Konfiguracja routerów – podstawy

Autorzy: Paweł Brzyski, Piotr Ptasznik IV FDS

STRESZCZENIE

Opracowanie to zawiera podstawowe informacje na temat konfiguracji routerów, wykorzystywanych przez nie protokołów trasowania, a także algorytmów trasowania. Przeznaczone jest dla początkujących użytkowników, których bardzo często odstraszają obszerne dokumentacje dostarczane przez producentów urządzeń sieciowych, dlatego zawarliśmy tylko najważniejsze i najczęściej używane polecenia IOS oraz najpopularniejsze opcje. Omówiono również współpracę z serwerem TFTP służącym do ładowania obrazu systemu operacyjnego oraz do zapisywania i pobierania pliku z konfiguracją routera. Przedstawiony jest opis zazwyczaj wykorzystywanych protokołów trasowania, a w rozdziale „Dodatek" zamieszczamy główne polecenia konfiguracyjne.

SPIS TREŚCI

1. WIADOMOŚCI OGÓLNE

1.1 Routery [3]

Węzły sieci operujące w trzeciej (sieciowej) warstwie modelu OSI noszą nazwę routerów. Są to urządzenia wyposażone najczęściej w kilka interfejsów sieciowych LAN, porty obsługujące sieci WAN, pracujący wydajnie procesor i specjalne oprogramowanie zawiadujące ruchem pakietów przepływających przez router. Chociaż routerem może też być zwykły komputer dysponujący kilkoma kartami sieciowymi i specjalnym oprogramowaniem, to jest to najczęściej dedykowany komputer, dysponujący rozwiązaniami znacznie zwiększającymi wydajność tego rodzaju węzłów sieci.

Routery są stosowane zarówno w sieciach LAN, jak i WAN. W sieciach LAN **(routery lokalne)** są używane wtedy, gdy system chcemy podzielić na dwie lub więcej podsieci, czyli poddać operacji segmentowania. Segmentacja sieci powoduje, że poszczególne podsieci są od siebie odseparowane i pakiety (zarówno *Point-to-Point,* jak i *multicast czy broadcast)* nie przenikają z jednej podsieci do drugiej. Korzyść jest oczywista: w ten sposób zwiększamy przepustowość każdej z podsieci.

Jak sama nazwa wskazuje (ang. *route* to trasa), routery wyznaczają pakietom marszruty, kierując je do odpowiedniego portu lub karty sieciowej. Routery nie interesują się adresami MAC, a po odebraniu pakietu odczytują i poddają analizie adres budowany w obszarze warstwy sieciowej. W sieciach Internet będzie to adres IP przypisywany przez administratora każdemu ze stanowisk pracy. Ponieważ routery służą do sprzęgania różnych sieci, to do routera zostaną wysłane tylko te pakiety, które są kierowane do innych sieci.

Inną rolę pełnią **routery dostępowe,** czyli sprzęgające sieć LAN ze światem zewnętrznym. W tym przypadku nie chodzi już o segmentację sieci LAN na mniejsze domeny rozgłoszeniowe, ale o zainstalowanie węzła sieci ekspediującego przez łącze WAN pakiety generowane przez pracujące w sieci LAN stacje do innego routera pracującego po drugiej stronie tego łącza. Oczywiście, może się zdarzyć i tak, że jeden router obsługuje zarówno pakiety lokalne, jak i te kierowane na zewnątrz.

Routery zakładają tabele routingu i mają zdolność „uczenia się" topologii sieci, wymieniając informacje z innymi routerami zainstalowanymi w sieci. Ponieważ prawie wszystkie operacje związane z odbieraniem i ekspediowaniem pakietów do odpowiedniego portu są realizowane w routerze przez oprogramowanie, to tego rodzaju węzły sieci pracują dużo wolniej niż np. przełączniki.

W sieciach szkieletowych instaluje się routery o **najwyższej wydajności** (klasy *high end),* które powinny wspierać wszystkie rodzaje interfejsów używanych w sieciach LAN i WAN oraz obsługiwać maksymalnie dużo protokołów transportu i trasowania (nawet tych rzadko używanych). Niektóre routery z tej grupy są w stanie obsłużyć nawet do 50 portów.

Routery **średniej mocy** są najczęściej używane w sieciach korporacyjnych do łączenia się z serwerami zainstalowanymi w sieciach bazowych. Mogą one też służyć do budowy sieci bazowych w mniejszych przedsiębiorstwach. Typowy router tej klasy składa się z dwóch do trzech portów sieci LAN oraz z czterech do ośmiu portów sieci WAN.

No i wreszcie **routery oddziałowe,** które łączą mało obciążone sieci LAN z resztą firmy. Są one z reguły wyposażone w jeden port LAN (obsługujący sieć Ethernet lub Token Ring) i dwa porty WAN małej szybkości, obsługujące łącza dedykowane lub komutowane. Są to chyba najczęściej kupowane routery, gdyż pozwalają stosunkowo niewielkim kosztem rozbudować sieć komputerową czy łączyć odległe biura i oddziały firmy z centralą.

Architektury routerów instalowanych w sieciach szkieletowych i routerów oddziałowych różnią się zasadniczo, ponieważ urządzenia te pełnią inne funkcje. Pierwsze dają się łatwo rozbudowywać i po ponownym skonfigurowaniu dostosowywać do nowych warunków pracy. Muszą

one dysponować dużą przepustowością i są wyposażane w szybko pracujące procesory i interfejsy oraz w oprogramowanie, które potrafi automatycznie optymalizować ruch pakietów krążących po sieci. Obsługują wiele protokołów transportu w sieciach LAN i WAN, od protokołu sieci Arcnet do protokołu X.25. Zupełnie inaczej jest z routerami oddziałowymi. Są to najczęściej urządzenia wyposażone na stałe w kilka portów i jeden procesor zarządzający pracą trzech do czterech interfejsów. I chociaż mogą one obsługiwać te same protokoły co router bazowy, to ich oprogramowanie jest stosunkowo proste. Wykonuje ono bowiem nieskomplikowane, rutynowe operacje przesyłania pakietów między określonymi portami.

1.2 Protokoły trasowania

1.2.1 Protokół RIP

Protokół RIP (ang. Routing lnformation Protocol) jest protokołem routingu o trybie rozgłoszeniowym, w którym zastosowano algorytm *distance-vector*, który jako metryki używa licznika skoków między routerami. Maksymalna liczba skoków wynosi 15. Każda dłuższa trasa jest jako nieosiągalna, poprzez ustawienie licznika skoków na 16. Informacje o routingu w protokole RIP przekazywane są z routera do sąsiednich routerów przez rozgłoszenie IP z wykorzystaniem protokołu UDP i portu 250. Jest on szeroko stosowany w sieciach jako protokół wewnętrzny **IGP** *(Interior Gateway Protocol),* co oznacza, że wykonuje routing pojedynczym autonomicznym systemem albo protokołem zewnętrznym **EGP** *(Exterior Gateway Protocol)* - wykonuje routing pomiędzy różnymi autonomicznymi systemami. Protokół RIP jest obecnie szeroko wykorzystywany w Internecie i używany w sieciach jako podstawowa metoda wymiany informacji o routingu pomiędzy routerami. Specyfikacje protokołu RIP definiują dwa dokumenty RFC (Request For Comments) 1058 i 1723. RFC 1058 opisuje pierwszą implementację protokołu, natomiast jego wersję zaktualizowaną opisuje dokument RFC 1723.[3]

1.2.2 Protokół IGRP

Protokół IGRP (ang. Interior Gateway Routing Protocol) został zaprojektowany, aby wyeliminować pewne mankamenty protokołu RIP oraz poprawić obsługę większych sieci o różnych przepustowościach łączy. IGRP, podobnie jak RIP, używa trybu rozgłoszeniowego do przekazywania informacji o routingu sąsiednim routerem. Jednak IGRP ma własny protokół warstwy transportu. Nie wykorzystuje UDP ani TCP do przekazywania informacji na temat trasy sieciowej. Oferuje on trzy główne rozszerzenia względem protokołu RIP. Po pierwsze może obsługiwać sieć do 255 skoków między routerami. Po drugie potrafi rozróżniać odmienne rodzaje nośników połączeń i związane z nimi koszty. Po trzecie oferuje szybszą konwergencję, dzięki użyciu aktualizacji typu flash.[1]

1.2.3 Protokół EIGRP

Protokół EIGRP (ang. Enhanced IGRP) podobnie jak IGRP, ogłasza informacje tablicy routingu tylko routerom sąsiednim. Jednak w przeciwieństwie do powyższego protokołu, sąsiedzi rozpoznawani są poprzez wymianę protokołu hello dokonywaną między routerami w tej samej sieci fizycznej. Po wykryciu sąsiednich routerów, EIGRP używa niezawodnego protokołu transportu, dzięki czemu zapewnia właściwe i uporządkowane informacje z tablicy routingu oraz aktualizacje. Router śledzi nie tylko połączone z nim trasy, ale także wszystkie trasy ogłaszane przez sąsiadów. Na podstawie tych informacji, protokół ten może szybko i efektywnie wybrać ścieżkę docelową o najniższym koszcie i zagwarantować, ze nie jest ona częścią pętli routingu. Dzięki przechowywaniu informacji na temat sąsiadów, algorytm może szybciej okre-

ślić trasę zastępczą lub dopuszczalne zastępstwo w przypadku awarii łącza bądź innego zdarzenia modyfikującego topologię.[1]

1.2.4 Protokół OSPF

Protokół OSPF (ang. Open Shortest Path First) został zaprojektowany, by spełniać potrzeby sieci opartych na IP, uwierzytelnianiu źródła trasy, szybkością konwergencji, oznaczaniem tras przez zewnętrzne protokoły routingu oraz podawanie tras w trybie rozgłoszeniowym. W przeciwieństwie do protokołów RIP i IGRP, które ogłaszają swoje trasy tylko sąsiednim routerem, routery OSPF wysyłają ogłoszenia stanu łącza do wszystkich routerów w obrębie tego samego obszaru hierarchicznego poprzez transmisję IP w trybie rozgłoszeniowym. Ogłoszenie stanu łącza zawiera informacje dotyczące podłączonych interfejsów, używanych metryk oraz inne niezbędne do przetwarzania baz danych ścieżek sieciowych i topologii. Routery OSPF gromadzą informacje na temat łącza danych i uruchamiają algorytm SPF (znany także jako algorytm Dijkstry), aby obliczyć najkrótszą ścieżkę do każdego węzła.[1]

1.2.5 Protokół IS-IS

Protokół IS-IS jest protokołem typu „link-state", który rozpowszechnia informacje o stanie łącz w celu utworzenia kompletnego obrazu topologii sieci. Aby umożliwić uproszczenie budowy routerów, protokół IS-IS wyróżnia systemy IS poziomu l i poziomu 2 (Level l router i Level 2 router). Routery poziomu l łączą ze sobą systemy w jednym obszarze, routery poziomu 2 łączą obszary między sobą, tworząc szkielet wewnątrzdomenowy. używa jednej domyślnej miary, której wartość nie przekracza 1024. Miarę przydziela administrator sieci. Pojedyncze łącze może przyjąć wartość nie większą niż 64, wartość ścieżki uzyskuje się sumując wartości łączy.[3]

1.2.6 Routing statyczny

Routing statyczny używany wówczas, gdy mapa połączeń sieciowych jest programowana w routerze „ręcznie" przez administratora. W razie, gdy jakaś ścieżka zostanie przerwana, administrator musi przeprogramować router, aby odpowiednie pakiety mogły dotrzeć do celu. W systemach sieciowych o kluczowym znaczeniu taki sposób trasowania jest niemożliwy do zaakceptowania. Stosuje się więc dynamiczne routery, które automatycznie diagnozują stan połączeń i wyznaczają połączenia alternatywne.[2]

1.3 Algorytmy trasowania [3]

1.3.1 Algorytmy statyczne i dynamiczne

Algorytm statyczny nie jest właściwie algorytmem. Wszystkie drogi routingu wyznacza tu bowiem na stałe sam administrator systemu. Jeśli topologia sieci zmieni się, router jest po prostu bezsilny. Algorytmy dynamiczne natomiast śledzą cały czas topologię sieci (praca w czasie rzeczywistym) i modyfikują w razie potrzeby tabele routingu zakładane przez router.

1.3.2 Algorytmy single path i multipath

Niektóre protokoły trasowania wyznaczają pakietom kilka dróg dostępu do stacji przeznaczenia, czyli wspierają multipleksowanie. I tak jak algorytm *single path* definiuje tylko jedną ścieżkę dostępu do adresata, tak algorytm *multi path* pozwala przesyłać pakiety przez wiele niezależnych ścieżek, co nie tylko zwiększa szybkość transmisji pakietów, ale też chroni sys-

tem routingu przed skutkami awarii.

1.3.3 Algorytmy płaskie i hierarchiczne

W przypadku algorytmów płaskich wszystkie routery są równorzędne. Można to porównać do sieci typu „peer-to-peer". Nie ma tu (ze względu na strukturę logiczną) ważniejszych i mniej ważnych routerów czy też nadrzędnych lub podrzędnych. Algorytmy hierarchiczne postrzegają sieć jako strukturę zhierarchizowaną, dzieląc ją na domeny. Pakietami krążącymi w obrębie każdej domeny zawiaduje wtedy właściwy router, przekazując je routerowi nadrzędnemu lub podrzędnemu.

