OK)  0   IP    172.16.0.1
serwtest.firma.local      None  (temp, OK)  0   IP    172.16.0.10
R3#
```

Jeśli w naszej sieci brak jest serwera DNS to dobrą praktyką jest wyłączenie funkcji zamiany podanej nazwy na adres IP. Funkcję tą wyłączymy po wpisaniu **no ip domain-lookup**. Wyłączenie funkcji spowoduje również zablokowanie dość irytującego przestoju, który pojawia się w razie wpisania błędnego polecenia.
Dodatkowo możemy zmienić domyślny sposób działania linii poleceń EXEC, który nakazuje routerowi nawiązanie połączenia sesji telnet, gdy zostanie wpisana nazwa, która nie jest poleceniem systemu IOS. Zmianę tą dokonamy wpisując polecenia zgodne z poniższym zrzutem. Wydane polecenia podajemy w trybie konfiguracji **linii wirtualnych**. Ten typ konfiguracji nie był jeszcze omawiany i podane polecenia stanowią nijako wyprzedzenie omawianych treści.

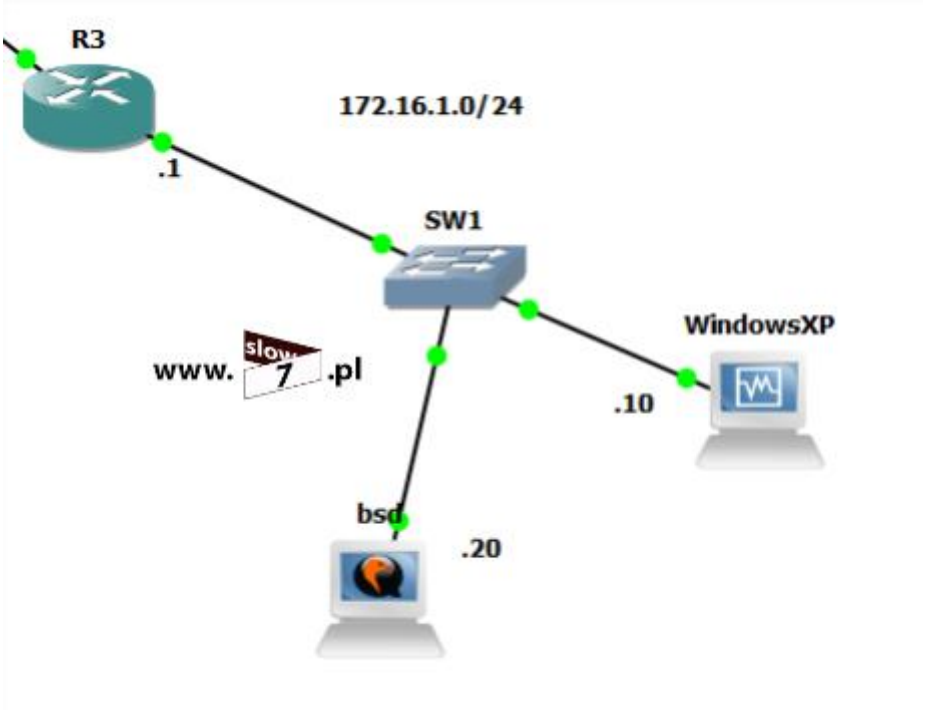
```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#line vty 0 4
R1(config-line)#transport preferred none
R1(config-line)#end
R1#
```

Każde urządzenie znajdujące się w naszej sieci LAN nieważne czy jest to router czy komputer tworzy swoją lokalną tablicę danych ARP (ang. Adress Resolution Protocol). Tablica ta zawiera odwzorowania adresów warstwy drugiej (adres MAC) na odpowiadające im adresy warstwy trzeciej (adres IP). Obydwa adresy kojarzone są w

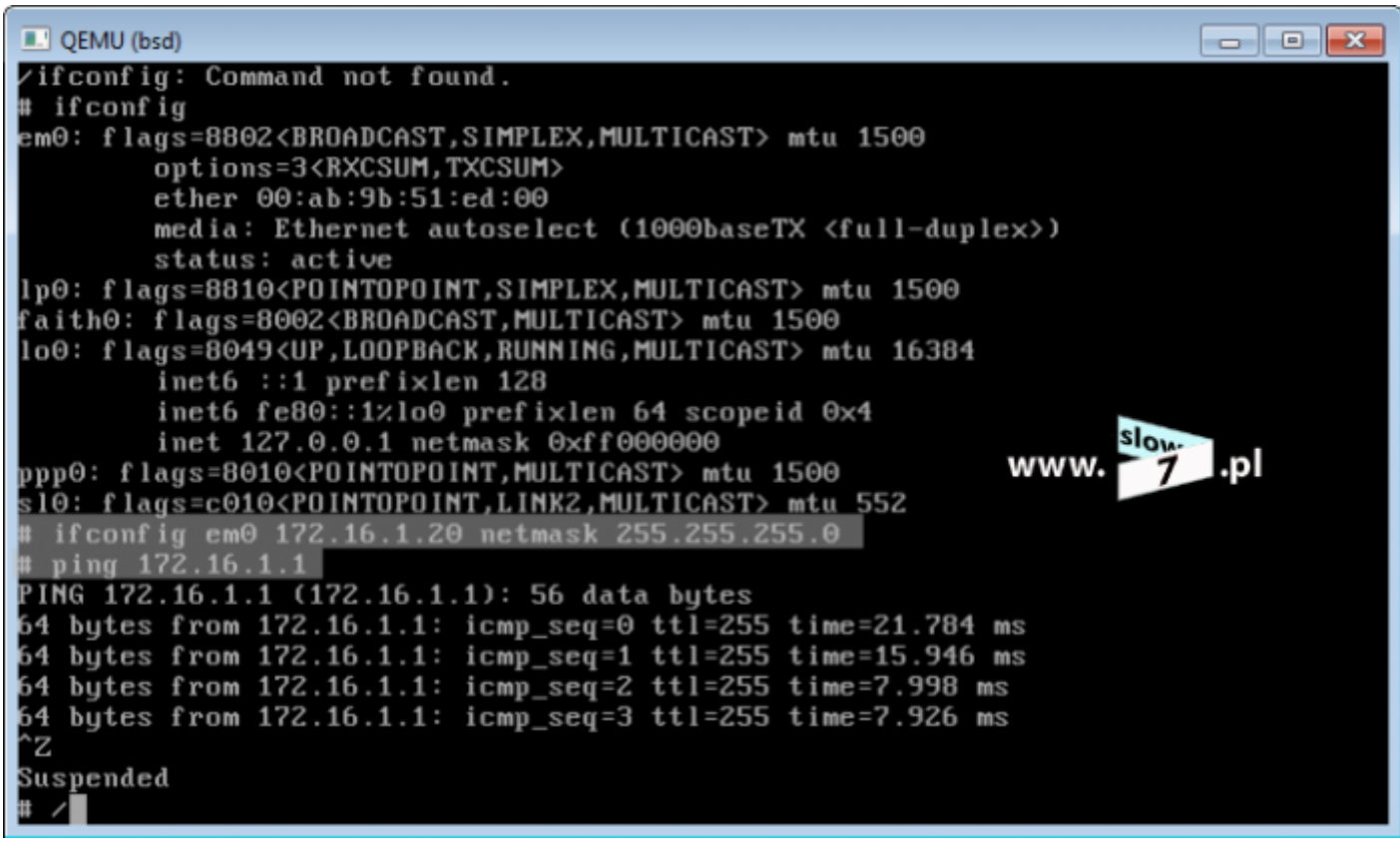
pary a proces ma z reguły charakter dynamiczny (odwzorowanie następuje automatycznie, dzięki protokołowi ARP), choć można powiązanie wykonać samemu (tu możesz doczytać - http://www.slow7.pl/windows-7/102-nie-samym-gui-czlowiek-zyje-rzecz-o-cmd?showall=&start=3).
Wyświetlenie tablicy ARP odbywa się po wydaniu polecenia – **show arp**. Zostaje wyświetlona tablica w której to zebrane są informacje o: protokole, adresie IP, czasie powiązania, adresie MAC oraz interfejsie.

