Konfiguracja routerów Cisco

Autor: Krzysztof Masłyk IVFDS

STRESZCZENIE

Routery są dzisiaj nieodzownym składnikiem niemalże wszystkich rodzajów sieci. Jako że internet ma strukturę hierarchiczną bez przełączania pakietów pomiędzy sieciami nie można się dzisiaj już obejść. Jedną z najbardziej liczących się firm na świecie produkująca routery jest firma Cisco Corp., dlatego też w tym projekcie zostanie omówiona podstawowa wiedza na temat konfiguracji interfejsów danego routera, podstawowe polecenia konfiguracyjne oraz informacje o rutingu. Na wstępie zostaną omówione polecenia i sposoby ich użycia w podstawowych trybach konfiguracji routera, następnie przedstawiona zostanie konfiguracja interfejsów innych niż Ethernet. Będzie też coś o trasowaniu statycznym.

SPIS TREŚCI

1. OPIS ŚRODOWISKA

Pierwszą czynnością administratora po zakupie lub rozbudowaniu routera jest ustanowienie połączenia z routerem poprzez port konsoli. Każdy router Cisco wyposażony jest w jeden taki port (interfejs RS-232 lub RJ-45), do którego podłączyć można 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.

Po włączeniu routera w oknie terminala pojawi się zestaw komunikatów związanych ze startem routera. Proces uruchamiania routera składa się z kilku etapów i jest inicjowany przez program rozruchowy (bootstrap), znajdujący się w pamięci ROM. Po przeprowadzeniu testów diagnostycznych sprzętu w ramach procedury POST, w której sprawdza się m.in. działanie procesora, pamięci i interfejsów, poszukiwany jest i ładowany obraz systemu operacyjnego IOS - zgodnie z ustawieniami w rejestrze routera oraz poleceniami zawartymi w skrypcie konfiguracyjnym.

Większość routerów zawiera pamięć Flash. Jest to pamięć typu EEPROM, jej zawartość może być wielokrotnie usuwana i zapisywana ponownie. Zawartość pamięci Flash nie ginie po wyłączeniu routera, dlatego przeznaczona jest przede wszystkim do przechowywania wielu kopii systemu operacyjnego IOS. Zwykle początkowo w pamięci Flash znajduje się tylko jeden obraz systemu operacyjnego (zwany domyślnym plikiem systemu operacyjnego) i właśnie on zostanie załadowany po pierwszym włączeniu routera. Pamiętać jednak należy, że niektóre routery (Cisco 2500, 4000, 4500) przechowują minimalną wersję systemu operacyjnego bezpośrednio w pamięci ROM. Inne, np. routery serii 7000 i 7500, wczytują pełen obraz systemu operacyjnego z pamięci ROM.

Po załadowaniu systemu operacyjnego poszukiwany jest skrypt konfiguracyjny, zawierający parametry definiujące pracę routera (np. hasło dla trybu uprzywilejowanego) oraz poszczególnych jego części (np. interfejsów). Skrypt konfiguracyjny zapisywany jest w nieulotnej pamięci NVRAM, skąd przy każdym ponownym uruchomieniu routera może być odczytany i załadowany do pamięci operacyjnej RAM. Aktualna konfiguracja oraz wszelkie dokonywane w niej zmiany przechowywane są tylko w pamięci RAM, aby więc utrwalić wprowadzane przez administratora modyfikacje, należy ręcznie zapamiętać tę konfigurację w pamięci NVRAM jako konfigurację startową. Przy pierwszym uruchomieniu routera skrypt konfiguracyjny w pamięci NVRAM nie istnieje, co powoduje automatyczne uruchomienie dialogu konfiguracyjnego.

2. Przegląd rozkazów i ich przeznaczenia.

W rozdziale tym postaram się opisać podstawowe polecenia z większości najczęściej używanych trybów. Oczywiście nie jestem tutaj w stanie opisać ich wszystkich ponieważ zajęło by to mniej więcej tyle co średniej wielkości książka. Tak więc skupiłem się tutaj na poleceniach z trybu podstawowego czyli użytkownika, w którym są polecenia służące administratorowi do wykonania najbardziej prostych a zarazem podstawowych czynności administracyjnych. Następnie w trybie uprzywilejowanym, w którym administrator danego routera może np. zabezpieczyć do niego dostęp poprzez identyfikację za pomocą hasła.

2.1 Tryb użytkownika

W trybie tym użytkownik ma do dyspozycji tylko podstawowe polecenia nie wpływające na pracę routera. Są tu między innymi komendy służące do podglądu parametrów pracy routera i inne takie jak:

disable – komenda , która wyłącza tryb uprzywilejowany
disconnect – rozłączenie połączenia sieciowego
enable – włącza tryb uprzywilekowany
exit – wyjście z trybu EXEC
help – prosta i niezbyt szczegółowa pomoc na temat poszczególnych komend

logout – robi dokładnie to samo co exit – wyjście z trybu EXEC

ping – mechanizm umożliwiający sprawdzenie stanu połączenia (reczej) fizycznego między

dwoma węzłami siec.

show – funkcja ta służy do podglądu wielu parametrów i ustawień routera.
telnet – otwiera połączenie telnetowe
terminal – ustawia parametry pracy linii terminala
traceroute – powoduje odtworzenie ścieżki określonej przez parametr przeznaczenia

2.2 Tryb uprzywilejowany

W trybie tym możemy spotkać się już z niektórymi poleceniami, które wystąpiły w trybie użytkownika. Aby maszyna pozwoliła nam wejść do tego trybu użyjemy polecenia ***enable*** (***en***).W tym punkcie zostaną omówione tylko nowo poznane komendy:

clear – służy do czyszczenia tablicy routowania albo pamięci odwzorowania adresów
clock – służy do zarządzania zegarem systemowym
configure – dzięki temu rozkazowi router wchodzi w stan konfiguracji
copy – kopiuje plik (albo do pliku) z ustawieniami startowymi bądź z aktualnymi routera
erase – usuwa pamięć w której jest przechowywana konfiguracja routera
reload – zatrzymuje system powodując jednocześnie zimny restart
write – zapisuje pamięć NVRAM do dowolnego interfejsu (serwer TFTP, terminal, pamięć NVRAM), polecenie działa podobnie jak w polecenie copy

2.3 Tryb konfiguracji

banner – po wpisaniu linii tekstu router ustawia wiadomość dnia

boot – służy do wyszukania w pamięci flash i załadowania obrazu plików określonych poprzez nazwę

cpd – służy do zarządzania podpoleceniami (nie wiem dokładnie jak działa)

hostname – ustawia nazwę routera, na którym pracujemy

interface – służy do konfigurowania interfejsów (ISDN, Ethernet,Serial)
ip – za pomocą tego polecenia tworzymy statyczną tablicę rutowania
ipx – polecenie włącza na routerze przekazywanie pakietów IPX
isdn - ustawia typ przełącznika isdn
line – służy do konfigurowania linii terminala lub terminali wirtulnych
logging – pozwala ustalić poziom raportowania dla komunikatów wysyłanych do usługi syslog
ntp – konfiguruje
router – włącza rutowanie dynamiczne posługując się protokołami takimi jak : rip(1,2), igrp, eigrp, ospf
tftp-srewer – zezwala na usługę ładowania plików poprzez serwer tftp

username – ustawia nazwę użytkownika

2.4 Tabela obrazująca tryby pracy routera

Tryb pracy	Działanie
Tryb użytkownika Router>	Ograniczony zestaw poleceń nieniszczących; definiowanie ustawień terminala; wyświetlanie statusu routera.
Tryb uprzywilejowany Router #	Pełen zestaw poleceń; tryb konfiguracyjny; śledzenie pracy routera poprzez polecenie debug.
Tryb konfiguracyjny Router(config)#	Globalne i główne polecenia konfiguracyjne; wywoływany z trybu uprzywilejowanego.
Tryb konfiguracyjny procesu Router	Konfiguracja specyficznego procesu lub interfejsu routera;
(config-proces)#	realizacja podpoleceń; wywoływany z trybu konfiguracyjnego.
Dialog konfiguracyjny	Konfiguracja routera w trybie ineraktywnym; wywoływany poleceniem setup lub automatycznie przy braku konfiguracji startowej.
Monitor pamięci ROM rommon>	Procesy naprawcze (hasła lub pamięci Flash); modyfikowanie rejestru; wywoływany ręcznie odpowiednią kombinacją (zwykle Ctrl_Break) lub automatycznie przy braku poprawnego systemu operacyjnego.

