Zarządzanie sieciami IP za pomocą ruterów CISCO

Scott Ballew

Podstawy sieci IP

1

Adresy i sieci
Adresy prywatne i publiczne
Algorytm rutowania IP
Nazwy domen i System Nazw Domen (DNS)

Ostatnio sieć IP staje się coraz popularniejsza, czego powodem jest rozwój i upowszechnienie sieci Internet. Niestety, niewielu jest przeszkolonych administratorów sieci, którzy są w stanie *zarządzać* pracą takich sieci. Często do pracy w charakterze administratorów sieci IP kierowani są i tak już zapracowani ludzie od obsługi komputerów. Są oni wtedy odpowiedzialni nie tylko za sprawną pracę serwerów i hostów w sieci, lecz również urządzeń takich jak rutery, przełączniki i koncentratory, które tworzą infrastrukturę sieciową. Jest to zadanie, do którego większość z nich nie jest przygotowana.

Mam nadzieję, że książka ta wypełni lukę w przygotowaniu specjalistów, którzy w swoich organizacjach rozpoczynają pracę z sieciami IP. Mam nadzieję, że stanie się ona użytecznym wprowadzeniem do zadań, zagadnień i narzędzi związanych z efektywnym zarządzaniem zbiorem ruterów, tak aby tworzyły one stabilną i niezawodną sieć IP, od której zależy praca wielu organizacji.

Stopień przygotowania osób, które skierowano do zadań administratorów sieci, jest bardzo zróżnicowany. Toteż czasem możesz napotkać w książce materiał, który będzie Ci dobrze znany. Oznacza to wprawdzie, że jesteś obeznany z tematem, lecz mimo to nalegam, abyś przeczytał także te informacje, które na pierwszy rzut oka wydają się znane. Być może będą one przedstawiane z innego punktu widzenia, co pomoże Ci zrozumieć *rzeczy,* które zawsze uważałeś za skomplikowane i niejasne. Możesz również dowiedzieć się czegoś nowego, czegoś, co wcześniej Ci umknęło.

Ten rozdział przedstawia podstawowe pojęcia związane z sieciami IP, łącznie z adresacją, podsieciami, super sieciami, maskami, algorytmem rutowania IP oraz wzajemnym odwzorowaniem nazw i adresów przy użyciu Systemu Nazw Domen (Domain Name System - DNS). Nie są to wyczerpujące informacje na temat IP, tak jak rozdział ten nie jest samouczkiem dla osób zupełnie nie obeznanych z tematem. Rozdział ten pozwala raczej na przygotowanie wspólnej płaszczyzny zrozumienia tematu *przez* różnych czytelników tej książki. Jeśli go pominiesz, może się okazać, że przy opisie jakiegoś zagadnienia w dalszej części książki znajomość pewnych tematów tu opisanych będzie niezbędna. Jeśli chcesz dowiedzieć się więcej na temat działania protokołów IP, zachęcam do przeczytania książki *Internetworking with TCP/IP, Vol. I.* Aby dobrze poznać podstawy administracji sieci IP, przeczytaj książkę *TCP/IP Administracja sieci* (wydaną przez Wydawnictwo RM).

Po upewnieniu się, że wszyscy mamy podobną wiedzę podstawową, w kolejnych kilku rozdziałach opisane zostanie zagadnienie budowy własnej sieci (w praktyce jest to raczej opis radzenia sobie z problemami wynikającymi z błędnej konfiguracji sieci, której pracę czytelnik nadzoruje). Dowiesz się, na co zwracać uwagę przy wyborze rutera; jak wybrać dynamiczny protokół rutowania oraz jak skonfigurować protokół, który został wybrany. Dalsze rozdziały zawierają opis tematów takich jak: utrzymanie i eksploatacja sieci, dołączenie sieci do innych sieci (włączając w to sieć Internet). Nauczysz się też, w jaki sposób zabezpieczać swoją sieć i konfigurować hosty w niej pracujące, tak by broniły się przed zagrożeniami płynącymi z pracy w sieci.

W książce tej znajdziesz przykłady, sposoby postępowania i porady odnoszące się do systemu *Cisco* o nazwie *Internetiuork Operating System* (/OS). Nie myśl jednak, że informacje te są Ci niepotrzebne, jeśli nie pracujesz z ruterami Cisco. Większość z przykładów i sposobów postępowania może być zastosowana do pracy z każdym ruterem, który obsługuje odpowiednie protokoły. Niektóre z porad, których być może nie wykorzystasz bezpośrednio w pracy z Twoim ruterem, pomogą Ci opracować metody postępowania z ruterami, których używasz w sieci, niezależnie od tego, kto jest ich dostawcą.

Adresy i sieci

W każdej sieci każde miejsce, do którego inne komputery wysyłają informacje, musi mieć niepowtarzalny identyfikator. Identyfikator taki nazywany jest zwykle *adresem.* W niektórych technologiach sieciowych adres wskazuje konkretną maszynę, podczas gdy w innych, takich jak IP, adres wskazuje punkt przyłączenia do sieci, który jest powszechnie nazywany *interfejsem.* W rezultacie pojedyncza maszyna pracująca w sieci, która jest wyposażona w kilka interfejsów, może mieć kilka adresów IP - po jednym dla każdego z tych interfejsów. Interfejsy to zwykle fizycznie rozróżnialne przyłącza (tzn. gniazda, do których dołączany jest kabel sieciowy), ale mogą być nimi również logiczne przyłącza, które mają jedno wspólne przyłącze fizyczne. Możesz się spotkać również z innym rozwiązaniem określanym jako *multipleksacja interfejsu,* które stosuje się w przyłączach do sieci ATM. Logiczny podział hostów w sieci ATM

na kilka grup pozwala na traktowanie każdej z nich jako oddzielnej sieci logicznej, mimo że wszystkie hosty przyłączone są do jednej sieci fizycznej. Urządzenie przyłączone do tego typu sieci fizycznej może jednocześnie należeć do kilku sieci logicznych dzięki nawiązaniu kilku logicznych połączeń, z których każde ma własny adres IP. Maszyny, które mają kilka adresów, określa się jako *multi-homed.* Wszystkie rutery są z definicji maszynami multi-homed, ponieważ zajmują się przesyłaniem pakietów pomiędzy kilkoma sieciami. Jednakże nie wszystkie maszyny określane mianem multi-homed są ruterami. Jedna maszyna może mieć kilka przyłączeń do sieci i nie jest to rzadkością, jeśli pełni funkcję serwera plików współdzielonego przez kilka różnych sieci, bez rutowania informacji pomiędzy tymi sieciami.

Struktura adresu IP

Adresy IP mają długość 32 bitów. Rozpatruje się je jako sekwencję czterech bajtów lub, stosując terminologię inżynierów sieciowych, czterech *oktetów* (bajtów 8-bito-wych). Aby zapisać adres IP, należy dokonać konwersji każdego z oktetów do postaci zapisu dziesiętnego i oddzielić cztery powstałe w ten sposób liczby dziesiętne kropkami. A zatem 32-bitowy adres IP:

10101100 00011101 00100000 01000010

zwykle zapisywany jest jako:

172.29.32.66

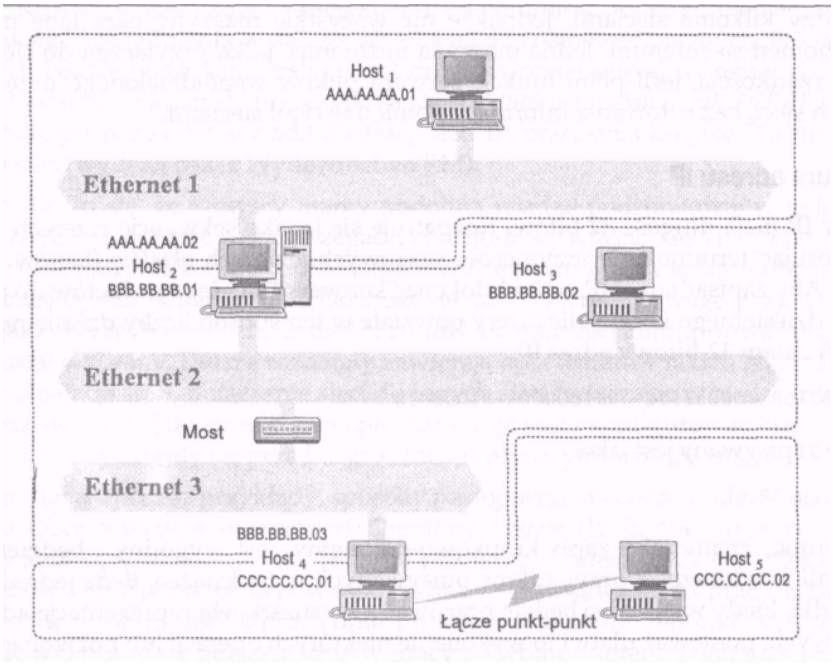
Taki format, znany jako zapis kropkowo-dziesiętny, jest wygodny i będziemy go stosowali w większości przypadków opisywanych w tej książce. Będą jednak takie przypadki, kiedy wygodniej będzie pracować z szesnastkową reprezentacją adresów 32-bitowych, ponieważ ułatwi to wykonanie niektórych operacji lub pozwoli je lepiej zrozumieć. W zapisie szesnastkowym adres IP, przedstawiony wyżej, będzie reprezentowany w następujący sposób:

Oxacld2042

Mimo że adres IP jest pojedynczą liczbą 32-bitową, to zbiór adresów IP nie jest płaski. Zamiast tego adresy zbudowane są w oparciu o dwupoziomową hierarchię sieci i hostów wchodzących w skład tych sieci. Każda z tych dwóch przestrzeni adresowych identyfikowana jest przez określoną część adresu IP, w wyniku czego każdy adres IP możemy podzielić na numer sieci i numer hosta. W protokole IP numer sieci reprezentuje zbiór maszyn, które zdolne są do bezpośredniej komunikacji w warstwie drugiej sieciowego modelu odniesienia ISO*. Warstwa ta to warstwa łącza danych, która odzwierciedla działanie takich rozwiązań jak Ethernet, Token Ring, FDDI *(Fiber Distńbuted Data Interconnect),* a także łącza typu punkt-punkt. Każda z tych technologii

*ISO to skrót od International Organizahon for Standardization. Ten model odniesienia pozwala na opis systemów sieciowych w oparciu o wspólne podstawy. Szczegółowy opis siedmiu warstw tego modelu dostępny jest w wielu tekstach zawierających opisy sieci i nie jest zamieszczony w tej książce.

sieciowych traktowana jest przez IP jako jedna sieć, niezależnie od tego, czy jest to rzeczywiście jeden kabel sieciowy, czy też składa się ona z kilku segmentów połączonych ze sobą przez wzmacniaki, mosty lub przełączniki. Nie powinieneś być zaskoczony, dowiadując się, że numer hosta określa konkretną maszynę, która należy do danej sieci. Na rysunku 1-1 pokazano przykład opisanego wyżej sposobu adresowania.



Rysunek 1 -1: Ethernety 2 i 3 to jedna sieć

Na rysunku 1-1 sieci Ethernet 2 i 3 tworzą jedną sieć IP, mimo że rozdziela je most, co wynika z faktu, że urządzenie takie jak most jest niewidoczne z poziomu protokołów warstwy sieci, jaką jest IP.* Host2, HostS i Host4 mają adresy IP, w których znajduje się taki sam numer sieci przydzielony dla tego podwójnego układu sieci Ethernet połączonych mostem. Łącze szeregowe pomiędzy Host4 a HostS tworzy drugą sieć IP i hosty te będą miały adresy składające się z numeru sieci tworzonej *przez* to połączenie szeregowe. Sieć Ethernet I jest więc trzecią siecią, a Host1 i Host2 będą miały adresy IP zawierające jej adres. Hosty o nazwach Host2 i Host4 mają po dwa adresy IP; są to hosty typu multi-homed i mogą pełnić funkcje ruterów. Dwupoziomowa struktura adresów IP będzie ważna w dalszej części książki, gdy będzie mowa o

*Dokładniejsze wyjaśnienie różnic pomiędzy ruterami a mostami znajduje się w rozdziale 3.

nitowaniu. Na razie wystarczy, jeśli wskażemy, która część adresu IP to numer sieci, a która - numer hosta.

Umieszczenie numeru sieci w adresie IP powoduje, że adres hosta zależy od sieci, w której ten host się znajduje. Oznacza to, że jeśli host zostanie przeniesiony do innej sieci, to konieczna jest zmiana jego adresu.

W przeciwieństwie do innych technologii sieciowych, takich jak IPX Novella, gdzie adres ustalany jest w oparciu o adres sprzętowy karty sieciowej lub AppleTalk firmy Apple Computer, gdzie adres wybierany jest automatycznie, adres IP jest nadawany i wyznaczany ręcznie. Mimo że dostępne są protokoły takie jak *Boot Strap Protocol (BOOTP)* i *Dynamie Host Configuration Protocol (DHCP),* które wspomagają wyznaczanie adresu IP dla maszyny w sieci, to serwery obsługujące te protokoły wymagają ręcznej konfiguracji i nie wszystkie urządzenia w sieci są w stanie wykorzystać zalety tych usług. Konieczność zmiany numeru hosta po zmianie jego miejsca pracy oznacza zawsze dodatkowe zadania dla personelu odpowiedzialnego za utrzymanie sieci.

Numery sieci i maski

Jak napisałem wcześniej, wszystkie adresy IP składają się z numeru sieci i numeru hosta w tej sieci. Jednakże granica pomiędzy numerem sieci i numerem hosta przebiega różnie w każdej z sieci. Aby oprogramowanie ruterów i hostów mogło w łatwy sposób określić, w którym miejscu znajduje się wspomniany podział adresu, każdy z nich ma dołączoną informację w postaci *maski sieci.* Maska ta to liczba 32-bitowa, podobnie jak w adresie IP, w której wszystkie bity określające sieciową część adresu są równe l, a bity określające część adresu będącą numerem hosta ustawione są na 0. Na przykład:

```
11111111  11111111  00000000  00000000
```

oznacza, że pierwszych 16 bitów adresu IP, z którym skojarzona jest ta maska, reprezentuje numer sieci, a ostatnich 16 bitów reprezentuje numer hosta w tej sieci. Komputer może w prosty sposób wyliczyć numer sieci z adresu IP stosując bitowe działanie AND pomiędzy adresem IP i jego maską.

Początkowo maski sieci mogły zawierać nie przylegające bity 1. Praktyka ta została jednak zmieniona, częściowo z powodu trudności, jakie sprawiała, a częściowo po to, by uprościć wymianę informacji o rutowaniu. Obecnie wszystkie maski muszą mieć wszystkie bity l przylegające. Oznacza to, że następująca maska:

```
11111111  11111111  00000011  00000000
```

jest niedozwolona, ponieważ ostatnie dwa bity l nie przylegają do innych. Ograniczenie to nie spowodowało większych kłopotów, ponieważ do chwili jego wprowadzenia używano niewielu masek, w których bity l nie były przylegające.

Podobnie jak adres IP, maska sieciowa jest tradycyjnie reprezentowana przy użyciu zapisu kropkowo-dziesiętnego lub szesnastkowego. A zatem maska może być zapisana jako 255.255.254.0 lub jako OxfffffeOO - ten sposób jest częściej używany w programach komputerowych.

Ponieważ jednak maski zawsze są związane z adresem IP i bez niego nie mają większego znaczenia, coraz popularniejszy staje się nowy format zapisu maski. W związku z tym, że wymagany jest obecnie zapis w postaci nieprzerwanego ciągu bitów l, możliwe jest posługiwanie się pojęciem maski 23-bito-wej. Takie określenie jednoznacznie mówi, że mamy na myśli maskę złożoną z 23 bitów l, po których następuje 9 bitów O lub w zapisie szesnastkowym Oxf f f f f eOO. Pozwala to na uproszczenie stwierdzenia że „sieć rozpoczyna się adresem 192. 168.2.0 z maską 255.255.254.0" i zapisanie go w postaci 192.168.2.0/23. Ten nowy zapis adresów i masek nazywany jest zapisem *adres/maska.* Mimo że większość oprogramowania nie pozwala na użycie tego zapisu przy wprowadzaniu adresu i maski, to coraz częściej pojawia się on przy wyświetlaniu informacji o adresach.

Na przykład aby w bieżącej sesji oglądać informacje o maskach w wybranym formacie w systemie IOS Cisco, należy wydać jedno z poleceń podanych w tabeli 1-1.

Tabela 1-1. Określanie formatu wyświetlania informacji o maskach

Polecenie	*Format wyświetlania*
terminal ip netmask-format bit-count	192.168.2.0/23
terminal ip netmask-format decimal	192.168.2.0 255.255.254.0
terminal ip netmask-format hexadecimal	192.168.2.0 0xFFFFFE00

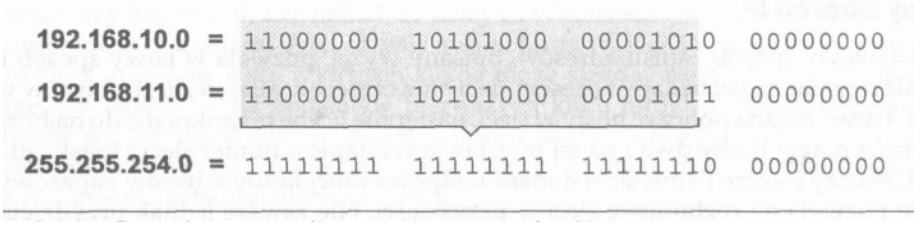
Innym sposobem jest określenie domyślnego formatu wyświetlania maski dla wszystkich sesji poprzez dodanie do konfiguracji rutera następujących poleceń:

```
line con 0
 ip netmask-format  bit-count
 line vty  0  4
 ip netmask-format  bit-count
```

Jeśli wolałbyś nie używać podanego wyżej formatu, to polecenie bit-count możesz zastąpić poleceniem decimal lub hexadecimal.

Podstawowy zapis adres/maska pozwala na opisywanie adresów IP o dowolnym rozmiarze, poczynając od prostego łącza punkt-punkt, w którym pracują dwa hosty w sieci, kończąc na sieciach, w których znajduje się wiele milionów hostów. Rozważmy na przykład dwa adresy pokazane na rysunku 1-2. Ponieważ mają one jednakowy 23-bitowy przedrostek i są kolejnymi numerami, to możliwe jest zapisanie przestrzeni adresowej obu wymienionych adresów przy użyciu wspomnianego zapisu, w wyniku czego powstaje adres w postaci 192.168.10.0/23.

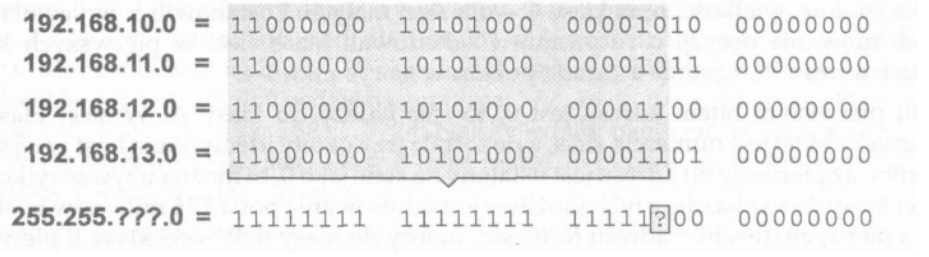
Nie wszystkie kombinacje adresów i masek sieci mogą być poprawnie zapisane przy użyciu takiego zapisu. Na rysunku 1-3 pokazano cztery adresy, które nie mogą być reprezentowane przez jeden zapis typu adres/maska. Dzieje się tak dlatego, że adresy, mimo swej ciągłości, nie mają jednakowego 22-bitowego przedrostka. Dlatego nie jest możliwe podanie maski o długości 22 bitów, która objęłaby wszystkie fe adresy. Jeśli będziesz chciał zapisać te adresy podając 192.168.10.0/22, to zapis ten obejmie tylko dwa z podanych czterech adresów, a dwa pozostałe zostaną pominięte.



Rysunek 1 -2: Dwa adresy ze wspólnym 23-bitowym przedrostkiem

Zamiast takiego zapisu należy użyć dwóch oddzielnych specyfikacji: 192.168.10.0/23 i 192. 168.12 .0/23, co oznacza dwa oddzielne zapisy w tablicy rutowania, o czym powiemy w dalszej części tego rozdziału.

Czy zapis 192.168.10.0/22 określa jakąś poprawną przestrzeń adresową? I tak, i nie. Jeśli użyjesz maski z tym adresem, okaże się, że powstała w ten sposób przestrzeń adresowa jest taka sama jak dla adresu 192.168.8.0/22. Czy w tego rodzaju zapisie ważny jest adres podstawowy? Tak! Nawet doświadczeni administratorzy błędnie sądzą, że opisana w ten sposób przestrzeń adresowa to numery od 192.168.10.0 do 192 .168.13.255, choć komputer na podstawie zapisu 192 .168.10.0/22 wyznaczy



Rysunek 1-3: Cztery adresy bez wspólnego 22-bitowego przedrostka

przestrzeń adresową od 192.168.8.0 do 192 .168.11.255. Są to oczywiście dwie zupełnie inne przestrzenie adresów. Takie błędne zapisy mogą powodować podwójne przydziały adresów, problemy z rutowaniem i inne tajemnicze błędy. Jeśli chcesz tego uniknąć i sprawić, że zapisy będą jednoznaczne, adres podstawowy, maskowany podaną maską, nie może mieć żadnego bitu I w części opisującej numery hostów. Ograniczenie to jest na tyle ważne, że każdy dobrze napisany program sieciowy będzie wymuszał taki właśnie zapis i informował o błędzie adresu w przypadku niezastosowania się do tej reguły.

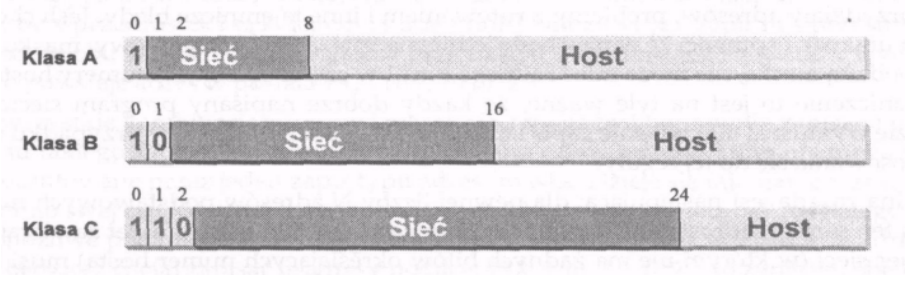
Ogólna zasada jest następująca: dla pewnej liczby *N* adresów podstawowych mających ten sam przedrostek *N* musi być podstawą potęgi 2, a ostatni oktet zawierający numer sieci (w którym nie ma żadnych bitów określających numer hosta) musi być bez reszty podzielny przez *N*.

Klasy adresów IP

Podstawowy sposób zapisu adresów, opisany wyżej, pozwala w łatwy sposób rozróżnić rozmiar części będącej adresem sieci oraz części określającej liczbę hostów w tej sieci. Łatwo można policzyć hosty w sieci, następnie liczbę tę zaokrąglić do najbliższej wartości potęgi liczby dwa i na tej podstawie wystąpić o numer sieci i maskę dla tej sieci. Należy jeszcze pamiętać o dodaniu odpowiedniej liczby adresów zapasowych, które pozwolą na rozbudowę sieci w przyszłości. Nie zawsze jednak przydzielanie adresów sieci odbywało się w taki sposób. W początkowym okresie rozwoju sieci IP maski miały ustalone wielkości, przez co po dodaniu ich do numerów sieci powstawały *klasy* sieci. Choć zastąpiono je bardziej elastyczną architekturą *klas sieci* opisaną wyżej, to w literaturze i w języku potocznym często występują odwołania do nich (czasem także w tej książce). Niektóre protokoły rutowania, takie jak RIP, nadal posługują się tym pojęciem, dlatego cofnijmy się w czasie i zajmijmy się tymi podstawowymi klasami sieci oraz ich ewolucją w kierunku używanej obecnie nowoczesnej architektury klas sieci.

Twórcy IP nie przewidywali, że protokół ten będzie musiał obsługiwać sieć o wielkości dzisiejszego Internetu. Zakładali, że będzie istniała potrzeba obsługi tylko kilku dużych sieci (działających w dużych firmach komputerowych i głównych uniwersytetach), średniej liczby sieci o średniej wielkości oraz wielu małych sieci. Dlatego też stworzyli trzy klasy sieci: klasę A przeznaczoną dla największych sieci, klasę B - dla sieci średniej wielkości oraz klasę C - dla sieci małych. Postanowili również ułatwić podejmowanie decyzji o nitowaniu i zakodowali klasę sieci w pierwszych kilku bitach adresu IP, zgodnie z zasadą pokazaną na rysunku 1-4.

Jeśli pierwszym bitem adresu jest O, to sieć należy do klasy A. W sieci klasy A pierwszy oktet jest numerem sieci, a pozostałe trzy oktety identyfikują host w tej sieci. Ponieważ pierwszy bit adresu jest ustalony na stałe jako O, to można używać tylko 127 sieci klasy A, a w każdej z nich możliwe jest adresowania ponad 16 milionów hostów. Jeśli pierwsze dwa bity adresu to 10, sieć należy do klasy B. W sieci klasy B pierwsze dwa oktety oznaczają numer sieci, a kolejne dwa - numer hosta w sieci. Pozwala to na utworzenie 16 384 sieci klasy B (zwróć uwagę, że podobnie jak w poprzedniej klasie, pierwsze dwa bity są stałe), a w każdej z nich może być 65 000 hostów.



Rysunek 1 -4: Klasa adresu jest zakodowana w pierwszych kilku bitach

Wreszcie jeśli pierwsze trzy bity to 110, sieć należy do klasy C. W sieci klasy C pierwsze trzy oktety są numerem sieci, a ostami oktet określa numer hosta w sieci. Pozwala to na utworzenie około 2 milionów sieci, z których każda może składać się z 256 hostów. Zwróć uwagę, jak łatwo jest na podstawie pierwszych kilku bitów określić klasę sieci, a następnie znaleźć część adresu opisującą numer sieci i część z numerem hosta. Taka prostota była konieczna, ponieważ komputery w tamtych czasach miały znacznie mniejsze moce przetwarzania niż obecnie.

Zgodnie z oryginalną definicją, adresy, w których pierwsze trzy bity to 111, należą do klasy D i zostały przeznaczone do wykorzystania w przyszłości. Od tego czasu definicja sieci tej klasy zmieniła się i klasa D definiowana jest obecnie jako adresy, w których pierwsze cztery bity to 1110. Adresy te nie oznaczają pojedynczego urządzenia, lecz zestaw urządzeń, które wchodzą w skład grupy IP, określanej jako *multicast,* i zostaną omówione w następnej części książki. Adresy rozpoczynające się od 1111 nazywane są obecnie adresami klasy E i są zarezerwowane do wykorzystania w przyszłości. Prawdopodobnie jeśli dla kolejnej klasy adresów zostanie przydzielony jakiś sposób ich wykorzystania, to definicja klas zostanie zmodyfikowana tak, że klasa E będzie się zaczynała od 11110, a nowa zdefiniowana klasa F (jako rezerwa na przyszłość) wyróżniana będzie początkowymi bitami w postaci 11111.*

Jak się więc mają opisane wyżej klasy sieci do swych najnowszych odpowiedników? Zwróć uwagę, że sieć klasy A ma 8-bitową maskę sieci. Oznacza to, że taka sieć o numerze 10.0.0.0 może być opisana jako 10.0.0.0/8 przy użyciu zapisu bezklasowego. Także *naturalna* maska sieci dla sieci klasy B ma długość 16 bitów, a dla sieci klasy C długość ta wynosi 24 bity. W wyniku tak ustalonych długości masek oznaczenie sieci klasy B 172.16.0.0 będzie następujące: 172.16.0.0/16, a dla sieci klasy C o adresie 192.168.1.0-192.168.1.0/24. Należy jednak pamiętać, że choć wszystkie sieci znane wcześniej jako sieci klasy B mają maski 16-bitowe, to nie jest prawdą, iż wszystkie sieci mające maski o długości 16 bitów są sieciami klasy B.[+]

Rozważmy przykład sieci 10.0.0.0/16. Wykorzystuje ona maskę 16-bitową, ale nadal pozostaje siecią klasy A (a raczej częścią takiej sieci), ponieważ jej binarna reprezentacja nadal zaczyna się od bitu 0. Na podobnej zasadzie skonstruowana jest sieć opisana przez 192.168.0.0/16, która nie jest siecią klasy B, lecz zbiorem 256 sieci klasy C. Różnice te mają duże znaczenie, gdy masz do czynienia z hostami i protokołami, które są świadome istnienia klas sieci. W takich przypadkach poprawne konfigurowanie maski jest sprawą niezmiernie istotną dla pracy systemu. W przypadku stosowania adresacji bezklasowej maska 16-bitowa to po prostu maska 16-bitowa.

*Wydaje się, że jest to ostatni sposób na wykorzystanie starej struktury klas dla adresów, ale także w tym przypadku najwłaściwszym określeniem tej klasy będzie przestrzeń adresów *multicast.* Puryści językowi mogą opisywać te adresy jako 244.0.0.0/4 lub odwoływać się do nich jako do adresów z zakresu od 224.0.0.0- 239.255.255.255. Używaj sposobu zapisu, który najbardziej Ci odpowiada. [+] Podobnie jak maska 8-bitowa nie musi wcale oznaczać sieci klasy A, a maska 24-bitowa nie musi oznaczać sieci klasy C.

Podsieci i super sieci

W miarę jak twórcy protokołów IP nabierali doświadczenia w pracy z siecią, odkryli, że ustanowione początkowo klasy sieci pozwalały na przydzielanie sieci o wielkościach, które nie pasowały do potrzeb pojawiających się technologii LAN. Na przykład nie ma potrzeby przydzielać sieci klasy B, dającej możliwość adresowania ponad 65 000 hostów, sieci Ethernet, w której będzie pracowało maksymalnie I 200 urządzeń. Opracowano rozwiązanie nazywane podziałem na *podsieć,* w którym po raz pierwszy rzeczywiście wykorzystane zostały maski sieciowe.

W podsieciach IP bity należące do adresu IP hosta wykorzystywane są w charakterze bitów rozszerzających numer sieci. Na przykład w sieci klasy A I O. O. O. O numer sieci opisany jest przez 8 pierwszych bitów, a pozostałe 24 bity tworzą numer hosta. Twórcy sieci IP zdali sobie sprawę, że możliwy jest podział tej sieci na podsieci dzięki wykorzystaniu kolejnych 8 bitów adresu, które z adresu hosta zostaną przypisane do adresu sieci, jak pokazano na rysunku 1-5. Takie rozwiązanie pozwala stworzyć 256 podsieci, a w każdej z nich zaadresować 65 000 hostów. Możliwe jest również wykorzystanie 16 bitów z numeru hosta dla określenia adresów podsieci, co zwiększa liczbę podsieci do 65 000, a liczbę hostów w każdej z nich do 256.

Maski sieciowe nie muszą przebiegać zgodnie z kolejnymi granicami wyznaczonymi przez 8-bitowe porcje adresu IP. W wielu miejscach używa się takiego rozwiązania, ponieważ sposób podziału adresu na część sieciową i numer hosta jest łatwy do zapamiętania. Jeśli sieci klasy A 10.0.0.0 nie będziemy dzielili na podsieci, podział pomiędzy adresem sieci i adresem hosta przebiega w miejscu pierwszej kropki w zapisanym dziesiętnie adresie. Jeśli użyjemy 8-bitowej podsieci (tzn. 16-bitowej maski sieci), to granica podziału pomiędzy podsiecią a adresem hosta będzie przebiegała w miejscu występowania drugiej kropki. Jeśli z kolei użyjemy podsieci o wielkości 16 bitów (24-bitowej maski sieci), to linia podziału przebiegała będzie w miejscu trzeciej kropki.

Sieć	Podsieć	Host
10		27.9.4
10	27	9.4
10	27.9	4

Rysunek 1-5: Różne interpretacje adresu 10.27.9.4

Choć dla komputerów takie ułatwienia nie mają żadnego znaczenia, to dla ludzi są one bardzo wygodne i pozwalają w bardziej naturalny sposób dzielić adres na poszczególne części. Na przykład jeśli w naszej przykładowej sieci 10.0.0.0 zdecydujemy się użyć maski o długości 10 bitów, to otrzymamy 1024 podsieci, a w każdej z nich po 4 miliony hostów. W takim przypadku granica podziału pomiędzy numerem podsieci a numerem hosta przebiega wewnątrz trzeciego oktetu i nie jest wyraźnie widoczna w zapisie kropkowo-dziesiętnym.

Zastanów się nad adresami 10.1.190.0 oraz 10.1.191.1. Czy należą one do tej samej podsieci? Tak, lecz adres 10 . l. 192. l już nie będzie do niej należał. Nawet szesnastkowy zapis adresu nie pokazuje wyraźnie tego rozdziału. Tylko zapis binarny pozwala na wyraźne rozróżnienie podsieci.

Maska podsieci ma zawsze przynajmniej tyle bitów l, ile jest ich w naturalnej masce dla danej klasy sieci. Oznacza to, że podsieć jest zawsze mniejsza od sieci, bez względu na to, z jakiej klasy ta sieć pochodzi. Kilka lat temu, gdy zaczęły się problemy związane z wyczerpywaniem się przestrzeni adresowej, zwrócono uwagę na fakt, że nie ma technicznego uzasadnienia dla tak sztywnego traktowania masek. Dlaczego nie przydzielać adresów sieci z maskami większymi od naturalnej maski dla sieci klasy C i nie stworzyć bloków kilku sieci C traktowanych jako jedna sieć lub *super sieć?** Właściwie dlaczego ograniczać takie podejście do sieci klasy C? Dlaczego nie połączyć kolejnych sieci klasy B w jedną super sieć?

Takie rozwiązania są podstawą *bezklasowego rutowania pomiędzy domenami (Classless Interdomain Routing - CIDR),* które tworzy stosowaną obecnie w sieci architekturę bezklasową. Dzięki zastosowaniu maski sieciowej do wyznaczania zarówno podsieci, jak i super sieci, powstała nowa grupa *bezklasowych* protokołów rutowania, pozwalająca na rozszerzenie funkcji rutowania, które wcześniej możliwe było tylko pomiędzy sieciami z klas. Protokoły rutowania pracujące z klasami i protokoły bezklasowe nie mogą być ze sobą mieszane, ponieważ te drugie wymagają znajomości maski adresu, podczas gdy protokół klasowy sam określa maskę dla klasy sieci na podstawie pierwszych bitów adresu. Możliwe jest jednak kontrolowane połączenie obu typów protokołów na obrzeżach domeny rutowania. Rozwiązanie takie powinno być jednak stosowane w ostateczności i z pełną świadomością jego konsekwencji.

Adresy broadcast i multicast

Zdarzają się sytuacje, w których host pracujący w sieci IP musi komunikować się ze wszystkimi innymi hostami pracującymi w tej sieci. Ponieważ nie ma łatwego sposobu na stwierdzenie, jakie inne adresy w sieci są przypisane do hostów, a nawet trudno jest stwierdzić, które hosty w danym momencie są uruchomione, to host może wysłać kopię komunikatu na każdy adres w danej sieci po kolei. Jest to marnotrawstwo pasma sieci i mocy pracujących w niej komputerów. Aby poradzić sobie z tym problemem, IP definiuje adres 255.255.255.255 jako adres *broadcast* w sieci lokalnej. Każdy host pracujący w sieci IP odbiera komunikaty przychodzące na jego własny adres IP oraz na adres typu *broadcast.*

Broadcast w sieci lokalnej działa dobrze, jeśli host chce tylko przesłać komunikat do innych hostów połączonych bezpośrednio do tej samej sieci. *Zdarzają,* się jednak sytuacje, kiedy host chce wysłać pakiet do wszystkich hostów, które nie są bezpośrednio połączone z siecią. IP definiuje taki pakiet jako *skierowany broadcast.* Jego adres zawiera numer sieci, do której jest on kierowany, oraz wszystkie bity numeru hosta ustawione na 1.

*Znanej również jako *sieć zagregowana* lub *blok sieci.*

A zatem broadcast skierowany do sieci 10.0.0.0/8 będzie miał adres 10.255.255.255, a w przypadku sieci 172.29.0.0/16 będzie to adres 172.29.255.255. W związku z potencjalnym zagrożeniem ze strony nieuczciwych użytkowników sieci lub ignorantów wiele ruterów może być skonfigurowanych tak, aby odrzucały skierowane pakiety broadcast, nie przepuszczając ich do wnętrza sieci, którą chronią. W rozdziale 10 pokazano przykłady takiej konfiguracji ruterów.

Niektóre wersje starszego oprogramowania stosowały bity O zamiast I dla oznaczania adresów *broadcast.* Pomimo że systemy takie zanikają, możesz się na nie natknąć, zwłaszcza jeśli w Twojej sieci pracują starsze systemy. Większość głównych dostawców systemów UNIX nadal stosuje domyślnie bity O dla oznaczania adresów broadcast. Najnowsze oprogramowanie powinno akceptować oba sposoby adresowania pakietów broadcast i mieć możliwość konfigurowania sposobu adresowania przez bity I lub O przy wysyłanych przez siebie pakietach broadcast. Domyślnym ustawieniem adresu broadcast w nowych systemach jest 1.

Podobnie jak adres broadcast, adres multicast jest pojedynczym adresem reprezentującym grupę urządzeń w sieci. W przeciwieństwie do adresu broadcast, maszyny korzystające z adresu multicast muszą wcześniej wyrazić życzenie otrzymania pakietów kierowanych na ten adres. Komunikat wysyłany na adres broadcast jest odbierany przez wszystkie maszyny obsługujące protokół IP, niezależnie od tego, czy są one zainteresowane jego zawartością, czy też nie. Na przykład niektóre protokoły rurowania wykorzystują adresy multicast jako adres przeznaczenia dla wysyłanych okresowo informacji o rutowaniu. Pozwala to na łatwe ignorowanie takich komunikatów przez maszyny, które nie są zainteresowane uaktualnianiem informacji o rutowaniu. Z kolei broadcast musi być odebrany i przeanalizowany przez wszystkie maszyny, włączając w to hosty, które nie obsługują protokołu IP. Dopiero po odebraniu takiego pakietu maszyna może stwierdzić, czy jest zainteresowana jego zawartością. Wynika to z faktu, że obsługa pakietów broadcast realizowana jest na poziomie sprzętowym i jest związana głównie z funkcją *broadcast IP.* Powoduje to, że pakiet tego typu wysyłany jest do wszystkich kart sieciowych niezależnie od tego, czy obsługuje je protokół IP, czy też inny protokół sieciowy, nie rozumiejący komunikatów broadcast. Hosty pracujące z innym protokołem powinny gubić pakiety broadcast, ale takie działanie wymaga od hosta przetworzenia pakietu w celu potwierdzenia, że nie jest on nim zainteresowany.

Inne adresy specjalne

Należy jeszcze wspomnieć o dwóch specjalnych adresach IP. Pierwszym z nich jest adres *loopback,* 127.0.0.1. Adres ten zdefiniowany jest jako adres programowego interfejsu pętli zwrotnej działającego na danej maszynie. Adres ten nie jest przypisany do żadnego interfejsu sprzętowego i nie łączy się z siecią. Jest używany głównie w celu testowania oprogramowania IP na maszynie, która nie jest przyłączona do sieci, i bez względu na to, czy interfejs sieciowy lub jego sterowniki działają poprawnie.

Może on być również używany na maszynie lokalnej jako adres interfejsu, który jest zawsze aktywny i osiągalny przez oprogramowanie, niezależnie od aktualnego stanu interfejsów sprzętowych. Adres ten może być na przykład używany do adresowania odwołań oprogramowania klienta z serwerem uruchomionym na tej samej maszynie, bez konieczności używania zewnętrznego adresu IP hosta.

Specyfikaq'a protokołu IP, znana jako *Recjuestfor Comment* (w skrócie RFC)*, wymaga aby adres ten, jak i cała sieć 171.0.0.0/8, nigdy nie był przypisywany do zewnętrznego interfejsu maszyny. Jeśli tak się zdarzy, adresy te będą gubione przez każdy host lub ruter, który będzie otrzymywał w taki sposób zaadresowane pakiety.

Zwróć uwagę, iż adres ten narusza zasadę, że adres IP jednoznacznie identyfikuje host, ponieważ wszystkie hosty pracujące w sieci IP wykorzystują ten sam adres dla obsługi interfejsu loopback. :

Drugim specjalnym adresem IP jest 0.0.0.0. Oprócz wykorzystania go w starszym oprogramowaniu jako adresu broadcast w sieci lokalnej, niektóre protokoły rutowania traktują go jako adres przechwytywania lub *domyślną* trasę. Więcej na temat tras domyślnych powiem przy omawianiu algorytmu rutowania IP.

Adresy nadające się do użytku przy danej masce sieci

Do tej pory mówiłem, że w każdej sieci z maską 24-bitową można umieścić do 256 hostów. Nie jest to do końca prawda. Przypomnij sobie, że adres zawierający bity l, w części określającej numer hosta, to adres broadcast. Przypomnij sobie również, że w niektórych starszych implementacjach dla określenia adresu broadcast stosowane są bity 0. W związku z tym adresy zawierające bity l i bity O w części określającej numer hosta nie mogą być stosowane do adresowania hosta w sieci. Daje to rzeczywistą liczbę dostępnych adresów hostów w takiej sieci, która wynosi 254. Takie same restrykcje dotyczą wszystkich sieci i podsieci, niezależnie od długości maski.

Na przykład maska o długości 31 bitów w zapisie szesnastkowym Oxf f f f f f e powinna dać możliwość wydzielenia podsieci, w której będą pracowały dwa hosty, idealnej dla konfiguracji łącza punkt-punkt. Ponieważ jednak nie możemy nadawać hostom numerów złożonych z samych bitów l ani samych bitów O, to sieć utworzona taką maską jest bezużyteczna. Poprawną maską dla sieci, w której będą dostępne dwa adresy hostów, jest maska 30-bitowa -Oxfffffffc. Pierwszy host w sieci będzie miał numer l, a drugi 2. Numer O nie jest dostępny dla hostów, a numer 3 będzie adresem broadcast.

Wyżej opisana niejednoznaczność występuje także w przypadku podsieci, dla których numer podsieci składa się z samych bitów O lub 1. Niektóre wersje oprogramowania sieciowego nie potrafią poprawnie obsługiwać tego typu podsieci. Inne wersje wymagają wyraźnego skonfigurowania funkcji programu, tak by te dwie sieci były obsługiwane poprawnie.

Instrukcja informująca, w jaki sposób uzyskać kopie dokumentów RFC, znajduje się w **dodatku B.**

Na przykład system operacyjny Cisco IOS będzie obsługiwał podsieć O, jeśli zostanie skonfigurowany poleceniem

```
ip subnet-zero
```

wchodzącym w skład konfiguracji protokołu. Nie zachęcam jednak do używania tej możliwości, ponieważ możemy w jej wyniku uzyskać numery podsieci i sieci, które będą nierozróżnialne. Może to nawet spowodować błędy w działaniu dynamicznego protokołu rutowania używanego w Twojej sieci! Jeśli nie masz pewności, czy całe wykorzystywane w Twojej sieci oprogramowanie obsługuje jedną lub obie wymie nione podsieci (wszystkie bity O i wszystkie bity 1), powinieneś unikać stosowania takich numerów podsieci.

W tabeli 1-2 pokazano liczbę podsieci i hostów dla wszystkich masek podsieci w trzech blokach sieci o różnej wielkości. Na przykład jeśli wykorzystywany przez Ciebie blok sieci ma długość 16 bitów, to możesz użyć 25-bitowej maski podsieci w celu uzyskania 510 podsieci i 126 hostów w każdej z nich. Jeśli jednak długość bloku sieci wynosi 20 bitów, to taka sama 25-bitowa maska pozwoli na zaadresowanie 30 podsieci i 126 hostów w każdej z nich. Zwróć uwagę na to, że niektóre maski nie tworzą użytecznej liczby podsieci. Takie przypadki oznaczono za pomocą kreski poziomej. Podobne numery sieci można łatwo podzielić na bloki sieci o innej długo ści. Gdy będziesz się zastanawiał nad wyborem maski dla Twoich podsieci, pamiętaj o przykładach z poniższej tabeli.

Tabela 1-2. Liczba podsieci i hostów w zależności od długości maski i sieci

Liczba bitów	*Maska podsieci*	*Liczba podsieci w bloku sieci*			*Efektywna liczba hostów*
		16 bitów	*20 bitów*	*24 bity*	
16	255.255.0.0	1	-	-	65534
17	255.255.128.0	-	-	-	32766
18	255.255.192.0	2	-	-	16382
19	255.255.224.0	6	-	-	8190
20	255.255.240.0	14	1	-	4094
21	255.255.248.0	30	-	-	2046
22	255.255.252.0	62	2	-	1022
23	255.255.254.0	126	6	-	510
24	255.255.255.0	254	14	1	254
25	255.255.255.128	510	30	-	126
26	255.255.255.192	1022	62	2	62
27	255.255.255.224	2046	126	6	30
28	255.255.255.240	4094	254	14	14
29	255.255.255.248	8190	510	30	6
30	255.255.255.252	16382	1022	62	2
31	255.255.255.254	32766	2046	126	-
32	255.255.255.255	65534	4094	254	-

Adresy prywatne i publiczne

Powiedziałem, że adres IP musi jednoznacznie identyfikować host, ale nie określiłem, w jakim zakresie. Aby adres IP mógł być jednoznacznie używany przez algorytm rutowania w celu określenia trasy do punktu przeznaczenia, musi być jednoznaczny wśród wszystkich sieci osiągalnych z danego hosta, przy wykorzystaniu protokołu IP. Taki zbiór sieci IP jest nazywany *intersieciij*. Najlepiej znanym przykładem inter-sieci jest *Internet*.

W sieci Internet unikalność adresów IP zapewnia system ich przydzielania. Centralna władza administracyjna, znana jako *Internet Registry,* przydziela numer sieci do miejsca, które dołączane jest do sieci Internet. Taki sposób przydzielania adresów gwarantuje, że żadne inne miejsce w sieci nie będzie miało przydzielonego tego samego numeru sieci. Dlatego dopóki jedna organizacja będzie przydzielała różne numery poszczególnym hostom w swojej sieci, każdy adres IP będzie unikalny. Tak więc Internet Registry zapewnia unikalne numery sieci, a użytkownicy tych sieci zapewniają unikalny przydział numerów wewnątrz własnych sieci. Takie globalnie unikalne adresy znane są jako *publiczne adresy IP*.

W związku z ogromnym wzrostem liczby komputerów przyłączanych do sieci Internet istniały obawy dotyczące wyczerpywania się przestrzeni adresowej IP. Toteż ustalono, że pewien zestaw numerów sieci IP zostanie przeznaczony do prywatnego adresowania hostów wewnątrz sieci wchodzących w skład różnych miejsc w Internecie. Sieci te nie są przydzielane przez Internet Registry, lecz można ich używać w każdym miejscu (dołączonym do sieci Internet lub nie), które zdecyduje się wykorzystywać prywatną przestrzeń adresową. Adresy IP muszą być unikalne wewnątrz prywatnej sieci, ale ich unikalność nie jest gwarantowana pomiędzy adresowanymi w ten sposób sieciami prywatnymi. Dwie sieci prywatne mogą bez problemu używać tego samego numeru, a więc przydzielić taki sam adres IP dwóm hostom (każdy z nich pracuje w innej sieci). Ponieważ adresy prywatne nie są unikalne, komunikacja pomiędzy adresowanymi w ten sposób sieciami nie jest możliwa bez odpowiednich uzgodnień administracji tych sieci, dotyczących przydziału poszczególnych numerów hostów. W wyniku skoordynowania przydzielanych w dwóch sieciach adresów prywatnych będziemy mieli do czynienia właściwie z jedną prywatną przestrzenią adresową.

Niektóre przedsiębiorstwa mogą czerpać wiele korzyści z zalet prywatnych przestrzeni adresowych. Są wśród nich przedsiębiorstwa, które raczej nie będą dołączone do Internetu, przedsiębiorstwa mające dużą liczbę maszyn, które wymagają specjalnych warunków bezpieczeństwa i nie powinny być ogólnie dostępne, oraz przedsiębiorstwa, które mają więcej komputerów niż adresów w przyznanej im już przestrzeni adresowej lub przestrzeni, o którą mogą się starać. Przykładem podawanym przez zwolenników prywatnych adresów jest duże lotnisko, na którym monitory wyświetlające informacje o przylotach i odlotach mają przydzielone adresy i są dostępne przez TCP/IP. Jest mało prawdopodobne, by monitory te były dostępne z innych sieci. Innym przykładem jest firma, której przydzielono niewielką przestrzeń adresów, mająca dużą liczbę komputerów w sieci laboratoryjnej lub produkcyjnej.

Komputery te powinny mieć dostęp do wspólnych zasobów korporacji, ale wyjście z nich do sieci zewnętrznych nie jest konieczne, a może być nawet niewskazane.* W takim przypadku prywatne adresy pozwalają zachować ograniczoną publiczną pulę adresową firmy.

Adresy przeznaczone do prywatnego użytku wymienione zostały w tabeli 1-3. Adresy te nie są unikalne w całej sieci Internet, lecz tylko wewnątrz sieci przedsiębiorstwa, które je stosuje. Hosty mające prywatne adresy są w stanie komunikować się ze wszystkimi innymi hostami o adresach prywatnych, działającymi w przedsiębiorstwie, jak również z hostami pracującymi w sieci tego przedsiębiorstwa, które mają adresy publiczne. Hosty te nie mogą jednak komunikować się z hostami pracującymi w sieci innego przedsiębiorstwa. Także hosty z adresami publicznymi mogą komunikować się ze wszystkimi hostami o adresach publicznych, niezależnie od tego, czy pracują one w sieci tego samego, czy innego przedsiębiorstwa, a także z hostami o adresach prywatnych z sieci przedsiębiorstwa. Nie mogą jednak komunikować się z hostami o prywatnych adresach pracującymi w sieci innego przedsiębiorstwa.

Tabela 1 -3. Adresy zarezerwowane jako prywatna przestrzeń adresowa

Początek	Koniec	Zapis bezklasowy
10.0.0.0 172.16.0.0 192.168.0.0	10.255.255.255 172.31.255.255 192.168.255.255	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16

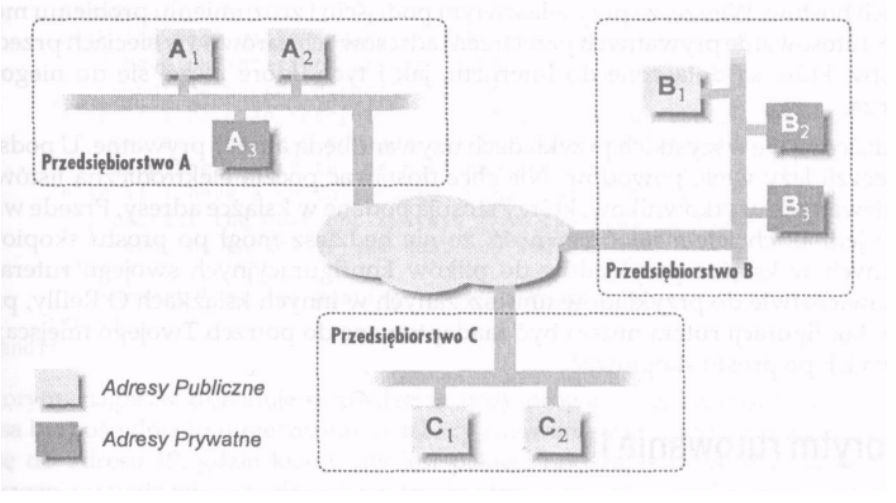
Na rysunku 1-6 pokazano trzy połączone ze sobą przedsiębiorstwa. Przedsiębiorstwa A i B zastosowały adresy z prywatnej przestrzeni adresowej dla niektórych hostów i adresy publiczne dla innych hostów. Przedsiębiorstwo C postanowiło używać tylko adresów publicznych. Hosty adresowane z puli prywatnej w sieci przedsiębiorstwa A, takie jak A3, mogą komunikować się z hostami wewnątrz przedsiębiorstwa A, ale nie mogą komunikować się z żadnym hostem poza siecią A, niezależnie od tego, jak zaadresowane są pracujące tam komputery. Także hosty adresowane z puli prywatnej w sieci przedsiębiorstwa B, takie jak B2, mogą komunikować się z hostami wewnątrz przedsiębiorstwa B, niezależnie od tego, czy mają one adresy publiczne, jak Bl, czy też prywatne, jak B3, ale nie mogą komunikować się z żadnym hostem poza siecią A. Natomiast hosty pracujące w sieci przedsiębiorstwa C, które mają publiczne adresy, mogą komunikować się ze wszystkimi hostami o publicznych adresach pracującymi w trzech przedsiębiorstwach, ale nie mogą komunikować się z adresowanymi z puli prywatnej hostami w przedsiębiorstwie A oraz B.

*Z początku dla prywatnych adresów używano sieci testowej 192.0.2.0/24. Dalsze użycie tych adresów jako stałych adresów w sieciach prywatnych nie jest wskazane. Zamiast tego zaleca się stosowanie adresów zarezerwowanych dla adresowania prywatnych sieci.

Adresy prywatne i publiczne

Należy pamiętać, że adresy prywatne nie są unikalne w sensie globalnym. Na rysunku 1-6 host A3 mógłby mieć ten sam adres IP co host B3. Dlatego każde przedsiębiorstwo, które stosuje adresy prywatne musi postępować zgodnie z określonymi zasadami. Zasady te oraz dodatkowe wskazówki zebrane są w dokumencie RFC 1918. Przedstawię je w skrócie.

- Informacje o rutowaniu sieci prywatnych nie mogą być propagowane przez łącza zewnętrzne przedsiębiorstwa (takie jak łącze z Internetem lub łącze prywatne z siecią innego przedsiębiorstwa).
- Pakiety zawierające adres źródła lub adres przeznaczenia pochodzące z sieci prywatnej nie mogą być przesyłane takimi zewnętrznymi łączami.
- Odwołania pośrednie do takich adresów (takie jak rekordy w tablicach DNS) muszą być przechowywane wewnątrz sieci przedsiębiorstwa.



Rysunek 1-6: Hosty o adresach prywatnych mogą komunikować się tylko z hostami pracującymi w sieci przedsiębiorstwa.

Jeśli chcesz dowiedzieć się więcej na temat zasad stosowania adresów prywatnych zapoznaj się z dokumentem RFC 1918. Wskazówki, jak je zdobyć, znajdują się w dodatku B.

Adresy prywatne należy stosować bardzo ostrożnie. Użycie tego typu adresów ma pewne zalety, np. przestrzeń adresowa znacznie większa niż przestrzeń, jaką przedsiębiorstwo może uzyskać w postaci puli adresów publicznych, oraz większy stopień bezpieczeństwa sieci, w której stosowane są takie adresy. Hosty z adresami prywatnymi nie są całkowicie odporne na atak z sieci, ale przynajmniej znacznie trudniej je zlokalizować i zaatakować spoza sieci przedsiębiorstwa. Stosowanie tego typu adresów nie jest wolne od wad. Podstawową wadą jest konieczność zmiany adresu hosta, gdy chcemy, by z prywatnego stał się on hostem pracującym w sieci o adresach publicznych.

Ponadto należy przedsięwziąć pewne środki ostrożności, by informacje o strukturze prywatnych adresów sieci nie wyciekały na zewnątrz. Kolejną wadą jest konieczność konfigurowania grup hostów pracujących w innej klasie, które będą mogły komunikować się z hostami pracującymi w sieci Internet. Problemów tych można częściowo uniknąć przez zastosowanie serwerów proxy lub funkcji translatora adresów *(Network Address Tmnslator - N AT),* ale należy pamiętać, że rozwiązania te komplikują konfigurację sieci. Mogą tam powstawać błędy konfiguracyjne wpływające na pracę sieci.

Ten ostatni powód doprowadził wielu użytkowników Internetu do wniosku, że nie należy stosować adresów prywatnych. Preferują oni raczej rozwiązanie, które doprowadzi do zlikwidowania problemu wyczerpujących się adresów IP. Choć takie podejście można uznać za właściwe jako rozwiązanie docelowe, to na razie nie ma żadnych rozwiązań, które pomogłyby przedsiębiorstwom rozwiązać problemy z adresacją swoich hostów. Wierzę, że przy właściwym podejściu i zrozumieniu problemu możliwe jest stosowanie prywatnych przestrzeni adresowych zarówno w sieciach przedsiębiorstw, które są dołączone do Internetu, jak i tych, które raczej się do niego nie dołączą.

W książce tej we wszystkich przykładach używane będą adresy prywatne. U podstaw tej decyzji leży wiele powodów. Nie chcę dostawać pocztą elektroniczną listów od zagniewanych użytkowników, którzy stosują podane w książce adresy. Przede wszystkim jednak chciałem mieć pewność, że nie będziesz mógł po prostu skopiować podanych w książce przykładów do plików konfiguracyjnych swojego rutera. W przeciwieństwie do przykładów umieszczanych w innych książkach O'Reilly, przykłady konfiguracji rutera muszą być zaadaptowane do potrzeb Twojego miejsca; nie można ich po prostu skopiować.

Algorytm rutowania IP

W sieci IP każde urządzenie podejmuje samodzielnie decyzje o rutowaniu. Wykorzystywany przy podejmowaniu tych decyzji algorytm jest taki sam, niezależnie od tego, czy jest to host, czy też ruter. Komputer wysyłający informacje nie musi definiować całej drogi prowadzącej przez sieć do punktu przeznaczenia. Musi jedynie wskazać kolejne urządzenie lub *przeskok,* wchodzący w skład pełnej trasy. Następnie pakiet wysyłany jest do wskazanego urządzenia, które jest odpowiedzialne za wskazanie kierunku następnego przeskoku prowadzącego do punktu przeznaczenia. Proces ten jest powtarzany dotąd, aż pakiet będzie ostatecznie dostarczony do urządzenia, do którego był adresowany. Informacje o kolejnych przeskokach w kierunku adresu przeznaczenia przechowywane są w *tablicy rutowania.* Każdy wiersz w tej tablicy opisuje jedną sieć IP, podsieć lub hosta oraz adres kolejnego przeskoku, który tam prowadzi.

Tradycyjne (klasowe) rutowanie IP

Mimo że większość ruterów i wiele hostów potrafi nitować pakiety w bezklasowych sieciach IP, wiele hostów i niektóre rutery nadal używają algorytmu rutowania powiązanego z klasą sieci, w której znajduje się adres przeznaczenia. Ten klasowy algorytm rutowania jest następujący:

```
For a given destination IP address:
if I have a host-specific route for this destination
extract the next hop address from the routing table entry send the packet to the next
hop address else
        determine the network nutnber of the destination if I have an
        interface on that network
                determine the subnet mask for the network from my interface else
                determine the subnet mask for the network from its class endif
        mask the destination address with the mask to get a subnet if I have on
        interface on that subnet
                send the packet directly to the destination else if I have an entry in my
        routing table for the subnet
                extract the next hop address from the routing table entry
                send the packet to the next hop address else if I have a default
        route in my routing table
                extract the next hop address from the routing table
                send the packet to the next hop address else
       report that the destination is unreachable
endif
endif
```

Algorytm najpierw dokonuje sprawdzenia trasy prowadzącej bezpośrednio do hosta. Trasa bezpośrednia to umieszczony w tablicy rutowania zapis, który dokładnie opisuje trasę do adresu IP, gdzie kierowany jest pakiet. Taki zapis może być używany dla wskazania urządzenia pracującego po drugiej stronie szeregowego łącza punkt-punkt.

Jeśli trasa bezpośrednia nie zostanie znaleziona w tablicy rutowania, algorytm próbuje określić maskę podsieci dla sieci przeznaczenia. W przypadku sieci odległych (takich, do których wysyłający pakiety komputer nie jest bezpośrednio dołączony) w tablicy rutowania nie ma informacji o używanej masce podsieci, używana jest więc naturalna maska z klasy sieci. Jeśli mamy do czynienia z połączeniem bezpośrednim do sieci, maska określana jest na podstawie konfiguracji interfejsu sieciowego hosta. Interfejs ten może, lecz nie musi, być dołączony do podsieci, w której znajduje się adres przeznaczenia, ale algorytm zakłada, że maska sieci jest taka sama. W rezultacie nitowanie klasowe nie będzie poprawnie działało w sieci, w której stosowane są różne maski podsieci w różnych obszarach, chyba że sieć taka będzie bardzo starannie skonfigurowana przez administratora, tak by uniknąć niejednoznaczności.

Kiedy algorytm określi maskę podsieci dla sieci, do której wysyłane są pakiety, adres przeznaczenia maskowany jest tą maską w celu uzyskania numeru podsieci, który zostanie użyty jako klucz dla przeszukania tablicy rutowania. Jeśli algorytm stwierdzi, że host jest dołączony bezpośrednio do tej sieci, to pakiet wysyłany jest wprost do adresata. W przeciwnym wypadku tablica rutowania przeszukiwana jest w celu znalezienia rekordu z informacjami o trasie do danej podsieci, a po znalezieniu takiego rekordu określany jest adres kolejnego przeskoku.

Jako ostatnia deska ratunku traktowane jest wyszukanie przez algorytm rekordu z informacją o nitowaniu domyślnym (nazywanego również *ostatnim wyjściem).* Rutowanie domyślne wskazuje zwykle inteligentniejszy ruter (taki, który ma pełniejszą tablicę rutowania), ale może również wskazywać ruter, który jest bliżej głównej sieci IP (rdzenia) niż nadawca.

Jeśli algorytm nie jest w stanie określić kolejnego przejścia, zwraca komunikat o tym, że adres przeznaczenia nie jest osiągalny. Informacja ta wysyłana jest bezpośrednio do programu użytkownika (jeśli komputer wysyłający pakiet nie może znaleźć kolejnego przejścia) lub przy użyciu protokołu *Internet Control Mcssage Protocol (ICMP).*

Bezklasowe rutowanie IP

Wraz z wprowadzeniem super sieci algorytm rutowania musi być uaktualniony tak, by mógł pracować z arbitralnie określoną częścią przestrzeni adresów IP. W każdym wpisie w tablicy rutowania konieczne jest umieszczenie adresu przeznaczenia i adresu kolejnego przeskoku, a także maski, która pozwoli określić wielkość przestrzeni adresowej opisywanej przez ten zapis. Dodanie tej maski do rekordu umieszczanego w tablicy rutowania pozwala na uogólnienie algorytmu rutowania klasowego do postaci algorytmu bezklasowego. Implementacja części wyszukującej w takim algorytmie jest znacznie bardziej skomplikowana niż w przypadku algorytmu klasowego, ale za to sam algorytm jest znacznie prostszy:

```
For a given destination IP address:
search the routing table for the longest prefix march for the address
extract the next hop address Erom the routing table entry
send the packet to the next hop address
if no match was found
report that the destination is unreachable
endif
```

Pierwszą widoczną różnicą jest fakt, że algorytm ten jest znacznie prostszy i mniej szczegółowy od algorytmu działającego w oparciu o sieci z klas. Umieszczenie masek sieci w tablicy rutowania pozwala redukować większość z działań nietypowych, koniecznych do wykonania w algorytmie klasowym. Na przykład trasy do hosta są w tym algorytmie zapisami z maską 255.255.255.255. Ponieważ takie 32-bitowe maski zawsze odpowiadają adresom przeznaczenia o przedrostku dłuższym niż jakakolwiek podsieć, sieć lub super sieć, są one zawsze preferowane przed mniej jednoznacznymi trasami, podobnie jak to miało miejsce w przypadku algorytmu klasowego.

Także trasa domyślna, jeśli istnieje, zapisana jest w postaci rekordu z adresem przeznaczenia 0.0.0.0 i maską 0.0.0.0. Jeśli maska ta zostanie użyta w stosunku do dowolnego adresu przeznaczenia, wynikiem będzie zawsze 0.0.0.0, co odpowiada adresowi przeznaczenia umieszczonemu w tym rekordzie. Powstały w ten sposób przedrostek będzie jednak zawsze krótszy niż jakakolwiek inna określona trasa, która może prowadzić do danej sieci, podsieci lub super sieci, co powoduje, że trasa ta pozostaje nadal trasą wybieraną na samym końcu.

Przydatną konsekwencją wymagania dotyczącego „najdłuższego dopasowania" jest możliwość umieszczenia w tablicy rutowania mniej określonej trasy, prowadzącej na przykład do super sieci oraz lepiej określonej trasy prowadzącej do podsieci. Obie te trasy prowadzą do adresu przeznaczenia pakietów, ale mają inny adres kolejnego przeskoku. Pozwala to na użycie jednego zapisu trasy prowadzącej do większości super sieci i dodanie zapisów tras, które zapełnią dziury w nitowaniu wynikające z tego ogólnego zapisu. Jest to wprawdzie przydatne, lecz należy unikać tworzenia zbyt dużej liczby dziur w bloku sieci lub bloku adresów, ponieważ nie pozwalają one na stworzenie małych, wydajniej pracujących tablic rutowania. Pamiętaj o tym, że jeśli masz dziury w bloku sieci lub w bloku adresów, to poza zapisami w tablicy rutowania, definiującymi trasę do super sieci lub sieci, musisz dopisać trasy odnoszące się do każdej z tych dziur.

Ostatnią zaletą dodawania do tablicy rutowania informacji o maskach jest to, że pozwala ono na ustalanie masek podsieci o różnej długości w różnych częściach sieci. Nadal trzeba pamiętać o sprawdzeniu, czy zdefiniowane w ten sposób maski nie powodują niejednoznaczności i pokrywania się sieci. Nie musisz już jednak opracowywać topologii sieci w taki sposób, aby zapobiegać dwuznacznym zapisom w tablicy rutowania, które powstają w wyniku różniących się masek podsieci. Technika przydzielania masek podsieci o zmiennej długości *(Variabk-Length Subnet Masks -VLSM)* zostanie omówiona w rozdziale 3.

Utrzymywanie tablicy rutowania

Ponieważ każde urządzenie w sieci IP przesyła pakiet IP do punktu kolejnego przejścia (bez zapamiętywania całej trasy tego pakietu), aż do punktu przeznaczenia, wszystkie urządzenia, a zwłaszcza wszystkie rutery, muszą na bieżąco tworzyć sobie obraz tras prowadzących w każdym z kierunków. Innymi słowy, najważniejsza jest synchronizacja tablic rutowania pomiędzy współpracującymi ze sobą ruterami. Aby zrozumieć, dlaczego jest ona niezbędna, rozważmy przypadek, w którym ruter A i ruter B wierzą, że ten drugi jest poprawną trasą kolejnego przeskoku do adresu przeznaczenia 10.0.0.1. Kiedy ruter A odbierze pakiet przeznaczony dla 10.0.0.1, prześle go do rutera B. Ruter B z kolei przejrzy swoją tablicę rutowania i stwierdzi, że ruterem kolejnego przeskoku dla tego adresu jest ruter A, po czym odeśle pakiet do tego rutera. W rezultacie otrzymamy *pętlę rutowania,* którą mogą tworzyć więcej niż dwa rutery.

Synchronizacja tablic rutowania może być wykonywana kilkoma metodami. Najprostszą do opanowania i wdrożenia jest rutowanie *statyczne.* W rutowaniu statycznym każdy z ruterów jest ręcznie konfigurowany, a do jego tablicy wpisywana jest lista adresów przeznaczenia i informacja o adresie kolejnego przejścia dla tych adresów.

W takim przypadku tablica rutowania jest przechowywana w pliku konfiguracyjnym, umieszczonym na trwałym nośniku. Zadaniem administratora sieci jest upewnienie się, czy wszystkie tablice rutowania współpracujących ze sobą ruterów są spójne. To administrator musi sprawdzić, czy nie powstały jakieś pętle rutowania, a także czy wszystkie kierunki są osiągalne ze współpracujących ruterów.

Prostota konfiguracji rutowania statycznego odnosi się do sieci, z których pakiety wychodzą do niewielu punktów lub do sieci końcowych, które mają tylko jedno lub dwa połączenia z resztą sieci. Jednak i ta konfiguracja nie jest pozbawiona wad. Najważniejszą z nich jest to, że rutowanie statyczne nie potrafi adaptować konfiguracji sieci do uszkodzeń, które w niej występują, ani też wykorzystywać zalet istnienia trasy alternatywnej prowadzącej do punktu docelowego. Ponadto kiedy liczba kierunków wysyłania pakietów, a także liczba ruterów, wzrośnie, uaktualnianie tablic rutowania przy zmianie topologii sieci staje się trudne i czasochłonne.

Elastyczniejsze rozwiązania stosują protokoły rutowania pozwalające ruterom na dynamiczne tworzenie tablic rutowania w oparciu o informacje przesyłane z innych ruterów pracujących w sieci. Opracowano i wdrożono wiele takich protokołów.
W kolejnych rozdziałach będziemy mówili o kilku z nich. Mówiąc ogólnie, rutery rozmawiają ze sobą stosując protokół, który potrafi dynamicznie ustalać bieżącą topologię sieci. Na podstawie tych informacji każdy z ruterów ustala rutery (jeden lub więcej) kolejnego przejścia do danego punktu przeznaczenia próbując określić najlepszą trasę. Jeśli nic nie będzie zakłócało komunikacji pomiędzy ruterami i jeśli wszystkie z nich będą poprawnie stosowały wspomniany protokół, to obliczą pasujące do siebie tablice rutowania. .;

Pomiędzy krańcowo różnymi rozwiązaniami, jakimi są rutowanie statyczne oraz rutowanie dynamiczne, istnieje wiele rozwiązań, które są połączeniem zalet funkcji dynamicznych i funkcji statycznych. Takie hybrydowe sposoby rutowania pozwalają znaleźć rozwiązanie mające zalety elastyczności rutowania dynamicznego i prostoty rutowania statycznego. Na przykład rutery pracujące w sieci mogą używać rutowania dynamicznego, a hosty przyłączone do pojedynczych sieci mogą mieć skonfigurowaną trasę domyślną. Możliwe jest również takie skonfigurowanie rutera, aby miał on w tablicy kilka tras statycznych, prowadzących na przykład do obszarów sieci znajdujących się poza kontrolowaną przez administratora domeną, oraz *rozgłaszał* trasy do innych ruterów, wykorzystując dynamiczny protokół rutowania. Niezależnie od wybranego schematu rutowania, rozwiązania oparte o rutowanie dynamiczne ograniczone są do sprzętu, znajdującego się pod bezpośrednią kontrolą administratora sieci. Taki protokół może być również stosowany w przypadku ruterów na granicach sieci, w których znajdują się grupy maszyn używających rutowania statycznego. A oto moja rada:

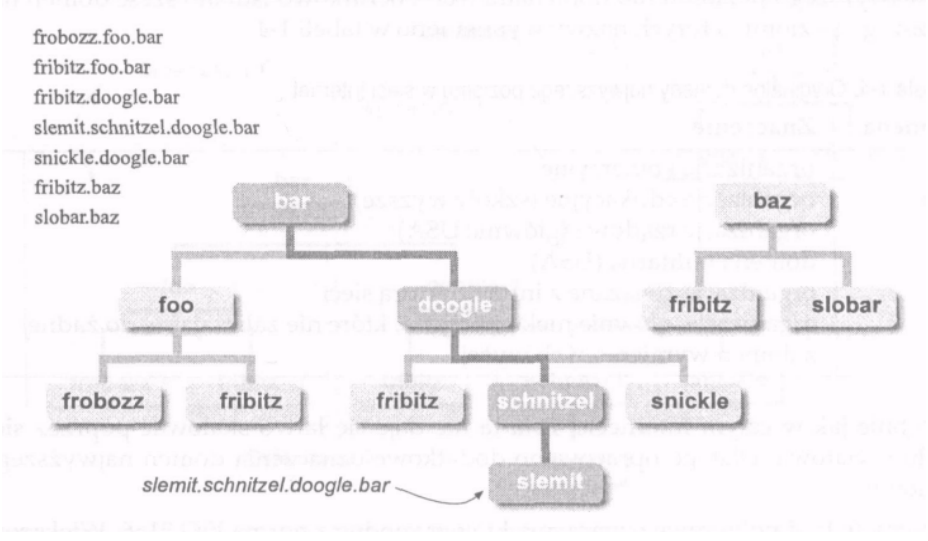
- Używaj rutowania statycznego, kiedy tylko jest to możliwe.
- Stosuj rutowanie dynamiczne tylko wtedy, gdy musisz.

Nazwy domen i System Nazw Domen (DNS)

Dotychczas pisałem tylko o adresach IP. Adresy takie są dobre dla komputerów, ponieważ są krótkie i zapisane w postaci numerycznej, ale taka postać jest trudna do zapamiętania i stosowania dla ludzi. Większość z nas jest w stanie zapamiętać kilka tuzinów różnych numerów. Pracuje się nam jednak znacznie lepiej z nazwami; łatwo potrafimy zapamiętać setki różnych nazw. Dlatego maszyny pracujące w sieciach IP mają swoje nazwy, które są powiązane z adresami IP.

Struktura Systemu Nazw Domen

Na początku nazwy komputerów przydzielane były z płaskiej przestrzeni adresowej, ponieważ konieczne było nazwanie kilkuset komputerów. Główna lista nazw przechowywana była w centralnym rejestrze w postaci pliku. Jednak w związku z rozrastaniem się sieci Internet rejestr centralny nie był w stanie nadążyć z dodawaniem, zmianą i usuwaniem nazw. Ponadto zaczęły się problemy ze znalezieniem unikalnej nazwy dla nowej maszyny w sieci. Toteż inżynierowie działający w Internecie opracowali nową hierarchiczną przestrzeń nazw, nazywaną Systemem Nazw Domen *(Domain Name System - DNS)*. DNS pozwala na przydzielenie odpowiedzialności za część przestrzeni nazw określonej grupie, która może następnie delegować kawałek swej części do innej grupy.



Rysunek 1 -7: Nazwy domen przedstawione w postaci drzewa

W DNS wszystkie nazwy składają się z zestawu słów, znanych jako *etykiety,* które oddzielone są kropkami. Dla ułożenia nazwy określonego hosta można użyć dowolnej liczby etykiet, w praktyce większość organizacji używa od trzech do sześciu etykiet.

Etykiety te tworzą układ drzewa, w którym etykieta znajdująca się po prawej stronie pełnej nazwy oznacza korzeń drzewa, a każda kolejna etykieta, patrząc od strony prawej do lewej, oznacza kolejną gałąź z coraz niższej warstwy. Na rysunku 1-7 pokazano kilka nazw domen i wynikające z nich struktury drzew.

Zwróć uwagę, że etykieta f r i b i t z pojawia się trzy razy: dwukrotnie w różnych miejscach drzewa ba r i raz w drzewie baz. Przykład ten przedstawia sposób, w jaki DNS rozwiązuje problem kolizji nazw. Jedna etykieta musi być unikalna tylko wśród nazw nadawanych na tym samym poziomie jednego z drzew.

Odpowiedzialność za obsługę nazw w DNS może być delegowana do innej organizacji na poziomie każdej gałęzi drzewa, ale nie jest to konieczne. Na przykład na rysunku 1-8 widzimy, że obsługa nazw delegowana została z Organizacji I do Organizacji 2 na poziomie gałęzi do o g l e, ale nie spowodowało to oddelegowania nazw na poziomie gałęzi *f o o*. Organizacja 2 delegowała obsługę gałęzi s c h n i t żel do Organizacji 3, ale pozostawiła sobie gałęzie *f r i b i t z* i *s n i c k l e*. Organizacja 4 postanowiła nie delegować nikomu obsługi żadnej z gałęzi swego drzewa. Możliwość delegowania obsługi części przestrzeni nazw pozwala na większą skalowalność procesu rejestracji nazw. Zamiast tworzyć centralną instytucję obsługującą rejestrację wszystkich nazw hostów, funkcje te przekazuje się lokalnym rejestratorom, których zadaniem jest przydzielanie nazw hostom pracującymi w danej organizacji.

Na rysunku 1-8 korzenie dwóch drzew mają nazwy b a r i b a z. Nazywa się je domenami najwyższego poziomu lub domenami *root.* Początkowo istniało sześć domen najwyższego poziomu, których nazwy wymieniono w tabeli 1-4.

Tabela 1-4. Oryginalne domeny najwyższego poziomu w sieci Internet

Domena	Znaczenie
com	organizacje komercyjne
edu	organizacje edukacyjne (szkoły wyższe)
gov	organizacje rządowe (głównie USA)
mil	domena militarna (USA)
net	organizacje związane z infrastrukturą sieci
org	organizacje, głównie nie komercyjne, które nie zaliczają się do żadnej z domen wymienionych wyżej

Podobnie jak w całym Internecie, lista ta nie daje się łatwo skalować poprzez sieć ogólnoświatową. Dlatego opracowano dodatkowe oznaczenia domen najwyższego poziomu.

Domeny te to dwuliterowe oznaczenia krajów zgodne z normą ISO 3166. Większość użytkowników spoza USA rejestruje swoje nowe domeny i przenosi domeny zarejestrowane wcześniej do nowych domen narodowych. Niektóre kraje wymagają, by ich mieszkańcy używali takich nazw domen, tak więc pierwszych sześć domen pozostawiono dla użytkowników w USA, choć istnieje również domena narodowa tego państwa - US.

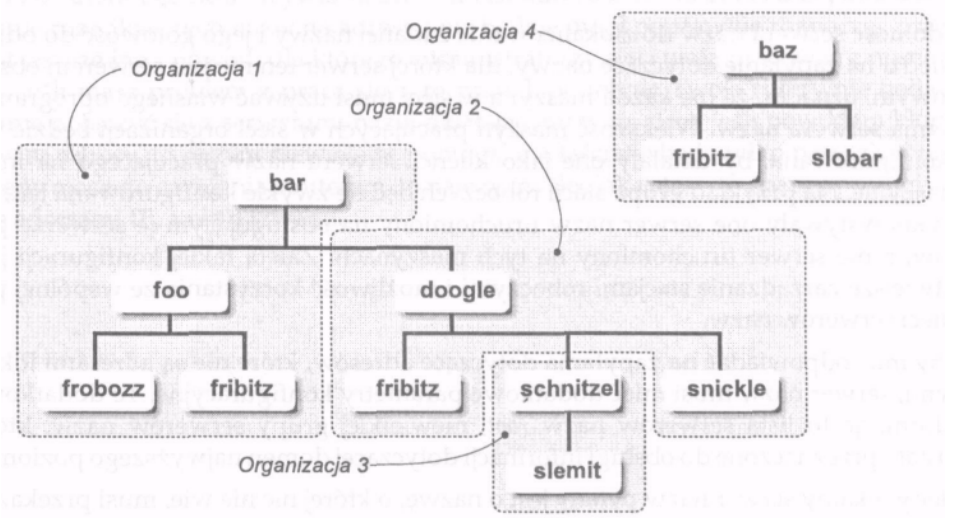
Podejmowane w Internecie działania doprowadziły do utworzenia listy proponowanych siedmiu dodatkowych ogólnych domen (w książkach oznacza się je często jako gTLD). Nazwy nowych domen oraz obszary działalności, dla których będą one stosowane, podano w tabeli 1-5.

Tabela 1-5. Ogólne domeny najwyższego poziomu (propozycja) **Domena**

Z

firm	działalność gospodarcza, firmy
storę	sklepy w sieci Internet
web	miejsca związane z działalnością w zakresie WWW
arts	miejsca związane z działalnością w zakresie kultury
rec	miejsca związane z działalnością w zakresie turystyki i wypoczynku
info	miejsca pełniące funkcje informacyjne
nom	miejsca wymagające indywidualnych lub prywatnych systemów nazw

Te nowe domeny nie zostały jeszcze uruchomione. Wybrano już organizacje odpowiedzialne za rejestrację adresów w tych domenach i trwa uzgadnianie ostatnich szczegółów związanych z tą działalnością. Dla tych, którzy są zainteresowani ostatnimi informacjami na temat zaawansowania prac nad tym projektem, podaję adres WWW: *http://www.iahc.org*.



Rysunek 1 -8: Odpowiedzialność za dowolną gałąź drzewa może być delegowana do innej organizacji

Serwery nazw domen

W przeciwieństwie do oryginalnego rozwiązania, jakim była tablica hostów, DNS ni działa w oparciu o statyczny plik umieszczony na każdej z maszyn w sieci, pozwala jacy na zamianę nazwy na adres IP. Zamiast tego w sieci IP znajdują się hosty pełniąc funkcję *serwerów nazw.* Żaden serwer nie ma pełnej kopii bazy nazw hostów z danej domeny. Zwykle każda organizacja umieszcza w sieci jedną maszynę, która pełń funkcję serwera nazw dla tej domeny i, jeśli to możliwe, dla innych domen, które t; organizacja zgodziła się obsługiwać. Komputery te posiadają wszystkie informacji dotyczące części systemu nazw domen, za który odpowiadają, oraz zapamiętuj; informacje, które uzyskały w wyniku rozwikłania innych nazw za pomocą innych serwerów nazw.

Kiedy serwer nazw odbierze z domeny, którą obsługuje, zapytanie dotyczące nazw hosta, to odpowiada na nie od razu (jeśli wysłane zostało ono przez program działający na innym serwerze lub przez klienta). Jeśli pytanie dotyczy nazwy z domeny której serwer nie obsługuje, to wysyła on zapytanie do innych serwerów nazw, ; następnie przekazuje klientowi wyniki tych poszukiwań. Umieszcza także kopii odpowiedzi w swojej pamięci na czas określony przez serwer, od którego uzyskał t< informacje. Jeśli po pewnym czasie jakiś inny program lub komputer z sieci zapyta (tę samą nazwę, a przechowywana w pamięci informacja nie uległa przedawnieniu, te serwer nazw odpowie na takie zapytanie sam, bez łączenia się z innymi serwerami nazw. Taki algorytm udzielania odpowiedzi powoduje znaczne zmniejszenie ruchu w sieciach pomiędzy serwerami nazw.

Zdolność serwera nazw do zlokalizowania żądanej nazwy i jego gotowość do odpowiedzi na zapytanie dotyczące nazwy, dla której serwer ten nie jest serwerem obsługowym, oznacza, że nie każda maszyna w sieci musi używać własnego oprogramowania serwera nazw. Większość maszyn pracujących w sieci organizacji będzie tal skonfigurowana, by działały one jako klienci serwera nazw pracującego na inne maszynie. Na przykład grupa stacji roboczych będzie zwykle konfigurowana tak, b) wykorzystywały one serwer nazw uruchomiony na obsługującym je serwerze plików, a nie serwer uruchomiony na tych maszynach. Zaletą takiej konfiguracji jest łatwiejsze zarządzanie stacjami roboczymi i możliwość korzystania ze wspólnej pamięci serwerów nazw.

Aby móc odpowiadać na zapytania dotyczące adresów, które nie są adresami lokalnymi, serwer nazw musi mieć dodatkowe parametry konfiguracyjne. Te dodatkowe informacje to lista serwerów nazw *root,* niewielkiej grupy serwerów nazw, które zostały przeznaczone do obsługi informacji dotyczącej domen najwyższego poziomu,

Kiedy lokalny serwer nazw pytany jest o nazwę, o której nic nie wie, musi przekazać to pytanie do jednego z serwerów root, skąd uzyska odpowiedź. Odpowiedzią tą będzie lista serwerów wyznaczonych do obsługi domen najwyższego poziomu, które posiadają poszukiwane informacje. Następnie serwer lokalny, po umieszczeniu odebranej listy serwerów w pamięci, wysyła zapytanie do jednego z tych serwerów z prośbą o rozwikłanie nazwy. Zapytany serwer może odpowiedzieć na pytanie, jeśli posiada potrzebne informacje. Jeśli ich nie ma, przekazuje pytanie do serwera niższego poziomu, który udziela odpowiedzi.

Może również, jeśli zajdzie taka potrzeba, zapytać serwer uzupełniający i wysłać do klienta odpowiedź.

Zdolność serwera nazw do zlokalizowania serwera, który może udzielić odpowiedzi na zapytanie dotyczące rozwikłania danej nazwy, bez konieczności specjalnej konfiguracji uwzględniającej strukturę sieci w odległym miejscu, oznacza, że każda organizacja ma prawie całkowitą niezależność, jeśli chodzi o decyzje dotyczące struktury nazw i delegowania obsługi części tej struktury do poszczególnych serwerów. O fakcie delegowania obsługi nazw muszą wiedzieć tylko serwery, które tę obsługę delegują. Dzięki tej autonomii i przezroczystości pełnionych usług dla końcowego użytkownika DNS jest chyba największą i najskuteczniejszą rozproszoną bazą danych na świecie.

Czytelnicy zainteresowani szczegółami dotyczącymi protokołu DNS powinni przeczytać dokumenty RFC 1034 oraz RFC 1035, które w pełni definiują ten system. Ci, którzy są zainteresowani obsługą i działaniem serwera nazw, powinni przeczytać książkę DNS *and Bind* (wydaną przez wydawnictwo O'Reilly).

Większość administratorów sieci posługuje się adresami sieciowymi, a nie nazwami hostów. Konfiguracja rutera *zawsze* powinna być wykonana w oparciu o adresy IP. Choć nazwy są łatwiejsze do zapamiętania i do stosowania, należy pamiętać, że ruter często czyta konfigurację dużo wcześniej, zanim serwer DNS będzie dostępny w sieci. Może to wynikać z faktu, że serwer nazw nie został jeszcze uruchomiony lub że ruter nie nauczył się jeszcze trasy do sieci, w której taki serwer pracuje. Jeśli w konfiguracji swego rutera będziesz używał nazw zamiast adresów IP, to ruter może nie być w stanie rozwikłać tych nazw na adresy i nie będzie mógł poprawnie rozpocząć pracy. Jest jeszcze inny powód, dla którego administratorzy sieci wolą pracować z numerami: jeśli masz problem z pracą sieci, to prawdopodobnie Twoje rutery nie będą w stanie połączyć się z serwerami nazw działającymi w tej sieci. Jeśli powodem kłopotów są adresy, to nazwy niewiele tu pomogą, a właściwie będą tylko przeszkadzały. Kiedy masz do czynienia z ruterem, to należy myśleć jak ruter - to znaczy posługiwać się adresami IP, a nie nazwami.

Projektowanie sieci - część 1

2

Określenie celów - najważniejszy pierwszy krok
Architektura sieci - jak to wszystko ze sobą współpracuje
Wybór medium - co z czym połączyć?
Fizyczna topologia sieci

Rozdział ten rozpoczyna tematykę dotyczącą projektowania sieci. Omówimy tu takie tematy jak: architektura sieci, wybór medium transmisyjnego oraz fizyczna topologia sieci. W kolejnym rozdziale będziemy kontynuować tę tematykę, rozpoczynając od analizy miejsc w sieci, w których należy umieścić rutery. Następne rozdziały zawierają informacje na temat doboru sprzętu i wyboru protokołu rutowania.

Jeśli masz już sieć komputerową, być może zadajesz sobie pytanie, po co tracić czas na czytanie rozdziału omawiającego projektowanie sieci. Przecież nie zamierzasz tworzyć nowej sieci, lecz zarządzać pracą sieci już istniejącej. Tylko niewielu administratorów ma tyle szczęścia, że może tworzyć własną sieć od podstaw. Tobie pozostaje niestety ciągłe dopracowywanie swojej sieci, tak aby jej konfiguracja była możliwie zbliżona do ideału. Proces doskonalenia sieci pozwoli Ci zrozumieć, co tak naprawdę chcesz osiągnąć, i zlikwidować ograniczenia wynikające z konfiguracji sieci, z którą obecnie pracujesz. Gdy już będziesz wiedział, jak ma wyglądać Twoja sieć, będziesz mógł wrócić do punktu wyjścia i rozpocząć adaptowanie tego ideału do realiów istniejącej sieci, biorąc pod uwagę inne ograniczenia, takie jak czas i pieniądze.

Kiedy skończysz, będziesz miał gotowe dwa rozwiązania. Pierwszym z nich będzie idealna sieć, a drugim sieć, którą możesz mieć w rzeczywistości. Obydwa są bardzo ważne. Projekt uwzględniający warunki, w jakich pracujesz, zawiera rozwiązania, które należy zastosować, tak aby sieć dobrze działała. Wyraźnie definiowane wymagania pomogą Ci podjąć decyzje dotyczące elementów sieci.

Do podjęcia niektórych z nich będziesz po prostu zmuszony. Projekt sieci idealnej jest ważny z innego powodu. Pomoże Ci podejmować decyzje, które nie są podyktowane realiami. Na przykład jeśli będziesz musiał wybrać opcję A lub B, z których opcja A odpowiada rozwiązaniu zastosowanemu w idealnej sieci A, a opcja B - nie, to oczywiście powinieneś wybrać A. Ważne są również różnice pomiędzy obydwoma projektami (idealnym i rzeczywistym). Pomagają one zauważyć kompromisy, na które poszedłeś. Na przykład jeśli idealna sieć obsługuje tylko Token Ring, a Ty potrzebujesz również obsługi istniejącej w dziale sieci LAN wykonanej w technologii Ethernet, to oczywiste jest, że nie będziesz instalował nowej sieci Ethernet. Zamiast tego Twoje działania powinny zmierzać do wyeliminowania starego rozwiązania, którego podstawą jest Ethernet.

Określenie celów - najważniejszy pierwszy krok

Pierwszym etapem działań związanych z projektowaniem sieci powinno być określenie celów, jakie sobie stawiasz. Powinny one dotyczyć następujących kluczowych elementów:

- Funkcjonalność - co sieć powinna robić?
- Niezawodność - jak dobrze powinna spełniać swoje funkcje?
- Dostępność - gdzie i w jakim zakresie będzie dostępna i jak długo będzie pracowała?
- Elastyczność - jak łatwo będzie zaadaptować ją do zmieniających się wymagań?
- Koszt - ile będzie kosztowało jej stworzenie i obsługa?

Do kosztów należy zaliczyć zarówno początkowe wydatki, jak i koszty kolejnych zmian w sieci. Te z kolei można podzielić na koszt sprzętu, oprogramowania, obsługi i utrzymania personelu. Choć nie jest konieczne wymienianie wszystkich kosztów jako jednego z elementów celu, jaki sobie zakładasz, to należy pamiętać, że nie wolno zaniedbać żadnego z nich.

Na żadne z pytań postawionych wyżej nie ma jednoznacznej odpowiedzi. Zamiast koloru czarnego i białego kryteria te tworzą raczej odcienie szarości. Ponadto nie są one całkowicie od siebie niezależne. Zwykle gdy zwiększa się koszt rozwiązania, można poprawić jeden, a nawet wszystkie składniki. Na przykład jeśli jesteś w stanie wydać więcej pieniędzy, możesz zbudować sieć o większej funkcjonalności, wyższym poziomie niezawodności i tak dalej. Jednak musisz pamiętać, że niektóre z tych kryteriów wzajemnie się wykluczają. Jeśli chcesz zwiększyć funkcjonalność, na przykład przez wprowadzenie obsługi dodatkowych protokołów, możesz to zrobić kosztem dostępności i niezawodności sieci. Uruchamiając drugi bądź trzeci protokół transportu danych możesz zwiększyć niestabilność sieci poprzez błędy w oprogramowaniu lub błędy wynikające z większego skomplikowania konfiguracji sieci. Możesz oczywiście przywrócić dostępność i niezawodność sieci zwiększając wydatki, budując na przykład całkowicie oddzielną strukturę rurowania dla każdego z pracujących w sieci protokołów.

Niemożliwe jest jednak osiągnięcie idealnego stanu we wszystkich wymienionych kategoriach, w każdym razie nie za rozsądną cenę.

Po określeniu celów, jakie ma spełniać Twoja sieć, a także zadań, jakie trzeba wykonać przy jej projektowaniu, musisz je zmodyfikować na podstawie już istniejącego systemu, który ma obsługiwać Twoja sieć. Zwykle istniejący system zmusza do rozszerzenia lub uogólnienia stawianych sieci celów. Na przykład jeśli Twoja sieć ma obsługiwać używany obecnie protokół, który nie jest oparty o IP, to musisz rozszerzyć funkcjonalność opracowywanego rozwiązania. Jak wykazałem wcześniej, działanie takie może spowodować spadek niezawodności i dostępności, jeśli nie możesz zwiększyć wydatków.

Gdy Twoje cele zostały przystosowane do istniejącego systemu i gdy uwzględniłeś inne ograniczenia, powinieneś zająć się dwoma rozwiązaniami. Pierwszym jest Twoja idealna sieć, a drugim sieć, jaka zadziała w rzeczywistości. Pamiętaj, że oba są ważne. Pierwszy jest celem końcowym, a drugi przedstawia prawdziwe działające rozwiązanie. W trakcie całego procesu tworzenia sieci należy pamiętać o obydwu rozwiązaniach. Jeśli kiedykolwiek napotkasz dwa lub więcej rozwiązania, które spełniają cele sieci rzeczywistej, to o wyborze jednego z nich powinno zdecydować wymaganie stawiane w rozwiązaniu idealnym. Toteż gdy w przyszłości będą znikać ograniczenia, które powodowały modyfikację Twojego idealnego rozwiązania, będziesz bliżej rozwiązania idealnego.

Architektura sieci - jak to wszystko ze sobą współpracuje

Kiedy znane są cele, jakie chcesz osiągnąć, możesz przystąpić do opracowania architektury sieci. Poprawnie zaprojektowana sieć składa się z trzech głównych komponentów:

- rdzenia
- punktów dystrybucyjnych
- punktów dostępu.

Rdzeń jest rodzajem kręgosłupa sieci, do którego dołączone są poszczególne elementy sieci. W środowisku sieci LAN lub sieci kampusowej jest to struktura zapewniająca dużą szybkość przesyłania danych i niezawodność. Użytkownicy sieci nie są bezpośrednio dołączani do jej rdzenia. W sieciach typu WAN rdzeń sieci tworzony jest zwykle w oparciu o długodystansowe, superszybkie łącza. Będzie to system rutowania o dużej szybkości i jako taki powinien - oprócz funkcji szybkiego podejmowania decyzji o rutowaniu - spełniać kilka innych wymagań. Jeśli w tej części sieci pojawią się problemy, będą miały wpływ na pozostałe części Twojej sieci.

Drugim elementem sieci jest system dystrybucyjny. W zależności od rozmiaru sieci może to być system kabli przyłączeniowych, łącza między budynkowe, a nawet krótko- i długodystansowe łącza sieci WAN. System dystrybucyjny łączy opisany niżej system dostępu z rdzeniem sieci. W sieci LAN system dystrybucyjny może mieć dowolną szybkość przesyłania danych, uzależnioną od wybranego medium transmisyjnego, ale zwykle jego prędkość i niezawodność waha się między wartościami osiąganymi w rdzeniu a wartościami uzyskanymi w elementach dostępowych sieci.

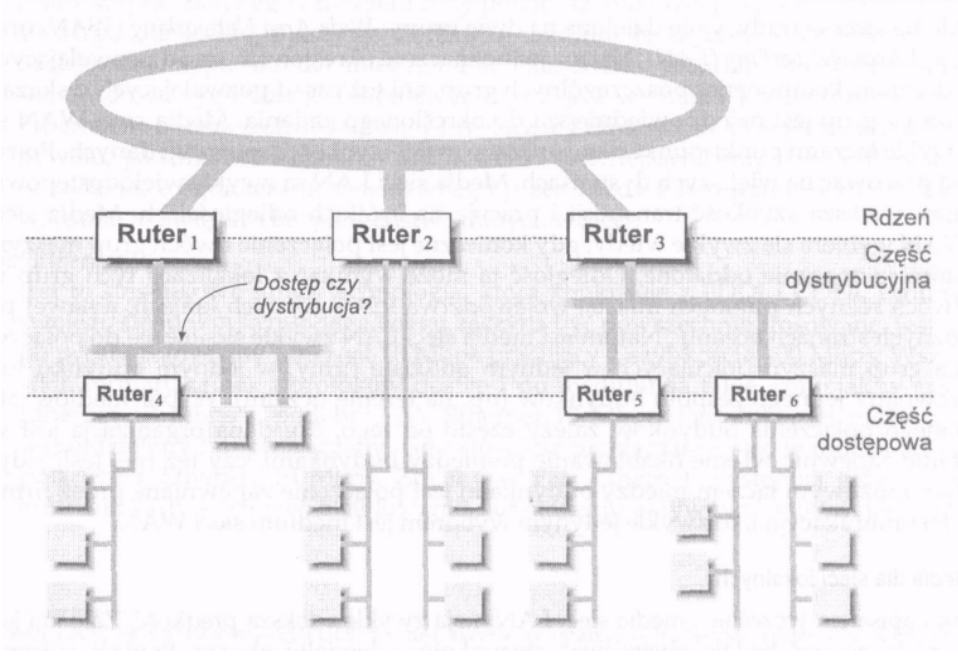
W środowisku sieci WAN systemem dystrybucyjnym będą łącza prowadzące z kilku miejsc do rdzenia sieci. W komponentach tworzących system dystrybucyjny mogą znajdować się niektóre z usług sieciowych, takie jak serwer Protokołu czasu w sieci *(Network Time Protocol — NTP),* serwer DNS lub inne usługi związane z infrastrukturą sieci. Nie jest to zwykle najlepsze miejsce na dołączanie użytkowników sieci, ale może być to dobry punkt dołączenia większych serwerów pracujących w sieci LAN. Jeśli usługa umieszczona jest w tym obszarze, to należy pamiętać, aby umieszczać ją jak najbliżej klienta, który będzie z niej korzystał, co zminimalizuje wpływ ewentualnych uszkodzeń tego typu usługi na inne. Każdy problem występujący w tej części sieci może mieć wpływ na dużą część całej sieci, ale skutki odczują głównie tylko systemy dostępu bezpośrednio dołączone do elementów, w których występują wspomniane problemy. Odczują je oczywiście wszyscy klienci, którzy mają dostęp do sieci w tym miejscu.

Trzecim elementem sieci jest system dostępu. Jest to zwykle najlepiej widoczny i najobszerniejszy komponent sieci. W środowisku sieci LAN w skład systemu dostępu wchodzą koncentratory (koncentratory sieci Ethernet, Token Ring itd.), okablowanie łączące komputery z tymi koncentratorami i karty interfejsów sieciowych umieszczone w komputerach. W skład systemu dostępu mogą również wchodzić rutery budynkowe (które częściej traktowane są jako komponenty systemu dystrybucyjnego) lub małe rutery dostępowe, które łączą biuro z korporacyjną siecią WAN. W sieci WAN systemy dostępu obejmują segmenty sieci LAN wraz z koncentratorami, działającymi w każdej z lokalizacji połączonych tą siecią WAN. Mogą się również do nich zaliczać zestawy serwerów dial-up IP oraz modemów dostępowych, a także małe rutery pracujące w tych lokalizacjach. Tak więc system dostępu jest elementem całej sieci, do którego dołączane są komputery użytkowników, serwery plików dla grup roboczych, serwery baz danych itd. Problemy występujące w tej części sieci dotyczą zwykle użytkowników danej grupy roboczej.

Jak pokazano na rysunku 2-1, granice pomiędzy poszczególnymi elementami sieci mogą przebiegać przez rutery, jak również przez inne miejsca w segmencie sieci. Zwróć uwagę na Ruter1, Ruter2 i Ruter3. Tworzą one granicę pomiędzy rdzeniem a częścią dystrybucyjną sieci, zapewniając usługi obu elementom sieci. Także Ruter4 i Ruter3 oraz Ruter6 tworzą granicę pomiędzy elementami dystrybucyjnymi a dostępowymi. W zależności od rozmiarów Twojej sieci, a także od zadań i celów jej stawianych, niektóre komponenty sieci będą pełniły funkcje w dwóch lub więcej z wymienionych obszarów. Zwróć uwagę na segment sieci dołączony do komponentów Ruter1 i Ruter4. Może on pełnić on zarówno funkcje dystrybucyjne, jak i dostępowe. Gdy tak się dzieje, należy rozważyć przesunięcie funkcji dystrybucyjnych bądź do rdzenia, bądź do systemu dostępowego. Przypadek ten pokazano w sieciach dołączonych bezpośrednio do Rutera2, w których nie ma wyraźnie widocznego elementu dystrybucyjnego. Mimo że nie jest to rozwiązanie idealne, często staje się konieczne.

Wybór medium - co z czym połączyć?

Najlepiej byłoby wybrać jedno lub najwyżej dwa media wykorzystywane w każdym z oddzielnych komponentów funkcjonalnych. Każde dodatkowe medium będzie wymagało dodatkowego wyposażenia i przeszkolenia personelu, a także spowoduje ograniczenie elastyczności sieci lub znaczne zwiększenie kosztów jej utrzymania. Aby zrozumieć, dlaczego tak się dzieje, zastanów się, co się stanie, gdy będziesz musiał przenieść komputer z jednego miejsca w sieci w drugie. Zmiana taka może być konieczna, na przykład z powodu zmian w strukturze firmy lub przeniesienia biura do innych pokoi. Jeśli komponenty odpowiedzialne za dostęp do sieci obsługują jedno medium transmisyjne, takie przenosiny są łatwe; możliwe, że będziesz musiał zmienić jedynie adres IP komputera. Jeśli stosujesz w sieci dwa lub więcej media, musisz się zastanowić, czy w nowym miejscu będziesz miał dostęp do medium, przez które obsługiwany jest obecnie dany komputer. Jeśli nie, to będziesz zmuszony do dokonania zmian sprzętowych w komputerze i zastosowania takiego interfejsu sieci, przez który będziesz mógł dołączyć komputer w nowym miejscu. Rozwiązaniem alternatywnym jest oczywiście zapewnienie dostępu do wszystkich mediów w każdym miejscu sieci, ale zwiększa to znacznie koszty.



Rysunek 2-1: Sieć z podziałem na część rdzeniowa, dystrybucyjna i dostępowa

Oczywiście, jak zawsze przy opracowywaniu sieci, obecność istniejącego rozwiązania może zmienić Twoje plany. Jeśli w systemie działa zarówno Ethernet, jak i Token Ring, to nie masz wyboru i musisz obsługiwać oba standardy. W takim przypadku spróbuj jednak wskazać jedną z technologii jako preferowaną i wszystkie nowe instalacje wykonuj zgodnie z nią, mając na uwadze fakt, że w końcu doprowadzi to do wycofania medium i technologii, które nie są przez Ciebie preferowane.

Rodzaje mediów sieci

Nie powinieneś jednak ograniczać liczby wybieranych dla wszystkich elementów sieci mediów do jednego. Takie podejście ogranicza możliwość zapewnienia właściwej jakości usług użytkownikom tej sieci. Zastanów się, co się będzie działo, jeśli rdzeń Twojej sieci wykonany zostanie w oparciu o to samo medium co sieć dostępowa. Kiedy sieć dostępowa urośnie do wymaganych rozmiarów, jej rdzeń będzie wąskim gardłem wydajności całego systemu. Na pewno nie o to Ci chodzi. Konieczne jest wnikliwe przeanalizowanie sposobów, w jaki każdy rodzaj medium spełnia wymagania stawiane elementom projektowanej *przez* Ciebie sieci.

Zanim jednak zaczniemy mówić o tym, jakie media należy brać pod uwagę, omówmy cechy powszechnie stosowanych mediów sieci, dostępnych w czasie, kiedy książka ta powstaje.

Media sieci są tradycyjnie dzielone na dwie grupy: Wide *Area Networking (WAN)* oraz *LocalArea Networking (LAN)*. Nie ma jednoznacznie określonych zasad pozwalających odróżniać komponenty poszczególnych grup, ani też zasad pozwalających wskazać, która z grup jest najodpowiedniejsza do określonego zadania. Media sieci WAN są zwykle łączami punkt-punkt o stosunkowo małej szybkości transmisji danych. Potrafią pracować na większych dystansach. Media sieci LAN są zwykle wielodostępowe, mają większą szybkość transmisji i pracują na krótkich odległościach. Media sieci WAN wybiera się zwykle wtedy, gdy konieczne jest połączenie dwóch grup maszyn, które są znacznie oddalone. Odległość ta może wynikać z lokalizacji tych grup w dwóch różnych punktach miasta, województwa lub w różnych krajach, a nawet po różnych stronach oceanu . Natomiast media sieci LAN zwykle stosuje się do połączenia grup maszyn pracujących w jednym oddziale firmy, w jednym budynku lub wewnątrz jednego zespołu budynków (np. na terenie uczelni). Wybór mediów dla danego połączenia budynków zależy często od tego, czy dana organizacja jest w stanie zapewnić własne okablowanie pomiędzy budynkami, czy też nie. Jeśli jedynym możliwym łączem między budynkami jest połączenie zapewniane przez firmę telekomunikacyjną, to zwykle jedynym wyborem jest medium sieci WAN.

Media dla sieci lokalnych

Jak napisałem wcześniej, media sieci LAN mają zwykle większą prędkość. Zakłada się w nich, że sieć będzie obejmować stosunkowo niewielki obszar. Poniżej opisane zostały media najczęściej stosowane w sieciach lokalnych:

Wybór medium -co z czym połączyć?

Ethernet

Ethernet jest prawdopodobnie najbardziej rozpowszechnionym medium sieci LAN. W swojej tradycyjnej formie jest to sieć o szybkości transmisji 10 megabitów na sekundę (Mbps), z dzielonym dostępem, która może być uruchomiona w oparciu o kabel koncentryczny (w dwóch rodzajach) lub nieekranowaną miedzianą skrętkę kablową.* Główną zaletą tego typu medium jest jego szeroka dostępność, niska cena i duża elastyczność przy dodawaniu kolejnych połączeń. Aby dołączyć urządzenie, należy jedynie połączyć je odpowiednim kablem z koncentratorem lub kablem koncentrycznym. Główną wadą takiego rozwiązania jest fakt, że gdy dwie szybkie maszyny pracujące w takiej sieci zaczną się ze sobą komunikować, łatwo mogą zmonopolizować ruch w sieci. Drugą wadą są problemy z zapewnieniem bezpieczeństwa przesyłanych danych, ponieważ każda maszyna pracująca w sieci może łatwo monitorować ruch w segmencie sieci.

Przełączany Ethernet

Wariantem tradycyjnego rozwiązania sieci Ethernet, który staje się coraz popularniejszy, jest Przełączany Ethernet. Przełączanie pozwala zapewnić pasmo 10 Mbps każdej maszynie lub niewielkiej grupie maszyn. To ostatnie rozwiązanie nazywane jest *mikrosegmentacja.* Pomaga ona zmniejszyć koszty Przełączanego Ethernetu, które są jego główną wadą. Do zalet Przełączanego Ethernetu należą wszystkie zalety współdzielonego Ethernetu przy powiększeniu dostępnego pasma sieci do 10 Mbps dla każdej maszyny. Ponieważ medium to wykorzystuje tradycyjne okablowanie typu skrętka miedziana w charakterze medium fizycznego oraz standardową sygnalizację Ethernet, możliwa jest wymiana koncentratora sieci Ethernet na przełącznik obsługujący Przełączany Ethernet, bez konieczności dokonywania jakichkolwiek zmian w okablowaniu i interfejsach komputerów. Ponadto w związku z ograniczeniem widzianego przez każdy z komputerów ruchu rozwiązanie to zwiększa bezpieczeństwo danych w sieci.

Fast Ethernet

Jest to stosunkowo nowa technologia, która konkuruje z FDDI i CDDI, i mimo swojego stosunkowo młodego wieku zaczyna być powszechnie stosowana. Jest to po prostu tradycyjny Ethernet 10 Mbps pracujący z szybkością 100 Mbps. Wszystkie formaty ramek i protokoły dostępu do medium są takie same jak w sieci Ethernet 10 Mbps i, podobnie jak Ethernet 10 Mbps, Fast Ethernet może być współdzielony lub przełączany. Gdy stosujesz przełączanie, sieć tę można łatwo połączyć z Ethernet 10 Mbps. Zmiany w Fast Ethernet występują głównie w budowie karty sieciowej, okablowaniu i urządzeniu aktywnym, którym jest koncentrator lub przełącznik.

*Sieci LAN, za wyjątkiem sieci FDDI, pracują zwykle w oparciu o tradycyjne systemy okablowania elektrycznego bazujące na miedzi. Należy jednak pamiętać, że wszystkie opisywane tu media mają wersje rozwiązań pracujące w oparciu o światłowody, pozwalające zwykle na pracę na dłuższym dystansie, dzięki czemu można ich użyć w łączach pomiędzy budynkami w sieci kampusowej. W praktyce nie powinno się używać połączeń między budynkowych opartych na miedzi w związku z ich podatnością na zakłócenia pracy spowodowane wyładowaniami atmosferycznymi.

Wszystkie te komponenty muszą być przygotowane do obsługi szybkości transmisji danych właściwej dla sieci Fast Ethernet.

Fast Ethernet zawdzięcza swą popularność również temu, że odpowiednik tego medium - Ethernet - jest powszechnie znany i nie ma między nimi większych różnic. Jeśli jednak występują różnice, to są one ważne. Ponieważ Fast Ethernet pracuje z większymi prędkościami, nie jest tak tolerancyjny dla okablowania nie spełniającego standardów jak Ethernet. Całkowita długość pojedynczego kabla miedzianego musi wynosić maksymalnie 100 metrów, podobnie jak to jest w przypadku sieci Ethernet, ale pomiędzy dwoma komputerami mogą znaleźć się tylko dwa wzmacniaki klasy II. Wzmacniaki te mogą być połączone kablem o długości nie większej niż 5 metrów. Oznacza to, że maksymalna odległość pomiędzy parą komputerów w sieci Fast Ethernet wynosi tylko 205 metrów, co jest znacznie gorszym wynikiem w porównaniu z siecią Ethernet, w której każdy kabel mieć 100 metrów, a przy tym można szeregowo połączyć do czterech wzmacniaków na odległość 500 metrów.

Nie jest to jedyna wada sieci Fast Ethernet. Na rynku dostępnych jest kilka niekompatybilnych ze sobą rozwiązań tej sieci. Najpowszechniej stosowanym rodzajem, który zdaje się być ostatecznym standardem, jest rozwiązanie o nazwie 100BaseTX. Dostępne są też rozwiązania 100BaseT4 i 100 VG AnyLAN. Mimo że dwa wymienione ostatnio standardy pracują dobrze, nie są one tak powszechnie stosowane jak 100BaseTX i prawdopodobnie nie mają szans stać się podstawowymi technologiami sieciowymi.

Gigabitowy Ethernet

Na zakończenie należy powiedzieć o prowadzonych pracach nad formalnym zatwierdzeniem standardu medium o nazwie Gigabitowy Ethernet (pierwsze urządzenia pracujące w tej technologii pojawiły się już na rynku, choć standard ma być zatwierdzony wiosną 1998 - przyp. tłum.). Standard ten używa tego samego rodzaju ramkowania co Ethernet i Fast Ethernet, ale trudno powiedzieć, jakie będą maksymalne długości stosowanych kabli i które z proponowanych przez różnych producentów rozwiązań zostanie wybrane. Należy się bacznie przyglądać tej technologii, ponieważ w ciągu następnych kilku lat może ona stać się bardzo popularna.

Token Ring

Po sieci Ethernet, stosowanej pod różnymi postaciami, drugim najbardziej popularnym rozwiązaniem medium dla sieci LAN jest Token Ring. Pomimo sugerowanej nazwą architektury, Token Ring jest układem stacji klienckich połączonych kablami z urządzeniem dostępowym o nazwie MAU *(medium access unii)*. Następnie MAU połączone są ze sobą w taki sposób, że tworzą podwójny pierścień. Podstawowy pierścień stosowany jest dla komunikacji, a pierścień zapasowy wykorzystuje się jako dodatkowe zabezpieczenie na wypadek awarii. To podwójne rozwiązanie połączeń pierścienia jest jedną z głównych zalet Token Ring - jeśli podstawowy pierścień ulegnie uszkodzeniu, na przykład z powodu uszkodzenia kabla lub błędów w warstwie transmisji, następuje automatyczne przekierowanie ruchu na pierścień zapasowy.

Wybór medium -co z czym połączyć?

Drugą główną zaletą sieci Token Ring jest jej odporność na zajmowanie całego pasma *przez* dwie silne maszyny. Sieć ta działa bowiem w oparciu o przekazywany pomiędzy stacjami logiczny żeton, który zezwala na nadawanie stacji, która go aktualnie posiada. Dzięki temu każda maszyna w sieci ma przez określony czas zagwarantowaną możliwość transmisji danych do sieci z wykorzystaniem całego dostępnego pasma. Popularne rozwiązania sieci Token Ring pracowały z szybkościami transmisji 4 Mbps, ale obecnie powszechny stał się standard pracujący z szybkością 16 Mbps.

Rozwiązanie Token Ring ma również wady. Podstawową wadą jest jego ograniczona dostępność. Obecnie większość sprzedawanych komputerów wyposażonych jest od razu w interfejsy sieci Ethernet, które równie łatwo można również kupić w postaci oddzielnych kart do komputerów PC. Interfejsy sieci Token Ring nie są tak powszechne i głównie dlatego są droższe od odpowiedników obsługujących Ethernet. Wydaje się, że interfejsy tego typu stosuje się tylko w pecetach i mainframe'ach IBM. Nie powinieneś jednak rezygnować z wykorzystywania Token Ring, zwłaszcza jeśli interfejsy będą dostępne dla wszystkich rodzajów komputerów w Twojej sieci.

FDDI

Kolejnym medium, o którym powinieneś wiedzieć i którego zastosowanie w swojej sieci mógłbyś rozważyć, jest FDDI. Nazwa ta jest skrótem od *Fiber Distribn-ted Data Interconnect*. Ta szybka technologia sieci LAN oparta jest na topologii podwójnego pierścienia podobnej do Token Ring, ale pracuje z prędkością 100 Mbps po światłowodach. Choć FDDI uznawany jest za medium sieci LAN, to możliwe jest wykonywanie w tej technologii pierścieni o długości kilku kilometrów.

W tradycyjnym podejściu FDDI wykorzystuje się jako technologię rdzenia sieci, głównie z powodu ograniczonej dostępności i wysokich kosztów zarówno interfejsów, jak i okablowania światłowodowego. Ograniczenia te znikają jednak w związku z obniżaniem się cen elementów tej sieci. Szacuje się, że światłowody kosztują obecnie tylko trochę więcej od instalacji wykonywanej skrętką miedzianą dobrej jakości, a interfejsy są coraz tańsze i dostępniejsze. Kiedy doda się do tego jakość rozwiązania i jego dostępność w wersji pracującej po miedzi CDDI *(Copper Distributed Data Interconnect),* FDDI staje się rozwiązaniem, które można zastosować w każdym z trzech elementów sieci, poczynając od rdzenia sieci aż do części dystrybucyjnej, a nawet przy doprowadzaniu danych do biurka.

