

(nieoficjalne) Cisco FAQ PL

czyli najczęściej zadawane pytania o Cisco z odpowiedziami po polsku

Lukasz Bromirski <lukasz@bromirski.net> (koordynator)

v0.99(4) 30/01/2006 23:53:21

Spis treści

Rozdział 1. Sprawy porządkowe.....	5
Oświadczenie i licencja.....	5
Dostęp do CVS i Twój udział w tym projekcie.....	5
Lista pocztowa - jak i gdzie?.....	5
Rozdział 2. Pytania ogólne.....	6
Gdzie można poczytać o firmie Cisco i produktach tej firmy?.....	6
Do kogo zwrócić się o pomoc, jeśli chciałbym zbudować swoją sieć w oparciu o produkty Cisco?.....	6
Jak skontaktować się z pomocą techniczną Cisco?.....	6
Gdzie można uzyskać pomoc dotyczącą sieci i Cisco?.....	6
Skąd mogę pobrać nowsze oprogramowanie do swojego urządzenia Cisco?.....	7
Słyszałem, że aktywacja szyfrowania 3DES i ew. AES jest na PIXach darmowa - czy to prawda?.....	7
Czy są jakieś strony sympatyków Cisco z ciekawymi materiałami?.....	7
Rozdział 3. Dokumentacja.....	7
Gdzie w Internecie znaleźć dobre materiały o sprzęcie Cisco? Konfiguracja, przykłady, zalecenia?.....	7
Jakie polecacie książki po Polsku, do pracy ze sprzętem Cisco?.....	8
A jakie w ogóle książki polecacie, poświęcone sieciom oraz sprzętowi Cisco?.....	8
Jak zainstalować Cisco Documentation pod Windows tak, by nie trzeba było za każdym razem korzystać z krążka?.....	9
Jak zainstalować Cisco Documentation pod Linuxem/BSD?.....	10
Gdzie sprawdzić składnię konkretnego polecenia?.....	10
Rozdział 4. Certyfikacje Cisco.....	10
Jakie są poziomy certyfikacji Cisco?.....	10
Jakie egzaminy muszę zdać na poziomie Associate?.....	11
Jakie egzaminy muszę zdać na poziomie Professional?.....	11
Jakie egzaminy muszę zdać na poziomie Expert?.....	12
Gdzie mogę znaleźć dokładną listę tematów na dany egzamin?.....	12
Czy dla zdających są jakieś pomoce?.....	13
Czy po egzaminie mogę podzielić się ze znajomymi treścią pytań?.....	13
Rozdział 5. Podstawy pracy z urządzeniami Cisco.....	13
Jak podłączyć się do.....	13
...routera Cisco?.....	13
...Cisco PIX?.....	13
...przełącznika Cisco Catalyst serii 1000, 2000 lub 3000?.....	13
...przełącznika Cisco Catalyst serii 4000/4500?.....	14
...przełącznika Cisco Catalyst serii 6000/6500?.....	14
...sondy Cisco IDS serii 42xx?.....	14
...punktu bezprzewodowego AP350, 1120 lub 1200?.....	14
Podłączyłem się i...?.....	14
...w oknie terminala nic nie widzę?.....	14
...jak dostawać informacje o zdarzeniach na routerze na konsolę?.....	14
...jaki dokładnie mam router? Ile mam pamięci RAM/flash? Co oznaczają poszczególne linijki z polecenia `show version`?.....	15
...gdy pomylę się w poleceniu, router zaczyna robić dziwne rzeczy.....	16
...chciałbym zapisać konfigurację routera/PIXa/przełącznika?.....	16
...chciałbym wymazać konfigurację routera/PIXa/przełącznika?.....	16
...jakiego użyć oprogramowania do połączenia się z routerem?.....	16
...jakiego użyć oprogramowania do serowania plików tftp/ftp?.....	17
Mój router uparcie próbuje ściągnąć z sieci plik network-config, network-cfg lub cisco.net.cfg - o co chodzi?.....	17
Rozdział 6. Podstawy konfiguracji usług.....	17
DHCP.....	17
Co to są prywatne/niezarejestrowane adresy IP?.....	17
Czy router może pełnić rolę serwera DHCP?.....	17
Jak przydzielić interfejsowi adres z serwera DHCP?.....	18
Jak przekazać dalej zapytania DHCP?.....	18
SNMP.....	19

Jak uruchomić na routerze SNMP?.....	19
Logowanie zdarzeń.....	19
Chciałbym logować zdarzenia zachodzące na routerze do pamięci. Jak to zrobić?.....	19
Chciałbym logować zdarzenia zachodzące na PIXie do pamięci. Jak to zrobić?.....	19
Chciałbym logować zdarzenia zachodzące na routerze do serwera syslog. Jak to zrobić?.....	19
Chciałbym logować zdarzenia zachodzące na PIXie do serwera syslog. Jak to zrobić?.....	20
Czas.....	20
Jak ustawić zegar na routerze?.....	20
Jak ustawić zegar wg. serwerów czasu z Internetu?.....	20
Skonfigurowałem na swoim routerze NTP, ale zegar pozostaje niezsynchronizowany - a minęło już parę godzin.....	21
NAT.....	21
W jakich wersjach oprogramowania obsługiwany jest NAT, PAT oraz mapowanie portów z adresów publicznych na prywatne?.....	21
Chcę uruchomić NAT - mam jeden interfejs publiczny i jeden prywatny. Jak to zrobić?.....	21
Mam router z jednym interfejsem i chcę robić NAT - czy to wykonalne?.....	22
Chcę przekierować port 25/tcp z adresu publicznego routera do sieci wewnętrznej - jak to zrobić?.....	23
Jak sprawdzić, które interfejsy przypisane są do NAT i jak są skonfigurowane?.....	23
NAT mi nie działa - co może być źle?.....	23
SSH.....	24
Jak skonfigurować SSH?.....	24
Jak sprawdzić, czy serwer SSH jest włączony?.....	24
Rejestr konfiguracyjny routerów.....	24
Po zapisaniu konfiguracji i przeładowaniu routera, tracę konfigurację - dlaczego?.....	24
Co dokładnie oznaczają bajty z rejestra konfiguracyjnego?.....	25
Czy do ustawiania rejestru konfiguracyjnego można użyć jakiegoś narzędzia?.....	25
VLANy.....	25
Co to są VLANy?.....	25
Co to jest VLAN "natywny"?.....	26
Co mają na myśli ludzie mówiąc "router na patyku" (ang. router on a stick)?.....	26
Czy Cisco PIX może obsługiwać VLANy?.....	27
Jak skonfigurować na PIXie VLAN?.....	27
Jak sprawdzić.....	28
...ile interfejsów logicznych obsłuży router X?.....	28
...aktualne obciążenie procesora?.....	28
...historyczne obciążenie procesora?.....	29
...w liście procesów tylko te, zajmujące jakieś zasoby procesora?.....	29
...zajętość pamięci?.....	29
...objętość pamięci wykorzystywaną przez procesy routingu?.....	30
...jakie karty zainstalowano w routerze?.....	30
...jakie karty zainstalowano w przełączniku pracującym pod kontrolą CatOS?.....	31
...co obsługuje dany feature-set?.....	32
...znając nazwę pliku Cisco IOS jaki to feature-set?.....	32
...czy dana karta/moduł kompatybilna jest z danym routerem?.....	33
...na którym porcie routera znajduje się urządzenie o danym adresie MAC lub IP?.....	33
...na którym porcie przełącznika Catalyst wpięto urządzenie o danym adresie MAC?.....	33
...budżet mocy na modularnym przełączniku Catalyst?.....	34
Rozdział 7. Wybór sprzętu pod konkretne zastosowanie.....	34
Jaki router wystarczy do małej sieci (10-15 użytkowników), w sytuacji, gdy Internet dochodzi do mnie Ethernetem?.....	34
Jaki router wystarczy do małej sieci (10-15 użytkowników), w sytuacji, gdy Internet dochodzi do mnie stykiem V.35 (Polpak-T)?.....	34
Jaki router wystarczy do małej sieci (10-15 użytkowników), w sytuacji, gdy chcemy bezpiecznie połączyć się VPNem do innej podobnej lokalizacji przez łącze zakończone Ethernetem?.....	35
Mam dwa łącza od dwóch ISP i chciałbym uruchomić BGP. Jakiego routera powinienem użyć?.....	35
Potrzebuję mały przełącznik Cisco, bez routingu.....	35
Potrzebuję przełącznik Cisco potrafiący realizować routing.....	36
Przełączniki niemodularne.....	36
Przełączniki modułowe.....	36
Czy Cisco sprzedaje tzw. "firewalle sprzętowe"?.....	36
Czy Cisco sprzedaje sprzęt do budowy sieci bezprzewodowych?.....	37
Rozdział 8. Jak skonfigurować router do.....	37
...usługi transmisji danych w sieci Polpak-T?.....	37
...InternetDSL lub innego dostawcy oferującego styk Ethernet?.....	38
...usługi SDI/CDI?.....	39
...usługi Neostrada+?.....	41
...do Neostrady+ ale dla routera Cisco 677?.....	42
...połączenia kablami V.35 dwóch routerów Frame Relay?.....	43

...obsługi dwóch równoległych łącz od niezależnych ISP?.....	43
A co jeśli mam więcej łącz - na przykład 3?.....	46
A co z lokalnym ruchem do/z routera?.....	46
...eksportu danych NetFlow?.....	46
...routingu pomiędzy VLANami na kartach WIC-4ESW, NM-16ESW lub NM-32ESW?.....	47
Rozdział 9. Routing	48
Mam na routerze dwa interfejsy z nadanymi adresami IP, ale router nie chce routować między nimi. O co chodzi?.....	48
Jak wskazać routerowi domyślną bramkę?.....	48
Na jednym routerze mam wiele różnych protokołów routingu. Informacje którego z nich, znajdują się w tablicy routingu?.....	49
Jak przebiega proces routingu na routerach Cisco? Co jest brane pod uwagę?.....	49
Co to jest trasa pływająca (ang. floating route)?.....	49
Chcę rozkładać obciążenie pomiędzy trasy o równej metryce. Jak wygląda konfiguracja tego w IOSie?.....	50
Chcę rozkładać obciążenie pomiędzy trasy o równej metryce w proporcji 1:2 - jak to zrobić?.....	50
Czym się różni protokół routingu typu link-state od distance-vector?.....	51
W jaki sposób protokoły typu dystans-wektor zapobiegają tworzeniu pętli?.....	51
Interfejsy loopback.....	52
Co to jest interfejs loopback? Gdzie fizycznie się znajduje?.....	52
RIP.....	52
Co to jest RIP?.....	52
Jak wygląda podstawowa konfiguracja RIPv1?.....	52
A jak uruchomić na routerze RIP w wersji 2?.....	53
OSPF.....	54
Co to jest OSPF?.....	54
Jak działa OSPF?.....	54
Jak router liczy w OSPFie metrykę dla połączenia?.....	55
O czym pamiętać przy sumaryzacji?.....	55
Jakie są typy LSA?.....	55
Co jest potrzebne żeby dwa routery wymieniły informacje o routingu OSPF?.....	55
Jak sprawdzić aktualny stan sąsiadów danego routera OSPF?.....	56
Jak skonfigurować OSPF?.....	57
Czy jest jakiś przewodnik po budowaniu sieci z OSPFem?.....	58
Routing BGP.....	58
Co to jest BGP?.....	58
Co to jest numer AS?.....	58
Jaki potrzebuję router do obsługi BGP?.....	58
Jak właściwie działa BGP?.....	59
Jakich atrybutów używa BGP?.....	59
Jak w BGP wybierana jest ścieżka?.....	63
Jak skonfigurować BGP?.....	64
Chciałbym uruchomić BGP - skąd mam wziąć swój numer AS?.....	64
Co to jest PI i czym różni się od PA?.....	65
Czy jest jakiś przewodnik po budowaniu sieci z BGP?.....	65
Rozdział 10. QoS - limitowanie, gwarantowanie i kontrola pasma	66
Co tak naprawdę oznacza akronim QoS?.....	66
Jeśli chodzi o klasyfikację, często słyszę akronimy ToS, Precedence i DSCP - o co chodzi?.....	66
Jak skonfigurować.....	67
...priorytetyzację określonego ruchu za pomocą PQ?.....	67
...priorytetyzację określonego ruchu za pomocą CQ?.....	67
...kolejkowanie WFQ?.....	68
...przycinanie pasma dla określonego ruchu?.....	68
...kształtowanie ruchu za pomocą CBWFQ?.....	69
Co to jest NBAR?.....	71
Rozdział 11. Bezpieczeństwo	72
Poszukuje informacji o zabezpieczeniu routerów, przełączników.....	72
Dostęp do routera.....	73
Jak spowodować, żebym logując się do routera musiał podać tylko hasło?.....	73
Jak spowodować, żebym logując się do routera musiał podać zarówno login jak i hasło?.....	73
W jaki sposób stworzyć stałe mapowanie IP na MAC na routerze?.....	73
Chciałbym upewnić się, że mój router nie jest łatwym celem dla włamywaczy. Co jako podstawę poleć?.....	74
Zabezpieczanie ruchu do i przez router.....	75
Jak działają ACL?.....	75
Jak mogę sprawdzić, czy moje ACL działają?.....	77
Jak zoptymalizować ACLkę?.....	77
Rozdział 12. VPN - Wirtualne Sieci Prywatne	82
Co tak naprawdę oznacza akronim VPN?.....	82

Jak skonfigurować.....	82
...tunel IPsec pomiędzy dwoma routerami połączonymi do Internetu kanałami Frame Relay PVC?.....	82
...tunel IPsec+GRE pomiędzy dwoma routerami połączonymi do Internetu kanałami Frame Relay PVC?.....	85
Rozdział 13. Telekomunikacja.....	88
ISDN.....	88
Jaką prędkość mogę uzyskać, stosując ISDN?.....	88
Co to jest Q.921? A Q.931? Jak to się ma do PPP czy IP?.....	89
Jaką kartę zastosować do połączenia ISDN BRI w celu przenoszenia danych?.....	89
Jaką kartę zastosować do połączenia ISDN PRI w celu przenoszenia danych?.....	89
Jak skonfigurować połączenie z routera do Internetu przez interfejs BRI?.....	89
Jak sprawdzić historię połączeń interfejsów ISDN?.....	90
E1/E3.....	90
Jaką kartę zastosować do połączenia E1 w celu przenoszenia danych?.....	90
Jaką kartę zastosować do połączenia E3 w celu przenoszenia danych?.....	90
ATM.....	91
Jaką kartę zastosować do połączenia ATM w celu przenoszenia danych?.....	91
Rozdział 14. Rodzaje komutacji w routerach Cisco.....	91
Co to jest switching? Jaki ma związek z komutacją?.....	91
Jakie są rodzaje switchingu?.....	91
Jak skonfigurować.....	93
...CEF (Cisco Express Forwarding)?.....	93
...CEF dla routingu wg. zasad (ang. policy-based)?.....	93
Jak sprawdzić.....	94
...jaki mechanizmy komutacji włączono na interfejsie?.....	94
...ile ruchu komutowanego jest danym mechanizmem komutacji?.....	94
Rozdział 15. Optymalizacja wydajności.....	95
Mam router X, który udostępnia Internet stacjom w sieci LAN. Ciągle mam problemy z obciążeniem procesora, lub zrywanymi sesjami.....	95
Mam router X, który udostępnia Internet stacjom w sieci LAN. Mam tylko 5 stacji a widzę tysiące translacji - o co chodzi?.....	96
Mam router X, który udostępnia Internet stacjom w sieci LAN. Router obsługuje ruch zaledwie X Mbit/s i już procesor obciążony jest w 100%! Na stronie Cisco znalazłem informację, że ten model może obsłużyć ruch znacznie większy!.....	96
Jakie rzeczy sprawdzić, optymalizując wydajność routera?.....	97
Jak wygląda wydajność szyfrowania ruchu dla routerów/PIXów?.....	98
Rozdział 16. Sieci bezprzewodowe.....	99
Który standard określa co w rodzinie 802.11?.....	99
Jak policzyć EIRP?.....	100
Rozdział 17. Dobór i wymiana sprzętu.....	100
Czy muszę kupować oryginalne pamięci Cisco?.....	100
Mam w routerze kartę X. Jaki kabel do niej dobrać?.....	100
Skąd mogę wiedzieć, że dany sprzęt nie jest już sprzedawany przez Cisco?.....	101
Rozdział 18. Rozwiązywanie problemów.....	101
Obrazy IOS i ich odzyskiwanie.....	101
Straciłem obraz z Flasha. Mam do dyspozycji tylko tryb ROMMON i obraz IOSa na komputerze. Jak załadować go do routera?.....	101
Jak załadować obraz Cisco IOS do pamięci Flash, dysponując tylko trybem ROMMON i połączeniem przez konsolę?.....	101
Jak załadować obraz Cisco IOS do pamięci Flash, dysponując tylko trybem ROMMON i połączeniem przez Ethernet?.....	102
Hasła na routerach.....	102
Jak odzyskać zapomniane hasło z routera?.....	102
A jak odszyfrować zaszyfrowane hasło w konfiguracji routera?.....	103
Interfejsy Ethernet i ruch na nich.....	103
Mam dużo kolizji na interfejsie Ethernet routera - co mogę z tym zrobić?.....	103
Próbuję zdebugować ruch na interfejsie routera poleceniem `debug ip packet`, ale widzę tylko pojedyncze pakiety?.....	104
Chciałbym na PIXie sniffować ruch i zapisywać go do dalszej analizy - jak to zrobić?.....	104
Problemy z pamięcią i IOSami.....	104
Dostaję na konsolę lub do logów komunikaty typu %ALIGN-3-SPURIOUS: Spurious memory access made [...]......	104
Mam za mało pamięci aby zapisać konfigurację - co mam zrobić?.....	104
Problemy z przełącznikami Catalyst.....	105
Mam przełącznik Cisco Catalyst i wiele stacji do niego podłączonych. Mam problemy z logowaniem się do sieci po starcie tych komputerów.....	105
Na swoim przełączniku 2950, 3550 czy 3750 otrzymuję komunikat %SYS-2-MALLOCFAIL: Memory allocation of (...) Cause: Memory fragmentation.....	105
Rozdział 19. Podziękowania.....	105
Rozdział 20. ChangeLog.....	106

Rozdział 1. Sprawy porządkowe

FAQ, jak sama nazwa wskazuje, to zbiór najczęściej zadawanych pytań, wraz z odpowiedziami na nie. Naszą ambicją jest zebrać w tym jednym dokumencie maksimum użytecznych i przydatnych informacji, nie tylko dla profesjonalistów, ale również dla ludzi, którzy sprzęt Cisco widzą pierwszy raz w życiu.

Jak to przyjęło się w dokumentach tego rodzaju - możesz się z nami skontaktować. Na co dzień pracujemy jednak zawodowo i zwykle po prostu nie mamy czasu na odpowiadanie na pytania. Nie zdziw się zatem, jeśli na pytanie dotyczące Cisco, sieci (albo co gorsza, takie, na które odpowiedź znajduje się w tym FAQ) czy innego tematu nie dostaniesz odpowiedzi, skierujemy Cię do google.com albo odpowiedź będzie niezbyt przyjemna.

Oświadczenie i licencja

Dokument ten rozpowszechniany jest w nadziei, że będzie użyteczny, ale BEZ ŻADNEJ GWARANCJI; nawet bez implikowanej gwarancji RĘKOJMI lub PRZYDATNOŚCI DO KONKRETNEGO ZASTOSOWANIA.

Krótko i po ludzku mówiąc, zebrane tu informacje wcale nie muszą być prawdziwe. Jeśli w wyniku ich zastosowania np. Twoja firma straci miliony złotych - to nie była nasza wina. Bardzo nam przykro - staraliśmy się podać pewne informacje w dobrej wierze. *Zastanów się zatem wielokrotnie zanim postanowisz coś kupić, włączyć lub (s|prze)konfigurować!*

Materiał zawarty w tym FAQ może być dystrybuowany tylko na zasadach określonych w Open Publication License, v1.0 lub późniejszej (ostatnia wersja jest obecnie dostępna pod adresem <http://www.opencontent.org/openpub/>).

Znaków towarowych firm, w szczególności firmy Cisco Systems, użyto tylko w celu identyfikacji produktów.

Namawiamy do darmowego kopiowania i dystrybuowania (sprzedawania lub rozdawania) tego dokumentu w dowolnym formacie. Wymagamy jednak, by poprawki i/lub komentarze przekazywać bezpośrednio na adres listy pocztowej, lub na adres koordynatora projektu - Łukasza Bromirskiego.

Dostęp do CVS i Twój udział w tym projekcie

Oryginał tego dokumentu w najnowszej wersji znajduje się pod adresem: http://lukasz.bromirski.net/docs/cisco/cisco_faq.html.

Koordynator tego FAQ pracuje nad uruchomieniem publicznie dostępnego serwera CVS.

Lista pocztowa - jak i gdzie?

Koordynator tego FAQ pracuje nad uruchomieniem publicznie dostępnego serwera CVS.

Rozdział 2. Pytania ogólne

Gdzie można poczytać o firmie Cisco i produktach tej firmy?

Najlepiej zacząć od polskich stron:

- <http://www.cisco.pl/>
- <http://www.ciscopoland.pl/cisco/main.asp>

Następnie udać się oczywiście na największą stronę główną:

- <http://www.cisco.com/>
-

Do kogo zwrócić się o pomoc, jeśli chciałbym zbudować swoją sieć w oparciu o produkty Cisco?

Powinieneś zgłosić się do firmy, która wykonuje projekty w oparciu o sprzęt Cisco. Najprościej będzie zadzwonić na numer linii konsultacyjnej Cisco Polska (0 801 340 755). Konsultant, w zależności od wielkości projektu, zaproponuje pomoc inżynierów Cisco Polska, sam przedstawi pomysł na budowę sieci i listę sprzętu, lub skieruje Cię do firm, które zajmują się profesjonalnymi usługami.

Jak skontaktować się z pomocą techniczną Cisco?

Aby skontaktować się z Cisco TAC (Technical Assistance Center) skorzystaj z listy dostępnej pod adresem: <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

Generalnie, europejski Cisco TAC dostępny jest pod numerem telefonu +32 2 704-58-69 (niestety, trzeba posługiwać się językiem angielskim) lub mailem tac@cisco.com.

Pamiętaj jednak, że:

- Aby skorzystać z tej pomocy, musisz posiadać wykupiony kontrakt serwisowy - SmartNET lub SmartSpares.
 - Musisz znać rodzaj sprzętu, o którym z Cisco TAC chciałbyś porozmawiać, jego numer seryjny i jeśli to możliwe - posiadać jak najdokładniejsze informacje o nim (zwykle na początku rozmowy inżynier TAC poprosi o zrzucenie do pliku wyniku działania polecenia `show tech-support`, więc warto od razu mieć go pod ręką).
 - Inżynierowie Cisco TAC z reguły nie pomagają w konfiguracji połączenia Internetowego, list kontroli dostępu czy nie zaprojektują Ci odpowiednio sieci. Postaraj się wykonać jak najdokładniejszy troubleshooting **zanim** poprosisz o pomoc.
-

Gdzie można uzyskać pomoc dotyczącą sieci i Cisco?

Najszybszą i darmową (zwykle) pomoc znaleźć można na listach usenetowych:

- pl.comp.networking - polska, dotycząca nie tylko sprzętu Cisco
- comp.dcom.sys.cisco - w języku angielskim, dotycząca tylko sprzętu Cisco
- fido7.ru.cisco - w języku rosyjskim, dotycząca tylko sprzętu Cisco

Trochę bardziej zaawansowane zagadnienia pojawiają się na listach, na które trzeba się zapisać. Są to:

- <http://www.prenumerata.pl/wwsympa.fcgi/info/isp-tech> - skupia wielu ludzi, którzy znają Cisco i inny sprzęt od podszewki
 - <https://puck.nether.net/mailman/listinfo/cisco-nsp> - prowadzona w języku angielskim, dla ISP
 - <http://forum.cisco.com/eforum/servlet/NetProf?page=main> - fora dyskusyjne Cisco oraz archiwa sesji pytań i odpowiedzi
-

Skąd mogę pobrać nowsze oprogramowanie do swojego urządzenia Cisco?

Dla zwykłych użytkowników, Cisco udostępnia bardzo okrojony zestaw oprogramowania, osiągalny pod adresem <http://www.cisco.com/public/sw-center/>.

Aby móc używać stale najnowszego oprogramowania, powinieneś do swojego urządzenia wykupić kontrakt SmartNET. Jeśli pozyskałeś urządzenie "szarym kanałem", jak nazywa się sprzęt nie sprzedany oficjalnie w Polsce tylko sprowadzony, będziesz miał problem z uzyskaniem legalnie nowszego/poprawionego oprogramowania. Dla sprzętu sprowadzanego i pozyskiwanego w ten sposób Cisco w Polsce nie prowadzi żadnego wsparcia projektowego/wdrożeniowego.

Pamiętaj również, że licencja Cisco **uniemożliwia** dzielenie się oprogramowaniem ze znajomymi, ani odsprzedaż urządzeń z zainstalowanym oprogramowaniem.

Słyszałem, że aktywacja szyfrowania 3DES i ew. AES jest na PIXach darmowa - czy to prawda?

Tak, wystarczy że użytkownik końcowy urządzenia zarejestruje się na stronie o adresie https://www.cisco.com/cgi-bin/Software/Crypto/crypto_main.pl?prod_refer=pix3des. Kod aktywacyjny umożliwiający szyfrowanie 3DES i AES (od PIX OS 6.3) otrzyma e-mailem.

Czy są jakieś strony sympatyków Cisco z ciekawymi materiałami?

Open Sourceowa grupa COSI (Cisco Centric Open Source Initiative) prowadzi projekt, w ramach którego zbiera najciekawsze narzędzia do wszelakiego sprzętu Cisco. Z ideą działania grupy i z narzędziami stworzonymi przez jej członków, możesz zapoznać się pod adresem <http://cosi-nms.sourceforge.net/>.

Rozdział 3. Dokumentacja

Gdzie w Internecie znaleźć dobre materiały o sprzęcie Cisco? Konfiguracja, przykłady, zalecenia?

Na początek zapoznaj się z CCO, czyli Cisco Connection Online. Jest to sekcja strony <http://www.cisco.com/univercd/home/home.htm>, będąca naprawdę kopalnią wiedzy - zarówno o danych fabrycznych produktów, jak i konfiguracji poszczególnych zagadnień czy zaleceniach Cisco.

Drugim, bardzo bogatym i obszernym miejscem, są prezentacje z corocznych spotkań organizowanych przez Cisco, nazywanych *Networkers*. Poniżej lista lokacji, z których ściągnąć można w formacie PDF prezentacje z poszczególnych lat:

- 1999: http://www.cisco.com/networkers/nw99_pres/
- 2000: <http://www.cisco.com/networkers/nw00/pres/>
- 2001: <http://www.cisco.com/networkers/nw01/pres/>
- 2002: <http://www.cisco.com/networkers/nw02/post/presentations.html>
- 2003 USA: <http://www.cisco.com/networkers/nw03/post/presos.html>
- 2003 Johannesburg: http://www.networkersafrica.com/nw03/POST_EVENT/PRESENTATIONS/Breakout_sessions/default.asp
- 2004 Brisbane: https://www.conveneit.com/secure/cisco_networkers/client/default.asp?pg=4
- 2004 Nowy Orlean: <http://www.cisco.com/go/networkersonline2004>

I na koniec - wiele odpowiedzi i często spotykanych konfiguracji, znaleźć można posługując się (jak zwykle, gdy masz wątpliwości) wyszukiwarką [google](#).

Jakie polecacie książki po Polsku, do pracy ze sprzętem Cisco?

Niestety, polskie wydawnictwa poskapiły dobrych książek o Cisco. Z wartych kupienia i dostępnych w języku polskim wymienić należy:

- "Routery Cisco. Czarna księga", ISBN: 83-7197-286-5, wydawnictwo Helion (<http://helion.pl/ksiazki/rcisbb.htm>)
- "Routery Cisco w praktyce", ISBN: 83-7197-214-8, wydawnictwo Helion (<http://helion.pl/ksiazki/rcisco.htm>)
- "Cisco. Receptury", ISBN: 83-7361-330-7, wydawnictwo Helion (<http://helion.pl/ksiazki/cisrec.htm>)

Zdecydowanie **nie polecam** tłumaczeń książek Cisco Press wydawnictwa Mikom. Aby zorientować się w jakości wydawanych przez nich książek, wystarczy skorzystać z przeglądarki Google. Dodatkowo, koordynator tego FAQ (Łukasz Bromirski) miał osobistą *nieprzyjemność* współpracować z tym wydawnictwem przy tłumaczeniu dwóch książek.

A jakie w ogóle książki polecacie, poświęcone sieciom oraz sprzętowi Cisco?

Generalnie, z wydawnictw zagranicznych, warto zainteresować się firmowym wydawnictwem [Cisco Press](#), oraz książkami wydawnictw [Syngress](#) i [Sybex](#). Bardzo dobre są również książki wydawane w wydawnictwie [O'Reilly](#) (ale to chyba akurat oczywiste).

Jeśli zajmujesz się sieciami, warto w swojej bibliotece posiadać minimum:

[TCP/IP Illustrated, Volume 1 - The Protocols](#)

Legendarna już książka Stevensa omawiająca zestaw protokołów wchodzących w skład TCP/IP i opisująca ich budowę oraz działanie. Podstawa podstaw. Druga część tej książki omawia implementację (jeśli nie programujesz, jest to mniej ciekawa lektura).

[Cisco IOS in a Nutshell](#)

Jeśli dopiero zaczynasz pracę z routerami Cisco i chcesz poznać ich budowę oraz sposób pracy z nimi, a nie posiadasz żadnych materiałów szkoleniowych czy książek do egzaminu CCNA, ta książka jest warta polecenia.

[Routing TCP/IP Volume I \(CCIE Professional Development\)](#) oraz [Routing TCP/IP, Volume II \(CCIE Professional Development\)](#)

Dwie książki poświęcone zagadnieniom routingu w sieciach TCP/IP - naprawdę rewelacyjna lektura.

[Cisco Certification: Bridges, Routers and Switches for CCIEs \(wydanie II\)](#)

Trochę już wiekowa (wydana 15 grudnia 2000 roku) książka, ale jednocześnie rewelacyjne źródło wiedzy o wszelakich zagadnieniach z którymi spotykają się ludzie projektujący, konfigurujący i utrzymujący sieci oparte o urządzenia Cisco.

[Internet Routing Architectures \(wydanie drugie\)](#)

Książka Sama Halabiego, omawiająca dokładniej zagadnienia budowy sieci połączonej do Internetu - w tym dokładnie konfigurację BGPv4.

[ISP Essentials](#)

Drukowana wersja elektronicznej książki, dostępnej też pod adresem <http://www.cisco.com/public/cons/isp/documents/IOSEssentialsPDF.zip>. Znajdują się w niej zalecenia dla dostawców Internetowych, ale porady są skierowane do wszystkich użytkowników routerów Cisco. Bardzo cenna pozycja dla kogoś, kto praktycznie zajmuje się tym sprzętem.

Pozostałe rekomendacje ściśle związane są ze specjalizacją, którą się zajmujesz - książek o sieciach jest mnóstwo.

Jak zainstalować Cisco Documentation pod Windows tak, by nie trzeba było za każdym razem korzystać z krążka?

Najwygodniej jest wykonać obraz drugiej płyty (np. programem CloneCD czy Nero), następnie zainstalować jeden z wielu programów umożliwiających wirtualizację napędów CD/DVD - polecam [Virtual Deamon](#) i wskazać mu ten plik jako wirtualny napęd CD. Pozostanie jedynie zmienić literkę, przypisaną w konfiguracji programu wyświetlającego dokumentację. W domyślnej instalacji, plik ten znajduje się w katalogu `c:\cisco` i nazywa `search.ini`. Należy otworzyć go za pomocą ulubionego edytora tekstowego, znaleźć ciąg znaków `SourceDrive` i po znaku równa się wpisać literę wirtualnego napędu.

W mojej instalacji, oryginalny plik miał taki wpis:

```
SourceDrive=E:
```

Ponieważ mój wirtualny dysk CD zainstalował się pod literą `F:`, zmieniłem ten wpis na:

```
SourceDrive=F:
```

Teraz wystarczy uruchomić plik `autorun.exe` z wirtualnego napędu, by uruchomić DocumentationCD bez potrzeby posiadania płytki w napędzie.

Jak zainstalować Cisco Documentation pod Linuxem/BSD?

Jeśli możesz uruchomić lokalny serwer Apache, nie ma z tym żadnego problemu. Pozostaje tylko przekonać przeglądarki, żeby odpakowały sobie "w locie" zawartość serwowanych stron. Do pliku konfiguracyjnego Apache dodaj:

```
Alias /cisco/ /gdzie_zamontowałeś_cd/  
  
<Directory /gdzie_zamontowałeś_cd>  
Options Indexes  
AllowOverride None  
order deny,allow  
deny from all  
allow from localhost  
</Directory>  
  
<Location /cisco/cc/>  
AddEncoding x-gzip htm pdf  
</Location>
```

Teraz uruchom przeglądarkę i wpisz adres: <http://localhost/cisco/home/home.htm>.

Gdzie sprawdzić składnię konkretnego polecenia?

Na CCO, w sekcji Cisco IOS: - dokumentacja od 11.3, 12.0, 12.1, 12.2 i 12.3.

- Dla Cisco IOS 11.3:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/prod_command_reference_list.html
 - Dla Cisco IOS 12.0:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/prod_command_reference_list.html
 - Dla Cisco IOS 12.1:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/prod_command_reference_list.html
 - Dla Cisco IOS 12.2:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html
 - Dla Cisco IOS 12.3:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_command_reference_list.html
-

Rozdział 4. Certyfikacje Cisco

Jakie są poziomy certyfikacji Cisco?

Cisco Systems podzieliło swoją ścieżkę certyfikacji na trzy poziomy:

- Associate
- Professional
- Expert

Dodatkowo istnieje niezależna grupa certyfikatów opisująca konkretne specjalności (Cisco Qualified Specialist, CQS).

Jakie egzaminy muszą zdać na poziomie Associate?

Aby otrzymać tytuł CCNA, czyli *Cisco Certified Network Associate* musisz posiadać ogólną wiedzę o sieciach, oraz podstawową o sprzęcie Cisco. Dostępny jest również tytuł CCDA, *Cisco Certified Design Associate*, bardziej ukierunkowany na projektowanie sieci w oparciu o sprzęt Cisco.

Aby uzyskać tytuł CCNA, możesz albo zdać jeden egzamin 640-801, albo rozłożyć sobie testy na dwa egzaminy: 640-821 i 640-811. Aby uzyskać tytuł CCDA, musisz zdać egzamin 640-861.

CCNA i CCDA są ważne przez trzy lata. Aby się recertyfikować należy zdać aktualny egzamin CCNA/CCDA lub zdobyć stopień Professional.

Jakie egzaminy muszą zdać na poziomie Professional?

Dostępne są cztery tytuły na tym poziomie, w zależności od specjalizacji:

- CCNP, czyli *Cisco Certified Network Professional*

Musisz posiadać ważny certyfikat CCNA, oraz posiadać dokładną wiedzę o budowie sieci typu dial-up, działaniu i konfiguracji protokołów routingu, metodyce rozwiązywania problemów oraz dużych sieciach LAN.

Wymagane egzaminy (zdawane w dowolnej kolejności): 642-801 BSCI, 642-811 BCMSN, 642-821 BCRAN i 642-831 CIT lub zamiast egzaminów 642-801 i 642-811 zdać jeden egzamin 642-891

Composite i pozostałe dwa.

CCNP jest ważny przez trzy lata. Aby się recertyfikować, należy zdać aktualny egzamin Composite.

- **CCDP, czyli *Cisco Certified Design Professional***

Podobnie jak CCDA skupiają się na projektowaniu sieci. CCDP wymaga ważnego certyfikatu CCDA.

Wymagane egzaminy (zdawane w dowolnej kolejności): 642-801 BSCI, 642-811 BCMSN, 642-871 ARCH, lub 642-891 Composite i 642-871 ARCH.

CCDP jest ważny przez trzy lata. Aby się recertyfikować, należy zdać aktualny egzamin Composite.

- **CCIP, czyli *Cisco Certified Internetwork Professional***

Certyfikat dla pracowników dostawców Internetowych, wymaga posiadania ważnego certyfikatu CCNA.

Wymagane egzaminy (zdawane w dowolnej kolejności): 642-801 BSCI, 642-641 QoS, 642-661 BGP i 640-910 MPLS, lub 642-801 BSCI, 642-641 QoS i 642-691 BGP+MPLS.

CCIP jest ważny przez trzy lata.

- **CCSP, czyli *Cisco Certified Security Professional***

Certyfikat obejmujący specjalizację w zabezpieczaniu sieci i dbaniu o ich bezpieczeństwo, a także w budowie i utrzymaniu sieci VPN. Wymaga posiadania certyfikatu CCNA lub CCIP.

Wymagane egzaminy (zdawane w dowolnej kolejności): 642-501 SECUR, 642-521 CSPFA, 642-531 CSIDS i 642-511 CSVPN, i 642-541 CSI.

CCSP jest ważny przez trzy lata.

Jakie egzaminy muszę zdać na poziomie Expert?

Dostępne są cztery tytuły na tym poziomie, w zależności od specjalizacji:

- **CCIE R&S, czyli *Cisco Certified Internetwork Expert, Routing & Switching***

Elitarny certyfikat, zaświadczaający o doskonałej wiedzy w dziedzinie budowy i utrzymania sieci każdej wielkości.

Wymaga zdania egzaminu 350-001, składającego się z dwóch części: pisemnego oraz w laboratorium. Bez zdania egzaminu pisemnego, nie możesz zdawać egzaminu w laboratorium.

CCIE jest ważny przez dwa lata. Aby się recertyfikować, należy zdać jeden z egzaminów pisemnych - w swojej specjalizacji lub innej.

- **CCIE Service Provider, czyli *Cisco Certified Internetwork Expert, Service Provider***

Elitarny certyfikat, zaświadczaający o doskonałej wiedzy w dziedzinie budowy i utrzymania sieci, ze szczególnym naciskiem na sieci budowane przez i dla dostawców usług.