1.3.4 Algorytmy host intelligent i router intelligent

Niektóre algorytmy zakładają, że całą drogę pakietu do stacji przeznaczenia wyznaczy od razu stacja nadająca. Mamy wtedy do czynienia z trasowaniem źródłowym (*source routing,* czyli *host inteligent*). W tym układzie router pełni tylko rolę „przekaźnika" odbierającego pakiet i ekspediującego go do następnego miejsca. W algorytmach *router intelligent stacja* wysyłająca nie ma pojęcia, jaką drogę przemierzy pakiet, zanim dotrze do adresata. Obowiązek wyznaczenia pakietowi marszruty spoczywa na routerach.

1.3.5 Algorytmy intradomain i interdomain

Algorytmy trasowania *intradomain* operują wyłącznie w obszarze konkretnej domeny, podczas gdy algorytmy *interdomain* zawiadują pakietami biorąc pod uwagę nie tylko zależności zachodzące w ramach konkretnej domeny, ale też powiązania między tą domeną i innymi, otaczającymi ją domenami. Optymalne marszruty wyznaczane przez algorytm *intradomain* nie muszą być (i najczęściej nie są) najlepsze, jeśli porównamy je z optymalnymi marszrutami wypracowanymi przez algorytm *interdomain* („widzący" całą strukturę sieci).

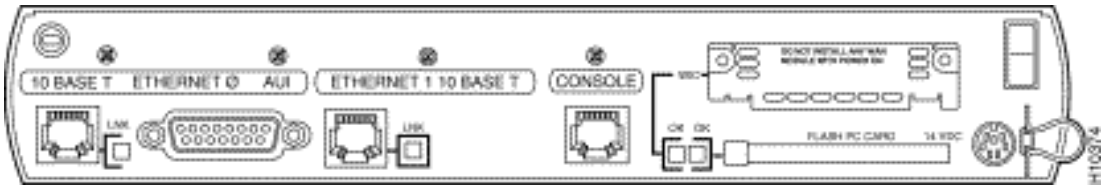
1.3.6 Algorytm link state i distance vector

Algorytm *link state* (znany jako *shortest path first*) rozsyła informacje routingu do wszystkich węzłów obsługujących połączenia międzysieciowe. Każdy router wysyła jednak tylko tę część tabeli routingu, która opisuje stan jego własnych łączy. Algorytm *distance vector* (znany też pod nazwą *Bellman-Ford*) wysyła w sieć całą tabelę routingu, ale tylko do sąsiadujących z nim routerów. Mówiąc inaczej, algorytm *link state* rozsyła wszędzie, ale za to niewielkie, wybrane porcje informacji, podczas gdy *distance vector* rozsyła komplet informacji, ale tylko do najbliższych węzłów sieci. Każdy z algorytmów ma swoje wady i zalety. *Link state* jest skomplikowany i trudny do konfigurowania oraz wymaga obecności silniejszego procesora CPU. Odnotowuje za to szybciej wszelkie zmiany zachodzące w topologii sieci. *Distance vector* nie pracuje może tak stabilnie, ale jest za to łatwiejszy do implementowania i sprawuje się dobrze w dużych sieciach składających się z kilkudziesięciu czy nawet kilkuset routerów.

2 PODSTAWOWA KONFIGURACJA ROUTERÓW

2.1 Pierwsze kroki w konfiguracji

Wszystkie urządzenia systemu IOS są konfigurowane przez producenta w minimalny sposób. Dla routerów i serwerów dostępowych Cisco dostarcza minimalną konfigurację, która od użytkownika wymaga zaledwie podania danych wejściowych, aby urządzenia zaczęły pełnić swoje funkcje. Po otrzymaniu routera bądź serwera dostępowego, wszystkie interfejsy urządzenia będą wyłączone lub administracyjnie niedostępne.
Aby skonfigurować urządzenie Cisco, najpierw należy podłączyć je do źródła zasilania i odszukać włącznik umieszczony na tylnej ściance urządzenia. Po włączeniu zasilania (przycisk często oznaczony numerem 1), urządzenie zacznie działać i zaświecą się diody stanu na przednim panelu. Wyjątkiem od tej reguły jest popularna seria routerów Cisco 2500. Routerów tej serii mają tylko jedna diodę stanu, umieszczoną z tyłu, blisko pomocniczego portu konsoli (AUX).



Rys. 1 Tylna ścianka routera Cisco 1605R

Następnym etapem konfiguracji urządzenia jest znalezienie portu konsoli (patrz rys. 1). Każde urządzenie firmy Cisco ma port konsoli, który umożliwia dostęp do niego za pośrednictwem terminalu. Port konsoli to często port RS-232C lub RJ-45, oznaczony jako „Console". Po zlokalizowaniu portu konsoli trzeba podłączyć do niego dedykowany terminal lub komputer osobisty z emulatorem terminalu. Cisco dostarcza kable niezbędne do połączenia portu konsoli z każdym urządzeniem. Używając dedykowanego terminalu, można jego złącze RS-232C podłączyć do kabla RJ-45, a następnie dołączyć tę konstrukcję bezpośrednio do urządzenia. Z routerem można podłączyć terminal znakowy lub komputer z emulatorem terminala (np. HyperTerminal w systemach Windows). Za pomocą terminala administrator może przeprowadzić proces konfiguracji routera. Pamiętać należy, iż poprawna komunikacja z routerem wymaga ustawienia odpowiednich parametrów transmisyjnych terminala - zwykle stosuje się: terminal typu VT100, prędkość 9600 (chociaż w rejestr routera można wpisać inną wartość), 8 bitów danych, 1 bit stopu, transmisję bez parzystości [3].
Jeśli te ustawienia są prawidłowe, można włączyć urządzenie. Pojawi się komunikat podobny do poniższego kodu, generowanego przez router Cisco serii 1600:

```
System Bootstrap, Version 12.0(3)T, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
C1600 platform with 12288 Kbytes of main memory
program load complete, entry point: 0x4020060, size: 0x165eac
%SYS-6-BOOT_MESSAGES: Messages above this line are from the boot loader.
program load complete, entry point: 0x2005000, size: 0x357236
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) 1600 Software (C1600-SY-M), Version 12.1(3), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Wed 05-Jul-00 10:52 by cmong
Image text-base: 0x02005000, data-base: 0x026FF050
cisco 1605 (68360) processor (revision C) with 11776K/512K bytes of memory.
Processor board ID 21858232, with hardware revision 00000003
Bridging software.
X.25 software, Version 3.0.0.
2 Ethernet/IEEE 802.3 interface(s)
1 Serial(sync/async) network interface(s)
System/IO memory with parity disabled
8192K bytes of DRAM onboard 4096K bytes of DRAM on SIMM
System running from RAM
7K bytes of non-volatile configuration memory.
4096K bytes of processor board PCMCIA flash (Read/Write)
```

Jeśli terminal lub emulator terminalu nie wyświetli żadnego komunikatu, należy sprawdzić połączenie oraz prawidłowość ustawień terminala. Można także odwołać się do przewodnika *Getting Started Guide* dołączonego do każdego urządzenia firmy Cisco.

2.2 Dialog konfiguracyjny

Dialog konfiguracyjny to interaktywna sekwencja pytań i odpowiedzi, pozwalających utworzyć pierwszą, bazową konfigurację routera. Dialog wywoływany jest również w przypadku usunięcia zawartości pamięci NVRAM lub po uruchomieniu routera w specjalnym trybie naprawczym z pominięciem odczytywania pamięci NVRAM. Administrator pracujący w trybie uprzywilejowanym może także w dowolnej chwili uruchomić dialog konfiguracyjny poleceniem SETUP. Zbiór parametrów, jakie można ustawić bezpośrednio w dialogu konfiguracyjnym, zależy od modelu routera i wersji systemu operacyjnego [4]. Poniżej przedstawiony jest przykładowy dialog konfiguracyjny dla routera 1605, w którym ustawiamy nazwę routera i hasła.

```
Would you like to enter basic management setup? [yes/no]: ?
% Please answer 'yes' or 'no'.
Would you like to enter basic management setup? [yes/no]: y
Configuring global parameters:

  Enter host name [Router]: Cisco

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: asia100
```

```
  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: asia100
% Please choose a password that is different from the enable secret
  Enter enable password: asia200

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: asia300
```

Pierwsze hasło, oznaczone jako **enable secret**, chroni dostępu do trybu uprzywilejowanego, w którym administrator może uruchamiać wszystkie polecenia, a także przeprowadzać dowolne zmiany konfiguracyjne. Konieczność zabezpieczania tego trybu przed nieautoryzowanym dostępem jest więc bezdyskusyjna. Hasło enable secret przechowywane jest w postaci zaszyfrowanej. Aby zapewnić zgodność z wcześniejszymi wersjami systemu operacyjnego, w dialogu konfiguracyjnym pozostawiono możliwość zdefiniowania również hasła **enable password.** Hasło to także chroni dostępu do trybu uprzywilejowanego, ale jest wykorzystywane tylko w starszych wersjach systemu oraz wtedy, gdy hasło enable secret nie jest zdefiniowane. Ponieważ enable password przechowywane jest w postaci niezaszyfrowanej, zalecane jest stosowanie enable secret. Trzecim wymagane hasło chroni dostępu do routera poprzez linie terminali wirtualnych VTY, zwykle są to połączenia z wykorzystaniem protokołu telnet. Standardowo router udostępnia pięć linii wirtualnych VTY. Należy zauważyć, że domyślnie dostęp do routera poprzez linię konsoli nie jest zabezpieczany żadnym hasłem.[4]
Po określeniu haseł, w dialogu konfiguracyjnym pojawia się możliwość zdefiniowania społeczności protokołu SNMP, w której pracować będzie router. Domyślnie proponowana jest społeczność Public i początkowo można tę nazwę pozostawić bez zmiany. Właściwe zdefiniowanie społeczności może mieć duże znaczenie dla pracujących w trybie graficznym programów do zdalnego zarządzania routerem, które działanie opierają na protokole SNMP. Kolejne pytania dialogu konfiguracyjnego dotyczą protokołów routingu dynamicznego, takich jak RIP czy IGRP. Można początkowo pozostawić proponowane, domyślne ustawienia lub wyłączyć routing dynamiczny.
Ostatnia sekcja dialogu konfiguracyjnego pozwala w pętli zdefiniować parametry dotyczące poszczególnych interfejsów routera, np.: adres IP czy maska podsieci. Po udzieleniu odpowiedzi na wszystkie pytania pojawia się możliwość przejrzenia zdefiniowanych ustawień oraz zapamiętania konfiguracji startowej w pamięci NVRAM. Odpowiednia opcja w menu wyboru pozwala opuścić dialog konfiguracyjny bez zapamiętywania zmian [4].
Następny etap w trybie Systems Configuration Dialog wymaga ustawienia parametrów protokołów. W tym momencie należy uruchomić Simple Network Management Protocol (SNMP). Na razie wystarczy włączyć SNMP i zaakceptować domyślny łańcuch dla opcji *public:*

```
Configure SNMP Network Management? [yes]: yes
Community string [public]: public
```

System teraz wyświetli zestawienie wszystkich portów routera:

```
Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration

Interface              IP-Address      OK? Method Status                Protocol
Ethernet0              unassigned      NO  unset  down                  down
Ethernet1              unassigned      NO  unset  down                  down
Serial0                unassigned      NO  unset  down                  down
```

Powyższe zestawienie interfejsów dotyczy urządzenia Cisco „prosto z fabryki", dlatego wszystkie interfejsy są przedstawione jako nieskonfigurowane (wskazuje na to wartość NO w kolumnie OK?). Interfejsy nie mają także przypisanych adresów IP, stąd kolumna IP-Address zawiera wartości **unassigned** dla każdego z interfejsów. Kolumna Method dotyczy sposobu konfiguracji interfejsu, którą można przeprowadzić ręcznie bądź automatycznie z sieci. W tej chwili interfejsy nie są skonfigurowane. Ostatnie dwie kolumny dotyczą stanu interfejsu oraz protokołu warstwy łącza danych, związanego z danym interfejsem. Domyślnie w nowym urządzeniu wszystkie interfejsy rozpoczynają od stanu **down** (wyłączony) oraz nieokreślonymi **(down)** nazwami protokołów warstwy łącza danych [1].

Teraz należy wybrać interfejs do SNMP:

```
Enter interface name used to connect to the
management network from the above interface summary: Ethernet0
Configuring interface Ethernet0:
Configure IP on this interface? [yes]:
IP address for this interface: 212.182.41.14
Subnet mask for this interface [255.255.255.0] : 255.255.255.192
Class C network is 212.182.41.0, 26 subnet bits; mask is /26
```

Teraz system wyswietli konfigurację routera:

```
The following configuration command script was created:
hostname Cisco
enable secret 5 $1$eEQz$AKxn/474WrYqxhRWy0IPT1
enable password asia200
line vty 0 4
password asia300
snmp-server community public
!
no ip routing
!
interface Ethernet0
no shutdown
ip address 212.182.41.14 255.255.255.192
!
interface Ethernet1
shutdown
no ip address
!
interface Serial0
shutdown
no ip address
!
end

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]: 1
```

Po wyświetleniu powyższego tekstu można teraz zachować konfigurację routera w pamięci NVRAM wybierając opcję 2.

