Router Cisco ISR4321/K9

Wprowadzenie

Routerem zawiaduje system operacyjny *IOS*[1] (*Internetwork Operation System*) opracowany przez Cisco, zapisany na pamięci ***flash*** (zajmuje kilkanaście MB na karcie o pojemności 64MB, posiada rozszerzenie **.bin,* a jego pełna nazwa dostępna jest po wydaniu polecenia "*show version*": "*System image file is 'nazwa.bin'*"). Rozmiar pamięci *flash* można sprawdzić przez wydanie polecenia "*show version*" ("*8192K bytes of processor board system flash [Read ONLY]*").

System uruchamiany jest przez program rozruchowy (tzw. *Bootstrap* zapisany na **ROM**) po przejściu procedury POST (*Power-On Self Test*). Ładowanie systemu sygnalizowane jest na ekranie w postaci ciągu znaków "########". Po załadowaniu IOS z pamięci FLASH do **RAM**, system (a konkretnie program "*configuration register*" znajdujący się na **NVRAM** [czarna kość na płycie głównej routera]) szuka i wczytuje plik konfiguracyjny (*config.text,* czyli *startup-config*) znajdujący się także w **NVRAM** (polecenie "*show version*": "*32K bytes of non-volatile Configuration memory*"). Jeśli go nie znajdzie, uruchamia kreator konfiguracji (*setup mode*).

Do pamięci **RAM** (polecenie "*show version*": "*...with 2048K/2048K bytes of memory*", gdzie pierwsza wartość wskazuje pamięć RAM procesora, a druga to współdzielona pamięć buforowania I/O) wczytywana jest również tablica routingu, tablica ARP, bufor pakietów.

Na pamięci **ROM** znajduje się okrojona wersja systemu IOS (Lite IOS; na wypadek, gdyby pełna wersja nie mogła być użyta) oraz oprogramowanie diagnostyczne.

Router można konfigurować w trybie graficznym (okrojona wersja) lub w trybie tekstowym CLI (*Command-Line Interface*). Pierwsza konfiguracja musi odbywać się przez port ethernetowy *CONSOLE* (z tyłu obudowy) za pomocą kabla szeregowego *RJ-45 --> RS-232*. Można także użyć kabla USB podłączanego do portu USB *CONSOLE*.

Program za pomocą którego można połączyć się z konsolą routera to w obu przypadkach:

- **PuTTY** - *Session / Connection Type: Serial / Serial line: COM1 (lub COM3), Speed: 9600*;
- **Tera Term**;
- **HyperTerminal**;
- **telnet** - klient telnet (tryb tekstowy) nie jest domyślnie zainstalowany w systemie Windows; jego instalację przeprowadzamy za pomocą: *Panel sterowania / Programy i funkcje / Włącz lub wyłącz funkcje systemu Windows / Klient Telnet;*

Domyślny użytkownik: *cisco* *(lub "admin", lub puste pole).*

Domyślne hasło: *cisco* *(lub brak; Uwaga: Na początku (przy ustawieniach fabrycznych) system poprosi nas o zdefiniowanie loginu i hasła).*

Domyślne IP: brak *(należy dopiero utworzyć; przykład poniżej)*

Porty fizyczne

GE MGMT - zarządzanie routerem;

USB typu B - połączenie z konsolą (np. przy użyciu *PuTTY*);

[1] Nie mylić z iOS (*Internet Operating System*) stworzonym przez Apple.

AUX (*auxiliary*) - wtyczka RJ45, połączenia VoIP (połączenia głosowe), czyli za pomocą modemu i połączenia komutowanego (do portu podłączamy modem), dzisiaj rzadko używane; można także bezpośrednio podłączyć do tego portu komputer z uruchomionym emulatorem terminala;

GE 0/0/1 RJ-45 - ethernet (*copper cable*);

GE 0/0/0 SFD - łącze optyczne (*fiber-optic*);

NIM - gniazdo rozszerzeń, czyli moduły, np. *Access Point*, *DSL*, interfejsy szeregowe WAN:

- duży *Serial-5in1* z WIC i kablem DB60 (drugi koniec kabla z wtyczką V.35 podłączany jest do urządzenia CSU/DSU otrzymanego od ISP, chyba że sam router ma port CSU/DSU, to wtedy łączymy go za pomocą ethernetowej skrętki T1 z odpowiednim wzorem skręcenia);

- mały *SmartSerial* z HWIC [*HighSpeedWIC*]);

Info: Za pomocą kabli DB60-V.35 można także połączyć dwa routery (wtyczki DB60 mają postać męską i żeńską do łączenia dwóch kabli tego typu ze sobą).

Uwaga: W systemie *Cisco IOS*, dwa interfejsy tego samego routera nie mogą należeć do tej samej podsieci. Każdy z portów ma własne IP i tworzy osobną podsieć.

Mechanizmy przekazywania pakietów

Przełączanie procesorowe - każdy pakiet trafia do procesora, który sprawdza IP w swojej tablicy powiązań i przekierowuje pakiet do danego portu. Czynność ta powtarzana jest dla każdego osobnego pakietu. Rozwiązanie stare i bardzo powolne.

Przełączanie szybkie - tylko pierwszy pakiet jest przekazywany do procesora, który sprawdza IP w swojej szybkiej pamięci *cache* (*FIB - Forwarding Information Base*); każdy następny pakiet o tym samym IP docelowym nie jest już analizowany przez procesor, lecz jest przekierowywany na ten sam port, co poprzedni w oparciu o zapisy w szybkiej pamięci *cache*.

Przekazywanie ekspresowe (*CEF - Cisco Express Forwarding*) - wpisy w tabeli powiązań (FIB) i w tabeli przyległości są dokonywane tylko wtedy, gdy topologia sieci ulegnie zmianie, a nie wraz z nadejściem każdego nowego strumienia pakietów; tabele są już wcześniej utworzone wraz z osiągnięciem zbieżności sieci. Jest to rozwiązanie najszybsze i polecane.