W zależności od pod-specjalizacji, CCIE SP zdaje jeden egzamin pisemny i jeden w laboratorium. Podobnie jak w przypadku CCIE R&S, porażka na etapie egzaminu pisemnego uniemożliwia zdawanie egzaminu praktycznego. Dostępne podspecjalizacje to: 350-020 Optical, 350-021 Cable, 350-022 DSL, 350-023 WAN Switching, 350-024 IP Telephony, 350-025 Dial, 351-026 Content Networking. Egzamin pisemny zawiera w połowie tematy z CCIE R&S, a w połowie z tematyki w której kandydat ma się specjalizować.

CCIE jest ważny przez dwa lata. Aby się recertyfikować, należy zdać jeden z egzaminów pisemnych - w swojej specjalizacji lub innej.

- **CCIE Security, czyli *Cisco Certified Internetwork Expert, Security***

Elitarny certyfikat, zaświadczaający o doskonałej wiedzy w dziedzinie budowy i utrzymania sieci, ze szczególnym naciskiem na szeroko rozumiane bezpieczeństwo.

Wymaga zdania egzaminu 350-018, składającego się z dwóch części: pisemnego oraz w laboratorium. Bez zdania egzaminu pisemnego, nie możesz zdawać egzaminu w laboratorium.

CCIE jest ważny przez dwa lata. Aby się recertyfikować, należy zdać jeden z egzaminów pisemnych - w swojej specjalizacji lub innej.

- CCIE Voice, czyli *Cisco Certified Internetwork Expert, Voice*

Elitarny certyfikat, zaświadczaający o doskonałej wiedzy w dziedzinie budowy i utrzymania sieci, ze szczególnym naciskiem na przenoszenie głosu.

Wymaga zdania egzaminu 350-030, składającego się z dwóch części: pisemnego oraz w laboratorium. Bez zdania egzaminu pisemnego, nie możesz zdawać egzaminu w laboratorium.

CCIE jest ważny przez dwa lata. Aby się recertyfikować, należy zdać jeden z egzaminów pisemnych - w swojej specjalizacji lub innej.

Gdzie mogę znaleźć dokładną listę tematów na dany egzamin?

Na tej stronie: <http://www.cisco.com/go/certifications> znajduje się spis wszystkich aktualnych egzaminów. Wystarczy wybrać jeden z nich i kliknąć na jego oznaczeniu, by otrzymać podstawowe informacje: czas trwania, orientacyjną liczbę pytań, listę zagadnień które mogą pojawić się na egzaminie oraz zalecenia dotyczące nauki przed egzaminem.

Dodatkowo, dla egzaminów CCIE dostępna jest osobna strona: <http://www.cisco.com/go/ccie>.

Czy dla zdających są jakieś pomoce?

Przede wszystkim, Cisco przez swoich autoryzowanych partnerów organizuje kursy przygotowujące do konkretnego egzaminu i/lub specjalizacji.

Po drugie, wydawnictwo CiscoPress ma specjalną sekcję wydawnictw poświęconych certyfikacji: <http://www.ciscopress.com/catalog/index.asp?st={E65E5189-F2F8-40AE-A827-D766D4879FDC}>.

Po trzecie, wiele firm oferuje swoje materiały, mające przygotować Cię do zdania wybranego egzaminu. Najpopularniejszą firmą jest Boson (<http://www.boson.com/>), która oprócz samych materiałów, oferuje również różnego rodzaju narzędzia.

Czy po egzaminie mogę podzielić się ze znajomymi treścią pytań?

Nie, pod rygorem utraty certyfikacji. Cisco bardzo poważnie traktuje naruszenia NDA (ang. *Non-Disclosure Agreement*), który musisz podpisać przed zdawaniem każdego egzaminu.

Rozdział 5. Podstawy pracy z urządzeniami Cisco

Jak podłączyć się do...

...routera Cisco?

Każdy router Cisco posiada port konsoli (port opisany niebieskim kolorem jako *CONSOLE*)- a kabel konsolowy dostarczany jest w pudełku z nowym urządzeniem (to ten niebieski, zakończony dwoma

stykami RJ-45 lub jednym stykiem RJ-45 i jednym RS-232C DB-9).

W zależności od oprogramowania, do routera można dostać się również Telnetem (znając adres IP i ewentualnie użytkownika i hasło), przez SSH czy nawet w nowym oprogramowaniu, przez przeglądarkę (jeśli na routerze zainstalowano SDM - Secure Device Manager - dostępny za darmo - będziesz miał wygodny interfejs do funkcjonalności routera; jeśli nie, będziesz miał dostęp do podstawowych statystyk oraz panel do wykonywania poleceń).

...Cisco PIX?

Podobnie jak routery, PIXy również posiadają port opisany niebieskim kolorem jako *CONSOLE*. Do PIXa również można podłączyć się przez Telnet, SSH lub od wersji 6.0 PIX OSA - PDM, czyli PIX Device Manager. Od wersji 7.0 graficzny interfejs użytkownika to ASDM - Advanced Security Device Manager.

...przełącznika Cisco Catalyst serii 1000, 2000 lub 3000?

Przełączniki niemodularne (19xx, 29xx, 3xxx) posiadają na tylnym panelu port opisany na niebiesko jako *CONSOLE*.

...przełącznika Cisco Catalyst serii 4000/4500?

W przełącznikach modułarnych 4000/4500 do modułu zarządzającego (Supervisora), można podłączyć się na dwa sposoby: konsolą, lub za pomocą Ethernetu.

Konsola na wszystkich Supervisorach (za wyjątkiem modelu I) to standardowy styk RJ-45, natomiast w Supervisorze I jest to żeński port DB-25.

Port Ethernetowy/FastEthernetowy opisany jest natomiast jako *Management Port* i służy tylko do *zarządzania* - łączności przez Telnet/SSH, zbierania informacji przez SNMP lub przesyłania obrazów z systemem. Port ten nie będzie przekazywał żadnego ruchu do innych modułów przełącznika. Dodatkowo, aby z tego portu skorzystać, należy go uprzednio skonfigurować (nadać adres IP).

Aby zarządzać urządzeniem z dwoma Supervisorami, należy podłączyć się do tego, na którym pali się dioda *Active*.

...przełącznika Cisco Catalyst serii 6000/6500?

Supervisory posiadają standardowy port konsolowy (RJ-45). Aby zarządzać urządzeniem z dwoma Supervisorami, należy podłączyć się do tego, na którym pali się dioda *Active*.

...sondy Cisco IDS/IPSa serii 42xx?

Do sond IDS można podłączyć się zarówno standardowym kablem konsolowym (jest w oryginalnym opakowaniu) do portu COM1, lub po prostu dołączając zwykłą klawiaturę PS/2 i monitor.

...punktu bezprzewodowego AP350, 11xx, 12xx, 13xx lub 14xx?

Podobnie jak w przypadku routerów, AP dysponują opisany na niebiesko portem konsoli. Zwróć uwagę, że w domyślnej konfiguracji wymagają zalogowania się na użytkownika `Cisco` z hasłem `Cisco`.

Podłączyłem się i...?

...w oknie terminala nic nie widzę?

Spróbuj parę razy wcisnąć *Enter* - urządzenie po drugiej stronie powinno zwrócić prompt o login, lub po prostu od razu umożliwić wykonywanie poleceń (w zależności od konfiguracji).

Jeśli nic się nie dzieje, a jesteś pewien że kabel konsolowy jest dobry, możliwe, że port ustawiony jest inaczej niż domyślnie (dla przypomnienia, prędkość 9600, 8 bitów danych, bez parzystości i 1 bit stopu). Spróbuj ustawienia 38400 8N1, 57600 8N1 lub 115200 8N1 w swoim terminalu.

...jak dostawać informacje o zdarzeniach na routerze na konsolę?

Jeśli jesteś podłączony przez konsolę, domyślnie otrzymujesz informacje o zdarzeniach na routerze. Np.:

```
router# conf t
router(config)# exit
router#

%SYS-5-CONFIG_I: Configured from console by console
```

Jeśli natomiast jesteś zalogowany przez Telnet lub SSH, musisz wprost włączyć kierowanie komunikatów na Twoją konsolę poleceniem `terminal monitor`:

```
router# terminal monitor
```

...jaki dokładnie mam router? Ile mam pamięci RAM/flash? Co oznaczają poszczególne linijki z polecenia `show version`?

Standardowo do sprawdzenia, z jakim urządzeniem mamy do czynienia, poza oczywistą inspekcją wizualną (jeśli pracujemy zdalnie niemożliwą) jest wydanie polecenia `show version`.

Poniżej przykładowy wynik takiego polecenia wraz z interpretacją wyniku:

```
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-Y-M), Version 12.1(22a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 23-Jan-04 20:40 by cmong
Image text-base: 0x80008088, data-base: 0x8060A5D4
```

Z tego fragmentu możemy dowiedzieć się, że mamy do czynienia z routerem (na urządzenie załadowano Cisco IOS, na PIXach mamy do czynienia z PIX Osem, na dużych przełącznikach Catalyst z CatOSem).

Po drugie, oprogramowanie należy do serii przeznaczanej dla routerów serii 1700 (C1700 Software), w wersji 12.1.22a (Version 12.1(22a)) i zawierającym funkcjonalność "IP" (C1700-Y-M). O tym jak rozszyfrować funkcjonalność oprogramowania odpowiadamy w dalszych pytaniach.

```
c1720 uptime is 10 minutes
System returned to ROM by power-on
System image file is "flash:c1700-y-mz.121-22a.bin"
```

Kolejna linijka określa, jak dawno resetowano router (uptime is 10 minutes - 10 minut temu), co było przyczyną restartu (power-on - włącznik, inne opcje to reload - restart wymuszony poleceniem reload), oraz jaki i skąd Cisco IOS został załadowany (flash:c1700-y-mz.121-22a.bin, z pamięci Flash i nazywa się c1700-y-mz.121-22a.bin).

```
cisco 1720 (MPC860) processor (revision 0x501) with 12288K/4096K bytes of memory.  
Processor board ID JAD01234567 (123456789), with hardware revision 0000  
M860 processor: part number 0, mask 32
```

Mamy do czynienia z routerem Cisco 1720 (Cisco 1720), sterowanym procesorem MPC860. Router posiada łącznie 16MB pamięci RAM (12288K/4096K bytes of memory, wartości należy zsumować). Dodatkowo, można sprawdzić numer seryjny urządzenia (JAD01234567).

```
1 FastEthernet/IEEE 802.3 interface(s)  
1 Serial(sync/async) network interface(s)
```

Router posiada jeden interfejs FastEthernet (standardowo zabudowany na routerach 1700) oraz jeden interfejs szeregowy (może pracować zarówno w trybie asynchronicznym jak i synchronicznym).

```
32K bytes of non-volatile configuration memory.  
4096K bytes of processor board System flash (Read/Write)
```

Dodatkowo, router posiada 32kB pamięci nieulotnej (NVRAM), w której przechowuje się aktualną i startową konfigurację, oraz 4MB pamięci Flash (używanej do przechowywania Cisco IOS, certyfikatów itp.).

```
Configuration register is 0x2102
```

Tzw. rejestr konfiguracyjny, kontrolujący pewne aspekty startu i pracy routera ustawiony został na wartość heksdecymalną 2102. O znaczeniu poszczególnych bajtów tego rejestru napisano niżej.

...gdy pomylę się w poleceniu, router zaczyna robić dziwne rzeczy...

Domyślnie, wydanie nieznanego routerowi polecenia, powoduje próbę połączenia się z nim. Wygląda to mniej więcej tak:

```
router# zlepolecenie  
Translating "zlepolecenie"...domain server (255.255.255.255)  
Translating "zlepolecenie"...domain server (255.255.255.255)  
Translating "zlepolecenie"...domain server (255.255.255.255)  
% Unknown command or computer name, or unable to find computer address
```

Takie zachowanie routera można zmienić, wyłączając rozwiązywanie nazw:

```
router(config)# no ip domain lookup
```

...chciałbym zapisać konfigurację routera/PIXa/przełącznika?

Na urządzeniach pracujących pod kontrolą Cisco IOS (routery, PIXy od wersji 6.0 i część przełączników) używa się do tego celu polecenia:

```
router# copy running-config startup-config
```

Ewentualnie, w bardzo starych Cisco IOS, w PIX OS starszych niż 6.0 i w urządzeniach pracujących pod kontrolą CatOS (przełączniki) poleceniem:

```
router# write memory
```

...chciałbym wymazać konfigurację routera/PIXa/przełącznika?

Na urządzeniach używających NVRAMu (routery i część przełączników), wystarczy wydać polecenie:

```
router# erase nvram
```

Na PIXach natomiast:

```
pix# write erase
```

...jakiego użyć oprogramowania do połączenia się z routerem?

Wszystko zależy od systemu operacyjnego.

Dla systemu Windows polecam program SecureCRT - obsługuje zarówno połączenia konsolowe jak i przez Telnet/SSH. Standardowo obecny w Windowsach program Hyperterminal jest bardzo ubogi i niewygodny w użytkowaniu.

Dla systemów Linux/BSD i połączeń przez konsolę polecam minicom, a przez telnet/ssh - natywnie wbudowane w te systemy programy.

...jakiego użyć oprogramowania do serwowania plików tftp/ftp?

Ponownie - wszystko zależy od systemu operacyjnego.

Dla systemu Windows polecam serwer TFTP firmy SolarWinds (darmowy): <http://support.solarwinds.net/updates/New-customerFree.cfm>. Jeśli chodzi o serwer FTP - polecam program BulletProof FTP Server (<http://www.bpftpserver.com/>) ale nie jest on niestety darmowy.

Dla systemów Linux/BSD zarówno serwer tftp jak i ftp dostarczane są zwykle z dystrybucją/w systemie podstawowym. Prawdopodobnie będzie jednak trzeba je wprost aktywować w konfiguracji demona inetd lub xinetd.

Mój router uparcie próbuje ściągnąć z sieci plik network-config, network-cfg lub cisco.net.cfg - o co chodzi?

Masz aktywną usługę wczytywania konfiguracji z sieci. Wyłącz ją, pisząc:

```
router(config)# no service config
```

Rozdział 6. Podstawy konfiguracji usług

DHCP

Co to są prywatne/niezarejestrowane adresy IP?

Na potrzeby przykładów, książek i innych opracowań IETF wydzielił z globalnej puli adresów IPv4 pewne zakresy, których nie przydzielono nigdzie w Internecie i nie powinny się one w nim pojawić (a jeśli się już nawet pojawiają, powinny zostać zignorowane lub odfiltrowane). Adresy te nazywane są *prywatnymi*, rzadziej *niezarejestrowanymi*.

Spis adresów aktualnie przydzielonych do celów testowych i na prywatny użytek, znajduje się w RFC 1918 (<http://www.ietf.org/rfc/rfc1918.txt>). Dla jasności, chodzi o adresy:

```
10.0.0.0 - 10.255.255.255 (10.0.0.0/8)
172.16.0.0 - 172.31.255.255 (172.16.0.0/12)
192.168.0.0 - 192.168.255.255 (192.168.0.0/16)
```

UWAGA! Pojęcie "adresy nieroutowalne" jest błędne - nie ma czegoś takiego. Każdy adres jest jak najbardziej routowalny, po prostu przeznaczeniem tego konkretnego zestawu adresów nie jest znalezienie się w Internecie.

Czy router może pełnić rolę serwera DHCP?

Tak, ale w przypadku routerów serii 1600, 1700, oraz niektórych linii Cisco IOS, możesz potrzebować funkcjonalności "Plus" - najlepiej skorzystaj z *Feature Navigator*, zanim założysz, że posiadasz tą funkcję.

Serwer DHCP uruchamia się, definiując pulę adresowe. Jeśli np. masz pojedynczą sieć i nie chcesz kojarzyć adresów IP z adresami MAC, możesz napisać:

```
router(config)# ip dhcp excluded-address 192.168.0.1
                Adres 192.168.0.1 nie zostanie przypisany - zwykle chodzi o
                zarezerwowanie adresu interfejsu routera
router(dhcp-config)# ip dhcp pool MojeDHCPPLAN
                Tworzymy pulę o nazwie MojeDHCPPLAN
router(dhcp-config)# network 192.168.0.0 255.255.255.0
                Przydzielamy adresy z puli 192.168.0.0/24 (za wyjątkiem
                zarezerwowanego wyżej adresu 192.168.0.1)
router(dhcp-config)# default-router 192.168.0.1
                Oprócz adresu IP dla stacji, serwujemy domyślną bramkę
                (zwykle interfejs routera)
router(dhcp-config)# dns-server IP_serwera_DNS1 IP_serwera_DNS2 itp.
                ...oraz od razu serwery DNS.
```

Jeśli natomiast chcesz konkretnej stacji/serwerowi przydzielić konkretny adres IP, możesz posłużyć się mapowaniem MAC-IP:

```
router(config)# ip dhcp pool SerwerPlikow
router(dhcp-config)# host 192.168.0.10 255.255.255.0
                Adres 192.168.0.10 z maską /24 przydzielony zostanie...
router(dhcp-config)# client-identifier 00c.09cb.9813
                ...hostowi z adresem MAC 00:0C:09:CB:98:13
router(dhcp-config)# default-router 192.168.0.1
                Oprócz adresu IP dla stacji, serwujemy domyślną bramkę
                (zwykle interfejs routera)
router(dhcp-config)# dns-server IP_serwera_DNS1 IP_serwera_DNS2 itp.
                ...oraz od razu serwery DNS.
```

Jak przydzielić interfejsowi adres z serwera DHCP?

W definicji interfejsu należy podać po prostu:

```
router(config)# interface FastEthernet 0/0
router(config-if)# ip address dhcp
```

Jak przekazać dalej zapytania DHCP?

Wystarczy w zasadzie, na interfejsie podłączonym do sieci, w której znajduje się stacja pobierająca informacje z serwera DHCP wydać polecenie:

```
router(config)# interface FastEthernet 0/0
router(config-if)# ip helper-address IP_serwera_DHCP
```

...ale to włącza przekazywanie wielu rodzajów ruchu. Możesz to zablokować, ograniczając się tylko do DHCP/BOOTP w ten sposób:

```
router(config)# no ip forward-protocol udp tftp
router(config)# no ip forward-protocol udp dns
router(config)# no ip forward-protocol udp time
router(config)# no ip forward-protocol udp netbios-ns
router(config)# no ip forward-protocol udp tacacs
...i dla pewności, że jest włączone:
router(config)# ip forward-protocol udp bootpc
```

SNMP

Jak uruchomić na routerze SNMP?

W najprostszym scenariuszu, wystarczy wydać polecenie:

```
router(config)# snmp-server community mojstring RO 15
```

...gdzie `mojstring` to klucz, który musi podać agent by odczytać dane, `RO` to tryb dostępu (tylko do odczytu, lub `RW` zezwalające również na zapis) i w końcu `100` to numer listy ACL kontrolującej kto może łączyć się z SNMP routera. Lista ta może mieć np. taką konstrukcję:

```
ip access-list standard 15
 permit 192.168.0.10
 permit 192.168.0.15
 deny any
```

...co pozwoli na odczytywanie informacji tylko stacjom o adresach 192.168.0.10 i 192.168.0.15. Numer listy dostępu można pominąć, ale wtedy dostęp do SNMP routera będzie miał każdy host, który nie zostanie odfiltrowany przez ew. ograniczenia ruchowe na interfejsach!

Logowanie zdarzeń

Chciałbym logować zdarzenia zachodzące na routerze do pamięci. Jak to zrobić?

W najprostszych scenariuszu, wystarczy wydać polecenie:

```
router(config)# logging buffered 128000
```

...gdzie 128000 to prośba o rezerwację 128kB pamięci na potrzeby bufora. Najstarsze zdarzenia zostaną nadpisane. Zawartość bufora obejrzyć można poleceniem `show log`.

Chciałbym logować zdarzenia zachodzące na PIXie do pamięci. Jak to zrobić?

Musisz wskazać od którego poziomu zdarzenia będą logowane (0 to najmniej szczegółowy poziom - tylko zdarzenia krytyczne, a 7 najbardziej szczegółowy) a następnie włączyć logowanie:

```
pix(config)# logging buffered 7  
pix(config)# logging on
```

Chciałbym logować zdarzenia zachodzące na routerze do serwera syslog. Jak to zrobić?

Powinieneś kolejno: wskazać host-serwer syslog (lub wiele, komunikaty będą wysyłane jednocześnie do wszystkich), ewentualnie wskazać od którego poziomu komunikaty mają być logowane (ang. *severity*) i jak będą identyfikowane (ang. *facility*), a w końcu włączyć wysyłanie komunikatów:

```
router(config)# logging host 192.168.0.10  
router(config)# logging severity debugging  
router(config)# logging facility local0  
router(config)# logging on
```

Chciałbym logować zdarzenia zachodzące na PIXie do serwera syslog. Jak to zrobić?

Powinieneś kolejno: wskazać host-serwer syslog (lub wiele, komunikaty będą wysyłane jednocześnie do wszystkich), wskazać od którego poziomu komunikaty mają być logowane (ang. *trap X*, gdzie 7 oznacza poziom debugging, czyli najbardziej szczegółowy), a w końcu włączyć wysyłanie komunikatów:

```
pix(config)# logging host 192.168.0.10  
pix(config)# logging trap 7  
pix(config)# logging on
```

Po wymianie karty w routerze statystyki się pomieszały. Co się stało?

Domyślnie routery Cisco po przeładowaniu budują od nowa tablicę indeksów interfejsów. W przypadku zmiany konfiguracji sprzętowej automatycznie poszczególne interfejsy mogą uzyskać inne indeksy. Można jednak zapisywać na stałe numerację interfejsów na pamięci flash, jeśli wydasz polecenie:

```
router(config)# snmp-server ifindex persist
```

Czas

Jak ustawić zegar na routerze?

Poleceniem:

```
router# clock set 16:13:00 23 feb 2004
```

Na mniejszych platformach, zegar nie jest jednak podtrzymywany baterią i po resecie, zostanie wyzerowany.

Jak ustawić zegar wg serwerów czasu z Internetu?

Za pomocą protokołu NTP (jeśli masz router serii 1600, 2500, czy 1700, NTP znajduje się dopiero w oprogramowaniu "IP Plus"). Wystarczy dodać do konfiguracji routera wskazanie serwera czasu (opłaca się wskazać wiele, router wybierze jeden, a jeśli nie będzie mógł się z nim skontaktować, wybierze kolejny z listy).

```
router(config)# ntp server 217.153.69.35
router(config)# ntp server 150.254.183.15
```

To, czy synchronizacja działa, możemy sprawdzić poleceniem `show ntp associations`:

```
router# show ntp associations

      address          ref clock      st when poll reach  delay  offset  disp
+~217.153.69.35      .PPS.          1  585 1024 377   28.7   1.96   15.7
*~150.254.183.15    .PPS.          1  534 1024 377   31.1  -0.83   17.4
 * master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
```

Symbol gwiazdki przy adresie serwera oznacza, że jest on aktualnie wybrany jako serwer czasu i router zsynchronizował pomyślnie czas wg jego wskazań. Należy zauważyć, że od wskazania serwera NTP do zsynchronizowania się z serwerem może minąć od 60 do 120 sekund.

Lista serwerów NTP Stratum 1 znajduje się pod adresem <http://www.eecis.udel.edu/~mills/ntp/clock1a.html> a Stratum 2 pod adresem <http://www.eecis.udel.edu/~mills/ntp/clock2a.html>.

Jeśli Twój router nie obsługuje pełnej implementacji NTP a jedynie SNTP, konfiguracja jest analogiczna ale słowo kluczowe ntp zastępujemy sntp:

```
router(config)# sntp server 217.153.69.35
router(config)# sntp server 150.254.183.15
```

Skonfigurowałem na swoim routerze NTP, ale zegar pozostaje niesynchronizowany - a minęło już parę godzin.

Po pierwsze upewnij się, że serwery które wskazałeś są osiągalne dla Twojego routera - najlepiej wykonaj ping z niego do kolejnych serwerów.

Po drugie sprawdź, czy nie blokujesz ruchu z routera do serwerów ACLkami - powinieneś zezwolić na ruch UDP z i do portu 123, np. w ten sposób:

```
ip access-list extended moj_fw_internet
```

```
permit udp host 217.153.69.35 eq ntp host 169.254.10.1 eq ntp
```

Gdzie 169.254.10.1 to adres interfejsu publicznego Twojego routera, ACLka *moj_fw_internet* przypisana jest w kierunku *in* na tym interfejsie, a 217.153.69.35 to adres serwera NTP. Pamiętaj również, że jeśli modyfikujesz już istniejącą ACLkę, ten wpis musi znaleźć się przed każdym innym, który mógłby go zablokować.

Po trzecie w końcu upewnij się, że administrator danego serwera nie żąda uwierzytelniania poszczególnych łączących się do niego klientów.

NAT

W jakich wersjach oprogramowania obsługiwany jest NAT, PAT oraz mapowanie portów z adresów publicznych na prywatne?

NAT pojawił się w wersji IOS 11.2 w feature-set "IP Plus". Od wersji 12.0 cała funkcjonalność NAT dostępna jest już w standardowej wersji "IP".

Chcę uruchomić NAT - mam jeden interfejs publiczny i jeden prywatny. Jak to zrobić?

W trzech krokach.

- Oznaczasz interfejsy jako publiczny (`ip nat outside`) i jako prywatny (`ip nat inside`) - może być wiele zarówno publicznych jak i prywatnych. Na przykład:

```
router(config)# interface serial 0/99
router(config-if)# ip nat outside
router(config-if)# exit
router(config)# interface fastethernet 0/0
router(config-if)# ip nat inside
router(config-if)# exit
```

Zwróć uwagę, że nazwy Twoich interfejsów mogą być inne.

- Definiujesz, jak ma być wykonywany NAT - na pulę przydzielonych adresów, czy na jakiś konkretny jeden adres - najczęściej publicznego interfejsu routera. Poniżej jak zdefiniować pulę:

```
router(config)# ip nat pool Pula1 169.254.10.1 169.254.10.15 255.255.255.240
```

- Na koniec określasz jaki ruch z interfejsów oznaczonych jako wewnętrzne będzie podlegał NATowaniu i na jakie adresy. Wpisy przeglądane są sekwencyjnie wg kolejności i jeśli router trafi na wpis pasujący do pakietu, nie przejrzy już wpisów późniejszych.

Poniżej przykład, w którym sieć 192.168.10.0/24 NATowana jest na zdefiniowaną wcześniej pulę, a sieć 192.168.20.0/24 na adres interfejsu serial 0.99:

```
! w celu wybrania ruchu z podsieci 192.168.10.0/24 definiujemy
! listę ACL:
router(config)# ip access-list extended Siec10NAT
router(config-acl)# permit ip 192.168.10.0 0.0.0.255 any
router(config-acl)# exit
! i to samo dla sieci 192.168.20.0/24:
router(config)# ip access-list extended Siec20NAT
router(config-acl)# permit ip 192.168.20.0 0.0.0.255 any
router(config-acl)# exit
```

```
! adresy źródłowe pasujące do ACLki Siec1ONAT NATowane są na pulę
! adresów zdefiniowanych wcześniej pod nazwą Pulal:
router(config)# ip nat inside source list Siec1ONAT pool Pulal overload
! ...a adresy źródłowe pasujące do ACLki Siec2ONAT na adres przypisany
! do interfejsu serial 0.99 routera:
router(config)# ip nat inside source list Siec2ONAT interface serial 0.99
overload
```

Mam router z jednym interfejsem i chcę robić NAT - czy to wykonalne?

Tak, taki układ nazywa się "NAT na patyku" (ang. *NAT-on-a-stick*). Na jednym interfejsie (zwykle Ethernetowym) obsługujesz zarówno ruch z sieci lokalnej jak i publicznej. Uważaj jednak, na aspekty bezpieczeństwa w takim układzie - zwykle w takiej topologii urządzenie dostawcy podpięte jest do koncentratora/przełącznika, a ten zarówno do routera jak i innych stacji. Oznacza to, że ktoś może zmienić sobie adres IP na stacji na publiczny i "obejść" Twój router w komunikacji z Internetem!

Na początek skonfigurujemy interfejs FastEthernet 0/0, który służyć nam będzie zarówno do obsługi sieci LAN jak i Internetu. Zakładam, że od dostawcy otrzymałeś publiczny adres 169.254.10.1, Twoją domyślną bramką jest 169.254.10.2 a sieć LAN ma numerację 192.168.0.0/24, przy czym interfejs routera w tej sieci posiada adres 192.168.0.1:

```
router(config)# interface FastEthernet0/0
router(config-if)# ip address 169.254.10.1 255.255.255.0
! Adresem głównym interfejsu jest adres publiczny
router(config-if)# ip address 192.168.0.1 255.255.255.0 secondary
! Dodatkowo przypisujemy do niego adres prywatny tak, by stacje
! w sieci LAN miały zapewnioną bramkę ze swojej podsieci
router(config-if)# ip nat outside
! Oznaczamy interfejs jako zewnętrzny
router(config-if)# ip policy route-map PetlaNAT
! ...i dodajemy do niego route-mapę, która obsługiwać będzie NAT
```

Teraz dodamy logiczny interfejs Loopback 0. Jest on potrzebny, ponieważ NAT na routerach Cisco wykonywany jest tylko i wyłącznie wtedy, gdy pakiet w czasie podróży przez router przechodzi przez interfejs oznaczony jako zewnętrzny (*outside*) i wewnętrzny (*inside*). Do interfejsu możesz przypisać dowolny adres, ale najlepiej żeby był to adres prywatny. W przykładzie użyjemy puli 172.16.0.1/24:

```
router(config)# interface Loopback0
router(config-if)# ip address 172.16.0.1 255.255.255.0
! Przypisujemy interfejsowi adres z innej puli prywatnej
router(config-if)# ip nat inside
! Oznaczamy interfejs jako wewnętrzny
```

Pozostaje teraz po pierwsze skonfigurować NAT, a po drugie route-mapę, która "wymusi" przejście pakietu przez dwa różnie oznaczone z punktu widzenia NATu interfejsy.

Zakładam, że NAT ma być realizowany na publiczny adres interfejsu routera:

```
router(config)# ip nat inside source list SiecDoNAT interface FastEthernet0/0
overload
! Wszystkie pakiety pasujące do ACL SiecDoNAT będą NATowane

! Pozostaje skonfigurować tą ACLkę:

router(config)# ip access-list extended SiecDoNAT
router(config-ext-nacl)# permit ip 192.168.0.0 0.0.0.255 any
```

A teraz konfiguracja route-mapy *PetlaNAT*. Każdy pakiet otrzymany z interfejsu FastEthernet 0/0 zostanie sprawdzony, czy nie pasuje do jej reguł. W naszym przypadku będzie tylko jedna - jeśli pasujesz do

ACLki SiecDoNAT, musisz trafić na interfejs Loopback 0. W ten sposób ruch z sieci LAN zawsze zostanie sztucznie przerzucony na interfejs Loopback 0, gdzie dojdzie do jego zNATowania. Następnie pakiet już z publicznym adresem, zgodnie z normalnymi regułami routingu, zostanie wysłany interfejsem FastEthernet 0/0 w stronę sieci ISP:

```
router(config)# route-map PetlaNAT permit 10
router(config-route-map)# match ip address SiecDoNAT
router(config-route-map)# set interface Loopback0
```

Chcę przekierować port 25/tcp z adresu publicznego routera do sieci wewnętrznej - jak to zrobić?

Zakładam, że chodzi o ruch na adres IP 169.254.10.10 (nasz fikcyjny adres publiczny) na port 25/tcp, i ma on trafiać do stacji gdzieś za routerem, o adresie 192.168.0.10 na ten sam port:

```
router(config)# ip nat inside source static tcp 192.168.0.10 25 169.254.10.10 25
extendable
```

Jak sprawdzić, które interfejsy przypisane są do NAT i jak są skonfigurowane?

Poleceniem:

```
router(config)# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial 0.99
Inside interfaces:
  FastEthernet 0/0
[...]
```

NAT mi nie działa - co może być źle?

Po pierwsze sprawdź (poleceniem `show ip nat stat`), że faktycznie masz przynajmniej jeden interfejs *inside* i jeden *outside*. Polecenie wyświetli również w ostatnich liniach kryteria dla ruchu NATowanego - sprawdź, czy w ogóle NAT zauważa jakieś pakiety godne NATowania (pozycja *hits*).

Po drugie sprawdź, że nie zamieniłeś interfejsu *outside* z *inside* - być może NAT chciałby tłumaczyć adresy, ale otrzymuje ruch nie pasujący do reguł.

Po trzecie, sprawdź czy ruchu do NATowania nie blokujesz w żaden sposób na interfejsie wewnętrznym, ani wracającego na interfejsie zewnętrznym. Zweryfikuj konfigurację routingu, jeśli NATujesz sieci nie podłączone bezpośrednio do routera - być może definicja co NATować jest zbyt wąska.

SSH

Jak skonfigurować SSH?

Po pierwsze, sprawdź czy w ogóle posiadasz w swoim IOSie funkcjonalność SSH. Pojawiła się ona w linii 12.0 i jest obecna tylko w feature-setach posiadających funkcjonalność "IPsec" (routery), "Service Provider SSH" (większe routery, od 7xxx) oraz "Crypto" (przełączniki Catalyst). Od wersji IOS 12.3 dostępna jest na routerach w każdym IOSie (za wyjątkiem tych oznaczonych 'W/O CRYPTO') oraz od linii 12.2(x) na przełącznikach Catalyst w nowych wersjach pakowania IOSa (również za wyjątkiem tych

oznaczonych 'W/O CRYPTO').

Pierwszym krokiem jest nadanie routerowi nazwy własnej i domenowej. Informacje te będą wymagane do wygenerowania kluczy: prywatnego i publicznego.

```
router# conf t
router(config)# hostname c1760
c1760(config)# ip domain name test.pl
```

Teraz generujemy klucze:

```
c1760(config)# crypto key generate rsa

The name for the keys will be: c1760.test.pl
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024

! Wybraliśmy klucze o długości 1024 bitów

% Generating 1024 bit RSA keys ...[OK]
```

W tym momencie serwer SSH zostaje włączony. Uwierzytelnianie odbywa się w oparciu o skonfigurowane, zewnętrzne bazy danych (RADIUS itp.), lub domyślnie - w oparciu o lokalną bazę użytkowników (poleceniami `username X [...]').

Dodatkowo, można ograniczyć dostęp do routera tylko do protokołu SSH, wydając na liniach wirtualnych terminali polecenie:

```
c1760(config)# line vty 0 15
c1760(config-vty)# transport input ssh
```

Jak sprawdzić, czy serwer SSH jest włączony?