2.3 System pomocy

System pomocy IOS dostępny jest w trybie EXEC, co pomaga w wydawaniu poleceń urządzeniu. System ten jest kontekstowy, co oznacza, że proponowana pomoc zależy od tego, co chcesz zrobić w systemie IOS. Na przykład po wprowadzeniu w wierszu poleceń znaku zapytania (?), pojawi się następująca informacja:

```
C1600>?
Exec commands:
  access-enable      Create a temporary Access-List entry
  access-profile     Apply user-profile to interface
  clear              Reset functions
  connect            Open a terminal connection
  disable            Turn off privileged commands
  disconnect         Disconnect an existing network connection
  enable             Turn on privileged commands
  exit               Exit from the EXEC
  help               Description of the interactive help system
  lock               Lock the terminal
  login              Log in as a particular user
  logout             Exit from the EXEC
  mrinfo             Request neighbor and version information from a multicast
                     router
  mstat              Show statistics after multiple multicast traceroutes
  mtrace             Trace reverse multicast path from destination to source
  name-connection    Name an existing network connection
  pad                Open a X.29 PAD connection
  ping               Send echo messages
  ppp                Start IETF Point-to-Point Protocol (PPP)
  resume             Resume an active network connection
  rlogin             Open an rlogin connection
  show               Show running system information
  slip               Start Serial-line IP (SLIP)
  systat             Display information about terminal lines
  telnet             Open a telnet connection
  terminal           Set terminal line parameters
  traceroute         Trace route to destination
  tunnel             Open a tunnel connection
  where              List active connections
  x28                Become an X.28 PAD
  x3                 Set X.3 parameters on PAD
```

Polecenia systemu IOS są wyszczególnione po lewej stronie ekranu, natomiast krótki opis każdego z nich umieszczony jest po prawej stronie ekranu. Niektóre polecenia składają się z jednego słowa: system pomocy informuje o tym, pokazując, że jedyną możliwością wydania polecenie jest wpisanie go i naciśnięcie klawisza Enter lub Return (<cr> to znak powrotu karetki):

```
C1600>lock ?
<cr>
C1600>lock
```

Podczas korzystania z systemu pomocy system IOS nie wymaga powtarzania pole cenią po wyświetleniu ekranu pomocy. W powyższym przykładzie słowo **lock** zostało automatycznie powtórzone przez system po pojawieniu się ekranu pomocy [1].

System pomocy można także wykorzystać do odszukania zestawu opcji dla danego polecenia trybu EXEC. IOS udostępnia wiele poleceń, które pokazują aktualny stan urządzenia. Sporo z nich rozpoczyna się od słowa **show.** W poniższym listingu jest fragment dostępnych opcji możliwych do wprowadzeniu po słowie **show:**

```
C1600>show ?
alps      alps Information
backup backup Status
bootflash:        display Information about bootflash: file
bootvar boot and related environment variable
calendar          display the hardware calendar
```

2.4 Tryb uprzywilejowany i nieuprzywilejowany

W trybie EXEC można wydawać dwa rodzaje poleceń: pierwszy rodzaj to polecenia wydawane w trybie nieuprzywilejowanym. W wierszu poleceń jest on oznaczony znakiem większości (>) po nazwie urządzenia, na przykład:

```
Cisco>
```

W tym trybie można sprawdzać stan urządzenia IOS, ale nie można zmieniać jego parametrów. Drugi rodzaj stanowią polecenia w trybie uprzywilejowanym znanym także jako *enable mode.* Aby wejść w tryb uprzywilejowany, trzeba znać hasło **enable secret** dla systemu. Wtedy można wprowadzić polecenie trybu EXEC, **enable,** które przełączy system z trybu nieuprzywilejowanego do uprzywilejowanego:

```
Cisco>enable
Password:
Cisco#
```

W powyższym przykładzie, wprowadzane hasło enable secret (w tym przypadku **asia100),** nie jest wyświetlone na ekranie terminalu. Urządzenie w trybie uprzywilejowanym zmienia znak większości (>) w wierszu poleceń na znak krzyżyka (#). Aby przejść z powrotem w tryb nieuprzywilejowany, trzeba użyć polecenia trybu EXEC **disable:**

```
Cisco#disable
Cisco>
```

2.5 Konfigurowanie pamięci

Pamięć urządzenia IOS dzieli się na trzy części, z których dwie przechowują konfigurację urządzenia, a trzecia IOS. Różnica między poleceniami konfiguracyjnymi a IOS jest taka, że polecenia są używane do konfigurowania urządzenia, natomiast IOS to oprogramowanie, które zarządza jego pracą.
W tym podrozdziale omówione zostaną oba typy pamięci, które przechowują polecenia konfiguracyjne IOS - pamięć o dostępie swobodnym (ang. *random-acces memory),* czyli RAM, oraz pamięć trwałą RAM (ang. *nonvolatile random-access memoiy),* czyli NVRAM. Opisany zostanie także sposób, jak załadować IOS do trzeciego typu pamięci urządzenia – pamięci stałej programowanej elektronicznie, która może być wymazywana i przeprogramowana (ang. *electronically erasable programmable read-only memory,* czyli EEPROM), znana także jako pamięć typu Flash. Polecenia związane z pamięcią w urządzeniu można uruchomić tylko w trybie uprzywilejowanym (co zilustrują poniższe przykłady) [1].

2.5.1 Pamięć konfiguracyjna urządzenia

Bieżącą (działającą) konfigurację urządzenia IOS można zobaczyć używając polecenia trybu EXEC **show running-config.** Rezultat tego polecenia wyszczególnia polecenia konfiguracyjne IOS, dla danego urządzenia:

```
Cisco#show running-config
Current configuration:

hostname Cisco
enable secret 5 $1$eEQz$AKxn/474WrYqxhRWy0IPT1
enable password asia200
line vty 0 4
password asia300
snmp-server community public
!
no ip routing
!
interface Ethernet0
no shutdown
ip address 212.182.41.14 255.255.255.
```

Komunikat został skrócony w celu zachowania przejrzystości.
Bieżąca konfiguracja (ang. *running-config)* urządzenia przechowywana jest w pamięci RAM, która jest wymazywana, jeśli urządzenie utraci zasilanie. Aktualną konfigurację należy zapisać w pamięci NVRAM, gdzie zyska ona status konfiguracji startowej (ang. *startup-config),* jeśli po powtórnym włączeniu zasilania urządzenie ma mieć taką samą konfigurację. Polecenie trybu EXEC **copy,** które kopiuje dane z pierwszej lokalizacji pamięci do drugiej, służy do zapisywania bieżącej konfiguracji w pamięci NVRAM:

```
Cisco#copy runninq-confia startup-config
[OK]
Cisco#
```

Zapisano tu bieżącą konfigurację z pamięci RAM jako konfigurację startową w pamięci NVRAM. Polecenia **copy** można użyć także w odwrotny sposób, czyli skopiować konfigurację startową do konfiguracji bieżącej:

```
Cisco#copy startup-config running-config
[OK]
Cisco#
```

Kiedy to się przydaje? Wtedy, gdy chcemy przywrócić konfigurację startową, bo wprowadzone zmiany do konfiguracji urządzenia okazały się niekorzystne. Jeśli bieżąca konfiguracja nie została skopiowana do konfiguracji startowej, teraz można skopiować konfigurację startową do bieżącej. Podczas kopiowania konfiguracji startowej z pamięci NVRAM do konfiguracji bieżącej w pamięci RAM, trzeba pamiętać, że może nastąpić scalanie poleceń konfiguracyjnych IOS omówione to zostanie w dalszej części pracy [1].
Aby przejrzeć konfigurację startową, wprowadzamy polecenie trybu EXEC **show startup-config:**

```
Cisco#show startup-config
```

Po wykonaniu polecenia **copy running-config startup-config** konfiguracja startowa jest identyczna z bieżącą. Jeżeli jednak skonfigurujemy urządzenie (co omówiono w następnej części) i nie zapiszemy bieżących ustawień jako startowych, po następnym włączeniu urządzenie przywraca ostatnią zapisaną konfigurację.

Konfigurację startową można wymazać poleceniem **erase startup-config:**

```
Cisco#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]  '
Cisco#
```

Jeśli teraz zrestarujemy router, wyłączając i włączając zasilanie bądź korzystając z polecenia trybu EXEC **reload,** konfiguracja startowa urządzenia przestanie istnieć. Taka kolejność wydarzeń - wymazanie konfiguracji startowej i ponowne uruchomienie urządzenia - spowoduje, że urządzenie IOS rozpocznie pracę od trybu System Configuration Dialog (Dialog konfiguracyjny), omówionego wcześniej.

2.5.2 Pamięć typu Flash

W pamięci typu Flash urządzenie Cisco przechowuje binarne, wykonywalne obrazy IOS, które składają się na system operacyjny urządzenia. Nie należy mylić obrazów IOS z konfiguracjami IOS. Konfiguracja IOS podaje urządzeniu bieżące ustawienie, podczas gdy obraz IOS to rzeczywisty binarny program, który je przekształca i wykonuje.
Zależnie od wielkości zainstalowanej pamięci typu Flash oraz rozmiaru obrazu IOS, urządzenie może przechowywać wiele obrazów IOS. Jeśli w danym urządzeniu znajduje się wiele obrazów IOS, można określić, który z nich zostanie uruchomiony po restarcie urządzenia. Obrazy IOS otrzymane od firmy Cisco można skopiować do urządzeń używając protokołów przesyłania plików opartych na TCP/IP: Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP) oraz protokołu zdalnego kopiowania systemu UNIX (rep). Omówione zostanie wykorzystanie protokołu FTP.[1]
W celu wysłania obrazu programu IOS protokół FTP wymaga podania nazwy użytkownika oraz hasła do identyfikacji i uwierzytelnienia urządzenia IOS, jak również administratora serwera FTP. Aby podać nazwę użytkownika i hasło, można wykorzystać dwie metody:

- wskazać nazwę użytkownika i hasło jako część polecenia trybu EXEC **copy ftp,**
- wstępnie zdefiniować nazwę użytkownika i hasło globalnym poleceniem konfiguracyjnym **ip ftp username** i **ip ftp password.**

Pierwsza metoda wykorzystywana jest wtedy, gdy wielu użytkowników aktualizuje obraz programu na routerze. Z kolei druga metoda jest użyteczna, kiedy tylko jeden użytkownik dokonuje aktualizacji albo, kiedy specyficzne konto logowania oraz hasło zostały ustawione wyraźnie w celu wysyłania obrazów programu IOS. W obu przypadkach odpowiednia nazwa użytkownika i hasło muszą się znaleźć na serwerze FTP jeszcze przed zainicjowaniem transferu. Zanim będzie można wysłać obraz IOS do urządzenia, jego plik należy umieścić na serwerze. Następnie używa się uprzywilejowanego polecenia trybu EXEC **copy ftp://username:password flash,** aby wskazać nazwę użytkownika oraz hasło w celu uwierzytelnienia i zainicjowania transferu. Przyjmując naszą nazwę użytkownika i hasło, polecenie będzie wyglądało następująco: **copy ftp://piotrek:haselko flash.** Router pokazuje bieżącą zawartość pamięci podręcznej, a następnie, przed zatwierdzeniem procesu kopiowania, prosi o adres IP serwera FTP oraz nazwę obrazu IOS. Opcjonalnie adres IP serwera FTP oraz nazwa obrazu IOS mogą także zostać wskazane jako część polecenia **copy,** podobnie jak nazwa użytkownika i hasło. Polecenie przyjmie wtedy formę: **ftp://username:password@ftpservername/ios-image-name.** Na koniec urządzenie sprawdzi, czy plik został załadowany bezbłędnie.
Możliwe jest wykonanie operacji odwrotnej do powyższego procesu - skopiowanie obrazu IOS z pamięci podręcznej urządzenia do serwera FTP -poleceniem trybu EXEC **copy flash ftp.** Tak jak w poprzednim procesie, trzeba wskazać nazwę użytkownika i hasło niezbędne do transferu FTP. Wartości te można wskazać jako część polecenia **copy** albo wstępnie zdefiniować je w bieżącej konfiguracji. Aktualizując obrazy IOS należy zawsze mieć na serwerze kopię ostatniej

działającej konfiguracji. Takie zabezpieczenie umożliwia w przypadku awarii przywrócenie działającego obrazu IOS poleceniem **copy ftp flash.**

2.6 Tryb konfiguracji użytkownika

Aby skonfigurować urządzenie IOS, trzeba użyć uprzywilejowanego polecenia trybu EXEC **configure.** Polecenie **configure** ma trzy opcje:

- Terminal (metoda domyślna) - konfiguracja ręczna poprzez wykonywanie poszczególnych poleceń z poziomu terminala,
- Memory - wczytanie pełnej konfiguracji z pamięci NVRAM (konfiguracja startowa) do pamięci RAM,
- Network - wczytanie skryptu konfiguracyjnego z serwera sieciowego TFTP.