Media sieci rozległych

Media stosowane w sieciach WA1J są bardziej podobne do siebie i nie są powszechnie znane. Ogólnie rzecz biorąc, można je podzielić na dwie kategorie, biorąc po uwagę czas trwania połączenia. Media WAN mogą obsługiwać połączenia na żądanie; gdy połączenie nawiązywane jest wtedy, gdy jest taka potrzeba, a po przesłaniu danych jest zamykane.

Drugim sposobem jest zestawianie stałych dedykowanych połączeń, które istnieją nieprzerwanie, niezależnie od tego, czy dane są przesyłane, czy też nie.

Najważniejszą zaletą połączenia na żądanie jest jego koszt. Połączenie takie istnieje tylko tak długo, jak długo istnieje potrzeba przesłania danych, co sprawia, że jego koszt jest znacznie mniejszy od kosztu stałych łączy o takich samych parametrach transmisji. Ponadto możliwe jest wykorzystanie kilku punktów, z którymi połączenie będzie kolejno nawiązywane, przy wykorzystaniu tylko jednego przyłącza do sieci.

Takie rozwiązanie nie jest oczywiście pozbawione wad. Ponieważ połączenie nie jest aktywne *przez* cały czas, początkowe dane są zawsze opóźnione w związku z czasem koniecznym dla nawiązania połączenia. Ponadto w przypadku, gdy kilka tego typu połączeń współdzieli jedno przyłącze do sieci, możliwe, że połączenie będzie zajęte. Jest to spowodowane nawiązaniem innego połączenia przez lokalny interfejs lub interfejs odległy, co sprawia, że komunikacja na innych połączeniach nie będzie możliwa, dopóki wcześniej otwarte połączenie nie zostanie zakończone. Nadal jednak, z punktu widzenia generowanego w sieci ruchu, który jest z natury przejściowy, połączenia zestawiane na żądanie mogą być rozsądnym kompromisem w wyborze między większą dostępnością a niższymi kosztami.

Modemy analogowe

Jakie rodzaje połączeń zestawianych na żądanie są powszechnie stosowane? Najpopularniejszym i prawdopodobnie najczęstszym rozwiązaniem dla sieci WAN są połączenia realizowane przez modemy analogowe. Są one przede wszystkim wykorzystywane jako technologia dostępu do sieci, ale prostota rozwiązania i niskie koszty sprawiają, że rozwiązania te są atrakcyjne dla wszystkich wolnych połączeń. Elementy wymagane na obu końcach połączenia to: port szeregowy, modem i zwykła linia telefoniczna, a także oprogramowanie, które potrafi zestawić i w odpowiednim momencie zakończyć takie połączenie.

Samo połączenie telefoniczne nie wystarcza do przesyłania danych. Konieczne jest *jeszcze* zastosowanie właściwego protokołu transmisji danych. Powszechnie stosowane do pracy w tego typu połączeniach są dwa protokoły. Starszy z nich to SLIP *(Serial Linę IP).* Protokół ten jest bardzo prosty, co stanowi jego zaletę. Potrafi on jednak przesyłać tylko pakiety IP. Ma też ograniczone możliwości wykrywania i usuwania błędów transmisji. Drugi protokół to PPP *(Point to Point Protocol),* który jest bardziej złożony, ale może obsługiwać ruch związany z innymi protokołami, ma możliwość ochrony połączeń poprzez funkcję oddzwaniania, kodowania danych, wykrywania błędów i wiele innych zalet. Jest to ponadto protokół stosowany powszechnie w sprzęcie sieciowym, takim jak rutery. Jeśli masz możliwość wyboru, stosuj PPP. Niestety, istniejące wcześniej rozwiązania w sieci mogą zmuszać do zastosowania protokołu SLIP.

Użycie modemów analogowych ma dwie poważne wady. Łącze telefoniczne jest zajęte *przez* cały, czas kiedy przesyłane są dane, a modem nie może zapewnić takiej prędkości transmisji, jaka jest możliwa w przypadku korzystania z innych technologii. Zajmowanie łącza telefonicznego może być ważne, kiedy łączymy się z biura utworzonego w domu, gdzie marny tylko jedną linię telefoniczną.

Kiedy my przesyłamy dane, to klienci lub współpracownicy próbujący się dodzwonić będą słyszeli sygnał zajętości. Jeśli chodzi o szybkość transmisji danych, to stosowane obecnie w modemach analogowych technologie ograniczają ją do 56 kbps i choć nie jest to jeszcze górna granica sprzętu, to analogowe łącza telefoniczne nie są w stanie przesyłać większych szybkości. Należy ponadto pamiętać, że szybkość 56 kbps osiągana jest tylko na łączu o szczególnie dobrych parametrach.

ISDN

Rozwiązaniem problemów związanych z modemami analogowymi jest technologia, która była znana od kilku lat, ale dopiero teraz staje się popularna. *Integrated Seruices Digital Network (ISDN)* to projekt oparty na transmisji cyfrowej, opracowany przez firmy telekomunikacyjne w celu stworzenia sieci zdolnej przesyłać głos, dane, obrazy wideo i inne sygnały za rozsądną cenę i przy użyciu istniejących miedzianych linii abonenckich. Podobnie jak w przypadku modemów analogowych, urządzenie ISDN nawiązuje połączenie z innym urządzeniem ISDN dodzwaniając się do niego i uzyskując połączenie lub sygnał zajętości. Jednakże w przeciwieństwie do modemów analogowych, szybkość transmisji jest większa (64 kbps dla każdego „dzwonienia"), a linia telefoniczna nie jest blokowana przez nawiązane połączenie, którym przesyłane są dane - możliwe jest nawiązanie kolejnego równoległego połączenia. Te kolejne połączenia mogą być nawiązywane z tym samym numerem w celu poszerzenia pasma, którym przesyłane są dane lub z innym numerem w sieci telefonicznej. Możliwe jest również mieszanie połączeń dla danych i głosu przy wykorzystaniu tego samego łącza.

To, ile jednoczesnych połączeń można nawiązać na tym samym łączu, zależy od rodzaju realizowanej usługi telekomunikacyjnej. Obecnie dostępne są dwa rodzaje usługi. *Basic Ratę Interface (BRI)* zapewnia dwa kanały B, z których każdym można przesyłać rozmowę telefoniczną lub dane, oraz jeden kanał D, używany do kontroli łącza i sygnalizacji. Łącząc dwa kanały B uzyskujemy całkowitą przepustowość 128 kbps dla danych przesyłanych pomiędzy dwoma punktami. Możliwe jest wykonanie dwóch oddzielnych telefonów do dwóch różnych miejsc. Ponadto możliwe jest nawiązanie połączenia telefonicznego, gdy oba kanały są zajęte przez przesyłane dane, poprzez czasowe przerwanie strumienia danych płynących jednym kanałem, tak by połączenie telefoniczne mogło być zaakceptowane. Redukuje to liczbę sygnałów zajętości, które słyszy klient lub współpracownik, próbując się do nas dodzwonić.

Drugim rodzajem usługi ISDN jest *Priman/ Ratę Interface (PR1).* PRI zapewnia dostęp do 23 kanałów B i jednego kanału D dla kontroli i sygnalizacji w Ameryce Północnej albo 30 kanałów B i jednego D (w innych częściach świata). Podobnie jak w poprzednim przypadku, każdy kanał może być wykorzystywany niezależnie do rozmów telefonicznych lub transmisji danych. Możliwe jest także agregowanie kilku kanałów B w celu uzyskania szerszego pasma dla transmisji danych poprzez nawiązanie kilku równoległych połączeń z tym samym miejscem. Usługa BRI wykorzystywana jest zwykle przez oddział biura lub przez biuro działające w domu, gdzie nie ma dużych wymagań odnośnie ilości transmitowanych danych.

Usługa PRI wykorzystywana jest w centrali biura, gdzie schodzą się wszystkie łącza prowadzące do oddziałów firmy. Taki sposób wykorzystywania łączy ISDN nie jest oczywiście jedynym rozwiązaniem. Dwa niewielkie biura mogą zamówić usługi BRI w celu nawiązywania łączności ze sobą, jak również dwa duże biura mogą się łączyć na żądanie, przy użyciu PRI. . • .

Aby skorzystać z usług ISDN, musisz dysponować urządzeniem o nazwie *ISDN Terminal Adapter (TA),* które często jest błędnie nazywane modemem ISDN. Urządzenie TA może być wykonane w formie karty rozszerzenia umieszczanej w komputerze PC lub oddzielnego urządzenia z interfejsem LAN, które ma możliwość rutowania lub mostowania ruchu w sieci. W każdym z rozwiązań w urządzeniu będzie również umieszczone gniazdo pozwalające na dołączenie zwykłego telefonu, faksu lub modemu analogowego. Wykorzystywanie usług sieciowych w oparciu o ISDN wymaga stosowania protokołu transmisji, którym prawie zawsze jest PPP.

ISDN jest prawdopodobnie najlepszym rozwiązaniem na zapewnienie dostępu z małego biura lub domu do korporacyjnej sieci LAN. *Łącza* tego typu można z powodzeniem wykorzystywać pomiędzy centralą a oddziałem firmy, zwłaszcza wtedy, gdy do transmisji danych wystarczają krótkotrwałe połączenia. ISDN dobrze spełnia średnie wymagania dotyczące transmisji danych, a jego zaletą jest fakt, że płacisz za faktyczne wykorzystanie łącza.

Łącza dzierżawione

Innym rodzajem połączeń w sieci WAN, o którym już wcześniej wspomniałem, są stałe, dedykowane łącza. W najprostszej formie jest to łącze pomiędzy dwoma lokalizacjami, wydzierżawione od firmy telekomunikacyjnej, które służy do transmisji danych. Na każdym z końców takiego łącza znajduje się urządzenie typu modem, które nosi nazwę DSU/CSU *(Data Seruice Unii/ Control Seroice Unit).* Dobrze jest zakupić oba urządzenia, dla dwóch końców łącza, od tego samego producenta, aby mieć pewność, że będą one ze sobą dobrze współpracowały. DSU pobiera dane (zwykle synchroniczne) z rutera, mostu lub komputera i wysyła je przez łącze dzierżawione do drugiego urządzenia, które dekoduje dane i przekazuje je do urządzenia odbiorczego, z którym współpracuje.

Ponad opisaną trasą danych urządzenia wykorzystują protokół transmisji, podobnie jak to ma miejsce w przypadku modemów analogowych i usług ISDN. Wykorzystywane zwykle protokoły to PPP (opisany wcześniej) lub *High-level Data Link Control (HDLC).* Każdy z wymienionych protokołów ma zalety w stosunku do innych, ale nie będziemy ich tutaj opisywali. Wybór protokołu powinien być uzależniony od protokołu obsługiwanego przez urządzenia pracujące w Twojej sieci. PPP jest obsługiwany przez wszystkich większych dostawców ruterów, tak więc jest dobrym wyborem z punktu widzenia współpracy tych urządzeń. HDLC jest trochę wydajniejszy z punktu widzenia wykorzystywanego pasma, ale nie wszyscy dostawcy sprzętu implementują ten protokół w swoich urządzeniach.

Ponieważ łącza dzierżawione wykorzystują cyfrową sygnalizację, można nimi przesyłać dane ze znacznie większą szybkością niż przez modemy analogowe. W związku z tym, że stosowane są w nich doskonałej jakości kable miedziane lub światłowody, osiągane szybkości transmisji są również większe niż te oferowane przez usługi ISDN. Łącza dzierżawione pozwalają na pracę z bardzo różnymi szybkościami. Najczęściej są to jednak *Digital Signaling O* (DS-0) lub 56 kbps; *DS-1* (nazywany również T-l), pracująca z szybkością 1,544 Mbps; oraz DS-3 (często błędnie nazywana T-3), pracująca z szybkością 44,736 Mbps. Bardzo często użytkownicy zamawiają części pasma, z którym pracuje T-l lub T-3, kiedy żadna z wymienionych szybkości nie spełnia ich wymagań.

Dzierżawione łącza punkt-punkt mają dwie podstawowe wady. Pierwszą z nich jest koszt. Zazwyczaj w łączu, po którym przesyłane są dane, mamy do czynienia z przedziałami czasu, gdy dane nie są przesyłane wcale lub gdy pasmo jest wykorzystywane w niewielkim procencie, ale w przypadku łącza dzierżawionego nie ma to wpływu na jego koszty. Niezależnie od tego, czy łącze wykorzystuje wszystkie swoje możliwości, czy też nie, opłaty są jednakowe. Z drugiej strony, jeśli dane z Twojego systemu płyną przez większą część dnia, to może się okazać, że zastosowane łącze zestawiane na żądanie jest praktycznie wcale nie rozłączane i będzie kosztowało więcej niż łącze dzierżawione pomiędzy tymi dwoma punktami.

Drugą wadą łączy dzierżawionych jest ich skalowalność. Ponieważ każde łącze dzierżawione przeznaczone jest do obsługi jednego miejsca, obsługa kilku różnych sieci znajdujących się w różnych miejscach wymaga zastosowania rutera wieloportowego, kilku zestawów urządzeń DSU i kilku łączy dzierżawionych, a to wszystko kosztuje sporo pieniędzy. To może doprowadzić do sytuacji, w której w centralnym punkcie tworzonej sieci będzie znajdował się tuzin, a może nawet kilkaset portów, urządzeń DSU i zbiegających się łączy. Zwykle okazuje się, że spora część tych łączy jest przez pewien czas nieaktywna. Z tych właśnie powodów łącza dzierżawione punkt-punkt są najlepiej wykorzystane, kiedy miejsc, które łączymy, jest niewiele lub kiedy pasmo, które mamy zapewnić, jest stosunkowo szerokie. W innych przypadkach lepszym rozwiązaniem może być zastosowanie jednej z technologii omówionych poniżej.

f ramę Relay

Jeśli moglibyśmy połączyć zdolność usług zestawiających połączenia na żądanie i obsługujących kilka połączeń przez jedno łącze fizyczne ze stałą dostępnością charakterystyczną dla łączy dzierżawionych, moglibyśmy zmniejszyć ilość problemów związanych ze skalowalnością łączy punkt-punkt, a także lepiej wykorzystać łącza. Brak aktywności łącza, po którym równocześnie nawiązuje się kilka połączeń, będzie raczej rzadkością. Technologią stosowaną w sieciach WAN, która to wszystko potrafi jest *Frame Relay*.

W sieci Frame Relay miejsce będące klientem sieci dzierżawi stałe łącze dedykowane, podobnie jak to było z łączami punkt-punkt. Różnica polega na tym, że po drugiej stronie łącza znajduje się port urządzenia zwanego przełącznikiem Frame Relay, które jest zwykle umieszczone w biurze centrali telefonicznej (CO). Następnie, w wyniku zamierzonych działań ludzi zajmujących się obsługą tych urządzeń, zestawiane są logiczne połączenia z innymi miejscami wykorzystującymi takie same połączenia Frame Relay.

Te logiczne połączenia, zwane kanałami wirtualnymi, współdzielą ten sam fizyczny port rutera lub mostu, te same urządzenia DSU i to samo łącze dzierżawione. Oprogramowanie pracujące na ruterze lub moście wykorzystuje następnie wirtualne kanały tak, jakby były one łączami punkt-punkt, i przesyła po nich dane do danego miejsca. Kanały wirtualne mogą być konfigurowane tak, aby tworzyły dowolną liczbę topologii, włączając w to topologię gwiazdy, częściową kratę lub pełną kratę. Wszystkie te topologie zostaną opisane w dalszej części tego rozdziału.

Rozwiązanie oparte na Frame Relay jest często znacznie korzystniejsze finansowo od łącza dzierżawionego. Opłaty za łącze dzierżawione są zwykle proporcjonalne do jego długości. W sieci Frame Relay opłaty za usługi zależą zwykle od zamawianego pasma, a nie od odległości, na których zestawiane są kanały.

Szybkość przesyłania danych w sieciach Frame Relay zależy od szybkości, jakie można osiągnąć na łączach, na których zbudowano te usługi, i nie musi być jednakowa dla wszystkich miejsc korzystających z sieci Frame Relay. Miejsce pełniące funkcję centralnego punktu sieci może wykorzystywać na przykład kanał DS-3, podczas gdy kilka biur regionalnych będzie wykorzystywać kanały DS-1 lub DS-0, w zależności od potrzeb. Takie możliwości sieci Frame Relay są jej kolejną zaletą w porównaniu do łączy punkt-punkt. Sieć ta jest szczególnie przydatna do łączenia biur regionalnych z centralą firmy lub połączenia dwóch lub większej liczby biur partnerskich przy wykorzystaniu minimalnej ilości sprzętu.

SMDS

Kolejną technologią, która wykorzystuje pojedyncze łącza dzierżawione od usługobiorcy do centrali usługodawcy, jest *Switched Multi-megabit Data Seruice (SMDS).* Podobnie jak w sieci Frame Relay, kanały SMDS prowadzą do przełącznika, który jest zwykle obsługiwany przez firmę telekomunikacyjną, choć może się znajdować również w centrali firmy i być *zarządzany* przez jej pracowników. W przeciwieństwie do Frame Relay, SMDS nie jest technologią opartą na przełączaniu kanałów. Pomiędzy poszczególnymi odbiorcami usług nie są tworzone kanały wirtualne. SMDS jest technologią opartą na przełączaniu pakietów. Podobnie jak inne technologie przełączania pakietów, włączając w to IP, każda ramka przesyłana w sieci zawiera adres źródła i adres przeznaczenia. W zasadzie SMDS jest czymś w rodzaju rozległej sieci Ethernet. Każde z urządzeń dołączonych do tej sieci może komunikować się z innym urządzeniem poprzez adresowanie ramki wysyłanej do tego urządzenia, chyba że zabronił tego administrator sieci.

Jednym z celów budowy SMDS było zapewnienie szybkich łączy systemom przetwarzania rozproszonego. Aby to osiągnąć, SMDS ma zdefiniowane prędkości dostępu jako DS-1 i DS-3, z kilkoma różnymi klasami dostępu w DS-3, które odpowiadają szybkościom 4, 10, 16, 25 i 34 Mbps. Podobnie jak w sieci Frame Relay, różne miejsca przyłączone do sieci mogą używać różnych szybkości transmisji, co pozwala stosować wolniejsze łącza dla biur regionalnych, a szybsze dla biur centralnych. Zalety te, w połączeniu z brakiem możliwości ręcznego konfigurowania kanałów wirtualnych, sprawiają, że SMDS jest atrakcyjną alternatywą dla połączeń biur partnerskich lub biur regionalnych z centrum komunikacyjnym firmy.

Wybór medium -co z czym połączyć?

Na zakończenie należy podkreślić, że różnice w wyposażeniu klienta w urządzenia pozwalające na korzystanie z łączy punkt-punkt, sieci Frame Relay lub SMDS, nie są tak ważne jak oprogramowanie tych urządzeń. Połączenia fizyczne są takie same: odpowiednio szybki port rutera lub mostu, urządzenie DSU i dzierżawiony kanał transmisyjny. Prawdziwe różnice widać na poziomie oprogramowania, które pracuje w tych urządzeniach. Ważne staje się również to, jaki rodzaj sprzętu i oprogramowania znajduje się po drugiej stronie połączenia. Rozwiązanie najkorzystniejsze dla Twojej sieci będzie zależało częściowo od liczby połączeń, które musisz nawiązywać, opłat za te połączenia w Twojej okolicy nakładanych przez usługodawcę i dostępności usług.

Asynchronous Transfer Modę (ATM)

Technologii *Asynchronous Transfer Modę (ATM)* poświęcam oddzielną część tego rozdziału, więc niektórzy czytelnicy mogą powiedzieć: „Wygląda na to że, mamy do czynienia z fanatykiem ATM". Choć rzeczywiście korzystam z tej technologii w mojej sieci, to w żadnym razie nie jestem jej fanatykiem. ATM opisany jest w oddzielnej części, ponieważ można go zaliczyć zarówno do technologii LAN, jak i WAN.

Standard ten został opracowany przez koncerny telekomunikacyjne jako technologia superszybkich sieci dla transmisji głosu, a następnie zaadaptowany przez społeczność sieci danych jako superszybka technologia sieciowa (szybkości transmisji od 25 Mbps aż po gigabity na sekundę). Technologia ta pozwala ponadto integrować głos, obrazy wideo i sieci transmisji danych w jednym urządzeniu, które jest w stanie zapewnić obsługę różnych specyficznych zadań związanych z przesyłaniem danych generowanych przez trzy dotychczas niezależne sieci. Ale to nie jest jedyna zaleta tego rozwiązania. Oprócz integracji głosu, obrazu i transmisji danych technologia ATM może łączyć sieci WAN i LAN w sposób, który nigdy dotychczas nie był możliwy.

Połączenie pomiędzy siecią LAN a WAN uzyskiwane jest w tej technologii poprzez przyłączenie lokalnego przełącznika ATM, który jest zwykle obsługiwany przez personel firmy, z innym przełącznikiem, obsługiwanym przez administratorów w innej organizacji, takiej jak firma telekomunikacyjna. Dzięki tak elastycznemu rozwiązaniu urządzenia pracujące w obu połączonych sieciach i dołączone do nich poprzez przełączniki (lub zdublowane układy przełączników ATM) mogą współpracować ze sobą, wykorzystując te same metody transmisji, fizyczne łącza, jak również komunikować się po tym samym protokole. Nie muszą wiedzieć, czy urządzenie, z którym wymieniają informacje, jest dołączone do przełącznika lokalnego, czy przełącznika pracującego gdzieś daleko.

Podobnie jak Frame Relay, ATM wykorzystuje kanały wirtualne do nawiązania połączeń z innymi urządzeniami. W przeciwieństwie do technologii Frame Relay, kanały te mogą być ustanawiane przez człowieka, jak to się często dzieje w przypadku rozległych sieci ATM, lub tworzone i usuwane na żądanie, jak to ma miejsce w lokalnej sieci ATM.

Ponadto, podobnie jak Frame Relay, łącza wykorzystywane w ATM nie muszą być takiej samej szybkości. *Łącza* lokalne mogą być mieszaniną połączeń od 100 do 622 Mbps, podczas gdy w sieci WAN mogą to być łącza DS-1, DS-3 lub 155 Mbps.

Ostatnią zaletą ATM, którą podkreślają wszyscy jego zwolennicy, jest jego zdolność do zapewnienia gwarantowanej jakości usługi. Większość tradycyjnych technologii sieciowych zakłada, że wszystkie przesyłane w sieci dane mają jednakowy priorytet. W takich sieciach dane obsługiwane są na zasadzie „pierwszy przyszedł - pierwszy wychodzi", przez co możliwe jest występowanie zatorów. W technologii ATM urządzenie informuje sieć, jakiego rodzaju usług oczekuje dla każdego z nawiązywanych połączeń, i może *zgodzić* się na przesyłanie generowanego przez to urządzenie ruchu przy zastosowaniu pewnych ograniczeń, uzgodnionych pomiędzy urządzeniem a siecią. Pozwala to sieci unikać sytuacji, w których łącze będzie przeładowane, a także usuwać dane z sieci, gdy nastąpi w niej zator, poczynając od danych należących do transmisji o najniższym priorytecie lub transmisji, która przekroczyła zakontraktowane wcześniej wartości. Oznacza to, że strumień danych, w postaci obrazów wideo, który nie może tolerować utraty danych lub opóźnień, przesyłany będzie z większym priorytetem niż strumień danych, którym przesyłany jest głos i dla którego dopuszczalne jest opóźnienie lub zgubienie części bitów. Oczywiście obydwa opisane wyżej strumienie będą ważniejsze od danych, które w razie zagubienia łatwo przesłać po raz drugi w wyniku działania protokołów warstw wyższych (np. poczta elektroniczna).

Niestety, ATM, zgodnie z tym, co podkreślają jego przeciwnicy, jest technologią opartą na bardzo skomplikowanym systemie kabli i przełączników i nadal wykorzystuje kilka standardów, które mają dopiero kilka lat, a niektórych standardów nawet jeszcze nie opisano. Biorąc pod uwagę nowość ATM i złożoność zarządzania nim, jego przeciwnicy powtarzają, że jest jeszcze za wcześnie na poważne traktowanie tej technologii. Niezależnie od tego, czy się z tym zgadzasz, czy nie, bez wątpienia powinieneś zapoznać się z tą nową technologią, posługując się choćby małą siecią testową. Możesz przekonać się, że jest to rozwiązanie idealne dla Twojej sieci lub że może Twoja sieć powinna ewoluować w tym kierunku. Jeśli tak nie jest, to będziesz gotów na kolejne podejście do tematu za kilka lat, kiedy standard ATM się upowszechni.

Ruch w sieci

Kiedy dokonujesz wyboru medium, musisz pamiętać o dwóch najważniejszych sprawach: o podstawowej funkcji każdej z części sieci oraz o tym, jakiego ruchu w każdej z nich się spodziewasz. Musisz mieć pewność, że łącza, które będą najczęściej wykorzystywane, są w stanie obsłużyć ruch, jaki będzie przez nie kierowany.

Przez wiele lat przy projektowaniu sieci stosowano zasadę dotyczącą ruchu, jaki przechodzi przez lokalną część sieci, a ile wychodzi na zewnątrz; zwykle 80/20, 70/30 albo 90/10. Liczby te wyrażały stosunek ruchu lokalnego w sieci do ruchu wychodzącego z sieci na zewnątrz. Nie jest tu ważne, czy właściwie je dobierano.

Wybór medium -co z czym połączyć?

Należy raczej zwrócić uwagę na fakt, że powszechnie zgadzano się z twierdzeniem, iż w dobrze zaprojektowanej sieci (lub podsieci) większość ruchu stanowią dane przesyłane lokalnie i powinny one pozostawać w sieci. Oznacza to, że umieszczanie wszystkich klientów w jednej sieci, a serwerów w drugiej nie było uznawane za dobry pomysł. Wynikało to z założenia, że klienci nie będą komunikowali się ze sobą tak często jak z serwerami w sieci, a w rezultacie że większość ruchu będzie wychodziła na zewnątrz. W środowisku sieci LAN nie jest to być może istotne, ale dla środowiska sieci WAN, gdzie łącza są zwykle wolniejsze i znacznie droższe, może być bardzo niebezpieczne.

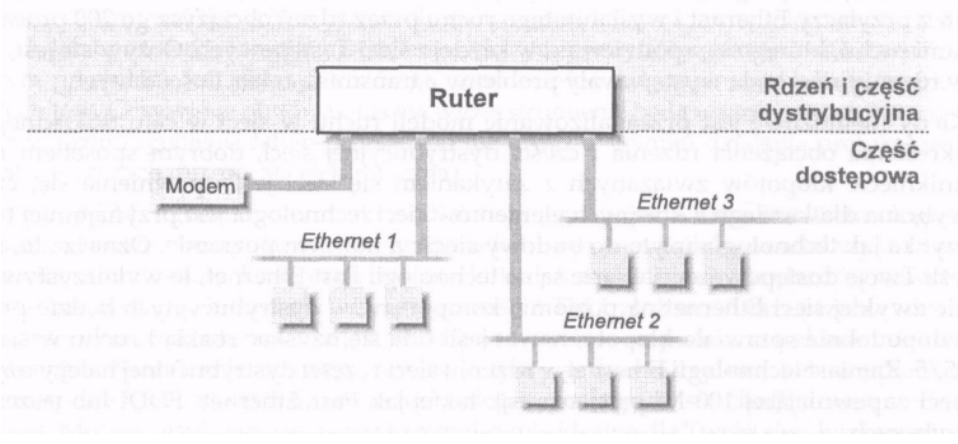
Czy oznacza to, że wszystkie najszybsze łącza należy umieścić w części sieci obsługującej dostęp użytkowników i dystrybuującej ruch sieciowy? Przecież to właśnie w tych miejscach klienci sieci (i prawdopodobnie serwery usług) są zlokalizowani. Nie jest to do końca prawdą. Choć większość ruchu w sieci rzeczywiście pozostaje na poziomie lokalnym w jednym segmencie sieci, to rdzeń sieci musi być w stanie przesłać wszystkie dane wychodzące z poszczególnych segmentów sieci, które są do niego dołączone. Na przykład zakładając, że Twoja sieć wykorzystująca 10 przyłączy Ethernet spełnia regułę ruchu 80/20, po pomnożeniu około 20 procent ruchu z każdego z przyłączy Ethernet i wysłaniu tego ruchu przez rdzeń obciążysz go 200 procentami ruchu, którego się spodziewasz w każdej z sieci dostępowych. Oczywiste jest, że w rdzeniu sieci będą występowały problemy z transmisją takiej ilości danych.

Kiedy niemożliwe jest przeanalizowanie modeli ruchu w sieci w celu dokładnego określenia obciążenia rdzenia i części dystrybucyjnej sieci, dobrym sposobem na uniknięcie kłopotów związanych z zatykaniem się sieci jest upewnienie się, czy wybrana dla każdego z kolejnych elementów sieci technologia jest przynajmniej tak szybka jak technologia użyta do budowy sieci na niższym poziomie. Oznacza to, że jeśli Twoje dostępowe sieci oparte są na technologii Fast Ethernet, to wykorzystywanie zwykłej sieci Ethernet na poziomie komponentów dystrybucyjnych będzie prawdopodobnie sprawiało kłopoty, nawet jeśli uda się uzyskać rozkład ruchu w sieci 95/5. Zamiast technologii Ethernet w rdzeniu sieci i części dystrybucyjnej należy użyć sieci zapewniającej 100 Mbps transmisji, takiej jak Fast Ethernet, FDDI lub jeszcze szybszych.

Pamiętaj, że prawie zawsze zagregowane pasmo jednej z warstw sieci przekroczy możliwości transmisyjne kolejnej warstwy, nawet jeśli linie dostępowe będą wolne. Rozpatrzmy na przykład sieć z 40 współdzielonymi segmentami Ethernet na poziomie komponentów dostępowych. Jeśli jej część dystrybucyjna składa się z dwóch ruterów połączonych ze sobą łączem Fast Ethernet o przepustowości 100 Mbps, z których każdy obsługuje po 20 segmentów Ethernet, to zagregowane pasmo wyniesie 400 Mbps, co oczywiście znacznie przekracza możliwości sieci 100 Mbps pracującej na poziomie dystrybucyjnym. Niemniej jeśli model ruchu dla tej przykładowej sieci będzie nawet 70/30, komponenty tworzące warstwę dystrybucyjną powinny być wystarczająco szybkie, by taki ruch obsłużyć.

Przykłady wyboru medium

W tej części rozdziału zaprezentuję kilka sieci i określę wykorzystywane w każdej części tych sieci media. Ponieważ wybór medium uzależniony jest częściowo od tego, w której części sieci będziemy je stosowali, ważne jest, abyśmy dobrze zrozumieli, gdzie przebiegają granice pomiędzy poszczególnymi elementami sieci. Należy przy tym pamiętać, że nie wszystkie sieci mają jasno zdefiniowane granice pomiędzy poszczególnymi częściami. Mała sieć biurowa może składać się z trzech segmentów dostępowych dołączonych do rutera i wychodzącego z rutera łącza do sieci Internet, zestawianego na żądanie. Na przykład sieć pokazana na rysunku 2-2 ma rdzeń, w którego skład wchodzi sam ruter. Komponent dystrybucyjny znajduje się również w ruterze, podczas gdy komponent dostępowy może być wykonany w postaci segmentu sieci, adapterów w komputerach oraz łącza komutowanego do sieci Internet.
W tego typu sieci elementy tworzące część dostępową mogą być wykonane w dowolnej technologii, która najbardziej odpowiada użytkownikowi; ruter powinien sobie łatwo poradzić z ruchem przychodzącym z sieci dostępowych.

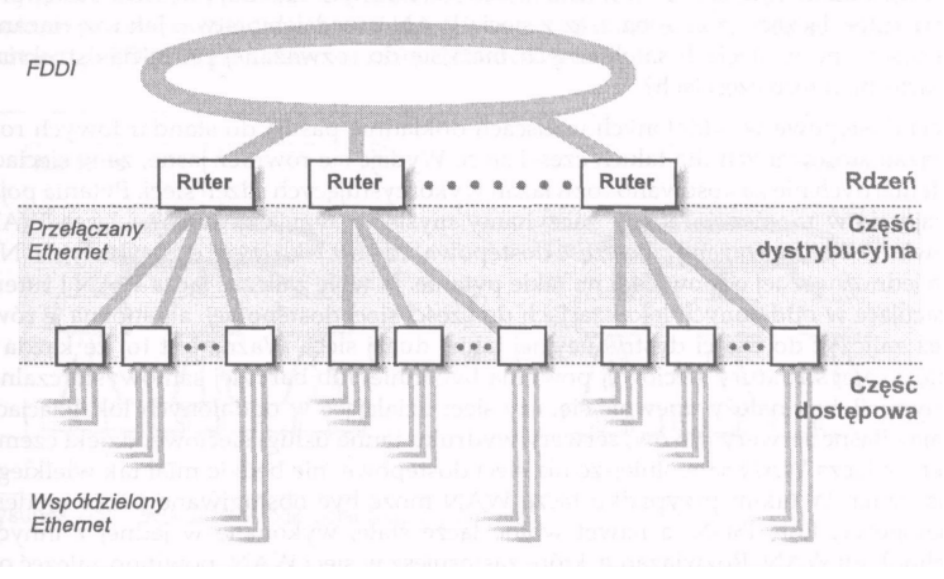


Rysunek 2-2: Niewielka sieć bez wyraźnie wydzielonej części dystrybucyjnej

Z drugiej strony mamy czasem do czynienia z sieciami dużego ośrodka akademickiego, gdzie jeden wydział może wykorzystywać setki sieci dostępowych, a rutery zlokalizowane są w różnych budynkach uczelni. Część dystrybucyjna takiej sieci będzie łączyła te rutery z ruterami pracującymi w centrum przetwarzania danych. Rutery pracujące w centrum przetwarzania danych oraz segment sieci przyłączający je do rdzenia pokazane zostały na rysunku 2-3. W takiej sieci łatwo jest zidentyfikować trzy elementy sieci.

Jeśli założymy, że sieci dostępowe wykonane są w technologii Ethernet (powszechnie stosowane rozwiązanie), to komponenty dystrybucyjne mogą być wykonane w technologii współdzielonego lub przełączanego Ethernetu lub jako kombinacja tych

dwóch rozwiązań. Dopóki matryca ruchu w sieci odpowiada którejś z wersji zasady 80/20, zastosowane w części dystrybucyjnej rozwiązanie powinno być odpowiednie. Rdzeń łączący te sieci powinien mieć jednak większą przepustowość od przełączanego Ethemetu. Jeśli policzy się zagregowane pasmo sieci dystrybucyjnych, nawet przy założeniu ruchu 90/10, to rdzeń wydaje się być trochę za słaby. Zamiast tego rozwiązania powinno się chyba pomyśleć o zastosowaniu czegoś w rodzaju pierścienia FDDI.

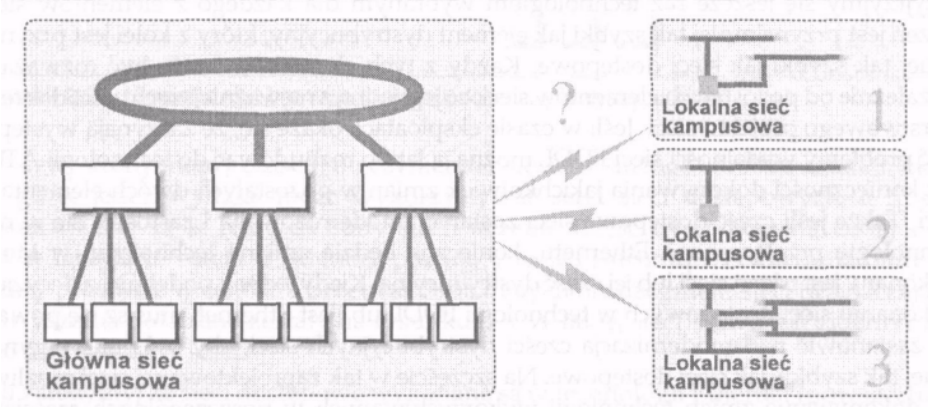


Rysunek 2-3: Duża sieć zbudowana z wielu sieci dostępowych i ruterów

Przyjrzyjmy się jeszcze raz technologiom wybranym dla każdego z elementów sieci. Rdzeń jest przynajmniej tak szybki jak element dystrybucyjny, który z kolei jest przynajmniej tak szybki jak sieci dostępowe. Każdy z tych elementów może być rozważany niezależnie od pozostałych elementów sieci, co jest jedną z najważniejszych zalet dobrego warstwowego projektu sieci. Jeśli w czasie eksploatacji okaże się, że zaczynają występować problemy wydajności sieci FDDI, można ją łatwo rozbudować do technologii ATM, bez konieczności dokonywania jakichkolwiek zmian w pozostałych dwóch elementach sieci. Także jeśli część dostępowa sieci zostanie zmodernizowana i zastosuje się w niej technologię przełączanego Ethemetu, konieczna będzie zmiana technologii, w której wykonany jest rdzeń sieci lub jej część dystrybucyjna. Kiedy jednak podejmiesz decyzję o wykonaniu sieci dostępowych w technologii FDDI lub Fast Ethernet, musisz się poważnie zastanowić nad modernizacją części dystrybucyjnych sieci, aby były one przynajmniej tak szybkie jak sieci dostępów *2.* Na szczęście w tak zaprojektowanej sieci możliwe jest dokonywanie zmian technologii wykorzystywanych w poszczególnych częściach sieci, bez konieczności zmian pozostałych jej elementów.

W kolejnych dwóch przykładach przyjrzymy się, jak powinno się projektować łącza WAN, przez które połączone są części wielkiej sieci uniwersyteckiej lub korporacyjnej. Jako pierwszy przykład przeanalizujemy sieć, w której główne centrum przetwarzania danych znajduje się w jednym miejscu, tworząc centralny punkt sieci, do którego przez łącza WAN dołączone są lokalizacje satelitarne. Sieć ta pokazana jest na rysunku 2-4. Załóżmy, że centralna sieć kampusowa jest zbudowana w taki sam sposób jak sieć, którą wcześniej opisywałem, z wyraźnie zdefiniowanymi komponentami. Załóżmy również, że w lokalizacjach satelitarnych znajdują się sieci dostępowe oraz ruter, łączący je ze sobą oraz z siecią WAN przedsiębiorstwa. Jak rozwiązania zastosowane w sieciach satelitarnych mają się do rozważanej przez nas struktury opartej na trzech częściach?

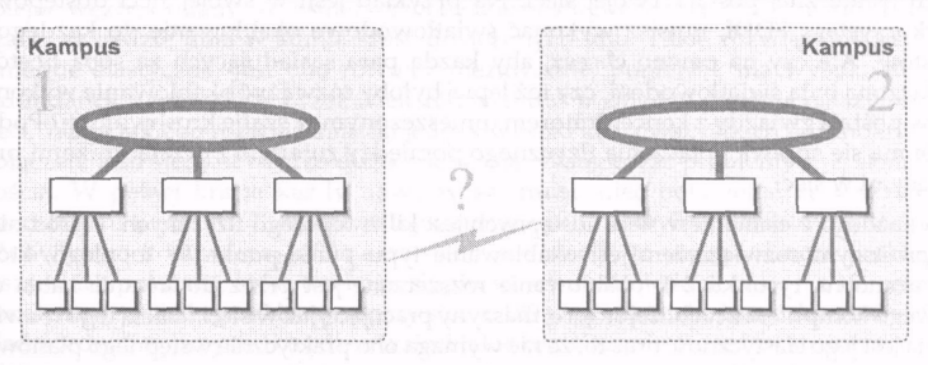
Sieci dostępowe w oddalonych miejscach dokładnie pasują do standardowych rozwiązań stosowanych dla takich części sieci. Wydaje się również jasne, że w sieciach satelitarnych nie zastosowano rozwiązań wykorzystujących rdzeń sieci. Pytania pojawiają się w momencie, kiedy zaczynamy myśleć o tym, czy rutery i łącza WAN powinny być rozważane jako część dostępowa, czy też jako część dystrybucyjna. Nie ma jednoznacznej odpowiedzi na takie pytanie. Ja wolę zaliczać łącza WAN i rutery pracujące w oddalonych lokalizacjach do części sieci dostępowej, ale można je również zaliczyć do części dystrybucyjnej takiej dużej sieci. Ważne jest to, że każda z gałęzi całej struktury sieciowej powinna być mniej lub bardziej samowystarczalna. Innymi słowy, należy upewnić się, czy sieci działające w oddalonych lokalizacjach mają własne serwery plików, serwery wydruku i inne usługi sieciowe, dzięki czemu fakt, że łącza WAN są wolniejsze niż sieci dostępowe, nie będzie miał tak wielkiego znaczenia. W takim przypadku łącze WAN może być obsługiwane przez modem analogowy, linię ISDN, a nawet wolne łącze stałe, wykonane w jednej z innych technologii WAN. Rozwiązanie, które zastosujesz w sieci WAN, powinno *zależeć* od ilości danych przesyłanych między różnymi miejscami sieci.



Rysunek 2-4: Główna część kampusowa z sieciami satelitarnymi

Wybór medium -co z czym połączyć?

Dla drugiego przykładowego rozwiązania sieci łączącej kilka lokalizacji rozważmy topologię pokazaną na rysunku 2-5. W sieci tej mamy dwa duże ośrodki uniwersyteckie (lub więcej ośrodków), w których znajdują się ich własne struktury sieci, połączone przez jedno lub więcej łącze WAN. Staje się oczywiste, że nie ma sensu zaliczanie komponentów którejkolwiek z sieci kampusowych do części dostępowej naszej przykładowej sieci. Znacznie rozsądniejsze jest traktowanie każdej z sieci kampusowych jako niezależnej sieci, która posiada rdzeń sieci, część dystrybucyjną i komponenty dostępowe. W naszym przykładzie rdzeniem sieci A jest mała sieć ATM, łącząca rutery pracujące w głównym centrum przetwarzania danych, podczas gdy w sieci B może to być większa struktura w technologii FDDI łącząca rutery w różnych budynkach.



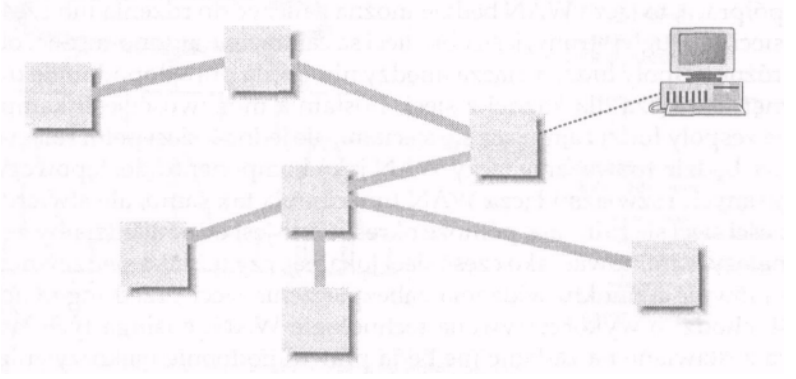
Rysunek 2-5: Dwa duże ośrodki połączone w jedną sieć

Łącza WAN, którymi połączone są poszczególne sieci kampusowe, mogą być tu zaliczone do części dostępowych obu tych sieci, do ich części dystrybucyjnej, do rdzenia sieci lub mogą być traktowane jako zewnętrzne łącza sieci kampusowych. To, które z przejść będzie właściwe, zależy od tego, jak oba ośrodki ze sobą współpracują. Jeśli są one centralnie zarządzane, a pomiędzy ośrodkami danych w obu sieciach jest ścisła współpraca, to łącza WAN będzie można zaliczyć do rdzenia lub części dystrybucyjnej sieci. Z drugiej strony, jeśli obie sieci są całkowicie autonomiczne, obsługiwane przez różne zespoły ludzi, to łącza między nimi będą prawdopodobnie traktowane jako zewnętrzne łącza dla każdej z sieci. I ostatnia możliwość; jeśli kampusy mają niezależne zespoły ludzi zajmujące się sieciami, ale jedna z sieci pełni rolę nadrzędną, to właściwe będzie rozważanie łączy WAN jako komponentu dostępowego. W każdym z opisanych rozwiązań łącza WAN funkcjonują tak samo, ale stwierdzenie, do której z części sieci się zaliczają, pomoże określić, kto jest odpowiedzialny za ich pracę oraz czy należy je traktować jako część sieci lokalnej, czy też jako sieć zewnętrzną. Jest to ważne głównie z punktu widzenia zabezpieczenia sieci przed ingerencją z zewnątrz. Jeśli chodzi o wykorzystywane technologie WAN, obsługa tych łączy przez połączenia zestawiane na żądanie nie będą prawdopodobnie najkorzystniejszym finansowo rozwiązaniem, ponieważ między sieciami będzie prawdopodobnie następowała nieprzerwana wymiana danych. Lepiej będzie wykorzystać wolne łącze stałe, choć nadal otwarta pozostaje kwestia przepustowości tego łącza.

Fizyczna topologia sieci

Kiedy już dokonasz wyboru medium, które będzie wykorzystywane w każdej z części sieci, zastanów się nad fizyczną topologią sieci. W sytuacji, gdy logiczna topologia sieci jest częścią definicji związanej z wyborem technologii, w jakiej pracuje sieć, a większość aspektów topologii fizycznej będzie pod wpływem, jeśli nie podyktowanych *przez* medium, które zostało wybrane, nadal pozostaje kilka kwestii dotyczących ostatecznej postaci Twojej sieci. Na przykład jeśli w swojej sieci dostępowej wykorzystasz FDDI, musisz wykonać światłowodowe okablowanie do każdego z hostów. Ale czy na pewno chcesz, aby każda para sąsiadujących ze sobą hostów połączona była światłowodem, czy też lepiej byłoby rozważyć okablowanie wykonane w postaci gwiazdy z koncentratorem umieszczonym w szafie krosowniczej? Podobnie ma się sprawa połączenia fizycznego pomiędzy ruterami i przełącznikami pracującymi w sieci.

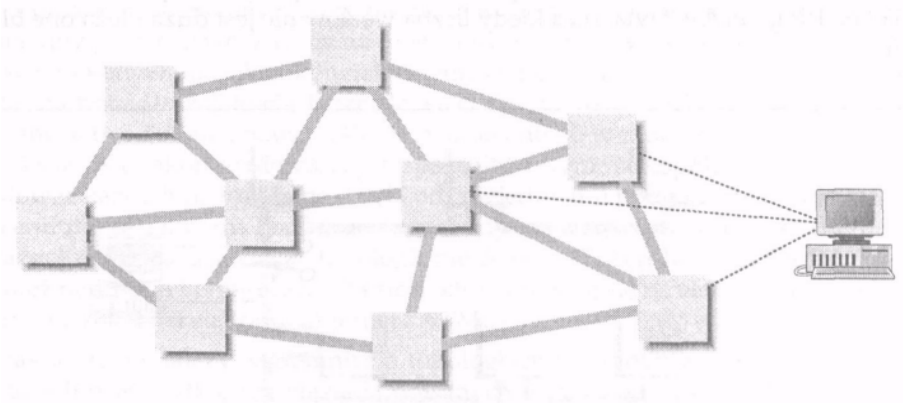
Dla każdego z elementów sieci dostępnych jest kilka topologii fizycznych. Wśród nich najprostszym rozwiązaniem jest okablowanie typu punkt-punkt. W topologii, którą pokazano na rysunku 2-6, okablowanie rozszerzane jest przez dodawanie kabla do nowego komputera z najbliżej stojącej maszyny pracującej już w sieci. Zaletą tego rozwiązania jest jego elastyczność oraz to, że nie wymaga ono praktycznie wstępnego planowania topologii sieci. Połączenia punkt-punkt są powszechnie stosowane w sieci WAN, gdzie koszty użytkowania łączy dzierżawionych zależą często od ich długości. Niemniej topologia zrealizowana w oparciu o połączenia punkt-punkt staje się po dodaniu nowych połączeń dość chaotyczna. W tak zorganizowanej sieci praktycznie niemożliwe jest ograniczenie wpływu zmian w okablowaniu do małego, przewidywalnego zestawu maszyn, ponieważ wzajemne zależności połączeń są zbyt duże.



Rysunek 2-6: Dodawanie kolejnego komputera w sieci punkt-punkt

Fizyczna topologia sieci

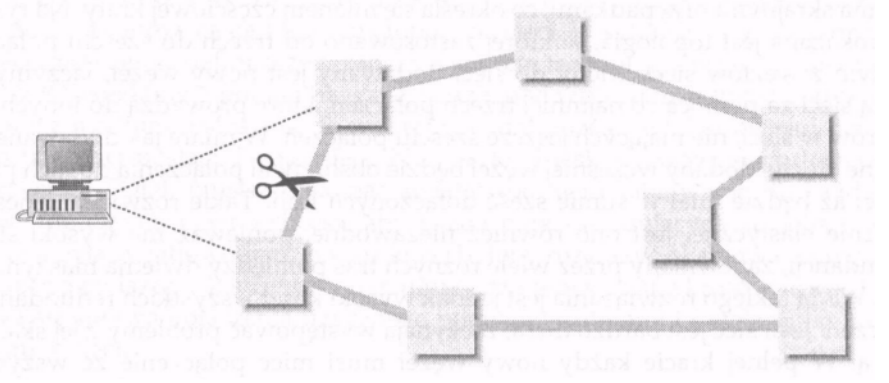
Topologia kraty pozwala na większe uporządkowanie połączeń. W kracie łącza dla nowej maszyny zestawiane są pomiędzy jej portami a kilkoma maszynami, które już pracują w sieci. Skrajnym rozwiązaniem jest zestawienie bezpośredniego połączenia z jedną maszyną w sieci, co daje sieć punkt-punkt. Drugą skrajnością jest zestawienie połączeń pomiędzy każdą z dwóch maszyn pracujących w sieci, co daje tzw. pełną kratę. Bardziej prawdopodobnym rozwiązaniem będzie jednak coś pomiędzy tymi dwoma skrajnymi przypadkami, co określa się mianem częściowej kraty. Na rysunku 2-7 pokazana jest topologia, w której zastosowano od trzech do sześciu połączeń z każdym z węzłów sieci. Kiedy do sieci dodawany jest nowy węzeł, łączymy go z resztą sieci za pomocą co najmniej trzech połączeń, które prowadzą do innych komputerów w sieci, nie mających jeszcze sześciu połączeń. W miarę jak dodawane będą kolejne węzły, dodany wcześniej węzeł będzie obsługiwał połączenia do nich prowadzące, aż będzie miał w sumie sześć dołączonych linii. Takie rozwiązanie jest niezmiernie elastyczne. Jest ono również niezawodne, ponieważ ma wysoki stopień redundancji, zapewniany przez wiele różnych tras pomiędzy dwiema maszynami w sieci. Wadą takiego rozwiązania jest jednak wysoki koszt wszystkich redundantnych połączeń. Jeśli sieć jest bardzo duża, zaczynają występować problemy z jej skalowalnością. W pełnej kracie każdy nowy węzeł musi mieć połączenie ze wszystkimi pozostałymi węzłami, co oznacza wykonanie wielu nowych połączeń dla każdego dodawanego komputera. Jeśli nasza sieć ma 4 węzły, to nie ma jeszcze problemu; wszystkich połączeń, które trzeba obsługiwać, jest sześć. Jednak w sieci z 10 węzłami konieczna jest obsługa 45 łączy, a przy sieci o 100 węzłach liczba łączy skacze do 4 000! Nadal jednak w przypadku rdzenia sieci takie rozwiązanie może być stosowane.



Rysunek 2-7: Dodawanie maszyny do topologii częściowej kraty

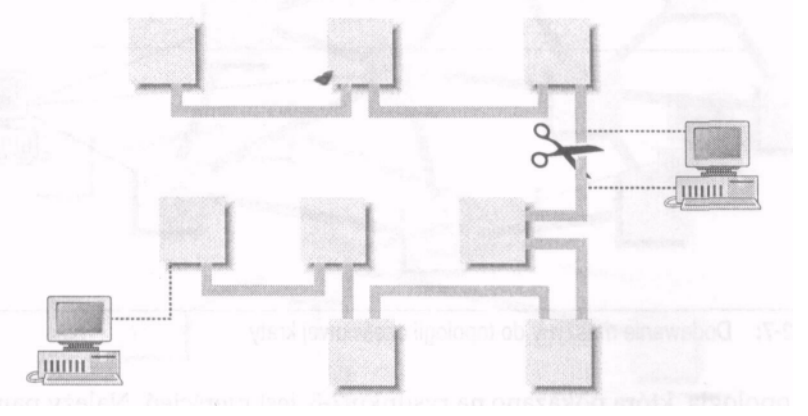
Trzecią topologią, którą pokazano na rysunku 2-8, jest pierścień. Należy pamiętać, że cały czas mówimy o topologii fizycznej, a zwłaszcza o sposobie prowadzenia kabli. W topologii pierścienia każdy węzeł dołączony jest do dwóch innych węzłów (każdy po innej stronie dołączanego węzła). Kiedy konieczne jest dodanie do sieci nowego węzła, połączenie pomiędzy dwoma sąsiednimi węzłami jest przerywane i dodawane są połączenia pomiędzy nowym węzłem a każdym z dwóch sąsiadujących ze sobą wcześniej węzłów.

Taka struktura połączeń ma cechy elastyczności połączeń punkt-punkt w sensie wzajemnego układu węzłów i mechanizmu zarządzania pracą sieci.



Rysunek 2-8: Dodawanie maszyny do topologii pierścienia

Główną wadą takiego rozwiązania jest trudność w określeniu, pomiędzy które węzły należy wstawić nowy węzeł, zwłaszcza kiedy w pobliżu węzła, który chcemy dołączyć do sieci, nie ma żadnych innych węzłów sieci. Niemniej wybór przebiegu połączeń jest dokonywany w naturalny sposób w sieciach opartych na pierścieniu, takich jak Token Ring i FDDI, zwłaszcza kiedy liczba węzłów nie jest duża i leżą one blisko siebie.



Rysunek 2-9: Dodawanie maszyny na końcach magistrali jest łatwe - w środku jest już trudniej

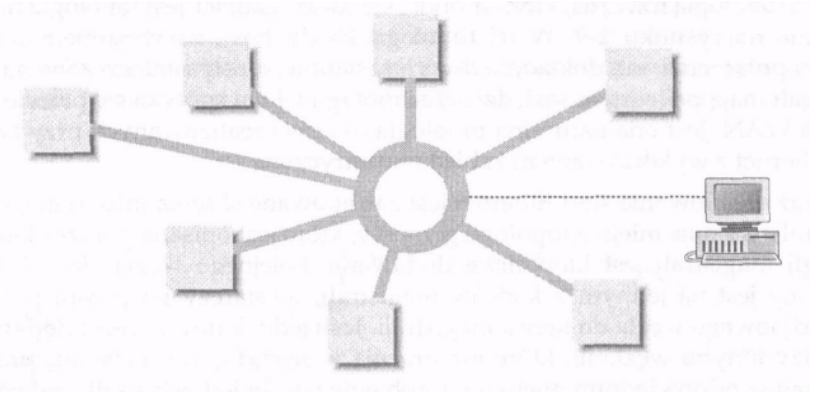
Fizyczna topologia sieci

Czwartą topologią *fizyczną,* którą spotyka się coraz rzadziej, jest topologia magistrali, pokazana na rysunku 2-9. W tej topologii każdy host, za wyjątkiem hostów na końcach połączenia, ma dokładnie dwóch sąsiadów. Hosty umieszczone na końcach magistrali mają po jednym sąsiedzie. Technologii tej nie spotyka się prawie nigdy w sieciach WAN. Jest ona naturalną topologią dla sieci realizowanych przy tworzeniu sieci Ethernet z wykorzystaniem kabla koncentrycznego.

Ponieważ okablowanie sieci Ethernet jest zastępowane skrętką miedzianą, topologia magistrali ustępuje miejsca topologii gwiazdy, która jest opisana poniżej. Dużą wadą topologii magistrali jest kłopotliwe dodawanie kolejnego węzła sieci. Jeśli węzeł dodawany jest na jednym z końców magistrali, wystarczy po prostu przeciągnąć kabel od nowego węzła do końca magistrali. Jeśli jednak nowy węzeł dodawany jest pomiędzy innymi węzłami, które już pracują w sieci, to konieczne jest przerwanie magistrali w odpowiednim miejscu i dorobienie odpowiednich kabli i zakończeń. W rezultacie praca sieci jest przerywana, co prowadzi do utrudnień w obsłudze sieci, gdyż przy usuwaniu już niepotrzebnej maszyny konieczne jest również usunięcie kabli, którymi była ona dołączona do sieci.

Piątą topologią fizyczną, o której będziemy mówili, jest topologia gwiazdy, pokazana na rysunku 2-10. W topologii tej wszystkie węzły są bezpośrednio dołączone do centralnego miejsca sieci. W części dostępowej tworzącej sieć lokalną centralny punkt sieci może być tworzony przez szafę krosowniczą, a w sieci WAN może być to centrum przetwarzania danych. Topologia ta ma wiele zalet. Najważniejszą z nich jest niewątpliwie skalowalność. Każdy dodawany do sieci węzeł otrzymuje oddzielne, niezależne połączenie z koncentratorem i nie może mieć bezpośredniego wpływu na już istniejące połączenia. Ponadto ponieważ wszystkie kable zaczynają się w centralnym punkcie sieci, możliwe jest rozłączanie istniejących połączeń lub ich przenoszenie na inny port, bez wpływania na pracę innych użytkowników, a nawet bez konieczności wykonywania jakichkolwiek czynności po drugiej stronie połączeń. Topologia ta ma ponadto zaletę elastyczności sieci opartej na łączach punkt-punkt. Nowe łącze może być dodane, nawet jeśli nie planowano go w momencie rozpoczęcia prac nad siecią. Na zakończenie należy wspomnieć o tym, że topologia gwiazdy może emulować każdą inną topologię dzięki odpowiedniemu przekrosowaniu połączeń w koncentratorze. Fizyczna konfiguracja gwiazdy używana jest często w sieci Ethernet i w każdej sieci pracujących w topologii pierścienia (Token Ring, FDDI itd.). Jest to również naturalna konfiguracja dla sieci, które opierają się na centralnym przełączniku (na przykład przełączany Ethernet i ATM).

Na zakończenie należy wspomnieć o topologiach hybrydowych, łączących w sobie niektóre lub wszystkie rozwiązania opisanych wyżej podstawowych topologii. Na przykład możemy zdecydować się na budowę grupy sieci w topologii gwiazd połączonych ze sobą za pomocą pierścienia. Możemy również stworzyć grupę sieci w oparciu o pierścienie połączone ^e sobą w topologii gwiazdy. W rzeczywistości rozwiązania hybrydowe są częściej stosowane niż jakiekolwiek z rozwiązań stosujących tylko podstawową topologię. Wynika to głównie z konieczności obsługi różnych mediów w różnych komponentach sieci, z kosztów, a także z faktu, że projektant sieci musi uwzględnić pewne ograniczenia fizyczne.

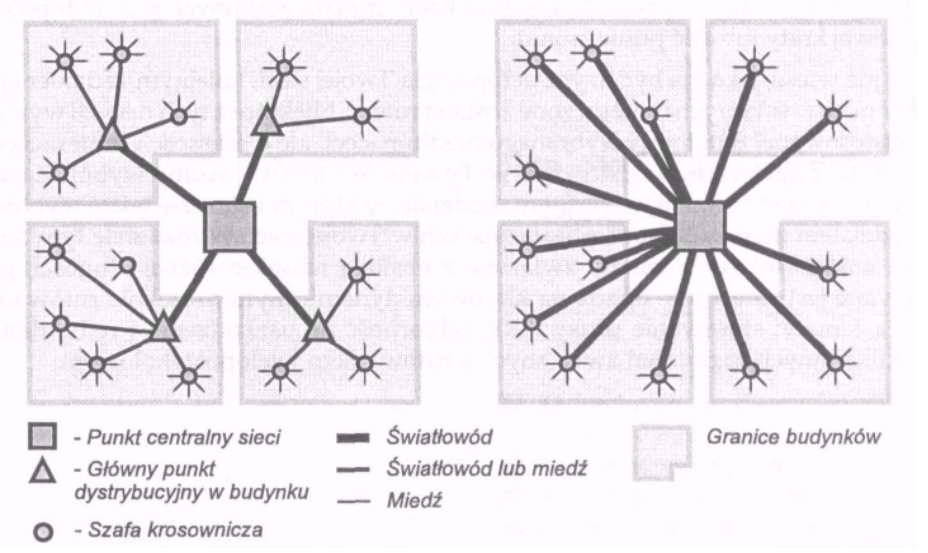


Rysunek 2-10: Dodawanie komputera do sieci wykonanej w topologii gwiazdy

Najczęściej wykorzystywaną topologią sieci hybrydowej i jednocześnie rozwiązaniem, które osobiście polecam do zastosowań w sieciach kampusowych, jest topologia gwiazdy gwiazd. W topologii tej można zwykle wyróżnić dwa lub trzy poziomy gwiazd. Rysunek 2-11 pokazuje obie opcje. W centralnym punkcie sieci znajduje się krosownica, z której gwiaździście rozchodzą się światłowody do poszczególnych budynków. Następnie, za pomocą kolejnej gwiazdy wykonanej światłowodami (lepsze rozwiązanie) lub miedzią, wykonuje się połączenia wewnątrz budynku. Połączenia te prowadzą z głównego punktu dystrybucyjnego do każdej szafy krosowniczej w budynku. Jeśli wolisz rozwiązanie oparte na dwupoziomowej gwieździe, połączenia światłowodowe wychodzące z centralnego punktu sieci musisz poprowadzić bezpośrednio do wszystkich szaf krosowniczych. Ostatnim elementem w obu rozwiązaniach jest okablowanie, wykonane miedzią w topologii gwiazdy, prowadzące z szaf krosowniczych do biurek użytkowników. W rozwiązaniach tego typu powinno się stosować systemy okablowania możliwie najwyższej jakości. Na przykład nawet jeśli okablowanie kategorii 5 jest za dobre dla sieci Ethernet lub Token Ring, to jest ono niewiele droższe od okablowania kategorii 4, a w przyszłości będzie mogło obsługiwać topologię CDDI, Fast Ethernet lub ATM. Należy pamiętać, że okablowanie może być bez zmian wykorzystywane przez 10, a nawet więcej lat. Pomimo że okablowanie jest najprostszym komponentem sieci, w praktyce najtrudniej jest je zmienić na inne, lepsze. Znacznie trudniej jest od nowa okablować budynek niż rozbudować konfigurację rutera.

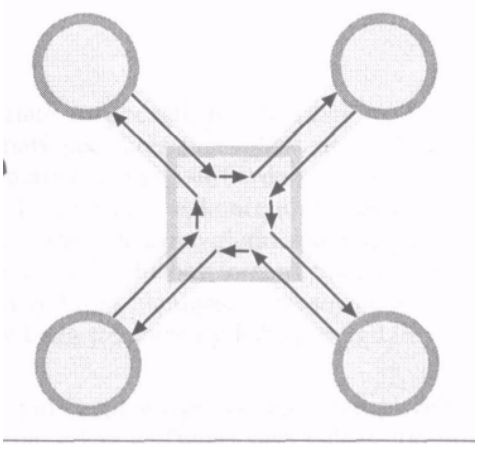
Topologia hybrydowa jest jedną z najczęściej stosowanych, głównie z powodu swej elastyczności. Jeśli do każdego promienia gwiazdy doprowadzisz więcej niż jeden kabel, możliwe będzie skonfigurowanie każdej z topologii opisanych wyżej, a także wielu prostszych topologii hybrydowych. Na przykład aby z gwiazdy zrobić pierścień, wystarczy mieć jeden kabel, który wychodzi do węzła, i jeden, który tą samą drogą z niego wraca.

Fizyczna topologia sieci



Rysunek 2-11: Trójwarstwowa (na lewo) i dwuwarstwowa (na prawo) topologia gwiazdy

Następnie wystarczy połączyć wychodzący z każdego węzła kabel z kablem wchodzącym do kolejnego węzła, co w efekcie da pierścień, jak pokazano na rysunku 2-12. W rezultacie otrzymujemy logiczną topologię pierścienia zbudowaną na podstawie fizycznej topologii gwiazdy.



Rysunek 2-12: Przy wykorzystaniu dodatkowych kabli topologię gwiazdy można zamienić w pierścień

Na podobnej zasadzie, przez dodawanie kabli, można zbudować sieć w topologii częściowej kraty lub sieć punkt-punkt.

Kiedy już wiesz, jaka ma być fizyczna topologia Twojej sieci, kolejnym zadaniem jest wybór miejsc, w których umieszczone zostaną rutery. Niektóre z tych decyzji wynikają z zastosowanej topologii i wybranego medium sieci, ale o miejscach umieszczenia większości ruterów musisz zdecydować Ty sam. Jest to Twój wolny wybór. Zagadnienie to opisane zostanie w kolejnym rozdziale, w którym zajmę się także wyborem i przydziałem masek dla podsieci pracujących w Twojej sieci. W rozdziale tym omówione zostaną również tematy związane z obsługą masek o różnej długości, gdy stosowane jest nitowanie oparte na klasowym dynamicznym protokole rutowania, a także tematy: stosowanie proxy ARP, odporność na uszkodzenia i redundancja oraz kilka innych zagadnień związanych z rutowaniem wieloprotokołowym.

Projektowanie sieci - część 2

3

Koncentratory, mosty, przełączniki i rutery
Rozmieszczenie ruterów
Podział na podsieci i wyznaczanie masek
Proxy ARP jako alternatywa dla podsieci
Redundancja i odporność na uszkodzenia
A co z sieciami wieloprotokołowymi?

W poprzednim rozdziale rozpoczęliśmy dyskusję na temat projektowania sieci i omówiliśmy takie tematy jak określenie celów, architektura sieci, wybór medium i topologia fizyczna. Tematy te wydają się bardzo abstrakcyjne i mogą być analizowane bez odwoływania się do rzeczywistej konfiguracji sieci i organizacji firmy. Oczywiście powinny być opracowywane z uwzględnieniem fizycznego projektu sieci. Dzięki opisom z poprzedniego rozdziału powinieneś mieć jasno sprecyzowaną opinię na temat topologii fizycznej, którą planujesz zastosować w swojej sieci, nawet jeśli nie wiesz jeszcze, którędy będą przebiegały kable, ani gdzie będą rozmieszczone szafy krosownicze.

Rozdział ten jest dalszym ciągiem dyskusji na temat projektowania sieci, rozpoczynającej się od określenia, gdzie w Twojej sieci należy lub można rozmieścić rutery. Zadanie to jest znacznie bardziej konkretne niż rozmyślanie na temat rodzaju użytych w sieci mediów lub rodzaju topologii fizycznej, którą należy zastosować w sieci. Aby dobrze wykonać to zadanie, musisz mieć jasny obraz fizycznych ograniczeń sieci oraz znać organizację firmy.

Po przedyskutowaniu sposobu rozmieszczania ruterów zajmiemy się tematem wyboru i przydzielania masek podsieci i numerów.

Będziemy mówili o maskach stałej i zmiennej długości, sposobie wykorzystywania masek o zmiennej długości w przypadku stosowania klasowego dynamicznego protokołu rutowania, przydzielani! numerów podsieci w sposób pozwalający na tworzenie sieci zagregowanych ora: wykorzystaniu proxy ARP do obsługi hostów, które nie mogą pracować z zastosowanym w sieci schematem podsieci. Na zakończenie zajmiemy się tematem odporność sieci na błędy i redundancją oraz nitowaniem wieloprotokołowym.

Koncentratory, mosty, przełączniki i rutery

Zanim omówimy rozmieszczenie ruterów w sieci, zastanówmy się, czy w ogóle s, one potrzebne. Czy nie lepiej wykorzystać urządzenia takie jak mosty lub przełączniki? Jest to bardzo ważne pytanie, często zadawane przez sprzedawców. Każdy rodzaj urządzenia ma właściwe dla siebie miejsce w sieci. Ważne jest, aby zrozumieć różnic pomiędzy tymi urządzeniami, a także ich słabe strony.

Najprostsze urządzenie sieciowe to koncentrator, który jest prawdopodobnie najczęściej spotykanym urządzeniem aktywnym w Twojej sieci. Koncentratory stosowane są w większości popularnych technologii LAN, takich jak Ethernet, Token Ring ora: FDDI, i w miarę łatwo wybrać je z oferty różnych producentów, zainstalować obsługiwać. Nie będziemy zajmowali się szczegółami dotyczącymi wyboru koncentratorów, ponieważ temat ten jest dość dobrze znany. Wybrane przez Ciebie medium dla sieci może wymagać koncentratora lub nie. Urządzenia te są u większości producentów takie same i z reguły różnią się tylko brakiem lub obecnością interfejsu di zarządzania ich pracą. Zupełnie inaczej sprawa ma się z urządzeniami takimi ja] mosty, przełączniki LAN i rutery.

Kilka lat temu gorącym tematem w środowisku sieciowym była kwestia, czy siec należy budować z użyciem mostów czy ruterów. Zwolennicy rozwiązań opartych n mostach narzekali, że rutery zmniejszają szybkość pracy sieci, obniżają jakość je usług i są zbyt skomplikowane do zarządzania i utrzymania. Z kolei zwolennicy ruterów twierdzili, że mosty nie zapewniają odpowiedniego stopnia kontroli prac; sieci i nie pozwolą się jej rozrastać. Obie grupy miały rację, ale jak zapewne wiesz wygrali zwolennicy ruterów, głównie z powodów większej skalowalności sieci zbudowanej w oparciu o rutery. Rzeczywiście sieci rozrosły się, i to bardzo.

Dlaczego sieci zbudowane z użyciem mostów dobrze się nie skalują? Odpowiedz tkwi w uproszczonej obsłudze transmisji danych, jaką wykonują. Kiedy most odbierze z sieci ramkę, sprawdza jej adres przeznaczenia i porównuje ją z tablicą adresów którą zna. Jeśli znajdzie taki sam adres, podejmuje decyzję o tym, czy przekażą ramkę do innego segmentu, opierając się na informacji, czy została ona wysłana : segmentu sieci, z której pochodzi jej adres przeznaczenia. Jeśli adres nadawcy i adres przeznaczenia ramki nie pochodzą z tego samego segmentu, most przekazuje ramkę di właściwego segmentu sieci. Jeśli most wie, że ramka wysłana została z tego samego segmentu sieci, z którego pochodzi jej adres przeznaczenia, ignoruje ją, wiedząc, ż maszyna, do której przesyłane są dane, odbierze je bez konieczności interwencji.

Jeśli most nic nie wie o adresie przeznaczenia ramki, przekazuje ją dalej, zakładając, że adres przeznaczenia musi być gdzieś w sieci. Jeśli ramka dotrze do adresata, a ten odeśle odpowiedź, to most - przepuszczając tę odpowiedź - zapisze adres jej nadawcy w swojej tablicy adresów. Tak więc most uczy się sieci obserwując ruch ramek i analizując adres źródłowy w ramkach, które odbiera.

Proces ten działa doskonale i jest podstawą mostowania sieci. Istnieje jednak grupa ramek, które most zawsze będzie przesyłał pomiędzy segmentami sieci. Są to sprzętowe ramki typu broadcast i multicast. Ponieważ ramki takie powinna odbierać każda maszyna pracująca w sieci, muszą być one zawsze przesyłane przez most, tzn. muszą przepływać w sieci.

Ramki typu broadcast i multicast ograniczają skalowalność sieci zbudowanej z wykorzystaniem mostów. W miarę jak w sieci rośnie liczba komputerów, proporcjonalnie rośnie liczba ramek broadcast. Jeśli średnio jedna maszyna w sieci wysyła jeden broadcast co 10 sekund, to w sieci, w której pracuje 1000 maszyn, w ciągu jednej sekundy przesyłanych będzie około 100 pakietów typu broadcast. Jeśli w sieci jest 10000 maszyn, to liczba pakietów broadcast rośnie do 1000 na sekundę. W sieci o 100000 maszyn pakietów takich będzie 10000 w jednej sekundzie!

Co złego jest w ramkach typu broadcast? Pomyśl, że każdy taki pakiet musi być odebrany przez każdą maszynę w sieci, co oznacza, że będzie przekazywany *przez* wszystkie mosty, jakie napotka po drodze. Oznacza to, że wszystkie wysyłane w sieci ramki broadcast pojawiają się w każdym jej segmencie. Jeśli teoretyczne maksimum przesyłanej w sieci Ethernet liczby pakietów na sekundę, niezależnie od tego, czy są to pakiety broadcast, czy nie, wynosi 14800, to widać, że w sieci z 10000 hostów większość ruchu generowana będzie pakietami broadcast.

Ale pasmo sieci to nie jedyny problem z ramkami broadcast. Każda taka ramka dociera do każdego hosta, który musi ją odebrać i sprawdzić, czy zawiera ona informacje interesujące dla tego hosta. Każda maszyna odbierając broadcast musi na chwilę przerwać przetwarzanie danych i zająć się zawartością tej ramki. Zwykle będzie to jedno przerwanie na każdą ramkę, co w sieci o 100000 hostów daje 10000 przerwań na sekundę. Taka liczba przerwań pochodzących z sieci może sprawić, że wolniejsza maszyna lub taka, która ma wolniejszy stos protokołów, po prostu stanie i nie będzie obsługiwała nic poza pakietami broadcast.

Czy rzeczywiście można założyć, że komputery wysyłają ramkę broadcast co 10 sekund? Zastanówmy się, do czego wykorzystywane są pakiety broadcast i multicast. W zestawie protokołów IP pakiety broadcast wykorzystywane są przy rozpoznawaniu adresów i nazw hostów *(Address Resolution Protocol),* uaktualnianiu tras rutowania, przesyłaniu informacji dla serwisów takich jak rwho i innych aplikacji. Multicasty mogą być używane częściowo do tych samych funkcji, głównie do uaktualniania tras rurowania i przy przesyłaniu pakietów przez nowsze wersje niektórych serwisów. Należy pamiętać, że z punktu widzenia sieci zbudowanych na mostach pakiety multicast niczym się nie różnią od broadcast i traktowane są identycznie. Niektóre z pakietów broadcast i multicast są wysyłane regularnie. Na przykład usługa rwho i niektóre protokoły rutowania wysyłają informacje co 30 sekund. Podczas gdy usługa

rwho wysyła z tą częstotliwością jeden pakiet, niektóre protokoły rutowania, takie jak RIP, wyślą tyle pakietów, ile potrzeba do przesłania całej informacji o rutowaniu. W dosyć dużej sieci może to być 10, a nawet więcej pakietów.

Inne protokoły również mają wpływ na ruch generowany przez pakiety broadcast i multicast. Rodziny protokołów takie jak AppleTalk często wykorzystują pakiety broadcast i multicast do lokalizacji zasobów w sieci, rutowania i przydzielania adresów. Także protokoły takie jak IPX firmy Novell (stosowany w systemie Netware) również często je stosują w rozgłaszaniu usług i lokalizacji zasobów.

Pamiętając o wszystkich opisanych wyżej rodzajach pakietów broadcast i multicast, nietrudno uwierzyć, że liczba wysyłanych w ciągu 10 sekund ramek tego typu jest bardzo duża. Bardzo prawdopodobne jest, że mieszanka różnych maszyn i protokołów, z którymi one pracują, spowoduje, że liczba ta będzie znacznie większa.

Dlaczego więc problemy związane z pakietami broadcast i multicast nie dotyczą sieci o budowie opartej na ruterach? Dlaczego sieci wykorzystujące rutery skalują się lepiej niż sieci mostowane? Aby odpowiedzieć na to pytanie, musisz zrozumieć, czym różni się nitowanie pakietów od przekazywania ramek przez mosty.

Czym różni się rutowanie?

Napisałem wcześniej, że most decyduje o tym, czy przesłać ramkę, czy nie, na podstawie sprzętowego adresu przeznaczenia tej ramki. Jeśli adres przeznaczenia jest nieznany lub wiadomo, że adresat znajduje się w segmencie innym niż segment, z którego ramka została nadesłana, to most przekazuje taką ramkę dalej. Ruter podejmuje identyczną decyzję podczas rutowania pakietu. Różnica polega jednak na tym, że ruter przygląda się adresowi warstwy sieci, a nie adresowi sprzętowemu, i na podstawie takiego adresu podejmuje decyzję. Ale jeśli byłaby to jedyna różnica pomiędzy tymi technologiami, to sieci rutowane nie skalowałyby się lepiej od sieci o budowie opartej na mostach.

Prawdziwa różnica polega na tym, że adresy sieciowe są przydzielane z uwzględnieniem topologii sieci. Przypisywane są w taki sposób, że w jednym segmencie sieci wszystkie adresy mają taki sam początek (numer podsieci). Natomiast adresy sprzętowe przydzielane są przez producentów kart sieciowych i nie mają żadnego związku z miejscem w sieci, w którym znajduje się urządzenie z interfejsem w postaci karty sieciowej. Przydzielanie adresów z uwzględnieniem topologii sieci pozwala na większe skupienie informacji o tej sieci. Most działający w sieci, w której pracuje 1000 hostów, musi przechowywać informację o 1000 adresach przeznaczenia, aby właściwie podejmować decyzje o przekazywaniu ramek pomiędzy segmentami sieci, podczas gdy ruter w tej samej sieci musi przechowywać w pamięci jedynie trasę do 10 lub niewielu więcej przedrostków adresów.

Agregowanie informacji jest główną zaletą rutowania. Pozwala ono r a lepszą skalowalność sieci, choć nie tylko. Most musi przeglądać każdą ramkę nadsyłaną z dołączonych do niego segmentów sieci, ponieważ dopóki nie obejrzy adresu przeznaczenia umieszczonego w ramce, to nie wie, czy ramka ta powinna być przesłana dalej.

Z drugiej strony ruter nie musi przeglądać każdego pakietu, ponieważ część decyzji o tym, czy pakiet ma być przesłany do innego segmentu sieci, została podjęta przez nadawcę tego pakietu. Jeśli nadawca stwierdzi, że adres przeznaczenia nie jest adresem lokalnego segmentu sieci, do którego nadający dane host jest dołączony (korzystając z odpowiedniego mechanizmu zaszytego w protokół), to wysyła pakiet bezpośrednio do rutera, umieszczając jego sprzętowy adres jako adres przeznaczenia. Tak więc ruter musi odbierać tylko te pakiety, które są do niego adresowane, co redukuje liczbę pakietów, które musi przetwarzać.

Mimo tych różnic w obsłudze pakietów opisany wyżej fakt jest najważniejszym powodem lepszej skalowalności nitowanych sieci. Most musi przesyłać każdy pakiet broadcast lub multicast, ponieważ wszystkie urządzenia w sieci powinny je otrzymywać. Ponieważ ruter rozumie topologię sieci, może w inteligentny sposób zająć się przesyłaniem pakietów broadcast i multicast. Rutery tworzą domeny rozgłoszeniowe *(broadcast domains),* stanowiące części sieci, w których rozsyłane broadcast widziane są przez wszystkie pracujące tam maszyny. Ruter nie przesyła pakietów broadcast, jeśli nie jest specjalnie w tym celu skonfigurowany. Jeśli skonfiguruje się go do przesyłania pakietów broadcast i multicast, to z reguły przesyła on tylko te pakiety, które spełniają określone w procesie konfiguracji kryteria. Na przykład możliwe jest skonfigurowanie rutera tak, by przesyłał zapytania broadcast BOOTP lub DHCP do serwera oraz pakiety multicast IP do segmentów, gdzie znajdują się zarejestrowani odbiorcy. Blokując rozgłaszanie innych pakietów broadcast i multicast, ruter chroni pasmo sieci w innych segmentach i pozwala na jej rozrastanie się.

Kiedy ruter odbierze pakiet przeznaczony dla adresata, którego nie zna, i nie wie, jak taki pakiet dostarczyć, odrzuca ten pakiet i może wysłać do nadawcy komunikat informujący o błędzie. Most natychmiast prześle taki pakiet dalej, w oczekiwaniu, że z wracającej odpowiedzi dowie się, gdzie znajduje się adresat. Dzięki blokowaniu przesyłania pakietów, które są niedostarczalne, rutery dodatkowo chronią pasmo sieci.

Mówiąc w skrócie, rutowanie pozwala na większą skalowalność sieci z następujących powodów:

- Zapewnia wysoki stopień agregacji informacji dzięki adresom sieciowym przydzielanym w oparciu o topologię sieci.
- Przesuwa do wysyłającego dane hosta decyzję o tym, czy konieczna jest pomoc rutera, dzięki czemu zwalnia rutery z konieczności analizowania wszystkich pakietów przesyłanych w sieci.
- Tworzy domeny rozgłoszeniowe, pozwalając tym samym zredukować liczbę pakietów broadcast i multicast w celu ochrony pasma sieci i zapobiegania przerywaniu pracy maszyn w innych segmentach sieci przez rozgłaszane tam pakiety.
- Odrzuca pakiety o nieznanym adresie przeznaczenia zamiast przesyłać je przez całą sieć. Chroni zatem pasmo sieci, nie marnując go na przesyłanie pakietów, które i tak nigdy nie dotarłyby do adresata.

Rutery a przełączniki

Nietrudno zrozumieć, dlaczego nitowanie wygrało z łączeniem sieci przez mosty. Nie wolno jednak ignorować zalet mostów, takich jak np. prostsza konfiguracja i lepsza przepustowość. W miarę jak pracujące w sieci komputery stają się coraz szybsze, mogą one monopolizować całe dostępne w segmencie sieci lokalnej pasmo, co powoduje, że zapewnienie odpowiedniego pasma w niektórych sieciach staje się problemem. Jest to powodem rosnącej popularności przełączników sieciowych.

Przełączniki pracujące w sieci, w większości w sieci Ethernet (choć coraz częściej spotyka się przełączniki Token Ring i FDDI), zwiększają efektywne pasmo segmentu sieci poprzez zredukowanie ilości konfliktów występujących w dostępnym paśmie. Jest to prosta koncepcja. Jeśli do dyspozycji są tylko ograniczone zasoby, których zaczyna brakować, to aby temu zaradzić można pójść dwiema drogami: zwiększyć te zasoby lub zredukować zapotrzebowanie na nie. W sieciach zwiększenie dostępnego pasma sieci uzyskuje się przez zmianę medium sieci. Na przykład jeśli wymienisz całą sieć 4 Mbps Token Ring na 16 Mbps Token Ring, czterokrotnie powiększysz dostępne w sieci pasmo. Także jeśli wymienisz urządzenia aktywne i wszystkie karty Ethernet 10 Mbps na karty Fast Ethernet pracujące z szybkością 100 Mbps, to zwiększysz dziesięciokrotnie dostępne w sieci pasmo. Niemniej wymiana całego aktywnego sprzętu w sieci oraz wszystkich adapterów w komputerach jest dość kosztowna. W związku z tym próbuje się powiększyć dostępne pasmo przy maksymalnym wykorzystaniu istniejącego sprzętu. Innym rozwiązaniem jest redukowanie zapotrzebowania na zasoby, przez co pozostałe maszyny w sieci będą widziały więcej użytecznego pasma w sieci, ponieważ będzie w niej mniej połączeń. Jednym ze sposobów zredukowania zapotrzebowania na pasmo jest usunięcie z sieci kilku maszyn. Nie jest to jednak najlepszy sposób, a poza tym to krok do tyłu.

Jest to moment, kiedy przełączniki sieciowe wchodzą do gry. Każda maszyna dołączona do współdzielonego segmentu sieci jest częścią jednej *domeny kolizyjnej,* nazywanej tak dlatego, że zajęcie pasma w sieci Ethernet powoduje wzrost liczby kolizji przy rozpoczynaniu transmisji. Jeśli zmniejszymy liczbę maszyn w domenie kolizyjnej, automatycznie zwiększamy dostępne dla każdej maszyny pasmo sieci, ponieważ jest ono współdzielone przez mniejszą liczbę komputerów. W skrajnym przypadku każda maszyna będzie tworzyła własną domenę kolizyjną, ale częściej domeny kolizyjne składają się z małych grup maszyn.

Redukowanie rozmiarów domen kolizyjnych możliwe jest również przy użyciu ruterów, ale takie rozwiązanie może być raczej drogie. Pojawia się tu także dokuczliwy problem małej szybkości ruterów oraz wysokiego stopnia skomplikowania ich konfiguracji. *Zwróć* uwagę na fakt, że bardzo szybki ruter z dołączonymi 24 segmentami sieci Ethernet może kosztować ponad 100 000 dolarów. Natomiast 24-portowy przełącznik dla sieci Ethernet pozwala osiągnąć ten sam poziom posegmentowania sieci za mniej niż 8 000 dolarów. Jest to więc ogromna oszczędność. Poza tym przełącznik jest znacznie łatwiejszy do instalacji i konfigurowania i prawdopodobnie będzie pracował szybciej.

Dlaczego więc nie wyrzucić wszystkich ruterów i przekształcić całą sieć w sieć przełączaną, jak sugerują sprzedawcy przełączników? Odpowiedź będzie prosta, jeśli zdasz sobie sprawę z tego, czym naprawdę jest sieć przełączana. Ale zamiast zepsuć Ci całą przyjemność przez wyjaśnienie tego w kilku słowach, przyjrzyjmy się, jak pracuje sieć oparta na przełącznikach.

Kiedy przełącznik odbierze z sieci ramkę, musi określić, gdzie w sieci znajduje się urządzenie, dla którego przeznaczona jest ta ramka. Aby to zrobić, przełącznik analizuje sprzętowy adres przeznaczenia ramki i porównuje go z przechowywaną w pamięci tablicą. Jeśli znajdzie pasującą do siebie parę adresów, przesyła ramkę do portu wskazanego w tablicy przełączania. Jeśli nie uda mu się znaleźć takiej pary adresów, to wysyła tę ramkę *do wszystkich portów za wyjątkiem portu, z którego nadeszła ramka,* oczekując, że adresat odeśle ramkę odpowiedzi, z której przełącznik będzie mógł uaktualnić sobie tablicę przełączania, notując adres źródłowy i numer portu, na którym ta ramka została odebrana. Ramki typu broadcast i multicast rozsyłane są na wszystkie porty przełącznika, czyli docierają do całej sieci.

Chwileczkę! Czy nie jest o ta sama metoda, którą wykorzystuje most? Odpowiedź brzmi: tak! Przełącznik sieciowy to po prostu wieloportowy most. Może to być bardzo elastyczny most wieloportowy, obsługujący wiele typów mediów, z możliwością grupowania różnych portów w jedną domenę rozgłoszeniową, ale nadal jest to po prostu most. Tak więc przełączniki prowadzą do tego samego problemu skalowalności sieci, który przesądził swego czasu o losie mostów. Rozważmy na przykład sieć składającą się ze 100 segmentów, czyli domen rozgłoszeniowych, w których jest po 150 hostów. Segmenty sieci połączone są sześcioma ruterami. Pojawia się sprzedawca przełączników, który przekonuje administratora sieci (lub jego szefa), że rutery te w rzeczywistości utrudniają pracę sieci. Zamieniając rutery na przełączniki będzie można posegmentować sieć na 1000 domen kolizyjnych (w każdej po 15 hostów), co niebywale zwiększy wydajność całej sieci. Ponadto przełączniki są łatwiejsze do konfiguracji i do tego mniej kosztują.

I co się będzie teraz działo? W końcu wszystkie 15 000 hostów zacznie generować ramki broadcast i multicast. Ponieważ w sieci nie ma ruterów, wszystkie maszyny pracują w jednej domenie rozgłoszeniowej, sieć odczuje ogromny spadek osiągów. Ale bez obaw! Przełączniki są lepszym rodzajem przełączników inteligentnych i mogą być skonfigurowane (stosunkowo łatwo) tak, by można było podzielić sieć na 100 domen rozgłoszeniowych, w których znajdzie się do 10 domen kolizyjnych (każda z 15 hostami). Takie rozwiązanie utrzyma pakiety broadcast na poziomie, którym można *zarządzać,* ponieważ nie będą one propagowane poza pojedynczą domenę rozgłoszeniową.

W porządku, rozwiązaliśmy problem pakietów broadcast, ale jak sprawić, by hosty znajdujące się w 100 domenach rozgłoszeniowych mogły ze sobą rozmawiać? Oczywiście dodamy rutery, które będą nitowały pakiety pomiędzy domenami rozgłoszeniowymi. Ale cóż to? Teraz oprócz naszych ruterów, które wróciły do sieci (w to samo miejsce), mamy jeszcze kilka przełączników, które trzeba konfigurować i którymi musimy zarządzać. Tyle na temat próby pozbycia się ruterów!

Odpowiedzią na te dylematy jest zrozumienie siły tkwiącej w każdym z tych typów urządzeń i wiedza o tym, jak i gdzie każdego z nich użyć. Zastosowanie przełączników sieciowych to doskonały sposób na zredukowanie liczby połączeń obciążających pasmo poprzez zmniejszanie rozmiarów domen kolizyjnych. Gorąco polecam wykorzystywanie ich w tym celu. Ponadto, ponieważ wiele przełączników jest teraz na tyle elastycznych, że może obsługiwać po kilka domen rozgłoszeniowych, możliwe jest użycie jednego przełącznika do obsługi kilku podsieci. Z drugiej strony rutery służą do łączenia domen rozgłoszeniowych i zapewniają agregację informacji, pozwalającą sieci na rozrastanie się. Jeśli chodzi o redukowanie połączeń oszczędzających pasmo w domenie kolizyjnej, nie bardzo się *przydają,* ale trzymają pakiety broadcast i multicast tam, gdzie powinny one pozostać.

Użycie ruterów w sieci wydaje się więc nieuniknione, ponieważ pozwolą one skleić ze sobą wszystkie małe sieci. Niestety, rutery nie mają tej prostoty, jaką charakteryzują się mosty, przełączniki i koncentratory, i muszą być konfigurowane, monitorowane i traktowane ostrożnie. To wszystko sprawia, że wielu administratorów sieci przeżywa czasem ciężkie chwile, i oczywiście jest powodem powstania tej książki.

Rozmieszczenie ruterów

Po podjęciu decyzji dotyczących fizycznej topologii okablowania oraz po stwierdzeniu, że musisz użyć kilku ruterów, powinieneś zastanowić się, w których miejscach sieci należy je umieścić. Doskonałym rozwiązaniem jest umieszczenie wszystkich ruterów w centralnym miejscu sieci, gdzie będą łatwo dostępne dla personelu zajmującego się obsługą sieci. Umieszczając rutery w jednym wspólnym miejscu, zapewnisz im nieprzerwane zasilanie, specjalne klimatyzowane pomieszczenia oraz łatwy dostęp do obsługi sprzętu i rekonfiguracji. Oczywiście takie umieszczenie ruterów w jednym miejscu może nie być możliwe. Bez wątpienia trudno jest rozmieścić w ten sposób rutery w sieci, która obejmuje kilka budynków i wykorzystuje łącza WAN. Takie rozwiązanie może być również trudne do zastosowania w sieci kampusowej, gdzie użyto topologii kraty, pierścienia lub rozwiązania hybrydowego z jednym z tych komponentów w centrum sieci. W takich przypadkach nadal należy dołożyć wszelkich starań, aby zminimalizować liczbę miejsc, w których zainstalowane są rutery.

Na przykład w sieci kampusowej zbudowanej w oparciu o pierścień możliwe jest obsługiwanie kilku budynków przez jeden ruter lub małą grupę ruterów zlokalizowaną w jednym z budynków, zamiast umieszczenia rutera w każdym z budynków.

Oczywiście za każdym razem, kiedy następuje zmiana medium, konieczne będzie dodanie pewnych elementów wyposażenia, zapewniających translację pomiędzy dwoma mediami wykorzystywanymi w sieci. Pierwszym z takich elementów wyposażenia, które zostały opisane wcześniej, jest ruter, drugim - most, a trzecim - przełącznik sieci LAN.

Rozmieszczenie ruterów jest jednak czymś więcej niż tylko zidentyfikowaniem miejsc, w których łączą się ze sobą dwa różne media sieci. Miejsca rozmieszczenia ruterów określają również granice podsieci IP (domeny rozgłoszeniowe w Twojej sieci).

Rozmieszczenie ruterów

W trakcie planowania rozmieszczenia ruterów należy pomyśleć o komunikacji wewnątrz całej organizacji. Niektóre połączenia są oczywiste, na przykład ludzie z jednego działu zwykle częściej wymieniają informacje między sobą niż z innymi działami. Jest prawdopodobne, że dział fakturowania będzie częściej wymieniał informacje z działem wysyłkowym. Niektóre ścieżki komunikacyjne nie będą jednak tak oczywiste. Na przykład dział inżynierski znacznie częściej będzie wymieniał informacje z działem marketingu niż produkcji, co na pierwszy rzut oka nie jest takie oczywiste.

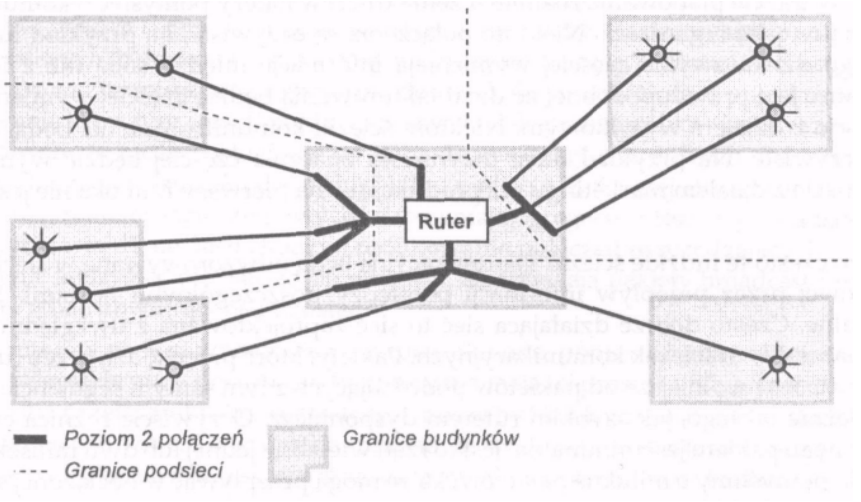
Bardzo często te ludzkie ścieżki komunikacyjne będą odwzorowywane w sieci komputerowej przez przepływ informacji pomiędzy poszczególnymi hostami. Jest to naturalne. Często dobrze działająca sieć to sieć zaprojektowana z uwzględnieniem tych naturalnych ścieżek komunikacyjnych. Pakiety, które przechodzą przez ruter, są zawsze trochę wolniejsze od pakietów podróżujących z tym samym segmencie LAN, niezależnie od tego, jak szybkim ruterem dysponujesz. Oczywiście różnica czasów dla jednego pakietu jest minimalna (jest to rząd wielkości jednej lub dwu milisekund), ale jeśli pomyślimy o milionie pakietów, które mogą przepływać w obciążonej sieci w stosunkowo krótkim czasie, to opóźnienia zaczynają być odczuwalne.

Przypomnij sobie, że wszystkie maszyny znajdujące się w jednej podsieci IP mogą się komunikować ze sobą bezpośrednio, bez pośrednictwa rutera. Ponieważ ruter dodaje do każdego obsługiwanego pakietu niezerowe opóźnienie, najszybsza z możliwych komunikacji ma miejsce wewnątrz tej samej podsieci. Wniosek wynikający z tego rozumowania wydaje się oczywisty:

> Jeśli tylko to możliwe, umieszczaj w tej samej podsieci maszyny, które się często ze sobą komunikują.

Niestety, ścieżki komunikacyjne nie są zawsze odzwierciedlone w fizycznej lokalizacji grup maszyn wymieniających informacje. Dwie grupy, które muszą się ze sobą komunikować (na przykład inżynierowie i technicy), mogą znajdować się w różnych budynkach na terenie firmy. I tu zaczyna mieć znaczenie topologia sieci. Jeśli wybrałeś dwuwarstwową topologię gwiazdy, to dosyć łatwo będziesz mógł zgrupować te dwa działy w jedną podsieć, łącząc w odpowiedni sposób promienie gwiazdy pierwszego poziomu i zapewniając połączenia pomiędzy grupami, jak pokazano na rysunku 3-1.

Jeśli gwiaździste połączenia tego pierwszego poziomu sieci mają odpowiednią przepustowość, to możliwe jest odizolowanie grup w budynku od pozostałych grup, przy jednoczesnym utworzeniu wspólnej podsieci dla tych grup oraz innych grup maszyn znajdujących się w budynku. Takie rozwiązanie może być konieczne, gdyż jedna z grup w budynku może wymieniać ważne dla firmy informacje, które należy zabezpieczyć lepiej niż pozostałe dane w sieci całej firmy. Takie wymagania powinny być rozważane w czasie planowania granic podsieci i lokalizacji ruterów.



Rysunek 3-1: Umieszczenie grup znajdujących się w różnych budynkach w jednej podsieci

Co jeszcze - oprócz ścieżek komunikacyjnych - należy rozważyć? Jeśli chcesz w swojej sieci rutować protokoły inne niż IP (omówione w dalszej części tego rozdziału), powinieneś rozważyć ich wpływ na sieć. Inne protokoły bardzo często pojawiają się w poszczególnych działach w ich sieci LAN; mogą powodować ograniczenia dotyczące tego, które z maszyn muszą pracować w tej samej podsieci, a także które z komputerów nie mogą być razem, ponieważ protokół nie zapewnia odpowiedniej separacji pomiędzy różnymi grupami.

Powinieneś również rozważyć wykorzystanie protokołów IP opierających się na pakietach broadcast, takich jak BOOTP lub DHCP. Pamiętaj, że ruter z definicji nie przesyła pakietów broadcast pomiędzy swoimi interfejsami. Jeśli zamierzasz umieścić klientów jednego z takich protokołów w segmencie, w którym nie ma serwera tego protokołu, musisz skonfigurować ruter tak, aby przesyłał pakiety protokołu do serwera. Konfiguracja taka jest łatwa; wymaga wpisania następujących poleceń:

```
interface Ethernet 2* ip address 17.16.1.1
 255.255.255.0 ip helper-address
 172.16.23.17
```

Polecenie helper-address powoduje przesyłanie wszystkich pakietów broadcast pochodzących z określonych protokołów i odebranych na tym interfejsie do hosta o podanym adresie. Przesyłanie to wykonywane jest pakietem typu *unicust,* tak więc żaden inny ruter znajdujący się na drodze tego pakietu nie musi brać udziału w obsłudze pakietów broadcast. Na różnych interfejsach można określić ten sam adres helper lub różne adresy.

*Informacje na temat konfiguracji typowych interfejsów w ruterach Cisco znajdują się w dodatku A.

Które protokoły będą więc przesyłane? Niektóre przesyłane są z definicji. Ponieważ te domyślnie przesyłane protokoły mogą ulec zmianie w przyszłych wersjach oprogramowania IOS, należy zawsze posługiwać się dokumentacją systemu rutera, z którego się korzysta. Aby móc kontrolować, który protokół będzie przesyłany, a który nie, należy dodać następujące linie konfiguracji:

```
\forward bootp and dhcp protocols* ip
forward-protocol udp bootp ! never foruard
the tftp protocol no ip forward-protocol
udp tftp
```

Polecenia te mają wpływ na wszystkie pakiety broadcast IP przesyłane przez ruter. Jeśli chcesz uchronić protokół przed przesyłaniem jego pakietów *przez* jeden z interfejsów rutera, konieczne będzie zdefiniowanie listy dostępu i przypisanie jej do tego interfejsu. Temat ten nie będzie tu opisywany, ponieważ każdy przypadek jest inny.

Podział na podsieci i wyznaczanie masek

Kiedy już masz ogólną koncepcję rozmieszczenia ruterów i wiesz, jak będą przebiegały granice podsieci, możesz rozpocząć przypisywanie każdemu z segmentów sieci numerów sieci lub podsieci. Najpierw musisz przewidzieć, ile maszyn wymagających numeru IP będzie się znajdować w każdej z podsieci. Nie zapomnij zostawić sobie pewnej rezerwy na adresowanie rozrastającej się grupy komputerów. Choć teoretycznie możliwe jest posiadanie podsieci dowolnej wielkości, to praktycznie medium sieci lub dostępne pasmo obniżają tę górną granicę do około 1000 hostów w podsieci. To niezbyt praktyczna liczba, jeśli nie masz do dyspozycji superszybkiego medium sieci lub nie tworzysz sieci dla maszyn, które rzadko używają sieci. Bardziej realną maksymalną liczbą komputerów w sieci wydaje się być liczba od 200 do 500 i to tylko pod warunkiem, że maszyny te nie za często korzystają z sieci i że masz do dyspozycji szybkie medium lub sieć pracuje w segmencie przełączanym lub składającym się z mikrosegmentów.

Skoro już wiesz, ile adresów będziesz obsługiwał w każdej podsieci, musisz podjąć ważną decyzję: czy należy używać jednakowych masek podsieci o stałej długości we wszystkich podsieciach, czy też stosować maski różnej długości w różnych segmentach?

* BOOTP i DHCP wykorzystują ten sam port UDP i zwykle są kompatybilne w górę (serwer DHCP może obsługiwać klientów zarówno DHCP, jak i BOOTP). Z tego powodu nie ma oddzielnych poleceń i p forward-protocol udp dhcp.

Maski o stałej długości a maski o zmiennej długości

Jeśli w każdej z Twoich sieci będzie tyle samo hostów, najprostszym rozwiązaniem jest zastosowanie maski o stałej długości, która pozwoli Ci na przydzielenie wystarczającej liczby adresów w każdym segmencie. Możesz się w tym celu posłużyć danymi z tabeli 3-1, umieszczonej w rozdziale 1. Taka sytuacja nie zdarza się jednak często...

Tabela 3-1. Liczba podsieci i hostów w różnych układach długości maski i bloków sieci

Liczba bitów	*Maska podsieci*	*Liczba podsieci 16 bitów*	*w bloku 20 bitów*	*podsieci 24 bity*	*Efektywna liczba hostów*
16	255.255.0.0	1	-	-	65534
17	255.255.128.0	-	-	-	32766
18	255.255.192.0	2	-	-	16382
19	255.255.224.0	6	-	-	8190
20	255.255.240.0	14	1	-	4094
21	255.255.248.0	30	-	-	2046
22	255.255.252.0	62	2	-	1022
23	255.255.254.0	126	6	-	510
24	255.255.255.0	254	14	1	254
25	255.255.255.128	510	30	-	126
26	255.255.255.192	1022	62	2	62
27	255.255.255.224	2046	126	6	30
28	255.255.255.240	4094	254	14	14
29	255.255.255.248	8190	510	30	6
30	255.255.255.252	16382	1022	62	2
31	255.255.255.254	32766	2046	126	-
32	255.255.255.255	65534	4094	254	-

Bardziej prawdopodobne jest, że będziesz potrzebował jednej lub dwóch bardzo dużych podsieci (a w każdej z nich może nawet około 400 maszyn), kilka podsieci średniej długości (około 50 maszyn w każdej) i kilka bardzo małych podsieci (mniej niż 10 maszyn w każdej), które będą obsługiwały grupy serwerów lub łącza sieci WAN. Jeśli wybierzesz jednakową maskę podsieci, na tyle dużą, aby objęła największą z wymienionych podsieci (co oznacza podsieć adresów dla 510 maszyn), większość pozostałych podsieci będzie się składała z niewykorzystanych adresów. A więc możesz zmarnować ponad połowę przestrzeni adresowej! W opisanym wyżej przypadku masz do wyboru dwa rozwiązania. Pierwsze z nich polega na zmianie aranżacji podsieci tak, aby w każdej z nich znalazło się mniej więcej tyle samo maszyn. Drugim rozwiązaniem jest użycie masek o zmiennej długości *(variable-length subnet masks - VLSM).*

Użycie masek o zmiennej długości *oznacza,* że każdy segment Twojej sieci będzie mógł mieć inną maskę podsieci. Dzięki temu możesz dobrać taką maskę, która pozwoli Ci na zaadresowanie wszystkich hostów w segmencie i zminimalizuje liczbę adresów zmarnowanych. Niełatwo jednak podjąć decyzję o użyciu masek o zmiennej długości. Jeśli zaczniesz wykorzystywać takie maski, to z pewnością będziesz miał problemy z zapamiętaniem długości maski w danej podsieci i konieczne będzie odwoływanie się do tablic pomocniczych. Ponieważ takie rozwiązanie jest stosunkowo nowe, mogą wystąpić problemy z adresowaniem niektórych urządzeń, co ograniczy stosowanie tego typu masek, na przykład do ruterów, które w pełni obsługują takie maski. Nie jest to prawdopodobnie poważne ograniczenie, ponieważ większość producentów ruterów zapewnia, że ich sprzęt obsługuje takie maski, ale może się okazać, że oprogramowanie IP pracujące na niektórych hostach w Twojej sieci nie obsługuje masek o zmiennej długości. Jeśli nawet, to nie wszystko jeszcze stracone. Możesz poradzić sobie z ograniczeniami hostów stosując proxy ARP, który będzie omawiany w dalszej części rozdziału. Być może będą one działały całkiem dobrze z domyślnym rutowaniem statycznym, zakładając oczywiście, że nie pracują na dwóch kartach sieciowych. Jeśli będziesz wykorzystywał maski o zmiennej długości, możesz być zmuszony wykorzystywać w sieci protokoły rutowania statycznego lub dynamicznego, które poprawnie obsługują maski o zmiennej długości, choć niektóre klasowe protokoły rutowania mogą również - choć w ograniczonym stopniu - obsługiwać maski o zmiennej długości, jeśli sieć została dobrze zaprojektowana. Temat ten zostanie dokładniej omówiony w dalszej części książki.

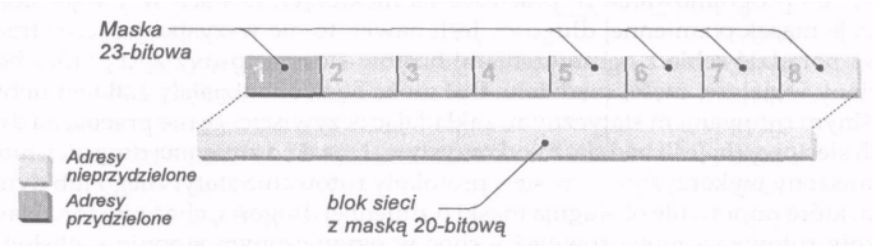
Maska o stałej długości ma tę zaletę, że nie jest skomplikowana. Łatwo zapamiętać, jaka maska jest użyta w każdej podsieci (ponieważ jest dokładnie taka sama we wszystkich innych podsieciach). Takie rozwiązanie jest również wygodniejsze dla administratora systemów, który konfiguruje hosty działające w różnych podsieciach. Główną wadą tego rozwiązania jest potencjalne marnowanie przestrzeni adresowej oraz mniejsza elastyczność sieci.

Wybór masek podsieci o zmiennej długości

Jeśli zdecydowałeś się wykorzystywać maski podsieci o zmiennej długości, to należy pamiętać o kilku szczegółach, które pomogą ograniczyć liczbę problemów z nimi związanych. Po pierwsze, należy używać jak najmniej różnych masek. Choć niewątpliwie zwiększy to liczbę marnowanych adresów, nie będzie to zbyt wielka strata, jeśli w jej wyniku konieczne będzie zapamiętanie tylko trzech lub czterech masek, zamiast dwunastu lub więcej. A przecież mówiliśmy o tym, że w każdej podsieci należy zostawić kilka adresów na przyszłość. Po drugie, nie należy przydzielać masek podsieci przypadkowo, gdyż trzeba będzie wtedy tworzyć specjalną tabelę, która pomoże w przyszłości wyszukiwać maski nadane wcześniej pewnym podsieciom. Jeśli nie będziesz ostrożny, możesz doprowadzić do pokrywania się sieci. Jeśli będziesz przydzielał maski w sposób uporządkowany, łatwiej będzie je zapamiętać albo przynajmniej zgadnąć, jaka maska mogła znajdować się w danej sieci.

Rozważmy 20-bitowy blok adresów jak `172.16.0.0/20`. Załóżmy, że potrzebujemy l podsieci dla około 400 maszyn, 10 podsieci dla około 100 maszyn w każdej, 12 podsieci dla około 45 maszyn w każdej i 6 podsieci dla 2 maszyn. Te najmniejsze podsieci posłużą do adresowania łączy WAN obsługujących połączenia z filiami firmy. Najpierw musimy zająć się podsiecią największą.* Zaczniemy od wyboru podsieci, która da nam przynajmniej 400 użytecznych adresów IP.

Z tabeli 3-1 wynika, że 23-bitowa maska daje nam 510 użytecznych adresów w podsieci. Użyjemy więc tej maski, aby podzielić naszą sieć na 8 podsieci o jednakowej wielkości i przypiszemy pierwszy blok adresów podsieci, w której jest 400 maszyn, jak pokazano na rysunku 3-2.

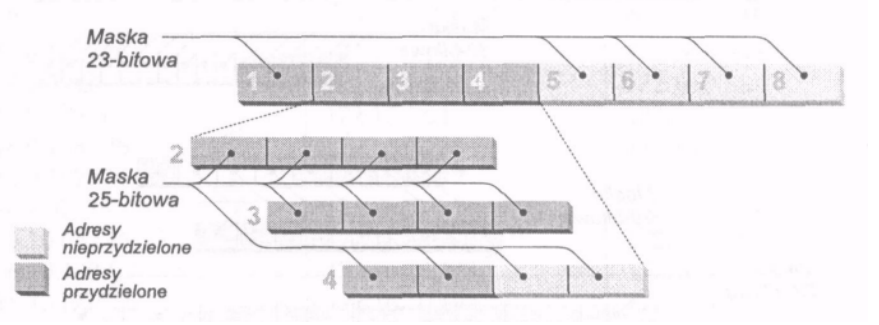


Rysunek 3-2: Przestrzeń adresową należy podzielić na bloki o wielkości wystarczającej dla adresowania największej podsieci

Jeśli używalibyśmy w naszej sieci masek o stałej długości, to sprawa byłaby rozwiązana. Okazałoby się również, że nie mamy wystarczającej liczby adresów, choć jeszcze nie zaczęliśmy ich przydzielać. Przecież z naszego opisu podziału sieci wynika, że potrzebujemy 29 podsieci, a przy masce podanej wyżej mamy tych podsieci tylko 8! Jest więc oczywiste, że musimy dzielić naszą przestrzeń adresową tak, aby móc obsłużyć wszystkie podsieci.

Kolejną czynnością jest przydzielenie adresów i masek podsieciom, w których pracuje po 100 maszyn. Popatrzmy do naszej tabeli, gdzie widzimy, że możemy użyć maski 25-bitowej, aby uzyskać 126 użytecznych adresów w każdej podsieci. Stosując taką maskę, zaczynamy dzielić niewykorzystane bloki adresów utworzone przez początkową maskę o długości 23 bitów. Wynika z tego, że uzyskaliśmy cztery podsieci o maskach 25-bitowych, wyodrębniając je z każdego z 23-bitowych bloków. Użyjemy więc trzech bloków 23-bitowych, co - przemnożone *przez* 4 - da nam ponad 10 podsieci (dokładnie 12); w każdej może pracować po około 100 hostów. Wyniki takiego podziału pokazane zostały na rysunku 3-3. Ponieważ potrzebowaliśmy 10 takich podsieci, to pozostały nam jeszcze dwa niewykorzystane 25-bitowe bloki. Te dwa bloki możemy pozostawić do zagospodarowania w przyszłości w celu utworzenia 25-bitowych podsieci lub podzielić je na jeszcze mniejsze części.

Inny sposób przydzielania podsieciom masek o zmiennej długości znajdziesz w RFC 1219.

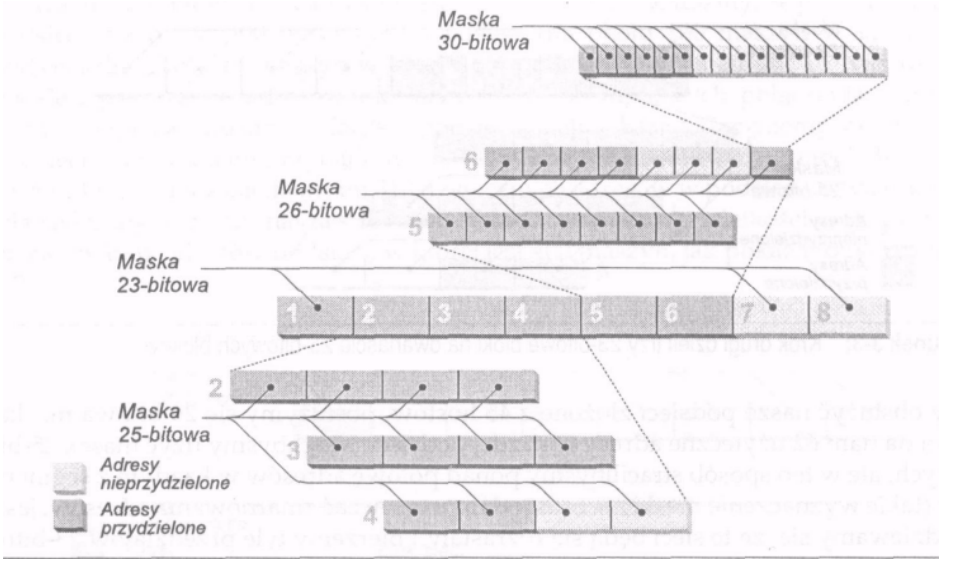


Rysunek 3-3: Krok drugi dzieli trzy 23-bitowe bloki na dwanaście 25-bitowych bloków

Aby obsłużyć nasze podsieci złożone z 45 hostów, posłużymy się 26-bitową maską, która da nam 62 użyteczne adresy w każdej podsieci. Moglibyśmy użyć masek 25-bitowych, ale w ten sposób stracilibyśmy ponad połowę adresów w każdym z segmentów (takie wyznaczenie maski nie musi od razu oznaczać zmarnowania adresów, jeśli spodziewamy się, że te sieci będą się rozrastały.) Bierzemy tyle przedziałów 23-bito-wych, ile potrzeba, aby uzyskać 12 podsieci. Ponieważ z każdego 23-bitowego bloku uzyskaliśmy 8 podsieci, a potrzeba nam 12, to konieczne jest dalsze podzielenie dwóch z tych bloków w celu uzyskania szesnastu 26-bitowych podsieci. Alternatywnym rozwiązaniem jest użycie jednego 23-bitowego bloku, który da nam 8 podsieci, i wykorzystanie dwóch nieużywanych 25-bitowych bloków w celu zaadresowania pozostałych czterech podsieci. Takie rozwiązanie da nam dokładnie 12 podsieci, ale nie zostawia żadnej przestrzeni na rozrastanie się sieci. Pozostawienie małej nieużywanej przestrzeni adresów nie nastręcza większych trudności.

Musimy jeszcze obsłużyć sześć łączy sieci WAN. Posługując się naszą tabelą, stwierdzamy, że aby uzyskać dwa użyteczne adresy w sieci, należy użyć maski o długości 30 bitów. Moglibyśmy podzielić kolejny duży blok z tych, które nam pozostały, ale to dałoby nam 128 podsieci z adresami dla dwóch hostów! Zamiast tego powinniśmy raczej rozważyć wykorzystanie jednego z mniejszych bloków, które pozostały po zdefiniowaniu innych masek. Jeśli wybierzemy jedną z czterech pozostałych 26-bitowych podsieci, możemy ją podzielić za pomocą 30-bitowej maski i uzyskać w ten sposób 16 podsieci (z dwoma adresami w każdej). Ostateczny wynik pokazano na rysunku 3-4.