Poleceniem `show ip ssh':

```
router# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

Rejestr konfiguracyjny routerów

Po zapisaniu konfiguracji i przeladowaniu routera, tracę konfigurację - dlaczego?

Jeśli faktycznie zapisanie konfiguracji się powiodło, to najprawdopodobniej problem leży w ustawieniu rejestru konfiguracyjnego na pomijanie plików startowych. Po zalogowaniu się na router wykonaj:

```
router# conf t
router(config)# config-register 0x2102
router(config)# exit
```

Co dokładnie oznaczają bajty z rejestra konfiguracyjnego?

Rejestr konfiguracyjny, to heksdecymalna wartość, na którą składają się następujące możliwe wartości:

Bit	Wartość	Znaczenie
00-03	0x0000-0x000F	Sposób startu urządzenia: 0x0000 - start do promptu bootstrap 0x0001 - start z obrazu przechowywanego w EPROMie 0x0002 do 0x000F - standardowy boot
06	0x0040	Zignoruj ustawienia z NVRAM (konfigurację)
07	0x0080	Wyłącz informacje wyświetlane podczas startu
08	0x0100	Wyłączona sekwencja Break. Niezależnie od tego ustawienia, przekazanie routerowi tej sekwencji podczas startu, spowoduje wejście do ROMMONa.
10	0x0400	Włączona obsługa broadcastów IP z samymi zerami
11-12	0x0800-0x1000	Ustawienie prędkości konsoli: 0x0800 - 9600 0x1000 - 115200
13	0x2000	Wystartuj z oprogramowania przechowywanego w ROMie, jeśli nie uda się wystartować z flasha/sieci
14	0x4000	Broadcasty IP nie mają dołączanych numerów sieci
15	0x8000	Włącz szczegółowe informacje diagnostyczne i pomiń konfigurację z NVRAMu

Domyślna wartość to 0x2102. Oznacza ona, że router powinien wystartować z obrazu przechowywanego w pamięci Flash i spróbować załadować konfigurację z pamięci NVRAM. Prędkość konsoli ustalona jest na 9600. Dokładnie takie samo zachowanie, ale z konsolą ustawioną na 115200 daje ustawienie rejestru konfiguracyjnego na wartość 0x3922.

Czy do ustawiania rejestru konfiguracyjnego można użyć jakiegoś narzędzia?

Firma Boson udostępniła program, umożliwiający konfigurację rejestru w systemie Windows "wizualnie": http://download.boson.com/utills/bos_calc.exe.

VLANy

Co to są VLANy?

VLAN, czyli *Virtual LAN*, to po prostu podział w warstwie drugiej sieci na wiele mniejszych domen rozgłoszeniowych. Aby ruch mógł być wymieniany pomiędzy dwoma hostami znajdującymi się w różnych VLANach, potrzebne jest urządzenie warstwy trzeciej - router. Dzisiaj bardzo często routing między VLANami realizuje się na przełącznikach, kiedyś rolę tę pełniły routery.

Istnieje standard tworzenia VLANów - zdefiniowany przez IEEE 802.1Q. Opisuje on dokładnie, jak rozszerzyć ramkę L2 aby zawrzeć w niej informacje, do którego VLANu ramka należy (są to w tzw. ramki tagowane). Połączenie, które przenosi ramki z jednocześnie wielu VLANów, nazywa się trunkiem. Cisco zdefiniowało wcześniej na swoich przełącznikach standard ISL - jest on bardzo często spotykany w starszych urządzeniach. Działa on w zasadzie tak samo jak 802.1Q, ale ramka ulega "zapakowaniu" w nową, co zwiększa czas potrzebny na przeprowadzanie operacji - i co ważniejsze, nie jest obsługiwane przez innych niż Cisco producentów.

Co to jest VLAN "natywny"?

To VLAN używany przez przełączniki do przenoszenia informacji administracyjnych (np. BPDU, CDP itp.). Domyślnie jest to VLAN 1. Porty przełączników Cisco w domyślnej konfiguracji należą właśnie do tego

VLANu.

Na trunkach (niezależnie czy 802.1Q czy ISL), VLAN natywny przenoszony jest bez tagowania.

Co mają na myśli ludzie mówiąc "router na patyku" (ang. *router on a stick*)?

Chodzi o topologię, w której jeden interfejs routera służy do obsługi routingu z wielu sieci.

Na przykład masz 24-portowy przełącznik warstwy drugiej, dwa VLANy i chcesz jakoś przekazywać ruch między nimi w oparciu o warstwę trzecią. Najprościej będzie zdefiniować na przełączniku jeden port jako trunk 802.1Q przenoszący oba VLANy, podłączyć ten port do routera skonfigurowanego analogicznie i nadać na routerze adresy IP obu podinterfejsom.

Oto przykładowa konfiguracja interfejsu FastEthernet (pamiętaj, że obsługa 802.1Q dla większości routerów zawarta jest dopiero w feature-set "IP Plus"):

```
interface FastEthernet0/0
  no ip address
!
interface FastEthernet0/0.1
  description VLAN 10, domyślna bramka dla pierwszej podsieci
  encapsulation dot1q 10
  ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/0.2
  description VLAN 20, domyślna bramka dla drugiej podsieci
  encapsulation dot1q 20
  ip address 192.168.20.1 255.255.255.0
```

Portu na przełączniku (tu akurat 2950), podłączonego do routera:

```
interface FastEthernet0/24
  switchport trunk allowed vlan 10,20
  switchport mode trunk
  no ip address
  spanning-tree portfast
```

W końcu port do którego podłączona jest stacja z VLANu 10:

```
interface FastEthernet0/1
  switchport mode access
  switchport access vlan 10
  no ip address
  spanning-tree portfast
```

Czy Cisco PIX może obsługiwać VLANy?

Tak, ale od PIX OS w wersji 6.3 i tylko modele od 515 w górę (525 i 535). Dokładna ilość VLANów obsługiwanych przez PIXa związana jest z posiadaną licencją i przedstawiono ją w poniższej tabelce:

Platforma	Licencja	Interfejsy fizyczne	Interfejsy logiczne
PIX-501	-	1+4 (przełącznik)	2
PIX-506/506E	-	2	2
PIX-515/515E	R	2+1 opcja	3
PIX-515/515E	UR/FO	6	8
PIX-520/525	R	6	10 (6+4)
PIX-520/525	UR/FO	8	10

PIX-535	R	6	8
PIX-535	UR/FO	10	22

Jak skonfigurować na PIXie VLAN?

Oto przykład konfiguracji PIXa 515 z VLANem na drugim porcie fizycznym:

```
interface ethernet0 auto
! interfejs eth0 nie jest tagowany
interface ethernet1 auto
! aktywujemy interfejs eth1
interface ethernet1 vlan20 physical
! VLAN 20 przynoszony będzie nietagowany
interface ethernet1 vlan30 logical
! VLAN 30 przynoszony będzie tagowany zgodnie z 802.1Q
...
nameif ethernet0 outside security0
! fizyczny interfejs eth0 podpinamy do routera ISP
nameif ethernet1 inside security100
! nietagowane ramki na fizycznym porcie eth1 należą do LANu
nameif vlan30 dmz security50
! tagowane ramki na fizycznym porcie eth1 (VLAN 30) należą do DMZtu

! Pozostaje nadanie adresów IP:

ip address dmz 169.254.76.1 255.255.255.0
ip address inside 192.168.0.1 255.255.255.0
ip address outside 169.254.12.2 255.255.255.252
```

Poniżej przykładowe fragmenty z konfiguracji przełącznika. Fizyczny interfejs eth1 PIXa dołączono do portu FE0/6, zdefiniowanego jako trunk 802.1Q, przynoszący VLAN 30, oraz VLAN 20 jako natywne:

```
interface FastEthernet0/6
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 30
switchport trunk native vlan 20
```

Jak sprawdzić...

...ile interfejsów logicznych obsłuży router X?

Każdy interfejs zajmuje minimalną ilość pamięci routera. Lista interfejsów przechowywana jest w tzw. IDB, czyli *Interface DataBase*. W zależności od wielkości routera, a także w mniejszym stopniu od wersji Cisco IOS na nim pracującego, pojemność tej bazy różni się. Aktualna lista znajduje się tutaj: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a0080094322.shtml

Na swoim routerze, ilość "wolnego miejsca" na dodatkowe interfejsy, możesz sprawdzić poleceniem `show idb`:

```
router# show idb

Maximum number of Software IDBs 300. In use 17.
```

	HWIDBs	SWIDBs
Active	13	13
Inactive	4	4
Total IDBs	17	17
Size each (bytes)	4648	1392
Total bytes	79016	23664

Powyższa informacja pochodzi z routera 1712 - widać, że router obsługuje do 300 interfejsów, z czego 17 jest już zajętych.

...aktualne obciążenie procesora?

Posługując się poleceniem ``show processes cpu``:

```
router# show processes cpu
CPU utilization for five seconds: 6%/2%; one minute: 6%; five minutes: 5%
  PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
    1     1808         833      2170   0.00%  0.00%  0.00%  0 Chunk Manager
    2      140       90945         1   0.00%  0.00%  0.00%  0 Load Meter
[...]
```

Wartość podzielona (6%/2%) to:

- **6%** - średnie ogólne zajęcie procesora przez ostatnie pięć sekund; jest ono *sumą* obciążenia wywołanego przez przerwania i procesy
- **2%** - średnie obciążenie przez ostatnie pięć sekund związane z przerwaniami

Jak nietrudno się domyślić, pierwsza wartość minus druga wartość daje obciążenie procesora przez różnego rodzaju procesy działające na routerze (NAT, DHCP, obsługa IP, IPsec itp.).

Pozostałe dwie wartości z wydruku, to zgodnie z nazwą uśrednione obciążenie ogólne za poprzednią minutę i pięć minut.

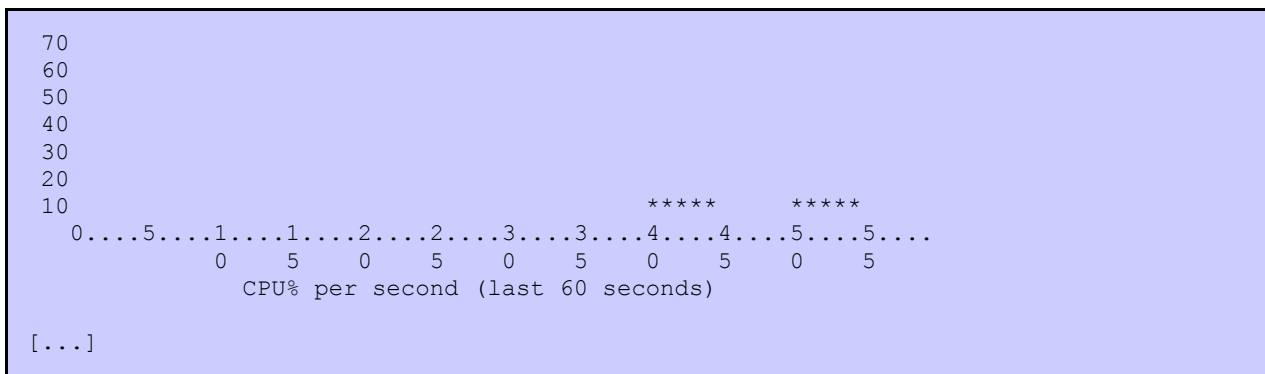
Parę uwag co do wartości podzielonej (6%/2%):

- W czasie normalnej pracy routera, obie wartości powinny być do siebie zbliżone.
- Jeśli pierwsza wartość jest dużo większa od drugiej (np. widzisz na swoim routerze wartość **75%/16%**), oznacza to jakiegoś rodzaju atak na router, lub istotny problem z któryś z procesów.
- Jeśli oba parametry są wysokie (np. **95%/92%**), router obsługuje za dużo ruchu - postaraj się zoptymalizować jego konfigurację, zweryfikować poprawność topologii swojej sieci lub wymienić router na większy.

...historyczne obciążenie procesora?

Posługując się poleceniem ``show processes cpu history``. Router pokaże trzy wykresy: za ostatnią minutę, za ostatnią godzinę i za ostatnie 72 godziny. Oś X pokazuje upływający czas, oś Y obciążenie procesora (zgrubnie), a wartości u góry wykresu - dokładne obciążenie. Np.:

```
router# show processes cpu history
      3333333333444443333333332222444444444555553333355553333
100
 90
 80
```



...w liście procesów tylko te, zajmujące jakieś zasoby procesora?

W ten sposób:

```
router# show processes cpu | exclude 0.00%_0.00%_0.00%
CPU utilization for five seconds: 5%/1%; one minute: 4%; five minutes: 4%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
  5      363736      51123      7114   0.00%  0.05%  0.05%  0 Check heaps
  9      34092       79729      427    0.07%  0.00%  0.00%  0 ARP Input
 24     3597724     451492     7968   2.00%  1.93%  1.94%  0 TTY Background
 29      9556       87956      108    0.07%  0.00%  0.00%  0 Net Input
 31     183808      7682      23927  0.00%  0.03%  0.00%  0 Per-minute Jobs
 40      5700       1894      3009   1.59%  0.29%  0.38%  6 SSH Process
 41     1092960    1344980     812   0.63%  0.32%  0.29%  0 IP Input
 59     228164     739184      308   0.07%  0.00%  0.00%  0 CEF process
 62     17884      98746      181   0.00%  0.01%  0.00%  0 IP-EIGRP: PDM
116     223904    1800331     124   0.00%  0.05%  0.06%  0 COLLECT STAT COU
126     13524      7591      1781   0.00%  0.01%  0.00%  0 SNMP ENGINE
132     14680     295105      49    0.00%  0.03%  0.01%  0 IP-EIGRP: HELLO
```

...zajętość pamięci?

Listę procesów z podstawowymi informacjami można sprawdzić poleceniem:

```
router# show processes memory
Total: 78044960, Used: 13534380, Free: 64510580
PID TTY  Allocated    Freed    Holding    Getbufs    Retbufs Process
  0  0    254908      55980    7590192      0          0 *Init*
  0  0      840       71100     840          0          0 *Sched*
  0  0  18419360    7879520    20080    252348      0 *Dead*
  1  0     3256         0     10100         0          0 Chunk Manager
  2  0      188         188     3844         0          0 Load Meter
  3 130  1288172    1196764    104264         0          0 SSH Process
  4  0      188         188     6844         0          0 fastblk backgrou
  5  0     65580         0     90424         0          0 EDDRI_MAIN
  6  0         0         536     6844         0          0 Check heaps
  7  0   9666440    7616660    619640    1091448    1447712 Pool Manager
```

Pierwsza linijka wydruku podaje informacje sumaryczne. Router ma ogółem 78MB pamięci użytecznej, z tego używa obecnie 13,5MB a wolne pozostaje 64MB.

Kolejne kolumny na liście to:

- PID - identyfikator procesu

- TTY - z którą konsolą skojarzony jest proces - większość procesów ma tutaj wartość 0, co oznacza, że skojarzone są tylko z procesem *Init*.
- Allocated - ile historycznie proces zaallokował pamięci
- Freed - ile historycznie proces zwolnił pamięci
- Holding - ile aktualnie rezerwuje/używa pamięci

Natomiast bardziej konkretną informację, dotyczącą tylko pamięci, można uzyskać wydając polecenie `show memory statistics`:

```
router# show memory statistics
```

	Head	Total (b)	Used (b)	Free (b)	Lowest (b)	Largest (b)
Processor	631920E0	78044960	13548532	64496428	64033028	63721760
I/O	7C00000	4194304	2399272	1795032	1457520	1653884

Tutaj dodatkowo widać pamięć zarezerwowaną na operacje I/O (ang. *Input/Output*), czyli na komunikację z zainstalowanymi kartami interfejsów.

...objętość pamięci wykorzystywaną przez procesy routingu?

W ten sposób:

```
router# show ip route summary
```

IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 16

Route	Source	Networks	Subnets	Overhead	Memory (bytes)
connected		0	4	288	544
static		32	2	2448	4624
eigrp	10	1	18	1368	2584
internal		2			2312
Total		35	24	4104	10064

W ostatniej kolumnie widać zajętość pamięci w bajtach. Zwróć jednak uwagę, że chodzi tylko o pamięć zajmowaną we wskazanej tablicy routingu (tutaj, `Default-IP-Routing-Table(0)`), czyli tablica główna). Same procesy routingu mogą zajmować dużo więcej pamięci.

...jakie karty zainstalowano w routerze?

Jeśli wynik polecenia `show version` jest niewystarczający, możesz dodatkowo użyć polecenia `show diag`. Powinno ono zwrócić masę szczegółów dotyczących zainstalowanych i wykrytych poprawnie kart. Poniżej lista kart w routerze 1712:

```
router# show diag
```

Slot 0:

- C1712 1FE 4ESW Mainboard Port adapter, 6 ports
- [...]
- WIC/VIC Slot 0:
- 4 Port FE Switch
- [...]
- Product (FRU) Number : WIC-4ESW=
- WIC/VIC Slot 1:
- BRI S/T - 2186
- [...]

Slot 3:

- Virtual Private Network (VPN) Module Port adapter, 1 port
- [...]

```
Product (FRU) Number      : MOD1700-VPN=
```

W nowszych IOSach pojawiło się również polecenie `show inventory`, które dotyczy mniej danych technicznych, a bardziej po prostu faktycznego wyposażenia routera. Poniżej wynik działania tego polecenia na routerze 2650XM:

```
2650xm# show diag
NAME: "2650XM chassis",
  DESCR: "2650XM chassis, Hw Serial#: JAE01234ABC (12345678), Hw Revision: 0x200"
  PID: 2650XM          , VID: 0x200, SN: JAE01234RAU (12345678)

NAME: "2600 Chassis Slot 0", DESCR: "2600 Chassis Slot"
PID: 2600 Chassis Slot , VID:      , SN:

NAME: "C2600 Mainboard", DESCR: "C2600 Mainboard"
PID: C2600 Mainboard   , VID: 2.0, SN: 12345678

NAME: "DaughterCard Slot 0 on Card 0", DESCR: "2600 DaughterCard Slot"
PID: 2600 DaughterCard Slot, VID:      , SN:

NAME: "WAN Interface Card - Serial (1T)", DESCR: "WAN Interface Card - Serial (1T)"
PID: WAN Interface Card - Serial (1T), VID: 1.0, SN: 20512345

NAME: "Serial0/0", DESCR: "PowerQUICC Serial"
PID: PowerQUICC Serial , VID:      , SN:

NAME: "DaughterCard Slot 1 on Card 0", DESCR: "2600 DaughterCard Slot"
PID: 2600 DaughterCard Slot, VID:      , SN:

NAME: "AIM Container Slot 0", DESCR: "AIM Container Slot 0"
PID: AIM Container Slot 0, VID:      , SN:

NAME: "FastEthernet0/0", DESCR: "AmdFE"
PID: AmdFE              , VID:      , SN:

NAME: "2600 Chassis Slot 1", DESCR: "2600 Chassis Slot"
PID: 2600 Chassis Slot , VID:      , SN:
```

...jakie karty zainstalowano w przełączniku pracującym pod kontrolą CatOS?

Wydając polecenie:

```
switchc> show module

Mod Slot Ports Module-Type           Model                Sub Status
-----
 1   1     2   1000BaseX Supervisor   WS-X6K-SUP1A-2GE    yes ok
15   1     1   Multilayer Switch Feature WS-F6K-MSFC         no  ok
 8   8    48   10/100BaseTX Ethernet   WS-X6248-RJ-45     no  ok
 9   9    48   10/100BaseTX Ethernet   WS-X6348-RJ-45     yes ok

[...]

Mod Sub-Type           Sub-Model            Sub-Serial  Sub-Hw
-----
 1  L3 Switching Engine  WS-F6K-PFC          SAD03462981 1.0
 9  Inline Power Module   WS-F6K-VPWR         1.0
```

...co obsługuje dany feature-set?

Dobrym źródłem informacji, jaka dokładnie funkcjonalność znajduje się w konkretnym obrazie, jest *Cisco Feature Navigator* dostępny pod adresem: <http://www.cisco.com/go/fn>.

Niestety, dostępny jest tylko dla posiadaczy kont CCO.

...znając nazwę pliku Cisco IOS jaki to feature-set?

Dla IOSów od 9 do 12.2 istnieją pewne reguły, opisujące co znaczy konkretna literka w nazwie. Opisano je tutaj: http://www.cisco.com/en/US/products/sw/iosswrel/ios_abcs_ios_networking_the_enterprise0900aecd800a4e14.html.

Generalnie, nazwa pliku (np. c2600-i-mz.123-1a.bin) z Cisco IOS składa się z:

- Platformy, na której będzie pracować obraz (c2600 to routery Cisco serii 2600);
- Funkcjonalności zawartej w obrazie (i, czyli tylko podstawowa funkcjonalność IP);
- Czy obraz wykonywany jest w pamięci RAM (literka m), czy w pamięci Flash (literka f) lub z ROM (literka r) lub relokowalny (literka l). Dodatkowo, można się dowiedzieć, że obraz jest spakowany zwykłym ZIPem (literka z), lub mZIPem (literka x);
- Numeru wersji Cisco IOS 123-1a czyli 12.3.1a;

Poniżej spis literek, które oznaczają funkcjonalności:

```
i - funkcjonalność "IP"
j - funkcjonalność "Enterprise"
c - funkcjonalność "Remote Access Server"
d - funkcjonalność "IP/IPX/AT/DECnet"
p - funkcjonalność "Service Provider"
y - ograniczona funkcjonalność "IP" (bez Kerberos, RADIUS,
  NTP, OSPF, PIM, SMRP, NHRP itp.)

s - funkcjonalność "Plus"
o - funkcjonalność "Firewall"
o3 - funkcjonalność "Firewall/IDS"
x - funkcjonalność "H.323"
n - funkcjonalność "IPX"

k8 - obraz z szyfrowaniem CET/DES
56i - obraz z szyfrowaniem CET/DES dla obrazów na starsze platformy
k9 - obraz z szyfrowaniem CET/DES/3DES (i AES, od 12.2T/12.3)
```

Najczęściej spotykane funkcjonalności to:

```
-i- = IP only
-is- = IP Plus
-oy- = IP Firewall (na starsze platformy)
-io3- = IP/FW/IDS
-x- = IP H.323
-ik8s- = IP Plus IPsec DES
-ik9s- = IP Plus IPsec 3DES
-ik9o3s- = IP/FW/IDS Plus IPsec 3DES
-k91p- = Service Provider + SSH
```

Natomiast od linii 12.3 pojawiło się nowe, mające uporządkować wiele różnych (ponad 80) wersji funkcjonalności nazewnictwo. Większość funkcjonalności IP Plus weszła do obecnie podstawowego obrazu **IP Base**. Zaawansowane usługi bezpieczeństwa (firewall CBAC, IDS/IPS, VPNy) znajdują się teraz od feature-setu **Advanced Security** (od linii 12.4(4)T jest tu również protokół BGP). Funkcjonalność potrzebna w środowiskach dostawców usług znajduje się w pakiecie **SP Services** (m.in. protokół BGP, ale również obsługa głosu i CallManager Express). Dokładniejszy podział funkcjonalności znaleźć można w

tym dokumencie:

<http://www.cisco.com/en/US/products/sw/iosswrel/ps5460/index.html>

Zmiany dotyczą również przełączników – na mniejszych Catalystach zanikają zatem funkcjonalności SMI/EMI (lub SI/EI dla przełączników L2) a pojawiają się LAN Base, Advanced IP Services itp.

...czy dana karta/moduł kompatybilna jest z danym routerem?

Dobrym źródłem informacji o wzajemnej kompatybilności jest *Cisco Hardware-Software Matrix* dostępny pod adresem: <http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi>.

Niestety, dostępny jest tylko dla posiadaczy kont CCO.

...na którym porcie routera znajduje się urządzenie o danym adresie MAC lub IP?

Wystarczy, że wydasz polecenie ``show ip arp aaaa.bbbb.cccc'`, gdzie ciąg `aaaa.bbbb.cccc` to szukany adres MAC, lub ``show ip arp A.B.C.D'`, gdzie ciąg `A.B.C.D` to adres IP:

```
! dla adresu MAC:
router# show ip arp 0000.cd0f.4feb

Protocol  Address          Age (min)  Hardware Addr  Type   Interface
Internet  192.168.10.10    2         0000.cd0f.4feb ARPA   FastEthernet0/0

! dla adresu IP:
router# show ip arp 192.168.10.10

Protocol  Address          Age (min)  Hardware Addr  Type   Interface
Internet  192.168.10.10    2         0000.cd0f.4feb ARPA   FastEthernet0/0
```

...na którym porcie przełącznika Catalyst wpięto urządzenie o danym adresie MAC?

Jeśli na przełączniku zainstalowano IOS, wystarczy, że wydasz polecenie ``show mac-address-table | include aaaa.bbbb.cccc'`, gdzie ciąg `aaaa.bbbb.cccc` to szukany adres MAC:

```
switch# show mac-address-table | include 0000.cd0f.4feb
1      0000.cd0f.4feb    DYNAMIC    Fa0/24
```

Jak widać, urządzenie o tym adresie MAC wpięte jest do portu FastEthernet 0/24 na lokalnym przełączniku. Jeśli zamiast portu wskazany jest trunk - należy sprawdzić na kolejnym przełączniku, podłączonym do lokalnego wskazanym trunkiem.

...budżet mocy na modularnym przełączniku Catalyst?

Skorzystaj z kalkulatora dostępnego pod adresem <http://www.cisco.com/go/powercalculator>.

Rozdział 7. Wybór sprzętu pod konkretne zastosowanie

Jaki router wystarczy do małej sieci (10-15 użytkowników), w sytuacji, gdy Internet dochodzi do mnie Ethernetem?

Rzuć okiem na router serii 830 - konkretnie interesować Cię będzie model Cisco 831, lub nawet PIX 501/506E. Pamiętaj, że PIXy nie obsługują tuneli GRE czy funkcjonalności QoS.

Jeśli jednak będziesz chciał zapewnić sieci połączenie zapasowe, musisz spojrzeć na wyższe modele.

Jaki router wystarczy do małej sieci (10-15 użytkowników), w sytuacji, gdy Internet dochodzi do mnie stykiem V.35 (Polpak-T)?

Najmniejszy router Cisco, do którego podłączyć można V.35 to model 805. Problem polega na tym, że interfejs tego routera obsługuje taktowanie tylko do 512kbit/s, co oznacza, że nie nadaje się raczej do większości instalacji (np. Polpak-T zestawia się zwykle na prędkości 1 lub 2Mbit/s).

Jeśli zależy Ci na sprzęcie używanym (niska cena, ale pamiętaj o braku oficjalnego serwisu dla tego sprzętu!), rozejrzyj się na Allegro za routerami klasy 1601 czy 2503. Posiadają one zamontowane porty szeregowy i Ethernet, przy czym porty szeregowy mają styk DB-60. Do takiego routera potrzebujesz jeszcze kabla DTE V.35 (oryginalny kabel posiada oznaczenie CAB-V35MT). Problemem tego sprzętu jest mała wydajność - 2Mbit/s łącze obsługuje bez problemu, ale dodawanie nowej funkcjonalności (dużych list ACL, kontroli zawartości pakietów przez NBAR itp.) może znacznie zmniejszyć wydajność i spowodować rwanie się połączeń, czy problemy z ich nawiązaniem.

Najmniejszy router dostępny "z półki" to 1721, do którego w celu obsługi łącza z V.35 należy dołożyć kartę WIC-1T (jeden styk DB-60, kabel CAB-V35MT) lub WIC-2T (dwa styki Smart Serial, dwa kable CAB-SS-V35MT). Routery te posiadają obecnie standardowo po 64MB RAM i 32MB flash, co pozwala na rozbudowę w przyszłości o Cisco IOS z większą funkcjonalnością.

Jeśli myślisz o obsłudze dwóch równoległych łączy 2Mbit/s i będziesz kupował nowy router, już dzisiaj zastanów się nad routerami klasy 2600XM. Routery 2610XM, 2620XM i 2650XM posiadają po jednym FastEthernetie, a 2611XM, 2621XM i 2651XM po dwa FastEthernety. Poza nimi, konfiguracja sprzętowa jest taka sama: wszystkie posiadają jeden slot NM i dwa sloty WIC, plus slot AIM ukryty w obudowie. Routery różnią się wydajnością (2610XM/2611XM w granicach 20kpps, 2620XM/2621XM 30kpps i 2650XM/2651XM 40kpps) i domyślnie dostarczaną wielkością pamięci (2610/11/20/21XM mają po 64MB RAM i 32MB flash, 2650/51XM 128MB RAM i 32MB flash).

Jaki router wystarczy do małej sieci (10-15 użytkowników), w sytuacji, gdy chcemy bezpiecznie połączyć się VPNem do innej podobnej lokalizacji przez łącze zakończone Ethernetem?

Cisco przewidziało specjalnie do takich celów routery 1711/1712. W cenie symbolicznie tylko wyższej od podstawowego modelu 1721 otrzymujemy router z:

- "WAN"-owskim portem Ethernet, do którego możemy podłączyć np. modem DSL (zakończony Ethernetem, *nie* stykiem ADSL!)
- cztero-portowym przełącznikiem 10/100 dla podłączenia urządzeń LAN, z obsługą VLAN-ów (a także routingu między nimi realizowanymi przez procesor routera)
- analogowym portem modemowym (1711) lub ISDN BRI (1712), na którym można zrealizować połączenie zapasowe (lub główne - pełna elastyczność)
- sprzętową obsługą szyfrowania DES/3DES/AES (zainstalowany moduł MOD1700VPN), co daje (wg dokumentacji) obsługę do 100 jednoczesnych tuneli VPN i przepustowość 3DES do 15 Mbit/s
- oprogramowanie o funkcjonalności Firewall/IDS IPsec 3DES.

Warto zauważyć, że dzięki połączeniu VLAN-ów z oprogramowaniem Firewall da się nawet zaimplementować na tym urządzeniu prosty DMZ.

Oczywiście, jeśli takie połączenia VPN schodzą się w jakimś punkcie centralnym to musi się tam znajdować odpowiednio mocniejsze urządzenie terminujące tunele, np. koncentrator VPN, lub większy router z kartą VPN albo PIX z kartą VAC.

Mam dwa łącza od dwóch ISP i chciałbym uruchomić BGP. Jakiego routera powinienem użyć?

Generalnie, routing BGP można uruchomić nawet na routerach serii 800. Zakładamy jednak, że chodzi o instalacje z dużą siecią LAN, relatywnie dużym ruchem z i do Internetu (rzędu 4-200Mbit/s) oraz chęcią realizowania innych usług - filtrowania ruchu, NATowania itp.

Bezpiecznie będzie założyć, że potrzebujesz routera z serii 7200 - 7204VXR lub 7206VXR (odpowiednio 4 lub 6 slotów na karty interfejsów). W takim routerze powinna znaleźć się karta z procesorem sieciowym, w nomenklaturze Cisco oznaczana jako NPE. Aby uruchomić BGP i sensownie obsługiwać ruch, powinieneś obecnie wyposażyć się w moduł NPE-400 lub NPE-1G, względnie NSE-1. Karta NPE/NSE powinna mieć minimum 256MB RAM, jeśli chcesz otrzymywać pełne światowe tablice BGP.

Zajrzyj również do sekcji poświęconej routingowi BGP, aby uzyskać więcej informacji o działaniu tego protokołu, jego konfiguracji i innych zaleceniach.

Potrzebuję mały przełącznik Cisco, bez routingu

Najmniejsze obecnie w sprzedaży nieroutujące przełączniki, to seria 2950. Oferowane są w wersjach bez modułów GBIC (WS-C2950-12 i WS-C2950-24, odpowiednio 12 i 24 porty 10/100), oraz z slotami na dwa moduły GBIC (WS-C2950G-12, WS-C2950G-24 i WS-C2950G-48). Dostępne są również małe modele 2940, zawierające osiem portów 10/100BaseTX oraz albo jeden port 1000BaseTX (WS-C2940-8TT), albo jeden port 100BaseFX z możliwością zamiennie wykorzystania jednego modułu SFP (WS-C2940-8TF). Dodatkowo, w sprzedaży znajdują się wersje, które zamiast slotów na moduły GBIC, mają zabudowane porty na stałe. Są to:

- WS-C2950T-24 - 24 porty 10/100 + 2 porty 10/100/1000BaseT
- WS-C2950T-48 - 48 portów 10/100 + 2 porty 10/100/1000BaseT
- WS-C2950C-24 - 24 porty 10/100 + 2 porty 100BaseFX
- WS-C2950SX-24 - 24 porty 10/100 + 2 porty 1000BaseSX
- WS-C2950SX-48 - 48 portów 10/100 + 2 porty 1000BaseSX

Część przełączników może dodatkowo posiadać oprogramowanie w wersji EI (lub jest z nim sprzedawana). W porównaniu do standardowego SI, EI oznacza obsługę jednocześnie większej ilości VLANów (250 w porównaniu do standardowych 64), możliwość konfigurowania ograniczania pasma per port (tylko policing, nie ma shapingu), a także możliwość obsługi połączeń przez SSH (tylko w specjalnych wersjach "Crypto").

Niezależnie od wersji, przełączniki obsługują oprogramowanie *CMS*, czyli *Cluster Management Suite*, które rezyduje w pamięci flash przełącznika i umożliwia zarządzanie nim za pomocą graficznego interfejsu użytkownika.

W sprzedaży znajduje się również model 2970, który ma architekturę zbliżoną do 2950, ale wyposażony jest w 24 porty 10/100/1000BaseTX + w jednej z wersji, w uplinki GBIC.

Potrzebuję przełącznik Cisco potrafiący realizować routing

Przełączniki niemodularne

Jeśli chodzi o przełączniki niemodularne, to w sprzedaży znajdują się przełączniki 3550 i 3750. Obie rodziny realizują routing IP z maksymalną prędkością na wszystkich portach (tzw. *wire-speed*). Dodatkowo mają możliwość filtrowania ruchu (zarówno wg adresów MAC i adresów IP, z dokładnością do portów TCP/UDP).

Oba modele obsługują dwie linie oprogramowania - SMI (*Standard Multilayer Image*) i EMI (*Enhanced Multilayer Image*). Wersja SMI zawiera routing IP statyczny oraz RIP obu wersji, w wersji EMI otrzymujemy dodatkowo IGRP, OSPF i EIGRP (dla 3550 dodatkowo BGP).

Więcej o przełącznikach 3550 możesz poczytać tu: <http://www.cisco.com/go/cat3550> a o 3750 tutaj: <http://www.cisco.com/go/cat3750>.

Przełączniki modułarne

Natomiast jeśli potrzebujesz modułarny przełącznik, obecnie Cisco sprzedaje serie 4500 oraz 6500. 4500 jest "zeskalowaną w dół" wersją 6500, ale oferuje zarówno porty 10/100BaseTX, 100BaseFX jak i gigabit we wszystkich standardach oraz realizuje większość funkcjonalności rodziny 6500. Niestety nadal karty 10GbE dostępne są tylko dla 6500/7600 (montaż takiej karty w 4500 nie ma sensu, każdy moduł ma zarezerwowane tylko 6Gbit/s do i z modułu zarządzającego). Więcej informacji o przełącznikach 4500 znajdziesz tutaj: <http://www.cisco.com/go/cat4000>, a o rodzinie 6500 tutaj: <http://www.cisco.com/en/US/products/hw/switches/ps708/index.html>.

Czy Cisco sprzedaje tzw. "firewalle sprzętowe"?

Tak, nazywają się Cisco PIX (ang. *Private Internet eXchange*). Oferowane są od modeli 501 i 506E (bez możliwości rozbudowy), przez 515, 525 do 535 (z modułami GigabitEthernet) do karty realizującej ścianę ogniową w przełącznikach Catalyst 6500 (karta nazywa się FWSM, a jej P/N handlowy to: WS-SVC-FWM-1-K9=). PIXy dedykowane są w stanie filtrować ruch do 1,7Gbit/s (pakiety 1400 bajtowe, PIX-535UR), natomiast karta do Catalysta ma przepustowość do 5,5Gbit/s.

PIXy obsługują programowe i sprzętowe (dodatkowa karta do modeli 515/525/535) szyfrowanie IPsec dla DES/3DES/AES (ten ostatni od PIX OS 6.3), oraz terminowanie tuneli L2TP i PPTP. Również od wersji 6 pojawiła się możliwość realizowania VLANów na PIXach (w standardzie 802.1Q, od modelu 515).

Więcej o PIXach znajdziesz pod adresem: <http://www.cisco.com/go/pix>.

Czy Cisco sprzedaje sprzęt do budowy sieci bezprzewodowych?

Tak, jest to seria produktów Cisco Aironet. Obecnie w sprzedaży znajdują się:

- Punkty dostępowe 1120. Są to urządzenia pracujące w standardzie 802.11b (P/N: AIR-AP1120B-E-K9), 802.11g kompatybilnym w dół z 802.11b (P/N: AIR-AP1121G-E-K9). W obu wersjach anteny zamontowane są wewnątrz urządzenia i nie ma możliwości dołączenia zewnętrznych. Do zakupionego AP serii 1120 ze starym radiem 802.11b, można dokupić nowe radio zgodne ze standardem 802.11g (P/N: AIR-MP21G-E-K9).
- Punkty dostępowe serii 1200. Wcześniejsza seria tych produktów (1220) posiadała system operacyjny oparty na platformie VxWorks. Na obecnie sprzedawanych AP (seria 1230) zainstalowany jest już zwykły Cisco IOS. Punkty dostępowe tej serii są dwusystemowe - posiadają dwa sloty na radia obu standardów: 802.11b lub 802.11g, oraz 802.11a. Do radia 802.11b lub 802.11g należy dokupić osobno anteny zewnętrzne, radio 802.11a posiada zamontowaną na stałe, zintegrowaną antenę.
- Punkty dostępowe serii 350. Starsza generacja sprzętu, kompatybilna tylko ze standardem

802.11b.

- Mosty bezprzewodowe 350. Starsza generacja sprzętu, kompatybilna tylko ze standardem 802.11b, umożliwia zestawianie połączeń punkt-punkt i punkt-wielopunkt.

Więcej o produktach bezprzewodowych możesz przeczytać pod adresem: <http://www.cisco.com/go/wireless>.

Rozdział 8. Jak skonfigurować router do...

...usługi transmisji danych w sieci Polpak-T?

Zakładając, że posiadasz kabel i wszystko odpowiednio podłączyłeś, poniżej gotowiec konfiguracji.

Przyjęto, że interesuje Cię podstawowa konfiguracja, bez dodatkowej funkcjonalności spotykanej tylko na niektórych routerach (firewall, IDS, wymyślne filtrowanie czy uwierzytelnianie).

Podsieć między Twoim routerem a routerem ISP to 169.254.1.0/30 (169.254.1.1 to adres routera ISP, 169.254.1.2 to adres Twojego routera), sieć LAN ma adresację 192.168.0.0/24, przy czym interfejs Ethernet Twojego routera ma adres 192.168.0.1 i jest dla tej sieci domyślną bramką.

Dodatkowo, sieć LAN wychodzi do Internetu z adresem publicznym routera (169.254.1.2), a interfejs Frame Relay ma DLCI równe 99.

```
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname rtr_cisco
!
enable password jakies_trudne_haslo
!
username user_1 password haslo_usera_1
ip subnet-zero
no ip source-route
no ip domain-lookup
ip tcp path-mtu-discovery
!
interface Ethernet0
 description Polaczenie dla sieci LAN
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
!
interface Serial0
 description Konfiguracja fizycznego interfejsu szeregowego
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
 description Polaczenie Polpak-T do Internetu 2Mbit
 ip address 169.254.1.2 255.255.255.252
 frame-relay interface-dlci 99 IETF
 ip nat outside
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0.1
no ip http server
!
ip nat inside source list 100 interface Serial 0.1 overload
!
```

```
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
access-list 100 deny ip any any
no cdp run
!
line con 0
  exec-timeout 5 0
  login local
line vty 0 4
  exec-timeout 5 0
  login local
!
end
```

...InternetDSL lub innego dostawcy oferującego styk Ethernet?

Zakładając, że posiadasz kabel i dwa interfejsy Ethernet/FastEthernet na routerze, oraz wszystko odpowiednio podłączyłeś, poniżej gotowiec konfiguracji.

UWAGA: możesz spiąć styk Ethernet dostawcy z interfejsem Ethernet/FastEthernet na swoim routerze pod warunkiem, że użyjesz kabla skrosowanego!

Przyjęto, że interesuje Cię podstawowa konfiguracja, bez dodatkowej funkcjonalności spotykanej tylko na niektórych routerach (firewall, IDS, wymyślne filtrowanie czy uwierzytelnianie).

Podsieć między Twoim routerem a routerem ISP to 169.254.1.0/30 (169.254.1.1 to adres routera ISP, 169.254.1.2 to adres Twojego routera), sieć LAN ma adresację 192.168.0.0/24, przy czym interfejs Ethernet Twojego routera ma adres 192.168.0.1 i jest dla tej sieci domyślną bramką.

Dodatkowo, sieć LAN wychodzi do Internetu z adresem publicznym routera (169.254.1.2).

```
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname rtr_cisco
!
enable password jakies_trudne_haslo
!
username user_1 password haslo_usera_1
ip subnet-zero
no ip source-route
no ip domain-lookup
ip tcp path-mtu-discovery
!
interface Ethernet0
  description Polaczenie dla sieci LAN
  ip address 192.168.0.1 255.255.255.0
  ip nat inside
!
interface Ethernet1
  description Polaczenie dla sieci Internet
  ip address 169.254.1.2 255.255.255.252
  ip nat outside
!
ip classless
ip route 0.0.0.0 0.0.0.0 169.254.1.1
no ip http server
!
ip nat inside source list 100 interface Ethernet 1 overload
!
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
```

```
access-list 100 deny ip any any
no cdp run
!
line con 0
  exec-timeout 5 0
  login local
line vty 0 4
  exec-timeout 5 0
  login local
!
end
```

...usługi SDI/CDI?

SDI/CDI można do routera Cisco podłączyć na dwa sposoby: do portu AUX routera (niepolecane, obciąża mocno procesor) lub do interfejs asynchronicznego.

Na mniejszych routerach (klasy 1700) port asynchroniczny znajduje się na karcie WIC-2A/S. Dodatkowo, ale tylko na platformie 1700, w tryb asynchroniczny można ustawić porty na karcie WIC-2T (lub jedyny port na karcie WIC-1T) - w konfiguracji interfejsu dodając polecenie `physical layer async`.

UWAGA: możesz spiąć styk Ethernet dostawcy z interfejsem Ethernet/FastEthernet na swoim routerze pod warunkiem, że użyjesz kabla skrosowanego!

Przyjęto, że interesuje Cię podstawowa konfiguracja, bez dodatkowej funkcjonalności spotykanej tylko na niektórych routerach (firewall, IDS, wymyślne filtrowanie czy uwierzytelnianie).

Zarówno w usłudze SDI jak i CDI router musi w ramach połączenia PPP uwierzytelnić się - login i hasło otrzymałeś od dostawcy. Sieć LAN ma adresację 192.168.0.0/24, przy czym interfejs Ethernet routera ma adres 192.168.0.1 i jest domyślną bramką dla sieci. Sieć LAN używa oczywiście w łączności z Internetem adresu publicznego przypisanego routerowi.

W poniższej konfiguracji zakładamy, że używasz karty WIC-1T lub pierwszego portu z karty WIC-2T.