```
R3#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.6               -   cc02.1220.0000  ARPA   FastEthernet0/0
Internet  10.0.0.5              84   cc01.1220.0000  ARPA   FastEthernet0/0
Internet  172.16.1.10            3   0800.2757.9081  ARPA   FastEthernet1/0
Internet  172.16.1.1             -   cc02.1220.0010  ARPA   FastEthernet1/0
R3#
```

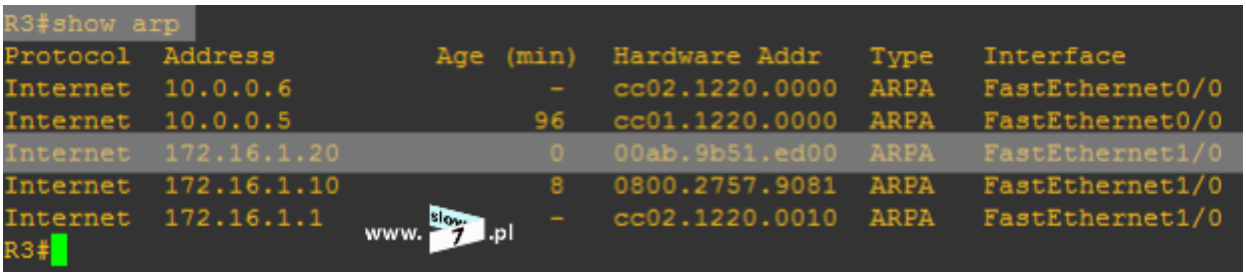

To, że jest to proces dynamiczny można zaobserwować w momencie podłączenia nowego hosta. Tablica ARP zostaje uzupełniona o nowy wpis w momencie zaistnienia pierwszej komunikacji z nowo podłączonym hostem. Aktualizacja tablic może nastąpić również już w momencie podłączenia nowego urządzenia do sieci. Ponieważ wiele urządzeń wysyła pakiet powiadomienia ARP zaraz po fakcie w którym stwierdzają, że są z siecią połączone. Pakiety ARP mają charakter rozgłoszeniowy i dlatego muszą być przetwarzane przez wszystkie urządzenia znajdujące się w określonej domenie rozgłoszeniowej.
Do naszej sieci został podłączony nowy host o adresie IP 172.16.1.20, jak widać po analizie tablicy ARP przedstawionej na powyższym zrzucie, host ten (a raczej adres IP przypisany temu hostowi) nie ma swojego odwzorowania w postaci pary adres IP – adres MAC.



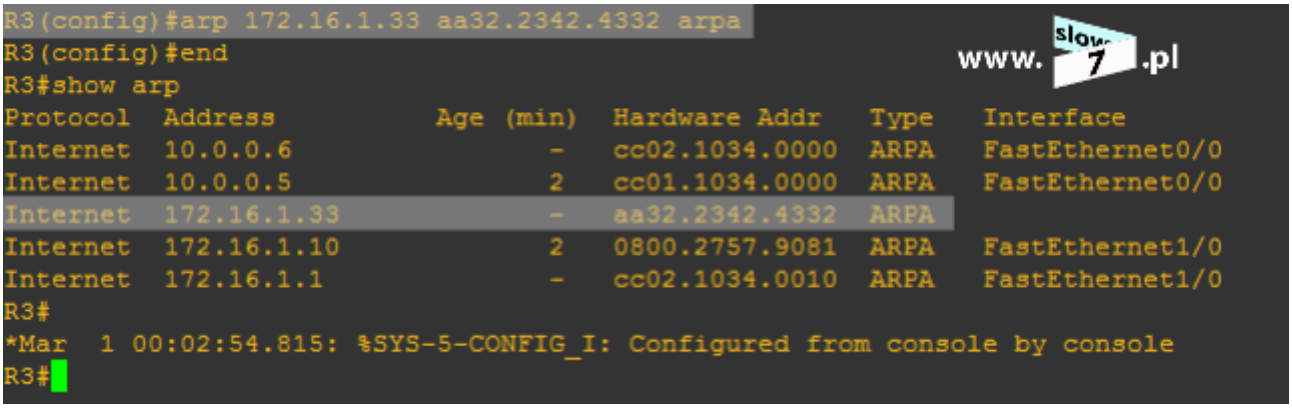
Po przypisaniu adresu IP zostaje wysłany ping do routera R3.



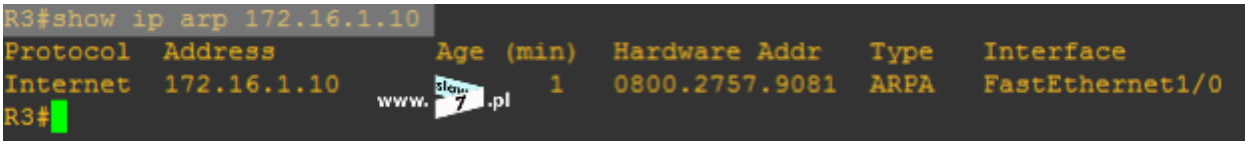
Jak widać poniżej po zaistnieniu komunikacji pomiędzy hostem a routerem w tablicy ARP pojawia się odpowiedni wpis.



Oczywiście jeśli istnieje taka potrzeba wpis ARP możemy ustawić samemu jako wpis statyczny. Cała procedura sprowadza się do wydania polecenia - **arp <adres_IP> <adres MAC> arpa** (arpa dla sieci typu Ethernet). Poprawność wprowadzenia wpisu sprawdzamy znanym nam poleceniem – **show arp**



By poznać jaki adres MAC przypisany jest do konkretnego adresu IP – wydaj komendę – **show ip arp <adres_IP>**



By poznać adres IP, który jest przypisany do adresu MAC – wydaj komendę – **show ip arp <adres_MAC>**