Wykorzystywanie struktury podsieci pokazanych na rysunku 3-4 dla sieci `172.16.0.0/20` daje liczbę podsieci przedstawioną w tabeli 3-2.



Rysunek 3-4: Ostateczny przydział masek podsieci dla 20-bitowego bloku sieci

Gwiazdkami oznaczono podsieci, które nie zostały wykorzystane i mogą być w przyszłości podzielone, jeśli *zajdzie* taka potrzeba. Zwróć uwagę na fakt, że pierwszy i ostatni adres w każdej z podsieci nie może być użyty jako adres hostów. Pierwszy adres określa samą podsieć, a ostatni to adres rozgłoszeniowy tej podsieci.

Tabela 3-2. Powstałe w wyniku podziału numery podsieci i adresy

Podsieć	*Adres pierwszy*	*Adres ostatni*
172.16.0.0/23	172.16.0.0	172.16.1.255
172.16.2.0/25	172.16.2.0	172.16.2.127
172.16.2.128/25	172.16.2.128	172.16.2.255
172.16.3.0/25	172.16.3.0	172.16.3.127
172.1 6.3.128/25	172.1 6.3.128	172.1 6.3.255
172.16.4.0/25	172.16.4.0	172.16.4.127
172.16.4.128/25	172.16.4.128	172.16.4.255
172.16.5.0/25	172.16.5.0	172.16.5.127
172.16.5.128/25	172.16.5.128	172.16.5.255
172.16.6.0/25	172.16.6.0	172.16.6.127
172.16.6.128/25	172.16.6.128	172.16.6.255
'172.16.7.0/25	172.16.7.0	172.16.7.127
'172.16.7.128/25	172.16.7.128	172.16.7.255
172.16.8.0/26	172.16.8.0	172.16.8.63
172.16.8.64/26	172.16.8.64	172.16.8.127
172.16.8.128/26	172.16.8.128	172.16.8.191

Podział na podsieci i wyznaczanie masek

Podsieć	*Adres pierwszy*	*Adres ostatni*
172.16.8.192/26	172.16.8.192	172.16.8.255
172.16.9.0/26	172.16.9.0	172.16.9.63
172.16.9.64/26	172.16.9.64	172.16.9.127
172.16.9.128/26	172.16.9.128	172.16.9.191
172.16.9.192/26	172.16.9.192	172.16.9.255
172.16.10.0/26	172.16.10.0	172.16.10.63
172.16.10.64/26	172.16.10.64	172.16.10.127
172.16.10.128/26	172.16.10.128	172.16.10.191
172.16.10.192/26	172.16.10.192	172.16.10.255
*172. 16.11.0/26	172.16.11.0	172.16.11.63
'172.16.11.64/26	172.16.11.64	172.16.11.127
*172.16.11.128/26	172.16.11.128	172.16.11.191
172.16.11.192/30	172.16.11.192	172.16.11.195
172.16.11.196/30	172.16.11.196	172.16.11.199
172.16.11.200/30	172.16.11.200	172.16.11.203
172.16.11.204/30	172.16.11.204	172.16.11.207
172.16.11.208/30	172.16.11.208	172.16.11.211
172.16.11.212/30	172.16.11.212	172.16.11.215
*172.16.11.216/30	172.16.11.216	172.16.11.219
172.16.11.220/30	172.16.11.220	172.16.11.223
172.16.11.224/30	172.16.11.224	172.16.11.227
*172.16.11.228/30	172.16.11.228	172.16.11.231
*172.16.11.232/30	172.16.11.232	172.16.11.235
*172.16.11.236/30	172.16.11.236	172.16.11.239
*172.16.11.240/30	172.16.11.240	172.16.11.243
*172.16.11.244/30	172.16.11.244	172.16.11.247
*172.16.11.248/30	172.16.11.248	172.16.11.251
*172.16.11.252/30	172.16.11.252	172.16.11.255
*172.16.12.0/23	172.16.12.0	172.16.13.255
*172.16.14.0/23	172.16.14.0	172.16.15.255

Jedyny problem, jaki może wystąpić w związku z tak przydzielonymi numerami podsieci, jest związany z tym, że użyliśmy *podsieci O* w największym przydzielonym bloku adresów. Początkowo nie można jej było stosować, ponieważ łatwo ją było pomylić z numerem sieci. Na podobnej zasadzie niedozwolone było również używanie ostatniego numeru sieci, ponieważ można go było pomylić z adresem rozgłoszeniowym wszystkich podsieci. Zgodnie z najnowszymi standardami, takie problemy już nie występują, dlatego możliwe jest wykorzystywanie obu wymienionych podsieci. Należy jednak pamiętać, że oprogramowanie pracujące na wielu hostach może nie potrafić obsługiwać zabronionych wcześniej adresów. Jeśli zetkniesz się z tym problemem, możesz go rozwiązać na jeden z trzech sposobów. Pierwszym jest pominięcie pierwszego i ostatniego numeru podsieci podczas przydzielania adresów. Niestety, rozwiązanie takie powoduje marnowanie przestrzeni adresowej, niezależnie od tego, ilu podsieci używasz i jak duże one są. Lepszym wyjściem jest przydzielenie mniejszych podsieci na początku *i* na końcu przestrzeni adresowej. Jedyną wadą takiego rozwiązania jest to, że Twoja przestrzeń adresowa będzie się składała z kilku mniejszych podsieci, rozdzielonych większymi.

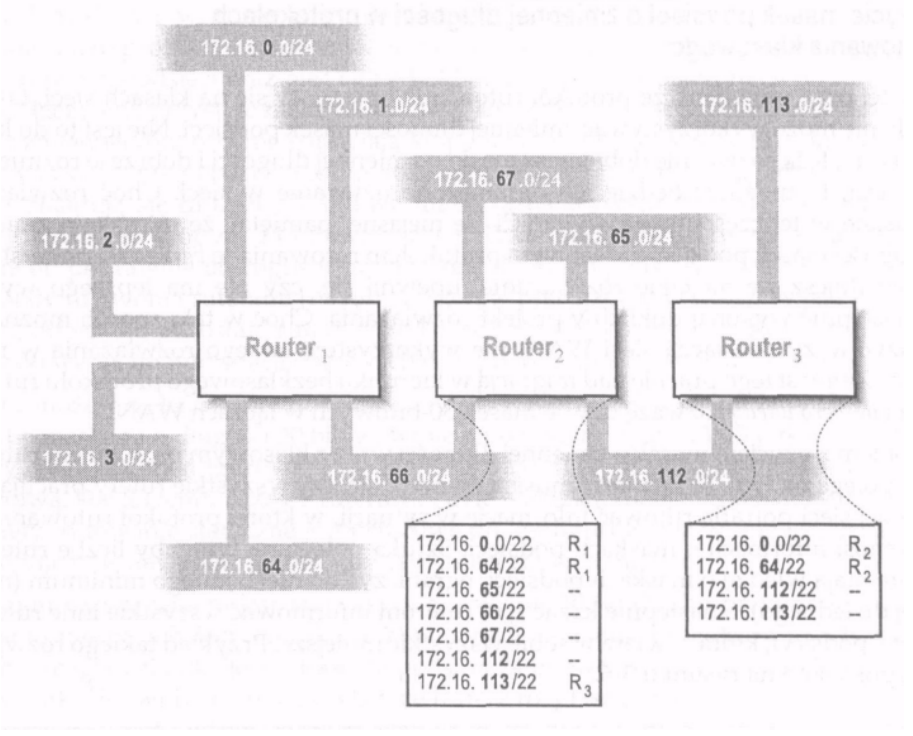
Ostatnim rozwiązaniem jest użycie proxy ARP w podsieciach z hostami, które nie potrafią pracować z nowymi standardem adresowania.

Przydzielanie numerów podsieci tak, by możliwe było ich agregowanie

Kiedy określasz zmienne maski podsieci lub przypisujesz numery podsieci do segmentów wykorzystując maskę o stałej długości, powinieneś starać się grupować numery podsieci uwzględniając topologię sieci, co pozwoli na ich agregowanie. Inny mi słowy, trzymaj adresy 172.16.14.0/24 i 172.16.15.0/24 obok siebie, dzięki czemu inne rutery będą musiały przechowywać tylko jedną trasę do tych podsieci opisaną jako 172.16.14.0/23. Zmniejszy to rozmiary tablic rutowania. Każda siei wymaga oddzielnego zapisu w tablicy rutowania każdego z ruterów. Wewnątrz jednej organizacji każda podsieć również wymaga oddzielnego zapisu w tablicy Umożliwiając zbieranie numerów podsieci w większe grupy możesz zmniejszyć rozmiary tablic rutowania w niektórych ruterach pracujących w Twojej sieci. Choć może nie jest to ważne w sieciach składających się z kilku podsieci, może to w znacznym stopniu wpływać na pracę dużych sieci podzielonych na wiele podsieci.

Przykład działania agregacji pokazano na rysunku 3-5. W przedstawionej sieci Ruter1 musi wiedzieć dokładnie, jakie są numery podsieci dołączonych do niego. Nie mus on jednak informować Rutera2 o każdej podsieci. Zamiast tego może wysłać dc Rutera2 informacje o jednej zagregowanej trasie, obejmującej cztery podsieci (podsieć od 172.16.0.0/24 do 172 .16 . 3.0/24 są opisane adresem 172.16.0.0/22), a piąta podsieć -172.16.66.0/24- opisana będzie oddzielną trasą. Ruter2 może przesłać do Rutera3 jeszcze mniej szczegółów, ponieważ może dokonać agregacji zarówno trą: do podsieci obsługiwanych przez Ruter1, jak i swoich dwóch podsieci (172 .16 . 0 .0/22 oraz 172 .16 .64. 0/22). Zatem mimo że sieć składa się z 10 segmentów, Ruter3 będzie miał tylko cztery zapisy w swojej tablicy rutowania.

Niestety, przydzielanie masek podsieci z uwzględnieniem wydajności adresów ora: przydzielanie tych masek z uwzględnieniem topologii sieci czasem trudno pogodzić Kiedy konflikt jest niewielki (dotyczy dwóch podsieci, które nie zostały zaadresowane zgodnie z topologią), można go po prostu zignorować. Jedna lub dwie (a nawę tuzin) podsieci, które nie mogą być agregowane, nie spowodują zatrzymania prac) Twojej sieci. Osiągnięcie 100 procent agregacji w jakiejkolwiek rzeczywistej sieci jest prawie niemożliwe. Musisz również wiedzieć, że w miarę rozrastania się sieci konieczne będzie dokonywanie w niej zmian, które będą powodowały powstawanie kolejnych wyjątków.



Rysunek 3-5: Agregowanie informacji o nitowaniu

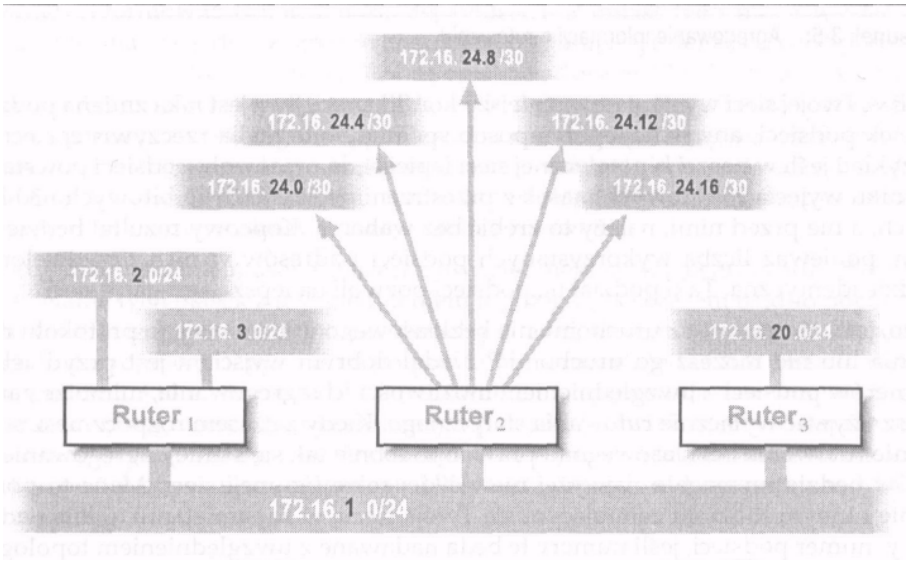
Jeśli w Twojej sieci wystąpi poważniejszy konflikt, możliwa jest taka zmiana podziału masek podsieci, aby w najlepszy sposób spełniały one realia rzeczywistej sieci. Na przykład jeśli w naszej hipotetycznej sieci lepiej będą pracowały podsieci powstałe w wyniku wyjęcia 25-bitowych masek z przestrzeni po maskach 26-bitowych i 30-bito-wych, a nie przed nimi, należy to zrobić bez wahania. Końcowy rezultat będzie taki sam, ponieważ liczba wykorzystanych podsieci i adresów w nich przydzielonych będzie identyczna. Taki podział na podsieci pozwoli na lepszą agregację sieci.

A co, jeśli nie planujesz uruchomienia bezklasowego dynamicznego protokołu rutowania lub nie możesz go uruchomić? Nadal dobrym wyjściem jest przydzielanie numerów podsieci z uwzględnieniem możliwości ich agregowania, mimo że zamierzasz używać wyłącznie rutowania statycznego. Kiedy z czasem rozpoczniesz stosowanie rutowania bezklasowego (a prawdopodobnie tak się stanie), agregowanie adresów będzie wymagało najwyżej niewielkiej rekonfiguracji sieci. Może to pomóc Tobie i innym ludziom zajmującym się Twoją siecią w zapamiętaniu, gdzie nadano dany numer podsieci, jeśli numery te będą nadawane z uwzględnieniem topologii.

Użycie masek podsieci o zmiennej długości w protokołach rutowania klasowego

Do tej pory mówiłem, że protokół rutowania opierający się na klasach sieci, taki ja RIP, nie może wykorzystywać zmiennej długości masek podsieci. Nie jest to do końca prawda. Jeśli rozważnie dobierzesz maski o zmiennej długości i dobrze je rozmieścić w sieci, to możliwe będzie ich ograniczone używanie w sieci. Choć rozwiązani opisane w tej części mogą wydać Ci się niejasne, pamiętaj, że mieszanie zmienni długości masek podsieci z klasowym protokołem rutowania to *bardzo zły* pomysł. Jeśli zdecydujesz się na takie rozwiązanie, upewnij się, czy nie ma lepszego wyjścia następnie wykonaj dokładny projekt rozwiązania. Choć w taki sposób można ot służyć wszystkie łącza sieci WAN, nie wykorzystuję takiego rozwiązania w mojej sieci. Zamiast tego pracuję nad migracją w kierunku bezklasowego protokołu nitowe nią i *dopiero wtedy* rozważę użycie masek 30-bitowych w łączach WAN.

Problem z użyciem masek o zmiennej długości wraz z klasowym protokołem rutowania polega na tym, że najpierw musisz upewnić się, czy wszystkie rutery pracujące \ Twojej sieci potrafią rutować informację w sytuacji, w której protokół rutowania ni przenosi informacji o maskach podsieci. Sztuka polega na tym, aby liczbę ruterów które mają wiedzę o maskach podsieci, ograniczyć do niezbędnego minimum (najlepiej do jednego), a następnie kazać tym ruterom informować wszystkie inne rutery dużej podsieci, która zawiera w sobie wszystkie mniejsze. Przykład takiego rozwiążą nią pokazano na rysunku 3-6.



Rysunek 3-6: Maski zmiennej długości użyte w sieci z klasowym protokołem rutowania

ProxyARP jako alternatywa dla podsieci

W przykładzie tym widzimy trzy rutery obsługujące część sieci klasy B przy użyciu dynamicznego protokołu rutowania. Sieć ta wykorzystuje 24-bitowe maski dla działających w niej podsieci oraz pięć łączy WAN punkt-punkt dołączonych do Rutera2. Te pięć łączy wykorzystuje maskę 30-bitową, aby zaoszczędzić przestrzeń adresową. Maski zmiennej długości nie sprawiają kłopotu ruterowi oznaczonemu jako Ruter2, ponieważ są do niego bezpośrednio dołączone. Ruter ten wie, że na łączach punkt-punkt znajdują się dłuższe, 30-bitowe maski, a na wszystkich innych kierunkach należy stosować krótszą, 24-bitową maskę. Takie zachowanie rutera sprawia, że będzie on poprawnie obsługiwał przyłączone do niego podsieci. Ale co się dzieje z pozostałymi dwoma ruterami (i z resztą ruterów pracujących w sieci)? W jaki sposób Ruter2 informuje pozostałe rutery o podsieciach, które obsługuje, bez konieczności przekazywania im informacji o maskach starego formatu? Są dwie możliwości.

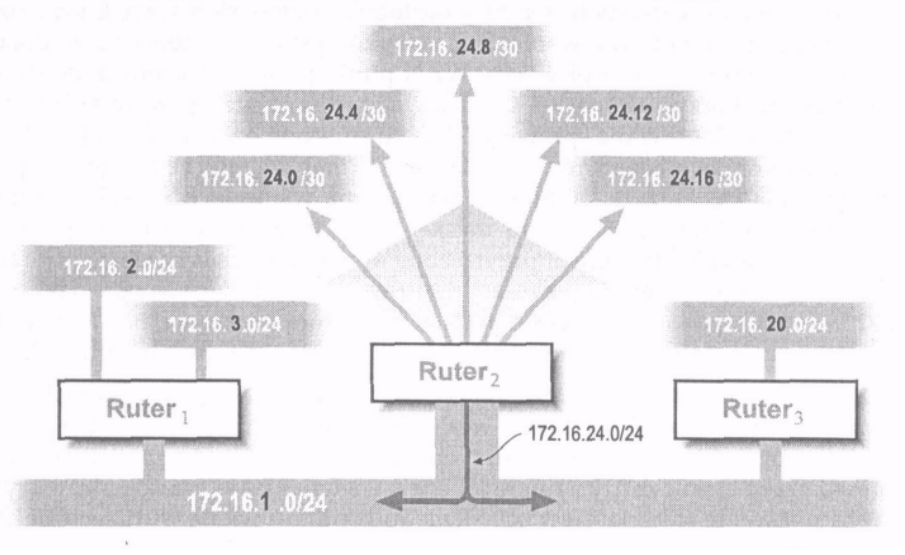
Ruter2 może przekazać innym ruterom w sieci informację o pięciu łączach punkt-punkt z maskami o długości 30 bitów, wcale im o tym *nie mówiąc.* Wszystkie pozostałe rutery mogą być skonfigurowane ze statyczną trasą dla tych łączy, zawierającą maskę 30-bitową. Dzięki temu każdy z ruterów będzie wiedział, jakiej maski należy używać. Niestety, nitowanie statyczne jest uciążliwe do konfigurowania w dużych sieciach i powoduje powstawanie błędów, gdy część sieci zmienia miejsce.

Lepszym rozwiązaniem jest takie skonfigurowanie Rutera2, aby przypominał on o istnieniu pięciu podsieci o maskach 30-bitowych i - zamiast rozgłaszania ich wszystkich - rozgłaszał tylko jedną trasę do podsieci 24-bitowej, która je wszystkie zawiera. Na rysunku 3-7 widzimy na przykład, że Ruter2 rozgłasza podsieć `172.16.24.0/24`, która zawiera pięć podsieci wykorzystanych do obsługi łączy (a także inne, które nie są wykorzystywane przez ten ruter). Ponieważ wszystkie 30-bitowe podsieci są dostępne z Rutera2, takie okłamywanie innych ruterów sprawia, że działają one poprawnie, choć nie są informowane o maskach zmiennej długości. Przykład opisano w rozdziale 6, zatytułowanym „Konfiguracja protokołu rutowania".

Dopóki te dziwne podsieci zawierają się w jednej podsieci pełno wymiarowej i są dołączone do jednego rutera, ten rodzaj ograniczonej obsługi masek zmiennej długości można zastosować wraz z klasowym protokołem dynamicznego rutowania. Znacznie łatwiej jest jednak obsługiwać maski o zmiennej długości przy użyciu bezklasowego protokołu rutowania; używaj go, kiedy tylko to możliwe. Protokół bezklasowy pozwala na obsługę masek podsieci o różnych rozmiarach. Nie musimy martwić się przy tym, w jaki sposób wiedza o nich dotrze do najmniejszych części sieci.

Proxy ARP jako alternatywa dla podsieci

Kiedy host przygotowuje się do wysłania datagramu IP, najpierw określa, czy adres przeznaczenia znajduje się w tym samym segmencie sieci, czy też w innym. Jeśli adres odbiorcy należy do innego segmentu, host wysyła datagram IP na adres rutera. Jeśli host wysyłający datagram oraz adres przeznaczenia znajdują się w tym samym segmencie sieci, to pakiet przesyłany jest bezpośrednio do odbiorcy.



Rysunek 3-7: Rozgłaszanie jednej pełnej podsieci zamiast kilku mniejszych podsieci

Warstwa łącza danych nie wie jednak nic o adresach IP. Każda maszyna ma zwykle niepowtarzalny adres sprzętowy, który nie ma nic wspólnego z adresem IP. Adresy sprzętowe przydzielane są maszynom (lub kartom interfejsów) przez producentów, bez względu na to, gdzie ta maszyna będzie używana. Adresy IP z kolei przydzielane są przez lokalnego administratora i mają strukturę, która jest kontrolowana lokalnie i zawiera wiele informacji o tym, gdzie dokładnie urządzenie się znajduje. Kiedy host IP chce wysłać datagram do lokalnego segmentu sieci, musi jakoś odwzorować adres IP przeznaczenia na odpowiedni adres sprzętowy.

Są trzy podstawowe metody odwzorowania adresów IP na adresy sprzętowe. Pierwszą z nich jest tablica lookup. Każda maszyna przechowuje skończoną listę odwzorowań adresów IP na adresy sprzętowe dla każdej z maszyn w lokalnym segmencie sieci. Choć wydaje się to bardzo proste, utrzymywanie tablicy powoduje powstawanie błędów, a uaktualnianie tablic hostów w całej sieci po zmianie jednego adresu staje się koszmarem, kiedy maszyn w sieci jest więcej niż tuzin.

Drugą metodą jest algorytmiczne mapowanie pomiędzy adresami IP i adresami sprzętowymi. Jednym z przykładów może być warstwa łącza danych pracująca z 8-bitowymi adresami sprzętowymi. W takim przypadku host może mapować adresy IP na adresy sprzętowe używając mniej znaczącego oktetu adresu IP jako adresu sprzętowego. Taki algorytm działa nieźle pod warunkiem, że administrator ma możliwość ustawiania adresu sprzętowego i że takie proste odwzorowanie w ogóle istnieje.

Trzecią metodą, najczęściej wybieraną w przypadku zestawu protokołów IP, jest użycie sieciowej bazy danych, którą host pyta o adres sprzętowy odpowiadający jakiemuś adresowi IP. Ta baza danych może być umieszczona na pojedynczym serwerze lub dystrybuowana pomiędzy hostami, które są wtedy odpowiedzialne za udzielanie odpowiedzi dotyczących ich adresów.

ARP - Address Resolution Protocol

W najczęściej używanych mediach sieci LAN standardową metodą odwzorowywania *adresów jest Address Resolution Protocol (ARP).* Używając tego protokołu wysyłający pakiet host wysyła najpierw komunikat za pomocą sprzętowej usługi broadcast (o ile to możliwe), prosząc maszynę o danym numerze IP, by odpowiedziała przez odesłanie swego adresu sprzętowego. Kiedy wskazana maszyna odpowie, maszyna nadająca wysyła kolejne datagramy IP, wykorzystując przekazany adres sprzętowy odbiorcy. Ponieważ jest bardzo prawdopodobne, że w najbliższej przyszłości zostaną przesłane kolejne datagramy, nadawca zachowuje w pamięci używane odwzorowanie, by móc go użyć w przyszłości.

Zwykle każda maszyna odpowiada na zapytania dotyczące jej własnego adresu IP. Nie ma jednak ograniczeń w protokole, które nie pozwalałyby, aby dana maszyna odpowiadała przez przekazanie odwzorowania adresów IP, do których trasa prowadzi przez ruter. W takim przypadku ruter odpowiada na pytanie przesyłając swój własny adres. Maszyna wysyłająca pytanie akceptuje ten adres jako obowiązujące mapowanie, a kolejne datagramy adresowane na to IP wysyła na adres sprzętowy interfejsu rutera. Działanie takie znane jest jako *proxy ARP* lub *ARP hack.*

Proxy ARP wymyślono jako sposób na złagodzenie przejścia do konfiguracji sieci wykorzystujących podsieci IP. Wiele maszyn pracuje z oprogramowaniem, które nie rozumie masek podsieci. Maszyny te wierzą, że wszystkie hosty w sieci klasowej będą dostępne bezpośrednio przez warstwę łącza danych, a ARP użyją w stosunku do maszyn pracujących w innych podsieciach. Zapewniając obsługę proxy ARP ruter IP sprawia, że maszyny te funkcjonują w podsieci IP, bez konieczności uaktualniania ich oprogramowania do nowszej wersji. Maszyny, które nie potrafią pracować w podsieciach IP, są obecnie rzadkością. Wielu ludzi wierzy jednak, że proxy ARP jest użyteczne jako alternatywa do konfigurowania poprawnych masek podsieci (a czasem nawet rutowania) na hostach pracujących w sieci. Często nie rozumieją oni wad, jakie niesie ze sobą nieostrożne stosowanie proxy ARP, aż jest za późno i trzeba rekonfigurować całą sieć.

Problemy związane z proxy ARP

Włączanie wszędzie usługi proxy ARP ma pewne zalety dla zapracowanego administratora sieci. Nie musi on już wtedy informować administratorów sieci LAN oraz użytkowników, jakie są ich maski podsieci, ani wyjaśniać, co to jest maska podsieci. Hosty pracujące w końcowych sieciach mogą nawet nie wiedzieć nic o rutowaniu IP i wszystko otrzymywać od ARP, nawet adres IP odległych miejsc. W takim przypadku to rutery wykonują całą pracę.

Jednym z problemów, jaki powstaje przy wykorzystywaniu ARP, jest to, *że* obciążenie ruterów, które i bez tego protokołu jest duże, wyraźnie wzrasta.

Poprawnie skonfigurowany host IP, który komunikuje się z czterema maszynami znajdującymi się w innym segmencie sieci, wie, że wszystkie datagramy wchodzące w skład tych sesji muszą być wysyłane do rutera IP. Kiedy pierwszy pakiet jest gotowy do wysłania, host, posługując się ARP, uzyskuje adres sprzętowy rutera i zapamiętuje go w pamięci podręcznej ARP, by móc go użyć ponownie. Kolejne trzy sesje będą nitowane przez ten sam ruter, ale host ma już informację o adresie sprzętowym rutera, więc nie musi wysyłać kolejnego pytania. Natomiast maszyna posługująca się proxy ARF musi wysłać zapytanie ARP o adres sprzętowy każdej z maszyn, z którą się komunikuje. W naszym przypadku działanie to zwiększa liczbę ramek ARP aż czterokrotnie Jeśli pomnoży się to przez wszystkie maszyny dołączone do wszystkich interfejsów ruterów, dodatkowe obciążenie ruterów może być znaczne. Ponieważ zapytania ARP wysyłane są jako broadcast, kierowany do wszystkich maszyn w lokalnym segmencie, każda maszyna pracująca w tym segmencie musi przerwać normalną pracę : sprawdzić nadchodzące pytanie ARP, upewniając się, czy nie dotyczy ono jej adresu IP. Tak więc stosowanie proxy ARP zwiększa nie tylko obciążenie ruterów, ale także innych hostów w sieci.

Kolejną wadą rozpowszechniania proxy ARP jest fakt, że usługa ta powoduje powstawanie błędów w konfiguracji sieci. Pracuję obecnie z zestawem maszyn w lokalne sieci kampusowej, które mają zapisaną trasę domyślną wskazującą na adres IP, który nie został nikomu przydzielony, ale będzie wykorzystany jako adres rutera w kolejne podsieci. Ruter działający w lokalnej podsieci został skonfigurowany do obsług proxy ARP wiele lat temu i do dziś nie sprawdzono, czy usługa ta jest jeszcze potrzebna. Źle skonfigurowane maszyny działające w tej sieci szczęśliwie poprawnie wysyłały pakiety. Jeśli jednak taka konfiguracja pozostałaby nadal nie wykryta, te jakakolwiek zmiana w sieci mogłaby spowodować, że maszyny te przestałyby się komunikować z kimkolwiek. Koszmarem dla każdego administratora jest sytuacja, w której po dokonaniu jakiejś zmiany w jednym miejscu sieci nagle ni stąd, ni zowąd przestaje coś działać w innym miejscu.

Na nieszczęście niektórzy producenci ruterów domyślnie włączają proxy ARP m wszystkich interfejsach. Sądzą, że proxy ARP pomaga w traktowaniu sieci IP jako sieci typu plug-and-play, zwłaszcza w przypadku małych miejsc, gdzie administratorzy nie mają dużego doświadczenia w konfigurowaniu sieci. Choć w niektórych przypadkach tak się rzeczywiście dzieje, nadal obstaję przy swoim zdaniu, że proxy ARP robi więcej złego niż dobrego. Na szczęście łatwo w większości dostępnych obecnie ruterów wyłączyć obsługę proxy ARP. Przedstawione poniżej kody pokazuj; część konfiguracji pary interfejsów Ethernet w ruterze Cisco. Pierwszy z nich m; włączoną obsługę ARP (domyślna konfiguracja), w drugim obsługa ta jest wyłączona ponieważ nie jest potrzebna.

```
! proxy ARP enabled explicitly (His on by default)
interface Ethernet 0/0
  ip address 172.16.1.1 255.255.255.0
  ip proxy-arp
! prozy ARP disabled on this interface
interface Ethernet 0/1
    ip address 172.16.2.1 255.255.255.0
    no ip proxy-arp
```

Kiedy niezbędne jest użycie proxy ARP?

Mimo wad proxy ARP, konieczne jest zastosowanie go, gdy pojawi się problem komunikacji w sieci. *Zdarza* się, że w Twojej sieci będą pracowały hosty, które nie potrafią obsługiwać podsieci IP. Jeśli nie możesz usunąć takich komputerów z sieci, to nie ma innego wyjścia, jak zastosować obsługę proxy ARP w segmencie lub segmentach, gdzie są one dołączone. Innym, dość częstym, przypadkiem, jest sytuacja, kiedy masz w sieci host, który nie może poprawnie komunikować się z hostami pracującymi w podsieci O i podsieci I (same bity 1). (Pamiętaj, że te dwie podsieci są formalnie zarezerwowane.) Kiedy natrafisz na taki host, możesz nie mieć innego wyjścia, jak tylko okłamać go, że jego maska podsieci jest maską dopuszczalnej podsieci, przez co będzie myślał, że adresy, z którymi się komunikuje, nie pochodzą z podsieci zerowej lub jedynkowej. Oczywiście konieczne będzie również uruchomienie proxy ARP na ruterze obsługującym ten segment.

Pamiętaj, że musisz uważnie kontrolować wykorzystanie proxy ARP i nie należy posługiwać się nim w całej sieci. Postaraj się trzymać maszyny, które naprawdę wymagają tej usługi, w jak najmniejszej liczbie segmentów. Możliwe, że uda się je wszystkie zebrać w jednym segmencie, dzięki czemu proxy ARP można będzie uruchomić tylko na jednym interfejsie rutera.

Redundancja i odporność na uszkodzenia

W tym miejscu kończysz projektowanie swojej sieci. Pozostało jednak jeszcze jedno zadanie, które należy wykonać, aby spełniała ona swoje zadanie. Chodzi o funkcję redundancji.

Redundancja we wszystkich swych formach jest doskonałym sposobem na zwiększenie niezawodności i dostępności Twojej sieci. Poprawnie zaprojektowane i redundantne komponenty mogą sprawić, że zamiast uszkodzenia sieci nastąpi tylko lekkie zaburzenie jej pracy, niezauważalne dla użytkowników. Redundancja jednak znacznie podnosi koszt całej sieci. Gdy w sieci nie ma redundancji, nie poniesiesz żadnych dodatkowych kosztów. W pełni redundantna sieć co najmniej podwaja koszty. Najlepiej znaleźć rozwiązanie leżące gdzieś pośrodku.

Gdzie potrzebuję redundancji?

Tylko Ty możesz zdecydować, które punkty sieci powinny być redundantne. Kilka porad może Ci jednak pomóc w określeniu tego, co jest dobre dla Twojej sieci.

Po pierwsze, przyjrzyj się swojemu projektowi sieci i spróbuj zastanowić się, jakie uszkodzenia mogą w niej wystąpić. Zacznij od spraw ogólnych, takich jak uszkodzenie rutera czy przerwanie kabli. Twoim zadaniem nie jest zidentyfikowanie najmniej prawdopodobnych scenariuszy (to zadanie niemożliwe do wykonania), ale racz wskazanie ogólnych rodzajów uszkodzeń.

Nie zapomnij dołączyć do powstałej w te sposób listy także „uszkodzeń planowanych". Dzięki funkcjom redundancji części Twojej sieci będzie mogła funkcjonować, gdy będziesz w niej dokonywał zmian, które wymagają wyłączenia niektórych *urządzeń* lub odłączenia kabli. Na przykład redundantny pierścień wykorzystywany w technologii FDDI pozwala na przerwanie pierścienia i dodanie nowego urządzenia bez przerywania pracy sieci. Zapomina się czasem o tego rodzaju *planowanych* przerwach w pracy sieci.

Kiedy identyfikujesz potencjalne miejsca uszkodzeń, wszystko uważnie przeanalizuj Jednym z często pomijanych powodów uszkodzeń jest działanie personelu. Na prz[1] kład kiedy służby porządkowe sprzątają budynek, mogą uszkodzić zasilanie, który odetnie dopływ energii do części urządzeń aktywnych sieci. Jeśli tego typu uszkodzi nią *zdarzają* się często, to na pewno o nich nie zapomnisz. Jeśli jednak podłóg woskowana była ostatni raz rok temu, możliwe, że nie będziesz o tym pamiętał.

Kiedy zidentyfikujesz ogólne grupy uszkodzeń, powinieneś spróbować oszacować prawdopodobieństwo ich wystąpienia i ewentualny wpływ na Twoją sieć i prac organizacji. Jest to często najtrudniejsza część zadania. Większość z nas ma różne poglądy na temat faktycznego prawdopodobieństwa wystąpienia określonej awarii: jej wpływu na pracę całej firmy. Zwykle nie doceniamy niebezpieczeństwa i przecinamy możliwe skutki awarii. Ważne jest, aby nasze przewidywania były jak najbardziej poprawne.

Kolejnym krokiem powinno być ułożenie listy uszkodzeń w kolejności od najbardziej prawdopodobnych i szkodliwych do najmniej prawdopodobnych i szkodliwych Lista ta będzie na pewno bardzo subiektywna, ale nie przejmuj się tym zbytni Twoim zadaniem jest określenie miejsc, w których Twoje starania i inwestycje zwrot się w najwyższym stopniu. Nie przygotowujesz przecież formalnej analizy niezawodności systemu.

Jak powinienem zareagować na możliwość wystąpienia uszkodzenia?

Mając w ręku tę uporządkowaną listę należy się zastanowić, jak postępować z każdym możliwym uszkodzeniem. Zacznij od tych najpoważniejszych i najbardziej prawdopodobnych i opracuj sposób zapobiegania im. Pamiętaj, aby nie przesadzać zastosowanymi rozwiązaniami. Na przykład jednym z najczęstszych uszkodzeń się jest zanik napięcia zasilania. Oczywistym rozwiązaniem jest dołączenie maksymalnej możliwej liczby urządzeń pracujących w sieci do bezprzerwowego zasilania. A pomyśl chwilę i zastanów się, czy w momencie zaniku napięcia każdy pracujący sieci host będzie pracował? Być może tym, czego potrzebujesz, jest bezprzerwowe zasilanie głównych ruterów i koncentratorów, a pozostałe urządzenia w sieci f prostu mogą zniknąć na czas braku zasilania.

Powinieneś być również realistą przy określaniu rozwiązań poprawiających redundancję. Jeśli wydasz odpowiednią ilość pieniędzy, będziesz mógł zabezpieczyć się przed wpływem niektórych uszkodzeń. Powinieneś się jednak zastanowić, czy rzeczywiście warto wydawać więcej pieniędzy i dodatkowo chronić sieć przed uszkodzeniami, które być może nigdy nie wystąpią?

Na przykład szansa, że uszkodzeniu ulegnie ruter, jest raczej mała. Niemniej takie uszkodzenie będzie miało zasadniczy wpływ na pracę całej sieci. Dlatego pierwszą decyzją powinna być budowa w pełni redundantnej instalacji ruterów. Niestety, rutery nie są urządzeniami tanimi i możesz wydać bardzo dużo pieniędzy na ochronę przed uszkodzeniami, które prawie nigdy nie wystąpią (w związku z czym straty mogą być niewielkie). Rozsądniejszym podejściem będzie zakupienie jednego pełnego zestawu części zamiennych, które można będzie wykorzystać do wymiany jednego z ruterów w sieci lub elementu tego rutera. Oczywiście może to spowodować niewielką przerwę w pracy, konieczną na zlokalizowanie uszkodzenia i wymianę elementu uszkodzonego rutera.

A co z łączami redundantnymi?

Jednym z rodzajów uszkodzeń, jakim prawie na pewno przyjdzie Ci się zająć, jest uszkodzenie kabli. Ktoś robiąc wykop może natrafić na pęk kabli, który przez nieuwagę przerwie. Możliwe, że ekipa remontowa pracująca w jakimś budynku objętym Twoją siecią przetnie kabel miedziany. Nieuważny pracownik może zerwać kabel i uszkodzić gniazdo naścienne, zaczepiając o nie nogą. Wszystkie te uszkodzenia mogą wpływać na pracę sieci i oczywistym zabezpieczeniem jest stosowanie łączy redundantnych. Zastosowanie ich może wynikać również z konieczności zabezpieczenia się przed uszkodzeniem rutera lub zanikiem napięcia w sieci pracującej w oddalonym budynku.

Zanim jednak zaczniesz planować zapasowe łącza i dorysujesz je na swoim projekcie sieci, zastanów się, jakie będą skutki zastosowania tych dodatkowych łączy. W wielu przypadkach dodanie łącza redundantnego może mieć skutek odwrotny do zamierzonego. Każde nowe łącze stanowi nowy element sieci, który może ulec uszkodzeniu i wpływać na pracę pozostałych elementów sieci, zwłaszcza w przypadku skomplikowanej architektury, jaką jest sieć z rutowaniem IP. Jeśli na przykład pomiędzy dwoma ruterami masz redundantne połączenie, musisz uruchomić dynamiczny protokół rutowania, bo w przeciwnym wypadku Twoje rutery nie będą w stanie wykryć uszkodzenia łącza i wykorzystać łącza zapasowego. Protokoły rutowania mogą być bardzo skomplikowane. Jeśli łącze ulegnie uszkodzeniu, to wykrycie awarii i przejście na nowy układ tras pomiędzy urządzeniami zajmie ruterom trochę czasu. Czas ten określany jest jako *czas zbieżności.* Zostanie on dokładniej opisany w rozdziale 5, zatytułowanym „Wybór protokołu rutowania". W niektórych przypadkach czas zbieżności może wynieść nawet kilka minut. Kiedy uszkodzone łącze zostanie naprawione i zacznie znowu pracować, rutery muszą to wykryć i ponownie przeliczyć optymalne trasy połączeń obsługiwane przez sieć.

Co się będzie działo, kiedy łącze ulega uszkodzeniu w wyniku przeciążenia? Kiedy rutery wykryją to uszkodzenie, rozpoczną rutowanie tego ruchu z pominięciem uszkodzonego łącza. Powoduje to zmniejszenie ruchu na łączu i powrót tego łącza do pracy. Rutery więc zaczną znowu wysyłać pakiety przez to łącze, zwiększając jego obciążenie, co wkrótce spowoduje kolejne uszkodzenie. Jeśli proces ten powtarza się, a zwłaszcza jeśli zachodzi szybciej niż wynosi czas zbieżności ruterów, to rutery będą cały czas w stanie niestabilności interfejsów i większą części mocy swoich procesorów CPU będą poświęcały na przeliczanie tras.

Sytuacja taka określana jest jako *routeflup* Gdyby łącza redundantnego tam nie było, reszta sieci stwierdziłaby po prostu, że główne łącze przestało istnieć, i zaczęłaby eliminować ruch wychodzący na to łącze.

Nie chcę nikogo przekonywać, że łącza redundantne są złe. Mogą mieć one duzi znaczenie w przypadku katastrofalnych uszkodzeń sieci. Trzeba je jednak ostrożnie rozmieszczać. Musisz również stale monitorować główne łącze, by wiedzieć, kiedy ulegnie ono uszkodzeniu. Czasami ze zdziwieniem dowiadywałem się, że w moje sieci FDDI został uszkodzony pierścień podstawowy i sieć pracuje na pierścieni! zapasowym. Sieć wykorzystująca topologię pierścienia FDDI funkcjonowała be: przerwy, ukrywając przed użytkownikami fakt wystąpienia awarii.

Do jakiej grupy należy zaliczyć łącza redundantne?

Jeśli Twoja sieć została zaprojektowana zgodnie z metodą, którą opisałem w te książce, to zapewne składa się z trzech elementów: rdzenia, części dystrybucyjnej sieci dostępowych. Łącza zapasowe najlepiej umieścić jak najbliżej sieci dostępowych Za takim rozwiązaniem przemawia fakt, że łącza te znajdują się ponad wszystkim innymi połączeniami, a ich zadaniem jest łatanie dziur powstałych w elementach dystrybucyjnych i rdzeniu sieci.

Typowym efektem takiego rozwiązania, zwłaszcza kiedy podstawową topologią siec jest gwiazda lub hybryda gwiazd, jest próba połączenia coraz większej liczby najbliższych sieci dostępowych, tak że struktura sieci będzie przypominała ogromne kot starej lokomotywy. Kiedy zastanowisz się nad tym, ile łączy należałoby dodać, zdasz sobie sprawę, że koszty takich redundantnych połączeń są dość wysokie, a zwiększony stopień złożoności sieci zmniejszył nie tylko jej niezawodność, ale także elastyczność. Pamiętaj, że wybór topologii gwiazdy podyktowany był możliwością stosunkowo łatwego przenoszenia urządzeń dołączonych do sieci.

Lepsze efekty przyniesie umieszczenie łączy zapasowych w elementach takich jak rdzeń lub część dystrybucyjna sieci. W elementach tych łącza redundantne będą zapewniały połączenie zapasowe, obsługujące kilka sieci dostępowych, przez co ni trzeba będzie stosować kilku oddzielnych łączy dla osiągnięcia tego samego poziomi redundancji. Ale nawet wtedy wystrzegaj się dowolnego rozmieszczania łączy redundantnych pomiędzy sieciami dystrybucyjnymi. Kilka rozsądnie rozmieszczonych łączy zwiększy niezawodność sieci i pozwoli jej przetrwać nawet w przypadku duże go uszkodzenia rdzenia. Zbyt duża liczba łączy zapasowych może spowodował spadek niezawodności i elastyczności sieci, a także zwiększyć stopień jej złożoności.

Jednym z najlepszych sposobów tworzenia łączy redundantnych, zwłaszcza w się ciach WAN, jest tworzenie dla łączy dzierżawionych zapasu w postaci łączy zestawianych na żądanie. Na przykład za dodatkowy koszt - kupienie pary analogowych modemów i pary łączy telefonicznych - możliwe jest skonfigurowanie wolnego łącz zapasowego dla szybkiego łącza WAN pomiędzy centralą a oddziałem firmy. Ponieważ łącze zapasowe nie będzie w stanie obsłużyć całego ruchu, jaki był generowań przez stałe łącze WAN, konieczne będzie zastosowanie filtrów, które pozwolą na przesyłanie tylko najważniejszych z punktu widzenia firmy danych.

Łącze takie może być również jedynym sposobem dotarcia do rutera w oddziale firmy w celu naprawienia błędu w konfiguracji, który być może spowodował przerwę w pracy łącza podstawowego. Przykład na to, jak należy konfigurować zestawiane na żądanie łącze zapasowe, opisany jest w rozdziale 6.

Po zidentyfikowaniu redundantnych komponentów sieci takich jak łącza, rutery lub bezprzerwowe zasilanie zastanów się, czy za ich pomocą rzeczywiście zapewniasz redundancję sieci. Łącza zapasowe często biegną tą samą drogą (na jednym odcinku lub nawet na całej długości) co łącza podstawowe. Jeśli Twoje łącze podstawowe i zapasowe wchodzą w skład tego samego pęku kabli, to taki zapas nie pomoże w przypadku, kiedy koparka przerwie kable. Nie pomogą także zdublowane zasilacze dołączone do tego samego urządzenia UPS, jeśli to urządzenie ulegnie uszkodzeniu.

Na zakończenie należy podkreślić, że jednym z najlepszych sposobów ochrony sieci przed uszkodzeniami jest dobre zarządzanie jej pracą. Większość przerw w pracy sieci spowodowanych jest nie przez zewnętrzne czynniki, ale przez normalne, codzienne działania związane z rekonfiguracją sieci, które wykonywane są przez personel. Instalator dodający nowe łącze do szafy kablowej może przez przypadek odłączyć jakąś linię lub błędnie zestawić połączenie. Operatorzy sieci mogą błędnie zmienić konfigurację rutera w taki sposób, że spowoduje ona falę uszkodzeń w całej sieci. Kable ułożone pod podłogą i doprowadzone do stelaży ze sprzętem mogą nagle zostać rozłączone i przestaną zasilać cały zestaw urządzeń. Wszystkie te uszkodzenia mogą nie wystąpić, jeśli odpowiednio wyszkolony personel będzie pracował ostrożnie, stosując odpowiednie metody, i działał zgodnie z opracowanym wcześniej planem.

Jeśli chodzi o uszkodzenia sprzętu, to dwoma najlepszymi rozwiązaniami jest posiadanie zestawu części zapasowych oraz zestawu zapasowych urządzeń wybranych z uwzględnieniem prawdopodobieństwa wystąpienia uszkodzeń i możliwości ich naprawy. W zasadzie jeśli sprzęt nie ulega uszkodzeniom, to nie powinieneś się w ogóle zajmować uszkodzeniem sieci, które może z tego wynikać. Jest to jedno z podstawowych kryteriów doboru urządzeń, o których będziemy mówili w rozdziale 4, zatytułowanym „Wybór sprzętu sieciowego".

A co z sieciami wieloprotokołowymi?

Choć jest to temat nie wchodzący w zakres tej książki, sieci wieloprotokołowe są zbyt często spotykane, aby je całkiem ignorować. Choć nie możemy doradzać, w jaki sposób można skonfigurować sieć, tak by mogły w niej koegzystować różne protokoły, możemy jednak zaprezentować kilka tematów związanych z sieciami wieloprotokołowymi. Tematy te będziesz musiał przeanalizować w swojej sieci, zwłaszcza jeśli taki rodzaj pracy może mieć wpływ na jej projektowanie.

Kilka sieci szczęśliwie pracuje z jedną, taką bądź inną, rodziną protokołów. Większość sieci musi jednak obsługiwać mieszankę protokołów takich jak IP, IPX (wykorzystywany przez Nowell Netware), AppleTalk, DecNet i wiele innych. Każdy z tych protokołów ma pewne zalety i każdy z nich posługuje się własnymi zasadami odnośnie adresowania, rutowania, nazewnictwa itd.

Zasady różnych protokołów często są sprzeczne.

Jak więc należy obsługiwać w sieci protokoły inne niż IP? Masz trzy możliwości:

- całkowicie *zakazać* używania protokołów innych niż IP;
- pozwolić na stosowanie tych protokołów, ale nie rutować ich pomiędzy segmentami sieci;
- rutować protokoły inne niż IP na takiej samej zasadzie co IP.

Każda z tych opcji ma swoje zalety i wady, tak jak wszystko inne w sieciach komputerowych. Na przykład trudno jest zabronić wykorzystania protokołu innego niż IP, jeśli nie możesz delegować jednej osoby, by zajmowała się wykrywaniem i usuwaniem prób niestosowania się do tego zakazu. Na szczęście rzadko stosuje się takie rozwiązanie.

Drugi sposób ma tę zaletę, że w sieci LAN jednego z działów możliwe będzie stosowanie protokołu innego niż IP, który w takiej sieci będzie najskuteczniejszy. Ponieważ jednak nie rutujesz tego protokołu pomiędzy segmentami, to wszelkie problemy, jakie może on powodować, ograniczają się do jednego segmentu sieci. Nie znaczy to, że masz się nimi przejmować, ale pamiętaj, że zakres występowania potencjalnych problemów w pracy sieci jest znacznie mniejszy.

Takie rozwiązanie ma jednak jedną podstawową wadę. Jeśli zezwolisz na stosowanie innych protokołów, ale nie będziesz ich rutował, to decyzje o przydzielaniu poszczególnych maszyn do podsieci IP będą musiały uwzględniać fakt, czy maszyna będzie używała jeszcze innego protokołu, czy też nie, i w jakiej grupie komputerów powinna pracować. Na przykład jeśli komputer w dziale księgowości, w którym stosowany jest protokół AppleTalk, ma być dołączony do sieci, to powinien znaleźć się w tej samej podsieci IP, co pozostałe maszyny z księgowości, by mógł wykorzystywać usługi AppleTalk. To może być dość kłopotliwe, drogie, a nawet niemożliwe do zrealizowania.

Zalety i koszty rutowania wieloprotokołowego

Dlaczego więc nie podjąć decyzji o nitowaniu protokołów innych niż IP? Przecież zalety rutowania innych protokołów nie są bez znaczenia:

- Większość protokołów sieciowych ma więcej podobieństw niż różnic. Ruter, który potrafi sprawnie rutować jeden protokół, może równie wydajnie obsługiwać inne protokoły.
- Rutowanie protokołów innych niż IP przez rutery sieci IP oznacza, że protokoły te są administrowane przez ten sam personel, który zajmuje się rodziną protokołów IP, co redukuje powtarzanie tych samych prac i dublowanie sprzętu.
- Wiele z protokołów innych niż IP znacznie wydajniej pracuje w sieci LAN. Na przykład protokoły takich firm jak Novell Netware (IPX) i Banyan Vines zapewniają wydajniejszą obsługę transferu plików i drukowania dla pecetów niż protokół o nazwie Sieciowy System Plików *(Network File System - NFS),* który wchodzi w skład zestawu IP.
- Rutowanie protokołów innych niż IP zwiększa elastyczność Twojej sieci i wychodzi naprzeciw potrzebom Twoich użytkowników.

A co z sieciami wieloprotokołowymi?

Rozważania te prowadzą do wniosku, że nitowanie wieloprotokołowe jest pomysłem dobrym, przynajmniej w teorii. Są jednak inne argumenty, które każą się dobrze zastanowić, jakie protokoły inne niż IP (jeśli w ogóle jakieś) powinno się rutować. Są pewne powody, dla których lepiej nie rutować protokołów innych niż IP:

- wymagania dotyczące dodatkowej wiedzy personelu; nie każdy jest ekspertem wiedzącym wszystko, ale będziesz potrzebował specjalistów od każdego z nitowanych w sieci protokołów, którzy potrafią określić potrzeby tego rutowania i wykrywać błędy w pracy sieci;
- dodatkowe obciążenie ruterów; każdy rutowany protokół wymaga przechowywania w pamięci urządzenia oddzielnej tablicy rutowania, a czasami nawet własnego dynamicznego protokołu rutowania, co dodatkowo obciąży pamięć i moc procesora;
- zwiększona złożoność sieci; ruter wieloprotokołowy jest znacznie bardziej skomplikowanym urządzeniem i oprogramowaniem niż ruter jednoprotokołowy, przez co błędy w implementacji i obsłudze jednego z protokołów mogą wpływać na stabilność obsługi pozostałych;
- bardziej złożony projekt; każda rodzina protokołów ma własne reguły rutowania, adresowania itd., a zasady te są często sprzeczne, co sprawia, że należy poświęcić wiele czasu i pracy na projektowanie sieci, która będzie obsługiwała poprawnie wszystkie konieczne protokoły;
- ograniczona skalowalność; niektóre protokoły nie skalują się tak dobrze jak inne, mogą także nie pracować dobrze w sieciach WAN, co ogranicza skalowalność całej sieci.

Tunelowanie jako alternatywa dla wieloprotokołowego rutowania

Rozwiązaniem pośrednim, które może być użyteczne lub zostanie wymuszone przez stosowanie innych protokołów w sieciach LAN bez ich rutowania, jest tworzenie tuneli łączących odizolowane od siebie sieci LAN pracujące z własnym protokołem. Tunel oznacza tu przesyłanie nie rutowalnych protokołów pomiędzy dwoma hostami pracującymi z tymi protokołami przez zamykanie ich pakietów w pakiety innego protokołu (w naszym przypadku będzie to IP), który jest rutowany. Maszyna pracująca na jednym końcu tunelu umieszcza kompletny pakiet wewnątrz części pakietu IP przeznaczonej na dane i przesyła go przez sieć do drugiego końca tunelu. Odbierająca taki pakiet maszyna wyjmuje go z protokołu tunelującego i przesyła dalej jako pakiet używanego protokołu, innego niż IP.

Choć zasada działania tunelowania jest prosta, to należy pamiętać że powoduje one nieznaczną utratę wydajności. Maszyna wysyłająca pakiet przesyła go przez siec lokalną do hosta tunelującego jako pakiet używanego zestawu protokołów. Host obsługujący tunelowanie pakuje ten pakiet w inny protokół i przesyła go na drugi koniec tunelu. Transmisja ta, w zależności od struktury sieci, może przechodzić prze/ ten sam segment sieci lokalnej, przez który przesłany był przed chwilą oryginalny pakiet. Drugi koniec tunelu odbiera zapakowany pakiet poprzez lokalny segment swojej sieci, wyjmuje go i przesyła do adresata. W najgorszym wypadku każdy pakiet przesyłany tunelem będzie przesyłany dwa razy przez lokalny segment sieci na każdym z obu końców tunelu. Ponadto należy policzyć dodatkowy czas potrzebny na hermetyzację pakietu, by przesłać go przez tunel, i rozhermetyzowanie go po drugie stronie tego tunelu.

Nie myśl jednak, że tunelowanie jest zawsze złym rozwiązaniem. Może to być najlepsza metoda umożliwiająca komunikację między małymi, odizolowanymi od siebie sieciami LAN. Sieci te mogą pracować ze swoim własnym protokołem, a Ty nie musisz obsługiwać tego protokołu na ruterach, by się widziały. Możliwe będzie nawet przekazanie odpowiedzialności za te tunele poszczególnym oddziałowym sieciom LAN, które je wykorzystują. Ponieważ ich administratorzy będą sami obsługiwać tunele, to może z czasem przemyślą sprawę i *zaczną* stosować protokół IP. To oni będą przekonywali dostawcę sprzętu, który wykorzystują, aby ten dostosował go do pracy z uniwersalnym protokołem transportowym, jakim jest IP.

Zalety rutowania wieloprotokołowego są duże, podobnie jak koszty takiego rozwiązania. Kiedy zastanawiasz się, jaki protokół inny niż IP będziesz rutował w swojej sieci, to pamiętaj o mojej zasadzie: rutuj jak najmniej protokołów i tylko te, które musisz. Staraj się, aby Twoja sieć była jak najmniej skomplikowana - nie rutuj innych protokołów tylko dlatego, że masz takie możliwości.

Wybór sprzętu sieciowego 4

Co to jest ruter IP? Kryteria doboru ruterów

W poprzednich rozdziałach omówiliśmy proces projektowania sieci. Jeśli postępowałeś zgodnie z zawartym tam opisem, to masz gotowe dwa opracowania. Pierwszym z nich jest Twój ideał sieci - sieć jaką chciałbyś zbudować, gdybyś nie był ograniczony istniejącymi już rozwiązaniami. Drugi natomiast to modyfikacja projektu Twojej idealnej sieci, uwzględniająca już istniejące rozwiązania.

Czasami konieczne jest zastosowanie ruterów. Ich liczba nie jest tu ważna, ponieważ z czasem odkryjesz, że obsługa takiej liczby segmentów, jaką planujesz zastosować w swojej sieci, wymaga kilku mniej lub kilku więcej ruterów. W trakcie realizowania projektu i tak będziesz go modyfikował. Ponadto podczas wykorzystywania sieci odkryjesz pewne ograniczenia, o których wcześniej nie pomyślałeś, i będziesz musiał sobie z nimi radzić, na przykład poprzez dodanie ruterów. Jako prosty przykład podam sytuację, kiedy w trakcie realizacji projektu sieci okaże się, że niemożliwe jest doprowadzenie wszystkich kabli sieciowych do użytkowników w budynku z jednej szafy krosowniczej. Niektóre z działów firmy mogą być umieszczone w częściach budynku, do których nie sięgają ograniczone wybranym medium kable sieciowe. Będziesz musiał dokonać wyboru pomiędzy zmianą medium a dodaniem drugiej szafy krosowniczej. Każde z tych rozwiązań może wpłynąć na sposób rozmieszczenia ruterów.

Jedną z najważniejszych części Twoich projektów są zadania stawiane sieci oraz liczba i rodzaj segmentów sieci, które będą obsługiwane z każdego miejsca lokalizacji ruterów. Zadania, jakie stawiasz sieci, pomogą Ci zdecydować, które funkcje muszą być obsługiwane przez oceniane rutery podczas dokonywania wyboru urządzenia, ze szczególnym uwzględnieniem takich parametrów jak: redundantne zasilanie, czas uruchamiania i użyteczność.

Zakładam, że liczba i rodzaj segmentów, które będziesz obsługiwał, są wartościami typowymi i nie mają większego wpływu na nasze rozważania. Jest przecież rzeczą oczywistą, że jeśli masz cztery segmenty sieci Ethernet stykające się w miejscu, w którym planujesz umieścić ruter, to musisz mieć do dyspozycji przynajmniej cztery porty Ethernet, niezależnie od tego, czy będą one obsługiwane przez jeden, czy przez klika ruterów. W tym rozdziale skoncentruję się jednak na ocenie ruterów na podstawie celów wynikających z projektu sieci.

Co to jest ruter IP?

Na wstępie powinniśmy dokładnie wyjaśnić, czym jest urządzenie nazywane ruterem IP. Choć może się to wydawać bezcelowe, to zdziwiłbyś się, ile różnych odpowiedzi otrzymasz (z których wszystkie mogą być poprawne) pytając o to. Ruter IP to urządzenie, które łączy dwie lub więcej sieci IP (lub podsieci) i przełącza pomiędzy nimi pakiety. Ponieważ definicja ta wykorzystywana jest w dyskusjach teoretycznych, jest dla nas zbyt abstrakcyjna. Pozwala jednak przynajmniej rozpocząć dyskusję.

W tej definicji mieszczą się trzy główne kategorie urządzeń. Pierwsza to tradycyjne urządzenia sieciowe pracujące w warstwie drugiej, takie jak mosty, koncentratory i przełączniki, które mają dodane funkcje rutowania. Drugą kategorią są komputery ogólnego zastosowania, wyposażone w dwa interfejsy lub więcej i oprogramowanie obsługujące rutowanie IP. Przykładem takiego rutera, którego budowa oparta jest na hoście, jest maszyna pracująca pod kontrolą systemu operacyjnego UNIX wyposażona w dwa interfejsy Ethernet. Trzecią kategorią jest sprzęt dedykowany i oprogramowanie, którego podstawowym (i prawdopodobnie jedynym) zadaniem jest rutowanie pakietów IP.

Pierwsza grupa ma wadę polegającą na ograniczonych osiągach lub ograniczonej elastyczności. Organizacje stosujące te urządzenia nie mogą już dłużej posługiwać się siecią o budowie opartej na mostach i muszą zastosować rutowanie. Często urządzenia te obsługują tylko jeden dynamiczny protokół rutowania (najczęściej jest to *Routing Information Protocol* - R/P). Funkcje rutowania dodane do tych urządzeń mogą wynikać z tego, że udało się zaadaptować oprogramowanie IP służące do zarządzania pracą tych urządzeń (funkcje takie jak SNMP lub Telnet). Urządzenia te można w łatwy sposób rozbudować tak, by obsługiwały podstawowe funkcje rutowania IP. Niestety, tak powstały kod rutera jest najczęściej źle zoptymalizowany i może obsługiwać małe sieci. Ogólnie rzecz biorąc, wolę nazywać te urządzenia *nitującymi koncentratorami* lub *nitującymi przełącznikami* i nie będę się nimi zajmował w dalszej części książki.

Obie pozostałe grupy (rutery zbudowane na bazie hostów i rutery dedykowane) mają swoich zagorzałych zwolenników pośród administratorów sieci IP. Są nawet tacy, którzy uważają oba rodzaje ruterów za jednakowo dobre. Zawsze jednak każda z grup zwolenników podkreśla zalety swoich ulubionych urządzeń przy wykonywaniu określonych zadań.

Rutery dedykowane a rutery działające na hostach

W początkowym okresie rozwoju sieci IP nie było na rynku dedykowanych ruterów. W sprzęcie ogólnego zastosowania dołączano kod rurujący do istniejącego systemu operacyjnego albo tworzono własny system operacyjny, w którym zaimplementowany był program rutera. Rutery z pierwszej grupy z czasem ewoluowały do ruterów działających na hostach, te z drugiej grupy - do dedykowanych ruterów.

Spośród systemów ogólnego zastosowania z osadzonym kodem obsługującym rutowanie jednym z najpopularniejszych stała się odmiana systemu operacyjnego UNIX przygotowana na Uniwersytecie Kalifornijskim w Berkeley i znana jako *Berkeley Software Distribution - BSD.* System ten został przeniesiony na wiele platform sprzętowych; opracowanie jego warstwy sieciowej jest podstawą dla większości implementacji systemu UNIX IP a także dla innych systemów. Większość sieci Internet zależy od rutowania obsługiwanego na tym systemie. Obecnie rutowanie oparte na hostach obsługuje również system operacyjny Windows NT.

Rutery o budowie opartej na hostach mają kilka zalet. Są zwykle tańsze od ruterów dedykowanych. Komputer, na którym są uruchomione, może być wykorzystywany do pełnienia innych funkcji w sieci, na przykład jako serwer plików. Pracownicy zajmujący się obsługą sieci znają ten sprzęt i oprogramowanie. W większości organizacji znajduje się sprzęt, który może z powodzeniem pełnić dodatkowo funkcję rutera, a dodanie kolejnego interfejsu sieciowego nie jest kosztowne. Większość zwolenników ruterów dedykowanych nie zgodzi się oczywiście z wymienionymi wyżej zaletami. Trzeba przyznać, że rutery działające na hostach także mają swoje wady i powinny być rozważnie stosowane. Trudno jest wykonywać wiele funkcji jednocześnie i wszystkie robić dobrze. Serwery plików z reguły źle obsługują dużą liczbę przerwań, a zbyt duża liczba przerwań sprawia, że serwery plików zaczynają wolno pracować. Wynika to z faktu, że systemy operacyjne serwerów plików są zoptymalizowane pod względem obsługi jednej funkcji kosztem pozostałych. W rezultacie serwery plików nie będą pracowały dobrze jako rutery, a rutery nie będą pracowały dobrze jako serwery plików.

W przeciwieństwie do ruterów pracujących na hostach, rutery dedykowane są dobrze zoptymalizowane do przełączania pakietów IP. Zarządzanie buforami w tych urządzeniach, kontrola procesów i schematy obsługi przerwań zostały opracowane z myślą o tym jednym zadaniu. Taka charakterystyka, w połączeniu z brakiem konieczności zapewnienia obsługi wielu użytkowników, kompilatorów i skomplikowanego systemu plików, pozwala im na znacznie wydajniejszą pracę. Drugą podstawową zaletą dedykowanych ruterów jest liczba obsługiwanych portów. Zwykle ruter działający na hoście ograniczony jest do 10 interfejsów sieciowych. Ograniczenie to wynika albo z systemu operacyjnego hosta, albo z fizycznych ograniczeń sprzętu. Często liczba interfejsów ograniczona jest do dwóch lub trzech. Ruter dedykowany może z łatwością obsługiwać jednocześnie 100, a nawet więcej portów. Większa liczba obsługiwanych portów pozwala sieciom zbudowanym na ruterach dedykowanych na łatwiejszą skalowalność, a tym samym zmniejsza znaczenie argumentu oszczędności kosztów, podawanego przy ruterach opierających się na hostach.

Jeśli ruter opierający się na hoście kosztuje tyle co dziesiąta część rutera dedykowanego, ale dedykowany ruter obsługuje 10 razy więcej portów, różnica w cenie *zaczyna* być mało istotna.

Trzecią podstawową zaletą ruterów dedykowanych jest ich elastyczność. Elastyczność ta wyraża się na dwa sposoby. Po pierwsze, dedykowane rutery obsługują więcej typów interfejsów. W zależności od systemu operacyjnego hosta ruter pracujący na hoście może obsługiwać tylko jeden lub dwa typy interfejsów, takie jak Ethernet oraz FDDI. Dedykowane rutery mogą obsługiwać tuzin, a nawet więcej różnych interfejsów umieszczanych w jednej obudowie, pozwalając Ci na połączenie wielu różnych mediów sieci bez konieczności kupowania oddzielnego hosta dla każdego z nich. Po drugie, rutery dedykowane obsługują z reguły wiele różnych dynamicznych protokołów rutowania, a część z nich obsługuje również protokoły inne niż IP. Rutery pracujące w oparciu o hosty obsługują zwykle jeden dynamiczny protokół rutowania (głównie RIP), chyba że zostanie dołączone dodatkowe oprogramowanie, takie jak *gated** Takie rutery rzadko mogą być jednak rozszerzone o obsługę rutowania protokołów innych niż IP, która może Ci być potrzebna.

Opisane tu wady ruterów opierających się na hostach sprawiają, że rutery te nadają się do obsługi sieci, która się rozrasta. Dlatego wiele organizacji wymienia rutery działające na hostach na rutery dedykowane. Jeśli jednak wierzysz, że rutery uruchamiane na hostach mogą znaleźć zastosowanie w sieci, którą zaprojektowałeś, powinieneś ich użyć. Choć nie będę w tej książce omawiał tematów związanych z ich konfiguracją i zarządzaniem, to w pracy nimi powinieneś stosować techniki omawiane w tej książce i stosowane przy pracy z ruterami dedykowanymi.

Niektóre tematy dotyczące konfigurowania ruterów pracujących na hostach możesz znaleźć w książce *TCP/IP Administracja sieci,* wydanej w Polsce przez wydawnictwo ReadMe, którą napisał Craig Hunt dla O'Reilly&Associates.

Kryteria doboru ruterów

Kiedy wybierasz ruter, pamiętaj o celach, jakie wyznaczyłeś swojej sieci w trakcie jej projektowania. Nie ma sensu martwić się o inne kryteria, kiedy podstawowe zadania sieci nie są dostatecznie dobrze określone. Kiedy zrozumiesz podstawowe cele, będziesz mógł określić różne kryteria, które pomogą Ci wybrać właściwy ruter. Na przykład jeśli Twoim celem jest osiągnięcie wysokiego stopnia dostępności sieci, to będziesz bardziej zwracał uwagę na niezawodność rutera niż na jego elastyczność. Każdy administrator sieci powinien rozważyć potencjalne kryteria wyboru ruterów stworzone na podstawie celów opisanych wyżej, ale każdy administrator będzie przykładał różną wagę do poszczególnych kryteriów.

Gated, demon gateway, został opracowany na Uniwersytecie Cornell, ale jest rozwijany przez MERIT, sieć badawczo-rozwojową stanu Michigan.

Funkcjonalność

Funkcjonalność oznacza stopień, w jakim ruter wypełnia funkcje, których się po nim spodziewasz. Każdy ruter IP będzie z pewnością rutował pakiety IP. W tym przypadku chodzi więc o inne funkcje. Na przykład jeśli zamierzasz uruchomić dynamiczny protokół rutowania, to oczywiste jest, że nie wybierzesz rutera, który nie ma takiej możliwości. Jakich funkcji spodziewasz się więc po ruterze, który ma pracować w Twojej sieci? Lista będzie różna dla różnych sieci, ale niektóre podstawowe funkcje będą musiały być obsługiwane zawsze. Należą do nich:

- obsługa przynajmniej jednego dynamicznego protokołu rutowania (RIP, OSPF, IGRP, EIGRP, BGP itd.);
- możliwość zrzucania informacji do pliku - z wykorzystaniem jakiegoś protokołu sieciowego lub buforowania online;
- interfejs konfiguracji i *zarządzania* rutera dostępny przez sieć (Telnet, WWW lub SNMP).

Dynamiczny protokół rutowania jest absolutnie konieczny, jeśli chcesz budować dużą sieć. Taki protokół może również ułatwić Ci zarządzanie małą siecią złożoną z kilku ruterów poprzez ograniczenie liczby zmian w konfiguracji ruterów, jakich należy dokonywać wraz ze zmianą konfiguracji całej sieci. Mając do wyboru wiele protokołów rutowania lepiej jest przemyśleć sprawę wyboru jednego z nich, zwłaszcza jeśli w sieci używany jest sprzęt pochodzący od różnych dostawców. Jeśli masz szczęście, to uda Ci się wybrać protokół rutowania, który jest obsługiwany przez wszystkie te urządzenia.

Zapisywanie informacji do rejestru jest prawdopodobnie jedną z najbardziej użytecznych funkcji diagnostycznych dostępnych dla administratora. Ponieważ sieć jest tworem dużym i dynamicznie się zmienia, to czasami trudno zdecydować, w którym miejscu należy zacząć szukać powodów jej wadliwego działania i czym jest ono spowodowane. Dobry, czytelny plik rejestru, który nie zasypuje Cię niepotrzebnymi szczegółami, może powiedzieć Ci nie tylko, gdzie powinieneś zacząć szukać usterki, ale również dlaczego występują problemy w pracy Twojej sieci. Najlepiej, jeśli informacje zapisywane w rejestrze są oznaczone jakimś rodzajem znacznika czasowego, o wartości absolutnej lub relatywnej w stosunku do siebie. Taki zapis pomaga w stwierdzeniu, kiedy jakieś zdarzenie ma miejsce.

Ostatnia z funkcji umożliwia konfigurowanie rutera i zarządzanie jego pracą przez sieć. Może zaoszczędzić Ci wielu wypraw do ruterów stojących w dalszej odległości lub pieniędzy wydanych na modemy i łącza telefoniczne. Najlepiej, jeśli interfejs sieciowy pozwala na wykonanie tych wszystkich poleceń, które dostępne są z terminala dołączonego bezpośrednio do rutera. Niezależnie od tego, jakie są Twoje plany i jak wygląda obecnie Twoja sieć, na pewno od czasu do czasu będziesz musiał konfigurować i testować jej pracę. Powinieneś mieć możliwość wykonywania tych funkcji przez sieć.

Oprócz podstawowych funkcji ruterów należy wspomnieć o innych funkcjach, które są pożądane:

- przesyłanie pakietów BOOTP/DHCP;
- zarządzanie przez SNMP;
- obsługa jakiegoś protokołu czasu, głównie po to, by ruter miał poprawną informację o czasie w sieci;
- możliwości filtrowania pakietów, które pozwolą Ci chronić segment sieci przeć dostępem z zewnątrz lub ograniczyć dostęp użytkowników segmentu sieci d' wybranych adresów przeznaczenia;
- obsługa zmiennej długości masek podsieci, nawet jeśli obecnie tego nie będziesz stosował.

Jeśli używasz dynamicznego protokołu przydzielania adresów, takiego jak BOOT lub DHCP, lub planujesz używanie go w przyszłości, musisz się zastanowić, czy Twoje przyszłe rutery będą przekazywały zapytania z jednego segmentu sieci d drugiego. Wiele ruterów powinno obsługiwać tę funkcję, ale niektóre z nich nie robi tego poprawnie. Bez tej możliwości będziesz zmuszony do zmiany planów dotyczących wykorzystywania wspomnianych protokołów lub do uruchomienia serwerów tych usług w każdym z segmentów. Takie rozwiązanie może być kosztowne i trudne w zarządzaniu, więc należy go unikać.

SNMP *(Simple Nctwork Management Protocol)* jest często uważany za coś, czego potrzebują tylko duże, rozległe sieci. Choć prawdą jest, że duża sieć może bardziej wykorzystywać SNMP i być bardziej uzależniona od tego protokołu, to należy pamiętać, że n wolno ignorować potencjału tego protokołu w małej sieci. Jeśli Twoja sieć jest nieduża, możesz używać prostego narzędzia opierającego się na SNMP w celu sprawdź nią osiągalności swojej sieci i zbierania informacji statystycznych. Jeśli jednak c samego początku nie będziesz rozważał użycia SNMP, to w miarę powiększania się sieci będziesz miał problemy z uruchomieniem w niej tych funkcji. Jeśli zakupiony wcześniej sprzęt nie może być zarządzany przez SNMP, to będziesz musiał zastosować ten protokół w części sieci, a pozostałymi elementami zarządzać starym sposobem.

Są dwa powody, dla których stosowane przez Ciebie rutery powinny obsługiwać standardowy protokół czasu. Bardziej oczywistym powodem jest to, że mogą o: wtedy służyć jako źródło czasu innym urządzeniom w sieci. Jeśli jednak Twoje rutę nie obsługują tej funkcji, to do podawania czasu w sieci możesz wykorzystywać jeden z pracujących w niej serwerów. Ważniejszym powodem stosowania protokołu czasu jest fakt, że rutery potrzebują poprawnej i dokładnej informacji o czasie w się Powinny pozwalać Ci skorelować pliki zawierające rejestry zdarzeń, a także inne działania, które mają zachowany znacznik czasu oraz porównanie wszystkich ty informacji z informacjami zbieranymi przez inne urządzenia pracujące w sieci. I przykład jeden z ruterów może regularnie zapisywać jakieś zdarzenia o czasie 5: AM. Informacja ta nie jest zbyt użyteczna, jeśli 5:35 AM na jednym ruterze oznacza 4:15 PM na drugim i 11:23 na jeszcze innym. Jeśli wszystkie Twoje rutery utrzymują dokładnie ten sam czas systemowy, to może się okazać, że zdarzenie występując 5:30 rano jest po prostu tworzeniem kopii zapasowej przez któryś z serwerów. Poprawna informacja o czasie zdarzenia może pomóc Ci stwierdzić, co dzieje się w Twojej sieci.

Kryteria doboru ruterów

Prawie każdy ruter obsługujący funkcję filtrowania pakietów pozwala na lokowanie ruchu w oparciu o adres IP źródła lub przeznaczenia pakietu. Funkcja ta jest tak powszechnie stosowana, że stała się praktycznie standardem. Może się jednak zdarzyć, że będziesz chciał zajrzeć do pakietu głębiej niż tylko do pól zawierających adresy. Może będziesz chciał zezwolić na pewną komunikację i zabronić innej. Może zechcesz na przykład zezwolić maszynie na wysyłanie i odbiór poczty elektronicznej, ale zabronić do niej dostępu *przez* Telnet. Elastyczny mechanizm filtrowania pakietów obsługiwany przez ruter powinien pozwolić Ci na takie działania. Musisz jednak pamiętać o tym, że jeśli ruter zacznie zaglądać głębiej do wnętrza pakietów, to jego wydajność prawie na pewno spadnie.

Nawet jeśli w obecnej chwili nie potrzebujesz obsługi zmiennej długości masek pod-sieci, powinieneś sprawdzić, czy Twoje rutery w pełni ją obsługują. Podobnie jak w przypadku SNMP, możesz nie potrzebować tej funkcji już teraz, ale jeśli zdecydujesz kiedyś zastosować takie maski, na pewno nie chciałbyś, aby kupiony wcześniej sprzęt uniemożliwił Ci zrealizowanie tego projektu. Ruter powinien być w stanie co najmniej współpracować z maskami, które nie kończą się na granicach oktetów. Powinieneś wybierać rutery poprawnie obsługujące maski podsieci, które są różne w różnych częściach sieci, nawet jeśli obecnie nie stosujesz żadnego dynamicznego protokołu rutowania, który mógłby obsługiwać tego typu informacje. Zawsze możesz dodać do konfiguracji trasy statyczne.

Pamiętaj, abyś był ostrożny i nie zaczął porównywać liczby funkcji jakie obsługuje każdy z analizowanych przez Ciebie ruterów. Jeśli jakaś funkcja nie będzie wykorzystywana w Twojej sieci, to nie ma sensu przejmować się tym, że jest ona obsługiwana przez jeden ruter, a przez inne nie (chyba że funkcja ta będzie stosowana w przyszłości). Porównuj tylko te funkcje, które zamierzasz wykorzystywać w swojej sieci.

Zgodność z resztą sprzętu

Jeśli będziesz musiał obsługiwać również istniejące rozwiązania sieciowe, to wymaganie dotyczące współpracy kupowanych urządzeń z tymi, które już masz, jest oczywiste. Nawet jeśli zaczynasz budować swoją sieć od zera, powinieneś zastanowić się nad tym, w jakim stopniu proponowane Ci rutery są zgodne ze sobą, z Twoimi hostami oraz urządzeniami sieciowymi pracującymi w warstwie 2, takimi jak koncentratory Ethernet lub przełączniki ATM. Nie myśl, że będziesz zawsze kupował urządzenia od jednego producenta. Upewnij się, że sprzęt, który zamierzasz kupić, będzie mógł współpracować ze sprzętem innych producentów. Mimo że wszyscy sprzedawcy planują wieczny udział w rynku, to niestety niektórzy z niego znikają, i być może będziesz musiał w pewnym momencie zmienić dostawcę. Jeśli tak się stanie, na pewno będziesz spokojniejszy wiedząc, że sprzęt oferowany przez firmy, które kiedyś odrzuciłeś, może współpracować ze sprzętem, który wybrałeś i zastosowałeś w swojej sieci. Konieczność wymiany wszystkich ruterów, by móc rozszerzać sieć, opierając się na innych urządzeniach, to katastrofa zbyt straszna, by o niej mówić.

Nie zakładaj również, że Twój sprzęt będzie współpracował poprawnie z innymi urządzeniami tylko dlatego, że wybrany przez Ciebie producent spełnia wymagania standardów. Standardy są często różnie interpretowane, co może czasem powodować niekompatybilność. Jeśli skupisz się tylko na jednej części całego procesu oceny urządzenia, tylko ona będzie w pełni zadowalająca. Nalegaj, aby dostawca udowodnił zgodność ze standardami każdego z elementów urządzenia.

Bądź ostrożny w rozmowach z dostawcą, który chce przekroczyć wymagane standardy, zwłaszcza jeśli chodzi o sprawy sprzętowe, takie jak długość kabli. Choć niewątpliwie nieznaczne przekroczenie standardów kusi i pozwala użyć kabla parę metrów dłuższego, niż określa to standard, zwłaszcza jeśli dostawca na to zezwala (i jeśli spełnia to Twoje wymagania odnośnie topologii sieci). Musisz jednak pamiętać, że kłopoty zaczną się, kiedy w przyszłości będziesz chciał wymienić ten sprzęt na inny, pochodzący od producenta, który bardziej dokładnie trzymał się standardów. Tak jak powinieneś naciskać na spełnianie standardów przez sprzedawcę, tak samo powinieneś nalegać, aby spełniane były one dokładnie, nawet jeśli trochę więcej będzie Cię to kosztowało. Kiedyś na pewno przekonasz się, że warto było tak postępować.

Jeśli to możliwe, spróbuj poświęcić trochę czasu i zestaw urządzenia w małą sieć testową, używając urządzeń tak wielu różnych producentów, jak to tylko możliwe. Wypróbuj w tej sieci działanie wszystkich funkcji, które zamierzasz wykorzystywać, sprawdzając, jak dobrze pracują one w heterogenicznym środowisku. Postaraj się przetestować współpracę na poziomie podstawowych funkcji, takich jak obsługa wysyłania i odbioru pakietów. Nie przesyłaj kilku zapytań o echo ICMP do rutera, a po otrzymaniu odpowiedzi nie stwierdzaj, że wszystko jest w porządku. Spróbuj raczej obciążyć testowaną sieć, przepuszczając przez ruter pakiety generowane na przykład przez własny personel. To jest jedyny pewny sposób wygenerowania nie tylko poprawnego ruchu w sieci, ale również innych danych, które są typowe dla pracy Twojej sieci.

Po drugie, sprawdź jakość współpracy ruterów przy wykorzystaniu różnych dynamicznych protokołów rutowania. Protokoły te są często dość skomplikowane i mają setki stron dokumentacji. Z punktu widzenia producenta najłatwiej jest zaimplementować poprawnie tylko jeden z nich.

Ostatecznie wypróbuj zachowanie sieci testowej przy symulowanych uszkodzeniach i sprawdź, jak poszczególne rutery wykrywają uszkodzenia i jak sobie z nimi *radzą,* a także jak przebiega proces odtwarzania połączeń po naprawieniu uszkodzeń. Spróbuj wyłączyć zasilanie ruterów i innego sprzętu sieciowego, robiąc to w różnej kolejności. Może się okazać, że niektóre urządzenia po ponownym włączeniu inicjują się poprawnie, a inne wcale nie zaczynają pracy. Wyłącz wszystkie urządzenia równocześnie, wyłączając na przykład główny bezpiecznik, co pozwoli Ci zasymulować podnoszenie się systemu bez nadzoru, po przerwie w zasilaniu. Kiedy odkryjesz jakieś cechy niekompatybilności, nie dyskwalifikuj od razu takiego rutera lub ruterów. Poproś dostawcę o pomoc w rozwiązaniu problemu. To pozwoli Ci również zapoznać się z jakością usług, jakie firma oferuje.

W mojej sieci na przykład rozpoczęliśmy testowanie ruterów dostarczonych nam przez pewną nową firmę. Nasza sieć szkieletowa składa się z pierścienia FDDI łączącego pięć ruterów znajdujących się w jednym pomieszczeniu. Kiedy do tego pierścienia dodaliśmy nowy ruter, praca pierścienia została zakłócona w wyniku niepoprawnej pracy jednego połączenia fizycznego. Wyizolowaliśmy to łącze i stwierdziliśmy, że problem występuje zawsze po stronie nowego rutera, niezależnie od tego, w którym miejscu sieci go umieszczamy. Zamiast dyskwalifikować nowy sprzęt poprosiliśmy o przybycie specjalistów z obu firm i poprosiliśmy ich o rozwiązanie tego problemu. Obydwie firmy bardzo chciały rozwiązać powstały problem. Dotychczasowy dostawca chciał przecież nadal sprzedawać nam swoje produkty i chętnie z nami współpracował, nawet jeśli problemy z siecią nie były spowodowane wadliwym działaniem jego urządzeń. Nowy producent natomiast musiał nam pokazać, jak potrafi radzić sobie z kłopotami tego typu, jeśli chciał robić z nami interesy.

W końcu obie firmy doszły do wspólnego wniosku (muszę dodać, że nie tak łatwo im to przyszło), że przyczyna kłopotów leży po stronie pierwszego (wcześniejszego) dostawcy. Taki wniosek nie zadowolił jednak naszego ewentualnego nowego dostawcy, który nas zapewnił, że popracują nad swoim ruterem, aby ten mógł współpracować z naszymi urządzeniami. Wtedy już wiedzieliśmy, kto będzie od teraz dostarczał nam rutery, zwłaszcza że dotychczasowy dostawca poinformował nas, że nie może nic zrobić, by rozwiązać nasz problem.

Niezawodność

Niezawodność jest jednym z kryteriów, które najtrudniej określić w procesie oceny każdego sprzętu. Sprzedawcy szybko wyznaczają i podają do wiadomości wartość parametru średniego czasu bezawaryjnej pracy *(mean time between failures - MTBF)* oraz średniego czasu naprawy *(mean time to repair - MTR)*,* ale wartości te nie są niczym innym jak średnimi uzyskanymi z danych producenta. Dane producenta opierają się zwykle na czasach związanych z naprawą sprzętu, a uszkodzenia oprogramowania są zupełnie ignorowane. Mimo to czasy te mogą być interesujące.

Jak więc można ocenić niezawodność rutera, jeśli nie mamy do dyspozycji pewnych danych porównawczych? Jest to sprawa niezwykle ważna, ponieważ niezawodność jest jednym z podstawowych czynników, który pomoże Ci lub przeszkodzi w osiągnięciu celów. Radzę porozmawiać z innymi administratorami sieci. Poproś przyszłych dostawców o listę klientów, którzy mieszkają w tym samym mieście i mają dany produkt lub takich, których sieci są podobne do Twojej i zbudowane z oferowanych Ci urządzeń. Jeśli sprzedawca odpowie Ci, że nie może zdradzać nazw i adresów swoich klientów, zacznij być podejrzliwy! Choć może chce chronić w ten sposób prywatność swoich klientów, to może również chcieć ukryć kłopoty z dotychczasowymi klientami.

*Znanego również jako MTTR.

Kiedy rozmawiasz z wcześniejszymi klientami dostawcy poinformuj ich, że chcesz kupić dany sprzęt. Możesz także opisać w skrócie rodzaj sieci, jaki chcesz obsługiwać za pomocą tych urządzeń. Zapytaj użytkowników, jakie problemy mieli ze stosowanym sprzętem, jaką pomoc otrzymali od dostawcy tego sprzętu, jak często zdarzają się kłopoty z oprogramowaniem oraz jakie jest ich ogólne zdanie na temat dokonanego wyboru. Być może Twoi rozmówcy poinformują Cię, jakich innych dostawców brali pod uwagę i co zaważyło na ich decyzji. Może się okazać, że wybierali spośród tych samych dostawców co Ty i być może przekażą Ci informacje, do których Ty sam jeszcze nie dotarłeś.

Na zakończenie trzeba stwierdzić, że wiele pytań dotyczących niezawodności sprowadza się do nazwy proponowanego sprzętu. Nie powinieneś spodziewać się problemów po ruterach, na których widnieją nazwy takie jak: Cisco, Bay lub Proteon, ale zakup rutera typu Joe's Routers powinieneś lepiej przemyśleć. Oszczędność w momencie zakupu może oznaczać większe koszty w późniejszym okresie eksploatacji rutera, zwłaszcza jeśli uszkodzony sprzęt będziesz musiał w końcu wymienić na nowy.

Obsługowość

Niezależnie od tego, czy używamy rutera dedykowanego, czy też rutera działającego na noście, ruter to jedno z najbardziej skomplikowanych urządzeń złożonych z części sprzętowej i oprogramowania. Bez względu na to, jak niezawodne są rutery, które wybrałeś, z pewnością nie unikniesz uszkodzeń sprzętu i oprogramowania. Jeśli ktoś próbuje Ci wmówić, że jego sprzęt nigdy nie ulega uszkodzeniom, to powinieneś od razu zwrócić się do innego dostawcy! Kiedy ruter ulega uszkodzeniu, to najważniejszym elementem jest obsługowość. Powinieneś zwrócić szczególną uwagę na:

- możliwość wymiany komponentów w czasie pracy urządzenia;
- dostęp personelu serwisowego do tych komponentów;
- funkcje samo diagnostyki urządzenia;
- łatwe uaktualnianie oprogramowania.

Jeszcze kilka lat temu komponenty wymieniane „na gorąco" - w czasie pracy urządzenia - były rzadkością. W miarę jak nieprzerwana praca sieci komputerowych była coraz ważniejsza, wyłączanie urządzenia tylko po to, aby wymienić jakiś jego komponent, stało się nierozsądne. Wielu producentów tego typu urządzeń mających modularną budowę opracowało metody wymiany poszczególnych modułów bez konieczności wyłączania urządzenia. Tak więc możliwa stała się wymiana uszkodzonej karty Ethernet rutera bez konieczności przerywania pracy użytkowników, którzy nie są do tej karty dołączeni. Możliwość wymiany komponentów w czasie pracy rutera może stać się niezwykle istotna, w miarę jak sieć będzie się rozrastała.

Rutery, które nie mają komponentów wymienianych „na gorąco", mogą umożliwiać łatwy dostęp do komponentów. Jako przykład podam urządzenie o nazwie DEC Rainbow PC, które można rozebrać na najmniejsze komponenty wraz z wyjęciem płyty głównej w ciągu niespełna 15 minut i bez użycia żadnych narzędzi.

Kryteria doboru ruterów

Nawet jeśli komponenty nie mogą być wymieniane bez wyłączania urządzenia, to gdy możliwa jest ich szybka wymiana/mogą być nadal stosowane w sieci, gdyż przerwy w jej pracy spowodowane serwisowaniem tego urządzenia są niewielkie. Łatwy dostęp do komponentów może być nawet bardziej przydatny niż możliwość wymiany ich „na gorąco". Oczywiście niezależnie od tego, w jaki sposób wymieniamy elementy, żadne z rozwiązań nie jest w niczym pomocne, jeśli nie można określić, co uległo uszkodzeniu. I tu zaczyna się problem samo diagnozowania urządzenia.

Czasami uszkodzenie może być tak wyraźne, że możliwe będzie zidentyfikowanie uszkodzonego komponentu na podstawie obserwacji urządzenia. Częściej jednak komponenty ulegają dziwnym uszkodzeniom lub uszkodzenie sprawia, że tylko częściowo przestają one funkcjonować. W takich przypadkach konieczny jest poszerzony zestaw możliwości diagnozowania pracy urządzenia. Ruter powinien przekazywać informację o tym, ile ruchu przesyła i odbiera na każdym z interfejsów, ile różnego rodzaju błędów notuje, a nawet informację o tym, jaka jest temperatura wewnątrz urządzenia lub napięcie zasilania. Dzięki takim informacjom możliwe jest dokładne przeanalizowanie poszczególnych komponentów rutera i określenie przyczyny występowania błędów, nawet bez konieczności fizycznego dotykania rutera. Koszty rozbudowanych możliwości diagnozowania rutera mogą się dość szybko zwrócić, ponieważ dzięki tym możliwościom znacznie zmniejszy się liczba Twoich wycieczek do rutera i z powrotem. Idąc naprawić ruter, od razu będziesz wiedział, jakie komponenty masz zabrać ze sobą.

Na przykład w jednym z naszych ruterów uległ uszkodzeniu interfejs FDDI. Taki rodzaj uszkodzenia zdarza się dość rzadko i ruter nie mógł dostarczyć nam zbyt dużo informacji na jego temat. Najgorsze jednak było to, że przestał funkcjonować cały pierścień FDDI. Sprawdzając informacje nadsyłane przez uszkodzony ruter i inne rutery, które z nim sąsiadowały, byliśmy w stanie wyizolować uszkodzenie i stwierdzić, że musiało ono wystąpić w konkretnym połączeniu fizycznym pomiędzy dwoma sąsiednimi ruterami. W końcu, posługując się kilkoma kablami, stwierdziliśmy, który z ruterów jest uszkodzony. Gdyby nasze rutery nie obsługiwały funkcji diagnostycznych na niskim poziomie, to naprawa takiego uszkodzenia polegałaby na kolejnym sprawdzaniu poszczególnych połączeń pomiędzy ruterami w pierścieniu.

Jeśli w ruterze występują przerwy lub błędy w pracy, których przyczyną jest oprogramowanie, musisz mieć jakiś sposób pozwalający na łatwe i szybkie uaktualnienie oprogramowania wersją, w której błąd został naprawiony. W niektórych przypadkach oprogramowanie może być uaktualniane bez przerywania pracy rutera; jest kopiowane do rutera przez sieć, po czym następuje ponowne uruchomienie rutera z nowym oprogramowaniem. W czasie tej rekonfiguracji ruter może nadal przełączać pakiet, przerywając usługi tylko na krótką chwilę, kiedy następuje ponowne załadowanie oprogramowania. Przykład takiego uaktualnienia oprogramowania w ruterze Cisco opiszę w rozdziale 8, zatytułowanym „Techniczna strona zarządzania siecią". Zdarzają się także sytuacje, kiedy uaktualnienie oprogramowania może wymagać również wymiany kości ROM na jednej lub kilku płytach rutera. Uaktualnienia tego typu są zwykle bardzo czasochłonne i wymagają opracowania odpowiednich procedur i użycia właściwych narzędzi. Staraj się ich unikać!

Poza kwestią naprawy uszkodzeń powinieneś przemyśleć dwa dodatkowe kryteria obsługowości rutera:

- wymagania dotyczące otoczenia;
- wymagania dotyczące zamocowania. ,

Jeśli nie masz doświadczenia z dużymi komputerami, możesz się zdziwić, że rutery wymagają dokładnie określonych i stałych warunków otoczenia. Podczas gdy mały komputer osobisty może spokojnie pracować w biurze, a nawet w domu, duże komputery wymagają pomieszczeń z dokładnie regulowaną temperaturą (np. pomieszczeń klimatyzowanych), wilgotnością, a nawet odpowiedniego zasilania. Często warunki panujące w biurze odpowiednie dla komputera osobistego mogą być nieodpowiednie dla większej maszyny. Duży ruter może mieć wymagania podobne do tych, które mają wielkie maszyny obliczeniowe pracujące w centrach przetwarzania danych. W końcu ruter to dość duży i mocny komputer. Powinieneś więc brać pod uwagę te wymagania, kiedy planujesz miejsca rozmieszczenia ruterów w Twojej sieci i rodzaj stosowanych urządzeń. Jeśli nie masz innego wyjścia i musisz umieścić ruter w pomieszczeniu o gorszych warunkach, takim jak zaplecze lub pomieszczenie kablowe, to staraj się nie wybierać rutera, który do poprawnej pracy wymaga lepszych warunków otoczenia. Pamiętaj, że pomieszczenie kablowe ma zwykle znacznie gorszy system wentylacji niż biuro i znajduje się w nim zwykle wiele urządzeń wytwarzających ciepło, takich jak koncentratory, przełączniki i rutery. Jeśli jednak musisz użyć takich pomieszczeń, to staraj się dobrze obliczyć, jaka temperatura będzie panowała w kablowni po zamontowaniu tam wszystkich planowanych urządzeń.

Zanim zamówisz urządzenia, powinieneś również dokładnie określić wymagania odnośnie sposobu zamocowania tych urządzeń. Powinieneś zastanowić się, czy ruter może (lub powinien) być zamocowany w stelażu, czy też można go postawić na stoliku lub półce. Ile wolnego miejsca należy zachować dookoła rutera? Czy urządzenie może być zamocowane bezpośrednio do ściany, jeśli zajdzie taka potrzeba? Czy będzie się mieściło w stelażu, którego obecnie używasz? Ile waży to urządzenie?

Choć sprawy te nie mają większego wpływu na inne kryteria, warto się zabezpieczyć przed sytuacją, w której przy próbie montażu urządzenia odkryjesz, że nie masz go do czego przykręcić albo że pieniądze, które zaoszczędziłeś wybierając właśnie ten typ rutera, musisz teraz wydać na wentylację pomieszczenia lub zasilanie wymagane przez to urządzenie.

Wsparcie od sprzedawcy

Oprócz stopnia łatwości wykonywania czynności obsługowych ruterów w razie awarii powinieneś uważnie sprawdzić, jak łatwo możesz otrzymać wsparcie od danego sprzedawcy i jaki będzie poziom techniczny tego wsparcia. Chodzi tu zarówno o wsparcie w przypadku usterki, jak i podczas normalnej eksploatacji urządzeń. Wsparcie takie może mieć różne formy.

A oto kilka pytań, które należy zadać:

- Czy firma, niezależnie od pomocy przy rozwiązywaniu konkretnych problemów, prowadzi punkt wsparcia, w którym możesz uzyskać odpowiedzi na rutynowe pytanie?
- Jaki szkolenia firma oferuje?
- Jakie wsparcie oferowane jest podczas instalacji sprzętu?
- Czy sprzęt jest w całości obsługiwany przez sprzedawcę, przez właściciela czy przez kogoś innego?
- Czy uaktualnienia oprogramowania będą dostępne, jak często i w jakiej formie?

Punkt wsparcia

Punkt wsparcia może odgrywać zasadniczą rolę, gdy Twoja sieć jest uszkodzona. Niezależnie od tego, jak dobrze udokumentowane jest oprogramowanie Twojego rutera, kiedy występuje uszkodzenie, możesz nie mieć czasu na przekopywanie się przez kilka tysięcy stron dokumentacji. Często ktoś w punkcie wsparcia może znacznie szybciej znaleźć odpowiedź lub przełączyć Cię do działu inżynierskiego, który pomoże zidentyfikować problem i doradzi, jak go rozwiązać. Ponieważ taki punkt może obsługiwać nawet tysiące klientów, którzy często mają podobne problemy do Twoich, to - znając problem na podstawie wcześniejszych przypadków - mogą oni znacznie szybciej zaproponować właściwe rozwiązanie.

Punkt wsparcia jest również dobrym kanałem przekazywania informacji producenta o wykrytych błędach w oprogramowaniu. Program rutera jest szczególnie skomplikowany i na pewno zawiera wiele błędów, poczynając od takich, które powodują pewne niedogodności, do takich, które powodują poważne problemy. Niezależnie od tego, jak długo ruter jest testowany, nie można u producenta stworzyć wszystkich możliwych konfiguracji sieci, w jakich będzie używany. Z tego powody producenci ruterów są uzależnieni od użytkowników, którzy znajdują i zgłaszają błędy w pracy urządzenia.

Kiedy zgłaszasz błąd, o ile to możliwe, nie zmieniaj stanu rutera. Jeśli zetknąłeś się z błędem, który powoduje tylko drobne utrudnienie w pracy, a nie awarię całej sieci, pozostaw ruter w takiej konfiguracji, w niezmienionym stanie, aż do skontaktowania się z personelem technicznym producenta lub sprzedawcy. Bardzo często poproszą Cię oni o przekazanie im wyników działania niektórych poleceń diagnostycznych. Dzięki takim danym mogą dokładnie zbadać problem i wskazać rozwiązanie, które zlikwiduje błąd. Z drugiej strony, jeśli Twoja sieć została poważnie uszkodzona w wyniku błędu rutera, powinieneś zrobić wszystko, co tylko możliwe, aby przywrócić pracę sieci, nawet jeśli oznacza to ponowne uruchomienie rutera (i zmianę stanu, w jakim się znalazł). Postaraj się, jeśli to możliwe, zachować maksymalnie dużo informacji o błędzie, który wystąpił.

W dalszej części książki, kiedy będziemy mówić o diagnozowaniu problemów występujących w pracy sieci, omówimy również rodzaje informacji, o których dostarczenie prosi producent przy zgłaszaniu błędu. Zwykle zebranie tych informacji zajmuje kilka minut. Nawet jeśli uszkodzenie spowodowało katastrofę, to warto poświęcić trochę czasu na zebranie informacji, których producent na pewno będzie potrzebował.

Jeśli nie pomożesz producentowi w naprawieniu usterki, to ona na pewno powróci i może się to stać, gdy na przykład będziesz zasiadał do miłej kolacji.

Powinieneś również sprawdzić, czy punkt wsparcia zajmuje się tylko rozwiązywaniem problemów zgłaszanych przez użytkowników, czy też zbiera informacje o nowych funkcjach, jakie chcieliby w kolejnych wersjach widzieć użytkownicy, a także czy zajmuje się wyjaśnianiem niejasności zawartych w dokumentacji produktu. Dobrze zorganizowany punkt wsparcia powinien chętnie odpowiadać na tego typu pytania po to, by w przyszłości uniknąć problemów.

Szkolenia

Niezależnie od tego, ile wiesz o administrowaniu siecią i ile czasu spędzisz na czytaniu dokumentacji produktu, powinieneś dowiedzieć się, jakie szkolenia oferuje dostawca sprzętu. Dokumentacja nie jest doskonała; nie można kawałkowi papieru *zadać* pytania, na które w dokumentacji nie ma odpowiedzi. Z dokumentacji nie dowiesz się również o subtelnych różnicach pomiędzy funkcjami rutera a potrzebami Twojej sieci. Aby znaleźć odpowiedź na tego typu pytania, powinieneś mieć możliwość kontaktu z osobą, która się na tym zna, a punkt wsparcia może tu niewiele pomóc. Powiedzieliśmy wcześniej, że ruter IP to szczególnie skomplikowany sprzęt i oprogramowanie. Kto zna się na tym sprzęcie lepiej niż ludzie, którzy go stworzyli? Dobrze opracowane szkolenie może zaoszczędzić Ci czasu i wysiłku i może pomóc w uchronieniu sieci przed kosztownymi uszkodzeniami. Mówiąc krótko, szkolenia to dobrze wydane pieniądze.

Jeśli producent sprzętu, który zakupiłeś, nie prowadzi szkoleń, to sprawdź, czy tego typu usługi wykonywane są przez firmy trzecie lub specjalizowane centra szkoleniowe. Być może producent Twojego sprzętu stwierdził, że bardziej opłacalne jest wyszkolenie kilku profesjonalnych instruktorów i kierowanie klientów do miejsc, gdzie oni pracują, niż utrzymywanie własnego personelu szkoleniowego. Jeśli producent popiera jakąś grupę szkoleniową, to powinieneś uważać ją za odpowiednik szkoleń prowadzonych bezpośrednio przez producenta.

Wsparcie przy instalowaniu urządzeń

W zależności od umiejętności Twojego personelu możesz stwierdzić, że pomoc producenta lub sprzedawcy sprzętu przy instalacji, przynajmniej pierwszego urządzenia, jest wskazana. Jeśli firma, z której usług korzystasz, ma dobre wsparcie instalatorskie, to będzie w stanie pomóc Ci uchronić się przed wieloma pułapkami, w jakie wpadają nowi klienci podczas samodzielnego instalowania sprzętu. Ponieważ pracownicy dostawcy są dobrze obeznani ze sprzętem, który ich firma oferuje, pomogą Ci w uruchomieniu sieci w oparciu o te urządzenia lub powiększeniu sieci już istniejącej. Jeśli do już istniejącej sieci dodajesz sprzęt nowego producenta, to takie wsparcie staje się jeszcze ważniejsze. Będziesz mógł się wtedy skupić na obsłudze istniejącej sieci i przygotowaniu jej na rozszerzenie. Pomoże Ci to również w ustaleniu, po stronie którego sprzętu leży przyczyna błędów. Przekonasz się, że nie wszystko idzie tak dobrze, jak zaplanowałeś.

Choć wielu producentów oferuje pewien poziom wsparcia instalatorskiego, to nie zawsze jest ono oferowane za darmo. Jeśli firma pobiera opłaty za instalowanie urządzeń, to powinieneś uwzględnić ten fakt w ogólnej ocenie kosztów urządzenia, sprawdzając, co dostawca oferuje w cenie urządzenia, a za co płacisz dodatkowo. Kiedy już zapoznasz się z urządzeniami, przekonasz się, że możesz je pewnie i bez obaw konfigurować, modernizować lub restartować, wykonując to nawet z domu, siedząc wygodnie i popijając kawę. Zanim jednak to nastąpi, poproś o pomoc.

Kto obsługuje urządzenia?

Pytanie to jest znacznie ważniejsze, niż się wielu administratorom wydaje. Przekonują się o tym wtedy, kiedy siedzą przed martwym ruterem starając się uruchomić sieć, a ich szef stoi za plecami i patrzy im na ręce. Kontrakty podpisywane z dostawcą rutera mogą zawierać zapisy o całkowitej obsłudze prowadzonej przez dostawcę aż po całkowitą obsługę wykonywaną przez kupującego. Poziom wsparcia, jakiego potrzebujesz, zależy od liczby personelu, jaki posiadasz, i od tego, jak łatwy w obsłudze jest kupowany sprzęt.

Wszystkie prace mogą być wykonywane przez dostawcę sprzętu, włączając w to konfigurację ruterów i dokonywanie wszystkich, nawet najdrobniejszych zmian w sieci. Jest to niewątpliwie drogie i choć zwykle zmiany wykonane zostaną natychmiast po zgłoszeniu, to musisz się liczyć z tym, że niektóre rekonfiguracje wykonywane będą z opóźnieniem. Jeśli Ty i Twoi ludzie nie macie zbyt wiele doświadczenia w obsłudze wybranych urządzeń, powinieneś wybrać rozwiązanie polegające na obsłudze sprzętu przez dostawcę. Za dodatkową opłatą możesz również wynegocjować wyższy poziom obsługi, nawet jeśli standardowy kontrakt przedstawiany przez dostawcę zakłada, że sprzęt obsługiwany będzie przez kupującego.

Zupełnie innym przypadkiem będzie sytuacja, w której sprzedawca nie robi nic poza wymianą uszkodzonego sprzętu i dostarczaniem łat do oprogramowania. Wtedy Twój personel musi mieć dodatkowe umiejętności związane z obsługą sprzętu, który zamierzasz kupić. Jeśli uszkodzeniu ulegnie na przykład jakiś komponent rutera, to najpierw ktoś musi określić, co się zepsuło. Czasami wcale nie jest łatwo z całą pewnością stwierdzić, która część tak skomplikowanego urządzenia uległa uszkodzeniu. Czy chodzi o oprogramowanie, czy też o sprzęt? Jeśli to sprzęt, to który moduł? Kiedy już zidentyfikujesz komponent, który uległ uszkodzeniu, musisz zamówić część na wymianę. Kiedy zostanie ona dostarczona, ktoś musi wyjąć i wymienić uszkodzony moduł. Niewątpliwie wykonywanie obsługi własnymi siłami ma wiele zalet, ale do tego celu konieczne jest posiadanie wyszkolonego personelu. Obsługa prowadzona przez dostawcę może być wykonywana tylko w jasno określonych godzinach i dniach, które nie zawsze będą Ci odpowiadały. Czasem dostawca nie zechce podpisać umowy, która zobowiąże go do obsługi urządzeń po godzinach pracy Twojej firmy. Obsługę prowadzoną własnymi siłami możesz zaplanować tak, jak Ci jest najwygodniej, z uwzględnieniem godzin pracy użytkowników.

Uaktualnienia oprogramowania

Ważne jest, abyś zapytał dostawcę o sposób, w jaki dokonywane jest uaktualnianie oprogramowania rutera. Jeśli podpisałeś kontrakt na obsługę, to część uaktualnień oprogramowania (może nawet wszystkie) może być objęta tym kontraktem. Uaktualnienia oprogramowania rozszerzające funkcje urządzenia mogą wymagać dodatkowych opłat, podczas gdy uaktualnienia poprawiające zauważone błędy są zwykle za darmo. W każdym przypadku powinieneś dowiedzieć się, jakie jest podejście dostawcy do sprawy uaktualnień, zanim zdecydujesz się na zakup danego urządzenia. W przeciwnym razie może się okazać, że dodanie do rutera funkcji, której potrzebujesz, będzie Cię kosztowało więcej, niż zaoszczędziłeś wybierając dane urządzenie.

Oprócz określenia, jakich uaktualnień oprogramowania możesz się spodziewać i ile one będą kosztowały, dobrze jest zapytać dostawcę, jak często pojawiają się uaktualnienia oprogramowania zawierającego nowe funkcje. Wszyscy producenci dodają nowe funkcje do swojego oprogramowania. Wynika to z faktu, że standardy IP cały czas ewoluują. Standardy te ulegają zmianom, w miarę jak definiowane są nowe funkcje lub okazuje się, że stosowane dotychczas funkcje mają braki, które uniemożliwiają dalsze ich stosowanie. Najlepiej byłoby, gdyby producent rutera mógł dostarczać Ci nowe funkcje z chwilą, kiedy będziesz ich potrzebował.

Warto poświęcić trochę czasu i starań, by sprawdzić w jakim stopniu firmy oferujące Ci rutery nadążają za pojawiającymi się standardami sieci Internet. Niestety, niektórzy producenci ruterów wydają się zupełnie nie rozumieć, czym naprawdę jest sieć Internet. Dokumenty RFC są ciągle zmieniającą się tablicą powiązanych ze sobą standardów, proponowanych nowych standardów i pomysłów, które są czasem nie do końca przemyślane. Choć producent rutera mógł swego czasu zaimplementować obsługę standardu w swoim produkcie, to jeśli nie śledzi na bieżąco rozwoju wydarzeń, można zakładać, że rutery te obsługują standardy, które już wychodzą z użycia. Najlepszym sposobem utrzymywania się na bieżąco w tematach związanych ze standardami jest aktywne uczestnictwo w ich kreowaniu. Sprawdź, czy producent rutera, który zamierzasz kupić, ma swoich przedstawicieli w którejś z grup roboczych *Internet Engineering Task Force (IETF)*. A jeszcze lepiej będzie, jeśli okaże się, że przewodniczą oni jakimś grupom roboczym. Wspomniane grupy robocze opracowują kierunki zmian protokołów wchodzących w skład zestawu protokołów IP i oczywiste jest, że ci, którzy uczestniczą w opracowywaniu standardów, znacznie lepiej rozumieją, jak należy je implementować w urządzeniach i oprogramowaniu.

Jeśli producent rutera często wypuszcza uaktualnienia, w których pojawiają się nowe, mało użyteczne funkcje, może się okazać, że nieświadomie płacisz za te funkcje. W rezultacie ruter może być bardziej podatny na błędy w pracy oprogramowania. Płacisz także więcej za urządzenie i kolejne uaktualnienia oprogramowania. Spróbuj znaleźć takiego producenta, u którego występuje właściwa zależność pomiędzy częstością dodawania uaktualnień a jakością funkcji, które są w nich dodowane.

Kolejnym pytaniem, które należy zadać, jest to, jak szybko producent udostępnia łaty na znalezione w oprogramowaniu błędy, które wpływają na pracę Twojej sieci. Współpracuję obecnie z dwoma różnymi producentami ruterów. Jeden z nich naprawia błędy po upływie 18 do 24 miesięcy po ich zgłoszeniu, a czasem wcale ich nie naprawia.

Drugi producent naprawia błędy często w ciągu krótszego czasu niż jeden tydzień i czasami wypuszcza kompletne oprogramowanie zawierające poprawki i dające się w łatwy sposób uruchomić na ruterze. Nie muszę chyba dodawać, że pierwszy z producentów nie znajdzie się już nigdy na mojej liście potencjalnych dostawców kolejnych ruterów. Kiedy otrzymasz odpowiedź na takie pytanie, postaraj się ją rozsądnie ocenić. Może ona zależeć od znaczenia błędu. Oczywiste jest, że błąd, który ma duży wpływ na pracę sieci, powinien zostać naprawiony w ciągu kilku dni, a nawet szybciej. Z drugiej strony małe niedogodności lub błędy, które ciężko znaleźć, mogą być naprawiane po miesiącu, a nawet dłuższym okresie testowania oprogramowania.

Na koniec powinieneś zapytać dostawcę, jak długo zamierza obsługiwać starsze wersje oprogramowania. Żaden producent nie będzie w nieskończoność wspierał starszych wersji oprogramowania, ale nie powinieneś dopuścić do tego, aby zmuszał Cię do zmiany oprogramowania na nowsze tylko dlatego, że wersja ta zawiera poprawki usuwające zgłoszone przez Ciebie błędy. Musisz pamiętać, że nowa wersja oznacza również nowe błędy, które będzie trzeba wykryć i usunąć.

Możliwości modyfikacji sprzętu

Kiedy kupujesz nowy sprzęt, to jedną z ostatnich rzeczy, o jakiej będziesz myślał, jest wymiana tego sprzętu na nowszy. Ale każdy sprzęt prędzej czy później będzie musiał być wymieniony, ponieważ przestanie spełniać swoją funkcję i konieczne będzie zastąpienie go czymś szybszym i mocniejszym. Kiedy nastąpi taki moment, to ważne stanie się pytanie, ile z zakupionego wcześniej sprzętu możesz sprzedać na rynku wtórnym lub zwrócić producentowi i za dopłatą uzyskać nowy sprzęt. Dobry producent wie, że kiedy będziesz zadowolony z jego usług, będziesz z nich korzystał często. Dlatego może zaproponować Ci całkiem niezłe warunki wymiany starszego sprzętu na nowszy za dopłatą. Jeden z producentów ruterów chciał nawet wziąć ode mnie stary sprzęt innego producenta w rozliczeniu za nowe rutery.

Z wymianą sprzętu na nowy wiąże się również sprawa systemu modyfikacji sprzętu proponowanego przez producenta. Modyfikacje te powinny umożliwić Ci ciągłe wykorzystywanie sprzętu poprzez dopasowywanie go do bieżących wymagań Twojej sieci. Zakupiliśmy np. kilka dużych przełączników LAN od dostawcy, który miał stosunkowo nową linię produktów (oprogramowanie było w wersji 1.1). W ciągu roku producent stwierdził, że zbyt skromnie określił wymagania sprzętu odnośnie pamięci i ogłosił, że nowa wersja oprogramowania nie będzie mogła pracować na urządzeniach bez rozszerzenia ich pamięci RAM. Zamiast kazać swoim lojalnym klientom płacić za błąd inżynierów, którzy projektowali ten sprzęt, producent zaproponował bezpłatne rozszerzenie pamięci operacyjnej w urządzeniach. Nie muszę mówić, ile punktów zdobył sobie u mojego szefostwa!

Nie chcę przez to powiedzieć, że wszyscy producenci powinni oferować darmowe modyfikacje sprzętu. Gdyby tak robili, to na pewno wypadliby z gry. Producent, który będzie rzeczywiście chciał zatrzymać klienta, znajdzie sposoby na wspieranie inwestycji w drogi sprzęt. Może to robić poprzez udzielanie kredytów na zakup nowego sprzętu, darmowe modyfikacje sprzętu, które będą naprawiały błędy, lub poprzez takie opracowania nowego sprzętu, które pozwalają wykorzystać część elementów starszego sprzętu, np. moduły interfejsów.

Niezależnie od tego, jakie to będzie rozwiązanie, taki rodzaj ochrony inwestycji może być wart mnóstwo pieniędzy i powinieneś go uwzględnić przy ocenie poszczególnych dostawców.

Należy pamiętać, że producent powinien jasno określić swoje plany dotyczące nowych modeli lub opcji sprzętowych oraz wsparcia dla sprzętu, który przestanie być produkowany. Oczywiste jest, że nie będziesz mógł spodziewać się pełnej obsługi starszego sprzętu. Jakość pomocy, jaką będziesz otrzymywał, będzie się pogarszała wraz z wiekiem urządzeń, ale nie ma nic gorszego niż kupowanie najnowszych ruterów, by po sześciu miesiącach przekonać się, że producent wycofuje to urządzenie z produkcji i nie zapewnia mu żadnej obsługi. Inni klienci mogą być dobrym źródłem informacji o tym, jakie w przeszłości było podejście producenta do obsługi i wspierania wychodzącego z produkcji sprzętu.