```
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname rtr_cisco
!
enable password jakies_trudne_haslo
!
username user_1 password haslo_usera_1
ip subnet-zero
no ip source-route
no ip domain-lookup
ip tcp path-mtu-discovery
!
interface Ethernet0
  description Polaczenie dla sieci LAN
  ip address 192.168.0.1 255.255.255.0
  ip nat inside
!
interface Serial0
  description Polaczenie SDI
  physical-layer async
  ip address negotiated
  no ip directed-broadcast
  ip nat outside
  encapsulation ppp
  async mode dedicated
```

```

no cdp enable
ppp pap sent-username nazwa_uzytkownika_sdi password haslo_uzyt_sdi
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial 0
no ip http server
!
ip nat inside source list 100 interface Serial 0 overload
!
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
access-list 100 deny ip any any
no cdp run
!
line con 0
  exec-timeout 5 0
  login local
line vty 0 4
  exec-timeout 5 0
  login local
!
end

```

...usługi Neostrada+?

Zakładam, że chodzi o Neostradę zakończoną stykiem ADSL. Odpowiednie routery Cisco do takiej konfiguracji, to np. Cisco 837 - który ma zabudowane na stałe styk ADSL, lub Cisco 1700 czy 2600 z modułem WIC-1ADSL. Zakładając, że posiadasz kabel i wszystko odpowiednio podłączyłeś, poniżej gotowiec konfiguracji.

Przyjęto, że interesuje Cię podstawowa konfiguracja, bez dodatkowej funkcjonalności spotykanej tylko na niektórych routerach (firewall, IDS, wymyślne filtrowanie czy uwierzytelnianie).

Adres publiczny przydzielany jest dynamicznie przy każdym połączeniu, sieć LAN ma adresację 192.168.0.0/24, przy czym interfejs Ethernet Twojego routera ma adres 192.168.0.1 i jest dla tej sieci domyślną bramką.

Sieć LAN wychodzi do Internetu z dynamicznie przyznanym adresem IP.

```

no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname rtr_cisco
!
enable password jakies_trudne_haslo
!
username user_1 password haslo_usera_1
ip subnet-zero
no ip source-route
no ip domain-lookup
ip tcp path-mtu-discovery
!
ip dhcp excluded-address 192.168.0.1
!
ip dhcp pool CLIENT
  import all
  network 192.168.0.0 255.255.255.0
  default-router 192.168.0.1
  dns-server 194.204.159.1 194.204.152.34
  lease 0 2
!

```

```

interface Ethernet0
  description Polaczenie dla sieci LAN
  ip address 192.168.0.1 255.255.255.0
  ip nat inside
!
interface ATM0
  description Polaczenie ADSL do ISP
  no ip address
  no atm ilmi-keepalive
  pvc 0/35
    encapsulation aal5mux ppp dialer
    dialer pool-member 1
!
  dsl operating-mode auto
  hold-queue 224 in
!
interface Dialer0
  description Interfejs dzwoniacy
  ip address negotiated
  ip nat outside
  encapsulation ppp
  dialer pool 1
  dialer-group 1
  ppp chap hostname login@neostrada.pl
  ppp chap password 0 twoje_haslo_do_neo+
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer 0
no ip http server
!
ip nat inside source list 100 interface Dialer 0 overload
!
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
access-list 100 deny ip any any
no cdp run
!
line con 0
  exec-timeout 5 0
  login local
line vty 0 4
  exec-timeout 5 0
  login local
!
end

```

...do Neostrady+ ale dla routera Cisco 677?

Przyjęto, że interesuje Cię podstawowa konfiguracja, bez dodatkowej funkcjonalności spotykanej tylko na niektórych routerach (firewall, IDS, wymyślne filtrowanie czy uwierzytelnianie).

Adres publiczny przydzielany jest dynamicznie przy każdym połączeniu, sieć LAN ma adresację 192.168.0.0/24, przy czym interfejs Ethernet Twojego routera ma adres 192.168.0.1 i jest dla tej sieci domyślną bramką.

Sieć LAN wychodzi do Internetu z dynamicznie przyznanym adresem IP.

```

cbos> enable
cbos# set password enable haslo_do_enable
cbos# set password exec haslo_do_telnet
cbos# set web enabled
cbos# set telnet enabled
cbos# set int eth0 address 192.168.0.1
cbos# set int eth0 netmask 255.255.255.0

```

```

cbos# set ppp wan0-0 login username_neostrada
cbos# set ppp wan0-0 password haslo_neostrada
cbos# set ppp wan0-0 ipcp 0.0.0.0
cbos# set ppp restart enabled

cbos# set dhcp server enabled
cbos# set dhcp server pool 0 ip 192.168.0.11
cbos# set dhcp server pool 0 size 200
cbos# set dhcp server pool 0 netmask 255.255.255.0
cbos# set dhcp server pool 0 gateway 192.168.0.1
cbos# set dhcp server pool 0 dns 194.204.159.1
cbos# set dhcp server pool 0 sdns 194.204.152.34
cbos# set nat enabled

cbos# set int wan0-0 close
cbos# set int wan0-0 vpi 0
cbos# set int wan0-0 vci 35
cbos# set int wan0-0 open
cbos# set route default wan0-0

cbos# write

```

...połączenia kablami V.35 dwóch routerów Frame Relay?

Jeśli chcesz zasymulować połączenie Frame Relay, posiadając dwa routery z odpowiednimi interfejsami i okablowaniem - nic prostszego. Jeden z nich będzie emulował przełącznik Frame Relay, a drugi "zwykły" router.

Na routerze emulującym przełącznik interfejs szeregowy skonfiguruj w ten sposób:

```

!
frame-relay switching
!
interface Serial0
description Emulacja 2Mbit/s FR - strona przelacznika
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
clockrate 2000000
frame-relay lmi-type ansi
frame-relay intf-type dce
!
interface Serial0/1.1 point-to-point
description Emulacja 2Mbit/s FR - do routera FR
ip address 169.254.10.1 255.255.255.252
frame-relay interface-dlci 99

```

Parametr `clockrate 2000000` decyduje o taktowaniu łącza - w powyższym przykładzie są to 2Mbit/s.

Konfiguracja routera do niego podłączonego:

```

interface Serial0
description Polaczenie FR 2Mbit/s
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
frame-relay lmi-type ansi
!
interface Serial0/1.1 point-to-point
description Polaczenie FR 2Mbit/s - do ISP
ip address 169.254.10.2 255.255.255.252
frame-relay interface-dlci 99

```

...obsługi dwóch równoległych łączy od niezależnych ISP?

Jest to bardzo popularny scenariusz. Załóżmy, że posiadasz dwa łączy: jedno Frame Relay i jedno Ethernet. Do obu dostałeś adresy połączeniowe (styk Twój router-router ISP) oraz adresy do użycia w ramach NATu.

Pierwszy dostawca przydzielił Ci adres połączeniowy 169.254.10.2/30 (jego router ma dla Ciebie adres 169.254.10.1), oraz zakres adresów 172.16.10.1-172.16.10.14 (172.16.10.0/28).

Drugi dostawca przydzielił Ci adres połączeniowy 169.254.20.2/30 (jego router ma dla Ciebie adres 169.254.20.1), oraz zakres adresów 172.16.20.1-172.16.20.14 (172.16.20.0/28).

W swojej sieci LAN (192.168.0.0/24), chcesz pierwszą połowę sieci NATować na pierwsze łączy, a drugą połowę na drugie łączy.

Notatka: Niestety, stosując statyczny mechanizm routingu wg zasad (ang. *policy based routing*), nie masz możliwości automatycznego przeciwdziałania awarii łączy lub sieci ISP - tj. jeśli zawiedzie któreś z łączy, ruch generowany od jednej z połówek sieci LAN będzie po prostu odrzucany.

Poniżej konfiguracja przykładowa routera, uwzględniająca powyższe założenia:

```
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname rtr_cisco
!
enable password jakies_trudne_haslo
!
username user_1 password haslo_usera_1
ip subnet-zero
no ip source-route
no ip domain-lookup
ip tcp path-mtu-discovery
!
interface Ethernet0
description Polaczenie dla sieci LAN
ip address 192.168.0.1 255.255.255.0
ip nat inside
ip policy route-map ruch_z_lan
!
interface Ethernet1
description Lacze od ISP #1
ip address 169.254.10.2 255.255.255.252
ip nat outside
!
interface Serial0
description Lacze od ISP #2
no ip address
encapsulation frame-relay
frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
description Lacze do Internetu 2Mbit/s
ip address 169.254.20.2 255.255.255.252
frame-relay interface-dlci 99 IETF
ip nat outside
!
ip classless
ip route 0.0.0.0 0.0.0.0 169.254.10.1
no ip http server
```

```

!
ip nat pool ISP1 172.16.10.1 172.16.10.14 netmask 255.255.255.240
ip nat pool ISP2 172.16.20.1 172.16.20.14 netmask 255.255.255.240
!
ip nat inside source list 1polowkaLAN pool ISP1 overload
ip nat inside source list 2polowkaLAN pool ISP2 overload
!
ip access-list extended 1polowkaLAN
 permit ip 192.168.0.0 0.0.0.127 any
ip access-list extended 2polowkaLAN
 permit ip 192.168.0.128 0.0.0.127 any
!
route-map ruch_z_lan permit 10
 match ip address 2polowkaLAN
 set ip next-hop 169.254.20.1
!
no cdp run
!
line con 0
 exec-timeout 5 0
 login local
line vty 0 4
 exec-timeout 5 0
 login local
!
end

```

Jak to działa? Do interfejsu Ethernet0 dociera ruch z sieci LAN, adresowany do Internetu. Route-mapa `ruch_z_lan` sprawdza, czy pakiet nie pasuje do ACL `2polowkaLAN`. Jeśli pakiet pasuje, wpis w route-mapie mówi, że należy go wyroutować przez adres, dla którego następnym "hopem" będzie 169.254.20.1, czyli interfejs Serial0.1 (podsieć 169.254.20.0/30). Jeśli nie pasuje, route-mapa kończy testy i przekazuje pakiet do normalnego procesu routingu. W tabeli routingu znajduje się tylko jeden wpis statyczny - trasa wskazuje na pierwsze łącze:

```
ip route 0.0.0.0 0.0.0.0 169.254.10.1
```

Ponieważ w trakcie podróży, pakiet przechodzi pomiędzy interfejsem oznaczonym jako `ip nat inside` (interfejs Ethernet0) a jednym z dwóch interfejsów oznaczonych jako `ip nat outside` wykonywany jest NAT.

O kolejności sprawdzania na jaki zakres adresów zNATować pakiet, decyduje kolejność wpisów `ip nat inside [...]`. W naszej konfiguracji są dwa:

```
ip nat inside source list 1polowkaLAN pool ISP1 overload
ip nat inside source list 2polowkaLAN pool ISP2 overload
```

Wpisy te wprost mówią: pakiety z adresami źródłowymi pasującymi do ACL o nazwie `1polowkaLAN` mają zostać zNATowane na adresy z puli `ISP1`, a pakiety z adresami źródłowymi pasującymi do `2polowkaLAN` na pulę adresów `ISP2`.

Notatka: Warto zwrócić uwagę, że ruch można rozkładać nie tylko ze względu na adres/podsieć IP. Mógłbyś na przykład zechcieć kierować ruch dla typowych usług kierować na jedno łącze, a całą resztę na drugie - dzięki temu, użytkownicy popularnych aplikacji P2P, czy namiętni ściągacze wszystkiego co tylko można za pomocą FTP nie będą przeszkadzać czytającym pocztę.

Musisz zmienić ACLkę `2polowkaLAN`:

```
ip access-list extended 2polowkaLAN
 permit tcp 192.168.0.0 0.0.0.255 any eq 22
 permit tcp 192.168.0.0 0.0.0.255 any eq 23
```

```
permit tcp 192.168.0.0 0.0.0.255 any eq 25
permit udp 192.168.0.0 0.0.0.255 any eq 53
permit tcp 192.168.0.0 0.0.0.255 any eq 80
permit tcp 192.168.0.0 0.0.0.255 any eq 110
permit tcp 192.168.0.0 0.0.0.255 any eq 143
permit tcp 192.168.0.0 0.0.0.255 any eq 445
permit tcp 192.168.0.0 0.0.0.255 any eq 465
permit tcp 192.168.0.0 0.0.0.255 any eq 993
permit tcp 192.168.0.0 0.0.0.255 any eq 995
permit icmp 192.168.0.0 0.0.0.255 any
```

Teraz ruch do serwerów popularnych usług oraz ruch ICMP będzie wychodził łączem, na które wskazuje route-mapa `ruch_z_lan`, a całą resztę ruchu router skieruje tam gdzie wskazuje zwykły wpis w tablicy routingu.

A co jeśli mam więcej łącz - na przykład 3?

Musisz dodać kolejne wpisy w route-mapie, wskazujące dla jakiegoś unikalnego typu ruchu kolejne interfejsy.

A co z lokalnym ruchem do/z routera?

W zasadzie całą konfigurację routingu można wykonać za pomocą routingu wg zasad (bez statycznego wpisu w tablicy routingu dotyczącego trasy domyślnej), ale wtedy musisz dodatkowo określić politykę dla tzw. *ruchu lokalnego*, czyli ruchu do/z routera.

Poniżej taki przykład - do konfiguracji z przykładu powyżej dodajemy definicję route-mapy, która kieruje ruch lokalny na oba łącza w zależności od tego, ruchu do jakiego IP dotyczy. Innymi słowy, jeśli ktoś np. spinguje Twój drugi interfejs, pasować będzie dopiero drugi wpis w route-mapie (`RuchLokalny permit 20`) i dopiero on spowoduje skierowanie pakietu odpowiedzi drugim łączem.

```
ip local policy route-map RuchLokalny
!
! dodajemy route-mapę dla ruchu lokalnego - jeśli robisz to zdalnie,
! powyższą komendę dodaj NA KOŃCU!
!
route-map RuchLokalny permit 10
match ip address 100
set ip next-hop 169.254.10.1
! cały ruch pasujący do ACL 10 przerzucić na interfejs, dla którego następnym
! "hopem" jest 169.254.10.1 i zakończ sprawdzanie route-mapy
!
route-map RuchLokalny permit 20
match ip address 101
set ip next-hop 169.254.20.1
! jeśli tu doszedłeś, cały ruch pasujący do ACL 10 przerzucić na interfejs,
! dla którego następnym "hopem" jest 169.254.20.1
!
ip access-list extended 100
remark ACL pasuje do ruchu do puli łącza ISP #1
permit ip any 169.254.10.0 255.255.255.252
ip access-list extended 101
remark ACL pasuje do ruchu do puli łącza ISP #2
permit ip any 169.254.20.0 255.255.255.252
```

W tym momencie, możesz usunąć z routera wpis statyczny domyślnego routingu, wskazujący na pierwsze łącze.

....eksportu danych NetFlow?

Jeśli chcesz zbierać informacje o strumieniach danych przepływających przez router, możesz skorzystać z mechanizmu NetFlow i zewnętrznego systemu, który dane te przerobi i np. przedstawi graficznie.

Pamiętaj, że na większości małych platform eksport danych NetFlow powoduje znaczny wzrost obciążenia routera - przemyśl to zatem.

Z punktu widzenia routera należy wykonać następujące polecenia:

```
! Włączamy CEF:
router(config)# ip cef

! Konfigurujemy mechanizm NetFlow:

router(config)# ip flow-export version 5 peer-as
! używamy wersji 5 NetFlow, większość kolektorów obsługuje poprawnie
! tylko ten format

router(config)# ip flow-export source-interface FastEthernet 0/0
! wskazujemy interfejs najbliższy sieci w której znajduje się kolektor,
! najlepiej oczywiście gdyby był to interfejs bezpośrednio do tej sieci
! podłączony

router(config)# ip flow-export destination adres_IP port_docelowy
! wskazujemy adres IP kolektora i port docelowy, na którym będzie on nasłuchiwał

! Dla IOSów 12.2/12.3:
router(config)# ip flow-cache timeout active 1
! a dla IOSów 12.0/12.1:
router(config)# ip flow-cache active-timeout 1

! Na każdym interfejsie, z którego ruch ma wchodzić w skład
! zbieranych statystyk:
router(config-if)# ip route-cache flow
```

Więcej o mechanizmie NetFlow przeczytać możesz tutaj: <http://www.cisco.com/go/netflow>. Jeśli natomiast chcesz skonfigurować stację odbierającą informacje z routera, zajrzyj pod te adresy: <http://www.linuxgeek.org/netflow-howto.php> i http://www.ncne.org/training/techs/2002/0127/presentations/200201-fullmer1_files/v3_document.htm.

...routingu pomiędzy VLANami na kartach WIC-4ESW, NM-16ESW lub NM-32ESW?

Wspomniane karty są przełącznikami L2, ale dzięki możliwości stworzenia na routerze logicznych interfejsów VLAN, można stworzyć mapowanie warstwy drugiej (VLAN przypisany do portu) na warstwę trzecią (adres IP przypisany do logicznego interfejsu o numeracji zgodnej z numerem VLANu).

Oba rodzaje modułów wymagają oprogramowania IP Plus - o ile w routerach 1711 i 1712 w których skład wchodzi moduł WIC-4ESW oprogramowanie to znajduje się "w zestawie" o tyle do pozostałych routerów, na których moduły te są obsługiwane (WIC-4ESW dla 1721/1751/1760, oraz moduły NM-16ESW i NM-32ESW dla serii 2600, 3600 i 3700) należy to oprogramowanie dokupić.

Konfigurację należy rozpocząć od zdefiniowania w bazie danych VLANów konkretnych VLANów, które chcemy założyć. Zakładam, że naszym celem jest stworzenie dwóch VLANów - 10 i 20:

```
router# vlan database
router(vlan)# vlan 10 name Siec1
VLAN 10 added:
  Name: Siec1
router(vlan)# vlan 20 name Siec2
VLAN 20 added:
```

```
Name: Siec2
router(vlan)# exit
APPLY completed.
Exiting....
router#
```

Teraz należy fizyczne porty na przełączniku przypisać do jednego z tych dwóch VLANów - 10 lub 20. Zakładam, że pierwsze dwa porty przypisujemy do 10, a pozostałe dwa do 20:

```
router(config)# interface range FastEthernet 0/0 - 1
router(config-if-range)# switchport mode access
router(config-if-range)# switchport access vlan 10
router(config-if-range)# exit
router(config)# interface range FastEthernet 0/2 - 3
router(config-if-range)# switchport mode access
router(config-if-range)# switchport access vlan 20
```

Pozostaje stworzyć logiczne interfejsy VLAN10 i VLAN20, do których przypiszemy adresy IP (i które będą dla stacji w odpowiednich VLANach domyślnymi bramkami). Zakładam, że sieć VLAN10 ma adresację 192.168.10.0/24 przy czym .1 to adres routera, a VLAN20 ma adresację 192.168.20.0/24 przy czym .1 to adres routera.

```
router(config)# interface vlan 10
router(config-if)# ip address 192.168.10.1 255.255.255.0
router(config-if)# no shutdown
router(config)# interface vlan 20
router(config-if)# ip address 192.168.20.1 255.255.255.0
router(config-if)# no shutdown
```

Do tak stworzonych logicznych interfejsów VLAN x można przypisać oczywiście ACLki, inspecty, routemapy itp.

Rozdział 9. Routing

Mam na routerze dwa interfejsy z nadanymi adresami IP, ale router nie chce routować między nimi. O co chodzi?

Należy wydać polecenie `ip routing`.

Jak wskazać routerowi domyślną bramkę?

Dodając trasę w ten sposób:

```
router(config)# ip route 0.0.0.0 0.0.0.0 adres_bramki
lub
router(config)# ip route 0.0.0.0 0.0.0.0 nazwa_interfejsu_do_bramki
```

Innymi słowy, jeśli cały ruch ma trafiać pod adres 169.254.10.1, napisz:

```
router(config)# ip route 0.0.0.0 0.0.0.0 169.254.10.1
```

...a jeśli adres bramki jest zmienny (np. Neostroda+), wskaź interfejs odpowiedzialny za terminowanie

IP, czyli np.:

```
router(config)# ip route 0.0.0.0 0.0.0.0 Dialer 0
```

UWAGA! Jeśli wpis ma wskazywać na interfejs Ethernet, powinieneś podać adres IP bramki! Wpisanie nazwy interfejsu może nie zadziałać tak, jak chciałeś.

Na jednym routerze mam wiele różnych protokołów routingu. Informacje którego z nich, znajdują się w tablicy routingu?

Informacje podawane przez protokół, który ma najmniejszy dystans administracyjny (ang. *administrative distance*). Jest to miara "wiarygodności" danych, podawanych przez konkretny protokół routingu.

Poniżej lista rodzajów tras i ich dystansów administracyjnych - ta o najniższej wartości znajdzie się w tablicy routingu i będzie używana:

trasa połączona	0
trasa wpisana statycznie	1
trasa sumaryczna EIGRP	5
trasa pozyskana z eBGP	20
trasa pozyskana z internal EIGRP	90
trasa pozyskana z IGRP	100
trasa pozyskana z OSPF	110
trasa pozyskana z IS-IS	115
trasa pozyskana z RIP	120
trasa pozyskana z external EIGRP	170
trasa pozyskana z iBGP	200

Jak przebiega proces routingu na routerach Cisco? Co jest brane pod uwagę?

W procesie routingu uczestniczą trzy niezależne od siebie zagadnienia:

- Aktywne procesy routingu działające na routerze - np. BGP, EIGRP i OSPF.
- Zawartość tablicy routingu, która otrzymuje informacje od procesów routingu i udziela pewnych informacji procesowi fizycznie przekazującemu pakiety
- Proces przekazujący pakiety (ang. *forwarding process*), który na podstawie informacji z tablicy routingu podejmuje decyzje co i jak wysłać.

Generalnie obowiązuje zasada, że najdokładniejszy wpis w tablicy routingu zwycięża, tj. najdłuższy pasujący prefiks do danej sieci ma pierwszeństwo nad bardziej ogólnymi. Jeśli pakiet przeznaczony jest do hosta o adresie 10.1.10.5, a w tablicy routingu istnieją dwa wpisy: do sieci 10.1.10.0/24 i do sieci 10.0.0.0/16, użyty zostanie ten pierwszy.

Procesy routingu dostarczają tablicy routingu najlepszych tras, zachowując dla siebie trasy o gorszych metrykach - czyli miarach "wartości" danej trasy. Decyzja co wpisać do tablicy routingu, jeśli wiele procesów posiada trasę do jednej sieci, podejmuje się na podstawie dystansu administracyjnego (można go dla danego protokołu zmienić). W ramach tego samego protokołu routingu, w tablicy routingu mogą pojawić się równoległe trasy, jeśli wynika to wprost z konfiguracji, lub metryki tych tras są sobie równe (nie myl dystansu administracyjnego i metryk!)

Doskonały artykuł na ten temat znajduje się tutaj:
http://www.cisco.com/en/US/tech/tk365/tk207/technologies_tech_note09186a0080094823.shtml.

Co to jest trasa pływająca (ang. *floating route*)?

Tras pływających używa się do uruchamiania łącz zapasowych. Wykorzystują one zasadę działania tablicy routingu - tylko wpis o najlepszym dystansie administracyjnym znajdzie się w tablicy. Wpisy o gorszym dystansie czekają na zniknięcie lub unieważnienie lepszego wpisu.

Załóżmy, że posiadasz router z interfejsem szeregowym (Serial 0) i ISDN. Chciałbyś wykorzystywać łącze ISDN ale tylko wtedy, gdy trasa przez łącze szeregowe nie działa. Wystarczy, że zdefiniujesz dwa wpisy o bramce domyślnej - jeden wskazujący na interfejs szeregowy, a drugi na interfejs ISDN (Dialer), ale o znacznie gorszej metryce. Pamiętaj, że trasy statyczne mają domyślnie metrykę 1:

```
router(config)# ip route 0.0.0.0 0.0.0.0 Serial 0
router(config)# ip route 0.0.0.0 0.0.0.0 Dialer 1 200
```

Podczas normalnej pracy (interfejs szeregowy działa) w tablicy znajduje się tylko wpis wskazujący na interfejs *Serial 0*. Jeśli interfejs ten zmieni stan na *down*, wpis zostanie wycofany z tablicy routingu i router sprawdzi, czy do tej sieci nie prowadzi inny wpis - w naszym przypadku będzie taki, wskazujący na interfejs Dialer 1. Po pewnym czasie, interfejs szeregowy zapewne znowu się podniesie - router znowu sprawdzi tablicę routingu i zamieni wpis wskazujący na Dialer 1 na wpis wskazujący na Serial 0, ponieważ ten ostatni ma lepszą metrykę. Zwykle od tego momentu interfejs ISDN nie przenosi już ruchu i po upływie skonfigurowanego czasu bezczynności zostanie zamknięty.

Chcę rozkładać obciążenie pomiędzy trasy o równej metryce. Jak wygląda konfiguracja tego w IOSie?

Domyślnie, router instaluje w tablicy routingu do 4 tras o tej samej metryce - z wyjątkiem BGP (domyślnie 1) i tras statycznych (do sześciu). Jeśli chcesz to zmienić, w konfiguracji protokołu routingu wydaj polecenie ``maximum-paths X'`, gdzie *X* to liczba od 1 do 6:

```
! Dla OSPF:
router(config)# router ospf 10
router(config-router)# maximum-paths 6

! Dla EIGRP:
router(config)# router eigrp 10
router(config-router)# maximum-paths 6

! Dla BGP:
router(config)# router bgp 10
router(config-router)# maximum-paths 6
! dodatkowo dla iBGP:
router(config-router)# maximum-paths ibgp 6
```

Pamiętaj, że jeśli zmieniasz domyślne ustawienia musisz wiedzieć, co robisz.

Chcę rozkładać obciążenie pomiędzy trasy o równej metryce w proporcji 1:2 - jak to zrobić?

Dopisz odpowiednio więcej tras do tej samej sieci. W przykładzie poniżej preferujemy łącze przez Serial 1, Serial 0 obsługuje tylko 1/3 ruchu:

```
router(config)# ip route 0.0.0.0 0.0.0.0 Serial 1
router(config)# ip route 0.0.0.0 0.0.0.0 Serial 1
router(config)# ip route 0.0.0.0 0.0.0.0 Serial 0
```

Czym się różni protokół routingu typu link-state od distance-vector?

Protokoły routingu typu link-state (łącze-stan), czyli OSPF, NSLP, BGP i IS-IS, opierają swoje działanie o przesyłanie uaktualnień do tablic routingu. Informacje przesyłane są pomiędzy routerami które w jakiś sposób nawiązały ze sobą sąsiedztwo. Do określenia metryki używa się zwykle wielu złożonych czynników. Protokoły tego typu działają w oparciu o algorytmy SPF (ang. *Shortest Path First*), takie jak np. algorytm Dijkstry.

Protokoły routingu typu distance-vector (dystans-wektor) takie jak RIP, RTMP czy IGRP wymieniają się pełnymi tablicami routingu co określone odcinki czasu. Do obliczania metryki trasy używa się algorytmu Bellmana-Forda.

Protokół hybrydowy, EIGRP (firmowy Cisco), nazywany jest tak, ponieważ co prawda wylicza metryki tras podobnie do protokołu IGRP, ale utrzymuje sąsiedztwa i wysyła tylko uaktualnienia jak protokoły typu link-state.

W jaki sposób protokoły typu dystans-wektor zapobiegają tworzeniu pętli?

Protokoły routingu typu dystans-wektor, używają paru mechanizmów, zapobiegających wadliwemu interpretowaniu otrzymywanych informacji, lub wstrzymujących rozpowszechnianie pewnych informacji. Są to:

Mechanizm split-horizon (dosłownie podzielony horyzont)

Router rozgłasza na danym łączu tylko takie trasy, o których dowiedział się z rozgłoszeń z innych łącz. Zapobiega to sytuacji, w której router "A" po otrzymaniu z routera "B" informacji o trasie "X", rozgłosi ją z powrotem do routera "B" z większą metryką.

Mechanizm poison reverse (dosłownie zatrucie wsteczne)

Kiedy trasa do jakiegoś miejsca docelowego zostaje wycofana, z uwagi na awarię łącza, router rozgłasza taką trasę z nieskończoną metryką. Zapobiega to wybraniu trasy do wysłania pakietów przez mechanizm routingu.

Licznik hold-down (dosłownie wstrzymanie się)

Mechanizm split-horizon działa dobrze w sieciach, w których nie ma redundantnych połączeń. W sytuacji, w której routery połączone są dwoma równoległymi trasami, router "A" otrzymując od routera "B" trasę do miejsca "X" łączem pierwszym, może wysłać tą informację z powiększoną metryką łączem drugim.

Reguła hold-down mówi, że w przypadku gdy router otrzyma informacje, że trasa do danego miejsca została unieważniona (np. w wyniku awarii), router ignoruje przez czas określony w liczniku hold-down kolejne informacje o tej trasie. Aktualne ustawienie licznika hold-down można sprawdzić poleceniem ``show ip protocol``:

```
router# show ip protocol
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 3 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
```

Interfejsy loopback

Co to jest interfejs loopback? Gdzie fizycznie się znajduje?

Interfejsy loopback (tak, może być ich wiele), są wirtualnym tworem, bardzo wygodnym z paru powodów:

- Jeśli tylko router działa, znajdują się w stanie "podniesionym" - ma to diametralne znaczenie dla dużych sieci, w których stabilność tablic routingu ma znaczenie;
- Ponieważ można przypisać im adres IP i wszelkie czynności administracyjne, "podpiąć" pod ten adres (np. tak, by w pakietach Syslog, SSH, Telnet, SNMP, NTP itp. jako źródło pakietu figurował adres interfejsu loopback), łatwo kontrolować listy dostępu (jeden, stały adres IP do przepuszczenia, zamiast stale zmieniającego się adresu lub grupy adresów), zezwalające na ruch do i z nich, oraz łatwiej zarządzać siecią złożoną z większej liczby urządzeń (jeśli np. interfejsy loopback wszystkich interfejsów w danej sieci wybrano z jednej podsieci /24, łatwiej jest je po kolei zlokalizować);
- Przy wykorzystaniu interfejsu loopback z przypisanym adresem IP, wygodnie pracuje się z interfejsami unnumbered - router może mieć dziesięć interfejsów fizycznych, z których każdy wskazuje jako swój adres IP aktualny adres interfejsu loopback;

RIP

Co to jest RIP?

RIP jest starym i obecnie rzadko używanym w konstrukcji nowoczesnych sieci protokołem typu dystans-vektor. Nowsza wersja RIPA, wersja 2 (opisana w [RFC 1723](#)) różni się od starszej wersji (v1, [RFC 1058](#)) tym, że oprócz sieci przesyła jej maskę, co efektywnie oznacza, że RIP wspiera VLSM (ang. *Variable Length Subnet Masks*, czyli sieci z maskami różnych długości). RIP w wersji 2 wspiera również uwierzytelnianie, co pozwala zwiększyć bezpieczeństwo sieci, a także rozgłaszanie informacji routingowych za pomocą multicastów (na adres 224.0.0.9).

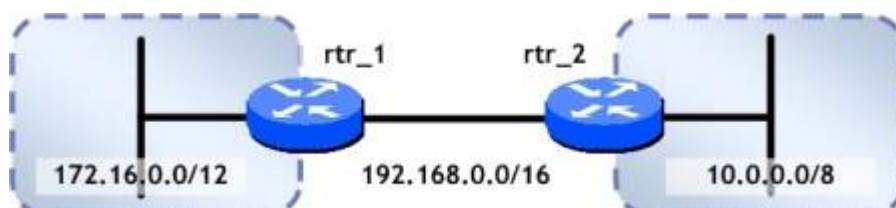
RIP rozsyła co 30 sekund na port 520/udp (v1, wersja druga używa multicastów dla normalnych rozgłoszeń i unicastów na port 520/udp dla uaktualnień wyzwolonych przez jakąś zmianę w sieci) całe tablice routingu do swoich sąsiadów. Jako jedynej metryki używa liczby przeskoków (hopów) do danej sieci. Ponieważ pole to ma maksymalną wartość 16, efektywnie obniża to skalowalność sieci do 15 hopów (gdzie 1 hop = sieć podłączona bezpośrednio, a 16 = sieć nieosiągalna). Podstawowym problemem w protokole RIP są zatem sytuacje, w których teoretycznie gorsza trasa (składająca się np. z 5 a nie z 2 hopów), jest bardziej niezawodna, ma większą przepustowość itp. - a RIP nie bierze tego pod uwagę.

Jak wygląda podstawowa konfiguracja RIPv1?

Standardowo, proces RIP zaczyna pracę po wydaniu w trybie konfiguracji polecenia:

```
router(config)# router rip
```

Samo polecenie nie zrobi jednak niczego atrakcyjnego - proces RIP wystartuje, ale nie będzie jeszcze zajmował się routingiem. Dopiero wskazanie sieci, którą ma zająć się RIP, powoduje rozpoczęcie pracy. Załóżmy, że mamy sieć składającą się z dwóch routerów, tak jak na rysunku poniżej:



Polecenie `network 172.16.0.0` wydane na routerze "rtr_1" spowoduje, że RIP rozpocznie przetwarzanie rozgłoszeń RIP na wewnętrznym interfejsie routera. Dopiero dodanie polecenia `network 192.168.0.0` spowoduje, że router "rtr_2" zacznie otrzymywać rozgłoszenia RIP od swojego sąsiada. Po dodaniu na routerze "rtr_2" analogicznej konfiguracji (do tego czasu "rtr_2" będzie otrzymywał rozgłoszenia, ale ignorował je), zobaczymy że routery "dowiedziały się" o istnieniu sieci podłączonych do interfejsów FastEthernet sąsiadów:

```
! Na routerze rtr_1:
rtr_1(config)# router rip
rtr_1(config)# network 172.16.0.0
rtr_1(config)# network 192.168.0.0

! Na routerze rtr_2:
rtr_2(config)# router rip
rtr_2(config)# network 10.0.0.0
rtr_2(config)# network 192.168.0.0
```

W głównej tablicy routingu, trasy poznane dzięki działaniu protokołu RIP oznaczone są literą "R":

```
rtr_1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       [...]
       P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 1 subnets
C       172.16.0.0 is directly connected, FastEthernet0
R       10.0.0.0/8 [120/1] via 192.168.0.254, 00:00:03, Serial0
C       192.168.0.0/16 is directly connected, Serial0
```

A jak uruchomić na routerze RIP w wersji 2?

Dodając do definicji procesu RIP polecenie `version 2`, np. tak:

```
router(config)# router rip
router(config)# version 2
router(config)# network 192.168.0.0
router(config)# network 169.254.10.0
```

OSPF

Co to jest OSPF?

OSPF (ang. *Open Shortest Path First*) jest protokołem dynamicznego routingu typu *link-state* i należy do kategorii IGP. Każdy router, w obrębie jednostek grupujących sieci zwanych areami (obszarami), posiada identyczną bazę stanu linków. Na bazie tych informacji tworzone jest drzewo najkrótszych ścieżek i wpisy do tablicy routingu. Podstawowymi cechami odróżniającymi go od protokołów typu distance-vector są:

- metryki/koszty przejścia pakietu przez dany link;
- oszczędność pasma - uaktualnienia wysyłane są na skutek zmiany stanu danego linku, a nie w formie okresowych rozgłoszeń;
- szybka konwergencja - zdolność do uzyskania stanu stabilnego po wykryciu zmiany w drzewie połączeń sieciowych;
- struktura hierarchiczna;

- wsparcie dla VLSM (subnetowania sieci);
 - możliwość uwierzytelniania sąsiadów (przyległych węzłów w rozumieniu sesji OSPF);
-

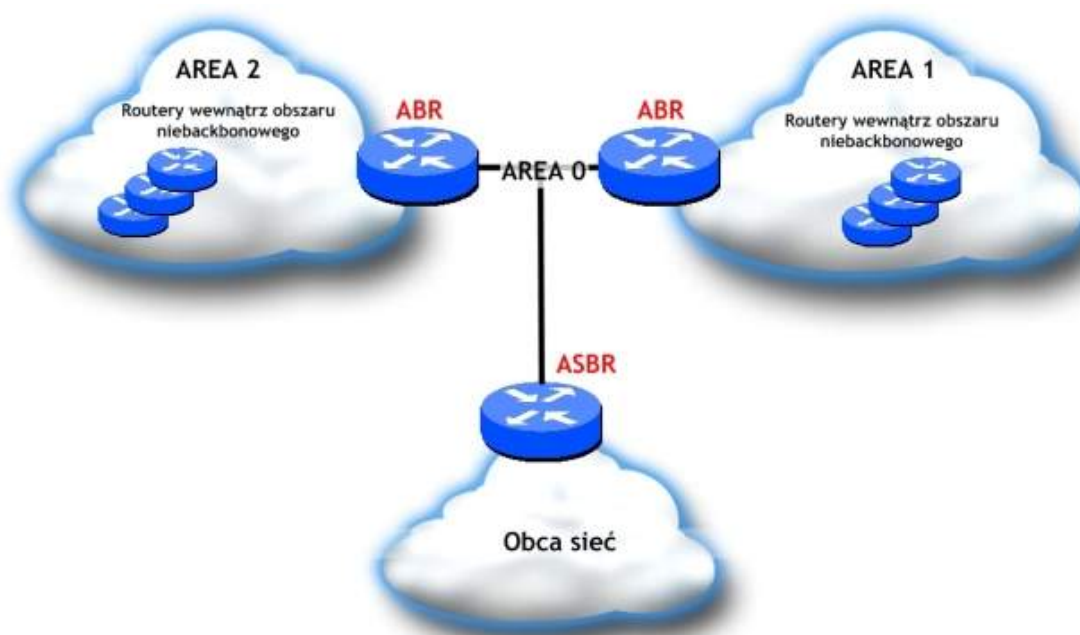
Jak działa OSPF?

Hierarchiczny model protokołu OSPF pozwala podzielić jedną wielką sieć korporacyjną na mniejsze segmenty zwane obszarami (ang. *area*). Obszar jest jakby samodzielną sekcją sieci, wewnątrz której odbywa się wymiana LSA (ang. *Link State Advertisement*, rozgłoszeń link-state), zakończona przeliczaniem ścieżek przy użyciu algorytmu SPF (ang. *Shortest Path First*). Podział sieci na obszary pozwala na ograniczenie rozmiaru tablic routingu na routerach - sieci z danego obszaru widziane są w innych obszarach tylko w postaci zsumaryzowanej. Innymi słowy, niestabilność jakiegoś linku wewnątrz obszaru nie przenosi się na zewnątrz.

Podział sieci na obszary spowodował również przypisanie różnych funkcji routerom w sieci z OSPF. Wyróżniamy zatem ich następujące typy:

- *internal router* - posiada wszystkie interfejsy w jednym obszarze. Jego zadania ograniczają się do ogłaszania LSA i utrzymywania aktualnych informacji w bazach danych.
- *backbone router* - OSPF zakłada istnienie specjalnego obszaru (nazywanego **area 0** bądź **backbone area**), który "spina" inne obszary ze sobą. Router pracujący w tym obszarze to właśnie backbone router.
- *Area Border Router (ABR)* - jest to router odpowiedzialny za łączenie dwóch lub większej ilości obszarów (jednym z nich musi być backbone area). Utrzymuje pełną topologiczną bazę o każdym obszarze, do którego jest podłączony i przesyła LSA między nimi. LSA zawierają zsumaryzowane informacje dotyczące sieci w danym obszarze.
- *Autonomous System Border Router (ASBR)* - aby wyjść poza swój system autonomiczny bądź wykorzystać informację pochodzącą z innego protokołu routingu (dynamicznego bądź statycznego) musisz opuścić domenę OSPFa. Router, na którym dochodzi do takiego przejścia z ospf na inny typ routingu (poprzez np. redystrybucję routingu statycznego) to właśnie ASBR. Funkcje ASBRa spełnia również router na którym jest dokonywana redystrybucja tras statycznych do ospfa.

Wizualnie, role poszczególnych routerów przedstawiają się następująco:



Jak router liczy w OSPFie metrykę dla połączenia?

W OSPFie metryka jest określana mianem kosztu. Domyślnie na routerach Cisco koszt jest odwrotnie proporcjonalny do pasma danego linku wg proporcji:

$$\text{Koszt} = \frac{100,000,000}{\text{pasma w bitach na sekundę}}$$

(dla pasma liczonego w kilobitach na sekundę, jak np. podaje się poleceniem `bandwidth X` przepustowość interfejsu dla protokołów routingu, wzór ten wygląda oczywiście $10^5/\text{pasma}$)

Innymi słowy, łącze E1 (2Mbit/s) wg OSPF będzie miało koszt 48, Ethernet 10Mbit/s 10, a jeden kanał 64Kbit/s ISDN BRI (kanał B) będzie miał koszt 1562.

O czym pamiętać przy sumaryzacji?

Należy pamiętać o następujących warunkach do spełnienia:

- sumaryzacji mogą dokonywać tylko ABRy i ASBRy;
- można sumaryzować do dowolnego rozmiaru podsieci (podsieć ma oczywiście rozmiar potęgi cyfry 2);
- sumaryzację należy skonfigurować ręcznie, uważnie rozplanowując sieć przy podziale na obszary;

Jakie są typy LSA?

Wyróżniamy 5 typów LSA:

- Router-link (LSA typ 1) - wszystkie linki, które posiada dany router wraz z lista wszystkich sąsiadów. Rozsyłany tylko wewnątrz obszaru.
- Network-link (LSA typ 2) - rozsyłana przez DR lista wszystkich routerów w danym segmencie, dla których służy jako DR i z którymi utrzymuje sąsiedztwo. Rozsyłany tylko wewnątrz obszaru.
- Summary link typu 3 - przesyłane między obszarami, sumaryzuje informacje o sieciach w danym obszarze. Tworzy je ABR.
- Summary link typu 4 - przesyłana między obszarami, zsumaryzowana informacja o sieciach pojawiających się w OSPFie wskutek redystrybucji. Tworzy je ASBR.
- External link (LSA typ 5) - informacje o redystrybuowanych sieciach. Rozsyłają je ASBRy. Wyróżniamy 2 podtypy:
 - Typ 1 - metryka jest sumą kosztu dojścia po OSPF i metryki zewnętrznego protokołu;
 - Typ 2 - metryka jest tylko kosztem zewnętrznego protokołu;
- NSSA external link (LSA typ 7) - typ specjalnie stworzony dla obszarów NSSA, przeznaczony do przenoszenia informacji o redystrybuowanych sieciach. Analogicznie jak LSA5 ma 2 typy. Tworzy je ASBR.

Co jest potrzebne żeby dwa routery wymieniły informacje o routingu OSPF?

Routery muszą być poprawnie skonfigurowane i zestawić ze sobą sąsiedztwo (ang. *adjacency*). Samo zestawienie sesji OSPF między routerami składa się z kilku etapów:

ustanowienie sąsiedztwa

Następuje wymiana pakietów OSPF Hello pomiędzy routerami przyłączonymi do jednego segmentu sieci (hello protocol). W pakietach hello routery umieszczają ID innych routerów od których usłyszały wcześniej hello w tym segmencie. Jeśli dany router zobaczy swój router ID w pakiecie hello od innego routera, uznaje, że ma już z nim ustanowioną przyległość (*adjacency*). Przyległość jest warunkiem koniecznym do wymiany baz danych swoich linków między routerami.

wybór DR i BDR

W środowiskach rozgłoszeniowych (broadcastowych) takich jak Ethernet, Token-Ring, i FDDI nie ma sensu, by każdy router wymieniał sesję OSPF z każdym routerem. Liczba takich sesji byłaby równa $n*(n-1)/2$, gdzie n jest liczbą węzłów w danym segmencie. Dla 10 routerów byłoby to 45 sesji. W zamian za to wybiera się spośród routerów w segmencie tzw. *Designated Router* (DR) oraz *Backup Designated Router* (BDR) i z nimi wszystkie routery zapinają sesje. W środowiskach nonbroadcast multiaccess (NBMA) tj. Frame Relay, DR i BDR muszą zostać specjalnie skonfigurowane. W połączeniach point-to-point wyznaczanie DR i BDR nie jest konieczne.

DR zajmuje się dystrybucją informacji routingowych uzyskanych od routerów danym segmencie. Gdy DR padnie, zastępuje go BDR, a nowy BDR jest wybierany z pozostałych routerów. Kryterium wyboru DR i BDR oparte jest o priorytet routera (najwyższy wygrywa). Domyślnie wszystkie routery mają priorytet 1 i wygrywa ten o najwyższym numerze router-id. Router-id to adres interfejsu loopback (wirtualny interfejs routera, który nigdy "nie pada") bądź najwyższy adres z innego typu interfejsów routera (jeśli nie ma loopbacka). Stosowanie interfejsów loopback na routerach korzystnie wpływa na wybór DR/BDR, a co za tym idzie stabilność sesji ospf. Warto jednak wymusić by DR i BDR były "najsilniejszymi" routerami w danym segmencie. Można tym sztucznieysterować ustawiając na interfejsie "silnego" routera stosunkowo wysoki priorytet (ustawienie go na zero powoduje, że dany router na pewno nie będzie DR/BDR).

wymiana informacji routingowych

Po ustanowieniu sąsiedztwa (i wybraniu DR/BDR dla segmentów wielodostępowych), routery z OSPFem są gotowe do wymiany informacji o sieciach, które wzajemnie posiadają. Informacje od stanach linków na danym routerze jest wymieniana poprzez tzw. *Link State Updates* (LSUs). LSU zawierają LSA, opisujące stan wszystkich linków bądź sieci, o których routery posiadają informacje. Wszystkie te LSA są przechowywane w link-state database, nazywanej czasem topological database. Ta link-state database jest perspektywą, z jakiej router widzi sieć. Wszystkie routery po zakończeniu procesu wymiany informacji powinny mieć identyczne link-state database (co nie oznacza, że takie same tablice routingu!).

Jak sprawdzić aktualny stan sąsiadów danego routera OSPF?

Tabela stanów OSPF można przejrzeć poleceniem ``show ip ospf neighbor'`.

Stan	Znaczenie
DOWN	Nie odpowiada na hello
ATTEMPT	Wysłane hello, ale jeszcze brak odpowiedzi
INIT	Usłyszane hello, ale jeszcze nie ma status sąsiada
TWO-WAY	Pełne sąsiedztwo. W takim stanie pozostają 2 routery w środowiskach multiaccess, gdy żaden z nich nie jest DR ani BDR
EXSTART/ EXCHANGE/ LOADING	Kolejne etapy mające na celu transfery bazy LSA między sąsiadami.
FULL	Stan pełnego zsynchronizowania baz LSA.
DR/ BDR/ DROTHER	Oznacza, że dany sąsiad jest DR bądź BDR bądź żadnym z nich.

Tak jak wskazała powyższa tabela stabilnymi stanami między sąsiadami są:

- dla środowisk multiaccess:

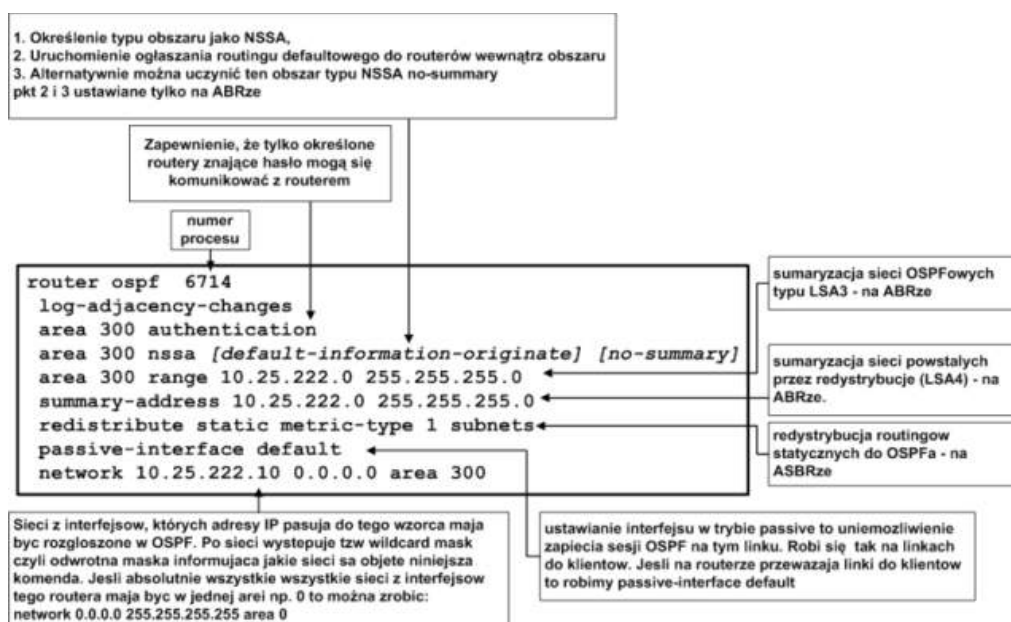
- FULL/DR lub FULL/BDR między routerem w segmencie a (B)DRem;
- 2WAY/DROTHER między 2 routerami niebędącymi DR ani BDR;
- dla środowisk point-to-point stan FULL

Jeśli w rezultacie komendy `show ip ospf neighbor` widzimy, że stan na jakimś podejrzanym interfejsie/linku odbiega od powyższych wskazań wtedy postępujemy wg wskazań z poniższej tabelki:

Utrzymujący się stan	Oznacza	Sprawdź....
DOWN	Nie ma odpowiedzi od żadnego sąsiada	...czy dany interfejs działa. Jeśli działa, to spróbuj wysłać: ping 224.0.0.6 powinni odpowiedzieć potencjalni sąsiedzi na linku
ATTEMPT	Wysłane HELLO, ale brak odpowiedzi	Sprawdź, czy dany sąsiad odpowiada, np. pingiem do niego
INIT	Wysłane i otrzymane HELLO, ale nie ustanowione sąsiedztwo	
2WAY/DR lub 2WAY/BDR	W środowiskach multiaccess normalne.	
2WAY	W środowiskach p-to-p oznacza problemy z rozpoczęciem transferu bazy topologicznej.	
EXSTART lub EXCHANGE lub LOADING	Transfer bazy topologicznej między sąsiadami nie może poprawnie dojść do skutku	...MTU (czy takie same) oraz link fizyczny. Wyślij większe (1550 bajtowe) pingi do sąsiada

Jak skonfigurować OSPF?

Poniższy schemat znacznie to ułatwia:



Czy jest jakiś przewodnik po budowaniu sieci z OSPFem?

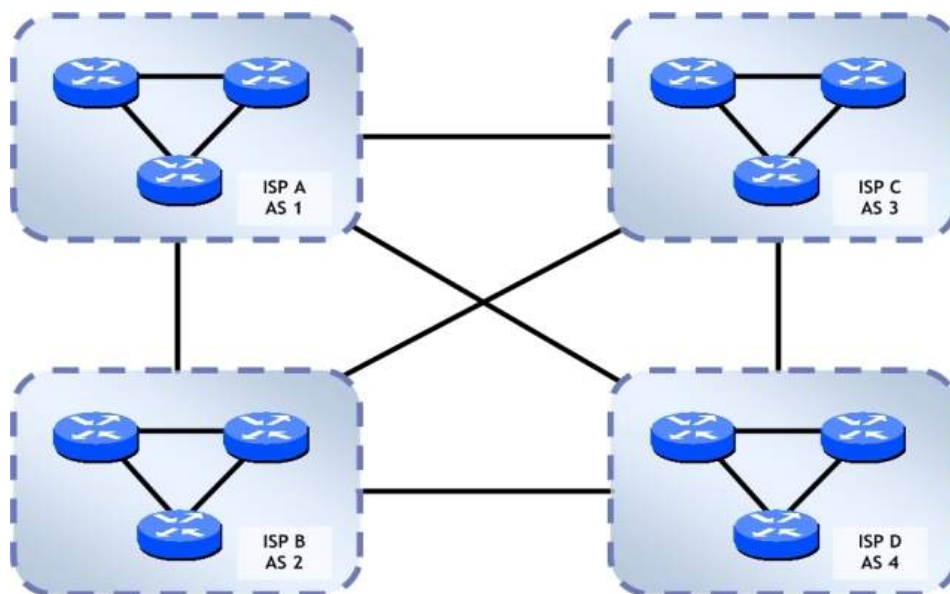
Cisco udostępniło swoje zalecenia co do budowania sieci wykorzystujących protokół OSPF. Jest on dostępny pod adresem http://www.cisco.com/en/US/tech/tk365/tk480/technologies_design_guide09186a0080094e9e.shtml, a PDF tego samego materiału pod adresem <http://www.cisco.com/warp/public/104/1.pdf>.

Routing BGP

Co to jest BGP?

Border Gateway Protocol jest protokołem typu external (zewnętrznym, choć może również pracować w konfiguracjach wewnętrznych), a służy głównie do komunikowania się routerów brzegowych różnych systemów autonomicznych. Wyróżnikiem systemu autonomicznego (AS) jest jego numer, przyznawany w Europie przez RIPE. Protokół BGP w wersji 4 posiada zaimplementowane mechanizmy ochrony przed zapętleniami pakietów i jest powszechnie stosowany dla zapewnienia komunikacji między sieciami dostawców internetu (ang. *Internet Service Providers*, ISP).

Komunikacja między routerami wymieniającymi wzajemnie tablice BGP (ang. *peer*, *neighbor*) oparta jest o protokół tcp, port 179. Routery należące do różnych AS'ów i wymieniające tablice BGP działają w ramach external BGP (EBGP).



Internet jako zbiór systemów autonomicznych wymieniających tablice BGP

Jak każdy protokół routujący, BGP zarządza tablicami routingu, wymienia informacje routingowe i opiera decyzje o routowaniu na metryce. Podstawową funkcją jest wymiana informacji o dostępności danej sieci zawierająca informacje o liście ścieżek ASów. Ta informacja może być wykorzystana do skonstruowania grafu dostępności systemu autonomicznego. W informacjach rozgłoszeniowych peerom BGP podsyłana jest tylko optymalna ścieżka do danej sieci.

Co to jest numer AS?

Każdy system autonomiczny musi posiadać swój unikalny identyfikator ASN (*Autonomic System Number*), nadawany przez odpowiednią organizację (w Europie jest to RIPE). Numer ten jest identyfikatorem wszystkich routerów BGP danego systemu. Powielenie numeru na zewnątrz grozi wyłączeniem dużych obszarów sieci ze względu na wewnętrzne zabezpieczenia protokołu przed zapętleniem. Do celów testowych można użyć prywatny numer AS z puli 64512-65535 - należy jednak

pamiętać, że nie wolno ogłasza takiego prywatnego ASa do swoich BGP peerów.

Jaki potrzebuję router do obsługi BGP?

Osobnym zagadnieniem ważnym przy uruchamianiu BGP jest wybór platformy sprzętowej do obsługi połączeń internetowych. Na chwilę obecną pełna tablica BGP to ponad 174 tysięcy wpisów (<http://www.cymru.com/BGP/robbgp01.html>) - na obróbkę takiej ilości, często zmieniających się danych, na dodatek otrzymanych od co najmniej 2 ISP potrzebny jest silny router z niemałą ilością pamięci. Zużycie zasobów możemy sprawdzić przez:

```
router_bgp# sh proc memory | inc Holding|BGP
PID TTY Allocated Freed Holding Getbufs Retbufs Process
 75 0 11856640 11855460 8008 0 0 BGP Open
121 0 971742788 51185912 85739960 4940 0 BGP Router
122 0 30531708 846392840 95900 14707036 2799936 BGP I/O
123 0 23816 4834392 32876 0 0 BGP Scanner
142 0 20688180 20687760 6968 0 0 BGP Open
149 0 15935988 14198940 6828 0 0 BGP Open
153 0 20680512 20675960 6976 0 0 BGP Open
```

..oraz:

```
router_bgp# sh proc cpu | exc 0.00% 0.00% 0.00%
CPU utilization for five seconds: 61%/31%; one minute: 36%; five minutes: 35%
PID Runtime (ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
 3 37272304 1981781 18807 0.00% 0.36% 0.42% 0 Check heaps
15 1331000 4103026 324 0.00% 0.03% 0.00% 0 ARP Input
22 744268 1573286 473 0.07% 0.02% 0.00% 0 Net Background
41 11547076 55980307 206 0.15% 0.07% 0.08% 0 IP Input
49 7493092 110337 67911 0.00% 0.09% 0.06% 0 IP Background
75 484 208 2326 0.76% 0.34% 0.09% 2 Virtual Exec
95 1549732 106200 14592 0.00% 0.02% 0.00% 0 Per-minute Jobs
112 3285676 20064138 163 0.00% 0.01% 0.00% 0 SNMP ENGINE
119 18127088 12981037 1396 0.07% 0.01% 0.10% 0 OSPF Router
121 18955580 34540455 548 0.07% 0.12% 0.12% 0 BGP Router
123 2648032 10310905 256 0.00% 0.01% 0.00% 0 BGP I/O
124 277728220 1697064 163655 29.08% 4.38% 3.70% 0 BGP Scanner
```

Powyższe statystyki zebrano na routerze 7200 z modułem NPE-300.

Generalnie, należy założyć, że 128MB pamięci to już dzisiaj za mało, żeby utrzymać pełne tablice i zapewnić jednocześnie sensowną funkcjonalność. Jako **minimum**, zalecamy zatem routery 3825/3845 (wydajność wg Cisco odpowiednio 225 i 500kpps) - można je rozbudować do 1GB RAMu i posiadają wydajność na dolnym pułapie sensownej obsługi 1-2 ISP. Oczywiście routery 3660 również można rozbudować do 256MB RAMu, ale od grudnia 2003r. routery te nie są już ani produkowane ani sprzedawane.

Powinieneś jednak *poważnie* rozważyć zakup routera klasy 7200 z modułem NPE-400 lub NPE-1G do obsługi "poważnego" BGP. (NPE-400 posiada wg Cisco wydajność do 400kpps, ale można je rozbudować do maksymalnie 512MB RAM, NPE-1G do 1GB RAM).

Jak właściwie działa BGP?

Pod kątem konwergencji BGP należy do jednych z wolniejszych protokołów routingu. Awaria połączenia wykrywana jest po ok. 1 minucie (chyba, że włączymy funkcję "**bgp fast-external-fallover**", ale nie jest to zalecane), nie może się zatem równać się z szybkimi protokołami IGP tj. OSPF czy EIGRP (tam awaria wykrywana jest po paru sekundach). Jednak takie spowolnienie reakcji może być dosyć korzystne w przypadku Internetu - zbyt szybka reakcja na chwilowe flapping (przejście ze stanu działania do awarii i po chwili z powrotem) linku mogłaby zachwiać stabilnością Internetu. Ponadto BGP znacznie lepiej się skaluje w internecie - użycie innego protokołu do internetu takiego jak OSPF spowodowałoby

natychmiastowe przeciążenie routera. Zaimplementowany mechanizm nie akceptowania od neighborów ścieżek zawierających własny numer ASa zabezpiecza przed zapętleniami.

Do badania dostępności neighborów BGP używane są pakiety Hello standardowo przesyłane co 60 sekund. Nie dotarcie trzeciego z kolei pakietu Hello implikuje "położenie" sesji BGP. Standardowo zatem pad połączenia, na którym zapięta jest sesja BGP, wykrywany jest po 3 minutach.

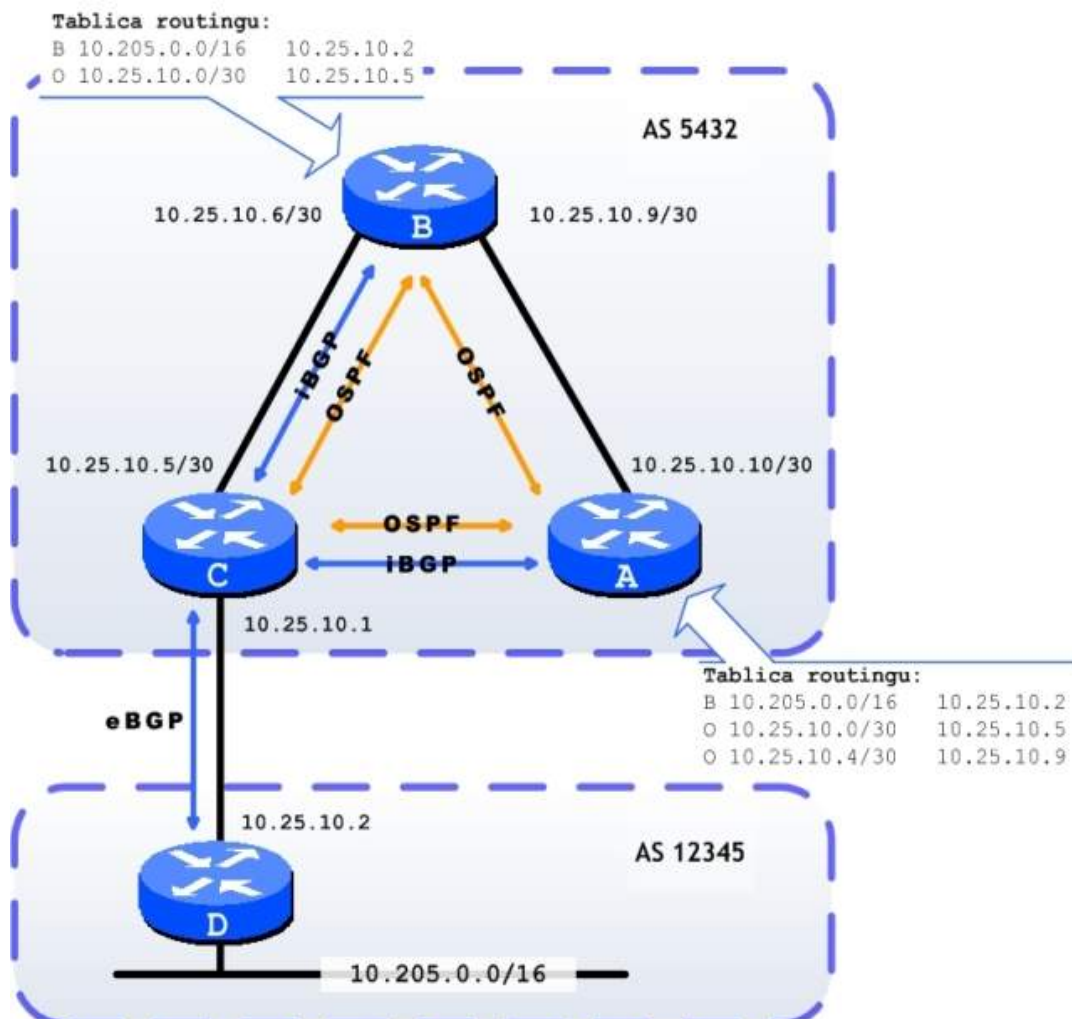
Jakich atrybutów używa BGP?

Ścieżka ASów

Jest listą numerów ASów, które update dotyczący danej sieci musiał przejść, by osiągnąć dany router. Numer AS jest dodawany na początku ścieżki w momencie przejścia przez dany system autonomiczny. Numery AS przedzielone są w ścieżce spacją.

Next hop

Jest adresem IP następnego kroku, który powinien być użyty celem dojścia do danej sieci. Uwaga: wpis w tablicy routingu w polu next hop może mieć adres IP gatewaya, do którego dany router nie jest przyłączony. Ważne, by inny wpis w tablicy routingu kierował na ten hop. Np. w poniższym przykładzie w tablicy routingu na routerach B i C znajduje się wpis kierujący do sieci 10.205.0.0/16 (informacja z BGP) na next hop o adresie 10.25.10.2. Żaden z tych 2 routerów nie jest bezpośrednio podpięty do gatewaya o tym adresie, ale w tablicy routingu znajduje się również informacja o tym, jak dojść do sieci 10.25.10.0/30 (uzyskana z OSPFa), dzięki temu pakiety do sieci 10.205.0.0 będą mogły swobodnie dojść.



Należy więc przy projektowaniu systemu autonomicznego pomyśleć o skonfigurowaniu zarówno protokołu BGP do komunikacji ze światem zewnętrznym oraz jakiegoś protokołu typu IGP np. OSPF wewnątrz samego systemu - od biedy funkcje IGP mogłyby przejąć iBGP, ale:

- jak wspomniano jest bardzo powolny w reagowaniu na awarie połączeń;
- na większości małych routerów Cisco (1000, 1600, 1700, 2500) BGP nie jest dostępne w standardowej wersji IOSa;
- jest protokołem typu distance-vector, nie biorącym pod uwagę parametrów technicznych linku takich jak jego przepustowość;

Waga (ang. *weight*) i local-preference

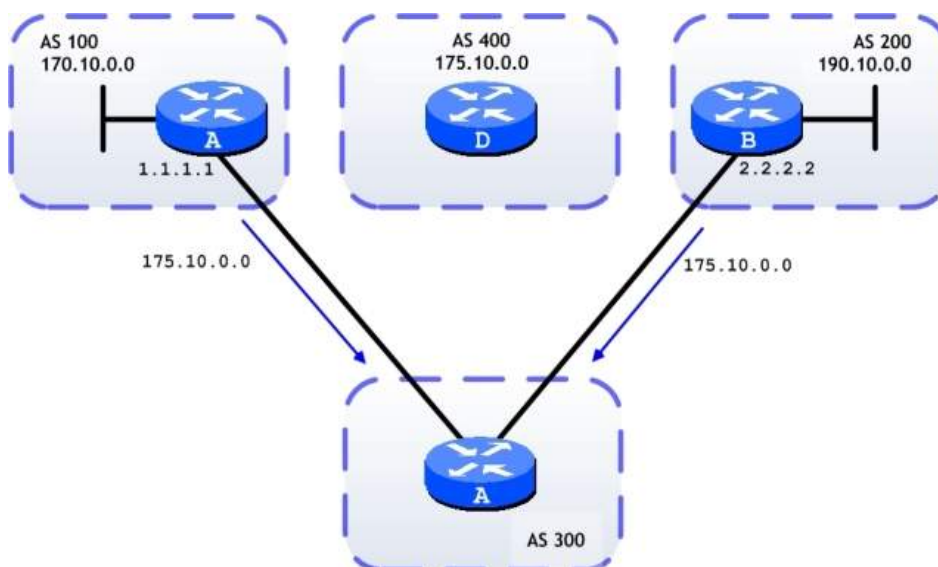
Gdy mamy dostępnych kilka ścieżek do jednego celu, musimy jakoś ustawić preferencję jednej nad drugą. Do tego służą właśnie parametry: *weight* i *local-preference*. Znaczenie ich jest podobne tzn. im wyższa waga lub *local-preference* dla danej ścieżki tym ścieżka jest bardziej pożądana. Różnica polega na tym, że:

- Parametr "*weight*" jest ważny tylko w obrębie danego routera, natomiast *local-preference* przenosi się w obrębie całego ASa (ale nie poza nim!),
- Wyższa waga ma pierwszeństwo nad wyższym *local-preference*.

Standardowe wartości to:

- Dla wagi, jeśli router jest tzw. originatorem danej sieci (ma ją w konfiguracji wpisaną ją komenda `network` bądź drogą redystrybucji) wtedy 32768, dla innych sieci zero;
- Dla *local-preference* jest to 100;

Oczywiście te wartości można modyfikować, np. dla wagi przy konfiguracji jak na rysunku poniżej:



...gdy z dwóch źródeł dostajemy tę samą sieć 175.10.0.0 możemy ustawić wyższą wagę dla jednego z kierunków na 3 sposoby:

- Przy użyciu ``ip as-path access-list``:

```
router bgp 300
```

```

neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 filter-list 5 weight 2000
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 filter-list 6 weight 1000
!
ip as-path access-list 5 permit ^100$
ip as-path access-list

```

- Przy użyciu route-map:

```

router bgp 300
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 route-map SETWEIGHTIN in
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 route-map SETWEIGHTIN in
!
ip as-path access-list 5 permit ^100$
!
route-map SETWEIGHTIN permit 10
match as-path 5
set weight 2000
route-map SETWEIGHTIN permit 20
set weight 1000

```

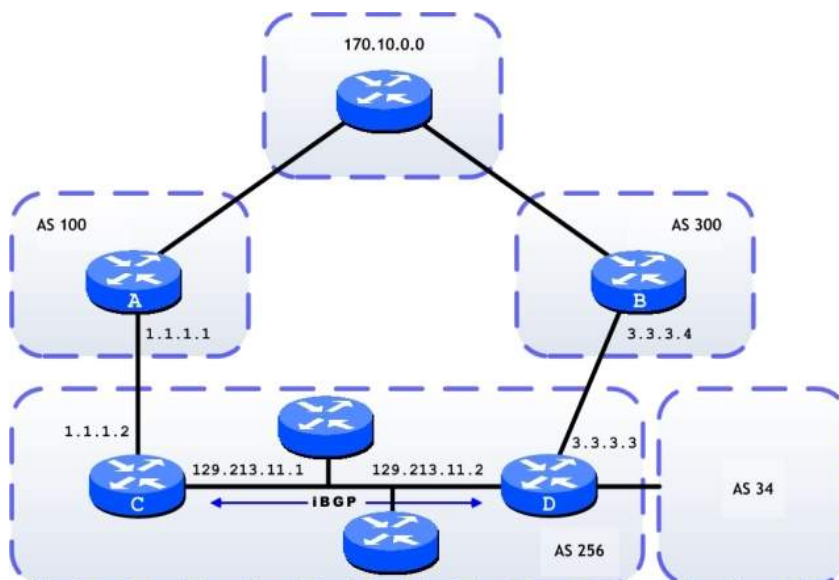
- Przy użyciu komendy `neighbor IP_sasiada weight waga`:

```

router bgp 300
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 weight 2000
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 weight 1000

```

Local-preference możemy natomiast zmodyfikować np. route-map:



```

! Na routerze D:
router bgp 256
neighbor 3.3.3.4 remote-as 300
route-map SETLOCALIN in
neighbor 128.213.11.1 remote-as 256

```

```

!
ip as-path 7 permit ^300$
!
route-map SETLOCALIN permit 10
  match as-path 7
  set local-preference 200
!
route-map SETLOCALIN permit 20
!

