informatyka+

Algorytmika i programowanie

Bazy danych

Multimedia, grafika i technologie internetowe

Sieci komputerowe

Tendencje w rozwoju informatyki i jej zastosowań

Człowiek – najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

informatyka+

Wszechnica Informatyczna: Sieci komputerowe

Podstawy działania routerów i routingu

Dariusz Chaładyniak

Józef Wacnik

Człowiek – najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Podstawy działania routerów i routingu

Rodzaj zajęć: Wszechnica Informatyczna
Tytuł: Podstawy działania routerów i routingu
Autor: dr inż. Dariusz Chaładyniak, mgr inż. Józef Wacnik

Redaktor merytoryczny: prof. dr hab. Maciej M Sysło

Zeszyt dydaktyczny opracowany w ramach projektu edukacyjnego **Informatyka+** — ponadregionalny program rozwijania kompetencji uczniów szkół ponadgimnazjalnych w zakresie technologii informacyjno-komunikacyjnych (ICT).
www.informatykaplus.edu.pl
kontakt@informatykaplus.edu.pl

Wydawca: Warszawska Wyższa Szkoła Informatyki
ul. Lewartowskiego 17, 00-169 Warszawa
www.wwsi.edu.pl
rektorat@wwsi.edu.pl

Projekt graficzny: FRYCZ I WICHA

Warszawa 2010

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Podstawy działania routerów i routingu

Dariusz Chaładyniak
Warszawska Wyższa Szkoła Informatyki
dchalad@wwsi.edu.pl

Józef Wacnik
Warszawska Wyższa Szkoła Informatyki
j_wacnik@poczta.wwsi.edu.pl

Streszczenie

W dzisiejszych czasach sieci komputerowe mają ogromny wpływ na nasze życie. Rozumiane także w kontekście Internetu, jak nigdy dotąd, umożliwiają ludziom komunikację, współpracę oraz interakcję. Używamy sieci komputerowych na wiele różnych sposobów i dla różnych zastosowań. Centralnym elementem architektury sieciowej jest router, który łączy ze sobą sieci – odpowiada także za przesyłanie pakietów poprzez różne sieci. Wykład zawiera podstawowe informacje o budowie, działaniu oraz zastosowaniu routerów. Opisuje możliwe tryby ich pracy, metody zakładania haseł a także proces konfiguracji ich interfejsów ethernetowych i szeregowych. Przedstawiono również podstawowe mechanizmy weryfikacji komunikacji międzysieciowej (protokoły ping, traceroute, telnet). Wykład jest ponadto wprowadzeniem do protokołów routingu statycznego i dynamicznego.

Warsztaty są okazją do praktycznego przećwiczenia materiału z wykładu.

Spis treści

1 BUDOWA, DZIAŁANIE I ZASTOSOWANIE ROUTERÓW

Wprowadzenie

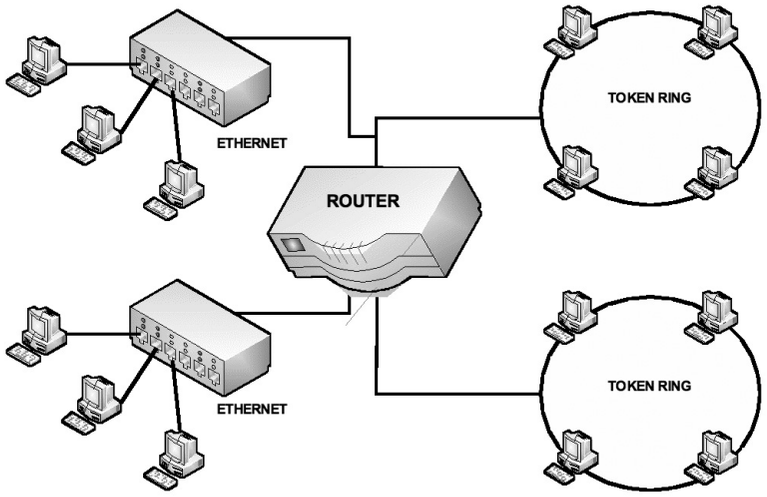
Router to specjalny typ komputera, zawiera te same podstawowe podzespoły, co zwykły komputer PC: procesor, pamięć, magistralę systemową oraz różne interfejsy wejścia/wyjścia. Routery to urządzenia sieciowe, realizujące usługi trasowania (tzn. wybierania optymalnej marszruty) i przełączania pakietów pomiędzy wieloma sieciami. Są one łącznikami sieci LAN z bardziej rozległymi sieciami WAN, tworząc rdzeń Internetu.

Tak samo jak komputery wymagają systemów operacyjnych do uruchamiania aplikacji, tak routery wymagają oprogramowania **IOS** (ang. *Internetwork Operating System*) do uruchamiania plików konfiguracyjnych. Pliki konfiguracyjne zawierają instrukcje i parametry sterujące przepływem komunikacji do routerów i z nich. Routery korzystają z protokołów routingu do określenia najlepszej ścieżki dla pakietów. Pliki konfiguracyjne określają wszystkie informacje konieczne do prawidłowej konfiguracji użycia przez router wybranych lub włączonych protokołów routingu.

Routery służą do zwiększania fizycznych rozmiarów sieci poprzez łączenie jej segmentów (patrz rys. 1). Urządzenie to wykorzystuje logiczne adresy hostów w sieci, dzięki temu komunikacja, jako oparta na logicznych adresach odbiorcy i nadawcy, jest niezależna od fizycznych adresów urządzeń.

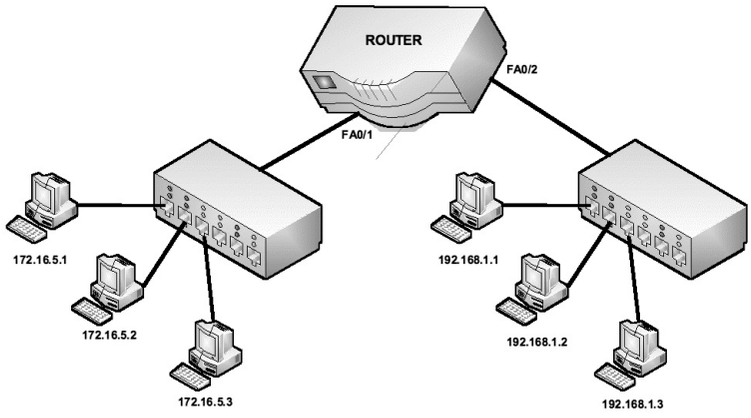
Oprócz filtracji pakietów pomiędzy segmentami, router określa optymalną drogę przesyłania danych po sieci. Dodatkowo eliminuje pakiety bez adresata i ogranicza dostęp określonych użytkowników do wybranych segmentów czy komputerów sieciowych.

Router jest konfigurowalny, umożliwia sterowanie przepustowością sieci oraz zapewnia pełną izolację pomiędzy segmentami.



Rysunek 1.
Przykładowe zastosowanie routera

TABLICA ROUTINGU	
SIEĆ	INTERFEJS
172.16.0.0/16	FA0/1
192.168.1.0/24	FA0/2

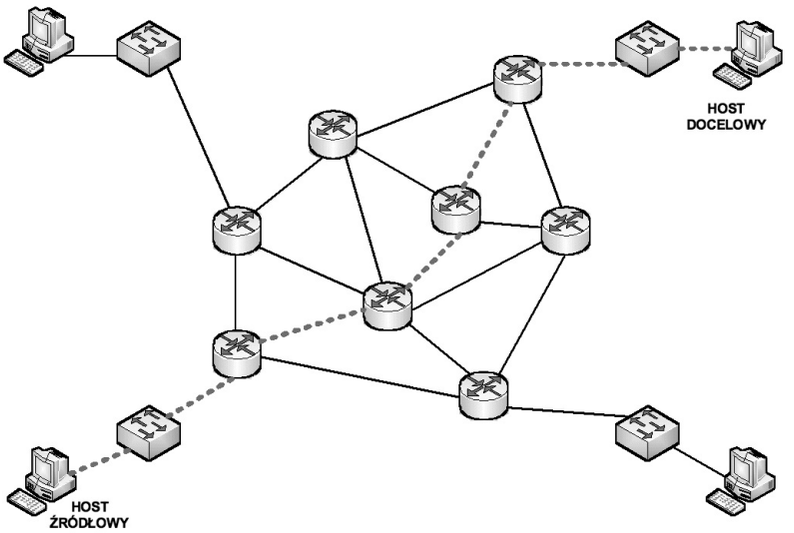


Rysunek 2.
Tablica routingu

Tablica routingu (ang. *routing table*) pokazana na rysunku 2 jest miejscem, w którym są przechowywane informacje o adresach logicznych sieci lub podsieci, maskach oraz interfejsach wyjściowych (ethernetowych lub szeregowych).

Wybór najlepszej ścieżki dla pakietów

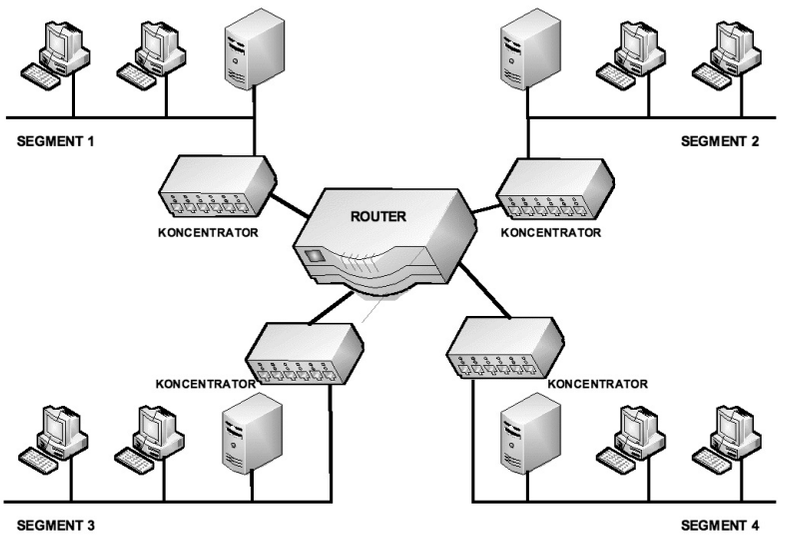
Podstawowym zadaniem routerów jest wybór optymalnej ścieżki dla pakietów na trasie od hosta źródłowego do hosta docelowego (patrz rys. 3). Routery do tego celu wykorzystują tablice routingu, które mogą być tworzone statycznie lub dynamicznie. Metoda statyczna polega na ręcznym budowaniu tablic routingu, natomiast metody dynamiczne wykorzystują odpowiednie algorytmy trasowania.



Rysunek 3.
Wybór optymalnej trasy dla pakietów

Segmentacja za pomocą routera

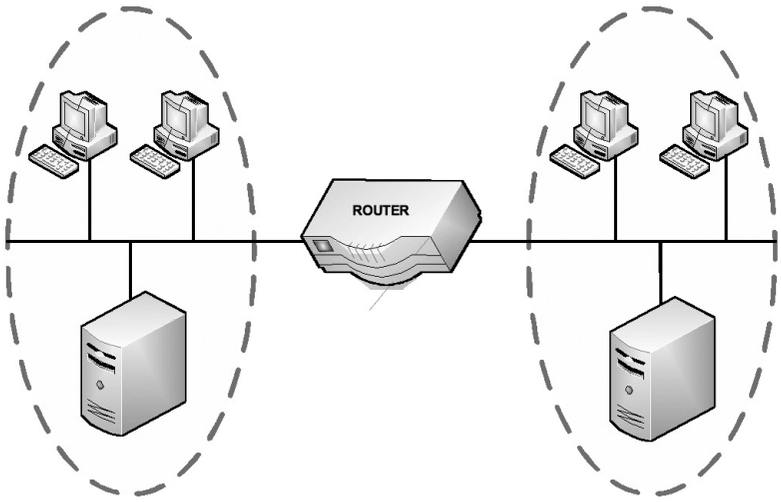
Segmentacja polega na podziale sieci na kilka mniejszych części (patrz rys. 4). Przy zastosowaniu segmentów oddzielonych routerami najintensywniej komunikujące się stacje robocze nie przeszkadzają sobie wzajemnie w pracy. Dzięki urządzeniom potrafiącym inteligentnie zatrzymać zbędny ruch sieć zostaje zrównoważona i znacznie odciążona.



Rysunek 4.
Przykład segmentacji sieci za pomocą routera

Router – nie przenosi kolizji

Przy zastosowaniu urządzeń sieciowych warstwy sieci, łączone ze sobą sieci stanowią osobne domeny kolizyjne (patrz rys. 5). Jest to bardzo pożądane rozwiązanie.



Rysunek 5.
Router nie powiększa domen kolizyjnych oraz rozgłoszeniowych

Rodzaje pamięci routera

Pamięć **RAM** ma następujące cechy i funkcje:
- przechowuje tablice routingu,
- zawiera pamięć podręczną protokołu **ARP** (ang. *Address Resolution Protocol*),
- zawiera aktualną konfigurację routera,
- buforuje pakiety (po odebraniu pakietu na jednym interfejsie, ale przed przekazaniem ich na inny interfejs są one okresowo składowane w buforze),
- traci zawartość po wyłączeniu lub restarcie routera.

Pamięć **NVRAM** (ang. *nonvolatile RAM*) ma następujące cechy i funkcje:
- przechowuje pliki konfiguracji początkowej (o ile została zapisana, w nowych, pierwszy raz uruchomionych routerach, jest ona pusta) i ich kopie zapasowe
- utrzymuje zawartość po wyłączeniu lub restarcie routera.

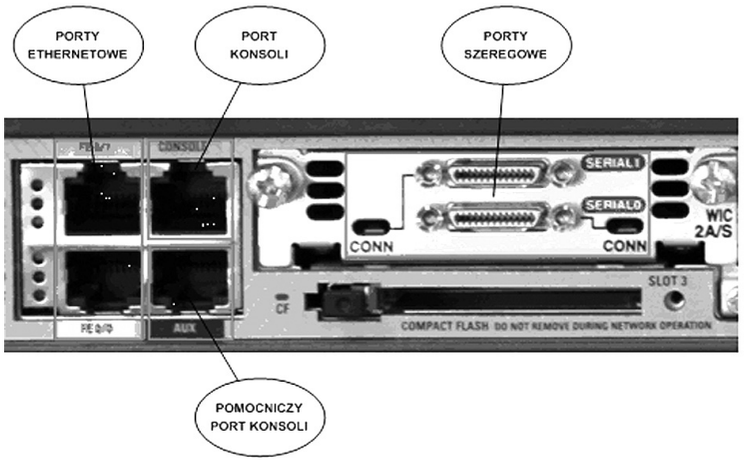
Pamięć **flash** (EPROM – ang. *Erasable Programmable ROM*) ma następujące cechy:
- przechowuje obraz IOS,
- umożliwia aktualizację oprogramowania bez konieczności wyjmowania i wymiany układów scalonych karty,
- utrzymuje zawartość po wyłączeniu lub restarcie routera,
- może przechowywać wiele wersji oprogramowania IOS.

Pamięć **ROM** ma następujące cechy i funkcje:
- zawiera instrukcje dla procedur diagnostycznych **POST** (ang. *Power-On Self Test*),
- przechowuje program uruchomieniowy (bootstrap) i podstawowe oprogramowanie systemu operacyjnego.

Porty routera

Routery są wyposażone w następujące porty (patrz rys. 6):
- ethernetowe – do podłączania sieci LAN,
- szeregowe – do łączenia sieci WAN,
- konsoli – do lokalnego konfigurowania,
- pomocniczy konsoli – do zdalnego konfigurowania.

2 PORTY SIECIOWE ROUTERÓW



Rysunek 6.
Przykładowe porty routera

Połączenia portu konsoli

Port konsoli służy do konfiguracji początkowej routera i do jego monitorowania. Port konsoli jest również używany w procedurach stosowanych w razie awarii. Do połączenia komputera PC z portem konsoli routera (patrz rys. 7) służy kabel konsolowy (rollover) i przejściówka z RJ-45 na DB-9 (lub DB-25). Komputer PC lub terminal muszą obsługiwać emulację terminala **VT100** (np. *HyperTerminal*). Aby podłączyć komputer do routera, należy wykonać następujące operacje:

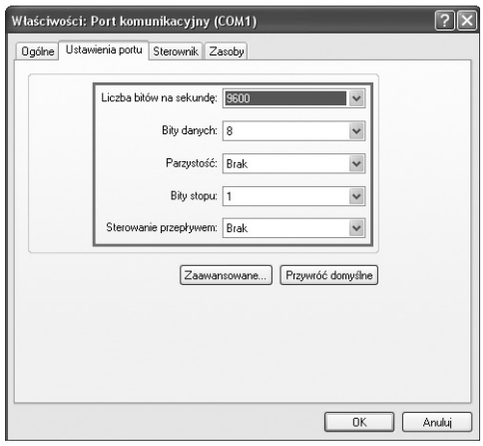
1. Podłącz złącze RJ-45 kabla rollover do portu konsoli routera.
2. Podłącz drugi koniec kabla rollover do przejściówki RJ-45 na DB-9 (lub DB-25).
3. Podłącz żeńskie złącze DB-9 (lub DB-25) przejściówki do komputera PC.

Rysunek 7.
Przykład połączenia komputera (terminala) do portu konsuli routera

Konfiguracja portu konsoli

Należy skonfigurować następujące parametry w oprogramowaniu emulacji terminala na komputerze PC (patrz rys. 8):

1. Odpowiedni port COM – COM1 lub COM2.
2. Liczba bitów danych na sekundę – 9600.
3. Liczba bitów danych – 8.
4. Kontrola parzystości – brak bitu kontroli parzystości.
5. Liczba bitów stopu – 1.
6. Sterowanie przepływem – brak kontroli przepływu.