Osiągi

W każdej sieci ruter łatwo może stać się wąskim gardłem. Sieci IP i rutery IP mają wiele cech wspólnych. Przeglądanie datagramów IP w poszukiwaniu adresu przeznaczenia, wyszukiwanie adresu przeznaczenia w tablicy rutowania i przesyłanie datagramu do innego segmentu sieci nie jest oczywiście wykonywane natychmiast. Działanie, które tradycyjnie nazywane jest *rutowaniem,* składa się tak naprawdę z kilku oddzielnych akcji. Mówiąc ogólnie, cały proces można podzielić na *przełączanie* datagramów z jednego segmentu sieci do drugiego oraz *dodatkową pracę* związaną z utrzymywaniem tablic rutowania, buforów pamięci itd. Ponieważ przełączanie datagramów IP jest działaniem najbardziej skoncentrowanym na obsłudze użytkowników sieci, to dobrze zaprojektowany ruter powinien minimalizować opóźnienia w pracy wynikające z obsługi wszelkich dodatkowych działań. O ile to możliwe, wszystkie działania dodatkowe powinny być wykonywane przez dodatkowy procesor.

Niezależnie od tego, jak dobrze ruter obsługuje dodatkowe działania, zawsze będą miały one wpływ na szybkość, z jaką ruter przełącza pakiety. Częściowo wynika to z konieczności uaktualnienia tablic rutowania, których proces przełączania używa przy podejmowaniu decyzji. Kiedy jakiś zapis w tablicy rutowania jest uaktualniany, to nie jest dostępny dla procesu przełączania. Wpływ na szybkość wykonywania podstawowego zadania rutera mają także wszystkie inne działania podejmowane przez niego. Do działań tych należą na przykład: obsługa dynamicznego protokołu rutowania, obsługa czasu sieciowego, a także odpowiadanie na zapytania systemu zarządzania siecią.

Ponieważ jest kilka działań podejmowanych przez ruter, które mają wpływ na jego osiągi, a każdy producent implementuje inną architekturę zarówno w sprzęcie, jak i w oprogramowaniu swoich ruterów, nie jest możliwe porównanie dwóch ruterów poprzez porównanie wpływu dodatkowych działań na pracę rutera. Producenci zwykle podają tylko osiągi w postaci liczb określających szybkość wykonania porównywalnych na różnych ruterach działań. Wielkości te są zwykle podawane na bazie dwóch podstawowych danych charakterystycznych dla rutera. Pierwszą z nich jest *przepustowość* rutera, a drugą - *opóźnienie.*

Przepustowość

Pierwszą ważną informacją charakteryzującą osiągi rutera jest jego przepustowość. Wartość ta określa ilość danych, jaką ruter może przesłać w określonej jednostce czasu. Najczęściej przepustowość jest mierzona i podawana w *pakietach na sekund? (pps).* W warunkach idealnych ruter, który ma przepustowość 1000 pps, byłby niewątpliwie szybszy, od rutera który ma przepustowość 900 pps. Niestety wartości określające przepustowość, podawane w oderwaniu od innych parametrów, nie są użyteczne, a nawet trudno je porównać.

Aby zrozumieć dlaczego przepustowość może być nieporównywalna, rozważmy wpływ różnej wielkości pakietu na osiągi rutera. Minimalna wielkość ramki w sieci Ethernet to 64 oktety. Maksymalny rozmiar ramki w tej technologii wynosi 1518 oktetów. Oczywiste jest, że przesłanie większej ramki będzie zajmowało więcej czasu niż przesłanie mniejszej ramki. Jeśli dłużej trwa przesłanie długiej ramki, to w przedziale czasu, w którym dokonujemy pomiaru, ruter widzi kilka pakietów i ma więcej czasu na powrót do normalnego stanu przed nadejściem kolejnej ramki. Dlatego większość sprzedawców testuje swój sprzęt przy przesyłaniu najmniejszych możliwych ramek, aby uzyskać *wyższy* wskaźnik przepustowości. Tak więc pierwszym pytaniem, jakie należy zadać, kiedy przegląda się wyniki testów określające przepustowość, jest: „Jaka była wielkość ramek testowych?".

Nawet jeśli dwóch producentów ruterów użyło tego samego rozmiaru ramki, wynik pomiaru może być w dużym stopniu zmieniony przez inne czynniki. Rozważmy przykład różnych sposobów testowania rutera wyposażonego w cztery interfejsy Ethernet. Przepustowość tego rutera będzie się w ogromnym stopniu zmieniała w zależności od kierunku przepływu ruchu. Na przykład jeśli dwa interfejsy będą pracowały jako wejścia informacji, a pozostałe dwa jako wyjścia, to zmierzona przepustowość rutera będzie zależała od tego, czy jeden interfejs wejściowy przesyła pakiety do jednego interfejsu wyjściowego i czy podobnie jest w przypadku drugiej pary interfejsów, czy też oba interfejsy wejściowe będą losowo wysyłały pakiety do obu interfejsów wyjściowych.

Musisz więc wiedzieć dokładnie, jakie działania wykonywał ruter w trakcie testów. Producenci chętnie porównują wyniki uzyskane przez ich sprzęt w momencie, kiedy rutery nie robiły nic innego. Starają się, aby liczby były możliwie największe, nawet jeśli są one nierealne. Na przykład jeden z producentów ruterów podaje imponującą wielkość przepustowości jednego ze swoich potężniejszych ruterów, która wynosi 250000 pps. Jeśli jednak do funkcji rutera doda się coś tak prostego jak filtrowanie pakietów, to osiągi tego rutera spadają z poziomu 250000 pps do 28000 pps. Jeśli dodasz do tego fragmentację IP, wynik spada do 2000 pps!

Jakie są więc rozsądne wartości określające przepustowość? Odpowiedź zależy w dużym stopniu od liczby i typu interfejsów znajdujących się w ruterze oraz od rodzaju ruchu w Twojej sieci.

Po dokonaniu niewielkich obliczeń możesz uzyskać liczby, które potwierdzą, że wybrany przez Ciebie ruter jest odpowiedni dla Twojej sieci; pierwszym czynnikiem jaki należy przeanalizować, jest liczba mediów jakie będą obsługiwane przez ruter. Ponieważ prędkości osiągane w poszczególnych mediach się różnią, podobnie jak rozmiar ramek przesyłanych w tych mediach, to liczba ramek docierających do rutera będzie się również zmieniała w zależności od obsługiwanego medium. Aby określić liczbę pakietów na sekundę, które będą docierały do rutera w danym medium, musisz wziąć pod uwagę czas potrzebny na odebranie najmniejszej możliwej ramki oraz czas pomiędzy kolejnymi ramkami przesyłanymi w medium. Teoretyczne wartości maksymalnej liczby pakietów na sekundę dla czterech typowych mediów podano w tabeli 4-1.

Tabela 4-1. Teoretyczne wartości maksymalnej liczby pakietów na sekundę w powszechnych

Medium	*Pasmo*	*Minimalny rozmiar pakietu*	*Maksymalna wartość PPS*
Ethernet	10 Mbps	64 oktety	14880
Token Ring	10 Mbps	64 oktety	24691
FDDI	100 Mbps	64 oktety	152439
T1	1,544 Mbps	64 oktety	3300

Wartości te to teoretyczne maksimum, a nie rzeczywiste liczby pakietów przesyłanych w pracującej sieci. Przy określaniu tych wartości zakłada się, że każdy pakiet w sieci skierowany jest do rutera, że nie ma żadnego ruchu wychodzącego z rutera do segmentu sieci (na przykład z innego segmentu sieci) oraz że wszystkie pakiety mają minimalny rozmiar. Analizy rzeczywistego ruchu w sieci wykażą zupełnie inne wartości określające obciążenie typowych mediów dołączanych do rutera. Jedna z takich analiz, zaprezentowana przez Billa Kelly'ego z Cisco Systems* wykazała, że w typowej, średnio obciążonej sieci Ethernet (30 procent pasma) rzeczywiste obciążenie rutera wynosi około 300 pps. Choć analiza ta nie określiła obciążenia dla innych mediów, to można założyć, że wartości te byłyby proporcjonalne do pasma tych mediów. Jeśli tak jest w rzeczywistości, to w typowej sieci FDDI przy wykorzystaniu 30 procent pasma i podobnej charakterystyce ruchu jak w prezentowanej sieci Ethernet obciążenie rutera wyniosłoby około 3000 pps. Takie obciążenie nie jest zbyt duże dla pierścienia FDDI, więc możemy zakładać, że występuje często. Większe wykorzystanie pasma, na przykład 60 procent, prawdopodobnie podwoi liczbę pakietów do około 6000 pps.

*Bili Kelly jest dyrektorem działu Enterprise Technical Marketing w Cisco Systems. Wspomniana analiza prezentowana była jako część prezentacji zatytułowanej „Cisco Router and Switch Performance Charac-teristics" na konferencji Cisco Networkers'95 w Stanford, w Kalifornii.

Kryteria doboru ruterów

Rozważmy przykład rutera mającego dwa interfejsy FDDI i 18 interfejsów Ethernet. Teoretycznie maksymalna liczba pakietów, z jaką może pracować, to suma pakietów na wszystkich interfejsach podzielona przez dwa (pakiety muszą przecież skądś wychodzić). Wartość ta wynika ze wzoru

$$\frac{18 \text{ x } 14880 + 2 \text{ x } 152439}{2} = 286359 \text{ pps}$$

i przekracza przepustowości większości ruterów dostępnych na rynku. Jest to jednak teoretyczne maksimum, zakładające, że pakiety o minimalnej długości przesyłane są zawsze pomiędzy segmentami sieci, co nie zdarza się w rzeczywistej sieci. Jeśli założymy, że ruch jest bardziej typowy i przyjmiemy wartości z analizy przedstawionej przez Billa Kelly'ego, to otrzymamy znacznie bardziej realistycze wartości:

$$18x300 + 2x3000/2 = 5700\,pps$$

Czy powinniśmy więc ignorować przepustowość rutera? Oczywiście, że nie! Choć prawdą jest, że średnie obciążenie rutera, który omawiamy w naszym przykładzie, będzie bardziej zbliżone do wartości 5700 pps, a nie do 286359, to charakterystyka pracy rzeczywistej sieci może być taka, że obciążenie rutera w krótkich okresach będzie się zbliżało do teoretycznego maksimum. Widać więc, że ruter powinien być w stanie obsłużyć takie chwilowe obciążenie. Powyższa analiza wykazuje, że podczas wyboru rutera powinieneś pamiętać o danych określających jego przepustowość. Jeśli ruter obsługujący osiem interfejsów Ethernet ma przepustowość 100000 pps, to wcale nie znaczy, że jest lepszy od rutera *o* przepustowości 75000 pps. Oba rutery z dużym zapasem przekraczają obciążenie, jakie są w stanie wygenerować sieci dołączone do ośmiu interfejsów Ethernet.

Opóźnienie

Kolejnym ważnym aspektem osiągów ruterów jest ich opóźnienie, nazywane również zwłoką. Większość producentów sprzętu podaje statystyki dotyczące opóźnienia, których dokładne przejrzenie powinno być jedną z części procesu wyboru rutera. Opóźnienie to po prostu czas, jaki pakiet spędza wewnątrz rutera. Niezależnie od tego, ile pakietów na sekundę ruter może teoretycznie przełączać, jeśli obsługa każdego pakietu zajmuje długi czas, to użytkownicy sieci będą widzieli, że sieć jest Wolna. Badania wykazały, że czas, jaki upływa od naciśnięcia klawisza przez użytkownika do potwierdzenia wpisanego znaku przez echo, powinien być krótszy niż pół sekundy. Jeśli czas ten będzie dłuższy, to użytkownik będzie odczuwał opóźnienie pracy sieci. Ponieważ większość sesji Telnet konfigurowana jest tak, że odległy host wysyła echo wpisywanych przez użytkownika znaków, to opóźnienie generowane przez ruter powinno być tak małe, aby użytkownik go nie zauważył.

Podobnie jak to miało miejsce w przypadku przepustowości, sposób pomiaru opóźnienia rutera ma wpływ na uzyskane wyniki. Na przykład zasadniczą sprawą jest określenie, od którego momentu zaczynamy mierzyć czas i kiedy kończymy. Można uzyskać bardzo małe opóźnienia, jeśli pomiar rozpocznie się w momencie, kiedy odebrany zostanie ostatni oktet pakietu i zakończy, gdy wysyłany jest z rutera pierwszy oktet. Najlepiej przeprowadzać pomiar w ten sposób, że zegar rozpoczyna go, kiedy odbierany jest pierwszy oktet i kończy, kiedy w sieć wysłany zostanie ostatni oktet pakietu. Podobnie jak poprzednio, rozmiar pakietu może mieć wpływ na mierzone czasy opóźnienia. Jeśli ruter musi kopiować dane do swojej pamięci, znajdujące się w pakiecie, to oczywiste jest, że dłużej będzie trwało kopiowanie pakietów długich niż krótkich.

Jeśli wiesz, w jaki sposób dokonywano pomiaru (kiedy uruchamiany był zegar i kiedy go zatrzymywano) oraz jak duże były pakiety, możesz dokonać konwersji dwóch wartości uzyskanych w różnie przeprowadzonych pomiarach, tak aby mogły być one porównywalne. Sposób dokonania pomiarów, jakim będziemy się posługiwali, opisano w tabeli 4-2.

Tabela 4-2. Określanie formatu wyświetlania informacji o maskach

	Ruter1	*Ruter2*
Zmierzone opóźnienie Rozmiar pakietu Czas pomiaru	1 ms 1500 oktetów Od ostatniego oktetu na wejściu do pierwszego oktetu na wyjściu	1,5 ms 1000 oktetów Od pierwszego oktetu na wejściu do pierwszego oktetu na wyjściu

Wartości umieszczone w tabeli 4-2 pokazują, że Ruter1 ma mniejsze opóźnienie. Jednak z pozostałych opisów wynika, że producent wybrał do pomiarów najkorzystniejsze warunki, jeśli chodzi o okres pomiaru. Gdyby rozmiary pakietów były takie same, to moglibyśmy skorygować powstałe różnice poprzez dodanie czasu, jakiego potrzebuje Ruter1 na odebranie pakietu z sieci (zakładamy, że mówimy o sieci Ethernet) lub skorygować wartość opóźnienia urządzenia Ruter2, odejmując czas potrzebny na odebranie pakietu z sieci.

Ponieważ jednak rozmiary pakietów są różne, musimy dokonać korekty obu wyników pomiarów opóźnienia ruterów. W przypadku Rutera1 musimy dodać czas potrzebny na odebranie z sieci pakietu o długości 1500 oktetów. Dla Rutera2 konieczne jest odjęcie od podanej wartości czasu potrzebnego na odebranie z sieci pakietu o długości 1000 oktetów, a następnie dodanie czasu potrzebnego na odebranie 1500 oktetów, podobnie jak zrobiliśmy to w przypadku Rutera1. Wyniki opisanych działań pokazano w tabeli 4-3.

Tabela 4-3. Korygowanie opóźnień zmierzonych dla obu ruterów

Prędkość sieci Ethernet:	10Mbps
Liczba bitów w oktecie:	8
Czas przesłania jednego bita:	1 / 1 0 Mbps = 0,1 ns
Czas przesłania jednego oktetu:	8 x 0,1 ns = 0,8 ns
Czas odebrania 1500 oktetów:	1500 x 0,8 ns = 1,2 ms
Czas odebrania 1000 oktetów:	1000 x 0,8 ns = 0,8 ms
Skorygowane opóźnienie dla Rutera1:	I ms + 1,2 ms = 2,2 ms
S	1,5 ms - 0,8 ms + 1,2 ms = 1,9 ms

Po skorygowaniu opóźnień tak, by mogły być one porównywalne, widzimy, że Ruter2 ma mniejsze opóźnienie niż Ruter1, który wydawał się lepszy. Niestety, korekty, jakich dokonaliśmy nie biorą pod uwagę odchyleń opóźnienia dla Rutera2, wynikających z kopiowania dłuższego pakietu, ponieważ nie mamy informacji o takich wartościach. Jednak dzięki takim korektom dysponujemy przynajmniej wartościami, które pozwalają nam dokładniej porównać opóźnienia obu ruterów.

Opisane wyżej sytuacje powinny przekonać Cię, że liczby określające przepustowość i opóźnienie powinny być analizowane przez ludzi, którzy zjedli beczkę soli w pracy z ruterami. Należy podkreślić konieczność zrozumienia warunków, w jakich dokonywane były pomiary, zanim przejdzie się do porównywania uzyskanych w nich wyników. Trzeba również pamiętać, że warunki pomiarów są zwykle prawie idealne, a prawdopodobieństwo, że uda się je osiągnąć w rzeczywistej sieci jest bardzo małe.

Elastyczność

Niektórzy mogą narzekać, że rutery dedykowane nie mogą być programowane. Jest w tym trochę racji. Możemy jednak założyć, że wszystkie języki programowania to zaawansowane narzędzia pozwalające tak skonfigurować komputer, aby wykonywał on określone zadania. Rozumując w ten sposób, dochodzimy do wniosku, że języki pozwalające konfigurować większość z dostępnych obecnie dedykowanych ruterów IP to tak naprawdę wysoko specjalizowane języki programowania.

Niezależnie od tego, czy będziesz używać określenia „programowalne" czy „konfigurowalne", zawsze chodzi o to, jak duży wpływ masz na zachowanie ruterów. Czasami nie masz prawie żadnej kontroli. Dostępne opcje zawierają niewiele więcej nad możliwość przypisania adresów IP do interfejsów, definiowanie masek podsieci i tworzenie statycznych tras. Z drugiej strony możesz mieć tak duże możliwości kontroli pracy rutera, że zaczniesz naruszać standardy albo sprawisz, że ruter przestanie funkcjonować zupełnie.

Kiedy oceniasz elastyczność proponowanego Ci rutera, zastanów się nad wadami i zaletami obu możliwości. Ruter, który ma kilka opcji konfiguracyjnych, może doskonale nadawać się do obsługi sporej liczby segmentów Twojej sieci. Prawdopodobnie większość opcji, których nie można konfigurować, została odpowiednio określona przez producenta.

Niewątpliwie jednak w Twojej sieci znajduje się kilka nietypowych segmentów, w których konieczna jest dodatkowa elastyczność stosowanego rutera. Prawdopodobnie będziesz potrzebował elastycznego rutera w miejscu, w którym będziesz dołączał nowe segmenty do istniejącej sieci. Zakupiony kiedyś sprzęt, pracujący w starszej sieci, może nie spełniać obecnych standardów, a producent nie zadbał o odpowiednie uaktualnienia. Możliwe, że firma, która wyprodukowała posiadany przez Ciebie sprzęt, przestała już istnieć, co jest jednym z powodów, dla których nowe segmenty sieci chcesz budować opierając się na ruterach innego producenta.

Sprawę pogarsza fakt, że segmenty sieci, w której możesz potrzebować większej elastyczności, nie istnieją w Twoim projekcie sieci. Żaden projekt nie może dokładnie przewidzieć przyszłego rozwoju sieci i dlatego nie możesz być pewien, czy opcje konfiguracyjne, których dziś potrzebujesz, będą tymi, których będziesz potrzebował w przyszłości. Dlatego dobrze jest rozejrzeć się za ruterami, które charakteryzują się elastycznością większą, niż na razie potrzebujesz.

Niestety, elastyczność ma również swoje wady. Zastanów się, jakie są różnice pomiędzy przenośnym radiem a tunerem będącym częścią systemu stereo. Obydwa można dostroić tak, by odbierały określoną stację radiową, i oba mogą mieć potencjometr wzmocnienia, pozwalający dobrać odpowiednią głośność. Ale element wieży stereo będzie miał prawdopodobnie pokrętło tonów niskich i wysokich, balans, a także korektor graficzny. Mogą się tam znajdować dodatkowe przyciski, które pozwolą sterować magnetofonami, zapamiętać ustawienia w zależności od rodzaju muzyki itd. Oczywiste jest, że każdy, kto zetknął się z tego rodzaju sprzętem stereo, nie zdaje sobie sprawy, że taka liczba gałek, przycisków i potencjometrów może być oszałamiająca i niezrozumiała dla przeciętnego człowieka, który chce po prostu posłuchać radia. Taka sama prawidłowość obowiązuje w przypadku ruterów IP. W miarę jak rośnie liczba opcji konfiguracyjnych, rośnie zawiłość wykonania zwykłej konfiguracji i konieczny poziom wyszkolenia osoby, która będzie tę konfigurację rutera wykonywała.

Na szczęście większość ruterów posiadających dużą liczbę opcji konfiguracyjnych posiada również rozsądnie określone wartości domyślne dla wielu z tych opcji. Takie podejście producenta pomaga, ale nie całkiem eliminuje konieczność zrozumienia znaczenia i funkcji tych opcji. Choć bardzo prawdopodobne jest, że większość domyślnych wartości dla opcji będzie właściwie ustawiona dla Twojej sieci, to nie będziesz mógł tego stwierdzić, jeśli nie będziesz wiedział, jakie są funkcje tych opcji.

Jaki jest więc rozsądny poziom elastyczności? *Zależy* on od Twojej sieci, ale minimalne wymagania, jakie powinien spełniać, i opcje, które powinien posiadać elastyczny ruter, są następujące:

- ustawienie adresów IP, masek i adresów broadcast dla każdego z interfejsów;
- możliwość określenia kilku adresów IP na jednym interfejsie;
- włączanie i wyłączanie proxy ARP dla każdego z interfejsów oddzielnie;
- możliwość skonfigurowania rutowania statycznego;

- możliwość skonfigurowania jednego lub więcej dynamicznych protokołów rutowania;
- możliwość wyłączenia uaktualnień dynamicznego protokołu na każdym z interfejsów oddzielnie;
- możliwość wymiany informacji pomiędzy dwoma protokołami rutowania;
- możliwość wybiórczego blokowania pakietów na wyjściu i wejściu każdego z interfejsów;
- możliwość zabronienia dostępu do rutera przez Telnet lub SNMP i zezwolenia na taki dostęp tylko wybranym maszynom w sieci;
- możliwość kontroli niektórych lub wszystkich aspektów działania dynamicznych protokołów rutowania, takich jak czasy, preferencje jednej trasy w stosunku do drugiej, a także określanie stron, z którymi rozmawia dany protokół;
- obsługa źródłowych pakietów IP;
- generowanie różnego typu pakietów ICMP;
- możliwość kontrolowania niektórych parametrów specyficznych dla każdego z interfejsów.

Ostatnie z wymagań jest prawdopodobnie jedną z najrzadziej spotykanych i najniebezpieczniejszych możliwości. Jeśli jednak sądzisz, że potrzebujesz takich możliwości, to na pewno tak jest! Można tu przytoczyć omawiany już przykład, w którym wystąpiła konieczność dodania nowego rutera innego producenta do istniejącej sieci opartej na ringu FDDI. Niezależnie od tego, jakie próby podejmowaliśmy, pierścień z włączonym nowym ruterem nie pracował poprawnie. Zawsze następowało przerwanie połączenia pomiędzy nowym ruterem i jednym ze starszych ruterów. W końcu stwierdziliśmy, że nowy ruter nie mógł poprawnie nawiązać połączenia FDDI ze starszymi ruterami używanymi dotychczas. Obydwaj producenci udowodnili, że ich sprzęt spełnia standardy; nowy dostawca przedstawił dokumentację, z której wynikało, że jego ruter jest nieznacznie szybszy. Rozwiązaniem było więc takie skonfigurowanie interfejsu nowego rutera, aby wykonał jeden z kroków przy zestawianiu połączenia kilka milisekund wolniej, dając w ten sposób starszym ruterom czas na odpowiedź. Jeśli taka opcja konfiguracji byłaby niemożliwa, to prawdopodobnie nasz pierścień nigdy nie zacząłby poprawnie pracować.

Kiedy więc oceniasz elastyczność konfiguracji proponowanych ruterów, powinieneś upewnić się, czy wybrany przez Ciebie ruter będzie na tyle elastyczny, aby spełniać Twoje obecne wymagania oraz wymagania, których jeszcze nie określiłeś. Pamiętaj jednak, aby wybrany przez Ciebie ruter nie był zbyt skomplikowany, bo inaczej pogubisz się w szczegółach jego konfiguracji. Powinieneś też upewnić się, czy domyślnie skonfigurowane opcje mają rozsądne wartości i czy rozumiesz, do czego one służą.

Metody konfigurowania ruterów

Jednym z ostatnich aspektów elastyczności rutera jest metoda wykorzystywana do jego konfigurowania. Jest kilka możliwości. Są wśród nich proste interfejsy, w których wykorzystuje się linię poleceń, systemy menu, systemy konfiguracji oparte na stronach WWW i pracujące z poziomu przeglądarki, protokół *Simple Network Management Protocol (SNMP),* a także własne pakiety producenta uruchamiane w środowisku graficznym na stacji roboczej. To, którą z metod wybierzesz, zależy w większości od gustu, ale warto rozważyć kilka z ich zalet i wad.

W interfejsie linii poleceń możliwy jest dostęp do pełnego zakresu funkcji konfiguracyjnych oferowanych przez ruter. Używając tego interfejsu możesz konfigurować różne parametry i możesz dostać się do rutera za pomocą prostego terminala lub programu emulującego pracę terminala, działającego na stacji roboczej. Często możliwe jest wykorzystywanie tego interfejsu konfiguracyjnego poprzez sieć z użyciem protokołu zdalnego logowania się, takiego jak Telnet. Dzięki temu możliwe jest konfigurowanie rutera lub rozwiązywanie problemów bez konieczności fizycznego chodzenia do urządzenia i włączania się do portu konfiguracyjnego tego urządzenia. Chyba największą zaletą interfejsu wykorzystującego linię poleceń jest możliwość konfigurowania rutera lub śledzenia jego pracy przy minimalnych wymaganiach sprzętowych i programowych wobec stacji roboczej, z której to robisz. Bez problemu można do tego celu wykorzystywać najprostsze terminale sieciowe i wszystkie inne interfejsy, aż po superemulatory terminala, które są częścią systemu terminala graficznego. Możliwa jest również praca w całym zakresie prędkości transmisji, poczynając od wolnych połączeń szeregowych realizowanych przez modemy, a kończąc na szybkich łączach sieciowych. Spróbuj popracować z tego typu konfiguracją przez graficzny interfejs, a następnie zrób to samo wykorzystując wolne łącze szeregowe -zobaczysz, jakie to frustrujące.

Proste interfejsy linii poleceń mogą być również obsługiwane przez skrypty generowane przez programy typu TCL Expect, który opisany jest w książce *Exploring Expect* napisanej przez Dona Libesa (wydawnictwo O'Reilly). Choć możliwe jest również pisanie skryptów dla innych rodzajów interfejsów konfiguracyjnych, takich jak menu tekstowe, to muszę przyznać, że z własnych doświadczeń wiem, iż pisanie tych skryptów jest znacznie trudniejsze niż posługiwanie się prostą linią poleceń. Pracowałem z obydwoma interfejsami. Ponieważ polecenia w linii poleceń nie wymagają zbyt wiele specjalnego formatowania, łatwiej jest w taki sposób zapisywać przykłady w instrukcjach dla pracowników, uwagi o błędach lub umieszczać je w wiadomościach e-mail wysyłanych do współpracowników lub pracowników obsługi technicznej producenta sprzętu.

Jedną z podstawowych wad interfejsu opartego na linii poleceń jest to, że zawsze należy wiedzieć, jaka opcja jest właściwa w danym punkcie procesu konfiguracji. W dobrze opracowanym interfejsie będzie się znajdowała pomoc kontekstowa (opisująca tylko te polecenia, które mają zastosowanie w danym punkcie procesu konfiguracji). Musisz jednak pamiętać, że nie wszyscy producenci oferują dobrze opracowane interfejsy konfiguracyjne. Ponadto w zależności od posiadanego przez Ciebie doświadczenia w pracy z klawiaturą oraz pomocy zapewnianej przez edytor konfiguracji rutera, pisanie poprawnych poleceń, które spowodują pożądaną konfigurację rutera, może być dość uciążliwe. Podobnie, jak w przypadku pomocy kontekstowej, i w tym miejscu warto zwrócić uwagę na jakość opracowania interfejsu, który powinien ułatwiać wydawanie właściwych poleceń. Ale naprawdę dobre interfejsy są rzadkością. Pomimo wymienionych wad jest to jednak interfejs konfiguracji rutera, który polecam.

Kryteria doboru ruterów

Za pomocą systemu konfiguracji opartego o menu producenci ruterów próbują dać użytkownikom przyjemny i uporządkowany sposób konfigurowania rutera. Zaletą systemu konfiguracji bazującego na strukturze menu jest to, że nie pogubisz się w szczegółach, które w danym momencie nie są ważne, gdy przeprowadzasz konfigurację jednej z opcji. Ponadto producent może dynamicznie zmieniać menu po to, by pokazać Ci wybory, których dokonałeś wcześniej, i w ten sposób uchronić Cię przed popełnianiem typowych błędów. System konfiguracji oparty na menu może być dostępny poprzez protokół zdalnego logowania, podobnie jak to miało miejsce w przypadku interfejsu linii poleceń.

Jedną z wad systemu konfiguracji opartej na menu jest fakt, że wymaga on inteligentnego terminala lub dobrego emulatora terminala. Częstym wymaganiem jest, aby terminal lub emulator potrafiły pracować zgodnie z terminalem DEC VT100. Choć ten typ terminala jest powszechnie spotykany, to jednak jest to pewne ograniczenie wpływające na wybór sprzętu, na którym będzie uruchomiony terminal oraz oprogramowanie. Drugą podstawową wadą tego typu systemu konfiguracji jest fakt, że zwykle nie obsługuje on wszystkich opcji konfiguracji, których możesz chcieć użyć. Jeśli nawet jakaś opcja jest dostępna, to często trudno ją odnaleźć w skomplikowanej strukturze menu i opcji menu. Dość trudno jest też obejrzeć wszystkie opcje konfiguracji jednocześnie, chyba że system ma wbudowaną opcję, która potrafi wyświetlić plik konfiguracji rutera.

Dostępną obecnie kombinacją interfejsu linii poleceń oraz systemu menu jest interfejs pracujący w WWW. Wykorzystując typową przeglądarkę możesz uzyskać dostęp do serwera wbudowanego w oprogramowanie rutera i wyświetlić informacje o jego stanie lub skonfigurować niektóre opcje. Jednym z takich rozwiązań, z którym osobiście się zapoznałem, jest serwer HTTP wbudowany w najnowsze wersje systemu Cisco IOS. Dodając do konfiguracji rutera polecenie

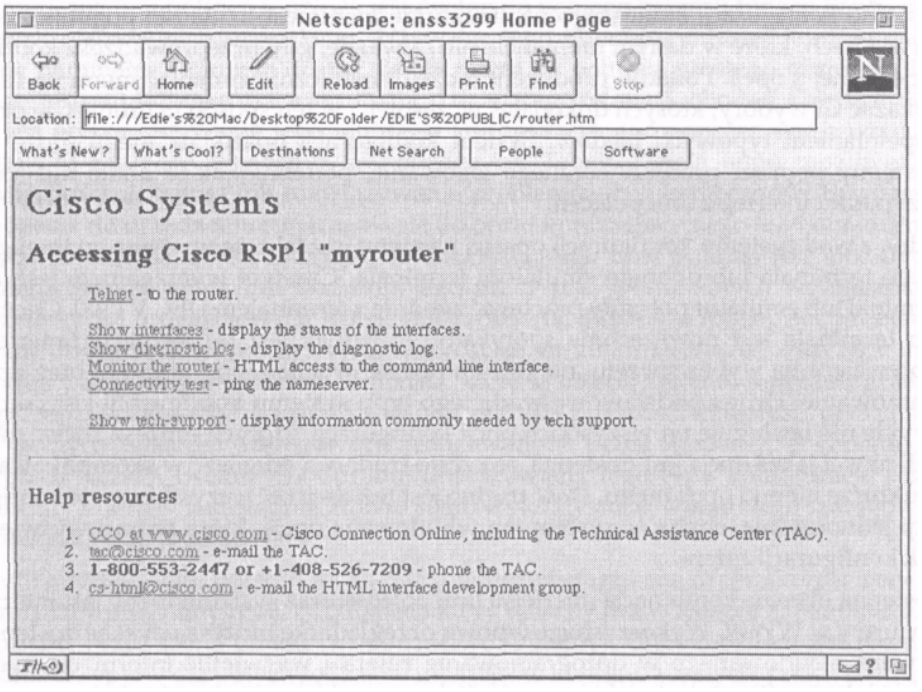
```
ip http server
```

możesz uaktywnić dostęp do rutera z dowolnej przeglądarki, nawet tekstowej, jaką jest lynx.*

Kiedy uzyskasz połączenie z ruterem wykorzystując przeglądarkę WWW, będziesz miał dostęp do kilku podstawowych poleceń poprzez łącza hipertekstowe, łącznie z dostępem do opcji konfiguracji rutera. Możliwy będzie również dostęp do kilku najczęściej stosowanych poleceń diagnostycznych, bez konieczności logowania się na ruterze. Taki sposób obsługi rutera może być użytecznym rozwiązaniem, łączącym w sobie cechy CLI i systemów opartych o menu.

*Podobnie jak każdy interfejs konfiguracyjny rutera, ten również powinien być chroniony, a dostęp do niego powinni mieć tylko pracownicy obsługujący sieć. W jaki sposób można chronić interfejs i ograniczać dostęp do niego, dowiesz się w rozdziale 10, zatytułowanym „Bezpieczeństwo sieci".

Strona WWW zawierająca opcje konfiguracji rutera pokazana została na rysunku 4-1. Interfejs ten nie jest może piękny, ale jest za to funkcjonalny.



Rysunek 4-1: Przykładowa strona domowa rutera

Problemy, które moim zdaniem występują w przypadku tego typu interfejsów, są w większości takie same jak w systemach opartych na menu oraz w systemach graficznych opisanych niżej. Mówiąc wprost, nie zawsze możliwy jest dostęp do tego oprogramowania, jeśli ma się prosty sprzęt. Ponadto, jak zaznaczyłem wcześniej, interfejs WWW jest raczej niewygodny i nie pozwala na dostęp do wszystkich funkcji konfiguracyjnych. W takim interfejsie nawet proste polecenie *traceroute* wymaga kilku poziomów odwołań, podczas gdy w interfejsie CLI konieczne jest wpisanie tylko kilku znaków z klawiatury. Powinieneś jednak obserwować rozwój tej szybko rozwijającej się metody konfiguracji i monitorowania pracy rutera. Może wkrótce zostanie ona poprawiona i stanie się ważnym narzędziem dla Twoich pracowników (przy odpowiednich zabezpieczeniach).

Coraz częściej urządzenia sieciowe wyposażone są w możliwość zarządzania przy użyciu protokołu SNMP. Protokół ten został opracowany dla potrzeb konfiguracji i monitorowania urządzeń w sieci. Zdefiniowano w nim bazy danych zawierające zmienne, które znane są pod nazwą *Management Inormation Base (MIB),* a zadania wykonywane są poprzez czytanie i zapisywanie wartości zmiennych, dokonywane pod kontrolą oprogramowania, które uruchomione jest na odległym komputerze. SNMP nie zastępuje zwykle innych opcji konfiguracyjnych. Protokół stosowany jest jako alternatywa lub rozszerzenie dla innych dostępnych w urządzeniu opcji.

Jedną z głównych zalet SNMP jest daleko posunięta standaryzacja tego protokołu. Ponieważ SNMP wykorzystuje standardowe protokoły transmisji i jest oparty na dobrze zdefiniowanych bazach MIB, możliwa jest konfiguracja sprzętu różnego typu pochodzącego od różnych producentów za pomocą tego samego oprogramowania. Dzięki połączeniu możliwości monitorowania stanu konfigurowanych urządzeń SNMP staje się jednym z najczęściej stosowanych rozwiązań konfiguracyjnych i platformą zarządzania pracą sieci.

Główną wadą SNMP jest to, że protokół ten wymaga uruchomienia na wydzielonym komputerze specjalnego oprogramowania służącego do zarządzania. Niektórzy producenci dostarczają oprogramowanie, które jest w stanie zarządzać ich własnym sprzętem, a przynajmniej monitorować stan tego sprzętu. Inni producenci natomiast pozostawiają użytkownikowi wybór platformy zarządzania. Na szczęście powszechnie dostępne jest oprogramowanie zarządzające pochodzące od różnych producentów i pracujące pod kontrolą różnych systemów operacyjnych. Do platform tych należą: HP OpenYiew, Sun Net Manager firmy Sun i Netview 6000 firmy IBM (obecnie IBM sprzedaje pakiet o nazwie Tivoli TME 10 - przyp. tłum.). Kolejną wadą SNMP jest złożoność tego protokołu. Moim zdaniem słowo „simple" występujące w nazwie odnosi się tylko do mechanizmu wykonywania wszystkich zadań, bazującego na czytaniu i zapisywaniu wartości poszczególnych zmiennych określonych w bazie danych. Próba wykonania choćby podstawowych konfiguracji przy wykorzystaniu samego protokołu, bez użycia specjalnego oprogramowania udostępnionego przez producenta sprzętu, raczej się nie powiedzie. Każda taka zmiana w konfiguracji może wymagać zmiany wartości kilkunastu, a nawet większej liczby zmiennych zdefiniowanych w MIB.

Ostatnią wadą SNMP jest to, że trudno w tym protokole wprowadzić podstawowe zabezpieczenia, chroniące proces konfiguracji. Każde zapytanie i odpowiedź SNMP zawiera nie kodowany ciąg znaków, który odpowiada hasłu w systemie operacyjnym. Jeśli ten ciąg znaków zostanie przechwycony przez kogoś obcego, to ruter będzie dla niego dostępny tak samo, jak jest dostępny dla administratora. Nic oprócz wspomnianej nazwy nie chroni go przed złośliwymi działaniami innych użytkowników sieci. Podobna sytuacja występuje również w przypadku stosowania hasła zabezpieczającego dostęp do rutera przez sesję Telnet, lecz hasło sesji Telnet przesyłane jest w sieci tylko raz, kiedy sesja jest rozpoczynana.

Znacznie trudniej jest więc podsłuchać hasło w sesji Telnet niż w sesji SNMP, gdzie jest ono przesyłane w każdym pakiecie. Problem zabezpieczenia haseł przesyłanych w sieci omówiony będzie w rozdziale 10, gdzie mówić będziemy również o systemie Kerberos, TACACS i RADIUS.

SNMP w wersji 2 ma znacznie lepiej opracowane zabezpieczenia przesyłanych danych i wykorzystuje silniejszy model autentykacji i zabezpieczeń. Trudno jest jednak znaleźć producenta rutera, który w pełni obsługuje zabezpieczenia implementowane w SNMPv2 . Konieczne będzie zastosowanie oprogramowania zarządzającego pracą sieci, które będzie w stanie współpracować poprawnie z lepszym systemem zabezpieczeń. Stosowanie bardziej rozwiniętego systemu zabezpieczeń znacznie komplikuje proces *zarządzania przez* SNMP. Mimo wymienionych wad SNMP ma wiele cech dodatnich, które sprawiają, że jest doskonałym narzędziem monitorowania pracy urządzeń i śledzenia problemów w nich występujących. Nie powinieneś więc zapominać o tym protokole.

Nie bierz poważnie producentów, którzy całą konfigurację swojego sprzętu opierają na działaniu własnego programu uruchamianego na jednym z hostów w sieci. Choć programy takie są często bardzo dobre i mają doskonałą formę graficzną dostosowaną do środowiska graficznego systemu operacyjnego hosta, to jednak mają wszystkie wady, które omówiliśmy podczas opisywania poprzednich interfejsów. Główną z nich jest to, że jesteś uzależniony od oprogramowania dostarczanego przez producenta sprzętu oraz od platformy sprzętowej i systemów operacyjnych, dla których zostało ono napisane. Jaki będziesz miał pożytek z programu, który pracuje na pecetach w środowisku Windows, jeśli wszystkie maszyny w twojej sieci to Apple Macintosh? Kolejną dużą wadą jest to, że oprogramowanie takie znacznie utrudnia dostęp do konfiguracji rutera z innych lokalizacji. Ktoś może zadzwonić do Ciebie o 3:00 w nocy, by zgłosić problem na jednym z ruterów. Jeśli do rutera tego masz dostęp jedynie *przez* komputer stojący u Ciebie na biurku, a sprawa nie może poczekać do rana, to nie będziesz miał innego wyjścia jak ubrać się i pojechać do biura. Gdyby ruter był obsługiwany *przez* jakiś rodzaj interfejsu ASCII (linia poleceń lub menu), to mógłbyś uruchomić program terminala na swoim komputerze w domu, połączyć się przez modem z ruterem i spróbować zdalnie naprawić problem.

Na zakończenie należy podkreślić, że graficzne systemy konfiguracji często utrudniają zrozumienie ostatecznej konfiguracji rutera. Dopiero po zakończeniu procesu konfiguracji możesz określić, co tak naprawdę zrobiłeś z ruterem, i to tylko dzięki producentowi, który dobrze opracował interfejs graficzny. Jeśli interfejs będzie kiepski, to nigdy do końca nie będziesz mógł dowiedzieć się, jak skonfigurowany jest Twój ruter. Powtórzę po raz kolejny: trzymaj się z dala od producentów, którzy zapewniają konfigurację swojego sprzętu tylko poprzez kolorowy i przyjemny dla oczu interfejs graficzny.

Rozbudowa konfiguracji

Ostatnim kryterium, które powinieneś rozważyć przy ocenie rutera, jest rozbudowa jego konfiguracji. Rzadko udaje się dokładnie przewidzieć liczbę i typ interfejsów, *w* które należy wyposażyć ruter. Kiedy źle ocenisz swoje potrzeby, staniesz prawdopodobnie przed problemem wymiany niedawno zakupionego rutera na nowy albo dokupienia kolejnego rutera do obsługi jednego czy dwóch segmentów sieci.

Najlepiej byłoby, gdyby ruter, który niedawno zakupiłeś, miał wolne miejsce na dołożenie kilku modułów, które pozwolą na obsługę Twojej rozrastającej się sieci.

Oczywiście nie chcesz również, aby zbyt dużo mocy rutera czekało na przyszłe moduły, chyba że jesteś absolutnie pewien, że będziesz jej potrzebował. Rozważmy sieć, gdzie docelowo przewiduje się obsługę 10 lub 11 segmentów sieci Ethernet, ale obecnie konieczna jest obsługa tylko 5. Możesz zakupić ruter z taką liczbą interfejsów, abyś nie musiał wymieniać go na nowy, kiedy sieć się rozrośnie. Jeśli jednak będziesz miał do wyboru ruter wyposażony w 6 interfejsów lub ruter z 12 interfejsami, to ciężko Ci będzie przekonać samego siebie, że pieniądze za 7 interfejsów to dobrze wydane pieniądze. Z drugiej strony 6 interfejsów lepiej pasuje do Twoich obecnych wymagań, ale nie pozwala Ci na rozbudowę sieci, dopóki nie wymienisz tego rutera na taki, który obsługuje 12 interfejsów.

I tu dochodzi do głosu ocena możliwości rutera. Jeśli ruter pozwala na dodanie interfejsów, to możliwa będzie jego rozbudowa wraz z rozrastaniem się sieci. Innymi słowy, idealnym ruterem byłoby urządzenie wyposażone początkowo w 6 interfejsów i pozwalające na dodawanie kolejnych w miarę potrzeb. W skrajnym przypadku można się pokusić o możliwość dodawania interfejsów pojedynczo, ale takie rozwiązanie jest zwykle dość kosztowne. Lepiej dodawać interfejsy przez moduły grupujące po kilka interfejsów. Kiedy zastanawiasz się nad możliwościami rozbudowy rutera, pomyśl również o jego obsłudze. Niewątpliwie idealnym rozwiązaniem byłaby możliwość dodawania nowych interfejsów bez konieczności wyłączania rutera i przerywania pracy użytkowników dołączonych do istniejących segmentów sieci. Tu przydałaby się możliwość wymiany modułów na gorąco.

Dodawanie większej liczby interfejsów do rutera nie przyniesie spodziewanych efektów, jeśli moc przetwarzania pakietów w tym ruterze jest ograniczona. Choć wygodnie byłoby założyć, że producenci ruterów nigdy nie sprzedają sprzętu, który można skonfigurować z taką liczbą interfejsów, która nie będzie mogła być obsłużona przez procesor i pamięci rutera, to jednak nie zawsze można mieć taką pewność. Często sytuacja taka nie wynika z tego, że producent próbuje nas oszukać, lecz z tego, że każda dołączana do rutera sieć jest inna i w innym stopniu obciąża ten ruter. Mówiąc krótko, upewnij się, że ruter ma wystarczającą moc dla obsługi docelowej jego konfiguracji lub że za rozsądne pieniądze istnieje możliwość zwiększenia mocy rutera poprzez jego modyfikację.

Interfejsy specjalnego przeznaczenia

W niektórych przypadkach konieczne będzie sprawdzenie, czy oferowany ruter obsługuje interfejsy specjalnego przeznaczenia. Prawie wszyscy producenci ruterów dostarczają interfejsy dla typowych technologii sieciowych, takich jak Ethernet, Token Ring, FDDI i łącza szeregowe, ale nie wszyscy będą w stanie sprostać Twoim specjalnym wymaganiom.

Trzy rodzaje interfejsów specjalnego przeznaczenia, których możesz potrzebować, to:

- bezpośrednie przyłącze do kanału transmisji komputera mainframe;
- *Asynchronous Transfer Mode* (ATM)
- *High Performace Par alei Interconnectb (HiPPF).*

Jeśli w Twojej sieci pracuje jeden lub więcej komputerów typu mainframe, może się okazać, że wygodnie byłoby mieć bezpośredni dostęp do kanału danych systemu mainframe. Takie szybkie łącze z tym systemem może zmniejszyć obciążenie centralnego procesora systemu i wyeliminować konieczność zakupu innego sprzętu, jak specjalne interfejsy sieciowe. Ponadto tańsze łącze tego typu zapewni prawdopodobnie szybszy dostęp do komputera mainframe niż sieć wykonana w technologii LAN, taka jak Ethernet lub Token Ring. Nie wszyscy producenci ruterów obsługują jednak takie przyłącza lub obsługują je nie we wszystkich modelach oferowanego sprzętu. Jeśli zakładasz, że Twoja sieć będzie z czasem migrowała do technologii ATM, lub jeśli masz lub planujesz zakup superkomputera wyposażonego w interfejs HiPPI, to możliwość obsługi takich interfejsów przez Twój ruter będzie bardzo istotna z punktu widzenia współpracy istniejącej sieci z nowym sprzętem.

Niestety, może się okazać, że nie jest łatwo znaleźć producenta ruterów, który będzie w stanie obsłużyć wszystkie interfejsy specjalnego przeznaczenia, a także spełnić inne dziwne wymagania, jakie możesz stawiać swojej sieci. Możesz być zmuszony zakupić rutery od dwóch lub większej liczby dostawców. Choć współpraca tego sprzętu będzie oczywiście możliwa, postaraj się zminimalizować liczbę dostawców. Mając sprzęt pochodzący od większej liczby producentów będziesz musiał spędzić więcej czasu na szkolenie personelu obsługującego sieć. Rośnie również prawdopodobieństwo występowania problemów we współpracy tych urządzeń i popełniania błędów przez administratorów, a także ograniczenie liczby wykorzystywanych funkcji do tych, które obsługiwane są we wszystkich ruterach. Wynikiem stosowania ruterów pochodzących od różnych producentów jest często niemożność osiągnięcia niektórych stawianych przed siecią celów, co stawia pod znakiem zapytania zyski ze stosowania takiego heterogenicznego środowiska.

Wybór protokołu rutowania 5

Rutowanie statyczne a rutowanie dynamiczne
Klasyfikacja dynamicznych protokołów rutowania Wybór protokołu rutowania

W poprzednich rozdziałach skupiliśmy się na projekcie sieci i wyborze właściwego rutera. Tematy te są bardzo ważne, kiedy tworzysz nową sieć od podstaw lub planujesz wymianę całej lub części dotychczasowej sieci. To są czysto teoretyczne zagadnienia w sytuacji, kiedy masz już sieć, która działa w Twojej firmie. W takim przypadku, który *zdarza* się znacznie częściej, nie masz możliwości wyboru topologii sieci, medium sieci ani producenta ruterów. Jesteś ograniczony decyzjami podjętymi wcześniej *przez* Ciebie samego lub Twojego poprzednika. W najlepszym wypadku masz możliwość zaprojektowania swojej idealnej sieci i przemyślenia sposobów migracji rozwiązań stosowanych w używanej obecnie sieci do tego ideału.

W rozdziale tym pozostawimy teoretyczne aspekty projektowania sieci i zajmiemy się bardziej praktycznymi aspektami *zarządzania praca,* sieci. Choć będziemy zajmowali się również teorią, zwłaszcza w pierwszych kilku częściach rozdziału, to tylko w związku z bardziej praktycznymi opisami dotyczącymi aspektów konfiguracji rutera dla obsługi nowych sieci lub sieci, które już istnieją.

Rutowanie statyczne a rutowanie dynamiczne

Zanim przejdziemy do dokładnego omawiania tematów dotyczących wyboru i konfigurowania dynamicznego protokołu rutowania IP, powinniśmy zająć się rurowaniem statycznym, które jest alternatywą dla rutowania dynamicznego. W rozdziale 1, zatytułowanym „Podstawy sieci *IP",* dowiedzieliśmy się, że każda maszyna w sieci IP podejmuje decyzję o tym, jak dostarczyć informację do adresata, sprawdzając zawartość własnej tablicy rutowania.

Zamiast wyznaczania pełnej trasy prowadzącej do odbiorcy, maszyna wybiera adres miejsca, które przekaże dane dalej w odpowiednim kierunku. Niezależne rutowanie opierające się na kolejnych przeskokach wymaga, aby każda maszyna pracująca w sieci miała zawsze aktualne informacje o tym, jak osiągnąć poszczególne adresy przeznaczenia. Jeśli z jakichś powodów uaktualnianie tych informacji zostanie przerwane, dwie (lub więcej) maszyny (prawdopodobnie rutery) mogą stworzyć coś, co nazywa się pętlą rutowania, i spowodować, że wysłane przez nadawcę pakiety nigdy nie dotrą do adresata.

Aby osiągnąć stan pełnej wymiany informacji o rutowaniu, administrator powinien ręcznie skonfigurować każdą maszynę, podając jej pewną liczbę tras, które będzie ona uważała za aktualne, lub poprzez wymianę informacji o rutowaniu dokonywaną między pracującymi w sieci maszynami, dokonywaną z użyciem jakiegoś protokołu. Pierwszy sposób znany jest jako *rutowanie statyczne,* drugi - *rutowanie dynamiczne.*

Zalety rutowania statycznego

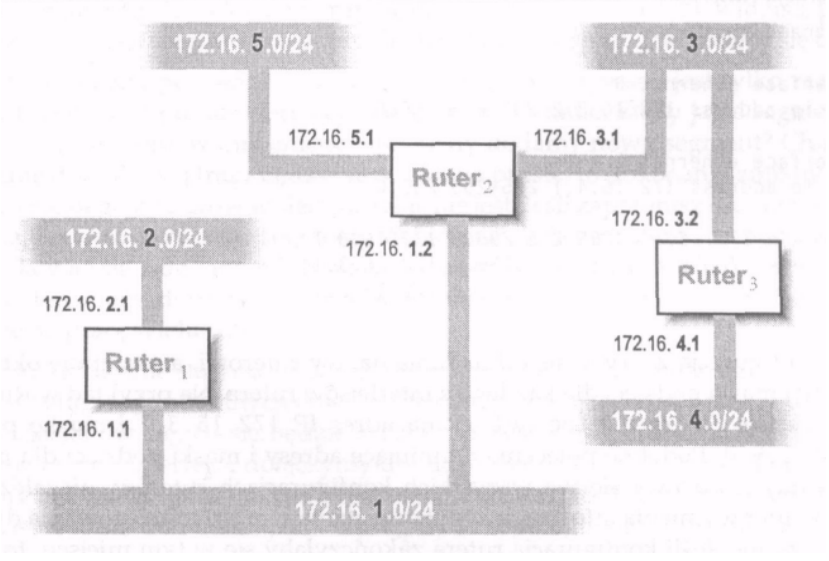
Rutowanie statyczne ma kilka ogromnych zalet w stosunku do rutowania dynamicznego. Przede wszystkim jest przewidywalne. Ponieważ administrator sieci wcześniej osobiście liczy tablice rutowania, trasa, po której pakiet jest przesyłany między dwoma miejscami, jest zawsze dobrze znana i może być dokładnie kontrolowana. W przypadku rutowania dynamicznego wybrana w danym momencie trasa zależy od tego, jakie urządzenia i łącza funkcjonują oraz jak ruter zinterpretował nadesłane przez inne urządzenia informacje z uaktualnieniami tras.

W związku z tym, że w rutowaniu statycznym nie jest potrzebny żaden protokół dynamicznej wymiany informacji, łącza sieci nie są dodatkowo obciążane informacjami generowanymi przez ten protokół. Choć to dodatkowe obciążenie może być minimalne w sieci opartej na pierścieniu FDDI lub w segmencie Ethernet, to może ono stanowić znaczącą część informacji przesyłanych w paśmie wolnego łącza modemowego. Rozważmy sieć składającą się z 200 segmentów. Co 30 sekund, zgodnie ze specyfikacją protokołu RIP, rutery powinny wysłać informacje aktualizacyjne zawierające opis dostępności wszystkich 200 segmentów sieci. Jeśli zapis każdej trasy zajmuje 16 oktetów (plus niewielka ilość danych dodatkowych), to minimalny rozmiar uaktualnień wysyłanych w tej sieci wynosi około 3 kilobajtów. Każdy ruter musi więc wysłać 3 Kb informacji w ciągu 30 sekund przez każdy ze swoich interfejsów. Jak widzisz, dla dużej sieci pasmo przeznaczone na przesyłanie uaktualnień rośnie dość szybko.

Poza tym rutowanie statyczne jest łatwe do skonfigurowania w małych sieciach. Administrator sieci musi po prostu powiedzieć każdemu z pracujących w sieci ruterów, w jaki sposób może on przesłać informacje do każdego segmentu sieci, do którego nie jest bezpośrednio dołączony. Rozważmy sieć pokazaną na rysunku 5-i. Składa się ona z trzech ruterów, połączonych pięcioma segmentami sieci. Z rysunku wyraźnie widać, że jedyna trasa z rutera o nazwie Ruter I do hosta w sieci 172.16.3.0/24 prowadzi przez Ruter2. Podobnie jedyna trasa do hosta pracującego w podsieci 172.16.4.0/24 prowadzi przez Ruter2.

Rutowanie statyczne a rutowanie dynamiczne

Poniżej przedstawiono odpowiednie fragmenty konfiguracji tych trzech ruterów, wykonanej przy użyciu rutowania statycznego. Zwróć uwagę na to, że konfiguracja każdego z ruterów musi zawierać trasę statyczną do każdej z sieci dołączonych do pozostałych ruterów, ale nie do tych sieci, które są dołączone bezpośrednio do tego rutera.



Rysunek 5-1: Mała sieć używająca rutowania statycznego

Konfiguracja Ruteral:

```
hostname routerl i
interface ethernet O
      ip address 172.16.1.1  255.255.255.0;
interface ethernet I
      ip address 172.16.2.1  255.255.255.0 i
ip  route    172.16.3.0 255.255.255.0 172.16.1.2
ip  route    172.16.4.0 255.255.255.0 172.16.1.2
ip  route    172.16.5.0 255.255.255.0 172.16.1.2
```

Konfiguracja Ruteral:

```
hostname router2 i
interface ethernet O
      ip address 172.16.1.2 255.255.255.0
      !
interface ethernet 1
      ip address 172.16.3.1  255.255.255.0
interface ethernet 2
      ip address 172.16.5.1  255.255.255.0
ip route 172.16.2.0  255.255.255.0  172.16161.1  ip route
172.16.4.0  255.255.255.0  172.16.3.2
```

Konfiguracja Rutera3:

```
hostname router3
!
interface ethernet O
      ip address 172.16.3.2 255.255.255.0
      !
interface ethernet 1
      ip address 172.16.4.1 255.255.255.0
      !
ip      route 172.16.1.0 255.255.255.0   172.16.3.1
ip      route  172.16.2.0 255.255.255.0   172.16.3.1
ip      route 172.16.5.0 255.255.255.0   172.16.3.1
```

Każda konfiguracja zaczyna się od nadania nazwy ruterowi, a następnie określenia adresu IP i maski podsieci dla każdego z interfejsów rutera. Na przykład w Ruterze2, drugi interfejs Ethernet (ethernet 1) ma adres IP 172.16.3.1 i maskę podsieci 255.255.255.0. Podobne polecenia definiujące adresy i maski podsieci dla interfejsów lokalnych pojawią się we wszystkich konfiguracjach ruterów, niezależnie od tego, czy ruter wymienia informacje z wykorzystaniem protokołu rutowania dynamicznego, czy nie. Jeśli konfiguracja rutera zakończyłaby się w tym miejscu, to każdy ruter miałby w swojej tablicy rutowania zapisy dotyczące wyłącznie sieci dołączonych do jego interfejsów. Konfiguracja jest jednak dłuższa i w dalszej części zawiera definicje rutowania statycznego pokazującego trasy do sieci, które dołączone są do innych ruterów. Każdy segment i p route definiuje trasę statyczną prowadzącą do podsieci, określoną przez numer sieci i maskę, a także adres IP rutera. Na przykład pierwszy segment i p route w konfiguracji Rutera3 definiuje trasę do podsieci 172.16.1.0, z maską 255.255 .255.0 (172.16.1.0/24), prowadzącą przez ruter o adresie 172.16.3.1. Trasy statyczne razem z interfejsami lokalnymi pozwalają każdemu z ruterów rozgłaszać zawartość ich tablicy rutowania, w której są informacje o adresach sieci oraz adresie rutera kolejnego przeskoku, przez który można się do danej podsieci dostać.

Choć w przypadku tej małej sieci nie trzeba podawać wielu tras statycznych, aby osiągnąć pełne połączenie wszystkich podsieci, a Ruter1 i Ruter3 mogą się łączyć za pośrednictwem statycznych tras do Rutera2, to łatwo się domyślić, że podobna konfiguracja dla większej sieci, składającej się z setek segmentów, będzie bardzo skomplikowana.

Wady rutowania statycznego

Choć rutowanie statyczne ma niewątpliwe zalety w stosunku do rutowania dynamicznego, nie jest wolne od wad. Ceną za prostotę rozwiązania jest brak skalowalności. Obliczenie tras z każdego rutera do każdej podsieci w sieci składającej się z trzech ruterów i pięciu segmentów nie stanowi problemu. Wiele sieci jest jednak znacznie większych. Zastanów się, jak będzie wyglądała lista tras w przypadku sieci, w której znajduje się 200 segmentów i kilkanaście ruterów. Zastosowanie rutowania statycznego w takiej sieci będzie wymagało policzenia ruterów następnego przeskoku dla każdego segmentu sieci i każdego rutera, czyli ponad 2400 tras! Jak widzisz, policzenie takich tras staje się poważnym problemem i na pewno trudno ustrzec się błędów.

Oczywiście można powiedzieć, że takie liczenie wykonywane jest tylko raz, kiedy sieć budowana jest po raz pierwszy. Co się jednak stanie, kiedy jakiś segment sieci zostanie przeniesiony w inne miejsce lub kiedy dodamy nowy segment? Choć samo policzenie dodatkowej trasy będzie stosunkowo proste, to dokonanie zmiany w konfiguracji każdego z ruterów w sieci już takie nie jest. Jeśli zapomnisz o jednej ze zmian, to w najlepszym wypadku segmenty dołączone do tego rutera nie będą w stanie komunikować się z dodanym lub przeniesionym segmentem. W najgorszym wypadku błąd ten może doprowadzić do powstania pętli rutowania, która negatywnie wpłynie na pracę wielu ruterów.

Ponieważ rutowanie statyczne jest z definicji statyczne, to nie można go wykorzystywać do obsługi redundantnych połączeń sieci, zapewniających jej pracę w przypadku awarii. Zastanów się, co się będzie działo z przykładową siecią, kiedy do Rutera3 dodamy kolejny interfejs i dołączymy do niego sieć 172 .16 .2 .0/24, ale trasy pozostawimy bez zmian. Jeśli uszkodzeniu ulegnie Ruter2, to Ruter3 nie będzie w stanie przystosować się do zmian, jakie wystąpiły w topologii sieci, i nadal nie będzie w stanie komunikować się z hostami pracującymi w sieci 172.16.1.0/24. Nieumiejętność dostosowania się do uszkodzeń sieci, nawet w sytuacji, kiedy dostępne są łącza redundantne, oraz problemy związane ze skalowalnością to główne wady rutowania statycznego i argumenty przemawiające za stosowaniem rutowania dynamicznego.

Zalety rutowania dynamicznego

Głównymi zaletami rutowania dynamicznego w stosunku do rutowania statycznego są skalowalność i zdolność dopasowywania się do zmieniających się połączeń sieci. Sieć obsługiwana przez dynamiczny protokół rutowania może się znacznie szybciej rozrastać. Jest także zdolna do dopasowywania się do topologii sieci, która zmienia się w wyniku rozbudowy lub w wyniku uszkodzeń jednego lub większej liczby komponentów sieci.

Rutery wykorzystujące dynamiczny protokół rutowania uczą się topologii sieci poprzez wymianę informacji z innymi ruterami. Każdy ruter rozgłasza do innych ruterów w sieci swoją obecność oraz informacje o trasach, jakie jest w stanie obsługiwać. Dlatego jeśli dodasz do sieci nowy ruter lub do istniejącego rutera dodasz kolejny segment sieci, pozostałe rutery dowiedzą się o tym fakcie i odpowiednio uaktualnią swoje tablice rutowania.

Nie musisz rekonfigurować ruterów, by poinformować je o zmianie, jaka nastąpiła w sieci. Podobny proces będzie zachodził, kiedy przeniesiesz jeden z segmentów sieci; pozostałe rutery dowiedzą się o tej zmianie od swoich sąsiadów. Musisz jedynie zmienić konfigurację rutera (lub ruterów), do którego przyłączony został przeniesiony segment sieci. Taki sposób dokonywania ręcznych zmian w sieci znacznie redukuje liczbę błędów, jakie mogą przy tym występować.

Możliwość uczenia się nowej topologii sieci może mieć skutki wykraczające daleko poza dodawanie nowych segmentów lub przenoszenie ich w inne miejsce. Możliwości te oznaczają również, że sieć może inteligentnie reagować na występujące w niej uszkodzenia. Jeśli znajdują się w niej połączenia redundantne, to częściowe uszkodzenie sieci z punktu widzenia ruterów wygląda tak jak przeniesienie kilku segmentów tej sieci (są one teraz osiągalne przez zapasowe ścieżki dostępu) lub usunięcie niektórych segmentów (są one teraz nieosiągalne). Mówiąc krótko, z punktu widzenia rutera pracującego z protokołem dynamicznego rutowania, nie ma większej różnicy pomiędzy uszkodzeniem sieci a zmianą jej konfiguracji. Rutowanie dynamiczne pozwala nawet częściowo uszkodzonej sieci funkcjonować nadal, choć być może z pewnymi ograniczeniami.

Wady rutowania dynamicznego

Rutowanie dynamiczne oczywiście ma także wady. Główną wadą jest większy stopień zawiłości działania sieci. Wymiana informacji o bieżącej topologii sieci nie jest tak prosta jak np. powiedzenie „Hej, mogę przesłać dane do..." Każdy ruter uczestniczący w wymianie danych poprzez dynamiczny protokół rutowania musi dokładnie określić, jakie informacje będzie wysyłał do innych ruterów. Jeszcze ważniejsze jest to, że na podstawie otrzymanych informacji od innych ruterów musi określić, która trasa jest najlepsza na dotarcie do każdej z podsieci. Ponadto jeśli ruter ma reagować na zmiany zachodzące w sieci, musi mieć możliwość usuwania starych lub bezużytecznych informacji ze swojej tablicy rutowania. Sposób, w jaki będzie określał, które informacje są przestarzałe lub bezużyteczne, jeszcze bardziej komplikuje protokół rutowania. Niestety, im lepiej protokół obsługuje różne sytuacje zdarzające się w sieci, tym bardziej jest skomplikowany. Stopień komplikacji protokołu prowadzi do błędów w jego implementacji lub różnic w interpretacji tego protokołu w sprzęcie różnych producentów.

Aby móc wymieniać informacje o topologii sieci, rutery muszą regularnie wysyłać komunikaty do innych ruterów posługując się dynamicznym protokołem rutowania. Komunikaty te muszą być wysyłane w segmentach sieci, podobnie jak wszystkie inne pakiety. W przeciwieństwie do innych pakietów przesyłanych w sieci, komunikaty ruterów nie zawierają żadnej informacji adresowanej do użytkowników, lecz informacje użyteczne dla ruterów. Z tego powodu z punktu widzenia użytkowników pakiety te są niepotrzebnym obciążeniem sieci. Na wolnych łączach mogą zajmować sporą część dostępnego pasma, zwłaszcza jeśli mamy do czynienia z dużą i niestabilną siecią.

I na zakończenie należy wspomnieć o tym, że niektóre (a może wszystkie) maszyny pracujące w Twojej sieci mogą nie potrafić posługiwać się żadnym z dynamicznych protokołów rutowania lub nie obsługują stosowanego w całej sieci protokołu. Jeśli tak, to rutowanie statyczne może być Twoim jedynym wyjściem.

Poznawszy wszystkie zalety i wady rutowania statycznego i dynamicznego, zaczniesz się prawdopodobnie zastanawiać, który z nich będzie lepszym wyborem. Jedyne, co możesz określić na pewno, to który z nich jest lepszy dla Twojej sieci. Jest jednak pośrednie rozwiązanie, które zmniejsza złożoność rutowania dynamicznego bez ograniczania jego skalowalności. To pośrednie rozwiązanie to schemat *hybrydowy,* w którym część sieci wykorzystuje rutowanie statyczne, a część - rutowanie dynamiczne.

Hybrydowe schematy rutowania

W hybrydowym schemacie rutowania niektóre części sieci wykorzystują rutowanie statyczne, a inne - rutowanie dynamiczne. To, która część sieci używa którego ze sposobów rutowania, nie jest ważne; możliwe jest stosowanie wielu rozwiązań. Jednym z częściej stosowanych schematów hybrydowych jest użycie rutowania statycznego na końcach sieci (w miejscach, które nazywałem wcześniej sieciami dostępowy-mi), a rutowania dynamicznego w podsieciach tworzących rdzeń i części dystrybucyjnej całej sieci. Zaletą stosowania rutowania statycznego w sieciach dostępowych jest to, że dołączone są w nich zwykle maszyny użytkowników. Maszyny te mają tylko w niewielkim stopniu zaimplementowaną obsługę rutowania dynamicznego (lub nie mają jej wcale). Ponadto sieci dostępowe mają zwykle tylko jedno przyłącze do ruterów (czasami dwa), przez co ilość pracy związanej z ręcznym konfigurowaniem tras jest niewielka. Często konieczne może być jedynie określenie domyślnej trasy rutowania w tego typu *sieciach końcowych.* W związku z ograniczoną liczbą połączeń z tymi sieciami często nie jest konieczne rekonfigurowanie rutowania w takiej końcowej sieci po przeniesieniu jej na nowe miejsce.

Z drugiej strony sieci dystrybucyjne i sieci tworzące rdzeń mają zwykle wiele przyłączy obsługiwanych przez rutery i w związku z tym wiele różnych tras, które muszą utrzymywać. Z tego powodu rutery pracujące w tych częściach sieci nie mogą posługiwać się trasą domyślną. Rutery (i hosty) znajdujące się w centralnej części sieci muszą znać pełną informację o rutowaniu w całej sieci. Ponadto rutery umieszczone w rdzeniu sieci i sieciach dystrybucyjnych muszą być informowane o zmianach, jakie występują w przyłączaniu sieci dostępowych. Choć możliwe jest ręczne poinformowanie każdego z ruterów o dokonanej zmianie, to zwykle znacznie łatwiej jest pozwolić na przekazywanie tych informacji za pośrednictwem dynamicznego protokołu rutowania.

Kolejną zaletą wykorzystywania tras statycznych w sieciach dostępowych jest możliwość ich kontroli. W zależności od struktury działu administrującego siecią, możesz nie mieć kontroli nad tym, co dzieje się w sieciach dostępowych. Mogą być one obsługiwane przez koordynatorów sieci LAN pracujących w poszczególnych działach firmy, którzy bezpośrednio Tobie nie podlegają.

Jeśli tak właśnie wygląda struktura organizacyjna, to znacznie wygodniej jest skonfigurować rutowanie statyczne z sieciami dostępowymi, a rutowanie dynamiczne uruchomić tylko na ruterach i maszynach, nad którymi masz bezpośrednią kontrolę. Ponieważ stosowanie dynamicznego protokołu rutowania wiąże się z pewnym zaufaniem do użytkowników, to często bezpieczniej jest nie używać go w takich lokalnych sieciach podlegających poszczególnym oddziałom firmy. Mówiąc krótko, kiedy masz do czynienia z rutera-mi, które nie są pod twoją bezpośrednią kontrolą, to najlepszym rozwiązaniem jest stosowanie rutowania statycznego wszędzie, gdzie to możliwe, a rutowania dynamicznego tam, gdzie jest to konieczne.

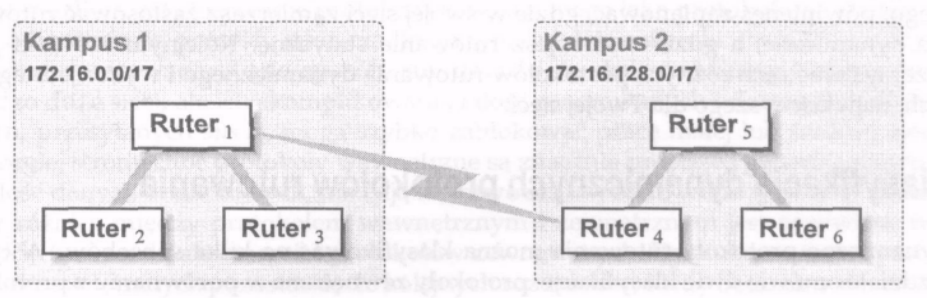
Kolejnym rodzajem hybrydowej struktury rutowania, którego zastosowanie powinieneś rozważyć, jest rozwiązanie oparte na paśmie w poszczególnych częściach sieci, a nie na sprawach związanych z administrowaniem siecią. W tym rodzaju struktury hybrydowej protokoły dynamicznego rutowania uruchamiane będą wszędzie tam, gdzie sieć pracuje po szybkich łączach LAN lub WAN, a rutowanie statyczne użyte jest tam, gdzie połączenia realizowane są za pomocą wolnych łączy. Jako przykład takiej sieci rozważmy sieć obejmującą cały uniwersytet. W każdym z budynków może znajdować się kilka ruterów połączonych ze sobą siecią Ethernet, FDDI i innymi szybkimi łączami. Poszczególne budynki połączono jednak za pomocą łączy WAN o przepustowości 56 kbps. Jeśli dwa budynki będą miały różne przestrzenie adresowe, to szybka zmiana ruterów obsługujących połączenie między tymi budynkami jest mało prawdopodobna. W takim przypadku jedyną zaletą wykorzystania dynamicznego protokołu rutowania pomiędzy budynkami jest to, że pakiety, które nie mogą być dostarczone do odbiorcy znajdującego się w innym budynku w związku z uszkodzeniem sieci, w której on pracuje, zatrzymane zostaną przed przesłaniem przez wolne łącze międzybudynkowe. Jest to jednak wyjątkowa sytuacja. Zwykle sieć jest stabilna, a pakiety docierają do adresatów.

Wiedząc o tym, należałoby zapytać, ile pasma wolnego łącza zabiera dynamiczny protokół rutowania. Choć większość protokołów rutowania jest tak opracowanych, aby zminimalizować wpływ uaktualnień tras na łącze, to dodatkowe obciążenie nigdy nie jest równe zeru. Lepiej więc używać dynamicznego rutowania w każdym z budynków, które obejmuje opisywana przez nas sieć, lecz na łączu pomiędzy budynkami, gdzie wolne pasmo jest najważniejsze, zastosować rutowanie statyczne.

Rutowanie statyczne pomiędzy częściami sieci połączonymi wolnym łączem może być jeszcze bardziej przydatne, jeśli obydwie podsieci współdzielą tę samą przestrzeń adresową (na przykład jedną sieć klasy B). W takim przypadku może być konieczne wykonanie wielu dodatkowych działań konfiguracyjnych. Problem ze wspólną przestrzenią adresową polega na tym, że zmiany w jednej z podsieci tworzących taką sieć powinny być widoczne dla dynamicznego protokołu rutowania działającego w drugiej podsieci. Jednym z rozwiązań tego problemu jest podział przestrzeni adresowej na dwie (lub więcej) podsieci, tak aby każda z nich tworzyła mniejszą, zamkniętą całość z agregowanymi adresami, jak pokazano na rysunku 5-2.

Ratowanie statyczne a nitowanie dynamiczne

Jeśli podzielisz przestrzeń adresową, to uprościsz rutowanie statyczne pomiędzy podsieciami znajdującymi się w różnych budynkach dzięki pracy ze zagregowanymi adresami.



Rysunek 5-2: Dwie sieci kampusowe współdzielące jedną przestrzeń adresową

Na powyższym rysunku Ruter1 musi mieć zdefiniowaną trasę statyczną prowadzącą do adresów w podsieci 172.16.128 .0/17. I, na podobnej zasadzie, Ruter5 musi mieć zdefiniowaną trasę statyczną dla zagregowanych adresów 172.16.0.0/17. Taka konfiguracja ruterów pozwala każdemu kampusowi na niezależne przydzielanie we własnym zakresie adresów pochodzących z jednej przestrzeni adresowej i upraszcza konfigurację rutowania pakietów pomiędzy kampusami.

Ostatnim problemem, jaki może wystąpić w omawianym przez nas hybrydowym schemacie rutowania pomiędzy kampusami, jest sytuacja, w której łącze spinające sieci kampusowe zostanie przełączone do innego rutera. Na przykład co się będzie działo, kiedy łącze zostanie przeniesione z Rutera1 do Rutera3? Konfiguracja ruterów w sieci kampusowej numer 2 nie ulegnie zmianie, ponieważ nadal można używać tych samych adresów IP dla łącza szeregowego, a zmiany, jakie trzeba będzie wykonać w sieci kampusu 1, nie będą zbyt duże. Na pewno o zmianach, jakie zaszły, muszą wiedzieć Ruter1 i Ruter3. Pomijając sprawy rekonfiguracji rutowania, konieczne jest dokonanie konfiguracji interfejsów wspomnianych ruterów. Zastanówmy się nad tym, czy Ruter2 musi zostać zrekonfigurowany tak, aby wiedział, że łącze prowadzące do sieci Kampus 2 zostało przeniesione? Nie jest to konieczne, jeśli wszystkie rutery skonfigurowane są tak, że umieszczają informacje o trasach statycznych w dynamicznym protokole rutowania.

Niektóre rutery mają możliwość przekazywania informacji z jednego źródła rutowania do drugiego. Zwykle mówiąc o wymianie informacji o rutowaniu myślimy o wymianie informacji pomiędzy dwoma dynamicznymi protokołami rutowania, ale przekazywanie informacji o rutowaniu statycznym do dynamicznego protokołu rutowania jest specjalnym przypadkiem takiej wymiany informacji. Nie będziemy się teraz zagłębiali w dokładne opisy sposobu, w jaki się to dokonuje, ponieważ łatwiej będzie wyjaśnić te zagadnienia w czasie, kiedy będziemy mówili o dynamicznym protokole rutowania i sposobach jego konfigurowania. Powinieneś jednak wiedzieć, że dołączanie informacji o konfiguracji tras statycznych do uaktualnień dynamicznego protokołu rutowania jest łatwym sposobem na ograniczenie liczby tras statycznych do minimalnej liczby ruterów.

Kiedy już omówiliśmy schematy rutowania statycznego, dynamicznego i hybrydowego, powinieneś zaplanować, gdzie w swojej sieci zamierzasz zastosować nitowanie dynamiczne, a gdzie zastosujesz rutowanie statyczne. Kolejnym krokiem jest przemyślenie cech różnych protokołów rutowania dynamicznego i wybór jednego z nich, najwłaściwszego dla Twojej sieci.

Klasyfikacja dynamicznych protokołów rutowania

Dynamiczne protokoły rutowania można klasyfikować na kilka sposobów. W tym rozdziale omówię dwie klasyfikacje: protokoły zewnętrzne w porównaniu z protokołami wewnętrznymi oraz protokoły typu dystans-wektor w porównaniu z protokołami stanu łącza. Pierwsza klasyfikacja opiera się na tym, w jakiej części sieci najlepiej stosować protokół; pomiędzy Twoją siecią a innymi sieciami, czy też wewnątrz Twojej sieci. Druga klasyfikacja opiera się na rodzaju informacji, które protokół wymienia oraz sposobie, w jaki każdy z ruterów podejmuje decyzje o wprowadzaniu do swojej tablicy rutowania otrzymywanych informacji.

Protokoły zewnętrzne a wewnętrzne

Dynamiczne protokoły rutowania są klasyfikowane jako *exterior gateway* protocol (EGP[+])* lub *interior gateway protocol (IGP).* Protokół klasyfikowany jako zewnętrzny odpowiada za wymianę informacji o rutowaniu pomiędzy dwiema niezależnymi administracyjnie sieciami, takimi jak sieci dwóch korporacji lub dwóch uniwersytetów. Każda z tych jednostek ma niezależną infrastrukturę sieciową i wykorzystuje EGP do przesyłania informacji o rutowaniu do innych podobnych jednostek. Najpopularniejszym obecnie zewnętrznym protokołem jest *Border Gateway Protocol (BGP).* Jest on podstawowym protokołem stosowanym pomiędzy sieciami tworzącymi globalną sieć Internet i specjalnie po to został opracowany.

W przeciwieństwie do protokołu opisanego wyżej, wewnętrzny protokół stosowany jest wewnątrz jednej domeny administracyjnej lub pomiędzy blisko współpracującymi grupami. Protokół ten został stworzony tak, aby był prostszy i w mniejszym stopniu obciążał rutery. Główną wadą tego typu protokołów jest to, że nie są one w stanie obsługiwać rozrastających się sieci. Najczęściej stosowanymi w sieciach IP protokołami są: *Routing Information Protocol (R1P), Open Shortest Patii First (OSPF)* oraz *Enhanced Interior Gateway Routing Protocol (E1GRP).**

*Protokoły stosowane w sieci Internet używały początkowo nazwy *gateway* dla określenia rutera. Takie nazewnictwo nie jest już stosowane, ale czasem pojawia się w dyskusjach na temat protokołów rutowania. [+] Nie należy tego mylić z protokołem o nazwie *Exterior Gateway Protocol* w wersji 2 (znanego również jako EGP), który jest jednym z wielu protokołów rutowania.

Pierwsze dwa protokoły są otwartymi standardami, które zostały użyte lub wymyślone przez społeczność sieci Internet, a trzeci jest protokołem firmowym, opracowanym przez Cisco Systems i stosowanym w ruterach tej firmy.

Choć możliwe jest stosowanie protokołu wewnętrznego jako protokołu zewnętrznego i odwrotnie, to pomysły takie rzadko przynoszą dobre wyniki. Protokoły zewnętrzne są opracowane w taki sposób, aby dawały się skalować i mogły obsługiwać bardzo duże sieci, ale ich skomplikowanie i ilość generowanych informacji dodatkowych, przesyłanych siecią, mogą szybko zablokować pracę małej lub średniej sieci. Z drugiej strony choć protokoły wewnętrzne są znacznie prostsze i generują niewielką ilość danych dodatkowych, nie dają się łatwo skalować do większych sieci. Ponieważ różnica między protokołem wewnętrznym i zewnętrznym jest oczywista, nie będę w tym rozdziale omawiał protokołów zewnętrznych. Dyskusję na temat protokołów zewnętrznych pozostawię do kolejnych rozdziałów, kiedy będziemy omawiali połączenia realizowane z naszej sieci na zewnątrz.

Protokoły dystans-wektor a protokoły stanu łącza

Innym sposobem klasyfikowania dynamicznych protokołów rutowania jest opieranie się na informacjach, jakie przekazują między sobą rutery oraz na sposobie, w jaki wykorzystują one informacje znajdujące się w ich tablicach rutowania. Większość protokołów należy do jednej z wymienionych kategorii.

Pierwsza kategoria to protokoły *dystans-wektor.* W protokołach tego typu ruter regularnie wysyła do swoich sąsiadów dwie części informacji, które posiada na temat adresów przeznaczenia, do których zna drogę. Pierwsza część informacji mówi sąsiadom rutera, jak daleko jest adres przeznaczenia, a druga informuje o tym, w jakim kierunku (wektorze) należy kierować pakiety, aby dotarły do punktu przeznaczenia."[1]" Ruter kolejnego przeskoku wskazuje kierunek, który należy wykorzystać, aby pakiety osiągnęły punkt przeznaczenia, a wymieniana informacja zwykle przyjmuje formę: „wyślij to do mnie, bo ja wiem, jak to przesłać dalej". Na przykład uaktualnienia tras RIP zawierają po prostu listę adresów, do których rozgłaszający je ruter zna trasę, a także odległość, w jakiej te adresy się znajdują. Na podstawie odbieranych uaktualnień inny ruter wnioskuje, że adresem kolejnego przeskoku prowadzącego do danego miejsca w sieci jest rozgłaszający informacje ruter.

*Protokół EIGRP jest powszechnie stosowany w miejsce IGRP, który był jego poprzednikiem. Dzieje się tak dlatego, że EIGRP ma wszystkie zalety elastyczności i jest prostszy w konfigurowaniu, przy jednoczesnej poprawie szybkości działania i zmniejszeniu zapotrzebowania na zasoby. Jest on również w stanie obsługiwać zarówno protokoły IP, jak i niektóre protokoły inne niż IP, co eliminuje potrzebę stosowania kilku protokołów rutowania w sieci, w której pracuje kilka protokołów warstwy transmisji. W dalszej części opisu podkreślę podstawowe różnice pomiędzy obydwoma wspomnianymi protokołami.

+ Matematyczna definicja wektora określa, że musi mieć on kierunek i długość. Niestety, kiedy sieciowcy posługują się określeniem wektora w przypadku protokołów dystans-wektor, to myślą tylko o jego kierunku. Aby uniknąć pomyłek postaram się ograniczyć stosowanie tej nazwy.

Uaktualnienie może jednak przyjąć formę przekazu typu: „prześlij to do innego rutera, który wie, jak się tam dostać". Ta druga forma uaktualnienia jest zwykle wykorzystywana wtedy, kiedy ruter, przez który można dotrzeć do danego miejsca, nie może (lub nie będzie mógł) rozgłaszać informacji z użyciem protokołu rutowania wykorzystywanego przez inne rutery w sieci. Nie wszystkie protokoły rutowania obsługują ten typ uaktualniania tras wykonywany przez stronę trzecią.

Druga część protokołu, którą jest informacja o odległości, stanowi o różnicy między protokołem dystans-wektor a innymi protokołami. W każdym z przypadków protokół używa pewnej *miary, aby* poinformować odbierające informacje rutery o tym, jak daleko jest adres przeznaczenia. Miara ta może być prawdziwym wskaźnikiem określającym odległość (na przykład okresowe sprawdzanie czasu podróży pakietu do miejsca przeznaczenia), czymś, co w przybliżeniu określa odległość (tak jak liczba przeskoków), lub może to być inna wartość nie związana wcale z odległością. Zamiast tego można na przykład mierzyć koszty danej drogi do miejsca przeznaczenia. Określanie tej wartości może być również wykonywane na podstawie skomplikowanych obliczeń, w których brane są pod uwagę czynniki takie jak obciążenie sieci, pasmo łącza, opóźnienie łącza i inne wartości opisujące ruter. Wartość ta może również zawierać wagę, określaną przez administratora sieci w celu wskazania jednej z tras jako preferowanej w stosunku do innych.

W każdym z przypadków wartość miary kosztu pozwala ruterowi wybrać najlepszą trasę ze wszystkich informacji, jakie do niego docierają w postaci rozgłaszanych informacji o trasach. Wybór dokonywany jest na podstawie porównania „odległości" podanej w różnych rozgłaszanych trasach. Sposób, w jaki dokonywane jest to porównanie, zależy od tego, jak liczona lub określana jest wartość przekazywanej miary. Na przykład miary w trasach przekazywanych w uaktualnieniach RIP są określone jako liczba przeskoków, gdzie jeden przeskok oznacza obsługę pakietu przez jeden ruter na drodze do miejsca przeznaczenia. Miejsce przeznaczenia z podaną liczbą przeskoków równą 16 uznaje się za nieosiągalne. Kiedy jakiś ruter odbiera uaktualnienia RIP od różnych ruterów, odnoszące się do tej samej sieci, wybiera trasę, która ma najmniejszą miarę. Jeśli miara ta jest mniejsza od tej, którą przechowuje w swojej tablicy rutowania, ruter wymienia trasę do danej sieci na nową, zakładając, że uzyskane z innego rutera informacje są aktualne.

Aby informacja o trasach do różnych podsieci mogła być propagowana poprzez sieć, każdy ruter umieszcza w rozgłaszanych komunikatach wszystkie kierunki, do których jest bezpośrednio dołączony, a także trasy do miejsc przeznaczenia, o których dowiedział się od innych ruterów. Kiedy ruter zaczyna przekazywać dalej informacje o trasach, o których dowiedział się od innych ruterów, to konieczny jest algorytm wchodzący w skład protokołu rutowania, który dokona odpowiedniego zwiększenia miary dla danej trasy. W przypadku protokołu RIP oznacza to, że zanim ruter rozpowszechni informację, którą wcześniej uzyskał z innego rutera, do metryki każdej z tych informacji dodaje jeden przeskok. Dzięki takiemu algorytmowi miara rośnie, gdy zwiększa się odległość od miejsca przeznaczenia wskazywanego przez zapis w tablicy rutowania.

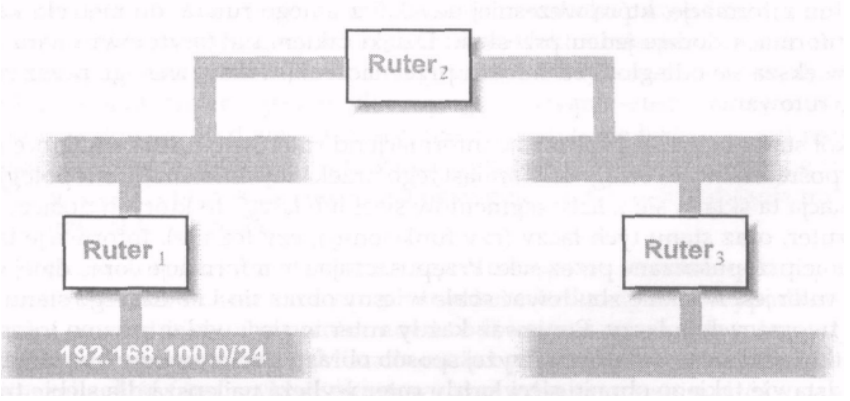
Klasyfikacja dynamicznych protokołów rutowania

Protokół stanu łącza nie przekazuje informacji od ruterów o miejscach, które można za ich pośrednictwem osiągnąć. Zamiast tego przekazuje informację o topologii sieci. Informacja ta składa się z listy segmentów sieci lub *łączy,* do których dołączony jest dany ruter, oraz stanu tych łączy (czy funkcjonują, czy też nie). Informacje takie są następnie przepuszczane przez sieć. Przepuszczając te informacje coraz dalej w sieci każdy ruter jest w stanie zbudować sobie własny obraz sieci i bieżącego stanu wszystkich tworzących ją łączy. Ponieważ każdy ruter w sieci widzi te same informacje, wszystkie stworzone w opisany wyżej sposób obrazy sieci powinny być identyczne. Na podstawie takiego obrazu sieci każdy ruter wylicza najlepszą dla siebie trasę do poszczególnych miejsc w sieci i na tej podstawie tworzy tablicę rutowania. To, w jaki sposób ruter określa, która trasa jest najlepsza, zależy od algorytmu zastosowanego w danym protokole. W najprostszych rozwiązaniach ruter może po prostu policzyć ścieżkę wykorzystując najmniejszą liczbę przeskoków. W bardziej złożonych protokołach informacje o stanie łącza mogą zawierać dodatkowe dane, które pomogą ruterowi określić najlepszą ścieżkę. Informacje takie mogą zawierać dane na temat pasma łącza, bieżącego obciążenia tego łącza, współczynników administracyjnych, a nawet ograniczenia przesyłania niektórych pakietów przez pewne łącza. Na przykład jakieś łącze w sieci może nie być wykorzystywane do przesyłania informacji tajnych.

Protokoły dystans-wektor oraz stanu łącza mają swoje dobre i złe strony. W poprawnie funkcjonującej i skonfigurowanej sieci każdy z tych protokołów poprawnie określi najlepszą trasę pomiędzy dwoma punktami. Nie chcę jednak powiedzieć, że nie należy zastanawiać się nad tym, który z protokołów będzie właściwszy w przypadku konkretnej sieci.

Wady protokołów dystans-wektor

Ogólnie *rzecz* biorąc, protokoły typu dystans-wektor są łatwiejsze w konfigurowaniu niż protokoły stanu łącza. Łatwiej też zrozumieć ich działanie. W mniejszym stopniu obciążają one również procesor, co pozwala ruterowi zająć się innymi zadaniami, takimi jak przełączanie pakietów. Główne wady tych protokołów wynikają często z ich prostej budowy. Jedną z największych wad jest to, że rutery nie przekazują informacji o tym, skąd dowiedziały się o danej trasie, którą umieściły w komunikacie zawierającym uaktualnienia. Rozważmy np. prostą sieć zbudowaną z użyciem trzech ruterów, pokazaną na rysunku 5-3. Ruter1 informuje Ruter2 o sieci 192 .168 .100 . 0/24. Ruter2 będzie oczywiście informował Ruter3 o tej sieci, ale taką samą informację może przekazać również do Rutera1. Rurter3 także może poinformować Ruter2 o tym, że wie, jak dostać się do tej samej sieci, nawet jeśli trasa będzie prowadziła przez Ruter2.



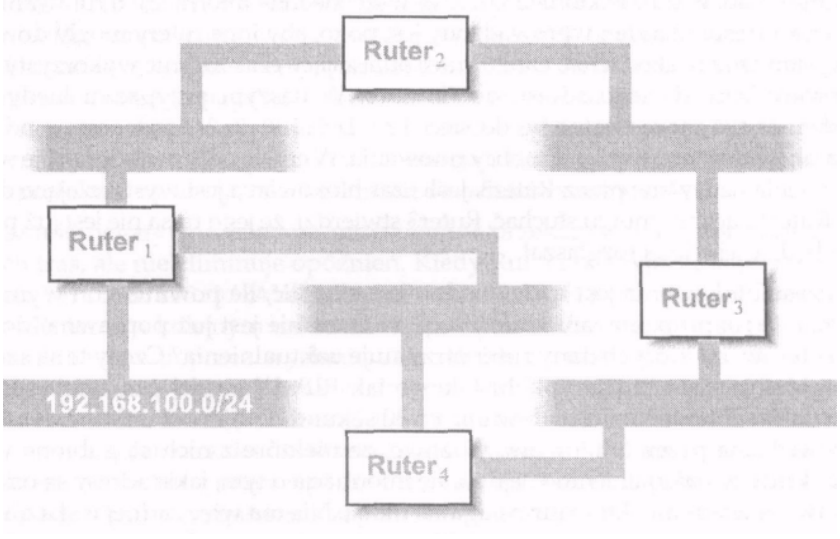
Rysunek 5-3: Prosta sieć złożona z trzech ruterów

Zwykle sytuacja taka nie jest problemem, ponieważ każdy ruter będzie porównywał miary tras, o jakich dowiaduje się z sieci, z miarami tras, które ma zapisane w tablicy rutowania, i na tej podstawie będzie wybierał najkorzystniejszą trasę. Co się jednak stanie, kiedy Ruter1 straci połączenie z siecią 192.168.100.0/24 z powodu uszkodzenia sprzętu? Przestanie ona informować Ruter2 o swoim istnieniu i w końcu zapis trasy do tej podsieci zostanie usunięty z tablicy rutowania tego rutera (trasa zostanie usunięta w wyniku upłynięcia określonego czasu lub na podstawie komunikatu przekazanego przez Ruterl1). Kiedy to nastąpi, Ruter2 może usłyszeć od Rutera3 o istnieniu takiej sieci i doda tę „nową" podsieć do swojej tablicy rutowania, przekazując o tym informację Ruterowi1. Oczywiście informacja wysłana zostanie również do Rutera3, który odkryje, że trasa prowadząca przez Ruter2 jest gorsza od zapisanej poprzednio. Nie zważając na to, ruter uaktualni swoją tablicę rutowania i miarę, z którą będzie teraz rozgłaszał te informacje, wysyłając je do Rutera2. Odebranie tego kolejnego uaktualnienia przez Ruter2 spowoduje, że ogłosi on tę trasę (z trochę gorszą miarą) Ruterowi3, który następnie zwróci informację do Rutera2 z jeszcze większą miarą. W końcu rutery osiągną wartość miary, która jest zdefiniowana w danym protokole jako „nieskończoność". Kiedy to się stanie, wszystkie rutery usuną tę trasę ze swoich tablic rutowania.

W zależności od tego, jak duża jest wartość „nieskończoności" określona w danym protokole, oraz od tego, jak często rutery wysyłają sobie uaktualnienia nawzajem, okres niestabilności i błędnego rutowania pakietów może trwać od kilku sekund do kilku minut. Niewątpliwie nie chcesz, aby tablice rutowania Twoich ruterów były niestabilne przez całe minuty za każdym razem, kiedy uszkodzeniu ulegnie jakaś część sieci! Większość protokołów typu dystans-wektor ma dodatkowe funkcje, które obsługują takie przypadki i zapobiegają przedłużaniu się czasu niestabilności. Pierwszą rzeczą, którą się zwykle dodaje, jest coś, co nazywane jest *domknięciem horyzontu.* W procedurze tej w momencie, kiedy ruter tworzy uaktualnienie dotyczące konkretnego interfejsu, pomija w nim wszystkie odniesienia do tras, których nauczył się od ruterów dostępnych przez ten interfejs.

W naszym przypadku oznacza to, że Ruter2 poinformuje Ruter3 o podsieci 192.168.100.0/2 4, której nauczył się z Rutera1, ale pominie wszelkie odwołania do tej sieci, kiedy będzie wysyłał uaktualnienie do Rutera1. Ruter3 także powstrzyma się od informowania Rutera2 o tej sieci, ponieważ to właśnie od tego rutera uzyskał o niej informacje. Niewielką modyfikacją metody „domkniętego horyzontu" jest metoda „poison reverse". W metodzie tej zamiast pomijania informacji o sieciach, których ruter nauczył się z danego interfejsu, ruter dołącza te informacje do rozsyłanego uaktualnienia, ale dodaje do nich znacznik informujący, że taka sieć jest nieosiągalna. Taka informacja powoduje, że odbierający ją ruter posługujący się niewłaściwą trasą może ją usunąć ze swojej tablicy rutowania.

Wynikiem działania w sieci opisanych wyżej metod jest fakt, że prosta niestabilność sieci opisana wcześniej nie może się w tej sieci zdarzyć. Niestety, ani jedna, ani druga metoda nie rozwiązują wszystkich problemów. Jeśli w sieci jest przejście łączące Ruter1 z Ruterem3, być może przez Ruter4, jak pokazano na rysunku 5-4, możliwe jest wystąpienie pętli rutowania, nawet jeśli uruchomione są algorytmy opisanych wyżej metod. W takiej sieci Ruter1 informuje Ruter2 i Ruter4 o swoim połączeniu z siecią 192.168.100.0/2 4, podając w obu przypadkach prawdopodobnie taką samą wartość miary. Rutery te z kolei poinformują Ruter3 o trasie prowadzącej do tej sieci, stosując prawdopodobnie tę samą miarę. Ruter3 wybierze jedną z tych tras (prawdopodobnie tę, którą odbierze jako pierwszą) i umieści ją w swojej tablicy rutowania.



Rysunek 5-4: Standardowe metody nie zapobiegają występowaniu pętli rutowania w sieciach, w których połączenia tworzą pierścień

Załóżmy, że Ruter3 wybierze trasę prowadzącą przez Ruter2. Ponieważ działa metoda „poison reverse", zgodnie z logiką działania tej metody wyśle on informację o tej trasie do Rutera2 z miarą informującą o tym, że adres jest nieosiągalny.

Ponieważ jednak zdecydował, że nie używa trasy prowadzącej przez Ruter4, nie zastosuje wymienionej wyżej metody dla tego łącza, ale zamiast tego dołączy trasę do sieci 192.168.100.0/24 przez Ruter2 do uaktualnienia wysyłanego do Rutera4, który z kolei zignoruje to uaktualnienie i wybierze trasę prowadzącą przez Ruter1.

Wszystko będzie działało dobrze do czasu, kiedy łącze pomiędzy Ruterem1 i siecią 192.168.100.0/24 nie ulegnie uszkodzeniu. Wtedy Ruter1 przestanie rozgłaszać tę trasę do Rutera2 i Rutera4. Rutery te z kolei przestaną rozgłaszać trasę do Rutera3, ale możliwe jest, że Ruter4 usłyszy komunikat rozgłoszeniowy od Rutera3, zanim opisany wyżej proces dobiegnie końca. Ponieważ ruter ten nie ma informacji o trasie w swojej tablicy rutowania, umieści ją tam i poinformuje Ruter1, że ma nową trasę. Następnie, zgodnie z działaniem algorytmu, Ruterl1 poinformuje o tej trasie Ruter2, który prześle informację dalej, do Rutera3.

Pętla ta zostanie w końcu przerwana, kiedy każdy z ruterów, zwiększając miarę przy każdym przesyłaniu informacji o trasie w pętli, zwiększy ją do pewnej granicznej wartości dla danego protokołu, którą określaliśmy wcześniej jako wartość „nieskończoności". Ile czasu zajmie ruterom tak zwane „odliczanie do nieskończoności", zależy w dużym stopniu od tego, jak często wymieniają między sobą uaktualnienia, jaka jest wartość graniczna dla używanego w sieci protokołu i ile ruterów uczestniczy w tej pętli. Rozwiązaniem opisanego problemu jest wprowadzenie czasu *blokowania.* Kiedy ruter dowie się, że jakiś adres nie jest już dostępny dla ścieżki, której używał wcześniej, rozpoczyna odliczanie czasu, w trakcie którego ignoruje wszelkie inne informacje o nitowaniu dotyczące tego adresu. Czas ten wprowadzony jest po to, aby inne rutery mogły dowiedzieć się o wystąpieniu uszkodzenia, zanim ruter odliczający czas zacznie wykorzystywać ich trasy prowadzące do tego adresu docelowego. W naszym przypadku kiedy Ruter1 stwierdza, że nie może dostać się do sieci 192.168.100.0/24, rozpoczyna odliczanie czasu blokowania tego zapisu w tablicy rutowania. W czasie odliczania ignoruje wszelkie uaktualnienia nadsyłane przez Ruter3. Jeśli czas blokowania jest wystarczająco długi, to zanim Ruter1 *zacznie* znowu słuchać, Ruter3 stwierdzi, że jego trasa nie jest już poprawna i nie będzie jej więcej rozgłaszał.

Wadą czasu blokowania jest to, że trudno jest określić, ile powinien on wynosić. Ile czasu zajmie rozpropagowanie informacji, że trasa nie jest już poprawna, do wszystkich ruterów, od których dany ruter otrzymuje uaktualnienia? Czasy te są szczególnie długie w przypadku protokołu takiego jak RIP. W swojej prostszej wersji RIP rozsyła uaktualnienia tablicy rutowania co 30 sekund. Ponieważ uaktualnienia te nie są potwierdzane przez odbiorców, możliwe, że niektóre z nich są gubione w sieci. Ponadto kiedy w uaktualnieniu znajduje się informacja o tym, jakie adresy są osiągalne, to nie zawsze wiadomo, które już osiągalne nie są. Nie ma więc żadnej wskazówki dla rutera, że powinien usunąć ze swojej tablicy rutowania trasę, która nie jest już dłużej poprawna.

Aby umożliwić wykrywanie zagubionych w sieci uaktualnień, RIP ustawia *zegar* dla każdej trasy, której się nauczył. Za każdym razem, kiedy RIP słyszy uaktualnienie dotyczące tej trasy, zegar jest zerowany. Jeśli ruter nie odbierze uaktualnienia w ciągu 180 sekund, usuwa trasę ze swojej tablicy rutowania i przestaje rozgłaszać ją swoim sąsiadom.

W rezultacie jeśli jakieś uaktualnienie zostanie zagubione, rutery nie będą natychmiast usuwały tras ze swoich tablic rutowania. Prawdopodobnie trasy te znajdą się w kolejnym uaktualnieniu i ich zegary zostaną wyzerowane.

W praktyce procedura opisana wyżej oznacza, że rozgłoszenie zmiany w topologii sieci i zapisanie jej w tablicach rutowania wszystkich ruterów, które w tej sieci pracują, może zająć sporo czasu. Zastanów się jeszcze raz nad działaniem sieci z trzema ruterami, pokazanej na rysunku 5-3. Kiedy Ruter1 stwierdzi, że utracił połączenie z siecią 192.168.100.0/24, to po prostu przestał rozgłaszać tę sieć w swoich uaktualnieniach wysyłanych do Rutera2 Mimo to przez kolejne 3 minuty od ostatniego komunikatu Ruter3 nadal wierzył, że ma trasę prowadzącą do tej sieci i wysyłał informację o tym w uaktualnieniach kierowanych do Rutera3 Po trzech minutach Ruter2 stwierdza, że Ruter1 musiał utracić tę trasę i usuwa zapis trasy do sieci 192.168.100.0/24 ze swojej tablicy rutowania, informując o tym Ruter3. Mimo to Ruter3 nadal będzie wykorzystywał starą, nieaktualną już informację przez kolejne trzy minuty.

Rozważmy teraz, co się będzie działo, jeśli taka procedura odliczania czasów na kolejnych ruterach wykonywana będzie w sieci składającej się z kilkunastu ruterów. Jeśli każdy z ruterów musi odczekać trzy minuty od czasu, kiedy najbliższy mu ruter przestał rozgłaszać daną trasę, to oczywiste staje się, że trasa może nie zniknąć całkowicie z sieci przez około 45 minut! Nierozsądne jest więc określanie tak długiego czasu blokowania rekordów w tablicy rutowania. Czas ten powinien stanowić niewielką część tych trzech minut. Aby redukować czas, kiedy w sieci występuje stan niespójności informacji o rutowaniu, protokół dystans-wektor umożliwia ruterom rozsyłanie informacji o *osiągalności negatywnej* dla tras, które zostały przez te rutery rozgłoszone, ale nie są już dłużej osiągalne. Informacje takie pozwalają ruterom na szybkie stwierdzenie faktu, że jakaś trasa nie jest dłużej dostępna. Dla protokołu RIP informacja o negatywnej osiągalności jest po prostu informacją o trasie z miarą ustawioną na wartość 16. Inne protokoły oznaczają taką informację we właściwy sobie sposób.

Rozgłaszanie negatywne pomaga przyspieszyć przekazywanie informacji o uszkodzeniach tras, ale nie eliminuje opóźnień. Kiedy Ruter1 odkryje, że jego połączenie z podsiecią 192.168.100.0/24 zostało przerwane (lub odtworzone), przekaże tę informację do Rutera2 w kolejnym uaktualnieniu. W przypadku stosowania protokołu RIP jest to realizowane poprzez wysłanie uaktualnienia i może upłynąć do 30 sekund, zanim zostanie ono wygenerowane. Ponadto jeśli Ruter2 dostanie wiadomość od Rutera1, to może również odczekać do 30 sekund, zanim powiadomi o zmianie Ruter3, który z kolei odczeka do 30 sekund itd. Nawet jeśli informacja o zmianie stanu łącza przesłana zostanie przez sieć dość szybko, zwłaszcza w porównaniu z czasem, jaki jest potrzebny do wygaśnięcia zapisu w tablicy rutowania, to nadal może to zająć kilka minut, zanim wszystkie rutery w sieci dowiedzą się o tej zmianie i odpowiednio uaktualnią swoje tablice rutowania. Opóźnienie pomiędzy czasem wystąpienia zmiany stanu łącza w sieci a chwilą, kiedy wszystkie rutery w tej sieci dopasują swoje tablice rutowania, określane jest mianem *czasu zbieżności*. Długi czas zbieżności jest niewątpliwie problemem dla każdego protokołu rutowania.

Aby zminimalizować czas konwergencji, protokół dystans-wektor może uruchomić wysyłanie uaktualnień *typuflash* lub *triggered.* Uaktualnienie *tńggered* wysyłane jest za każdym razem, kiedy tablica rutowania danego rutera zmieni się w sposób, który może wpływać na rozsyłanie uaktualnień innych tras tego rutera. Jeśli każdy ruter używa uaktualnień tego typu i umieszcza w nich informacje o negatywnej osiągalności, to możliwe jest, że informacja o uszkodzeniu połączenia z Rutera1 do sieci 192 .168.100.0/24 zostanie przekazana do wszystkich ruterów pracujących w sieci w ciągu kilku sekund. Dzięki temu znacznie zmniejszy się czas zbieżności oraz czas, jaki ruter odczekuje przed usunięciem zapisu z tablicy rutowania.

Ten mechanizm nie jest prosty. Jeśli dodatkowe uaktualnienia nie będą dokładnie kontrolowane, to chwilowe uszkodzenie może powodować rozsyłanie w sieci tam i z powrotem różnych uaktualnień, co będzie zajmowało pasmo i moc obliczeniową procesorów w ruterach, które będą się zajmowały przetwarzaniem uaktualnień, a nie przełączaniem pakietów. Powszechnie stosowanym rozwiązaniem jest nieznaczne wydłużenie czasu odczekiwania przed usunięciem zapisu z tablicy rutowania oraz dodanie krótkiego czasu oczekiwania, który ustawiany jest po każdym uaktualnieniu typu *flash.* W czasie tego oczekiwania ruter nie przyjmuje żadnych innych uaktualnień, co pomaga złagodzić efekty faktycznych uszkodzeń. ;

Kolejną dużą wadą protokołu typu dystans-wektor jest wada wynikająca z faktu, że nie jest to protokół zbyt skomplikowany. Ponieważ topologia sieci może ulec zmianie, w wyniku uszkodzenia łącza lub dodania albo usunięcia segmentu sieci, wszystkie dynamiczne protokoły rutowania muszą przekazywać do ruterów informacje o tych zmianach. W protokole dystans-wektor uaktualnienia wykonywane są zwykle poprzez okresowe rozsyłanie pakietów typu broadcast (lub multicast) poprzez niektóre lub wszystkie interfejsy rutera. Często uaktualnienia te zawierają pełną informację o rutowaniu, którą posiada ruter wysyłający to uaktualnienie. Okresowe uaktualnienia są przydatne, gdyż pozwalają ruterom pracującym w danym segmencie sieci informować się wzajemnie. Niestety, komunikaty te generują dodatkowy ruch w sieci nawet wtedy, kiedy sieć pracuje stabilnie (co, mamy nadzieję, stanowi większość czasu pracy sieci). Niektóre nowsze protokoły dystans-wektor, takie jak Cisco EIGRP, rozgłaszają tylko zmiany zachodzące w tablicach rutowania, ale protokół ten nadal jest rzadko stosowany.

Podczas gdy protokół dystans-wektor jest raczej nieskomplikowany oraz łatwy w obsłudze dla procesora rutera, prostota ta może prowadzić do nietypowych zachowań w wyniku uszkodzeń sieci i długich czasów zbieżności sieci. W sieci obsługiwanej przez ten protokół czas pomiędzy wystąpieniem uszkodzenia jednego z komponentów sieci a ustaleniem trasy obejściowej obsługiwanej przez poprawnie pracujące rutery może być dość długi. Działanie tego protokołu może również prowadzić do dużego wykorzystania pasma sieci i znacznego obciążenia procesora rutera nawet wtedy, gdy sieć pracuje stabilnie. Choć zmiany dokonywane w samym protokole mogą zmniejszyć te problemy, to po dodaniu dodatkowych funkcji rozgłaszania, obsługi czasów oczekiwania itd. protokół przestanie być zrozumiały i nieskomplikowany i znacznie trudniej będzie śledzić jego działanie.

Wady protokołów stanu łącza

Protokoły stanu łącza mają kilka ważnych zalet. Ponieważ obliczają trasy rutowania na podstawie znajomości topologii sieci, o której dowiadują się z uaktualnień informujących go o stanie łączy, nie mogą tworzyć pętli w wyniku częściowego uszkodzenia sieci, jak to zdarzało się w przypadku protokołów typu dystans-wektor. Ponieważ zmiany stanu łączy przekazywane są przez sieć natychmiast po ich wystąpieniu i docierają do wszystkich ruterów, które następnie uaktualniają swoje mapy topologii i tablice rutowania, to czas zbieżności sieci obsługiwanej przez taki protokół jest minimalny. Ostatnią zaletą, o której należy wspomnieć, jest fakt, że większość protokołów stanu łącza jest opracowana tak, by wysyłała uaktualnienia stanów łącza tylko wtedy, kiedy stan ten się zmieni, co sprawia, że protokoły tego typu oszczędzają pasmo i moc procesorów w czasie, kiedy sieć jest stabilna. .

Choć protokoły stanu łącza zapobiegają powstawaniu pętli, skracają czasy zbieżności sieci i stopień wykorzystania zasobów sieci, mają też wady. Główną wadą jest ich złożoność. Złożoność jest głównym aspektem implementacji protokołu, ale często daje o sobie znać również podczas konfigurowania sprzętu. Tak naprawdę protokół OSPF, uważany za protokół wewnętrzny, jest znacznie bardziej skomplikowany od BGP, który stosowany jest jako protokół zewnętrzny. Na szczęście w typowej konfiguracji większość skomplikowanych funkcji ukryta jest przed użytkownikiem.

Dlaczego protokół stanu łącza jest tak złożony? Rozważmy jeszcze raz to, co mówiliśmy o sposobie, w jaki rutery określają swoje trasy. Zbierają one wszystkie uaktualnienia stanów łącza nadsyłane przez inne rutery i na ich podstawie budują mapę topologii sieci. Wykorzystując tę mapę rutery obliczają następnie najlepsze trasy do różnych miejsc w sieci. Pierwszym problemem jest generowanie mapy topologii. Choć człowiek może dość szybko narysować mapę połączeń sieci, bazując na informacjach o tym, co jest z czym połączone, to komputer musi mieć jakiś sposób zapisu tego ludzkiego rysunku w elektronicznej formie pozwalającej na dalsze przetwarzanie tych informacji. Standardowym sposobem zapisu tych informacji jest wykorzystanie jednego z wielu rodzajów grafów sieci. Każdy rodzaj grafów ma pewien zestaw działań, które dobrze obsługuje, i zestaw funkcji, których nie obsługuje prawie wcale. Przeprowadzono wiele badań w celu opisania różnych typów grafów i funkcji, które te grafy obsługują. Bardzo często specyfikacja protokołu nie określa sposobu, w jaki ma być on implementowany. Możliwe, że w specyfikacji nie określa się nawet rodzajów danych, jakie będą konieczne do poprawnej pracy tego protokołu. Nawet jeśli rodzaje danych określone są w specyfikacji, to sposób w jaki dane te są reprezentowane (tzn. jaki rodzaj grafu zostanie użyty) pozostawia się temu, kto implementuje protokół. Zły wybór grafu może doprowadzić do trudno rozpoznawalnych uszkodzeń i błędów w kodzie oprogramowania rutera.

Drugą trudnością związaną z implementacją protokołu stanu łącza jest sposób liczenia najlepszej trasy do wszystkich miejsc w sieci. Choć istnieją algorytmy obliczające najlepszą ścieżkę za pomocą różnych typów grafów i miar, to nadal jest to kwestia odpowiedniej implementacji. Popełnione w procesie implementacji błędy dają ciekawe rezultaty w czasie działania produktu końcowego, jakim jest protokół rutowania w sieci.

Złożoność implementacji nie powinna być jednak przedmiotem zainteresowania administratora sieci, jeśli kod wynikowy, jaki otrzymał wraz z ruterami, działa poprawnie. Nawet jeśli kod jest poprawny, to skomplikowana implementacja wymaga zwykle większej mocy procesora i większej pamięci w ruterze. Na przykład wygenerowanie grafu topologii będzie zajmowało trochę czasu, a graf ten należy przecież jeszcze gdzieś zapisać. Musi on być przechowywany w dość bezpiecznym miejscu, ponieważ uaktualnienia stanu łączy zawierają tylko informacje o zmianach, jakie nastąpiły w topologii sieci. Dodatkowe wymagania dotyczące pamięci i mocy procesora sprawiają, że niektórzy administratorzy sieci trzymają się z dala od protokołów stanu łącza, ale nie jest to jedyny powód takiego postępowania. Ważniejszym powodem jest złożoność tych protokołów lub założenie, że są one skomplikowane i trudno je konfigurować.

Większość protokołów stanu łącza jest znacznie trudniejsza w konfiguracji niż protokoły typu dystans-wektor. Jeśli jednak interfejs konfiguracyjny jest dobrze zaimplementowany i jeśli zawiera zestaw właściwie określonych parametrów domyślnych, to możliwe jest skonfigurowanie protokołu stanu łącza przy niewiele większym nakładzie pracy niż dla protokołu dystans-wektor. Jeśli w procesie konfiguracji będziesz trzymał się wartości domyślnych, to konfiguracja tego protokołu nie powinna nastręczać większych trudności.

Zarówno protokół stanu łącza, jak protokół dystans-wektor będą działały poprawnie, jeśli rutowanie w stabilnej sieci będzie bezbłędne. Powinny one ponadto zmienić rutowanie na inne w sytuacji, kiedy w sieci wystąpi jakieś uszkodzenie. Dlatego też protokół, który wybierzesz dla swojej sieci, zależy głównie od Twoich prywatnych preferencji. Jeśli złożoność protokołu stanu łącza nie jest tym, co lubisz, lub jeśli jesteś zainteresowany zmniejszeniem wykorzystania zasobów w Twoich ruterach, spróbuj wybrać jeden z protokołów stosujących algorytm dystans-wektor. Jeśli z drugiej strony chcesz uzyskać w sieci krótkie czasy zbieżności i małe zużycie pasma gwarantowane przez protokół stanu łącza lub nie chcesz zajmować się rozwiązywaniem problemów wynikających z powstawania pętli rutowania, to powinieneś wybrać jeden z rodziny protokołów stanu łącza.

Wybór protokołu rutowania

Teraz, kiedy mamy za sobą omówienie większości podstawowych informacji na temat dynamicznych protokołów rutowania, nadszedł czas na rozważenie kryteriów, które należy rozważyć przy wyborze dynamicznego protokołu rutowania. Możesz wybrać protokół stanu łącza lub protokół dystans-wektor, ale pamiętaj, że nierozważna decyzja może w dużym stopniu ograniczyć Twój wybór i uzależnić go od tego, jakie protokoły obsługuje sprzęt wybranego przez Ciebie dostawcy. Znacznie lepiej jest zastanowić się, jaki protokół lub protokoły będą najlepiej obsługiwały Twoją sieć, a następnie posłużyć się preferencjami jako czynnikiem dodatkowym, a nie decydującym.