Tryby zarządzania systemem

Router> *(tryb użytkownika z ograniczeniami, tzw. User Exec Mode, poziom 1)*

Router# *(tryb uprzywilejowany, administratora, tzw. Privileged Exec Mode, poziom 15)*

Router (config)# *(tryb konfiguracji globalnej)*

Router (config-if)# *(tryb konfiguracji szczegółowej: konfiguracja interfejsu)*

Router (config-router)# *(tryb konfiguracji szczegółowej: konfiguracja routingu)*

Router (config-line)# *(tryb konfiguracji szczegółowej: konfiguracja dostępu)*

Uwaga: Wydając polecenie logowania "enable", tak naprawdę (w domyśle) wydajemy polecenie "enable 15", gdzie 15 jest najwyższym numerem poziomu uprawnień. Po zdefiniowaniu innych poziomów, możemy wydawać polecenia typu "enable 6" (logowanie się do poziomu 6).

Zapis ustawień

Wszelkie dokonane ustawienia routera zapisujemy za pomocą komendy:

Router# **copy running-config startup-config** *(zapis ustawień do pamięci trwałej NVRAM)*

Router# **copy running-config slot0** *(skopiowanie ustawień na kartę pamięci)*

Router# **show flash: filesys** *(zawartość pamięci flash, czyli system operacyjny)*

Router# **erase nvram** *(bardzo niebezpieczne polecenie, kasuje plik startowy; dlatego należy wcześniej wykonać kopię tego pliku; w razie potrzeby, należy skopiować plik z innego identycznego routera)*

Router# **erase startup-config** *(jeśli chcesz usunąć konfigurację początkową)*
Tworzenie kopii zapasowej na serwerze FTP:
Router# **ip ftp username anonymous**
Router# **ip ftp password twoj@adres.email**
Router# **copy flash ftp** *(kopiuje system IOS na serwer FTP)*
Router# **copy running-config ftp** *(kopiuje konfigurację routera na serwer FTP)*
adresIP
nazwaZdalnejKopii
lub
Router# **copy running-config tftp** *(należy podać IP serwera oraz nazwę pliku do zapisu)*

Router# **copy running-config usbflash0:/** *(kopiowanie obecnej konfiguracji do katalogu głównego USB)*
Router# **copy usbflash0:/***nazwaPlikuKonfiguracji* **running-config**

Router# **copy ftp: running-config** *(przywracanie kopii konfiguracji ze zdalnego serwera FTP)*
lub
Router# **copy tftp running-config**

Router# **copy ftp flash** *(kopiuje system IOS z serwera FTP do routera; seria znaków '!!!!!!' oznacza pobieranie pliku)*
lub
Router# **copy ftp://*naszLogin:naszeHasło@192.168.17.2/nazwa-kopii* running-config**

Ustawianie IP

Router> **enable**
Router# **show interfaces**
Router# **show ip interface brief** *(pokazuje skrótowy obecny wykaz numerów IP)*
Router# **config t**
Router(config)# **interface FastEthernet0/0**
Router(config-if)# **ip address 192.168.10.1 255.255.255.0**

lub (dla IPv6):
Router# **show ipv6 interface brief**
Router(config)# **ipv6 unicast-routing** *(aktywowanie routera do trybu IPv6, gdyż routery Cisco domyślnie pracują w trybie IPv4; w tym momencie router zacznie rozsyłać rozgłoszenia ICMPv6 Router Advertisment, co pozwoli mu automatycznie skonfigurować IP oraz bramę domyślną)*
Router(config-if)# **ipv6 enable** *(automatycznie generuje adres IPv6 lokalny)*
Router(config-if)# **ipv6 address 2001:0DB8:ACAD:0001:/64** *(statyczny globalny typu unicast)*
Router(config-if)# **ipv6 address FE80::1 link-local** *(statyczny lokalny; ten sam adres może być nadany innym interfejsom routera, gdyż musi być unikalny tylko w ramach podsieci)*
Router(config-if)# **ipv6 address 2001:0DB8:ACAD:1::/64 eui-64** *(w tym przypadku prefiks sieci / adres sieci jest stały / statyczny, a druga część adresu IPv6 - identyfikator interfejsu - jest generowana w oparciu o adres MAC [np. 00:AB:29:8C:3E:00] uzupełniony w środku przez FF:FE i przez dodanie siódmego bitu w systemie binarnym; więc cały adres po wygenerowaniu będzie miał postać: 2001:0DB8:ACAD:1:**2AB:29FF:FE8C:3E00**/64)*
Uwaga: Każdy z portów może mieć wiele adresów IPv6 zarówno lokalnych, jak i globalnych.

Router(config-if)# **description** *Siec domowa*
Router(config-if)# **no shutdown** *(czyli włączamy / uruchamiamy interface)*
Router(config-if)# **exit**
Router# **copy running-config startup-config** *(zapis ustawień do pamięci trwałej NVRAM)*
Router# **show ipv6 interface gigabitethernet 0/0**

Ustawianie IP lookback

Router(config)# **interface lookback 0**
Router(config-if)# **ip address 127.0.0.1 255.0.0.0**
Uwaga: Na routerze można utworzyć wiele pętli zwrotnych z różnymi IP i maskami. Loopback to po prostu wirtualny interface, do którego nie będzie podłączone żadne urządzenie.

Ustawianie IP zarządzania

Router(config)# **interface vlan 1**
Router(config-if)# **ip address 192.168.10.10 255.255.255.0**
Router(config-if)# **no shutdown**

Ustawianie routingu

Istnieją trzy rodzaje wyznaczania sieci i trasy:

- **DR** - *default route*, pasuje tutaj każdy adres;
- **SR** - *summary route*, czyli router z włączoną funkcją *auto-summary*, będzie sumował sieci 172.16.0.0/16, 172.17.0.0/16, 172.18.0.0/16 i wysyłał info, że ma sieć 172.16.0.0/14 (np. RIPv2 jest protokołem bezklasowym, ale patrzy na adresy IP w sposób klasowy, nie zna ich masek, więc dla niego te trzy sieci są jedną); sumaryzacja (agregacja) możliwa jest także wtedy, gdy trasa do kilku sieci przebiega przez jeden router (wtedy wystarczy znać trasę do tego routera i poszerzyć trochę maskę);
- **FR** - *floating route* (trasa pływająca; gdy mamy dwie trasy, domyślnie router wysyła dane przez obie równoważąc ruch; chcemy jednak aby ta druga była wykorzystana tylko w przypadku awarii tej pierwszej - regulujemy to więc określaniem *dystansu administracyjnego*);

Router# **show ip route**
Router# **show ipv6 route**
Router# **show ip protocols** *(jakie protokoły routingu są już w użyciu)*
Info: Kolumna "*Źródło trasy*" raportuje, w jaki sposób router dowiedział się o trasie do konkretnej sieci. I tak:

C - sieć bezpośrednio podłączona (*connected*) np. przez przełącznik;

L - sieć lokalna;

D - dynamicznie (na podstawie informacji uzyskanych od innego routera, protokół EIGRP);

S - statycznie (administrator wprowadził);

O - dynamicznie od innych routerów, w oparciu o protokół OSPF (*Open Shortest Path First*).