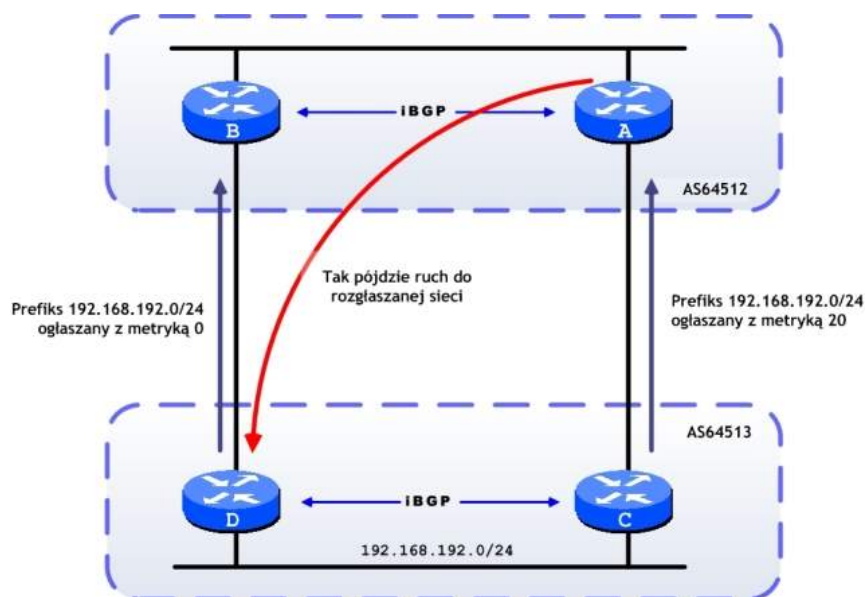
```

UWAGA: Należy zwrócić uwagę na pusta instancję route-map! W przypadku jej braku, wszystko, co nie pasowało do wzorca w poprzednich instancjach zostanie odrzucone.

Metryka

O ile weight i local-preference były parametrami pozwalającymi na ustawianie preferencji przychodzących prefiksów BGP (a co za tym idzie trasy dla pakietów danych wychodzących z naszego ASa do świata), o tyle do wpływania na trasę powrotną pakietów ze świat do nas musimy użyć innych mechanizmów. Pierwszym z nich jest metryka inaczej określana jako *multi-exit discriminator* (MED). W przeciwieństwie do local-preference, przenosi się ona poza AS, z tym, że nie dalej niż sąsiadujący AS. Jeśli nasz prefiks przesyłamy w dwóch kierunkach, ale w pierwszym z nich markujemy go metryką wyższą niż defaultowa (0), a w drugim nie ustawiamy jej (pozostawiamy zero), to spowodujemy, że pakiety powrócą do nas drugą z tras.

Poniższy przykład pokazuje rzeczywiste rozwiązanie jakie zaimplementowaliśmy na łączach do Ebone. W poniższym przykładzie, gdzie AS64513 ogłasza przez 2 różne sesje BGP do AS64512 ten sam prefiks, ale z różnymi metrykami: 0 i 20, ruch z AS64512 do sieci 192.168.192.0/24 pójdzie lewą ścieżką.



Standardowo dany AS porównuje metrykę dla tego samego prefiksu otrzymanego z 2 różnych sesji BGP, ale tylko, gdy obie sesje zapięte są między tymi samymi parami ASów. Dopiero włączenie komendy: ``bgp always-compare-med'` powoduje włączenie na danym routerze porównywania metryk w prefiksach otrzymanych z dwóch różnych źródeł. Niestety bardzo rzadko ISP włączają taką funkcję, więc ten mechanizm był dobry w powyższy przykładzie, ale niezbyt często jest przydatny.

Drugą metodą na wpływanie na drogę pakietów powrotnych do naszych sieci jest manipulacja długością ogłaszanej ścieżki poprzez sztuczne jej wydłużania tzw. *prepend*. Po prostu ogłaszamy jakąś ścieżkę dalej z naszym numerem ASa dodanym w niej więcej niż raz.

BGP community

Jest atrybutem służącym do markowania (tagowania) określonych prefiksów, celem określenia ich przynależności do jakiejś grupy prefiksów oraz późniejsze rozróżnianie po tym zamarkowaniu pośród innych prefixów. Zwyczajowo przyjęło się, że w danej organizacji community mają postać `<numer AS>:<numer community>` np. `8246:1`.

Znane są również powszechnie znane community służące określonym celom:

Community	Prefiksów oznaczonych tym community.....
No-export	... nie ogłaszaj do peerów eBGP
No-advertised	... nie ogłaszaj nikomu

Przykład konfiguracji:

```
router bgp 100
 neighbor 3.3.3.3 remote-as 300
 neighbor 3.3.3.3 send-community
 neighbor 3.3.3.3 route-map setcommunity out
 !
 route-map setcommunity
 match as-path 1
 set community 200 additive
 !
```

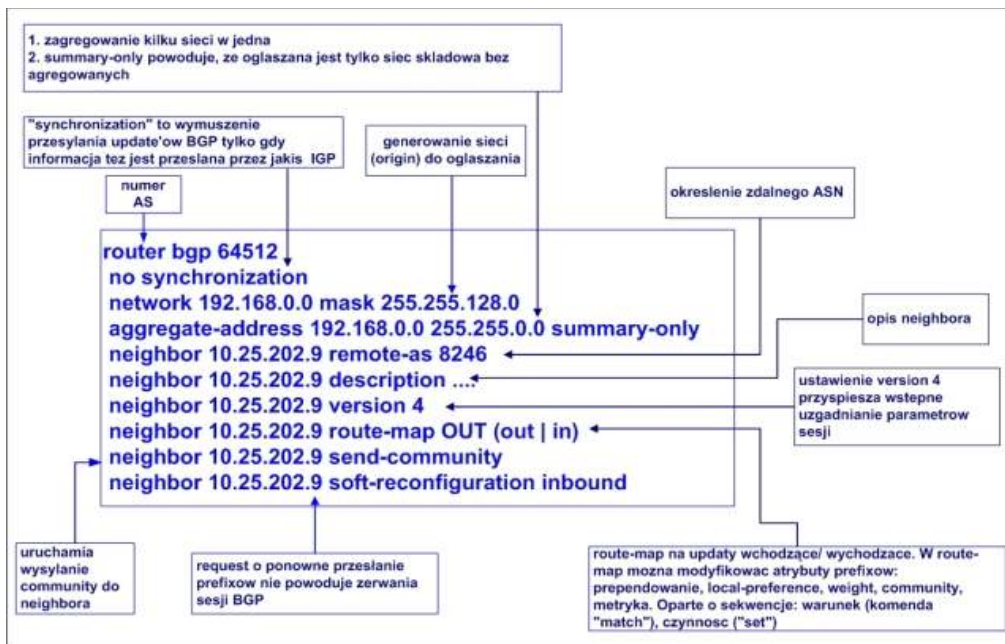
Jak w BGP wybierana jest ścieżka?

Algorytm wyboru ścieżki w BGP jest następujący:

- Jeśli ścieżka wskazuje next hop, do którego nie ma dojścia, update jest usuwany.
- Wybierana jest ścieżka z większą wagą.
- Jeśli wagi są takie same, wybierana jest z wyższym local-preference.
- Jeśli local-preference są takie same, wybierana jest ścieżka zdefiniowana generowana (origin) na danym routerze (komendą `network` lub droga redystrybucji).
- Następnie wybierana jest ta z krótszą ścieżką.
- IGP < EGP < incomplete
- Najniższy MED
- EBGP ponad IBGP
- Najniższy nexthop
- Najniższy Router-ID

Jak skonfigurować BGP?

Poniższy schemat znacznie to ułatwia:



UWAGA: standardowo włączona jest opcja `auto-summary`. Powoduje ona, że:

- Przy redystrybucji z np. RIPv2 do BGP, sieci pojawiają się w tablicy BGP z maską classful
- Wpisanie sieci komendą `network` nawet bez maski, powoduje, że ta sieć musi być obecna w RIB z dokładnością do długości prefixu

Chciałbym uruchomić BGP - skąd mam wziąć swój numer AS?

Po pierwsze, zastanów się czy BGP jest Ci na pewno potrzebne. **Nie potrzebujesz** BGP jeśli:

Masz pojedyncze połączenie do Internetu

Zastosuj po prostu domyślną trasę statyczną, wskazującą na router brzegowy Twojego ISP. To Twój ISP zadba, o rozgłoszenie informacji o osiągalności Twojej sieci (zakresu publicznych adresów IP) w Internecie.

Masz wiele połączeń, ale tylko do jednego ISP

Zwykle w takich sytuacjach chodzi o zapewnienie redundancji połączenia Twój ISP - Ty. Nadal to Twój ISP dba o widoczność publicznego zakresu adresów IP przypisanych do Twojej instalacji.

Nie masz odpowiedniego sprzętu do obsługi BGP.

W zależności od wybranego scenariusza BGP, będziesz potrzebował routera klasy 17xx/18xx/26xx/28xx (pobierasz tylko trasy domyślne i rozgłaszasz swoje IP), klasy 36xx/37xx/38xx (pobierasz część tras od jednego ISP i całą tablicę od drugiego ISP) oraz 37xx/38xx/7xxx (pobierasz od wszystkich ISP do których jesteś połączony pełne światowe tablice BGP).

Zawsze jednak skonsultuj się z kimś, kto ma praktykę w konfiguracji BGP - ważne będzie aktualne obciążenie Twojego routera i inne czynniki, które mogą wpłynąć na wybór scenariusza.

Formularz podania o własny numer AS dla RIPE znajduje się tutaj: <http://www.ripe.net/ripe/docs/asnrequestform.html>.

Co to jest PI i czym różni się od PA?

Pula adresowa PA, czyli *Provider Aggregatable* przyznawana jest lokalnym dostawcom (LIR, *Local Internet Registry*), do dalszego wykorzystania i podziału np. na pule adresowe dla użytkowników.

Pula adresowa PI, czyli *Provider Independent* (niezależna od dostawcy), jak sama nazwa wskazuje, oznacza przydział zakresu adresów dla konkretnego użytkownika końcowego. Oznacza to, że otrzymujesz własną, unikalną pulę adresów w Internecie, nie należącą do nikogo innego. Zwróć jednak uwagę, że jeśli będzie to pula z prefiksem /23 lub /24, mogą (nie muszą) pojawić się mniejsze lub większe problemy z osiągalnością Twojej sieci w Internecie (niektórzy ISP odrzucają informacje dokładniejsze niż /20, /21 czy /22 akceptując tylko "ogólniejsze" informacje).

Dokładniej różnice między PI a PA opisano w tym dokumencie: http://www.ripe.net/ripe/docs/ipv4-policies.html#pa_pi.

Formularz zamówienia na przestrzeń adresową PI dla RIPE znajduje się tutaj: <http://www.ripe.net/ripe/docs/pi-requestform.html>
a dla PA tutaj: <http://www.ripe.net/ripe/docs/iprequestform.html>.

Czy jest jakiś przewodnik po budowaniu sieci z BGP?

Przed konfiguracją BGP najlepiej dużo poczytać. Cisco stworzyło osobną sekcję swojej strony WWW poświęconom zagadnieniom związanym z BGP. Znajduje się ona pod adresem http://www.cisco.com/pcgi-bin/Support/browse/psp_view.pl?p=Technologies:BGP.

Bardzo dobry przewodnik po konfiguracji BGP z opisem konkretnych scenariuszy znajduje się pod adresem <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/icsbgp4.htm>, dokładny opis poleceń pod adresem http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a_00800d97fc.html, warto również zajrzeć do książki Sama Halabiego, do której link znajduje się na początku tego FAQ w rozdziale poświęconym dokumentacji.

Rozdział 10. QoS - limitowanie, gwarantowanie i kontrola pasma

Co tak naprawdę oznacza akronim QoS?

QoS to dokładnie akronim od *Quality of Service*, czyli *Jakość Usługi*.

Jest to bardzo popularne słowo-klucz stosowane (na nieszczęście), głównie w materiałach handlowych i oznacza zwykle tylko mały fragment całej rozległej dziedziny, zajmującej się gwarantowaniem jakości usług w sieciach.

Według Cisco, na możliwość zapewnienia QoS w sieci składa się:

- Klasyfikacja ruchu (ang. *Traffic Classification*) - chodzi o możliwość identyfikacji otrzymanego ruchu tak, by na tej podstawie można było później kształtować jego charakterystyki, czy gwarantować mu np. pierwszeństwo, lub stałe pasmo. W skład klasyfikacji ruchu na routerach Cisco wchodzi zagadnienia:
 - Routingu według zasad (ang. *policy-based routing*), czyli wprost wskazywania, że ruch o danej charakterystyce powinien być routowany w taki a nie inny sposób
 - Committed Access Rate
 - Class-Based Weighted Fair Queuing
- Zarządzanie zatorami (ang. *Congestion Management*) - próba ograniczenia wpływu niesfornych protokołów i aplikacji na pozostały ruch wymieniany w sieci. W skład wchodzi:
 - Weighted Fair Queuing

- Class-Based Weighted Fair Queuing
- Priority Queuing
- Custom Queuing
- Unikanie zatorów (ang. *Congestion Avoidance*) - próba proaktywnego zapobiegania wysyceniu łącza, lub wprost narzucanie polityki uniemożliwiającej danemu rodzajowi ruchu wysycenia całego dostępnego pasma.
 - Random Early Detection / Weighted Random Early Detection
 - Committed Access Rate

Jeśli chodzi o klasyfikację, często słyszę akronimy ToS, Precedence i DSCP - o co chodzi?

ToS, czyli *Type of Service* (Rodzaj Usługi) to standard definicji "klasy ruchowej" pakietu IP, opisany dokładniej w [RFC 1349](#). Definiuje sześć "typów" ruchu, i przypisuje każdemu z nich wartość, zapisywaną do bitów 3-6, w 1-bajtowym polu nagłówka pakietu IPv4. Pole *Precedence* to wartość z bitów 0-2 tego samego 1-bajtowego pola, określające "pierwszeństwo" danego ruchu.

DSCP, czyli *Differentiated Services Codepoint*, zdefiniowany w nowszym standardzie ([RFC 2474](#)), opisuje jak za pomocą tego samego, 1-bajtowego pola w nagłówku IPv4 podzielić ruch na klasy trochę inaczej - posługując się przy tym bitami 0-5, pozostałe dwa pozostawiając jako nieużywane.

Za pomocą odczytywania lub oznaczania pakietów pasujących do konkretnych kryteriów, routery i przełączniki są w stanie różnicować traktowanie ruchu w sieci. Zwykle zakłada się, że inteligentne urządzenia sieciowe (zwykle chodzi o przełączniki, ale czasami wykonują tą pracę również routery) znajdujące się najbliżej stacji użytkowników, serwerów, czy innych urządzeń generujących ruch, *oznaczają* różne rodzaje ruchu różnymi etykietami ToS/Precedence lub DSCP (wg przyjętego w danej sieci standardu; dobrze jest robić w taki sam sposób w całej sieci pod swoją kontrolą), a kolejne urządzenia "w łańcuszku" posługują się już tymi etykietami do priorytezyzacji ruchu, gwarantowania pasma czy jego ograniczania.

Jak skonfigurować...

...priorytezyzację określonego ruchu za pomocą PQ?

PQ, czyli *Priority Queueing* (kolejki z priorytetami) używa czterech kolejek i klasyfikowania ruchu do jednej z nich. Kolejki te nazywają się od posiadającej największy priorytet *high*, przez *medium*, *normal* do *low*.

Cechą charakterystyczną PQ jest fakt, że dopóki jakiegokolwiek pakietu znajdują się w kolejce o wyższym priorytecie, router nie wyśle pakietów oczekujących w kolejkach o priorytecie niższym. Łatwo doprowadzić w ten sposób do "umierania" transmisji, klasyfikowanych do kolejek o niższych priorytetach.

Założmy, że chcemy priorytezyzować cały ruch SSH, ICMP oraz Telnet. W kolejnej, mniej ważnej kolejce powinien znaleźć się ruch DNS, ISAKMP (500/udp) oraz ESP (protokół 50). Do trzeciej kolejki wrzucimy ruch WWW, SMTP, POP3, IMAP4 a cała reszta ruchu trafi do domyślnej, czwartej, najmniej uprzywilejowanej kolejki:

```
!  
interface serial 0.99  
  priority-group 10  
  ! do interfejsu szeregowego przypisujemy grupę priorytetów o  
  ! identyfikatorze 10  
  !  
  ! konfigurujemy wspomnianą grupę priorytetów:  
  priority-list 10 protocol ip high list 100
```

```

priority-list 10 protocol ip medium list 110
priority-list 10 protocol ip normal list 120
priority-list 10 default low
!
! access lista 100 - wybiera ruch SSH, ICMP oraz Telnet:
ip access-list extended 100
 permit tcp any any eq 22
 permit tcp any any eq 23
 permit icmp any any
!
! access lista 110 - wybiera ruch DNS, ISAKMP i ESP:
ip access-list extended 110
 permit udp any any eq 53
 permit udp any any eq 500
 permit esp any any
!
! access lista 120 - wybiera ruch WWW, SMTP, POP3, IMAP4:
ip access-list extended 120
 permit tcp any any eq 25
 permit tcp any any eq 80
 permit tcp any any eq 110
 permit tcp any any eq 143

```

...prioretyzację określonego ruchu za pomocą CQ?

CQ, czyli *Custom Queueing* (kolejkowanie konfigurowalne) jest mechanizmem podobnym do PQ, ale możemy po pierwsze używać do 16 kolejek, a po drugie opróżniane one są na zasadzie round-robin: najpierw X bajtów z kolejki pierwszej, później Y bajtów z kolejki drugiej i tak dla wszystkich kolejek i od początku. Taka konstrukcja zapobiega wymieraniu potoków mniej uprzywilejowanych.

Poniżej analogiczna konfiguracja, jak w przykładzie z PQ:

```

!
interface serial 0.99
 custom-queue-list 10
!
! konfigurujemy kolejkowanie, tworząc cztery kolejki: 1, 2, 3 i 4
queue-list 10 protocol ip 1 list 100
queue-list 10 protocol ip 2 list 110
queue-list 10 protocol ip 3 list 120
queue-list 10 default 4
!
! dla każdej z kolejek, określamy limity ruchowe w bajtach:
queue-list 1 queue 1 byte-count 3000
queue-list 1 queue 2 byte-count 2000
queue-list 1 queue 3 byte-count 1000
queue-list 1 queue 4 byte-count 500
!
! access lista 100 - wybiera ruch SSH, ICMP oraz Telnet:
ip access-list extended 100
 permit tcp any any eq 22
 permit tcp any any eq 23
 permit icmp any any
!
! access lista 110 - wybiera ruch DNS, ISAKMP i ESP:
ip access-list extended 110
 permit udp any any eq 53
 permit udp any any eq 500
 permit esp any any
!
! access lista 120 - wybiera ruch WWW, SMTP, POP3, IMAP4:
ip access-list extended 120
 permit tcp any any eq 25
 permit tcp any any eq 80

```

```
permit tcp any any eq 110
permit tcp any any eq 143
```

...kolejkowanie WFQ?

WFQ, czyli *Weighted Fair Queueing* (ważone, sprawiedliwe kolejkowanie) jest domyślnym mechanizmem kolejkowania, włączonym na interfejsach szeregowych o przepływności do 2Mbit/s. WFQ klasyfikuje ruch w potoki, przy czym do jednego potoku należą pakiety o takim samym źródłowym i docelowym adresie IP, portach TCP/UDP, należące do tego samego protokołu i posiadające tę samą wartość pola ToS (Type of Service).

Jeśli na interfejsie wyłączono WFQ, można je włączyć wydając polecenie `fair-queue`.

...przycinanie pasma dla określonego ruchu?

Cisco oferuje mechanizm CAR (*Committed Access Rate*) oraz GTS (*Generic Traffic Shape*). O ile CAR po prostu odrzuca pakiety przekraczające zadane wartości (i może działać zarówno dla ruchu wchodzącego jak i wychodzącego), GTS stara się delikatniej wpływać na przebieg transmisji, manewrując opóźnieniami pakietów, gdy pasmo zajmowane przez wskazany typ ruchu zbliża się do założonych ograniczeń. GTS działa tylko dla ruchu wychodzącego z routera.

Przycięcie ruchu FTP do 256kbit/s przez CAR:

```
interface Ethernet0
  rate-limit input access-group 100 256000 8192 8192 conform-action transmit exceed-
  action drop
  rate-limit output access-group 100 256000 8192 8192 conform-action transmit exceed-
  action drop
!
access-list 100 permit tcp any any eq ftp
access-list 100 permit tcp any eq ftp any
access-list 100 permit tcp any any eq ftp-data
access-list 100 permit tcp any eq ftp-data any
```

Przycięcie ruchu FTP do 256kbit/s przez GTS:

```
interface Ethernet0
  traffic-shape group 100 256000 8192 8192
!
access-list 100 permit tcp any any eq ftp
access-list 100 permit tcp any any eq ftp-data
```

...kształtowanie ruchu za pomocą CBWFQ?

CBWFQ, czyli *Class-Based WFQ* (WFQ oparte o klasy), jest potężnym mechanizmem, umożliwiającym łączenie wielu różnych innych mechanizmów w jedną całość na interfejsie routera.

Aby wykorzystać CBWFQ, należy najpierw wskazać, czyli inaczej sklasyfikować ruch, który będzie traktowany w różny sposób - innymi słowy, podzielić go na klasy. Cisco IOS daje wiele metod klasyfikacji - możemy wskazywać ogólnie protokoły (np. IP, EIGRP, ESP), dowolny ruch pasujący do jakiegoś rodzaju ACLek (np. tylko ruch do konkretnego hosta na port 80/tcp itp.), a także z wykorzystaniem mechanizmu NBAR, zagłębiać się w konstrukcję pakietu i np. wykrywać sieci P2P.

W poniższym przykładzie wyjdziemy z następujących założeń:

- Posiadamy symetryczne łącze 2Mbit/s
- Przede wszystkim interesuje nas ruch z wewnętrznych serwerów poczty i WWW - chcemy, by miały w ruchu wychodzącym gwarantowane do 1Mbit/s ruchu, przy czym jeśli "rozpedzą" się powyżej 1,2Mbit/s zaczynamy ten ruch shape'ować by nie wysycił nam zupełnie pasma w ruchu wychodzącym;
- Aplikacjom typu SSH czy Telnet dajemy osobne 256kbit/s starając się, by pakiety należące do tego ruchu utrzymywały możliwie małe opóźnienia. Podobnie jak dla powyższego ruchu, powyżej 384kbit/s zaczynamy ten ruch shape'ować.
- Statycznie przycinamy cały ruch UDP i ICMP do po 64kbit/s zarówno przychodzący jak i wychodzący. Nie spodziewamy się otrzymywać więcej ruchu tego typu w jednostce czasu, a na pewno nie będziemy również więcej generować (to w ograniczonym stopniu powstrzyma też trojany, które mogą zainstalować się na stacjach naszych użytkowników i próbować przeprowadzać ataki DDoS na innych użytkowników Internetu)
- Przycinamy wszelakie protokoły P2P które jesteśmy w stanie rozpoznać do minimalnej wartości - 16kbit/s. To nie zablokuje w całości ruchu i nie zagwarantuje, że ruch P2P nie wysyci naszego pasma od ISP do naszego routera (pojedynczy request z aplikacji P2P potrafi wygenerować wiele jednoczesnych strumieni które są w stanie zapchać naprawdę wielkie łącza), ale będzie naszym sposobem na kontrolę tego, co kontrolować trudno.
- Całą resztę ruchu kolejujemy wg WFQ w 64 osobne potoki.

```
class-map match-any cm_serwery
  match access-group name acl_serwery
  ! klasa cm_serwery wybiera tylko ruch pasujący do ACL acl_serwery
class-map match-any cm_ruch_gwarantowany
  match access-group name acl_ruch_gwarantowany
  ! klasa cm_ruch_gwarantowany wybiera tylko ruch pasujący do ACL
  ! acl_ruch_gwarantowany
class-map match-any cm_udp_icmp
  match access-group name acl_udp_icmp
  ! klasa cm_udp_icmp wybiera tylko ruch pasujący do ACL acl_udp_icmp
class-map match-any P2Ptraffic
  match protocol kazaa2
  match protocol http url "\.hash="
  match protocol gnutella
  match protocol napster
  match protocol fasttrack
  match protocol bittorrent
  ! wykorzystujemy tutaj funkcjonalność NBAR; umożliwia ona routerowi
  ! zagłębienie do wnętrza przesyłanych danych i analizę ich
  ! przynależności do różnego rodzaju aplikacji
!
policy-map pm_lan2internet
  class cm_serwery
    bandwidth 1016
    ! ruch zaliczony do klasy cm_serwery ma gwarantowane
    ! pasmo do 1Mbit/s, przy czym
    shape average 1256000 32768 32768
    ! jeśli zajmie 1,25Mbit/s zaczyna być shape'owany
  class cm_ruch_gwarantowany
    bandwidth 256
    ! ruch zaliczony do klasy cm_ruch_gwarantowany ma gwarantowane
    ! pasmo do 256kbit/s, przy czym
    shape average 384000 32768 32768
    ! jeśli zajmie 384kbit/s zaczyna być shape'owany
  class cm_udp_icmp
    police 256000 conform-action transmit exceed-action drop
    ! ruch zaliczony do klasy cm_udp_icmp jest odrzucany jeśli
    ! przekracza 256kbit/s
  class P2Ptraffic
    police 16384 conform-action transmit exceed-action drop
    ! ruch zaliczony do klasy P2Ptraffic powinien zostać
```

```

! przycięty do 16kbit/s, z uwagi na mechanizmy działania
! aplikacji tego typu trudno spodziewać się jednak że
! to ograniczenie będzie działało zawsze idealnie do
! zadanej przepustowości
class class-default
fair-queue 64
! pozostały ruch, który nie trafił do żadnej z klas powyżej
! rozkładany jest do 64 niezależnych kolejek
!
ip access-list extended acl_serwery
permit tcp host 192.168.10.10 eq 25 any
permit udp host 192.168.10.10 eq 53 any
permit tcp host 192.168.10.11 eq 80 any
permit tcp host 192.168.10.10 eq 110 any
permit tcp host 192.168.10.10 eq 143 any
!
ip access-list extended acl_ruch_gwarantowany
permit tcp any any eq 22
permit tcp any any eq 23
!
ip access-list extended acl_udp_icmp
permit icmp any any
permit udp any any

```

Oczywiście, tak stworzoną konfigurację należy przypisać jeszcze do interfejsu:

```

!
interface Serial 0.99
description Polaczenie WAN
service-policy output pm_lan2internet
!
interface FastEthernet 0
description Polaczenie LAN
ip nbar protocol-discovery

```

Co to jest NBAR?

NBAR, czyli *Network-Based Application Recognition*, to mechanizm "wykrywania" na podstawie oglądania zawartości pakietów, do jakiej aplikacji lub usługi danych ruch należy.

NBAR pojawił się w IOSie 12.0(5)XE2 i jest dostępny w podstawowej wersji oprogramowania (nawet na małych platformach). Aby go użyć, musisz zdefiniować na interfejsie politykę (service policy), która w ramach class-map sprawdzających kryteria przynależności ruchu do klas zawiera sprawdzanie protokołu poleceniem `match protocol [...]`. W przykładzie powyżej użyto funkcjonalności NBAR do wykrycia protokołów takich jak Bittorrent, Kazaa1/2 itp.

Przykładowe statystyki udostępniane przez polecenie `show ip nbar protocol-discovery` poniżej:

```

router# show ip nbar protocol-discovery

Serial0/0.99

Protocol                               Input                               Output
Packet Count                            Packet Count
Byte Count                               Byte Count
5 minute bit rate (bps)                 5 minute bit rate (bps)
-----
kazaa2                                   386586                              338412
Pierwsza linijka to odpowiednio ilość pakietów wchodzących
i wychodzących, które sklasyfikowano jako należące do danego protokołu

                                   403005080                            121530825
Kolejna linijka to ten sam podział na ruch wchodzący i

```

```

wychodzący, ale wyrażony w bajtach
                    567000                    380000
Ostatnia linijka to aktualne statystyki za ostatnie
5 minut pracy, w bitach na sekundę
http                393493                    205820
                    322833938                103136747
                    123000                    122000
ssh                 263541                    158289
                    391470822                9749154
                    220000                    10000
[...]

```

Więcej o obsługiwanych standardach i idei działania przeczytać można tutaj: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800c75d1.html#54116, a konfigurację opisano np. tutaj: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800c75d0.html#80560.

Rozdział 11. Bezpieczeństwo

Poszukuje informacji o zabezpieczaniu routerów, przełączników...

Bardzo wiele informacji znajduje się na stronach Cisco:

<http://www.cisco.com/go/safe>

Cała strona poświęcona zabezpieczaniu sieci opartych o sprzęt Cisco. Zawiera dokumenty z serii SAFE, nieocenione źródło wiedzy jeśli chodzi zarówno o kompleksowe podejście teoretyczne, jak i praktyczne do budowy bezpiecznej sieci.

<http://www.cisco.com/warp/public/707/21.html>

Improving Security on Cisco Routers

Dokument zawierający podstawowe wskazówki dotyczące zwiększania bezpieczeństwa routerów.

<http://www.cisco.com/warp/public/707/index.shtml>

Cisco's Security Technical Tips

Strona z serią porad dotyczących bezpieczeństwa.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/sec_vcg.htm

Cisco IOS Security Configuration Guide, Release 12.3

Podręcznik do najnowszej obecnie wersji IOS (12.3), opisujący wszystkie zagadnienia związane z bezpieczeństwem i podstawy ich konfiguracji.

<http://www.cisco.com/go/autosecure>

Cisco AutoSecure

Opis dostępnego od wersji 12.3 mechanizmu AutoSecure, ułatwiającego zabezpieczenie routera.

Dodatkowo, ciekawe materiały znaleźć można na innych stronach:

[NSA Security Recommendation Guides](#)

Dokumenty opisujące rekomendowane przez NSA (*National Security Agency*, Agencję Bezpieczeństwa Narodowego USA) konfiguracje routerów Cisco. Rewelacyjna lektura.

[Building Bastion Routers Using Cisco IOS](#)

Publikacja w ramach ezinu Phrack, którego nikomu chyba nie trzeba przedstawiać. Dotyczy starszych wersji IOSów, ale przedstawia metodyczne podejście do zabezpieczania routera i jego otoczenia.

[Dokumenty Roba Thomasa](#)

Strona zawierająca m.in. stale aktualizowaną listę sieci, które nie powinny pojawić się w Internecie (tzw. "Bogons List"), oraz rozmaite wzorce konfiguracji i zalecenia dla optymalizacji. Doskonała referencja, warto często zaglądać.

[Qorbit Safe templates](#)

Strona z wzorcami konfiguracji różnych urządzeń pod konkretne zastosowania - może okazać się przydatna.

[Black Hat briefings](#)

Jak nietrudno zgadnąć, zbiór prezentacji ze zlotów konferencji ludzi zajmujących się bezpieczeństwem.

[Hardening Cisco Routers step-by-step](#)

Dokument stworzony w ramach certyfikacji SANS. Warto przeczytać, wiedza zebrana z paru źródeł i skompilowana.

Dostęp do routera

Jak spowodować, żebym logując się do routera musiał podać tylko hasło?

Najprościej jest ustawić na wirtualnych liniach terminali (ang. *VTY*, *Virtual Teletypes*), wymuszenie podania konkretnego hasła:

```
router(config)# line vty 0 15
router(config-line)# login
router(config-line)# password jakieś_hasło
```

Jak spowodować, żebym logując się do routera musiał podać zarówno login jak i hasło?

Jeśli router ma sprawdzać istnienie konta o danym loginie i poprawność hasła bez zewnętrznej bazy danych, należy skonfigurować użytkowników lokalnie, np. tak:

```
router(config)# username lukasz password ala10
```

Następnie, należy włączyć lokalne uwierzytelnianie:

```
router(config)# aaa new-model
router(config)# aaa authentication login default local
```

...i skonfigurować wirtualne linie terminali tak, by wymagały uwierzytelnienia się, w oparciu o lokalną bazę użytkowników:

```
router(config)# line vty 0 15
router(config-line)# login local
```

W jaki sposób stworzyć stałe mapowanie IP na MAC na routerze?

Najczęściej potrzeba przypisania adresu IP do MAC karty sieciowej wynika z chęci zablokowania użytkownikom, możliwości samowolnej zmiany adresu IP. W Cisco istnieje możliwość przypisania adresu MAC do adresu IP poleceniem:

```
router(config)# arp 192.168.5.5 aaaa.bbbb.cccc arpa

! I sprawdzenie lokalnej bazy ARP:

router# show arp
Protocol Address           Age (min)  Hardware Addr  Type   Interface
Internet 192.168.5.1             -          000c.0c93.115a  ARPA   Ethernet0
Internet 192.168.5.5             -          aaaa.bbbb.cccc  ARPA
```

Jednak przypisanie takie dotyczy tylko mapowania IP -> MAC, ale nie na odwrót. Jeśli komputerowi o adresie MAC aaaa.bbbb.cccc użytkownik przypisze inny adres IP, będzie on mógł komunikować się z siecią. Natomiast przypisanie adresu IP 192.168.5.5 komputerowi o adresie MAC innym niż zdefiniowany uniemożliwi komunikację, gdyż wszystkie ramki przesyłane do adresu 192.168.5.5 zostaną skierowane na MAC adres aaaa.bbbb.cccc.

Jeśli zatem zrobimy statyczne mapowania IP->MAC wszystkim użytkownikom, a resztę adresów IP zablokujemy odpowiednią access-listą to uzyskamy zamierzony efekt - nikt nie będzie mógł zmienić adresu IP w taki sposób, aby nadal mógł komunikować się z siecią.

Chciałbym upewnić się, że mój router nie jest łatwym celem dla włamywaczy. Co jako podstawę polecacie?

W zasadzie najlepiej najpierw dużo poczytać. Większość zaleceń sprowadza się jednak do: a) wyłączyć niepotrzebne usługi, b) upewnij się, że routerowi nic nie przeszkadza.

Poniżej lista podstawowych poleceń, które warto wykonać. Jednak **UWAGA**: po pierwsze możesz coś zepsuć(!), po drugie takie pójście na skróty powinno być dopiero *początkiem* do dalszej dogłębnej analizy konfiguracji!

W konfiguracji globalnej wykonaj:

```
router(config)# no service udp-small-servers
router(config)# no service tcp-small-servers
router(config)# no service finger
router(config)# no service dhcp
router(config)# no service config
router(config)# no service pad
router(config)# no ip domain-lookup
router(config)# no ip finger
router(config)# no ip http server
router(config)# no ip http secure-server
router(config)# no ip bootp server
```

```

router(config)# no ip source-route
router(config)# no snmp-server
router(config)# no cdp run
! teraz trochę rzeczy włączymy:
router(config)# ip cef
router(config)# service tcp-keepalives-in
router(config)# service tcp-keepalives-out
router(config)# service password-encryption
router(config)# ip tcp path-mtu-discovery
router(config)# ip tcp selective-ack
router(config)# ip tcp timestamp
router(config)# service timestamps debug datetime localtime msec
router(config)# service timestamps log datetime localtime msec
router(config)# logging buffered 64000
! ustaw zegar i strefę czasową
router# clock set HH:MM:SS DD MIE ROK
router(config)# clock timezone MST 1
router(config)# clock summer-time MET recurring last Sun Mar 2:00 last Sun Oct 3:00
! usuń hasło enable szyfrowane słabym algorytmem:
router(config)# no enable password
! ...i ustaw hasło enable kodowane jednostronną funkcją mieszającą
router(config)# enable secret jakieś_trudne_hasło

```

W konfiguracji poszczególnych (pod)interfejsów:

```

router(config-if)# no ip redirects
router(config-if)# no ip directed-broadcast
router(config-if)# no ip mask-reply
router(config-if)# no ip proxy-arp
router(config-if)# ip verify unicast reverse-path

```

Na koniec zapisz konfigurację:

```

router# copy running-config startup-config

```

Zabezpieczanie ruchu do i przez router

Jak działają ACL?

ACL, czyli *Access Control List* (lista kontroli dostępu) jest listą reguł, które kolejno sprawdzają pewne właściwości pakietu. ACL używane są głównie do filtrowania pakietów na interfejsach routerów i przełączników, ale służą też do wskazywania ruchu route-mapom, crypto-mapom itd. Pamiętaj, że każdą stworzoną ACLkę musisz przypisać do jakiegoś interfejsu, lub do konkretnej funkcjonalności - inaczej po prostu nie będzie działać!

Dla ruchu IP interesujące są dwa typy list ACL - standardowe i rozszerzone. Standardowa lista IP pozwala sprawdzić tylko adres źródłowy pakietu, np.:

```

ip access-list standard 10
 permit host 192.168.0.10
 ! Pozwalamy przejść pakietom z 192.168.0.10

```

Każda zdefiniowana ACLka zawiera domyślnie na końcu wpis odrzucający każdy ruch (*default deny*), jeśli więc skonstruujesz swoją ACLkę tak, by najpierw odrzucała jakiś konkretny ruch, a później chciałbyś żeby przepuszczała pozostały, musisz go wprost przepuścić, np. tak:

```

ip access-list standard 10

```

```
deny host 192.168.0.10
! blokujemy wprost ruch z 192.168.0.10
deny host 192.168.0.11
! blokujemy wprost ruch z 192.168.0.11
deny host 192.168.0.33
! blokujemy wprost ruch z 192.168.0.33
deny host 192.168.0.91
! blokujemy wprost ruch z 192.168.0.91
deny host 192.168.0.206
! blokujemy wprost ruch z 192.168.0.206
permit any
! przepuszczamy pozostały ruch IP
```

Stworzenie standardowej listy ACL odbywa się przez nadanie jej identyfikatora od 1 do 99 (oraz od IOSu 12.0, z dodatkowego zakresu 1300-1999).

Rozszerzone ACL dostępne są w dwóch rodzajach - numerowane, w zakresie od 100 do 199 (od IOS 12.0 również 2000-2699), oraz nazwane. Termin *rozszerzone* oznacza, że pozwalają one sprawdzać ze szczegółami pewne standardowe pola pakietów (IP oraz w warstwie czwartej, czyli porty TCP/UDP oraz rodzaje i typy ICMP).

Założmy, że chcemy zablokować ruch do naszego routera o adresie 169.254.10.1 na port 80. Możemy napisać:

```
ip access-list extended 100
deny tcp any host 169.254.10.1 eq 80
! ruch pakietów zawierających TCP z dowolnej lokalizacji
! (any) do hosta o adresie 169.254.10.1 na port docelowy 80
! ma zostać zablokowany
permit ip any any
! przepuszczamy pozostały ruch IP
```

Warto zwrócić na skrócony zapis - rozszerzone listy dostępu wymagają użycia adresu źródłowego i docelowego, jako pary adres i maska. Zamiast takiej konstrukcji można użyć słów **any** (odpowiada konstrukcji 0.0.0.0 0.0.0.0, czyli dowolny adres), oraz **host A.B.C.D** (co odpowiada konstrukcji A.B.C.D 255.255.255.255, czyli tylko ten konkretny jeden adres).

Rozszerzone ACL oferują pewne dodatkowe testy - podstawowe, dostępne w praktycznie wszystkich IOSach począwszy od 12.0 to między innymi:

Dla protokołów TCP i UDP dostępne są słowa kluczowe sprawdzające port:

eq X

port źródłowy lub docelowy równy X, w zależności od miejsca umieszczenia warunku

gt X

port źródłowy lub docelowy większy niż X, w zależności od miejsca umieszczenia warunku

lt X

port źródłowy lub docelowy mniejszy niż X, w zależności od miejsca umieszczenia warunku

range X Y

zakres portów źródłowych lub docelowych od X do Y, w zależności od miejsca umieszczenia warunku

Natomiast dla TCP możemy jeszcze dodatkowo wskazać flagi ustawione w pakiecie:

syn

Ustawiona flaga SYN, początek normalnego połączenia, np.:

```
!  
ip access-list extended Internet2Serwer  
  permit tcp any gt 1023 host 169.254.10.1 eq 25 syn  
!
```

ack

Ustawiona flaga ACK - większość pakietów w strumieniu TCP.

established

Specjalne słowo kluczowe, pasuje do pakietów, z ustawioną flagą ACK, ale zgaszoną flagą SYN, RST lub FIN. Innymi słowy, chodzi o pakiety należące do zestawionych połączeń.

rst

Ustawiona flaga Reset - zwykle koniec połączenia.

Stworzoną ACL należy przypisać do interfejsu. Obowiązuje reguła, że do jednego interfejsu można przypisać dwie ACLki - jedną kontrolującą ruch wejściowy i jedną kontrolującą ruch wyjściowy (z routera, bądź przechodzący przez router i wychodzący tym akurat interfejsem).