Rysunek 8.
Konfiguracja portu szeregowego komputera (terminala)

Połączenia pomocniczego portu konsoli

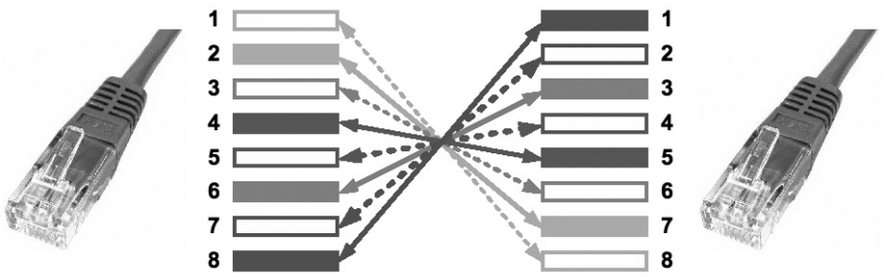
Rysunek 9.
Przykład połączenia modemu do pomocniczego portu konsuli routera

Pomocniczy port konsoli jest portem służącym do zdalnej konfiguracji początkowej routera i do jego monitorowania za pomocą modemu (rys. 9). Do połączenia modemu z pomocniczym portem konsoli routera służy kabel konsolowy (rollover) i przejściówka z RJ-45 na DB-9 (lub DB-25). Aby podłączyć modem do routera, należy wykonać następujące operacje:

1. Podłącz złącze RJ-45 kabla rollover do pomocniczego portu konsoli routera;
2. Podłącz drugi koniec kabla rollover do przejściówki RJ-45 na DB-9 (lub DB-25);
3. Podłącz męskie złącze DB-9 (lub DB-25) przejściówki do portu szeregowego modemu.

Kabel konsolowy

Kabel konsolowy (ang. *rollover cable*) charakteryzuje się tym, że wszystkie jego pary są zamienione miejscami – pin nr 1 w miejsce pinu nr 8, pin nr 2 w miejsce pinu nr 7 itd. (patrz rys. 10). Wykorzystywany jest przy połączeniach typu: komputer PC (terminal) – router (port konsoli), komputer PC (terminal) – przełącznik (port konsoli).



Rysunek 10.
Schemat zaterminowania kabla konsolowego

3 PODSTAWOWA KONFIGURACJA ROUTERÓW

Interfejs wiersza poleceń

Interfejs wiersza poleceń **CLI** (ang. *Command Line Interface*) jest tradycyjną konsolą wykorzystywaną przez oprogramowanie Cisco IOS. Istnieje kilka metod dostępu do środowiska CLI.

1. Zazwyczaj dostęp do interfejsu CLI jest realizowany poprzez sesję konsoli. Konsola korzysta z połączenia szeregowego o małej prędkości, które łączy bezpośrednio komputer lub terminal ze złączem konsoli w routerze.
2. Do sesji CLI można również uzyskać dostęp zdalny przy użyciu połączenia telefonicznego, wykorzystując modem dołączony do portu AUX routera. Żadna z tych metod nie wymaga skonfigurowania usług IP w routerze.
3. Trzecią metodą uzyskiwania dostępu do sesji CLI jest ustanowienie z routerem sesji Telnet. Aby ustanowić sesję Telnet z routerem, należy skonfigurować adres IP dla co najmniej jednego interfejsu, a dla sesji terminala wirtualnego trzeba ustawić login i hasła.

Tryby pracy na routerze

W interfejsie CLI jest używana struktura hierarchiczna. Struktura ta wymaga przejścia do odpowiedniego trybu w celu wykonania określonych zadań. Na przykład, aby skonfigurować interfejs routera, należy włączyć tryb konfiguracji interfejsu. Wszystkie ustawienia wprowadzone w trybie konfiguracji interfejsu dotyczą tylko danego interfejsu. Każdy z trybów konfiguracji jest oznaczony specjalnym symbolem i umożliwia wprowadzenie tylko tych poleceń, które są właściwe dla danego trybu.

System IOS udostępnia usługę interpretacji poleceń o nazwie **EXEC**. Po wprowadzeniu każdego polecenia, usługa EXEC sprawdza jego poprawność i wykonuje je. W celu zapewnienia bezpieczeństwa, w IOS występują dwa poziomy dostępu do sesji EXEC. Są to tryb EXEC użytkownika oraz uprzywilejowany tryb EXEC. Uprzywilejowany tryb EXEC po angielsku jest również nazywany trybem *enable*.

Tryb EXEC użytkownika udostępnia jedynie ograniczony zestaw podstawowych poleceń do monitorowania. Z tego powodu jest on również nazywany trybem „tylko do odczytu". Tryb EXEC użytkownika nie udostępnia żadnych poleceń, które umożliwiają zmianę konfiguracji routera. Tryb EXEC użytkownika jest oznaczony symbolem **›**.

Uprzywilejowany tryb EXEC umożliwia dostęp do wszystkich poleceń routera. Do wejścia w ten tryb może być potrzebne hasło. Dodatkową ochronę można zapewnić, ustawiając żądanie podania identyfikatora użytkownika tak, aby dostęp do routera miały tylko uprawnione osoby. Aby z poziomu EXEC użytkownika uzyskać dostęp do uprzywilejowanego poziomu EXEC, należy po symbolu **›** wprowadzić polecenie **enable**. Jeśli skonfigurowane jest hasło, router zażąda jego podania. Po wprowadzeniu poprawnego hasła, symbol zachęty routera zmieni się na symbol **#**. Oznacza to, że użytkownik jest w uprzywilejowanym trybie EXEC.

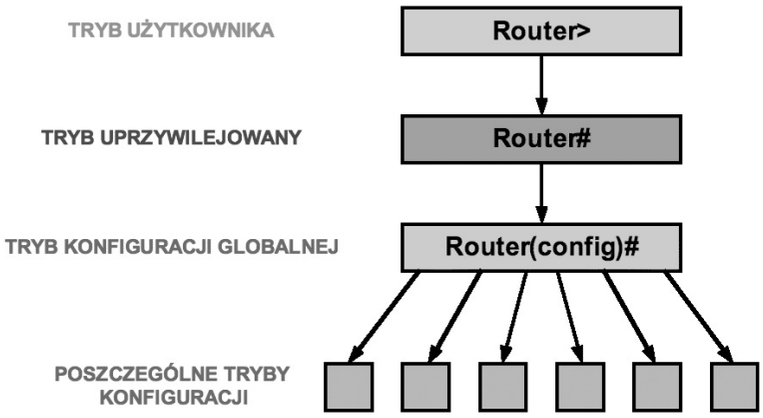
Tryb konfiguracji globalnej oraz wszystkie inne bardziej szczegółowe tryby konfiguracji są dostępne tylko z uprzywilejowanego trybu EXEC. Aby przejść do trybu konfiguracyjnego należy wprowadzić polecenie **configure terminal**. O tym, że pracujemy w trybie konfiguracyjnym zawiadamia nas znak gotowości np. **Router(config)#**. Zakończenie pracy w tym trybie realizowane jest poprzez wprowadzenie kombinacji klawiszy **CTR-L+Z**. Ponadto tryb konfiguracyjny można opuścić, wprowadzając w wierszu poleceń: **end** lub **exit**.

Przełączanie pomiędzy trybami EXEC
Aby przejść z trybu użytkownika do trybu uprzywilejowanego wpisujemy polecenie **enable** a następnie podajemy hasło. Aby powrócić z powrotem do trybu użytkownika, wpisujemy polecenie **disable** (patrz rys.11).

```
Router con0 is now available.

Press RETURN to get started.


User Access Verification
Password:
Router>                          <-- Tryb EXEC użytkownika
Router> enable
Password:
Router#                          <-- Tryb EXEC uprzywilejowany
Router# disable
Router>
Router> exit
```

Rysunek 11.
Przełączanie pomiędzy trybami pracy routera

Tryby konfiguracji IOS



Rysunek 12.
Tryby konfiguracji routera

Wyróżniamy następujące tryby konfiguracji w systemie operacyjnym IOS (patrz rys. 12):
- tryb użytkownika;
- tryb uprzywilejowany;
- tryb konfiguracji globalnej;
- poszczególne tryby konfiguracji.

Lista poleceń w trybie użytkownika
W trybie użytkownika mamy ograniczoną liczbę poleceń, które możemy wydawać systemowi operacyjnemu IOS, patrz rys. 13.

Lista poleceń w trybie uprzywilejowanym
W trybie uprzywilejowanym możemy korzystać ze wszystkich dostępnych poleceń systemu operacyjnego IOS, patrz rys. 14.

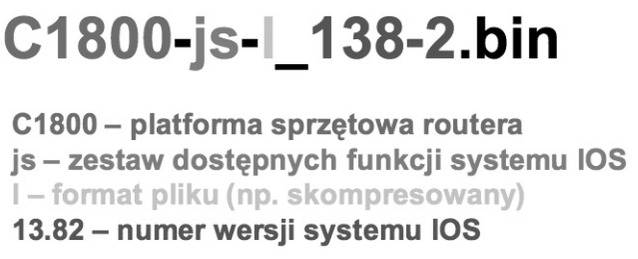
Pola w nazwie pliku obrazu IOS
Istnieje wiele różnych wersji oprogramowania Cisco IOS. System IOS obsługuje różne platformy sprzętowe i funkcje (patrz rys. 15). W celu zapewnienia możliwości rozróżnienia poszczególnych wersji utworzona została konwencja nazewnictwa plików systemu IOS. W konwencji tej rozróżniane są poszczególne pola nazwy. Są to między innymi: identyfikator platformy sprzętowej, identyfikator zestawu funkcji i numer wersji.

```
Router> ?
Exec Commands:
access-enable Creates a temporary access list entry
atmsig        Executes ATM signaling commands
cd            Changes current device
clear         Resets functions
connect       Opens a terminal connection
dir           Lists files on a given device
disable       Turns off privileged commands
disconnect    Disconnects an existing network connection
enable        Turns on privileged commands
exit          Exits EXEC
help          Gets a description of the interactive help
              system
lat           Opens a LAT connection
lock          Locks the terminal
login         Logs in as a particular user
logout        Exits from EXEC mode
mrinfo        Requests neighbor and version information
              from a multicast router

--More--
```

Rysunek 13.
Przykładowe polecenia systemu IOS dostępne w trybie użytkownika

```
Router> ena
Password:
Router# ?
access-enable       Creates a temporary access list entry
access-template     Creates a temporary access list entry
appn                Sends a command to the APPN subsystem
atmsig              Executes ATM signaling commands
bfe                 Sets manual emergency modes
calendar            Manages the hardware calendar
cd                  Changes the current device
clear               Resets functions
clock               Manages the system clock
cmt                 Starts or stops FDDI connection management functions
configure           Enters configuration mode
connect             Opens a terminal connection
copy                Copies configuration or image data
debug               Uses debugging functions (see also undebug)
delete              Deletes a file
dir                 Lists files on a given device
```

Rysunek 14.
Przykładowe polecenia systemu IOS dostępne w trybie uprzywilejowanym



Rysunek 15.
Przykład nazwy pliku obrazu systemu IOS

Praca z systemem IOS

Istnieją trzy środowiska operacyjne (tryby) urządzeń z systemem IOS:

- tryb ROM monitor,
- tryb Boot ROM,
- tryb IOS.

Tabela 1.
Środowiska operacyjne systemu IOS

Środowisko operacyjne	Symbol zachęty	Wykorzystanie
Tryb ROM monitor	> lub ROMMON>	Awaria lub odzyskiwanie hasła
Tryb Boot ROM	Router(boot)>	Aktualizacja obrazu systemu operacyjnego IOS w pamięci FLASH
System operacyjny IOS	Router>	Normalna praca

Po uruchomieniu, router ładuje do pamięci RAM jedno z powyższych środowisk operacyjnych i rozpoczyna jego wykonywanie. Administrator systemu może przy użyciu ustawienia rejestru konfiguracji wybrać domyślny tryb uruchamiania routera.

Tryb **ROM monitor** realizuje proces uruchomieniowy udostępnia funkcje niskopoziomowe i diagnostyczne. Jest używany w przypadku awarii systemu oraz w celu odzyskania utraconego hasła. Tryb ROM monitor nie jest dostępny za pośrednictwem żadnego interfejsu sieciowego. Jedyną metodą dostępu jest bezpośrednie fizyczne połączenie przez port konsoli.

Podczas pracy w trybie **Boot ROM** na routerze dostępny jest tylko ograniczony zestaw funkcji systemu IOS. Tryb Boot ROM umożliwia operacje zapisu do pamięci błyskowej i jest używany głównie w celu zastąpienia obrazu systemu IOS znajdującego się w tej pamięci. W trybie Boot ROM można modyfikować obraz systemu IOS, używając polecenia **copy tftp flash**. Polecenie to powoduje skopiowanie obrazu systemu IOS przechowywanego na serwerze TFTP do pamięci flash routera.

Podczas normalnego działania routera jest wykorzystywany pełny obraz systemu IOS zapisany w pamięci flash. W przypadku niektórych urządzeń system IOS jest uruchamiany bezpośrednio z pamięci flash. Jednak w przypadku większości routerów Cisco kopia systemu IOS jest ładowana do pamięci RAM i z niej uruchamiana. Niektóre obrazy systemu IOS są zapisane w pamięci flash w postaci skompresowanej i podczas kopiowania do pamięci RAM muszą zostać zdekompresowane.

Aby zobaczyć informacje o obrazie i wersji uruchomionego systemu IOS, należy użyć polecenia **show version**, które wyświetla również ustawienie rejestru konfiguracyjnego. Aby sprawdzić, czy w systemie jest wystarczająca ilość pamięci do załadowania nowego obrazu systemu IOS, należy użyć polecenia **show flash**.

Nazwa routera

Jednym z pierwszych zadań konfiguracyjnych powinno być nadanie routerowi unikatowej nazwy (patrz rys. 16). Zadanie to wykonuje się w trybie konfiguracji globalnej za pomocą następującego polecenia:

```
Router(config)#hostname Darek
```

Po naciśnięciu klawisza **Enter** nazwa w symbolu zachęty zmieni się z domyślnej (**Router**) na nowo skonfigurowaną (**Darek**).

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# hostname Darek
Darek(config)#
```

Rysunek 16.
Zmiana nazwy routera

Konfigurowanie haseł routera

a) **Hasło dla konsoli routera**

Hasła ograniczają dostęp do routerów. Należy je zawsze konfigurować dla **linii terminala wirtualnego** (ang. **vty** – *virtual terminal lines*) oraz **linii konsoli** (ang. *line console*). Hasła służą także do określania praw dostę-

pu do uprzywilejowanego trybu EXEC tak, aby zmian w pliku konfiguracyjnym mogli dokonywać wyłącznie uprawnieni użytkownicy. W celu ustawienia opcjonalnego, ale zalecanego, hasła dla linii konsoli (patrz rys. 17) używa się następujących poleceń (cyfra 0 oznacza numer portu konsoli):

```
Router(config)#line console 0
Router(config-line)#password ‹hasło›
```

Aby wymusić logowanie do portu konsoli za pomocą zdefiniowanego hasła, należy użyć polecenia **login**. Brak tego polecenia daje swobodny dostęp do routera.