```
R3#show ip arp 00ab.9b51.ed00
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.1.20             9  00ab.9b51.ed00  ARPA   FastEthernet1/0
R3#
```

Aby poznać powiązania, które są dostępne przez konkretny interfejs – wydaj komendę – **show ip arp <interfejs>**

```
R3#show ip arp f1/0
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.1.20             14  00ab.9b51.ed00  ARPA   FastEthernet1/0
Internet  172.16.1.10              8  0800.2757.9081  ARPA   FastEthernet1/0
Internet  172.16.1.1               -  cc02.1220.0010  ARPA   FastEthernet1/0
R3#
```

Aby przeszukiwanie było szybkie i efektywne mechanizm odpowiedzialny za obsługę tablicy ARP, po określonym czasie usuwa nie odświeżone wpisy. By poznać czas usunięcia nieaktywnego wpisu, wydaj polecenie - **show interfaces <nazwa_interfejsu>**.
Sekcja **ARP Timeout** dostarczy Ci informacji o czasie usunięcia.
Jak widać router usunie niewykorzystane dane ARP po czterech godzinach (ustawienie domyślne).

```
R3#show interfaces f0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is cc02.1220.0000 (bia cc02.1220.0000)
  Internet address is 10.0.0.6/30
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:57, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     236 packets input, 50570 bytes
     Received 114 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     947 packets output, 93701 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     1 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R3#
```


Aby zmienić domyślny czas usunięcia danych ARP w trybie **konfiguracji interfejsu** wydaj komendę - **arp timeout <czas_w_sek>** Możliwy dostępny zakres: od 0 do 2147483.

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface f0/0
R3(config-if)#arp timeout 900
R3(config-if)#
```


Jak widać powyższe polecenie zmieniło czas usunięcia na 15 minut.

```
R3#show interfaces f0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is cc02.1220.0000 (bia cc02.1220.0000)
  Internet address is 10.0.0.6/30
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 00:15:00
  Last input 00:00:14, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     244 packets input, 53164 bytes
     Received 121 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     993 packets output, 98540 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     1 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R3#
```


W razie wystąpienia problemów i jeśli tych problemów doszukujemy się w protokole ARP można ręcznie wymusić oczyszczenie pamięci ARP. Oczyszczenie pamięci dokonasz za pomocą polecenia – **clear arp-cache**

```
R2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.2                -   cc01.1220.0010  ARPA   FastEthernet1/0
Internet  10.0.0.1                6   cc00.1220.0010  ARPA   FastEthernet1/0
Internet  10.0.0.6                7   cc02.1220.0000  ARPA   FastEthernet0/0
Internet  10.0.0.5                -   cc01.1220.0000  ARPA   FastEthernet0/0
Internet  172.16.0.10             4   0800.27d1.908f  ARPA   FastEthernet2/0
Internet  172.16.0.1                -   cc01.1220.0020  ARPA   FastEthernet2/0
R2#clear arp-cache
R2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.2                -   cc01.1220.0010  ARPA   FastEthernet1/0
Internet  10.0.0.1                0   cc00.1220.0010  ARPA   FastEthernet1/0
Internet  10.0.0.6                0   cc02.1220.0000  ARPA   FastEthernet0/0
Internet  10.0.0.5                -   cc01.1220.0000  ARPA   FastEthernet0/0
Internet  172.16.0.10             0   0800.27d1.908f  ARPA   FastEthernet2/0
Internet  172.16.0.1                -   cc01.1220.0020  ARPA   FastEthernet2/0
R2#
```