```
interface serial 0.99  
  ip access-group 100 in  
  ! ruch wchodzący interfejsem będzie sprawdzany wg ACLki 100  
  ip access-group 110 out  
  ! ruch wychodzący interfejsem będzie sprawdzany wg ACLki 110
```

Jak mogę sprawdzić, czy moje ACL działają?

Sprawdź, czy router odnotował jakieś trafienia (*hits*) w poszczególne reguły ACLki poleceniem ``show ip access-lists``:

```
router# show ip access-lists  
  
Extended IP access list KillWinTraffic  
 10 deny udp any any range 135 netbios-ss (241919 matches)  
 20 deny tcp any any range 135 139  
 30 deny tcp any range 135 139 any  
 40 deny udp any range 135 netbios-ss any  
 50 deny tcp any any eq 445 (7614819 matches)  
 60 deny tcp any eq 445 any  
 70 permit ip any any (281099 matches)
```

Zwróć uwagę na liczby w nawiasach w regułach 10, 50 i 70. Jest to ilość pakietów, która pasowała do danej reguły i router albo je odrzucił (reguły 10 i 50), albo przepuścił dalej (reguła 70).

Jak zoptymalizować ACLkę?

Nie jest to pytanie proste, ale spróbujmy na nie zgrubnie odpowiedzieć.

Na początek warto wiedzieć, że ACLki z dodanym słowem kluczowym *log* (czyli logujące trafienie), powodują przejście procesora routera w tryb *process switching*. Dla dużego ruchu, korzyści z

wykorzystania innych optymalizacji, w tym optymalniejszych ścieżek komutacji, zostają w tym momencie zniweczone.

Po pierwsze, dla długich ACLek (od 6 wpisów i więcej), w niektórych IOSach (od 12.0(6) linii S, oraz od 12.3 dla niektórych routerów mniejszych) istnieje możliwość pre-kompilowania reguł w kod optymalniejszy do testowania na każdym pakiecie. Funkcjonalność ta nazywa się *Turbo Access List* (Cisco używa jej zamiennie z *compiled Access List* i jako takie pojawiają się w słowach kluczowych konfiguracji routera) i włącza się ją poleceniem ``access-list compiled'`. Router wykona w tym momencie proces optymalizacji ACLek dłuższych niż 5 reguł, a później przy każdej zmianie w ACLkach, powtórzy ten proces. Skuteczność działania tej funkcji, oraz listę ACLek które zostały skompilowane można sprawdzić poleceniem ``show access-lists compiled'`:

```
router# show access-lists compiled
Compiled ACL statistics:
ACL      State      Entries  Config  Fragment  Redundant
10       Operational  1        1        0          0
98       Operational  1        1        0          0
99       Operational  7        7        0          0
100      Operational  2        2        0          0
110      Operational  14       12       2          0
antispoof Operational  42       43       0          1
block_mswin Operational  14       14       0          0
nachi_worm Operational  3        2        1          0
8 ACLs, 8 active, 1 builds, 89 entries, 3 mem fill, 762 updates
  L0: 1805Kb  5/6    42/43  11/12  2/3    2/3    13/14  14/15  4/5
  L1:   9Kb   67/250 11/36  13/42  15/75
  L2:  55Kb   69/350 105/300
  L3: 217Kb  337/500
Misc:  30Kb
Totl: 2119Kb 710 equivs (617 dynamic)
```

Należy pamiętać, że wykorzystanie tej funkcjonalności pochłonie trochę pamięci (w zależności od ilości i wielkości istniejących i tworzonych list), jednak w zamian za to, każdy pakiet zostanie sprawdzony najwyżej pięć razy (dla list rozszerzonych) - adres źródłowy, adres docelowy, protokół, opcje protokołu - i wynik, powodujący przejście do przetwarzania następnego pakietu. Funkcjonalność tą opisano szerzej pod <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s6/turboacl.htm>.

Po drugie, staraj się ograniczyć liczbę reguł, zawierając w poszczególnych warunkach jak najogólniejsze stwierdzenia (jeśli nie powoduje to oczywiście przepuszczania niechcianego ruchu). Innymi słowy, na przykład zamiast wpisać ACLkę z 254 wpisami typu `permit ip 192.168.0.1, permit ip 192.168.0.2, permit ip 192.168.0.3` zastosuj jeden wpis w ramach listy rozszerzonej, który będzie brzmiał `permit ip 192.168.0.0 0.0.0.255 any`.

Po trzecie, przemyśl konstrukcję ACLki starając się ocenić, jaki ruch najczęściej będzie docierał do Twojego routera - i jak najwcześniej w liście reguł akceptuj go lub odrzucaj. Pomocne jest w tym momencie polecenie ``show ip access-lists'`. Przeanalizujmy taką ACLkę:

```
10 permit ip host 169.254.10.1 host 169.254.9.4
20 permit gre any host 169.254.20.6
30 permit udp host 150.254.183.15 eq ntp host 169.254.9.4 eq ntp (11460
matches)
40 deny ip 192.168.0.0 0.0.255.255 any (9865451 matches)
50 deny ip 173.0.0.0 0.255.255.255 any (124 matches)
60 deny ip 10.0.0.0 0.255.255.255 any
70 deny ip 172.16.0.0 0.15.255.255 any (42 matches)
80 deny ip 0.0.0.0 1.255.255.255 any
90 deny ip 2.0.0.0 0.255.255.255 any
100 deny ip 5.0.0.0 0.255.255.255 any
110 deny ip 7.0.0.0 0.255.255.255 any
120 deny ip 23.0.0.0 0.255.255.255 any (847618 matches)
130 deny ip 27.0.0.0 0.255.255.255 any
140 deny ip 31.0.0.0 0.255.255.255 any
150 deny ip 36.0.0.0 1.255.255.255 any
160 deny ip 39.0.0.0 0.255.255.255 any
```

```

170 deny ip 41.0.0.0 0.255.255.255 any
180 deny ip 42.0.0.0 0.255.255.255 any
190 deny ip 49.0.0.0 0.255.255.255 any
200 deny ip 50.0.0.0 0.255.255.255 any
210 deny ip 58.0.0.0 1.255.255.255 any (749 matches)
220 deny ip 70.0.0.0 1.255.255.255 any
230 deny ip 72.0.0.0 7.255.255.255 any (6 matches)
250 deny ip 88.0.0.0 7.255.255.255 any
260 deny ip 169.254.0.0 0.0.255.255 any
270 deny ip 174.0.0.0 1.255.255.255 any
280 deny ip 176.0.0.0 7.255.255.255 any
290 deny ip 184.0.0.0 3.255.255.255 any
300 deny ip 189.0.0.0 0.255.255.255 any
310 deny ip 190.0.0.0 0.255.255.255 any
320 deny ip 192.0.2.0 0.0.0.255 any
330 deny ip 197.0.0.0 0.255.255.255 any
340 deny ip 198.18.0.0 0.1.255.255 any
350 deny ip 223.0.0.0 0.255.255.255 any
360 deny tcp any any range 135 139 (138750 matches)
370 deny ip 96.0.0.0 31.255.255.255 any (6974 matches)
380 deny udp any any range 135 netbios-ss (79235152 matches)
390 deny tcp any range 135 139 any (8371 matches)
400 deny udp any range 135 netbios-ss any

```

Widać od razu, że reguła pasująca do zdecydowanie największej ilości pakietów (nr. 380, 79,235,152 trafienia) znajduje się na szarym końcu - jest sprawdzana dopiero 38. Powoduje to niewielkie, ale jednak opóźnienia i oczywiście przyczyna się do zwiększonego obciążenia na routerze (pamiętaj, że ACLka przeglądana jest za każdym razem, gdy do interfejsu dotrze, lub ma go opuścić pakiet!). Porządkując listę według trafień otrzymamy coś takiego:

```

10 deny udp any any range 135 netbios-ss (79235152 matches)
20 deny ip 192.168.0.0 0.0.255.255 any (9865451 matches)
30 deny ip 23.0.0.0 0.255.255.255 any (847618 matches)
40 deny tcp any any range 135 139 (138750 matches)
50 permit udp host 150.254.183.15 eq ntp host 169.254.9.4 eq ntp (11460
matches)
60 deny tcp any range 135 139 any (8371 matches)
70 deny ip 96.0.0.0 31.255.255.255 any (6974 matches)
80 permit ip host 169.254.10.1 host 169.254.9.4
90 deny ip 58.0.0.0 1.255.255.255 any (749 matches)
100 deny ip 173.0.0.0 0.255.255.255 any (124 matches)
110 deny ip 172.16.0.0 0.15.255.255 any (42 matches)
120 deny ip 72.0.0.0 7.255.255.255 any (6 matches)
130 permit gre any host 169.254.20.6
140 deny ip 10.0.0.0 0.255.255.255 any
150 deny ip 0.0.0.0 1.255.255.255 any
160 deny ip 2.0.0.0 0.255.255.255 any
170 deny ip 5.0.0.0 0.255.255.255 any
180 deny ip 7.0.0.0 0.255.255.255 any
190 deny ip 27.0.0.0 0.255.255.255 any
200 deny ip 31.0.0.0 0.255.255.255 any
210 deny ip 36.0.0.0 1.255.255.255 any
220 deny ip 39.0.0.0 0.255.255.255 any
230 deny ip 41.0.0.0 0.255.255.255 any
240 deny ip 42.0.0.0 0.255.255.255 any
250 deny ip 49.0.0.0 0.255.255.255 any
260 deny ip 50.0.0.0 0.255.255.255 any
270 deny ip 70.0.0.0 1.255.255.255 any
280 deny ip 88.0.0.0 7.255.255.255 any
290 deny ip 169.254.0.0 0.0.255.255 any
300 deny ip 174.0.0.0 1.255.255.255 any
310 deny ip 176.0.0.0 7.255.255.255 any
320 deny ip 184.0.0.0 3.255.255.255 any
330 deny ip 189.0.0.0 0.255.255.255 any
340 deny ip 190.0.0.0 0.255.255.255 any
350 deny ip 192.0.2.0 0.0.0.255 any
360 deny ip 197.0.0.0 0.255.255.255 any

```

```
370 deny ip 198.18.0.0 0.1.255.255 any
380 deny ip 223.0.0.0 0.255.255.255 any
390 deny udp any range 135 netbios-ss any
```

Warto taką "optymalizację" przeprowadzić raz na jakiś czas - charakterystyki ruchu zmieniają się okresowo i coś co polepszyło sytuację pół miesiąca temu, może teraz ją pogarszać.

Po czwarte, w większości topologii w jakich router może się znaleźć, warto unikać filtrowania na interfejsie ruchu w obu kierunkach. Jeśli router posiada dwa interfejsy, to zakładając, że filtrujemy ruch wchodzący na obu interfejsach, nie trzeba już specjalnie sprawdzać ruchu wychodzącego drugim interfejsem - wiadomo, że przefiltrowaliśmy go już, gdy wchodził interfejsem pierwszym. Jeśli jednak wykonujesz routing, a jakiś ruch może być generowany z routera, być może będziesz musiał jednak coś filtrować - wszystko zależy od Twojej polityki bezpieczeństwa.

Po piąte, warto zastępować reguły odrzucające ruch do konkretnych adresów IP czy podsieci, statycznymi wpisami routingu wskazującymi na odpowiednio skonfigurowany interfejs Null 0. Routery dużo lepiej radzą sobie z routowaniem ruchu (nawet jeśli chodzi o routowanie do interfejsu będącego "czarną dziurą") niż jego filtrowaniem, czy wykonywaniem skomplikowanych operacji. Innymi słowy, po skonfigurowaniu wirtualnego interfejsu **Null 0** w ten sposób:

```
interface Null0
  description Interfejs wyrzucający pakiety
  no ip unreachable
```

Wpisy w ACLce odrzucającej ruch w ten sposób:

```
[...]
deny ip 10.0.0.0 0.255.255.255 any
deny ip 0.0.0.0 1.255.255.255 any
deny ip 2.0.0.0 0.255.255.255 any
deny ip 5.0.0.0 0.255.255.255 any
deny ip 7.0.0.0 0.255.255.255 any
deny ip 27.0.0.0 0.255.255.255 any
deny ip 31.0.0.0 0.255.255.255 any
deny ip 36.0.0.0 1.255.255.255 any
deny ip 39.0.0.0 0.255.255.255 any
deny ip 41.0.0.0 0.255.255.255 any
[...]
```

Można zastąpić następującymi wpisami statycznymi routingu (zwróć jednak uwagę, by nie dopisać takiego filtrowania dla adresów sieci, które w twojej konkretnej instalacji występują!):

```
router# ip route 10.0.0.0 255.0.0.0 null 0
router# ip route 0.0.0.0 254.0.0.0 null 0
router# ip route 2.0.0.0 255.0.0.0 null 0
router# ip route 5.0.0.0 255.0.0.0 null 0
router# ip route 7.0.0.0 255.0.0.0 null 0
router# ip route 27.0.0.0 255.0.0.0 null 0
router# ip route 31.0.0.0 255.0.0.0 null 0
router# ip route 36.0.0.0 254.0.0.0 null 0
router# ip route 39.0.0.0 254.0.0.0 null 0
router# ip route 41.0.0.0 255.0.0.0 null 0
```

Po szóste i ostatnie, jeśli filtrujesz ruch na interfejsach wewnętrznych pod kątem poprawności adresów (tzn. nie chcesz, by ktoś w Twojej sieci 192.168.0.0/24 mógł wysyłać pakiety z adresem źródłowym np. 172.16.0.0/16), a masz lub możesz włączyć mechanizm CEF, możesz ACLkę w tej postaci:

```
ip access-list extended RuchLAN
deny tcp any any range 135 139
deny udp any any range 135 139
deny tcp any range 135 139 any
```

```
deny udp any range 135 netbios-ss any
permit ip 192.168.0.0 0.0.0.255 any
deny ip any any
```

...zmodyfikować do postaci:

```
ip access-list extended RuchLAN
deny tcp any any range 135 139
deny udp any any range 135 139
deny tcp any range 135 139 any
deny udp any range 135 netbios-ss any
permit ip any any
```

A w zamian za to, włączyć na interfejsie do którego przypisana była ta ACLka, mechanizm uRPF, czyli *unicast Reverse-Path-Filtering*, w ten sposób:

```
router# ip cef
router# conf t
router(config)# interface FastEthernet 0
router(config-if)# ip verify unicast reverse-path
```

Jak to działa? uRPF opiera swoje działanie o tablicę budowaną przez CEF - FIB (ang. *Forwarding Information Base*). Po otrzymaniu przez router pakietu, przechodzi on następującą drogę:

- Sprawdzana jest wejściowa ACLka przypisana do interfejsu.
- uRPF sprawdza, czy droga powrotna dla pakietu wskazuje na interfejs, którym dotarł on do routera - jeśli nie, pakiet jest odrzucany
- CEF sprawdza FIB, by wyznaczyć dalszą drogę dla pakietu (jeśli nie został odrzucony)
- Na interfejsie, którym pakiet ma opuścić router, sprawdzana jest ACLka wyjściowa
- Pakiet jest wysyłany przez interfejs.

Innymi słowy, założmy, że masz router z dwoma interfejsami - Ethernetowym, o adresie 192.168.0.1/24 i szeregowy, z adresem 169.254.10.2/30. Po włączeniu mechanizmu CEF, budowany jest FIB. Znajdzie się w nim wpis dla sieci 192.168.0.0/24 jako "zaczepionej" na interfejsie Ethernet. Zarażona stacja w sieci LAN zaczyna generować pakiety, z losowo wybranymi adresami źródłowymi. Dla każdego pakietu otrzymanego interfejsem Ethernet, router sprawdza, czy jeśli przysłaby na niego odpowiedź, miałby wysłać ją interfejsem, z którego właśnie ją odebrał. Założmy, że router otrzymał pakiet ze sfałszowanego adresu 10.7.65.2. Sprawdza tablicę FIB i nie znajduje wpisu, który mówiłby, że do sieci 10 należy wychodzić interfejsem Ethernetowym - pakiet jest w związku z tym odrzucany. Na tej samej zasadzie działa ochrona ruchu, otrzymywanego przez interfejs szeregowy - jeśli tylko włączono na nim mechanizm uRPF. Pakiet, który chciałby zostać "wstrzelony" do sieci LAN (założmy, że przyszedł z adresem należącym do Twojej sieci LAN), zostanie odrzucony, ponieważ przyszedł złym interfejsem.

Działanie funkcji uRPF na konkretnym interfejsie potwierdzić można wydając polecenie:

```
router# show ip interface fastethernet 0

FastEthernet0 is up, line protocol is up
[...]
IP verify source reachable-via RX, allow default
! włączona weryfikacja adresów źródłowych
642 verification drops
! ilość odrzuconych pakietów z uwagi na zły adres źródłowy
```

A ogólnie dla całego routera:

```
router# show ip traffic
```

```
IP statistics:
[...]
Drop: 0 encapsulation failed, 0 unresolved, 0 no adjacency
      0 no route, 2512 unicast RPF, 0 forced drop
```

Rozdział 12. VPN - Wirtualne Sieci Prywatne

Co tak naprawdę oznacza akronim VPN?

VPN to *Virtual Private Network*, czyli wirtualna sieć prywatna. Termin "wirtualna" oznacza, że jest to sieć stworzona w oparciu o współdzieloną z innymi użytkownikami infrastrukturę sieciową (router, media dostępne itp.), ale jednak odrębna.

Sieci VPN można zatem tworzyć zarówno w oparciu o protokoły takie jak ATM czy Frame Relay (osobne kanały PVC/SVC), MPLS (osobne instancje routingu) czy IPsec, L2TP oraz PPTP (tunele L3 lub połączenia punkt-punkt sąsiednich urządzeń)

Jak skonfigurować...

...tunel IPsec pomiędzy dwoma routerami połączonymi do Internetu kanałami Frame Relay PVC?

Zakładamy, że łączymy dwie lokalizacje ("A" i "B") wyposażone w pojedyncze PVC do Internetu (w obu przypadkach DLCI 99).

Dane lokalizacji "A":

- Połączenie dostępne do routera brzegowego: 169.254.10.0/30, przy czym .1 to adres routera ISP a .2 to adres routera klienta
- Sieć lokalna ma adresację 192.168.10.0/24, przy czym .1 to adres interfejsu routera.
- Ruch nie chroniony tunelem IPsec wysyłany jest normalnie do Internetu, po zNATowaniu na publiczny adres interfejsu routera.

Dane lokalizacji "B":

- Połączenie dostępne do routera brzegowego: 169.254.20.0/30, przy czym .1 to adres routera ISP a .2 to adres routera klienta
- Sieć lokalna ma adresację 192.168.20.0/24, przy czym .1 to adres interfejsu routera.
- Ruch nie chroniony tunelem IPsec wysyłany jest normalnie do Internetu, po zNATowaniu na publiczny adres interfejsu routera.

Poniżej konfiguracja routera w lokalizacji "A":

```
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
no service dhcp
!
hostname rtr_a
!
enable password jakies_trudne_haslo
```

```
!  
username user_1 password haslo_usera_1  
ip subnet-zero  
no ip source-route  
no ip domain-lookup  
ip tcp path-mtu-discovery  
logging buffered 64000  
!  
crypto isakmp policy 1  
! konfigurujemy politykę dla ISAKMP, reguła #1  
hash md5  
! wiadomości ISAKMP mają używać algortmu mieszającego MD5  
! (jest szybszy ale i mniej bezpieczny niż SHA1)  
authentication pre-share  
! uwierzytelnienie węzłów ISAKMP odbędzie się w oparciu o  
! współdzielony tajny klucz  
crypto isakmp key trudne_haslo_isakmp address 169.254.20.2  
! dla partnera o adresie 169.254.20.2 używać będziemy dla  
! nawiązania sesji tajnego klucza "haslo_isakmp"  
! oczywiście klucz po obu stronach musi się zgadzać  
!  
!  
crypto ipsec transform-set myset esp-des esp-md5-hmac  
! Po nawiązaniu sesji ISAKMP, IPsec będzie używał  
! protokołu ESP z algorytmem szyfrowania ESP i algorytmu  
! mieszającego MD5-HMAC  
mode tunnel  
! połączenie IPsec będzie połączeniem w trybie tunelu  
!  
crypto map MapaISAKMP 1 ipsec-isakmp  
! po otrzymaniu przez router pakietu ISAKMP na port 500/udp  
! zaczyna on sekwencyjne sprawdzanie kolejnych reguł w crypto-mapach  
! ta, jedyna, ma numer 1 i zostanie sprawdzona pierwsza  
set peer 169.254.20.2  
! reguła pasuje do partnera o adresie 169.254.20.2  
set transform-set myset  
! używamy dla niego przekształcenia o nazwie "myset"  
match address 110  
! ruchem szyfrowanym wg tej reguły jest ruch pasujący do ACL 110  
!  
interface FastEthernet 0/0  
description Polaczenie dla sieci LAN  
ip address 192.168.10.1 255.255.255.0  
ip nat inside  
!  
interface Serial0  
description Konfiguracja fizycznego interfejsu szeregowego  
no ip address  
encapsulation frame-relay  
frame-relay lmi-type ansi  
!  
interface Serial0.1 point-to-point  
description Polaczenie do Internetu 2Mbit  
ip address 169.254.10.2 255.255.255.252  
frame-relay interface-dlci 99 IETF  
ip nat outside  
crypto map MapaISAKMP  
! ruch przechodzący przez ten interfejs, ma trafiać do  
! crypto-mapy MapaISAKMP  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 Serial0.1  
no ip http server  
!  
ip nat inside source list 100 interface Serial 0.1 overload  
!  
access-list 100 permit ip 192.168.10.0 0.0.0.255 any  
access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255  
! ACLka używana w określeniu reguł szyfrowania - podlega mu
```

```

! ruch z podsieci 192.168.10.0/24 do podsieci 192.168.20.0/24
! (z "naszego" LANu do zdalnego
!
no cdp run
!
line con 0
  exec-timeout 5 0
  login local
line vty 0 4
  exec-timeout 5 0
  login local
!
end

```

..a teraz konfiguracja routera w lokalizacji "B":

```

no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
no service dhcp
!
hostname rtr_b
!
enable password jakies_trudne_haslo
!
username user_1 password haslo_usera_1
ip subnet-zero
no ip source-route
no ip domain-lookup
ip tcp path-mtu-discovery
logging buffered 64000
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key trudne_haslo_isakmp address 169.254.10.2
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
mode tunnel
!
crypto map MapaISAKMP 1 ipsec-isakmp
  set peer 169.254.10.2
  set transform-set myset
  match address 110
!
interface FastEthernet 0/0
  description Polaczenie dla sieci LAN
  ip address 192.168.20.1 255.255.255.0
  ip nat inside
!
interface Serial0
  description Konfiguracja fizycznego interfejsu szeregowego
  no ip address
  encapsulation frame-relay
  frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
  description Polaczenie do Internetu 2Mbit
  ip address 169.254.20.2 255.255.255.252
  frame-relay interface-dlci 99 IETF
  ip nat outside
  crypto map MapaISAKMP
!

```

```

ip classless
ip route 0.0.0.0 0.0.0.0 Serial0.1
no ip http server
!
ip nat inside source list 100 interface Serial 0.1 overload
!
access-list 100 permit ip 192.168.20.0 0.0.0.255 any
access-list 110 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
!
no cdp run
!
line con 0
  exec-timeout 5 0
  login local
line vty 0 4
  exec-timeout 5 0
  login local
!
end

```

...tunel IPsec+GRE pomiędzy dwoma routerami połączonymi do Internetu kanałami Frame Relay PVC?

Zakładamy, że łączymy dwie lokalizacje ("A" i "B") wyposażone w pojedyncze PVC do Internetu (w obu przypadkach DLCI 99). Dodatkowo, chcemy chronić tunel GRE, ponieważ oprócz ruchu unicastowego, chcemy przynosić ruch broadcastowy lub np. inne protokoły (IPX itp.)

Dane lokalizacji "A":

- Połączenie dostępne do routera brzegowego: 169.254.10.0/30, przy czym .1 to adres routera ISP a .2 to adres routera klienta
- Sieć lokalna ma adresację 192.168.10.0/24, przy czym .1 to adres interfejsu routera.
- Tunel ma adres 192.168.254.1, drugi koniec (po stronie drugiej lokalizacji) ma adres 192.168.254.2, w obu przypadkach używamy maski /30.
- Ruch nie chroniony tunelem IPsec wysyłany jest normalnie do Internetu, po zNATowaniu na publiczny adres interfejsu routera.

Dane lokalizacji "B":

- Połączenie dostępne do routera brzegowego: 169.254.20.0/30, przy czym .1 to adres routera ISP a .2 to adres routera klienta
- Sieć lokalna ma adresację 192.168.20.0/24, przy czym .1 to adres interfejsu routera.
- Tunel ma adres 192.168.254.2, drugi koniec (po stronie drugiej lokalizacji) ma adres 192.168.254.1, w obu przypadkach używamy maski /30.
- Ruch nie chroniony tunelem IPsec wysyłany jest normalnie do Internetu, po zNATowaniu na publiczny adres interfejsu routera.

Poniżej konfiguracja routera w lokalizacji "A":

```

no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
no service dhcp
!
hostname rtr_a

```

```

!
enable password jakies_trudne_haslo
!
username user_1 password haslo_usera_1
ip subnet-zero
no ip source-route
no ip domain-lookup
ip tcp path-mtu-discovery
logging buffered 64000
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key trudne_haslo_isakmp address 169.254.20.2
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
mode transport
!
crypto map MapaISAKMP 1 ipsec-isakmp
set peer 169.254.20.2
set transform-set myset
match address SiecIPSEC
! ponieważ używamy tunelu GRE, szyfrowaniu podlegają już pakiety
! GRE wymieniane pomiędzy publicznymi adresami routerów - ta ACLka
! dokładnie to wskazuje
!
interface Tunnel0
! Dodajemy wirtualny interfejs Tunel 0
ip address 192.168.254.1 255.255.255.252
! nadajemy mu adres IP - może to być dowolny adres prywatny,
! sensownie jest zarezerwować sobie np. całą klasę C na potrzeby
! tuneli i brać z nich kolejne /30
tunnel source Serial 0.1
! źródłem tunelu jest interfejs publiczny routera
tunnel destination 169.254.20.2
! a miejscem docelowym publiczny adres naszego partnera
crypto map MapaISAKMP
! ruch przechodzący przez ten interfejs ma być chroniony
! regułami zawartymi w crypto-mapie MapaISAKMP
!
interface FastEthernet 0/0
description Polaczenie dla sieci LAN
ip address 192.168.10.1 255.255.255.0
ip nat inside
!
interface Serial0
description Konfiguracja fizycznego interfejsu szeregowego
no ip address
encapsulation frame-relay
frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
description Polaczenie do Internetu 2Mbit
ip address 169.254.10.2 255.255.255.252
frame-relay interface-dlci 99 IETF
ip nat outside
crypto map MapaISAKMP
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0.1
ip route 192.168.20.0 255.255.255.0 Tunnel0
! statycznie wskazujemy, że ruch do podsieci 192.168.20.0/24
! (LAN naszego partnera) ma się odbywać przez Tunel 0
no ip http server
!
ip nat inside source list 100 interface Serial 0.1 overload
!
access-list 100 permit ip 192.168.10.0 0.0.0.255 any

```

```

!
ip access-list extended SiecIPSEC
  permit gre host 169.254.10.2 host 169.254.20.2
  ! szyfrujemy ruch protokołu GRE pomiędzy publicznymi adresami
  ! partnerów
!
no cdp run
!
line con 0
  exec-timeout 5 0
  login local
line vty 0 4
  exec-timeout 5 0
  login local
!
end

```

..a teraz konfiguracja routera w lokalizacji "B":

```

no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
no service dhcp
!
hostname rtr_b
!
enable password jakies_trudne_haslo
!
username user_1 password haslo_usera_1
ip subnet-zero
no ip source-route
no ip domain-lookup
ip tcp path-mtu-discovery
logging buffered 64000
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key trudne_haslo_isakmp address 169.254.10.2
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
mode transport
!
interface Tunnel0
  ip address 192.168.254.2 255.255.255.252
  tunnel source Serial 0.1
  tunnel destination 169.254.10.2
  crypto map MapaISAKMP
!
crypto map MapaISAKMP 1 ipsec-isakmp
  set peer 169.254.10.2
  set transform-set myset
  match address SiecIPSEC
!
interface FastEthernet 0/0
  description Polaczenie dla sieci LAN
  ip address 192.168.20.1 255.255.255.0
  ip nat inside
!
interface Serial0
  description Konfiguracja fizycznego interfejsu szeregowego
  no ip address
  encapsulation frame-relay

```

```
frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
description Polaczenie do Internetu 2Mbit
ip address 169.254.20.2 255.255.255.252
frame-relay interface-dlci 99 IETF
ip nat outside
crypto map MapaISAKMP
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0.1
ip route 192.168.10.0 255.255.255.0 Tunnel0
no ip http server
!
ip nat inside source list 100 interface Serial 0.1 overload
!
access-list 100 permit ip 192.168.20.0 0.0.0.255 any
!
ip access-list extended SiecIPSEC
permit gre host 169.254.20.2 host 169.254.10.2
!
no cdp run
!
line con 0
exec-timeout 5 0
login local
line vty 0 4
exec-timeout 5 0
login local
!
end
```

Rozdział 13. Telekomunikacja

ISDN

Jaką prędkość mogę uzyskać, stosując ISDN?

ISDN dostarczany jest w dwóch rodzajach: ISDN BRI, czyli *Basic Rate Interface*, na który składają się 2 kanały B i jeden D, oraz ISDN PRI, czyli *Primary Rate Interface*, składający się w Europie z 30 kanałów B i jednego D. Kanały B mają standardową przepustowość 64kbit/s, natomiast kanał D dla łącz BRI ma przepustowość 16kbit/s, a dla łącza PRI 64kbit/s.

Uwaga: tylko kanały B przenoszą dane, kanały D używane są tylko do sygnalizacji.

Co to jest Q.921? A Q.931? Jak to się ma do PPP czy IP?

Protokoły Q.921 i Q.931 działają w kanale D połączenia ISDN. Protokół Q.921 odpowiedzialny jest za warstwę drugą połączenia - sygnalizację między routerem a centralką ISDN. Protokół Q.931 odpowiada natomiast za konfigurację połączenia po tym, jak w ramach protokołu Q.921 strony strony uzgodnią warstwę transportową.

Protokoły PPP, HDLC, IP czy IPX przenoszone są w kanale B połączenia ISDN. Protokoły PPP i HDLC to protokoły warstwy drugiej, natomiast IP i IPX to protokoły warstwy trzeciej. Najczęściej przy połączeniach routerów przez ISDN, przenosi się pakiety IP w ramach PPP (po uprzednim uwierzytelnieniu się).

Jaką kartę zastosować do połączenia ISDN BRI w celu przenoszenia danych?

Jeśli masz wolny slot WIC (routery 1600, 1700, 2600, 3600 i 3700), możesz zastosować kartę WIC-1B-S/T. Zawiera ona pojedynczy port ISDN BRI.

Jeśli masz wolny slot NM (routery 2600, 3600 i 3700), możesz zastosować karty NM-4B-S/T lub NM-8B-S/T, zawierające odpowiednio 4 i 8 styków ISDN BRI.

Jeśli natomiast masz wolny slot PA (routery serii 7000) i zależy Ci na portach BRI, dostępna jest tylko jedna karta: PA-8B-S/T, zawierająca osiem portów BRI.

Jaką kartę zastosować do połączenia ISDN PRI w celu przenoszenia danych?

Jeśli masz wolny slot NM (routery 2600, 3600 i 3700), możesz zastosować kartę NM-1CE1T1-PRI lub NM-2CE1T1-PRI. Zawierają one odpowiednio jeden i dwa styki ISDN PRI.

Jak skonfigurować połączenie z routera do Internetu przez interfejs BRI?

Jest to często spotykana konfiguracja, w sytuacji, gdy Internet dostarczany jest np. przez połączenie z darmową linią 0202422 TP S.A. Uwaga – to tylko częściowa konfiguracja, musisz dodać konfigurację interfejsu wewnętrznego oraz NATu (jako minimum).

```
!  
isdn switch-type basic-net3  
! określamy typ centrali ISDN jako basic-net3 (standard w Europie)  
!  
interface BRI 0  
no ip address  
! fizyczny interfejs nie ma adresu IP  
dialer pool-member 1  
! jest członkiem pierwszej puli dialerów  
isdn spid1 Nasz numer telefonu  
no fair-queue  
no cdp enable  
!  
interface Dialer1  
! interfejs wirtualny odpowiadający za przywiązanie  
! warstwy trzeciej  
ip address negotiated  
! adres IP otrzymujemy dynamicznie  
encapsulation ppp  
! używamy protokołu PPP  
dialer pool 1  
! jest członkiem pierwszej puli dialerów  
dialer remote-name ppp  
! zdalny host ma nazwę ppp (chodzi o przywiązanie loginu do hasła)  
dialer string 0202422  
! dzwonimy pod numer 0202422  
dialer-group 1  
! jest członkiem pierwszej grupy dzwoniącej  
no cdp enable  
ppp authentication chap callin  
! używamy uwierzytelniania CHAP w ramach PPP  
ppp multilink  
! staramy się zestawić połączenie multilink PPP (oba kanały B)  
ppp chap hostname TwójLogin  
! login, które otrzymałeś w ramach usługi - dla ogólnego dostępu jest to ppp  
ppp chap password TwojeHasło  
! hasło jak wyżej - dla tego numeru jest to ppp  
!  
ip route 0.0.0.0 0.0.0.0 Dialer1  
!  
ip dialer-list 1 protocol ip
```

Jak sprawdzić historię połączeń interfejsów ISDN?

Poleceniem `'show isdn history'`:

```
router# show isdn history
-----
                        ISDN CALL HISTORY
-----
History table has a maximum of 100 entries.
History table data is retained for a maximum of 15 Minutes.
-----
Call    Calling    Called    Remote    Seconds  Seconds  Seconds  Charges
Type   Number      Number    Name      Used     Left     Idle     Units/Currency
-----
Out     +0202124    +0202124  ppp       360      0        0        0
Out     +0202124    +0202124  ppp       392      0        0        0
-----
```

E1/E3

Jaką kartę zastosować do połączenia E1 w celu przenoszenia danych?

Jeśli masz wolny slot WIC (routery 1600, 1700, 2600, 3600 i 3700), możesz zastosować kartę VWIC-1MFT-E1 lub VWIC-2MFT-E1. Zawierają one odpowiednio jeden i dwa porty E1.

Jeśli natomiast masz wolny slot PA (routery serii 7000) masz do wyboru kartę PA-4E1G/75 (75 ohmów) lub PA-4E1G/120 (120 ohmów). Każda z kart zawiera po cztery porty E1, które obsługują również pracę w trybie G.703.

Jaką kartę zastosować do połączenia E3 w celu przenoszenia danych?

Jeśli masz wolny slot NM (routery 2600, 3600 i 3700), możesz zastosować kartę NM-1T3/E3. Zawiera one pojedynczy port E3 (przepływność do 34Mbit/s).

Jeśli masz wolny slot PA (routery serii 7000) masz do wyboru kartę PA-E3 (jeden port E3) lub kartę PA-2E3 (dwa porty E3).

ATM

Jaką kartę zastosować do połączenia ATM w celu przenoszenia danych?

Jeśli masz wolny slot WIC (routery 2600, 3600 i 3700), możesz użyć karty VWIC-1MFT-E1 lub VWIC-2MFT-E1 oraz karty-akceleratora AIM-ATM, by zaterminować ATM.

Jeśli masz wolny slot NM (routery 2600, 3600 i 3700), możesz zastosować kartę NM-1ATM. Zawiera one pojedynczy port RJ-48C i obsługuje przepływności do 25Mbit/s. Warto dokupić również kartę-akcelerator AIM-ATM, ponieważ wydajność bez niej może być bardzo mała.

Routery 2691, 3600 i 3725 obsługują również kartę NM-1A-OC3MM, która zawiera styk ATM OC3 - do przepływności 155Mbit/s.

Jeśli masz wolny slot PA (routery serii 7000) masz do wyboru kartę PA-A3-E3 (ATM w oparciu o łącze E3 34Mbit/s) lub PA-A3-OC3MM (ATM w oparciu o OC3 - 155Mbit/s).

Rozdział 14. Rodzaje komutacji w routerach Cisco

Co to jest switching? Jaki ma związek z komutacją?

Proces mapowania adresów warstwy 2 w 3 i przekazywania pakietów na docelowy interfejs, nosi nazwę *switchingu* (po polsku komutacja).

Jakie są rodzaje switchingu?

- **Process Switching**

Metoda ta była pierwszą metodą zaimplementowaną w IOS i jest to metoda najprostsza. Pierwszy pakiet w strumieniu (ang. *flow*) jest kopiowany do bufora systemowego, a następnie procesor przeszukuje tablicę routingu w poszukiwaniu miejsca docelowego. Suma kontrolna (CRC) liczona jest przez procesor. Następnie informacje warstwy 2 są przepisywane i pakiet wysyłany jest na docelowy interfejs. Każde następane pakiety strumienia są komutowane podobnie.

Process switching ma najdłuższy czas komutacji pakietów, ponieważ używa buforów systemowych i procesora głównego, aby "obrobić" każdy pakiet otrzymany przez router. Niemniej jednak, ten rodzaj komutacji potrzebny jest przy niektórych zadaniach, nawet, jeśli na routerze działają inne, optymalniejsze mechanizmy komutacji - np. logowanie pakietów trafiających w ACLki, debuggng pakietów IP itp.

Minusy process switchingu: wymaga aby dla każdego pakietu zajrzeć do tablicy routingu - kosztuje to czas. Jeśli tablica routingu rozrośnie się, zwiększy się również czas przetwarzania każdego pakietu. Rekursywne zapytania także zwiększają czas przetwarzania pakietu. Zwiększa się także obciążenie CPU routera, co przy małych sieciach może być do pominięcia, ale przy większych staje się problemem. Innym problemem rzutującym na wydajność jest szybkość transferu danych z pamięci.

- **Fast Switching**

Fast switching używa pamięci podręcznej by przechowywać informacje o przepływającym przez router strumieniu (ang. *flow*). W momencie włączenia fast switching, pierwszy pakiet w strumieniu jest zapisywany w pamięci packet (oddzielny obszar w buforach systemowych). Następnie procesor przelicza mapowanie warstwy 3 na 2, zapisuje trasę w pamięci route (ang. *route cache*) i każdy następny pakiet ze strumienia jest już komutowany z wykorzystaniem zapisanych w pamięciach podręcznych informacji.

Ponieważ adres pakietów w strumieniu jest już znany, route cache służy również do sprawdzenia interfejsu docelowego, przez który pakiet powinien opuścić router. Następnie pakiet ma przepisywany nagłówek warstwy 2 a procesor interfejsu oblicza sumę CRC. Kolejne pakiety z potoku nie przerywają działania procesora głównego, a ponieważ interfejs docelowy jest znany (przechowywany w route cache) również bufor systemowe nie są używane do przetrzymywania pakietu.

Fast switching jest domyślnym mechanizmem komutacji na routerach 1600, 1700, 2500 oraz 2600 na interfejsach Ethernet, FastEthernet oraz Serial. Jeśli fast switching zostało wyłączone, można przywrócić je używając polecenia `ip route-cache` na interfejsie. Aby monitorować informacje o działaniu tego mechanizmu, należy wydać komendę `show ip cache`.

- **Optimum oraz Distributed Switching**

Metody te nie są dostępne w routerach serii 1600, 1700, 2500 oraz 2600. Przy optimum switching używana jest metoda podobna do fast switching, z tym, że po tym jak pierwszy pakiet strumienia został przetworzony, informacja o trasie dla dalszych pakietów jest wpisywana do osobnej pamięci podręcznej (optimum switching cache), która działa szybciej i optymalniej niż w metodzie fast. Optimum switching dostępne jest na routerach klasy 7200.

Aby włączyć optimum switching należy wydać komendę: `ip route-cache optimum` na każdym

interfejsie. Monitoring lub troubleshooting wymaga użycia komendy: `show ip cache optimum`.

Distributed switching wymaga z kolei użycia osobnych Versatile Interface Processor (VIP). Karta VIP przechowuje lokalną kopię route cache i przeprowadza cały proces komutacji lokalnie - interfejs nie musi czekać na pamięć.

- **NetFlow Switching**

NetFlow switching pozwala na zbieranie informacji o ruchu IP do celów rozliczeniowych i/lub dokładniejszej analizy obciążenia sieci. NetFlow używa domyślnie fast switchingu lub optimum switchingu do przekazywania ruchu IP. Strumienie (ang. *flows*) śledzone są z dokładnością do protokołu, portu (TCP/UDP), typu serwisu. Informacje te mogą być eksportowane do stacji zarządzającej. Ponieważ dane zbierane przez NetFlow są przechowywane w routing cache, proces komutacji NetFlow jest przezroczysty dla wszystkich urządzeń sieciowych. NetFlow zwiększa jednak obciążenie procesora oraz pamięci. Domyślnie NetFlow cache używa 64 bajty pamięci na każdy strumień.

Komutację NetFlow można włączyć wydając polecenie `ip route-cache flow`. Aby monitorować pracę NetFlow można użyć polecenia `show ip cache flow`. Eksport danych NetFlow następuje dopiero, gdy wskażesz adresata danych poleceniem `ip flow-export adres_IP`.

- **Cisco Express Forwarding - CEF**

Tablica FIB (ang. *Forwarding Information Base*) używana jest do przechowywania wszystkich znanych tras z tablicy routingu, a do jej przeszukiwania używany jest zaawansowany algorytm. FIB zmienia się, jeśli zmieniają się wpisy w tablicy routingu routera. Tablica FIB (ewentualnie CEF table) implementowana jest jako "zmniejszona" tablica routingu, za pomocą 256-ścieżkowej tablicy mtrie. Aby wyświetlić tablicę użyj polecenia `show ip cef summary`. W tablicy każdy węzeł (ang. *node*) może posiadać do 256 "dzieci". Każde "dziecko" (link) używane jest do reprezentacji innego adresu dla każdego oktetu w adresie IPv4.

Tablica sąsiedztw (ang. *adjacency*) używana jest w mechanizmie CEF do przechowywania informacji o sąsiadach. Sąsiadem może zostać tylko taki host, który jest w odległości jednego hopa. Tablica sąsiedztw przechowuje adresy warstwy 2 sąsiadów, dla każdego wpisu w FIB. Aby wyświetlić tablicę użyj polecenia `show adjacency`.

Ponieważ adresy docelowe mogą mieć więcej niż jedną ścieżkę, CEF może zostać użyty do rozkładania obciążenia (ang. *load balancing*), poprzez różne ścieżki. Jeśli interfejs otrzymuje pakiet i włączony jest mechanizm CEF, router przeszukuje tablicę FIB. Po znalezieniu pasujących informacji, tworzony jest nagłówek warstwy 2 i pakiet jest komutowany.

CEF opisano dokładniej tutaj:
http://www.cisco.com/warp/public/cc/pd/iosw/iore/tech/cef_wp.htm.

Jeśli masz ochotę poczytać dokładniej o metodach komutacji, warto zajrzeć do podręcznika do najnowszej wersji IOS poświęconego właśnie tym zagadnieniom:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/swit_vcg.htm.

Jak skonfigurować...

...CEF (Cisco Express Forwarding)?

Na platformach, które CEF wspierają i w których załadowano IOS z feature-setem obsługującym go, wystarczy wydać polecenie:

```
router(config)# ip cef
```

Spowoduje to włączenie **na wszystkich** interfejsach tego routera, chyba, że w konfiguracji konkretnego interfejsu(-ów) wskazano wprost inny rodzaj mechanizmu komutacji, lub w ogóle wyłączono na nim jakiegokolwiek mechanizmy (np. poleceniem `no ip route-cache`).

Uwaga: Włączenie CEFu powoduje zajęcie pewnej ilości pamięci. Jeśli masz jej bardzo mało, postaraj się najpierw ją rozszerzyć lub wyłączyć nieużywane usługi, a dopiero później włączyć CEF.

...CEF dla routingu wg zasad (ang. *policy-based*)?

W nowych IOSach (ścieżka 12.2 i 12.3) samo włączenie CEFu powoduje włączenie również zaawansowanych mechanizmów dla ruchu obsługiwanego route-mapami. Na pozostałych platformach należy dodatkowo w definicji konkretnego interfejsu (do którego już przypisano polecenie `ip route-map nazwa_route_mapy`). dodać:

```
router(config)# interface FastEthernet 0/0
router(config-if)# ip route-map moja-mapa
router(config-if)# ip route-cache policy
```

Jeśli włączyłeś CEF i nie wiesz, czy obsługuje on również ruch obsługiwany przez route-mapy, sprawdź to na przykład tak:

```
router# show ip interface FastEthernet 0/0 | include route-cache
IP route-cache flags are Fast, CEF
```

Jeśli natomiast mechanizm CEF jest wyłączony (ale włączony pozostaje fast-switching, domyślna konfiguracja wielu mniejszych routerów), stan interfejsu wygląda tak:

```
router# show ip interface FastEthernet 0/0 | include route-cache
IP route-cache flags are none
```

Jak sprawdzić...

...jakie mechanizmy komutacji włączono na interfejsie?

Posługując się poleceniem `show ip interface X`.