```
Router(config-line)#login
```

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# line console 0
Router(config-line)# password Darek
Router(config-line)# login
```

Rysunek 17.
Konfiguracja hasła dla konsoli routera

b) **Hasło dla terminala wirtualnego**
Aby użytkownicy mieli zdalny dostęp do routera przez połączenie Telnet, należy ustawić hasło dla jednej lub wielu linii vty. Większość routerów Cisco obsługuje pięć linii vty o numerach od 0 do 4. Inne platformy sprzętowe obsługują różne liczby połączeń vty. Zazwyczaj używa się tego samego hasła dla wszystkich linii vty. Można jednak ustawić inne hasło dla każdej z linii. Do ustawienia hasła dla wszystkich linii vty używa się następujących poleceń (patrz rys. 18):

```
Router(config)#line vty 0 4
Router(config-line)#password ‹hasło›
Router(config-line)#login
```

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# line vty 0 4
Router(config-line)# password Olek
Router(config-line)# login
```

Rysunek 18.
Konfiguracja hasła dla wirtualnych terminali

c) Hasła dla trybu uprzywilejowanego
Polecenia **enable password** i **enable secret** służą do ograniczania dostępu do uprzywilejowanego trybu EXEC (patrz rys. 19).

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# enable password Warszawa
Router(config)# enable secret Wroclaw
```

Rysunek 19.
Konfiguracja hasła dla trybu uprzywilejowanego

Polecenie **enable password** jest używane tylko wtedy, gdy nie zostało zastosowane polecenie **enable secret**. Należy korzystać z polecenia **enable secret**, ponieważ jest ono szyfrowane, podczas gdy polecenie **enable password** nie jest (zapisane jest otwartym tekstem i doskonale widoczne w konfiguracji routera). Do ustawienia haseł używa się następujących poleceń:

```
Router(config)#enable password ‹hasło›
Router(config)#enable secret ‹hasło›
```

Szyfrowanie haseł

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# service password-encryption
Router(config)# no service password-encryption
```

Rysunek 20.
Szyfrowanie haseł

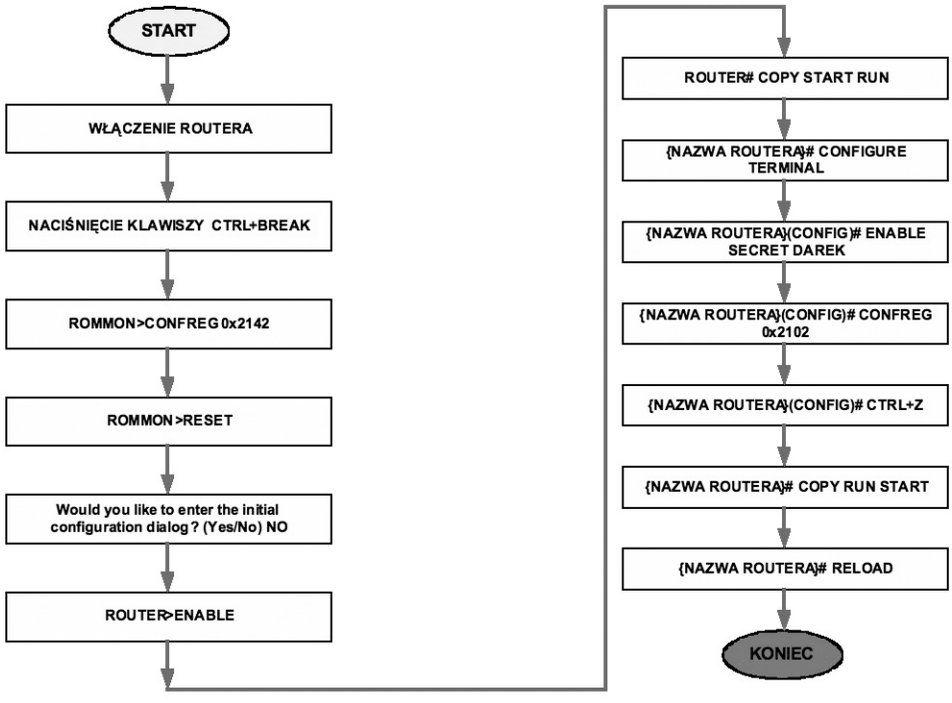
Czasami jest niepożądane, aby hasła były widoczne w postaci niezaszyfrowanej w danych wyświetlanych przez polecenie **show running-config** lub **show startup-config**. Następujące polecenie służy do szyfrowania haseł w danych wyjściowych poleceń konfiguracyjnych:

```
Router(config)#service password-encryption
```

Polecenie **service password-encryption** włącza szyfrowanie wszystkich niezaszyfrowanych haseł za pomocą nieskomplikowanego algorytmu. Aby wyłączyć szyfrowanie haseł służy poniższe polecenie:

```
Router(config)#no service password-encryption
```

Procedura odzyskiwania haseł



Rysunek 21.
Procedura odzyskiwania haseł na routerze

Procedura odzyskiwania haseł na routerze jest bardzo ważną i wartościową umiejętnością. Przeprowadza ją się według kroków przedstawionych na rysunku 21. W zależności od modelu routera i jego systemu operacyjnego IOS mogą być minimalne różnice w procedurze odzyskiwania haseł.

Polecenia show

Wiele poleceń **show** służy do sprawdzania zawartości plików w routerze i rozwiązywania problemów. Zarówno w uprzywilejowanym trybie EXEC, jak i w trybie EXEC użytkownika polecenie **show ?** wyświetla listę dostępnych poleceń **show**. Lista ta jest znacznie dłuższa w uprzywilejowanym trybie EXEC niż w trybie EXEC użytkownika. Wybrane polecenia **show**:

show controllers serial – wyświetla specyficzne informacje dotyczące sprzętu interfejsu. W poleceniu należy także podać port lub numer gniazda/portu interfejsu szeregowego. Na przykład:

Router#show controllers serial 0/1

show clock – wyświetla godzinę ustawioną w routerze.

show hosts – wyświetla przechowywaną w pamięci podręcznej listę nazw i adresów hostów.

show users – wyświetla nazwy wszystkich użytkowników podłączonych do routera.

show history – wyświetla historię wprowadzonych poleceń.

show arp – wyświetla tablicę ARP routera.

show protocols – wyświetla status wszystkich skonfigurowanych protokołów warstwy 3 w ujęciu globalnym i z uwzględnieniem konkretnych interfejsów.

show version – wyświetla informacje o załadowanej w danym momencie wersji oprogramowania wraz z danymi o sprzęcie i urządzeniach, patrz rysunek 22.

- **wersja Cisco IOS,**
- wersja programu bootstrap ROM,
- czas pracy routera,
- ostatni sposób restartu routera,
- **nazwa pliku obrazu IOS i jego lokalizację,**
- **platforma routera i ilość pamięci RAM**
- **fizyczne interfejsy routera,**
- ilość pamięci NVRAM,
- **ilość pamięci flash,**
- **ustawienie rejestru konfiguracji**

```
Cisco#show version

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JK8S-M), Version
12.2(12c), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 05-Feb-03 16:36 by kellythw
Image text-base: 0x8000808C, data-base: 0x8156F2AC

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE
SOFTWARE (fc1)
R2 uptime is 4 weeks, 2 days, 17 hours, 9 minutes
System returned to ROM by reload
System image file is "flash:c2600-jk8s-mz.122-12c.bin"

cisco 2620 (MPC860) processor (revision 0x102) with
59392K/6144K bytes of memory
Processor board ID JAB04210736 (3772949214)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology
Corp).
TN3270 Emulation software.

Basic Rate ISDN software, Version 1.1.
1 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash
(Read/Write)

Configuration register is 0x2102
```

Rysunek 22.
Podgląd polecenia **show version**

show flash – wyświetla **zawartość pamięci flash** i sprawdza, czy system zawiera wystarczającą ilość **wolnej pamięci** do wczytania nowego obrazu IOS.

```
BHM#show flash
PCMCIA flash directory:
File  Length    Name/status
  1   6007232   c1700-bnsy-1.212-11.p
[6007296 bytes used, 284160 available, 6291456
total]
6144K bytes of processor board PCMCIA flash (Read
ONLY)
BHM#
```

- zawartość pamięci flash
- wolna pamięć do wczytania nowego obrazu IOS

Rysunek 23.
Podgląd polecenia **show flash**

show interfaces – wyświetla dane statystyczne dotyczące wszystkich interfejsów routera. Aby wyświetlić dane statystyczne dotyczące określonego interfejsu, należy wpisać polecenie **show interface** wraz z nazwą określającą typ interfejsu oraz numerem gniazda/portu. Pokazano to na poniższym przykładzie:

Router#show interface serial 0/1
Router#show interface ethernet 0

- Dane statystyczne interfejsu FastEthernet
- Dane statystyczne interfejsu szeregowego

```
R1#show interfaces
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0007.eca7.1511 (bia 00e0.f7e4.e47e)
  Description: R1 LAN
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  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
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Description: Link to R2
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
```

Rysunek 24.
Podgląd polecenia **show interfaces**

show ip interface brief – wyświetla skróconą informację o konfiguracji interfejsu, w tym adres IP i stan interfejsu. Polecenie to jest przydatnym narzędziem podczas rozwiązywania problemów i pozwala szybko ustalić stan wszystkich interfejsów routera.

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/0/0            192.168.2.1     YES manual up                    up
Serial0/0/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

Rysunek 25.
Podgląd polecenia **show ip interface brief**

show startup-config – wyświetla zawartość pamięci NVRAM, jeśli istnieje i jest poprawna, lub prezentuje plik konfiguracyjny wskazywany przez zmienną środowiskową CONFIG_FILE.

```
R1#show startup-config
Using 728 bytes          // ilość bajtów konfiguracji zapisanej w pamięci NVRAM
!
version 12.3
!
hostname R1
!
interface FastEthernet0/0
 description R1 LAN
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
 description Link to R2
 ip address 192.168.2.1 255.255.255.0
 clock rate 64000
!
banner motd ^C
****************************************
WARNING!! Unauthorized Access Prohibited!!
****************************************
^C
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

Rysunek 26.
Podgląd polecenia **show startup-config**

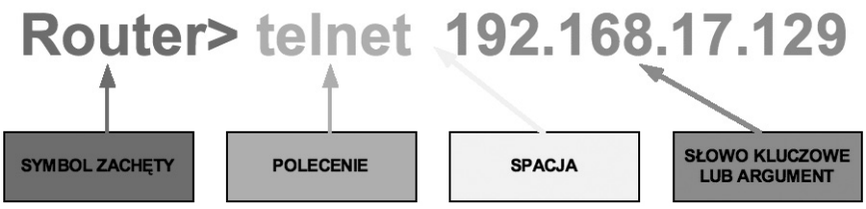
show running-config – wyświetla zawartość wykorzystywanego w danym momencie pliku konfiguracyjnego lub konfigurację dla konkretnego interfejsu.

```
R1#show running-config
!
version 12.3
!
hostname R1
!
interface FastEthernet0/0
 description R1 LAN
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
 description Link to R2
 ip address 192.168.2.1 255.255.255.0
 clock rate 64000
!
banner motd ^C
****************************************
WARNING!! Unauthorized Access Prohibited!!
****************************************
^C
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

Rysunek 27.
Podgląd polecenia **show running-config**

Podstawowa struktura poleceń IOS

Każda komenda w IOS ma specyficzny format i składnię oraz jest wykonywana we właściwym wierszu poleceń. Ogólna składnia polecenia rozpoczyna się komendą, a po niej następują właściwe słowa kluczowe oraz argumenty (patrz rys. 28). Niektóre komendy zawierają podzbiór słów kluczowych i argumenty, które dostarczają dodatkową funkcjonalność. Na rysunku są pokazane wspomniane części polecenia.



Rysunek 28.
Struktura składni poleceń dla routera

Komenda jest początkowym słowem (lub słowami) wpisanym w wierszu poleceń. Komendy nie rozróżniają wielkości liter. Po komendzie występuje jedno lub więcej słów kluczowych i argumentów.

Słowa kluczowe opisują specyficzne parametry dla interpretera. Dla przykładu, polecenie **show** służy do wyświetlania informacji o urządzeniu. Komenda ta, może zawierać wiele słów kluczowych, które mogą być użyte do zdefiniowania wyniku, jaki ma zostać wyświetlony. Na przykład:

Router# show running-config

Komenda **show** została uzupełniona słowem kluczowym **running-config**. Wydanie polecenia wskazuje, że na wyjściu powinna zostać wyświetlona konfiguracja bieżąca urządzenia.

Komenda może wymagać jednego lub więcej argumentów. W przeciwieństwie do słowa kluczowego, argument nie jest słowem predefiniowanym. Argument jest wartością lub zmienną definiowaną przez użytkownika. Dla przykładu, gdy chcemy dołączyć opis do interfejsu korzystając z komendy **description**, wpisujemy:

Router(config-if)# description Sala komputerowa 213

Komenda to: **description**. Argument to: **Sala komputerowa 213**. Użytkownik definiuje argumenty. Dla tej komendy argument może być dowolnym ciągiem tekstowym o długości nieprzekraczającej 80 znaków.

Po każdej pełnej komendzie, ewentualnie uzupełnionej słowami kluczowymi oraz argumentami, należy nacisnąć klawisz Enter, aby przesłać komendę do interpretera poleceń.

Korzystanie z pomocy wiersza poleceń

IOS zawiera kilka rodzajów dostępu do pomocy:

1. Pomoc kontekstowa w postaci podpowiedzi
2. Weryfikacja składni komendy
3. Skróty i „gorące klawisze”

Ad.1. Pomoc kontekstowa w postaci podpowiedzi

Pomoc kontekstowa dostarcza wiersz komend i związanych z nimi słów kluczowych, pasujących do bieżącego trybu. Aby uzyskać pomoc należy wpisać znak zapytania ? w dowolnym miejscu wiersza poleceń. Następuje wówczas natychmiastowa odpowiedź –znaku ? nie trzeba potwierdzać klawiszem Enter.

Korzystając z pomocy kontekstowej otrzymujemy listę dostępnych komend. Takie rozwiązanie może być używane jeśli np. nie mamy pewności co do nazwy polecenia lub jeśli chcemy sprawdzić, czy IOS wspiera konkretną komendę. Dla przykładu, w celu uzyskania listy komend dostępnych w trybie EXEC użytkownika wprowadź ? w wierszu poleceń po znaku zachęty Router›.

Kolejnym przykładem pomocy kontekstowej jest wykorzystanie komendy do wyświetlenia listy komend rozpoczynających się od określonego znaku lub znaków. Po wpisaniu znaku lub sekwencji znaków, jeśli naciśniemy ? bez spacji, to IOS wyświetli listę poleceń lub słów kluczowych dla kontekstu rozpoczynającego się od podanych znaków. Na przykład, wpisz sh?, aby wyświetlić listę komend, które rozpoczynają się od ciągu sh.

Kolejnym zastosowaniem pomocy kontekstowej jest próba określenia, które opcje, słowa kluczowe czy argumenty są powiązane z określoną komendą. Aby sprawdzić, co może lub powinno zostać wprowadzone, po wpisaniu komendy należy nacisnąć spację i wprowadzić znak ?. Na przykład, po wpisaniu komendy **clock set 19:50:00** możemy wpisać znak ? i w ten sposób dowiedzieć się, jakie opcje lub słowa kluczowe pasują do tej komendy.

Ad.2. Weryfikacja składni komend
Po zatwierdzeniu komendy klawiszem Enter, w celu określenia żądanej akcji interpreter parsuje polecenie od lewej strony do prawej. IOS dostarcza informacji na temat błędów w składni. Jeśli interpreter zrozumie komendę, żądana akcja zostaje wykonana, a wiersz poleceń zwraca właściwy znak zachęty. Jednakże, jeśli interpreter nie rozumie wprowadzonego polecenia, to dostarczy informację zwrotną z opisem, co zostało wprowadzone błędnie.

Są trzy różne rodzaje komunikatów o błędach:
- niejednoznaczne polecenie,
- niekompletne polecenie,
- niepoprawne polecenie.

Ad.3. Skróty i „gorące klawisze"
Wiersz poleceń CLI dostarcza tzw. **gorące klawisze** (ang. *hot keys*) oraz skróty, które ułatwiają konfigurację, monitoring i rozwiązywanie problemów. Następujące skróty zasługują na specjalną uwagę:

Tab – dopełnia komendę lub słowo kluczowe,
Ctrl-R – odświeża linię,
Ctrl-Z – wychodzi z trybu konfiguracji i wraca do trybu EXEC,
Strzałka w dół – pozwala użytkownikowi na przewijanie do przodu wydanych komend,
Strzałka w górę – pozwala użytkownikowi na przewijanie do tyłu wydanych komend,
Ctrl-Shift-6 – pozwala użytkownikowi na przerwanie procesu IOS takiego jak ping czy Traceroute,
Ctrl-C – przerywa aktualną komendę i wychodzi z trybu konfiguracji.

Funkcje edycyjne systemu IOS
Tabela 2.
Przykładowe kombinacje klawiszy edycyjnych systemu IOS

POLECENIE	OPIS POLECENIA
CTRL-A	Przeniesienie kursora na początek linii poleceń
ESC-B	Przeniesienie kursora o jedno słowo do tyłu
CTRL-B	Przeniesienie kursora o jeden znak do tyłu
CTRL-E	Przeniesienie kursora na koniec linii poleceń
CTRL-F	Przeniesienie kursora o jeden znak do przodu
ESC-F	Przeniesienie kursora o jedno słowo do przodu

W systemie IOS jest dostępny zestaw klawiszy edycji, które umożliwiają użytkownikowi edycję wiersza poleceń w trakcie jego wpisywania. Sekwencji klawiszy przedstawionych na rysunku można używać do przesuwania kursora w wierszu poleceń oraz do wprowadzania poprawek lub zmian. W aktualnych wersjach oprogramowania zaawansowany tryb edycji jest automatycznie włączany. Jeśli jednak przeszkadza on w wykonywaniu utworzonych skryptów można go wyłączyć – należy wpisać polecenie:

Router#terminal no editing

Aby ponownie włączyć zaawansowany tryb edycji (umożliwia korzystanie ze skrótów) należy wpisać polecenie:

Router#terminal editing

Historia poleceń w systemie IOS
Interfejs IOS zawiera historię wprowadzonych poleceń. Funkcja ta jest szczególnie przydatna w przypadku przywoływania długich lub złożonych poleceń. Funkcji historii poleceń można używać do: ustawiania wielkości buforu historii,

Tabela 3.
Przykładowe polecenia edycyjne systemu IOS

POLECENIE	OPIS POLECENIA
CTRL-P lub klawisz ze strzałką do góry	Przywołanie ostatniego (poprzedniego) polecenia
Router# show history	Wyświetla zawartość bieżącego bufora historii poleceń
Router# no terminal editing	Wyłączenie zaawansowanego trybu edycji poleceń
Router# terminal editing	Włączenie zaawansowanego trybu edycji poleceń
<TAB>	Kompletowanie wprowadzanych poleceń

przywoływania poleceń, wyłączania funkcji historii poleceń. Historia poleceń jest włączana domyślnie, a system zapisuje dziesięć wierszy poleceń w buforze historii. Aby zmienić liczbę wierszy poleceń, które system zapisuje podczas sesji terminala, należy użyć polecenia **terminal history size** lub **history size**. Maksymalna liczba poleceń wynosi 256.

Konfiguracja interfejsu ethernetowego

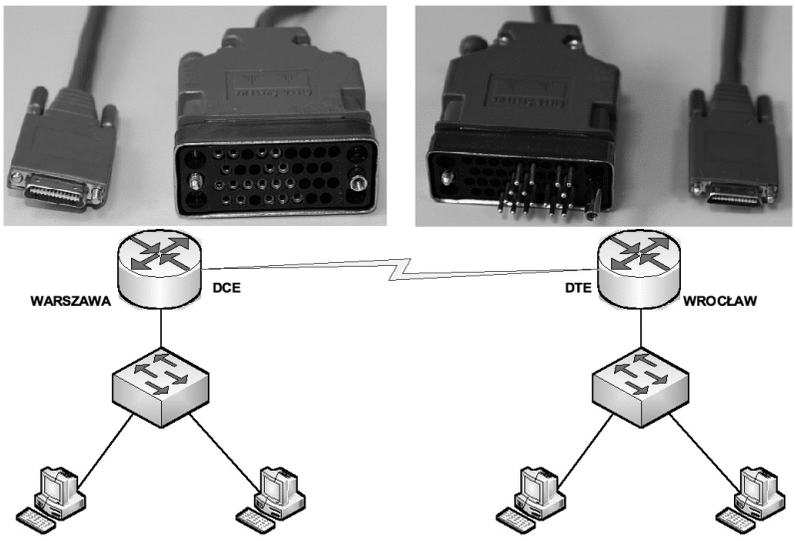
Każdy interfejs Ethernet musi mieć zdefiniowany adres IP i maskę podsieci, aby mógł przesyłać pakiety IP. Aby skonfigurować interfejs Ethernet, należy wykonać następujące czynności (patrz rys. 29):

1. Przejść do trybu konfiguracji globalnej.
2. Przejść do trybu konfigurowania interfejsu.
3. Podać adres interfejsu i maskę podsieci.
4. Włączyć interfejs.
5. Domyślnie interfejsy są wyłączone lub nieaktywne. Aby włączyć lub uaktywnić interfejs, należy użyć polecenia **no shutdown**.

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

Rysunek 29.
Przykład konfiguracji interfejsu ethernetowego

Połączenia w sieciach WAN

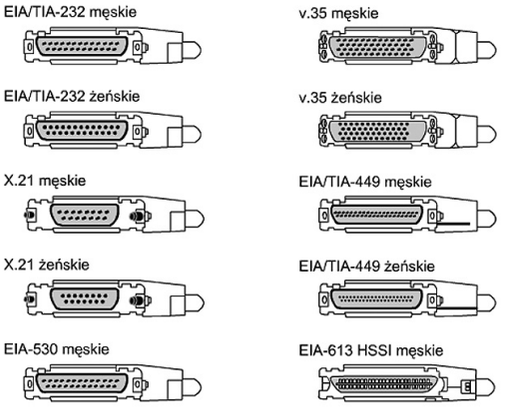


Rysunek 30.
Przykład połączeń pomiędzy sieciami rozległymi

W laboratorium wszystkie sieci będą połączone kablami szeregowymi lub Ethernet. W przeciwieństwie do instalacji w laboratorium, w rzeczywistości kable szeregowe nie łączą urządzeń bezpośrednio ze sobą. W rzeczywistości jeden router może znajdować się w Warszawie, podczas gdy inny może znajdować się we Wrocławiu.

Sieci WAN korzystają z wielu różnych technologii do realizowania połączeń danych na dużych obszarach geograficznych. Usługi komunikacji WAN są zazwyczaj dzierżawione od dostawców usług. Typy połączeń WAN obejmują linie dzierżawione, połączenia z komutacją łączy oraz połączenia z komutacją pakietów.

Szeregowe złącza WAN



Rysunek 31.
Przykłady szeregowych złączy WAN

Na rysunku 31 przedstawiono wybrane szeregowe złącza WAN:

EIA/TIA-232 – umożliwia połączenia z szybkością do 64 kbps. Używa 25-pinowe złącze typu D.
EIA/TIA-449/530 – umożliwia połączenia do 2 Mbps. Używa 36-pinowe złącze typu D.
EIA/TIA-612/613 – zapewnia dostęp do usług z szybkością do 52 Mbps przez interfejs **HSSI** (ang. *High Speed Serial Interface*). Używa 60-pinowe złącze typu D.
V.35 – standard ITU-T dla synchronicznej komunikacji z szybkością od 48 kbps do 2 Mbps. Używa 34-pinowe złącze prostokątne.
X.21 – standard ITU-T dla synchronicznej komunikacji cyfrowej. Używa 15-pinowe złącze typu D.

Konfiguracja interfejsu szeregowego

Aby skonfigurować interfejs szeregowy, należy wykonać następujące czynności (patrz rys. 32):

1. Przejść do trybu konfiguracji globalnej.
2. Przejść do trybu konfigurowania interfejsu.
3. Podać adres interfejsu i maskę podsieci.
4. Ustawić częstotliwość zegara taktującego synchronizację połączenia (np. 56000).
5. Włączyć interfejs.

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# interface serial 0/0
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# clock rate 56000
Router(config-if)# no shutdown
```