Wybór protokołu ratowania

Jednym z podstawowych kryteriów jest to, jak szybko dany protokół adaptuje się do zmian występujących w sieci. Wcześniej określiliśmy ten czas jako czas zbieżności i powiedzieliśmy, że jest to okres pomiędzy wystąpieniem zmiany w topologii sieci a odtworzeniem spójnych i poprawnie rutujących tablic rutowania na wszystkich ruterach w sieci. Najlepiej, gdy czas ten jest na tyle krótki, aby nie został zauważony przez użytkowników sieci.

Zwykle kolejnym ważnym kryterium jest wykorzystywanie zasobów. W związku z występującym trendem lepszego wykorzystania przestrzeni adresowej IP jest bardzo prawdopodobne, że planujesz wykorzystanie w podsieciach masek o zmiennej długości. Jeśli tak, zdolność ich obsługi jest prawdopodobnie najważniejszą funkcją, którą musi obsługiwać wybrany przez Ciebie protokół rutowania. Jeśli protokół nie będzie obsługiwał wykorzystywanych przez Ciebie masek, nie przyda Ci się w sieci.

Trzecim kryterium, które powinieneś przeanalizować, to ilość zasobów sieci wykorzystywanych przez protokół rutowania. Zastanów się nie tylko nad wykorzystaniem pasma sieci przez komunikaty protokołu, ale również nad tym, ile mocy procesora i pamięci wymagane jest dla tego protokołu na Twoich ruterach. Protokoły stanu łącza będą zwykle lepsze z punktu widzenia wykorzystania pasma, a protokoły dystans-wektor będą korzystniejsze z punktu widzenia wykorzystania mocy procesora i zajętości pamięci, choć czasem może być inaczej.

Następnie powinieneś rozważyć, jak wybierany przez Ciebie protokół radzi sobie z kilkoma trasami prowadzącymi do jednego miejsca w sieci. Może to być niezwykle istotne dla pracy Twojej sieci, a zależy to od tego, jaką sieć zaprojektowałeś. Jeśli nie masz w swojej sieci redundantnych połączeń, to nie będziesz prawdopodobnie zwracał uwagi na to, jak dobrze wybrany przez Ciebie protokół obsługuje takie trasy. Mimo że nie masz ich obecnie, to możliwe jest, że dodasz je w przyszłości i na pewno nie chcesz, aby wystąpiła konieczność zmiany protokołu rutowania w całej sieci w związku z tymi nowymi połączeniami. Nawet jeśli jeden z wybieranych przez Ciebie protokołów nie obsługuje redundantnych połączeń, to sprawdź, czy implementacja tego protokołu dokonana przez producenta ruterów nie ma takiej funkcji. Na przykład protokół RIP w zwykłej wersji nie obsługuje kilku ścieżek do sieci docelowej, ale implementacja RIP wykonana przez Cisco obsługuje taką redundancję, a nawet potrafi rozdzielać ruch pomiędzy dwa łącza, które mają jednakowy koszt (miarę).

Możliwe, że będziesz musiał również rozważyć skalowalność wybieranego protokołu do rozmiarów sieci, jakie spodziewasz się osiągnąć w przyszłości. Protokoły stanu łącza skalują się zwykle lepiej od protokołów dystans-wektor, ale kilka z tych ostatnich, jak na przykład Cisco EIGRP, udowodniły swoją przydatność w sieciach złożonych z 1000 lub większej liczby ruterów.

Powinieneś też rozważyć również to, czy protokół jest standardem otwartym, czy też protokołem firmowym. Konieczność stosowania standardów może wynikać z polityki Twojej firmy lub z faktu, że protokół będzie obsługiwał rutery pochodzące od kilku różnych producentów. Protokół, którym potrafi rozmawiać tylko połowa Twoich ruterów, nie jest zbyt użyteczny. W tabeli 5-1 podsumowano opisane wyżej kryteria i opisano, jak spełniają je powszechnie stosowane protokoły rutowania, które prawdopodobnie będziesz chciał zastosować w swojej sieci.

Tabela 5-1. Podsumowanie funkcji powszechnie stosowanych protokołów rutowania

Protokół	*RIP*	*OSPF*	*IGRP*	*EIGRP*
Rodzaj	dystans-wektor	link-state	dystans-wektor	dystans-wektor
Czas zbieżności	wolny	szybki	wolny	szybki
VLSM	nie	tak	nie	tak
Wykorzystanie pasma	duże	małe	duże	małe
Wykorzystanie zasobów	małe	duże	małe	małe
Obsługa wielu połączeń równoległych	nie[a]	tak	tak	tak
Dobra skalowalność	nie	tak	tak	tak
Czy firmowy	nie	nie	tak	tak
Rutowanie protokołów innych niż IP	nie	nie	nie	tak

[a] Niektórzy producenci obsługują połączenia równoległe w swoich implementacjach RIP.

Na podstawie tej tabeli może się wydawać, że EIGRP jest idealnym wyborem. Jest on szybki, zużywa niewiele zasobów, obsługuje VLSM i dobrze się skaluje. Jest to jednak prywatny protokół i jeśli nie masz ruterów Cisco Systems, to nie będziesz mógł go wykorzystywać. Będziesz musiał wybrać kilka protokołów rutowania, które obsłużą sprzęt od różnych producentów i powinieneś pamiętać, że złożoność systemu, w którym pracuje kilka protokołów, jest ważną kwestią. Zanim więc podejmiesz decyzję, przyjrzyj się dokładnie firmowym rozwiązaniom lub poszczególnym implementacjom protokołów.

Kiedy już dokonasz wyboru protokołu lub uda Ci się przynajmniej ograniczyć listę możliwości do dwóch, to oznacza, że nadszedł czas na przemyślenie sposobu konfiguracji tego protokołu. Konfiguracja protokołu powinna być przeprowadzona w taki sposób, aby cele stawiane przed Twoją siecią zostały spełnione i aby nie dopuścić do powstawania problemów. Kolejny rozdział zawiera opis kilku typowych scenariuszy, które mogą Ci się przydać, a także pokazuje sposoby wykorzystania każdego z wymienionych w tabeli 5-1 protokołów w typowej sieci. Analizując te przykłady możesz odkryć, że wybrany przez Ciebie protokół może sprawiać pewne trudności z rozwiązaniem niektórych problemów występujących w Twojej sieci. Jeśli nadal masz możliwość wyboru jednego z dwóch lub trzech protokołów, jakie pozostały na Twojej skróconej liście, to dzięki opisanym w kolejnym rozdziale przykładom możesz wybrać ten, który najlepiej spełni wymagania stawiane sieci.

6

Konfiguracja protokołu rutowania

Podstawy konfiguracji
Rozgłaszanie tras statycznych
Użycie zmiennej długości masek podsieci w klasowym protokole rutowania
Zapasowe trasy statyczne
Ograniczone rozgłaszanie tras
Ograniczanie źródeł informacji o rutowaniu
Filtrowanie określonych tras z informacji uaktualnienia
Rutowanie dynamiczne z użyciem wielu ścieżek
Jednoczesne użycie wielu protokołów rutowania

Gdy wybrałeś już protokół rutowania lub przynajmniej ograniczyłeś liczbę protokołów, które będziesz stosował, musisz skonfigurować swoje rutery tak, by obsługiwały ten protokół. Niewątpliwie przekonasz się, że domyślne ustawienia rutera, wykonane przez producenta, będą wystarczające w większości przypadków. Czasami jednak nie będą spełniały Twoich oczekiwań. Być może konieczne będzie skonfigurowanie rutera tak, by obsługiwał specjalne przypadki występujące w Twojej sieci. W tym rozdziale zaprezentuję kilka najczęściej stosowanych przypadków, z którymi prawdopodobnie się spotkasz, i przedstawię sposoby skonfigurowania rutera do ich obsługi, z wykorzystaniem protokołów RIP, OSPF i EIGRP.*

Nie będę przedstawiał konfiguracji EIGRP. EIGRP jest zastępowany przez IGRP w związku z lepszymi osiągami tego ostatniego i powinien być stosowany zamiast IGRM wszędzie, gdzie to możliwe. Łatwo można zaadaptować konfigurację opartą na protokole EIGRP do pracy z IGRP, ponieważ różnice w konfiguracji obu protokołów są niewielkie.

Mimo że przykładowe konfiguracje bazują na języku, którym konfiguruje się rutery Cisco, to koncepcja zastosowana w tych przykładach może być zastosowana do każdego innego rutera. Pamiętaj o tym, że opisywane przykłady prezentują tylko jedno rozwiązanie każdego z problemów. Nie obiecuję, że przykłady będą dobre do każdej ze spotykanych w sieci sytuacji: może się nawet zdarzyć, że wcale nie będziesz mógł ich użyć w swojej sieci.

Podstawy konfiguracji

Zanim zaprezentuję konfiguracje właściwe do zastosowania w specjalnych przypadkach lub do rozwiązania określonych problemów, określę kilka podstawowych konfiguracji, które będą podstawą do zastosowania bardziej zaawansowanych rozwiązań. Te podstawowe konfiguracje zawierają minimum konieczne do poprawnego funkcjonowania każdego z protokołów rutowania i nie mogą być stosowane w żadnej, poza najprostszymi, sieci. Ich zaletą jest jednak to, że dosyć łatwo jest je zrozumieć.

RIP

Aby zaprezentować podstawową konfigurację wykorzystującą protokół RIP, użyjmy dwóch sieci 172.16.0.0/151192.168.100.0/24. Konfiguracja przedstawiona poniżej rozpoczyna się od polecenia uruchamiającego na ruterze proces RIP. Następnie ruter otrzymuje informację o sieciach, do których powinien wysyłać i z których powinien odbierać uaktualnienia tras RIP. Ponieważ RIP jest protokołem klasowym, nie jest możliwe podanie jednym poleceniem informacji o zagregowanych sieciach 172.16.0.0/15; zamiast tego podajemy polecenie network dla każdej z sieci klasy B tworzących sieć zagregowaną (172.16.0.0 i 172.17.0.0). Taki sposób zapisu sieci nie ogranicza tras, jakie mają być obsługiwane do i z tego rutera, informuje tylko, które z bezpośrednio dołączonych do rutera sieci skonfigurowane będą do obsługi przez RIP.

```
! start a RIP process on my networks
router rip
 network 172.16.0.0
 network 172.17.0.0
 network 192.168.100.0
```

OSPF

Nasza sieć obsługiwana przez OSPF składa się również z sieci 172.16.0.0/15 i 192 .168.100 .0/24. Konfiguracja tej sieci rozpoczyna się także od polecenia ruterowi, aby uruchomił obsługę procesu rutowania OSPF. Liczba występująca po poleceniu router ospf identyfikuje numer procesu OSPF, który jest uruchamiany, ponieważ jeden ruter może obsługiwać wiele procesów OSPF. Powinno się konsekwentnie używać tego samego numeru na wszystkich ruterach uczestniczących w obsłudze OSPF w danej sieci.

Podstawy konfiguracji

```
! start on OSPF process and place all interfaces in area 0
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
```

Drugi wiersz tej konfiguracji zawiera deklarację, że wszystkie interfejsy sieciowe nie-dołączone do innych obszarów (wyjaśnienie znajduje się niżej) powinny być przypisane do obszaru 0. Maska użyta w tym poleceniu network różni się od masek, z którymi stykaliśmy się dotychczas w tej książce. W tak zapisanej masce bit l jest gwiazdką i określa, że odpowiadający mu bit w adresie może wynosić albo jeden, albo zero. Tak więc maska 255.255.255.255 określa w*szystkie* adresy, a polecenie network umieszcza wszystkie interfejsy w obszarze 0. Jeśli konieczne będzie określenie innych obszarów, to będą one zdefiniowane za pomocą takich samych instrukcji network, z których każda będzie zawierała numer sieci i maskę, definiujące zbiór interfejsów sieciowych, i przypisze je do odpowiedniego obszaru. Każdy z interfejsów może znajdować się tylko w jednym obszarze; lista obszarów przeglądana jest w kolejności i każdy interfejs przypisywany jest do pierwszego obszaru, który odpowiada zdefiniowanemu dla tego interfejsu numerowi.

Obszary OSPF

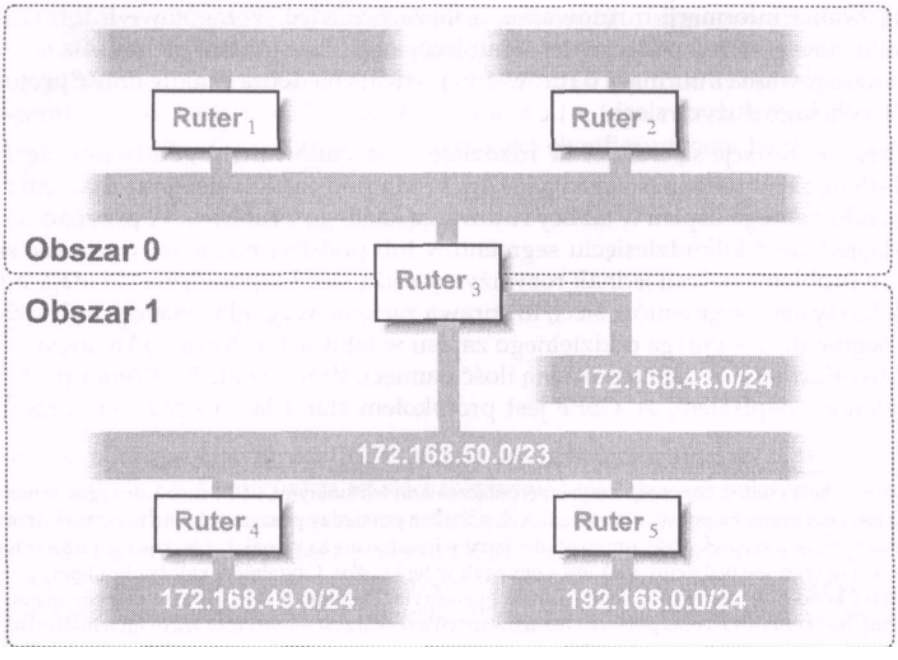
W przeciwieństwie do innych protokołów rutowania, o których będę mówił, OSPF działa w oparciu o koncepcję obszarów. Obszar to oddzielna ciągła część sieci, której szczegóły wewnętrznej topologii nie są widoczne przez rutery znajdujące się poza tym obszarem.* Obszary pozwalają na wprowadzenie dodatkowego poziomu hierarchii sieci, różnej od tej, którą zapewniają klasy sieci IP, i mogą być używane do agregowania informacji o rutowaniu, a także posiadać szczegółowe informacje na temat elementów wchodzących w skład całej sieci. Ta zdolność ukrywania szczegółów i agregowania informacji o rutowaniu pozwala na dobrą skalowalność protokołu OSPF i obsługę dużych sieci.

Dlaczego te funkcje są ważne? W rozdziale I, zatytułowanym „Podstawy sieci IP", napisałem, że w większości przypadków każda podsieć lub sieć przeznaczenia wymaga oddzielnego zapisu w tablicy rutowania każdego z ruterów. W przypadku sieci składającej się z kilkudziesięciu segmentów lub podsieci może nie wydawać się to jeszcze problemem. Jeśli jednak rozważymy dużą sieć korporacyjną składającą się z setek lub tysięcy segmentów sieci, to sprawa zaczyna wyglądać inaczej. Jeśli każdy z tych segmentów wymaga oddzielnego zapisu w tablicach rutowania każdego z ruterów, to informacje te zajmą pokaźną ilość pamięci.

*Dzięki wykorzystaniu koncepcji nazywanej połączeniami wirtualnymi, OSPF może obsługiwać nieciągły obszar sieci tworzony na podstawie wirtualnych połączeń pomiędzy poszczególnymi częściami tworzącymi obszar tej sieci. W większości przypadków łącza wirtualne nie są jednak konieczne i ich użycie nie jest zalecane, tak więc nie będziemy się nimi zajmowali w tej książce. Czytelnicy, którzy chcą lepiej poznać i zrozumieć koncepcję sieci wirtualnych, powinni przeczytać dokument RFC 1583, w którym znajduje się definicja protokołu OSPF i opis połączeń realizowanych z wykorzystaniem łączy wirtualnych. Aby uzyskać szczegółowe informacje o tym, jak zestawić takie połączenia w swojej sieci, powinieneś zajrzeć do dokumentacji swych ruterów.

W rozdziale 5, „Wybór protokołu rutowania", napisałem, że OSPF jest protokołem stanu łącza i przesyła przez sieć informacje o wszystkich segmentach sieci. Kiedy informacja o topologii sieci zostanie odebrana *przez* inne rutery, *zaczną* one wyliczać najkrótsze trasy prowadzące do każdego z segmentów sieci. Jeśli takich segmentów sieci będzie tysiące i będą one dołączone do ruterów *przez* kilkaset przyłączy, to liczba obliczeń wykonywanych *przez* każdy z ruterów nie będzie bez znaczenia. Co najgorsze, jeśli zmieni się stan choć jednego łącza w sieci, to wszystkie rutery będą musiały przeliczyć od nowa najkrótszą trasę do *wszystkich* docelowych podsieci.

Obszar OSPF może być więc użyty do zawężenia informacji o trasach wewnątrz podsieci oraz o wewnętrznej topologii sieci do tych ruterów, które dołączone są do tego obszaru. Wszystkie pozostałe rutery widzą po prostu zagregowaną trasę obejmującą wiele podsieci, a cała sieć postrzegana jest jako zamknięta całość, której wewnętrznej struktury rutery te nie znają i nie muszą się nią przejmować. Rozważmy na przykład sieć pokazaną na rysunku 6-1. W sieci tej rutery znajdujące się w obszarze l muszą znać szczegóły dotyczące łączy pomiędzy nimi a segmentami sieci Ethernet, które obsługują, a także szczegóły poszczególnych tras do podsieci. Rutery znajdujące się poza obszarem 1 widzą tylko łącza pomiędzy nimi a całym obszarem 1 i dwie zagregowane trasy: `172.16.48.0/22` oraz `192.168.0.0/24`, które określają wszystkie podsieci znajdujące się w obszarze 1. Jeśli w obszarze l przerwane zostanie jakieś łącze, to tylko rutery pracujące w tym obszarze będą musiały przeliczyć swoje najkrótsze trasy. Pozostałe rutery nawet nie będą wiedziały, że zmienił się stan tego łącza.



Rysunek 6-1: Obszary OSPF pozwalają ukryć szczegóły topologii sieci i podział na podsieci

Obszar OSPF musi być ciągły. W naszym przykładzie trasa pomiędzy każdą parą segmentów sieci wchodzących w skład obszaru 1 może być poprowadzona bez konieczności przejścia przez segmenty znajdujące się poza obszarem 1. Segment sieci lub łącze mogą należeć tylko do jednego obszaru. A zatem jeśli usuniemy połączenie Rutera4 z siecią 172.16. 50.0/23 z obszaru 1, to konieczne jest również usunięcie innych połączeń z ruterami oraz samego segmentu.

Mimo że interfejsy ruterów traktowane są jako część obszaru, to same rutery zwykle nie należą do obszaru. Zwróć uwagę na to, że Ruter3 tworzy połączenie pomiędzy obszarem l i resztą sieci, co *oznacza,* że niektóre jego interfejsy znajdują się w obszarze 1, a inne poza tym obszarem. Jeśli wszystkie interfejsy rutera należą do tego samego obszaru, taki ruter może być traktowany jako część obszaru. We wszystkich innych przypadkach ruter określany jest mianem *obszarowego rutera granicznego,* co oznacza, że znajduje się on na granicy obszaru i przekazuje do reszty sieci sumaryczną informację o łączach i ruterach z wnętrza obszaru.

Protokół OSPF nie pozwala na realizację arbitralnych połączeń z jednego obszaru do drugiego. Choć taka możliwość w znaczny sposób zwiększyłaby elastyczność tworzonych sieci, to jednocześnie ogromnie wzrósłby stopień złożoności tego typu sieci, co prowadziłoby do powstawania błędów.* Twórcy OSPF poprzestali na ograniczeniach wymagających, aby wszystkie obszary łączyły się bezpośrednio ze specjalnym obszarem zwanym obszarem *rdzenia.* Obszar ten ma identyfikator O i musi istnieć w każdej sieci odsługiwanej przez protokół OSPF. Pamiętając o tym wymaganiu, jesteśmy teraz gotowi, by przyjrzeć się fragmentom konfiguracji niektórych ruterów tworzących naszą sieć przykładową. Najpierw obejrzymy konfigurację OSPF rutera o nazwie Ruter1 Zakładamy, że ruter ten nie jest dołączony do żadnego obszaru innego niż obszar 0:

```
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
```

Jak widzisz, konfiguracja ta jest identyczna z tą pokazaną w naszym podstawowym przykładzie. Zdefiniowany został proces rutowania OSPF i przekazano ruterowi informację o tym, że wszystkie interfejsy są częścią obszaru O, i to wszystko. Ruter2 będzie miał identyczną konfigurację, zakładając, że wszystkie jego interfejsy również należą do obszaru 0. Konfiguracja Rutera4 i RuteraS będzie wyglądała podobnie, ale z jedną poważną różnicą:

```
router ospf 1
network 0.0.0.0 255.255.255.255 area 1
```

Różnica ta polega na tym, że w konfiguracji dwóch ostatnich ruterów wszystkie interfejsy są częścią obszaru l, a nie obszaru 0. Zwróć uwagę, że nie ma potrzeby informowania Rutera5 o sieci 192.168.0.0/24, gdyż informacje te są już podane w instrukcji network.

*Protokół OSPF opracowany został w roku 1989, kiedy moc przetwarzania ruterów była bardzo ograniczona. Nawet przy ograniczeniu wymagań protokołu co do połączeń obszarowych wiele osób uważało wtedy, że OSPF zbyt mocno obciążał procesory ruterów, aby mógł być stosowany w większych sieciach.

Tylko konfiguracja Rutera3 wygląda inaczej:

```
router ospf l
 network 172.16.48.0  0.0.3.255          area l
 network 0.0.0.0      255.255.255.255  area 0
```

Konfiguracja ta zaczyna się od uruchomienia procesu rutowania OSPF i poinformowania rutera, że każdy interfejs będący częścią sieci 172.16.48.0/22 należy do obszaru 0. Zwróć uwagę, że konfiguracja ta nie musi informować rutera, iż sieć 192.168.0.0/24 jest częścią obszaru l, nawet jeśli sieć ta nie jest objęta definicją znajdującą się w pierwszej instrukcji network, ponieważ ruter ten nie ma połączenia z tą siecią. Taka konfiguracja jest wystarczająca na początek i pozwala na utworzenie obszarów i zawężenie wymiany informacji o stanie łączy do wymienionych obszarów. Nie nastąpi jednak automatyczne sumowanie tras, ponieważ ruter nie otrzymał informacji o tym, jaki obszar ma obejmować takie sumowanie, a sam tego określić nie może. Ponadto opisywany ruter nie wie jeszcze, co znajduje się za ruterami Ruter4 i Ruter5. Aby powiedzieć mu, ile tras ma sumaryzować, dołączam do konfiguracji następującą instrukcję:

```
area l rangę 172.16.48.0 255.255.252.0
```

Mówi ona urządzeniu Ruter3, że powinien generować sumaryczną trasę dla obszaru l, gdy zna poprawną trasę do każdej z części zagregowanej sieci oraz że powinien przekazać tę sumaryczną trasę do sieci. Po raz kolejny zwróć uwagę, że nie informuję rutera o sieci 192.168.0.0/24, ponieważ trasa ta jest już zsumowana w maksymalnym stopniu; nie można jej połączyć z żadną inną siecią z obszaru 1.

Co więc powinno znajdować się w konfiguracji różnych obszarów OSPF, które będziesz definiował w swojej sieci? Jest to trudne pytanie; odpowiedź na nie będzie różna dla różnych sieci OSPF. Poniżej przedstawiono kilka wskazówek, które powinny pomóc w podjęciu decyzji:

- Każdy obszar sieci OSPF *musi* być ciągły i *musi* być bezpośrednio dołączony do obszaru 0.
- Każdy segment sieci i każdy interfejs rutera powinien należeć do *dokładnie* jednego obszaru. Te dwie reguły dyktują kilka rozwiązań dla Twojej sieci.
- Rozgłaszanie stanu łącza jest wykonywane wewnątrz obszaru, ale nie wychodzi poza granicę jednego obszaru. Ponadto zawsze kiedy łącze zmieni stan, każdy ruter pracujący w obszarze musi przeliczyć swoje najkrótsze trasy do wszystkich podsieci. Dlatego pamiętaj, aby wyznaczone przez Ciebie obszary były maksymalnie stabilne, co spowoduje minimalizację liczby wykonywanych przeliczeń tras. Oznacza to, że nie jest dobrym pomysłem umieszczanie w obszarze O nietrwałych łączy (takich jak łącza ISDN lub łącza zestawiane na żądanie). Takie łącza nie powinny być też umieszczane w dużych obszarach. Za każdym razem, kiedy takie łącze będzie zestawione lub rozłączone, wszystkie rutery dołączone do danego obszaru, w którym łącze to się znajduje, będą musiały przeliczyć zapamiętane *przez* siebie najkrótsze trasy.

Zastanów się, czy nie jest możliwe umieszczenie w Twojej sieci wszystkich łączy nietrwałych i zestawianych na żądanie w jednym wspólnym obszarze, który będzie zawierał tylko takie łącza. Najlepiej jednak będzie, jeśli dla tego typu łączy zostanie zastosowane rutowanie statyczne i nastąpi redystrybucja tras statycznych w sieci OSPF (rozwiązanie takie opisane jest w dalszej części książki).

- Rozmieść obszary w taki sposób, by zminimalizować agregowanie tras. Ponieważ agregowanie występuje tylko na granicach obszarów, to idealnym obszarem jest taki, w którym tworzona jest jedna trasa sumaryczna do każdego innego obszaru. Pozwoli to zmniejszyć rozmiary tablic rutowania Twoich ruterów.
- Staraj się, by w jednym obszarze znajdowała się rozsądna liczba łączy i interfejsów. Jedna z podstawowych reguł mówi, że w jednym obszarze nie powinno się znaleźć więcej niż 100 łączy, chyba że łącza te są *bardzo* stabilne. Liczba ta może być zbyt duża dla Twojej sieci, ale może być także za mała. Najlepszym wyjściem jest przyjęcie jakiejś rozsądnej wartości początkowej, którą następnie należy dostosować w górę lub w dół w oparciu o uzyskiwane osiągi sieci.
- Kolejna zasada mówi, że jeden ruter nie powinien znajdować się w więcej niż czterech obszarach. Także ta liczba może być znacznie większa od Twoich wymagań albo zbyt mała w stosunku do potrzeb Twojej sieci. Jeśli obszary są stosunkowo stabilne i nieduże, to jeden ruter może z powodzeniem obsłużyć ich nawet kilkanaście. Z drugiej strony jeśli obszary, które wyodrębniłeś w swojej sieci, są choć trochę niestabilne albo bardzo duże, to wykorzystanie pamięci i obciążenie procesora będzie tak wielkie, że ruter powinien znaleźć się w maksymalnie dwóch obszarach. Eksperymentuj i dopasuj te liczby w oparciu o osiągi sieci.

Ostateczną decyzję o podziale sieci na obszary podejmiesz prawdopodobnie po wykonaniu kilku kolejnych analiz sieci. Być może początkowo umieścisz całą sieć w obszarze 0. Kiedy zidentyfikujesz *łącza,* które są trochę niestabilne, lub kiedy okaże się, że mapowanie topologii stanu łącza OSPF zajmuje zbyt dużo pamięci w ruterach, dokonasz podziału segmentów sieci na kilka nowych obszarów. Dlatego ważne jest, aby przydzielane obszarom numery odpowiadały (przynajmniej w pewnym zakresie) topologii Twojej sieci. W przeciwnym wypadku okaże się, że Twoje graniczne rutery nie są w stanie utworzyć odpowiednich sumarycznych tras, kiedy nadejdzie czas tworzenia obszarów.

Jest wiele poleceń, umożliwiających strojenie i regulowanie zachowania protokołu OSPF. Niektóre z nich umożliwiają zastosowanie kluczy autentykacji* dla obszarów, niektóre pozwalają regulować zegary sterujące komunikatami OSPF, a jeszcze inne zmieniają domyślne wartości kosztów przypisane do różnych typów interfejsów. Tych funkcji będziesz potrzebował raczej rzadko i powinieneś je ignorować, chyba że dokładnie wiesz, co za ich pomocą możesz zrobić i dlaczego.

*Potrzeba użycia kluczy autentykacji i sposób *ich* wykorzystania opisane zostaną w rozdziale 10, „Bezpieczeństwo sieci", przy okazji omawiania zabezpieczeń stosowanych w sieci.

EIGRP

W celu przedstawienia konfiguracji protokołu EIGRP wykorzystamy taki sam układ dwóch sieci: 172.16.0.0/15 oraz 192 .168.100. 0/24. Utworzenie procesu rutowania EIGRP wymaga podania identyfikatora, który, podobnie jak w OSPF, może być wybrany arbitralnie, ale, w przeciwieństwie do OSPF, musi być jednakowy dla wszystkich ruterów w sieci. Możliwe jest uruchomienie kilku procesów rutowania EIGRP na tym samym ruterze poprzez przydzielenie im różnych identyfikatorów. W przypadku równoczesnej obsługi kilku procesów EIGRP ruter traktuje każdy z nich jako oddzielny protokół rutowania i nie przekazuje automatycznie żadnych informacji pomiędzy tymi procesami. Użycie kilku procesów może być przydatne w kilku specjalnych przypadkach, ale nie powinno być sposobem konfigurowania rutera w normalnych warunkach.

```
! start an EIGRP process on my networks
router eigrp 1
 network 172.16.0.0
 network 172.17.0.0
 network 192.168.100.0
```

Choć EIGRP jest bezklasowym protokołem rutowania, to nadal konieczne jest rozdzielenie naszej zagregowanej sieci na dwie sieci z klasy, kiedy mówimy ruterowi, gdzie powinien działać proces rutowania. Stąd w konfiguracji użyte zostały trzy instrukcje network, podobnie jak to robiliśmy w przypadku konfigurowania protokołu RIP, nawet jeśli tak naprawdę mamy tylko dwie sieci. Funkcja ta sprawia, że konfiguracja EIGRP jest podobna do konfiguracji IGRP, swej poprzedniczki. W naszym przykładzie ruter wysyła i odbiera komunikaty EIGRP w obu sieciach.

Rozgłaszanie tras statycznych

Jednym z najczęściej występujących problemów, z którymi będziesz się spotykał, będzie sposób propagowania tras statycznych stosowanych w Twojej sieci. Te statyczne trasy rutowania występują wtedy, gdy masz w swojej sieci sprzęt, który nie obsługuje protokołu rutowania dynamicznego stosowanego w Twojej sieci. Możliwe również, że nie chcesz otrzymywać uaktualnień z dynamicznego protokołu rutowania używanego w sieci administrowanej przez inny zespół, która dołączona jest do Twojej sieci. A może - co jest bardziej prawdopodobne - posiadasz domyślną trasę statyczną łączącą Twoją sieć z siecią Internet. W takim wypadku konieczne jest zdefiniowanie rutowania statycznego na ruterze lub ruterach, które tego wymagają. Lepiej jednak nie instalować rutowania statycznego ręcznie na wszystkich ruterach w sieci, ponieważ może to zająć sporo czasu i spowodować wiele błędów. Zamiast tego rutery brzegowe powinny rozgłaszać zdefiniowane w nich trasy statyczne poprzez wykorzystywany w sieci dynamiczny protokół rutowania.

Rozgłaszanie tras statycznych

RIP

W pokazanej poniżej konfiguracji dodałem domyślną trasę statyczną prowadzącą poprzez host 192.168.100.250, która jest prawdopodobnie połączeniem z siecią Internet, i kazałem ruterowi rozsyłać wszystkie trasy statyczne wykorzystując do tego protokół RIP. Jest to ogólna forma polecenia, które uruchamia dystrybucję tras, ale ostrzegam, że dystrybucja tras z jednego protokołu do drugiego nie jest zadaniem prostym. Dokładniej opiszę je w dalszej części książki. Należy pamiętać, że zawsze jednym z najważniejszych problemów jest sposób tłumaczenia miar jednego protokołu na odpowiednią informację do drugiego protokołu. W przypadku tras statycznych i protokołu RIP oprogramowanie definiuje domyślną miarę równą l, tak więc ruter konfigurowany przez nas w tym przykładzie będzie rozsyłał tę domyślną trasę w swoich uaktualnieniach posługując się taką właśnie miarą.

```
router rip
 network 172.16.0.0
 network 172.17.0.0
 network 192.168.100.0
 ! redistribute my static routes with a default metric
 redistribute static
 !
ip route 0.0.0.0 0.0.0.0 192.168.100.250
```

OSPF

Podobnie jak w poprzednim przypadku, dodałem trasę statyczną prowadzącą przez 192.168.100.250i chciałbym rozgłaszać informację o tej trasie w mojej sieci obsługiwanej przez OSPF. Inaczej niż w protokole RIP, OSPF nie ma domyślnej miary dla tras statycznych. Ponieważ mogłem zdefiniować domyślną wartość wykorzystywaną do przypisania miar trasom pobieranym z innych protokołów rutowania, to moje możliwości są ograniczone, i -jak widać - wszystkie trasy statyczne powinny otrzymywać miarę OSPF równą 1. W przeciwieństwie do miar protokołu RIP, miary OSPF nie określają liczby przeskoków. Wykorzystuje sieje do porównania kosztu tej domyślnej trasy z kosztem innej trasy, jakiej mógł się nauczyć ruter.

```
router ospf 1
 network 0.0.0.0 255.255.255.255 area 0
 ! redistribute my static routes with a type-2 external metric of 1
 redistribute static metric 1
 !
ip route 0.0.0.0 0.0.0.0 192.168.100.250
```

W przykładzie tym wybrałem użycie miary typu 2. Typ miary oznaczany jako l może być określony instrukcją:

```
redistribute static metric 1 metric-type 1
```

Protokół OSPF definiuje trzy typy miar. Pierwszy z nich używany jest dla sieci wchodzących w skład domeny rutowania odsługiwanej przez OSPF.

Ten rodzaj miar nie jest odpowiedni dla tras, które trafiły do domeny rutowania OSPF jako trasy redystrybuowane. Zamiast takich miar konieczne jest użycie wersji rozszerzonych typu I lub typu 2. Różnica pomiędzy tymi dwoma typami miar i wybór właściwego typu dla Twojej sieci wykracza poza zakres tematyczny tej książki. Musisz jednak upewnić się, czy wszystkie zewnętrzne trasy, które będą ze sobą porównywane, opisane są tym samym typem metryki. W przypadku opisywanym wyżej domyślnym typem miary jest typ 2.

EIGRP

Zdefiniowałem domyślną trasę statyczną, którą chcę redystrybuować. Podobnie jak w przypadku protokołu RIP, EIGRP definiuje domyślną miarę kosztu używaną do opisu tras statycznych, nie muszę więc robić nic więcej.

```
router eigrp 1
 network 172.16.0.0
 network 172.17.0.0
 network 192.168.100
 !redistribute mystatic routes with adefault metric
 redistribute static

ip route 0.0.0.0 0.0.0.0 192.168.100.250
```

Użycie zmiennej długości masek podsieci w klasowym protokole rutowania

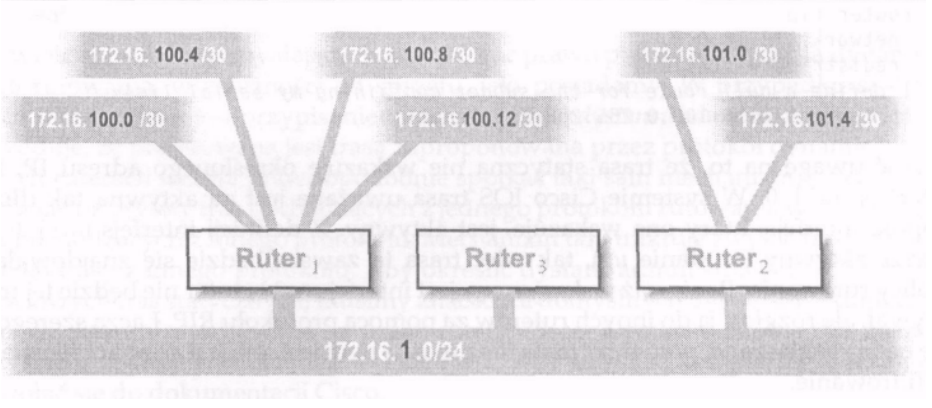
W rozdziale 3 - „Projekt sieci - część 2" - napisałem, że w pewnych ograniczonych warunkach możliwe jest użycie zmiennej długości masek podsieci podczas pracy z protokołem rutowania obsługującym tylko maski sieci z określonych klas. Napisałem też, że jest to kiepski pomysł, a takie rozwiązanie powinno być używane tylko w ostateczności. Jeśli stosujesz w swojej sieci klasowy protokół rutowania, powinieneś w całej pojedynczej sieci IP zastosować taką samą maskę podsieci, z klasy A, B lub C. W różnych sieciach nadal możliwe jest stosowanie różnych masek. Jeśli jednak zmuszony jesteś do zastosowania masek o zmiennej długości w jednej sieci, musisz postępować dokładnie według podanych niżej zasad:

- maska nieparzysta musi być dłuższa (opisywać mniejsze podsieci) niż normalna maska;
- grupa podsieci używających masek nieparzystych musi należeć do jednej podsieci, w której użyta została maska z klasy;
- każda grupa podsieci używających masek nieparzystych (i należących do jednej podsieci z klasy) musi być dołączona do tego samego rutera.

Na rysunku 6-2 przedstawiono sieć zbudowaną w oparciu o te zasady. Maska podsieci z klasy ma długość 24 bity (255.255.255.0), a dla łączy punkt-punkt wybrałem maskę o długości 30 bitów. Takie rozwiązanie jest zgodne z pierwszą zasadą, ponie*waż* maska 30-bitowa jest dłuższa od 24-bitowej.

Użycie zmiennej długości masek podsieci w klasowym protokole ratowania

Numery podsieci zostały przydzielone pierwszej grupie łączy szeregowych w taki sposób, że wszystkie one są częścią sieci 172.16.100.0/24, która jest podsiecią z klasy, wykorzystującą maskę 24-bito-wą. Wszystkie te łącza szeregowe dołączone są do Rutera1. Ponadto utworzyłem drugą grupę łączy szeregowych, które również wykorzystują maskę o długości 30 bitów. Wszystkie te łącza są częścią sieci 172.16.101.0/24, używającej standardowej maski, i wszystkie dołączone są do Rutera2. Obydwie grupy łączy spełniają wymagania reguł drugiej i trzeciej. Ponieważ obie grupy dołączone są do dwóch różnych ruterów, muszą wykorzystywać różne podsieci pochodzące z klasy, nawet jeśli żadna z nich nie jest w pełni wykorzystywana.



Rysunek 6-2: Zmiennej długości maski podsieci używane w sieci obsługiwanej przez klasowy protokół rutowania

Ponieważ stosowany w sieci dynamiczny protokół rutowania nie może przenosić informacji o łączach szeregowych, miałem do wyboru dwie możliwości poinformowania reszty świata o tych łączach. Pierwsza polega na dodaniu na wszystkich ruterach tras statycznych opisujących te łącza szeregowe. Takie rozwiązanie jest czasochłonne, generuje również wiele błędów, zwłaszcza jeśli do skonfigurowania jest kilkaset ruterów. Drugie rozwiązanie polega na okłamaniu innych ruterów i przekazaniu im nieprawdziwej informacji o tych łączach. Jest to rozwiązanie, które teraz zastosujemy. Celem Rutera1 jest rozgłaszanie trasy do sieci 172.16.100.0/24 i milczenie na temat poszczególnych łączy szeregowych. Ruter2 ma rozgłaszać trasę do sieci 172.16.101.0/241 milczeć na temat dokładniej opisanych tras.

W jaki sposób można skłonić Ruter1, aby kłamał na temat łączy szeregowych? Należy odpowiednio skonfigurować trasę statyczną w Ruterze1 do sieci 172.16.100.0/24,a następnie w rozpropagować ją do innych ruterów:

```
hostname router1
!
interface serial 0
```

```
  ip address 172.16.100.1 255.255.255.252
!
interface serial 1
  ip address 172.16.100.5 255.255.255.252
!
interface serial 2
ip address 172.16.100.9 255.255.255.252
!
interface serial 3
  ip address 172.16.100.13 255.255.255.255
!
interface ethernet O ip address 172.16.1.1 255.255.255.0 i
router rip
  network 172.16.0.0
  redistribute static
! define a null route for the subnet containing my serial lines ip route
172.16.100.0 255.255.255.0 null 0
```

Zwróć uwagę na to, że trasa statyczna nie wskazuje określonego adresu IP, lecz interfejs null 0. W systemie Cisco IOS trasa uważana jest za aktywną tak długo, dopóki interfejs, który ona wskazuje, jest aktywny. Z definicji interfejs null O jest *zawsze* aktywny (w stanie *np),* tak więc trasa ta zawsze będzie się znajdowała w tablicy rutowania. Ponieważ wskazywany jest interfejs n u 11, ruter nie będzie tej trasy używał, ale rozgłosi ją do innych ruterów za pomocą protokołu RIP. *Łącza* szeregowe nie będą rozgłaszane, ponieważ mają inną maskę podsieci, nie jest więc konieczne ich odfiltrowanie.

Konfiguracja Rutera2 będzie zasadniczo taka sama, za wyjątkiem tego, że zmienione będą adresy i nazwy interfejsów, tak by odpowiadały połączeniom tego rutera. Ru-ter3 nie wymaga specjalnej konfiguracji; ma standardową konfigurację protokołu RIP, taką, jaka jest stosowana w ruterach, które pracują z jedną maską podsieci. Oczywiście, protokoły takie jak EIGRP lub OSPF będą obsługiwały taką sieć bez żadnej dodatkowej konfiguracji, ponieważ są to protokoły bezklasowe.

Jak widzisz, możliwe jest stosowanie ograniczonej liczby zmiennej długości masek podsieci wraz z protokołem rutowania obsługującym tylko sieci z klasy. Lepiej jest jednak często nie wykorzystywać tej możliwości. Zawsze należy dokładnie przetestować działanie wykonanej konfiguracji. Zamiast takich rozwiązań lepiej zastosować bezklasowy protokół rutowania, który będzie poprawnie obsługiwał maski o zmiennej długości.

Zapasowe trasy statyczne

Możliwe, że w Twojej sieci przyda się trasa statyczna działająca jako trasa zapasowa dla uruchomionego dynamicznego protokołu rutowania. Trasa taka może być skonfigurowana na odległym ruterze (na przykład w terenowym oddziale firmy), do którego nie masz łatwego dostępu. Trasa taka zabezpieczy Cię przed utratą połączenia z ruterem, jeśli podczas zdalnej konfiguracji tego rutera popełnisz jakiś błąd.

Zapasowe trasy statyczne

Posiadając zapasową trasę statyczną możesz wykorzystać zalety dynamicznego rutowania, poprawiając i optymalizując konfigurację odległego rutera bez obawy, że utracisz z nim połączenie. Zawsze będziesz mógł, wykorzystując trasę statyczną, naprawić popełnione błędy bez konieczności podróżowania do tego rutera.

Problem ze statycznymi trasami polega na tym, że w większości ruterów trasy te zastępują dowolną trasę, która jest przekazana przez dynamiczny protokół. Chcielibyśmy, aby trasa statyczna zadziałała np. w przypadku awarii, kiedy popełnimy jakiś błąd przy konfigurowaniu protokołu dynamicznego. Innymi słowy, chcemy, aby w czasie normalnej pracy pierwszeństwo miały trasy protokołu dynamicznego, ale jednocześnie nie chcemy pozostać bez trasy, gdy protokół dynamiczny nie będzie jej oferował.

Jest wiele sposobów pozwalających zastosować prawo pierwszeństwa dla dynamicznego rutowania, w zależności od sprzętu, jaki posiadamy. W przypadku systemu Cisco IOS możliwe jest przypisanie trasie statycznej *dystansu administracyjnego,* który powoduje, że preferowana jest trasa zaproponowana przez protokół dynamiczny. W innych ruterach można prawdopodobnie spotkać taki sam mechanizm, pozwalający ustawiać priorytety tras pochodzących z jednego protokołu rutowania w stosunku do tras pochodzących z innego protokołu. Mechanizm taki traktuje zwykle trasy statyczne jako trasy z innego protokołu. Aby określić dystans administracyjny dla naszych zapasowych tras statycznych, musimy znać kilka domyślnych dystansów administracyjnych, które przypisywane są przez rutery Cisco. Dystansy istotne dla naszego przykładu zostały wymienione w tabeli 6-1. Aby uzyskać kompletną listę, należy odwołać się do dokumentacji Cisco.

Tabela 6-1. Domyślne dystansy administracyjne dla wybranych protokołów rutowania stosowane

Źródło informacji o trasie	*Domyślny dystans*
Dołączony interfejs	0
Trasa statyczna	1
EIGRP sumaryczna[a]	5
EIGRP wewnętrzna	90
IGRP	100
OSPF	110
RIP	120
EIGRP zewnętrzna	170
Nieznane	255

[a] Protokół EIGRP definiuje trzy różne typy tras; trasy wewnętrzne są trasami przekazanymi z dołączonych do różnych ruterów segmentów sieci; trasy sumaryczne są zagregowanymi trasami wykonanymi przez ruter EIGRP gdzieś w sieci, które obejmują wiele tras wewnętrznych, a trasy zewnętrzne są dystrybuowanymi trasami przekazanymi do EIGRP przez inne protokoły rutowania.

Dystans administracyjny o mniejszej wartości preferowany jest przed dystansem o większej wartości, a źródło rutowania, dla którego dystans wynosi 255, nigdy nie jest używane. Tak więc w każdym z naszych przykładów konieczne jest tylko powiększenie dystansu administracyjnego dla trasy statycznej prowadzącej do segmentu sieci, w której znajduje się stacja zarządzająca pracą sieci. Powiększona wartość powinna być większa od dystansu administracyjnego przypisanego przez stosowany w sieci protokół dynamiczny. Aby to zrobić, wystarczy wpisać wartość dystansu na końcu instrukcji konfigurującej trasę statyczną. Mógłbym określić ten dystans nawet wartością 254, aby uchronić się przed zastąpieniem jej przez jakikolwiek inny protokół rutowania, ale lepiej jest ostrożnie podchodzić do określania tej wartości. Jeśli w przyszłości nastąpi zmiana stosowanych w sieci protokołów rutowania, konieczne będzie uważne przeanalizowanie konfiguracji tras i dopasowanie wartości dystansów administracyjnych do wartości stosowanych przez nowe protokoły.

W każdym z niżej przedstawionych przykładów usunąłem redystrybucję tras statycznych do dynamicznego protokołu rutowania. Należy dokładnie pamiętać, jaka jest kolejność działań. Rozpoczęliśmy od błędnego skonfigurowania protokołu, co spowodowało, że utraciliśmy dynamiczną trasę do stacji, z której zarządzamy siecią; chcemy, aby dalsza komunikacja odbywała się za pośrednictwem trasy statycznej. Trasa statyczna *zależy* jednak od rutera następnego przeskoku, który powinien w tym momencie działać poprawnie. Takie podejście jest poprawne, ale tylko w przypadku, gdy ruter ten nie został błędnie skonfigurowany lub został błędnie skonfigurowany, ale ma zdefiniowaną zapasową trasę statyczną. W obu przypadkach, jeśli pozwolę, aby mój ruter rozgłaszał trasę zapasową, to spowoduję zmianę zapisu o zapasowej trasie statycznej w ruterze kolejnego przeskoku na rozgłaszaną trasę lub rozgłoszę lepszą miarę trasy generowanej *przez* uaktualnienie dynamicznego rutowania, co spowoduje, że ruter założy, iż pierwszy ruter jest lepszą trasą do sieci. W każdym z opisanych przypadków utworzę pętlę rutowania i utracę kontrolę nad ruterem. Wniosek jest więc taki, że nie należy rozgłaszać zapasowych tras statycznych za pomocą dynamicznego protokołu rutowania. Jeśli kilka ruterów wymaga skonfigurowania zapasowej trasy statycznej, należy każdą z nich skonfigurować oddzielnie na tych ruterach.

Jeśli chcesz propagować trasy statyczne, które nie są zapasowymi, i jednocześnie używać zapasowych tras statycznych, konieczne będzie zastosowanie mechanizmu filtrowania rozgłaszanych tras. Filtrowanie tras zostanie krótko opisane w dalszej części książki.

RIP

```
router rip
  network 172.16.0.0
  network 172.17.0.0
  network 192.168.100.0
! set the administrative distance on my static route to be higher than ! RIP ip route
172.16.10.0 255.255.255.0 172.16.1.5 130
```

Zapasowe trasy statyczne

OSPF

```
router ospf 1
 network 0.0.0.0 255.255.255.255 area 0
! set the administrative distance on my static route to be higher than ! OSPF
ip route 172.16.10.0 255.255.255.0 172.16.1.5 120
```

EIGRP

```
router eigrp 1
 network 172.16.0.0
 network 172.17.0.0
 network 192.168.100
! set the administrative distance on my static route to be higher than ! EIGRP ip route
172.16.10.0 255.255.255.0 172.16.1.5 100
```

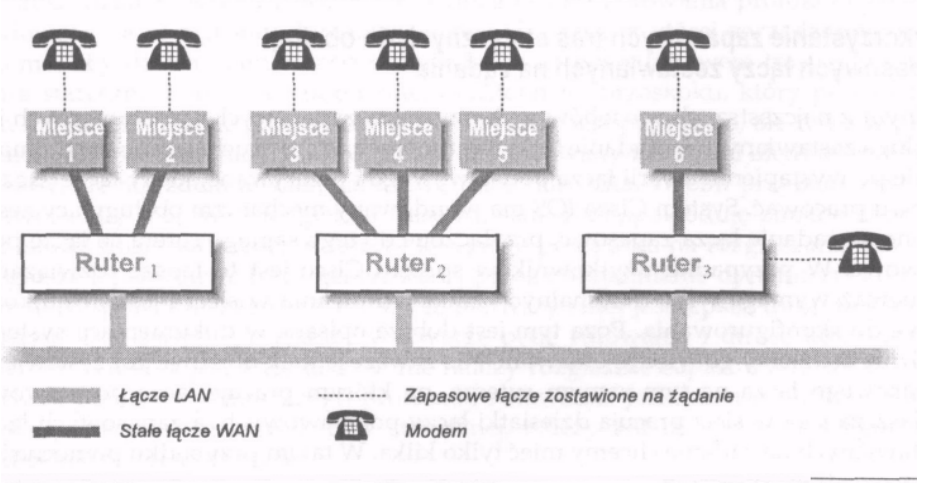
Wykorzystanie zapasowych tras statycznych do obsługi zapasowych łączy zestawianych na żądanie

Jednym z najczęstszych sposobów wykorzystania zapasowych tras statycznych jest obsługa zestawianych na żądanie łączy zapasowych, które uruchamiane są automatycznie po wystąpieniu awarii łącza podstawowego i przerywane, kiedy łącze zacznie znowu pracować. System Cisco IOS ma wbudowany mechanizm obsługujący zestawiane na żądanie łącza zapasowe, przyłączone do tego samego rutera co łącze podstawowe. W przypadku użytkowników sprzętu Cisco jest to lepsze rozwiązanie, ponieważ wymaga tylko minimalnych zmian rutowania w sieci i jest stosunkowo łatwe do skonfigurowania. Poza tym jest dobrze opisane w dokumentacji systemu IOS, nie będziemy go więc tu omawiali. Nie zawsze jednak możliwe jest zestawienie zapasowego łącza na tym samym ruterze, na którym pracuje łącze podstawowe, zwłaszcza jeśli w sieci pracują dziesiątki łączy podstawowych, a zapasowych łączy zestawianych na żądanie chcemy mieć tylko kilka. W takim przypadku pomocna jest zapasowa trasa statyczna.

Zastanówmy się nad konfiguracją sieci, która ma dołączonych kilka łączy WAN do różnych ruterów. Jako administrator takiej sieci chciałbyś mieć pewność, że w przypadku wystąpienia awarii któregokolwiek z tych łączy nadal możliwe będzie przekazywanie ważnych informacji do danego miejsca, nawet jeśli podstawowe łącza prowadzące do tego miejsca nie funkcjonują. Chcesz mieć również pewność, że będziesz mógł się dostać do odległego rutera za pośrednictwem sieci, nawet w czasie takiej awarii. W związku z koniecznością ograniczenia kosztów systemu łączy zapasowych jesteś w stanie zaakceptować rozwiązanie, które zapewnia pracę tylko jednego zapasowego łącza w danym momencie, tzn. jeśli równocześnie uszkodzone zostaną dwa łącza jedno z miejsc pozostanie odcięte, a drugie będzie dołączone do sieci za pośrednictwem łącza zestawionego na żądanie. Kiedy przestaną Cię obowiązywać ograniczenia budżetowe, chcesz mieć możliwość dodania większej liczby łączy zapasowych, ale nie stanie się to na pewno w tym roku.

Opisana sytuacja pokazana została na rysunku 6-3. W warunkach normalnej pracy dane przesyłane są stałymi łączami WAN, a w momencie wystąpienia uszkodzenia chcesz, by Ruter3 zatelefonował do odległego miejsca i zestawił łącze, po którym możliwe będzie przesyłanie części danych.

Jaka więc będzie kolejność Twoich działań? Najpierw musisz wyposażyć każde z odległych miejsc w jakieś zestawiane na żądanie łącze WAN. Nie jest przy tym ważne, czy łącze to będzie realizowane przez asynchroniczny interfejs szeregowy i analogowy modem, przez interfejs ISDN, czy też przełączany synchroniczny interfejs szeregowy. Załóżymy w tym przykładzie, że najłatwiej jest używać analogowych modemów i wielofunkcyjnych asynchronicznych portów szeregowych znajdujących się w każdym z ruterów. Konieczne jest więc wyposażenie rutera znajdującego się w centrali w taki sam analogowy modem dołączony do asynchronicznego portu szeregowego tego rutera. Każdy ruter na pewno ma taki port.



Rysunek 6-3: Wykorzystanie modemów do tworzenia zapasowych łączy dla sieci WAN

Teraz jesteś gotów do skonfigurowania swoich ruterów tak, aby obsługiwały zestawiane łącze zapasowe. Ponieważ jedyną różnicą w konfiguracji każdego z odległych ruterów jest używany przez nie adres IP, przedstawię tylko jeden przykład konfiguracji takiego rutera:

```
! this dial-up link will be used as a backup only interface
async 2
  ip address 172.16.200.2 255.255.255.0
  ! limit traffic on this link to avoid swamping it with our norma! load
  ip access-group 101
  dialer in-band
```

```
 dialer-group 1
 ! map the central site IP address to its phone nutnber
dialer map ip 172.16.200.1 5551000 i
! allow traffic to the network management station and to the order
! entry subnet so that business can continue
access-list 101 permit ip 0.0.0.0 255.255.255.255 172.16.100.97 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 172.16.131.0 0.0.0.255
!
dialer-list 1 list 101 i
! mąkę surę this route to the central site has a high administratiye
! distance so itis only used as a backup
ip route 0.0.0.0 0.0.0.0 172.15.200.1 250
```

W konfiguracji tej kazałem ruterowi uaktywnić asynchroniczny interfejs o nazwie async 1, którego adres IP to 172.16.200.2 z maską o długości 24 bitów. Twoją pierwszą reakcją może być stwierdzenie: „24 bity na łącze punkt-punkt! Co za marnotrawstwo!". Musisz mi jednak tym razem zaufać. Kiedy za chwilę będziemy omawiać konfigurację centralnego węzła sieci, wyjaśnię, dlaczego konieczna jest taka duża maska podsieci.

Następnie informuję ruter, że do tego interfejsu ma przypisać listę kontroli dostępu, co pozwoli ograniczyć ruch generowany w tym łączu. Instrukcja i p access-group powoduje powiązanie listy kontroli dostępu z interfejsem. Liczba występująca po tej instrukcji określa numer listy, którą należy zastosować. Same listy tworzone są za pomocą instrukcji access-list, które występują w dalszej części przedstawionej konfiguracji. Instrukcja access-1 jest pozwala określić szereg warunków zezwolenia i zakazu, bazujących na adresie IP źródła i przeznaczenia. Warunki te zapisywane są za pomocą podstawowego adresu IP i maski z bitami gwiazdkowymi określającymi adres źródła, po których występuje podstawowy adres IP przeznaczenia i jego maska. Bezwarunkowa instrukcja „zabroń wszystkiego" umieszczona jest przez program automatycznie na końcu listy.

W naszym przykładzie pierwsza instrukcja *access-1 list* informuje, że chcemy zezwolić na przesyłanie pakietów z dowolnym adresem źródła do hosta o adresie 172.16.100.97. Jest to nasza stacja zarządzająca pracą sieci; dzięki tej instrukcji do stacji zarządzającej pracą sieci będą docierały raporty o błędach i możliwe będzie zdalne załogowanie się do rutera. Drugie polecenie access-1 ist informuje, że chcemy, aby przesyłane były również wszystkie pakiety z każdego hosta do sieci 172.16.131.0/24. Podsieć ta zawiera komputery obsługujące przyjmowanie zleceń i chcemy, aby w czasie awarii te informacje docierały do centrali łączem zapasowym.

Dlaczego więc zdefiniowany został dostęp zapisany w pierwszej instrukcji? Dlaczego nie pozwolić, aby wszystkie pakiety wysyłane z odległej sieci trafiały do centrali? Analogowe łącze modemowe prawie zawsze będzie miało mniejsze pasmo niż stałe łącze dzierżawione. Jeśli pozwoliłbym na przesyłanie całego ruchu generowanego w łączu podstawowym przez łącze zapasowe, to prawdopodobnie bym je zapchał i niewiele użytecznych danych mogłoby dotrzeć do centrali. Tworzenie łącza zapasowego bez żadnych restrykcji dotyczących ruchu, który to łącze może obsługiwać, nie jest rozsądnym rozwiązaniem.

Poza kontrolą przesyłanego przez łącze ruchu określiłem również, jaki ruch należy uznać za „interesujący" na tyle, aby spowodował zestawienie tego łącza i utrzymywanie go w stanie aktywności. Aby to zrobić, z interfejsem skojarzyłem grupę wymuszającą dzwonienie, posługując się instrukcją `dialer-group`, która określa grupę o numerze 1. Następnie z grupą taką skojarzyłem listę dostępu (możliwe jest skojarzenie kilku takich list). To drugie zadanie wykonane zostało w poleceniu *dialer-list* umieszczonym w dalszej części konfiguracji. Skojarzyłem w nim listę kontroli dostępu numer 101 z grupą dzwoniącą o numerze 1. Jeśli wybrałbym inną listę kontroli dostępu, określającą inne kryteria wyboru, to należałoby *uznać,* że ruch, na który zezwala ta lista, jest na tyle ważny, aby również powodował zestawienie i podtrzymanie połączenia. W związku z tym użyłem powtórnie listy, która już wcześniej została zdefiniowana i zastosowana.

Poinformowałem też ruter, że interfejs ten obsługuje łącze zestawiane na żądanie i że wybieranie numeru będzie się odbywać z wykorzystaniem kontroli *in-band* dołączonego modemu. Szczegóły komunikacji *in-band z* modemem oraz logowania się do odległego rutera kontrolowane są przez skrypty, których tutaj nie pokazano. Ponieważ skrypty *zależą* od używanego modemu, powinieneś zajrzeć do dokumentacji Cisco IOS oraz dokumentacji posiadanego modemu i na tej podstawie napisać odpowiedni skrypt.

Na koniec dołączyłem statyczną trasę domyślną wskazującą adres `172.16.200.1`, czyli ruter znajdujący się w centrali mojej firmy, i kazałem ruterowi używać podane go numeru telefonu w celu nawiązania połączenia z tym ruterem. Nadałem również trasie statycznej bardzo dużą wartość dystansu administracyjnego, dzięki czemu każdy protokół dynamicznego rutowania będzie mógł przejąć tę trasę. A skoro mówi my o dynamicznym protokole rutowania, powinieneś się upewnić, czy interfejs rutera obsługujący to zapasowe łącze jest interfejsem pasywnym, przez co łącze nie będzie zestawiane przy każdej próbie wymiany informacji o rutowaniu przez ten interfejs.

Ruter znajdujący się w centrali ma podobną konfigurację. Główna różnica polega na tym, że w konfiguracji tej znajduje się kilka instrukcji di a l er map oraz że inaczej zdefiniowana została lista kontroli dostępu. Listy kontroli dostępu stosuje się do pakietów, które wysyłane są przez dany interfejs. Ponieważ jesteśmy teraz po drugiej stronie łącza, pakiety, w stosunku do których działają te listy, są przesyłane w drugą stronę, dlatego adres źródła i przeznaczenia muszą być zamienione miejscami.

```
! this dial-up link will be used as a backup oni y interface async 1
 ip address 172.16.200.1 255.255.255.0
 ! limit traffic on this link to avoid swamping it with our norma] load
ip access-group 101
dialer in-band
dialer-group 1
! map each s;te's backup IP address to its phone number
dialer map ip 172.16.200.2 5551212
dialer map ip 172.16.200.3 5552889
!
! allow traffic from the netuork management station and from the order
! entry subnet so that business can continue
access-list 101 permit ip 172.16.100.97 0.0.0.0   0.0.0.0 255.255.255.255
access-list 101 permit ip 172.16.131.0   0.0.0.255 0.0.0.0 255.255.255.255
i
dialer-list 1 list 101
!
! make sure these routes to the remote sites have a high administrative
! distance so they ara only used as backups
ip route 172.16.95.0 255.255.255.0 172.16.200.2 250
ip route 172.16.64.0 255.255.252.0 172.16.200.3 250
```

Instrukcja dialer map informuje ruter o tym, jakiego numeru telefonu należy użyć, aby połączyć się z każdym z odległych miejsc. Dla każdego rutera znajdującego się poza centralą konieczne jest podanie jednego numeru telefonu. W naszej przykładowej konfiguracji opisaliśmy tylko dwa miejsca, z którymi nawiązywane jest połączenie. Dla każdego z odległych ruterów konieczne jest również podanie zapasowej trasy statycznej, przez którą do tego rutera będzie wysyłany ruch z innych sieci.

Teraz już powinno być jasne, dlaczego dla łączy zestawianych na żądanie zdefiniowałem maskę o długości 24 bitów. Aby maksymalnie uprościć konfigurację rutowania i nawiązywania połączeń, wszystkie zapasowe interfejsy powinny znajdować się w jednej podsieci. Można zastosować maskę trochę dłuższą, ale musi ona zapewnić wystarczającą liczbę adresów dla wszystkich ruterów, które wykorzystują to łącze zapasowe. Gdybym skonfigurował oddzielne łącza na żądanie dla każdego z odległych miejsc - zamiast zastosowania jednego wspólnego łącza - zastosowałbym maski o długości 30 bitów, które byłyby bardziej odpowiednie dla tych łączy.

Wykorzystanie zapasowych tras statycznych do ograniczenia migotania tras

Zapasowe trasy statyczne stosuje się do ograniczania migotania tras. Trasa zaczyna migotać, kiedy w krótkim czasie przechodzi przez kilka stanów osiągalności i nieosiągalności. Choć taka sytuacja jest normalna w przypadku występowania jakiegoś błędu w pracy sieci i nie powinna trwać zbyt długo, to może się zdarzyć, że będziesz musiał pracować w sieci, w której taka sytuacja będzie trwała przez całe dni, a nawet tygodnie. Możliwe jest również, że problem będzie występował w którejś z sąsiadujących sieci, a jej administratorzy nie mają zamiaru lub nie mogą tego naprawić. Konieczne będzie ograniczenie wpływu migotania na Twoją sieć. W każdym z opisanych przypadków sprawę załatwi zapasowa trasa statyczna.

Zastanówmy się, co się stanie, kiedy zainstalujesz zapasową trasę statyczną w ruterze, który dołączony jest do sieci z opisanym wyżej problemem lub do którego dołączone jest uszkodzone łącze. Kiedy trasa zniknie i przestanie być rozgłaszana przez protokół rutowania dynamicznego, Twój ruter prześle tę informacje dalej do całej sieci tylko po to, aby po kilku sekundach, kiedy trasa pojawi się ponownie, przesłać nową informację, zmieniającą poprzednią. Instalując zapasową trasę statyczną umożliwisz ograniczenie rozpowszechniania informacji o migoczącej trasie do tego jednego rutera.

Kiedy trasa zniknie, ruter umieści w tablicy rutowania zapasową trasę i nie musi informować pozostałych ruterów w sieci o wystąpieniu takiej zmiany; nadal jest to najlepsza trasa, po której można osiągnąć dane miejsce przeznaczenia (nawet jeśli na tym łączu będą gubione pakiety, ponieważ nie jest ono jeszcze aktywne).

To, jakie miejsce wskaże Twoja statyczna trasa zapasowa, zależy od tego, która trasa w danym momencie jest niestabilna. Jeśli stan trasy zmienia się, ponieważ sąsiadująca z Tobą sieć wysyła do Ciebie migotanie występujące wewnątrz niej (delikatnie mówiąc, nie jest to najprzyjemniejsze), prawdopodobnie będziesz chciał skierować trasę zapasową na jeden z ruterów pracujących w tej sieci. Choć ruter ten nie musi wcale być najlepszą drogą do sieci, w której występuje problem, to może on obsługiwać inne trasy, o których nawet nie wiedziałeś. Kiedy właściwa trasa zacznie znowu poprawnie pracować, Twój ruter wymieni w swojej tablicy rutowania zapasową trasę na coś bardziej odpowiedniego. Jeśli jednak migotanie spowodowane jest zmianami stanu łącza pomiędzy Twoim ruterem a ruterem odległym i łącze to nie może być naprawione przez kilka dni, to być może należy wskazać zapasową trasę prowadzącą przez inne dobrze działające łącze (może łącze zestawiane na żądanie) lub do interfejsu zerowego rutera (w ruterach Cisco interfejs ten nazywa się null 0). Interfejs taki gubi wszystkie pakiety, które są do niego wysyłane i zawsze jest aktywny, w przeciwieństwie do uszkodzonego łącza. Kiedy uszkodzone łącze zostanie naprawione, obsługę ruchu przejmie protokół dynamiczny, trasa przestanie migotać, a zapasowa trasa statyczna przestanie być wykorzystywana. Nie musisz jednak od razu jej usuwać z konfiguracji rutera (na przykład o 2:00 w nocy, kiedy naprawiono łącze). Możesz ją usunąć wtedy, kiedy będziesz miał na to czas.

Taka sama metoda postępowania może być wykorzystana w sytuacji, w której migotanie występuje w Twojej własnej sieci i nie chcesz propagować go do sąsiednich sieci. Z punktu widzenia kilku połączonych sieci (zwłaszcza sieci Internet) lepszym rozwiązaniem jest gubienie pakietów, niż dopuszczenie do migotania tras i propagowanie tych zmian w sieci, co powoduje zwiększone obciążenie odległych ruterów.

Ograniczone rozgłaszanie tras

W Twojej sieci mogą występować *łącza,* po których nie chcesz rozsyłać uaktualnień generowanych przez dynamiczny protokół rutowania. Jednym z powodów może być fakt, że łącze pomiędzy dwoma miejscami sieci ma małą przepustowość i zdecydowałeś się na obsługiwanie go przez rutowanie statyczne. Możliwe także, że w odległej sieci nie ma urządzenia, które jest w stanie odbierać i rozumieć wysyłane tam uaktualnienia -jest to sieć końcowa, obsługiwana przez domyślną trasę statyczną. W takim przypadku nie ma sensu zajmowanie pasma przez komunikaty, które nikogo nie obchodzą.

Ograniczone rozgłaszanie tras

Interfejsy obsługujące tego typu łącza określane są mianem *interfejsów pasywnych.* Większość ruterów i protokołów rutowania pozwala na zdefiniowanie kilku, a nawet wszystkich, interfejsów rutera jako interfejsów pasywnych. Mechanizm ten wygląda różnie w różnym sprzęcie, ale zwykle przyjmuje jedną z dwóch postaci. Pierwsza wykorzystuje nazwę interfejsu stosowaną przez język konfigurowania rutera, taką jak serial 2. Druga wykorzystuje adresy IP skonfigurowanych interfejsów. W obu przypadkach wszystkie interfejsy traktowane są jako interfejsy aktywne, dopóki ruter nie powie wyraźnie, że któryś z nich ma być pasywny. W ruterze, który obsługuje kilka protokołów, zwykle każdy z protokołów przechowuje własne informacje o stanie poszczególnych interfejsów, tak więc w każdym z tych protokołów oddzielnie należy określić, który interfejs jest pasywny, a który aktywny.

W każdym z przedstawionych niżej przykładów są dwa pasywne interfejsy: jeden Ethernet i jeden interfejs szeregowy, tak więc ruter nie będzie przez nie wysyłał uaktualnień generowanych przez protokół. Numer sieci lub podsieci dołączonych do danego portu zostanie umieszczony w uaktualnieniach tras przesyłanych do innych interfejsów rutera, jeśli takie się w nim znajdują.

Zadeklarowanie interfejsu jako pasywnego nie oznacza, że nie będziesz na nim odbierał uaktualnień rutowania, które są na ten interfejs nadsyłane. Jeśli jakaś maszyna wysyła uaktualnienia w łączu dołączonym do jakiegoś interfejsu rutera, to ruter będzie je odbierał i przetwarzał niezależnie od tego, czy interfejs ten jest zadeklarowany jako pasywny czy aktywny. Może to prowadzić do powstawania wielu problemów rutowania. Rozważmy przypadek, gdzie ruter wykorzystuje informację z odległego rutera, którego nie może poinformować o swoich trasach. Sposoby zabezpieczenia się przed odbieraniem informacji o takich trasach opisane zostaną w dalszej części rozdziału.

RIP

```
router rip
 network 172.16.0.0
 network 172.17.0.0
 network 192.168.100.0
 ! suppress advertisements on these interfaces
 passive-interface ethernet 1
 passive-interface serial 0
```

OSPF

```
router ospf 1
network 0.0.0.0 255.255.255.255 area 0
! suppress advertisements on these interfaces
passive-interface ethernet 1
passive-interface serial 0
```

EIGRP

```
router eigrp 1
 network 172.16.0.0
 network 172.17.0.0
 network 192.168.100
 ! suppress advertisements on these interfaces
 passive-interface ethernet 1
 passive-interface serial 0
```

Ograniczanie źródeł informacji o rutowaniu

W poprzednim przykładzie opisywałem, jak redukować wysyłanie uaktualnień rutowania przez określona łącza. Temat jednak nie został wyczerpany. Często kiedy zablokujesz wysyłanie uaktualnień przez dany interfejs, chciałbyś również zablokować możliwość odbierania informacji o jakichkolwiek trasach, które rozgłasza dołączony do tego interfejsu ruter. Można sobie zadać pytanie: dlaczego ten ruter wysyła informacje? Odpowiedzi na nie są różne, począwszy od przyjętej w sieci polityki, a na błędach konfiguracji skończywszy. Możliwe, że chcesz ograniczyć odbieranie uaktualnień na danym interfejsie, ponieważ źródło tych uaktualnień nie jest pewne. Być może do tego łącza przyłączona jest inna domena administracyjna i nie chciałbyś, aby Twoja struktura rutowania była uszkadzana przez błędy generowane w tamtej sieci. Możliwe, że chcesz po prostu bardziej szczegółowo filtrować źródła uaktualnień. Być może chcesz odbierać niektóre uaktualnienia tras przesyłane po współdzielonym łączu, pochodzące z innego rutera, który znajduje się pod Twoją kontrolą, ale jednocześnie chcesz mieć pewność, że inne uaktualnienia, przesyłane na przykład *przez źle* pracujące urządzenia, nie będą słyszane przez Twój ruter.

Konsekwencje ograniczania informacji o rutowaniu, które docierają do rutera, są oczywiste. W najgorszym wypadku rutery, których nie słyszysz, mogą rozgłaszać jedyną trasę prowadzącą do pewnego miejsca, przez co miejsce to będzie nieosiągalne z Twojej sieci. Skutki będą mniej drastyczne, gdy rutery, których nie słuchasz, rozgłaszają lepsze trasy niż rutery, których uaktualnienia odbierasz. W takim przypadku w Twojej tablicy rutowania nie zostaną umieszczone trasy optymalne. Oczywiście kilka nieosiągalnych miejsc i nieoptymalne trasy to wyjście lepsze niż zapchanie Twojego rutera uaktualnieniami wysyłanymi z rutera, któremu nie można ufać, nie znajdującego się pod Twoją kontrolą. Powinieneś jednak zdawać sobie sprawę, że jest to zawsze „coś za coś".

Jednym ze sposobów określania, co słyszy Twój ruter, jest zmiana wartości dystansów administracyjnych. W następnej części zostaną opisane sposoby uzyskania większej kontroli nad odbieranymi informacjami o trasach, osiągane przez przepuszczanie informacji od jednych ruterów wchodzących w skład zestawu a blokowanie informacji nadsyłanych przez inne.

Ograniczanie źródeł informacji o rutowaniu

RIP

```
router rip
 network 172.16.0.0
 network 172.17.0.0
 network 192.168.100.0
 passive-interface ethernet 1
 passive-interface serial O
 ! set the default administrative distance to ignore routing updates
 distance 255
 ! set the administrative distance for these sources back to normal
 distance 120 172.16.1.0 0.0.0.255
 distance 120 172.16.2.0 0.0.0.255
 distance 120 172.16.8.0 0.0.0.255
```

W przykładzie tym wykorzystałem jeden z dwóch sposobów ograniczania odbioru nadsyłanych uaktualnień. Przypomnij sobie, że dystans administracyjny o wartości 255 traktowany jest przez oprogramowanie Cisco jako trasa nie nadająca się do użycia. Skonfigurowałem ruter w taki sposób, aby domyślnie stosował ten dystans administracyjny dla wszystkich źródeł uaktualnień RIP. Następnie dołączyłem listę źródeł RIP, które powinny być opisane domyślnym dla RIP dystansem wynoszącym 120. Pary adres-maska użyte w tych instrukcjach różnią się od wszystkich pozostałych, ale są dokładnie takie same jak pary używane w instrukcjach sieciowych protokołu OSPF. Zamiast bitu l, stosowanego w masce dla określenia, że odpowiadający mu bit w adresie jest ważny, oznaczają one, że ten bit w adresie może być dowolny (gwiazdkowy). Tak więc pierwsza instrukcja występująca po instrukcji określającej domyślny dystans mówi, że każde uaktualnienie RIP nadsyłane z rutera o adresie 172.16.1.0/24 powinno być zapisane w tablicy rutowania z dystansem administracyjnym o wartości 120.

Takie rozwiązanie jest przydatne, jeśli chcesz otrzymywać informacje o trasach od kilku ruterów, a ignorować uaktualnienia nadsyłane przez większość ruterów. Jeśli chcesz odbierać uaktualnienia wysyłane przez większość ruterów, włączając tylko kilka określonych źródeł komunikatów, powinieneś zastosować rozwiązanie opisane w przykładzie, w którym używałem protokołu EIGRP.

OSPF

Użycie dystansów administracyjnych w celu filtrowania uaktualnień tras w domenie rutowania OSPF jest bardzo niebezpiecznym rozwiązaniem, które nie jest zalecane. Aby protokół OSPF mógł poprawnie funkcjonować, każdy ruter wymaga spójnej informacji o topologii sieci, a to wymaganie nie jest spełnione, jeśli zastosujemy ograniczanie przesyłania uaktualnień tras. Z tego powodu nie będę przedstawiał żadnego przykładu ograniczania uaktualnień w sieci obsługiwanej przez OSPF. Osiągnięcie tego samego efektu jest możliwe tylko dzięki zdefiniowaniu interfejsu OSPF rutera jako pasywnego. Jeśli interfejs OSPF jest pasywny, to proces rutowania nie będzie tworzył połączenia wymiany informacji z żadnym z ruterów znajdujących się po drugiej stronie tego łącza, a sieć znajdująca się na drugim końcu tego łącza będzie traktowana jako sieć końcowa. Daje to prawie identyczny efekt, a jest znacznie bezpieczniejsze.

EIGRP

W przykładzie tym zakładam, że chcemy, aby ruter odbierał uaktualnienia od większości ruterów za wyjątkiem tych, które znajdują się w określonych podsieciach. Aby tak skonfigurować ruter, pozwalam na to, by domyślny dystans administracyjny dla EIGRP przeważał nad innymi dystansami, a w przypadku kilku wybranych tras, które odpowiadają podanym parom adres-maska, mówię ruterowi, by zastosował dystans, który określi te trasy jako nie do użycia. Jeśli będę chciał ignorować uaktualnienia nadsyłane ze wszystkich podsieci za wyjątkiem tych, które określę, to konfiguracja będzie wyglądała podobnie, jak w opisanym wcześniej przykładzie z protokołem RIP.

```
router eigrp 1
 network 172.16.0.0
 network 172.17.0.0
 network 192.168.100
 passive-interface ethernet 1
 passive-interface serial 0
 ! set the administrative distance for these sources to ignore them
 distance 255 172.16.1.0 0.0.0.255
 distance 255 172.16.2.0 0.0.0.255
 distance 255 172.16.8.0 0.0.0.255
```

Mogę nawet znacznie bardziej uszczegółowić moje ograniczenia, blokując informacje nadsyłane z pewnych ruterów, a zezwalając na pobieranie uaktualnień z innych. Aby to zrobić, wystarczy tylko dokładnie dobrać pary adres-maska w instrukcjach d i -s tańce, tak aby do każdego źródła komunikatów o uaktualnieniu tras przypisany został odpowiedni dystans. Na przykład stwierdziłem, iż rutery pracujące w sieci 172.16.8.0/24 są całkiem niezłe, ale jeden z nich, o adresie 172.16.8.24, rozsyła błędne informacje. W takim wypadku instrukcja filtrująca będzie miała postać:

```
distance 255 172.16.1.0 0.0.0.255

distance 255 172.16.2.0 0.0.0.255

distance 255 172.16.8.24 0.0.0.0
```

Aby osiągnąć ten sam efekt, w przykładzie, w którym używany jest protokół RIP, konieczne jest użycie następujących instrukcji:

```
distance 255
distance 120 172.16.1.0 0.0.0.255
distance 120 172.16.2.0 0.0.0.255
distance 255 172.16.8.24 0.0.0.0
distance 120 172.16.8.0 0.0.0.255
```

W przykładzie z RIP dwie ostatnie instrukcje wskazują ruter pracujący pod adresem 172.16.8.24. Kiedy kilka instrukcji wskazuje ten sam ruter, stosowana jest pierwsza pasująca instrukcja. Kiedy więc proces RIP określa, czy powinien przetwarzać uaktualnienie nadesłane z rutera 172.16.8.24, po dojściu do pierwszej z wymienionych wyżej instrukcji podejmowana jest decyzja o ignorowaniu tego rutera.

Możliwe jest zastosowanie dystansów administracyjnych, które pozwolą na wybranie tych uaktualnień tylko w pewnych warunkach. Być może ten błędnie pracujący ruter o adresie 172.16.8.24 jest lepszy niż nic, jeśli wszystkie inne trasy w podsieci przestaną pracować. W takim wypadku można przypisać dystans administracyjny, który będzie większy od tego, jaki odbiera zwykle dynamiczny protokół rutowania, a jednocześnie mniejszy od 255. Jeśli jednak postąpię w ten sposób, to ruter będzie ignorował każdą trasę od 172.16.8.24, którą otrzyma od innych ruterów, niezależnie od tego, jak zła jest jej miara. Tymczasem ten sam ruter chętnie będzie używał każdej trasy nadesłanej przez podejrzany ruter, jeśli tylko nie zostanie ona nadesłana przez inny ruter. Jeśli nie jest to efekt, jakiego się spodziewałeś, zastanów się nad bardziej szczegółowym określeniem dystansów administracyjnych.

Filtrowanie określonych tras z informacji uaktualnienia

Możliwe, że będziesz potrzebował bardziej wyrafinowanego filtrowania uaktualnień rutowania niż to, które można osiągnąć wykorzystując rozwiązania przedstawione w poprzednich przykładach. Na przykład chcesz otrzymywać informacje o trasach rozgłaszanych przez ruter, który nie jest pod Twoją kontrolą, ale pragniesz zablokować otrzymywanie kilku określonych tras, które ten ruter może rozgłaszać.

Potraktuj ten przykład poważnie! Parę lat temu moja sieć utraciła domyślną trasę w związku z przerwą, jaka wystąpiła na łączu z siecią Internet. Jeden z oddziałów znajdujący się w tej samej sieci kampusowej był w tym momencie w trakcie wysyłania uaktualnienia, które zawierało trasę domyślną. Trasa ta nie została odfiltrowana *przez* rutery, które ją odebrały. Te rutery wierzyły więc, że nadal mają taką trasę, i bez przerwy z niej korzystały, co spowodowało wystąpienie pętli i sporo ciekawych raportów o błędach pracy sieci. Mimo że trasa ta powinna się w pewnym momencie zestarzeć, kiedy zwiększana ciągle miara doszłaby do wartości nieskończoność, to nic takiego się nie stało, ponieważ błąd w konfiguracji jednego z ruterów pracującego w innym dziale powodował, że miara tej domyślnej trasy była ciągle *odnawiana.* Niezależnie od tego, jaką miarę dla trasy odbierał ten ruter w kolejnych uaktualnieniach, za każdym razem zmieniał tę wartość na stosunkowo niewielką i wysyłał informacje o tej trasie do innych ruterów. Problem ten mógłby nie wystąpić, gdyby na ruterach założono filtrowanie uaktualnień nadsyłanych przez rutery z tego oddziału, dzięki czemu wszelkie podejrzanie wyglądające uaktualnienia byłyby odrzucane. Taka konfiguracja działa obecnie i wszystko jest w porządku. Krótko mówiąc, staraj się stosować nitowanie zabezpieczone, ponieważ jeśli zastosujesz rutowanie bez zabezpieczeń, choćby z jednym ruterem, to jednocześnie zastosowałeś takie rutowanie ze wszystkimi ruterami, z którymi ten jeden ruter nie ma zabezpieczeń.

Jako alternatywę dla blokowania określonych tras, których nie chcemy odbierać z określonych ruterów, możesz wybrać odrzucanie wszystkich tras za *wyjątkiem* kilku wyraźnie zdefiniowanych, o których informacje chcesz otrzymywać. Oba rozwiązania mogą być stosowane na różne sposoby, aby osiągnąć spodziewany efekt. Przedstawię teraz dwie powszechnie znane możliwości. W przykładzie wykorzystującym protokół RIP pokażę, jak skonfigurować oba sposoby filtrowania tras wykorzystując wartość dystansu administracyjnego, a w przykładzie z EIGRP użyję list dystrybucyjnych.

Podobnie jak we wcześniejszych przykładach, w związku z faktem, że OSPF opiera się na wszystkich ruterach w sieci, które tworzą wspólny obraz topologii sieci, raczej nie należy stosować filtrowania zawartości uaktualnień rutowania odbieranych lub wysyłanych przez poszczególne rutery. Zamiast tego w przykładzie z OSPF opisany zostanie sposób tworzenia komunikatów OSPF wysyłanych do sąsiednich ruterów, który pozwala kontrolować, jakie trasy włączane są do Twojego systemu rutowania.

RIP

W przykładzie tym zakładam, że chcę ograniczyć źródła, z których odbieram informacje o trasach, ale jednocześnie zamierzam zaufać ruterom z sieci 172.16.1.0/241 172.16.2.0/24, niezależnie od tego, jakie informacje one nadsyłają. Takie zaufanie może być podyktowane na przykład tym, że rutery te znajdują się pod moją kontrolą. Natomiast do ruterów pracujących w sieci 172.16.8.0/24 pełnego zaufania nie mam. Dołączając listę dostępu do instrukcji distance opisującej dane łącze, mogę dowolnie definiować, które trasy będę odbierał z tej sieci.

```
router rip
 network 172.16.0.0
 network 172.17.0.0              .          .
 network 192.168.100.0
 passive-interface ethernet 1
 passive-interface serial 0
 distance 255
 distance 120 172.16.1.0 0.0.0.255
 distance 120 172.16.2.0 0.0.0.255
! set the administrative distance for these sources back to norma!
I but on Ty for routes that pass access list 1
distance 120 172.16.8.0 0.0.0.255 1
i
access-list I permit 172.16.9.0   0.0.0.255
access-list 1 permit 172.16.20.0 0.0.0.255
access-list 1 permit 172.17.0.0   0.0.255.255
access-list I deny   0.0.0.0   255.255.255.255
```

Listy dostępu to jedna z podstawowych funkcji systemu Cisco IOS. Kiedy wprowadzono je po raz pierwszy, większość ludzi zakładała, że będą one używane jako narzędzie kontroli dostępu, ograniczające wysyłanie pakietów z określonych adresów IP na interfejsy rutera. Takie wykorzystanie list dostępu omówię w rozdziale 10. Listy dostępu znalazły również szersze zastosowanie. Cisco wykorzystuje je jako sposób zapisu każdego kryterium wyboru bazującego na adresie IP.*

*Odpowiednie listy dostępu są opracowane również dla każdego innego protokołu obsługiwanego przez Cisco IOS.

Filtrowanie określonych tras z informacji uaktualnienia

W innych ruterach wykorzystywane są inne rozwiązania, czasem kilka różnych, które pozwalają spełnić takie same funkcje.

W naszym przykładzie lista dostępu określa, które trasy nadsyłane z sieci 172.16.8.0/24 mogą być odbierane przez konfigurowany właśnie ruter. Instrukcja access-list pozwala odległym ruterom na przesyłanie do mojego rutera informacji o trasach z sieci 172.16.9.0/24, 172.16.20.0/24 oraz 172.17.0.0/16 i żadnych innych. Sprawdzanie zgodności z listą dostępu jest działaniem bezpośrednim. Każdy nadsyłany adres porównywany jest z parą adres-maska zgodnie z kolejnością umieszczenia w liście dostępu instrukcji opisujących warunki. Kiedy porównanie zakończy się sukcesem, wykonywane jest określone w instrukcji działanie (zezwolenie lub zabronienie) i kończy się przeszukiwanie listy. Gdy cała lista zostanie przeanalizowana i nie nastąpi zakończone sukcesem porównanie z żadnym z warunków, wtedy zadziała ostatni warunek zabraniający wszystkiego (który został wyróżniony w przykładzie) i adres będzie odrzucony. Zwróć uwagę na to, że trasy, które docierają do mojego rutera, nie muszą dokładnie odpowiadać tym podsieciom. Podsieci o adresach 172.17.0.0/16 przejdą pomyślnie porównanie z listą dostępu i zostaną przeanalizowane przez protokół rutowania. . . . ,.

Sposób przetwarzania list dostępu oparty na kolejnym sprawdzeniu instrukcji sprawia, że są one łatwo analizowane przez ruter, ale dość trudno je edytować. Nie jest możliwe zwykłe dodanie nowego zapisu do listy, na jej końcu (co jest jedyną operacją, poza możliwością usunięcia zapisu, wykonywaną na listach w systemie Cisco IOS). Takie umieszczenie warunku nie da spodziewanych wyników, ponieważ nowy zapis znajdzie się na końcu i nigdy nie będzie przetwarzany. W rozdziale 8 prezentuję kilka wskazówek i porad, które pozwalają poradzić sobie z tym ograniczeniem.

W tym przykładzie zakładam, że nie chcę, aby do mojego rutera docierały informacje propagowane przez większość ruterów. Jeśli chciałbym, aby mój ruter odbierał informacje o wszystkich docierających do niego trasach za wyjątkiem tych, które uważam za błędne, to taki sam poziom kontroli nad ruterami z sieci 172.16.8.0/24 osiągnę używając instrukcji distance i takiej samej listy dostępu:

```
distance 120 172.16.8.0 0.0.0.255 l
distance 255 172.16.8.0 0.0.0.255
```

W przedstawionych instrukcjach akceptuję wszystkie trasy opisane normalnym dystansem administracyjnym dla protokołu RIP (120). Następnie deklaruję, że wszystkie rutery w sieci 172.16.8. 0/24, które spełniają warunki listy dostępu numer l, powinny być również akceptowane z dystansem 120. Na końcu deklaruję, że wszystkie inne trasy rozgłaszane przez rutery pracujące w sieci 172.16.8.0/24 powinny być ignorowane poprzez nadanie im wartości dystansu 255.

OSPF

Konieczność posiadania tego samego obrazu topologii sieci przez wszystkie rutery pracujące w sieci obsługiwanej przez OSPF sprawia, że filtrowanie tras w takiej sieci jest trochę kłopotliwe. Zgodnie z podstawową zasadą, wszystkie rutery powinny znajdować się w jednej domenie administracyjnej wchodzącej w skład domeny rutowania OSPF.

Zdarzają się jednak przypadki, kiedy chciałbyś, aby odległy ruter (lub rutery) mógł wymieniać informacje o rutowaniu z ruterami pracującymi w Twojej sieci. Można to osiągnąć przez uruchomienie dwóch procesów rutowania OSPF na jednym ruterze (lub ruterach), który musi wymieniać informacje z innymi ruterami. Pierwszy proces OSPF pozwoli na wymianę informacji pomiędzy ruterami znajdującymi się pod Twoją kontrolą. Proces ten może zostać skonfigurowany bez żadnych ograniczeń nakładanych na informacje o rutowaniu, ponieważ Twoje rutery przesyłają poprawne informacje (miejmy nadzieję!). Drugi proces OSPF będzie skonfigurowany tak, by mógł wymieniać informacje o rutowaniu z odległymi hostami. Aby pozwolić na rozgłaszanie informacji nadsyłanych przez odległe rutery w Twojej sieci, konieczne będzie skonfigurowanie kontrolowanej redystrybucji informacji pomiędzy procesami, które będzie przepuszczało tylko informacje o trasach, które Cię interesują. Szczegóły dotyczące funkcjonowania redystrybucji mogą wydać się niejasne. Poniżej przedstawiam prosty przykład, w którym pozwalam ruterom odbierać informacje o wszystkich trasach przesyłanych przez odległe rutery za wyjątkiem trasy domyślnej:

```
! start an OSPF process for my routers router
ospf 1
  network 172.16.0.0 0.0.255.255 area 0
  redistribute ospf 2 route-map nodefault metric 1
! start a second OSPF process for the foreign routers router ospf 2
  network 192.168.128.0 0.0.0.255 area O
! define route maps to block the default route from the foreign routers route-map nodefault
deny match ip address 1
!
route-map nodefault permit match
ip address 2
!
access-list 1 permit 0.0.0.0 0.0.0.0
!
access-list 2 permit 0.0.0.0 255.255.255.255
```

W przykładzie tym uruchomiłem dwa procesy OSPF. Pierwszy z nich (obsługujący moje rutery) uruchomiony jest na wszystkich interfejsach sieci 172.16.0.0/16. Drugi proces (obsługujący odległe rutery) uruchomiony jest na wszystkich interfejsach (prawdopodobnie jest to tylko jeden interfejs) znajdujących się w sieci 192.168.128 .0/24. Sztuka polega na określeniu sposobu, w jaki trasy będą kontrolowane przy przechodzeniu pomiędzy obiema domenami OSPF.

Filtrowanie określonych tras z informacji uaktualnienia

W systemie Cisco IOS definiuje się *mapę tras,* która określa przetwarzanie informacji o trasach. Każda z map tras ma nazwę i możliwe jest współdzielenie tej samej nazwy przez wiele różnych map. Kiedy pod jedną nazwą zdefiniowanych zostanie kilka map, to przetwarzane są one w kolejności, w jakiej znalazły się w konfiguracji.

Każda mapa tras definiuje zestaw warunków o nazwie *match,* które są stosowane do filtrowania informacji. Możliwe jest również zdefiniowanie jednego lub więcej działań *set,* które pozwalają na dokładne określenie parametrów stosowanych w danym protokole rutowania; działań tych nie ma w naszym przykładzie. Każda mapa tras definiuje ponadto rozdział tras, które spełniają jej warunki i mogą być odebrane przez dany ruter.

W naszym przykładzie skonfigurowałem dwie mapy tras o nazwie nodefault. Pierwsza z nich mówi, że każda trasa (adres), która spełnia warunki stawiane w liście dostępu numer l, spełnia również warunki tej mapy i zostanie odrzucona. Kiedy porównanie z kolejnym warunkiem zakończy się sukcesem, nie są brane pod uwagę dalsze mapy tras, co zapobiega rozgłaszaniu tras, które spełniają warunki listy dostępu numer 1. W naszym przykładzie domyślna trasa pasuje do warunków określonych w liście dostępu numer 1. Druga mapa tras mówi, że każda trasa, która pasuje do listy dostępu numer 2, spełnia również warunki tej mapy i jej odebranie przez ruter jest możliwe. W omawianym przypadku do listy dostępu numer 2 pasują wszystkie trasy. Obie definicje razem wskazują, że domyślna trasa będzie odfiltrowana, a wszystkie inne trasy będą odebrane i propagowane w sieci.

Pozostaje tylko dołączenie mapy tras do tras obsługiwanych przez drugi proces OSPF i ich redystrybucja w podstawowym procesie OSPF. Funkcję tę można uruchomić poleceniem redistribute. Polecenie `redistribute` użyte w naszym przykładzie informuje ruter, że proces OSPF o numerze 1 (ten, który obsługuje rutery w naszej sieci) powinien odbierać wszystkie trasy przesyłane mu przez proces numer 2 (obsługujący odległe rutery), które przeszły przez mapę tras o nazwie `nodefault`. Trasy te powinny być ponadto zapisane z miarą równą 1. Trasy takie będą domyślnie dystrybuowane w sieci przez nasze rutery jako zewnętrzne trasy typu 2.

Jak widać, próba uruchomienia protokołu OSPF na zestawie ruterów, z których nie wszystkie są pod naszą kontrolą, może się szybko stać konfiguracyjnym koszmarem. Opisany przykład był jednym z najprostszych, a i tak jest dość złożony. Jeśli będziesz chciał uzyskać większą kontrolę nad odbieranymi informacjami o trasach lub zechcesz dokładnie określić każdy z wielu różnych parametrów pracy protokołu OSPF, konfiguracja będzie tak trudna, iż zarządzanie nią stanie się prawie niemożliwe.

EIGRP

W przykładzie tym używam listy dystrybucyjnej do kontrolowania, które informacje o trasach ruter ma odbierać i na których interfejsach maje rozgłaszać. Zwróć uwagę, że jest to pierwszy przykład, który wybiórczo traktuje rozgłaszanie informacji, a nie tylko pozwala na zdefiniowanie adresów ruterów, od których mają być odbierane informacje.

```
 router eigrp 1
 network 172.16.0.0
 network 172.17.0.0
 network 192.168.100
! fliter EIGRP from ethernet 2 through access list 12, and EIGRP to be! sent on
serial I through access list 22
 distribute-list 12 in ethernet 2
 distribute-Ust 22 out serial


access-list     12  permit 172.17.0.0  0.0.255.255
access-list     12  deny 0.0.0.0        255.255.255.255
!
access-list  22 deny 192.168.128.0  0.0.0.255
access-list  22 permit 0.0.0.0      255.255.255.255
```

Instrukcja distribute-list in określa, które trasy docierają do rutera. Instrukcja ta informuje ruter o tym, że powinien przetwarzać wszystkie uaktualnienia odbierane z określonego interfejsu (ethernet 2) po odfiltrowaniu ich w oparciu o listę dostępu 12 i pozwolić na dalsze przesłanie tylko tych tras, które przejdą przez tę listę dostępu. Oznacza to, że tylko trasy spełniające warunki listy dostępu numer 12 będą odbierane *przez* interfejs ethernet 2. Zwróć uwagę na fakt, że opisywany mechanizm nie pozwala zastosować różnych reguł bazujących na adresie rutera źródłowego. Do tego celu konieczne jest użycie dystansów administracyjnych.

W podobny sposób użyłem instrukcji distribute-listoutdo kontroli tego, co ruter będzie rozgłaszał na danym interfejsie. Poinformowałem ruter, że chcę rozgłaszać tylko trasy prowadzące do adresów spełniających warunki listy dostępu 22 na interfejsie serial 1. Ponieważ lista dostępu numer 22 pozwala na przejście wszystkich tras za wyjątkiem tras do sieci 192.168.128.0/24, ruter nie będzie rozgłaszał tras do tej sieci i do jej podsieci przez interfejs serial I. Podobnie jak w przypadku instrukcji distribute-list in, nie jest możliwe zastosowanie różnych reguł rozgłaszania opartych na parametrach innych niż nazwa interfejsu. Jeśli jednak przypomnisz sobie, że komunikaty zawierające uaktualnienia tras są zwykle typu *broadcast* lub *multicast,* to okazuje się, że nie ma sensu próbować żadnych bardziej zaawansowanych metod.

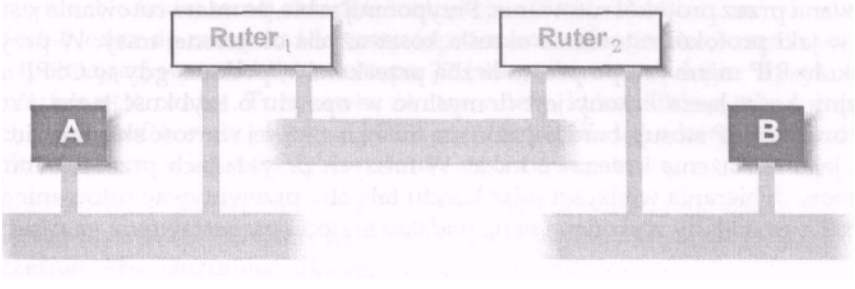
Rutowanie dynamiczne z użyciem wielu ścieżek

Jedną z bardziej przydatnych i interesujących funkcji, które będziesz musiał skonfigurować, jest obsługa rutowania dynamicznego wykorzystującego istnienie wielu tras pomiędzy dwoma różnymi punktami w sieci. Oczywiste jest, że jeśli zaprojektowałeś sieć posiadającą zapasowe łącza, to chciałbyś, aby były one wykorzystywane w przypadku wystąpienia awarii. Chciałbyś również, aby te ścieżki mogły służyć do obsługi równoważenia ruchu w sieci.

Kontrolowanie wyboru tras w sieci posiadającej wiele równoległych ścieżek nie jest zadaniem łatwym. Ponieważ każdy ruter podejmuje własne decyzje o tym, jak ma rutować pakiety, możliwe, a nawet bardzo prawdopodobne jest, że rutery pracujące w różnych częściach Twojej sieci będą wybierały różne trasy. Pakiety przesyłane z hosta A do B mogą podróżować po jednej trasie, podczas gdy pakiety przesyłane z hosta B do A mogą podróżować po innej trasie.

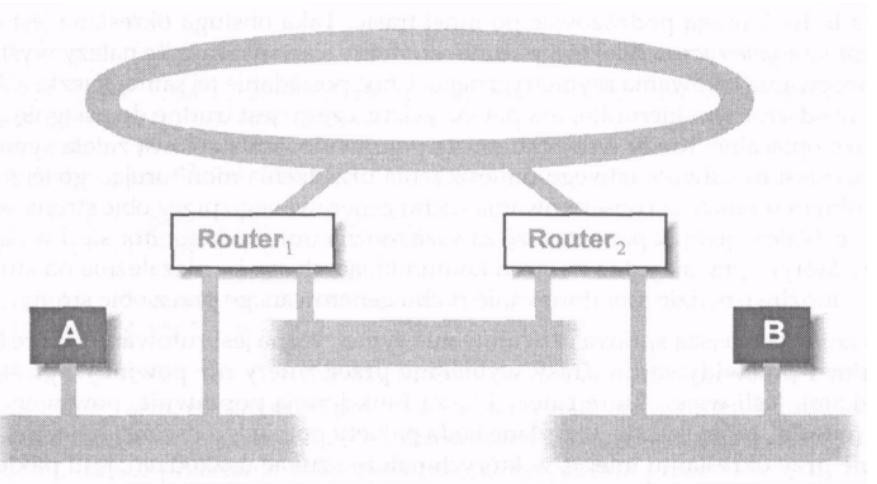
hosta B do A mogą podróżować po innej trasie. Taka obsługa określana jest nazwą *nitowanie asymetryczne*. Niektórzy administratorzy sieci uważają, że należy wystrzegać się stosowania rutowania asymetrycznego. Choć posiadanie tej samej ścieżki z A do B, jak i w odwrotnym kierunku, ma pewne zalety, często jest trudne do osiągnięcia i nie zawsze opłacalne. Kiedy wszystko działa poprawnie, podstawową zaletą symetrycznej sieci jest możliwość łatwego umieszczenia urządzenia monitorującego jej pracę w dowolnym segmencie i obserwowania ruchu generowanego przez obie strony w danej ścieżce. Należy jednak pamiętać, że zawsze można umieścić monitor sieci w segmencie, w którym pracuje jedna ze stron komunikujących się, i - niezależnie od struktury sieci - możliwe będzie monitorowanie ruchu generowanego przez obie strony.

Znacznie ważniejszą sprawą niż nitowanie symetryczne jest rutowanie, które będzie stabilne i przewidywalne. Trasy wybierane przez rutery nie powinny być ślepymi uliczkami. Jeśli wiesz, które rutery i łącza funkcjonują poprawnie, powinieneś móc sam określić, którą ścieżką wysyłane będą pakiety pomiędzy dwoma hostami. Jest to ważne przy określaniu miejsc, w których należy szukać uszkodzeń, jeśli pakiety nie będą przesyłane poprawnie. Jeśli masz np. trzy segmenty sieci, połączone ze sobą przez dwa rutery, jak pokazano na rysunku 6-4, oczywiste jest, że pakiety przesyłane z hosta A do hosta B muszą przejść przez wszystkie trzy segmenty sieci, poczynając od strony lewej rysunku, a kończąc na prawej. Jeśli zdarzy się, że pakiety przestaną docierać do odbiorcy, to masz jasno określony zestaw tras, po których powinny one podróżować, i łatwo wtedy określić miejsca, w których mogły wystąpić uszkodzenia.



Rysunek 6-4: Pakiety przesyłane z hosta A do hosta B muszą przejść przez wszystkie trzy segmenty

Jeśli pomiędzy dwoma ruterami dodasz łącze zapasowe (powiedzmy, pierścień FDDI), to pakiety przesyłane z A do B będą mogły podróżować łączem umieszczonym na górze rysunku lub na dole. Gdy pakiety nie dotrą do punktu przeznaczenia, które łącze należy sprawdzać? Jeśli rutowanie w Twojej sieci jest przewidywalne, będziesz wiedział, które łącze należy sprawdzać, co znacznie skróci czas lokalizowania i usunięcia uszkodzenia, zwłaszcza jeśli Twoja sieć składa się z kilkudziesięciu ruterów i kilkuset segmentów.



Rysunek 6-5: Jeśli dodane zostanie drugie łącze, ścieżka, po której przesyłane są pakiety z A do B, staje się trudna do przewidzenia

Sposób, w jaki można osiągnąć stan przewidywalności rutowania, zależy od topologii sieci i stosowanego protokołu rutowania. Decyzje podejmowane przez ruter oparte są na kilku kryteriach, a każdy z protokołów w różny sposób wpływa na te decyzje. Mówiąc ogólnie, podstawowym elementem, który można kontrolować, jest miara stosowana przez protokół rutowania. Przypomnij sobie, że miara rutowania jest sposobem, w jaki protokół rutowania określa koszt użycia określonej trasy. W przypadku protokołu RIP miara jest po prostu liczbą przeskoków, podczas gdy w OSPF administracyjny koszt łącza liczony jest domyślnie w oparciu o szybkość łącza. Protokoły IGRP oraz EIGRP stosują bardziej złożoną miarę, na której wartość składają się: pasmo łącza, jego obciążenie i niezawodność. W naszych przykładach przedstawimy kilka sposobów dobierania wielkości miar kosztu tak, aby przewidywać rutowanie w sieci. Wszystkie przykłady wykonane są na podstawie sieci i przedstawione na rysunku 6-5.

RIP

Protokół RIP nie wie nic o paśmie i stopniu wykorzystania poszczególnych łączy w sieci. Ruter podejmuje decyzje o rutowaniu pakietów tylko i wyłącznie na podstawie miary protokołu RIP, która jest licznikiem przeskoków na drodze do miejsca przeznaczenia. W naszym przykładzie przeskok przez sieć Ethernet jest traktowany na równi z przeskokiem przez pierścień FDDI. Ruter korzystający z protokołu RIP nie będzie w stanie wykorzystać zalet zwielokrotnionych ścieżek. Zamiast tego ustawia się na pierwszą trasę, którą usłyszy, i zmieni ją na trasę opisaną niższą miarą tylko w przypadku, gdy wcześniej wybrana ścieżka ulegnie uszkodzeniu.*

Rutowanie dynamiczne z użyciem wielu ścieżek

Ponieważ nie jest możliwe przewidywanie kolejności, w jakiej do rutera dotrą informacje o poszczególnych ścieżkach, aby móc przewidywać nitowanie, konieczne jest porównywanie miary jednej ścieżki z miarą drugiej. Jedną z najprostszych metod jest użycie instrukcji o f f s et-l i s t ln oraz off s e t-1 i st o ut. Należy jednak używać ich bardzo ostrożnie! Nieostrożne i nieprzemyślane zastosowanie takiej kompensacji do miar poszczególnych tras może łatwo spowodować zapętlenie rutowania i wystąpienie czarnych dziur.

```
router rip
 network 172.16.0.0
 network 172.17.0.0
 network 192.168.100.0 ! increase the metric for all routes learned or sent over
ethernet 4
 offset-list 32 in  l ethernet 4
offset-list 32 out l ethernet 4

access-list 32 permit 0.0.0.0 255.255.255.255
```

W przykładzie tym instrukcja offset -list mówi ruterowi, że wszystkie uaktualnienia odbierane na porcie ethernet 4, które spełniają wymagania listy dostępu numer 32, mają mieć miarę powiększoną o jeden (oprócz powiększenia wartości miary wynikającego z dodania kolejnego przeskoku). Ponieważ lista dostępu 32 przepuszcza wszystkie trasy, wszystko, co ruter usłyszy na porcie ethernet 4, będzie miało miarę o jeden większą od tras odebranych na interfejsie *fddi 1*. W rezultacie trasy odebrane na interfejsie *fddi 1* będą preferowane zawsze, kiedy łącze to będzie działało poprawnie. Na takiej samej zasadzie instrukcja o f f s e t-l i s t out mówi ruterowi, że ma dodać jeden do miary każdej trasy (oprócz normalnego zwiększania wartości miary), spełniającej warunki listy dostępu 32 (wszystkie trasy), która wysyłana jest przez interfejs ethernet 4. To sprawia, że inne rutery, które odbiorą taką informację o trasach, będą preferowały pierścień FDDI jako ścieżkę dla wysyłanych pakietów. Po takim określeniu miar segment Ethernet staje się trasą zapasową.

Generalnie lepiej jest jednak stosować kompensację miary tylko dla uaktualnień tras nadsyłanych do rutera albo tylko dla uaktualnień wysyłanych z rutera, a nie dla obu równocześnie. Aby zrozumieć, dlaczego należy tak postępować, zastanówmy się, co się będzie działo, jeśli jeden z ruterów z naszego przykładu zastosuje kompensację w przeciwnym kierunku dla informacji przychodzących i wychodzących:

```
offset-list 32 in  1 fddi 2

offset-list 32 out 1 fddi 2
```

Pomińmy przez chwilę fakt, że mało prawdopodobne jest, abyś przedkładał Ethernet nad pierścień FDDI.

*System Cisco IOS będzie wykorzystywał zwielokrotnione ścieżki o takim samym koszcie, nawet jeśli pochodzą one z protokołu RIP. Wykonywane jest przy tym coś w rodzaju równoważenia ruchu przez kilka ścieżek, a jego działanie zależy od innych czynników konfiguracji rutera, których nie będziemy w tej książce omawiali.

Rezultat takiej konfiguracji będzie taki, że pierwszy ruter z naszej przykładowej sieci będzie preferował FDDI i wymuszał na drugim ruterze to samo, podczas gdy drugi ruter będzie próbował faworyzować segment Ethernet i wymuszał na pierwszym takie samo postępowanie. Rezultatem będzie znoszenie się działań obu ruterów; żadna z sieci nie będzie preferowana, a pakiety będą przesyłane trasą, którą ruter usłyszy jako pierwszą.

OSPF

W przeciwieństwie do protokołu RIP, OSPF posiada informacje o paśmie łącza w sieci, ale informacje te nie są uzyskiwane bezpośrednio z łącza. Każde łącze wchodzące w skład sieci ma określony koszt, nadany przez protokół OSPF. Domyślnie koszt łącza liczony jest zgodnie ze wzorem:

$$\frac{10^8}{\text{pasmo}}$$

Policzone w ten sposób koszty dla różnych łączy pokazano w tabeli 6-2. Tabela 6-2.

Domyślne koszty OSPF dla różnych szerokości pasma sieci

Pasmo łącza	*Domyślny koszt OSPF*
Łącze szeregowe 56 kbps	1785
Łącze szeregowe 64 kbps	1562
Łącze szeregowe T1 (1,544 Mbps)	
Łącze szeregowe E1 (2,048 Mbps)	
Token Ring 4 Mbps	25
Ethernet	10
Token Ring 16 Mbps	
FDDI lub FastEthernet	1

W związku z istnieniem domyślnych kosztów ruter pracujący z protokołem OSPF automatycznie będzie przedkładał pojedynczy przeskok przez łącze FDDI nad pojedynczy przeskok przez segment Ethernet. Dlatego zmieniłem naszą przykładową sieć tak, by zapasowe łącza były jednakowe (Ethernet), dzięki czemu ich domyślny koszt będzie równy.

OSPF jest przeciwieństwem protokołu RIP w jeszcze innym zakresie. Kiedy OSPF obsługuje kilka ścieżek o równym koszcie prowadzących do tego samego miejsca, wszystkie one będą wykorzystywane równocześnie w wyniku zastosowania funkcji równoważenia ruchu. Prawdopodobnie to chciałbyś osiągnąć. Jeśli jednak nie chcesz, aby tak było, konieczna będzie zmiana kosztu poszczególnych łączy. Taka zmiana może być wymaganą ze względów bezpieczeństwa lub dlatego, że w Twojej sieci wykonywane są jakieś procesy czasu rzeczywistego, które nie będą tolerowały nadsyłania pakietów w niewłaściwej kolejności lub z różnymi opóźnieniami. Aby zademonstrować ten przykład, przystosowałem odpowiednio koszty poszczególnych łączy.

```
interface ethernet 1
 ip address 172.16.1.1 255.255.255.0 ! change the cost of this interface
to mąkę it less preferred
 ip ospf cost 11
!
interface ethernet 2 ip address 172.16.2.1 255.255.255.0 ! explicitly set the default
cost as a retninder that it is what we want
 ip ospf cost 10

router ospf 1
 network 0.0.0.0 255.255.255.255 area 0
```

Koszt segmentu sieci podpiętego do interfejsu ethernet 1 ustawiłem na 11, a dla interfejsu ethernet 2 ustawiłem 10 (wartość domyślna). Taka konfiguracja sprawia, że interfejs ethernet 2 obsługuje trasę preferowaną. Mogłem pozostawić koszt interfejsu ethernet 2 jako domyślny (równy 10), ale podając go w konfiguracji mamy pewność, że taka wartość będzie przypisana. Za każdym razem, kiedy odchodzisz od wartości domyślnych, dobrze jest zdefiniować ręcznie również niezmienione wartości domyślne. Pozwoli to pamiętać, jakie są te wartości domyślne oraz zaznaczyć, że wartości kosztów tych interfejsów są wartościami domyślnymi.

EIGRP

Protokół RIP wykorzystuje w normalnych warunkach tylko jedną ścieżkę, nawet jeśli dostępnych jest kilka ścieżek o tym samym koszcie. Implementacja tego protokołu na ruterze może pozwalać na równoczesne użycie kilku ścieżek o tym samym koszcie, ale jest to rozwiązanie specyficzne dla danej implementacji i nie jest opisane w specyfikacji protokołu. Protokół OSPF potrafi wykorzystywać zastępczo ścieżki o takim samym koszcie, ale wszystkie inne ścieżki, mające wyższy koszt, nie będą używane wcale. EIGRP różni się od obu wspomnianych wcześniej protokołów, ponieważ nie tylko potrafi wykorzystywać wiele ścieżek o tym samym koszcie, ale także ścieżki, dla których koszt jest różny. Ponadto każda ze ścieżek jest używana do przesyłania ilości danych odwrotnie proporcjonalnej do kosztu tej ścieżki.

W naszym przykładzie powróciłem do początkowej konfiguracji sieci, w której jednym ze zdublowanych łączy jest Ethernet, a drugim - pierścień FDDI. Instrukcja variance pozwala na poinformowanie rutera, że ma akceptować do czterech ścieżek, które będą gorsze od najlepszej ścieżki (jest to definiowane w implementacji Cisco). Ścieżki te będą używane zgodnie z odwrotnością proporcji ich miar. Tak więc ścieżka, która jest trzy razy gorsza od najlepszej ścieżki, będzie używana tylko w jednej trzeciej tego, co jest przesyłane przez najlepszą ścieżkę.

```
router eigrp 1
 network 172.16.0.0
 network 172.17.0.0
 network 192.168.100
 ! a 11 ów unequal cost paths to be considered for use
 variance 10
```

Znalezienie najlepszych wartości dla poszczególnych ścieżek będzie wymagało przeprowadzenia kilku eksperymentów. Zwiększając różnice pomiędzy kosztami pozwalasz ruterowi brać pod uwagę coraz gorsze ścieżki. Jeśli jednak rozbieżności będą zbyt duże, to użyta może być również ścieżka, której nigdy nie planowałeś wykorzystywać. Dobrze jest początkowo skonfigurować sieć z zastosowaniem różnic równych l (domyślnie), a następnie powolnie je zwiększać aż do momentu, kiedy ruter zacznie wykorzystywać do transmisji trasy z tablicy rutowania, które są na granicy dopuszczalności. Zwiększanie różnic należy zakończyć przed wartością, przy której ruter zacznie wykorzystywać trasy, jakich nie chcesz używać.

Jednoczesne użycie wielu protokołów rutowania

Jeśli możesz, powinieneś wybrać jeden protokół IGP i zastosować go w całej swojej sieci. Każdy protokół pracuje inaczej i rzadko zamiana miar jednego protokołu na miary innego wykonywana jest poprawnie. Rozważmy np. równoczesne użycie protokołów EIGRP i RIP. Oba są protokołami typu dystans-wektor i dlatego zachowują się mniej więcej podobnie. Zastanów się jednak, w jaki sposób dokonać zamiany miar RIP, określających tylko liczbę przeskoków, na złożone miary EIGRP, ustalane w oparciu o pasmo, opóźnienie, obciążenie łącza itd.? Pomyśl, co się będzie działo, jeśli jednym z używanych w sieci protokołów będzie OSPF, protokół stanu łącza. Tłumaczenie jednej miary na drugą będzie w takim przypadku jeszcze mniej poprawne.