Po wejściu do trybu konfiguracyjnego z opcją domyślną zmienia się odpowiednio znak zachęty, zgodnie z notacją: Nazwa_routera(config)#. Wyróżniamy trzy rodzaje poleceń konfiguracyjnych: globalne, główne i podpolecenia. Komendy globalne, zapisywane w pojedynczej linii, definiują parametry dotyczące pracy routera jako całości [1]. Poniżej przedstawione są trzy przykłady poleceń globalnych, definiujących odpowiednio: logiczną nazwę routera, hasło chroniące dostęp do trybu uprzywilejowanego (przechowywane w postaci zaszyfrowanej) i routing dla protokołu IP:

```
Cisco(config)#hostname C1600
C1600(config)#enable secret password
C1600(config)#ip routing
```

Polecenia główne nie definiują bezpośrednio żadnych parametrów routera, lecz wyróżniają konkretny proces lub interfejs, który ma podlegać dalszej konfiguracji. Dostępnych jest ponad 17 specyficznych trybów konfiguracyjnych, wybieranych poleceniami głównymi. Poniższe dwa przykładowe polecenia główne wybierają odpowiednio interfejs Ethernet0 oraz protokół routingu dynamicznego IGRP [4]. Zauważyć należy, że wykonanie polecenia głównego, poza zmianą znaku zachęty wskazującego wybrany proces, nie powoduje praktycznych zmian w konfiguracji:

```
C1600(config)#interface Ethernet0
C1600(config-if)#

C1600(config)#router IGRP 10
C1600(config-router)#
```

Właściwą konfigurację procesu czy interfejsu wybranego poleceniem głównym przeprowadza się, podając w kolejnych liniach podpolecenia. Polecenie główne musi mieć przynajmniej jedno podpolecenie. Listę specyficznych dla danego trybu podpoleceń można wyświetlić, wciskając znak "?". Na przykład podpolecenie definiujące tekstowy opis dla interfejsu Ethernet0 wygląda następująco:

```
C1600(config)#interface Ethernet0
C1600(config-if)#description Pierwszy segment sieci lokalnej
```

Zmiany przeprowadzane w trybie konfiguracyjnym dotyczą zawsze konfiguracji aktualnej, przechowywanej w pamięci RAM. Aby zmiany te utrwalić, należy nagrać konfigurację aktualną w pamięci nieulotnej NVRAM jako konfigurację startową. W tym celu wykonujemy polecenie:

```
C1600#copy running-config startup-config
```

Zarówno konfigurację aktualną, jak i startową można w dowolnej chwili wyświetlić na ekranie za pomocą odpowiedniej składni polecenia show. W poniższych przykładach wyświetlana jest

konfiguracja aktualna i startowa, zwana też czasami konfiguracją zapasową. Warto zwrócić uwagę na skrótowy zapis w drugim przykładzie:

```
C1600#show running-config
C1600#sh start
```

Skrypt konfiguracyjny odczytywany przy każdym uruchomieniu routera z pamięci NVRAM może być także przechowywany i pobierany z zewnętrznego serwera sieciowego, np. z serwera TFTP. Dzięki temu możliwe jest przygotowanie i publikowanie na niezależnym serwerze sieciowym wzorcowego zbioru konfiguracyjnego dla oryginalnego routera bądź wielu routerów podobnych.
Przechowywanie skryptu konfiguracyjnego na serwerze TFTP ułatwia też jego edycję przy użyciu dowolnego edytora tekstowego (np. WordPad). Przydaje się to szczególnie wtedy, gdy często modyfikujemy złożone polecenia konfiguracyjne.
Plik konfiguracyjny na serwerze TFTP tworzymy najczęściej nie od podstaw, lecz przez zapamiętanie na serwerze sieciowym aktualnej konfiguracji. W tym celu wykonujemy następującą komendę:

```
C1600#copy running-config tftp
```

Aby powyższe polecenie zadziałało poprawnie, określić należy prawidłowy adres IP serwera TFTP oraz nazwę pliku, w którym nagrana zostanie aktualna konfiguracja. W zależności od stosowanej usługi TFTP najczęściej możliwe jest podawanie również pełnej ścieżki do pliku. Przykład procedury nagrywania aktualnej konfiguracji na serwerze TFTP przedstawiony jest poniżej:

```
C1600#copy running-config tftp
Remote host []? 212.182.41.14
Name of configuration file to write [c1600-confg]? /1600/c1600-confg
Write file /1600/c1600-confg on host 212.182.41.14? [confirm]
Building configuration...
Writing /1600/c1600-confg !! [OK]
C1600#
```

Jeśli konieczne jest wprowadzenie zmian w skrypcie konfiguracyjnym, otwieramy plik zapamiętany na serwerze TFTP w odpowiednim edytorze tekstowym i poddajemy go dalszej edycji. Jeśli pojawi się konieczność pobrania wzorcowego pliku konfiguracyjnego zapamiętanego na serwerze TFTP, wykonujemy następujące polecenie, podając odpowiednie parametry, podobnie jak w poprzednim przykładzie:

```
C1600#copy tftp running-config
```

Jeżeli zachodzi taka konieczność, można zastąpić konfigurację startową przechowywaną w pamięci NVRAM, nadpisując ją plikiem konfiguracyjnym z serwera TFTP:

```
C1600#copy tftp startup-config
```

Wczytując plik konfiguracyjny z serwera TFTP do pamięci NVRAM, nadpisujemy w całości konfigurację startową. Natomiast pobierając skrypt z serwera TFTP do pamięci RAM, wykonujemy poszczególne polecenia linia po linii - w tej sytuacji konfiguracja aktualna nie zostanie nadpisana. W przypadku poleceń wykluczających się, są one nadpisywane (np. nazwa routera musi być tylko jedna). Niektóre polecenia mogą się logicznie sumować, a nie nadpisywać (np. router może należeć do dwu społeczności protokołu SNMP - jedna zdefiniowana w konfiguracji aktualnej, a druga w pliku na serwerze TFTP).
Należy pamiętać o tym, że jeżeli w pliku konfiguracyjnym na serwerze TFTP nie występuje jakieś polecenie, to nie znaczy, że będzie ono usunięte z konfiguracji aktualnej (np. jeżeli w pliku

na serwerze TFTP nie podano komendy shutdown, polecenie to pozostanie, jeśli było zdefiniowane wcześniej, w aktualnej konfiguracji interfejsu) [4].

3 KONFIGURACJA INTERFEJSÓW ROUTERA

Jednym z pierwszych zadań konfiguracyjnych, jakie wykonać musi administrator nowego routera, będzie właściwe zdefiniowanie parametrów komunikacyjnych dla poszczególnych interfejsów - zarówno tych dotyczących segmentów sieci lokalnej, jak i interfejsów szeregowych, wykorzystywanych najczęściej do połączeń w sieci WAN. Dla interfejsów sieci LAN, takich jak Ethernet, zwykle wystarczające jest zdefiniowanie parametrów dotyczących adresowania w protokole warstwy sieciowej (np. IP) oraz odwołanie domyślnie włączonego polecenia shutdown, które blokuje pracę interfejsu. Czynności te mogą być niepotrzebne, jeśli interfejs skonfigurowano z poziomu dialogu konfiguracyjnego [4].

3.1 Interfejsy LAN

Poniższa sekwencja poleceń pokazuje wywołanie trybu konfiguracyjnego, wybór właściwego interfejsu, przypisanie adresu IP i maski podsieci do interfejsu Ethernet0, Ethernet1 oraz wyłączenie polecenia shutdown blokującego interfejs. Na przykładzie polecenia shutdown warto zwrócić uwagę na sposób odwoływania poleceń przez wykorzystanie komendy no, dopisywanej na początku oryginalnej linii.

```
C1600#configure terminal
C1600(config)#interface Ethernet0
C1600(config-if)#ip address 212.182.41.1 255.255.255.0
C1600(config-if)#no shutdown
C1600(config-if)#interface Ethernet1
C1600(config-if)#ip address 212.182.41.65 255.255.255.0
C1600(config-if)#no shutdown
```

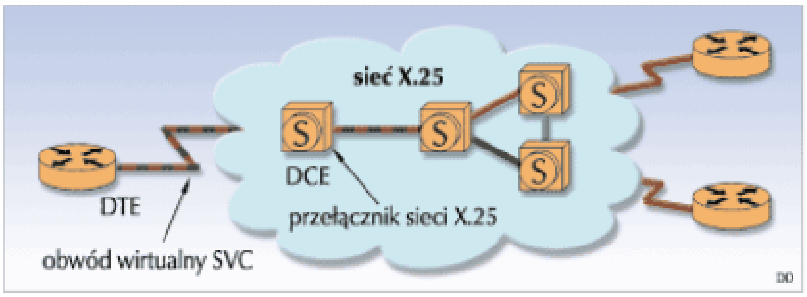
W niektórych sytuacjach może okazać się konieczne przypisanie do jednego interfejsu więcej niż jednego adresu IP. Dzieje się tak na przykład wtedy, gdy router obsługuje kilka wirtualnych sieci IP w jednym segmencie fizycznym. Polecenie dodające do interfejsu kolejny adres IP (drugi, trzeci itd.) ma składnię:

```
C1600(config-if)#ip address 212.182.40.23 255.255.255.128 secondary
```

3.2 Wielopunktowe interfejsy WAN

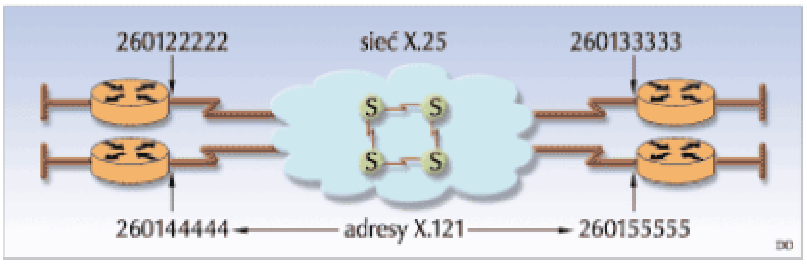
3.2.1 Sieć X.25

X.25 to jeden z najstarszych standardów sieci rozległej, wspierany przez Międzynarodową Unię Telekomunikacyjną (ITU). Wprawdzie posługujemy się określeniem protokół X.25, ale w zasadzie należy używać pojęcia stos X.25, gdyż jest to grupa protokołów umiejscowiona w trzech dolnych warstwach modelu OSI. Sieć X.25 nazywana jest siecią pakietową, gdyż komunikacja w niej opiera się na przełączaniu pakietów zmiennej długości (w przeciwieństwie do przełączania komórek o stałym rozmiarze), a realizowana jest poprzez połączenia wirtualne (rys. 2). Wymiana danych między dwoma urządzeniami wymaga wcześniejszego zestawienia obwodu wirtualnego, czyli wyznaczenia przez przełączniki trasy, którą wysłane zostaną wszystkie pakiety [4].



Rys. 2 Obwody wirtualne w sieci X.25

Wyróżniamy dwa rodzaje obwodów wirtualnych: połączenia trwałe PVC oraz połączenia zestawiane SVC, które zrywane są po zakończeniu transmisji danych lub po pewnym czasie bezczynności. Pierwsze rozwiązanie jest droższe, a drugie bardziej czasochłonne. Protokół X.25 definiuje połączenie typu punkt-punkt między urządzeniami DTE i DCE - znaczenie obu urządzeń jest podobne, jak w przypadku warstwy fizycznej. Zwykle urządzeniem biernym DTE będzie interfejs szeregowy routera, natomiast urządzeniem aktywnym - modem dostawcy lub przełącznik brzegowy w sieci WAN.
Na pojedynczym interfejsie szeregowym można ustanowić wiele kanałów wirtualnych do urządzenia DCE, dzięki czemu możliwe jest tworzenie obwodów wirtualnych do wielu odbiorców jednocześnie. Trasy przekazywania pakietów w sieci rozległej dostawcy wyznaczane są przez przełączniki X.25, odpowiedzialne za wymianę danych między dwoma urządzeniami DTE.
Każde urządzenie pracujące w sieci X.25 musi mieć unikatowy adres, definiowany zgodnie ze standardem X.121 (ITU). Adres składa się z maksymalnie 14 cyfr dziesiętnych i ma znaczenie globalne w ramach danej sieci X.25 (rys. 3). Pierwsze trzy cyfry oznaczają kraj, czwarta definiuje konkretnego dostawcę w ramach kraju, natomiast pozostałe dziesięć cyfr przyznaje dostawca swojemu klientowi. Czasami dostawca przypisuje odbiorcy tylko ośmiocyfrowy numer, natomiast dwie ostatnie cyfry określa indywidualnie klient [4].