3. 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.

Listę dostępnych poleceń w dowolnym trybie pracy routera wyświetlić można przez wciśnięcie znaku „?”. W trakcie wpisywania poleceń o złożonej składni wciśnięty znak „?” przywołuje kontekstową pomoc z informacjami o kolejnych parametrach czy słowach kluczowych wymaganych w danym poleceniu. Bardzo użyteczną cechą systemu operacyjnego jest rozróżnianie poleceń na podstawie wpisanych początkowych znaków nazwy. Wpisana część nazwy komendy musi jednoznacznie identyfikować polecenie, np. słowo ***en*** oznaczać będzie w praktyce polecenie ***enable.*** System operacyjny pamięta również historię ostatnio wykonywanych poleceń, po której w większości terminali poruszać można się za pomocą klawiszy kierunkowych w górę i w dół.

Po wyświetleniu pierwszego pytania wciskamy klawisz Enter, aby wejść do trybu interaktywnego. Niewątpliwie warto wyświetlić na ekranie podsumowanie dotyczące aktualnej konfiguracji interfejsów, w tym celu w odpowiedzi na drugie pytanie wciskamy ponownie Enter, zatwierdzając proponowaną domyślną wartość podaną w nawiasach kwadratowych. W pierwszej

kolumnie wyświetlonego zestawienia sprawdzić można, jak oznaczane są w danym routerze poszczególne interfejsy. Nazwa interfejsu składa się z typu (np. Ethernet lub Serial) oraz numeru. W routerach niemodularnych (poniżej rodziny 2600) numer interfejsu jest pojedynczą liczbą (np. Serial 0, Ethernet 1), natomiast w routerach modularnych, które mogą być rozbudowywane o kolejne karty interfejsów, stosuje się zestaw dwu liczb w notacji nr_karty/nr_portu (np. Serial 0/1 oznacza drugi port szeregowy na pierwszej karcie). W routerach serii 7000 i 7500, wyposażonych w złącza (slot) dla kart VIP, oznaczenie interfejsu złożone będzie z trzech liczb, zgodnie z konwencją nr_karty_VIP/nr_karty/nr_portu (np. Ethernet 1/0/1).

Następne kolumny podsumowania dotyczącego interfejsów zawierają informacje o przypisanych adresach IP, aktualnym statusie pracy interfejsu i wybranym protokole warstwy łącza danych. Zauważmy, że domyślnie wszystkie interfejsy są wyłączone (status oznaczony jako down), nie mają adresów IP ani określonego protokołu warstwy łącza danych. W kolejnych etapach dialogu konfiguracyjnego zdefiniować należy parametry globalne, w tym logiczną nazwę urządzenia wykorzystywaną w różnych procesach identyfikacyjnych oraz trzy hasła dostępowe wykorzystywane na routerze.

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.

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. Z trybu dialogu można także wyjść w dowolnej chwili, wybierając kombinację Ctrl_C. W ramce zamieszczamy fragment dialogu konfiguracyjnego z pytaniami dotyczącymi nazwy routera oraz haseł dostępu.

4. Tryby pracy i zarządzanie skryptem konfiguracyjnym – rozszerzenie

Po zapamiętaniu konfiguracji startowej oraz po ponownym uruchomieniu routera administrator podłączony do routera poprzez port konsoli automatycznie uzyskuje dostęp do trybu wykonywania poleceń, zwanego trybem EXEC. Tryb EXEC pozwala na pracę na szesnastu poziomach uprzywilejowania, choć zwykle wykorzystywane są tylko dwa: poziom użytkownika (poziom 1) oraz poziom uprzywilejowany (poziom 15). Poziomem domyślnym - oznaczanym przez znak zachęty zakończony symbolem > - jest poziom użytkownika, na którym dostępne są tylko niektóre polecenia sprawdzające status routera oraz definiujące pracę terminala.

Pełen zestaw poleceń łącznie z trybem konfiguracyjnym przypisany jest do poziomu uprzywilejowanego oznaczanego znakiem zachęty zakończonym symbolem „#" (poziomy 2 - 14 też oznaczane są symbolem „#"). Aby przejść na poziom 15, należy wykonać polecenie ***enable***, pamiętając o tym, że dostęp do poziomu uprzywilejowanego chroniony jest hasłem ***enable secret***, zdefiniowanym w dialogu konfiguracyjnym (jeżeli zdefiniowane jest hasło ***enable secret***, nie można wykorzystać hasła ***enable password*** do przejścia na poziom 15). Powrót na poziom domyślny (poziom 1) realizowany jest poleceniem ***disable***.

Ponieważ interaktywny dialog konfiguracyjny nie pozwala na zdefiniowanie wszystkich parametrów pracy routera, administrator będzie musiał dokończyć proces konfiguracji ręcznie z wykorzystaniem specjalnego trybu pracy routera, zwanego trybem konfiguracyjnym. Tryb ten (podobnie jak tryb śledzenia, wywoływany poleceniem debug) zarezerwowany jest dla poziomu uprzywilejowanego, a wchodzi się do niego komendą ***configure*** - pozwala ona skonfigurować router trzema różnymi metodami:

- 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. Poniżej przedstawiamy trzy przykłady poleceń globalnych, definiujących odpowiednio: logiczną nazwę routera, hasło chroniące dostęp do trybu uprzywilejowanego (przechowywane w postaci zaszyfrowanej) i routing dla protokołu IP:

```
C2600(config)#hostname Router
Router(config)#enable secret password
Router(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 Ethernet 0/1 oraz protokół routingu dynamicznego IGRP. Zauważmy, że wykonanie polecenia głównego, poza zmianą znaku zachęty wskazującego wybrany proces, nie powoduje praktycznych zmian w konfiguracji:

```
Router(config)#interface Ethernet 0/1
Router(config-if)#
Router(config)#router IGRP 10
Router(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 Ethernet 0/1 wygląda następująco:

```
Router(config)#interface Ethernet 0/1
Router(config-if)#description Drugi 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:

```
Router #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:

```
Router# show running-config
Router# 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:

```
Router# 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 przedstawiamy poniżej:

```
Router#copy running-config tftp
Remote host []? 131.108.1.250
Name of configuration file to write [Router -confg]?
/2600/c2600-confg
Write file /2600/ Router-confg on host 131.108.1.250? [confirm]
Building configuration...
Writing /2600/c2600-confg !! [OK]
Router
```

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:

```
Router copy tftp running-config
```

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

```
Router #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).

5. Konfigurowanie interfejsów

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.

Poniższa sekwencja poleceń pokazuje wywołanie trybu konfiguracyjnego, wybór właściwego interfejsu, przypisanie adresu IP i maski podsieci do interfejsu Ethernet 0/0 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.