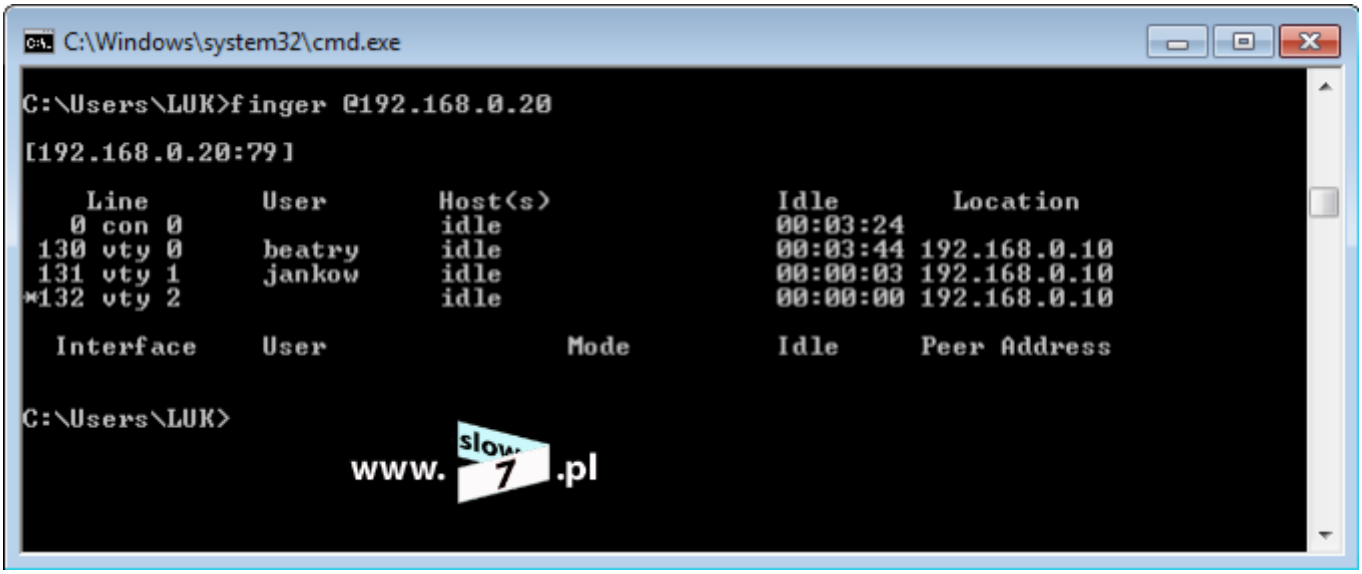
Można wymusić również oczyszczenie pamięci ARP dla konkretnego interfejsu, polecenie – **clear arp-cache <interfejs>**

```
R3#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.6               -   cc02.1220.0000  ARPA   FastEthernet0/0
Internet  10.0.0.5               2   cc01.1220.0000  ARPA   FastEthernet0/0
Internet  172.16.1.20            2   00ab.9b51.ed00  ARPA   FastEthernet1/0
Internet  172.16.1.10            2   0800.2757.9081  ARPA   FastEthernet1/0
Internet  172.16.1.1             -   cc02.1220.0010  ARPA   FastEthernet1/0
R3#clear arp-cache interface f1/0
R3#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.6               -   cc02.1220.0000  ARPA   FastEthernet0/0
Internet  10.0.0.5               3   cc01.1220.0000  ARPA   FastEthernet0/0
Internet  172.16.1.20            0   00ab.9b51.ed00  ARPA   FastEthernet1/0
Internet  172.16.1.10            0   0800.2757.9081  ARPA   FastEthernet1/0
Internet  172.16.1.1             -   cc02.1220.0010  ARPA   FastEthernet1/0
R3#
```


Router umożliwia włączenie dodatkowych funkcji, które nazywane są „małymi serwerami”, funkcje te powinny być włączane tylko podczas prowadzenia testów, gdyż uruchomienie niektórych z nich obniża bezpieczeństwo naszej sieci. Jedną właśnie z takich usług jest usługa **finger**. Aplikacja **finger** umożliwia zdalne sprawdzenie, kto aktualnie jest zalogowany na routerze. Włączenie funkcji odbywa się za pomocą polecenia – **ip finger**.

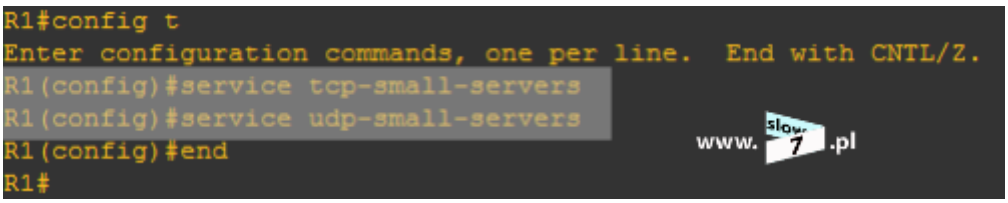
```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip finger
R1(config)#end
R1#
```


Po włączeniu funkcji, możliwe jest sprawdzenie kto korzysta z routera. Aplikacja dostępna jest z linii poleceń systemu Windows. Jak widać po wywołaniu polecenia aplikacja zdradzi nam loginy aktualnie zalogowanych użytkowników.



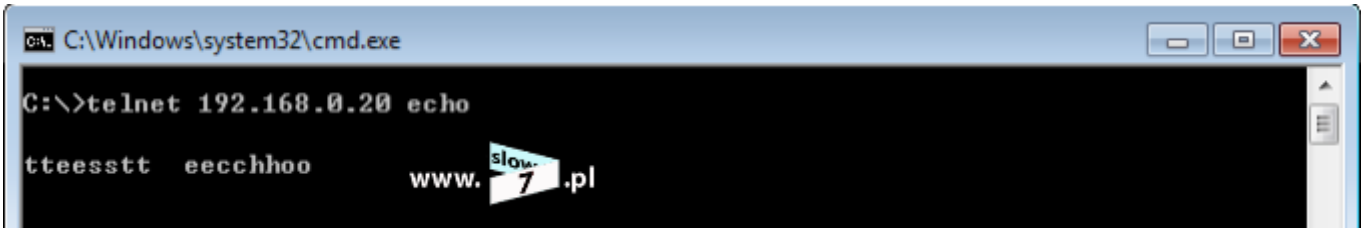
Możliwe jest również wywołanie usługi **finger** z poziomu linii poleceń innego routera. Wywołanie odbywa się poprzez usługę telnet przy wykorzystaniu portu 79.