Rys. 3 Przykład adresowania X.121 w sieci X.25

Aby podłączyć router do sieci rozległej WAN z wykorzystaniem stosu protokołów X.25, należy rozpocząć konfigurację od włączenia właściwej hermetyzacji na poziomie interfejsu szeregowego. W trybie konfiguracji interfejsu wykonujemy polecenie **Encapsulation X25**, jeśli konfigurujemy interfejs szeregowy jako urządzenie DTE (sytuacja typowa), lub polecenie **Encapsulation X25 DCE** dla urządzenia DCE (np. podczas testów). Następnie nadajemy unikatowy (przyznany przez dostawcę) adres X25, zgodny ze standardem X.121, poleceniem: **X25 address x21_adres**. W przypadku kilku interfejsów szeregowych pracujących z protokołem X.25, każdy z nich musi mieć własny adres. Adresy sieci X.25 są zupełnie niezależne od adresów właściwych protokołów warstwy sieciowej, np. protokołu IP.
Dostawca może wymagać określenia maksymalnego rozmiaru wysyłanego i odbieranego pakietu dla protokołu PLP. Dopuszczalne rozmiary pakietu wahają się w granicach 16 - 4096 bajtów. Zwykle dostawcy korzystają z pakietów o rozmiarach 128 lub 256 bajtów. Dla interfejsów szeregowych routera Cisco domyślnie ustawiany jest maksymalny rozmiar pakietu na 128 bajtów. Pakiety przesyłane w sieci X.25, które przekraczają dopuszczalny rozmiar, muszą być dzielone na mniejsze części (oznaczane specjalnymi bitami flagowymi), a scalane są dopiero na

routerze odbierającym [4]. Poniższe polecenia ustalają maksymalny rozmiar pakietu wchodzącego i wychodzącego na 256 bajtów:

```
C1600(config-if)#x25 ips 256
C1600(config-if)#x25 ops 256
```

Protokoły sieci X.25 wyposażone są w silne procedury korekcji błędów, m.in. przesuwne okno transmisji danych. Rozmiar okna określa, ile pakietów może być jednorazowo wysyłanych przy pojedynczym potwierdzeniu - wielkość tę podaje się niezależnie dla okna wysyłania i okna odbierania danych. Maksymalny dopuszczalny rozmiar okna przy typowych ustawieniach wynosi siedem pakietów, a domyślnie ustawiany jest na dwa pakiety. Aby ustalić rozmiar okna nadawania i okna odbioru, należy w trybie konfiguracji interfejsu posłużyć się poleceniami: **X25 wout rozmiar i X25 win rozmiar**. Maksymalny rozmiar okna ustawiany jest poleceniem **X25 modulo parametr**, przy czym jako parametr podać można tylko dwie wartości: 8 lub 128. Domyślnie wybrana jest wartość 8, ale po wykonaniu polecenia **X25 modulo 128** można ustawić rozmiar okna na 127 pakietów.
Jednym z najważniejszych zadań podczas konfiguracji protokołu X.25 jest poprawne wskazanie routerów sąsiedzkich, czyli tych, z którymi ustanawiana jest komunikacja poprzez sieć X.25. Realizuje się to poprzez przyporządkowanie (odwzorowanie adresów) zdalnego adresu protokołu warstwy sieciowej (np.: IP, IPX, DECNET, APPLETALK) do zdalnego adresu urządzenia w sieci X.25 [4]. Składnia takiego polecenia jest następująca:

```
C1600(config-if)#X25 map protokół adres adres_x121 [opcje]
```

Parametr protokół oznacza protokół warstwy sieciowej (np. IP), pole adres to konkretny adres routera zdalnego dla wybranego protokołu, a adres_x121 oznacza adres routera zdalnego w sieci X.25. Typową opcją jest **broadcast** - jej włączenie spowoduje wysyłanie komunikacji rozgłoszeniowej przez wskazany interfejs do podanego adresu X121 (w danym połączeniu wirtualnym). W praktyce opcję **broadcast** stosuje się przy rozsyłaniu informacji związanych z protokołami routingu dynamicznego - zwykle mają one postać ruchu rozgłoszeniowego. Odwzorowanie adresów (mapping) opisujące zdalnych sąsiadów wpisywane jest ręcznie i ma postać statycznej tablicy, wypełnianej osobno dla każdego z protokołów warstwy sieciowej. Trzeba jednak dodać, że dla węzłów obsługujących hermetyzację wieloprotokołową zgodną z RFC1356 możliwe jest utworzenie odwzorowania adresów dla różnych protokołów sieciowych w pojedynczym zapisie, zgodnie ze składnią:

```
C1600(config-if)#X25 map protokół adres [protokół adres]
      * adres_x121 [opcje]
```

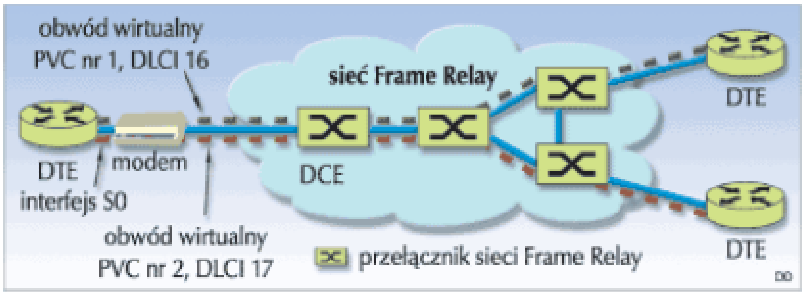
Symbol "*" oznacza, że w pojedynczej linii można podać do dziewięciu protokołów warstwy sieciowej rozdzielonych [4]. Poniżej przykład kompletnej konfiguracji interfejsu szeregowego Serial 0 routera Cisco 1600, przez który użytkownicy wielosegmentowej sieci lokalnej firmy uzyskują dostęp do Internetu, korzystając z usług dostawcy sieci X.25:

```
C1600(config-if)#encapsulation x25
C1600(config-if)#x25 address 26013456789876
C1600(config-if)#ip address 213.15.8.9 255.255.255.252
C1600(config-if)#x25 map ip 213.15.8.10 26019876543212
```

3.2.2 Sieć Frame Relay

Protokół X.25 opracowano dla sieci o dużej zawodności i dużej liczbie błędów transmisji, dlatego też poszczególne węzły na trasie pakietu mogły weryfikować transmitowane dane niezależnie: przez protokół warstwy sieciowej (PLP) oraz protokół warstwy łącza danych (LAPB). Specyfikacja Frame Relay powstała natomiast dla szybkich łączy o niewielkiej ilości błędów w

transmisji. Pozwoliło to zrezygnować ze złożonych procedur korekcji i retransmisji stosowanych w sieci X.25 i w efekcie znacznie przyspieszyć transmisję danych (w typowych rozwiązaniach nawet do 2 Mb/s na łączu do odbiorcy). Podobnie jak X.25, Frame Relay opisuje komunikację na styku między klientem a dostawcą usług sieci WAN. Urządzeniem klienckim DTE może być na przykład router Cisco, natomiast urządzeniem aktywnym DCE będzie zwykle przełącznik w sieci dostawcy (patrz Rys.4).



Rys. 4 Obwody wirtualne w sieci Frame Relay

Pojedynczy interfejs szeregowy routera Cisco pozwala zestawić wiele obwodów wirtualnych między routerem (DTE) i przełącznikiem brzegowym (DCE) w sieci WAN usługodawcy. Do identyfikacji poszczególnych obwodów służą numery DLCI (Data-Link Connection Identifier) - mają one znaczenie lokalne i w różnych częściach sieci Frame Relay mogą być podłączone do niej routery korzystające z tych samych numerów DLCI [4].
Podłączając router do sieci Frame Relay, należy w ramach konfiguracji interfejsu szeregowego ustawić właściwy typ hermetyzacji stosowany w fizycznym interfejsie, poprzez który router łączy się z siecią usługodawcy (zwykle przez modem):

```
C1600(config-if)#encapsulation frame-relay [cisco | ietf ]
```

Opcje cisco należy wybierać przy połączeniach z innym routerem firmy Cisco, natomiast opcję ietf dla połączeń z urządzeniami innych firm, wartością domyślną jest cisco. Następnie należy wybrać typ protokołu LMI:

```
C1600(config-if)#frame-relay lmi-type [ansi | cisco | q933a]
```

Domyślną wartością jest cisco. Warto pamiętać, że od wersji 11.2 systemu operacyjnego router próbuje dynamicznie wykryć typ protokołu LMI stosowany przez przełącznik Frame Relay - komenda ta może więc być niepotrzebna.
Zauważmy, że w tej konfiguracji nie jest konieczne określenie numeru DLCI - router pracuje jako urządzenie DTE, któremu brzegowy przełącznik Frame Relay (DCE) dynamicznie przypisuje numer DLCI. Jeżeli jednak dwa routery połączone są bezpośrednio poprzez interfejsy szeregowe (specjalną parą kabli DTE i DCE), to w ramach konfiguracji interfejsu, który będzie pełnił role urządzenia DCE, należy wykonać dodatkowe polecenia. Po pierwsze należy zdefiniować typ interfejsu jako DCE:

```
C1600(config-if)#frame-relay intf-type DCE
```

Oprócz opcji DCE można także wybrać DTE (wartość domyślna) oraz NNI (przy bezpośrednim połączeniu dwóch routerów pracujących jako przełączniki Frame Relay). Następnie należy określić numer DLCI, który będzie dynamicznie przydzielony urządzeniu DTE:

```
C1600(config-if)#frame-relay interface-dlci numer
```

Standardowo pakiety keepalive wysyłane są co 10 sekund, a komunikaty o stanie obwodów wirtualnych odbierane co 60 sekund (6 razy parametr keepalive). Zmienić to można poleceniem:

```
C1600(config-if)#keepalive ilość_sekund
```

Aby możliwe było komunikowanie się z innymi routerami podłączonymi do sieci Frame Relay, niezbędne jest powiązanie ich adresów sieciowych (np. IP) z numerami DLCI obwodów wirtualnych, przez które realizowana będzie transmisja. Podobnie jak w sieci X.25, proces ten nazywany jest odwzorowaniem (mapping) adresów lub w terminologii Microsoftu, mapowaniem. Adresy można przypisać statycznie (ręcznie), korzystając z polecenia **frame-relay map**, bądź dynamicznie (automatycznie) za pomocą protokołu Inverse ARP - to drugie rozwiązanie jest wygodniejsze i nie wymaga od administratora żadnej dodatkowej konfiguracji. W poniższym przykładzie przypisania statycznego router C1600 komunikuje się z zewnętrznym routerem o adresie 131.108.1.2, wykorzystując lokalny kanał logiczny DLCI 17. Dodatkowo w ramach tego połączenia włączono obsługę komunikacji rozgłoszeniowej (opcja broadcast) i ustawiono typ hermetyzacji (opcja ietf nadpisuje globalne ustawienie podane w poleceniu encapsulation frame-relay):

```
C1600(config-if)#frame-relay map IP 131.108.1.2 17 broadcast ietf
```

Ponieważ router może poprzez jeden interfejs fizyczny komunikować się z wieloma odbiorcami, konieczne jest ręczne utworzenie niezależnych (i statycznych) powiązań do wszystkich odbiorców [4].
Protokół Inverse ARP dynamicznie tworzy tablicę powiązań odległych adresów sieciowych z lokalnymi numerami DLCI, przez które adresy te są dostępne (odwzorowanie w sieci X.25 dotyczyło zdalnych adresów sieciowych i zdalnych adresów X.121). Protokół Inverse ARP jest domyślnie włączony, jeśli jednak został w ramach interfejsu wyłączony, można odblokować go komendą:

```
C1600(config-if)#frame-relay inverse-arp [protokół] [dlci]
```

Parametr protokół oznacza protokół warstwy sieciowej (np. IP, IPX, APPLETALK), natomiast dlci jest numerem kanału, przez który wysyłane będą komunikaty Inverse ARP.
Poleceniem show **frame-relay pvc** wyświetlić można: stan każdego skonfigurowanego połączenia oraz numer DLCI, wykorzystywany interfejs fizyczny, statystyki dotyczące transmisji danych oraz liczbę otrzymanych pakietów BECN i FECN informujących o przeciążeniach w sieci Frame Relay.
Komenda **show frame-relay map** pozwala zweryfikować zawartość tablicy, w której znajdują się powiązania adresów sieciowych (IP) odległych routerów i przypisanych im lokalnych numerów DLCI. Jeżeli stosowany jest protokół Inverse ARP, wpisy mają włączone opcje dynamic i broadcast [4].

4 KONFIGUROWANIE ROUTINGU IP

4.1 Polecenia konfiguracyjne routingu IP

Do włączenia routingu IP używa się globalnego polecenia konfiguracyjnego IOS **ip routing.** Program IOS domyślnie skonfigurowany jest do routingu IP w urządzeniach takich jak autonomiczne routery. Jednak jeśli routing IP został wyłączony w takim urządzeniu, trzeba włączyć go ponownie przed komutowaniem pakietów i włączeniem protokołów routingu. Niektóre urządzenia zintegrowane z routrami Cisco nie mają domyślnie włączonego routingu IP. W takim przypadku także należy użyć polecenia **ip routing** przed komutacją pakietów i uruchomieniem protokołów routingu [1].

```
C1600#conf t
C1600(config)#ip routing
C1600(config)#^Z
```

Po włączeniu routingu IP, można zbudować tablicę routingu do komutowania pakietów. Domyślnie, kiedy interfejs ma przypisany adres IP i jest włączony, to jego adres sieciowy zostanie umieszczony w tablicy routingu. Wszystkie działające interfejsy połączone z routerem są umieszczane w tablicy routingu. Dlatego też, jeśli w sieci jest tylko jeden router, ma on informacje na temat wszystkich sieci lub podsieci i nie trzeba konfigurować routingu statycznego czy też dynamicznego. Statyczne lub dynamiczne pozycje tablicy routingu są potrzebne tylko wtedy, gdy w sieci jest więcej niż jeden router.
Chcąc obejrzeć tablicę routingu używamy polecenia trybu EXEC **show ip route.** Wprowadzone bez parametrów wyświetli całą tablicę routingu. Polecenie **show ip route** dostarcza administratorowi sieci ogromną ilość danych. Jest kluczowym narzędziem określania ścieżki pakietu w sieci [1].