Mimo to często nie masz większego wyboru, jeśli chodzi o zastosowanie kilku dynamicznych protokołów rutowania w swojej sieci. Dwa najczęstsze powody to chęć obsługi dynamicznego rutowania z ruterami należącymi do innej domeny administracyjnej oraz fakt, że jesteś w trakcie przechodzenia z używania jednego protokołu w sieci na używanie drugiego. Niezależnie od tego, jakie są powody, dla których stosujesz więcej niż jeden protokół rutowania w swojej sieci, dobrze jest mieć jasno określoną granicę pomiędzy tymi dwoma protokołami (chyba nie myślałeś poważnie o zastosowaniu trzech protokołów?). Jeśli to tylko możliwe, postaraj się, aby granica podziału pomiędzy dwiema domenami rutowania przebiegała przez jeden lub dwa rutery. Takie rozwiązanie ograniczy problemy związane z obsługą kilku protokołów pracujących na jednym ruterze do kilku ruterów w sieci.

W naszym przykładzie dotyczącym stosowania kilku protokołów rutowania zakładam, że masz do czynienia z siecią kampusową, w której protokołem rutowania jest EIGRP. Jednak oddział firmy znajdujący się nieopodal, który obsługuje własną sieć, chce ją dołączyć do Twojej sieci. Jedyny problem polega na tym, że w oddziale jest używany protokół RIP, być może w związku z jego łatwym stosowaniem lub dlatego, że jest to jedyny protokół, obsługujący wszystkie znajdujące się tam rutery. Masz więc do wyboru trzy rozwiązania:

- zaimplementować w ich sieci protokół EIGRP;
- zaimplementować protokół RIP w swojej sieci;
- uruchomić dwa protokoły rutowania na ruterze z Twojej sieci, do którego dołączona będzie sieć tego oddziału.

Jednoczesne użycie wielu protokołów rutowania

Pierwsza opcja - o ile możliwa do zastosowania - jest prawdopodobnie najlepszym rozwiązaniem, ponieważ nie zetkniesz się z problemami związanymi z obsługą więcej niż jednego protokołu na ruterze. Jeśli jednak firma nie może zmienić protokołu lub chce pozostać przy używanym dotychczas, to opcja ta jest niedostępna. Druga możliwość jest identyczna, lecz działa w odwrotną stronę. Dlaczego masz zrezygnować z zalet Twojej porządnie skonfigurowanej sieci tylko dlatego, że będzie ona dołączona do innej sieci? Co się stanie, jeśli w przyszłości zechcesz dołączyć sieć kolejnego oddziału, w której używany będzie jeszcze inny protokół? Nie możesz ciągle zmieniać swojego protokołu rutowania tylko po to, by dopasować sieć do konfiguracji dołączanych do niej nowych segmentów.

Tak więc pozostaje zdecydowanie się na użycie dwóch protokołów na ruterze, do którego dołączysz sieć wspomnianego oddziału. Po pierwsze, musisz jasno określić stawiane sobie cele. Pierwszym z nich jest ochrona stabilności własnego systemu rutowania. Jeśli taki cel nie *znalazł* się dotychczas na Twojej liście, to popełniasz duży błąd. Choć jest mało prawdopodobne, aby administrator sieci pracujący w innym oddziale specjalnie chciał zakłócić pracę Twojej sieci, należy pamiętać o tym, że błędy konfiguracji czasem się zdarzają. Poza tym tamten administrator powinien być równie ostrożny. Będzie chciał zabezpieczyć swoją sieć przed błędami, jakie Ty możesz popełniać. Jednym z najlepszych sposobów ochrony stabilności rutowania jest wyraźne wskazanie tras przesyłanych przez odległe rutery, które będą akceptowane przez Twoją sieć. Jeśli nie chcesz zmieniać konfiguracji swojej sieci za każdym razem, kiedy tamten oddział doda jakąś nową sieć, możesz po prostu wymienić trasy, których nie będziesz akceptował, jeśli informacje o nich będą przesyłane z tamtej sieci. Na tej liście znajdą się prawdopodobnie trasy prowadzące do Twojej sieci oraz do innych sieci, o których na pewno nie chcesz nigdy słyszeć z ruterów pracujących w tamtej sieci. Nie chcesz również akceptować domyślnych tras do innych sieci, jeśli jesteś połączony ze światem własnymi łączami.

Drugim celem, jaki powinieneś sobie postawić, jest zapewnienie pozostałym ruterom w Twojej sieci zwięzłej informacji o tych odległych trasach, przy jednoczesnym zapewnieniu poprawnego rutowania pomiędzy sieciami. Nie chcesz np. rozgłaszać tras do podsieci przesyłanych do Twojego rutera z dołączonej sieci, jeśli znajdujesz się w innych sieciach IP.

Twoim trzecim celem powinna być optymalizacja sposobu, w jaki Twoja sieć wybiera ścieżki prowadzące do sieci Twoich sąsiadów, zwłaszcza jeśli połączony jesteś z nimi w dwóch lub więcej miejscach. Aby to zrobić, należy wybrać poprawny sposób zamiany miar stosowanych przez protokół z tamtej sieci na miary Twojego protokołu. Jeśli sieci połączone są tylko w jednym miejscu, łatwo możesz określić domyślną wartość dla wszystkich miar tras z sąsiedniej sieci na wartość stosowaną w Twoim protokole rutowania.

Na szczęście, nowsze protokoły rutowania, takie jak EIGRP oraz OSPF, mogą obsługiwać różne typy tras. W obu tych protokołach trasy nadsyłane z zewnątrz są oznaczane jako trasy zewnętrzne i w specjalny sposób przetwarzane przez odbierające je rutery.

Protokół RIP nie obsługuje takiego rozwiązania, przez co trasy odbierane z zewnątrz i zapisywane w tablicy rutowania nie są odróżniane od tras wewnętrznych.

Po określeniu sposobu przetwarzania informacji nadsyłanej do Twojej sieci przez sąsiada musisz zdecydować, jakie informacje o swojej sieci chcesz mu przekazywać. Jeśli Twoja sieć jest jedynym zewnętrznym połączeniem dla tej sąsiedniej sieci, najprościej będzie wysłać do ich ruterów informację o trasie domyślnej. Jest to również najczęściej występujący przypadek. W innym przypadku, kiedy sąsiadująca sieć ma kilka połączeń z różnymi grupami, domyślna trasa może nie być najlepszym rozwiązaniem. W takim przypadku musisz upewnić się, czy to, co wysyłasz do ich sieci, zawiera wszystkie wymagane informacje, zapisane w formacie, z którego mogą korzystać, i pozwala na policzenie optymalnych tras prowadzących do Twojej sieci, bez niepotrzebnego powiększania tablic rutowania w ich ruterach.

```
router eigrp 71
 network 172.16.0.0
! pass my neighbor's routes into my network via EIGRP with a default \ metric
 redistribute rip
default-metric 10000 250 255 1 1500
!
router rip
 network 172.30.0.0
! pass my routes to my neighbor via RIP with a metric of 1
 redistribute igrp 71
 default-metric 1
 ! limit what I hear from my neighbor, and only send him the default
! route
 distribute-list 11 in
 distribute-list 12 out igrp 71

access-list 11 permit 172.30.0.0 0.0.255.255
access-list 11 permit 192.168.15.0 0.0.0.255
access-list 11 deny 0.0.0.0 255.255.255.255
!
 access-list 12 permit 0.0.0.0 0.0.0.0
```

W tym przykładzie uruchomiłem proces EIGRP w celu komunikowania się z rutera-mi pracującymi w mojej sieci. Uruchomiłem również proces RIP, który pozwoli mi komunikować się z ruterami moich sąsiadów. Każdemu z protokołów rutowania kazałem rozgłaszać swoje trasy rutowania do drugiego procesu i przypisywać im poprawną domyślną miarę. Dla RIP ta domyślna miara jest liczbą przeskoków wynoszącą 1. Natomiast dla EIGRP miara jest trochę bardziej złożona, dlatego muszę określić wartości wszystkich elementów, w oparciu o które jest ona wyznaczana. Elementy te oraz ich wartości, które skonfigurowałem, są następujące:

pasmo łącza (w kbps):	10000
opóźnienie trasy (x 10 us):	250
niezawodność (0-255)	255
obciążenie (0-255)	1
MTU ścieżki:	1500

Wartości te określają mało obciążone i bardzo niezawodne łącze sieci Ethernet. Jeśli obciążenie Twojej sieci jest większe, powinieneś podać większą wartość obciążenia łącza. Jeśli wykorzystywane w Twojej sieci łącza są zawodne, zmniejsz odpowiednio wartość niezawodności. Dokładne wartości nie są takie ważne, jeśli informacje o trasach przesyłane z sąsiedniej sieci nie są odbierane przez zapasowe ścieżki.

W procesie rutowania RIP poszedłem trochę dalej i skonfigurowałem więcej parametrów niż sama redystrybucja tras. Kazałem ruterowi przekazywać wszystkie trasy, jakich nauczy się z procesu 71 protokołu EIGRP, przez listę dostępu numer 12. Tylko te trasy, które spełnią warunki wymienionej listy, będą mogły być przesłane do protokołu RIP i rozgłoszone dalej. W naszym przykładzie warunki listy dostępu 12 spełnia tylko trasa domyślna. Ponieważ w instrukcji `distribute-list in` nie umieściłem nazwy interfejsu źródłowego ani protokołu rutowania, to ruter wie, że ma przesyłać *wszystkie* wchodzące informacje o uaktualnieniach RIP przez listę dostępu 11 w celu odfiltrowania wszelkich rozgłoszeń, których nie chcę słyszeć w mojej sieci. W tym wypadku lista dostępu numer 11 określa dwie sieci, które będą akceptował, prawdopodobnie należące do oddziału, z którym jestem połączony. Wszystkie inne trasy będą ignorowane.

Zamiast stosowania wejściowych list dystrybucyjnych w procesie RIP mógłbym umieścić wyjściową listę dystrybucyjną na procesie EIGRP i w tym miejscu odfiltrować trasy rozgłaszane przez RIP. Choć takie rozwiązanie uchroniłoby inne rutery przed odbieraniem informacji o niechcianych trasach rozgłaszanych przez sąsiadów, to nie chroniłoby ono wcale samego rutera, na którym pracują oba protokoły. Umieszczając filtr na procesie wejściowym protokołu RIP, mogę zatrzymać rozgłaszanie tras, zanim jeszcze dostaną się one do tablicy rutowania.

Jak widzisz, uruchomienie kilku protokołów rutowania na jednym ruterze może prowadzić do pewnych pomyłek. Jeszcze gorzej jest wtedy, kiedy zdecydujesz się na równoległą pracę tych protokołów po łączach Twojej sieci. Staraj się za wszelką cenę nie dopuszczać do takich sytuacji. Możesz stosować takie rozwiązania tylko na (miejmy nadzieję) krótki czas, kiedy przeprowadzasz zmianę protokołu rutowania swojej sieci. Wtedy postaraj się liberalnie podejść do określania dystansów administracyjnych lub innego mechanizmu obsługiwanego przez Twój ruter w celu wybierania jednego z dwóch pracujących protokołów. Staraj się tak ustawić wartości miar, aby wybierany był protokół, który dotychczas obsługiwał Twoją sieć. Kiedy już będziesz miał pewność, że nowy protokół został poprawnie skonfigurowany, zmień dystanse administracyjne tak, by kontrolę przejął nowy protokół rutowania, a poprzedni pracował cały czas jako zapasowy. Po kolejnych testach i upewnieniu się, że wszystko działa poprawnie, możesz na dobre usunąć z sieci obsługę starego protokołu rutowania.

7

Nietechniczna strona zarządzania pracą sieci

Jak widzisz swoją sieć
Określenie granic sieci
Doświadczenie personelu
Koszty
Tworzenie działu wsparcia dla użytkowników

Prawdziwa praca rozpoczyna się od momentu operacyjnego uruchomienia sieci. Starania, aby sieć pracowała płynnie, naprawianie uszkodzeń i ciągłe doskonalenie są jak niekończąca się gra. Na szczęście dobrze zaprojektowana sieć nie będzie sprawiała zbyt dużo problemów i pozostawi Tobie oraz innym administratorom dużo czasu, który będziecie mogli przeznaczyć na rozwijanie i doskonalenie sieci, co jest zajęciem znacznie przyjemniejszym.

Kiedy ludzie zastanawiają się nad zarządzaniem siecią, to zawsze myślą o kilku podstawowych sprawach. Są to zwykle protokoły rutowania i tablice rutowania, zarządzanie ze stacji SNMP, okablowanie (itd.). Często również zapominają o kilku mniej konkretnych lub mniej technicznych sprawach związanych z zarządzaniem siecią, które czasem są ważniejsze od wszystkich innych. Rozdziały 7 1 8 zawierają informacje o zarządzaniu i utrzymaniu sieci i opisują niektóre narzędzia i sposoby postępowania, które pomogą Ci uniknąć problemów. Ponadto opisane zostały sposoby lokalizowania problemów z pracą sieci oraz kontroli rozbudowy sieci z punktu widzenia niezakłóconego zarządzania tą siecią. W rozdziale 8, zatytułowanym „Techniczna strona zarządzania siecią", znajduje się opis technik i narzędzi, które przydadzą się administratorowi sieci. Ten rozdział natomiast skupia się na bardziej abstrakcyjnej i mniej konkretnej części działań składających się na zarządzanie siecią.

Jak widzisz swoją sieć

Być może jednym z najważniejszych aspektów zarządzania siecią jest to, w jaki sposób ją postrzegasz. Z moich doświadczeń wynika, że dobrzy administratorzy sieci zdają się mieć zbliżony do siebie sposób postrzegania swoich sieci, podczas gdy administratorzy mający więcej problemów ze swoimi sieciami patrzą na nie w taki sposób, że nie widzą pewnych elementów sieci. Sposób postrzegania sieci jest łatwy do opisania (choć nie zawsze łatwo się nim posługiwać):

> Sieć jest czymś więcej niż tylko sumą poszczególnych jej części. Jest to pełny, wzajemnie na siebie oddziałujący system i jako taki musi być ona traktowana.

Zastanów się, w jaki sposób myślisz o swoim ciele. W większości przypadków myślisz o swoim ciele jako o całości, a nie o każdym organie oddzielnie. Nawet wtedy, kiedy myślisz o poszczególnych organach, na pewno nie myślisz o tkankach lub komórkach, które tworzą te organy. Czy kiedykolwiek zdarzyło Ci się myśleć o ciele jako o nieuporządkowanym zbiorze komórek, które poruszają się w tym samym kierunku?

Twoje sieć jest takim samym zbiorem. Jeśli myślisz o niej jako o ruterach, które są w tych miejscach, serwerze plików, który znajduje się gdzieś tam, kilku kablach i kilkudziesięciu hostach, to znaczy, że nie myślisz o tej sieci jako o systemie. Jeśli natomiast myślisz o sieci jako o przepływających pomiędzy klientami a serwerami danych, gdzie rutery, koncentratory i kable są tylko podstawą, która trzyma to wszystko razem, to masz właściwy pogląd na swój system sieci. Inaczej mówiąc, musisz zauważać drzewa, ale powinieneś widzieć cały las. Jeśli to Ci może pomóc, to staraj się myśleć o swojej sieci jak o żywym organizmie. Każda zmiana, jakiej dokonasz w jednej części takiego systemu, ma wpływ na inne części umieszczone dość daleko. Jeśli skaleczysz się w nogę, możesz pr/y tym odczuwać nieprzyjemny ból w żołądku, nawet jeśli z rany nie płynie krew, która mogłaby spowodować omdlenie. Skaleczenie może ponadto powodować ból odczuwalny w częściach ciała, które nie zostały skaleczone. Na tej samej zasadzie działa Twoja sieć; kłopoty występujące w jednej części sieci mogą być bardzo mocno odczuwane w innym, odległym obszarze.

Ostatnio prawie trzy tygodnie zajęło mi zlokalizowanie uszkodzenia, które wystąpiło w płycie głównej jednego z ruterów pracujących w mojej sieci. Było to trudne, ponieważ symptomy, które najłatwiej było zauważyć, wskazywały na wystąpienie problemów sprzętowych w *czterech* innych ruterach (chociaż nie równocześnie). Ruter, który uległ uszkodzeniu, działał prawie cały czas bez oznak uszkodzenia. Wykazywał poważne uszkodzenie tylko wtedy, kiedy w sieci miał miejsce jakiś inny poważny problem. Musisz nauczyć się przewidywać wpływ podejmowanych działań nie tylko na ruter lub przełącznik, który właśnie konfigurujesz, ale również na sieć jako całość. Cały czas powinieneś powtarzać sobie pytanie „Jak ta zmiana wpłynie na stabilność i wydajność mojej sieci?", a nie pytanie „Jak ta zmiana wpłynie na pracę rutera bądź przełącznika?". Kiedy zaczniesz patrzeć na swoją sieć jako na system, będziesz miał znacznie większą szansę zrozumieć, jakie konsekwencje będzie miało określone działanie i za jaką cenę możesz podejmować pewne decyzje lub działania.

Określenie granic sieci

Z postrzeganiem sieci jako spójnego systemu mocno związane jest określenie granic tej sieci. Często granice te zdefiniowane są *przez* strukturę Twojej firmy. Są one oczywiście arbitralne i sztuczne, ale mimo że na ich kształt wpływają czynniki, których nie kontrolujesz, istnieją one w rzeczywistości. W niektórych przypadkach będziesz w stanie określić te granice samodzielnie. Być może tworzysz nową sieć i dano Ci dużą swobodę w określaniu jej struktury. Być może dostałeś zadanie zreorganizowania starszej sieci i Twój pracodawca dał Ci wolną rękę, jeśli chodzi o sprawy określenia celów stawianych przed nową siecią. Niezależnie od sytuacji, w jakiej się znajdujesz, ważne jest, abyś wiedział, gdzie są te granice lub abyś je bardzo dokładnie zdefiniował, jeśli masz takie uprawnienia. Wiedząc, gdzie przebiegają granice, lub określając je osobiście, pomagasz samemu sobie i swoim pracownikom zrozumieć granice odpowiedzialności i uprawnień. W ten sposób ograniczysz liczbę problemów z siecią oraz określisz ich rodzaj.

Na pytanie, gdzie umieścić te granice, jest trudniej odpowiedzieć, niż Ci się wydaje. Rozważmy kilka możliwości zdefiniowania granic w sieci kampusowej obejmującej kilka budynków:

- Granica Twojej sieci przebiega na końcach światłowodów doprowadzonych do poszczególnych budynków.
- Granica Twojej sieci przebiega w miejscach połączenia Twojego rutera z sieciami LAN w poszczególnych oddziałach firmy.
- Granica Twojej sieci przebiega w szafie krosowniczej.
- Granica Twojej sieci przebiega przez gniazdka dostępu do sieci umieszczone na ścianach.
- Granica Twojej sieci przebiega z tyłu maszyny, która jest do niej dołączona.
- Granica Twojej sieci przebiega przez kartę interfejsu sieciowego znajdującą się w komputerze.
- Hosty pracujące w Twojej sieci znajdują się w granicach tej sieci.

W miarę jak poruszasz się w dół listy, granica sieci odsuwa się dalej, aż w końcu znajdą się w niej komputery dołączone do sieci. Sieć staje się w ten sposób bardziej skomplikowana i podatna na wzajemny wpływ poszczególnych segmentów. Która z wymienionych granic jest poprawna? Wszystkie one są poprawne w zależności od rodzaju sieci, z jaką masz do czynienia. Poprawna odpowiedź będzie zależała od kilku czynników, które są właściwe tylko Twojej firmie oraz strukturze Twojej sieci, i nad którymi nie masz żadnej kontroli. Jeśli jednak określasz granicę sieci osobiście, to pamiętaj o kilku podstawowych sprawach:

- Jeśli określona przez Ciebie granica będzie przebiegała zbyt blisko rdzenia sieci, to zmniejszysz możliwość zapewnienia dobrej jakości obsługi i niezawodność sieci, z której korzystają Twoi klienci. Na przykład, jeśli granica Twojej sieci przebiega na końcu światłowodu prowadzącego do odległego budynku, to może się zdarzyć, że trudno będzie zapewnić zapasowe połączenie pomiędzy budynkami (a może się to nawet okazać niemożliwe).
- Z drugiej strony im dalej przesuwasz granicę sieci, tym więcej problemów masz do rozwiązania. Rozważmy różnicę pomiędzy przeprowadzeniem granicy sieci przez gniazdka sieci umieszczone na ścianach a doprowadzeniem jej do komputerów. Pozornie jest to dołożenie sobie odpowiedzialności za kilka metrów kabla. Co się jednak stanie, kiedy użytkownik biura postanowi zmienić układ mebli w swoich pokojach? Mając większą granicę sieci, to Ty będziesz odpowiedzialny za odłączenie kabli stacyjnych od gniazdek na ścianach przed rozpoczęciem robót i przyłączenie ich po zakończeniu (być może konieczne będzie użycie dłuższych kabli).

Jako przykład rozważmy określenie granic sieci w przypadku małej firmy obsługiwanej przez dwie sieci Ethernet, jeden ruter, serwer plików i dwadzieścia komputerów PC. Możliwe, że jesteś jedyną osobą w firmie odpowiedzialną za sprawy komputerowe, a Twoja działalność obejmuje również sprawy związane z administrowaniem systemu serwera oraz administrowaniem komputerami klientów. Jeśli Twoja organizacja wchodzi w skład wielkiej korporacji międzynarodowej działającej na trzech kontynentach, to granice Twojej sieci mogą być określone przez zarząd korporacji i mogą dochodzić do końca łącza WAN w każdym z miejsc sieci.

Znowu wraca pytanie, gdzie należy umieścić granicę sieci, i w tym przypadku odpowiedź może zależeć od struktury sieci w całej korporacji, ale najlepszym rozwiązaniem będzie jedno z przedstawionych poniżej:

- Granica przebiega przez połączenie pomiędzy Twoim ruterem a siecią LAN całego oddziału. W ten sposób wyraźnie widać, którym sprzętem zajmujesz się Ty, a który sprzęt należy do ludzi z oddziału firmy i jest przez nich obsługiwany.
- Granica przebiega przez szafę krosowniczą. Takie rozwiązanie pozwala oddzielić sprawy elektroniki sieciowej (koncentratory, rutery itd.) od okablowania poziomego i jest użyteczne, kiedy odpowiedzialność za komponenty pasywne spoczywa na innej grupie ludzi, zgodnie z umową, jaką podpisała Twoja firma.
- Granica przebiega przez gniazdko na ścianie. Takie rozwiązanie wyraźnie oddziela sprzęt, którego może dotykać użytkownik, od sieci, której nie powinien dotykać, co znacznie ograniczy możliwość występowania problemów powstających w związku z działaniami użytkowników.

Ważną rzeczą, o której należy pamiętać, jest to, że granica nie przebiega tam, gdzie jest to najwygodniejsze z punktu widzenia Twojej sieci, ale tam, gdzie została uzgodniona i zaplanowana, zwłaszcza że jest to granica sztuczna. Nie tylko zaoszczędzi Ci to sporo czasu przy usuwaniu usterek, ale również pomoże w dokładnym określeniu granic odpowiedzialności i zasad postępowania w przypadku awarii.

Zastanów się, co oznacza zdefiniowanie granicy sieci tak, że przechodzi ona przez gniazdka na ścianie. Kiedy telefonuje użytkownik i oświadcza, że jego komputer przestał widzieć sieć, Ty (lub Twoi ludzie) szybko sprawdzasz stan swoich ruterów i koncentratorów, i stwierdzasz, że wszystko pracuje poprawnie. Kolejnym krokiem jest wzięcie pod pachę komputera typu laptop lub innego urządzenia testowego i skierowanie się do pokoju użytkownika.

Kiedy tam dotrzesz, odłączasz komputer od gniazdka na ścianie i podłączasz tam swojego laptopa, za pomocą własnego kabla. Jeśli laptop działa poprawnie w sieci, informujesz użytkownika, że problem wynika z uszkodzenia kabla, którym dołączony jest jego komputer lub z błędów w konfiguracji tego komputera i że powinien zwrócić się o pomoc do ludzi odpowiedzialnych za te komponenty. Jeśli jesteś w dobrym nastroju lub to Twój dobry kolega, możesz szybko przetestować jego kabel stacyjny, dołączając swój laptop do sieci za pomocą kabla, co pozwoli wyeliminować jedną z przyczyn. Ale musisz zdawać sobie sprawę, że takie działanie może być uznane za wtrącanie się w nie swoje sprawy przez dział, który zajmuje się stacjami klientów i ich dołączaniem do sieci. Choć opis tego działania wygląda na zalecenia biurokraty, to chcę podkreślić, że nie taki był mój zamiar. Konieczne jest wyraźne rozgraniczenie obszarów odpowiedzialności (i uprawnień), nie tylko po to, by Twoi ludzie nie wchodzili komuś w drogę, ale również po to, by nie zajmowali się godzinami uszkodzeniami, których nie potrafią naprawiać. Jeśli raz naruszysz tak wyraźnie określone zasady, to prawdopodobieństwo, że zrobisz to po raz kolejny, jest bardzo duże.*

Kolejną sprawą wiążącą się ze zrozumieniem zasad określania granic sieci jest wiedza o tym, w jaki sposób można odizolować uszkodzony sprzęt od reszty sieci. Jeśli granica przebiega przez gniazdka na ścianach, możesz odłączyć maszynę, która zakłóca pracę sieci, wyjmując z gniazdka kabel, którym dołączona jest do sieci. Jeśli granica przebiega przez łącze międzybudynkowe, to w przypadku występowania w sieci tego budynku błędów, które zakłócają pracę całej sieci, konieczne będzie odłączenie całego budynku.

Doświadczenie personelu

Jednym z najtrudniejszych i najmniej konkretnych składników systemu zarządzania siecią jest ocena doświadczenia i wiedzy, które posiada (lub powinien posiadać) Twój personel. Jest to również jeden ze składników, który bywa przeoczony, być może dlatego, że jest on trudny do określenia i dokładnego opracowania. Niemniej musisz dołożyć wszelkich starań, aby dobrze ocenić doświadczenie, jakie posiadają Twoi pracownicy, choćby po to, by wiedzieć, który z nich jest najlepszy do wykonywania określonych zadań.

Jeśli Twoja firma bardzo chce być politycznie poprawna, to postępując zgodnie z określonymi zasadami, nie narażasz się na oskarżenia o faworyzowanie kogokolwiek, jeśli okaże się, że pomagasz jednej osobie, a innym nie. W dzisiejszym konfliktowym społeczeństwie tylko sztywne trzymanie się określonych zasad uchroni Cię przed problemami.

Niezależnie od tego, czy jesteś szefem, który ocenia umiejętności potencjalnych pracowników, czy też jesteś pracownikiem, który chce podnieść swoje kwalifikacje, problem jest taki sam. Zanim będziesz w stanie określić, czy dana osoba ma odpowiednią wiedzę wymaganą do pracy w Twoim zespole, musisz najpierw zrozumieć, jakie umiejętności są najważniejsze w zarządzaniu pracą sieci. Trudno odpowiedzieć jednoznacznie na pytanie, jakie to są umiejętności, a lista, którą podaję, nie jest na pewno wyczerpująca. Bez wątpienia będziesz miał jeszcze inne wymagania, które Twoim zdaniem są ważniejsze i bardziej potrzebne w Twojej sieci i firmie niż te, które wypisałem ja. Możliwe, że część wymagań znajdujących się na mojej liście wcale nie będzie miała zastosowania w Twoim przypadku. Pomyśl, zanim zmienisz tę listę, ale możesz to zrobić, ponieważ to w końcu Twoja sieć i Twój kłopot.

Jeśli sieć tworzy pojedynczy system, to większość wymagań odnoszących się do umiejętności pracowników jest taka sama jak te, które dotyczą zarządzania dużym systemem komputerowym. Są to m. in.:

- dobra organizacja;
- zwracanie uwagi na szczegóły;
- dobra pamięć;
- umiejętność rozwiązywania problemów;
- umiejętność pracy w zespole;
- komunikatywność.

Do tego dochodzą wymagania, które musi spełnić każdy dobry pracownik. Są również umiejętności związane bardziej z technicznymi aspektami sieci komputerowych:

- rozumienie i umiejętność stosowania standardów okablowania i łączy oraz dokładne stosowanie tych standardów;
- umiejętność diagnozowania i usuwania uszkodzeń w komponentach elektronicznych;
- umiejętność diagnozowania i usuwania uszkodzeń w oprogramowaniu;
- umiejętność planowania i nadzorowania instalacji sieciowych, poczynając od małych sieci LAN, a kończąc na dużych, wielobudynkowych lub kampusowych sieciach;
- umiejętność rozpoznawania relacji pomiędzy komponentami całego systemu.

Nie każdy z członków Twojego zespołu musi spełniać wszystkie te wymagania, ale wszyscy powinni spełniać większość z nich. Grupa techniczna powinna natomiast spełniać wszystkie wymienione wyżej wymagania. Na szczęście, w przeciwieństwie do pierwszej listy cech pracowników, umiejętności wymienione na liście drugiej można wyćwiczyć.

I tu dochodzimy do najważniejszego wymagania stawianego personelowi zajmującemu się sieciami. W działalności tej najważniejsze jest, aby każda osoba chciała się uczyć i rozwijać swoje umiejętności i wiedzę oraz być na bieżąco z trendami występującymi w przemyśle.

Doświadczenie personelu

Uważa się, że co roku około 20 procent wiedzy personelu zajmującego się sieciami staje się nieaktualne. Oznacza to, że jeśli masz pracowników którzy nie pogłębiają swojej wiedzy, to za pięć lat będą oni w tyle. Niestety, jak się wydaje, tylko kilka dużych korporacji jest w stanie zaznajamiać swych pracowników z najnowszymi technologiami, a niewiele firm próbuje to robić. Być może jest to spowodowane faktem, że korporacje obawiają się, iż wyszkoleni pracownicy będą szukali lepiej płatnej pracy gdzie indziej. W rezultacie jednak pracownicy są pozostawieni samym sobie i muszą się sami starać o dostęp do nowych technologii i nadążać za zmianami w starszych technologiach.

Kolejną cenną umiejętnością każdego pracownika jest zdolność intuicyjnego rozumienia technologii. Osoba posiadająca taką umiejętność nie musi koniecznie rozumieć, co oznacza każdy z bitów w nagłówku datagramu IP, ani fizycznych aspektów propagowania sygnału w kablu. Potrafi zobaczyć szerszy obraz systemu - to, jak mają się do siebie poszczególne elementy oraz jakie są miedzy nimi zależności. Na przykład osoba o takich umiejętnościach będzie rozumiała, że błąd sumy kontrolnej w kablu sieci Ethernet spowoduje retransmisję segmentów TCP. Ważniejsze jest jednak to, że będzie rozumiała wpływ tej retransmisji na sieć: spadek przepustowości sieci wynika zarówno z konieczności ponownego wysłania tych samych danych, jak i spowolnienia pracy protokołu TCP w momencie retransmisji.

Na szczęście choć opisane wyżej zdolności są rzadkością i nadal brakuje osób o takim doświadczeniu w pracy z protokołem TCP/IP, to zestawy protokołów sieciowych są raczej podobne do języków programowania. Na przykład kompetentny programista, który rozumie wszystkie aspekty opracowywania oprogramowania i potrafi takie programy projektować, nie musi znać doskonale każdego istniejącego języka programowania. Po nauczeniu się pierwszego lub dwóch, kolejnych może się nauczyć łatwo i dość szybko. Tak samo jest w przypadku protokołów sieciowych. Gdy ktoś zrozumie podstawowe zasady, na których opiera się działanie sieci jako systemu, może z łatwością zrozumieć szczegóły działania protokołu, z którym dotychczas nie miał do czynienia. Innymi słowy, jeśli ktoś widzi obraz całej sieci i ma niewielkie doświadczenie z protokołem TCP/IP, ale dobrze zna protokoły takie jak IPX lub AppleTalk, to szybko nauczy się pracować z TCP/IP. Tak samo rzadką umiejętnością jak umiejętność intuicyjnego postrzegania całości sieci, jest umiejętność bycia otwartym na nowe technologie, a nie zamykania się w dobrze znanym i rozumianym temacie sieci IP.

Jednym z powodów, dla których możesz do mojej listy umiejętności dopisać kolejne wymagania albo coś wykreślić, jest definicja granic Twojej sieci. Jeśli Twoja sieć składa się również ze wszystkich komputerów, które w niej pracują, to prawdopodobnie dodasz takie umiejętności jak tworzenie i konfigurowanie aplikacji, wsparcie użytkownika oraz obsługa powszechnie stosowanych systemów operacyjnych. Być może umiejętności te powinny być na Twojej liście, nawet jeśli granica sieci przebiega gdzie indziej, ponieważ wymagania te są ważne w związku z koniecznością obsługi kilku własnych hostów, zapewniających w sieci usługi takie jak DNS. Kolejnym powodem dodawania specjalnych wymagań jest fakt, że Twoje firma nie ma oddzielnej grupy ludzi zajmującej się instalowaniem kabli i światłowodów, a także ludzi, którzy są w stanie doprowadzić zasilanie do miejsc, w których umieszczone będą urządzenia elektroniczne.

Poza tymi specjalnymi wymaganiami każda grupa pracowników obsługujących sieć potrzebuje przynajmniej jednej osoby, która potrafi określić, doskonalić i dobrze opisywać spójną wizję sieci w kontaktach z innymi pracownikami firmy. Wiele problemów powodowanych zwłaszcza niekontrolowanym rozrastaniem się sieci, występuje głównie dlatego, że nie ma w firmie nikogo, kto jest w stanie nakreślić wizję rozwoju tej sieci. Symptomy są łatwe do zidentyfikowania: wydaje się, *że* nie ma jasnego planu rozwoju sieci, a wszelkie działania są podejmowane bez powodu i bezładnie. Personel odpowiadający za taką sieć przechodzi od zdania do zadania, a nawet od jednej technologii do drugiej, bez wyraźnie określonego celu tych działań. Podobne problemy pojawiają się, kiedy kilka osób w takiej grupie ma różną wizję rozwoju sieci, albo kiedy osoba odpowiedzialna za nakreślanie kierunków rozwoju sieci musi postępować zgodnie z wewnętrznie sprzecznymi decyzjami zarządu.

Roli planisty nie można powierzyć każdemu - to dlatego rozpatruję to działanie w kategoriach umiejętności. Osoba ta musi zdawać sobie sprawę z tego, że sieć to *żywy* organizm. Musi być w stanie wyobrazić sobie obraz całej sieci, a nie skupiać się na pojedynczych komponentach sieci. Osoba ta powinna być lubiana, a inni pracownicy firmy muszą mieć do niej zaufanie. Powinna poszukiwać i przyglądać się nowym technologiom, a także mieć na uwadze obecnie wykorzystywane komponenty. Niemożliwe jest podejmowanie decyzji o najlepszych dla sieci rozwiązaniach bez zrozumienia współczesnych realiów, które wpływają na dalekosiężne cele. Osoba ta musi rzeczywiście rozumieć swoją wizję i nie tracić jej z zasięgu wzroku; musi ponadto umieć wyjaśnić ją innym w taki sposób, by ją zrozumieli.

Niekiedy osobą odpowiedzialną za kreowanie wizji jest szef zespołu (być może Ty jesteś tą osobą), nie jest jednak ważne, kto jest za to odpowiedzialny, jeśli ma on zaufanie kierownictwa firmy. Największe problemy powstają wtedy, kiedy szefom firmy wydaje się, że ich pozycja jest zagrożona w wyniku swobody i uprawnień wizjonera. Łatwiej jest, gdy planista jest jednocześnie szefem grupy administratorów. Jeśli jednak nie jest to ktoś z kierownictwa, to szefowie firmy muszą zaufać wizji, którą on wypracował i wesprzeć go swoim autorytetem. Brak wsparcia ze strony kierownictwa staje się dużym problemem w sytuacji, kiedy trzeba wybrać nowe technologie. W takich przypadkach kierownictwo firmy może, czasem nawet nieświadomie, sabotować działania podejmowane przez wizjonera.

Koszty

Większość administratorów zbyt mało czasu poświęca na oszacowanie kosztów obsługi ich sieci komputerowej. Dzieje się tak prawdopodobnie dlatego, że ludzie zajmujący się obsługą sieci to zwykle technicy, którzy nie chcą rozmawiać na tematy finansowe. Jednakże ignorowanie kosztów doprowadzi niewątpliwie do *zagłady* sieci i może zaszkodzić interesom prowadzonym przez firmę. Kolejnym powszechnym błędem jest złe oszacowanie kosztów obsługi sieci. Powiedzmy sobie szczerze: budowa sieci to drogie przedsięwzięcie, a jej utrzymanie jest jeszcze droższe.

Koszty

Większość administratorów ma kłopoty ze zrozumieniem struktury kosztów związanych z ich siecią. Są oni w stanie określić, jaki rodzaj sprzętu i typ okablowania będzie wymagany i obliczyć te koszty. Następnie szacują oni czas potrzebny na zainstalowanie kabli i elementów aktywnych i powiększają te koszty tak, by osiągnąć sumę, która jest ich zdaniem konieczna do zrealizowania całego przedsięwzięcia. Szacowanie kosztów utrzymania takiej sieci jest jednak tajemnicą. Nie musi jednak tak być. Jeśli pomyślisz o tym, na co będziesz musiał wydawać pieniądze, zrozumiesz, że możliwe jest określenie rozsądnych wielkości kosztów obsługi sieci.

Najłatwiej policzyć te koszty, które są znane od samego początku. Jeśli masz łącze dzierżawione w swojej sieci WAN, to znasz miesięczne lub roczne opłaty ponoszone z tytułu dzierżawy tego łącza i cenę za łącze, jaka będzie obowiązywała przynajmniej w ciągu najbliższego roku. Cena ta nie zmieni się za bardzo w ciągu następnych lat, możesz więc zaplanować te wydatki nawet na kilka lat do przodu. Podobnie ma się sprawa z kosztami ponoszonymi na pensje i dodatki dla pracowników, które można z dużym przybliżeniem oszacować, zakładając, że wiesz, ilu specjalistów każdej specjalności będziesz potrzebował w swojej sieci. Pamiętaj, że w przyszłości będziesz potrzebował więcej pracowników w związku z rozrastaniem się sieci, a pracownicy będą oczekiwać wzrostu wynagrodzeń w miarę upływu czasu.

Trudniej jest oszacować koszty w przypadku planowanej rozbudowy sieci i wymiany jej elementów na nowe. Jeśli sieć, z którą pracujesz, nie jest zaplanowana tak, że nie wymaga rozbudowy, to z pewnością będziesz musiał zakupić nowe urządzenia -rutery, koncentratory, przełączniki, modemy i tak dalej - aby umożliwić tę rozbudowę. A propos, jeśli zaplanowałeś sieć w taki sposób, że cały jej przyszły rozwój opiera się na sprzęcie zakupionym w momencie instalowania sieci, to prawdopodobnie straciłeś w ten sposób trochę pieniędzy.

Sposób oszacowania kosztów rozbudowy sieci wykracza poza zakres tej książki, która mówi o zarządzaniu siecią. Aby dać Ci jednak kilka wskazówek, trzeba zacząć od faktu, że sieć Internet staje się dwukrotnie większa co około 9 do 12 miesięcy! Choć prawdopodobnie nie będziesz widział tak silnej tendencji w swojej sieci, to jeśli zaczniesz się interesować tymi sprawami, będziesz szczerze zdziwiony. Moja sieć notuje obecnie sześcioprocentowy wzrost co pół roku. W ciągu ostatnich sześciu lat powiększyła się trzy razy i obecnie zaczyna się bardzo rozrastać z powodu nowych inicjatyw telekomunikacyjnych. Spróbuj więc szybko zastanowić się, jak szybko, Twoim zdaniem, będzie rosła sieć, z którą pracujesz, a następnie pomnóż uzyskany wynik przez dwa. Lepiej jest przecenić tempo rozrastania się sieci i mieć trochę pieniędzy w rezerwie niż nie docenić kosztów rozrastania się sieci i naruszyć budżet! Po pierwszym roku pracy będziesz miał lepszą wiedzę na temat kosztów rozbudowy sieci, ponieważ będziesz mógł posługiwać się danymi o rzeczywistej rozbudowie swojej sieci. Posiadając takie sprawdzone informacje, będziesz mógł zrewidować swoje założenia i dokładniej oszacować ilość nowego sprzętu, który będziesz musiał zakupić.

Rozrastanie się sieci to nie jedyny powód, dla którego konieczny będzie zakup nowego sprzętu. Od czasu do czasu konieczna jest wymiana starszego sprzętu - z powodu jego uszkodzenia lub w związku z koniecznością dostępu do nowych funkcji. Jeśli masz dobry kontrakt na utrzymanie sieci, to koszty wymiany elementów możesz kalkulować na podstawie zapisów o upustach zagwarantowanych tym kontraktem. Taki kontrakt oznacza jednak również dodatkowe wydatki. Na szczęście możesz je obliczyć z pewnym wyprzedzeniem. Jeśli nie masz podpisanego kontraktu na utrzymanie sieci, nadal możesz posługiwać się kosztami podstawowego kontraktu przy liczeniu kosztów wymiany urządzeń. Typowy kontrakt zawierający zapisy o utrzymaniu sprzętu takiego jak ruter będzie kosztował około 10 procent ceny katalogowej rutera w skali rocznej. Ponieważ dostawca, z którym podpisano taki kontrakt, musi pokrywać wszystkie wydatki związane z utrzymaniem rutera, to jest to dobra podstawa do oszacowania własnych kosztów samodzielnej obsługi sprzętu.

Pamiętaj, że kontrakty na utrzymanie obejmują zwykle więcej niż tylko naprawę uszkodzeń sprzętu. Zwykle zapewniają również uaktualnienia oprogramowania, dostęp do wsparcia technicznego oraz specjalistyczne szkolenia przeprowadzane przez dostawcę sprzętu. Bez kontraktu na utrzymanie koszty powyższych elementów muszą być w jakiś sposób uwzględnione w Twoich szacunkach. Na pewno od czasu do czasu będziesz uaktualniał oprogramowanie, będziesz czasem potrzebował wsparcia technicznego i będziesz również musiał przeszkolić swoich pracowników. Ponadto w kontrakcie na utrzymanie całego dostarczonego sprzętu ukryte są również inne koszty. Jeśli wystąpią jakieś problemy z pracą sieci, to bez takiego kontraktu, Ty i Twoi pracownicy będziecie musieli sami zlokalizować przyczynę nieprawidłowej pracy sieci i dopiero wtedy zgłosić ją dostawcy sprzętu. To zabiera sporo czasu, który można by poświęcić na inne działania. Ponieważ działania te i tak muszą być wykonane, to może się okazać, że wzrośnie liczba nadgodzin lub wystąpi potrzeba zatrudnienia kolejnych osób, które pozwolą Ci na wykonanie wszystkich prac. Postaraj się dobrze oszacować wartość kontraktu na utrzymanie takiej sieci!

Należy pamiętać też o zakupach związanych z koniecznością obsługi nowych funkcji przez sieć. Ocenia się, że szybkość pracy procesorów CPU zwiększa się obecnie dwukrotnie co 12 do 18 miesięcy. Jeśli założymy, że nowe, szybsze maszyny (albo ich użytkownicy) wymagają szybszych połączeń sieciowych, to konieczne będzie regularne zwiększanie szybkości sieci. Na szczęście większość komponentów sieci może być używana dłużej niż wynosi zakładany czas życia dla komputera PC, który określony jest na trzy lata. Powinieneś jednak dobrze zaplanować procedurę modernizacji istniejących ruterów, pamiętając, że stosowane w nich technologie nadają się do użytku przez pięć do ośmiu lat. W takiej ocenie pomoże Ci szczera rozmowa z dostawcą sprzętu. Dostawca powinien na bieżąco przedstawiać Ci plany dotyczące nowego, szybszego sprzętu i współpracować z Tobą nad ochroną inwestycji, jakie ponosisz kupując dane typy urządzeń.

Rozważając koszt utrzymywania swojej sieci, pamiętaj o wszystkich kosztach samodzielnej obsługi sieci. Zawsze znajdą się rzeczy, które będziesz w stanie wykonać lepiej, poświęcając im więcej czasu, pieniędzy lub kupując lepszy sprzęt. Kupowanie tańszego sprzętu nie zawsze prowadzi do oszczędzania pieniędzy, zwłaszcza gdy obsługa tego tańszego będzie wymagała znacznie więcej czasu. To samo dotyczy współpracy z kilkoma różnymi dostawcami sprzętu. Pamiętaj o kosztach związanych ze szkoleniem personelu na obsługę wielu konfiguracji i interfejsów użytkownika oraz kosztach integracji tych urządzeń w sieci i problemach z lokalizacją uszkodzeń.

Tworzenie działu wsparcia dla użytkowników

Niezależnie od tego, gdzie ustaliłeś granicę Twojej sieci, Twoi użytkownicy będą od czasu do czasu mieli problemy wymagające pomocy. Kiedy maszyna użytkownika nie może połączyć się z serwerem plików, użytkownik ten wymaga czyjejś pomocy, niezależnie od tego, czy granica sieci przebiega przez gniazdka na ścianie, czy też w granicach tej sieci znajdują się również komputery użytkowników. Jeśli nie stworzysz działu wsparcia dla użytkowników, choćby nawet nieformalnego, to ludzie ci będą albo sfrustrowani tym, że nie mają do kogo zadzwonić po pomoc, albo zaczną telefonować bezpośrednio do Twoich administratorów. Jeśli uda im się rozwiązać problem w wyniku takiej bezpośredniej rozmowy z którymś z Twoich pracowników, to w przyszłości będą telefonowali do tej samej osoby, niezależnie od tego, jaki tym razem będą mieli problem. Jeśli taka osoba nie będzie w stanie uporać się z jakimiś problemami, będzie musiała zatelefonować do kogoś innego lub poprosić użytkownika o taki telefon, a cały proces będzie zabierał niepotrzebnie czas i odciągał ludzi od ich normalnych zajęć. Jeszcze gorzej, jeśli osoba ta będzie na urlopie, a użytkownicy nie będą wiedzieli, do kogo tym razem mają zatelefonować.

Tworząc komórkę wsparcia dla użytkowników załatwiasz kilka ważnych spraw:

- Oddajesz do dyspozycji użytkowników jeden stały punkt kontaktowy. Użytkownicy zawsze będą mieli kogoś, do kogo mogą zatelefonować. Ponieważ użytkownicy będą telefonowali zawsze pod ten sam numer lub wysyłali pocztę elektroniczną pod ten sam adres, to będą nieskrępowani i zadowoleni, że spokojnie mogą zgłosić problem lub poprosić o pomoc.
- Uwolnisz w ten sposób przepracowany personel techniczny od załatwiania powszechnie znanych i trywialnych problemów. Z doświadczenia wiem, że ponad połowa zgłaszanych problemów należy do dających się łatwo rozwiązać. Są to zadania dla personelu tworzącego komórkę wsparcia dla użytkowników.

  Nie chcę przez to powiedzieć, że dział wsparcia użytkownika powinien poradzić sobie z każdym zgłaszanym problemem. Dział ten powinien jednak być w stanie obsłużyć często występujące, łatwiejsze problemy (takie jak upewnienie się, czy maszyna jest poprawnie wpięta do sieci) i wyeliminować kilka typowych powodów wystąpienia problemu (uszkodzenie zasilania w budynku, w którym umieszczono serwer plików). Po wyeliminowaniu najczęściej występujących i trywialnych problemów, ludzie ci powinni być w stanie przedstawić powstały problem, z którym nie mogą sobie poradzić, odpowiedniej osobie lub grupie osób.

- Wyeliminujesz zjawisko zgłaszania zaawansowanemu personelowi problemów, które się powtarzają. Kiedy uszkodzeniu ulegnie ruter, wielu ludzi odczuje to uszkodzenie i wielu z nich zgłosi ten fakt. Nie zrozum mnie źle, zgłaszanie zauważonych problemów przez pracowników w żadnym wypadku nie jest niewłaściwe. Ale na pewno nie chcesz odbierać kilkudziesięciu telefonów od ludzi zgłaszających ten sam problem. Odpowiadanie na taką ilość telefonów skutecznie uniemożliwi możliwość rozwiązania go. Działające stanowisko wsparcia dla użytkowników umożliwi udzielenie odpowiedzi na te wszystkie telefony przez ludzi, którzy nie zajmują się usuwaniem przyczyn zgłaszanego problemu.

Skoro już zdecydowałeś się powołać do życia stanowisko wsparcia dla użytkowników, to jaki tryb postępowania powinieneś przyjąć? Najpierw zapytaj samego siebie, jak bardzo sformalizowany powinien być tworzony system wsparcia. Jeśli Twoja sieć jest stosunkowo niewielka i składa się z kilku segmentów Ethernet dołączonych do dwóch ruterów znajdujących się w jednym budynku, to stanowisko wsparcia powinno być raczej nieformalne. Powinno się ono ograniczyć do telefonu przenośnego lub komórkowego, który jest przekazywany różnym osobom z Twojego działu, tak że każda z tych osób odpowiada na pytania użytkowników przez tydzień. W innym przypadku, kiedy Twoja sieć jest duża i skomplikowana, być może obejmuje wiele budynków i setki segmentów sieci, to konieczne może się okazać powołanie działu zatrudniającego kilku pracowników. Ludzie ci będą się zajmowali wyłącznie odbieraniem telefonów od setek albo tysięcy użytkowników.

W obu przypadkach konieczne jest jasne określenie punktu kontaktowego. Numer telefonu, pod który dzwonią użytkownicy w celu zgłaszania problemów, musi być stały; nie powinien on być związany z osobą, która aktualnie pełni dyżur. To dlatego sugerowałem użycie telefonu przenośnego lub telefonu komórkowego; taki telefon łatwiej jest przekazywać kolejnym osobom. Dobrze jest również utworzyć specjalne konto pocztowe, które będzie używane przez osobę lub osoby zatrudnione w dziale wsparcia użytkowników. Takie konto pocztowe nie powinno być jednak jedynym sposobem kontaktu, gdyż w sytuacji, w której sieć przestanie pracować, wiadomości elektroniczne również nie będą przesyłane.

Ludzie pracujący w dziale wsparcia powinni mieć listę najczęściej występujących problemów, do których będą wzywani oraz najczęściej zadawanych pytań. Pytania te mogą być przygotowane w postaci wydrukowanej książki, ale - ponieważ powinny być one często uaktualniane - trzeba pamiętać, że taki dokument dość szybko się dezaktualizuje. Lepszym rozwiązaniem jest więc utworzenie listy dostępnej w sieci komputerowej, a doskonałym formatem dla zapisu tych informacji mogą być strony specjalnie przeznaczonego do tego serwera WWW. Strony takie można w łatwy sposób uaktualniać, mogą one zawierać rysunki, wiele różnych czcionek oraz odwołania hipertekstowe pozwalające na przeszukiwania zawartości serwera w miarę jak użytkownik precyzuje swoje zgłoszenie pozwalając nawet na udzielanie odpowiedzi na podstawie zmieniającej się z minuty na minutę zawartości serwera.

Tworzenie działu wsparcia dla użytkowników

Powinieneś także pamiętać, że dział wsparcia musi mieć dokładnie opracowany zestaw procedur opisujących obsługę przychodzących telefonów i rozdzielanie ich do personelu technicznego, który będzie w stanie je obsłużyć. Jednym z doskonałych sposobów realizowania takich procedur jest stworzenie systemu oznaczania zgłaszanych problemów. Niezależnie od tego, jak bardzo formalna jest struktura Twojego działu wsparcia, koncepcja jego pracy powinna być wyraźnie określona i musi umożliwiać właściwą reakcję na zgłoszenia użytkowników przekazywane w dokładnie określonych godzinach pracy tej komórki. Jeśli użytkownicy kontaktują się bezpośrednio z Tobą lub z Twoim personelem, to uprzejmie zwracaj im uwagę, że dział wsparcia jest właściwym miejscem, gdzie należy zgłaszać tego typu uwagi. To, czy zgłoszony bezpośrednio problem zostanie rozwiązany od razu, czy też przesłany do działu wsparcia, jest kwestią przyjętej polityki.

Tworzenie systemu oznaczeń zgłaszanych problemów

Jedną z największych zalet powołania do życia działu wsparcia użytkowników jest to, że będziesz miał możliwość śledzenia powstających problemów i ich rozwiązywania. Zebrane w ten sposób informacje są nieocenione przy oszacowywaniu kosztów utrzymania sieci lub analizowaniu występujących przez dłuższy czas problemów o podobnym charakterze. Jednym z najskuteczniejszych sposobów zbierania tych informacji jest stworzenie systemu oznaczeń zgłaszanych problemów.

Na wypadek, gdybyś nie miał doświadczenia z takimi systemami, postaram się w kilku słowach opisać typową strukturę takiego rozwiązania. Zawsze, kiedy użytkownik zgłasza jakiś problem do działu wsparcia, otwierana jest nowa karta problemu, której nadawane jest numeryczne oznaczenie. Karta ta powinna dokumentować sam problem, zawierać dane o zgłaszającym go użytkowniku, czas wystąpienia problemu i nazwisko osoby, która przyjęła zgłoszenie. W miarę jak zgłoszony problem będzie rozwiązywany przez kolejnych specjalistów, powinni oni dodawać do tej karty wszystkie informacje związane z kolejnymi kontaktami z użytkownikiem oraz dokładny opis prób rozwiązania tego problemu. Kiedy w końcu problem zostanie rozwiązany, do karty należy dodać dokładny opis tego rozwiązania oraz czas zakończenia działań. Użytkownik powinien zostać poinformowany o rozwiązaniu problemu. Taka zamknięta karta jest następnie umieszczona wraz z kartami innych załatwionych spraw i może być w przyszłości wykorzystana do rozwiązania podobnego problemu lub do celów statystycznych, rozrachunkowych lub innych. Przykładowa karta zgłoszenia problemu pokazana poniżej zawiera wszystkie opisane elementy.

Sprawa: A923
Czas zgłoszenia: 31/5/96 13.27
Czas zakończenia:
Osoba przyjmująca zgłoszenie: Jan
Osoba zgłaszająca: Maria Kowalska
Telefon: 222-333-444
Email: m.kowalska@marketing

Opis problemu:

Maria Kowalska zgłasza, że jej komputer (mk.marketing) nie ma dostępu do serwera działu marketingu od czasu powrotu pracownicy z obiadu. Potwierdzono poprawną pracę połączenia i funkcjonowanie sieci (ping). Nie można jednak przetestować pracy serwera działu marketingu z komputera działu wsparcia.

Status: Przekazano Robertowi do sprawdzenia ':

Informacje dodatkowe:
31.5.96 14:00
Po sprawdzeniu serwera okazało się, że ma on uszkodzoną kartę sieciową. Rozpoczęto działania zmierzające do wymiany karty. Przewidywany czas zakończenia naprawy: godzina 14:30.

Rozwiązanie:

Każdy problem, nawet drobny, powinien mieć założoną kartę. Pozwoli Ci to stworzyć statystyki analizujące błahe problemy, jak również liczbę poważnych problemów, które występują w Twojej sieci. Mogąc np. przedstawić karty opisujące dużą liczbę problemów wynikających z braku zasilania w określonym miejscu sieci, będziesz mógł uzasadnić konieczność zakupu zasilaczy bezprzerwowych dla części sprzętu, który się tam znajduje. Możliwe, że uda Ci się odciążyć obwód elektryczny dzięki zainstalowaniu drugiego obwodu dla zasilania części urządzeń.

Aplikacja, której będziesz używał do obsługi systemu kart zgłoszeń, w dużym stopniu będzie *zależała od* tego, czego się po tym systemie spodziewasz. Na rynku dostępnych jest kilka tego typu aplikacji, a niektóre z nich są nawet rozpowszechniane za darmo. Kiedy będziesz wybierał aplikację do obsługi kart zgłoszeń, pamiętaj o kilku kryteriach:

- *Łatwość użycia.* Twoi pracownicy nie będą chcieli uaktualniać karty, gdy będzie to dla nich dużym obciążeniem.
- *Przechowywanie danych.* Na pewno zechcesz przechowywać karty nie tylko przez czas obsługi zgłoszenia, ale również przez kilka miesięcy, a nawet lat, po jego załatwieniu. Takie dane pozwolą Ci śledzić długoterminowe trendy lub identyfikować podobne problemy.
- *Uaktualnianie elektroniczne.* Najszybszym sposobem utraty karty zgłoszenia usterki jest wydrukowanie jej. Zamiast tego rozważ możliwość pełnej obsługi karty w systemie komputerowym. Takie rozwiązanie pozwoli Ci przesyłać karty pocztą elektroniczną (przechowując oczywiście ich kopie w systemie), wyszukiwać karty
, i uaktualniać je. Co więcej taki sposób jest jedynym rozwiązaniem, które pozwoli Ci na tworzenie statystyk dotyczących uszkodzeń i podejmowanych działań.

Tworzenie działu wsparcia dla użytkowników

- *Tworzenie statystyk*. Od aplikacji obsługującej karty zgłoszeń będziesz prawdopodobnie oczekiwał możliwości tworzenia raportów w oparciu o zdefiniowane zapytania dotyczące problemów obsłużonych przez pracowników wsparcia oraz tych, które wymagały interwencji zespołu technicznego, a także średniego czasu załatwiania spraw. Może będziesz chciał również uzyskać informacje o tym, jaki procent wszystkich zgłoszeń stanowią zgłoszenia dotyczące konkretnej usterki.
- *Relacje.* Kilka kart zgłoszeń zwykle wiąże się ze sobą. W naszym przypadku jest mało prawdopodobne, aby tylko pani Maria zgłaszała problem z dostępem do serwera plików. Inne telefony w tej samej sprawie mogą generować kolejne karty zgłoszeń, które powiązane są z kartą zgłoszenia pani Marii, i powinny być odnotowane tylko jako materiał statystyczny. Związki między kartami pozwolą na rozpoznanie, czy zgłoszenie zostało tylko powierzchownie załatwione, czy też usunięto prawdziwą przyczynę określonego typu problemów. Dzięki możliwości śledzenia i głębokiej analizy informacji zawartych w kartach zgłoszeń można przeanalizować trendy, które pomogą w znalezieniu prawdziwej przyczyny powstawania problemów w sieci.

Nawet jeśli nie będziesz robił nic więcej ponad wykorzystanie standardowego formatu karty zgłoszenia, podobnego do zaprezentowanego *wyże]* i przekazywania go za pomocą poczty elektronicznej, to już znacznie ułatwisz sobie pracę. Uważaj jednak z wdrażaniem dużych, kłopotliwych systemów obsługi zgłoszeń awarii, ponieważ może się to skończyć tym, że obsługa takiego systemu zabierze Tobie i personelowi większość czasu.

Prawdopodobnie jednym z największych niebezpieczeństw wynikających ze stosowania rozbudowanego systemu jest błędne wykorzystywanie statystyk tworzonych na podstawie kart do oceny produktywności pracowników. Twoim zadaniem jest rozwiązywanie problemów występujących w sieci, a nie jak najszybsze zamykanie kart zgłoszeń przez Twój personel. Jeśli zaczniesz porównywać pracowników biorąc za kryterium liczbę obsługiwanych kart zgłoszeń, to, po pierwsze, Twoi pracownicy zaczną wybierać karty zawierające najprostsze sprawy, które będą mogli szybko załatwić, unikając spraw trudniejszych, które często w największym stopniu wpływają na pracę sieci i dlatego powinny być załatwiane w pierwszej kolejności, a po drugie, będą czuli nacisk i zaczną zamykać karty zgłoszeń, nawet jeśli problem nie został jeszcze rozwiązany do końca tylko po to, by zaliczyć więcej zleceń.

Możesz uniknąć obu opisanych wyżej problemów, jeśli dokładnie i świadomie określisz sposób tworzenia statystyk. Być może Jan zamyka kilka zgłoszeń mniej niż Robert, ponieważ przekazane mu sprawy były po prostu trudniejsze. Może się również okazać, że Maria ma znacznie więcej otwartych spraw niż inni pracownicy. Powodem takiej sytuacji może być to, że nie potrafi sprawnie ich załatwiać albo to, że jest ona jedyną osobą w Twoim zespole, która potrafi rozwiązywać większość tego typu problemów sieciowych. Jeśli jest jedyną specjalistką w tym zakresie, to powinieneś postarać się o jakąś pomoc dla niej, szkoląc kolejnego pracownika lub przyjmując do działu kogoś z odpowiednimi umiejętnościami. Najbezpieczniej śledzić trendy w sieci, a nie prawidłowości zachowania pracowników. Są inne, znacznie lepsze i rzetelniejsze, sposoby oceny pracowników.

Często znacznie łatwiej zrozumieć techniczne aspekty *zarządzania* pracą sieci, takie jak monitorowanie pracy sieci, wykrywanie problemów, lokalizacja uszkodzeń, identyfikowanie i usuwanie wykrytych problemów i zarządzanie zmianami. Wymienione działania zostaną omówione w kolejnym rozdziale.

8

Techniczna strona zarządzania pracą sieci

Monitorowanie pracy sieci Wykrywanie uszkodzeń Narzędzia pomocne przy monitorowaniu i wykrywaniu uszkodzeń Zarządzanie zmianami

W poprzednim rozdziale omówiliśmy nietechniczną stronę zarządzania siecią, rozpatrując sprawy takie jak koszty, doświadczenie personelu, dział wsparcia użytkowników i tak dalej. Ważniejsze jest jednak to, że zaprezentowano w tym rozdziale ideę sieci postrzeganej jako żywa jednostka. Jest to niezwykle ważne, ponieważ tematy tu omawiane - monitorowanie pracy sieci, wykrywanie uszkodzeń i zarządzanie zmianami - wydają się być sprawami bardziej praktycznymi i mają bezpośredni wpływ na pracę sieci. Jeśli nie zrozumiesz sposobu, w jaki będzie reagowała Twoja sieć, lub nie przewidzisz efektów swoich działań w sieci, to wykonywanie takich zadań jak np. lokalizacja uszkodzeń stanie się koszmarem.

Na szczęście dla wielu administratorów sieci techniczna strona zarządzania siecią jest często znacznie przyjemniejsza niż szacowanie kosztów lub rozmowy z kandydatami do pracy; prawdopodobnie dlatego, że działania techniczne są bardziej praktyczne i wymagają dokładnie określonej jakości wykonania i przygotowania, w przeciwieństwie do działań opisanych w poprzednim rozdziale.

Monitorowanie pracy sieci

Gdy sieć zostanie skonfigurowana i uruchomiona, nie powinno się z nią dziać nic złego. Niestety, sieci komputerowe nie działają w świecie idealnym. Poza nieprzewidywalnymi uszkodzeniami spowodowanymi problemami sprzętowymi, przerwami w dopływie prądu, uszkodzeniami kabli i błędami w oprogramowaniu jest jeszcze wiele innych przyczyn problemów w codziennej pracy sieci.

Czasem coś tak prostego jak dodanie nowej aplikacji pracującej w sieci może spowodować nieprzewidywalne zakłócenia transmisji danych, prowadzące do kompletnego zatrzymania sieci. Duże znaczenie ma więc monitorowanie pracy sieci.

Niezależnie od rozmiarów sieci, składającej się z kilkudziesięciu lub kilku tysięcy węzłów, musisz określić sposób, w jaki będziesz obserwował jej pracę w celu stwierdzenia, które jej części pracują poprawnie, a które nie. Jeśli tego nie zrobisz, to nigdy nie będziesz wiedział, co naprawdę dzieje się w sieci, i ciągle będziesz walczył z problemami, których można było uniknąć lub stłumić w zarodku.

Na szczęście monitorowanie pracy sieci nie musi być koniecznie zadaniem skomplikowanym lub drogim. W zależności od rodzaju monitorowania, którego chcesz używać, będziesz w stanie wykorzystać nawet własne oprogramowanie pracujące na jednym z komputerów w sieci. Jednak czasem konieczne może się okazać zakupienie oprogramowania specjalnego przeznaczenia, wykonanego dla celów monitorowania pracy sieci.

Monitorowanie osiągalności sieci

Monitorowanie osiągalności sieci to punkt, od którego zaczyna się nadzorowanie pracy większości sieci komputerowych. W tego typu rozwiązaniu interesuje Cię tylko to, czy dwie maszyny dołączone do sieci mogą się w tej sieci porozumiewać. Należy sobie jednak zdać sprawę z tego, że niemożliwe jest testowanie komunikacji pomiędzy każdą parą maszyn w sieci, zwłaszcza w przypadku sieci składających się z kilkudziesięciu lub więcej hostów.

Oczywiście, niektórzy mogą powiedzieć, że sami użytkownicy sieci będą wykonywali coś w rodzaju monitorowania osiągalności za każdym razem, kiedy będą używali sieci, po co więc ma się tym zajmować administrator? Choć zasadniczo prawdą jest, że użytkownicy sami odkryją problemy występujące w sieci, to nie zawsze będzie im się chciało zgłaszać te problemy, zwłaszcza jeśli nie są zadowoleni ze sposobu, w jaki Twoi pracownicy reagują na zgłaszane problemy. Poza tym, źle będzie o Was świadczyć, jeśli na zgłoszenie o przerwie w pracy sieci Twój personel lub Ty odpowiecie na przykład: „Czyżby? Nie wiedziałem!".

Skoro więc monitorowanie każdej pary hostów w sieci, które mogą się ze sobą komunikować, nie jest możliwe, to powinieneś przynajmniej monitorować sieć jako całość, by móc wykryć problemy komunikacyjne, zanim zrobi to użytkownik. Jak należy zorganizować takie monitorowanie sieci? Choć nie jest to najlepsze rozwiązanie, dobrze jest określić w sieci jeden (lub kilka) punktów, które będą podejmowały próby komunikowania się z innymi punktami w sieci. Jeśli maszyna A (która pełni funkcję maszyny monitorującej) może połączyć się z maszyną B i z maszyną C, to bardzo prawdopodobne, że maszyny B i C również mogą się ze sobą komunikować. Zdarzają się jednak sytuacje, kiedy takie założenia nie są prawdziwe, nawet jeśli sieć pracuje poprawnie, np. przy ograniczeniu ruchu w sieci za pomocą ściany ogniowej lub funkcji filtrowania pakietów. Może się zdarzyć, że konfiguracja zabezpieczeń sieci pozwoli Twojemu komputerowi na komunikowanie się z obydwoma innymi komputerami, ale nie na komunikowanie się tych komputerów między sobą.

Monitorowanie pracy sieci

Takie nieciągłości wynikające z konfiguracji sieci wykonanej przez administratora są rzeczą normalną, należy jednak pamiętać, że powinny być dobrze udokumentowane. Możliwa jest sytuacja, w której prosty test osiągalności drugiej maszyny nie powiedzie się, ponieważ dynamiczny protokół rutowania źle działa lub został błędnie skonfigurowany. Pomyśl o sytuacji, gdzie ruter, do którego dołączony jest komputer monitorujący pracę sieci, ma zdefiniowane trasy do sieci, w których pracują hosty B i C, ale rutery dołączone do tych sieci nie mają określonej trasy pomiędzy sobą. W większości wypadków taka sytuacja wynika z błędnego skonfigurowania protokołów rutowania, ale błędy te mogą być tak subtelne, że wyjdą na jaw dopiero wtedy, gdy uszkodzeniu ulegnie łącze podstawowe.

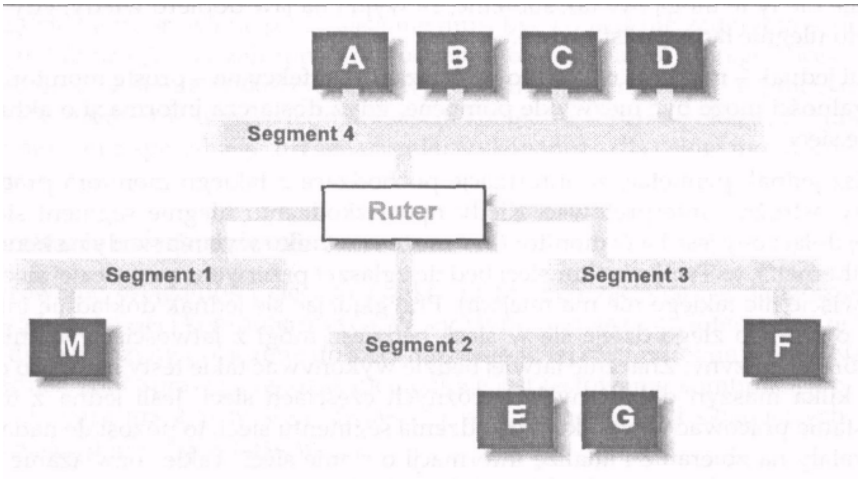
Nadal jednak - mimo że nie jest to rozwiązanie perfekcyjne - proste monitorowanie osiągalności może być niezwykle pomocne, gdyż dostarcza informacji o aktualnym stanie sieci.

Musisz jednak pamiętać, że informacje pochodzące z takiego monitora pracy sieci należy ostrożnie interpretować. Kiedy np. uszkodzeniu ulegnie segment sieci, do której dołączony jest Twój monitor (być może w wyniku wylania wody na koncentrator Ethernet*), to Twój monitor sieci będzie zgłaszał przerwę w pracy całej sieci (choć oczywiście nic takiego nie ma miejsca). Przyglądając się jednak dokładnie informacjom o tym, co złego dzieje się w sieci, będziesz mógł z łatwością wyeliminować niektóre przyczyny. Znacznie łatwiej będzie wykonywać takie testy mając do dyspozycji kilka maszyn dołączonych w różnych częściach sieci. Jeśli jedna z maszyn przestanie pracować w wyniku uszkodzenia segmentu sieci, to pozostałe nadal będą pozwalały na zbieranie i analizę informacji o stanie sieci. Takie rozwiązanie działa najlepiej, gdy maszyny monitorujące dołączone do różnych segmentów sieci są zebrane obok siebie, na przykład w głównym pomieszczeniu monitorowania pracy sieci, co pozwala na równoczesne wykorzystywanie zgłaszanych przez nie informacji. Jeśli nie jest to możliwe, ponieważ masz do czynienia z siecią kampusową, to dobrze byłoby mieć w każdym z odległych miejsc wyszkolonych ludzi, którzy będą pełnili funkcję Twoich oczu. Można też użyć innych rozwiązań pozwalających na dostęp do informacji sczytywanych z sieci, których działanie nie będzie się opierało na podstawowych łączach Twojej sieci, których uszkodzenia będziesz chciał monitorować.

Co powinieneś monitorować, aby uzyskać możliwie najwięcej informacji? Oczywiste jest, że nie będzie możliwe monitorowanie każdej maszyny w sieci. Jeśli w sieci pracują tysiące komputerów, to komputer monitorujący cały swój czas poświęci na ich odpytywanie, co z kolej spowoduje znaczne wykorzystanie pasma sieci, do której jest dołączony. Kolejnym problemem jest fakt, że wiele stacji roboczych pracujących w Twojej sieci może być regularnie wyłączana lub restartowana. Jeśli monitorujesz połączenia z każdą z takich stacji, to Twoja stacja monitorująca będzie generowała takie ilości alarmów, że w pewnym momencie zaczniesz je wszystkie ignorować.

*Taki przypadek naprawdę mi się zdarzył! Na szczęście użytkownicy szybko się przyznali i w ciągu kilku minut udało się uruchomić na nowo usługi sieciowe.

Kiedy zaczniesz zastanawiać się, co powinieneś monitorować, zadaj sobie pytanie, co chcesz osiągnąć. Kiedy będziesz się zastanawiał nad dodaniem kolejnego hosta do listy monitorowanych urządzeń w sieci, powinieneś zapytać sam siebie, jakie dodatkowe informacje da Ci monitorowanie tego hosta. Jeśli jedynym powodem dodania tego hosta do listy jest chęć uzyskania odpowiedzi na pytanie „Czy ta maszyna pracuje w sieci?", to powinieneś upewnić się, czy host ten jest istotny dla pracy całej sieci. Dobrym kandydatem na listę monitorowanych hostów będzie na pewno główny serwer DNS. Zastanówmy się nad przypadkiem pokazanym na rysunku 8-1.



Rysunek 8-1: Decydowanie o tym, które hosty monitorować

Zakładamy, że do każdego segmentu sieci dołączonych jest jeszcze kilka innych maszyn, ale są to głównie stacje klientów. Maszyna monitorująca pracę sieci znajduje się w segmencie I i oznaczona jest literą M. Pierwszym kandydatem do monitorowania pracy jest ruter dołączony do segmentu sieci, w którym pracuje host M. Ruter ten ma jednak wiele adresów IP. Który z nich powinniśmy monitorować? W zależności od producenta ruterów odpowiedź będzie prawdopodobnie brzmiała: wszystkie. Jeśli ruter ten zgłasza komunikat zawsze, gdy jeden z segmentów sieci do niego dołączonych jest nieosiągalny z powodu uszkodzenia tego segmentu (tak działa Cisco IOS), to monitorowanie wszystkich interfejsów rutera będzie prowadziło do dość żmudnego procesu określania, który interfejs jest uszkodzony. Z drugiej strony, jeśli ruter wysyła odpowiedź na wszystkie interfejsy, niezależnie od stanu każdego z nich, to testowanie osiągalności kilkunastu interfejsów jednego rutera nie daje nic poza dodatkowym obciążeniem procesora rutera i pasma sieci. Będzie znacznie lepiej, jeśli będziesz sprawdzał osiągalność przez jeden interfejs rutera, na przykład ten, którym ruter dołączony jest do rdzenia sieci, a poszczególne segmenty sieci będziesz testował w inny sposób.

Monitorowanie pracy sieci

Ograniczenie monitorowania tylko do interfejsów rutera prawdopodobnie nie wystarczy, by mieć obraz całej sieci. Poza Twoim ruterem w segmentach sieci znajdują się różne kombinacje kabli, koncentratorów, przełączników i tak dalej. Elementy te mogą ulec uszkodzeniu, a ruter nadal będzie wierzył, że dołączony do niego segment nadal pracuje. Co więcej, jest bardzo prawdopodobne, że producent rutera określił funkcję wysyłania odpowiedzi na zapytania stacji monitorującej jako mającą priorytet niższy niż przełączanie pakietów (miejmy nadzieję!). Jeśli tak jest w przypadku Twojego rutera, to bardzo możliwe, że w przypadku dużego obciążenia nie będzie on odpowiadał na niektóre zapytania stacji monitorującej, ale nadal będzie przełączał pakiety. Dlatego powinieneś się zastanowić nad monitorowaniem kilku hostów poza Twoim ruterem, nawet jeśli nie są one ważne dla pracy całej sieci. Dobrym rozwiązaniem jest monitorowanie dwóch hostów w każdym segmencie sieci, zwłaszcza jeśli pracują one w innych pomieszczeniach lub budynkach, co uchroni Cię przed pomyłkami związanymi z przerwami w zasilaniu. Oczywiście hosty te powinny pracować stabilnie (hosty obsługujące wielu użytkowników lub serwery plików, a nie maszyny użytkowników).

Na rysunku 8-1 widać tylko dwa hosty w segmencie 2, tak więc do listy monitorowanych urządzeń trzeba dodać oba z nich. W segmencie 3 jest tylko jedna maszyna, serwer plików oznaczony jako F, tak więc na liście znajdzie się tylko to urządzenie. W segmencie 4 masz do wyboru cztery maszyny, konieczne jest więc podjęcie decyzji, które z nich będą monitorowane. Oczywiście mógłbyś dodać wszystkie cztery, ale na pewno chciałbyś utrzymać ruch w sieci generowany przez stację monitorującą na rozsądnym poziomie, a jednocześnie otrzymywać pełne informacje. Ponieważ host D jest również Twoim serwerem DNS, powinien pracować stabilnie i ważne jest, aby był on zawsze osiągalny. Tak więc musi się *znaleźć* na liście. Pozostałe trzy hosty, oznaczone literami A, B i C, są po prostu maszynami wykorzystywanymi przez wielu użytkowników, bez żadnych szczególnych dodatkowych zastosowań. Należy więc wybrać losowo jeden z nich i dodać go do listy monitorowanych urządzeń. Tabela 8-1 zawiera wszystkie urządzenia, które znalazły się na liście do monitorowania.

Tabela 8-1. Monitorowane urządzenia w każdym z segmentów naszej przykładowej sieci

Segment	*Monitorowane urządzenie*
1	R1 (Interfejs numer 1 rutera)
2	R2, E, G
3	R3, F
4	R4, A, D

Zastanówmy się teraz, jakie kombinacje pojawiających się alarmów będą nam mówiły o różnych stanach sieci. Jeśli R1, R2, R3 i R4 są osiągalne, a host D nie jest osiągalny, możesz zakładać, że Twój ruter pracuje poprawnie i powinieneś skoncentrować się na sprawdzeniu, czy uszkodzeniu uległ host D, czy też przestała działać cała część sieci, do której dołączony jest host D. Jeśli host A jest również nieosiągalny, to prawdopodobnie uszkodzeniu uległ koncentrator lub kabel w segmencie 4. Jeśli host A jest osiągalny, to największym podejrzanym jest sam host D, choć nadal wina może leżeć po stronie koncentratora lub okablowania.

Niezależnie od tego, jak jest naprawdę, możesz skupić się na sprawdzeniu stanu tej części sieci. A co może być powodem, że zarówno host D, jak i host A, są nieosiągalne, a ponadto nieosiągalny jest R4? Taka sytuacja wskazuje na uszkodzenie koncentratora lub kabla, którym do segmentu 4 dołączony jest ruter, lub uszkodzenie samego interfejsu rutera. Podobnie jak poprzednio, aby dokładnie określić przyczyny, trzeba będzie obejrzeć te urządzenia na miejscu.

A co może być przyczyną tego, że wszystkie hosty są osiągalne, ale żaden z interfejsów rutera nie odpowiada poprawnie? Taka sytuacja występuje wtedy, gdy ruter jest stosunkowo mocno obciążony i przestał odpowiadać na Twoje zapytania, by zająć się obsługą przełączania pakietów. Choć nie jest to uszkodzenie, powinieneś dowiedzieć się, dlaczego ruter jest tak bardzo obciążony. Może to wynikać z błędnej konfiguracji lub był to po prostu moment dużego obciążenia, który nie występuje zbyt często w sieci. Podobnie jak w opisanej wyżej sytuacji, wskazane jest obejrzenie rutera i przeanalizowanie jego konfiguracji na miejscu, pomimo że sieć jeszcze nie przestała pracować.

Jakiego rodzaju narzędzi powinno się używać do monitorowania osiągalności *urządzeń* w sieci? Odpowiedź uzależniona jest od kilku czynników. Jednak zamiast opisywania kilku przykładów monitorowania różnych sieci, zastanówmy się nad innymi rodzajami monitorowania, które będziesz chciał stosować w sieci, a dopiero potem omówimy powszechnie stosowane narzędzia.

Monitorowanie tras: bardziej zaawansowana forma monitorowania

Jednym z problemów występujących przy stosowaniu prostego monitorowania osiągalności jest to, że nie zawsze prawdą będzie wnioskowanie, iż skoro host A widzi B a B widzi C, to host A będzie widział host C. Choć dokładne przeanalizowanie sieci i wybór hostów, które monitorujemy, może pomóc w rozwiązaniu tego problemu, to nie jest możliwe całkowite wyeliminowanie takich sytuacji. Aby rozwiązać tego typu problemy, musisz zastosować lepsze narzędzie, które pozwoli Ci monitorować zawartość tablic rutowania w różnych miejscach sieci.

Jeśli Twoja sieć została dobrze zaprojektowana, to struktura rutowania w tej sieci powinna być przewidywalna i stabilna. Powinna się ona zmieniać tylko w wyniku zmian zachodzących w topologii sieci, przy okazji przełączeń wykonywanych Twoimi rękoma. W pozostałych przypadkach zmiany powinny wynikać z faktu występowania uszkodzeń w różnych częściach sieci. Monitorowanie topologii sieci nie zawsze jest jednak możliwe. Aby to zrobić poprawnie, konieczne byłoby fizyczne monitorowanie każdego kabla, koncentratorów i połączeń pomiędzy nimi w celu określenia, które urządzenie jest dołączone i gdzie. Ważniejsze jest więc monitorowanie topologii sieci z punktu widzenia sieci, czyli zapisów w tablicach rutowania. Kiedy zmianie ulegają tablice rutowania, to można na tej podstawie wnioskować, że zmieniła się topologia sieci.

Monitorowanie pracy sieci

Jednym z problemów występujących przy monitorowaniu tras jest fakt, że wymaga ono stosowania znacznie bardziej zaawansowanego oprogramowania. Zastanówmy się, jak powinno wyglądać oprogramowanie do monitorowania osiągalności. Powinno obsługiwać wejściową listę urządzeń, które mają być monitorowane, i testować je co jakiś czas, sprawdzając, czy są jeszcze osiągalne. Takie sprawdzanie może być wykonane za pomocą prostego zapytania o echo ICMP (ping) lub za pomocą datagramów wysyłanych na usługę echo w UDP. Możliwe jest również wykorzystanie każdego innego narzędzia, które pozwoli na stwierdzenie, czy adres przeznaczenia jest osiągalny bez generowania zbyt dużego ruchu w sieci. Następnie oprogramowanie takie powinno zbierać wyniki próbkowania i zawierać jakiś mechanizm alarmowania operatora, jeśli adres przeznaczenia nie odpowie na pakiet próbkujący. Trochę lepszy program pozwoliłby na przechowywanie danych i tworzenie statystyk określających szybkość uzyskiwania odpowiedzi, co może pomóc w określaniu wielkości ruchu w sieci. Programista znający się na pisaniu programów sieciowych jest w stanie napisać taki program monitorujący w kilka dni.

Rozważmy teraz, jak powinno działać oprogramowanie służące do monitorowania tras. Podobnie jak poprzednio, program ten powinien posługiwać się listą urządzeń (prawdopodobnie ruterów), z których pobiera tablice rutowania. Następnie konieczne będzie zebranie wszystkich tablic i dokonanie analizy ich zawartości w celu stworzenia aktualnego obrazu topologii sieci. Od programisty *zależy, co* dalej będzie robione z tym obrazem. Jednym z rozwiązań może być wysyłanie do operatora zawiadomień w wypadku, kiedy topologia sieci ulegnie zmianie. Bardziej zaawansowana opcja będzie pozwalała na wyświetlanie graficznego obrazu sieci. Niezależnie od tego, która opcja została wybrana, napisanie takiego oprogramowania jest znacznie trudniejsze od pisania prostych funkcji monitorujących osiągalność urządzeń w sieci.

Kolejnym problemem przy monitorowaniu tras jest fakt, że musimy założyć, iż w sieci pracują urządzenia, które można odpylać o zawartość ich tablicy rutowania. Zwykle oznacza to, że rutery pracujące w sieci obsługują protokół *Simple Network Management Protocol* (SNMP), że dynamiczny protokół rutowania używany w sieci obsługuje wymianę informacji między ruterami lub że informacje o rutowaniu mogą być uzyskiwane w oparciu o podsłuchiwanie protokołu rutowania. Nie ma jednak żadnej gwarancji, że Twoje rutery posługują się którąś z tych metod pracy, choć dostęp przez SNMP staje się powoli standardem.

Ostatnim problemem związanym z monitorowaniem tras jest to, że nie obsługuje ono monitorowania osiągalności, chyba że tablice rutowania pobierane są z urządzeń innych niż rutery. Aby zrozumieć, dlaczego tak się dzieje, przyjrzyjmy się naszej przykładowej sieci. Pobieranie tablic rutowania tylko z ruterów pozwala nam określić stan ich interfejsów i przyłączenia do segmentów sieci. Innymi słowy, jeśli interfejs rutera dołączony do segmentu l funkcjonuje poprawnie, to tablica rutowania tego rutera będzie zawierała zapis dotyczący segmentu 1. Taka informacja nie mówi nam jednak nic na temat tego, czy host D jest w stanie komunikować się z segmentem sieci o numerze 1.

Mimo że ograniczenie to ma pewną wadę, monitorowanie tras może mieć duże znaczenie dla całego procesu monitorowania Twojej sieci, ponieważ daje znacznie lepszy obraz odległych części sieci niż prosty system monitorowania osiągalności.

Monitorowanie ruchu: najdokładniejszy obraz sieci

Aby uzyskać kompletny i szczegółowy obraz stanu sieci, powinieneś zastanowić się nad zastosowaniem narzędzia monitorującego ruch w każdym segmencie tej sieci. Oprócz informacji o tym, w której części sieć nie pracuje z powodu uszkodzenia jej komponentów, monitor ruchu ostrzega Cię przed możliwością wystąpienia przerwy w pracy sieci z powodu jej przeciążenia. Program taki może nawet pokazać Ci miejsca, w których sieć - choć nadal funkcjonująca - pracuje źle z powodu złego rozkładu ruchu. Chodzi tu, na przykład, o miejsca, gdzie równoważenie ruchu na równoległych łączach nie działa poprawnie.

Najtrudniejszą sprawą w monitorowaniu ruchu w sieci jest fakt, że nie można tego wykonywać obserwując sieci z jednego centralnego punktu. Powróćmy jeszcze raz do rysunku 8-1, na którym widać, że monitor oznaczony M nie może nic powiedzieć o ruchu w segmencie 3 lub o ruchu pomiędzy segmentami 2 i 4, obserwując tylko ruch w segmencie 1. Konieczne jest rozmieszczenie w całej sieci odpowiednich urządzeń, które będą zbierały informacje o ruchu w sieci z ich punktu widzenia. Informacje te będą następnie analizowane przez centralną stację zbierającą informacje, na podstawie których tworzony będzie obraz ruchu w sieci.

Nie oznacza to, że w każdym segmencie sieci musisz umieszczać urządzenie specjalnego przeznaczenia. Prawie wszystkie rutery, przełączniki i koncentratory mają zaimplementowane funkcje tworzenia statystyk ruchu w sieci. Na przykład większość ruterów posiada liczniki pakietów i oktetów, które weszły i wyszły z rutera przez każdy z interfejsów, a nawet mogą podzielić te pakiety na różne kategorie, w zależności od rodzaju protokołu, który generował te pakiety. Przełączniki i koncentratory także potrafią zbierać takie statystyki dla każdego z portów. Pozostaje tylko kwestia, jak zbierać te informacje i co z tymi informacjami robić.

Jeśli chodzi o sposób zbierania informacji, częstym rozwiązaniem jest SNMP. SNMP nie definiuje, jakie informacje powinny być zbierane przez urządzenie pracujące w sieci, lecz wymaga stosowania *Management Information Base* (M/B) w standardowym formacie. Kiedy opracowywano SNMP, jego autorzy chcieli, aby MIB mógł być rozszerzany o obsługę nowych urządzeń i nowych produktów. W związku z tym, mimo że standard opracowano zanim na rynku pojawiły się powszechnie używane obecnie urządzenia (a nawet zanim część z nich powstała), rozszerzenia MIB można zdefiniować w taki sposób, aby możliwe było uzyskiwanie informacji z prawie każdej klasy urządzeń sieciowych, jakie tylko można sobie wyobrazić. Jednym ze stosunkowo najnowszych rozszerzeń, opracowanych specjalnie dla zdalnego monitorowania, jest RMON MIB (RFC 1757). Choć RFC określa wymagania dedykowanego urządzenia do monitorowania sieci, to wielu producentów zaczęło dołączać część lub wszystkie grupy monitorowania RMON do swoich koncentratorów, przełączników i ruterów. Obiekty zdefiniowane w RMON MIB są pogrupowane w 10 kategoriach, z których każda jest implementowana opcjonalnie.

Jeśli jednak implementowana jest jakaś grupa, to konieczna jest implementacja wszystkich zdefiniowanych w niej obiektów. Poniżej wymienione zostały wszystkie grupy. Umieszczono też krótki opis działania i zadań każdej z nich:

The Ethernet Statistics Group
Zawiera statystyki mierzone w oparciu o próbkowanie każdego z monitorowanych interfejsów Ethernet.

The History Control Group
Kontroluje okresowe próbkowanie statystyczne danych z różnych typów sieci.

The Ethernet History Group
Zbiera okresowe wyniki próbkowania sieci Ethernet i zapisuje je w celu późniejszego użycia.

The Alarm Group
Okresowo pobiera wartości statystyczne ze zmiennych próbkowanych i porównuje je ze skonfigurowanymi wcześniej progami. Jeśli monitorowana zmienna przekroczy założony próg, generowana jest informacja o takim zdarzeniu.

The Host Group
Zawiera statystyki skojarzone z każdym hostem wykrytym w sieci.

The HostTopN Group
Używana do przygotowywania raportów, które opisują hosty ustawione w kolejności wynikającej z wartości określonej zmiennej statystycznej.

The Matrix Group
Przechowuje statystyki odnoszące się do wymiany informacji pomiędzy parami dwóch adresów.

The Filter Group
Pozwala na filtrowanie pakietów i tworzenie z nich strumienia danych, który następnie może być przechwytywany lub może generować zdarzenia.

The Packet Capture Group
Pozwala na przechwytywanie pakietów po ich przejściu przez filtry opisane w grupie filtrów.

The Euent Group
Kontroluje generowanie poszczególnych zdarzeń i informowanie o nich.

W większości osadzonych agentów RMON nie zaimplementowano wszystkich tych grup, ponieważ kilka z nich (na przykład grupa przechwytywania pakietów) może zajmować dużą ilość pamięci i innych zasobów komputera. Jednak grupy zaimplementowane zapewniają zwykle lepszy zestaw zmiennych monitorowanych niż ten, który znajduje się w standardowych specyfikacjach MIB. Powinieneś sprawdzić, jakie grupy RMON zaimplementowane są w Twoich urządzeniach lub zastanowić się nad zakupem dedykowanych narzędzi próbkowania RMON, które będą zbierały informacje z różnych punktów sieci.

Drugie pytanie, na które znacznie trudniej jest odpowiedzieć, brzmi: co należy zrobić z informacją, którą już mamy? Jeśli założymy, że do zbierania danych wykorzystujemy SNMP, to Twoje oprogramowanie na stacji zarządzającej pracą sieci może obsługiwać kilka sposobów manipulowania i analizy danych o sieci. Niestety, programy takie posługują się zwykle danymi o historii zdarzeń w sieci i pracują w oparciu o duże próbki danych zbierane co pewien czas, zamiast regularnie analizować dane o obciążeniu sieci.

W najprostszej formie analizy mogą być wykonywane w ten sposób, że dane o aktualnym ruchu w sieci porównywane są z zestawem wartości progowych i gdy znajdą się powyżej (lub poniżej, jeśli tak jest określony próg) założonych progów, to wygenerowany zostanie odpowiedni alarm. Taki sposób analizy nie będzie zawierał danych o trendach, które dostępne są w bardziej zaawansowanych metodach analizy, ale mimo to może być to dość użyteczny obraz aktualnego stanu sieci. Kiedy dostępne są dane o ruchu w sieci, to łatwo oglądać dane z poprzednich próbkowań i na ich podstawie określać przyszłe trendy. Dlatego ważne jest, aby szczegółowo przeanalizować dostępne informacje i zastanowić się, które z nich i jak często powinny być zbierane. W przypadku dużych sieci, składających się z setek ruterów, w których zbieranych jest zbyt dużo danych, łatwo można dojść do terabajtów informacji dziennie! W związku z tym, że większość maszyn nadal stosuje dyski, których pojemności mierzone są w dziesiątkach lub setkach gigabajtów, łatwo domyślić się, że istnieje potrzeba dokładnego selektywnego zbierania monitorowanych danych, określenia mniejszej częstotliwości próbkowania lub zrezygnowania z zapisywania informacji w celu analiz historycznych. Jeśli zrezygnujesz z zapisywania wcześniej uzyskanych danych, nie będzie możliwa analiza ruchu, a monitorowanie sieci zostanie zdegradowane do czegoś niewiele lepszego niż testowanie osiągalności.

Które z nich powinieneś wybrać, mając do dyspozycji różne rodzaje monitorowania? Odpowiedź zależy od tego, jak duża jest Twoja sieć, jak drogie są przestoje sieci i jakimi zasobami rozporządzasz. W związku z prostotą i małym zapotrzebowaniem na zasoby - wymagana jest jedynie maszyna i stosunkowo proste oprogramowanie -monitorowanie osiągalności jest często pierwszym rozwiązaniem wybieranym w małych sieciach lub w sieciach, które nie dysponują zasobami wystarczającymi do obsługi innych typów monitorowania. Nawet większe sieci mogą wykorzystywać z powodzeniem proste monitorowanie osiągalności urządzeń i nie ma powodu, aby przestać je wykorzystywać, kiedy zaimplementowane zostaną inne techniki monitorowania.

Monitorowanie tras w połączeniu z monitorowaniem osiągalności dobrze pracuje w sieciach średniej wielkości, ale zwykle jest to zbyt wiele jak na potrzeby małych sieci. W większych sieciach oprogramowanie służące do analizy zawartości tablic rutowania, pobranych z różnego rodzaju sprzętu, staje się bardzo skomplikowane, jeśli jego działanie nie zostanie ograniczone do mniejszych części sieci, na przykład do tych, które są bardziej narażone na występowanie uszkodzeń lub których przestoje są zbyt kosztowne.

Monitorowanie ruchu zużywa najwięcej zasobów. Zwykle wymaga dedykowanej stacji zarządzającej, której zadaniem jest zbieranie, przechowywanie i analiza statystyk ruchu w sieci, a następnie przedstawianie wyników personelowi obsługującemu sieć. Wymaga ono również obsługi pewnych metod pobierania informacji o ruchu ze wszystkich urządzeń lub przynajmniej z dość dużej grupy urządzeń pracujących w sieci. W związku z dużym zapotrzebowaniem na zasoby nie warto stosować monitorowania ruchu w większość małych sieci, którym nie przyniesie to korzyści uzasadniających poniesione wydatki. Jeśli przestoje powodują duże koszty, to monitorowanie ruchu jest jedyną metodą pozwalającą zidentyfikować problemy, zanim wystąpi uszkodzenie sieci i wszystko naprawić przy mniejszych kosztach. Możliwe jest więc stosowanie takich zaawansowanych rozwiązań w ograniczonej liczbie części sieci, których przestoje powodują największe koszty.

Wykrywanie uszkodzeń

Problemy w sieci będą występowały zawsze, niezależnie od tego, ile monitorujesz, analizujesz i ile prognoz wykonujesz, a także bez względu na to, jak niezawodne są urządzenia, których używasz, i jak dobry jest projekt i wykonanie sieci. Kiedy problem wystąpi, będziesz musiał go wyizolować i naprawić, działając pod silnym naciskiem. Zakładając, że niewiele osób potrafi jasno myśleć pod presją, powinieneś wcześniej przyjrzeć się swojej sieci, zidentyfikować najbardziej prawdopodobne uszkodzenia i określić sposoby ich usuwania.

Dwa najbardziej prawdopodobne uszkodzenia sieci to uszkodzenia sprzętowe, wynikające z uszkodzenia samego sprzętu lub oprogramowania, a także błędy popełniane przez ludzi. Trudno jest zapobiegać uszkodzeniom sprzętu, ponieważ tylko niektóre urządzenia zgłaszają wcześniej możliwość wystąpienia uszkodzenia, a każde urządzenie pracujące w sieci może ulec uszkodzeniu w dowolnym momencie. Na *szczęście* uszkodzenia sprzętu łatwo jest zlokalizować i naprawić. W dalszej części rozdziału omówię sposoby identyfikowania uszkodzonych komponentów.

Gdy już zlokalizujesz uszkodzony komponent, to - o ile to możliwe - powinieneś go wymienić na nowy, a uszkodzony odesłać do naprawy. Powinieneś więc zawsze dysponować zestawem części zapasowych. Wielkość tego zestawu zależy od rozmiarów Twojej sieci i od tego, jak ważny jest brak przestojów w pracy sieci. Jako minimum powinieneś przechowywać po jednej sztuce wszystkich elementów, których prawdopodobieństwo uszkodzenia jest duże, a w przypadku części drogich powinieneś podpisać porozumienie o szybkiej wymianie. Przechowywanie zapasowych części jest jednym z powodów, dla których warto ograniczyć liczbę różnych urządzeń stosowanych w sieci. Jeśli na przykład używasz w swojej sieci koncentratorów czterech różnych firm, to powinieneś zakupić i utrzymywać w zapasie cztery zapasowe koncentratory. Takie rozwiązanie może nie być zbyt drogie, ale zastanów się, co się będzie działo, kiedy w sieci zastosujesz cztery różne typy ruterów. Przekonasz się, że koszty mogą być bardzo wysokie.

Znacznie trudniej jest zidentyfikować błędy wynikające z uszkodzenia oprogramowania, jeszcze trudniej je naprawić. Łatwiej jest jednak zapobiegać takim błędom niż błędom sprzętowym. Jednym z najprostszych sposobów zapobiegania uszkodzeniom jest powstrzymanie się od instalowania ostatniej wersji oprogramowania dostarczanej przez producenta. Jeśli już to robisz, to przynajmniej nie rób tego pierwszego dnia po wypuszczeniu tego oprogramowania. Pozwól innym ludziom podjąć to ryzyko, a następnie poczekaj na zgłaszane przez nich informacje o błędach i problemach przy uaktualnianiu starszej wersji. Ostatnio jeden z głównych producentów sprzętu sieciowego wycofywał po dwóch dniach nową wersję oprogramowania, ponieważ znaleziono w nim bardzo poważne błędy, których nie udało się wykryć i usunąć na etapie testowania tego oprogramowania. Choć takie przypadki zdarzają się stosunkowo rzadko, to powstrzymanie się z instalacją nowego oprogramowania przez kilka tygodni może Ci oszczędzić testowania tego typu przypadków na własnej skórze.

Bez względu na to, jak ostrożnie podchodzisz do nowego oprogramowania, będą takie chwile, kiedy będziesz musiał iść do przodu - po to, by za pomocą jakiejś funkcji obsługiwanej przez nową wersję oprogramowania usunąć problem występujący w Twojej sieci. Właśnie zakończyłem dwudniową walkę z katastrofalnym uszkodzeniem oprogramowania w sieci, które ma już cztery tygodnie. Mimo że cztery tygodnie to obecnie dość długi czas, jeśli chodzi o oprogramowania ruterów, to nadal oprogramowanie to posiadało ukryty defekt, który ujawniał się tylko w określonej konfiguracji sieci. Tak się akurat złożyło, że w mojej sieci wystąpiła właśnie taka konfiguracja. Co możesz zrobić, kiedy zdarzy się taki przypadek? Po pierwsze zastanów się, jakie były powody uaktualnienia oprogramowania. Czy powodem była chęć posiadania wersji, która jest nowa? Czy dzięki temu chciałeś mieć dostęp do nowych funkcji? Czy chciałeś usunąć jakiś poważny błąd, który występował w poprzedniej wersji oprogramowania? Jeśli zainstalowałeś nowe oprogramowanie z któregoś z dwóch pierwszych powodów, to powinieneś zastanowić się nad ponowną instalacją poprzedniej wersji oprogramowania. Jeśli uaktualniałeś oprogramowanie, by usunąć problem z poprzedniej wersji, to musisz zdecydować, który z problemów jest poważniejszy, i postąpić zgodnie z tą decyzją. Oczywiście powrócenie do poprzedniej wersji nie jest jedyną dostępną możliwością. Możliwe, że będziesz mógł dokonać kolejnego uaktualnienia i zainstalować jeszcze nowszą wersję, która usunie występujące problemy. Możliwe również, że dostawca sprzętu przygotuje odpowiednią łatę lub przyśle Ci poprawioną nową wersję oprogramowania, która nie będzie zawierała błędu powodującego kłopoty w Twojej sieci.

Bez względu na to, co zrobisz, nie zapomnij o poinformowaniu producenta o problemach, które wystąpiły i warunkach, w jakich występowały. Możliwe, że natknąłeś się na problem, który jest już znany i producent posiada gotową łatę, która koryguje ten błąd. Możliwe również, że jesteś pierwszą osobą, która zgłosiła taki problem, i producent powinien o tym wiedzieć, by móc rozpocząć pracę nad usunięciem błędu. Kiedy zgłaszasz informację o problemie, powinieneś być przygotowany na przekazanie szczegółowych informacji dotyczących Twojej sieci, bieżącej konfiguracji urządzeń, wersji oprogramowania i urządzeń, których używasz, a zwłaszcza tego, co - Twoim zdaniem - wywołało problem. Jeśli producent nie będzie mógł odtworzyć warunków, w jakich wystąpił problem, to bardzo trudno będzie go usunąć.

Wykrywanie uszkodzeń

Informacje, których potrzebuje każdy z producentów, często *zależą* od urządzenia, w którym wystąpił błąd. Spróbuj wcześniej dowiedzieć się, jakich informacji potrzebuje w takich wypadkach producent posiadanego sprzętu. Jeśli problem wystąpi, będziesz wiedział, co przygotować, zanim przekażesz informację do producenta, kontaktując się z jego działem obsługi technicznej. Jeśli nie możesz uzyskać listy informacji, których zwykle potrzebuje w takich wypadkach, to możesz posłużyć się listą przedstawioną poniżej:

- dokładna informacja o modelu i opis konfiguracji rutera lub innego urządzenia, w którym wystąpiły problemy; informacje te powinny zawierać dane zainstalowanych kart interfejsów, a także sprzętowe weryfikacje kart;
- dokładny numer wersji oprogramowania zainstalowanego na wszystkich komponentach tego urządzenia, zwłaszcza jeśli poszczególne karty obsługiwane są przez własne wersje oprogramowania różniące się od wersji głównego systemu;
- konfiguracja, w której pracowało urządzenie w momencie wystąpienia uszkodzenia;
- wszelkie wyświetlane przez urządzenie informacje w momencie wystąpienia uszkodzenia lub informacje zapisane w rejestrze tego urządzenia, kiedy ulegało ono uszkodzeniu lub kiedy zostało ponownie uruchomione;
- jeśli uszkodzenie wywołane zostało przez Twoje działania, to powinieneś dokładnie zapisać, co robiłeś, zwłaszcza jeśli możesz powtórzyć tę sytuację i świadomie wywołać ten sam problem powtórnie;
- opis topologii sieci w sąsiedztwie urządzenia, które uległo uszkodzeniu; należy uwzględnić takie informacje jak numer, typ i model ruterów lub przełączników, a także informacje o tym, kiedy każde z tych urządzeń miało uaktualniane oprogramowanie lub moduły sprzętowe; jeśli to konieczne, należy wykonać odpowiedni rysunek.

Polecenia, które pozwolą na zebranie części wymienionych informacji, są w ruterach Cisco następujące:

show diag

Wyświetla informacje o wersji sprzętu wszystkich kart znajdujących się w ruterze, a także informację, w którym słocie każda z nich się znajduje. Polecenie dostępne jest tylko w niektórych modelach ruterów. Sprawdź w dokumentacji, czy Twój ruter przekazuje te informacje lub po prostu spróbuj. Jeśli polecenie nie jest zaimplementowane, to nic złego się nie stanie.

shoiwersion

Wyświetla informację o wersji oprogramowania uruchomionego w danym urządzeniu, włączając datę kompilacji i informacje o tym, kto dokonał kompilacji.

write term

Wyświetla informacje o bieżącej konfiguracji, z jaką pracuje urządzenie. Jeśli konfiguracja ta nie jest tą, z którą pracował ruter w momencie wystąpienia błędu, to powinieneś za wszelką cenę zdobyć właściwe informacje.

Polecenie to różni się od innych z powodów historycznych. Odpowiadające mu nowe polecenie to `show running-conf i g`, ale jeśli polecenie to jest dostępne, możesz prawdopodobnie użyć polecenia `show tech-support`, które jest jeszcze lepsze.

showstack

Wyświetla informacje o stosie odpowiadające ostatniej awarii.

show log

Wyświetla informacje rejestru dla aktualnie uruchomionego oprogramowania, jeśli zapisywanie informacji do rejestru jest buforowane. Szczegóły dotyczące konfiguracji plików rejestru w ruterze, a także informacje o tym, jak interpretować informacje z plików rejestru Twojego rutera, zostaną omówione w dalszej części tego rozdziału.

show tech-support

Wyświetla wszystkie informacje, których potrzebuje dział wsparcia technicznego. Polecenie to dostępne jest tylko w nowszych wersjach oprogramowania Cisco IOS.

Możesz również rozważyć możliwość udostępnienia swojej sieci pracownikom firmy, do której zwracasz się o pomoc. Jeśli zetknąłeś się ze szczególnie trudnym problemem', to umożliwienie im dostępu do sieci i przejrzenie konfiguracji i sposobu działania Twojej sieci może bardzo pomóc w szybkim rozwiązaniu.

Na razie najlepszą metodą radzenia sobie z błędami w oprogramowaniu jest ich unikanie. Jeśli masz możliwość przetestowania nowej wersji oprogramowania w wydzielonym do tego środowisku, zanim załadujesz je do swojej sieci, to w większości przypadków będziesz mógł zidentyfikować problemy, zanim wpłyną one na pracę Twojej sieci. Konieczne jest wtedy zbudowanie sieci testowej, w której będziesz wykonywał swoje test. Aby mieć pewność, że testy, które wykonasz, będą miały jakąś wartość, sieć testowa powinna składać się z tego samego typu komponentów co Twoja sieć zasadnicza. Jest to kolejny powód ograniczenia różnorodności sprzętu stosowanego w sieci. Każdy typ i marka urządzenia używanego w podstawowej sieci powinny być użyte również w sieci testowej. Jednym z dobrych sposobów uzyskania tej jednorodności sprzętu jest zbudowanie testowej sieci z części zapasowych, ale upewnij się, czy w ten sposób nie naruszysz licencji na oprogramowanie lub warunków kontraktu określających sposób wykorzystania zapasowych modułów. Niezależnie od tego, skąd weźmiesz elementy do sieci testowej, powinny być one jak najbardziej zgodne z tymi, których używasz w sieci podstawowej. Niewiele korzyści będziesz miał z używania w sieci testowej rutera Cisco 2501, jeśli w podstawowej sieci stosowane są rutery Cisco 7000. Każdy z tych dwóch typów rutera wykorzystuje inny model binarny systemu, co powoduje, że rodzaje błędów występujących w tych ruterach mogą być zupełnie inne. Prawdą jest, że różne modele ruterów tego samego producenta współdzielą prawdopodobnie sporą część kodu, zwłaszcza obsługującego protokoły rutowania, ale na pewno będą miały różny kod obsługi różniących się między sobą architektur pamięci, różne programy obsługi interfejsów i tak dalej.

Wykrywanie uszkodzeń

Jeśli urządzenia te zbudowano w oparciu o różne CPU to na pewno do kompilacji binarnego obrazu systemu używano różnych narzędzi, które same mogły zawierać drobne błędy. Mimo to trzeba pamiętać, że każde testy są lepsze od zainstalowania oprogramowania bez żadnego sprawdzenia.

Niestety, sieć testowa nie jest w stanie dokładnie symulować warunków sprzętowych Twojej sieci podstawowej i trudno w niej stworzyć realną strukturę ruchu w sieci. Dlatego warto zastanowić się nad połączeniem sieci testowej z siecią podstawową w dobrze kontrolowanym punkcie, przeniesieniem obsługi użytkowników sieci na część testową i obserwowaniem pracy takiego układu przez kilka tygodni. Jeśli nie wystąpią żadne problemy, to możesz spokojnie zainstalować nowe oprogramowanie w całej sieci podstawowej. Jeśli natomiast wystąpią problemy, to dotkną one również samych użytkowników i od nich możesz uzyskać dokładne informacje o tym, co się wydarzyło. Jeśli problemy będą poważne, to nie pozostanie Ci nic innego jak rozłączyć sieć testową i podstawową.

Najczęstszym powodem kłopotów z pracą sieci są błędy użytkowników. Błędy te mogą dotyczyć Twojego personelu i obejmować pomyłki w konfiguracji oprogramowania i w zestawianiu połączeń lub mogą to być błędy użytkowników sieci, którzy mogą na przykład wykasować pliki konfiguracyjne sieci ze swoich komputerów PC. Choć nie masz wpływu na błędy użytkowników końcowych, to błędom popełnianym przez Twój personel możesz w większości przypadków zaradzić. Sposoby zapobiegania błędom popełnianym przez personel obsługujący sieć zostaną omówione później. Kiedy jednak takie błędy występują, to najlepszym sposobem ich wykrywania i usuwania jest posiadanie dokładnego zapisu czynności, jakie wykonywali ludzie z Twojego działu. Jeśli nie wiesz, który z pracowników robił coś, w której z szaf krosowniczych to robił lub co zostało ostatnio zmienione w konfiguracji oprogramowania, to zlokalizowanie przyczyn wystąpienia przerw w pracy sieci staje się bardzo trudne. Z drugiej strony, jeśli wiesz, że Janek był właśnie na czwartym piętrze w zlokalizowanym tam punkcie krosowniczym i dołączał nowe kable sieciowe, a w tym samym czasie zatelefonował użytkownik z czwartego piętra z informacją, że nagle stracił połączenie z siecią, to wiesz, od czego zacząć poszukiwanie przyczyn uszkodzenia. Być może Janek przypadkowo wyciągnął wtyczkę kabla łączącego z siecią tego właśnie użytkownika lub źle wykonał przekrosowanie. W obu przypadkach dzięki informacjom o tym, gdzie był i co robił pracownik, możesz przystąpić do naprawy powstałego błędu.

Procedury wykrywania uszkodzeń

Choć dobrze jest podzielić źródła uszkodzeń sieci na te, których przyczyny leżą w sprzęcie, oprogramowaniu i błędach ludzi, to kiedy wystąpi takie uszkodzenie, często nie można określić, jakiego rodzaju uszkodzenia poszukujemy lub gdzie go szukać. Z tego powodu konieczne jest opracowanie zestawu procedur wspomagających wykrywanie uszkodzeń.

Rób notatki

Nie ma nic bardziej denerwującego niż odkrycie, że problem z pracą sieci wynika z tego, że umieściłeś w niej uszkodzony komponent wierząc, że jest on dobry. Najlepszym sposobem zapobiegania takim problemom jest robienie notatek na temat tego, które elementy sprawdzałeś, jakie były wyniki tych działań, który element i gdzie został przeniesiony. Notatki te mogą przybierać różne formy, poczynając od najprostszej (papier i ołówek) i mogą zawierać dowolną liczbę informacji. Jako minimum powinieneś prowadzić zapisy dotyczące wszystkich przemieszczeń sprzętu, zmian okablowania, wymiany płyt w urządzeniach i zmian konfiguracyjnych w oprogramowaniu. W przypadku przemieszczania sprzętu upewnij się, czy zapisałeś numer seryjny urządzeń, które zmieniły miejsce, ponieważ jest to jedyny sposób na określenie, gdzie znajduje się jeden z kilkudziesięciu koncentratorów Ethernet. Takie notatki pomogą Ci choćby w przypadku, kiedy po usunięciu problemu będziesz chciał dokładnie odtworzyć poprzednią konfigurację sprzętową sieci. Jeśli będziesz musiał zatelefonować do sprzedawcy z prośbą o pomoc, to Twoje dokładne notatki pozwolą producentowi na sprawne rozpoczęcie diagnozowania zgłoszonego problemu. Być może szybciej połączą Cię z inżynierem, ponieważ stwierdzą, że nie jesteś niezorientowanym użytkownikiem, który nie wie w ogóle, o co chodzi i co się stało.

Wszystko oznaczaj

Z robieniem dobrych notatek związane jest również oznaczanie wszystkiego, zanim jeszcze wystąpią jakiekolwiek problemy. Przede wszystkim należy oznaczyć każde z urządzeń znajdujących się po obu stronach każdego z kabli. Oznaczenia te powinny wyraźnie informować, z jakim urządzeniem mamy do czynienia, gdyż w typowej sieci jest zwykle wiele urządzeń tego samego typu. Oznaczenie każdej strony kabla powinno informować o tym, jaki port i jakie urządzenie obsługuje to łącze. Powinno również wskazywać, gdzie jest drugi koniec kabla, choć nie musi być to tak szczegółowa informacja. Powodem, dla którego powinieneś oznaczyć swoje urządzenia aktywne, jest to, że możesz mieć w sieci sześć identycznych koncentratorów Ethernet umieszczonych w stojaku i chciałbyś wiedzieć, który z nich próbujesz właśnie naprawiać. Oznaczenia te rozszerzają informacje zawarte w Twoich notatkach (nie powinny natomiast zastąpić tych notatek) o przemieszczaniu sprzętu. Pamiętaj o uaktualnianiu etykiet, kiedy dokonasz zmiany miejsca, w którym sprzęt pracuje. Nie odkładaj wykonania tych uaktualnień, bo jeśli coś się stanie, to będziesz musiał pracować z bezużytecznymi etykietami urządzeń.

Oczywiste jest również to, dlaczego powinieneś oznaczyć końce kabli zapisując informację o tym, do czego są one dołączone. W sytuacji poważnej awarii będziesz musiał odłączyć kilka kabli od uszkodzonego urządzenia lub karty interfejsu; ostatnią rzeczą, którą w takiej chwili będziesz chciał się zajmować jest niewątpliwie zapamiętywanie, który kabel gdzie był przyłączony. Oznakowanie każdego kabla zawierające informacje o tym, gdzie znajduje się jego drugi koniec, nie jest już takie oczywiste. Przecież skoro odłączasz tylko jeden koniec kabla, to czy obchodzi Cię, gdzie znajduje się jego drugi koniec? Czasem może być konieczna wymiana całego kabla. Podczas sprawdzania urządzenia podejrzanego o uszkodzenie może się też okazać, że pracuje ono poprawnie, a powodem usterki jest urządzenie dołączone na drugim końcu kabla. W takich przypadkach etykieta, która wskaże Ci, gdzie znajduje się drugi koniec kabla (do którego urządzenia, a nawet portu, jest włączony), może oszczędzić Ci sporo czasu.