```
Router# configure terminal
```

!!! Można również `conf t`

```
Router(config)#interface Ethernet 0/0
Router(config-if)#ip address 131.108.1.1 255.255.255.0
Router(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:

```
Router(config-if)#ip address 212.1.1.1 255.255.255.0 secondary
```

W przypadku interfejsów szeregowych konfiguracja jest bardziej złożona, bowiem oprócz parametrów warstwy sieciowej (adres IP czy maska podsieci) określić należy również ustawienia dla warstwy łącza danych oraz warstwy fizycznej (dostępne protokoły warstwy fizycznej oraz sposób ich wyboru, a także protokoły warstwy łącza danych przedstawimy szczegółowo w artykule o pracy routera Cisco w sieciach WAN w następnym numerze).

W przypadku komunikacji synchronicznej, typu punkt-punkt z wykorzystaniem interfejsów szeregowych, jedno urządzenie w parze pełni rolę urządzenia biernego typu DTE, zaś drugie jest urządzeniem aktywnym DCE, definiującym parametry transmisyjne, np. parametr zegara transmisji. W typowej sytuacji, gdy router podłącza się do sieci WAN, rolę DCE pełni urządzenie brzegowe dostawcy, a DTE - interfejs szeregowy routera oraz odwołanie domyślnie włączonego polecenia shutdown, które blokuje pracę interfejsu. Czynności te mogą być niepotrzebne, jeśli interfejs skonfigurowano z poziomu dialogu konfiguracyjnego. W warstwie łącza danych, jako typ hermetyzacji (encapsulation) dla przesyłanych danych, wybierany jest automatycznie i domyślnie protokół HDLC. W zależności od potrzeb protokół ten można zmienić.

Jeżeli interfejs szeregowy routera pracuje jako urządzenie DCE, obowiązkowo dla tego interfejsu zdefiniować należy parametr zegara transmisji. W tym celu wykonujemy następujące polecenie w ramach konfiguracji interfejsu, podając jako parametr jedną z dozwolonych wartości (wyrażoną w bps):

```
Router(config-if)#clock rate 128000
```

Parametr polecenia clock rate musi być dostosowany do wybranego protokołu warstwy fizycznej oraz do typu interfejsu szeregowego. System nie przyjmie wartości zegara większej niż maksymalna obsługiwana przez konkretny interfejs, co np. dla interfejsów szeregowych dostępnych na asynchroniczno - synchronicznych kartach WIC 2A/S oznacza dozwoloną prędkość do 128 kbps.

Dla wszystkich interfejsów szeregowych można dodatkowo skonfigurować przepustowość oraz opóźnienie wprowadzane przez dany interfejs. Trzeba jednak pamiętać, że obydwa te parametry są statycznie wpisywane przez administratora (początkowo mają wartości domyślne, wynikające z typu interfejsu), mają znaczenie etykietowe i nie odzwierciedlają w żadnym wypadku faktycznej komunikacji przez konkretny interfejs. Modyfikuje się je w celu zmiany środowiska pracy protokołów routingu dynamicznego, takich jak IGRP czy OSPF.

W poniższym przykładzie polecenia definiują przepustowość i opóźnienie dla interfejsu szeregowego. Parametr dla polecenia bandwidth wyrażany jest w kbps, natomiast opóźnienie podaje się w dziesiątkach mikrosekund:

```
Router(config-if)#bandwidth 128
Router(config-if)#delay 2000
```

Zdefiniowane dla interfejsów parametry oraz stan ich pracy można w dowolnej chwili obejrzeć poleceniem show interfaces - wyświetla ono m.in. następujące komunikaty dla konkretnego interfejsu Serial 0/0:

```
Router# show interfaces serial 0/0
Serial0/0 is up, line protocol is up
Hardware is PowerQUICC Serial
Internet address is 131.107.11.1/24
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

Informacja typu „Serial0/0 is up” oznacza poprawne działanie interfejsu w warstwie fizycznej (status down sygnalizuje na przykład brak częstotliwości nośnej lub niepodłączony kabel). Komunikat „line protocol is up” opisuje tu poprawne działanie protokołu warstwy łącza danych, czyli otrzymywanie pakietów keepalive (status down może oznaczać na przykład niezgodność protokołu warstwy drugiej bądź niezdefiniowany zegar (clock rate) w urządzeniu pracującym jako DCE). W pewnych sytuacjach stan interfejsu wyświetlany jest jako „administratively down”, co oznacza, że w konfiguracji interfejsu włączono polecenie shutdown, blokujące pracę interfejsu.

Wśród innych ciekawych informacji wyświetlanych poleceniem show znaleźć można: adres sprzętowy MAC (dla interfejsów typu Ethernet), przypisany adres IP, parametr MTU (maksymalny rozmiar pola danych transmitowanej ramki), przepustowość (BW), opóźnienie (DLY), niezawodność i obciążenie interfejsu (dwa parametry rzeczywistej transmisji) oraz włączony protokół warstwy łącza danych (np. HDLC dla interfejsu szeregowego lub ARPA,czyli Ethernet II dla interfejsu typu Ethernet). Więcej parametrów dotyczących tylko protokołu IP dla wybranego interfejsu zobaczyć można po wykonaniu następującego polecenia:

```
Router# show ip interface Serial 0/0
```

Jeżeli administrator routera chce sprawdzić, które interfejsy szeregowe pracują jako urządzenia DTE, a które jako DCE, jaki został zdefiniowany zegar oraz jaki jest stosowany (zwykle zależny od wybranego kabla) protokół warstwy fizycznej, może wykonać komendę show controllers interfejs, które wyświetla parametry fizyczne interfejsu:

```
Router# show controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 56000
```

6. Ładowanie systemu operacyjnego

Omówienie etapu poszukiwania i ładowania obrazu systemu operacyjnego zaczniemy od wyjaśnienia pojęcia rejestru systemowego, którego zawartość może mieć istotny wpływ na proces wczytywania systemu. Rejestr routera Cisco jest 16-bitową strukturą, przedstawianą najczęściej w postaci czterech cyfr szesnastkowych (np. dla routera 2600 rejestr może przyjmować domyślnie wartość 0x2102). W poszczególnych bitach zapamiętane są różne opcje dotyczące pracy routera, a fragment rejestru definiuje sposób ładowania systemu operacyjnego. Wartość ostatniej cyfry szesnastkowej, nazywanej też polem startu (boot field), określa sposób uruchomienia routera, zgodnie z następującą konwencją:

0 - uruchomienie routera w naprawczym trybie monitora pamięci ROM (nie jest ładowany żaden system operacyjny);
1 - załadowanie systemu operacyjnego z pamięci stałej ROM (część routerów ma w pamięci ROM tylko minimalną wersję systemu operacyjnego);
2‚F - załadowanie systemu operacyjnego zgodnie z sekcją poleceń boot system, znajdującą się w skrypcie konfiguracyjnym w pamięci NVRAM.

Ponieważ na ostatniej pozycji rejestru występuje domyślnie wartość 2, administrator może dość dowolnie sterować kolejnością poszukiwania systemu operacyjnego. Polecenie konfiguracyjne Boot system pozwala jawnie wskazać źródło, z którego ładowany jest system operacyjny, np. plik w pamięci Flash, serwer sieciowy TFTP czy pamięć ROM. Należy pamiętać, że kolejność prób załadowania systemu operacyjnego definiowana jest kolejnością komend boot system zawartych w skrypcie konfiguracyjnym.

Załóżmy, że router zawiera pamięć Flash, w której przechowywanych jest kilka obrazów systemu operacyjnego. Niezależnymi poleceniami boot system można wskazać różne pliki w pamięci Flash. Jeżeli w pamięci Flash nie będzie można znaleźć pierwszego pliku, system spróbuje załadować następny. W przypadku, gdy komendą boot system wskazywany jest plik systemu operacyjnego na serwerze sieciowym TFTP, w składni polecenia podać należy nazwę pobieranego pliku oraz adres IP serwera TFTP. Poniższy przykład pokazuje przykładową sekwencję poleceń boot system, określającą kolejność prób załadowania systemu operacyjnego:

```
Router(config)#boot system Flash IOS_Plik_nr 1
Router(config)#boot system Flash IOS_Plik_nr 2
Router(config)#boot system TFTP IOS_Plik_nr_3 131.108.1.250
```

```
Router(config)#boot system ROM
```

Jeżeli w skrypcie konfiguracyjnym nie zdefiniowano poleceń boot system (sytuacja początkowa), następuje próba załadowania domyślnego pliku z pamięci Flash; jest to pierwszy plik systemu operacyjnego nagrany w pamięci Flash (niezależnie od jego nazwy). Może się jednak zdarzyć, że pamięć Flash jest pusta (na przykład skasowana), wówczas router próbuje załadować plik o domyślnej nazwie z serwera sieciowego TFTP. Nazwa pliku tworzona jest na podstawie ustawień w rejestrze routera, a serwer TFTP poszukiwany jest metodą rozgłoszeniową. Jeśli ta metoda nie da pozytywnego rezultatu, router uruchamia się w specjalnym trybie monitora pamięci ROM (zgłasza się w postaci: rommon>) i nie jest ładowany żaden system operacyjny.

Aby przygotować zapasową kopię systemu operacyjnego, administrator powinien nagrać plik z pamięci Flash na serwerze sieciowym TFTP (bądź RCP lub FTP, jeśli dostępna jest taka opcja). W tym celu wykonać należy polecenie Copy Flash TFTP, podając jako parametry nazwę pliku źródłowego, adres IP serwera TFTP oraz nazwę i ścieżkę dostępu do pliku docelowego. Jeżeli pojawi się taka potrzeba, można wczytać plik systemu operacyjnego z powrotem do pamięci Flash za pomocą polecenia Copy TFTP Flash.

Przed rozpoczęciem właściwego kopiowania można (ale nie trzeba) wybrać opcję kasowania pamięci Flash. Komendy dotyczące ręcznego kasowania pamięci Flash mogą być różne, w zależności od wersji systemu. Przykładowo, na routerze 2600 z systemem 11.3 dostępne jest tylko polecenie erase Flash, pozwalające usunąć całą zawartość pamięci Flash. W innych przypadkach może być dostępna również komenda delete, umożliwiająca skasowanie wybranego pliku z pamięci Flash. Aktualną zawartość pamięci Flash oraz inne parametry (np. jej rozmiar czy ilość wolnego miejsca) wyświetlić można na ekranie poleceniem show Flash:

```
Router# show flash
System flash directory:
File Length Name/status
1 3119712 c2600-i-mz.113-10.T
[3119776 bytes used, 5268832 available, 8388608 total]
```

W sytuacji, gdy program ładujący (bootstrap) nie może zlokalizować i załadować żadnego systemu operacyjnego, router uruchamiany jest w specjalnym trybie naprawczym monitora pamięci ROM. Sytuacja taka ma miejsce na przykład wówczas, gdy skasowano pamięć Flash i nie podano żadnego innego źródła systemu operacyjnego. W trybie monitora pamięci ROM, który zgłasza się znakiem zachęty rommon>, można pobrać plik systemu operacyjnego z serwera TFTP i nagrać go do pamięci Flash. W tym celu należy zdefiniować pięć zmiennych środowiskowych, których znaczenie jest następujące:

- IP_ADDRESS - adres IP interfejsu routera,
- IP_SUBNET_MASK - maska podsieci interfejsu routera,
- IP_DEFAULT_GATEWAY - adres IP domyślnego routera, gdy serwer TFTP jest w innym segmencie,
- TFTP_SERVER - adres IP serwera TFTP,
- TFTP_FILE - nazwa pliku pobieranego z serwera TFTP.

Następnie w trybie monitora pamięci ROM uruchamiamy polecenie tftpdnld, które domyślnie próbuje wczytać wskazany plik z serwera TFTP i nagrać go w pamięci Flash (jeśli powyższe zmienne nie zostały wcześniej określone, wyświetlane są odpowiednie komunikaty). Po naprawieniu zawartości pamięci Flash należy uruchomić ponownie router poleceniem Reset.

Nazwa oryginalnego pliku systemu operacyjnego dostarczanego w pamięci Flash składa się z kilku części, z których każda ma specyficzne znaczenie - weźmy na przykład nazwę C2600-i-mz.113-10.T:

- Router - platforma urządzenia, na którym uruchamiany jest ten obraz systemu.
- I - specyficzne cechy i składniki systemu operacyjnego. Ta część może być też opisana przez grupę symboli. W tym wypadku **i** oznacza obsługę protokołu IP, ale np. symbol **js** opisuje rozszerzony system w wersji enterprise.
- **mz** - kompresja oraz miejsce uruchamiania. W tym wypadku **mz** oznacza plik skompresowany, uruchamiany w pamięci RAM.
- 113 - wersja systemu operacyjnego.
- 10 - kolejna aktualizacja systemu operacyjnego.
- T - rozszerzenie nazwy pliku.

7. Ochrona dostępu do routera

W konfiguracji standardowej dostęp do routera poprzez linię konsoli nie jest chroniony żadnym hasłem. Jeżeli w konkretnej firmie obowiązują bardziej restrykcyjne zasady bezpieczeństwa sieci, należy to zmienić. Opiszemy dwie metody zabezpieczania dostępu do routera: w pierwszej użytkownicy muszą znać wspólne dla wszystkich hasło, w drugiej każdy użytkownik uwierzytelniany jest na podstawie indywidualnego konta i hasła. Aby zdefiniować wspólne dla wszystkich hasło chroniące dostęp do routera poprzez linię konsoli, należy przejść do trybu konfiguracyjnego linii konsoli numer 0, następnie włączyć uwierzytelnianie i określić hasło:

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password haslo
```

Ponieważ w tej metodzie od wszystkich użytkowników wymagane jest to samo hasło, może się ona okazać w pewnych sytuacjach niewystarczająca. Lepszą metodą weryfikowania dostępu do routera będzie sprawdzanie użytkownika poprzez indywidualne konto i hasło. Konfiguracja linii konsoli w tym przypadku będzie nieco inna. Komenda login musi być uruchomiona z parametrem określającym bazę kont użytkowników. Jeżeli na przykład stosowana ma być lokalna, utworzona na routerze baza kont, to konfiguracja jest następująca:

```
Router(config)#line console 0
Router(config-line)#login local
```

Zauważmy, że w powyższym przykładzie nie ma komendy **password**, gdyż hasło wspólne dla wszystkich użytkowników nie ma w tym przypadku zastosowania. Przy używaniu komendy **login local** należy unikać pewnej pułapki, która może zablokować normalne korzystanie z routera - po wykonaniu polecenia **login local**, przy każdej próbie podłączenia się do routera pojawi się pytanie o konto użytkownika i hasło; jeżeli więc nie będzie lokalnej bazy kont (a standardowo jej nie ma), nie będzie możliwe poprawne uwierzytelnianie. Trzeba najpierw zdefiniować konta użytkowników, a dopiero potem użyć komendy **login local**.