4.2 Routing statyczny

Jak wspomniano wcześniej, informacje na temat routingu statycznego mogą zostać wykorzystane do budowy tablicy routingu, a co za tym idzie, informacji n temat ścieżki sieciowej.
Do konfiguracji tras statycznych służy globalne polecenie konfiguracyjne **ip route**. Polecenie to przyjmuje kilka parametrów, parametrów tym:
- adres sieciowy i związaną z nim maskę sieci,
- informacje dotyczące miejsca, gdzie router powinien wysłać pakiety.

Informacje na temat celu, gdzie pakiet ma być dostarczony, mogą przybrać jedną z następujących form:
- konkretny adres IP następnego routera na ścieżce,
- adres sieci następnej trasy tablicy routingu, do której powinny być przekazane pakiety,
- bezpośrednio podłączony interfejs, umieszczony w sieci docelowej.

Pierwsza opcja jest dominującą metodą wprowadzania tras statycznych [1].

```
C1600#config t
C1600(config)#ip route 212.182.41.0 255.255.255.0 212.182.40.65
C1600(config)#^Z
```

Druga opcja jest użyteczna, gdy od pożądanego adresu sieciowego prowadzi wiele ścieżek. Jedną z zalet jest możliwość rozdzielenia ładunku ruchu na wiele ścieżek o podobnych parametrach, inną, że awaria jednej ze ścieżek powoduje przekierowanie ruchu na ścieżkę alternatywną [1].

```
C1600#config t
C1600(config)#ip route 212.182.41.0 255.255.255.0 212.182.40.0
C1600(config)#^Z
```

Ostatnia opcja jest najrzadziej używana. Wskazując bezpośrednio podłączony interfejs jako cel trasy, administrator sieci informuje, że urządzenia o adresach IP z tej sieci są połączone ze wskazanym interfejsem. W wyniku tego pakiety przeznaczone do adresów IP dla tej sieci muszą mieć swoje adresy IP przekształcone na adres łącza danych interfejsu określonego typu. W przypadku Ethernetu adres IP jest przekształcony na adres MAC [1].

```
C1600#config t
C1600(config)#ip route 212.182.41.0 255.255.255.0 Ethernet1
C1600(config)#^Z
```

4.3 Konfigurowanie protokołów routingu IP

4.3.1 Protokół RIP

Wersja l protokołu RIP to klasowy protokół routingu, który nie obsługuje rozgłaszania informacji na temat maski sieci. RIP w wersji 2 jest już protokołem bezklasowym, który umie obsłużyć CIDR, VLSM, podsumowanie tras oraz mechanizmy bezpieczeństwa wykorzystujące otwarty tekst i uwierzytelnianie MD5.
Konfiguracja protokołu routingu RIP składa się z trzech podstawowych etapów: zezwolenia routerowi na korzystanie z protokołu RIP, wyboru wersji tego protokołu, oraz wyboru adresów sieci i interfejsów, które zostaną zawarte w aktualizacjach routingu. Aby zezwolić routerowi na uruchomienie protokołu RIP, używamy głównego polecenia konfiguracyjnego **router rip.** Aby wskazać wersje, używamy podpolecenia konfiguracyjnego routingu IOS **version.** Polecenie version przyjmuje parametr l lub 2, zależnie od używanej wersji RIP. Jeśli nie wskaże się żadnej wersji, program IOS domyślnie uruchamia wersje l, ale odbiera aktualizacje dla obu [1]. W poniższym przykładzie uruchomiono protokół routingu i wskazano wersję protokołu RIP 2:

```
C1600#config t
C1600(config)#router rip
C1600(config-router)#version 2
```

Interfejsy oraz adresy sieci, które mają być zawarte w ogłoszeniach routingu RIP, określamy za pomocą polecenia konfiguracji routingu IOS **network.** Polecenie to jako parametr przyjmuje adres klasowej sieci, który ma być zawarty w aktualizacjach routingu. Polecenie **network** jest używane do identyfikowania tylko tych adresów IP sieci, które są bezpośrednio połączone z konfigurowanym routerem i mają być zawarte i uwzględnione routingu RIP. W aktualizacjach routingu zawarte są tylko interfejsy o adresach IP w zidentyfikowanej sieci [1].
Przypuśćmy, że router ma dwa interfejsy o adresach IP 212.182.41.1 i 212.182.41.65, oraz trzeci interfejs o adresie IP 213.23.45.67. Polecenie **network** 212.182.41.0 powoduje, że ogłoszenia routingu są wysyłane tylko do podsieci sieci 212.182.41.0. Żeby dołączyć aktualizacje routingu dla interfejsu 213.23.45.67, trzeba skonfigurować dodatkowe polecenia **network** 213.23.45.0**.**
Poniżej znajduje się przykład konfiguracji polecenia **network** wykorzystanego do dołączenia podsieci i interfejsów sieci:

```
C1600#config t
C1600 (config)#router rip
C1600 (config-router)#network 212.182.41.0
C1600 (config-router)#network 212.23.45.0
C1600 (config-router)#^Z
```

4.3.2 Protokół IGRP

Konfiguracja procesu routingu IGRP składa się z dwóch etapów: zezwolenia routerowi na uruchomienie IGRP oraz zidentyfikowania, które adresy sieciowe oraz interfejsy są zawarte w aktualizacjach routingu. Aby uruchomić IGRP, używamy polecenia **router igrp.** Polecenie to wymaga podania parametru nazywanego *identyfikatorem procesu.* Identyfikator procesu może być liczbą całkowitą z zakresu od l do 65535. Ponieważ w tym samym routerze może działać wiele procesów IGRP, identyfikator jest niezbędny do rozróżniania ich. Wiele procesów IGRP może działać w routerze, który łączy dwa oddziały firmy, z których oba chcą mieć własną administrację sieciową. Wszystkie routery w jednym oddziale mogą mieć ten sam identyfikator procesu IGRP [1].

Tak jak w przypadku RIP, do określenia interfejsów i adresów sieci, które mają być zawarte w ogłoszeniach routingu IGRP, służy polecenie konfiguracyjne **network.** Jako parametr przyjmuje ono adres klasowej sieci, który ma być zawarty w aktualizacjach routingu. Polecenie **network** jest używane do identyfikowania tylko tych adresów IP sieci, które są bezpośrednio połączone z konfigurowanym routerem, i które mają być zawarte w procesie routingu IGRP. W aktualizacjach routingu zawarte są tylko interfejsy z adresami IP w zidentyfikowanej sieci.
Jeśli router ma dwa interfejsy o adresach IP 212.182.41.65 i 212.182.41.1, oraz trzeci interfejs o adresie IP 213.23.45.67, polecenie **network 212.182.41.0** spowoduje, że ogłoszenia routingu będą wysyłane tylko o podsieciach sieci 212.182.41.0 i tylko do interfejsów 212.182.41.0. Żeby dołączyć aktualizacje routingu dla interfejsu znajdującego się w przestrzeni adresowej 213.23.45.0, trzeba wpisać dodatkowe polecenie **network 213.23.45.0.**
Poniżej podano przykład konfiguracji routingu IGRP dla sieci 213.23.45.0:

```
C1600#config t
C1600(config)#router igrp 25000
C1600(config-router)#network 213.23.45.0
C1600(config-router)#^Z
```

4.3.3 Protokół OSPF

Na konfigurację procesu routingu OSPF składają się dwa etapy: zezwolenie routerowi na uruchomienie OSPF oraz identyfikacja adresów sieci i interfejsów, które mają być zawarte w aktualizacjach routingu, a także obszarów, do których należą te interfejsy.
Aby uruchomić OSPF, używamy polecenia konfiguracyjnego **router ospf.** Jeśli w tym samym routerze działa wiele procesów OSPF, polecenie to wymaga podania identyfikatora procesu jako parametru,. Tak jak w przypadku innych protokołów routingu, trzeba określić, które adresy sieci i interfejsy zostaną zawarte w ogłoszeniach routingu OSPF. Ponadto trzeba zidentyfikować obszary OSPF, w którym znajduje się interfejs.
Aby zidentyfikować adresy sieci i interfejsy zawarte w OSPF, jak również obszarów, do których należą, używamy podrzędnego polecenia konfiguracyjnego **network area.** Polecenie to ma dwa parametry. Pierwszy to adres sieci i maski zastępczej używane do porównywania z adresami IP przypisanymi interfejsom. Maska zastępcza to metoda dopasowywania adresów IP lub zakresów adresów IP. Kiedy maska zastępcza zostanie zastosowana do adresu IP interfejsu, a wynikowy adres sieci pasuje do adresu podanego w poleceniu **network area,** interfejs zostanie włączony do procesu routingu OSPF dla wskazanego obszaru. Drugi parametr, nazywany identyfikatorem obszaru, używany jest do określenia obszaru, do którego należy interfejs. Identyfikator może być liczbą całkowitą lub liczbą dziesiętną oddzieloną kropkami, tak jak adres IP [1].
Jeśli router ma trzy interfejsy i przypisane im są odpowiednio adresy 212.182.41.1, 212.182.41.65 i 213.23.45.67. Pierwsze dwa interfejsy są przypisane obszarowi l, natomiast trzeci jest przypisany obszarowi 0 bądź szkieletowemu. Oto oparty na powyższych założeniach przykład konfiguracji OSPF:

```
C1600#config t
C1600(config)#router ospf 25000
C1600(config-router)#network 212.182.41.0 0.0.0.127 area 1
C1600(config-router)#network 213.23.45.0 0.0.0.255 area 0
C1600(config-router)#^Z
```

Tylko te adresy i interfejsy sieciowe, które odpowiadają adresom w poleceniu **network area** są włączane do uaktualnień routingu OSPF.

4.3.4 Protokół EIGRP

Konfiguracja routingu EIGRP składa się z dwóch etapów: zezwolenia routerowi na uruchomienie EIGRP, oraz zidentyfikowania adresów sieci i interfejsów, które mają być zawarte w aktualizacjach routingu.
Aby zezwolić routerowi na włączenie EIGRP, używamy głównego polecenia konfiguracyjnego **router eigrp.** Gdy w tym samym routerze działa wiele procesów EIGRP. Polecenie to wymaga podania identyfikatora procesu jako parametru. Tak jak w przypadku IGRP, wyboru adresów sieci oraz interfejsów, które mają być zawarte w ogłoszeniach EIGRP, dokonuje się poleceniem konfiguracyjnym IOS **network.** Polecenie to jako parametr przyjmuje adres sieci klasowej, który ma być zawarty w aktualizacjach routingu. Polecenie **network** jest używane do identyfikowania tylko tych adresów IP sieci, które są bezpośrednio połączone z konfigurowanym routerem i które mają być zawarte w procesie routingu EIGRP. W aktualizacjach routingu zawarte zostaną tylko te interfejsy, których adresy IP należą do zidentyfikowanej sieci [1].
Jeśli router ma interfejsy w sieci 213.23.45.0 i w sieci 192.34.7.0. Polecenie **network** 213.23.45.0 określa, iż ogłoszenia routingu będą rozsyłane do podsieci należących do sieci 213.23.45.0 oraz interfejsów, które należą do sieci 213.23.45.0. Aby dołączyć aktualizacje routingu dla interfejsu znajdującego się w przestrzeni i adresowej 192.34.7.0, trzeba skonfigurować dodatkowe polecenie **network 192.34.7.0.** W tym przypadku sieć 192.34.7.0 to połączenie z dostawcą usług internetowych. Nie jest włączona do procesu routingu EIGRP, ponieważ usługodawca nie używa tego protokołu.
Poniżej znajduje się przykład konfiguracji EIGRP dla sieci **213.23.45.0**:

```
C1600#config t
C1600 (config)#router eigrp 25000
C1600 (config-router)#network 213.23.45.0
C1600 (config-router)#^Z
```

5 KONFIGURACJA LIST DOSTĘPU

Listy dostępu nie dają wprawdzie możliwości porównywalnych do specjalizowanych zabezpieczeń sieciowych, pozwalają jednak na wstępną kontrolę i ograniczenie ruchu w sieci TCP/IP.
Każdy system operacyjny routerów Cisco ma wbudowany mechanizm filtrowania ruchu poprzez listy dostępu. Filtrowanie pakietów jest jedną z podstawowych metod zabezpieczenia i ograniczenia ruchu w sieci. Mechanizm ten pozwala określić, z jakiej sieci źródłowej do jakiej sieci docelowej może odbywać się komunikacja, a także wskazać typ pakietów oraz aplikacji występujących na danym połączeniu.