Pozostałe usługi włączamy za pomocą poleceń: **service tcp-small-servers** oraz **service udp-small-servers**.



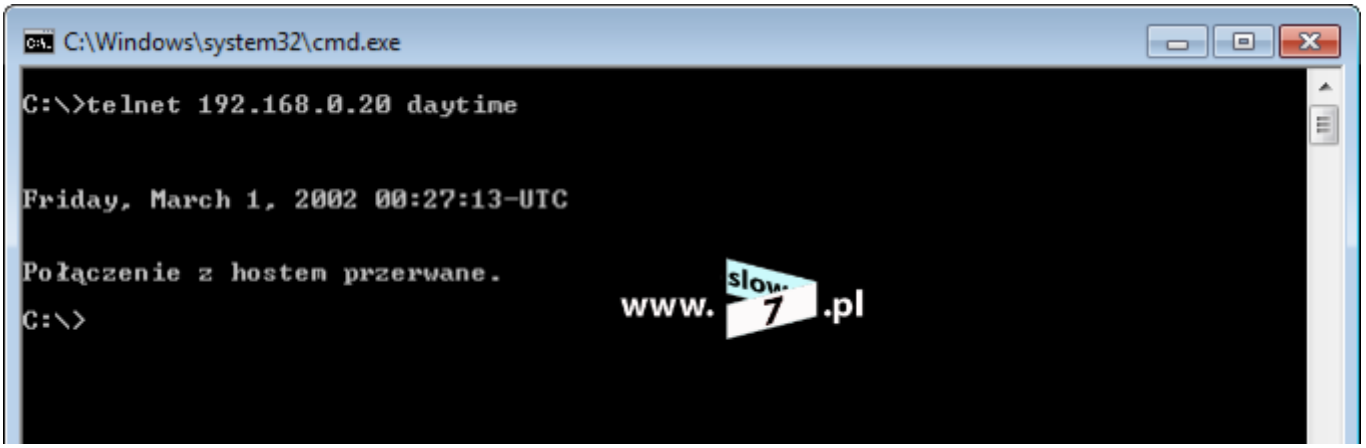
Wydanie tych poleceń spowoduje włączenie takich usług jak: **echo**, **discard**, **daytime** oraz **chargen**.

Usługa **echo** działa na porcie 7 a jej działanie polega na odesłanie do klienta pakietu, który od niego otrzymał. Poniżej przykład w którym klient wprowadza znaki z klawiatury i ten sam znak zostaje do niego odesłany.

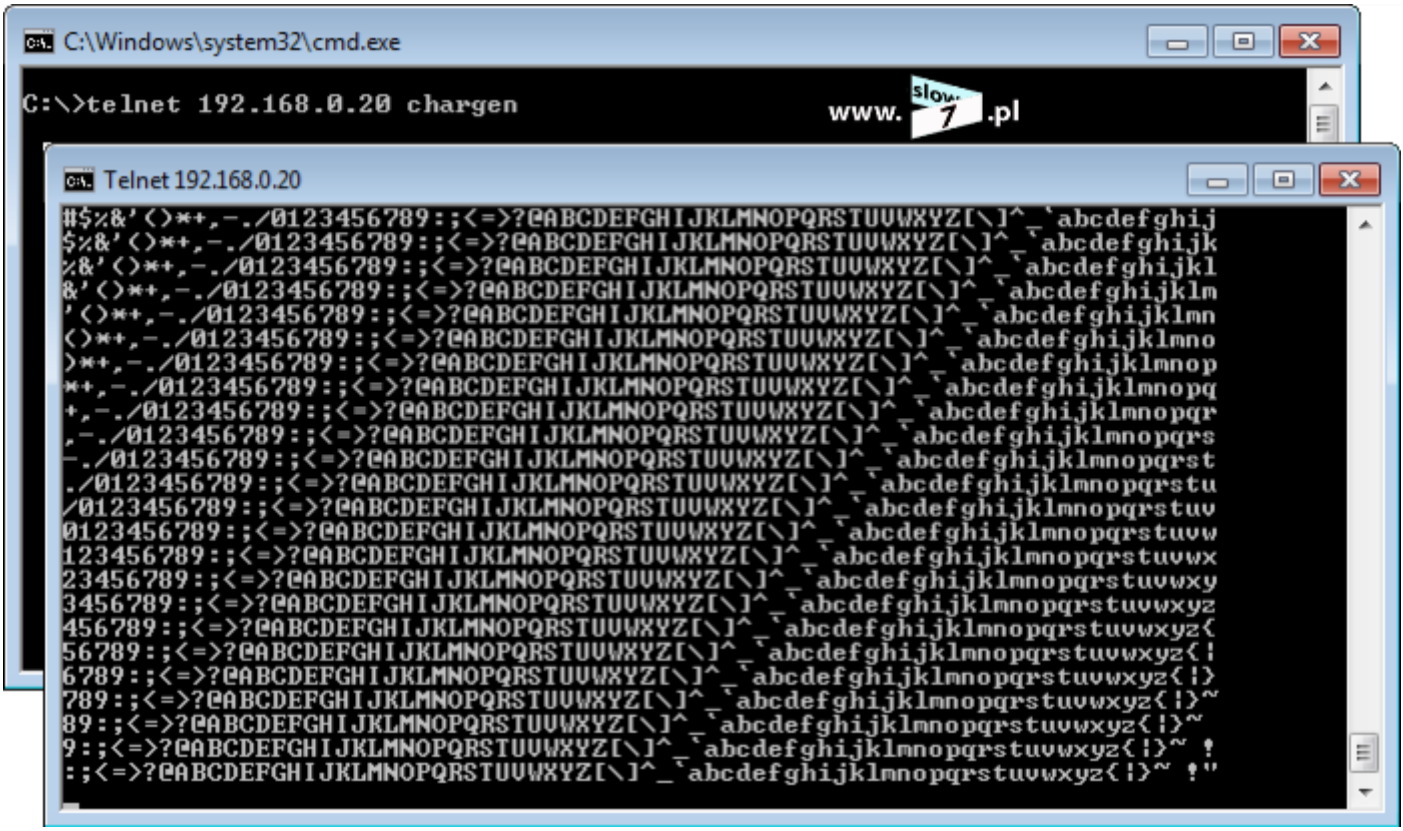


Usługa **discard** do działania wykorzystuje port 9 a umożliwia nawiązanie sesji z routerem, dalsze działanie sprowadza się do ignorowania wszystkich przesyłanych danych.