Kolumna "*Dystans administracyjny*" mówi o poziomie zaufania do danego źródła informacji.
Kolumna "*Metryka*" mówi o jakości trasy prowadzącej do celu (im niższa wartość - tym lepiej).
Router zna zawartość sieci, które są do niego fizycznie podłączone i w tym wypadku nie trzeba konfigurować routingu. Nie zna natomiast sieci, które są podłączone do sąsiadującego routera - w tym przypadku należy skonfigurować tablicę routingu.

Routing statyczny:

Stosowany w małych sieciach, bardziej bezpieczny (bo nie rozsyła ogłoszeń), nie obciąża routera.

Router(config)# **ip route 192.168.30.0 255.255.255.0 10.0.0.2** *(pakiety kierowane dla sieci 192.168.30.0/24, której router nie zna - przesyła do drugiego routera 10.0.0.2, który tę sieć zna)*

lub

Router(config)# **ip route 192.168.30.0 255.255.255.0 Serial0/0/0** *(metoda szybsza niż w przypadku podawania IP)*

lub

Router(config)# **ip route 192.168.30.0 255.255.255.0 Serial0/0/0 10.0.0.2** *(w pełni określona trasa statyczna)*

Definicja bramy domyślnej:

Router(config)# **ip route 0.0.0.0 0.0.0.0 Serial0/0/0** *(router ma tylko jedno wyjście przez port Seria0/0/0, więc: pakiety kierowane do jakiejkolwiek sieci o jakiejkolwiek masce kieruj na port Seria0/0/0; skrócona forma maski to /0 - czyli żaden bit nie musi być dopasowany, aby być przekierowanym na tę trasę)*

Gdy chcemy tę statyczną trasę domyślną rozpropagować do innych routerów za pomocą protokołu RIPv2:

Router(config)# **router rip**

Router(config-router)# **default-information originate**

Trasa domyślna w przypadku IPv6:

Router(config)# **ipv6 unicast-routing** *(włączenie routingu IPv6)*

Router(config)# **ipv6 route ::/0 Serial0/0/0**

lub

Router(config)# **ipv6 route 2001:0DB8:ACAD:1::/64 2001:0DB8:ACAD:3::1**

lub w pełni określona trasa:

Router(config)# **ipv6 route 2001:0DB8:ACAD:1::/64 Serial0/0/0 2001:0DB8:ACAD:3::1**

oraz trasa domyśla:

Router(config)# **ipv6 route ::/0 2001:DB8:ACAD:4::2**

Router# **show ipv6 route**

Routing dynamiczny RIPv2 (*Routing Information Protocol*):

Info: Protokół "bramy wewnętrznej". Najpierw wykrywa sieci bezpośrednio do niego podłączone a następnie rozgłasza sąsiadom co 30 sekund informacje o o nich nawet wtedy, gdy nic się nie zmieniło (używa do tego celu protokołu UDP w trybie *multicast* na adres 224.0.0.9:520; RIPv1 wysyłał rozgłoszenia na *broadcast*). Inne routery z protokołem RIP odbierają te informacje i wpisują do swojej tablicy routingu, po czym rozgłaszają swoją tablicę następnym sąsiednim routerom. Po pierwszym rozgłoszeniu mają informację jedynie o sieciach podłączonych bezpośrednio do swoich sąsiadów. Dopiero następne rozgłoszenia zwiększają zasięg informacji (zasięg zapisują za pomocą ilości przeskoków). Maksymalny zasięg takiego rozgłoszenia wynosi 15 skoków. Router używa przy tym mechanizmu "podzielonego horyzontu" (aby zapobiec nieskończonym pętlom), który zapobiega wysyłaniu informacji z tego samego interfejsu, z którego została już odebrana.

Protokół wybiera trasy w oparciu tylko o ilość przeskoków, czyli metrykę (w przeciwieństwie do protokołów OSPF i EIGRP [protokół własnościowy *Cisco*], które biorą pod uwagę także obciążenie poszczególnych sieci, ich szybkość, dystans administracyjny [wiarygodność źródła trasy]). Ustalanie najlepszej trasy odbywa się dopiero po osiągnięciu pełnej zbieżności (czyli to fazie pełnego wielokrotnego rozgłoszenia) i oparte jest o algorytm Bellmana-Forda.

Router(config)# **router rip** *(włączamy dostęp do konfiguracji RIP)*

Router(config-router)# **version 2** *(ma używać RIPv2 zamiast domyślnego RIPv1)*

Router(config-router)# **no auto-summary** *(wyłączamy domyślną sumaryzację sieci)*

Router(config-router)# **network *IP_sieci1*** *(podajemy mu sieci, które są do niego bezpośrednio podpięte i które ma rozgłaszać innym routerom)*

Router(config-router)# **network *IP_sieci2***

itd.

Router(config-router)# **passive-interface Fa0/0** *(wyłączamy wysyłanie rozgłoszeń na ten interfejs, gdyż tam nie ma żadnych routerów)*

Uwaga: Jeśli router jakąś sieć współdzieli z innym routerem i nie ma innych sąsiadów, nie musi jej rozgłaszać.

Router# **show ip protocols** *(upewniamy się, że sumaryzacja jest wyłączona)*

*Automatic network summarization **is not** in effect...*

Router# **show ip rip database**

Routing dynamiczny RIPng (*RIP New Generation*):

Protokół obsługujący IPv6.