Wykrywanie uszkodzeń

Fizyczne oznaczenie kabli i urządzeń to jeszcze nie wszystko. Wiele urządzeń aktywnych pracujących w sieci pozwala na programowe oznaczanie poszczególnych portów urządzenia. Możesz, więc zapytać ruter, przełącznik lub koncentrator, co jest dołączone do jego portu. W naszych przełącznikach sieci Ethernet wykorzystujemy tę funkcję. Każdy port w naszej sieci ma wypełnione pole oznaczenia, w którym znajduje się informacja o tym, dokąd prowadzi dołączony do tego portu kabel. Jeśli drugi koniec kabla kończy się na porcie innego koncentratora sieci Ethernet, to oznaczenie nosi nazwę tego koncentratora. Jeśli koniec kabla prowadzi do gniazdka w pokoju biurowym, to w etykiecie umieszczona jest informacja o numerze pokoju i identyfikatorze gniazda. Takie rozwiązanie pomaga nam w wykonywaniu przełączeń. Jest też przydatne podczas lokalizacji uszkodzeń w okablowaniu sieci. Etykiety opisane na portach rutera mogą zawierać informację o grupach lub budynkach obsługiwanych przez ten interfejs LAN lub nazwę odległego urządzenia albo numer obwodu w przypadku, gdy jest to łącze WAN. Na przykład, aby oznaczyć port rutera dołączony do łącza WAN prowadzącego do Gdańska, umieszczając tam identyfikator obwodu, należy w konfiguracji interfejsu użyć następującego polecenia:

```
description łącze WAN do Gdańska -1ZB33489-997F
```

Informacja ta wyświetlana będzie po wykonaniu polecenia `show interface`. Choć informacje te dostępne są na pewno w bazie danych okablowania lub w wydrukowanych zestawach, to przeszukiwanie materiałów w celu odszukania określonych informacji jest stratą czasu, zwłaszcza gdy musimy szybko usunąć awarię. Znacznie łatwiej jest zapytać urządzenie, co jest do niego dołączone lub spojrzeć na kable i zobaczyć, gdzie znajduje się urządzenie, do którego prowadzi ten kabel. Oczywiście opisany system oznaczeń programowych działa poprawnie, gdy oznaczenia te są uaktualniane na bieżąco.

Określ problem

Pierwszą rzeczą, jaką powinieneś zrobić, kiedy stwierdzisz, że sieć uległa uszkodzeniu, to wziąć głęboki wdech i zrelaksować się. Potem weź kolejny głęboki wdech i ponownie się zrelaksuj. Może brzmi to dziwnie, ale to naprawdę bardzo ważne. Za chwilę poprosisz Twój mózg i ciało, aby dość ciężko popracowały, tak więc kilka głębokich wdechów dostarczy Twemu ciału trochę więcej tlenu, przygotowując je do pracy.

Teraz już jesteś gotowy, ale zanim zaczniesz w pośpiechu naprawiać sieć, spróbuj dokładnie określić, czego dotyczy problem. Być może konieczne będzie wykonanie telefonu do użytkownika, który zgłosił problem, w celu uzyskania szczegółów. Możesz też spróbować powtórzyć na swojej stacji roboczej działania, które doprowadziły do jego wystąpienia. Jeśli problem dotyczy określonej grupy maszyn lub danego serwera, nie wyciągaj od razu wniosków, że powstał w tej grupie lub serwerze. Jest to bardzo prawdopodobne, ale nie ma całkowitej pewności, że tak właśnie jest. Jeśli problem wydaje się być związany z osiągalnością poszczególnych adresów, wykonaj kilka szybkich testów z różnych miejsc w sieci, aby stwierdzić, czy jest to problem występujący lokalnie, czy też jest on globalny i występuje w całej sieci.

Innymi słowy, zatrzymaj się i pomyśl przez chwilę o problemie, który masz rozwiązać, a jego przyczyny staną się być może bardziej wyraźne. Najgorszą rzeczą jest w takich wypadkach pośpiech i rozpoczęcie naprawy od wymiany komponentów sieci, które mają coś wspólnego z uszkodzoną częścią sieci. Kiedy już zidentyfikujesz problem, gotów jesteś na jego usunięcie i przywrócenie poprzedniego stanu sieci.

Proces eliminacji

Kolejną techniką, której być może będziesz musiał użyć, jest proces eliminacji kolejnych przyczyn wystąpienia uszkodzenia. Czasami problem wyraźnie można zdefiniować. Na przykład masz użytkownika, który nie może połączyć się z serwerem plików, a wstępne sprawdzenie sieci wykazało, że zarówno maszyna użytkownika, jak i serwer plików, funkcjonują normalnie. I co teraz?

Jeśli możesz określić, które części sieci na pewno nie są związane z tą awarią, to możesz wyeliminować sieci z dalszych rozważań. Na przykład większość urządzeń, które znajdują się w innym budynku niż komputer użytkownika i serwer plików, można z pewnością skreślić z listy sprzętu powodującego problemy. Dokładne sprawdzenie tego, co zostało, powinno więc doprowadzić do zlokalizowania przyczyn. Jeśli takie postępowanie nie przyniesie efektów, to przynajmniej masz ograniczony zestaw urządzeń do dokładniejszego przetestowania. Czasami samo zastanowienie się, jakie urządzenia nie powodują takich błędów, może podsunąć pomysł, które z pozostałych urządzeń jest winne. Na przykład kiedy będziesz eliminował urządzenia znajdujące się w innych budynkach, to na pewno zajmiesz się również serwerem DNS, i może się okazać, że skoro maszyna użytkownika lub serwer plików nie może komunikować się z DNS, to połączenie między tymi dwoma urządzeniami może być uszkodzone. Może się również okazać, że rekordy DNS opisujące maszynę użytkownika zostały przypadkowo usunięte, przez co serwer plików odmawia nawiązania połączenia.

Bądź ostrożny podczas eliminowania *rzeczy,* które na pierwszy rzut oka nie wydają się być przyczyną występujących w sieci problemów. Czasami uszkodzenie występujące w jednym z komponentów może mieć duży wpływ na sieć lub może mieć dziwne, niezwiązane z tym urządzeniem symptomy, co spowoduje, że zaczniesz przyglądać się innej części sieci.

Dziel i eliminuj

Jeśli problem jest rozległy lub trudno go usunąć, to opisane wyżej techniki nie mają większego zastosowania i nie pozostaje Ci nic innego, jak użyć techniki polegającej na dzieleniu sieci na mniejsze części i usuwaniu problemu w każdej z tych części po kolei. Podstawy tej techniki są proste: większość ludzi stosuje ją w codziennym życiu bez zastanawiania się nad tym, jaka to technika. Kiedy problem, z którym się stykamy, jest zbyt duży lub zbyt skomplikowany, by rozwiązać go jako całość, powinno się go podzielić na mniejsze zadania i rozwiązać każde z nich oddzielnie, a następnie złożyć wszystko z powrotem do kupy.

Wykrywanie uszkodzeń

Pomyśl na przykład, w jaki sposób wyszukujesz czyjeś nazwisko w książce telefonicznej. Otwierasz książkę w losowo wybranym miejscu i sprawdzasz, czy pierwsza litera szukanego nazwiska jest wcześniej niż miejsce, w którym otworzyłeś książkę czy też za nim. Następnie przerzucasz kartki aż do litery, od której zaczyna się nazwisko, i odszukujesz kartkę, na której wydrukowano nazwiska zaczynające się na tę literę. Następnie przeszukujesz stronę za stroną, aż znajdziesz stronę zawierającą to nazwisko, i - opierając się na pozostałych danych osoby - odszukujesz właściwe nazwisko. Gdybyś na samym początku zdecydował się na przeglądanie książki telefonicznej strona po stronie od samego początku, to odszukanie tego nazwiska zajęłoby Ci godziny, a nawet dni. Dzięki podzieleniu zadania na mniejsze części możesz je wykonać w ciągu minuty lub dwóch. Ta sama technika postępowania może pomóc Ci w usuwaniu problemów z siecią, zwłaszcza w przypadku uszkodzeń mających rozmiary katastrof.

Kiedy wystąpią poważne uszkodzenia, określane jako katastrofy, to pierwszym krokiem powinno być podzielenie sieci na tyle mniejszych części, ile koniecznych jest do odtworzenia funkcji w tych częściach sieci. Oznacza to, że być może będziesz musiał odłączyć główne części rdzenia sieci, aż do pojedynczego rutera w sieci. Kiedy już uruchomisz niektóre części tak podzielonej sieci, możesz zacząć dołączać je do siebie i do głównej części, obserwując, jak się zachowują, i testując działanie tak połączonej sieci. Postępuj tak z każdą częścią sieci, aż trafisz na część, której nie możesz dołączyć, bo jest uszkodzona, lub aż odtworzysz poprzednią architekturę sieci. Postępując w ten sposób powinieneś znaleźć część, której nie możesz dołączyć do reszty. Aby zlokalizować uszkodzenie, możesz ją podzielić na mniejsze części i - dołączając każdą z tych mniejszych części do reszty sieci - dojdziesz do miejsca, które powoduje uszkodzenie.

Na przykład jeśli masz w sieci ruter obsługujący wiele portów Ethernet i połączenie FDDI z rdzeniem sieci i ruter ten pracuje poprawnie, ale po dołączeniu do rdzenia FDDI powoduje zatrzymanie pracy sieci, spróbuj odłączyć wszystkie segmenty Ethernet, a następnie dołącz ruter łączem FDDI. Jeśli tak połączone urządzenia będą pracowały poprawnie, to możesz zakładać, że problemy nie są spowodowane złą pracą łącza FDDI lub rutera i trzeba przeanalizować poszczególne segmenty sieci Ethernet dołączając je do rutera po kolei. Segment, który powoduje problemy, należy teraz podzielić na mniejsze części i przeanalizować każdą z nich. W końcu znajdziesz maszynę, która przy próbie dostępu do innego rutera powoduje zamknięcie pętli rutowania, a generowany w ten sposób ruch powoduje uszkodzenie rutera.

Jeśli problem występujący w sieci jest trudny do rozwiązania, ale nie można go zaliczyć do katastrof, spróbuj podzielić sieć na dwie części (niekoniecznie równe) i ustal, po której stronie podziału występuje ten problem. Następnie część tę podziel znowu na połowy i część, która pracuje, poprawnie dołącz, jeśli to możliwe, do funkcjonującej połowy. Kontynuując dzielenie uszkodzonej części sieci na dwie części dojdziesz do momentu, kiedy będziesz w stanie wyizolować problem i usunąć go. Po wykonaniu naprawy połącz wszystkie części sieci i sprawdź, czy usterka znikła.

Narzędzia pomocne przy monitorowaniu i wykrywaniu uszkodzeń

Niezależnie od rodzaju monitorowania, które zastosowałeś w swojej sieci, pamiętaj, że w sieci nie musisz stosować tylko jednego rodzaju monitorowania lub pozostać przy jednym programie monitorującym w całej sieci. Skoro nie ma takich ograniczeń, to na pewno będziesz potrzebował narzędzi, które pomogą Ci skutecznie monitorować sieć. Kiedy będziesz miał kłopoty z pracą sieci lub będziesz musiał zlokalizować uszkodzenie, to dobry zestaw narzędzi może sprawić, że teoretycznie niemożliwe zadanie da się w miarę szybko wykonać. Często narzędzia do wykrywania uszkodzeń i narzędzia do monitorowania pracy sieci są te same.

Możesz oczywiście zakupić specjalne narzędzia dostępne na rynku. W przypadku narzędzi pracujących z wykorzystaniem SNMP jest to prawdopodobnie jedyny sposób zdobycia takiego oprogramowania. Dostępnych jest jednak także sporo darmowych programów, które mogą pomóc Ci monitorować pracę sieci i wykrywać jej uszkodzenia. W części tej opiszę krótko kilka z nich. Większa lista narzędzi, zarówno tych dostępnych za darmo, jak i kompletnych rozwiązań firmowych, dostępna jest dla całej społeczności internetowej w RFC 1470.

Dostęp Out-of-Band

Większość urządzeń sieciowych posiada mechanizm umożliwiający monitorowanie ich pracy i konfigurację typu *in-band.* Urządzenie może być dostępne przez Telnet, SNMP lub na oba sposoby. Kiedy jednak sieć ulegnie uszkodzeniu, nawiązanie połączenia z urządzeniem za pomocą tych mechanizmów może być niemożliwe. Możliwość dostępu do urządzenia w trybie *out-of-band w* takich przypadkach może zaoszczędzić sporo czasu i może być jedynym sposobem uzyskania dostępu do urządzenia, które znajduje się dość daleko, bez konieczności fizycznego dotarcia do niego.

Najbardziej naturalnym sposobem uzyskiwania dostępu *out-of-band* do urządzenia sieciowego jest użycie modemu przyłączonego do portu zarządzania tego urządzenia. Dzięki takiemu rozwiązaniu możliwe jest dodzwonienie się do urządzenia z własnego peceta lub terminala w przypadku, kiedy nie można się do niego dostać przez sieć. Oczywiście konieczne jest zabezpieczenie tych zestawianych na żądanie połączeń hasłem ustawionym na modemie, przez oddzwanianie modemu pod określony numer, hasła na porcie zarządzającym lub przez dowolne kombinacje tych metod. Największym problemem wykorzystywania modemu jest to, że rozwiązanie takie staje się dość drogie, kiedy chcesz w ten sposób obsługiwać wiele urządzeń w sieci, włączając w to koncentratory i przełączniki. Wydatki te szczególnie trudno uzasadnić, jeśli rozważy się liczbę przypadków, kiedy takie połączenie jest wykorzystywane.

Rozwiązaniem, alternatywnym jest wykorzystanie serwera terminali. Działa ono dobrze, kiedy chcesz uzyskać dostęp do wielu urządzeń rozmieszczonych blisko siebie, na przykład w punkcie krosowym lub w pomieszczeniu przeznaczonym na sprzęt aktywny sieci. Zamiast dołączania terminali do każdego z portów serwera możliwe jest dołączenie portów zarządzania urządzeniami, do których chcesz mieć dostęp. Aby uzyskać dostęp do serwera można dołączyć do niego pojedynczy modem lub terminal, w zależności od tego, czy ten serwer terminali jest umieszczony blisko, czy też znajduje się w odległym miejscu. Modem lub terminal można wykorzystywać następnie do uzyskania dostępu do każdego z urządzeń przyłączonych do serwera terminali. Jeśli serwer znajduje się w centrum obliczeniowym, to być może nie musisz nawet dołączać terminala bezpośrednio do serwera terminali, lecz będziesz mógł dołączyć ten serwer do segmentu sieci, do którego dołączona jest stacja zarządzania. Tak zrealizowane połączenie będzie pracowało poprawnie pod warunkiem, że uszkodzeniu nie ulegnie wspomniany segment sieci lub sama stacja zarządzająca. Na szczęście segment zarządzania siecią to zwykle segment lokalny i łatwo go szybko naprawić.

Kolejną zaletą wykorzystania serwera terminali jest to, że możliwe jest takie skonfigurowanie stacji roboczej, aby pozostawała ona logicznie dołączona do portów serwera terminali, a zatem do portów zarządzania poszczególnych urządzeń sieciowych, i *przez* takie połączenie odbierała wszystkie informacje rozsyłane przez te urządzenia. Czasami komunikaty będą jedyną wskazówką, dlaczego dane urządzenie uległo uszkodzeniu. Na przykład, nawet jeśli Twój ruter ma bufor, w którym przechowuje pewne informacje, i mimo że zawartość tego bufora nie zostanie usunięta w momencie uszkodzenia sprzętu, mechanizm ten działa dobrze tylko w określonych przypadkach. Co się stanie, jeśli ruter ten po prostu się zawiesi i przestanie reagować na Twoje działania, ale nie wykona automatycznego restartu? Skoro się nie zrestartował, to nie dysponujesz żadnymi informacjami wysyłanymi przez ruter w takiej sytuacji. Być może ruter umieścił coś w buforze, ale Ty nie możesz uzyskać żadnych informacji z bufora, ponieważ ruter nie reaguje na zapytania. Jeśli zdecydujesz się wyłączyć urządzenie, aby odzyskać nad nim kontrolę, to informacje zapisane w buforze prawdopodobnie zostaną utracone. Jeśli jednak masz możliwość przekazywania komunikatów z portu zarządzania na konsolę, to być może ruter wyśle tą drogą jakieś ważne informacje tuż przed zawieszeniem się.

Ping

Ping jest programem dołączonym do większości wersji oprogramowania TCP/IP. Jest również dostępny na różne platformy, poczynając od komputerów osobistych, a na wysoko wydajnych superkomputerach kończąc. Większość ruterów, koncentratorów i przełączników obsługuje polecenie *ping* jako jedno z poleceń swego interfejsu konfiguracyjnego. *Ping* wysyła komunikat zawierający zapytanie o echo ICMP do określonego hosta. Każde urządzenie, w którym zaimplementowano obsługę IP, musi odpowiadać na zapytanie o echo protokołu ICMP, odsyłając komunikat odpowiedzi. *Ping* mierzy czas pomiędzy wysłaniem zapytania a odebraniem odpowiedzi i wyświetla informację o tym, czy adres jest osiągalny (czy usłyszał odpowiedź echo, czy nie), a także czas podróży pakietów tam i z powrotem.

Ping jest prawdopodobnie najczęściej stosowanym narzędziem monitorowania i wykrywania błędów w pracy sieci, ponieważ jest szeroko dostępny, mimo że liczba informacji jakie dostarcza jest ograniczona, a nawet mogą być one nieprawdziwe. Przede wszystkim należy pamiętać o tym, że zapytanie o echo i odpowiedź na nie mogą być przesłane różnymi ścieżkami; rutowanie asymetryczne jest spotykane dość często w dużych redundantnych sieciach. Wiedząc o tym, trzeba zdawać sobie sprawę, że brak odpowiedzi na echo nie informuje, która z kilku dostępnych ścieżek może być uszkodzona, tylko o tym, że nie można osiągnąć miejsca przeznaczenia i wrócić. Pakiety zapytania o echo ICMP mogą być gubione w wyniku wystąpienia przeciążenia sieci, a nawet mogą zwiększać to przeciążenie, ponieważ z punktu widzenia sieci są tylko kolejnymi pakietami. Pomimo tych wad *ping* pozwala na szybkie sprawdzenie osiągalności danego adresu i jako taki może posłużyć do stworzenia podstawowego i niedrogiego systemu monitorowania osiągalności urządzeń w sieci. Jest to bardzo często pierwsze narzędzie wykorzystywane przy lokalizowaniu uszkodzeń, stosowane do wstępnego określenia, z jak rozległym problemem mamy do czynienia.

Traceroute

Ping jest bardzo przydatny do ustalenia, czy dane miejsce w sieci jest osiągalne. Jeśli jednak *ping* nie zadziała, to nie informuje, który z kilkunastu ruterów, przez które prowadzi ścieżka łącząca dwa punkty, uległ uszkodzeniu i nie przesyła pakietów. *Traceroute* załatwia ten problem pozwalając znaleźć każdy z ruterów, przez który przesyłany jest pakiet od hosta A do hosta B. Informacje te uzyskiwane są dzięki temu, że każdy z ruterów, przez które prowadzi ścieżka, odsyła w odpowiedzi komunikat o błędzie ICMP. Pakiety IP zawierają wartość czasu życia (TTL), którą każdy z ruterów obsługujących pakiet zmniejsza o jeden. Kiedy wartość ta osiągnie zero, ruter odrzuca pakiet i odsyła z powrotem do nadawcy komunikat ICMP o przekroczeniu czasu życia pakietu. Program *traceroute* wysyła pierwszy pakiet z TTL równym 1. Pierwszy ruter zmniejsza tę wartość i odsyła w odpowiedzi wspomniany komunikat o błędzie ICMP, na podstawie którego *traceroute* odkrywa ruter pierwszego przeskoku. Następnie wysyłany jest pakiet z TTL równym 2, wartość ta zmniejszana jest o l przez pierwszy ruter i pakiet przesyłany jest dalej. Drugi ruter zmniejsza tę wartość do zera, co powoduje odesłanie z powrotem komunikatu o błędzie ICMP, dzięki któremu program zdobywa informację o drugim ruterze. Postępując w ten sam sposób, *traceroute* zmusza wszystkie rutery na ścieżce do miejsca docelowego do wysłania komunikatu o błędzie ICMP i zidentyfikowania się. W końcu wartość TTL jest na tyle duża, że pakiet dociera do miejsca docelowego i *traceroute* kończy swoje działanie. Program *traceroute* przestaje również odkrywać kolejne rutery na ścieżce, kiedy TTL przekroczy pewną maksymalną wartość (zwykle jest to 30).

Czy w tym pomysłowym planie może coś nie zadziałać? Mnóstwo rzeczy! Niektóre urządzenia nie generują komunikatów ICMP o przekroczeniu czasu życia, a to dlatego, że implementacja IP w tych urządzeniach nie do końca jest zgodna ze standardami IP, lub dlatego, że urządzenia te zostały tak skonfigurowane. Nie jest to jednak zwykle duży kłopot, ponieważ kolejne urządzenie odeśle taki komunikat i będziemy mieli po prostu niezidentyfikowaną dziurę pomiędzy kolejnymi urządzeniami.

Problemy zaczynają się, kiedy zastanowimy się nad tym, jakie pakiety wysyła *traceroute,* i jak to się ma do konfiguracji niektórych ścian ogniowych pracujących w sieci. Większość programów typu *traceroute* wysyła datagram UDP do losowo wybranego wysokiego portu UDP. W większości przypadków ściany ogniowe nie odfiltrowują tego typu pakietów, ponieważ trudno jest odróżnić je od dozwolonego ruchu generowanego przez użytkowników. Niestety czasami pakiety te są odfiltrowane, co powoduje, że *traceroute* po prostu przestaje działać. Inne programy typu *traceroute, z* których najpopularniejszy jest program *tracert* firmy Microsoft, wykorzystuje do pracy zapytania o echo ICMP (pakiety *ping).* Znacznie bardziej prawdopodobne jest, że tego typu pakiety zostaną odfiltrowane przez ścianę ogniową, choć komunikacja oparta o protokoły TCP i UDP jest przez nie przepuszczana. Jeśli trafisz na takie zabezpieczenia, po prostu nie miałeś szczęścia. Mimo że różne wersje opisanego programu mają kłopoty we współpracy ze ścianami ogniowymi lub ruterami nie spełniającymi standardów implementacji, użycie tego typu programów jest niewątpliwie konieczne. Należy tylko pamiętać o wymienionych wyżej różnicach, co pozwoli lepiej zrozumieć, dlaczego wyniki śledzenia tras wykonane za pomocą *traceroute* różnią się w zależności od tego, na którym stanowisku w sieci je uzyskano.

W najprostszej formie program *traceroute* (lub *tracert)* wymaga podania tylko jednego parametru: nazwy odległego hosta:

```
Tracert www.ora.com

Tracing route to amber.ora.com [198.112.208.11] over a
maximum ot 30 hops:

1   *     *          *          Request timed out.
2   187 ms 2743 ms 169 ms     laf-gwO.hol l i.com [204.95.254.1]
3   235 ms 154 ms   1745 ms    204.95.255.245
4   157 ms 155 ms   180 ms     204.95.255.241
5   167 ms 154 ms   149 ms     204.180.39.42
6   202 ms 157 ms   153 ms     noon.nap.net [206.54.224.142]
7   158 ms 165 ms   156 ms     aads.mci.net [198.32.130.12]
8   404 ms 282 ms   257 ms     core3-hssil-0.WillowSprings.mci.net
                                   [204.70.1.197]
9   221 ms 229 ms   181 ms     core-hssi-2.Boston.mci.net [204.70.1.45]
10  189 ms 176 ms   247 ms     borderl-fddi-0.Boston.mci.net [204.70.2.34]
11  177 ms 170 ms   171 ms     nearnet.Boston.mci.net [204.70.20.6]
12  182 ms 185 ms   245 ms     cambridge2-cr2.bbnplanet.net [192.233.33.2]
13  495 ms 219 ms   242 ms     cambridgel-crl.bbnplanet.net [192.233.149.201]
14  186 ms 196 ms   176 ms     cambridgel-cr4.bbnplanet.net [199.94.205.4]
15  209 ms 280 ms   209 ms     ora.bbnplanet.net [192.233.149.74]
16  221 ms 265 ms   193 ms     amber.ora.com [198.112.208.11]

Tracę complete.
```

Z wyświetlonego polecenia możemy się bardzo dużo dowiedzieć. Pierwszy wiersz wskazuje, że pierwsza maszyna wcale nam nie odpowiedziała. Nie oznacza to, ż< wystąpił jakiś błąd, lecz to, że maszyna ta nie mogła lub nie chciała udzielić odpowiedzi na nasze zapytanie. Ponieważ kolejne zapytania są przesyłane dalej i uzyskujemy na nie odpowiedzi, możemy wnioskować, że w pierwszej maszynie nie dzieje się nic złego.

Z uzyskanych odpowiedzi wynika, że maszyna, na której pracuję, znajduje się K przeskoków od hosta *www.ora.com* i wszystkie rutery pośredniczące w przekazywaniu pakietów zostały wymienione wraz z ich adresami IP i nazwami - jeśli te był} dostępne. Jeśli nie chcesz, aby *traceroute* dokonywał rozwikłania adresów na nazwy musisz podać w poleceniu odpowiednią opcję (zwykle jest to -n w *traceroute z* systemów Unix i -d w *tracert* firmy Microsoft). Opcji tej użyjesz na pewno wtedy, gdy mas: problemy z dostępem do serwera DNS lub jeśli Twój serwer DNS ma problemy : dostępem do sieci Internet (na przykład uszkodzone jest łącze z Internetem) W wyświetlanych wynikach znajdują się również informacje o tym, ile czasu zajęła pakietowi podróż (wraz z powrotem) do każdego z ruterów. Ponieważ czasy te mogą się różnić między sobą, a niektóre pakiety mogą się zagubić, *traceroute* wysyła zwykli trzy zapytania do każdego rutera, aby uzyskać większą niezawodność i dokładność odpowiedzi.

Jeśli program nie dotrze do punktu przeznaczenia, to przyczyną jest jeden z dwóch przypadków, z których każdy wyświetla inny rodzaj odpowiedzi. Polecenia pokazane poniżej pokazują, że ruter przeskoku numer 12 wysłał do nas komunikat ICMP c nieosiągalności, informując, że nie zna trasy do podanego punktu przeznaczenia:

```
12 !H !H !H cambridge2-cr2.bbnplanet.net [192.233.33.2]
```

Jeśli ruter ten znajduje się pod kontrolą i powinien znać tę trasę, to powinieneś dowiedzieć się, dlaczego przestał obsługiwać ten kierunek. *Traceroute* może równie: przestać pracować, wyświetlając kilka komunikatów takich jak pokazane poniżej:

```
10      189 ms      176 ms    247 ms borderl-fddi-0.Boston.mci.net [204.70.2.34]
11        * *       *    Reąuest timed out.
12        * *       *    Reąuest timed out.
13        * *       *     Request timed out.
14        * *       *    Request timed out.
```

Jeśli niczego nie zrobimy, to informacja wyświetlana będzie aż do osiągnięcia maksymalnej liczby przeskoków (domyślnie 30). Wyświetlane informacje wskazują, że rutę numer 10 przesłał dalej pakiet do kolejnego rutera lub do miejsca przeznaczenia, ale adres ten nie odpowiada. Może to być spowodowane tym, że urządzenie jest wyłączone lub tym, że nie zna powrotnej trasy do naszego hosta. W obu przypadkach kolejnym krokiem jest przejście do przeskoku 10 i dalsza praca związana z wykrywaniem kolejnych ruterów sieci umieszczonych pomiędzy tym miejscem a miejscem przeznaczenia. Nie daj się jednak wprowadzić w błąd. W związku z funkcjonowaniem asymetrycznego rutowania rutery, które obsługiwały przesyłanie pakietu na drodze od hosta A do B, nie muszą być tymi samymi ruterami, które obsługują pakiet punktu docelowego, a nie z powrotem.

Bardzo możliwe, że przeskok 11 widzi nasz pakiet i wysyła z powrotem odpowiedź przesyłaną zupełnie inną trasą, która nie pokrywa się z żadnym z pierwszych 10 ruterów, przez co pakiet zostaje zgubiony. Także przeskoki 12,13 i kolejne widzą nasze pakiety, ale ich odpowiedzi są gubione, ponieważ trasa powrotna, którą wybiera dla nich ruter 11, jest uszkodzona.

Jedynym sposobem uzyskania pełnego obrazu trasy powrotnej jest wykonanie polecenia *traceroute* z hosta B do hosta A. Niestety, takie działanie nie zawsze jest możliwe. Jednym z potencjalnych sposobów obejścia tego problemu jest użycie pakietów *source-routedw* celu prześledzenia trasy przez sieć. Pakiet IP może zawierać opcję, która wymusza określoną trasę przez sieć prowadzącą przez punkt pośredni aż do miejsca docelowego. Niektóre programy typu *traceroute* pozwalają na określenie takiego żądania wobec trasy. Podając informację o pierwszym punkcie, którym ma być host B, i miejscu docelowym, którym ma być punkt A, można zmusić program do pokazania całej trasy do określonego miejsca i z powrotem. Na przykład, aby zobaczyć, po jakiej ścieżce maszyna noon.nap.net (odległy host) komunikuje się z maszyną laf-gw0. holli. com (ostatni przeskok przed moją maszyną w domu) powinniśmy kazać programowi *traceroute* przejść do miejsca noon.nap.net, zanim pakiety zaczną być wysyłane do laf-gwO. holli.com:

```
tracert -j noon.nap.netlat-gw0.holli.com

Tracing route to lat-gwO.holli.com [204.95.254.1] over a
tnaximum ot 30 hops:

  1    187 ms    146 ms    169  ms    lat-gwO.holli.com [204.95.254.1]
  2    235 ms    154 ms    1745 ms    204.95.255.245
  3    157 ms    155 ms    180  ms    204.95.255.241
  4    167 ms    154 ms    149  ms    204.180.39.42
  5    202 ms    157 ms    153  ms    noon.nap.net [206.54.224.142]
  6    161 ms    163 ms    154  ms    206.54.225.250
  7    169 ms    155 ms    180  ms    204.95.255.241
  8    201 ms    154 ms    154  ms    204.95.255.245
  9    155 ms    155 ms    169  ms    lat-gwO.holli.com [204.95.254.1]

Tracę completę.
```

Nie dziw się, jeśli przeskoki w jednym kierunku nie są dokładnie takie same jak w drugim i różnią się nazwą, a nawet adresem. W obu przypadkach widzisz nazwy urządzeń pobierane z kierunku, z którego nadsyłany jest pakiet. Jeśli adresy lub nazwy są podobne do siebie, to można zakładać, że obie ścieżki są naprawdę symetryczne lub prawie symetryczne.

Sposób, w jaki definiowane jest rutowanie źródła, zależy od implementacji programu. Dlatego powinieneś przejrzeć dokumentację systemu. W przypadku polecenia *traceroute* z systemu Unix często konieczne jest użycie opcji -g. W poleceniu *tracert* z systemów firmy Microsoft żądanie rutowania źródłowego podawane jest za pomocą opcji -j, jak pokazano w przykładzie powyżej.

Jeśli wykorzystujesz rutowanie źródłowe, wskazując miejsca znajdujące się poza siecią, to powinieneś zdawać sobie sprawę z tego, że wielu dostawców Internetu konfiguruje swoje rutery w taki sposób, że odrzucają one pakiety tego typu. Wynika to z chęci zwiększenia poziomu bezpieczeństwa sieci oraz ograniczenia możliwości wykorzystywania pasma dostawcy bez płacenia za to pasmo. W takich przypadkach odpowiedź, jaką uzyskasz, może wyglądać tak:

```
12 !S !S !S cambridge2-cr2.bbnplanet.net [192.233.33.2]
```

Z odpowiedzi tej wynika, że ruter przeskoku 12 odrzucił żądanie wykonania rutowania źródła. Kolejnym problemem, z którym możesz się zetknąć, jest fakt, że niektóre hosty przeznaczenia nie obsługują poprawnie pakietów rutowania źródła. Choć powinno tak być, to niestety, nie wszystkie implementacje protokołów TCP/IP są w pełni zgodne ze standardami. Jeśli zetkniesz się z takim przypadkiem, spróbuj wykonać to samo polecenie, ale jako przeznaczenia użyj adresu rutera pierwszego przeskoku dla adresu docelowego (ostami przeskok przed adresem przeznaczenia), podając go jako adres punktu pośredniego. Nie jest to doskonałe rozwiązanie, ale przynajmniej daje dobre przybliżenie spodziewanej ścieżki.

Pamiętaj, że podstawowym zadaniem ruterów, zarówno tych pracujących w Twojej sieci, jak i tych poza nią, jest przełączanie pakietów, a nie odpowiadanie na Twoje pakiety *traceroute* lub *ping.* Nie oznacza to, że nie powinieneś wykorzystywać tych narzędzi do wykrywania błędów lub monitorowania pracy sieci, ale pamiętaj, aby stosować je niezbyt często. Jeśli narzędzia te używane będą bez żadnych ograniczeń, mogą spowodować, że zwykle mało obciążona sieć znajdzie się na granicy uszkodzenia w związku z dodatkowym ruchem.

Telnet

Często administratorzy sieci nie zauważają tego, że dysponują programem *Telnet,* który jest narzędziem mogącym posłużyć do lokalizowania i usuwania problemów w sieci. Jako narzędzie do monitorowania program ten jest prawdopodobnie zbyt obciążający dla sieci, ale jako narzędzie do usuwania problemów może się okazać bardziej przydatny niż myślisz. Kiedy użytkownik zgłasza problem z dostępem do hosta obsługującego wielu użytkowników, to często Twoim pierwszym działaniem jest wysłanie pakietu *ping* do tego hosta. Jest to dobry pierwszy krok działania, ale jeśli zakończy się on sukcesem, to czy masz pewność, że host ten jest dostępny dla użytkowników?

Używając programu *Telnet* dla nawiązania połączenia z tym hostem możesz jednocześnie sprawdzić działanie znacznie większej liczbie funkcji niż samym poleceniem *ping. Telnet* pracuje ponad protokołem TCP, pozwala więc na dokładniejsze sprawdzenie dostępności niż zapytanie o echo ICMP. Program ten pozwala ponadto przetestować obsługę funkcji wysokiego poziomu na hoście docelowym. Maszyna obsługująca wielu użytkowników może odpowiedzieć na *ping,* ponieważ pakiety te są często obsługiwane na poziomie jądra systemu operacyjnego, ale nadal będzie niedostępna dla użytkowników. Oczywiście możliwe jest również, że maszyna ta zaakceptuje połączenie TCP, wykorzystywane przez *Telnet,* które również często obsługiwane jest przez jądro systemu, ale z powodu jakiegoś problemu nie wyświetli linii pozwalającej na załogowanie się użytkownika.

Narzędzia pomocne przy monitorowaniu i wykrywaniu uszkodzeń

Ponadto większość klientów *Telnet* pozwala Ci łączyć się z portami innymi niż domyślny port usługi *Telnet.* Dwa najbardziej przydatne do wykrywania błędów w sieci porty to usługa *echo,* pracująca na porcie 7, i usługa *daytime,* pracująca na porcie 13. Pierwsza z nich zwraca w postaci echa każdą linię znaków, jaką do niej wyślesz, a druga przesyła aktualny czas i datę hosta przeznaczenia w formacie zrozumiałym dla człowieka. Niestety, te podstawowe usługi TCP wykorzystywane były ostatnio do wykonania ataków typu *denial of seruice.* Musisz więc rozważyć stosowanie tych usług jako narzędzia diagnostycznego, biorąc pod uwagę możliwość wykonania ataku na host przy ich użyciu. Jeśli zdecydujesz się na wyłączenie obsługi tych portów UDP w hostach i ich odpowiedników w ruterach, musisz dodać do konfiguracji następujące polecenia:

```
no service tcp-small-servers no
seryice udp-small-servers
```

Jeśli pozostawisz te usługi aktywne, rozważ możliwość zastosowania filtrowania pakietów, które ograniczy dostęp do tych usług spoza Twojej sieci. Możesz również wykonać połączenie *Telnet* na inne porty UDP obsługiwane na Twoich hostach, aby przetestować działanie innych funkcji. Możliwe jest np. nawiązanie połączenia *Telnet z* portem 25 w celu sprawdzenia, czy serwer poczty elektronicznej odpowiada na żądania połączenia lub nawiązanie połączenia z portem 80 w celu zweryfikowania pracy serwera WWW.

Statystyki zbierane w koncentratorach, przełącznikach i ruterach

Większość pracujących w sieci koncentratorów i przełączników posiada liczniki, które pozwalają określić, jaki ruch (często zarówno w postaci pakietów, jak i oktetów) został odebrany i wysłany przez każdy z portów. Można spotkać również liczniki specyficzne dla danego medium transmisyjnego, które przechowują liczby określające utratę nośnej, utratę pierścienia lub inne błędy. Jeśli nie chcesz używać w sieci stacji zarządzającej, obsługującej SNMP, to informacje te można zbierać przy użyciu programu *Telnet* lub przez połączenie szeregowe RS-232. Dzięki okresowemu zbieraniu statystyk, połączonemu z wyzerowaniem liczników (lub zbieraniu statystyk i jednoczesnym przechowywaniu wcześniejszych wartości), możliwe jest określenie, które z urządzeń pracujących w sieci są najbardziej obciążone i na których łączach występuje największa liczba błędów.

W ruterach często zbierane są te same dane statystyczne co w koncentratorach i przełącznikach, ale oprócz nich zapisywane są również informacje z wyższych warstw, takie jak liczba pakietów i oktetów przesyłanych przez każdy adres w sieci. Dzięki zbieraniu tych dodatkowych informacji można określić, jakimi trasami w sieci przesyłane są dane, a nie tylko skąd one napływają i gdzie są przesyłane.

Netstat

Każda maszyna dołączona do sieci IP przechowuje tablicę rutowania IP. To, czy możliwe jest wyświetlenie zawartości tej tabeli i jak się to robi, zależy od systemu operacyjnego, który uruchomiony jest na tej maszynie. W maszynach z systemem UNIX oraz w wielu stosach protokołów IP, wywodzących się z implementacji UNIX, dostępne jest zwykle polecenie *netstat,* które pozwala na obejrzenie wielu informacji związanych z sieciową warstwą obsługiwaną przez ten system. Najbardziej przydatnymi informacjami są zapisy znajdujące się w tablicy rutowania IP.

Jeśli w sieci pracuje dynamiczny protokół rutowania lub jeśli wykorzystujesz hosty UNIX jako rutery, to dostęp do zawartości tablicy rutowania jest podstawą zrozumienia działania struktury rutowania. Dzięki tym informacjom będziesz mógł zrozumieć, dlaczego maszyny mogą komunikować się ze sobą lub dlaczego niektóre z nich nie mogą połączyć się z jakimś miejscem w sieci. Wyświetlenie zawartości tablicy rutowania możliwe jest przy użyciu polecenia:

```
%netstat -r
Routing tables
Destination      Gateway      Flags    Refcnt      Use      Interface
localhost        localhost    UH       10       10622800     lo0
172.16.2.0       myhost       U        12       5275781      le0
default          myrouter     UG       14       12265327     le0
```

Wynik działania tego polecenia nie jest zbyt czytelny, a jeśli w sieci występują jakieś problemy, to rozwikłanie adresów na nazwy hostów może być bardzo trudne i powolne. W związku z tym tablica rutowania wygląda najlepiej, jeśli nie ma w niej podanych nazw hostów. Aby wyświetlić

```
%netstat -n -r
Routing tables
Destination      Gateway      Flags    Refcnt      Use      Interface
127.0.0.1        127.0.0.1    UH       10       10622800     lo0
172.16.2.0       172.16.2.127 U        12       5275781      le0
default          172.16.2.45  UG       14       12265327     le0
```

W każdym wierszu tego wyniku znajduje się informacja o jednej trasie zapisanej w tablicy rutowania hosta. Będzie tam np. trasa do interfejsu lokalnego (`127.0.0.1`), wskazującego interfejs o nazwie loopback (Lo0), który jest osiągany lokalnie, ponieważ jest to interfejs tego hosta (`127.0.0.1` jest zawsze interfejsem lokalnym dla każdego z hostów). Widzimy również, że host ma bezpośrednie połączenie do pod-sieci `172.16.2.0` przez interfejs *le0*, a także, że adres IP tego hosta to `172.16.2.127`. Ostatni wiersz wyświetlonych informacji oznacza, że nasza domyślna trasa prowadzi również przez interfejs *le0* i przez ruter pod adresem `172.16.2.45`. Gdyby ta maszyna pełniła funkcję rutera IP, to widzielibyśmy również trasy określone dla każdej z dołączonych podsieci, a każda z nich wskazywałaby odpowiedni interfejs maszyny. Aby uzyskać szczegółowe informacje na temat tego, co wyświetlane jest w poszczególnych kolumnach, należy zajrzeć do dokumentacji systemu, ponieważ w różnych systemach pola te będą miały różny układ i zawartość.

Ripquery

Czasami nie jest możliwe dostanie się do maszyny z systemem UNIX lub do rutera, by obejrzeć zawartość jego tablicy rutowania, być może z powodu braku konta na maszynie. Wtedy powinieneś rozważyć możliwość przesyłania zawartości tablic rutowania hostów lub ruterów przez sieć. Operację taką umożliwiają dwa narzędzia: *ripquery* oraz SNMP. Użycie SNMP do pobierania zawartości tablic rutowania i innych informacji zostanie opisane później.

Ripquery jest prostym narzędziem systemu UNIX, które było początkowo dystrybuowane z demonem rutowania o nazwie *gated.* Narzędzie to pracuje tylko wtedy, gdy używasz w sieci dynamicznego protokołu RIP, a uzyskane informacje zależą od implementacji protokołu RIP w danym ruterze lub hoście. Pomimo tych wad jest to bardzo użyteczne narzędzie. Użycie *ripquery* jest bardzo prostą czynnością, wystarczy tylko jako parametr podać nazwę hosta lub rutera, którego tablice rutowania chcemy obejrzeć.

ripquery my router

```
om myrouter (172.16.245.2):
  ???(172.16.103.0), metric 4
  ???(172.16.100.0), metric 4
  ???(172.16.101.0), metric 5
  ???(192.168.1.0),  metric 2
  ???(10.0.0.0),     metric 3
  ???(192.168.40.0), metric 3
  ???(192.168.41.0), metric 3
  ???(192.168.42.0), metric 3
  ???(192.168.43.0), metric 3
  ???(192.168.44.0), metric 3
  ???(192.168.45.0), metric 3
  ???(192.168.46.0), metric 3
  ???(192.168.47.0), metric 3
  ???(192.168.32.0), metric 2
  ???(192.168.33.0), metric 3
  ???(192.168.35.0), metric 3
  ???(192.168.36.0), metric 3
  ???(192.168.37.0), metric 3
  ???(192.168.38.0), metric 3
  ???(192.168.39.0), metric 3
```

Wynik działania polecenia mówi, że urządzenie my router ma trasę prowadzącą do podsieci 172.16.103.0 z miarą 4. Problem z interpretacją tej informacji polega na tym, że nie wiadomo, czy miara 4 jest zapisana w tablicy rutowania (niektóre implementacje odpowiadają w ten sposób), czy też jest to miara, z którą ruter wysyła uaktualnienie RIP przez interfejs, z którego nadeszło nasze zapytanie *ripquery.* Tak dokładne informacje nie zawsze są jednak wymagane. Nie ma także znaczenia fakt, że nie znamy rutera kolejnego przeskoku, ponieważ w otrzymywanych przez *ripquery* danych nie ma takiej informacji. Dzięki temu programowi wiemy natomiast, że urządzenie my r o u t e r ma zapisaną w tablicy trasę do tego miejsca i wiemy o nim więcej!

A propos, trzy znaki zapytania wyświetlane na początku każdego wiersza oznaczają, że maszyna, na której uruchomiono *ripquery,* nie zna nazw sieci, do których ma zapisane trasy. Gdyby maszyna znała nazwy, to *ripquery* wyświetliłby je w tym miejscu.

Oprogramowanie zarządzające przez SNMP

Jeśli w sieci nie działa RIP jako dynamiczny protokół rutowania lub jeśli pracujące w tej sieci hosty oraz rutery nie odpowiadają na zapytania generowane przez program *ripquery* (przynajmniej nie wszystkie), to konieczne jest zastosowanie innej metody uzyskania zawartości tablic rutowania przechowywanych na odległych maszynach. Możliwość taką daje protokół SNMP. *Simple Network Management Protocol (SNMP)* opracowany został po to, by stacje zarządzające ruterami i innymi urządzeniami w sieci mogły być wykorzystywane przy prostej komunikacji typu zapytanie - odpowiedź. Zarządzanie i monitorowanie urządzenia obsługującego protokół SNMP zachodzi wtedy, kiedy oprogramowanie uruchomione na stacji zarządzającej wysyła zapytanie do agenta uruchomionego na zarządzanym urządzeniu. Zapytanie to może zawierać polecenie przesłania określonych informacji o stanie urządzenia lub polecenie zmiany konfiguracji tego urządzenia.

Każde urządzenie SNMP przechowuje bazę danych nazywaną *Management Information Base* (w skrócie MIB), w której zawarte są wszystkie informacje dotyczące tego urządzenia lub wykorzystywane do jego rekonfiguracji. Aby móc monitorować stan urządzenia należy pobierać informacje z jego MIB. Na przykład baza MIB zawiera liczniki oktetów odebranych przez każdy z interfejsów urządzenia. Pobierając wszystkie wartości liczników urządzenia, można uzyskać sumaryczną liczbę oktetów odebranych przez urządzenie od czasu wyzerowania jego liczników, co zwykle oznacza ostatnie przeładowanie systemu lub ostatnie uruchomienie tego urządzenia. Aby móc *zarządzać* pracą urządzenia MIB, użytkownik zapisuje do jego bazy MIB pewne wartości, które mają następnie wpływ na pracę urządzenia. Na przykład adres IP przypisany do portu rutera jest przechowywany w bazie MIB. Określając odpowiednio zapis w bazie MIB dotyczący tej zmiennej możliwa jest zmiana adresu IP odpowiedniego portu rutera.

Oprogramowanie do zarządzania przez SNMP może być bardzo proste i ograniczać się do typowego programu, który potrafi generować zapytania, za pomocą których administrator sieci może pobierać wartości zmiennych. Może to być również zestaw programów pracujących na dedykowanej maszynie i wykonujących automatycznie funkcje monitorowania pracy urządzeń. Jeśli oprogramowanie to stanowi część programu działającego na stacji zarządzającej, to możliwe jest nawet zaplanowanie pewnych zmian w konfiguracji urządzeń, które wykonywane będą w określonym czasie (na przykład w nocy) lub w wyniku wystąpienia określonych warunków w sieci.

Podstawową wadą protokołu SNMP jest to, że informacje przechowywane w bazach MIB wielu urządzeń są zapisane w najprostszej formie i bez możliwości ich kontroli, a zastosowanie RMON nie poprawia wcale tej sytuacji! Niektórzy ludzie myślą, że słowo „prosty" użyte w nazwie *Simple Network Management Protocol* oznacza, że dzięki temu protokołowi łatwo można pozwolić na zasypanie stacji zarządzającej danymi. Jest w tym trochę prawdy, ale trzeba pamiętać, że liczba danych przekazywanych przez SNMP z MIB jest taka sama jak dane dostępne dla użytkownika pracującego z linii poleceń i jakoś nikt z tych użytkowników nie narzeka na zbyt dużą liczbę informacji w tego typu interfejsie.

Najważniejszą sprawą w pracy z SNMP jest zrozumienie, których informacji potrzebujemy i kiedy są one nam potrzebne. Jeśli np. nie używasz w swoim ruterze funkcji obsługi protokołu AppleTalk, to nie warto pobierać i analizować wartości odnoszących się do tego protokołu i powinno się je zignorować. Podobnie należy postępować, gdy nie chcesz monitorować ruchu przechodzącego przez urządzenie, ponieważ liczniki danych nie są nam wtedy potrzebne. Protokół SNMP staje się łatwiejszy w użyciu, gdy dysponujesz stacją zarządzającą, na której jest zainstalowany dobry zestaw aplikacji służących do monitorowania i zarządzania pracą sieci. Aplikacje te mogą być dobrymi narzędziami do przeglądania zawartości sieci i tworzenia jej graficznego obrazu wyświetlanego w postaci mapy topologii sieci. Mapa ta może mieć kilka zdefiniowanych poziomów szczegółów i obsługiwać zmianę koloru reprezentowanych urządzeń w reakcji na nadchodzące alarmy. Programy takie zawierają często wcześniej zdefiniowane procedury umożliwiające tworzenie kompletnych list interfejsów urządzeń pracujących w sieci wraz z ich adresami IP i stanem liczników na tych interfejsach oraz przedstawianie tych informacji w postaci łatwej do zrozumienia tabeli. Takie samo przeanalizowanie sieci wykonane przy użyciu podstawowych programów z obsługą SNMP musiałoby zawierać setki zapytań i odpowiedzi, które musiałyby zostać zinterpretowane i wyświetlone, i z pewnością ich ilość zaskoczyłaby zarówno eksperta, jak i początkującego użytkownika.

Podstawową zaletą stacji zarządzającej, która obsługuje standardowy protokół SNMP, jest to, że potrafi ona komunikować się z urządzeniami różnych producentów, stosując te same interfejsy i polecenia. Nie musisz już więcej pamiętać dziesiątek różnych poleceń, by pobrać z urządzeń pracujących w sieci potrzebne wartości, które w efekcie pozwolą na określenie ścieżki pomiędzy serwerem a hostem i ewentualne wykrycie błędów transmisji.

Pułapki SNMP

Protokół SNMP został opracowany jako system odpytujący. Oprogramowanie zarządzające pracą sieci odpytuje okresowo agentów zainstalowanych w urządzeniach. Choć narzędzie to jest generalnie przydatne w takiej postaci dla celów monitorownia, a jeszcze bardziej odpowiednie dla zadań związanych z zarządzaniem, to trzeba pamiętać, że odpytywanie *urządzeń związane jest z* pewnymi opóźnieniami, które nie powinny mieć miejsca w przypadku wystąpienia niektórych problemów. Aby zrozumieć, dlaczego jest to tak ważne, rozważmy przykład odpytywania rutera o stan jego interfejsów z częstotliwością pięciu minut. Jeśli interfejs ulegnie uszkodzeniu zaraz po tym, jak oprogramowanie zarządzające zapytało ruter o jego stan, to upłynie prawie pięć minut, zanim oprogramowanie to wykryje fakt wystąpienia błędu!

Drugi kłopot związany z takim trybem pracy jest jeszcze poważniejszy. Co się będzie działo, jeśli interfejs rutera zacznie pracować poprawnie przed kolejnym od-pytaniem o jego stan? Możliwe, że nie będziesz nawet wiedział o tym, że interfejs ten uległ uszkodzeniu!

Aby poradzić sobie z takimi przypadkami, standardy SNMP definiują operację określaną jako pułapka, która pozwala urządzeniu wysłać raport do stacji *zarządzającej,* informujący o jakimś określonym zdarzeniu, bez wcześniejszego zapytania skierowanego przez oprogramowanie tej stacji. Używając pułapek, ruter jest w stanie zgłosić fakt wystąpienia uszkodzenia zaraz po jego wykryciu. W zależności od tego, jak zaawansowane jest oprogramowanie SNMP uruchomione na stacji *zarządzającej,* może ono po odebraniu takiej pułapki wysłać do rutera zapytanie o więcej szczegółów dotyczących stanu obecnego, a jednocześnie zgłosić problem administratorowi.

To, jakie pułapki SNMP potrafi wysyłać urządzenie, zależy od typu tego urządzenia oraz od jego producenta. Zwykle pułapki wysyłane są w przypadku uszkodzenia łącza lub portu, naprawy łącza lub portu, a także restartowania maszyny (reboot). Niektóre urządzenia potrafią wysłać odpowiednią pułapkę, kiedy ich temperatura przekroczy dopuszczalną wartość, jeśli spadnie zasilanie, kiedy ktoś źle wprowadzi hasło logowania się lub kiedy wystąpią inne przypadki naruszenia bezpieczeństwa urządzenia.

Posiadając oprogramowanie, które potrafi odbierać te pułapki,* powinieneś je uruchomić i wykorzystywać w swojej sieci. Prawdę powiedziawszy, jedynymi pułapkami, które wyłączyłem ze swojej sieci, są pułapki *link/port up/down* na portach przełączników i koncentratorów Ethernet, dołączone bezpośrednio do stacji roboczych użytkownika. Nie muszę wiedzieć, kiedy użytkownik wyłącza swoją stację roboczą na noc, ale chciałbym wiedzieć, kiedy uszkodzeniu ulegnie łącze pomiędzy koncentratorem a przełącznikiem. Aby uruchomić wysyłanie pułapek, musisz zwykle poinformować system, że chcesz ich używać, i podać adres hosta, na który mają być wysyłane. W ruterze Cisco polecenie to będzie miało postać:

```
snmp-server host 172.16.11.22 public
```

Polecenie to każe ruterowi wysyłać pułapki SNMP na podany adres hosta, wykorzystując zbiorowość `public`, której większość odbiorców pułapek się spodziewa.

*Biblioteki SNMP API, w skład których wchodzi demon obsługujący pułapki, działający na większości systemów UNIX, dostępne są za darmo przez FTP pod *adiesemftp.net.cmu.edu w* katalogu */pub/snmp-dist.* Jest to oprogramowanie, którego używam do odbierania pułapek wysyłanych w mojej sieci. Logowanie tych pułapek jest obsługiwane przez demon *syslog* w moim systemie UNIK. Oprócz demona obsługującego pułapki, który niewątpliwie się przydaje, należy się jeszcze zaopatrzyć w zestaw programów SNMP pracujących w linii poleceń, które można wykorzystywać do ograniczonego zarządzania przez SNMP. Jednym z bardziej przydatnych poleceń jest *snmpnetstat,* które wykorzystuje SNMP do pobierania wiadomości, podobnie jak robi to polecenie *netstat* w systemach UNIX. Warto sprawdzić te programy.

Możliwe jest określenie listy adresatów, z których każdy otrzyma kopię wysłanych komunikatów pułapek. Opcja ta może się przydać, jeśli masz ruter pracujący w odległej sieci i chcesz, aby komunikaty docierały zarówno do centrum zarządzania pracą tamtej sieci, jak i do głównej stacji zarządzającej pracą całej Twojej sieci. Instrukcja `snmp-server` wystarcza dla uaktywnienia obsługi pułapek. Domyślnie uaktywniane są pułapki obsługujące kontrolę stanu łącza i portów, a także pułapka obsługującą procedurę restartowania urządzenia. Aby włączyć obsługę pułapek śledzących błędy autentykacji spowodowane naruszeniem praw dostępu do SNMP należy dodać pole cenie:

```
snmp-server trap-authentication
```

Na zakończenie można (a nawet powinno się) dodać pułapki obsługujące zmiany w konfiguracji oraz problemy zgłaszane *przez* monitor otoczenia, jeśli obsługa tych pułapek jest dostępna. Aby to zrobić należy użyć poleceń:

```
snmp-server enable traps config
snmp-server enable traps envmon
```

Możliwe jest nawet takie skonfigurowanie rutera, aby przesyłał on różne typy pułapek do różnych hostów, które je obsługują. Być może chcesz, aby pułapki związane z monitorowaniem otoczenia były wysyłane do wszystkich demonów obsługujących takie pułapki w sieci, natomiast pułapki związane z konfiguracją urządzeń powinny być wysyłane tylko do Twojej stacji roboczej. Taki sposób rozsyłania pułapek można osiągnąć dodając typ pułapki na końcu instrukcji `snmp-server host`:

```
snmp-server host 172.16.1.1 public erwmon config
snmp-server host 172.16.1.2 public envmon
```

Ponieważ lista pułapek może zmieniać się wraz z tworzeniem nowszych wersji oprogramowania lub znaleźć się w nowym modelu używanego przez Ciebie rutera, powinieneś za każdym razem sprawdzać dokumentację i włączać wszystkie inne dostępne pułapki, które uznasz za przydatne.

System Nazw Domen

Choć nie jest to narzędzie do wykrywania błędów lub monitorowania pracy sieci, należy o tym systemie wspomnieć przy omawianiu funkcji monitorowania pracy sieci i usuwania uszkodzeń. Posiadając kompletną i bezbłędną bazę danych nazw i adresów w sieci, możesz zaoszczędzić całe godziny podczas wykrywania i usuwania uszkodzeń. Taką bazą danych jest właśnie DNS. Powinieneś upewnić się, czy baza ta jest kompletna i bezbłędna.

Jak napisałem w rozdziale I - „Podstawy sieci IP" - DNS jest systemem, który przypisuje nazwy hostów do adresów IP i odwrotnie. Większość ludzi jest w stanie zapamiętać od kilku do kilkudziesięciu adresów IP, a przecież większość administratorów sieci to tylko ludzie.*

Tak, zgadzam się, że wszyscy spotkaliśmy administratorów systemów, których trudno nazwać ludźmi. Niektórych z nich nie zakwalifikowalibyśmy prawdopodobnie nawet do grupy podludzi.

Ponieważ ludzie mają ograniczoną zdolność pracy z adresami *IP,* to oczywiste jest, że maszyny pracujące w sieci z adresami IP mają również przypisywane nazwy. Nazwy te niekoniecznie muszą opisywać funkcje, jakie w sieci pełni dana maszyna, nie muszą też odpowiadać lokalizacji hosta ani nazwisku osoby, która na nim pracuje. Tak naprawdę wymienione sposoby nazewnictwa są często bardzo złym wyborem, ponieważ funkcja, lokalizacja i użytkownik mogą się zmienić wraz ze zmianą maszyny lub przeniesieniem tego hosta w inne miejsce.

Nazwy, które odpowiadają typowi maszyny, są również kiepskim wyborem, zwłaszcza gdy mają być wymieniane w dokumentacji lub powszechnie używane przez pracowników. Jednym z przykładów jest maszyna, która była wykorzystywana jako punkt dystrybucyjny oprogramowania protokołu Kermit. *Przez* prawie dziesięć lat każdy z dokumentów dotyczących tego protokołu odwoływał się do tej maszyny, która nosiła nazwę c u 2 O b, aż wszyscy ludzie zapamiętali ją bardzo dobrze. Problem polegał na tym, że nazwa tej maszyny powstała prawdopodobnie w oparciu o to, że była to druga maszyna typu DEC 2020, zainstalowana na Uniwersytecie Columbia (stąd c u 2 O b). Kiedy maszyna się zestarzała i wymieniona została na nową maszynę z systemem UNIX, nazwa ta przestała mieć takie znaczenie jak poprzednio, ale była tak dobrze znana, że należało ją utrzymać przez kolejne lata do czasu, kiedy uaktualniono nazwy w dokumentacji produktu i zmieniły się przyzwyczajenia użytkowników.

Znacznie lepszym sposobem nazewnictwa jest wybranie grupy nazw, którymi mogą być kolory, kwiaty, drzewa i tak dalej, a następnie nazywanie kolejno uruchamianych w sieci maszyn, opierając się na nazwach pochodzących z tej grupy. Nazwy takie są zupełnie abstrakcyjne i znacznie lepiej się z nimi pracuje niż z samymi adresami IP. Wyjątkiem od tej zasady jest sposób nazewnictwa urządzeń tworzących infrastrukturę sieciową. Są to Twoje koncentratory, przełączniki i rutery, ale nie *zaliczają* się do nich serwery plików, serwery nazw lub serwery wiadomości. Ponieważ ludzie spoza grupy odpowiadającej za pracę sieci nie powinni się odwoływać do tych urządzeń, a nazwy te będą używane tylko w przypadku wystąpienia jakiegoś problemu w sieci, dobrze jest dobrać je tak, aby kojarzyły się jednoznacznie z urządzeniami.

Istnieje wiele sposobów takiego dobrania nazw, aby łatwo było je skojarzyć z danym urządzeniem w sieci. Konieczne będzie stworzenie schematu nazewnictwa obrazującego konfigurację sieci, który będzie pomagał Tobie i Twoim pracownikom identyfikować poszczególne urządzenia. Zamiast więc nadawać urządzeniom nazwy takie jak hubl, hub2, hub3, które nie mówią niczego więcej jak tylko to, że urządzenia te są koncentratorami, zastanów się nad zastosowaniem nazewnictwa takiego jak `math-230-hub-01` lub `cs-b27-hub-01`, które będą informowały, gdzie znajduje się ten koncentrator oraz który to jest koncentrator w znajdującym się zestawie. Pamiętaj o tym, że nazwy te będą użyteczne tylko wtedy, kiedy Twój DNS będzie zawierał aktualne informacje.

Dobrym pomysłem jest również nadawanie unikalnych nazw każdemu interfejsowi rutera. Nazwy te mogą być bardzo szczegółowe lub dość proste, ale zawsze powinny mieć rozpoznawalne znaczenie, dzięki czemu będziesz mógł je zapamiętać. Na przykład jedno z urządzeń może mieć nazwę `chicago-s2-3` w przypadku interfejsu `serial 2/3` w ruterze o nazwie `chicago` oraz nazwę `chicago-fl-0` dla interfejsu `fddi 1/0` na tym samym ruterze.

Po co potrzebne są takie nazwy? Dlaczego nie nazwać wszystkich interfejsów tak samo? Zaletą nazywania każdego interfejsu inaczej jest to, że będziesz mógł wykonać *ping* na określony interfejs, używając jego nazwy, bez konieczności pamiętania jego numeru IP. Może się również okazać, że różne nazwy interfejsów pokazywane w wynikach pracy programu *traceroute* pomogą lepiej określić trasę jaką przesyłane są pakiety pomiędzy dwoma ruterami.

Oprócz nazw interfejsów powinieneś określić również bardziej ogólne nazwy dla każdego z ruterów. Nazwa taka powinna opisywać interfejs lokalny rutera wykorzystywany do zarządzania lub bardzo niezawodny interfejs sieci szkieletowej. Jeśli nazwa będzie przypisana do interfejsu *loopback,* to niewątpliwą jej zaletą będzie fakt, że interfejs ten będzie zawsze dostępny, nawet jeśli poszczególne interfejsy rutera nie pracują, ale wspomniany niezawodny interfejs sieci szkieletowej może być równie dobry. Nazwy takiego interfejsu będziesz używał do pracy z *Telnet,* SNMP, NTP i tak dalej, a także jako adresu źródłowego dla wysyłanych przez ruter komunikatów, takich jak pułapki SNMP. Nazwy pomogą w sortowaniu komunikatów zapisywanych w pliku rejestru i wybraniu tych, które pochodzących z danego rutera.

Jeśli używane przez Ciebie rutery (a nawet koncentratory i przełączniki) mogą pracować jako klienci DNS, powinieneś odpowiednio je skonfigurować. Powiedzmy, że właśnie próbowałeś wykonać *ping* maszyny me r l i n ze swojej stacji roboczej. Wysłany do tej maszyny *ping* działa, ale chciałbyś sprawdzić połączenie z innego punktu sieci. Niestety, najbardziej wygodne miejsca, z których możesz wykonać takie próby, to rutery, które jednak nie zostały skonfigurowane do pracy z DNS. Musisz więc pamiętać adres IP (lub za każdym razem go szukać) maszyny me r l i n. Gdyby pracujące w Twojej sieci rutery były skonfigurowane do pracy z DNS, to sprawa byłaby o wiele prostsza.

Sposób konfiguracji rutera do pracy w charakterze klienta DNS zależy oczywiście od rutera, jaki posiadasz. W przypadku rutera Cisco, polecenia konfiguracyjne są dość proste:

```
ip name-server 172.16.1.5

ip name-server 172.16.203.197

ip name-server 192.168.0.1

!
ip domain-list my-corp.com
ip domain-list your-school.edu
```

Pierwsze trzy instrukcje definiują zestaw serwerów DNS. Ilość tych serwerów zależy od Ciebie, ale należy pamiętać o podaniu więcej niż jednego na wypadek, gdyby pierwszy serwer był nieosiągalny lub w danym momencie wyłączony. Instrukcja i p d o m a i n - 1 i s t definiuje listę domen, dodawanych do nazw, o których rozwikłanie poprosisz ruter. Lista ta może mieć dowolną długość, ale powinieneś pamiętać o tym, że wydłużanie jej spowoduje, iż czas potrzebny na rozwikłanie błędnie podanej nazwy i podanie komunikatu o błędzie rośnie wraz z liczbą pozycji na tej liście. Jeśli masz do czynienia z pojedynczą domeną, to możesz użyć instrukcji ip domain - name.

Jedną z zasadniczych różnic pomiędzy tymi dwoma instrukcjami jest to, że domena w instrukcji ipdomain-name dodawana będzie tylko do nazw, które nie zawierają żadnych kropek. Lista podana za pomocą instrukcji ipdomain-list będzie przeszukiwana dla każdej z podanych nazw, niezależnie od tego, czy zawiera kropki, czy też nie, pod warunkiem, że nazwa ta nie kończy się kropką.

Skonfigurowanie rutera tak, by rozwikływał nazwy hostów za pomocą DNS, może oszczędzić sporo czasu, zwłaszcza w przypadku gorączkowego poszukiwania przyczyn uszkodzenia sieci. Jak jednak powiedziałem w rozdziale I, *nigdy* nie powinieneś polegać na rozwikłaniu nazw przez DNS w samym procesie konfiguracji urządzeń. Jeśli serwer DNS będzie nieosiągalny lub nie będzie udzielał odpowiedzi w czasie, kiedy ruter jest uruchamiany, to taka konfiguracja zostanie wykonana z błędami. Możliwe jest uchronienie się przed częścią takich przypadków poprzez statyczne zdefiniowanie mapowania pomiędzy nazwami hostów a ich adresami IP i umieszczenie tych definicji w konfiguracji rutera jako:

```
host merlin 172.16.105.98
```

Takie mapowanie jest bardzo pracochłonne, biorąc pod uwagę nakład pracy przy początkowym konfigurowaniu oraz podczas dalszego utrzymania i obsługi sieci. Jeśli host merlin kiedykolwiek zmieni adres IP, to oprócz zmian w DNS konieczna będzie rekonfiguracja wszystkich ruterów. Łatwiej jest więc w konfiguracji ruterów używać tylko i wyłącznie adresów IP.

Network Time Protocol (NTP)

Network Time Protocol (NTP) jest kolejnym narzędziem monitorowania i wykrywania uszkodzeń w sieci, o którym często się zapomina. Choć nie jest narzędziem do wykrywania uszkodzeń lub monitorowania, może znacznie poprawić wykorzystanie innych narzędzi. Rozważmy sytuację, kiedy oglądasz zawartość plików, w których rejestrowane są wszystkie zdarzenia na ruterze, i trafiasz na komunikat wskazujący, że o 6:15 rano na ruterze A wystąpił jakiś problem. Taki sam komunikat zauważyłeś również na ruterze B, ale informacja o czasie zapisania komunikatu w pliku wskazuje na godzinę 4:37 po południu. Powstaje pytanie: czy obie informacje dotyczą tego samego problemu, czy też dwóch różnych zdarzeń? Jedynym sposobem, by skojarzyć te dwa komunikaty, jest porównanie wskazań czasu na obu ruterach.

Protokół *Network Time Protocol* pozwala na uzgodnienie czasu pomiędzy urządzeniami pracującymi w sieci. Wykonywane jest to na podstawie okresowo wymienianej informacji o tym, jaka jest różnica czasu urządzenia od uzgodnionego dla sieci, a następnie - na podstawie tej różnicy - dostrojenie zegara urządzenia do czasu sieci. Jeśli jedno z urządzeń w sieci dołączone jest do zewnętrznego źródła czasu, takiego jak zegar radiowy, to czas, na podstawie którego synchronizowane są urządzenia w sieci, jest bardzo zbliżony do rzeczywistego. Używając NTP i dobrego źródła czasu można utrzymywać jednakowy czas w sieci, który tylko o milisekundy będzie różnił się od czasu absolutnego, podawanego przez ogólnoświatowe źródło czasu.

Aby skonfigurować ruter Cisco jako klienta NTP (i jednocześnie jako serwer dla reszty sieci) musisz wykonać następujące polecenia:

```
clock timezone EST -5*
clock summer-time EDT recurring ! ifneeded
ntp update-calendar                ! on a Cisco 7XXX or 4500/4700
ntp source Fddi 1/0                ! always use the same source address
ntp peer 192.168.100.1             ! stratum 1: foo.blech.bar
ntp peer 172.16.234.97             ! stratom 7: twiddle.dee.dum
```

Zawsze staraj się uzyskać pozwolenie na użycie czyjegoś serwera NTP jako źródła czasu dla Twojej sieci. Wiele miejsc w Internecie bardzo chętnie świadczy takie usługi dla reszty maszyn w sieci. Spróbuj wybrać na źródła miejsca zlokalizowane w pobliżu Twojej sieci i pamiętaj, aby wcześniej poprosić o zgodę. Nawet jeśli zewnętrzne źródło czasu rzeczywistego, takie jak zegar radiowy, nie jest dostępne, możliwe jest określenie podstawy czasu NTP w oparciu o czas jednego z hostów. Nie będzie to czas zbyt dokładny, ale przynajmniej identyczny dla wszystkich urządzeń w sieci. Jeśli zegar maszyny będącej źródłem czasu będzie ustawiany na podstawie dość dobrego czasu odniesienia, którym może być nawet Twój własny zegarek, to różnica pomiędzy czasem w sieci a czasem rzeczywistym może wynosić tylko kilka sekund, co w zupełności wystarcza do skorelowania informacji zapisanej w plikach rejestrów z rzeczywistymi wydarzeniami. Kiedy mamy do czynienia z zarządzaniem siecią, to znacznie ważniejszy od dokładnego czasu jest zgodny czas wszystkich urządzeń, które w tej sieci pracują.

Jeśli masz w swojej sieci rutery Cisco 7000 lub 7500, to możesz wykorzystać fakt, że mają one wbudowany bardzo dokładny zegar, przez co stanowią bardzo dobre źródło czasu w przypadku, kiedy zewnętrzne źródła są niedostępne. Aby skonfigurować jeden z takich ruterów (i *tylko* jeden) jako serwer NTP, należy wykonać następujące instrukcje:

```
clock timezone EST -5
clock summer-time EDT recurring    ! ifneeded
clock calendar-valid               ! my clock ts good - use it
ntp master                         ! be the NTP master for the network
ntp source Fddi 1/0                ! always use the same source address
```

Niezależnie od tego, którą z metod wybierzesz, czy zdecydujesz się na użycie czasu lokalnego, jeśli jest dokładny, czy też odległego źródła czasu, pozostałe urządzenia możesz skonfigurować tak, by wykorzystywały ten ruter jako serwer NTP, i bez konieczności stosowania dodatkowego sprzętu możesz uzyskać zgodność czasów poszczególnych urządzeń w sieci.

Oczywiście musisz być pewien, że uaktywnione są opcje zapisujące w pliku rejestru czasy poszczególnych zdarzeń.

*Upewnij się, że zastosowałeś poprawną strefę czasową.

Posiadanie dobrego czasu w sieci w niczym nie pomoże, jeśli funkcje nie będą tego czasu używały. W przypadku rutera Cisco instrukcja uaktywniająca zapis czasów wygląda następująco:

```
service timestamps log datetime localtime
```

Ostatni parametr tej instrukcji powoduje konwersję czasu do postaci czasu lokalnego. Jeśli nie użyjesz tej opcji, to wszystkie czasy zapisywane będą jako *Uniwersal Coordinated Time (UTQ.*

Pliki rejestrów rutera .

Wiele urządzeń pracujących w sieci, a zwłaszcza rutery, wysyła na port konsoli lub port zarządzania komunikaty, jeśli wystąpi jakieś ważne zdarzenie. Komunikaty te zawierają wiele przydatnych informacji na temat działania lub uszkodzeń rutera. Możliwe jest również uaktywnienie komunikatów pomagających w wykrywaniu błędów pracy urządzenia, co pozwoli na uzyskanie dokładniejszych danych potrzebnych działowi wsparcia technicznego, który rozpoznaje występujący w urządzeniu problem. Niestety, jeśli do portu zarządzania rutera nie jest dołączone żadne urządzenie, które odbiera te komunikaty, to są one gubione. Ponieważ nie zawsze dobrze jest mieć dołączone tego typu urządzenia do wszystkich portów konsoli na ruterach (nie wspominając o przełącznikach i koncentratorach), konieczne jest takie skonfigurowanie urządzeń, aby komunikaty te były przechwytywane i aby możliwe było ich odebranie z urządzenia w czasie lub po wystąpieniu uszkodzenia.

System Cisco IOS obsługuje dwa sposoby przechwytywania tych komunikatów w czasie, kiedy nie jesteś zalogowany na ruterze, i dodatkowo jeden sposób przekazywania komunikatów na Twoją konsolę, kiedy jesteś zalogowany do rutera. Pierwszym sposobem jest tworzenie w ruterze bufora rejestru, którego zawartość może być oglądana za pomocą polecenia show log. Użycie tego bufora nie jest domyślnie skonfigurowane, ale łatwo jest go dodać do konfiguracji rutera. Wystarczy tylko wykonać instrukcję:

```
logging buffered
```

Umieść ją w konfiguracji, co spowoduje, że każdy komunikat, który normalnie wysyłany jest na konsolę rutera, będzie teraz umieszczany w buforze. W rzeczywistości komunikaty te nie są nawet wysyłane na konsolę, co pomaga w ograniczeniu niepotrzebnych komunikatów wyświetlanych na konsoli w czasie, kiedy za jej pomocą próbujesz wykryć i usunąć problem, który powoduje ich generowanie.

Wadą stosowania bufora jest to, że jego pojemność jest ograniczona. W tego typu buforze, jeśli konieczne jest zapisanie kolejnych komunikatów i przestają się one mieścić, kasowane są starsze komunikaty. Czas przechowywania komunikatu w buforze zależy od tego, jak długie są te komunikaty oraz jak często nadsyłane są kolejne. Niektóre komunikaty znajdowały się przez całe tygodnie w buforach moich ruterów, podczas gdy na innych ruterach, które częściej generowały komunikaty, ich wymiana następowała nawet co kilka minut. Jeśli masz ruter, który generuje dużą liczbę komunikatów, lub komunikaty te są długie i jest to normalny tryb pracy tego rutera, powinieneś zastanowić się nad powiększeniem rozmiarów bufora rejestru.

Możesz to zrobić, dodając na końcu instrukcji logging buffered parametr określający w bajtach nowy rozmiar bufora. Rozmiar ten może być od 4096 do 4294967295, ale domyślną wartością jest 4096. Pamiętaj, że im więcej pamięci przeznaczasz na obsługę bufora, tym mniej jej pozostaje dla pozostałych ważnych zadań rutera, takich jak przełączanie pakietów.

Niezależnie od tego, jak duży będzie bufor, to prędzej czy później zostanie on wypełniony i możesz utracić informacje, które chciałeś obejrzeć. Alternatywą dla takiego bufora jest wykorzystanie w ruterze funkcji syslog , która będzie wysyłała komunikaty do hosta, na którym uruchomiony jest demon syslog. Większość hostów UNIX i część hostów pracujących z innym systemem operacyjnym, ma wbudowaną obsługę tego właśnie demona. Wykorzystując taką funkcję możesz wykorzystywać bufor rejestru, którego wielkość ograniczona będzie jedynie rozmiarem dysku zamontowanego we wspomnianym hoście. Możliwe jest również użycie narzędzi hosta do *przeglądania* zapisanych w takim rejestrze komunikatów, robienia zestawień, wyszukiwania informacji o nieprawidłowych zdarzeniach i tak dalej. Zaletą takiego rozwiązania jest również możliwość zebrania w jednym miejscu komunikatów pochodzących z kilku ruterów, co pozwoli na łatwe ich porównanie i skojarzenie ze sobą. Aby ruter wykorzystywał funkcję syslog i wysyłał komunikaty do hosta, w konfiguracji tego rutera należy umieścić następującą instrukcję:

```
logging 172.16.1.234
```

Można również powtórzyć instrukcję kilka razy, podając różne nazwy hostów, z których każdy będzie otrzymywał kopię komunikatu. Pomoże to uchronić się przed niebezpieczeństwem utraty komunikatów, spowodowanej tym, że jeden z serwerów będzie niedostępny lub zostanie wyłączony. Pamiętaj, że niezależnie od tego, ile hostów wymienisz w tej konfiguracji, to jeśli wszystkie one będą niedostępne (być może w wyniku uszkodzenia interfejsu, którym ruter dołączony jest do rdzenia sieci), nie będzie możliwe zapisanie żadnego z wysyłanych komunikatów i wszystkie zostaną utracone. Jeśli jednak ostrożnie wybrane zostaną hosty odbierające komunikaty, to liczba tych, które w danym momencie będą niedostępne, może być ograniczona do minimum.

Czasem będziesz preferował rozwiązanie polegające na wysyłaniu komunikatów na terminal w czasie, kiedy jesteś zalogowany do rutera. Być może pracujesz razem z inżynierem technicznym i prosi on o podanie wyników działania niskopoziomowych funkcji analizy błędów. Jeśli siedzisz przy konsoli, to nie ma żadnego problemu; wystarczy tylko zatrzymać pracę bufora i odczytywać komunikaty kierowane na konsolę. Jeśli jednak jesteś połączony z ruterem przez Telnet, chciałbyś, aby komunikaty te przesyłane były na Twoją sesję, dodaj instrukcję:

```
logging monitor debug
```

do konfiguracji rutera, a kopia każdego komunikatu będzie przesyłana na Twoją sesję po napisaniu polecenia terminal monitorów linii poleceń. Należy pamiętać, że wszystkie terminale, które w danym momencie monitorują pracę rutera, będą dostawały kopie tych samych komunikatów; nie ma mechanizmu pozwalającego na wysyłanie części komunikatów do jednej sesji, a pozostałych do innej.

Takie rozwiązanie może być więc problemem, jeśli w tym samym czasie do rutera dołączonych jest kilku administratorów, ale taka sytuacja zdarza się bardzo rzadko.

Jak będziesz interpretował otrzymywane komunikaty? W systemie Cisco IOS wszystkie komunikaty o błędach i zdarzeniach mają następującą formę:

```
%FACILITY-SUBFACILITY-SEVERITY-MNEMONIC: Message-text
```

FACILITY to kod składający się z dwóch lub większej liczby wielkich liter oznaczających urządzenie, do którego odnosi się dany komunikat. Urządzeniem takim może być sprzęt, protokół lub moduł oprogramowania systemu. *SUBFACILITY* odnosi się tylko do wybranych urządzeń oznaczających oprogramowanie i w większości komunikatów ta informacja nie będzie się pojawiała.

SEVERITY to oznaczenie stopnia ważności komunikatu lub tego, jak poważne jest zdarzenie, które wygenerowało ten komunikat. Wartości tego parametru są z przedziału od O do 7, gdzie mniejsza liczba oznacza bardziej krytyczną sytuację. Wartości te wymienione zostały w tabeli 8-2. Komunikaty, które mają wartość 6 (informacje), lub większą, są ignorowane, chyba że jesteś w trakcie wykonywania analizy błędów. Wiele komunikatów o wartości 5 może być również ignorowanych, chyba że tekst komunikatu zawiera informacje, które są ważne. Komunikaty o ważności poniżej 5 (oraz niektóre o wartości 5) powinny zwracać Twoją uwagę. Komunikaty te mogą wskazywać dowolne zdarzenia, począwszy od tego, że przestał pracować interfejs (zwykle ważność 5), aż do występowania błędów pamięci (ważność 3) oraz poważnych błędów w sprzęcie lub oprogramowaniu rutera (ważność 0).

Tabela 8-2. Poziomy ważności komunikatów zapisywanych w rejestrze

Poziom		*Opis*
O	stan zagrożenia	system nie nadaje się do użycia konieczne szybkie
1	alarm	podjęcie działań warunki krytyczne warunki błędu
2	krytyczny	warunki ostrzeżenia warunki normalne, lecz ważne
3	błąd	komunikaty zawierające tylko informacje pojawiają
4	ostrzeżenie	się tylko podczas analizy błędów
5	powiadomienie	
6	informacja	
7	śledzenie błędów	

Na przykład komunikat o następującej treści:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface serial O changed stale to down
```

wskazuje, że interfejs serial O właśnie zmienił stan na nieaktywny. Zwróć uwagę, że komunikat ma poziom ważności 5 (powiadomienie). Choć jest to potencjalnie poważny komunikat w przypadku interfejsu Ethernet, to prawdopodobnie jest on czymś normalnym w przypadku szeregowego interfejsu obsługującego łącze zestawiane na żądanie. Związany z tym komunikatem kolejny odebrany komunikat będzie następujący:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface serial O changed state to up
```

Będzie on informował, że interfejs wrócił do normalnego stanu pracy. Inne komunikaty takie jak:

```
%RSP-2-STALL: partially inserted or removed IPs on cyBusO
```

lub

```
%ALIGN-1-FATAL: Illegal access to low address [hex]
```

wskazują, że wystąpiły poważniejsze problemy. Pierwszy komunikat może być odczytany jako potwierdzenie, że wszystkie karty z procesorami interfejsu zostały umieszczone poprawnie, ale drugi komunikat powinien być dokładnie przepisany lub skopiowany i przekazany do działu wsparcia technicznego. Tak naprawdę komunikat pokazany jako ostatni przykład powinien doprowadzić do szybkiego przeładowania systemu.

Istnieją setki innych komunikatów, które generuje system Cisco IOS. Te, które z nich będziesz oglądał, zależy od modelu rutera, którego używasz, rodzaju zainstalowanych w nim interfejsów oraz - w największym stopniu - od wersji oprogramowania zainstalowanego na ruterze. Wymienienie wszystkich możliwych komunikatów zajęłoby wiele stron i lista ta byłaby nieaktualna po wprowadzeniu na rynek kolejnej wersji IOS. Postaraj się więc dobrze rozumieć komunikaty, które zwykle otrzymujesz, i naucz się rozpoznawać ich wzajemną ważność w oparciu o informacje zapisane w oznaczeniu poziomu ważności. Kiedy będziesz miał wątpliwości, przejrzyj posiadaną dokumentację i zobacz, czy znajdują się w niej jakieś informacje na temat komunikatu, z którego zrozumieniem masz problemy lub na temat innego podobnego komunikatu.

Zarządzanie zmianami

Najlepszym sposobem obsługi problemów występujących w sieci jest zapobieganie ich występowaniu. Problem, którego nie musisz naprawiać, kosztuje znacznie mniej. Większość problemów pojawiających się w pracy sieci wynika z błędów popełnianych przez ludzi; często są to ludzie z działu obsługującego sieć komputerową. Występujące w sieci problemy mogą dotyczyć warstwy fizycznej sieci i wynikać z błędnego wykonania rozłączenia lub mogą być powodem błędów w konfiguracji urządzeń. Na szczęście problemy tego typu najłatwiej jest usuwać.

Rób dobre notatki

Jeśli robienie notatek podczas usuwania problemu pomaga Ci w wybraniu właściwego podejścia do problemu, to pomyśl, jak wiele problemów mógłbyś uniknąć, gdybyś zbierał dokładne informacje o podejmowanych działaniach. Jeśli masz np. aktualną bazę zawierającą opis wszystkich połączeń zrealizowanych w danym punkcie krosowym, to prawdopodobieństwo błędnego rozłączenia jakiegoś połączenia jest o wiele mniejsze.

Jakie informacje należy gromadzić? Po pierwsze powinieneś mieć pełną i dokładną bazę danych wszystkich połączeń fizycznych wykonanych w sieci. Za pomocą zapisanych w taki sposób informacji powinieneś mieć możliwość (bez odwoływania się do innych źródeł i ruszania się ze swojego biura) prześledzenia połączenia zrealizowanego pomiędzy dwiema maszynami w sieci. Zapisy w tej bazie danych powinny być na tyle dokładne, aby definiowały, która para kabli lub światłowodów łączy ze sobą dwa urządzenia, a także wymieniały numery portów na każdym z urządzeń pośredniczących w tej transmisji.

Po drugie, zapisy zmian wykonanych we wszystkich konfiguracjach. W idealnym przypadku zapisy te powinny zawierać informacje o wszystkich dodanych lub zmienionych łączach, a także łączach, które zostały zlikwidowane wraz z czasem i datą przełączenia, informacją o tym, kto tego dokonał, i krótkim opisem powodów wykonania przełączenia. Informacje te dają możliwość przeglądania zmian wykonywanych w okablowaniu sieci i mogą pomóc potwierdzić, czy zamierzone cele zostały osiągnięte.

Czas przechowywania tych wszystkich zapisów zależy od Ciebie, ale im jest on dłuższy, tym lepiej. Kiedyś zdarzyło mi się powiązać pewien rzadko występujący problem w pracy jednego z segmentów sieci Ethernet z faktem, że dwa lata wcześniej odłączyłem go od jednego rutera i dołączyłem do interfejsu drugiego rutera. Doszedłem do tego przeglądając po prostu zapisy zmian konfiguracji tych ruterów. Na szczęście zbieranie takich informacji o zmianach w okablowaniu nie zajmuje zbyt wiele czasu i może być wykonywane prawie automatycznie.

Planowanie i analiza zmian

Zbyt często ludzie obsługujący systemy komputerowe myślą o „planie" jako o słowie, które ma po prostu cztery litery. Uważają, że planowanie to działanie, którego prawdziwy komputerowiec nie musi wykonywać lub że to strata czasu i wysiłku. Niemniej dzięki dokładnej analizie zmiany przed jej ostatecznym zatwierdzeniem można zidentyfikować wiele błędów i -jeśli nie można im zapobiec - przynajmniej zminimalizować ich wpływ na pracę sieci. Ten proces planowania i analizy zmian nie musi być zbyt wyczerpujący, ale powinien być dość dokładny. Nie wolno niczego zakładać z góry i im więcej zmian mamy dokonać, tym dłuższy i dokładniejszy powinien być proces planowania.

Jeśli np. jakiś ważny segment sieci ma być przeniesiony z jednego rutera na drugi w środę rano, to zmiany, jakich trzeba będzie dokonać w konfiguracji, powinny - o ile to możliwe, zostać przygotowane i wprowadzone we wtorek wieczorem.

Także wszystkie kable, które trzeba będzie przełączyć, powinny być wyszukane i wyraźnie oznaczone, a wszyscy ludzie włączeni w procedurę tego przełączenia powinni wiedzieć, jakie są funkcje tych kabli, zanim zaczną pracę w środę rano. Cała operacja przygotowania zmian powinna prawdopodobnie zakończyć się najpóźniej w czwartek wieczorem. Jeśli jednak zamierzasz dokonywać zmian w protokole rutowania lub wymienić jeden z głównych modułów urządzenia, to powinieneś te zmiany przygotować wcześniej i uruchomić wiele testów, które *przez* kilka wcześniejszych dni, a nawet tygodni, powinny potwierdzić poprawność planowanych zmian.

Analiza zmian nie musi być procesem, który będzie obciążał działania Twoje i personelu. Może to być po prostu druga para znających się na rzeczy oczu człowieka, który będzie się przyglądał temu, co i jak robisz. Taka kontrola powinna być wykonana po wcześniejszym zaproponowaniu rozwiązania przez wykonawcę i przedyskutowaniu proponowanych zmian przez obie strony. Innym sposobem jest wykonanie zmian i -po krótkim ich omówieniu - pozostawienie osoby kontrolującej w spokoju, by mogła przejrzeć wykonaną konfigurację. Ponieważ każda z osób prawdopodobnie będzie inaczej oceniała wykonane prace, osoba analizująca Twoje rozwiązanie powinna starać się wskazać jego wady, których nie przewidziałeś lub nie zauważyłeś.

Zanim dokonasz jakichkolwiek zmian, upewnij się, że masz pełną świadomość tego, z jakiego powodu wykonujesz te zmiany. Jeśli nie wiesz do końca, dlaczego te zmiany mają być wykonane, to po prostu ich nie rób! Jest to ważne zwłaszcza w przypadku uaktualnień oprogramowania. Jeśli nie wykonujesz uaktualnienia w związku z chęcią osiągnięcia określonego celu, to po co próbować? Obecnie używane oprogramowanie pracuje przecież zupełnie dobrze.

Konfigurowanie urządzeń odpornych na błędy przy uruchamianiu

Jednym z najniebezpieczniejszych okresów dla Twojej sieci są chwile, kiedy dokonujesz w niej jakichś zmian. Sieć pracująca stabilnie może generować tylko kilka typów uszkodzeń, z którymi trzeba sobie radzić. Ale Twoja sieć nie może ciągle pracować w stanie stabilnym. Będziesz dokonywał w niej zmian, dodając nowe połączenia lub uruchamiając nowe usługi. Jedną ze zmian, która w największym stopniu wpływa na przerwy w pracy sieci, jest uaktualnianie wersji oprogramowania nadzorującego pracę ruterów lub innych urządzeń w sieci. Przemyśl powody, dla których dokonujesz tej zmiany, i upewnij się, że potencjalne zyski są wystarczająco duże, aby uzasadniały podejmowane ryzyko.

Największym ryzykiem związanym ze zmianą oprogramowania rutera (lub innego urządzenia w sieci) na nowszą wersję jest to, że nowe oprogramowanie może spowodować błąd już w momencie uruchamiania urządzenia. Błąd taki może być spowodowany tym, że w ruterze występuje jakiś błąd sprzętowy, którego wpływ na pracę oprogramowania nie został wykryty w trakcie testowania tego oprogramowania. Takie przyczyny występują jednak dość rzadko i łatwo jest ich uniknąć, powstrzymując się przed instalowaniem nowej wersji oprogramowania przez kilka tygodni od momentu, kiedy oprogramowanie się pojawi. Kolejnym poważnym problemem, który może wystąpić jest to, że pomimo bezbłędnego obrazu sprzętu kopia oprogramowania wgrana do rutera zawiera błędy, które sprawiają, że staje się bezużyteczna.

Może się to przejawiać, na przykład, zatrzymaniem procesu uruchamiania urządzenia, a jedynym, sposobem odzyskania nad nim kontroli będzie podłączenie się do portu konsoli. Możliwe, że konieczne będzie usunięcie niektórych komponentów oprogramowania, aby ruter uruchomił się, ładując do pamięci poprawny obraz konfiguracji. Tego typu uszkodzeń trudno jest uniknąć, ale jest kilka sposobów działania, które pozwolą na zachowanie kontroli nad ruterem w czasie jego uruchamiania. Najpierw konieczne jest jednak zrozumienie tego, co dzieje się w czasie procesu uruchamiania rutera i które z podejmowanych wtedy działań mogą zakończyć się niepowodzeniem.

Kiedy ruter jest włączany, wykonywany jest mały program umieszczony w pamięci tylko do odczytu (ROM). Program ten jest bardzo prosty i robi niewiele więcej poza przekazaniem kontroli do mądrzejszego programu po wykonaniu pewnej liczby działań inicjalizujących. Inicjalizacja ta zawiera zwykle podstawowe testy diagnostyczne i wykrycie urządzeń. Testy wykonywane w tym czasie mogą być poszerzone, ale w większości przypadków są one minimum koniecznym do zapewnienia poprawnego przejścia do kolejnego etapu procesu uruchamiania urządzenia, w którym wykonane zostaną pełne testy.

Ten bardziej zaawansowany program, który uruchamiany jest przez podstawowy kod znajdujący się w ROM, może być również umieszczony w pamięci ROM lub na dołączonych urządzeniach typu napęd dyskietek lub pamięć typu flash, a nawet możliwe jest ściąganie go przez sieć. Kod ten zawiera znacznie dokładniejsze procedury testowe i pełniej inicjalizuje sprzęt Może prowadzić do utworzenia ostatecznego obrazu systemu lub może powtórzyć proces, uruchamiając kolejny program znajdujący się na jakimś nośniku i przekazać do niego kontrolę. Proces ten można powtarzać wiele razy, ale większość producentów wykorzystuje maksymalnie trzy lub cztery poziomy ładowania systemu, wliczając w to początkową inicjalizację za pomocą kodu zapisanego w ROM.

Co więc może się nie udać w trakcie wykonywania tych działań? Oczywiście mogą się nie udać niektóre testy diagnostyczne. W takim przypadku niewiele można zrobić i nie ma strategii uruchamiania urządzenia, która pozwalałaby na obejście uszkodzeń wynikających z diagnozowania urządzenia. Nie będę się więc dalej zajmował tym tematem. Jedyne, co możesz zrobić w takim przypadku, to sprawdzenie, czy powodem zatrzymania procesu uruchamiania urządzenia nie jest przypadkiem brak jakiegoś pośredniego programu lub programu zasadniczego, których może w ogóle nie być w wersji oprogramowania, jaką posiadasz, lub mogą one być uszkodzone.

Rzadko się zdarza, aby obraz systemu kopiowany do pamięci rutera (dyskietka lub pamięć typu flash) mógł być uszkodzony i to uszkodzenie nie zostało wykryte. Protokoły sieciowe używane do kopiowania takich plików są jednak podatne na wiele błędów, ale Cisco IOS stara się je wykrywać, uruchamiając liczenie sum kontrolnych odebranego obrazu i zgłaszając wszelkie przypadki wykrycia różnicy. Nigdy nie powinieneś próbować uruchamiać oprogramowania, na które narzeka ruter!

Możliwe jednak,, że przesiany do rutera obraz systemu ulegnie uszkodzeniu w momencie jego zapisu do pamięci nieulotnej. Pamięć typu flash może mieć uszkodzony bit, który tylko czasem ulega zmianie, lub występujący w pracującym systemie błąd może przypadkowo zmienić część informacji zapisywanych do pamięci. Dyskietka może ulec uszkodzeniu w taki sam sposób, może być to błąd nośnika lub błąd wynikający ze złej pracy oprogramowania.

Bardziej prawdopodobnym błędem jest przypadek, kiedy obraz systemu, który ma być załadowany do pamięci operacyjnej rutera, nie jest tam, gdzie spodziewał się go znaleźć ruter. To może być Twój błąd, jeśli na przykład zapomniałeś umieścić na ruterze kopii oprogramowania lub w wyniku błędnego podania nazwy pliku przy jego zapisie na nośniku lub błędnej nazwy podanej w pliku konfiguracji rutera. Niezależnie od tego, jaki jest powód, brak takiego pliku może doprowadzić do całkowitego zawieszenia się systemu - możliwa jest utrata kontroli nad ruterem.

Na szczęście możliwe jest takie skonfigurowanie rutera Cisco, że jeśli nie powiedzie się załadowanie pierwszego obrazu spowodowane uszkodzeniem lub brakiem pliku, to podejmowana jest próba załadowania obrazu zapasowego.* Najlepiej, jeśli ten drugi obraz systemu jest tym, który wcześniej bezbłędnie pracował na tym ruterze. Aby zastosować strategię bezpiecznego uruchamiania rutera konieczne jest dokonanie pewnych zmian w różnych miejscach procesu uaktualniania oprogramowania. Po pierwsze, musisz upewnić się, że dysponujesz bezbłędnie pracującym zapasowym obrazem systemu. Najłatwiej jest go uzyskać po upewnieniu się, że medium, na którym zapisywane są konfiguracje rutera, ma wystarczającą ilość miejsca do jednoczesnego zapisania kilku obrazów systemu. Ponieważ rutery Cisco wykorzystują pamięć typu flash, może to oznaczać konieczność zamówienia i rozszerzenia pamięci tak, aby każdy ruter posiadał jej przynajmniej dwa razy tyle, ile potrzeba do zapisania działającej obecnie konfiguracji. Najlepiej jednak od razu zakupić trzy, a nawet cztery razy więcej pamięci niż jest obecnie wykorzystywane. Dzięki takiemu zapasowi nie będziesz się obawiał wzrostu ilości pamięci wykorzystywanej przez kolejne wersje oprogramowania i będziesz mógł uruchomić funkcje, które wymagają większej ilości pamięci, a jednocześnie nadal będziesz miał możliwość zapisania dwóch działających obrazów systemu. Mając do dyspozycji dodatkową ilość pamięci możesz zapisać nową wersję oprogramowania w pliku, którego nazwa różni się od nazwy działającego obecnie oprogramowania, *co pozwoli na pozostawienie bieżącej wersji oprogramowania w pamięci.* Starsze obrazy systemu można wtedy usunąć. Opisany wyżej proces wykonany dla rutera Cisco 75XX pokazano poniżej. Różne modele ruterów Cisco odwołują się do pamięci wykorzystując różne jej nazwy, sprawdź więc w swojej dokumentacji, jaką nazwę noszą poszczególne urządzenia w Twoim ruterze.

*Możliwe jest nawet takie skonfigurowanie rutera, że będzie on podejmował próbę załadowania trzech, czterech, a nawet większej liczby obrazów, Na niektórych platformach możliwe jest również wykorzystanie obrazu systemu zapisanego w pamięci ROM.

```
router# cd slot0:
router# dir                                              .
-#- -length- -----date/time------ name
l   6732912 May 13 1997 13:56:56 rsp-jv-mz.111-10.bin
9650960 bytes available (6733040 bytes used)
router# copy tftp slot0:rsp-jv-mz.111-12.bin
Enter source file name: code/rsp-jv-mz.111-12.bin
9650832 bytes available on device slot0, proceed? [confirm]
Address or name of remote host [255.255.255.255]? 192.168.12.156
Accessing file "code/rsp- jv-rnz . 111-12. bin" on tnyhost.mycorp.com
. . .FOUND
Loading code/rsp-jv-mz.111-12.bin from 192.168.12.156 (via FDDIO/0):!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 6762468/13523968 bytes]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
router# dir
-#- -length- -----date/time------ name
   1   6732912 May 13 1997 13:56:56 rsp-jv-mz.111-10.bin
   2   6762468 Jul  4 1997 8:01:18 rsp-jv-mz.111-12.bin
2888492 bytes available (13523968 bytes used)
```

Najpierw zmieniłem bieżący katalog na urządzenie pamięci typu flash, które w moim ruterze nosi nazwę slot 0:, i wyświetliłem zawartość, aby upewnić się, czy dysponuję wystarczającą ilością miejsca do zachowania nowego obrazu. Jeśli ilość miejsca nie byłaby wystarczająca, konieczne byłoby usunięcie starszych wersji oprogramowania po to, by mieć więcej dostępnego miejsca. Po zweryfikowaniu, że ilość miejsca jest wystarczająca, kazałem ruterowi użyć TFTP dla skopiowania pliku o nazwie *code/rsp-jv-mz.11-12.bin* z serwera 192.168.12.156 do pliku lokalnego o nazwie *rsp-jv-mz.ll-12.bin* w urządzeniu slot0:. Pamiętaj o tym, że nazwa pamięci typu flash w każdym z ruterów może być inna. Następnie ruter pokazuje, wyświetlając wykrzykniki, że pakiety są odbierane przez ruter, a oznaczenie za pomocą wielkich liter C wskazuje, że wykonywana jest suma kontrolna odebranego pliku w celu zweryfikowania jego integralności. Ponownie wyświetliłem zawartość pamięci i -jak widać - pierwszy z plików to aktualnie uruchomiony obraz systemu, a drugi to obraz, który zamierzam uruchomić. Zanim pokażę, w jaki sposób konfigurować ruter, aby uruchamiał się wykorzystując te pliki w sposób zapobiegający zawieszeniu się urządzenia, pomówmy o tym, co możesz zrobić, jeśli nie masz wystarczającej ilości pamięci, by zapisać w niej dwa obrazy systemu.

Wiele ruterów może uruchamiać oprogramowanie ściągając je przez sieć. Choć nie jest to dobre rozwiązanie dla systemów, które powinny bezawaryjnie pracować, to można je wykorzystać do bezpiecznego uruchamiania systemu operacyjnego rutera. W takim przypadku na serwerze TFTP posiadasz kopię bieżącego obrazu systemu {z ostatniego uaktualnienia) lub powinieneś taką kopię umieścić na tym serwerze.

Aby skopiować obraz systemu z rutera, musisz wykonać te same czynności, co w przypadku kopiowania obrazu z serwera TFTP do pamięci rutera.

```
router# cd slot0:
router# dir
-#- -length- -----date/time------ name
1 6732912 May 13 1997 13:56:56 rsp-jv-mz.111-10.bin

50960 bytes available (6733040 bytes used)
router# copy slotO:rsp-jv-mz.111-10.bin tftp
Enter destination file name: code/rsp-jv-mz.111-10.bin
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Address or name of remote host [ ]? 192.168.12.156
!
```

Tym razem wyświetliłem zawartość pamięci rutera, aby zobaczyć, jak nazwany jest plik, który zamierzam skopiować. Następnie wydałem polecenie copy, każąc ruterowi skopiować plik z *slot0:rsp-jv-mz.111-10.bin* do serwera TFTF pod adresem 192.168.12.156 i nadać mu nazwę *code/rsp-ju-mz.111-10.bin.* Tym razem ruter policzył sumę kontrolną, zanim rozpoczęło się kopiowanie pliku. Taka kolejność działań zapobiega umieszczeniu uszkodzonej kopii obrazu systemu na serwerze TFTP. Jeśli liczenie sumy kontrolnej nie powiedzie się, to konieczne będzie skopiowanie obrazu z innego rutera lub przeprowadzenie dodatkowych testów systemu. Bez względu na to, czy obraz systemu rutera przechowywany w jego pamięci jest dobry, czy nie, konieczne będzie usunięcie go stamtąd, by zrobić miejsce dla nowego obrazu, który będzie skopiowany do pamięci z serwera TFTP. Niezależnie od tego, jaka będzie kolejność Twoich działań i do czego one doprowadzą, pamiętaj o tym, by na serwerze TFTP zostawić kopię poprzedniej wersji obrazu systemu!

W tym miejscu powinieneś mieć już nowy obraz w pamięci rutera, a kopia aktualnie uruchomionego systemu powinna znajdować się w pamięci urządzenia lub na serwerze TFTP. Musisz teraz kazać ruterowi uruchomić się, wykorzystując nowy obraz systemu, i w przypadku wystąpienia problemów przejść na poprzedni obraz systemu. Jeśli obszar pamięci rutera pozwala na przechowywanie obydwu obrazów systemu to wystarczy do konfiguracji rutera dodać następujące linie:

```
boot system flash slotO:rsp-jv-mz.111-12.bin boot
system flash slotO:rsp-jv-mz.111-10.bin
```

Jeśli pamięci rutera nie wystarcza do zapisania obu obrazów systemu, to konieczne będzie załadowanie kopii zapasowej (jeśli będzie ona potrzebna) z serwera TFTP. Aby to zrobić, musisz użyć następujących dwóch linii:

```
boot system flash slot0:rsp-jv-mz.111-12.bin
boot system tftp:code/rsp-jv-mz.111-lO.bin 192.168.12.156
```

Kiedy ponownie uruchomisz ruter, to zgodnie z Twoim planem uruchomiony zostanie pierwszy obraz systemu pod warunkiem, że plik o takiej nazwie zostanie znaleziony w pamięci rutera i w trakcie uruchamiania nie wystąpią jakieś błędy.

Jeśli pierwszy plik nie zostanie znaleziony lub okaże się, że jest on uszkodzony, to ruter podejmie próbę załadowania drugiego obrazu pliku. Obraz ten powinien być bezbłędny, ponieważ jest to ta wersja systemu, która dotychczas była uruchomiona na ruterze, i po to właśnie ją zapisałeś.

Kiedy ruter zostanie uruchomiony powtórnie, musisz sprawdzić, który obraz systemu został w rzeczywistości załadowany do pamięci operacyjnej rutera. Jeśli nowy obraz został poprawnie załadowany, możesz usunąć z pamięci rutera obraz zapasowy i instrukcję `boot system`, ponieważ załadowany właśnie obraz systemu powinien poprawnie działać aż do kolejnego uaktualnienia. Z drugiej strony może zechcesz pozostawić zapasowy obraz systemu, by móc go wykorzystać do konfiguracji tymczasowej sieci w przypadku wystąpienia uszkodzeń wynikających ze złej pracy najnowszej wersji oprogramowania. Choć rzadko się zdarza, aby obraz systemu skopiowany do pamięci typu flash uległ uszkodzeniu, to jednak taki przypadek może wystąpić i wtedy posiadanie konfiguracji zawierającej bezpieczne uruchamianie rutera - w oparciu o dwa obrazy systemu - może zaoszczędzić konieczności chodzenia lub jeżdżenia do tego rutera.

Powinieneś również pamiętać, że wykorzystywanie TFTP jest często traktowane jako naruszenie zasad bezpieczeństwa, ponieważ protokół ten nie wykonuje sprawdzenia autentyczności użytkownika i nie wymaga żadnego hasła przy dostępie do plików umieszczonych na serwerze. Wiele serwerów TFTP zostało zmodyfikowanych tak, by zapewniały pewien poziom bezpieczeństwa i powinieneś zacząć stosować taki serwer lub wykorzystać inne metody ograniczania dostępu do zasobów tego serwera.

Konfiguracja przez sieć a konfiguracja off-line

Wielu administratorów sieci nie dopuszcza do siebie myśli, że metody konfiguracji ruterów przez sieć dostarczone przez producentów urządzeń mogą być nie najlepszym sposobem na przeprowadzanie konfiguracji urządzeń. Zamiast tego chętnie wykorzystują oni dostarczane przez producenta oprogramowanie i wychwalają możliwości, zalety i dostępność narzędzi, które sprawiają, że ich praca staje się łatwiejsza.

Wiele urządzeń pracujących w sieci może kopiować konfigurację z pliku znajdującego się na serwerze *Tnvid File Transfer Protocol* (TFTP), który znajduje się gdzieś w sieci, a część z nich potrafi współpracować z bardziej niezawodnymi (i -jak twierdzą niektórzy - bezpieczniejszymi) usługami protokołu o nazwie *Remote Copy Protocol* (RCP). Choć nie jest to najlepsze rozwiązanie w przypadku ściągania konfiguracji w momencie startu rutera, to możliwość tego typu pracy pozwala na konfigurowanie systemu operacyjnego urządzenia z wykorzystaniem hosta UNIX lub stacji roboczej. Kiedy zmiany w konfiguracji zostaną naniesione, wystarczy tylko skopiować tę poprawioną konfigurację do pamięci urządzenia. Można ją tam umieścić tak, by została użyta przy kolejnym uruchomieniu urządzenia lub wymusić na urządzeniu przeładowanie systemu i natychmiastowe wczytanie tej nowej konfiguracji. W systemie Cisco IOS operacja ta jest dość łatwa i wymaga tylko podania następujących poleceń:

```
routertf copy tftp startup
Address ot remote host [255.255.255.255]? 192.168.12.156
Name of configuration file [router-config]? router/config
Configure using router/config from 192.168.12.156? [confirm]
Loading router/config from 192.168.12.156 (via FDDI0/0): ! ! ! ! ! ! ! !
[OK - 3/344/128975 bytes]

Warning: distilled config is not generated

[OK]
```

Polecenia te kopiują plik konfiguracyjny o nazwie *router/config z* serwera TFTP pod adresem 192.168.12.156 do pliku konfiguracyjnego rutera znajdującego się w bezpiecznym obszarze pamięci RAM. Ostrzeżenie „distilled config is not generated" przypomina o tym, że konfiguracja ta nie została skopiowana do aktualnie pracującej konfiguracji systemu. Stan taki można osiągnąć używając polecenia configure memory, które spowoduje dołączenie tej konfiguracji znajdującej się w obszarze nie ulotnej pamięci RAM do pracującej konfiguracji, która znajduje się w ulotnej pamięci RAM. Zwróć uwagę na to, że jest to dołączenie do konfiguracji już działającej., a nie zamiana uruchomionej konfiguracji. Jest to bardzo ważne,, ponieważ wpływa na sposób, w jaki w pliku konfiguracyjnym umieszczane są polecenia.

Na przykład listy kontroli dostępu (niezależnie od tego, czy stosowane w związku z zabezpieczeniem systemu, wyborem trasy, czy z innych powodów) są wykonywane w kolejności, w jakiej podano instrukcje. Pierwszy zapis takiej listy, który spełnia warunki filtrowania, powoduje zakończenie przeglądania takiej listy. Oznacza to, że nie można po prostu dodać zapisu na końcu listy kontroli dostępu, gdyż warunek ten być może powinien być umieszczony w środku listy. Jeśli więc warunek taki umieścisz w pliku konfiguracyjnym, następnie załadujesz go do systemu, wykorzystując opisaną wyżej procedurę, to nie osiągniesz zamierzonego efektu. Zastanów się nad następującą listą:

```
access-list l permit 172.16.1.0 0.0.0.255
access-list l deny 172.16.0.0 0.0.255.255
```

Jak widać, lista ta zezwala (przepuszcza) wszystkie protokoły adresów z podsieci 172.16.1.0/24, ale zabrania dostępu wszystkim innym adresom z sieci 172.16.0.0/16. Takie warunki odpowiadają wybraniu jednej podsieci w związku z chęcią zachowania bezpieczeństwa. Załóżmy, że taka lista kontroli dostępu przechowywana jest w pliku i zmieniasz ją do następującej postaci:

```
access-list  l  permit 172.16.1.0 0.0.0.255
access-list  l  permit 172.16.27.0 0.0.0.255
access-list  1  deny 172.16.0.0 0.0.255.255
```

Innymi słowy, rozszerzasz zakres listy, pozwalając na przechodzenie przez nią wszystkich pakietów z podsieci 172 .16. 27.0/24. Jeśli jednak skopiujesz ten plik konfiguracyjny do rutera i dołączysz go do uruchomionej konfiguracji, to efekt będzie następujący:

```
access-list 1 permit 172.16.1.0 0.0.0.255
access-list 1 deny 172.16.0.0 0.0.255.255
access-list 1 permit 172.16.27.0 0.0.0.255
```

Druga klauzula opisuje adresy podsieci `172.16.27.0/24`, zabrania im dostępu i kończy przeglądanie listy, zanim sprawdzona będzie klauzula trzecia. Nie jest to chyba działanie, którego się spodziewałeś.

Jak więc poradzić sobie z tym problemem? Są dwa rozwiązania. Pierwsze z nich polega na zmianie numeru listy tak, by utworzyć nową listę, a następnie uaktualnić informację zapisaną w konfiguracji rutera, by wykorzystywana była lista z nowym numerem. Takie działanie można wykonać, jeśli lista jest wykorzystywana tylko w jednym miejscu i nie przeszkadza ciągłe zmienianie numerów list kontroli dostępu. Jednak nie zalecam stosowania takiego rozwiązania. Zmiana wszystkich miejsc, które odwołują się do poprzedniego numeru listy, może powodować powstawanie błędów w konfiguracji i bez wątpienia któregoś dnia pogubisz się w tych numerach. Ponadto - o ile to możliwe - dobrze jest mieć na wszystkich ruterach skonfigurowane listy dostępu, które są wykorzystywane w taki sam sposób, zawierają te same definicje i mają takie same numery. Dzięki temu numery list kontroli dostępu będą miały jakieś znaczenie informacyjne dla Ciebie i Twojego personelu.

Zamiast więc kopiować listy i zmieniać ich numery przed dokonaniem ich edycji, wykorzystuję inny mechanizm konfiguracji list dostępu. Ponieważ ruter dokona połączenia konfiguracji startowej z aktualnie uruchomioną, to dlaczego nie poprzedzić listy, którą zmieniamy, poleceniem, które ją wyczyści? W naszym pliku konfiguracyjnym będziemy więc mieli następujące polecenia:

```
no access-list 1

access-list 1 permit 172.15.1.0 0.0.0.255
access-list 1 permit 172.16.27.0 0.0.0.255
access-list 1 deny 172.16.0.0 0.0.255.255
```

Takie zapisy powodują wyczyszczenie listy numer 1 i ponowne jej odtworzenie w momencie łączenia obu konfiguracji przez ruter. Jedyną wadą takiego sposobu postępowania jest to, że w czasie kiedy ruter wyczyszcza i odbudowuje listę kontroli dostępu mogą się przez jego filtry kontroli bezpieczeństwa przedostawać pakiety lub niechcący może on pobrać jakieś trasy rutowania. W praktyce jednak zdarza się to rzadko. Możesz zredukować szansę, że coś przedostanie się przez ruter, kiedy nie jest on chroniony, usuwając z pliku konfiguracyjnego offline instrukcję `no access-list` po załadowaniu jej do rutera. Kiedy następnym razem będziesz uaktualniał konfigurację rutera, to instrukcji tej nie będzie w jego konfiguracji startowej. Wszystkie inne części konfiguracji rutera mogą być obsługiwane w podobny sposób, ponieważ ich zmiany występują dość rzadko w porównaniu z listami kontroli dostępu.

Wykonywanie innych poleceń umieszczanych w plikach konfiguracyjnych nie musi być uzależnione od kolejności, w jakiej zostały one umieszczone, ale mimo to konieczne będzie ich usunięcie. Na przykład, choć możliwa jest łatwa zmiana adresu JP danego interfejsu za pomocą kolejnej instrukcji `ip address`, umieszczonej w pliku konfiguracyjnym, to aby usunąć adres z interfejsu, który nie będzie więcej używany,

nie wystarczy po prostu pominąć tej instrukcji. Konieczne jest użycie polecenia, które usunie adres z interfejsu. W systemie Cisco IOS robi się to zwykle poprzez umieszczenie przed, poleceniem słówka no. Tak więc aby usunąć adres IP z interfejsu Ethernet, należy zastosować polecenie:

```
interface ethernet O no ip
 address
```

Inne polecenia zachowują się podobnie, a niektóre wymagają bardziej rozszerzonego zaprzeczenia. Choć wyłączenie procesu rutowania RIP możliwe jest poprzez umieszczenie polecenia no router rip w konfiguracji rutera, to jeśli używasz rozszerzonej sekcji konfiguracji RIP, a jest ona umieszczona w uruchomionej aktualnie konfiguracji systemu, to IOS może się zacząć dość dziwnie zachowywać (nie powinien, ale czasem się to zdarza). W takich przypadkach może być konieczne załadowanie pośredniej konfiguracji, która odwoła wszystkie polecenia konfigurujące RIP, zanim wyłączony zostanie sam proces obsługi mtowania RIP. Innymi słowy, może być konieczne załadowanie do pamięci rutera następujących poleceń:

```
router rip
 no network 172.16.0.0
 no redistribute ospf 101
! include other configured RIP commands here no router rip
```

a następnie, po usunięciu w trybie off-line z konfiguracji wszystkich odwołań do procesu rutowania RIP, ponowne załadowanie tak poprawionej konfiguracji. Innym rozwiązaniem może być po prostu przeładowanie rutera i uruchomienie go z czystą kopią konfiguracji startowej, choć takie rozwiązanie nie jest prawdopodobnie najlepsze, kiedy rekonfigurację przeprowadzasz w środku dnia.

Zarządzanie konfiguracją w trybie offline ma wiele zalet:

- Możesz wykorzystywać swój ulubiony edytor tekstu do wykonywania zmian w plikach konfiguracyjnych. Edytor ten ma prawdopodobnie wiele funkcji, których pozbawione są edytory dostarczane przez producenta rutera, a ponadto - ponieważ go dobrze znasz - prawdopodobieństwo popełnienia błędu jest znacznie mniejsze.
- Możesz wykorzystywać wszystkie narzędzia dostępne na platformę Twojego ho-sta. Narzędzia te, to często programy przeszukujące, testery konfiguracji, języki programowania makr, a nawet możliwość wydrukowania konfiguracji w celu jej dokładnego przejrzenia i wykonanie notatek o koniecznych zmianach. Rzadko narzędzia dostarczane *przez* producenta rutera mogą się równać z narzędziami dostępnymi na Twoim hoście.
- Możesz dodawać komentarze do plików konfiguracyjnych. Jak wspomniałem wcześniej, plik konfiguracyjny rutera (lub innego urządzenia) jest specjalnym programem napisanym w języku konfiguracji danego urządzenia. Podobnie jak komentujesz działanie programu umieszczając w jego kodzie różne uwagi, tak samo powinieneś komentować polecenia umieszczane w pliku konfiguracyjnym.