Jak się można spodziewać wywołanie funkcji **daytime** spowoduje zwrócenie informacji o dacie i czasie urządzenia. Do działania jest wykorzystywany port 13.



Chargen jest funkcją generowania znaków. Po nawiązaniu polecenia router zaczyna generować dane, które są następnie wysyłane w kierunku klienta. Funkcja działa na porcie 19 i może być wykorzystana do badania obciążenia sieci.



Działanie funkcji w zależności od wykorzystywanego protokołu (TCP bądź UDP) może sięróżnić.

Wyłączenie „małych serwerów” odbywa się za pomocą poleceń **no service tcp-small-servers** oraz **no service udp-small-servers**.

Jeżeli chcemy aby router o zadanej godzinie przeładował swój system możemy do tego celu wykorzystać dwa polecenia. Pierwsza komenda to **reload in** natomiast druga to **reload at**. Polecenia te mogą stanowić swego rodzaju sposób zabezpieczenia przed wydaniem niewłaściwych poleceń, które spowodują brak dostępu do routera. Wyobraź sobie czytelniku o to taką sytuację w której to administrator zdalnie konfiguruje router wprowadzając poprawki dotyczące routingu czy administrator modyfikuje listy ACL i w skutek błędnie wprowadzonego polecenia następuje zerwanie połączenia z urządzeniem. Brak łączności uniemożliwia naprawienie pomyłki. Cały trik polega na tym, aby przed zaczęciem wprowadzania potencjalnie niebezpiecznych zmian wprowadzić mechanizm opóźnionego restartu. W ten sposób nawet jeśli dojdzie do pomyłki router uruchomi się ponownie z konfiguracją startową, która nie będzie uwzględniała wprowadzonych zmian. W przypadku wykorzystania polecenia **reload in** po poleceniu musimy podać czas po którym ma nastąpić ponowne uruchomienie urządzenia. Polecenie przyjmuje kształt **reload in <czas_po_którym_nastąpi_restart>**. Po wydaniu polecenia nastąpi:

1.
1. jeśli konfiguracja routera uległa zmianie, pytanie o zapisanie zmian,
2. potwierdzenie wydania polecenia.

Drugie polecenie wymaga od nas podania dokładnej daty i czasu wykonania ponownego rozruchu. Polecenie przyjmuje kształt**reload at <czas> <data>**.

Router domyślnie na 1 godzinę, 30 minut, 15 minut, 5 minut oraz minutę przed wykonaniem wymuszonego restartu powiadomi nas o tym stosownym komunikatem.

Przegląd zaplanowanych restartów można dokonać po wydaniu polecenia – **show reload**.

Anulowanie procedury restartu następuje po wydaniu komendy – **reload cancel**.
Do określenia kondycji routera i jego aktualnego stanu możemy posłużyć się kilkoma poleceniami z rodziny **show**.
Każdy z routerów oprócz interfejsów fizycznych może obsługiwać interfejsy logiczne (np. interfejsy loopback czy subinterfejsy) lecz ilość obsługiwanych interfejsów logicznych jest ograniczona i zależy od modelu routera jak i wersji systemu IOS. Ilość maksymalnych obsługiwanych interfejsów logicznych w zależności od modelu urządzenia i wersji systemu sprawdzisz tu -