Polecenie konfiguracyjne pozwalające utworzyć nowe konto użytkownika ma składnię: **username Nazwa password Haslo**. Polecenie to wymaga podania nazwy konta i hasła wykorzystywanego w procesie uwierzytelniania. Konta utworzone poleceniem username są przechowywane i widoczne w aktualnej konfiguracji routera, stąd należy pamiętać o regularnym zapisywaniu jej w pamięci NVRAM. Domyślnie użytkownik, który weryfikowany jest przy dostępie do routera poprzez indywidualne konto i hasło, umieszczany jest na poziomie 1 (poziom użytkownika). Można również do każdego konta indywidualnie przypisać inny domyślny poziom pracy, na który użytkownik będzie automatycznie przełączany. W tym celu należy ponownie posłużyć się komendą **username**. W poniższym przykładzie tworzone jest konto Ad-

min2 z hasłem cisco, a dodatkowo do tego konta przypisywany jest domyślny poziom uprzywilejowania 7:

```
Router(config)#username Admin2 password cisco
Router(config)#username Admin2 privilege level 7
```

Korzystanie z polecenia konfiguracyjnego **login local** jest rozwiązaniem skutecznym, choć może być nieco uciążliwe, gdyż wymaga definiowania lokalnej bazy danych na każdym z routerów. Innym sposobem rozwiązania problemu weryfikacji jest zastosowanie centralnej usługi uwierzytelniającej podłączających się użytkowników. Rozwiązanie to oparte w praktyce na usługach zewnętrznych RADIUS lub TACACS+ oferuje również możliwość autoryzacji i rejestracji wykonywanych działań. Przykładową sytuację, w której router Cisco jest klientem serwera RADIUS przedstawia rysunek poniżej.

Przy próbie podłączenia się do routera, np. poprzez port konsoli, router pracujący jako klient przesyła do centralnego serwera prośbę o uwierzytelnienie użytkownika. Serwer RADIUS, zawierający centralną bazę informacji o użytkownikach, przeprowadza proces weryfikacji, dodatkowo może określić rodzaj dozwolonych dla użytkownika operacji (autoryzacja) oraz kontrolować i zapisywać w dzienniku ich realizację. Protokół RADIUS pozwala w praktyce na wykonywanie trzech niezależnych działań (nie tylko uwierzytelniania), jest on przykładem tzw. protokołu AAA (Authentication, Authorization, Accounting). Aby włączyć na routerze Cisco korzystanie ze wszystkich usług AAA, należy w trybie konfiguracji globalnej wykonać polecenie **aaa new-model,** a następnie skonfigurować realizację procesu uwierzytelniania, autoryzacji i kontroli poleceniami: **aaa authentication, aaa authorization i aaa accounting**. Poniższe przykładowe komendy konfiguracyjne pozwalają wskazać serwer RADIUS oraz określić klucz stosowany do zaszyfrowania przesyłanego hasła użytkownika (podobnie konfiguruje się współpracę z serwerem TACACS+, który też jest protokołem AAA):

```
Router(config)#radius-server host 131.107.2.250
Router(config)#radius-server key klucz
```

Zastosowanie protokołów AAA pozwala w optymalny sposób zarządzać procesem uwierzytelniania użytkowników, zwłaszcza w środowisku dużej, wielosegmentowej sieci lokalnej, wyposażonej w wiele routerów. Przed wdrożeniem tego rozwiązania należy zastanowić się nad wyborem odpowiedniego protokołu. Protokół RADIUS (oparty na UDP) jest rozwiązaniem otwartym, nadającym się bardzo dobrze dla środowisk niejednorodnych, w których wykorzystywane są urządzenia różnych producentów. Natomiast protokół TACACS+ (oparty na TCP) jest rozwiązaniem firmy Cisco i przeznaczony jest dla sieci wykorzystujących urządzenia tej firmy.

Oprócz podłączenia poprzez port konsoli możliwy jest także dostęp do routera poprzez linie terminali wirtualnych VTY. Najczęściej wykorzystywany jest do tego celu protokół Telnet. Aby ustanowić sesję telnetową do zdalnego routera, konieczne jest wcześniejsze poprawne skonfigurowanie interfejsu tego routera (m.in. wpisanie adresu IP), poprzez który sesja zostanie nawiązana. Standardowo router Cisco udostępnia 5 linii terminali wirtualnych, przez które można się do niego podłączyć. Linie te przyznawane są użytkownikom dynamicznie i nie wiadomo, która zostanie wykorzystana na kolejne połączenie. Z tego powodu najczęściej konfiguruje się wszystkie 5 linii VTY jednocześnie. Ochrona dostępu do routera poprzez linie VTY wygląda bardzo podobnie, jak w przypadku podłączania się poprzez port konsoli. Dlatego bez dodatkowego omawiania tych samych rozwiązań, zapoznajmy się z przykładami konfiguracji linii VTY. Aby włączyć ochronę dostępu do routera na poziomie pojedynczego hasła, należy wykonać polecenia:

```
Router(config)#line VTY 0 4
Router(config-line)#login
Router(config-line)#password haslo
```

Zapis **line VTY 0 4** w pierwszym poleceniu oznacza linie VTY o numerach od 0 do 4, czyli wszystkie 5 linii. Pamiętajmy, że hasło chroniące dostęp przez linie VTY definiowane jest już w dialogu konfiguracyjnym (w odróżnieniu od portu konsoli), zatem polecenie **password** w tym przypadku służyć będzie jedynie do jego zmiany. Aby włączyć korzystanie z lokalnej bazy kont użytkowników w procesie uwierzytelnienia, należy wykonać następujące polecenia:

```
Router(config)#line VTY 0 4
Router(config-line)#login local
```

Dodatkowym sposobem zwiększenia bezpieczeństwa przy dostępie do routera poprzez linie VTY jest określenie dozwolonych adresów, z których połączenie może być ustanowione. Można wskazać na przykład adresy komputerów, przy których pracują administratorzy. Realizuje się to przez wykorzystanie podpolecenia **access-class** w ramach konfiguracji linii VTY. W praktyce polecenie to korzysta ze zdefiniowanych wcześniej list dostępu dla protokołu IP, które omówione zostaną w jednym z dalszych artykułów. Dodatkowo dla linii terminali wirtualnych warto zdefiniować parametry automatycznego rozłączania połączenia. Poniżej pokazujemy dwa przykłady ustawiające czasy rozłączania. Komenda pierwsza oznacza bezwzględne rozłączenie sesji użytkownika po 60 minutach. Polecenie drugie ustawia rozłączanie po 15 minutach i 30 sekundach bezczynności. Komenda **absolute-timeout** nie ma zdefiniowanej wartości domyślnej, polecenie **exec-timeout** przyjmuje domyślnie wartość 10 minut:

```
Router(config)#line VTY 0 4
Router(config-line)#absolute-timeout 60
Router(config-line)#exec-timeout 15 30
```

Zarówno hasło zdefiniowane poleceniem **enable password**, jak i hasła przypisane do kont użytkowników oraz hasła zabezpieczające dostęp do routera poprzez linie konsoli czy linie VTY przechowywane są w postaci jawnej w konfiguracji routera. Może się zdarzyć, zwłaszcza gdy skrypt konfiguracyjny nagrywany jest na serwerze TFTP, że hasła te zostaną odczytane przez niepowołane osoby. Aby temu zapobiec, należy w trybie konfiguracji globalnej wykonać polecenie **service password-encryption**. Wszystkie wprowadzone jawnie hasła przedstawione zostaną w konfiguracji w postaci zaszyfrowanych łańcuchów znaków, poprzedzonych cyfrą 7, wskazującą algorytm szyfrowania (z wyjątkiem hasła enable secret, które szyfrowane jest innym algorytmem). Oczywiście podczas logowania użytkownik cały czas posługuje się hasłem w postaci jawnej. Warto zauważyć, że wyłączenie usługi szyfrującej nie powoduje odszyfrowania haseł. W postaci jawnej hasła zostaną pokazane w konfiguracji dopiero po ich następnej zmianie.