```
router# show ip interface FastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
Internet address is 169.254.10.1/24
Broadcast address is 255.255.255.255
[...]
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
```

...ile ruchu komutowanego jest danym mechanizmem komutacji?

Ogólne zestawienie, zawierające podział ruchu na obsługiwany przez procesor lub inne mechanizmy komutacji (zbiorczo), uzyskać można wydając polecenie `show interface stats`:

```
router# show interface stats
```

```

FastEthernet0
  Switching path   Pkts In   Chars In   Pkts Out   Chars Out
  Processor        1061140  147825393  1527082    123126868
  Route cache      15218207 2362951731 14344465   2136433785
  Total            16279347 2510777124 15871547   2259560653
FastEthernet1
  Switching path   Pkts In   Chars In   Pkts Out   Chars Out
  Processor        18912250 2891638844 18435628    47230091
  Route cache      0         0          0          0
  Total            18912250 2891638844 18435628    47230091

```

Natomiast posługując się poleceniem `show interface switching` możesz uzyskać dokładniejsze informacje, z rozbiciem na konkretne typy komutacji:

```

router# show interface switching

FastEthernet0/0 Do sieci LAN
  Throttle count      0
  Drops               RP      4102      SP      0
  SPD Flushes         Fast      0         SSE      0
  SPD Aggress         Fast      0
  SPD Priority         Inputs    344036    Drops    0

  Protocol            Path      Pkts In   Chars In   Pkts Out   Chars Out
  Other               Process   0         0          29273     1756380
  Cache misses
  Fast                0         0          0          0
  Auton/SSE           0         0          0          0
  IP                  Process   27314376  623508416  7373999   764616258
  Cache misses
  Fast                50915903  2865863510 70504415  1275783563
  Auton/SSE           0         0          0          0
  ARP                 Process   350986   21059160   143215    8592900
  Cache misses
  Fast                0         0          0          0
  Auton/SSE           0         0          0          0

```

Jak widać, fast-switching obsłużył na interfejsie FastEthernet 0/0 50,915,903 pakiety przychodzące i 70,504,415 pakietów wychodzących. Tylko 27,314,376 pakietów przychodzących i 7,373,999 pakietów wychodzących obsługiwane było przez process-switching.

Poniżej to samo, ale dla interfejsu szeregowego:

```

Serial0/0
  Throttle count      0
  Drops               RP      511      SP      0
  SPD Flushes         Fast      0         SSE      0
  SPD Aggress         Fast      0
  SPD Priority         Inputs    60384    Drops    0

  Protocol            Path      Pkts In   Chars In   Pkts Out   Chars Out
  Other               Process   0         0          29282     409958
  Cache misses
  Fast                0         0          0          0
  Auton/SSE           0         0          0          0
  IP                  Process   4418141  455923877  24316765  123842058
  Cache misses
  Fast                37269672 2769716975 17250459  2590666322
  Auton/SSE           0         0          0          0

```

Rozdział 15. Optymalizacja wydajności

Mam router X, który udostępnia Internet stacjom w sieci LAN. Ciągłe mam problemy z obciążeniem procesora, lub zrywanymi sesjami.

Najprawdopodobniej problemem jest wyczerpanie pamięci na wykonywanie translacji NAT. Jeśli masz stacje intensywnie korzystające z NAT, powinieneś skrócić czasy życia translacji - oszczędzając w ten sposób pamięć.

```
router(config)# ip nat ip nat translation timeout X
```

...gdzie *X* to limit czasu dla beczynnej translacji w sekundach. Domyślnie równy jest 86400, czyli 24 godziny. Sensowną wartością na początek byłoby 3600, czyli 1 godzina.

Limit ten dotyczy jednak tylko translacji, które *nie* odbywają się w ramach translacji typu **overload**, czyli takiej, w której liczba stacji z adresami prywatnymi jest większa, niż liczba publicznych adresów IP (innymi słowy, jeśli masz 1 czy 2 adresy publiczne, a sieć LAN ma 200 stacji, takiej translacji właśnie używasz).

Aby w takiej sytuacji skrócić domyślne czasy translacji, należy użyć następujących poleceń (jeśli używasz dla swojej sieci zarówno translacji typu **overload** jak i 1:1, zastosuj oba wpisy):

```
router(config)# ip nat ip nat translation tcp-timeout A
```

..gdzie *A* to limit czasu w sekundach dla połączeń TCP (domyślnie również 86400, czyli 24 godziny). Jeśli masz opisane wyżej problemy - skróć czas translacji TCP na początek do 1 godziny (3600).

Mam router X, który udostępnia Internet stacjom w sieci LAN. Mam tylko 5 stacji a widzę tysiące translacji - o co chodzi?

Jeśli to stacje z systemem operacyjnym Microsoft Windows, to problem mogą powodować połączenia z i do mechanizmów Microsoft Networking, pracujących standardowo w zakresie portów 135-139 zarówno w oparciu o TCP jak i UDP.

Jeśli Twoja konfiguracja NAT wygląda obecnie tak:

```
interface Ethernet0
 ip nat inside
!
interface Ethernet1
 ip nat outside
!
ip nat inside source list 100 interface Ethernet 1 overload
!
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
access-list 100 deny ip any any
```

...wystarczy, że zmienisz ACL 100 tak, by odrzucała ruch należący do Microsoft Networking. Docelowo lista ta powinna wyglądać np. tak:

```
access-list 100 deny tcp any any range 135 139
access-list 100 deny udp any any range 135 139
access-list 100 deny tcp any range 135 139 any
access-list 100 deny udp any range 135 139 any
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
access-list 100 deny ip any any
```

Mam router X, który udostępnia Internet stacjom w sieci LAN. Router obsługuje ruch zaledwie X Mbit/s i już procesor obciążony jest w 100%! Na stronie Cisco znalazłem informację, że ten model może obsłużyć ruch znacznie większy!

Informacje podawane w zestawieniach dotyczą zwykle *kpps* lub *Mpps* - oznaczające odpowiednio kilo pakietów na sekundę i mega pakietów na sekundę. Np. 100 kpps oznacza wydajność rzędu 100,000 pakietów na sekundę.

Teraz zderzamy się z rzeczywistością.

Po pierwsze, taka wydajność osiągnięta jest bez skonfigurowanych żadnych usług (NAT, ACL, QoS itp.) i jest **sumą** ruchu do i z routera.

Po drugie, wartości te podawane są niestety dla różnych wielkości pakietów. Z uwagi na konstrukcję i działanie, router gorzej znosi routing pakietów mniejszych (np. 64-bajtowych), ponieważ dla każdego musi wykonać pewien zestaw czynności, a lepiej większych (np. 1500-bajtowych). Co więcej, routing tej samej ilości pakietów ale o różnych rozmiarach, daje diametralnie różne wartości przepustowości - 100kpps dla pakietów o długości 64-bajtów to "zaledwie" 51Mbit/s, ale już dla pakietów 1500-bajtowych - 1,2Gbit/s! Przyjęło się, zgodnie z RFC dotyczącym pomiaru wydajności routerów, że pomiary powinny być wykonywane dla wielu rozmiarów pakietów - ale producenci podają zwykle pomiary wykonane dla pakietów o długości 384-512 bajtów.

Po trzecie w końcu, należy wziąć pod uwagę architekturę urządzenia - routery Cisco są w stanie wykonywać routing na wiele różnych sposobów, począwszy od routingu wykonywanego tylko przez procesor (ang. *process switching*) po wykorzystanie zaawansowanych mechanizmów opracowanych w tej firmie (np. ang. *CEF, Cisco Express Forwarding*).

W zależności od zbioru realnie używanych usług, czyli ACL, QoS, NATa czy protokołów routingu, dany router może być idealny do danego zastosowania, lub na przykład zupełnie się do niego nie nadawać.

W sytuacji gdy dysponujesz jednym łączem do Internetu, o przepustowości do 2Mbit/s (symetrycznie), dobrym wyborem będzie router klasy 1700. Przy sensownych kompromisach, router sprawdzi się również w konfiguracji z dwoma łączami 2Mbit/s.

Routery serii 2600XM (routery bez literek XM mają słabsze procesory i mniej pamięci, nie są już produkowane ani sprzedawane) produkowane są w trzech wersjach biorąc pod uwagę procesory, oraz w dwóch wersjach wyposażenia w interfejsy (jeden lub dwa interfejsy FastEthernet). Routery te sprawdzają się w instalacjach z dwoma-trzema łączami 2Mbit/s, lub wymagających koncentracji połączeń typu dial-up (moduły z 4 i 8 portami ISDN BRI, czy 16 i 32 portami asynchronicznymi). Wydajność tej serii wg Cisco wynosi od 20kpps (2610XM/2611XM), przez 30kpps (2620XM/2621XM) po 40kpps (2650XM/2651XM) czy 70kpps (2691).

Routery serii 3600 wyszły już z produkcji i sprzedaży (w grudniu 2003r.). Ich podstawowym mankamentem był brak zabudowanych interfejsów Ethernet (tylko 3661/3662 miały odpowiednio jeden i dwa). Doskonale sprawdzają się w scenariuszach, w których wymagana jest agregacja dużej ilości portów ISDN BRI, PRI, asynchronicznych czy też E1/G.703 (dostępne są również moduły ATM, ale o wydajności OC3 można niestety tylko pomarzyć na tej platformie). Przy rozbudowanej do maksimum pamięci RAM (dla 3620 do 64MB, dla 3640/3640A do 128MB, dla 3660 do 256MB), oraz sensownej konfiguracji, router 3660 całkiem dobrze sprawdzają się w konfiguracjach z "małym" BGP. Wydajność tej serii wg Cisco wynosi od 35kpps (3620), przez 50kpps (3640/3640A) do ~110kpps dla 3661/3662.

Routery serii 3700 - 3725 i 3745 to następcy serii 3600. Posiadają odpowiednio dwa i cztery sloty na moduły NM, po trzy sloty WIC i po dwa sloty AIM. Dodatkowo, na obu zainstalowano na stałe dwa porty FastEthernet. Biorąc pod uwagę fakt, że można na nich zainstalować maksymalnie 256MB RAM, mogą sprawdzić się w sytuacjach w których do tej pory sprawdzała się seria 3600 oraz z routingiem BGP. Wydajność 3725 Cisco ocenia na 100kpps, a 3745 - 225kpps.

Jakie rzeczy sprawdzić, optymalizując wydajność routera?

Nie ma uniwersalnych metod "optymalizacji" routera - dam Ci tylko pewne wskazówki, które mogą, ale nie muszą(!), pomóc.

- Włącz CEF (`ip cef`) - automatycznie spowoduje to włączenie mechanizmu zwiększanie wydajności na wszystkich interfejsach sieciowych, które CEF obsługuje w danym IOSie. W stosunku do *process switching*, czyli obróbki każdego pakietu przez CPU, wzrost wydajności (lub chociaż spadek obciążenia CPU) powinien być dramatyczny.
- Upewnij się, że router nie robi niepotrzebnych rzeczy - wyłącz nieużywane usługi, zoptymalizuj używane ACLki, a te, które kontrolują poprawność routowanego ruchu, zastąp mechanizmem uRPF (ang. *Unicast Reverse-Path Filtering*, polecenie `ip verify unicast reverse-path`).
- Upewnij się, że jeśli wykonujesz NAT, translacji podlega tylko sensowny i pożądany ruch - pozostały blokuj.
- Jeśli zamierzasz coś zablokować za pomocą ACLki, zastanów się, czy nie lepiej wykorzystać routingu do wirtualnego interfejsu `Null 0`. Architektura routerów optymalizowana jest do routingu a nie filtrowania pakietów, w związku z czym zwykle routing "w nicość" działa szybciej i stanowi mniejsze obciążenie dla procesora niż filtrowanie tego samego ruchu z odrzucaniem go.
- W ACLkach wyłącz logowanie w regułach - powoduje to powrót do obróbki pakietu przez CPU i może powodować wyzwalenie dodatkowych mechanizmów (logowanie na konsolę, do pamięci, do serwerów syslog itp.)
- Wyłącz wszelkie włączone sesje odpluskwiania (`undebug all`), oraz logowanie informacji na konsolę (`no logging console`)
- Wyłącz eksport i zbieranie informacji w ramach mechanizmów NetFlow - w szczególności na mniejszych platformach (1700/2600/3600/3700) włączenie tego mechanizmu przy nawet umiarkowanym ruchu może dosłownie zabić router (`no ip route-cache flow` na interfejsach, na których został włączony oraz `no ip export` w konfiguracji globalnej)
- Stosuj rozkładanie ruchu w ramach routingu domyślnego, lub w ramach jednego z protokołów routingu dynamicznego, zamiast łącz Multilink PPP. Zawsze przy takich łączach upewnij się, że routing pakietów odbywa się za pomocą najoptymalniejszej ścieżki komutacji.
- Wykorzystaj tłumienie zdarzeń związanych z IP (ang. *IP event dampening*) do ograniczenia kosztownych czasowo i obliczeniowo operacji na tablicach routingu.
- Zastanów się nad optymalnym doбором protokołu routingu do zadania: w sieciach hierarchicznych OSPF będzie sprawował się lepiej niż EIGRP, a w sieciach z jednym wyjściem do Internetu utrzymywanie routingu BGP jest generalnie bez sensu. Wykorzystaj sumaryzację do oszczędzania procesorów i pamięci.
- Dla sesji zestawianych do/z routera, np. peeringu BGP, włącz wykrywanie optymalnego MTU na łączy (`ip tcp path-mtu-discovery`). Domyślna wartość MSS (segmentu TCP) to 536 bajtów - na łączach typu Ethernet czy ATM jest mało optymalna. Zmiana ta powinna zmniejszyć ilość pakietów, a wydłużyć ich wielkość, dzięki czemu do przesłania informacji będzie potrzebna mniej pakietów. Dla Ethernetu wartość MSS wynosi generalnie 1460 bajtów, a np. dla łącz PoS/ATM - 4430 bajtów.
- Staraj się korzystać z połączeń przez sieć (Telnet/SSH) a nie przez konsolę. Na wszystkich platformach, każdy znak otrzymany/wysłany do konsoli obsługiwany jest przez procesor (ew. główny procesor), wywołujący w tym celu przerwanie. Na tej samej zasadzie, staraj się nie korzystać z portu AUX routera, jeśli nie jest to konieczne.

Gdzie Cisco publikuje informacje o wydajności swoich urządzeń?

Informacje katalogowe znajdują się zwykle w kartach katalogowych. Dodatkowo, zebrano najczęściej używane informacje w grupach arkuszy podzielonych wg. kategorii sprzętu:

<http://www.cisco.com/warp/public/765/tools/quickreference/>

Dodatkowo wydajności poszczególnych platform pod kątem szyfrowania tuneli IPsec zebrano w dokumencie z serii SRND pod adresem:

<http://www.cisco.com/warp/public/779/largeent/it/ese/SiteVPN.pdf>

Rozdział 16. Sieci bezprzewodowe

Który standard określa co w rodzinie 802.11?

Poniżej krótka lista:

802.11a

Standard określający pracę w paśmie 5GHz. Dostępne jest 13 niezakłócających się kanałów radiowych. Urządzenia mogą pracować używając kodowania OFDM z prędkościami 54, 48, 36, 24, 18, 12, 9 i 6Mbit/s.

Urządzeniami produkcji Cisco pracującymi w tej technologii są AP 10xx, 1130AG, 1200 (z radiem 802.11a) oraz most bezprzewodowy Aironet 1400.

802.11b

Standard określający pracę w paśmie 2,4GHz. Dostępne są 3 niezakłócające się kanały radiowe. Urządzenia mogą pracować używając kodowania DSSS z prędkościami 11, 5.5, 2 i 1 Mbit/s.

Urządzeniami produkcji Cisco pracującymi w tej technologii są: AP serii 350, 1120 oraz AP 1200 (z radiem 802.11b), a także bezprzewodowy most Aironet 350.

802.11g

Standard określający pracę w paśmie 2,4GHz. Dostępne są 3 niezakłócające się kanały radiowe. Urządzenia mogą pracować w trybie zgodności w dół z 802.11b używając kodowania DSSS z prędkościami 11, 5.5, 2 i 1 Mbit/s, oraz używając kodowania OFDM z prędkościami 54, 48, 36, 24, 18, 12, 9 i 6Mbit/s.

Urządzeniami produkcji Cisco pracującymi w tej technologii są: AP serii 10XX, 1130AG, 1120 oraz AP 1200 (z radiem 802.11g).

Jak policzyć EIRP?

Korzystając z poniższego wzoru:

$$\text{EIRP}_{\text{dBm}} = P_{\text{t}} + G_{\text{ant}} - L_{\text{l}}$$

Gdzie EIRP(dBm) - efektywna moc wypromieniowywana, P(t) moc nadawcza nadajnika w dBm, G(ant) - wzmacnienie anteny i L(l) - strata na kablu łączącym antenę i nadajnik.

Rozdział 17. Dobór i wymiana sprzętu

Czy muszę kupować oryginalne pamięci Cisco?

Nie, ale pamiętaj, że Cisco TAC nie wspiera konfiguracji, w których na sprzęcie Cisco zainstalowano nieoryginalne pamięci.

Bardzo dobre pamięci do routerów i przełączników Cisco sprzedaje Kingston - łącznie, z konfiguratorem dostępnym tutaj: <http://www.kingston.com/products/default.asp>.

Mam w routerze kartę X. Jaki kabel do niej dobrać?

Zbiór dostępnych kabli wraz z ich rysunkami znajduje się tutaj:
<http://www.cisco.com/univercd/cc/td/doc/pcat/#ch8>.

Skąd mogę wiedzieć, że dany sprzęt nie jest już sprzedawany przez Cisco?

Notki pojawiają się zwykle jako biuletyny na stronach poszczególnych produktów, można również posiadając konto CCO zapisać się do rozsyłanego e-mailem biuletynu informacyjnego.

Produkty obecnie zaklasyfikowane jako *EoL*, czyli *End of Life* zebrano tutaj:
<http://www.cisco.com/univercd/cc/td/doc/pcat/#ch27>.

Rozdział 18. Rozwiązywanie problemów

Obrazy IOS i ich odzyskiwanie

Straciłem obraz z Flasha. Mam do dyspozycji tylko tryb ROMMON i obraz IOSa na komputerze. Jak załadować go do routera?

Możesz skorzystać z transferu pliku przez konsolę (rozwiązanie wolniejsze) i przez TFTP - rozwiązanie zdecydowanie szybsze.

Jak załadować obraz Cisco IOS do pamięci Flash, dysponując tylko trybem ROMMON i połączeniem przez konsolę?

Zakładam, że obraz Cisco IOS znajduje się w miejscu dla Ciebie dostępnym i masz możliwość transmisji XMODEM ze swojego terminala a nazwa pliku z IOsem to `c2600-i-mz.123-1a.bin`. Wydadaj polecenie:

```
rommon 1> xmodem c2600-i-mz.123-1a.bin
Do not start the sending program yet...
device does not contain a valid magic number
dir: cannot open device "flash:"

WARNING: All existing data in bootflash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n [n]:
```

Należy potwierdzić transmisję klawiszem **Y** a następnie po pokazaniu się komunikatu:

```
Ready to receive c2600-i-mz.123-1a.bin...
```

Włączyć transmisję XMODEM ze swojego terminala, obrazu z Cisco IOS. Jeśli wszystko się powiedzie, router należy zresetować - można to zrobić sprzętowo, lub poleceniem:

```
rommon 2> reset
Po starcie routera powinien załadować się IOS:
program load complete, entry point: 0x80008000, size: 0x54ab60
Self decompressing the image : #####
##### [OK]
```

Jak załadować obraz Cisco IOS do pamięci Flash, dysponując tylko trybem ROMMON i połączeniem przez Ethernet?

Zakładam, że obraz Cisco IOS znajduje się w miejscu dla Ciebie dostępnym (w tym przykładzie plik ma nazwę `c2600-i-mz.123-1a.bin`), masz do swojej dyspozycji serwer TFTP skonfigurowany na serwowanie tego pliku i albo połączyłeś się skrosowanym kablem Ethernet do pierwszego portu Ethernet routera ze stacji, albo podłączyłeś ten port do sieci, w której będzie można osiągnąć serwer TFTP.

Należy nadać routerowi tymczasowy adres IP, w podsieci w której znajduje się również Twoja stacja. W naszym przykładzie jest to jedna podsieć - Twoja stacja ma w niej adres 169.254.10.5/24 a routerowi nadamy adres 169.254.10.2/24:

```
rommon 1> IP_ADDRESS=169.254.10.2
rommon 2> IP_SUBNET_MASK=255.255.255.0
rommon 3> DEFAULT_GATEWAY=169.254.10.1
```

Teraz wskaż adres serwera TFP oraz nazwę pliku:

```
rommon 4> TFTP_SERVER=169.254.10.5
rommon 5> TFTP_FILE=c2600-i-mz.123-1a.bin
```

Na koniec, rozpoczynamy procedurę ściągania obrazu:

```
rommon 6> tftpdnld
```

Jeśli nie chcesz zapisywać obrazu na pamięć flash a po prostu chcesz załadować obraz do pamięci i uruchomić z niego router, wydaj polecenie `tftpdnld -r`.

Hasła na routerach

Jak odzyskać zapomniane hasło z routera?

Poniższy opis dotyczy większości routerów. Oryginalne procedury do całego sprzętu produkcji Cisco Systems znajdują się tutaj: http://www.cisco.com/en/US/products/hw/contnetw/ps789/products_tech_note09186a00801746e6.shtml.

Musisz uzyskać dostęp do konsoli i zresetować router. Zaraz po rozpoczęciu ładowania:

```
System Bootstrap, Version 12.2(7r) [cmong 7r], RELEASE SOFTWARE (fc1)
Copyright (c) 2002 by cisco Systems, Inc.
C2600 platform with 65536 Kbytes of main memory
```

...musisz ze swojego terminala wysłać sekwencję Ctrl+Break. Spowoduje to wejście do ROMMONa:

```
PC = 0xffff0ac3c, Vector = 0x500, SP = 0x680127c0
monitor: command "boot" aborted due to user interrupt
rommon 1>
```

Pozostaje zmienić rejestr konfiguracyjny na wartość, która pominie wczytanie pliku konfiguracyjnego, a następnie zresetować router:

```
rommon 1> conf-reg 0x2142
rommon 2> reset
```

Po załadowaniu się Cisco IOS, wejdź do trybu uprzywilejowanego, skopiuj zawartość pliku `startup-`

config do aktualnej konfiguracji running-config i ewentualnie dokonaj zmiany haseł. Na przykład:

```
router> enable
router# copy startup-config running-config
c1760# conf t
c1760(config)# enable password moje_nowe_haslo
```

A jak odszyfrować zaszyfrowane hasło w konfiguracji routera?

Jeśli hasło zostało zaszyfrowane zwykłym mechanizmem Cisco (w konfiguracji cyfry zaszyfrowanego hasła poprzedza liczba 7, np. username szopen password 7 00170909145E05), możesz posłużyć się różnymi narzędziami, które odszyfrowują ten zapis.

Dobry i zawsze dostępny, pod warunkiem że masz dostęp do Internetu, jest serwis <http://www.securitystats.com/tools/ciscocrack.php>.

Hasła szyfrowane poleceniem *secret* używają jednokierunkowej funkcji mieszającej i ich odszyfrowanie można wykonać jedynie przez żmudne sprawdzanie kolejnych kombinacji znaków.

Interfejsy Ethernet i ruch na nich

Mam dużo kolizji na interfejsie Ethernet routera - co mogę z tym zrobić?

Najprawdopodobniej źle ustawiłeś tryb pracy portu (half lub full duplex). Starsze routery (seria 1600, 2500) posiadają interfejsy Ethernet będące w stanie pracować tylko w trybie half-duplex. Teoretycznie, port routera i przełącznik powinny dostosować sobie tryb pracy, ale w praktyce ta "autonegociacja" często zawodzi i mamy problemy z łącznością.

Najlepiej jest, po ustaleniu w jakich dokładnie trybach może pracować interfejs routera, skonfigurowanie na sztywno prędkości pracy portu i trybu duplex. Jeśli na routerze nie możesz tego zrobić - ustaw na stałe parametry pracy przynajmniej portu na przełączniku.

Na przykład, na routerze z interfejsem Ethernet:

```
router(config)# interface ethernet 0
router(config-if)# speed 10
router(config-if)# duplex half

! Teraz to potwierdzimy:

router# show interface ethernet 0

Ethernet0 is up, line protocol is up
  Hardware is AmdFE, address is 000e.1111.2222 (bia 000e.1111.2222)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 10Mb/s, 10BaseT
```

Na przełączniku natomiast (tutaj 2950, port podłączony do routera to FE0/34) ustawiamy:

```
switch(config)# interface fastethernet 0/34
switch(config-if)# speed 10
switch(config-if)# duplex half

! Teraz to potwierdzimy:
```

```
switch# show interface fastethernet 0/34

FastEthernet0/34 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 000d.1111.3333 (bia 000d.1111.3333)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 10Mb/s, media type is unknown media type
```

Próbuję zdebugować ruch na interfejsie routera poleceniem `debug ip packet`, ale widzę tylko pojedyncze pakiety?

Wyłącz CEF (`no ip cef`) - ale **uważaj(!)** na obciążenie procesora - może gwałtownie wzrosnąć - wszystko zależy od ilości obsługiwanego ruchu.

Chciałbym na PIXie sniffować ruch i zapisywać go do dalszej analizy - jak to zrobić?

Zdefiniuj ACLkę, która będzie pasowała do ruchu przeznaczonego do sniffowania. Załóżmy, że interesuje nas tylko ruch na port 80 dowolnego hosta:

```
pix(config)# access-list 100 permit tcp any any eq 80
```

Teraz uruchamiamy sniffowanie, podając tą ACLkę, rozmiar bufora (w bajtach), długość pakietu która ma być "podśluchana", a w końcu nazwę pliku, do którego zapisywany będzie wynik sniffowania:

```
pix(config)# capture in-www access-list 100 buffer 256000 interface inside packet-length 1518
```

W pamięci Flash zostaje utworzony plik o nazwie `in-www`, który zawiera zapis podsłuchanych sesji (pierwsze 256kB, później PIX przestanie nasłuchiwać) na interfejsie "inside". Możesz go skopiować np. na serwer TFTP lub FTP do dalszej analizy narzędziami takimi jak `tcpdump` czy `Ethereal` (plik jest w formacie `pcap`).

Problemy z pamięcią i IOSami

Dostaję na konsolę lub do logów komunikaty typu `%ALIGN-3-SPURIOUS: Spurious memory access made [...]`

Najczęściej jest to problem związany z brakiem pamięci (sprawdź `show memory summary`) lub błędem w oprogramowaniu.

O rozwiązywaniu tego typu problemu można poczytać np. tutaj: <http://www.cisco.com/warp/public/63/spuraccess.html>.

Mam za mało pamięci aby zapisać konfigurację - co mam zrobić?

Włączyć kompresję konfiguracji:

```
router# service compress-config
```

Problemy z przełącznikami Catalyst

Mam przełącznik Cisco Catalyst i wiele stacji do niego podłączonych. Mam problemy z logowaniem się do sieci po starcie tych komputerów.

Domyślnie port przełącznika postara się wynegocjować parametry pracy z podłączoną stacją, oraz sprawdzić, czy nie uczestniczy ona w pracy mechanizmu Spanning Tree. Ponieważ zwykła karta sieciowa nie wynegocjuje trunku 802.1Q czy ISL, ani innych dodatkowych usług, warto ustawić porty podłączone do zwykłych stacji w tryb pomijający te testy.

Dla przełączników z systemem Cisco IOS:

```
switch(config)# interface fastethernet 0/6  
switch(config-if)# spanning-tree portfast
```

Dla przełączników z systemem CatOS:

```
switch > (enable) set port host 4/9
```

Mam przełącznik 2970 lub 3750 - port 10/100/1000 podłączony do karty sieciowej 1Gbit/s (np. Intel 1000MT) nie chce przesyłać danych. W czym tkwi problem?

Porty 3, 4, 7, 8, 11, 12, 15, 16, 19, 20, 23, 24 mogą się tak zachowywać, ale oficjalny komunikat firmy Cisco wskazuje na Intela jako winowajcę. Intel przygotował odpowiednie łątki. Masz trzy alternatywy:

- Zmienić port z SGMII na RGMII czyli 1, 2, 5, 6, 9, 10, 13, 14, 17, 18, 21 lub 22
- Wydać na tym konkretnym interfejsie polecenie ``speed 1000`` by wymusić tryb pracy 1Gbit/s
- Wymienić karty sieciowe jeśli instalacja łąt i uaktualnień przygotowanych przez firmę Intel jest niemożliwa

Na swoim przełączniku 2950, 3550 czy 3750 otrzymuję komunikat %SYS-2-MALLOCFAIL: Memory allocation of (...) Cause: Memory fragmentation

Prawdopodobnie masz po prostu pętlę w sieci. Upewnij się, że na wszystkich przełącznikach włączony jest protokół Spanning Tree lub Rapid Spanning Tree.

Starsze IOSy (12.1.8-12.1.11) bardzo nie lubią takich okresowych sztormów pakietów w ramach pętli i zwykle kładą interfejs do następnego restartu (nie pomaga ``no shut``). Nowsze IOSy (od 12.1.12) lepiej radzą sobie z wysyceniem pamięci i potrafią mimo "klapnięcia" interfejsu podnieść go po chwili, ale nie jest to stan, który powinieneś w sieci pozostawić.

Typowym objawem tego problemu, są np. takie informacje w logach:

```
%SYS-2-MALLOCFAIL: Memory allocation of 1680 bytes failed from 0x156550, alignment 0  
Pool: I/O Free: 2172 Cause: Memory fragmentation  
Alternate Pool: None Free: 0 Cause: No Alternate pool
```

Jak można przeczytać, przełącznik wysycił całą pamięć I/O przeznaczoną do tymczasowego kolejkowania ramek i zgłasza błąd sfragmentowania pamięci. Postępując się poleceniem `show memory summary` można to potwierdzić:

switch#	show memory summary					
	Head	Total (b)	Used (b)	Free (b)	Lowest (b)	Largest (b)
Processor	BDDF8C	54655092	4842004	49813088	47010552	47973440
I/O	80000000	8388608	1128084	7260524	2172	7187568

Rozdział 19. Podziękowania

Chcielibyśmy wymienić tu wszystkich, którzy przyczynili się do rozwoju tego FAQ. Jak zauważyliście, poszczególne wpisy w FAQ nie są opisywane konkretną osobą - uznaliśmy, że tak będzie bardziej przejrzyste, a pytania co do zawartości FAQ powinny i tak trafiać na listę.

W kolejności jak najbardziej alfabetycznej:

- Szymon Kosmała, szymon at netfusion.pl
- Marek Moskał, moskit at irc.pl
- Szczepan Pacut, spacut at ccie.pl
- Marcin Strzyżewski, marcins at ccie.pl
- Mariusz Trojanowski, mariusz421 at wp.pl
- Adam Obszyński, awo at freebsd.pl

Rozdział 20. ChangeLog

Poniżej lista zmian w kolejnych wersjach dokumentu, wraz z osobami, które do tych zmian się przyczyniły.

v0.99(4) 27/01/2006 17:29:53

niezgodność komentarz-polecenie w CBWFQ (Mariusz Ratajczak)

typ ACL/zawartość w konfiguracji NAT (Paweł Bień)

typ ACL a konstrukcja wyrażeń w rozdziale o ACL (Paweł Bień)

v0.99(3) 27/01/2006 17:29:53

poprawka w URL dla BGP (Mariusz Wołek)

v0.99(2) 26/01/2006 10:09:09

poprawka do konfiguracji CBWFQ (Paweł Grzelewski)

v0.99(1) 14/01/2006 18:15:09

opis nowego nazewnictwa IOSów od 12.3 + parę drobnych poprawek z tym związanych (Łukasz Bromirski)

v0.99 14/01/2006 00:11:09

PDM jest na PIXach od wersji 6.0 a nie od 6.3 (Przemysław Dubicki)

DHCP podaje adresy serwerów DNS a nie DHCP (niezależnie Michał Ciepły i Krzysztof Roślowski)

Metryka OSPF-u dla ISDNu dotyczy przepustowości kanału B a nie D (Paweł Bień)

wg./wg oraz inne literówki (Sierp)

RIPv2 i maski oraz prawidłowy numer dostępowy dla TP ISDN (Krzysztof Olędzki)

Kosmetyka w konfiguracji wdzwaniania po ISDN BRI do TP (Maciej Browarski)

Pierwszy/drugi dostawca powtórzone dwukrotnie (Kaneda)

Konfiguracja SNTP do NTP (Dariusz Sznajder)

SGMII/RGMII (Łukasz Bromirski)

Stałe indeksy interfejsów w SNMP (Łukasz Bromirski)

URLe do zestawów wydajności poszczególnych platform (Łukasz Bromirski)

v0.50 21/03/2004 21:42:03

Brakujące `xmodem` przy transferze IOSu przez konsolę (Mariusz Trojanowski).

Dodanie paru pytań i odpowiedzi dla PIXów [logowanie, sniffowanie ruchu z interfejsów do plików pcap itp.], sieci WLAN, ISDNu, routingu IP oraz konfiguracji (Łukasz Bromirski).

v0.42 17/03/2004 12:49:06

Dodanie rozwiązania DSL/VPN (Mariusz Trojanowski)

Dodanie tabelki z wydajnością VPN urządzeń Cisco, konfiguracja eksportu NetFlow, routingu między VLANami na kartach WIC-4ESW oraz NM-16ESW/32ESW a także trochę kosmetycznych poprawek (Łukasz Bromirski)

v0.40 10/03/2004 14:59:06

Dodanie sekcji o OSPFie (Szczepan Pacut)

Dodanie uszczegółowień do opisu obciążenia (Marek Moskal)

Poprawki, uszczegółowienia do paru pytań oraz parę nowych pytań (Szymon Kosmala)

Konfiguracja "NATu na patyku" (Adam Obszyński)

Dodanie paru podstawowych pytań o innych protokołach routingu (Łukasz Bromirski)

Dodanie sekcji o VPNach (Łukasz Bromirski)

v0.37 08/03/2004 10:57:15

Czytelniejsze URLe oraz parę niezależnych sugestii (Marek Moskal)

labolatorium != laboratorium (Mariusz Trojanowski i Jacek Zapała)

CCIE - INTERNetwork Expert (Tomasz Mistat)

v0.36 05/03/2004 17:10:15

literówki i różne inne (Marcin Jurczuk)

v0.35 05/03/2004 09:59:16

Przygotowania do wydania publicznego