Router(config)# **ipv6 unicast-routing** *(włączamy RIPng)*

Router(config)# **interface gigabitethernet 0/0** *(konfiguracja tego routingu będzie odbywać się na konkretnym interfejsie, w przeciwieństwie do zwykłego RIPv2)*

Router(config-if)# **ipv6 rip RIP-AS enable** *(RIP-AS to domena routingu)*

Router(config-if)# **ipv6 rip** *Test1* **default-information originate** *(rozsyłanie statycznej trasy domyślnej)*

Router(config-if)# **no shutdown**

Router# **show ipv6 protocols** *(upewniamy się, że wszystko jest w porządku)*

Router# **show ipv6 route**

Routing dynamiczny OSPFv2 (*Open Shortest Path First*):

Protokół "bramy wewnętrznej", oparty o "stan łącza", szybko uzyskuje zbieżność, ale mocno obciąża router. Najpierw wykrywa, czy jego interfejsy są włączone, czy posiadają IP, jaki to jest typ łącza (*Ethernet* czy *Serial*), koszt łącza. Potem wysyła do sąsiadów pakiety *HELLO* (ID, priorytet), co 10 sekund. Jeśli na jakimś interfejsie odbierze pakiet *HELLO*, wysyła w zamian pakiet LSP (*Link-State Packet*) zawierający stan swoich łączy oraz odbiera pakiety LSP od innych zapisując je w swojej bazie danych i na tej podstawie tworzy mapę topologii. Router co jakiś czas ponownie wysyła pakiet *HELLO*, aby podtrzymać znajomość tworząc tzw. "przyległość". Jeśli przyległy router nie odpowie pozdrowieniem, uznany zostanie za nieosiągalny i kończy się "przyległość". Pakiety LSP wysyłane są ponownie tylko w przypadku zmiany topologii sieci. Koszt: bierze pod uwagę nie ilość przeskoków, ale szybkość łącza (szerokość pasma) opierając się na algorytmie SPF (*Shortest Path First*) Edsgera Dijkstry.

Router(config)# **router ospf**

Routing dynamiczny EIGRP (*Enhanced Interior Gateway Routing Protocol*):

Protokół "bramy wewnętrznej" opracowany przez *Cisco*. W komunikacji (*multicast* / *unicast*) używa wyrażeń: *HELLO, Update, Query, Reply, Acknowledge*. Tworzy tablicę sąsiadów, tablicę topologii i najlepszą trasę (algorytm *DUAL - Diffusing Update Algorithm*). Metrykę tworzy w oparciu o: czas dostarczenia pakietu, szerokość pasma, natężenie ruchu, niezawodności łącza.

Istnieją dwie grupy protokołów:

- **IGP** (*Interior Gateway Protocols*) - stosowany w ramach pojedynczego AS (*Autonomic System*; pojedynczy system autonomiczny, pojedyncza jednostka organizacyjna, np. ISP lub firma, która zawsze posiada wiele podsieci; każdy AS ma nadany swój indywidualny identyfikator); maksymalnie są w stanie obsłużyć ok. 4 tysięcy podsieci;
- **EGP** (*Exterior Gateway Protocols*) - skalowalny routing między systemami autonomicznymi; (Uwaga: EGP to także nazwa starego nieużywanego już protokołu);

Dystans administracyjny (*Administrative Distance*) określany jest przez IOS w przypadku, gdy na routerze działają dwa różne dynamiczne protokoły routingu określające trasę w oparciu o różne kryteria (różne metryki). IOS bierze wtedy pod uwagę dystans administracyjny (im mniejsza liczba, tym lepiej):

- trasa bezpośrednio dołączona;
- trasa statyczna: **1** *(będzie miała zawsze pierwszeństwo przed trasami dynamicznymi; zalecana w przypadku tras do sieci szczątkowych [stub network], czyli mających jedną trasę)*;
- protokół **eBGPv4** (*external Border Gateway Protocol*): **20**; używany między ISP (*Internet Service Providers*); pochodzi z 1995 roku, a wersja obsługująca IPv6 (BGP-MP) pochodzi z 1999; należy do grupy protokołów wektorowych trasy EGP i jest jedynym protokołem "bramy zewnętrznej" (używany jest do komunikacji między wieloma systemami autonomicznymi / domenami routingu, odpowiada za wymianę informacji o podsieciach między AS); używa protokołu TCP (port 179) jako warstwy transportowej, każda zmiana w sieci powoduje wysłanie zawiadomienia o aktualizacji; obecnie jest to **jedyny** protokół z grupy protokołów EGP i zawiera spis prawie pół miliona tras; decyzję o wyborze trasy podejmuje w oparciu o aż 14 atrybutów i nie występują tutaj trasy o takiej samej metryce; sąsiedztwo w tym protokole ustawiane jest zawsze statycznie; wolno osiąga zbieżność (celowo);
- protokół **EIGRP** (*Enhanced Interior Gateway Routing Protocol*; trasa wewnętrzna): **90** *(pasmo, opóźnienie, obciążenie, niezawodność; tylko w przypadku tego protokołu można stosować "nierówne obciążenie" podczas równoczesnego wysyłania pakietów przez dwie trasy)*; protokół z grupy IGP (maksymalnie kilka tysięcy podsieci), pochodzi z 1992 roku, a wersja obsługująca IPv6 pochodzi z 2005 roku; należy do grupy protokołów wektorowych odległości (wektor = kierunek przesyłu, czyli IP lub interfejs), czyli nie jest świadom topologii sieci; maksymalna ilość przeskoków to 255, rozgłoszenia multicastowe na adres: 224.0.0.10; starsza klasowa wersja tego protokołu to **IGRP** (*Interior Gateway Routing Protocol*) o dystansie **100** (pochodzi z 1985 roku);
- protokół **OSPFv2** (*Open Shortest Path First*): **110** (szerokość pasma); protokół z grupy IGP (maksymalnie kilka tysięcy podsieci), rozgłoszenia multicastowe (cykliczne „*Hello*” co 10 sekund) na adres: 224.0.0.5 oraz 224.0.0.6; brak odpowiedzi po 40 sekundach ustawia metrykę takiego routera na „martwy”; pochodzi z 1991 roku, a jego wersja obsługująca IPv6/IPv4 (**OSPFv3**) pochodzi z 1999 roku; należy do grupy protokołów stanu łącza (jest świadom topologii sieci z własnego punktu widzenia i wymienia się tą bazą z innymi), a aktualizacja wysyłana jest tylko wtedy, gdy zmieni się topologia; jest opakowany przez pakiet IP; szybko osiąga zbieżność; korzysta z algorytmu Dijkstry (jak w nawigacji) przy ustalaniu najlepszej trasy;
- protokół **IS-IS** (*Intermediate-System-to-Intermediate-System*): **115**; opracowany przez ISO, pochodzi z 1990 roku, a wersja obsługująca IPv6 pochodzi z 2000 roku; należy do grupy protokołów stanu łącza i jest protokołem "bramy wewnętrznej", choć używany jest także przez ISP; opiera się na algorytmie SPF Edsgera Dijkstry; szybko osiąga zbieżność;
- protokół **RIPv2** (*Routing Information Protocol*): **120** (ilość przeskoków); rozgłoszenia multicastowe co 30 sekund na adres: 224.0.0.9; pochodzi z 1993 roku; jego wersja obsługująca IPv6 (czyli **RIPng**) pochodzi z 1997 roku; należy do grupy protokołów wektorowych odległości (do 15 hopów maksymalnie); jest opakowany przez protokół UDP 520; wolno osiąga zbieżność (z natury swojej); jeśli nie odpowie w ciągu 180 sekund, uważa się go za martwy, a po kolejnych 120 sekundach wpis usuwany jest w metryki;
- protokół **EGP** (*Exterior Gateway Protocol*): **140**; pochodzi z 1982 roku;