Rysunek 32.
Przykład konfiguracji interfejsu szeregowego

Jeśli podłączony jest kabel DCE, ustaw częstotliwość zegara. Pomiń tę czynność, jeśli podłączony jest kabel DTE. Interfejsy szeregowe wymagają sygnału zegarowego sterującego komunikacją. W większości środowisk sygnału zegarowego dostarcza urządzenie DCE, takie jak **CSU/DSU** (ang. *Channel Service Unit/Data Service Unit*). Domyślnie routery Cisco są urządzeniami DTE, ale można je skonfigurować jako urządzenia DCE.

W przypadku bezpośrednio połączonych ze sobą łączy szeregowych, na przykład w laboratorium, jedna ze stron musi być traktowana jako urządzenie DCE i dostarczać sygnału zegarowego. Polecenie **clock rate** powoduje włączenie zegara i określenie jego szybkości. Dostępne szybkości w bitach na sekundę to: 1200, 2400, 9600, 19 200, 38 400, 56 000, 64 000, 72 000, 125 000, 148 000, 500 000, 800 000, 1 000 000, 1 300 000, 2 000 000 i 4 000 000. W przypadku niektórych interfejsów szeregowych pewne szybkości mogą nie być dostępne.

Domyślnie interfejsy są wyłączone lub nieaktywne. Aby włączyć lub uaktywnić interfejs, należy użyć polecenia **no shutdown**.

Opis interfejsów routera

Opis interfejsu powinien zawierać istotne informacje, na przykład dotyczące sąsiedniego routera, numeru obwodu lub konkretnego segmentu sieci. Opis interfejsu może pomóc użytkownikowi sieci zapamiętać określone informacje na jego temat, na przykład do jakiej sieci jest on podłączony (patrz rys. 33).

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# interface fastethernet 0/0
Router(config-if)# description Podłączenie do pracowni komputerowej111
```

Rysunek 33.
Przykładowy opis interfejsu routera

Chociaż opis jest umieszczony w plikach konfiguracyjnych przechowywanych w pamięci routera, nie wpływa on na funkcjonowanie routera. Opis zawiera jedynie informacje dotyczące interfejsu. Tworzy się go w oparciu o standardowy format, który ma zastosowanie do każdego interfejsu.

Komunikat logowania

```
LAB_A con0 is now available

Press RETURN to get started.

This is a secure system. Authorized Access
ONLY!!!

User Access Verification

password:

LAB_A>enable

Password:

LAB_A#
```

Rysunek 34.
Przykładowy komunikat logowania

Komunikaty logowania są wyświetlane na ekranie w trakcie logowania. Mogą one służyć do przekazywania informacji istotnych dla wszystkich użytkowników sieci, na przykład o zaplanowanych wyłączeniach systemu. Są one widoczne dla każdego użytkownika. Dlatego należy zwracać szczególną uwagę na ich treść.

Komunikat logowania powinien ostrzegać użytkowników, aby nie próbowali zalogować się, jeśli nie mają do tego uprawnień. Na przykład komunikat „To jest system chroniony, dostęp jedynie dla uprawnionych użytkowników!" informuje niepożądanych gości o nielegalności ewentualnego wtargnięcia.

System IOS obsługuje wiele komunikatów logowania, a najpopularniejszy z nich to tzw. komunikat dnia. Aby utworzyć i wyświetlić komunikat dnia **MOTD** (ang. *message-of-the-day*) – wyświetlany na wszystkich podłączonych terminalach – należy wykonać poniższe czynności:

1. Za pomocą polecenia **configure terminal** przejść do trybu konfiguracji globalnej.
2. Wpisać polecenie **banner motd # *‹komunikat dnia›***.
3. Za pomocą polecenia **copy running-config startup-config** zapisać zmiany.

Odwzorowanie nazw hostów

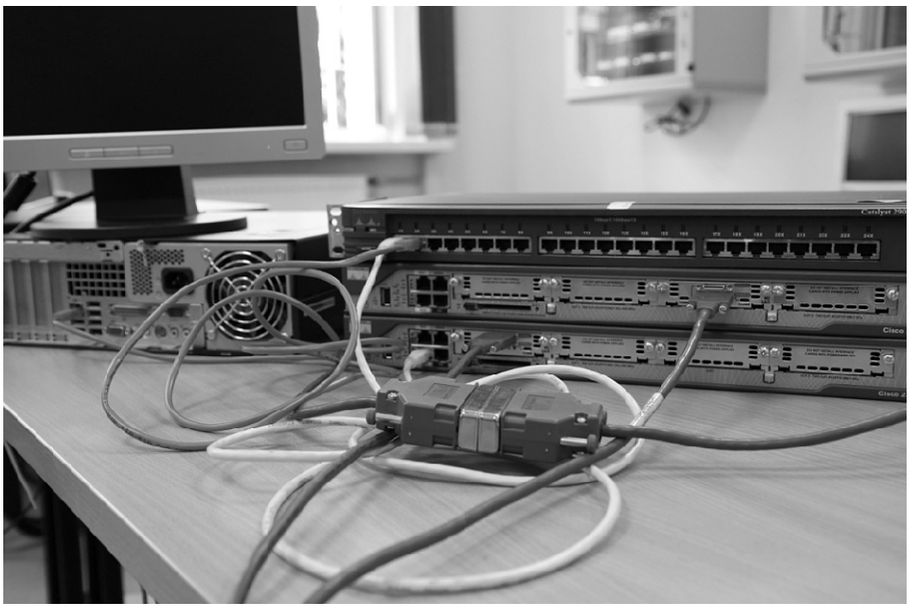
Odwzorowywanie nazw hostów jest procesem, za pomocą którego system komputerowy kojarzy nazwę hosta z adresem IP (patrz rys. 35). Aby móc używać nazw hostów do komunikowania się z innymi urządzeniami IP, urządzenia sieciowe, takie jak routery, muszą być w stanie powiązać te nazwy z odpowiednimi adresami IP. Lista nazw hostów i powiązanych z nimi adresów IP nosi nazwę **tablicy hostów**.

```
Router>
Router> enable
Password:
Router#
Router# configure terminal
Router(config)# ip host Warszawa 192.168.10.15
Router(config)# ip host Wroclaw 192.168.30.49
Router(config)# ip host Torun 192.168.70.36
Router(config)# ip host Krakow 192.168.90.53
```

Rysunek 35.
Przykłady odwzorowania nazw hostów

4 SPRAWDZANIE KOMUNIKACJI W SIECI

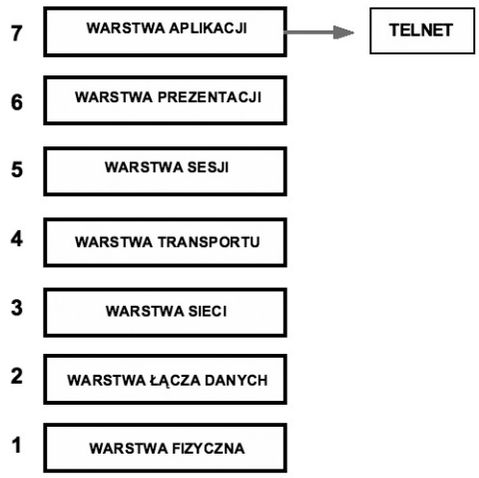
Przykładowy zestaw laboratoryjny



Rysunek 36.
Przykładowy zestaw laboratoryjny do weryfikacji połączeń sieciowych

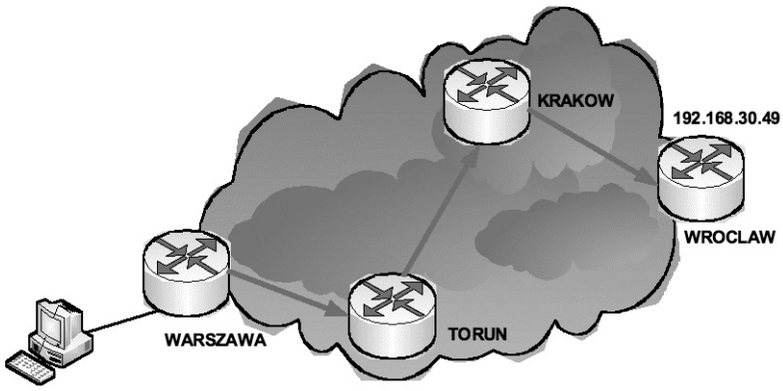
Aby sprawdzić poprawność komunikacji w sieciach komputerowych należy dokonać właściwych połączeń fizycznych urządzeń sieciowych. Na rysunku 36 przedstawiono przykładowy zestaw laboratoryjny, który posłuży powyższym celom.

a) Protokół Telnet



Rysunek 37.
Odwzorowanie protokołu **Telnet** na tle modelu odniesienia ISO/OSI

Protokół wirtualnego terminala Telnet umożliwia nawiązywanie połączeń ze zdalnymi hostami. Zapewnia funkcje terminala sieciowego czyli możliwość zdalnego logowania. Polecenie Telnet systemu IOS umożliwia sprawdzenie oprogramowania warstwy aplikacji między źródłem a celem (patrz rys. 38). Każdy router może obsłużyć kilka sesji Telnet równocześnie. Dostępnych jest pięć linii dla terminali VTY lub Telnet o numerach od zero do cztery. Protokół Telnet jest używany głównie do ustanawiania zdalnych połączeń z urządzeniami sieciowymi.



Rysunek 38.
Przykładowy scenariusz na weryfikację połączenia **Telnet**

Pięć poniższych poleceń umożliwia osiągnięcie takiego samego efektu – próby nawiązania zdalnego połączenia z routerem o nazwie Wroclaw z adresem IP 192.168.30.49:

```
Warszawa› telnet Wroclaw                  //wcześniej należy odwzorować adres IP do hosta Paris
Warszawa› telnet 192.168.30.49
Warszawa› Wroclaw                         //gdy polecenie IP host wykorzystuje domyślny port
Warszawa› connect Wroclaw
Warszawa› 192.168.30.49
```

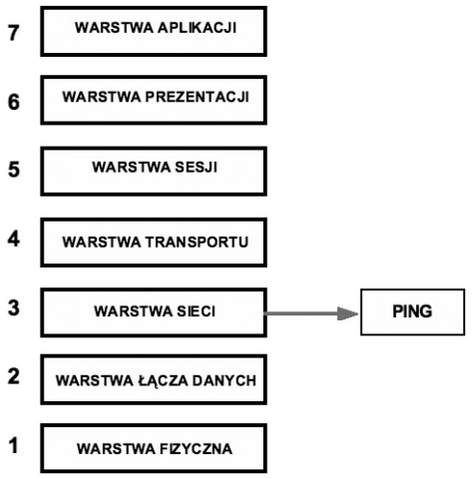
Źródłem potencjalnego problemu może być naciśnięcie klawisza **Enter**, gdy sesja Telnet jest zawieszona. W takiej sytuacji oprogramowanie IOS wznawia połączenie z ostatnio zawieszoną sesją. Gdy sesja Telnet jest zawieszona, możliwe jest ustanowienie połączenia z innym routerem. Jest to niebezpieczne, gdy wykonywane są zmiany konfiguracji lub używane są polecenia EXEC. Korzystając z funkcji zawieszania sesji Telnet, nale-

ży zawsze sprawdzać, z którym routerem jest nawiązane połączenie. Aktywne sesje Telnet można wyświetlić przy użyciu polecenia **show sessions**.

Gdy otwartych jest kilka sesji Telnet jednocześnie użytkownik może przełączać się między nimi. Dozwolona liczba otwartych jednocześnie sesji jest definiowana za pomocą polecenia **session limit**.

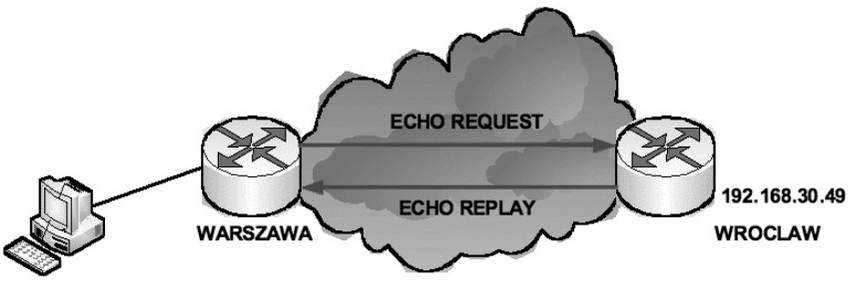
Między sesjami można przechodzić, naciskając kombinację klawiszy **Ctrl-Shift-6**, a następnie **x**. Sesję można wznowić klawiszem **Enter** (Cisco IOS wznawia to połączenie Telnet, które zostało zawieszone jako ostatnie). W przypadku użycia polecenia **resume** należy podać identyfikator połączenia. Do wyświetlania identyfikatora połączenia służy polecenie **show sessions.**

b) Protokół ping



Rysunek 39.
Odwzorowanie protokołu **ping** na tle modelu odniesienia ISO/OSI

Polecenie ping

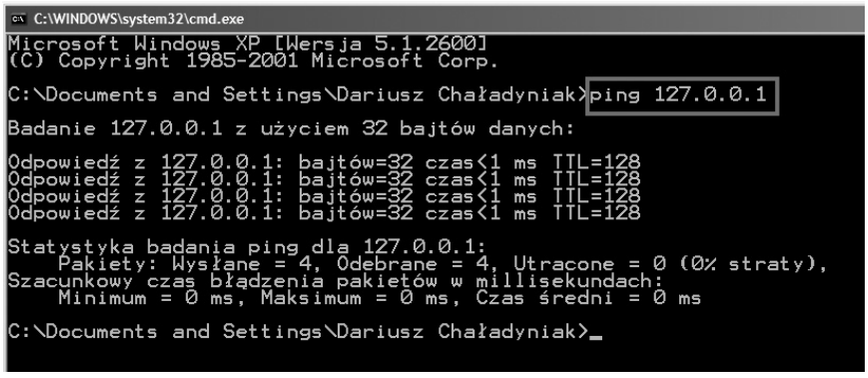


Rysunek 40.
Przykładowy scenariusz na weryfikację połączenia **ping**

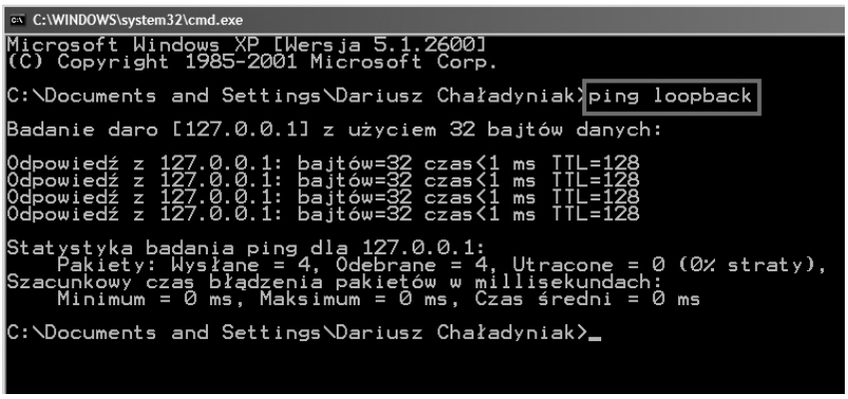
Polecenie **ping** wysyła pakiet do hosta docelowego, a następnie oczekuje na pakiet odpowiedzi tego hosta. Wyniki otrzymane w wyniku stosowania tego protokołu mogą pomóc w ocenie niezawodności ścieżki do hosta, występujących na niej opóźnień oraz tego, czy host jest dostępny i działa. Jest to podstawowy mechanizm testowania. W poleceniu ping wykorzystywany jest protokół **ICMP** (ang. *Internet Control Message Protocol*).

Na rysunku 41 przedstawiono sytuację, gdy docelowy host (adres pętli zwrotnej) 127.0.0.1 odpowiedział na wszystkie cztery wysłane do niego pakiety. Adres pętli zwrotnej można również przetestować poleceniem – **ping loopback** (patrz rys. 42).

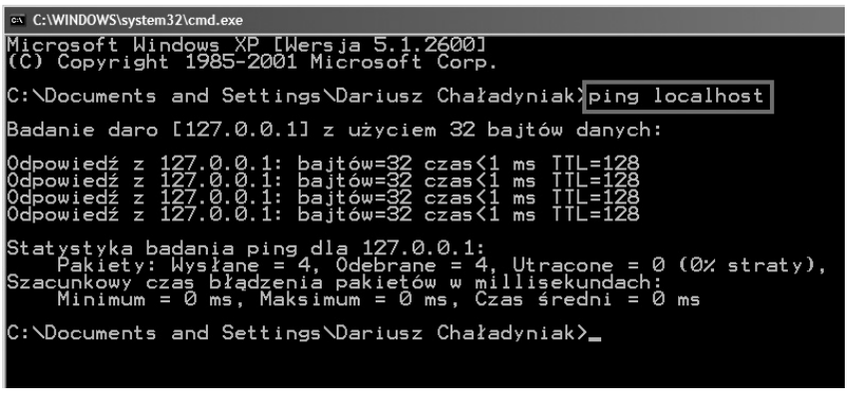
Można użyć również zlecenia **ping localhost** (patrz rys. 43), ale pod warunkiem, że w katalogu C:/Windows/System32/drivers/etc/ znajduje się plik hosts, w którym jest wpis – 127.0.0.1 localhost.



Rysunek 41.
Przykład testowania **pętli zwrotnej** za pomocą polecenia **ping 127.0.0.1**



Rysunek 42.
Przykład testowania **pętli zwrotnej** za pomocą polecenia **ping loopback**

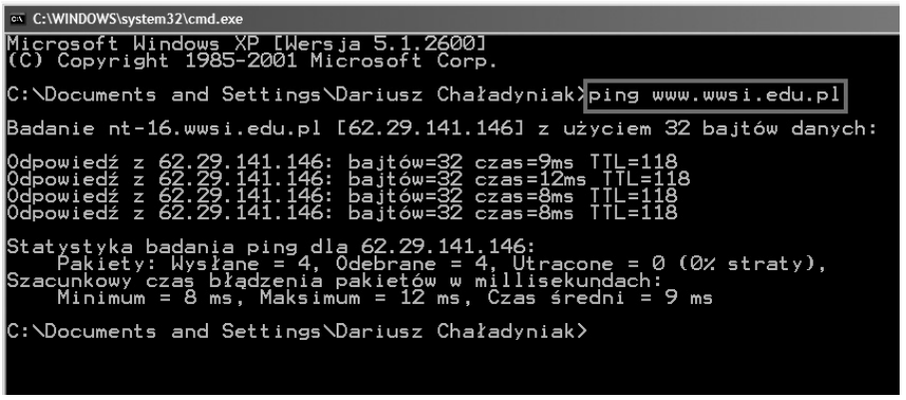


Rysunek 43.
Przykład testowania **pętli zwrotnej** za pomocą polecenia **ping localhost**

Przykład zlecenia ping testującego osiągalność zdalnego hosta w Internecie www.wwsi.edu.pl jest pokazany na rys. 44.

Polecenie ping można użyć z wieloma opcjami w zależności od konkretnych potrzeb np.:

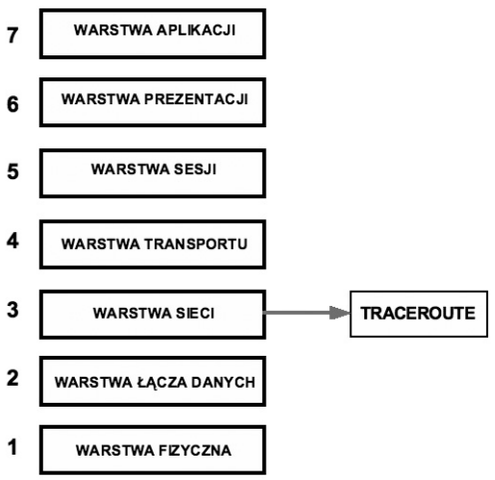
ping –n 10 – liczba wysyłanych powtórzeń żądania - w tym przypadku 10 powtórzeń;
ping –l 1024 – rozmiar buforu transmisji – w tym przypadku 1024 bajtów;
ping –i 128 – czas wygaśnięcia – w tym przypadku 128 (sekund lub liczba przeskoków);
ping –w 500 – limit czasu oczekiwania na odpowiedź – w tym przypadku 500 milisekund.



Rysunek 44.
Przykład testowania osiągalności zdalnego hosta w Internecie

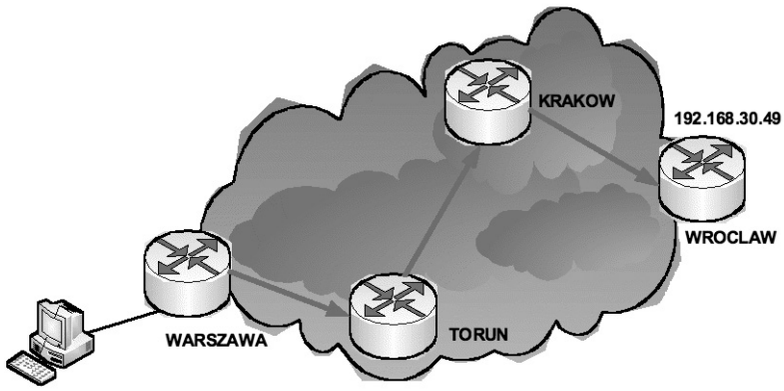
Rysunek 45.
Rezultat wydania polecenia **ping /?**

c) Protokół traceroute



Rysunek 46.
Odwzorowanie protokołu **traceroute** na tle modelu odniesienia ISO/OSI

Polecenie **traceroute** (w systemie MS Windows – **tracert**), umożliwia znalezienie drogi przesyłania danych w sieci. Polecenie traceroute jest podobne do polecenia ping. Główna różnica polega na tym, że polecenie ping testuje tylko osiągalność hosta, a polecenie traceroute - każdy etap drogi pakietu.



Rysunek 47.
Przykładowy scenariusz na weryfikację połączenia **traceroute**

Na rysunku 48 przedstawiono sytuację, w której śledzona jest ścieżka od lokalnej bramy do hosta – www.wwsi.edu.pl.

Polecenie **tracert** można wydać w z następującymi opcjami:

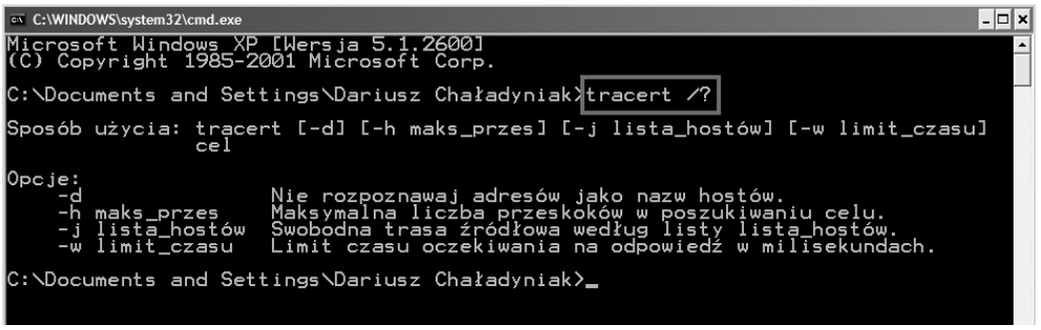
tracert –d – nie rozpoznawaj adresów jako nazw hostów;
tracert –h 15 – maksymalna liczba przeskoków w poszukiwaniu celu – w tym przypadku 15
tracert –j lista_hostów – swobodna trasa źródłowa według listy lista_hostów;
tracert –w 300 – limit czasu oczekiwania na odpowiedź w milisekundach – w tym przypadku 300 milisekund.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Wersja 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Dariusz Chaładyniak>tracert www.wwsi.edu.pl

Trasa śledzenia do nt-16.wwsi.edu.pl [62.29.141.146]
przewyższa maksymalną liczbę przeskoków 30

  1     8 ms     1 ms     1 ms  10.1.82.254
  2     3 ms    10 ms    <1 ms  cajun-wic.wat.edu.pl [10.1.1.18]
  3     1 ms     1 ms    <1 ms  elf.wat.edu.pl [10.0.0.2]
  4     4 ms     3 ms    <1 ms  wat-warman.wat.edu.pl [148.81.117.254]
  5     4 ms     1 ms     1 ms  pw-r2-at0-1-1-151.warman.nask.pl [148.81.175.153
]
  6     4 ms     2 ms     2 ms  pw-r1-ae1-300.warman.nask.pl [148.81.166.46]
  7     4 ms     1 ms     2 ms  pw-gw-z-as1887.warman.nask.pl [195.187.255.52]
  8     3 ms     2 ms     2 ms  pkp-gw-ae1-100.core.nask.pl [195.187.255.153]
  9     4 ms     2 ms     2 ms  lim-gw-ae0-100.core.nask.pl [195.187.255.157]
 10     *        7 ms     3 ms  energis-lim.wix.net.pl [195.85.195.9]
 11     9 ms     3 ms     3 ms  212.38.193.85
 12     5 ms     3 ms     2 ms  e-waw-dbp-r01p11.plwaw.energis.pl [62.29.240.166
]
 13     7 ms     3 ms     3 ms  212.38.205.173
 14     6 ms     6 ms     6 ms  212.38.198.173
 15    17 ms     7 ms    21 ms  212.38.196.230
 16    10 ms    10 ms     7 ms  62.29.141.146

Śledzenie zakończone.
```

Rysunek 48.
Przykład śledzenia ścieżki do docelowego hosta

Zapisywanie plików konfiguracyjnych

Na wypadek problemów, należy utworzyć i zapisać kopie zapasowe plików konfiguracyjnych. Pliki konfiguracyjne mogą być przechowywane na serwerze **TFTP** (ang. *Trivial File Transfer Protocol*), nośnikach CD czy pamięciach przenośnych Pendrive USB w bezpiecznym miejscu. Plik konfiguracyjny powinien być również załączony do dokumentacji sieci.



Rysunek 49.
Rezultat wydania polecenia **tracert /?**

```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm] y
Writing tokyo.2 !!!!!! [OK]
```

Rysunek 50.
Sposób zapisywania zawartości plików konfiguracyjnych

Kopiowanie konfiguracji na serwer TFTP

Aby zachować konfigurację bieżącą lub początkową na serwerze TFTP, należy wybrać jedno z poleceń – **copy running-config tftp** lub **copy startup-config tftp**. Aby to zrobić należy wykonać następujące kroki:

1. Wpisać polecenie **copy running-config tftp**.
2. Wpisać adres IP hosta, na którym będzie przechowywany plik konfiguracji.
3. Wpisać nazwę pliku konfiguracyjnego.
4. Odpowiedzieć yes, aby potwierdzić wprowadzone dane.

5 PODSTAWY ROUTINGU STATYCZNEGO

Wprowadzenie do routingu

Główne przeznaczenie routera jest przekazywanie pakietów z jednej sieci do drugiej. Aby router mógł wykonać to zadanie poprawnie musi wiedzieć, co zrobić z dostarczonym mu pakietem; gdzie go dalej przesłać, aby osiągnął on swoje przeznaczenie. Router wykorzystuje w tym celu tablicę routingu, czyli wskazówki, na który interfejs, pod jaki adres IP, przesłać pakiet. **Tablica routingu** może być zbudowana na kilka sposobów:

- na pewno znajdują się tam adresy sieci bezpośrednio połączonych do interfejsów routera (np. fastethernet 0/0 i serial 0/0);
- inne sieci dostępne poprzez poszczególne interfejsy można wpisać ręcznie – routing statyczny;
- lub posłużyć się protokołami routingu dynamicznego (np. RIP, IGRP, OSPF).

Routing statyczny

Najprostszą formą budowania informacji o topologii sieci są ręcznie podane przez administratora trasy. Przy tworzeniu takiej trasy jest wymagane jedynie podanie adresu sieci docelowej, maski podsieci oraz interfejsu, przez który pakiet ma zostać wysłany lub adresu IP następnego routera na trasie. Routing statyczny ma wiele zalet:

1. Router przesyła pakiety przez z góry ustalone interfejsy bez konieczności każdorazowego obliczania tras, co zmniejsza zajętość cykli procesora i pamięci.
2. Informacja statyczna nie jest narażona na deformację spowodowaną zanikiem działania dynamicznego routingu na routerach sąsiednich.
3. Zmniejsza się zajętość pasma transmisji, gdyż nie są rozsyłane pakiety rozgłoszeniowe protokołów routingu dynamicznego.

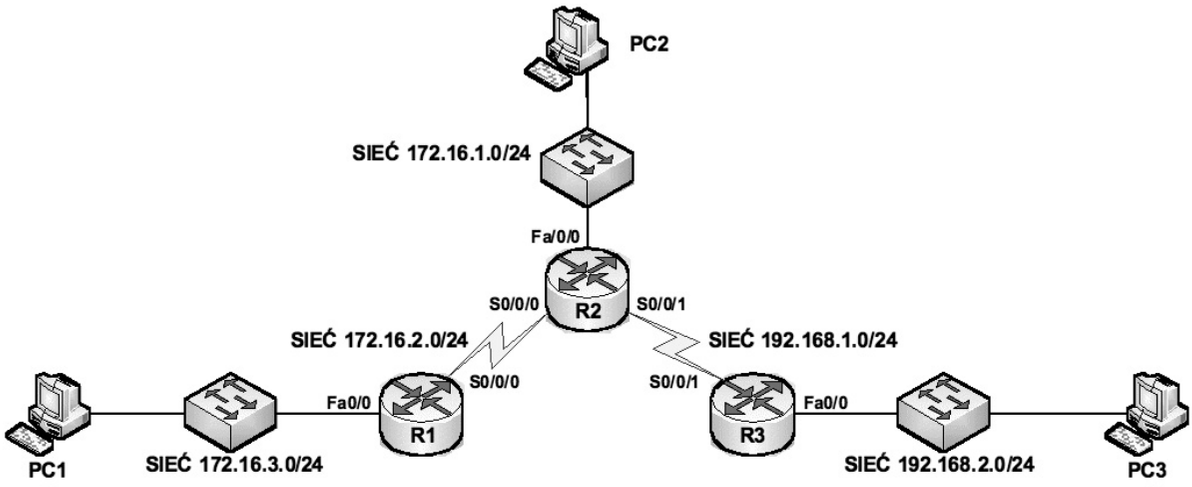
Dla małych sieci jest to doskonałe rozwiązanie, ponieważ nie musimy dysponować zaawansowanymi technologicznie i rozbudowanymi sprzętowo routerami.