5.1 Standardowe listy dostępu

Listy standardowe są proste w konfiguracji, nie mają jednak zbyt wielu możliwości zaawansowanej analizy pakietów. Podczas konfiguracji warunków jedynym kryterium wyboru pakietu jest adres źródłowy (adres nadawcy). Standardową listę dostępu tworzymy poleceniem trybu konfiguracyjego:

```
C1600(config)#access-list numer_listy_dostępu {permit|deny} adres_źródłowy_pakietu maska_wzorca log
```

Numer listy dostępu to wartość z przedziału od 1 do 99 (dla IP), natomiast adres źródłowy pakietu w połączeniu z maską wzorca jest zapisem adresu hosta lub sieci nadawcy. Zwróćmy uwagę na to, że w standardowej liście dostępu jedynie numer listy pozwala wskazać routerowi, które pakiety nas interesują. Lista ta nie odróżnia ruchu związanego z protokołem TCP czy UDP, nie wspominając już o typach aplikacji. Każdy kolejny warunek, który chcemy dopisać

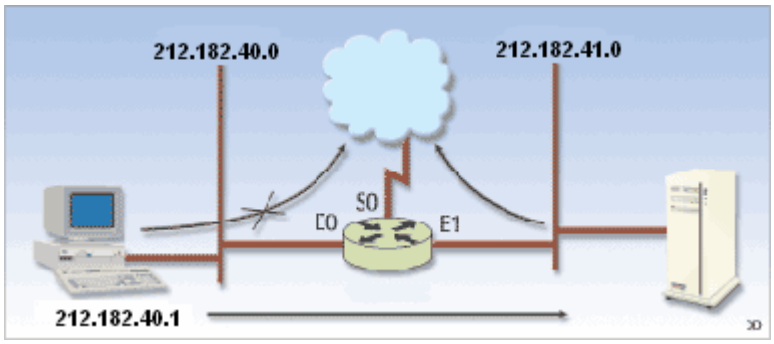
do listy dostępu musi zawierać ten sam numer listy, bardzo ważna jest kolejność warunków podawanych poleceniem **access-list**, ponieważ w takiej kolejności będą one analizowane. Opcja **log** spowoduje wysłanie komunikatu dla każdego pakietu dopasowanego do wzorca, korzystanie z niej nie jest zalecane podczas normalnej pracy routera ze względu na duże obciążenie procesora. Listę dostępu przypisujemy do wybranego interfejsu poleceniem trybu konfiguracji interfejsu:

```
C1600(config-if)#ip access-group numer_listy_dostępu {in|out}
```

Polecenie to dotyczy filtrowania pakietów na poziomie danego interfejsu i jest jednym z wariantów wykorzystania list dostępu. Oprócz podania numeru listy, którą chcemy skojarzyć z danym interfejsem, określamy tryb, w jakim lista ma być analizowana: na wejściu (**in**) czy na wyjściu pakietu z interfejsu (**out**) [4].

5.1.1 Przykład konfiguracji listy standardowej na przykładzie routera z dostępem do dwóch sieci lokalnych i sieci rozległej

Na rys. 5 przedstawiono typową konfigurację sieci z dostępem do Internetu. W przykładzie tym należy zabronić komputerowi o adresie 212.182.40.1 korzystania z sieci rozległej (np. z Internetu), lecz nie chcemy blokować mu dostępu do serwera znajdującego się w innej sieci lokalnej.



Rys. 5 Przykład dwóch sieci lokalnych z dostępem do Internetu

Lista standardowa obejmuje jedynie adres nadawcy pakietu, więc nie można przypisać takiej listy do konfiguracji interfejsu E0, ponieważ to zablokowałoby nie tylko dostęp do zasobów sieci rozległej, lecz również do sieci lokalnej 212.182.41.0 - na tym poziomie router wie, od kogo jest pakiet, ale nie wie, do kogo jest kierowany. W tym przypadku listę dostępu najlepiej jest przypisać do wyjścia (out) interfejsu S0, czyli do granicy sieci lokalnych. W trybie konfiguracji należy wydać polecenie:

```
C1600(config)#access-list 1 deny 212.182.40.1  0.0.0.0
```

lub w postaci skróconej:

```
C1600(config)#access-list 1 deny host 212.182.40.1
```

Tak zakończona lista spowodowałaby, iż żaden komputer z obu sieci lokalnych nie mógłby korzystać z Internetu, ponieważ każda lista zawiera *niejawny warunek odrzucający wszystko* (**deny any**). Potrzebne są więc dodatkowe warunki:

```
C1600(config)#access-list 1 permit 212.182.40.0 0.0.0.255
C1600(config)#access-list 1 permit 212.182.41.0 0.0.0.255
lub w skrócie:
C2600(config)#access-list 1 permit any
```

Tego rodzaju zapis nie jest wcale groźny. Pierwszy warunek określa adres hosta (212.182.40.1) i zabrania mu dostępu; ponieważ wszystkie pozostałe hosty nie spełniają tego warunku, będą podlegać regule zezwalającej na dostęp. Tak przygotowaną listę możemy przypisać do interfejsu S0:

```
C1600(config-if)ip access-group 1 out
```

W konfiguracji routera C1600 zobaczymy:

```
!
Interface Serial 0
ip address 213.11.11.1 255.255.255.0
ip access-group 1 out
!
access-list 1 deny host 212.182.40.1
access-list 1 permit 212.182.40.0 0.0.0.255
access-list 1 permit 212.182.41.0 0.0.0.255
```

Należy teraz zmodyfikować zadanie tak, żeby dać dostęp do Internetu tylko komputerom z sieci 212.182.41.0, a komputerom z sieci 212.182.40.0 ze względów bezpieczeństwa należy umożliwić korzystanie tylko z usług (np. FTP) serwera o adresie 212.182.41.254. Na routerze C1600 wykonywane są polecenia:

```
C1600(config)#access-list 1  permit 212.182.41.0 0.0.0.255
C100(config)#access-list 2  permit host 212.182.41.254
C1600(config)#interface S0
C1600(config-if)#ip access-group 1 out
C1600(config-if)#interface E0
C1600(config-if)#ip access-group 2 out
```

Lista dostępu 1 pozwala na dostęp tylko nadawcom z sieci 212.182.41.0, co dla pakietów wysyłanych przez interfejs S0 jest wystarczające (należy pamiętać o ukrytej zasadzie deny any). Trudniejsze zadanie dotyczy sieci 212.182.40.0 – nie można w liście standardowej podać adresu docelowego (212.182.41.254), trzeba więc prześledzić drogę pakietów IP. Jeżeli dowolny host z sieci 212.182.40.0 wyśle pakiet na adres 212.182.41.254, to router przy takiej konfiguracji nie ma podstaw, aby ten pakiet odrzucić. Co więcej, gdy pakiet z sieci 212.182.40.0 przesyłany jest na dowolny adres w sieci 212.182.41.0, router nie ma prawa zareagować. Ale gdy po otrzymaniu takiego pakietu odbiorca próbuje odesłać go do pierwotnego nadawcy (do sieci 212.182.40.0), router wstrzyma transmisję wszystkich pakietów zwrotnych do momentu, gdy nadawcą (odpowiadającym) będzie serwer o adresie 212.182.41.254, ponieważ reguła skojarzona z interfejsem E0 pozwala na wysłanie tylko takiego pakietu przez ten interfejs. Należy zwrócić uwagę na to, że filtrowanie to zostało zrealizowane poprzez utworzenie dwóch niezależnych, standardowych list dostępu. Przy korzystaniu z nich należy jednak pamiętać o zasadzie, która pozwala na wykorzystanie w ramach jednego interfejsu TYLKO jednej listy dostępu związanej z określonym protokołem.

DODATEK – ZESTAWIENIE POLECEŃ KONFIGURACYJNYCH ROUTERA [1]

Tabela 1. Podsumowanie poleceń trybu EXEC dla podstawowej konfiguracji routera

Polecenie	Opis
configure	Konfiguruje urządzenie IOS z terminalu, pamięci bądź sieci.
copy flash ftp	Kopiuje plik obrazu IOS z pamięci Flash do serwera FTP.
copy flash tftp	Kopiuje plik obrazu IOS z pamięci Flash do serwera TFTP
copy ftp flash	Kopiuje plik obrazu IOS z serwera FTP do pamięci podręcznej Flash.
copy running-config startup-config	Zapisuje bieżącą konfigurację do pamięci NVRAM
copy startup-config running-config	Tworzy konfigurację startową z pamięci NVRAM konfigurację
copy tftp flash	Kopiuje plik obrazu IOS z serwera TFTP do pamięci podręcznej Flash.
delete *nazwa obrazu IOS*	Usuwa wskazany obraz IOS z pamięci podręcznej Flash.
disable	Przechodzi z trybu uprzywilejowanego do trybu nieuprzywilejowanego.
enable	Wchodzi w tryb uprzywilejowany.
erase flash	Usuwa całą zawartość pamięci Flash.
erase startup-config	Wymazuje konfigurację startową.
lock	Blokuje bieżącą sesję terminala.
session *nazwa modułu*	Ustanawia sesję ze wskazanym modułem.
show flash	Wyświetla zawartość pamięci podręcznej Flash.
show running-config	Wyświetla bieżącą konfigurację urządzenia.
show sessions	Wyświetla aktualne sesje użytkownika.
show startup-config	Wyświetla konfigurację zapisaną w pamięci NVRAM, której urządzenie użyje przy następnym uruchomieniu.
squeeze	Wymazuje plik zaznaczony do usunięcia z pamięci podręcznej Flash.

Tabela 2. Podstawowe polecenia konfiguracyjne urządzenia

Polecenie	Opis
default polecenie	Ustawia domyślną wartość polecenia
enable password hasło	Ustawia hasło wejścia w tryb uprzywilejowany
enable secret hasło	Ustawia jednokierunkowe hasło kryptograficzne wejścia w tryb uprzywilejowany

hostname	Ustawia nazwę hosta urządzenia
interface typ	Określa, który interfejs będzie konfigurowany
ip ftp password	Określa hasło, które będzie używane do uwierzytelniania podczas używania protokołu FTP do transferu obrazów IOS oraz innych celów
ip ftp username	Określa nazwę użytkownika, która będzie używana do identyfikacji podczas używania protokołu FTP do transferu obrazów IOS oraz innych celów
no polecenie	Usuwa polecenie konfiguracyjne

Tabela 3. Zestawienie poleceń trybu EXEC dla IP.

Polecenie	Opis
clear host	Usuwa tymczasowe pozycje z tablicy hostów IP.
clear ip access-list counters	Zeruje liczniki podsumowujące, ile razy dopasowano każdą z pozycji listy dostępu IP.
flear ip route	Czyści całą tablice routingu, albo - jeśli została wskazana - konkretną trasę.
ping ip-address	Sprawdza wskazany adres IP, aby określić, czy jest osiągalny i czy udziela odpowiedzi.
show {frame-relay | atm | x25 | dialer} map	Pokazuje odwzorowania adresów IP na adresy łącza danych we wskazanym rodzaju nośnika WAN.
show access-lists	Pokazuje wszystkie listy dostępu zdefiniowane w routerze
show host	Sprawdza konfigurację DNS na routerze i wyświetla listę hostów, których nazwy zostały przekształcone na adresy IP.
show interface *interfejs*	Wyświetla ogólne informacje na temat interfejsu, w tym jego adres IP i maskę sieci.
show ip access-lists	Pokazuje wszystkie listy dostępu zdefiniowane w routerze.
show ip arp	Wyświetla wszystkie adresy IP, które router przekształcił w adresy MAC.
show ip dhcp binding	Wyświetla informacje dotyczące przypisań adresów dla serwera DHCP IOS.
show ip dhcp conflict	Wyświetla informacje na temat konfliktowych adresów IP wykrytych przez serwer DHCP IOS podczas procesu alokacji
show ip dhcp database	Wyświetla informacje dotyczące lokalizacji i stanu bazy danych używanej przez serwer DHCP IOS do archiwizowania przypisań adresów i konfliktów.
show ip dhcp server statistics	Wyświetla informacje dotyczące stanu oraz liczniki związane z działaniem serwera DHCP IOS.
show ip interface brief	Pokazuje krótkie zestawienie informacji dotyczących adresu IP i stanów interfejsów dla wszystkich dostępnych w urządzeniu interfejsów.
show ip interface *interfejs*	Pokazuje wszystkie parametry związane z konfiguracją interfejsu IP.
show ip masks *adres-sieci*	Wyszczególnia maski sieci, które zostały zastosowane w danej sieci, oraz liczbę tras, których używa każda maska.

show ip protocols	Pokazuje, które protokoły routingu działają, oraz różne atrybuty tych protokołów. Użyte ze słowem kluczowym summary, pokazuje tylko nazwy protokołów i numery identyfikacyjne procesów.
show ip route	Wyświetla tablicę routingu IP routera.
show ip route connected	Pokazuje trasy związane z działającymi, bezpośrednio połączonymi interfejsami routera.
show ip route *adres-ip*	Pokazuje informacje routingu dla wskazanej trasy.
show ip route static	Pokazuje trasy utworzone ręcznie, za pomocą odpowiednich poleceń konfiguracyjnych.
show ip traffic	Wyświetla ogólne statystyki dotyczące działania IP w routerze.
show standby	Wyświetla informacje na temat działania HSRP.
terminal ip netmask-format {decimal | bit-count | hexidecimal}	Określa format wyświetlania masek sieci, używany podczas bieżącej sesji wirtualnego terminalu lub sesji konsoli.
trace *adres-ip*	Wyświetla każdy etap ścieżki sieciowej, którą wędruje pakiet, aby osiągnąć wskazany adres IP.