Uwaga: Domyślny dystans administracyjny można zmieniać. Jeśli dwie trasy mają identyczną metrykę, pakiety będą wysyłane obiema trasami (rozkładanie obciążenia). Dystans administracyjny określony jest przez kolor czerwony, a metryka przez kolor niebieski:

Router# **show ip route**

S 10.2.0.0 [1/0] via 172.16.2.2 00:00:12 Serial0/0/0

Router(config)# **router ?** *(wyświetla możliwe protokoły routingu)*

Włączanie protokołu i jego konfiguracja:

Router(conf)# **router ospf 1**

Router(conf)# **network 192.168.0.0 0.0.0.255 area 0** *(stosujemy maski blankietowe [wild card bits], które zazwyczaj - upraszczając - są odwrotnością maski zwykłej; likwiduje to problem z sumaryzacją, która występowała w przypadku RIP)*

Router(conf)# **network 172.16.15.8 0.0.0.3 area 0**

Router(conf)# **network 172.16.15.0 255.255.255.252 area 0** *(Co się stanie, gdy podamy zwykłą maskę? Protokół domyśli się!)*

Info: Wartość parametru "*area*" określa administrator. Zazwyczaj w jednym obszarze gromadzi się do 50 routerów. Powyżej tej liczby, tworzy się osobny obszar, aby uniknąć nadmiernych rozgłoszeń. Każdy z obszarów (np. numer 12, numer 32) musi być podczepiony pod "*area 0*", która stanowi szkielet całej grupy routerów.

Router# **show ip ospf neighbor** *(ilu ma sąsiadów)*

Router(conf)# **default-information originate** *(ogłasza swoją trasę domyślną)*

Router(conf-if)# **bandwidth 64** *(szybkość na tym interfejsie ustawiamy na 64Kb/s)*

Uwaga: Chociaż router jest dla innych maszyn bramą domyślną, sam też może mieć taką bramę, którą nazywamy "bramą ostatniej szansy" (*Gateway of Last Resort*). Używana jest ona wtedy, gdy w tablicy routingu nie ma podanej określonej trasy. Gdy "brama ostatniej szansy" nie jest skonfigurowana - pakiet jest odrzucany, a do nadawcy wraca komunikat ICMP o nieosiągalności sieci.

Frame Relay

Stara technologia (wyparta przez ATM) może służyć jako pośrednik w sieci WAN, według schematu:

Router1 <----------> ***Cloud-PT*** <----------> *Router2*

Komunikacja oparta jest na **DTE** (*Data Terminal Equipment* - komputery, routery) oraz na pośredniczących między nimi urządzeniami *Frame Relay*, czyli **DCE** (*Data Communications Equipment*), które synchronizują połączenia między routerami i przełączają je (połączenia są typu *full-duplex*). Błędne ramki są kasowane, więc urządzenia powtarzają je.

Do chmury można podłączyć wiele routerów, gdzie każdy będzie połączony z każdym (sieć "*fully meshed*", *multipoint*) lub gdzie jeden router będzie połączony z drugim (sieć "*partially meshed*", *point-to-point*).

Urządzenia połączone są kablem szeregowym. W konfiguracji *Cloud-PT* programu *Packet Tracer*:

Se0/0/0 -->	*DLCI: 100*	*R1-do-R2*
Se0/0/1 -->	*DLCI: 101*	*R2-do-R1*
Frame Relay -->	*Serial0 - R1-do-R2*	*Serial1 - R2-do-R1*

gdzie **DLCI** (*Data Link Connection Identifier*) to unikatowy numer kanału służącego do połączenia (może istnieć wiele połączeń na jednym łączu fizycznym, jak w przypadku łączy TRUNK).

Skonfigurowane muszą być także same routery podłączone do *Cloud-PT*. Muszą one być w tej samej grupie IP.

Konfiguracja *Router1*:

Router(config)# **interface Serial0/0/0**

Router(config-if)# **encapsulation frame-relay** *(domyślna enkapsulacja w routerach Cisco to HDLC)*
Router(config-if)# **ip address 150.0.0.1 255.255.0.0**
Router(config-if)# **frame-relay interface-dlci 100**
Router(config-if)# **frame-relay lmi-type cisco**
Router(config-if)# **no shutdown**
Konfiguracja *Router2*:
Router(config)# **interface Serial0/0/0**
Router(config-if)# **encapsulation frame-relay**
Router(config-if)# **ip address 150.0.0.2 255.255.0.0**
Router(config-if)# **frame-relay interface-dlci 101**
Router(config-if)# **frame-relay lmi-type cisco**
Router(config-if)# **no shutdown**

NAT

Router z NAT zamienia w ramce prywatny adres źródłowy IP jakiegoś komputera na swój adres źródłowy publiczny. Czasami zmienia też źródłowy port (jeśli dwa komputery w sieci prywatnej wylosują ten sam port). Nie opakowuje ramki we własną ramkę (tak robi VPN). NAT w swojej własnej tablicy przetrzymuje powiązania, np.:
192.168.0.3:6000 *(prywatny)* → **20.0.0.2**:6000 *(publiczny; jeśli port powtarza się, to zamieni go na 6001)*