8. Procedura naprawiania hasła

Jeżeli administrator routera zapomni hasła uprawniającego do przejścia na poziom 15, nie będzie mógł wprowadzić żadnych zmian konfiguracyjnych. Podobny problem może pojawić się wówczas, gdy administrator otrzymuje router już skonfigurowany, na przykład z innego oddziału firmy, bez informacji o związanym z nim haśle. Proces tzw. naprawienia hasła dla trybu uprzywilejowanego polega w zasadzie na jego nadpisaniu nową wartością. Może go przeprowadzić osoba podłączona do routera poprzez port konsoli. Przede wszystkim router musi zostać uruchomiony w specjalnym trybie monitora pamięci ROM po to, aby zmodyfikować szesnastobitową wartość rejestru systemowego. W tym celu w ciągu pierwszych 60 sekund od włączenia routera (wartość podawana w dokumentacji Cisco), z konsoli należy wybrać specjalną kombinację klawiszy, przerywającą normalny proces startu. Najczęściej jest to kombinacja CTRL_Break, choć może być różna w zależności od rodzaju emulowanego terminala. Inne kombinacje, które warto przetestować to np. CTRL_B lub Alt_B. Przykładowo kombinacja CTRL_Break działa poprawnie w programie HyperTerminal systemu Windows 98 czy Windows 2000 (ale nie Windows NT 4.0). Po wybraniu CTRL_ Break router uruchamiany jest w trybie monitora pamięci ROM. Przy każdym starcie routera hasło związane z poziomem 15 od-

czytywane jest z konfiguracji startowej. Procedura naprawcza rozpocznie się więc od ustawienia w rejestrze wartości, która zmusi router do pominięcia (ale nie skasowania) konfiguracji startowej przy jego następnym uruchomieniu. W tym celu na routerze 2600, wykorzystywanym w większości naszych przykładów, wykonać należy polecenie **confreg** 0x2142 (standardowa wartość rejestru to 0x2102). Cyfra szesnastkowa 4 na trzeciej pozycji rejestru oznacza pominięcie wczytywania konfiguracji startowej. Jeżeli nie wiemy, jaką wartość rejestru należy ustawić, można uruchomić program **confreg** w trybie dialogowym, w którym odpowiedzi na kolejne pytania pozwalają zdefiniować różne parametry pracy routera, ustawiając odpowiednie bity w rejestrze. Większość pytań nie dotyczy w ogóle hasła, więc można pozostawić proponowane domyślne wartości. Tylko pytanie Ignore system config info wymaga odpowiedzi Yes. Po zdefiniowaniu rejestru należy ponownie uruchomić router poleceniem **reset.**

Proces uruchamiania routera powinien zakończyć się pytaniem o wejście do dialogu konfiguracyjnego. Dzieje się tak dlatego, iż router nie wczytał konfiguracji startowej i wówczas zawsze proponuje dialog konfiguracyjny. Po udzieleniu przeczącej odpowiedzi zauważymy, że nazwa routera ma postać: Router. W kolejnych krokach należy:

1. Wejść do trybu uprzywilejowanego poprzez wykonanie komendy **enable** (system nie zapyta o hasło);
2. Wczytać konfigurację startową do pamięci RAM: **copy start runn;**
3. wejść do trybu konfiguracyjnego: **conf term**;
4. Zdefiniować nowe hasło, np.: **enable secret cisco1**;
5. Przywrócić poprzednią postać rejestru: **config-register 0x2102**;
6. W konfiguracji każdego interfejsu wyłączyć polecenie **shutdown** (domyślnie router nieskonfigurowany ma wyłączone interfejsy, a jest nim na przykład router, który nie wczytał konfiguracji startowej);
7. Nagrać konfigurację aktualną z nowym hasłem w pamięci NVRAM: **copy runn start**;
8. Ponownie uruchomić router i przetestować nowe hasło.

4.0 Konfigurowanie protokołu SNMP

Protokół SNMP (Simple Network Management Protocol) opracowany został do nadzorowania, diagnozowania oraz zdalnego zarządzania urządzeniami pracującymi w sieci TCP/IP. Wyróżniamy dwa podstawowe składniki w architekturze SNMP: oprogramowanie agenta, zwykle zaszyte w urządzeniu sieciowym oraz oprogramowanie menedżera SNMP, dostarczane na przykład jako specjalizowana aplikacja (p. rysunek).

Komunikacja między menedżerem i agentem, realizowana przy wykorzystaniu standardowego zestawu poleceń, pozwala menedżerowi zebrać podstawowy zestaw informacji o urządzeniu, na którym pracuje agent. Informacje, które menedżer może uzyskać od agenta zdefiniowane są w postaci obiektów w bazach danych MIB (Management Information Base). Każdy obiekt w bazie ma swój unikatowy identyfikator, poprzez który menedżer ma do niego dostęp. Typowe polecenia, za pomocą których menedżer uzyskuje informacje o określonych obiektach to: GET i GET-NEXT, natomiast poleceniem SET menedżer wymusza ustawienie wartości wybranego obiektu. Dodatkowo agent może z własnej inicjatywy wysyłać do menedżera komunikaty typu TRAP, co dzieje się na skutek wystąpienia pewnych zdarzeń. System operacyjny routera Cisco wyposażony jest w oprogramowanie agenta SNMP, ale do poprawnej pracy wymaga dodatkowej konfiguracji. Aby agent zaakceptował polecenie przysyłane od menedżera. musi być spełniony warunek przynależności do tej samej społeczności SNMP (community). Nazwę społeczności, do której należy agent (router Cisco) można zdefiniować już w dialogu konfiguracyjnym lub później globalnym poleceniem konfiguracyjnym **snmp-server community**. W poleceniu tym można też podać tryb dostępu do agenta: **RO** (tylko do odczytu - polecenia GET i GET-NEXT) bądź **RW** (do odczytu i zapisu - również polecenie SET) oraz numer standardowej listy dostępu, dzięki której można określić dozwolone adresy IP dla menedżerów

przysyłających żądania. Do standardowych zdarzeń zachodzących na routerze Cisco, które powodują wysłanie komunikatu Trap do wybranego menedżera należy błąd uwierzytelnienia. Jest to przypadek, gdy do agenta przychodzi żądanie z obcej społeczności. Oprócz informowania o próbach nieuprawnionego dostępu, agent wysyła typowo do swojego menedżera komunikaty Trap dla zdarzeń ponownego uruchomienia routera bądź zmiany stanu interfejsu. Inne komunikaty typu Trap wysyłane przez agenta konfiguruje się poleceniem **snmp-server host**. Komenda ta pozwala określić adres IP menedżera SNMP, nazwę społeczności menedżera oraz rodzaje komunikatów Trap, które będą do menedżera wysyłane.