Tabela 4. Zestawienie poleceń konfiguracyjnych dla IP.

Polecenie	Opis
aaa authentication ppp *lista metod*	Określa, że PPP jest uwierzytelniany przy życiu wyszczególnionej metody AAA.
aaa **authorization network** *metoda*	Określa, że usługi sieciowe są uwierzytelniane przy użyciu wyszczególnionej metody AAA.
access-list	Tworzy numerowaną listę dostępu i związane z nią kryteria filtrowania.
arp-server	Identyfikuje serwer ATM ARP, który potrafi przekształcać adresy IP na adresy ATM NSAP.
async-bootp dns-server *adres-ip*	Wskazuje adres IP serwera DNS dostarczany klientom połączenia podczas nawiązywania połączenia na zasadach ogólnych.
async-bootp nbns-server *adres-ip*	Wskazuje adres(y) IP serwera nazw NetBIOS dostarczany klientom połączenia podczas nawiązywania połączenia na zasadach ogólnych.
async mode {interactive | dedicated}	Określa metodę interfejsu asynchronicznego interakcji ze zdalnym użytkownikiem.
autoselect during-login	Wskazuje, że podczas uwierzytelniania powinien być przeprowadzony automatyczny wybór.
autoselect ppp	Wskazuje, że na linii asynchronicznej konfigurowanej w trybie interaktywnym powinna być wykonana autodetekcja PPP.
compress	Wskazuje, że podczas negocjacji połączenia PPP następuje próba negocjacji algorytmu kompresji.
default-metric	Określa domyślne wartości metryki routingu, które są używane podczas redystrybucji trasy pomiędzy protokołami routingu dynamicznego.
default-router *adres*	Definiuje jeden lub więcej adresów IP domyślnych routerów, które są dostarczane klientom DHCP przez serwer DHCP IOS.

dialer-group *liczba całkowita*	Wskazuje grupę wyboru połączenia, do której należy interfejs, oraz wskazuje, która lista wyboru połączenia jest używana do definiowania interesującego ruchu.
dialer-list *nume- typ* ***listy*** **protocol** *typ metoda*	Definiuje listę wyboru połączenia, która określa, jakie protokoły sieciowe i jakie metody są używane do definiowania ruchu jako interesującego dla sesji połączenia.
dialer map ip	Odwzorowuje adres IP na nazwę systemu i numeru telefonu dla wywołań ISDN.
dialer rotary-group *liczba całkowita*	Przypisuje interfejs ISDN do struktury grupy interfejsu wybierania.
distribute list	Stosuje listę dostępu do filtrowania odbieranych i ogłaszanych tras sieciowych.
dns-server *adres*	Definiuje jeden lub więcej adresów IP serwera DNS, które są dostarczane klientom DHCP przez serwer DHCP IOS.
domain-name *domena*	Definiuje nazwę domeny DNS, która jest dostarczana klientom DHCP przez serwer DHCP IOS.
flowcontrol hardware | softwa-re}	Określa metodę kontroli przepływu na linii asynchronicznej.
frame-relay map ip	Odwzorowuje adres IP na adres DLCI Frame Relay.
group-range *początek koniec*	Określa, które interfejsy asynchroniczne są zawarte w strukturze grupowego interfejsu asynchronicznego.
ip access-group list {in | out}	Stosuje wskazaną listę dostępu do filtrowania przychodzących i wychodzących pakietów w interfejsie.
ip access-list (extended | standard} *nazwa*	Tworzy nazwaną listę dostępu IP i związane z nią kryteria filtrowania.
ip address *adres-ip maska-sieci*	Przypisuje adres IP i maskę sieci interfejsom LAN i WAN
ip classless	Pozwala routerowi działać w trybie bezklasowym, w którym docelowe adresy IP pasują do tras nadsieci i bloków CIDR.
ip default-information originate	Sprawia, że OSPF generuje domyślną trasę z granicznego routera systemu autonomicznego do reszty domeny OSPF
ip default-network *adres-sieci*	Konfiguruje adres wskazanej sieci jako sieć podsumowującą lub domyślną.
{no} ip dhcp conflict logging	Włącza lub wyłącza archiwizowanie przez serwer DHCP IOS informacji dotyczących adresów konfliktowych.
ip dhcp database *adres-url*	Definiuje lokalizację i metodę archiwizowania przypisań adresów DHCP i informacji dotyczących konfliktów.
ip dhcp excluded-address	Wskazuje jeden lub więcej adresów IP, które powinny być wyłączone z ofert DHCP kierowanych do klientów DHCP przez serwer DHCP IOS.
ip dhcp pool *nazwa*	Tworzy pulę adresową DHCP, która może być konfigurowana dodatkowymi podpoleceniami konfiguracyjnymi DHCP.
ip dhcp-server *adres-ip*	Określa adres IP serwera DHCP, który może dynamicznie przypisywać adresy IP klientom połączenia.
ip domain-list *nazwa*	Tworzy listę nazw domen, które są dołączane do niepełnych nazw hostów.
ip domain-lookup	Włącza DNS.
ip domain-name *nazwa*	Konfiguruje nazwę podstawowej domeny, która będzie dołączana do niepełnych nazw hostów.
ip forward-protocol udp type	Określa, który rodzaj rozgłoszeń UDP będzie przekazany.

ip helper-address *adres-ip*	Przekazuje rozgłoszenia UDP pod wskazany adres IP-
ip host	Konfiguruje statyczne odwzorowania nazwy hosta na adre syIP.
ip local pool {default | pool-name} *początkowy-adres-ip końcowy-adres-ip*	Tworzy pulę adresów IP dla dynamicznego przypisy[wanl] adresów IP klientom połączeń.
ip name-server *adres-ip*	Konfiguruje serwer(y) nazw DNS.
ip netmask-format {decimal | bit-count | hexadecimal}	Konfiguruje format wyświetlania masek sieci, które będą używane podczas sesji wirtualnego terminalu lub sesji konsoli.
ip ospf network {broadcast | non-broadcast | point-to-multipoint}	Konfiguruje rodzaj sieci - rozgłoszeniową, bez rozgłaszania, wielopunktową - do której interfejsu podłączony jest OSPF.
ip rip {send | receive} version	Wskazuje, która wersja RIP ma być odbierana i wysyłana do konkretnego interfejsu.
ip route 0.0.0.0 0.0.0.0 *docelowy-adres-ip*	Konfiguruje domyślną trasę jako 0.0.0.0.
ip route *adres-sieci maska sieci docelowy-adres-ip*	Konfiguruje trasę podsumowującą, jako parametry przyjmując trasę podsumowującą, maskę sieci i niepołączoną podsieć.
ip routing	Włącza routing IP na routerze.
ip subnet-zero	Pozwala na przypisanie interfejsowi pierwszej podsieci w zakresie adresów sieci (podsieć zero).
ip unnumbered *interfejs*	Konfiguruje nienumerowany dwupunktowy interfejs WAN IP.
map-group	Przypisuje interfejsowi określoną grupę odwzorowań, której będzie używał do odwzorowywania adresów IP na adresy łącza danych ATM w interfejsie.
map-list	Tworzy określoną listę odwzorowań, służącą do konfigurowania odwzorowywania adresów IP na stałe obwody wirtualne lub komutowane obwody wirtualne w adresowaniu ATM.
modem autoconfigure {discover | *rodzaj modemu }*	Wskazuje, że modem podłączony do linii asynchronicznej powinien zostać automatycznie skonfigurowany poprzez wykrycie lub użycie ustawień podanego rodzaju modemu.
modem {dialin | inout}	Wskazuje dozwolony kierunek połączeń asynchronicznych.
neighbor adres-ip	Wskazuje adres IP routera sąsiadującego, z którym następuje wymiana informacji o routingu dynamicznym.
neighbor *adres-ip* **description**	Zezwala na dodawanie komentarzy do polecenia BGP neighbor.
neighbor *adres-ip* **distribute-list**	Zezwala na filtrowanie trasy na zasadach równorzędności BGP.
neighbor *adres-ip* **remote-as** *numer-asn*	Konfiguruje router sąsiadujący za pomocą wskazanego adresu jako równorzędny BGP we wskazanym systemie autonomicznym.
neighbor *adres-ip* **update-source** *interfejs*	Wskazuje, że źródłowy adres IP służący do ustanawiania sesji równorzędnych BGP jest wyprowadzony z określonego interfejsu.
netbios-name-server *adres*	Definiuje jeden lub więcej adresów IP serwera NetBIOS, który będzie dostarczany klientom DHCP przez serwer DHCP IOS.

netbios-node-type *typ*	Definiuje zachowanie trybu NetBIOS dostarczanego klientom DHCP przez serwer DHCP IOS.
network *adres-sieci*	Wskazuje, że podłączone interfejsy pasujące do wskazanego adresu sieci powinny być zawarte w ogłoszeniach routingu.
network *adres-sieci* **area *strefa#***	Wskazuje, że podłączone interfejsy pasujące do wskazanego adresu powinny być zawarte w ogłoszeniach routingu OSPF oraz że te interfejsy są przypisane do wskazanego obszaru.
network *numer-sieci [maska | długość-prefiksu]*	Wskazuje zakres adresów IP, które będą oferowane klientom DHCP dla danej puli adresowej DHCP przez serwer DHCP IOS.
no auto-summary	Zapobiega automatycznemu podsumowywaniu adresu w granicach sieci klasowej i zezwala na rozpowszechnianie informacji na temat podsieci.
no inverse-arp	Wyłącza funkcję dynamicznego odwzorowania adresów IP na numery DLCI w sieci Frame Relay.
passive-interface *interfejs*	Konfiguruje router, aby nasłuchiwał, ale nie ogłaszał informacji routingu we wskazanym interfejsie.
peer default ip address {pool | dhcp | *adres-ip }*	Określa metodę użytą do przypisania adresu IP stacji roboczej klienta połączenia.
ppp authenticatin *metoda*	Wskazuje, że przed udostępnianiem usług sieciowych musi zostać przeprowadzony proces uwierzytelnienie PPP. Pomiędzy serwerem dostępowym a klientem połączenia używany jest określony protokół uwierzytelniania.
ppp ipcp {dns | wins}	Wskazuje adres(y) IP serwerów DNS lub NetBIOS, które są dostarczane klientom połączenia podczas ustanawiania sesji) PPP na podstawie każdego interfejsu.
ppp multilink	Wskazuje, że multipleksowanie kanału oparte na oprogramowaniu ma być włączone w interfejsie.
redistribute protocol	Włącza redystrybucję trasy wskazanego protokołu.
router {rip | igrp | eigrp | bgp}	Zezwala routerowi na włączenie wskazanego protokołu routingu dynamicznego.
speed *bity-na-sekundę*	Określa szybkość transmisji linią asynchroniczną.
standby ip *adres-ip*	Konfiguruje wskazany adres IP jako wirtualny adres IP dla grupy HSRP.
standby preempt	Powoduje, że router o wyższym priorytecie przejmuje przekazywanie, gdy znów jest dostępny.
standby priority *priorytet*	Przypisuje wartość priorytetu routerowi HSRP, aby kontrolować wybór podstawowego routera przekazującego.
standby track *interfejs*	Włącza dynamiczne przypisywanie priorytetu HSRP dla routera HSRP na podstawie statusu operacyjnego wskazanego interfejsu.
standby use-bia	Wymusza, związanie wirtualnego adresu IP HSRP z fizycznym, sprzętowym adresem MAC interfejsu.
{no} synchronization	Włącza lub wyłącza wymóg, aby trasy były poznawane za pomocą routingu IGP przed ogłoszeniem ich sąsiadom EBGP.
username *nazwa* **password** *słowo*	Definiuje lokalną parę użytkownik/hasło, która ma być używana do uwierzytelniania użytkowników połączenia
version *wersja-rip*	Określa, która wersja RIP ma być używana w routerze.
x25 map ip	Odwzorowuje adres IP na adres X.121.

LITERATURA

[1] Allan Leinwand, Bruce Pinsky: „Konfiguracja routerów Cisco-podstawy“, Wydawnictwo MIKOM, Warszawa 2002.

[2] Tom Sheldon: „Wielka Encyklopedia Sieci Komputerowych”, Wydawnictwo Robomatic, Wrocław 1999.

[3] Praca zbiorowa: „Vademecum teleinformatyka“, Wydawnictwo IDG Poland S.A., Warszawa 1999.

[4] www.pckurier.pl/archiwum

[5] www.cisco.com/en/us/products/hw/routers/