Router(config-if)# **ip nat outside** *(interfejs publiczny)*
Router(config-if)# **ip nat inside** *(interfejs wewnętrzny)*
Router(config)# **ip nat inside source static 192.168.0.2**
Router(config)# **ip route 200.0.0.0 255.255.255.240 se0/0/0**
Router# **show ip nat translations**
Router# **clear ip nat translation** *(wyczyści, ale pozostawi statyczne)*
Router(config)# **ip nat pool** *PULA_PUB IP_początkowe IP_końcowe* **netmask 255.255.255.240**
Router(config)# **access-list 1 permit 10.0.1.0 0.0.0.255**
Router(config)# **ip nat inside source list 1 pool** *PULA_PUB* **overload**

Serwer DHCP

Router> **enable**
Router# **configure terminal**
Router(config)# **service dhcp**
Router(config)# **ip dhcp pool marketing**
Router(dhcp-config)# **network 192.168.17.0 255.255.255.0**
Router(dhcp-config)# **default-router 192.168.17.1** *(informujemy serwer DHCP, gdzie jest domyślna brama)*
Router(config)# **ip dhcp excluded-address 192.168.17.1 192.168.17.10**
Router(dhcp-config)# **dns-server 192.168.17.1**
Router#**show ip dhcp binding**
Router(config)# **ip domain name teb**
Router(config)# **exit**

Dostęp przez SSH

Uwaga: Aby możliwe było stosowanie SSH (kryptografii) potrzebny jest system operacyjny IOS z końcówką "k9".

Router(config)# **show ip ssh** *(sprawdzamy, czy w ogóle protokół jest obsługiwany; jeśli komenda nie jest rozpoznawana - nie obsługuje)*

Router(config)# **hostname** *nowaNazwaRoutera*

Router(config)# **ip domain-name** *nazwaDomeny*

Router(config)# **crypto key generate rsa** *(utworzenie klucza jest tożsame z aktywacją SSH; wybieramy długość 2048 - większe bezpieczeństwo, ale dłuższy czas szyfrowania danych; wygenerowanie klucza jednokierunkowego jest konieczne do szyfrowania danych i zdalnego logowania się: połączenie oparte o hasło)*

Router(config)# **username** *robert* **password** *treśćHasła* *(tworzymy w systemie IOS użytkownika i hasło, aby uwierzytelniać połączenie lokalnie, a nie w oparciu o inny serwer)*

Router(config)# **ip ssh version 2** *(będziemy korzystać z wersji 2)*

Router(config)# **line vty 0 15**

Router(config-line)# **login local** *(wymuszamy lokalne logowanie za pomocą użytkownika)*

Router(config-line)# **transport input ssh** *(zdalny dostęp tylko przez ssh, nie przez telnet)*

Z klienta:

C:\> **ssh -l robert 192.168.10.1**

Aby sprawdzić, kto jest podłączony przez SSH:

Router# **show ssh**

Aby wyłączyć SSH, należy usunąć klucze:

Router(config)# **crypto key zeroize rsa**

Ustawienia czasu

Router> **show clock** *(pokazuje czas)*

Router# **clock set** *12:45:00 7 November 2019* *(ustawianie czasu / daty)*

Router (config)# **ntp server** *ntp1.tp.pl* *(synchronizacja z serwerem czasu)*

Router (config)# **sntp server** *ntp1.tp.pl* *(synchronizacja z serwerem czasu)*

Router# **show ntp associations** *(wyświetla ustawienia synchronizacji serwera czasu)*

Ustawienia bannerów

Ustawienie bannera (komunikatu) powitalnego:

Router (config)# **banner motd %** *(MOTD = Message Of The Day; zamiast znaku % można użyć dowolnego innego, który będzie oznaczał koniec komunikatu; banner pojawi się zaraz po połączeniu z routerem)*

==========

Witam na moim routerze!

Tutaj jakiś komunikat...

==========

%

Router (config)# **banner login %** *(pojawi się przed zalogowaniem; dobrze jest poinformować w tym miejscu, iż zabronione jest logowanie przez nieuprawnione osoby)*

Router (config)# **banner exec %** *(pojawi się po zalogowaniu)*

Tworzenie i reset haseł

Router (config)# **enable password** *mojeTajneHasło* *(tworzenie hasła niezaszyfrowanego do trybu uprzywilejowanego)*

Router (config)# **enable secret** *mojeTajneHasło* *(tworzenie hasła zaszyfrowanego za pomocą algorytmu MD5 do trybu uprzywilejowanego)*

Poniżej tworzymy hasło zabezpieczające do portu CONSOLE:

Router (config)# **line console 0** *(port konsoli nr 0)*

Router (config-line)# **password** *naszeNoweHasło* *(hasło może zawierać spacje oraz znaki specjalne)*

Router (config-line)# **login** *(wymuszamy uwierzytelnienie)*

Poniżej tworzymy hasło zabezpieczające do połączenia telnet / SSH:

Router (config)# **line vty 0 15** *(Virtual Terminal Line, ustawiamy operację na linie od 0 do 15, czyli wszystkie porty)*

Router (config-line)# **exec-timeout 10** *(wylogowanie w przypadku bezczynności przez 10 minut)*

Router (config-line)# **password** *naszeNoweHasło* *(hasło może zawierać spacje oraz znaki specjalne)*

Router (config-line)# **login** *(wymuszamy uwierzytelnienie)*

Router (config)# **no enable password** *mojeTajneHasło* *(usuwanie hasła)*

Router (config)# **username** *piotrek* **secret** *hasłoPiotrka* *(tworzymy użytkownika i jego hasło)*

Router (config)# **username krzysiek nopassword** *(tworzymy użytkownika "krzysiek" bez hasła)*

Router (config)# **login delay 8** *(opóźnienie 8 sekund przy logowaniu; zabezpieczenie przed atakami)*

Router (config)# **security passwords min-length 12** *(minimalna ilość znaków w haśle)*

Router (config)# **login block-for 120 attempts 3 within 60** *(blokuje na 120 sekund, gdy wystąpią 3 nieudane próby logowania w ciągu 60 sekund)*