Poniżej przedstawiamy przykład konfiguracji protokołu SNMP. Zauważmy, że router może należeć do kilku społeczności. Dla społeczności Public włączona jest opcja RO (tylko do odczytu), dla społeczności Private włączony jest pełen dostęp (RW). W przypadku społeczności Private ustawiono kontrolowanie adresu IP menedżera poprzez listę dostępu nr 5. Ostatnia komenda definiuje adres IP menedżera, do którego wysyłane będą komunikaty Trap, określa też rodzaj wysyłanych komunikatów trap. W tym przykładzie router C2600 informować będzie swojego menedżera o zdarzeniach dotyczących protokołu ISDN oraz o zmianach w konfiguracji.

```
Router(config)# snmp-server community Public RO
Router(config)#snmp-server community Private RW 5
Router(config)#snmp-server host 131.107.10.245 Public isdn config
```

Programy graficzne przeznaczone do zdalnego zarządzania routerem Cisco bardzo często opierają swoje działanie na protokole SNMP. W takim przypadku niezbędne będzie określenie właściwej nazwy społeczności, w której pracuje router. Dodatkowo, aby ułatwić zarządzanie, na routerze można skonfigurować dwa parametry opisowe, określające położenie routera oraz osobę kontaktową. Parametry te definiuje się w postaci łańcuchów znaków za pomocą polecenia **snmp-server location** oraz **snmp-server contact**.

9. Obsługa komunikatów obsługiwanych przez router

Zdarzenia zachodzące na routerze oraz poszczególne działania systemu operacyjnego mogą być monitorowane i zapisywane w postaci komunikatów, co ułatwia diagnostykę i naprawianie ewentualnych błędów. Komunikaty opisujące pracę routera oraz będące wynikiem działania polecenia **debug,** śledzącego wybrane procesy, mogą być wysyłane do czterech różnych odbiorców, zgodnie z rysunkiem poniżej.

Standardowo wszystkie komunikaty wyświetlane są na terminalu konsoli. Dodatkowo można skonfigurować wyświetlanie komunikatów w sesjach telnetowych (połączenia VTY) oraz wysyłanie komunikatów do zewnętrznego serwera usługi syslog. Czwartą opcją jest zapisywanie komunikatów w wewnętrznym buforze routera. Dla każdego z wymienionych czterech przypadków można niezależnie skonfigurować poziom szczegółowości raportowanych zdarzeń (p. tabela). Standardowo dla linii konsoli oraz linii terminali wirtualnych włączony jest najbardziej szczegółowy poziom raportowania (debugging) oznaczający monitorowanie wszystkich zdarzeń, dla usługi syslog włączony jest poziom komunikatów informacyjnych (informational), natomiast buforowanie komunikatów w pamięci jest wyłączone.

Poziom 7 (debugging), oprócz tego, że oznacza zbieranie wszystkich komunikatów opisujących pracę routera, jest również wymagany dla poprawnego raportowania zdarzeń związanych z działaniem polecenia **debug**. Podstawową komendą konfiguracyjną służącą do określania miejsc, w których będą zbierane komunikaty oraz definiowania poziomów szczegółowości jest globalne polecenie konfiguracyjne **logging**. W poniższej sekwencji poleceń wyłączono rapor-

towanie na linii konsoli, włączono wysyłanie komunikatów na linie VTY (na poziomie 6), zdefiniowano maksymalny poziom szczegółowości (7) komunikatów wysyłanych do zewnętrznej usługi syslog pracującej pod adresem 131.108.1.250 oraz ustalono, że zdarzenia będą monitorowane w wewnętrznym buforze (8192 bajty) routera:

```
Router(config)#no logging console

Router(config)#logging monitor informational

Router(config)#logging 131.108.1.250

Router(config)#logging trap debugging

Router(config)#logging buffered 8192
```

Polecenie **logging trap** pozwala ustalić poziom raportowania dla komunikatów wysyłanych do usługi syslog. Najczęściej jest to usługa uruchamiana na hostach systemu Unix, a zbierane zdarzenia zapisywane będą w pliku tekstowym.

Poleceniem **logging monitor** włącza się wysyłanie komunikatów na linie terminali wirtualnych VTY, ale nie jest to równoznaczne z odbieraniem ich w sesjach protokołu Telnet. Po ustanowieniu połączenia na jednej z pięciu linii terminali wirtualnych, wymagane jest dodatkowo wykonanie polecenia **terminal monitor**, które spowoduje wyświetlanie komunikatów w tej konkretnej sesji telnetowej.

Polecając zbieranie komunikatów do wewnętrznego bufora na routerze, pamiętać należy o tym, iż jest on tworzony w pamięci RAM, tak więc wszystkie zgromadzone w nim komunikaty zostaną utracone po każdym ponownym uruchomieniu routera. To rozwiązanie, choć wygodne - komunikaty z bufora można w dowolnej chwili wyświetlić na ekranie konsoli - nie nadaje się do archiwizowania zdarzeń. Do tego celu należy wykorzystać zewnętrzną usługę syslog. Domyślny rozmiar bufora komunikatów wynosi 4096 bajtów, a zawarte w nim komunikaty oraz aktualną konfigurację raportowania wyświetlić można poleceniem **show logging**. Poniżej prezentujemy wynik tego polecenia dla przykładowej konfiguracji routera, w której włączono buforowanie komunikatów. Zwróćmy uwagę na wyświetlany czas monitorowanych zdarzeń:

```
Router#show logging

Syslog logging: enabled (0 messages dropped,0 flushes, 0 overruns)

Console logging: level debugging, 25 messages logged

Monitor logging: level debugging, 5 messages logged

Logging to: vty66(5)

Trap logging: level informational, 29 message lines logged

Buffer logging: level debugging, 25 messages logged

Log Buffer (4096 bytes):

02:34:23: %SYS-5-CONFIG_I: Configured from console by console

02:35:22: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up

02:35:24: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to
administratively down
```

Jak zaznaczyliśmy wcześniej, włączenie najwyższego poziomu raportowania 7 jest wymagane do poprawnego posługiwania się poleceniem **debug**. Komenda ta, dostępna na poziomie uprzywilejowanym, pozwala monitorować pracę różnego rodzaju procesów i protokołów działających na routerze. Poszczególne komunikaty opisujące śledzony proces mogą być wysyłane do jednego z czterech odbiorców, jak to opisaliśmy wcześniej. Jako przykład posługiwania się poleceniem debug, prezentujemy narzędzie przeznaczone do testowania komunikacji w sieci IP - program ping. Wysyła on sekwencję pakietów echo protokołu ICMP pod wskazany adres IP, oczekując na taką samą liczbę odpowiedzi w postaci pakietów echo reply. Śledzenie działania programu ping wymaga następującej składni komendy debug: **debug ip icmp**. Oto przykładowa sekwencja komunikatów wynikowych:

```
Router#debug ip icmp

ICMP packet debugging is on

Router#ping 131.107.10.245

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 131.107.10.245, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), Round-trip min/avg/max = 1/2/4 ms

Router#

03:30:53: ICMP: echo reply rcvd, src 131.107.10.245, dst 131.107.10.1

03:30:53: ICMP: echo reply rcvd, src 131.107.10.245, dst 131.107.10.1

03:30:53: ICMP: echo reply rcvd, src 131.107.10.245, dst 131.107.10.1

03:30:53: ICMP: echo reply rcvd, src 131.107.10.245, dst 131.107.10.1

03:30:53: ICMP: echo reply rcvd, src 131.107.10.245, dst 131.107.10.1
```

Warto zauważyć, iż polecenie debug nie obejmuje pakietów echo protokołu ICMP wysyłanych przez router. Dlatego też w komunikatach wynikowych widać tylko pięć pakietów zwrotnych echo reply (nie ma 5 wysyłanych pakietów echo).