Routing statyczny zapewnia również konfigurację tras domyślnych, nazywanych **bramami ostatniej szansy** (ang. *gateway of the last resort*). Jeżeli router uzna, iż żadna pozycja w tablicy routingu nie odpowiada poszukiwanemu adresowi sieci docelowej, korzysta ze statycznego wpisu, który spowoduje odesłanie pakietu w inne miejsce sieci. Routing statyczny wymaga jednak od administratora sporego nakładu pracy w początkowej fazie konfiguracji sieci, nie jest również w stanie reagować na awarie poszczególnych tras.

Konfigurowanie tras statycznych

Aby skonfigurować trasy statyczne, należy wykonać następujące czynności:

1. Określ sieci docelowe, ich maski podsieci oraz bramy. Brama może być zarówno interfejsem lokalnym, jak i adresem następnego przeskoku prowadzącym do sąsiedniego routera.
2. Przejdź do trybu konfiguracji globalnej.
3. Wpisz polecenie **ip route** z adresem i maską sieci oraz adresem określonym w kroku 1.
4. Powtórz krok 3 dla wszystkich sieci docelowych zdefiniowanych w kroku 1.
5. Opuść tryb konfiguracji globalnej.
6. Za pomocą polecenia **copy running-config startup-config** zapisz aktywną konfigurację w pamięci NVRAM.



URZĄDZENIE SIECIOWE	INTERFEJS	ADRES IP	MASKA PODSIECI	BRAMA DOMYŚLNA
ROUTER R1	Fa0/0 S0/0/0	172.16.3.1 172.16.2.1	255.255.255.0 255.255.255.0	
ROUTER R2	Fa0/0 S0/0/0 S0/0/1	172.16.1.1 172.16.2.2 192.168.1.2	255.255.255.0 255.255.255.0 255.255.255.0	
ROUTER R3	Fa0/0 S0/0/1	192.168.2.1 192.168.1.1	255.255.255.0 255.255.255.0	
HOST PC1	Karta sieciowa	172.16.3.10	255.255.255.0	172.16.3.1
HOST PC2	Karta sieciowa	172.16.1.10	255.255.255.0	172.16.1.1
HOST PC3	Karta sieciowa	192.168.2.10	255.255.255.0	192.168.2.1

Rysunek 51.
Przykładowy scenariusz połączeń sieciowych

Konfigurację routingu statycznego przeprowadzimy dla przykładowej sytuacji sieciowej pokazanej na rysunku 51. W przedstawionym przykładzie są 3 routery, które łączą ze sobą 5 sieci. Kolejne rysunki obrazują poszczególne etapy konfiguracji routingu statycznego.

Sieci podłączone bezpośrednio

Zanim router będzie mógł przekazywać pakiety do innych (zdalnych) sieci, jego sieci połączone bezpośrednio muszą być aktywne. Sieci podłączone bezpośrednio do routera R1 sprawdzamy poleceniem – **R1# show ip route**, patrz rys. 52.

```
R1#show ip route
(**output omitted**)

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0


R2#show ip route
172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1


R3#show ip route
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Rysunek 52.
Podgląd konfiguracji sieci połączonych bezpośrednio do routerów R1, R2 i R3

Konfiguracja na routerze R1 (z wykorzystaniem adresu IP następnego skoku)

Na rysunku 53 przedstawiono konfigurację routingu statycznego dla routera R1 z wykorzystaniem adresu IP następnego skoku.

```
R1(config)#ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1(config)#end
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.2
S    192.168.2.0/24 [1/0] via 172.16.2.2
```

Rysunek 53.
Konfiguracja routingu statycznego przeprowadzona dla routera R1

Konfiguracja na routerze R2 i R3 (z wykorzystaniem adresu IP następnego skoku)

```
R2>
R2> enable
Password:
R2#
R2# configure terminal
R2(config)# ip route 172.16.3.0 255.255.255.0 serial 0/0/0
R2(config)# ip route 192.168.2.0 255.255.255.0 serial 0/0/1


R3>
R3> enable
Password:
R3#
R3# configure terminal
R3(config)# ip route 172.16.1.0 255.255.255.0 serial 0/0/1
R3(config)# ip route 172.16.2.0 255.255.255.0 serial 0/0/1
R3(config)# ip route 172.16.3.0 255.255.255.0 serial 0/0/1
```

Rysunek 54.
Konfiguracja routingu statycznego przeprowadzona dla routerów R1 i R2

Sprawdzanie zmian w tablicy routingu

Skonfigurowane statycznie sieci podłączone do routerów R1, R2 i R3 można sprawdzić poleceniami jak na rysunku 55.

```
R1#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 is directly connected, Serial0/0/0
S    192.168.2.0/24 is directly connected, Serial0/0/0

R2#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 is directly connected, Serial0/0/1

R3#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/1
S       172.16.2.0 is directly connected, Serial0/0/1
S       172.16.3.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Rysunek 55.
Podgląd tablic routingu dla routerów R1, R2 i R3.

Weryfikacja połączeń

Weryfikację połączeń przeprowadzamy za pomocą polecenia **ping**. Z rysunku 56 wynika, że wszystkie połączenia są poprawne.

```
R1#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
R1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
R1#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
R1#
```

Rysunek 56.
Weryfikacja połączeń sieciowych za pomocą polecenia **ping**

Konfiguracja na routerze R1 (z wykorzystaniem interfejsu wyjściowego)

```
R1(config)#ip route 172.16.1.0 255.255.255.0 serial 0/0/0
R1(config)#ip route 192.168.1.0 255.255.255.0 serial 0/0/0
R1(config)#end
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.2
S    192.168.2.0/24 is directly connected, Serial0/0/0
```

Rysunek 57.
Konfiguracja routingu statycznego dla routera R1 z wykorzystaniem interfejsu wyjściowego

Konfiguracja na routerze R2 i R3 (z wykorzystaniem interfejsu wyjściowego)

```
R2> enable
Password:
R2#
R2# configure terminal
R2(config)# ip route 172.16.3.0 255.255.255.0 serial 0/0/0
R2(config)# ip route 192.168.2.0 255.255.255.0 serial 0/0/1


R3>
R3> enable
Password:
R3#
R3# configure terminal
R3(config)# ip route 172.16.1.0 255.255.255.0 serial 0/0/1
R3(config)# ip route 172.16.2.0 255.255.255.0 serial 0/0/1
R3(config)# ip route 172.16.3.0 255.255.255.0 serial 0/0/1
```

Rysunek 58.
Konfiguracja routingu statycznego dla routerów R2 i R3 z wykorzystaniem interfejsu wyjściowego

Sprawdzanie zmian w tablicy routingu

Skonfigurowane statycznie sieci podłączone do routerów R1, R2 i R3 można sprawdzić poleceniami jak na rysunku 59.

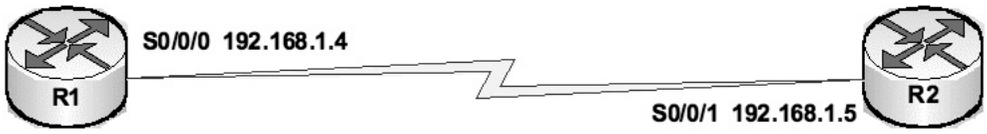
Trasy statyczne a odległość administracyjna