Router (config)# **aaa new-model** *(tworzymy nowy model logowania / autentykacji użytkowników; AAA = Authentication Authorization Accounting)*

Router (config)# **aaa authentication login default local** *(do autentykacji użytkowników, router będzie używał lokalnej bazy danych [a nie np. serwera kerberos / radius)*

Router (config)# **aaa local authentication attempts max-fail 6** *(ustalamy ilość prób nieudanych logowań na 6; potem konto zostanie zablokowane)*

Router# **show aaa local user lockout** *(wykaz zablokowanych kont)*

Router# **clear aaa local user lockout username** *piotrek* *(odblokowanie konta "piotrek")*

Router# **show login failures** *(wykaz nieudanych logowań do routera)*

Router (config)# **no service password-recovery** *(polecenie blokuje odzyskiwanie hasła; nigdy tego nie rób!)*

Uwaga: Hasła domyślnie mogą być zapisywane w formie tekstu. Sprawdzamy, czy tak jest:

Router# **show running-config | include username**

Router (config)# **service password-encryption** *(włączamy szyfrowanie wszystkich haseł, obecne hasła zostaną zaszyfrowane; wyłączenie tej usługi nie spowoduje jednak odszyfrowania haseł uprzednio zaszyfrowanych)*

Przywrócenie ustawień fabrycznych (gdy znamy hasło):

Router> **enable**

Router# **write erase**

Router# **reload**

Przywrócenie ustawień fabrycznych (gdy nie znamy hasła / gdy router został zabezpieczony przez kogoś innego):

1. Po napotkaniu zapytania o nieznane nam hasło, należy na routerze przeprowadzić tzw. "twardy reset" (*power cycle*), czyli odłączyć od źródła zasilania na ok. 5 sekund, a następnie uruchomić ponownie, wciskając rytmicznie na klawiaturze klawisze: **Ctrl + Break** lub **Break** (zanim rozpocznie się ładowanie obrazu systemu, około 30 sekund, aż do momentu pojawienia się wyrażenia "*rommon 1>*"). Zamiast naciskać klawisz *Break*, można także wysłać sygnał *Break* z poziomu okna konsoli *PuTTY*: *Właściwości konsoli PuTTY / Special Command / Break*.

Current image running: Boot ROMO.

...

Last reset cause: PowerOn.

...

rommon>

2. Wydajemy polecenia:

rommon 1> **confreg 0x2142** *(lub "config 0x2142"; zmieniamy rejestr konfiguracyjny na taki, który ignoruje zawartość NVRAM)*

...

You must reset or power cycle for new config to take effect.

rommon 2> **reset** *(system jest ponownie bootowany, ale ignoruje zapisaną konfigurację; po ponownym uruchomieniu systemu, będzie dostępny tryb automatycznej konfiguracji; jeśli system "zatrzyma się" w jakimś miejscu dłużej, należy wcisnąć ENTER)*

...

System integrity status: 0x610

Rom image verified correctly

Last reset cause: LocalSoft.

##########################...

Uwaga: Jeśli system zapyta o ustawienia początkowe (tak dzieje się w przypadku, gdy system nie znajduje pliku startowego), odpowiadamy na wszystkie pytania "no" lub wciskamy Ctrl+C, aby je pominąć. Zapytanie o te ustawienia możemy wywołać w każdym momencie, wydając polecenie "setup" w trybie uprzywilejowanym.

Router> **enable** *(nie powinien pytać o hasło)*

Router# **copy startup-config running-config** *(lub "copy start run"; informacje kopiowane są z pamięci trwałej NVRAM [Nonvolatile Random Access Memory] do pamięci RAM; Uwaga: Gdy system zapyta, czy zapisać nowe ustawienia pod daną nazwą pliku, NIE wpisujemy "yes", tylko wciskamy ENTER!)*

Router# **show running-config** (*warto spojrzeć na obecną konfigurację; informacje są stronicowane [== More ==], aby przewijać strony, użyj spacji)*

Router# **show startup-config** (*warto także spojrzeć na starą konfigurację)*

Router# **conf t**

Router (config)# **enable secret** *noweHasło*

Router (config)# **config-register 0x2102** *(zmieniamy rejestr na domyślny, efekty będą widoczne dopiero po ponownym uruchomieniu systemu; domyślny rejestr ładuje obraz systemu z pamięci flash, a "startup-config" z pamięci NVRAM)*

Router (config)# **end**

Router# **copy running-config startup-config** *(zapisujemy bieżące ustawienia; działa także skrót komendy: "copy run start"; informacje zapisywane są do pamięci trwałej, czyli NVRAM [Nonvolatile Random Access Memory])*

Building configuration...

Router# **reload**

Kody rejestracyjne (wprowadzane albo w trybie "*config*" albo "*rommon*"):

- **0x0040** - ignoruje zawartość NVRAM;
- **0x2100** - ładuje *ROM Monitor Mode* do postaci "*rommon>*" (bootowanie ręczne za pomocą polecenia "b");
- **0x2101** - ładuje system *mini-IOS* z ROM do postaci "*router (boot)>*";
- **0x2102** - ładuje system z pamięci FLASH, a następnie konfigurację z NVRAM (odnosi efekt dopiero po ponowny restarcie); jest to domyślny tryb;
- **0x2142** - ładuje system z pamięci FLASH, ale nie ładuje domyślnej konfiguracji (*startup-config*);
- **0x8000** - tryb diagnostyczny, ignoruje zawartość NVRAM.

Uwaga: Wyrażenie "0x" oznacza, że liczby następujące po tym znaku są w systemie szesnastkowym. Aby zobaczyć obecnie załadowany tryb, należy użyć polecenia "show version".

ACL (Access Control List)

ACL proste:

W tym przypadku brany pod uwagę jest tylko adres źródłowy.