Czasami w procesie rozwiązywania problemów komunikacyjnych, niezbędne jest włączenie śledzenia całej komunikacji protokołu IP. W tym celu wykonać należy komendę: **debug ip packet**. Poniżej przedstawiamy ponownie przykład działania programu ping - fragment komunikatów wyraźnie pokazuje, iż tym razem komenda debug obejmuje zarówno pakiety wysyłane, jak i odbierane.

```
Router# debug ip packet IP packet debugging is on

Router#ping 131.107.10.245 Sending 5, 100-byte ICMP Echos to 131.107.10.245,
timeout is 2 seconds: !!!!!Success rate is 100 percent (5/5), round-trip
min/avg/max = 1/2/4 ms

Router# 03:35:19: IP: s=131.107.10.1 (local),d=131.107.10.245 (Ethernet0/0),
len 100, sending 03:35:19: IP: s=131.107.10.245 (Ethernet0/0),
d=131.107.10.1 (Ethernet0/0), len 100, rcvd 3
```

Innym często stosowanym poleceniem jest komenda **debug ip rip**, pozwalająca nadzorować i wykrywać ewentualne błędy w działaniu protokołu routingu dynamicznego RIP. Ponieważ

proces śledzenia może generować na ekranie konsoli bardzo dużo komunikatów, które nakładają się na inne wpisywane polecenia, psując ich czytelność (ale nie składnię), można posłużyć się poleceniem konfiguracyjnym linii konsoli: **logging synchronous**. Komenda ta zablokuje nakładanie się wyświetlanych komunikatów na aktualnie wpisywane polecenie. Do wyłączenia polecenia debug służy standardowo składnia **no debug śledzony_proces**. Przykładowo polecenie **no deb all** wyłącza wszystkie procesy śledzenia.

10. Konfiguracja protokołu SNMP

Protokół SNMP (Simple Network Management Protocol) opracowany został do nadzorowania, diagnozowania oraz zdalnego zarządzania urządzeniami pracującymi w sieci TCP/IP. Wyróżniamy dwa podstawowe składniki w architekturze SNMP: oprogramowanie agenta, zwykle zaszyte w urządzeniu sieciowym oraz oprogramowanie menedżera SNMP, dostarczane na przykład jako specjalizowana aplikacja (p. rysunek).

Komunikacja między menedżerem i agentem, realizowana przy wykorzystaniu standardowego zestawu poleceń, pozwala menedżerowi zebrać podstawowy zestaw informacji o urządzeniu, na którym pracuje agent. Informacje, które menedżer może uzyskać od agenta zdefiniowane są w postaci obiektów w bazach danych MIB (Management Information Base). Każdy obiekt w bazie ma swój unikatowy identyfikator, poprzez który menedżer ma do niego dostęp. Typowe polecenia, za pomocą których menedżer uzyskuje informacje o określonych obiektach to: GET i GET-NEXT, natomiast poleceniem SET menedżer wymusza ustawienie wartości wybranego obiektu. Dodatkowo agent może z własnej inicjatywy wysyłać do menedżera komunikaty typu TRAP, co dzieje się na skutek wystąpienia pewnych zdarzeń. System operacyjny routera Cisco wyposażony jest w oprogramowanie agenta SNMP, ale do poprawnej pracy wymaga dodatkowej konfiguracji. Aby agent zaakceptował polecenie przysyłane od menedżera. musi być spełniony warunek przynależności do tej samej społeczności SNMP (community). Nazwę społeczności, do której należy agent (router Cisco) można zdefiniować już w dialogu konfiguracyjnym lub później globalnym poleceniem konfiguracyjnym **snmp-server community**. W poleceniu tym można też podać tryb dostępu do agenta: **RO** (tylko do odczytu - polecenia GET i GET-NEXT) bądź **RW** (do odczytu i zapisu - również polecenie SET) oraz numer standardowej listy dostępu, dzięki której można określić dozwolone adresy IP dla menedżerów przysyłających żądania. Do standardowych zdarzeń zachodzących na routerze Cisco, które powodują wysłanie komunikatu Trap do wybranego menedżera należy błąd uwierzytelnienia. Jest to przypadek, gdy do agenta przychodzi żądanie z obcej społeczności. Oprócz informowania o próbach nieuprawnionego dostępu, agent wysyła typowo do swojego menedżera komunikaty Trap dla zdarzeń ponownego uruchomienia routera bądź zmiany stanu interfejsu. Inne komunikaty typu Trap wysyłane przez agenta konfiguruje się poleceniem **snmp-server host**. Komenda ta pozwala określić adres IP menedżera SNMP, nazwę społeczności menedżera oraz rodzaje komunikatów Trap, które będą do menedżera wysyłane.

Poniżej przedstawiamy przykład konfiguracji protokołu SNMP. Zauważmy, że router może należeć do kilku społeczności. Dla społeczności Public włączona jest opcja RO (tylko do odczytu), dla społeczności Private włączony jest pełen dostęp (RW). W przypadku społeczności Private ustawiono kontrolowanie adresu IP menedżera poprzez listę dostępu nr 5. Ostatnia komenda definiuje adres IP menedżera, do którego wysyłane będą komunikaty Trap, określa też rodzaj wysyłanych komunikatów trap. W tym przykładzie router C2600 informować będzie swojego menedżera o zdarzeniach dotyczących protokołu ISDN oraz o zmianach w konfiguracji.

```
Router(config)#snmp-server community Public RO
Router(config)#snmp-server community Private RW 5
Router(config)#snmp-server host 131.107.10.245 Public isdn config
```

Programy graficzne przeznaczone do zdalnego zarządzania routerem Cisco bardzo często opierają swoje działanie na protokole SNMP. W takim przypadku niezbędne będzie określenie właściwej nazwy społeczności, w której pracuje router. Dodatkowo, aby ułatwić zarządzanie, na routerze można skonfigurować dwa parametry opisowe, określające położenie routera oraz osobę kontaktową. Parametry te definiuje się w postaci łańcuchów znaków za pomocą polecenia **snmp-server location** oraz **snmp-server contact**.

10. Przykładowy skrypt konfiguracyjny

```
Router #sh runn
Current configuration:
version 11.3
no service password-encryption
! Nazwa routera
hostname C2600
! System operacyjny wczytywany będzie z serwera TFTP
boot system /2600/C2600-i-mz.113-10.T 131.108.1.250
! zaszyfrowane hasło enable secret
enable secret 5 $1$souK$dTxfqZuhZCFSE/figBoA41
! nieszyfrowane hasło enable password
enable password haslo2
! Dla interfejsu Ethernet 0/0 zdefiniowano 2 adresy IP
interface Ethernet0/0
ip address 212.1.1.1 255.255.255.0 secondary
ip address 131.108.1.1 255.255.255.0
! Dla S0/0 (DCE) zdefiniowano przepustowość, opóźnienie i zegar
interface Serial0/0
ip address 131.107.11.1 255.255.255.0
no ip mroute-cache
bandwidth 128
delay 2000
clockrate 56000

! interface Ethernet0/1
ip address 131.109.1.1 255.255.255.0
! Dla S0/1 (też DCE) przepustowość i opóźnienie są domyślne
interface Serial0/1
ip address 131.107.12.1 255.255.255.0
clockrate 56000
! Routing nieklasowy
ip classless
! Społeczność SNMP Public pozwala tylko na odczyt informacji (RO)
snmp-server community public RO
! Port konsoli nie jest chroniony hasłem
line con 0
line aux 0
! Linie terminali wirtualnych (telnet) są chronione hasłem
line vty 0 4
password haslo3
login
end
```

LITERATURA

[1] PC Kurier – Archiwum „Dialogi i polecenia ”.
[2] PC Kurier – Archiwum „Zabezpieczenie i diagnostyka”.
[2] Leinwand Allan, Pinsky Bruce „ Konfiguracja routerów Cisco- Podstawy“