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a0080094322.shtml

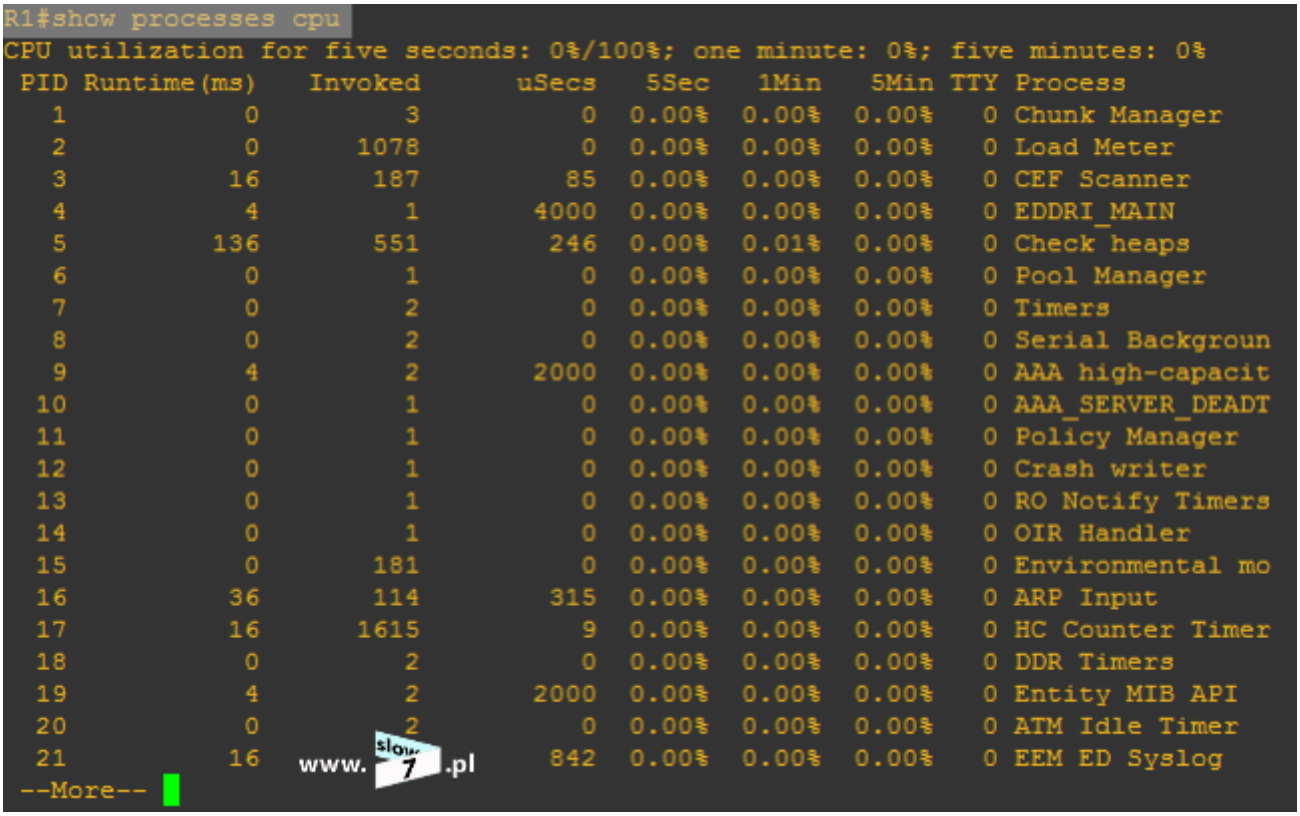
Aby sprawdzić ten parametr na urządzeniu wydaj polecenie - **show idb**

```
R1#show idb

Maximum number of Software IDBs 800.  In use 7.

                     HWIDBs     SWIDBs
Active                    5          5
Inactive                  2          2
Total IDBs                7          7
Size each (bytes)      2912       1280
Total bytes           20384       8960

Type SIdx Idx  St,O,Sh Interface Name (subblocks)
-------------------------------------------------
H     1    2   U,I,R  FastEthernet0/0 (HW SB CDP(3), MAC ADDR(2), Ether(1))
H     2    3   U,I,R  FastEthernet1/0 (HW SB CDP(3), MAC ADDR(2), Ether(1))
H     3    4   A,I,R  FastEthernet2/0 (HW SB CDP(3), MAC ADDR(2), Ether(1))
H     4    5   A,I,R  FastEthernet3/0 (HW SB CDP(3), MAC ADDR(2), Ether(1))
H     5    1   U,D,R  VoIP-Null0

S     1    3   U      FastEthernet0/0 (SW CDP(5), DSS(4), Dynamic DNS Updates(3), NetBIOS(2), KEEPALIVE(1))
S     2    4   U      FastEthernet1/0 (SW CDP(5), DSS(4), Dynamic DNS Updates(3), NetBIOS(2), KEEPALIVE(1))
S     3    5   U      FastEthernet2/0 (SW CDP(5), DSS(4), NetBIOS(2), KEEPALIVE(1))
S     4    6   U      FastEthernet3/0 (SW CDP(5), DSS(4), NetBIOS(2), KEEPALIVE(1))
S     5    2   U      VoIP-Null0 (NetBIOS(2), KEEPALIVE(1))

Key: SIdx=Sort Index, Idx=hw_if_index or if_number
     St=Current State, O=Old State, Sh=Shadow State
     A=Admindown, D=Down, G=Going Down, I=Init
     R=Reset, T=Testing, U=Up, X=Deleted
```


Interfejsy logiczne używamy do różnych celów np. subinterfejsy do tzw. routingu na patyku (ang. routing on a stick) zapewniającego routing pomiędzy VLAN-ami czy przy interfejsach loopback (testowanie). Ponieważ uruchomienie takiego interfejsu zużywa pewne zasoby routera (pamięć, procesor) dlatego ustalono ich maksymalną liczbę. Aby pokazać zmianę w uzyskiwanych informacjach uruchomiłem dodatkowy interfejs loopback i subinterfejs.

```
R1#show idb

Maximum number of Software IDBs 800.  In use 9.

                    HWIDBs     SWIDBs
Active                   6          7
Inactive                 2          2
Total IDBs               8          9
Size each (bytes)     2912       1280
Total bytes          23296      11520

Type SIdx Idx  St,O,Sh Interface Name (subblocks)
-------------------------------------------------
H     1    2   U,I,R  FastEthernet0/0 (HW SB CDP(3), MAC ADDR(2), Ether(1))
H     2    3   U,I,R  FastEthernet1/0 (HW SB CDP(3), MAC ADDR(2), Ether(1))
H     3    4   A,I,R  FastEthernet2/0 (HW SB CDP(3), MAC ADDR(2), Ether(1))
H     4    5   A,I,R  FastEthernet3/0 (HW SB CDP(3), MAC ADDR(2), Ether(1))
H     5    7   U,D,R  Loopback1
H     6    1   U,D,R  VoIP-Null0

S     1    3   U      FastEthernet0/0 (SW CDP(5), DSS(4), Dynamic DNS Updates(3), NetBIOS(2), KEEPALIVE(1))
S     2    9   U      FastEthernet0/0.1 (DSS(4), SW CDP(5))
S     3    4   U      FastEthernet1/0 (SW CDP(5), DSS(4), Dynamic DNS Updates(3), NetBIOS(2), KEEPALIVE(1))
S     4    5   U      FastEthernet2/0 (SW CDP(5), DSS(4), NetBIOS(2), KEEPALIVE(1))
S     5    6   U      FastEthernet3/0 (SW CDP(5), DSS(4), NetBIOS(2), KEEPALIVE(1))
S     6    8   U      Loopback1 (KEEPALIVE(1))
S     7    2   U      VoIP-Null0 (NetBIOS(2), KEEPALIVE(1))

Key: SIdx=Sort Index, Idx=hw_if_index or if_number
     St=Current State, O=Old State, Sh=Shadow State
     A=Admindown, D=Down, G=Going Down, I=Init
     R=Reset, T=Testing, U=Up, X=Deleted
```


Dzięki poleceniu **show processes cpu** możemy sprawdzić stan obciążenia routera. Wydanie polecenia powoduje wyświetlenie listy wszystkich uruchomionych procesów wraz z ich procentową wartością obciążenia. Dodanie do polecenia słowa **sorted**spowoduje posortowanie procesów według obciążenia.