Trasa statyczna używająca albo adresu IP następnego skoku, albo interfejsu wyjściowego domyślnie ma odległość administracyjną 1. Jednak, kiedy konfigurujemy trasę statyczną, określając interfejs wyjściowy, w wyniku polecenia **show ip route** nie ma wartości odległości administracyjnej. Kiedy trasa statyczna zostanie skonfigurowana z interfejsem wyjściowym, w wynikach widzimy sieć jako bezpośrednio połączoną z tym interfejsem. Domyślną wartością administracyjną każdej trasy statycznej, również tej skonfigurowanej z interfejsem wyjściowym jest 1. Pamiętajmy, że tylko sieć połączona bezpośrednio może mieć odległość administracyjną równą 0.

```
R1#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 is directly connected, Serial0/0/0
S    192.168.2.0/24 is directly connected, Serial0/0/0

R2#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 is directly connected, Serial0/0/1

R3#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/1
S       172.16.2.0 is directly connected, Serial0/0/1
S       172.16.3.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Rysunek 59.
Podgląd tablic routingu dla routerów R1, R2 i R3.

Konfigurowanie trasy domyślnej



R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.5
LUB
R1(config)# ip route 0.0.0.0 0.0.0.0 S0/0/0

Rysunek 60.
Konfigurowanie trasy domyślnej

Trasy domyślne służą do routingu pakietów, których adresy docelowe nie odpowiadają żadnym innym trasom w tablicy routingu. Routery mają zazwyczaj skonfigurowaną trasę statyczną dla ruchu związanego z Internetem, ponieważ utrzymywanie tras do wszystkich sieci w Internecie jest zwykle niepotrzebne. Trasa domyślna to w rzeczywistości specjalna trasa statyczna zgodna z następującym formatem (patrz rys. 60):

ip route ***0.0.0.0 0.0.0.0*** **[*adres-następnego-skoku* | *interfejs-wychodzący*]**

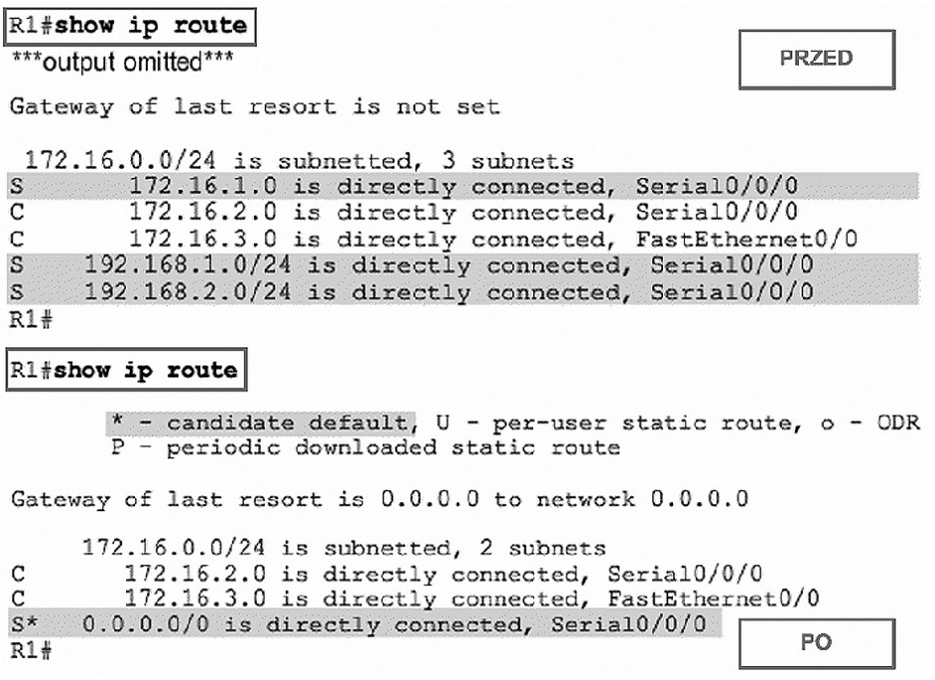
Maska 0.0.0.0 poddana logicznej operacji AND z docelowym adresem IP pakietu przeznaczonego do przesłania zawsze da w wyniku sieć 0.0.0.0. Jeśli pakiet nie pasuje do trasy precyzyjniej określonej w tablicy routingu, zostanie przesłany do sieci 0.0.0.0. Aby skonfigurować trasy domyślne, należy wykonać następujące czynności:

1. Przejść do trybu konfiguracji globalnej.
2. Wpisać polecenie **ip route**, podając 0.0.0.0 jako adres sieci i 0.0.0.0 jako maskę. Parametr *adres* oznaczający trasę domyślną może być interfejsem routera lokalnego połączonego z sieciami zewnętrznymi lub adresem IP routera następnego przeskoku. W większości przypadków należy określić adres IP routera następnego przeskoku.

3. Opuścić tryb konfiguracji globalnej.
4. Za pomocą polecenia **copy running-config startup-config** zapisać aktywną konfigurację w pamięci NVRAM.

Sprawdzenie zmian w tablicy routingu

Wydając polecenie **show ip route**, sprawdzamy zmiany wprowadzone do tablicy routingu. Należy zwrócić uwagę, że gwiazdka (*) obok kodu S oznacza trasę domyślną. Właśnie dlatego nazywana jest „domyślną trasą statyczną" (patrz rys. 61).



Rysunek 61.
Sprawdzenie zmian w tablicy routingu po konfiguracji tras domyślnych

6 WPROWADZENIE DO PROTOKOŁÓW ROUTINGU DYNAMICZNEGO

Protokoły routingu

Protokoły routingu różnią się od protokołów routowanych (routowalnych) zarówno pod względem funkcjonowania, jak i przeznaczenia. Protokół routingu to metoda komunikacji pomiędzy routerami, umożliwia routerom współużytkowanie informacji na temat sieci i dzielących je odległości. Routery wykorzystują te informacje do tworzenia i utrzymywania tablic routingu. Przykłady protokołów routingu:

- protokół **RIP** (ang. *Routing Information Protocol*),
- protokół **IGRP** (ang. *Interior Gateway Routing Protocol*),
- protokół **EIGRP** (ang. *Enhanced Interior Gateway Routing Protocol*),
- protokół **OSPF** (ang. *Open Shortest Path First*).

Protokoły routowane

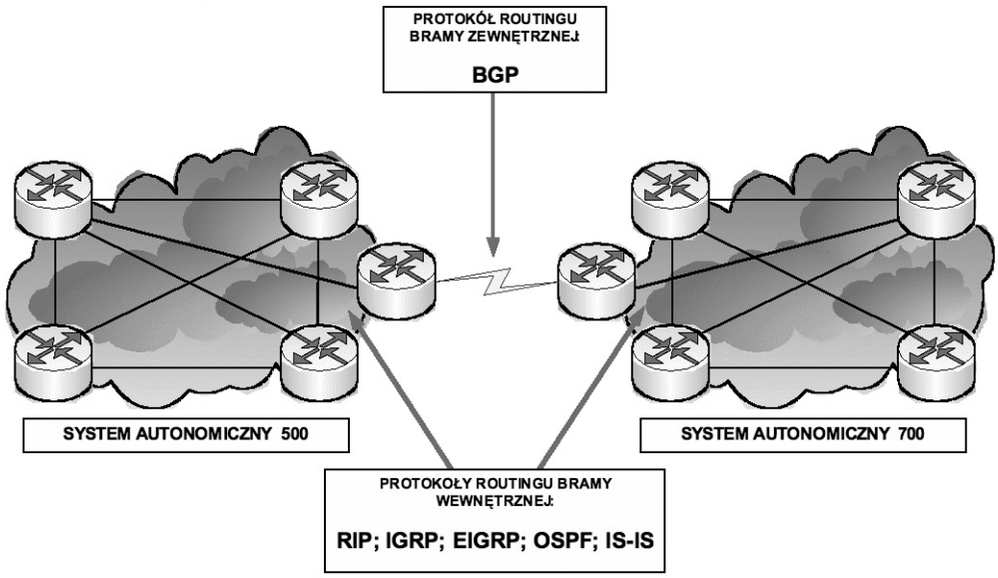
Protokół routowany służy do kierowania ruchem użytkowym. Zawiera w adresie warstwy sieciowej wystarczającą ilość informacji, aby umożliwić przesłanie pakietu z jednego hosta do innego w oparciu o właściwy dla siebie schemat adresowania. Przykłady protokołów routowanych:

- **IP** (ang. *Internet Protocol*),
- **IPX** (ang. *Internetwork Packet Exchange*),
- **DECnet** (ang. *Digital Equipment Corporation network*)
- **AppleTalk**,
- **Banyan VINES**,
- **XNS** (ang. *Xerox Network Systems*).

Wyróżniamy dwie kategorie protokołów routingu:

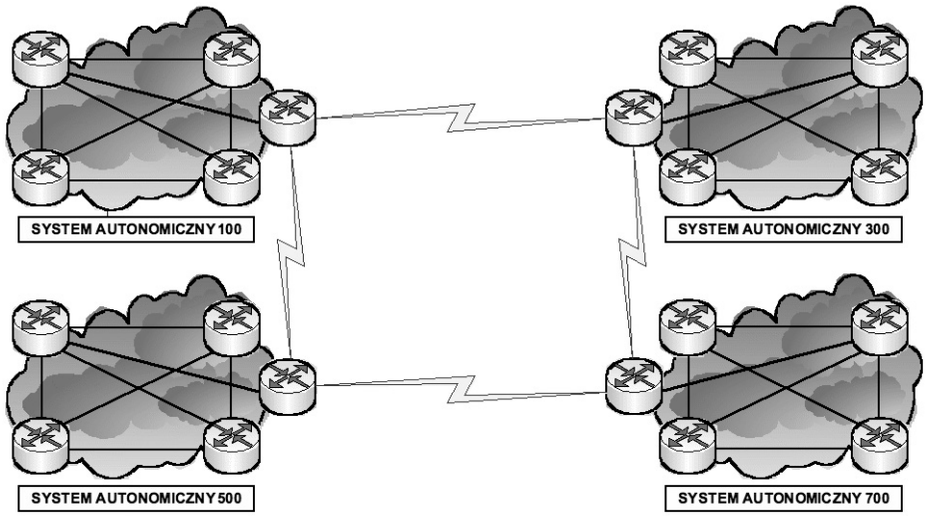
1. Protokoły wewnętrznej bramy **IGPs** (ang. *Interior Gateway Protocols*):
- **RIP**
- **IGRP**
- **EIGRP**
- **OSPF**
- **IS-IS** (ang. *Intermediate System-to-Intermediate System*).

2. Protokoły zewnętrznej bramy **EGPs** (ang. *Exterior Gateway Protocols*):
- **BGP** (ang. *Border Gateway Protocol*).



Rysunek 62.
Protokoły routingu bramy wewnętrznej oraz bramy zewnętrznej

Systemy autonomiczne

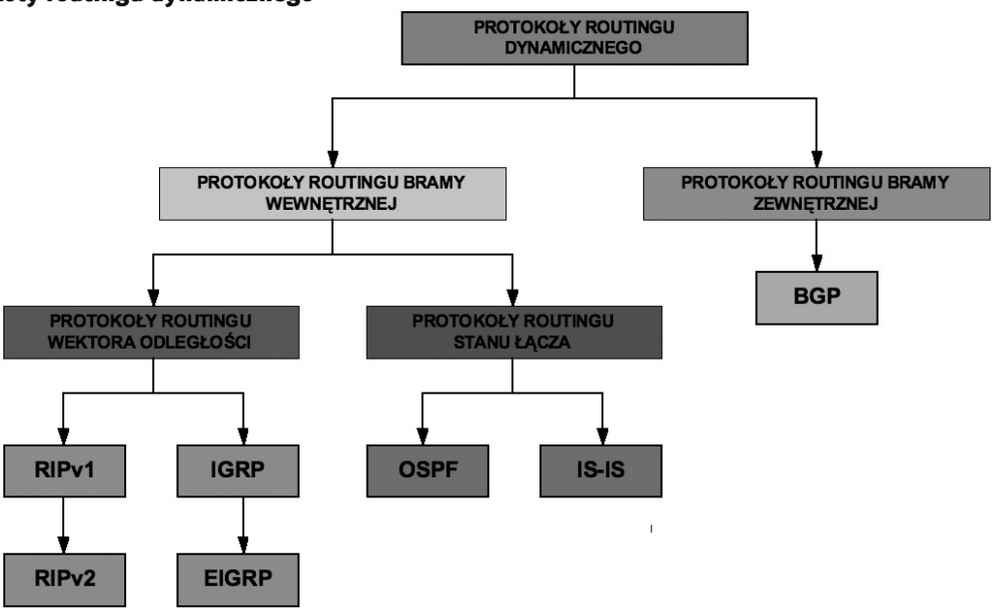


Rysunek 63.
Przykłady systemów autonomicznych

System autonomiczny (patrz rys. 63) to grupa sieci pozostających pod wspólną administracją i współdzielących tę samą strategię routingu. Z zewnątrz system autonomiczny jest widoczny jako pojedyncza jednostka. System autonomiczny może być prowadzony przez jednego lub kilku operatorów, prezentując jednocześnie spójny widok routingu dla świata zewnętrznego.

IANA (ang. *Internet Assigned Numbers Authority*) nadaje numery systemów autonomicznych regionalnym organizacjom rejestrującym. Numer systemu autonomicznego jest 16-bitowym (aktualnie 32-bitowym) numerem identyfikacyjnym. Protokół **BGP** (ang. *Border Gateway Protocol*) wymaga aby określić ten unikatowy, przypisany numer systemu autonomicznego w swojej konfiguracji.

Protokoły routingu dynamicznego



Rysunek 64.
Klasyfikacja protokołów routingu dynamicznego

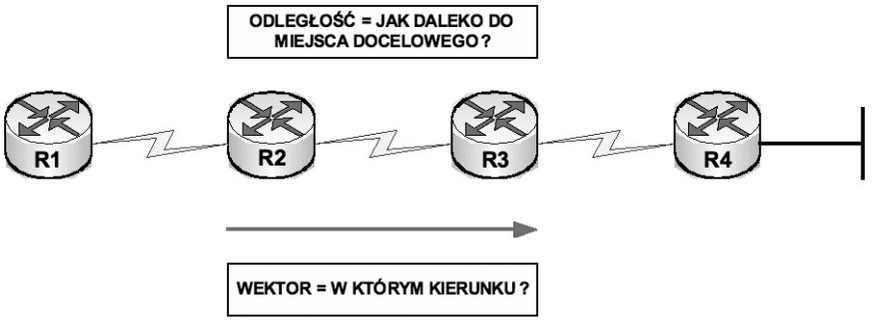
Celem protokołu routingu jest stworzenie i utrzymywanie tablicy routingu. Tablica ta zawiera sieci zapamiętane przez router oraz przypisane im interfejsy. Routery używają protokołów routingu do zarządzania informacjami odbieranymi od innych routerów i ich interfejsów oraz informacjami zawartymi w trasach skonfigurowanych ręcznie. Protokół routingu zapamiętuje wszystkie dostępne trasy, umieszcza najlepsze trasy w tablicy routingu i usuwa trasy, gdy te nie są już poprawne. Router korzysta z informacji zawartych w tablicy routingu do przesyłania pakietów protokołu routowanego.

Algorytm routingu stanowi podstawę routingu dynamicznego. Gdy topologia sieci zmieni się z powodu rozrostu, rekonfiguracji lub awarii sieci, baza wiedzy o sieci musi również ulec zmianie. Baza wiedzy o sieci musi odzwierciedlać dokładnie kształt nowej topologii.

Gdy wszystkie trasy w intersieci działają w oparciu o te same informacje, mówi się, że intersieć osiągnęła **zbieżność** (ang. *convergence*). Pożądane jest szybkie osiąganie zbieżności, ponieważ skraca to czas, w jakim routery podejmują niewłaściwe decyzje o routingu.

Systemy autonomiczne dzielą globalną intersieć na sieci mniejsze i łatwiejsze w zarządzaniu. Każdy system autonomiczny ma swój własny zbiór reguł i zasad oraz numer AS, który odróżnia go od innych systemów autonomicznych.

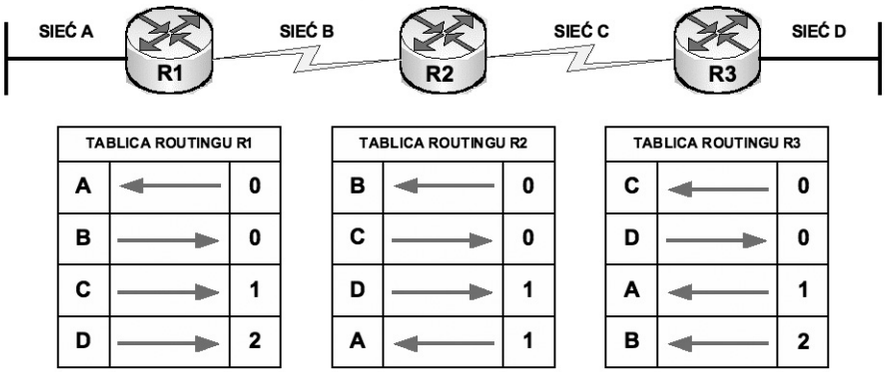
Protokoły routingu wektora odległości



Rysunek 65.
Parametry uwzględniane w protokołach routingu wektora odległości

Algorytm działający na podstawie wektora odległości okresowo przekazuje pomiędzy routerami kopie tablicy routingu. Takie regularne aktualizacje dokonywane pomiędzy routerami przekazują informacje o zmianach topologii. Algorytm routingu działający na podstawie wektora odległości, jest znany jako **algorytm Bellmana-Forda**. Każdy router otrzymuje tablicę routingu od bezpośrednio z nim połączonych routerów sąsiednich. Router R2 odbiera informacje od routera R1, po czym dodaje wartość wektora odległości, na przykład liczbę przeskoków. Liczba ta zwiększa wektor odległości. Następnie router R2 przekazuje nową tablicę routingu innemu sąsiadowi, routerowi R3 a ten przekazuje dalej do routera R4. Ten sam proces zachodzi we wszystkich kierunkach pomiędzy sąsiednimi routerami (patrz rys. 65). Algorytm powoduje w efekcie zebranie sumarycznych informacji o odległościach dzielących sieci, dzięki czemu możliwe jest utrzymywanie bazy danych topologii sieci. Jednakże algorytm działający na podstawie wektora odległości nie umożliwia routerowi poznania dokładnej topologii sieci, ponieważ każdy router widzi jedynie swe routery sąsiednie.

Działanie protokołu routingu wektora odległości



Rysunek 66.
Podgląd tablic routingu z wykorzystaniem algorytmu Bellmana-Forda

Każdy router korzystający z routingu działającego na podstawie wektora odległości w pierwszej kolejności identyfikuje swoich sąsiadów. Interfejs prowadzący do każdej bezpośrednio podłączonej sieci ma odległość administracyjną równą 0.

W miarę postępu procesu rozpoznawania opartego na algorytmie wektora odległości, na podstawie informacji otrzymanych od swoich sąsiadów, router ustala najlepsze trasy do sieci docelowych (patrz rys. 66). Router R1 zapamiętuje informacje o innych sieciach w oparciu o dane odebrane z routera R2 i tak dalej. Każda z pozycji reprezentujących inną sieć w tablicy routingu ma przypisany skumulowany wektor odległości pokazujący, jak daleko w danym kierunku znajduje się ta sieć. Aktualizacje tablic routingu następują w przypadku zmian topologii sieci. Tak jak w przypadku procesu wykrywania sieci, aktualizacje topologii sieci postępują od routera do routera.

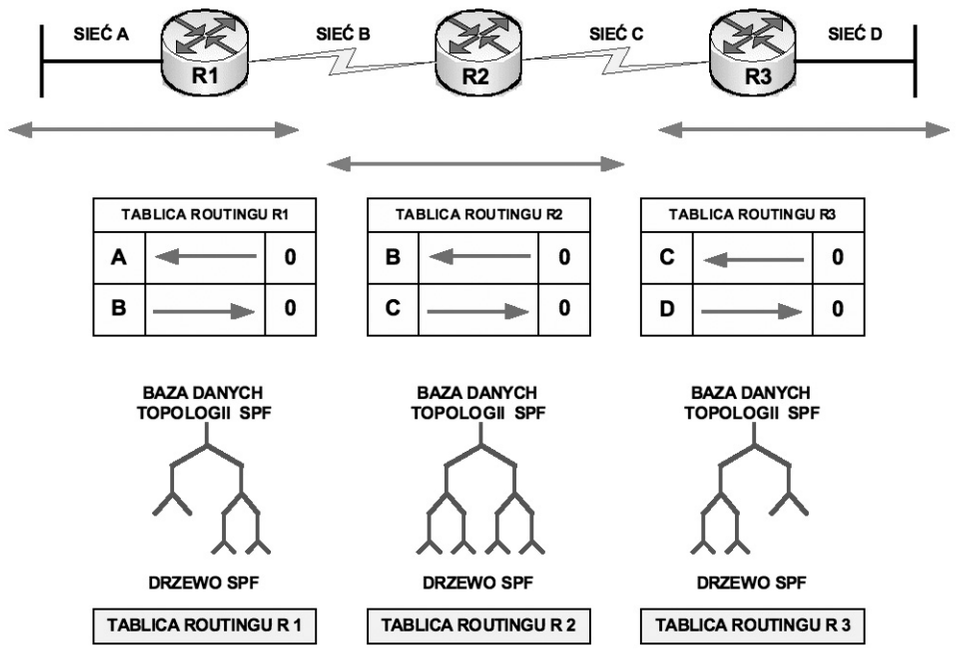
Algorytmy działające na podstawie wektora odległości nakazują każdemu routerowi wysłanie swojej tablicy routingu do każdego z sąsiednich routerów. Tablice routingu zawierają informacje na temat całkowitego kosztu ścieżki zdefiniowanego przez jego metrykę oraz adresu logicznego pierwszego routera na drodze do każdej sieci zawartej w tablicy.

Działanie protokołu routingu stanu łącza

Algorytm stanu łącza jest również znany jako **algorytm Dijkstry** lub algorytm **SPF** (ang. *Shortest Path First*). Routing stanu łącza wykorzystuje następujące elementy (patrz rys. 67):

1. Ogłoszenie **LSA** (ang. *Link-state advertisement*) – mały pakiet informacji o routingu wysyłany pomiędzy routerami.
2. Baza danych topologii – zbiór informacji zebranych na podstawie ogłaszania LSA.
3. Algorytm SPF – obliczenia wykonywane na podstawie informacji z bazy danych, dające w wyniku drzewo SPF.
4. Tablica routingu – lista znanych ścieżek i interfejsów.

Proces wymiany informacji LSA między routerami rozpoczyna się od bezpośrednio połączonych sieci, co do których zostały zgromadzone informacje. Każdy router tworzy bazę danych topologii składającą się z wszystkich informacji LSA.



Rysunek 67.
Parametry uwzględniane w protokołach routingu stanu łącza

Algorytm SPF oblicza osiągalność danej sieci. Router tworzy topologię logiczną w postaci drzewa, w którym sam zajmuje główną pozycję. Topologia ta składa się z wszystkich możliwych ścieżek do każdej sieci w intersieci protokołu stanu łącza. Następnie router sortuje ścieżki za pomocą algorytmu SPF – umieszcza najlepsze ścieżki i interfejsy do tych sieci docelowych w tablicy routingu. Utrzymuje również inną bazę danych elementów topologii i szczegółów stanu.

Pierwszy router, który otrzyma informację o zmianie topologii stanu łącza, przekazuje ją dalej, aby pozostałe routery mogły dokonać na jej podstawie aktualizacji. Wspólne informacje o routingu są wysyłane do wszystkich routerów w intersieci. Aby osiągnąć zbieżność, każdy router gromadzi informacje o sąsiednich routerach. Obejmują one nazwę każdego sąsiedniego routera, stan interfejsu oraz koszt łącza do sąsiada. Router tworzy pakiet LSA zawierający tę informację oraz dane o nowych sąsiadach, zmianach w koszcie łącza oraz o łączach, które nie są już aktualne. Pakiet LSA jest następnie wysyłany, aby pozostałe routery go odebrały. Gdy router odbierze pakiet LSA, aktualizuje tablicę routingu z użyciem bieżących informacji. Skumulowane dane służą do utworzenia mapy intersieci, a algorytm SPF jest używany do obliczenia najkrótszej ścieżki do innych sieci. Za każdym razem, gdy pakiet LSA powoduje zmianę bazy danych stanu łącza, za pomocą algorytmu SPF oblicza się najlepszą ścieżkę i aktualizuje tablicę routingu.

Z protokołami stanu łącza są związane następujące trzy zasadnicze problemy:

- zużycie czasu procesora,
- zapotrzebowanie na pamięć,
- zużycie pasma.

Routery wykorzystujące protokoły stanu łącza wymagają większej ilości pamięci i przetwarzają więcej danych, niż te wykorzystujące protokoły routingu działające na podstawie wektora odległości. Routery stanu łącza wymagają większej ilości pamięci do przechowywania wszystkich informacji z różnych baz danych, drzewa topologii i tablicy routingu. Początkowy rozpływ pakietów stanu łącza wymaga przesłania dużej ilości danych. W trakcie początkowego procesu wykrywania wszystkie routery korzystające z protokołów routingu według stanu łącza wysyłają pakiety LSA do pozostałych routerów. Powoduje to zalewanie intersieci i tymczasowo zmniejsza pasmo dostępne dla ruchu routowanego przenoszącego dane użytkowe. Po początkowym rozpływie protokoły routingu według stanu łącza wymagają minimalnej ilości pasma do sporadycznego lub wyzwalanego zdarzeniami wysyłania pakietów LSA odzwierciedlających zmiany topologii.

Odległość administracyjna trasy

W miarę gromadzenia uaktualnień w procesie routingu, router wybiera najlepszą ścieżkę do dowolnego celu i próbuje dodać ją do tablicy routingu. Router decyduje, co zrobić z trasami dostarczanymi przez procesy routingu w oparciu o odległość administracyjną trasy. Jeśli dana ścieżka ma najmniejszą odległość administracyjną do danego celu, jest dodawana do tablicy routingu; jeśli tak nie jest, trasa jest odrzucana. W tabeli 4 zestawiono domyślne wartości dla protokołów obsługiwanych przez system Cisco IOS.

Tabela 4.
Wykaz wybranych wartości odległości administracyjnej trasy

Źródło trasy odległości administracyjnej	Odległość domyślna
DOŁĄCZONY BEZPOŚREDNIO INTERFEJS	0
TRASA STATYCZNA	1
SKONSOLIDOWANA TRASA PROTOKOŁU EIGRP	5
ZEWNĘTRZNA TRASA PROTOKOŁU BGP	20
WEWNĘTRZNA TRASA PROTOKOŁU EIGRP	90
PROTOKÓŁ IGRP	100
PROTOKÓŁ OSPF	110
PROTOKÓŁ IS-IS	115
PROTOKÓŁ RIP	120
ZEWNĘTRZNA TRASA PROTOKOŁU EIGRP	170
WEWNĘTRZNA TRASA PROTOKOŁU BGP	200
TRASA NIEZNANA	255

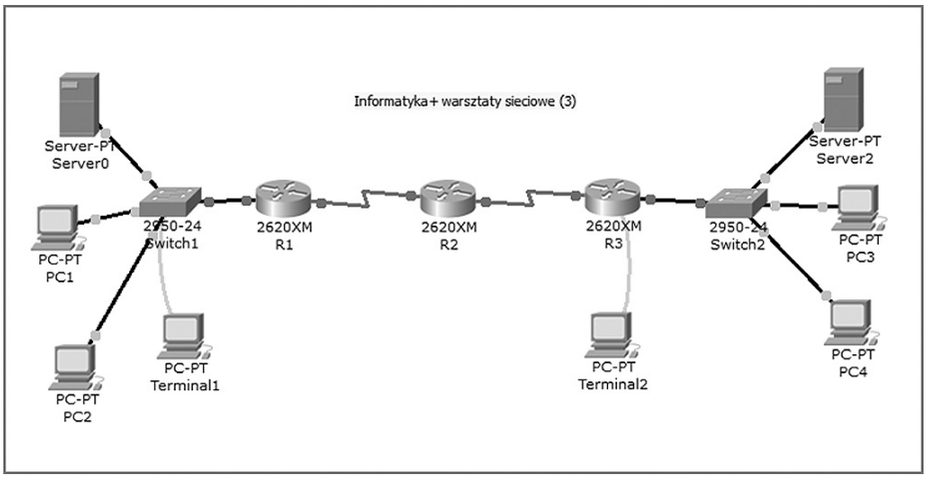
LITERATURA

1. Empson E., *Akademia sieci Cisco. CCNA Pełny przegląd poleceń*, WN PWN, Warszawa 2008
2. Graziani R., Johnson A., *Akademia sieci Cisco. CCNA Exploration. Semestr 2. Protokoły i koncepcje routingu*, WN PWN, Warszawa 2008
3. Józefiok A., *Budowa sieci komputerowych na przełącznikach i routerach Cisco*, Helion, Gliwice 2009
4. Krysiak K., *Sieci komputerowe. Kompendium*, Helion, Gliwice 2005.
5. Mucha M., *Sieci komputerowe. Budowa i działanie*, Helion, Gliwice 2003
6. Odom W., McDonald R., *CCNA semestr 2. Routery i podstawy routingu*, WN PWN, Warszawa 2007

WARSZTATY

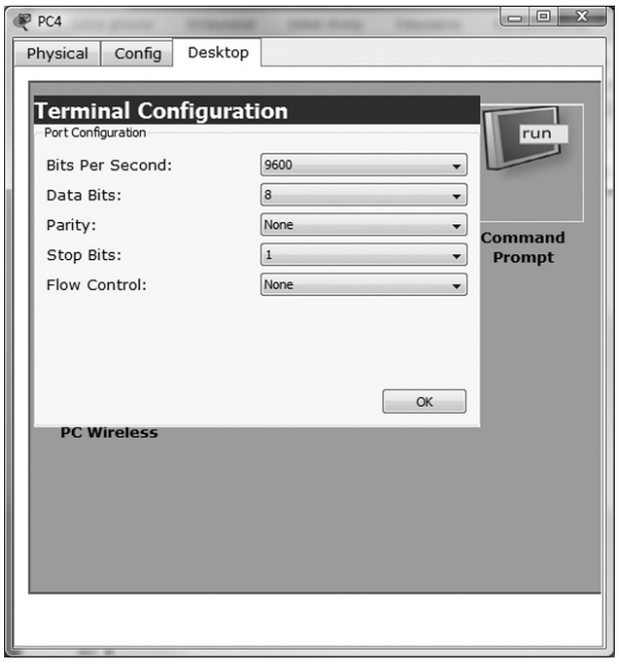
Celem warsztatów jest konfiguracja podstawowych parametrów urządzeń sieciowych, uruchomienie niezbędnych procesów oraz implementacja mechanizmów zarządzania ruchem w sieciach komputerowych. Zwrócona zostanie uwaga na możliwości weryfikacji poprawności konfiguracji i działania sprzętu. Interaktywny model zostanie stworzony indywidualnie przez uczestników z wykorzystaniem oprogramowania Packet Tracer (firmy Cisco Systems)

Ćwiczenie 1. Budowa modelu sieci według schematu jak na rysunku 68 oraz parametrów podanych przez wykładowcę.



Rysunek 68.
Przykładowy schemat sieci komputerowej

Ćwiczenie 2. Konfiguracja portu terminala/portu szeregowego do komunikacji z aktywnym urządzeniem sieciowym.



Rysunek 69.
Konfiguracja portu szeregowego komputera

Ćwiczenie 3. Uruchomienie routera.

System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2620 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory

Self decompressing the image :
[OK]
Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
cisco 2620 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
4 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Ćwiczenie 4. Sprawdzenie podstawowych parametrów oraz ukompletowania.

Router#show version (przejście do trybu uprzywilejowanego)
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC
ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
System returned to ROM by reload
System image file is „flash:c2600-i-mz.122-28.bin” *(plik z obrazem systemu operacyjnego)*
cisco 2620 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.

X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
4 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102

Ćwiczenie 5. Sprawdzenie stanu interfejsów.

Router#show ip interface brief

Interface	IP-Address	OK? Method Status	Protocol
FastEthernet0/0	unassigned	YES manual administratively down	down
Serial0/0	unassigned	YES manual administratively down	down
Serial0/1	unassigned	YES manual administratively down	down
Serial0/2	unassigned	YES manual administratively down	down
Serial0/3	unassigned	YES manual administratively down	down

Ćwiczenie 6. Sprawdzenie bieżącej konfiguracji.