Router(config)# **access-list 1 deny 10.0.1.0 0.0.0.255** *(maska blankietowa!)*

Router(config-if)# **ip access-group 1 out** *(lista wyjściowa nr 1)*

Router# **show access-lists**

Każda lista powinna mieć na końcu akcję dla wszystkich pozostałych przypadków:

Router(config)# **access-list 1 permit any** *(pozwól wszystkim innym)*

W przypadku błędu:

Router(config)# **no access-list 1** *(kasowanie ACL)*

Tworzenie ACL (lista prosta):

Router(config)# **ip access-list standard** *nazwaRegułACL*

Router(config-std-nacl)# **deny 10.0.1.0 0.0.0.255**

Router(config-std-nacl)# **permit any**

Router(config-if)# **ip access-group** *nazwaRegułACL* **out** *(instalowanie listy na danym porcie)*

Tworzenie ACL (lista rozszerzona):

Router(config)# **ip access-list extended** *banowanieGrześka*

Router(config-std-nacl)# **deny ip host** *IP_Grześka* **host** *IP_Grażyny* *(Grzesiek ma zabroniony dostęp do komputera Grażyny)*

Router(config-std-nacl)# **permit ip host** *IP_Grześka IP_Jakiejś_Sieci* **0.0.0.255** *(pozwalam Grzesiowi)*

Router(config-std-nacl)# **permit tcp host** *IP_Grześka* **host** *IP_Serwera* **eq www** *(pozwalam Grzesiowi, ale tylko na połączenia z serwerem www)*

Router(config-std-nacl)# **deny ip host** *IP_Grzesia* **any** *(w innych przypadkach blokuję Grzesia)*

Router(config-std-nacl)# **permit ip any any** *(w innych przypadkach pozwalam)*

SNMP

Konfiguracja agenta SNMP:

Router(config)# **snmp-server community public ro** *(odczyt ustawiony na publiczny)*

Router(config)# **snmp-server community** *hasłoJakieś* **rw 50** *(lista reguł nr 50; prawo do zapisu uwarunkowane jest podaniem hasła i numerem IP z access-list)*

Router(config)# **access-list 50 permit 192.168.7.5** *(pozwalamy na dostęp zarządcy o określonym IP)*

Router(config)# **access-list 50 permit 192.168.7.6** *(zapasowy zarządca)*

Router(config)# **snmp-server enable traps** *(aktywancja „pułapek" na agencie)*

Router(config)# **snmp-server enable traps envmon temperature** *(„pułapka" dotyczy temperatury)*

Router(config)# **snmp-server host 192.168.7.2** *jawneHasło (agent wyśle alarm na adres IP zarządcy)*

Info: Rodzaje pułapek (alarmów) to: ***config*** (zmiany w konfiguracji), ***syslog*** (komunikaty o błędach), itp.

Inne polecenia

Uwaga: Obecność niektórych poleceń uzależniona jest od istniejącego systemu plików.

Router> *jakieśPolecenie* **?** *(pomoc na temat polecenia)*

Router (config)# **hostname** *nazwaRoutera (nadajemy albo zmieniamy nazwę routera)*

Router# **disable** *(wyjście z trybu)*

Router# **exit** *(wyjście z trybu)*

Router# **end** *(wyjście z trybu)*

Router# **ping** *(włączenie rozszerzonej i konfigurowalnej wersji narzędzia ping; znak '.' oznacza zablokowanie ruchu przez firewall na jakimś routerze)*

Router# **ping 192.168.0.3 source S0/0/0** *(określenie, przez który interfejs należy puścić pinga; zamiast nazwy interfejsu można podać IP tego interfejsu)*

Router# **show history**

Router# **show hosts** *(wyświetla zawartość pliku "hosts")*

Router# **ip hosts 192.168.17.53 komp12** *(dodawanie wpisu do "hosts"; aby go wykasować , należy go poprzedzić wyrażeniem "no")*

Router# **show arp** *(wykaz numerów MAC)*

Router# **show ip arp** *(powiązanie numerów IP z MAC; odpowiednik windowsowej komendy "arp -a")*

Router> **show cdp neighbors** *(pokazuje konfiguracje sąsiednich routerów wykrytych w oparciu o protokół CDP [Cisco Discovery Protocol]; dodanie "detail" powoduje wyświetlenie IP sąsiada)*

Router(config)# **no cdp run** *(wyłącza protokół CDP)*

Router(config-if)# **no cdp enable** *(wyłączenie rozgłaszania protokołu CDP na konkretnym interfejsie)*

Router# **reload** *(ponowne wczytanie / uruchomienie systemu)*

Router# **reload at 22:45 Nov 7**

Router# **reload in 150** *(ponowne załadowanie systemu nastąpi za 150 minut)*

Router# **show file systems** *(wyświetla informacje o zamontowanych dyskach / pamięciach)*

Router# **show version** *(wyświetla informacje o systemie)*

Router# **show slot0** *(wyświetla strukturę danych na karcie pamięci)*

Router# **format slot0** *(formatuje kartę pamięci)*

Router# **more** *slot0:jakiśPlik (wyświetla zawartość pliku tekstowego)*

Router# **mkdir** *slot0:nazwaFolderu (tworzenie folderu na karcie pamięci)*

Router# **cd** *slot0:nazwaFolderu (przejście do folderu)*

Router# **cd nvram:**

Router# **cd usbflash0:**

Router# **dir** *(wyświetlanie zawartości bieżącego folderu)*

Router# **do show ...** *(wykonaj komendę ignorując obecny tryb)*

Router# **delete** *nazwaPliku (usuwanie pliku)*

Router# jakieśPolecenie **| include** *jakieśWyrażenie (odpowiednik komendy grep w Linux, np. "show running-config | include password")*

Router# jakieśPolecenie **| exclude** *jakieśWyrażenie (wyświetla wszystko oprócz...)*

Router (config)# **ip http server** *(uruchomienie serwera http [jeśli nie był uruchomiony domyślnie], czyli umożliwienie połączenia przez przeglądarkę internetową, konfiguracja przez GUI)*

Router (config)# **ip http secure-server** *(uruchomienie serwera https, wygenerowanie pary kluczy)*

Router (config)# **ip http authentication local** *(logowanie do GUI odbędzie się na podstawie lokalnej bazy haseł)*

Router (config)# **secure boot-image** *(zabezpieczenie obrazu systemu IOS przed usunięciem przez złośliwego lub głupiego użytkownika)*

Router (config)# **secure boot-config** *(zapisanie obecnie działającej konfiguracji jako backup; można ją zobaczyć poprzez polecenie "show secure bootset")*

rommon 1> **dir**

Ostatnia aktualizacja: 1 sierpnia 2022.