Podobnie możemy sprawdzić ilość pamięci jaka jest zajmowana poprzez poszczególne procesy – **show processes memory**.

```
R1#show processes memory
Processor Pool Total:   67603136 Used:   10926060 Free:   56677076
      I/O Pool Total:    6291456 Used:    2583968 Free:    3707488

 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0   0   19959528    5556132   10908068          0          0 *Init*
   0   0      12052      86480      12052          0          0 *Sched*
   0   0        860    1766116         76     163260     163260 *Dead*
   0   0          0          0     496872          0          0 *MallocLite*
   1   0          0          0       6972          0          0 Chunk Manager
   2   0        196        196       3972          0          0 Load Meter
   3   0        164          0       7160          0          0 CEF Scanner
   4   0      65588          0      90560          0          0 EDDRI_MAIN
   5   0       3100          0      10072          0          0 Check heaps
   6   0          0          0       6972          0          0 Pool Manager
   7   0        196        196       6972          0          0 Timers
   8   0        196        196       6972          0          0 Serial Backgroun
   9   0        196        196       6972          0          0 AAA high-capacit
  10   0          0          0       6972          0          0 AAA_SERVER_DEADT
  11   0          0          0      12972          0          0 Policy Manager
  12   0          0          0      24972          0          0 Crash writer
  13   0          0          0       6972          0          0 RO Notify Timers
  14   0          0          0      12972          0          0 OIR Handler
  15   0        196        196       6972          0          0 Environmental mo
 --More--
```

Wydanie polecenia **show memory statistics** spowoduje wyświetlenie statystyki używanej pamięci.

```
R1#show memory statistics
                Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor   63987540    67603136    10927024    56676112    54985396    54910196
      I/O    7A00000     6291456     2583976     3707480     3707480     3707452
R1#
```

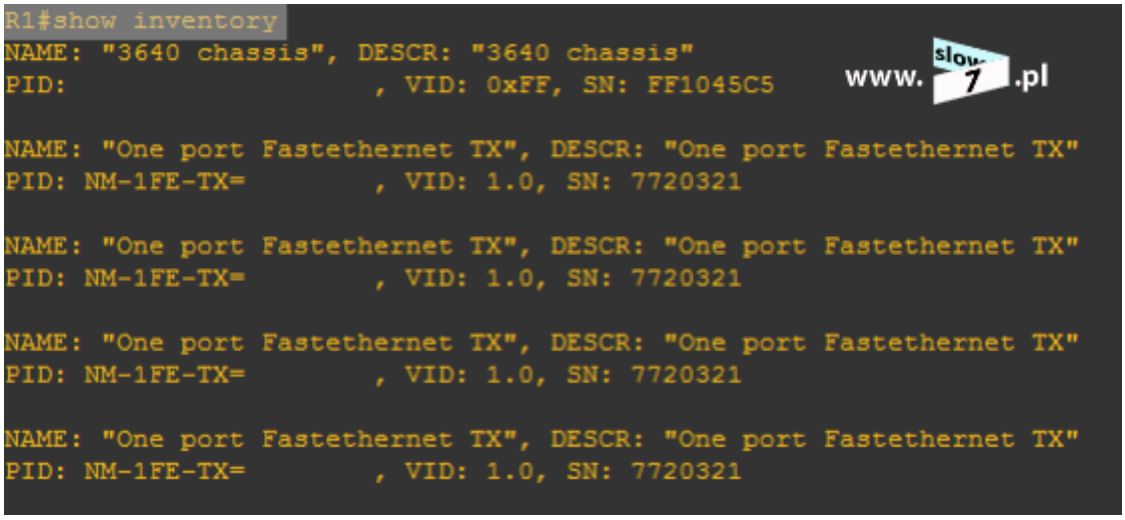
Jeżeli chcesz sprawdzić historię zajętości procesora użyj komendy - **show processes cpu history**. Po wydaniu komendy zostaną wygenerowane trzy wykresy, które ukarzą nam procentowe użycie procesora w ostatnich 60 sekundach, 60 minutach oraz 72 godzinach.

```
R3#show processes cpu history

R3   12:05:34 AM Friday Mar 1 2002 UTC



                                  11111
100
 90
 80
 70
 60
 50
 40
 30
 20
 10
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
               CPU% per second (last 60 seconds)
```

Aby poznać szczegóły dotyczące zainstalowanych i wykrytych kart, posłuż się poleceniem – **show diag**

```
R1#show diag
Slot 0:
        Fast-ethernet Port adapter, 1 port
        Port adapter is analyzed
        Port adapter insertion time 01:39:08 ago
        EEPROM contents at hardware discovery:
        Hardware revision 1.0           Board revision B0
        Serial number     7720321       Part number    800-03490-01
        FRU Part Number     NM-1FE-TX=
        Test history      0x0           RMA number     00-00-00
        EEPROM format version 1
        EEPROM contents (hex):
          0x00: 01 44 01 00 00 75 CD 81 50 0D A2 01 00 00 00 00
          0x10: 58 00 00 00 98 03 20 00 FF FF FF FF FF FF FF FF
          0x20: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x30: FF FF FF FF FF FF FF FF FF FF FF FF

Slot 1:
        Fast-ethernet Port adapter, 1 port
        Port adapter is analyzed
        Port adapter insertion time 01:39:08 ago
        EEPROM contents at hardware discovery:
        Hardware revision 1.0           Board revision B0
        Serial number     7720321       Part number    800-03490-01
 --More--
```

Dodatkowo możesz się posłużyć poleceniem – **show inventory**



Kolejna porcja poleceń w następnym wpisie dotyczącym urządzeń Cisco. W następnej odsłonie zajmiemy się poleceniami związanymi z użytkownikiem, hasłami oraz dostępem innym niż konsola.