```
Router#show running-config
Building configuration...
Current configuration : 424 bytes
!
version 12.2
no service password-encryption
!
hostname Router
!
ip ssh version 1
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0
no ip address
shutdown
!
interface Serial0/1
no ip address
shutdown
!
interface Serial0/2
no ip address
shutdown
!
interface Serial0/3
no ip address
shutdown
!
```

```
ip classless
!
line con 0
line vty 0 4
login
!
end
```

Ćwiczenie 7. Sprawdzenie aktywnych procesów.

```
Router# show processes
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID QTy        PC Runtime (ms)  Invoked     uSecs          Stacks  TTY Process
1 Csp 602F3AF0 0                1627        0 2600/3000    0       Load Meter
2 Lwe 60C5BE00 4                136         29 5572/6000   0       CEF Scanner
3 Lst 602D90F8 1676             837         2002 5740/6000 0       Check heaps
4 Cwe 602D08F8 0                1           0 5568/6000    0       Chunk Manager
5 Cwe 602DF0E8 0                1           0 5592/6000    0       Pool Manager
6 Mst 60251E38 0                2           0 5560/6000    0       Timers
7 Mwe 600D4940 0                2           0 5568/6000    0       Serial Backgrou
8 Mwe 6034B718 0                1           0 2584/3000    0       OIR Handler
9 Mwe 603FA3C8 0                1           0 5612/6000    0       IPC Zone Manage
10 Mwe 603FA1A0 0               8124        0 5488/6000    0       IPC Periodic Ti
11 Mwe 603FA220 0               9           0 4884/6000    0       IPC Seat Manage
12 Lwe 60406818 124             2003        61 5300/6000   0       ARP Input
13 Mwe 60581638 0               1           0 5760/6000    0       HC Counter Time
14 Mwe 605E3D00 0               2           0 5564/6000    0       DDR Timers
15 Msp 80164A38 079543          0           5608/6000      0       GraphIt
16 Mwe 802DB0FC 0               2           011576/12000   0       Dialer event
17 Cwe 801E74BC 0               1           0 5808/6000    0       Critical Bkgnd
18 Mwe 80194D20 4               9549        010428/12000   0       Net Background
19 Lwe 8011E9CC 0               20          011096/12000   0       Logger
20 Mwe 80140160 8               79539       0 5108/6000    0       TTY Background
21 Msp 80194114 0               95409       0 8680/9000    0       Per-Second Job
22 Mwe 8047E960 0               2           0 5544/6000    0       dot1x
23 Mwe 80222C8C 4               2           2000 5360/6000 0       DHCPD Receive
24 Mwe 800844A0 0               1           0 5796/6000    0       HTTP Timer
25 Mwe 80099378 0               1           0 5612/6000    0       RARP Input
26 Mst 8022F178 0               1           011796/12000   0       TCP Timer
27 Lwe 802344C8 0               1           011804/12000   0       TCP Protocols
28 Hwe 802870E8 0               1           0 5784/6000    0       Socket Timers
29 Mwe 80426048  64             3           21333 4488/6000 0      L2MM
30 Mwe 80420010 4               1           4000 5592/6000 0       MRD
31 Mwe 8041E570 0               1           0 5584/6000    0       IGMPSN
32 Hwe 80429B40 0               1           0 2604/3000    0       IGMP Snooping P
33 Mwe 804F43B0 0               5           0 5472/6000    0       Cluster L2
34 Mwe 804F18D0 0               17          0 5520/6000    0       Cluster RARP
35 Mwe 804EA650 0               23          0 5440/6000    0       Cluster Base
36 Lwe 802A1158 4               1           4000 5592/6000 0       Router Autoconf
37 Mwe 80022058 0               1           0 5624/6000    0       Syslog Traps
38 Mwe 8031CE88 0               1           0 5788/6000    0       AggMgr Process
39 Mwe 8035EF88 0               407         0 5592/6000    0       PM Callback
40 Mwe 80437B58 0               3           0 5556/6000    0       VTP Trap Proces
```

41 Mwe 80027D40	0	2	0 5676/6000	0	DHCPD Timer
42 Mwe 8040D3B0	0	2	0 2560/3000	0	STP STACK TOPOL
43 Hwe 8040E338	0	2	0 2560/3000	0	STP FAST TRANSI

Ćwiczenie 8. Wykonanie podstawowej konfiguracji przełącznika.

Tabela 5.
Schemat adresacji

Urządzenie	Interfejs	Adres	Maska	Brama domyślna
Router1	**Fa0/0**	192.168.50.1	255.255.255.0	N/A
	Fa0/1.10	192.168.10.1	255.255.255.0	N/A
	Fa0/1.20	192.168.20.1	255.255.255.0	N/A
	Fa0/1.30	192.168.30.1	255.255.255.0	N/A
	Fa0/1.99	192.168.99.1	255.255.255.0	N/A
Switch1	**VLAN 99**	192.168.99.31	255.255.255.0	192.168.99.1
Switch2	**VLAN 99**	192.168.99.32	255.255.255.0	192.168.99.1
Switch3	**VLAN 99**	192.168.99.33	255.255.255.0	192.168.99.1
PC1	**NIC**	192.168.10.21	255.255.255.0	192.168.10.1
PC2	**NIC**	192.168.20.22	255.255.255.0	192.168.20.1
PC3	**NIC**	192.168.30.23	255.255.255.0	192.168.30.1
PC4	**NIC**	192.168.10.24	255.255.255.0	192.168.10.1
PC5	**NIC**	192.168.20.25	255.255.255.0	192.168.20.1
PC6	**NIC**	192.168.30.26	255.255.255.0	192.168.30.1

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 99
Switch(config-if)#ip address 192.168.99.33 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet 0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport acces vlan 99

%LINK-5-CHANGED: Interface Vlan99, changed state to up% Access VLAN does not exist. Creating vlan 99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to upSwitch(config-if)
Switch(config)#ip default-gateway 192.168.99.1
Switch(config)#end
%SYS-5-CONFIG_I: Configured from console by console

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable secret class
Switch(config)#line vty 0 15
Switch(config-line)#password test
Switch(config-line)#^Z
%SYS-5-CONFIG_I: Configured from console by console

Ćwiczenie 9. Podstawowa konfiguracja routera.

```
Router#configure terminal #przechodzimy w tryb konfiguracji z terminala#
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname INFORMATYKA+_01 #wprowadzamy nazwę routera#
INFORMATYKA+_01(config)#enable secret 12345678 #wprowadzamy hasło na tryb uprzywilejowany#
INFORMATYKA+_01(config)#line vty 0 4
INFORMATYKA+_01(config-line)#password 987654321     #wprowadzamy hasło na linie wirtualnego terminala
(telnet)#
INFORMATYKA+_01(config-line)#exit
INFORMATYKA+_01(config)#line console 0
INFORMATYKA+_01(config-line)#password qwerty #wprowadzamy hasło na port konsoli#
INFORMATYKA+_01(config-line)#^Z
%SYS-5-CONFIG_I: Configured from console by console
INFORMATYKA+_01#
INFORMATYKA+_01#copy running-config startup-config #zapisanie konfiguracji#
Destination filename [startup-config]?
Building configuration...
[OK]
INFORMATYKA+_01#
```

Ćwiczenie 10. Konfiguracja interfejsów sieciowych routera.

```
Konfiguracja interfejsów LAN I WAN
INFORMATYKA+_01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
INFORMATYKA+_01(config)#interface fastethernet 0/0 #wybór interfejsu#
INFORMATYKA+_01(config-if)#ip address 192.168.1.1 255.255.255.0 #ustawienie adresu IP#
INFORMATYKA+_01(config-if)#no shutdown #włączenie interfejsu#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

INFORMATYKA+_01(config-if)#exit
INFORMATYKA+_01(config)#interface serial 0/0
INFORMATYKA+_01(config-if)#ip address 10.10.10.1 255.255.255.252
INFORMATYKA+_01(config-if)#clock rate 128000 #ustawienie prędkości łącza WAN#
INFORMATYKA+_01(config-if)#encapsulation ppp #ustawienie rodzaju protokołu WAN#
INFORMATYKA+_01(config-if)#no shutdown

Serial0/0 LCP: State is Open
Serial0/0 PPP: Phase is FORWARDING, Attempting Forward
Serial0/0 Phase is ESTABLISHING, Finish LCP
Serial0/0 Phase is UP
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up

INFORMATYKA+_01(config-if)#
```

Ćwiczenie 11. Sprawdzenie działania interfejsów routera.

NFORMATYKA+_01#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up (connected)
Hardware is Lance, address is 0001.9781.1a57 (bia 0001.9781.1a57)
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of „show interface" counters never
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
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

Ćwiczenie 12. Konfiguracja i weryfikacja działania routingu statycznego.

INFORMATYKA+_01(config)#ip route 172.16.0.0 255.255.0.0 10.10.10.2
INFORMATYKA+_01(config)#ip route 10.10.10.4 255.255.255.252 10.10.10.2

INFORMATYKA+_00(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.1
INFORMATYKA+_00(config)#ip route 172.16.0.0 255.255.0.0 10.10.10.6

INFORMATYKA+_02(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.5
INFORMATYKA+_02(config)#ip route 10.10.10.0 255.255.255.252 10.10.10.5

Ćwiczenie 13. Weryfikacja tablicy routingu.

INFORMATYKA+_01#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
- candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/30 is subnetted, 2 subnets
C 10.10.10.0 is directly connected, Serial0/0
S 10.10.10.4 [1/0] via 10.10.10.2

```
S    172.16.0.0/16 [1/0] via 10.10.10.2
C    192.168.1.0/24 is directly connected, FastEthernet0/0
INFORMATYKA+_01#
```

Ćwiczenie 14. Użycie komendy **ping.**

```
PC3›ping 192.168.1.11
Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=188ms TTL=125
Reply from 192.168.1.11: bytes=32 time=171ms TTL=125
Reply from 192.168.1.11: bytes=32 time=143ms TTL=125
Reply from 192.168.1.11: bytes=32 time=171ms TTL=125

Ping statistics for 192.168.1.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 143ms, Maximum = 188ms, Average = 168ms
```

Ćwiczenie 15. Użycie komendy **tracert.**

```
PC3›tracert 192.168.1.101
Tracing route to 192.168.1.101 over a maximum of 30 hops:

1   63 ms    62 ms    40 ms    172.16.0.1
2   94 ms    93 ms    93 ms    10.10.10.5
3   141 ms   94 ms    111 ms   10.10.10.1
4   141 ms   173 ms   156 ms   192.168.1.101

Trace complete.
PC›
```

Ćwiczenie 16. Konfiguracja dynamicznego protokołu routingu **RIP.**

```
INFORMATYKA+_01(config)#router rip
INFORMATYKA+_0(config-router)#network 192.168.1.0
INFORMATYKA+_0(config-router)#network 10.10.10.0
INFORMATYKA+_0(config-router)#
INFORMATYKA+_01#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
- candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/30 is subnetted, 2 subnets
C       10.10.10.0 is directly connected, Serial0/0
```

```
R      10.10.10.4 [120/1] via 10.10.10.2, 00:00:13, Serial0/0
R    172.16.0.0/16 [120/2] via 10.10.10.2, 00:00:13, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
INFORMATYKA+_01#show ip protocols
Routing Protocol is „rip”
Sending updates every 30 seconds, next due in 18 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
Interface            Send  Recv  Triggered RIP  Key-chain
FastEthernet0/0      1     2 1
Serial0/0            1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
10.0.0.0
192.168.1.0
Passive Interface(s):
Routing Information Sources:
Gateway         Distance      Last Update
10.10.10.2           120      00:00:12
Distance: (default is 120)
.
```

W projekcie **Informatyka +**, poza wykładami i warsztatami, przewidziano następujące działania:

- 24-godzinne kursy dla uczniów w ramach modułów tematycznych
- 24-godzinne kursy metodyczne dla nauczycieli, przygotowujące do pracy z uczniem zdolnym
- nagrania 60 wykładów informatycznych, prowadzonych przez wybitnych specjalistów i nauczycieli akademickich
- konkursy dla uczniów, trzy w ciągu roku
- udział uczniów w pracach kół naukowych
- udział uczniów w konferencjach naukowych
- obozy wypoczynkowo-naukowe.

Szczegółowe informacje znajdują się na stronie projektu

www.informatykaplus.edu.pl