Takie komentarze pozwalają na umieszczenie w pliku informacji własnych, dotyczących spodziewanych zmian, komentarzy odnośnie błędów lub uzasadnienia zastosowanych w danym miejscu poleceń i ich argumentów. Dzięki temu kiedy Ty lub któryś z pracowników będzie oglądał po sześciu miesiącach ten plik, zrozumie *dlaczego* to zostało zrobione w taki a nie inny sposób, a nie tylko *jak* to jest wykonywane.

- Z pewnością będziesz używał na swoim hoście jakiegoś programu służącego do tworzenia kopii zapasowych, dzięki czemu przygotowane konfiguracje będą automatycznie dodawane do kopii zapasowych. Kiedy jakieś urządzenie ulegnie uszkodzeniu lub utraci wszelkie informacje konfiguracyjne, konieczne będzie tylko odtworzenie w rym urządzeniu (lub w nowym, które zostanie umieszczone w miejsce starego) informacji konfiguracyjnych koniecznych do uzyskania połączenia z hostem, na którym przechowywane są konfiguracje offline. Po takim podstawowym skonfigurowaniu urządzenia będzie możliwe załadowanie do jego pamięci pełnego pliku konfiguracyjnego i ponowne uruchomienie urządzenia. Takie podejście do rekonfiguracji sprzętu już nieraz mi pomogło.
- Możliwe jest wykorzystywanie systemu kontrolującego poprawki i zmiany, takiego jak RCS,* pozwalającego na zapisywanie historii zmian plików konfiguracyjnych. System kontroli poprawek jest zestawem narzędzi, które przechowują informacje o wszystkich wykonanych w danym pliku zmianach, informacje te zawierają czas dokonania zmiany, dane o tym, co zostało zmienione, oraz informację o tym, kto wykonał te zmiany; jest to więc zestaw wszystkich informacji, które w takiej sytuacji powinny być zapisane. Większość tego typu programów pozwala ponadto na odtworzenie każdej poprzedniej wersji pliku, dzięki czemu zawsze możesz zobaczyć, jak ten plik wyglądał przed wykonaniem określonych zmian. System kontroli poprawek zapewnia również obsługę prostego mechanizmu zabezpieczeń/ które uniemożliwiają dwóm osobom wykonywanie zmian jednego pliku *w* tym samym czasie. Choć nie jest to system w pełni bezpieczny, powinien on uchronić Cię przed często spotykaną sytuacją, kiedy to dwóch administratorów równocześnie dokonuje różnych niespójnych zmian w tym samym pliku.

Jedyną poważną wadą konfiguracji robionej poza ruterem jest to, że niektóre urządzenia mają zaimplementowaną obsługę specjalnego systemu pomocy oraz system wykrywania na bieżąco błędów konfiguracji urządzenia. Narzędzia te mogą znacznie ułatwić zmiany i pozwalają zabezpieczyć się przed pomyłką w zapisie funkcji, której dobrze nie znamy. Ponadto zaimplementowany system sprawdzania poprawności składni instrukcji sprawia, że wykonywana konfiguracja będzie bezbłędna. Jeśli jednak ostrożnie będziesz wykonywał zmiany w trybie konfiguracji offline oraz wiesz, co chcesz w plikach konfiguracyjnych zapisać, to brak tych dodatkowych narzędzi nie jest wcale dokuczliwy.

*RCS, *Revision Control System,* jest dostępnym bezpłatnie oprogramowaniem pracującym na wielu platformach sprzętowych, takich jak UNIX, VMS, DOS i Macintosh. Program ten można uzyskać poprzez anonimowe FTP pod adresem *prep.ai.niit.ectit.* Aby uzyskać więcej informacji o RCS, zajrzyj do książki „Applying RCS and SCCS" napisanej przez Dona Bouingera oraz Tana Bronsona (wydawnictwo O'Reilly).

Po rozważeniu wszystkich argumentów za i przeciw widać, że zalety konfiguracji off-line przeważają nad tymi kilkoma wadami. Ten tryb konfiguracji może zaoszczędzić Ci wiele godzin, które musiałbyś spędzić na usuwaniu błędów i problemów występujących w konfiguracjach tworzonych, za każdym razem od nowa, w pamięci ruterów.

Konfiguracja umożliwiająca **zarządzanie**

Na zakończenie należy wspomnieć o tym, że powinieneś znaleźć czas, aby skonfigurować swoją sieć w sposób ułatwiający zarządzanie jej pracą. Powinieneś wykorzystać zalety funkcji i poleceń obsługiwanych przez Twoje rutery, przełączniki, koncentratory i stacje robocze, które sprawiają, że urządzenia te stają się partnerami z punktu widzenia procesu zarządzania całym systemem sieci komputerowej. Dotychczas podałem dwa przykłady takiej konfiguracji: konfiguracja rutera do pracy z DNS oraz skonfigurowanie ruterów tak, by mogły wykorzystywać serwery NTP w celu pozyskiwania informacji o czasie i rozpowszechniania do innych urządzeń w sieci.

Innym sposobem konfiguracji uwzględniającej zarządzanie jest użycie instrukcji description. Instrukcja ta pozwala na dołączenie do każdego z interfejsów krótkich opisów, które mogą pomóc w identyfikacji zakładanego przeznaczenia każdego z tych interfejsów. Opis ten wyświetlany jest zawsze, kiedy wyświetlane są informacje o stanie tego interfejsu rutera. Może znaleźć się w nim np. informacja o tym, jakie grupy hostów, budynki lub funkcje dołączone są do tego interfejsu.

Warto jest również wypisać w pliku konfiguracyjnym domyślne opcje konfiguracji interfejsu lub całego urządzenia. Oczywiście nie musisz tego robić. Podawanie tych informacji ma dwa cele. Po pierwsze, domyślne wartości mogą się zmienić w kolejnych wersjach kodu systemu operacyjnego danego urządzenia i możesz nie zwrócić uwagi na te zmiany do czasu, kiedy nie spowodują one problemów w sieci. Po drugie, warto jest wyraźnie wskazać, że takie domyślne wartości są skonfigurowane i że wpływają na pracę urządzenia, zwłaszcza jeśli w innych miejscach sieci te wartości domyślne zostały zmienione na inne, określone przez Ciebie.

Pamiętaj o tym, aby zablokować wszystkie porty i usługi, których nie wykorzystujesz. Pomoże to uniknąć późniejszego zastanawiania się, dlaczego dany interfejs jest wyłączony lub czy dana usługa jest rzeczywiście potrzebna. Taka konfiguracja ograniczy również liczbę potencjalnych konfliktów wynikających z połączenia Twojej sieci z innymi sieciami. Na przykład ruter Cisco zgłasza informację o tym, że interfejs jest *administratively down,* jeśli został wyłączony w procesie konfiguracji, w przeciwieństwie do zgłaszanej informacji *down* w przypadku interfejsu, do którego nic w danej chwili nie jest dołączone. Pierwsza informacja wyraźnie informuje o tym, że administrator zdecydował, iż interfejs ma być wyłączony, a nie że coś uległo uszkodzeniu.

I na zakończenie: jeśli masz możliwość konfigurowania rutera w trybie offline, a język konfiguracji rutera pozwala na umieszczanie komentarzy w pliku konfiguracyjnym, powinieneś z tej możliwości korzystać. Podobnie jak każdy inny program, plik konfiguracyjny rutera może być trudny do zrozumienia po upływie kilku miesięcy od czasu, kiedy go napisałeś. Komentarze umieszczone przy poszczególnych poleceniach i instrukcjach pozwolą Ci przypomnieć sobie, dlaczego zrobiłeś to w taki a nie inny sposób i co chciałeś przez to osiągnąć.

9

Połączenie ze światem zewnętrznym

Planowanie połączeń z innymi sieciami
oraz siecią Internet
Jak dołączyć się do Internetu?
Adresy
Rutowanie zewnętrzne
Łącza stałe czy zestawiane na żądanie?

W poprzednich rozdziałach omówiliśmy tematy związane z projektowaniem, tworzeniem i zarządzaniem siecią w Twojej organizacji. W rozdziale tym skupimy naszą uwagę na świecie zewnętrznym i przedyskutujemy tematy związane z połączeniem naszej sieci z innymi sieciami; czy będzie to połączenie z siecią Internet, czy też z sieciami innych organizacji.

Kiedy większość ludzi zajmujących się zawodowo sieciami myśli o połączeniu się ze światem to pierwszą, jeśli nie jedyną, siecią, którą mają na myśli, jest Internet. Jest to zwłaszcza widoczne obecnie, kiedy Internet stał się częścią kultury masowej: magazyny informacyjne, gazety, reklamy telewizyjne, a także przedstawienia, filmy i książki - wszystkie firmy zajmujące się tego typu działalnością mają w sieci WWW swoje strony. Jest to jednak jeden z rodzajów połączenia naszej sieci ze światem i wbrew pozorom nie jest on najczęściej stosowany. Znacznie częściej stosowane są prywatne połączenia pomiędzy sieciami takimi jak Twoja a sieciami innych organizacji. Połączenia takie powinny być planowane i zestawiane tak ostrożnie, jak robi się to z połączeniami do Internetu.

Niezależnie od rodzaju połączenia zewnętrznego, przy jego tworzeniu i zamówieniu pierwszego łącza należy wykonać kilka analiz dotyczących pewnych wspólnych problemów. Sprawy te zostaną teraz omówiono z punktu widzenia organizacji, która podejmuje pierwszą próbę połączenia swojej sieci z innymi sieciami znajdującymi się poza nią, ale tematy te mają również zastosowanie do organizacji, które mają już połączenia zewnętrzne. Na podstawie zawartych w tym rozdziale uwag zechcesz być może przeanalizować ponownie wszystkie połączenia, które wykorzystujesz, i możliwe, że konieczne stanie się dokonanie kilku zmian w konfiguracji tych połączeń.

Planowanie połączeń z innymi sieciami oraz siecią Internet

Z punktu widzenia koncepcji w połączeniu z siecią Internet a połączeniu z inną organizacją nie ma żadnej różnicy. Zagadnienia związane z tymi łączami są takie same, poza niewielkimi wyjątkami.

Jeśli jakaś organizacja nie jest dołączona do Internetu, to może ona stosować dowolne numery sieci IP dla adresowania urządzeń pracujących w swojej sieci komputerowej. Najlepszym rozwiązaniem jest stosowanie prywatnych adresów sieci IP, które zarezerwowane są w RFC 1918. W najgorszym wypadku dwie organizacje pragnące połączyć swoje sieci, stosują te same numery sieci i konieczne będzie dokonanie analizy tych adresów z punktu widzenia połączenia pomiędzy sieciami lub zastosowanie technologii *Network Address Translation (NAT)* opisanej poniżej. Ponieważ różne połączenia ze światem mają więcej wspólnego niż różnic, potraktuję je tak, jakby były one jednakowe, i w przypadku występowania różnicy zostanie ona pokazana.

Zanim zaczniesz budować połączenie pomiędzy sieciami, powinieneś odpowiedzieć sobie na kilka podstawowych pytań lub uzyskać te odpowiedzi od współpracowników. Upewnij się, czy uzyskane odpowiedzi są pełne i wyjaśniają dokładnie zagadnienie!

- Kto będzie odpowiedzialny za utrzymanie łącza?
- Gdzie kończy się ta odpowiedzialność (tzn. gdzie jest granica pomiędzy strefami wpływów)?
- Jaki rodzaj ruchu sieciowego będzie mógł być przesyłany tym łączem?
- Kto może wysyłać dane przez to łącze? .
- Kiedy dane będą przesyłane tym łączem?

Pierwsze dwa pytania określają dokładny przebieg granicy odpowiedzialności pomiędzy Twoją siecią a siecią, z którą zestawiasz połączenie. Jest to poszerzenie wiedzy o tym, gdzie dokładnie przebiega granica Twojej sieci. Kolejne trzy pytania upewnią Cię, że wszyscy jednakowo rozumieją potrzebę zastosowania tego łącza. Na przykład, jeśli masz połączenie z siecią Internet i zestawiasz właśnie prywatne połączenie z siecią innej organizacji, to trzeba wyraźnie określić, czy organizacja ta będzie miała dostęp do Internetu przez Twoją sieć. Czy Twój dostawca usług internetowych zgodzi się na takie rozwiązanie?

Jeśli tworzysz łącze do sieci Internet, odpowiedzi na powyższe pytania są zawarte w kontrakcie na dostawę usług sieciowych, który podpisujesz. Ty i pracownicy powinniście zrozumieć, jakie są te odpowiedzi, ponieważ zapisy zawarte w tym dokumencie powinny być dokładnie przedyskutowane w czasie negocjowania warunków kontraktu.

Planowanie połączeń z innymi sieciami oraz siecią Internet

Prywatne łącze nie jest zwykle tworzone w oparciu o podpisany pomiędzy stronami kontrakt i prawdopodobnie wcale takiego kontraktu podpisywać nie trzeba. Dlatego jeszcze ważniejsze jest w takim przypadku uzyskanie odpowiedzi na te pytania i pewność, że obydwie strony jednakowo zrozumiały warunki umowy, którą zawierają.

Odpowiedzi na podane wyżej pytania zależą często od stosunków pomiędzy dwiema organizacjami. Stosunki wzajemne można zwykle podzielić na dwie kategorie. Jeśli jedna z organizacji podlega drugiej, to polityka stosowana przy zestawianiu takich połączeń jest określana zwykle przez organizację główną, a podlegające jej inne organizacje muszą po prostu postępować zgodnie z tymi wytycznymi. Jeśli np. zestawiasz połączenie pomiędzy centralą firmy a jej oddziałem, to centrala będzie w tym przypadku określała warunki zestawienia i wykorzystywania tego łącza. W szczególnym przypadku to nowe łącze stanie się częścią sieci WAN całej korporacji, do której dołączone są sieci lokalne znajdujące się w obu lokalizacjach.

Kolejnym rodzajem wzajemnych stosunków jest sytuacja, kiedy obie organizacje są partnerami lub prawie partnerami. Każda z organizacji ma prawo stanowienia o sobie i konieczne jest przedyskutowanie koncepcji połączenia i współpraca przy jego zestawianiu. Niestety, często faza negocjacji jest pomijana lub przykłada się do niej małą wagę, co powoduje, że rezultaty takiego działania są inne od tych, których się spodziewano. Co gorsza, obie strony nie zdają sobie z tego sprawy do czasu wystąpienia pierwszych problemów z pracą łącza i pierwszych nieporozumień. Jak powiedziałem wcześniej, ważne jest, aby obie strony dobrze rozumiały warunki i kształt porozumienia, które jest podstawą do tworzenia połączenia.

Niezależnie od tego, czy łącze jest prywatne, czy też jest to łącze do Internetu, istnieje kilka sposobów określenia, kto jest odpowiedzialny za łącze i gdzie kończy się ta odpowiedzialność, a ilość możliwych kombinacji tych rozwiązań jest chyba nieograniczona. Są jednak dwie kombinacje, które działają dość dobrze i niewiele się między sobą różnią. Pierwsza z nich występuje, kiedy każda z organizacji posiada własny ruter i jedna z nich dostarcza dzierżawione łącze i urządzenia DSU obsługujące obie strony połączenia i bierze na siebie odpowiedzialność za obsługę całego łącza wraz z DSU znajdującym się w drugiej organizacji. Zaletą takiego rozwiązania są jego niskie koszty, zakładając, że każda z organizacji ma port rutera, który może być wykorzystany dla tego łącza. Wadą tego rozwiązania jest to, że organizacja która jest „właścicielem", nie może monitorować ani zarządzać ruterem znajdującym się w drugiej organizacji, co pozwalałoby na szybkie usuwanie lub izolowanie występujących w łączu problemów.

Wady te prowadzą do drugiego rozwiązania, które jest rzadziej stosowane, ale wielu ludzi uważa je za lepsze. W scenariuszu tym jedna z organizacji obsługuje łącze dzierżawione oraz sprzęt DSU, a także ruter znajdujący się w siedzibie drugiej organizacji, i do tego rutera dołącza segment sieci lokalnej. Takie rozwiązanie pozwala organizacji, która zarządza łączem, posługiwać się nim jak w pełni funkcjonalną

podsiecią IP, co pozwala na wysyłanie komunikatów *ping* do urządzeń w drugiej organizacji i wykorzystanie programu *Telnet* do zmiany konfiguracji rutera, który się tam znajduje, bez konieczności dokładnego uzgadniania podejmowanych działań. Wyraźną wadą tego rozwiązania jest oczywiście koszt rutera, ale należy pamiętać, że rutery znacznie ostatnio staniały.

Pytanie, co jest dozwolone na łączu - kto może wysyłać informacje i dokąd - również może mieć wiele odpowiedzi, ale konieczne jest zrozumienie podjętych ustaleń przez obie strony. Na przykład jeśli organizacja A chce zestawić łącze do organizacji B, które będzie obsługiwało przepływ danych pomiędzy tymi dwiema organizacjami i nic poza tym, to organizacja B musi zrozumieć, że łącze to nie będzie obsługiwało ich połączenia z siecią Internet, ani też nie będzie służyło jako łącze zapasowe do tych celów. Podobnie, jeśli łącze ma być używane do przesyłania poufnych danych lub wybranych rodzajów komunikacji, to obydwie strony powinny uzgodnić wymagany poziom zabezpieczeń. Czy łącze ma być szyfrowane? Jeśli tak, to jak silny ma być algorytm szyfrowania? Jeśli nie, to kto może mieć dostęp do tego łącza? Są to trzy rodzaje pytań, na które należy uzyskać odpowiedzi.

Na zakończenie trzeba dodać, że musisz wiedzieć, kto będzie płacił za łącze. Z początku możesz powiedzieć, że płacić powinna strona, która obsługuje łącze i urządzenia, które je tworzą. Ale taka odpowiedź nie zawsze jest właściwa. W mojej sieci znajdują się trzy łącza do regionalnych placówek uniwersyteckich. Każde z tych łączy składa się z dzierżawionego łącza, pary urządzeń DSU i rutera znajdującego się w regionalnej placówce. Wszystkie te urządzenia zarządzane są przez centrum sieciowe uniwersytetu, ale opłacane przez regionalne placówki, które są właścicielem tego sprzętu. Taki układ wynika z tego, że to regionalne placówki chciały mieć dostęp do centrali i do siebie nawzajem poprzez tą centralę. Taki sam rodzaj porozumienia może być podpisany pomiędzy dwiema równorzędnymi organizacjami lub pomiędzy organizacją a dostawcą usług internatowych. Częstym przypadkiem jest porozumienie, w którym organizacja nie mająca doświadczenia w zarządzaniu łączami sieci rozległych woli, aby obsługiwał je ktoś inny, podczas gdy ona pokrywa wszystkie koszty związane z budową i późniejszym zarządzaniem tego typu łączy.

Jak dołączyć się do sieci Internet?

Jedną z największych różnic pomiędzy połączeniem z siecią Internet a łączami prywatnymi jest sposób realizacji tego połączenia. W przypadku prywatnego łącza konieczne jest tylko uzgodnienie z inną organizacją, że łącze takie jest potrzebne, następnie zamówienie sprzętu, wydzierżawienie łącza i wykonanie połączenia. W przypadku sieci Internet sprawy nie zawsze są takie proste, w związku ze zdecentralizowaną strukturą tej sieci i jej prawie anarchiczną budową.

NSP i ISP

Do kogo więc trzeba zwrócić się o pomoc? Od wiosny roku 1995 Internet, przynajmniej w USA, stał się produktem komercyjnym. Do tego momentu większość inwestycji dokonywanych w rdzeniu sieci realizowana była przez wybrane organizacje zapewniające usługi w sieci na podstawie kontraktów rządowych i w oparciu o pieniądze pochodzące od rządu USA. Ostatnią formą jaką przyjęła ta współpraca było powołanie National Science Foundation (NFS), w której uczestniczą organizacje takie jak IBM, MCI i MERIT Networking, i której zadaniem jest obsługa rdzenia sieci znanego pod nazwą NSFNet. To trójstronne porozumienie ewoluowało do czasu, kiedy to powołana została niezależna korporacja, której zadaniem stało się tylko i wyłącznie zarządzanie rdzeniem sieci. Korporacja ta obsługiwała rdzeń sieci NSFNet na podstawie kontraktów rządowych aż do zlikwidowania jej w roku 1995. Opłacanie utrzymania rdzenia sieci NSFNet przez rząd zostało wstrzymane w związku z tym, że NSF chciała obsługiwać również komercyjne organizacje, a nawet oprzeć na nich dalszy rozwój sieci Internet, która miała stać się teraz miejscem bardziej komercyjnym.

Ale NSF nie chciała, aby sieć Internet przestała się rozwijać, i uniemożliwił realizację zaawansowanych połączeń pomiędzy placówkami, które nie pełnią funkcji komercyjnych. Określono więc kilka warunków, jakie należy spełnić, aby móc udostępniać różnego rodzaju usługi w sieci. Ustalono również kilka zasad, które określają minimalny obowiązkowy poziom wzajemnych połączeń pomiędzy różnymi grupami oraz miejsca występowania tych wzajemnych połączeń. Wynikiem tych wszystkich ustaleń jest definicja dwóch rodzajów usługodawców sieciowych, którzy mogą działać na rynku. Najwięksi z nich nazywani są *National Service Providers* lub *Network Service Providers (NSP).* Organizacje określane jako NSP utrzymują duże sieci szkieletowe, które pokrywają teren Stanów Zjednoczonych i często sięgają również do Kanady, a także poza oceany. Klientami tych dostawców są regionalne sieci pracujące na uczelniach, w laboratoriach badawczych lub dużych firmach. Ich klientami są również firmy będące drugim rodzajem usługodawców, które znane są jako *ISP* lub *Internet Service Providers.* ISP to zwykle mniejsi dostawcy usług, którzy obsługują sieci regionalne lub miejskie i którzy przyłączają do swoich sieci mniejsze firmy, szkoły i urzędy publiczne. Aby mieć połączenie z siecią Internet usługodawcy ci muszą kupić usługi od NSP.

Wystarczy już tej historii i informacji podstawowych. Czy powinieneś skontaktować się z ISP, czy też z NSP? Podobnie jak w przypadku wielu pytań w tej książce, odpowiedź zależy od wielu czynników. Jeśli pracujesz w dużej organizacji i chciałbyś, aby Twoje połączenie z Internetem mogło obsługiwać również wymagania innych organizacji, z którymi współpracujesz, to prawdopodobnie powinieneś zwrócić się do NSP. Łącze z NSP będzie realizowane jako dedykowane łącze dzierżawione, ale nie jest to warunek konieczny. Z drugiej strony, jeśli pracujesz w małej firmie lub chcesz zaoszczędzić trochę pieniędzy i samemu obsługiwać swoje połączenie z Internetem, bardziej odpowiednim partnerem do rozmów będzie ISP. Połączenia z ISP będą realizowane za pomocą łączy komutowanych lub linii ISDN, choć wielu z działających obecnie ISP zapewnia również obsługę łączy dzierżawionych.

Wybór pomiędzy NSP a ISP ma bardzo duże znaczenie z punktu widzenia jakości zrealizowanego połączenia. Jeśli generowany przez Twoją sieć ruch będzie dochodził do sieci Internet przez jedno współdzielone łącze wraz z ruchem innych klientów danego ISP, to może się okazać, że parametry transmisji uzyskiwane z takiego połączenia nie są takie, jakich się spodziewałeś. Nie pozostawaj więc przy jednym dostawcy, rozejrzyj się, czy w okolicy nie ma innego, który oferuje być może lepsze usługi. Pamiętaj jednak o tym, że jest wiele prawdy w stwierdzeniu, iż otrzymujesz zawsze to, za co zapłaciłeś!

Powinieneś również przeanalizować usługi, jakie oferuje dostawca usług internetowych. Niektórzy po prostu dołączają do swojego rutera jeden koniec Twojego łącza i spodziewają się, że swoją stronę skonfigurujesz sam, bez ich pomocy. Inne firmy oferują w ramach umowy cały konieczny do zestawienia połączenia sprzęt (na przykład do dołączenia Twojej sieci Ethernet) i przejmują na siebie obowiązek zarządzania tym połączeniem. Niektórzy dostawcy mogą również obsługiwać Twój DNS, a inni pozostawiają ten problem Tobie samemu. *Zdarza* się, że niektórzy dostawcy oferują również usługę ochrony Twojej sieci, obsługę serwisów WWW, możliwość korzystania z bezpłatnych numerów telefonów przez Twoich pracowników, którzy są w danym momencie poza firmą i inne dodatkowe usługi. Każda usługa oznacza zwykle dodatkowy koszt i powinieneś je porównać z kosztem tych usług proponowanych przez innych dostawców, analizując nawet ceny usług, których na razie nie zamierzasz wykorzystywać.

Można stwierdzić, że wybór dostawcy NSP lub ISP niewiele się różni od wyboru dostawcy sprzętu dla Twojej sieci. Nie chcesz na pewno skakać od jednego usługodawcy do drugiego za każdym razem, kiedy oferowane usługi okażą się nie takie, jakich się spodziewałeś. Powinieneś więc dobrze odrobić swoją pracę domową, wykonując dokładną analizę ofert dostawców, co zaoszczędzi Ci kłopotów w przyszłości. Powinieneś również popytać innych użytkowników i administratorów sieci z okolicy i uzyskać od nich opinie na temat dostawców, z którymi współpracują.

Kilku dostawców czy kilka łączy?

Podobnie jak podczas projektowania sieci zastanawiałeś się nad zapewnieniem w niej nadmiarowości, powinieneś to samo zrobić w przypadku połączeń z siecią Internet. Jest to szczególnie ważne, jeśli połączenie z Internetem jest istotne dla interesów Twojej firmy. Są dwa sposoby uzyskania nadmiarowych połączeń z siecią Internet. Jednym z nich jest przyłączenie swojej sieci do kilku różnych usługodawców sieciowych, którzy z kolei dołączeni są do sieci Internet w różnych miejscach. Na przykład jeśli zdecydujesz się na współpracę z dwoma ISP, upewnij się, że nie dzielą oni opłat za wykorzystywanie wspólnego szybkiego łącza od NSP. To wspólne połączenie w znacznym stopniu ograniczy zalety zastosowanego przez Ciebie nadmiarowego połączenia. Drugim rozwiązaniem jest zestawienie kilku łączy jednego dostawcy, który połączony jest z siecią Internet poprzez własne nadmiarowe łącza. Na przykład jeśli wybrany przez Ciebie ISP ma łącze prowadzące do jednego NSP o nazwie A, obsługującego południową część miasta, i drugie łącze do dostawcy NSP B obsługującego północną część, to zestawienie dwóch łączy do takiego ISP będzie prawdopodobnie tańsze, łatwiejsze i tak samo niezawodne jak dwa łącza prowadzące do różnych ISP.

Jako alternatywne rozwiązanie stosowane w przypadku korzystania z usług MSP można rozważyć zestawienie dwóch łączy prowadzących do dwóch odległych punktów przyłączenia do szkieletu sieci NSP.

Które rozwiązanie jest najlepsze? Można by długo na ten temat dyskutować, bez wątpienia jednak posiadanie kilku łączy prowadzących do tego samego usługodawcy ma kilka zalet w stosunku do współpracy z dwoma różnymi dostawcami. Nie musisz się martwić o to, że dostawcy będą się nawzajem obwiniać, kiedy coś przestanie działać. Ponadto z pewnością taniej będzie uzyskać drugie łącze od tego samego dostawcy niż od innego. I na zakończenie wspomnę o tym, że zwykle łatwiej jest skonfigurować poprawnie usługi sieciowe, kiedy rozmawiasz tylko z jednym usługodawcą, który wie, że masz nadmiarowe połączenia z jego siecią.

Adresy

Jeśli Twoja sieć jest odizolowana od świata zewnętrznego, możesz w niej stosować dowolne adresy, jakie sobie wybierzesz. Choć dobrze jest posługiwać się adresami zalecanymi w dokumencie RFC 1918, to nic się złego nie stanie, jeśli nie będziesz postępował zgodnie z tymi zaleceniami. Kiedy jednak dołączasz swoją sieć do innych sieci, posługując się prywatnym łączem do innej organizacji lub publicznym łączem z siecią Internet, to sytuacja ulega zmianie. Adresy IP muszą być unikatowe w skali połączonych ze sobą sieci IP. W jaki sposób spełnisz to wymaganie, zależy od rodzaju połączenia, które zestawiasz.

W przypadku łączy prywatnych pomiędzy dwiema sieciami różnych organizacji, musisz się jedynie upewnić, że sąsiad, z którym się łączysz nie używa takich samych adresów. Taki rodzaj koordynacji jest stosunkowo łatwy, kiedy dotyczy dwóch organizacji, ale może stać się znacznie trudniejszy, w miarę jak dołączane będą kolejne sieci. W przypadku łącza z siecią Internet sprawa wygląda trochę inaczej, ponieważ przydział stosowanych w tej sieci adresów jest koordynowany centralnie, dzięki czemu żaden z tych adresów nie może się powtórzyć w sieci obejmującej cały świat. Adresy takie można uzyskać z jednego lub dwóch źródeł.

Adresy niezależne od dostawcy a adresy przydzielone przez dostawcę usług

Po pierwsze, adresy IP możesz otrzymać z organizacji, która zajmuje się przydzielaniem ich dla Twojego regionu. Organizacje takie działają w Europie i na terenie Azji i Australii, a także na terenie Stanów Zjednoczonych.* Adresy uzyskane bezpośrednio *z* tych organizacji określane są jako adresy niezależne od dostawcy.

*Adresy i numery telefonów tych organizacji znajdują się w dodatku D.

Teoretycznie adresy te mogą być wykorzystywane bez żadnych zmian, niezależnie od tego, z usług którego dostawcy korzystasz w danym momencie. W praktyce jednak zasady przydzielania adresów są takie, że powodują przydzielanie grup adresów, które są zbyt małe, aby mogły być wykorzystywane *przez* większe organizacje i poszczególne części takiej grupy adresów, mogą nie być nitowane przez większych dostawców obsługujących szkielet sieci.
Alternatywą dla adresów niezależnych od dostawcy jest stosowanie adresów przydzielanych przez dostawcę. Adresy te są częścią przestrzeni adresowej, która została przydzielona do dyspozycji Twojego dostawcy usług. Zaletą stosowania takich adresów jest to, że możesz zwykle uzyskać od niego znacznie większą pulę adresów niż pula, którą przydziela organizacja centralna, a ponadto adresy te są obsługiwane przez dostawców na tyle dużych, że ich adresy rutowane są globalnie. Zaletą stosowania takich adresów w sieci Internet jest fakt, że ponieważ pochodzą one z dużych bloków adresów obsługiwanych przez usługodawcę, to łatwiejsze jest ich agregowanie do postaci jednego zapisu w tablicy rutowania. Taka funkcjonalność ogranicza znacznie rozmiary tablicy rutowania w Internecie i jest ważna zwłaszcza teraz, kiedy tablice te są coraz większe.

Niestety, adresy przydzielane przez dostawcę mają również swoje wady. Największa ujawnia się w momencie, kiedy Twoja organizacja postanawia zmienić dotychczasowego dostawcę usług internetowych. W związku z tym, że adresy, które dotychczas stosowałeś, są własnością poprzedniego usługodawcy, to możesz być zmuszony do ponownego przydzielenia i skonfigurowania adresów IP na hostach pracujących w Twojej sieci. Choć protokoły takie jak DHCP i BOOTP mogą ułatwić wykonanie tego zadania, to powinno się raczej unikać przeprowadzania takich zmian w sieci. Jest to więc kolejny argument przemawiający za przemyślanym i właściwym wyborem usługodawcy, którego nie trzeba będzie w przyszłości zmieniać.

I na zakończenie: należy dobrze przemyśleć potrzebę zastosowania adresów, które będą mogły być przenoszone pomiędzy dostawcami i rutowane w szkielecie sieci. Wybór adresów rutowalnych (tzn. adresów przydzielanych przez dostawcę) i implementacja w sieci dynamicznych protokołów obsługujących przydział adresów, takich jak DHCP i BOOTP, sprawia, że sieć może być łatwo adaptowana do zmieniających się warunków.

Skoro konieczność zmiany adresów sprawia, że musisz dużo czasu poświęcić na przemyślenie odpowiedniego rozwiązania, to wspomnę o tym, że w wersji 6 protokołu IP znajduje się zalecenie, aby adresy przydzielane były topologicznie, co jest wyłącznie inną nazwą adresów przydzielanych przez dostawcę usług. W związku z trwającymi pracami nad tą wersją protokołu rozpoczęto omawianie sposobów wspomagania organizacji w procesie przeadresowania ich sieci. Na szczęście prace wykonane dla obsługi IPv6 będą prawdopodobnie mogły być wykorzystane przy adresowaniu w protokole Ipv4.

Tłumaczenie adresów sieciowych

Jednym ze sposobów uniknięcia pracochłonnej zmiany adresów stosowanych w Twojej sieci za każdym razem, kiedy zmieniasz dostawcę usług internetowych, jest użycie wewnątrz własnej sieci prywatnych adresów IP (zgodnie z zaleceniami RFC 1918) i zainstalowanie pomiędzy tą siecią a połączeniem z siecią Internet urządzenia o nazwie *Network Address Translator (NAT).* NAT znajduje się pomiędzy siecią Twojej organizacji a Internetem lub pomiędzy sieciami dwóch organizacji i zajmuje się zamianą adresów prywatnych na unikatowe adresy globalne stosowane na zewnątrz Twojej sieci.

Ideą leżącą u podstaw NAT jest założenie, że tylko kilka hostów z Twojej sieci jednocześnie korzysta z połączenia z siecią Internet, dzięki czemu mogą one współużytkować małą pulę dynamicznie przyznawanych adresów. Kiedy jakiś host z sieci wewnętrznej firmy chce uzyskać dostęp do Internetu, NAT przydziela mu adres pochodzący ze wspomnianej puli. Kiedy host ten wysyła pakiety do Internetu, NAT zamienia umieszczony w nich wewnętrzny adres hosta na adres zewnętrzny. Kiedy pakiet wraca i kierowany jest na ten adres, NAT wykonuje operację odwrotną i zamienia zewnętrzny adres na odpowiedni adres wewnętrzny. Kiedy host kończy transmisję z siecią zewnętrzną, NAT zwalnia stosowany do jej obsługi adres i możliwe jest jego wykorzystanie dla połączenia nawiązywanego przez inny host. Rozwiązanie oparte na NAT nie jest wolne od wad. Największym problemem jest to, że urządzenia te potrafią zamieniać adresy IP umieszczone tylko w nagłówkach IP i innych dobrze znanych miejscach w części pakietu zawierającej dane. Na przykład w protokole FTP jedna maszyna informuje drugą o tym, pod jakim adresem IP i numerem portu oczekuje na nadejście zapytania. Informacja ta powinna być poprawnie obsługiwana przez NAT, gdyż w przeciwnym wypadku przesyłanie plików nie będzie możliwe. NAT potrafi obsługiwać taką zamianę adresów w większości stosowanych obecnie protokołów, ale może nie być w stanie obsłużyć jej w nowych protokołach lub protokołach, które nie są powszechnie stosowane.

Kolejnym problemem występującym przy korzystaniu z NAT jest sposób, w jaki wykrywane jest zakończenie połączenia, co pozwala na zwolnienie przydzielonego dla tego polecenia adresu IP. W przypadku połączeń TCP jest to dość prosta czynność, ponieważ TCP obsługuje dobrze zdefiniowane funkcje nawiązania i zamknięcia połączenia. W przypadku protokołu UDP, który jest protokołem bezpołączeniowym, NAT nie zawsze może z całą pewnością stwierdzić, czy połączenie zostało zakończone. W takich przypadkach można jedynie polegać na tym, że skoro połączenie nie jest aktywne, to prawdopodobnie zostało ono zakończone. Takie założenie nie zawsze jednak jest prawdziwe. Kolejną sprawą są osiągi sieci łączącej się za pośrednictwem NAT. Protokół IP obsługuje sumę kontrolną nagłówka, która zawiera zarówno adres źródła, jak i adres docelowy. Kiedy któryś z tych adresów ulega zmianie, konieczne jest ponowne obliczenie tej sumy kontrolnej, co nie jest oczywiście problemem, gdyż każdy ruter musi uaktualnić tę sumę, kiedy uaktualnia zawartość innych pól w nagłówku IP. Ale trzeba pamiętać jeszcze o tym, że TCP i UDP również stosują sumy kontrolne, które obejmują dane znajdujące się w pakiecie oraz pseudonagłówek, który zawiera adres IP źródła i adres docelowy.

Kiedy następuje zmiana tych adresów, to konieczne jest uaktualnienie również tych sum kontrolnych. Podczas gdy suma kontrolna IP pokrywa zwykle 20 oktetów informacji znajdujących się w nagłówku, to sumy kontrolne TCP i UDP liczone są w oparciu o całą zawartość danych w pakiecie. Ponowne obliczenie takich sum kontrolnych wymaga trochę większej mocy obliczeniowej niż liczenie sum samego nagłówka. Jeśli jednak połączenie obsługiwane przez NAT nie jest szybsze od łącza TI, to osiągnięcie zadowalającej szybkości pracy tego urządzenia nie powinno stanowić problemu. Musisz się jedynie upewnić, czy w związku z zastosowaniem NAT Twoje łącze będzie pracowało z szybkością wymaganą do obsługi wysyłanych z i do sieci danych.

Stosowanie NAT do obsługi połączeń z siecią Internet ma wiele istotnych zalet. Pierwszą z nich jest to, że nie musisz podejmować trudnej decyzji o użyciu w wewnętrznej sieci adresów przydzielonych przez dostawcę, czy też niezależnych od dostawcy. W wewnętrznej sieci możesz stosować adresy prywatne, a w zależności od wybranego dostawcy konieczne będzie tylko skonfigurowanie NAT do korzystania z przydzielonej puli adresów przy obsłudze połączeń wychodzących z sieci. Ponieważ główną wadą korzystania z adresów przydzielanych przez dostawcę jest ewentualna konieczność ich zmiany, to wykorzystanie NAT ogranicza ten problem do konieczności wpisania w konfigurację NAT nowej puli adresów obsługujących łącze z dostawcą. Dzięki takiemu rozwiązaniu możesz zastosować zewnętrzne adresy pochodzące z dużego bloku adresów, które będą na pewno rutowane globalnie. Drugą zaletą jest to, że możliwe jest stosowanie wewnętrznej przestrzeni adresowej o dowolnych rozmiarach. Obecnie większość organizacji będzie miała problemy z uzyskaniem puli adresów pozwalającej na zaadresowanie więcej niż kilkaset lub maksymalnie kilka tysięcy hostów. Używając prywatnych adresów zalecanych przez RFC 1918, możesz łatwo wykorzystywać podsieci pozwalające na adresowanie do kilku milionów hostów! Jest to z pewnością o wiele więcej niż liczba adresów, jakie dostałbyś od organizacji zajmującej się rozdziałem adresów w Internecie lub od swojego dostawcy. Ostatnia zaleta to znaczne zwiększenie poziomu bezpieczeństwa. Ponieważ używane wewnątrz sieci adresy nie są dostępne dla świata zewnętrznego, a host otrzymuje od NAT zewnętrzny adres tylko na czas połączenia, to uzyskanie nieuprawnionego dostępu z zewnątrz do takiej maszyny jest bardzo utrudnione. Z tego punktu widzenia NAT jest w pewnym zakresie ścianą ogniową, broniącą Twojej sieci przed dostępem z zewnątrz.

Technologia NAT jest stosunkowo młoda i być może trudno będzie znaleźć takie urządzenie, które spełni Twoje wymagania odnośnie osiągów, a jednocześnie będzie dostępne za rozsądną cenę. Obecnie dostępnych jest na rynku tylko kilka komercyjnych produktów, ale ich liczba niewątpliwie będzie się zwiększała wraz z rosnącymi trudnościami w uzyskaniu odpowiedniej przestrzeni adresowej. Wiedząc o istnieniu technologii NAT i znając jej możliwości będziesz mógł przygotować swoją organizację tak, by możliwe było z czasem wykorzystanie jej zalet. W rezultacie Twoja sieć będzie bardziej elastyczna i łatwa w adaptacji do zmieniających się warunków.

Adresy przydzielane dla łączy zewnętrznych

Jednym z tematów, nad którym powinieneś się trochę zastanowić, jest to, czy Twoje łącza zewnętrzne powinny mieć przydzielone adresy IP. Wiele ruterów pozwala na obsługę linii punkt-punkt bez konieczności ich adresowania, co pozwala na zaoszczędzenie adresów pochodzących z Twojej puli lub z puli sąsiada. Jest jednak kilka wad takiego rozwiązania, które powinieneś rozważyć, zanim podejmiesz decyzję o stosowaniu go. Po pierwsze, brak adresów odbierze Ci jedyną możliwość zabezpieczenia się przez przypadkową zamianą kabli różnych łączy zewnętrznych, które nie są ponumerowane. Ponieważ urządzenia dołączone do tych łączy nie mają adresów IP przypisanych do interfejsów szeregowych, możliwe jest błędne połączenie dwóch różnych interfejsów do jednego kabla i stworzenie niewłaściwego połączenia pomiędzy ruterami. W zależności od tego, jak skonfigurowane są te rutery, możesz nawet nie zauważyć tego błędu do czasu, kiedy nie wyłączysz jakiegoś połączenia i nie okaże się, że wyłączone zostało zupełnie inne niż chciałeś. Po drugi , łącza, które nie mają przydzielonych numerów, nie pozwolą na sprawdzenie ich za pomocą polecenia *ping,* które jest podstawowym narzędziem służącym do wykrywania uszkodzeń. Choć nadal będziesz miał możliwość wysłania *ping* na inny interfejs danego rutera, to nie będziesz miał pewności, jaką trasą dotarł pakiet potwierdzający, że interfejs ten działa poprawnie. Możliwe, że pakiety generowane przez *ping* były przesyłane w jedną ze stron, a nawet w obie, po trasie zapasowej. Należy także wspomnieć o tym, że łącza nie posiadające adresów mogą powodować problemy w pracy wykorzystywanych w sieci protokołów rutowania. Jeśli producent używanych przez Ciebie ruterów obsługuje nienumerowane łącza, to prawdopodobnie obsługa ta będzie zaimplementowana w protokoły rutowania obsługiwane przez te rutery, choć niekoniecznie. Protokół, który wybierzesz dla swojej sieci, może niezbyt dobrze obsługiwać takie nienumerowane łącza. Ich stosowanie może mocno skomplikować proces konfiguracji protokołu.

Jedyną alternatywą dla nienumerowanych łączy jest dedykowanie kilku podsieci do obsługi takich łączy. Podsieci te powinny mieć taką wielkość, aby można było w nich używać maksymalnie dwóch adresów (taki podział sieci na podsieci omawiałem w rozdziale 3, „Projektowanie sieci - części 2").Tego typu podsieci są dokładnie tym, czego potrzebujesz do obsługi połączeń punkt-punkt wewnątrz sieci lub na zewnątrz. Musisz jeszcze pamiętać o tym, że jeśli nie stosujesz bezklasowych protokołów rutowania IGP, takich jak OSPF lub EIGRP, to konieczne jest ostrożne dobranie podsieci o takich maskach, aby nie powodowały one niejednoznaczności rutowania. Kolejną możliwością jest zastosowanie prywatnych numerów sieci zalecanych w RFC 1918 do obsługi połączeń punkt-punkt. Takie rozwiązanie pracuje dobrze, jeśli możesz zastosować je Ty oraz sąsiedzi i jeśli nie ma potrzeby, aby punkty końcowe tych połączeń dostępne były spoza sieci wewnętrznej. Prawdą jest też stwierdzenie, że zawsze możesz wykorzystać część swojej przestrzeni adresowej i do obsługi zewnętrznych łączy zastosować pełną podsieć adresów. Choć rozwiązanie takie może wydawać się marnotrawstwem, to jeśli zmuszony jesteś do korzystania z klasowego protokołu IGP i nie zdecydowałeś się na wykorzystywanie nienumerowanych interfejsów, będzie to jedyne dostępne rozwiązanie.

Większość organizacji posiada stosunkowo niewiele łączy zewnętrznych, dlatego nie chcą one *przeznaczać* na obsługę tych łączy zbyt dużej liczby adresów z przydzielonej im przestrzeni adresowej.

Rutowanie zewnętrzne

W rozdziale 6 - „Konfiguracja protokołów rutowania" - w którym omawiałem protokoły wewnętrzne (IGP) powiedzieliśmy, że do rutowania pakietów na łączach zewnętrznych stosowane są inne protokoły dynamiczne. Dlaczego występuje różnica pomiędzy protokołami IGP a protokołami rutowania zewnętrznego *Exterior Gateway Protocol* (EGP)? Jednym z powodów jest liczba szczegółów w obsługiwanych przez te protokoły komunikatach. Protokół IGP musi obsługiwać takie szczegóły jak trasy do poszczególnych hostów i podsieci. Szczegóły te są konieczne dla zapewnienia poprawnego rutowania w sieciach IP przydzielanych z klasy. Zwykle jednak każda organizacja ma jedno lub dwa łącza ze światem zewnętrznym, co sprawia, że wspomniane szczegóły mogą zostać zsumowane i usunięte z informacji o rutowaniu, która rozgłaszana jest na łączach zewnętrznych. Wyeliminowanie tych szczegółów pozwala na zmniejszenie wielkości tablic rutowania w sieci Internet. Rutery nie muszą nic wiedzieć o wewnętrznej strukturze każdej z odległych sieci. Dlatego protokoły EGP nie muszą obsługiwać takiej liczby szczegółowych informacji, jaką przesyłają protokoły IGP, posługując się zamiast tego zagregowaną informacją o poszczególnych sieciach. Dzięki skupieniu się na przesyłaniu zagregowanych informacji protokoły EGP skalują się znacznie lepiej i mogą obsługiwać znacznie większe sieci niż protokoły IGP.

Oba rodzaje protokołów zapewniają również inny poziom kontroli przesyłanych pakietów. Większość protokołów IGP opracowana została przy założeniu, że będą obsługiwały one zestawy ufających sobie ruterów, które administrowane są przez jedna grupę ludzi. W modelu tym informacja o rutowaniu przesyłana jest bez żadnych ograniczeń w całej sieci i nie jest zbyt mocno zabezpieczana. Model ten przestaje jednak działać, kiedy zaczynamy mówić o zewnętrznych łączach. W takim przypadku rutery nie są już administrowane przez jedną grupę ludzi i nie można zakładać tak wysokiego poziomu ufności pomiędzy sieciami. Zastosowanie różnych protokołów do obsługi sieci wewnętrznej i do obsługi łączy zewnętrznych pozwala na rozbicie struktury zaufania pomiędzy dwiema różnymi organizacjami. Taka przerwa chroni obie sieci przed wymianą błędnych informacji, które w innym przypadku mogłyby się łatwo rozprzestrzeniać z jednej sieci do drugiej powodując ich uszkodzenie i przerwy w pracy.

Trzecia różnica wynika również z konieczności odseparowania organizacji od siebie. Tym razem jednak powodem nie jest brak zaufania, ale zakres, w którym każda z tych organizacji zmuszona jest koordynować dokonywane w sieci zmiany. Nie chcesz zapewne być zmuszony do kontaktowania się z administratorem sąsiedniej sieci lub jakąś centralną administracją za każdym razem, kiedy zamierzasz dodać jakąś nową sieć, przesunąć segment w inne miejsce lub usunąć go ze swojej wewnętrznej struktury sieci. Dzięki agregowaniu informacji o działających w Twojej organizacji sieciach możesz odizolować inne organizacje od zmian wykonywanych wewnątrz Twojej sieci i obsługiwanych przez wewnętrzny protokół IGP. Tak więc EGP zapewnia Ci autonomię, która pozwala na sprawne zarządzanie pracą własnej sieci.

Wykorzystanie wewnętrznego protokołu rutowania do obsługi zewnętrznych łączy

Wszystko, co zostało napisane wcześniej, nie zmienia faktu, że możliwe jest użycie wewnętrznego protokołu rutowania do obsługi łączy prowadzących do innych sieci. W niektórych przypadkach takie rozwiązanie jest bardzo dobrym pomysłem. Problem polega jedynie na tym, aby wiedzieć, gdzie najlepiej zastosować ten protokół, i zrozumieć, jakie ograniczenia niesie za sobą jego użycie. Złym przykładem zastosowania takiego rozwiązania jest obsługa za pomocą IGP połączenia sieci dużej organizacji z Internetem. Obie sieci powinny być izolowane od siebie za pomocą funkcji, które zapewnia tylko EGP. Natomiast połączenie dwóch mniejszych organizacji lub połączenie małej organizacji z jej centralą nie musi wcale upoważniać do stosowania skomplikowanego rutowania opartego na EGP. W rzeczywistości takie połączenie może być na tyle proste, że można je obsługiwać za pomocą rutowania statycznego. Czasem jednak rutowanie statyczne nie daje wystarczającej elastyczności i nie zawsze może spełnić dodatkowe wymagania stawiane sieci.

Jedną z pierwszych *rzeczy,* jaką należałoby rozważyć, kiedy zastanawiasz się nad użyciem IGP do obsługi połączenia z inną organizacją, jest to, czy powinieneś zastosować ten sam protokół IGP, którego używasz wewnątrz swojej sieci, czy też skorzystać z innego. Zaletą zastosowania innego protokołu IGP niż ten stosowany wewnątrz sieci jest fakt, że dzięki niemu osiągniesz takie samo rozgraniczenie zaufania i zakresu odpowiedzialności, jakie zapewnia protokół EGP. Na przykład, jeśli w swojej sieci stosujesz OSPF, a na łączach zewnętrznych zastosujesz RIP, to masz jasno zdefiniowany punkt kontroli poziomu szczegółowości informacji i poziomu zaufania pomiędzy Twoją siecią wewnętrzną a łączem zewnętrznym. Punktem tym jest miejsce, w którym dokonujesz redystrybucji informacji pomiędzy protokołem OSPF a RIP. Wadą stosowania innego protokołu do obsługi łącza zewnętrznego jest to, że rozwiązanie takie może być równie skomplikowane jak użycie protokołu EGP. Nadal musisz uruchomić dwa protokoły rutowania, z których każdy musisz znać, a ponadto istnieje konieczność kontrolowania wymienianych między nimi informacji. Rozszerzenie stosowanego w sieci protokołu OSPF na obsługę łącza zewnętrznego byłoby o wiele prostsze. Oczywiście, jeśli sąsiad stosuje w sieci inny protokół IGP, to z tych samych powodów on też może chcieć, abyście do obsługi tego łącza użyli jego protokołu. Któryś z Was będzie musiał w takiej sytuacji ustąpić.

Niezależnie od tego, jaki protokół IGP wybierzesz do obsługi łącza zewnętrznego, musisz zdawać sobie sprawę z ograniczeń związanych z takim rozwiązaniem. Na przykład protokół RIP ogranicza *średnicę* sieci - odległość pomiędzy dwoma najbardziej oddalonymi od siebie ruterami - do maksymalnie 15 przeskoków, ponieważ wartość 16 stosowana jest w tym protokole dla określenia nieskończoności i oznacza miejsce, które nie jest osiągalne w sieci. Jeśli Twoja sieć ma średnicę równą 10, a sieć sąsiada ma średnicę 11, to zastosowanie protokołu RIP do obsługi łącza pomiędzy waszymi sieciami sprawi, że nie będzie ono zbyt dobrze pracowało, ponieważ sumaryczna średnica powstałej po takim połączeniu sieci wynosi 21 przeskoków!

Choć można sobie poradzić z tym problemem poprzez zastosowanie rekonstrukcji miar (przełączanie miary z powrotem na małą wartość w momencie, kiedy pakiet przekracza granicę sieci), to rozwiązanie może sprawić, że konfiguracja sieci będzie bardziej skomplikowana i mogą występować problemy. Bez wątpienia znacznie lepiej w takim wypadku zadziała rozwiązanie wykorzystujące inny protokół IGP.

Jeśli zdecydujesz się na stosowanie tego samego protokołu IGP do obsługi łączy wewnętrznych i zewnętrznych, to rzadko będziesz musiał martwić się o jakieś specjalne rozwiązania konfiguracyjne dla tej sieci. Powinieneś jednak zadbać o to, aby dość dokładnie skonfigurować stosowany w sieci IGP, by uniknąć przenikania problemów występujących w sieci sąsiada do Twojej sieci. Jako rozwiązanie minimalne powinieneś zastosować konfigurację, która nie pozwoli na wymianę informacji o trasach wewnętrznych pomiędzy obiema połączonymi sieciami. A najlepiej, jeśli będziesz akceptował tylko informacje dotyczące tras, które Ty sam określisz jako interesujące. Zastanówmy się nad konfiguracją pokazaną poniżej. Zastosowałem protokół RIP jako IGP, a także ten sam protokół do obsługi łącza z sąsiednią siecią. Bardzo szczegółowo zdefiniowałem listę tras, o których informacji spodziewam się od sąsiada pod adresem 192.168.100.0/24 (spodziewam się, że będę otrzymywał informacje o trasach do podsieci 10 .0 .0.0/8 i 192.168.101.0/255), i nie będę akceptował żadnych innych informacji nadsyłanych z tej sieci. Jednocześnie mój ruter będzie miał dostęp do wszystkich informacji, które będą do niego przesyłane z innych ruterów pracujących w mojej sieci wewnętrznej.

```
router rip
  network 172.16.0.0
  network 172.17.0.0
  network 192.168.100.0
  distance 255
  distance 120 172.16.1.0 0.0.0.255
  distance 120 172.16.2.0 0.0.0.255
  distance 120 192.168.100.0 0.0.0.255 21
!
! define the networks I expect my neighbor to send to me
access-list 21 permit 10.0.0.0          0.255.255.255
access-list 21 permit 192.168.101.0     0.0.0.255
access-list 21 deny 0.0.0.0             255.255.255.255
```

Nie ograniczyłem w żaden sposób informacji, które wysyłam do mojego sąsiada. Choć oczywiście mogłem to *zrobić,* to mogę się spodziewać, że administrator tej sieci również skonfiguruje swój ruter w taki sposób, aby odrzucał on informacje, które nie powinny przenikać do jego sieci wewnętrznej. Może to być jedyne dobre rozwiązanie, jeśli inni sąsiedzi również wykorzystają sieć 192.168.100.0/24.W związku w wysyłanymi przez RIP komunikatami zawierającymi uaktualnienia nie jest możliwe rozgłaszanie do różnych sąsiadujących ze mną sieci różnych informacji. Muszą oni po prostu odfiltrować sobie to, czego nie chcą słyszeć.

Rutowanie zewnętrzne

Jeśli do obsługi zewnętrznych łączy wybierzesz inny protokół IGP, konieczna będzie prawdopodobnie redystrybucja informacji o rutowaniu z jednego protokołu IGP do drugiego, a także obsługa tej samej funkcji w odwrotnym kierunku. Podobnie jak w poprzednim przykładzie, najlepiej jest akceptować tylko te trasy, o których spodziewasz się słyszeć od sąsiada. Poniżej przedstawiono przykład takiej konfiguracji. Tym razem wewnątrz sieci używam protokołu EIGRP, a mój sąsiad poprosił mnie, abym użył protokołu RIP do obsługi zewnętrznego łącza, ponieważ jego rutery nie potrafią rozmawiać językiem EIGRP. Moim pierwszym zadaniem jest skonfigurowanie połączenia pomiędzy procesem obsługującym protokół EIGRP a procesem RIP, dzięki czemu będę mógł przekazywać sąsiadowi informacje o moich sieciach. Ponadto muszę nawiązać połączenie pomiędzy RIP a EIGRP, aby do moich pozostałych ruterów docierały informacje o sieciach sąsiada. Zdefiniuję również domyślną miarę kosztu dla każdego ze stosowanych przeze mnie protokołów rutowania. Ponieważ nie stosuję protokołu RIP wewnątrz mojej sieci, lecz tylko jako pseudo-EGP do łączności z sąsiadem, to łatwiej jest zastosować te domyślne wartości niż wybierać właściwą miarę dla każdego z ruterów. Zakładam przy tym, że mój sąsiad słyszy informacje o moich sieciach tylko z mojej sieci, a ja słyszę informacje o jego sieciach tylko z jego sieci.

```
router eigrp 71
 network 172.16.0.0
 network 172.17.0.0
 redistribute rip
default-metric 10000 250 100 1 1500
!
router rip
 network 192.168.100.0
 redistribute eigrp 71
 default-metric 1
 ! use access list 21 to restrict what myneighbor tells me
 distribute-list 21 in
 ! use access list 22 to restrict what I ten myneighbor
distribute-list 22 out eigrp 71
!
! define the routes I will accept frommyneighbor
access-list 21 permit 10.0.0.0          0.255.255.255
access-list 21 permit 192.168.101.0 0.0.0.255
access-list 21 deny 0.0.0.0          255.255.255.255
!
! invert access list 21 so that I tell my neighbor about everything
! except his routes (avoid feedback loops)
access-list 22 deny 10.0.0.0          0.255.255.255
access-list 22 deny 192.168.101.0     0.0.0.255
access-list 22 permit 0.0.0.0         255.255.255.255
```

Jeśli poprzestanę na zwykłym redystrybuowaniu tras protokołu RIP do mojego EIGRP i takiej samej funkcji wykonywanej w drugą stronę, to będę miał dwa problemy. Pierwszy z nich to ryzyko, że sąsiad nic mi nie będzie przesyłał, w co uwierzy mój ruter i przekaże tę informację do całej mojej sieci.

Drugi problem to sytuacja polegająca na redystrybuowaniu moich tras z protokołu EIGRP do RIP, które następnie będą do mnie wracały jako redystrybuowane z RIP z powrotem do EGRP. Powinno się zapobiegać powstawaniu tego rodzaju pętli zwrotnej. W naszym przykładzie rozwiązałem obydwa wspomniane problemy poprzez zastosowanie list dostępu. Lista dostępu numer 21 filtruje nadsyłane od sąsiada uaktualnienia RIP, przepuszczając tylko te, które zawierają informacje o jego dwóch sieciach. Skonfigurowałem również mój proces RIP tak, aby filtrował moje trasy rozgłaszane przez EIGRP przy użyciu listy dostępu numer 22, która jest po prostu odwrotnością listy 21. Filtrowanie wychodzących tras upewnia mnie, że wśród wysyłanych informacji nie ma informacji o trasach mojego sąsiada, co zabezpiecza pętlę sprzężenia zwrotnego. Mógłbym też wymienić informacje, które mają być rozgłaszane do sąsiada i umieścić tę definicję w liście dostępu 22. To, które rozwiązanie wybierzesz w swojej sieci, powinno zależeć od tego, którą konfigurację łatwiej Ci będzie uaktualniać.

Protokoły rutowania zewnętrznego

Protokoły EGP pozwalają na tworzenie punktów rozgraniczenia pomiędzy informacjami przenoszonymi przez protokoły IGP stosowane w sieciach łączących się ze sobą organizacji. Obsługują one również funkcję sumaryzacji informacji o wewnętrznych sieciach, dzięki czemu szczegóły ich dotyczące mogą być niewidoczne dla innych organizacji. Niestety, protokoły te są zwykle bardziej skomplikowane niż protokoły IGP, głównie z powodu wielkości sieci, jakie powinny być w stanie obsługiwać. Podczas gdy typowy protokół IGP potrafi obsługiwać sieć zbudowaną z około stu ruterów i kilku tysięcy segmentów sieci, to typowy protokół EGP opracowany jest tak, aby mógł obsługiwać sieci zawierające tysiące ruterów i dziesiątki, a nawet setki tysięcy, segmentów sieci. Podam przykład - moja sieć składa się z dwudziestu ruterów, do których dołączonych jest prawie 300 segmentów sieci. Taka sieć z łatwością obsługiwana jest przez RP lub OSPF. Ale pełna tablica rutowania sieci Internet zawiera obecnie ponad 45000* tras, które obsługiwane są przez kilka tysięcy ruterów. Do obsługi takiej sieci RIP zupełnie się nie nadaje, a OSPF musiałby zostać bardzo dokładnie i umiejętnie skonfigurowany.

Systemy autonomiczne

W dwóch najczęściej stosowanych protokołach typu EGP, *Exterior Gateway Protocol (EGP)* i *Border Gateway Protocol (BGP),* zastosowano koncepcję *systemóio autonomicznych.* System autonomiczny to grupa sieci i ruterów zarządzanych przez jedną organizację. Zwykle będą to sieci należące do jednej organizacji, ale może być to również grupa współpracujących ze sobą organizacji, a także autonomiczna część jakiejś organizacji, np. podległa jej firma. Choć definicja ta wydaje się być mglista, to w rzeczywis tości granice systemów autonomicznych są bardzo dokładnie zdefiniowane i ściśle przestrzegane. Dana sieć lub ruter należy do *dokładnie* jednego systemu autonomicznego.

*Liczba ta rośnie z niesamowitą szybkością. Po kilku miesiącach od napisania tego akapitu książki podana w nim liczba wzrosła o 20000 tras. Do czasu, kiedy ta książka zostanie wydana, liczba ta będzie już nieaktualna.

Rutowanie zewnętrzne

Niezależnie od tego, w jaki sposób tworzone są systemy autonomiczne, z punktu widzenia protokołów EGP, wnętrze takich systemów jest niewidoczne. Szczegóły wewnętrznej struktury takiego systemu powinny być obsługiwane przez jeden lub kilka protokołów IGP. EGP zakłada, że każdy pakiet adresowany do sieci znajdującej się wewnątrz systemu autonomicznego może być dostarczony do dowolnego rutera, który się w tym systemie znajduje. To system autonomiczny ponosi odpowiedzialność za dostarczenie tego pakietu do adresata.

Ponieważ rutery uczestniczące w pracy EGP muszą wiedzieć, w którym systemie autonomicznym się znajdują, a także gdzie są sąsiadujące systemy autonomiczne, każdy taki system ma przydzielony unikatowy 16-bitowy numer. Numery systemów autonomicznych (AS) przydzielane są przez tę samą organizację, która przydziela numery sieci IP. Jeśli chcesz uzyskać numer AS, powinieneś wspólnie ze swoim ISP wystąpić o przydział takiego numeru. Dostawca powinien posiadać wszystkie potrzebne informacje i pomóc Ci w wypełnieniu formularza zgłoszeniowego.

Protokół Exterior Gateway Protocol (EGP)

Oryginalny protokół EGP nazywany był po prostu *Exterior Gateway Protocol* lub EGP. W tamtych czasach stosowany był tylko jeden taki protokół. Obecnie dostępnych jest kilka protokołów typu EGP, co powoduje powstawanie wątpliwości, czy oznaczenie EGP odnosi się do typu protokołów, czy też wskazuje jeden konkretny. W dalszym opisie oznaczenie EGP będzie oznaczało ten jeden protokół, chyba że zostanie wyraźnie podkreślone, iż mowa jest o rodzinie protokołów.

EGP został opracowany jako protokół, za pomocą którego systemy autonomiczne zgłaszały informacje o trasach do swoich sieci, przekazując je do ruterów rdzenia sieci ARPANet. Te rutery tworzyły w tamtych czasach szkielet sieci Internet. Pomiędzy sobą rozmawiały za pomocą protokołu o nazwie *Gateway to Gatetuay Protocol (GGP).* Ponieważ były pod kontrolą jednej organizacji, tworzyły system autonomiczny.

Obecnie protokołu EGP nie używa się już tak powszechnie, a nawet powinno się unikać stosowania go wszędzie, gdzie to tylko możliwe. Ma on wiele ograniczeń, które uniemożliwiają skalowanie go do rozmiarów i złożoności obecnej sieci Internet. Powinno się go używać jedynie wtedy, kiedy musisz dołączyć swoją sieć do organizacji, która z jakichś powodów nie może używać nowocześniejszego protokołu. (Jeśli rozważasz dołączenie się do Internetu przez ISP, który sugeruje Ci użycie protokołu EGP, to powinieneś poszukać innego dostawcy usług sieciowych.) Choć nie będę w tej książce przedstawiał przykładów wykorzystania EGP, to warto jest omówić i zrozumieć kilka z jego ograniczeń, co pomoże w zrozumieniu potrzeby stosowania nowszych protokołów. Jednym z głównych ograniczeń EGP jest sposób, w jaki wymienia on informacje o ratowaniu. Protokół ten wymaga, aby każdy ruter wysyłał co 30 sekund sygnał *hello* do każdego z sąsiadów. Komunikat ten służy jedynie do potwierdzenia, że rutery pracują, i do ewentualnego wykrycia, że któryś z nich uległ uszkodzeniu. Sam komunikat *hello* nie jest być może problemem, ale EGP wymaga, aby każdy z ruterów co dwie minuty (120 sekund) wysyłał do sąsiadów całą swoją tablicę rutowania.

W czasach, kiedy rozmiary tablicy rutowania każdego z ruterów ograniczały się do około tysiąca zapisanych w nich tras, to nie był żaden kłopot. Jednak teraz, kiedy tablice zawierają ponad 45000 tras, przetworzenie takiej nadesłanej przez sąsiada tablicy i dokonanie uaktualnień w swojej staje się problemem, a trzeba to zrobić, zanim za dwie minuty nadesłana zostanie kolejna tablica!*

Aby jeszcze bardziej pogorszyć sprawę, EGP pracuje bezpośrednio nad IP, a nie nad jakimś protokołem transportowym. Ponieważ każde uaktualnienie to pojedynczy pakiet IP, uaktualnienia te mogą zawierać najwyżej 65536 oktetów informacji. Choć fakt ten ogranicza ilość tras, które mogą być w taki sposób obsługiwane, to znacznie ważniejsze ograniczenia wynikają z tego, co dzieje się przy przesyłaniu takich olbrzymich pakietów. Pakiety są zwykle dzielone na fragmenty, zgodnie z wymaganiami protokołów niższych warstw. W segmencie sieci Ethernet pakiet o długości 65536 oktetów zostanie podzielony na ponad 40 oddzielnych pakietów. Jeśli choć jeden z nich zostanie utracony, to tracona jest cała wiadomość, ponieważ złożenie dużego pakietu, który ją zawierał, nie jest możliwe. Konieczne jest więc ponowne przesłanie całej wiadomości.

Pozostałe problemy wynikają z tego, że EGP opracowany został w czasach, kiedy w sieci Internet pracował tylko jeden rdzeń i wszystkie systemy autonomiczne dołączone były bezpośrednio do tego rdzenia. Tak więc protokół ten nie potrafi obsługiwać sieci Internet w obecnym stanie, gdy składa się ona z kilku rdzeni sieci.

EGP nie pozwala, aby jakiś system autonomiczny rozgłaszał trasy w imieniu innego systemu autonomicznego, za wyjątkiem sytuacji, w której wszystkie te systemy pracują w jednym (i tylko w jednym) systemie autonomicznym tworzącym rdzeń sieci. Jeśli uwzględnimy fakt, że obecnie Internet składa się z wielu rdzeni, i uświadomimy sobie, jakie informacje powinny być przesyłane pomiędzy rdzeniami przez systemy autonomiczne, to będzie wiadomo, dlaczego EGP nie jest już zbyt często stosowany.

Border Gateway Protocol (BGP)

W odpowiedzi na wiele błędów i ograniczeń EGP społeczność internetowa opracowała nowy protokół zewnętrzny, który nazwano *Border Gateway Protocol (BGP).* BGP nie ma już tych problemów, które miał EGP, i daje się skalować do obsługi znacznie większych sieci. Na przykład aby naprawić problem czasu przetwarzania uaktualnień występujący w EGP, BGP wymienia informacje o pełnej tablicy rutowania tylko przy pierwszym uruchomieniu.

*W moim przypadku kłopoty zaczęły się, kiedy tablica rutowania Internet przekroczyła wielkość około 5000 tras. Kuter rozmawiający z Internetem za pomocą EGP nie był w stanie obsługiwać zapytań w czasie krótszym niż 2 minuty, a tyle wynosił przedział pomiędzy nadesłaniem kolejnego zapytania. Tymczasowym rozwiązaniem było wstawienie pośrednika i działało ono do momentu, kiedy wielkość tablicy rutowania przekroczyła 8000 tras. Wtedy zdecydowaliśmy się na zmianę protokołu na BGP. Z nowym protokołem nie ma już takich kłopotów.

W dalszej pracy wymieniane są uaktualnienia zawierające tylko informacje o tym, co uległo zmianie w tablicy rutowania danego rutera. Aby naprawić problem fragmentacji IP, BGP wykorzystuje do przesyłania komunikatów połączenia realizowane przez TCP, które gwarantują dostarczenie pakietów w kolejności, bez strat i duplikacji.

Jest jeszcze wiele innych zmian, które zostały wprowadzone w celu lepszej obsługi sieci Internet. Jedną z największych jest to, że BGP eliminuje koncepcję rdzenia sieci Internet. Ponieważ rdzeń został opracowany do wykorzystywania w sieci złożonej z wielu rdzeni i obsługiwanej przez wielu dostawców, to jego twórcy zdecydowali się na elastyczną konstrukcję BGP, która jest w stanie obsługiwać arbitralną topologię sieci opierającą się na wielu ścieżkach pomiędzy różnymi miejscami. Jest to realizowane *przez* utrzymywanie listy systemów autonomicznych, przez które prowadzi każda trasa. Pozwala to poszczególnym ruterom na wykrywanie pętli w strukturze rutowania BGP (ten sam numer AS pojawia się dwa razy), a także na porównywanie dwóch różnych tras BGP i wybór krótszej (preferowana jest zawsze krótsza trasa), a nawet zastosowanie filtrowania, które zapobiega przechodzeniu niechcianego ruchu przez system autonomiczny (odrzucane są wszystkie trasy zawierające dany numer AS w opisie trasy).

Ostatnią ważną zmianą jest to, że BGP w wersji 4 (BGP4) obsługuje domenowe nitowanie bezklasowe *Classless Interdomain Routing (CIDIR).* Użycie funkcji CIDIR oznacza, że nie trzeba się więcej przejmować starymi klasami sieci IP. Numery sieci są bowiem podawane jako podstawowy numer sieci (prefiks) i maska złożona z ciągłych bitów. BGP potrafi bezbłędnie przenosić te informacje i nie robi żadnych założeń co do wielkości sieci tworzonej w oparciu o jej klasę. Oznacza to, że sieć taka jak `172.16.0.0` w tradycyjnej przestrzeni klasy B musi być przenoszona wraz ze swą maską. Obsługa CIDIR umożliwia sieci Internet ciągły rozwój, zwłaszcza w związku z wyczerpywaniem się dostępnych adresów IP i bardzo dużym wzrostem tablic rutowania w obsługujących ją ruterach. Bez stosowania CIDIR rutery obsługujące szkielet sieci Internet w pewnym momencie przestałyby pracować, ponieważ nie byłyby w stanie obsłużyć większej liczby informacji.

BGP jest protokołem znacznie elastyczniejszym niż EGP. Niestety, kiedy protokół staje się elastyczniejszy, to staje się również bardziej skomplikowany. BGP nie stanowi wyjątku od tej reguły, ale jeśli dostawca sprzętu jest w stanie określić rozsądne domyślne wartości dla większości parametrów konfiguracyjnych, to może się okazać, że większość tej złożoności staje się niewidoczna dla użytkownika. Będziemy przedstawiali tylko przykłady typowych konfiguracji protokołu BGP, gdyż omówienie wszystkich aspektów konfiguracji tego protokołu oznaczałoby napisanie oddzielnej książki tylko na ten temat.

Podstawowa konfiguracja protokołu BGP w ruterach Cisco dołączonych do jednej lokalnej sieci i jednej sieci zewnętrznej została przedstawiona niżej. Nie jest ona wcale bardziej skomplikowana od podstawowych konfiguracji protokołów IGP, przedstawionych w rozdziale 6. W konfiguracji tej mamy instrukcję `router`, która uruchamia proces rutowania BGP. Numer podany na końcu instrukcji `router bgp` jest numerem systemu autonomicznego, w którym pracuje ten ruter.

Nie wolno wybierać tego numeru samemu, tak jak to robiliśmy w przypadku numerów procesów dla protokołów OSPF i EIGRP. Po instrukcji router następuje jedna lub więcej instrukcji network. W przeciwieństwie do protokołów IGP, takich jak EIGRP, gdzie ta instrukcja określała sieć, która będzie brała udział w procesie rutowania IGP, instrukcja network w BGP określa sieci, które z punktu widzenia BGP będą lokalne dla danego systemu autonomicznego i jako takie będą partnerami dla innych sieci w wymienianych przez BGP trasach. Na zakończenie musimy jeszcze powiedzieć procesowi BGP, kim są jego sąsiedzi, wykorzystując do tego celu instrukcję neighbor. Minimalna liczba informacji, jaką musi znać BGP - do którego systemu autonomicznego należy każdy z jego sąsiadów.

```
! our AS number is 101, our provider's is 102
router bgp 101
network 172.16.0.0
neighbor 192.168.1.1 remote-as 102
```

Powiedziałem wcześniej, że BGP4 (najnowsza wersja) potrafi obsługiwać trasy sieci bezklasowych. Zwróć uwagę, że w instrukcji network nie podałem parametru określającego maskę sieci. Jeśli maska nie zostanie podana w tej instrukcji, to IOS rozumie to tak, że chcesz, aby stosowana była naturalna maska dla sieci zgodnej z klasowym podziałem. Może to być dokładnie to, czego się spodziewałeś, i jest wspaniałym skrótem myślowym ułatwiającym proces konfiguracji. Jeśli jednak chcesz określić adres sieci bezklasowej, musisz w instrukcji network umieścić maskę tej sieci:

```
network 192.168.2.0 mask 255.255.254.0
```

Powyższy zapis oznacza, że w uaktualnieniach BGP ma być rozgłaszana informacja o supersieci 192.168.2.0/23 . Nie oznacza to jednak, że BGP dokona automatycznie agregacji dwóch sieci 192.168.2.0/24 i 192 .168.3.0/24. Zapis ten oznacza jedynie, że jeśli wykorzystywany przez Ciebie IGP obsługuje trasę do supersieci, to BGP prześle ją dalej. Aby sumaryzacja wykonywana była automatycznie, konieczne jest zastosowanie znacznie bardziej złożonej konfiguracji:

```
! our AS number is 101, our provider's is 102

router bgp 101
  network 172.16.0.0 I
  aggregate-address 192.168.2.0 255.255.254.0 summary-only
  neighbor 192.168.1.1 remote-as 102
  redistribute rip route-map aggregate
!
! set the origin of any route matching access list 41 to IGP
route-map aggregate
march ip address 41 set origin igp !
 ! select the component routes of 192.168.2.0/23 for aggregation
access-list 41 permit 192.168.2.0 0.0.1.255                    :
```

Wykorzystując taką konfigurację, BGP będzie rozgłaszał informację o sieci 172.16.0.0/16 zawsze, kiedy w głównej tablicy rutowania rutera pojawi się zapis o tej sieci lub którejś z tworzących ją podsieci. Ponadto kiedy obie lub jedna z sieci 192 .168. 2.0/24 i 192 .168.3. 0/24 pojawią się w tablicy rutowania, BGP dołączy w wysyłanym przez siebie uaktualnieniu CIDIR zagregowany zapis 192.168.2.0/23i nie będzie rozgłaszał dwóch bardziej szczegółowych tras. Taką funkcję uruchamia klauzura summary-on l y.

Instrukcje redistribute, route-map i access-list są konieczne ze względu na rozgłaszanie tras do dwóch sieci, które są redystrybuowane z używanego przez Ciebie IGP (w tym przykładzie jest to RIP) i przekazywaniu ich do BGP. Jeśli do obsługi tych tras lub do obsługi ich zagregowanego adresu użyta zostałaby tylko instrukcja network, to BGP rozgłaszałby dokładnie to, co znajduje się w instrukcji network, bez względu na to, czy dokonywana jest agregacja.* Oczywiście, jeśli IGP obsługuje trasy bezklasowe i będzie przesyłał trasę prowadzącą do sieci 192.168.2.0/23, te skomplikowane zapisy nie będą w ogóle konieczne. Jako alternatywne rozwiązanie tego problemu możesz zastosować trasę statyczną prowadzącą do zerowego interfejsu Twojego rutera:

```
! our AS number is 101, our provider's is 102
router bgp 101
  network 172.16.0.0
  network 192.168.2.0 255.255.254.0
 neighbor 192.168.1.1 remote-as 102
!
! create anailed-up static route for 192.168.2.0/23
ip route 192.168.2.0 255.255.254.0 nullO
```

Taka konfiguracja pozwala na obsługę komponentów zagregowanej trasy przez klasowy protokół IGP, podczas gdy BGP będzie rozgłaszał tylko zagregowaną trasę. Jedyną wadą takiego rozwiązania jest to, że ruter zawsze będzie rozgłaszał tę wytyczoną trasę, nawet jeśli nie będzie dostawał żadnych informacji od IGP o sieciach składających się na tę supersieć. Choć jest to dobre rozwiązanie dla Internetu, ponieważ redukuje migotanie trasy, to może się okazać, że nie jest to rozwiązanie działające tak, jak się tego spodziewałeś, zwłaszcza jeśli z Twojej sieci do świata zewnętrznego prowadzi kilka łączy.

Jak widać, konfiguracja BGP, która z początku wydaje się prosta jak bułka z masłem, może szybko stać się niezmiernie skomplikowana. Dobrym sposobem na rozwiązywanie własnych kłopotów z konfiguracją rutera jest przejrzenie innych konfiguracji i dokładne pytanie ich autorów o szczegóły, zanim przystąpisz do konfigurowania jakichś dziwnych rzeczy. Para ruterów testowych może być w takich przypadkach szczególnie pomocna i pozwoli Ci na przetestowanie stworzonej konfiguracji, zanim pokażesz ją światu, instalując na działającym w sieci ruterze.

*Zauważyłem to, kiedy konfigurowałem rozgłaszanie mojej pierwszej zagregowanej sieci pod koniec roku 1994. Nie mogłem sobie z tym poradzić i w końcu poprosiłem autora kodu Cisco o wyjaśnienie przyczyn tego zjawiska, który wyjaśnił mi, jak ta funkcja działa. Wciąż jestem zaskakiwany tym, jaką siłę użytkownikowi daje narzędzie takie jak poczta elektroniczna!

Skonfiguruj jeden z tych ruterów wykorzystując standardową konfigurację protokołu, a następnie dołącz do niego drugi ruter, zawierający Twoją skomplikowaną konfigurację protokołu BGP. Analizując zachowanie się obydwu procesów BGP i tablic rutowania obu ruterów możesz dokładnie przetestować działanie wykonanej przez siebie konfiguracji bez wpływu na pracę sieci. Należy jednak pamiętać, że skomplikowane konfiguracje nie zawsze są potrzebne. Jeśli zaczniesz konfigurować proces BGP na ruterze współpracującym z kilkoma sąsiadami, z których jedni znajdują się w tym samym systemie autonomicznym, a inni w innych systemach autonomicznych, to możesz zdać się na BGP, który sam wybierze rutery, jakie chce słyszeć, a o trasach dowie się i tak, bez konieczności wykonywania specjalnych konfiguracji.

Tak więc masz w sieci działający IGP, który rozgłasza Twoje wewnętrzne trasy do rutera brzegowego, który następnie wysyła je do sieci Internet (lub do sąsiadów) za pomocą BGP. A co z informacjami przesyłanymi w drugą stronę? Jak poinformować rutery wewnętrzne o trasach prowadzących na zewnątrz, których nauczył się BGP? Jeśli w prosty sposób wykonasz redystrybucję tras z BGP do IGP, to możesz zablokować pracę wewnętrznego protokołu i z pewnością utracisz część informacji, jeśli stosowany w Twojej sieci IGP jest protokołem obsługujących tylko sieci z klasy. W takich przypadkach konieczne jest filtrowanie informacji, które redystrybuowane są do IGP, tak jak robiliśmy to pomiędzy dwoma IGP stworzenie domyślnej trasy i włączenie jej do protokołu IGP. Które z tych rozwiązań będzie właściwe dla Twojej sieci, zależy od tego, czy ruter brzegowy jest jedyną trasą do świata zewnętrznego czy też jest jednym z wielu ruterów brzegowych. Jeśli jest to jedyny ruter, to skonfigurowanie trasy domyślnej wydaje się najbardziej sensownym rozwiązaniem; i tak cały ruch na zewnątrz musi przechodzić przez ten ruter. Jeśli zdecydowałeś się na redystrybucję wszystkich lub części tras z BGP do IGP, to musisz uważać na możliwość utworzenia pętli sprzężenia zwrotnego, kiedy trasy te będą następnie redystrybuowane z IGP do BGP.

Istnieje kilka sposobów tworzenia trasy domyślnej rozgłaszanej *przez* IGP. Jednym z nich jest zdefiniowanie statycznej trasy domyślnej, która wskazuje interfejs zerowy, a następnie redystrybuowanie go do protokołu IGP. Trasa taka nie będzie wykorzystywana przez ruter brzegowy, ale dzięki jej istnieniu wszystkie rutery w sieci będą wysyłały cały ruch wychodzący bezpośrednio do rutera brzegowego. Jedyną wadą takiego rozwiązania jest to, że ruter brzegowy będzie rozgłaszał tę trasę domyślną, nawet jeśli jego łącze ze światem zewnętrznym będzie niedostępne. Pakiety wysyłane w sieci i kierowane na zewnątrz będą zawsze przekazywane do rutera brzegowego, który będzie je odbierał, i jeśli łącze zewnętrzne będzie niedostępne, to je po prostu odrzuci. Jeśli takie działanie rutera nie jest właściwe, możesz dodać do konfiguracji polecenia, które sprawią, że domyślna trasa będzie się zachowywała bardziej dynamicznie. Należy wybrać trasę informującą, że sesja BGP jest aktywna i działa poprawnie, o ile trasa ta jest obecna w tablicy rutowania. Powinna ona być jedną z tras prowadzących do Twojego usługodawcy sieciowego, który znajduje się w pobliżu Twojej sieci. Dobrym przykładem może być trasa do sieci używanej dla obsługi łącza WAN lub sieci szkieletowej dostawcy.

Rutowanie zewnętrzne

W moim przykładzie zakładam, że jest to sieć 10.0.0 .0/8, która - choć jest teraz siecią o adresie prywatnym - była wykorzystywana do obsługi rdzenia sieci ARPANet. Jeśli dodasz polecenie:

```
ip default-network 10.0.0.0
```

to Twój ruter wygeneruje domyślną trasę zawsze, kiedy informacja o tej sieci pojawi się w tablicy rutowania obsługiwanej przez ruter. Jeśli sieć jest bezpośrednio dołączona do rutera, to będzie on zawsze tworzył trasę domyślną, chyba że interfejs przestanie pracować. Należy ostrożnie wybrać sieć, która będzie sterowała tworzeniem domyślnej trasy. Ponieważ jesteś uzależniony od czegoś, co nie znajduje się pod Twoją kontrolą, musisz się upewnić, czy sieć ta nie zniknie bez żadnego ostrzeżenia, pozostawiając Cię bez domyślnej trasy rozgłaszanej przez Twój IGP. Aby zabezpieczyć się przed taką ewentualnością, możesz w konfiguracji umieścić klika instrukcji ip default-network, odwołujących się do różnych sieci. Ponadto tworzona w ten sposób trasa domyślna będzie używana przez Twój ruter brzegowy. Jeśli nie chcesz, aby tak było, konieczna jest redystrybucja sieci do IGP i zastosowanie instrukcji i p default-route w konfiguracji jednego z wewnętrznych ruterów lub wykorzystanie statycznej trasy zerowej, opisanej wcześniej.

Może się okazać, że chcesz dokonać filtrowania tras, których nauczyłeś się od sąsiadów BGP. Możliwe jest filtrowanie uaktualnień przychodzących na podstawie analizy poszczególnych adresów sieci tak, jak to opisałem przy konfiguracji IGP, ale jeśli Twoim celem jest zabezpieczenie się przed używaniem tras przechodzących przez jakiś określony system autonomiczny, to filtrowanie oparte na adresie sieci nie da Ci pożądanych efektów. Załóżmy np. że chcesz odfiltrować wszystkie trasy przechodzące przez sieć konkurencji, aby mieć pewność, że nie będzie ona szpiegowała Twoich danych przesyłanych siecią. Nie chcesz jednocześnie filtrować tras, które prowadzą do tej sieci ponieważ nadal chcesz się z nimi komunikować poprzez sieć.* Musisz więc usunąć trasy prowadzące do tej sieci w oparciu o ścieżki AS, które BGP przechowuje wraz z informacją o trasie. Taka ścieżka AS jest listą systemów autonomicznych, przez które będzie przesyłany pakiet korzystający z danej trasy. Dzięki ostrożnemu dobraniu ścieżek AS, które mają zostać odfiltrowane, możesz wyeliminować zapisywanie w tablicy rutowania informacji o trasach, które będą używały określonych ścieżek. W naszym przykładzie chcemy usunąć wszystkie trasy przechodzące przez sieć konkurencji, ale jednocześnie pozostawić trasy prowadzące do tej sieci. Załóżmy, że numer tego systemu autonomicznego to 777. Ścieżki AS, które chcesz odfiltrować z nadsyłanych uaktualnień, to ścieżki, które gdzieś w środku będą zawierały numer 777, ale nie te, które kończą się numerem 777. Nie powinieneś się dziwić, że w przypadku używania sprzętu Cisco filtrowanie takie wykonywane będzie przy użyciu listy dostępu. Inni producenci mogą mieć zaimplementowaną obsługę podobnej

*Takie zabezpieczenie wcale nie musi wystarczać. Jak przekonamy się w rozdziale 10, problemem są zawsze złośliwi lub nieuważni użytkownicy, którzy powodują wyciekanie informacji na zewnątrz firmy. Filtrowanie tras prowadzących przez sieć konkurencji to jednak lekka przesada.

funkcji; powinieneś sprawdzić to w dokumentacji. Oto dość prosty filtr napisany dla rutera Cisco:

```
! our AS number is 101, our provider's is 102, and our competitor's is
! 777
router bgp 101
  network 172.16.0.0
  neighbor 192.168.1.1 remote-as 102
neighbor 192.168.1.1 filler-list 61 in
!
! define an AS path access list that blocks routes traversing our
! competitor's AS, but not those originating there
ip as-path access-list 61 permit _777$
ip as-path access-list 61 deny _777_
ip as-path access-list 61 permit .*
```

Zastosowałem filtrowanie ścieżek AS przez listę kontroli dostępu numer 61, definiując je za pomocą instrukcji `as-path`, i nałożyłem to filtrowanie na nadsyłane od mojego dostawcy uaktualnienia o rutowaniu za pomocą instrukcji `neighbor`, która określa wejściową listę `filter-list`. Żadna trasa nadsyłana przez mojego dostawcę, która w ścieżce AS zawiera umieszczony wszędzie, lecz nie na końcu, numer systemu autonomicznego 777, nie zostanie przepuszczona przez listę dostępu 61 i nie będzie przetwarzana przez mój ruter.* Gdybym chciał eliminować trasy prowadzące do sieci znajdujących się w systemie autonomicznym 777, a nie te, które prowadzą *przez* ten system, to po prostu pominąłbym pierwszą instrukcję i p `as-path`, która wyłapuje wszystkie trasy zaczynające się w AS 777. Będą to więc trasy należące do konkurenta. Ale skoro nie ma żadnych innych ścieżek prowadzących do tych odfiltrowanych sieci, nie będziesz mógł wcale się z nimi komunikować. Dlatego filtrów ścieżek AS nie stosuje się w sieciach, które nie mają kilku sąsiadów. W takim przypadku możliwe jest zastosowanie pomysłowych filtrów dla wszystkich połączeń z sąsiadami. Dzięki różnym kombinacjom dostępu można doprowadzić do tego, że określone ścieżki będą prowadziły przez określone sieci sąsiadów, a inne - przez sieci innych sąsiadów.

Filtrowanie z użyciem ścieżek AS jest korzystne, jeśli filtry mają być stosowane w całych systemach autonomicznych. Czasami jednak konieczne jest filtrowanie uaktualnień nadsyłanych przez sąsiadów na podstawie numerów sieci. Jednym z takich przypadków, kiedy chcesz filtrować ruch w oparciu o numery sieci, jest sytuacja, w której współpracujesz z jednym z klientów jako dostawca usług sieciowych. Wtedy konieczne jest upewnienie się, czy - niezależnie od kiepskiej konfiguracji w swojej sieci - będziesz odbierał od nich tylko informacje o trasach, o których chcesz słyszeć.

Składnia ścieżki AS w ruterach Cisco jest trochę zawiła. Należy pamiętać, że jest to składnia, która pozwala znaleźć identyczny ciąg znaków na podstawie systemu UNIX. Nie musisz być specjalistą od obsługi wyrażeń regularnych, aby zrozumieć, jak ta funkcja działa; wystarczy, abyś tylko zapamiętał kilka podstawowych zasad ich pisania. Po pierwsze znak „$" oznacza koniec ścieżki, a „^" oznacza początek ścieżki. Ponieważ ścieżka AS opisuje zawsze drogę od Twojej sieci do sieci docelowej, oznacza to, że numer Twojego AS (lub twojego usługodawcy) będzie zwykle na początku każdej ze ścieżek, jakie widzisz, a numer docelowego AS będzie na końcu. Po drugie „." oznacza cokolwiek, a „" oznacza „zero lub więcej razy". Tak więc sekwencja dwóch znaków „.*" oznacza cokolwiek lub nic. Znak „_" oznacza każdą przerwę pomiędzy dwoma numerami *AS* lub pomiędzy numerem AS a początkiem lub końcem ścieżki. Proste, nieprawdaż?

Rutowanie zewnętrzne

W rozdziale 6 mówiliśmy o robieniu takich zabezpieczeń w protokole IGP; takie same zasady dotyczą zewnętrznego protokołu, a ich stosowanie w tym przypadku może być znacznie ważniejsze, gdyż uszkodzenia spowodowane propagowaniem błędnych uaktualnień mogą teraz dotknąć znacznie większą ilość urządzeń. Aby skonfigurować filtrowanie sieci na łączu z sąsiednim BGP, należy stworzyć ilość dostępu opisującą sieci, które chcesz słyszeć, a następnie zastosować tę listę w instrukcjach neighbor za pomocą klauzuli distribute-list in. Istnieje również klauzula distribute-list out, która pozwala na nakładanie takich samych ograniczeń na to, co jest przez Ciebie wysyłane do sąsiadów. Składnia tej drugiej klauzuli jest identyczna, jak w przypadku filtrowania komunikatów przychodzących, nie będę więc prezentował oddzielnego przykładu jej stosowania.

```
! our AS number is 101, our customer's is 102 router bgp 101
  network 172.16.0.0
  neighbor 192.168.1.1 remote-as 102
neighbor 192.168.1.1 distribute-11st 97 in i
! define the list of routes we expect to hear from our customer access-list 97 permit
192.168.2.0 255.255.254.0 access-list 97 permit 192.168.4.0
255.255.255.0 access-list 97 deny    0.0.0.0      0.0.0.0
```

W przykładzie tym zdefiniowałem listę dostępu 97, która pozwala na przejście informacji o trasach, które będę akceptował w oparciu o podpisane z klientem porozumienie. W tym przypadku pozwalam na przejście dwóch tras 192.168.2.0/23 i 192.168.2.0/23. Ostatnia instrukcja deny nie jest konieczna, ponieważ lista kontroli dostępu z definicji zabrania wszystkiego, co nie jest w niej dozwolone, ale umieściłem ten zapis, by wszystko było jasne. Przy takiej konfiguracji listy, niezależnie od tego, jak kiepska będzie konfiguracja rutowania u mojego klienta, mój ruter będzie ignorował wszystko, co z tej sieci do mnie dociera, za wyjątkiem informacji o tych dwóch trasach. Gdybym jednak zastosował filtrowanie AS, to mój klient mógłby próbować mnie oszukać, rozgłaszając trasy stosujące do przejścia inne AS, które specjalnie u siebie stworzył, by omijać moją listę filtrowania. To, czy takie działanie jest przypadkowe, czy też zamierzone, nie ma znaczenia, mój ruter nadal akceptowałby takie rozgłaszane trasy jako poprawne.

Jako ostatni przykład rozważmy przypadek, w którym nasza sieć jest dołączona do dwóch dostawców i chcielibyśmy, aby pakiety przesyłane były po najkrótszej ścieżce. Nie wymaga to stosowania żadnych filtrów. Oprócz tego chcesz mieć pewność, że ruch kierowany do sieci przyjaciół zawsze będzie przechodził przez sieć dostawcy A, nawet jeśli trasa prowadząca przez sieć dostawcy B będzie lepsza. Takie przekierowanie ruchu ma działać zawsze, chyba że łącze z siecią A przestanie pracować. Oznacza to, że nie chcesz filtrować tras prowadzących do sieci przyjaciół nadsyłanych w uaktualnieniach od dostawcy B, chcesz jedynie preferować te, które nadsyłane są z A. Ponadto chcesz mieć pewność, że dostawcy bez uzgodnienia z Tobą nie zaczną wykorzystywać Twojej sieci do tranzytu informacji między swoimi sieciami.

Innymi słowy, chcesz mieć pewność, że trasy, których sieć nauczy się od dostawcy A, nie będą rozgłaszane do dostawcy B i odwrotnie.

```
! our AS number is 101, provider A's is 102, provider B's is 103, and
! our friend's is 777
router bgp 101
  network 172.16.0.0
  neighbor 172.16.1.1 remote-as 102     ! provider A
  neighbor 172.16.1.1 filter-list 81 weight 100
  neighbor 172.16.1.1 filter-list 82 out
  neighbor 172.16.2.7 remote-as 103     ! provider B
neighbor 172.16.2.7 filter-list 83 out
!
! define an AS path access-list that selects our friend's routes
ip as-path access-list 81 permit _777$
!
! define an AS path access-list that blocks provider B's routes
ip as-path access-list 82 deny ^103_                    ! B's routes
ip as-path access-list 82 permit .*
j
! define an AS path access-list that blocks provider A's routes
ip as-path access-list 83 deny ^102_                    ! A's routes
ip as-path access-list 83 permit .*
```

Część tej konfiguracji powinna wyglądać znajomo. Numer Twojego AS to 101, jest w nim jedna sieć lokalna rozgłaszana do sieci obu dostawców, a także dwóch sąsiadów, każdy dołączony do innego dostawcy. Mamy również zestaw trzech filtrów dla ścieżek AS . Listy filtrów o numerach 82 i 83 definiują po prostu trasy przesyłane do nas od każdego z sąsiadów. Te, które przychodzą od sąsiada A, mają jego numer (102) jako pierwszy numer w ścieżce AS, te nadsyłane od sąsiada B mają na początku ścieżki AS jego numer AS (103). Blokując przesyłanie tych tras pomiędzy dostawcami, zabezpieczamy się przed wykorzystywaniem naszej sieci jako sieci tranzytowej. Aby to osiągnąć, konieczne jest zastosowanie tych filtrów w wychodzących na zewnątrz uaktualnieniach kierowanych do obu sąsiadów przy użyciu klauzuli filter-list. Oczywiście oni sami powinni filtrować to, co do nich przesyłamy, ale teraz na pewno jesteśmy bezpieczni.

Lista filtrowania o numerze 81 definiuje każdą sieć, która zaczyna się w AS naszych przyjaciół; jego numer to 777. Ponieważ zakładamy, że są to ich sieci, to administracyjnie nadamy im wagę 100 w momencie, kiedy są one nadsyłane od dostawcy A. Ponieważ domyślna wartość dla ścieżek BGP uzyskanych z sieci zewnętrznych wynosi O, a preferowane są wyższe wartości, to po takiej konfiguracji będziemy preferowali każdą ścieżkę prowadzącą do tych sieci przez dostawcę A tak długo, jak jego sieć będzie dostępna. Zwróć uwagę na to, że nie filtrujemy tych tras z nadsyłanych *przez* B uaktualnień. Gdybyśmy tak zrobili, to nie moglibyśmy wcale komunikować się z naszymi przyjaciółmi, kiedy trasy prowadzące przez sieć dostawcy A przestałyby być dostępne.

Jak widzisz, tego typu opcji jest mnóstwo. Każdy BGP ma niepowtarzalną konfigurację i nie ma czegoś takiego jak *typowa* konfiguracja rutera BGP.

Ratowanie zewnętrzne

Najlepszym sposobem uzyskania informacji o tym, jak uzyskać konfigurację, która pozwala osiągnąć określony cel, jest kontakt z ludźmi o większym doświadczeniu, przeglądanie przykładowych konfiguracji i eksperymentowanie. Dostawca internetowy, z którym współpracujesz powinien mieć ludzi, którzy będą w stanie Ci pomóc.

Wpływ na inne łącza - publiczne i prywatne

Jest jeszcze jeden aspekt związany z konfigurowaniem zewnętrznego rutowania, do którego należy podejść bardzo ostrożnie. Jeśli masz kilka zewnętrznych łączy, nieważne czy są one publiczne czy też prywatne, to każde nowe łącze zewnętrzne może mieć wpływ na konfigurację pozostałych łączy. Na przykład, jeśli masz publiczne łącze prowadzące do Internetu i skonfigurowałeś je tak, żeby zawartość twojego IGP redystrybuowana była w to łącze bez żadnego filtrowania, to pomyśl, co się stanie, kiedy dodasz prywatne łącze prowadzące do innej organizacji i zredystrybuujesz ich trasy do swojego IGP? Może się okazać, że w ten sposób po cichu zapewnisz swojemu sąsiadowi połączenie z siecią Internet. Taka usługa może naruszać umowę, którą podpisałeś z dostawcą, a także spowodować kłopoty z nitowaniem u sąsiada i niepotrzebne przeładowanie Twoich łączy. Jest to więc jeden z ważniejszych powodów, dla których powinno się dokładnie określać trasy w konfiguracji protokołów rutowania, które mają być między nimi wymieniane, pozostawiając tylko te, które mają być obsługiwane *przez* współpracujące ze sobą sieci. Jeśli Twoje połączenie z Internetem skonfigurowane jest tak, że redystyrybuowane są tylko Twoje własne sieci z używanego przez Ciebie IGP do EGP, to redystrybucja tras z prywatnego łącza do Twojego IGP nie powinna mieć wpływu na pracę połączenia z Internetem, ponieważ trasy te zostaną odfiltrowane. Także konfiguracja prywatnego łącza z wykorzystaniem odpowiednich mechanizmów filtrowania tras uchroni nowego sąsiada lub łącze publiczne przed przypadkowym wpływem wspomnianych tras na jego pracę.

Oczywiście nie możesz wymagać od sąsiadów stosowania tych samych zasad, chyba że są to organizacje, które Ci podlegają. Wszystko, co możesz zrobić, to z nimi współpracować i upewnić się, że po ich stronie skonfigurowane zostały odpowiednie zabezpieczenia, dzięki którym Twoje trasy nie są propagowane do ich sąsiadów, i dalej nadzorować pracę ich sieci. Jeśli Twoje trasy przeciekają do świata zewnętrznego przez sieć sąsiada, może się okazać, że ruch przychodzący do Twojej sieci preferuje wolniejsze łącze z tym sąsiadem i nie wykorzystuje wspaniałego nowego połączenia TI z Internetem. W takim przypadku powinieneś przygotować się na przerwanie połączenia z sąsiadem do czasu, aż on rozwiąże ten problem.

Nie wolno Ci zakładać, że skoro po dodaniu sieci sąsiada wszystko działa dobrze, to tak będzie w przyszłości. Błędy się *zdarzają,* ludzie się zmieniają, a sieci rosną. To, co mogło być skonfigurowane poprawnie w zeszłym tygodniu, nie musi być bezbłędne w tym tygodniu, skoro Ty sam lub sąsiedzi dodaliście kolejne łącze, zmieniliście dostawcę usług lub uaktualniliście oprogramowanie ruterów. Konieczne jest stałe nadzorowanie obsługi rutowania z zewnętrznymi sieciami, z którymi Twoja sieć wymienia informacje.

Łącza stałe czy zestawiane na żądanie?

Wiele osób zakłada, że jest tylko jeden sposób na nawiązanie zewnętrznego, trwałego połączenia z siecią sąsiedniej organizacji lub z siecią Internet. Natychmiast myślą oni, że jedyną dobrą odpowiedzią we wszystkich przypadkach jest stałe łącze dzierżawione. Prawdą jest, że to najczęściej stosowany typ łącza zewnętrznego, ale nie jest to jedyna dostępna opcja. Zanim z góry założysz, że jest to jedyne rozwiązanie, zastanów się nad zaletami i wadami rozwiązań opartych na wykorzystaniu łącza stałego i łącza zestawianego na żądanie. Takim zestawianym łączem może być na przykład ISDN. Nie zawsze takie łącze musi oznaczać stosowanie modemów analogowych.

To, który rodzaj połączenia zostanie przez Ciebie wybrany, zależy również od tego, które z tych łączy jest dla Ciebie dostępne. Jeśli zamierzasz dołączyć swoją sieć do Internetu, a wybrany przez Ciebie dostawca usług nie obsługuje połączeń zestawianych na żądanie, to może się okazać, że jesteś zmuszony do zastosowania łącza stałego. Możliwe, że Twoja decyzja będzie zależała również od tego, co może zapewnić lokalny dostawca łączy telefonicznych lub jakiego łącza chce używać sąsiad.

Jedną z zalet łącza zestawianego na żądanie jest jego koszt. Zwykle usługi połączenia na żądanie kosztują mniej niż stałe połączenie o takiej samej przepustowości, przy założeniu, że sposób, w jaki to łącze jest wykorzystywane nie powoduje, że będzie ono w stanie połączenia przez cały czas. Jeśli zamierzasz używać połączenia przez większość czasu, to łącze zestawiane na żądanie będzie kosztowało prawdopodobnie tyle samo, co łącze stałe lub nawet więcej. Należy więc bardzo ostrożnie rozważyć te ekonomiczne aspekty. Jeśli tworzysz połączenie z siecią Internet, to musisz wiedzieć, co dostawca usług zrobi, kiedy odbierze jakiś ruch przeznaczony dla Twojej sieci w czasie, kiedy łącze jest w stanie rozłączenia. Niektórzy dostawcy usług mają tak skonfigurowany sprzęt, że inicjuje on zestawienie połączenia z automatycznym oddzwanianiem, dzięki czemu Ty płacisz wszystkie rachunki za połączenia. Jednak większość takich firm odmówi zestawiania połączeń i kierowany do Ciebie ruch zostanie odrzucony. Jeśli spodziewasz się czegoś innego, upewnij się, że dostawca usług, którego wybrałeś, będzie w stanie i będzie chciał spełnić Twoje życzenia.

Usługi stałe mają zwykle tę zaletę, że są dość szybkie i nieskomplikowane. Często najszybszym połączeniem zestawianym na żądanie, które może zostać zrealizowane, jest połączenie 64 kbps lub 128 kbps. Stałe połączenia zaczynają się zwykle od 56 kbps i mogą dość łatwo osiągnąć szybkość transmisji aż 45 Mbps, tj. cztery i pół razy więcej niż szybkość pracy sieci Ethernet! W niektórych lokalizacjach możliwe jest nawet uzyskanie szybszych łączy, takich jak 155 Mbps. Wszystko *zależy* od tego, w jakim miejscu się znajdujesz i z jakim miejscem chcesz się połączyć. Należy pamiętać, że niektóre formy połączeń zestawianych na żądanie pozwalają Ci na wykonanie dodatkowych połączeń z tym samym miejscem w przypadku, kiedy Twoje łącze wymaga większej przepustowości, i na rozłączenie ich, kiedy wykorzystanie pasma spadnie. Takie rozwiązanie może być bardzo przydatne, kiedy generowany na tym łączu ruch przez bardzo krótki okres wymaga szerokiego pasma, a *przez* resztę czasu ruch na nim jest znacznie mniejszy.

Łącza state czy zestawiane na żądanie?

Stałe łącze ma jeszcze jedną wyraźną zaletę. Takie połączenia nie są zbyt skomplikowane, ponieważ nie jest dla nich konieczne określanie zasad nawiązywania połączenia, czasu, po którym takie połączenie jest rozłączane w przypadku braku aktywności oraz czasu, jaki musi upłynąć przed kolejnym połączeniem. Ponadto pakiety transmitowane przez takie połączenie nie muszą czekać, aż połączenie zostanie nawiązane. Nadal jednak w przypadku małych organizacji ważnym czynnikiem są koszty. Jedną z opcji, która zdobywa coraz większą popularność, jest utrzymywanie wąskopasmowych łączy dzierżawionych, a także zestawianie połączenia na żądanie z tym samym miejscem. Takie zestawiane połączenie może służyć jako łącze zapasowe lub - w przypadku zapotrzebowania na większe pasmo - może być wykorzystane jako tanie łącze równoległe. Dokładne przeanalizowanie dostępnych opcji może w efekcie pozwolić na zaoszczędzenie pieniędzy przy jednoczesnym zapewnieniu wystarczających osiągów łącz.

Jeśli wybierzesz opcję wykorzystującą łącza zestawiane na żądanie, musisz zwrócić szczególną uwagę na konfigurację swojego protokołu rutowania. Wiele osób stosujących tego rodzaju połączenia odkrywało z czasem, że były one nawiązywane i utrzymywane tylko po to, by ich dynamiczny protokół rutowania mógł pracować. Takie wykorzystanie łącza jest marnotrawstwem i do tego kosztownym. Skoro producent stosowanych w Twojej sieci ruterów implementuje w nich obsługę wielu różnych pomysłowych opcji, to sprawdź, czy wśród nich jest funkcja pozwalająca na statyczne rutowanie przez łącza zestawiane na żądanie. Jeśli na przykład Twoje łącze zestawiane na żądanie prowadzi do Internetu, to powinieneś doprowadzić do tego, aby dostawca utrzymywał trasy statyczne prowadzące do każdej z twoich sieci i rozgłaszał je w sieci Internet w Twoim imieniu, podczas gdy Ty po swojej stronie będziesz musiał jedynie utrzymywać statyczną trasę domyślną. W takiej konfiguracji każdy ruch generowany z Twojej sieci do Internetu będzie powodował zestawianie połączenia; po przesłaniu tych danych, łącze będzie rozłączane. Oprócz zredukowania czasów połączenia takie rozwiązanie zmniejsza również niestabilność Twoich tras w sieci Internet. Jest to bardzo ważne, ponieważ każde rozgłoszenie nowej trasy lub jej usunięcie powoduje, że wszystkie rutery w sieci Internet będą musiały poświęcić trochę czasu na przeanalizowanie tych zmian.

Niezależnie od tego, czy łączysz się z Internetem, czy też z siecią innej organizacji, czy jest to łącze stałe, czy też zestawiane na żądanie, wszystkie połączenia sieci ze światem zewnętrznym powinny być dokładnie przemyślane, zaplanowane i wykonane. Skoro sieć traktujemy jak żyjący organizm, wpływ zewnętrznego połączenia na jego funkcjonowanie powinien interesować nas przynajmniej tak mocno jak dodanie nowego łącza wewnątrz sieci. Jest to zwłaszcza ważne w związku z bezpieczeństwem sieci, które jest najbardziej zagrożone właśnie przez każde połączenie naszej sieci ze światem zewnętrznym. Będzie to temat kolejnego rozdziału tej książki.

10

Bezpieczeństwo sieci

Co to jest bezpieczeństwo? Ocena wymagań dotyczących bezpieczeństwa Kontrola dostępu Rozszerzanie prywatności Utrzymywanie integralności danych Zapobieganie atakowi denial of service Inne sprawy związane z bezpieczeństwem

Kiedy omawiane są sieci komputerowe, to tematem, który najczęściej powoduje wątpliwości i komplikuje sprawę, jest ich bezpieczeństwo. Niektórzy twierdzą, że to sieć jest odpowiedzialna za udostępnienie bezpiecznego środowiska do pracy ho-stów, tak by były one równie bezpieczne jak wtedy, gdy nie są dołączone do sieci. Inni utrzymują, że sieć nie ponosi odpowiedzialności za bezpieczeństwo. Zdaniem większości rozwiązanie leży gdzieś pośrodku. Bez względu na to, jaka jest Twoja opinia na ten temat, na pewno zdarzają Ci się sytuacje, kiedy z pewną obawą myślisz o bezpieczeństwie swojej sieci i pracujących w niej hostów. Nawet jeśli wierzysz, że sieć nie ponosi odpowiedzialności za bezpieczeństwo, to z pewnością nie będziesz twierdził, że dołączone do tej sieci hosty są tak zabezpieczone, jak być powinny.

W rozdziale tym omówimy kilka tematów związanych z bezpieczeństwem sieci, włączając w to również rozwiązania, w których sieć może wspomagać zabezpieczenie hostów, a także bronić samą siebie przed atakami. Być może omawiane tu sprawy nie będą zawierały odpowiedzi na wszystkie pytania, ale powinny przynajmniej dać Ci dobry punkt wyjścia do dalszych rozważań.

Co to jest bezpieczeństwo?

Jeśli zapytasz grupę ekspertów sieciowych o to, co oznacza termin „bezpieczeństwo sieci", to otrzymasz prawdopodobnie tyle odpowiedzi, ilu ludzi znajduje się we wspomnianej grupie. Większość z tych odpowiedzi będzie poruszała sprawę zabezpieczenia sieci i hostów przed nieautoryzowanym dostępem.

Bezpieczeństwo jest kwestią określenia poziomu zabezpieczeń, jaki możemy zastosować. Odpowiedź, w której stwierdza się, że dana maszyna w sieci jest bezpieczna, a inna nie, nie jest prawdziwa. Zamiast tego należy mówić, jak zabezpieczona jest dana maszyna lub cała sieć przed określonymi lukami, które zauważono i usunięto, czyli w jakim stopniu spełnia wymagania zabezpieczeń. Im wyższy jest ten stopień, tym maszyna powinna być bezpieczniejsza. Ale, podobnie jak w większości spraw związanych z przemysłem komputerowym, bezpieczeństwo jest rodzajem handlu. Spójrz na sprawę bezpieczeństwa hosta lub sieci jak na oś poziomą, której jeden koniec nazywa się *bezpieczeństwo,* a drugi - *użyteczność.* W miarę jak przesuwamy naszą maszynę lub sieć w kierunku większego stopnia bezpieczeństwa zwykle stają się one mniej nadające się do użytku. Sieć bardziej użyteczna staje się mniej bezpieczna.

Jeśli masz co do tego wątpliwości, zastanów się nad ekstremalnymi rozwiązaniami. Która maszyna jest najlepiej zabezpieczona w każdym środowisku? Odpowiedź brzmi: maszyna, której nigdy nie włączamy, zamknięta w pokoju pilnowanym przez uzbrojonego strażnika. Taka maszyna może być chyba uznana za dość bezpieczną. Nie można jej zrobić nic złego bez poważnych działań wymagających sporo zachodu. Niemniej maszyna taka nie jest przydatna. Drugim krańcowym przykładem jest maszyna wystawiona na korytarz i nie zabezpieczona żadnym hasłem. Każda osoba może do takiego komputera podejść i zrobić na nim wszystko bez żadnych ograniczeń. Większość ludzi stwierdzi, że taki komputer jest szczególnie użyteczny, ale jednocześnie trzeba stwierdzić, że poziom jego zabezpieczeń jest właściwie żaden. Podobne przykłady można przedstawić dla sieci komputerowych; bezpieczne sieci znacznie utrudniają pracę, podczas gdy łatwe w użyciu sieci nie mają zwykle ograniczeń, które podnosiłyby ich poziom bezpieczeństwa. Mając cały czas w pamięci te dwie skrajności, powinieneś zastanowić się, jak duży stopień bezpieczeństwa jesteś w stanie zastosować w swojej sieci kosztem utraty jej użyteczności. Im łatwiejsza w użyciu będzie Twoja sieć, tym będzie prawdopodobnie mniej bezpieczna, i vice versa; im bardziej ją zabezpieczysz, tym trudniej będzie użytkownikom wykonywać pracę w takiej sieci

Aspekty bezpieczeństwa

Bezpieczeństwo jako funkcja sieci komputerowych ma różne znaczenie dla różnych ludzi. W większości przypadków będzie oznaczało kontrolowanie dostępu do maszyn i zasobów udostępnianych w sieci. Na przykład, ludzie obawiają się nieautoryzowanego dostępu innych użytkowników, którzy mogą włamać się cło ich komputerów. Jest to jeden z aspektów bezpieczeństwa sieci, na który bardzo duży wpływ ma istnienie łączy prowadzących na zewnątrz sieci. Nie jest to jednak jedyny aspekt, którym powinieneś się zajmować.

Co to jest bezpieczeństwo?

Drugim ważnym punktem, który jest często pomijany, jest bezpieczeństwo danych. Musisz rozważyć to, jak ważne jest podsłuchiwanie komunikacji odbywającej się w Twojej sieci. Niestety ochrona przed wszystkimi metodami podsłuchu jest zwykle niemożliwa. W segmencie sieci Ethernet lub każdej innej wielodostępnej sieci pracującej z rozgłaszaniem, nie jest możliwe stwierdzenie, czy jakaś maszyna została nielegalnie dołączona do sieci lub - jeśli dołączenie było legalne - nie można wykryć faktu, że maszyna ta podsłuchuje komunikację odbywającą się między innymi maszynami. Są jednak działania, które możesz podjąć w celu ograniczenia możliwości podsłuchu komunikacji w sieci oraz jego wpływu na bezpieczeństwo danych.

Integralność danych jest trzecim aspektem bezpieczeństwa sieci. Jaką masz pewność, że dane, które wysłałeś, to te same dane, które zostały odebrane? Protokoły sieciowe mają wbudowaną ochronę przed przypadkowymi zmianami danych, które mogą być spowodowane uszkodzeniem sprzętu lub innymi zdarzeniami w sieci. Nie ma jednak takich mechanizmów, które chroniłyby dane przechowywane na jakimś tymczasowym hoście, tak jak to ma miejsce w przypadku wiadomości poczty elektronicznej przechowywanych na serwerze poczty. Nawet jeśli dane nie zostaną zmienione, to jaką mamy pewność, że nadawca rzeczywiście je wysłał i że odebrana przez nas wiadomość nie jest tylko pomysłowym fałszerstwem? Fałszowanie poczty elektronicznej jest działaniem trywialnym; większość uczniów szkół średnich może sobie z tym poradzić w godzinę, a my będziemy błędnie zakładali, że wiadomości, które otrzymujemy od Marysi, rzeczywiście wysłała ona sama.

Ostatni opisywany aspekt bezpieczeństwa nie ma nic wspólnego z ochroną dostępu do systemu, sieci lub do danych w niej przesyłanych. Jest on natomiast związany z wykorzystywaniem sieci w celu blokowania usług sieciowych właściwym jej użytkownikom i dołączonym do niej systemom. Ataki typu *denial of service* - choć możliwe do przeprowadzenia na odizolowanych systemach - stają się stosunkowo łatwe do przeprowadzenia, jeśli maszyna będąca celem ataku jest dołączona do sieci. Ataki takie są dość efektywne. Dlatego stają się coraz popularniejsze. Dzieje się tak również dlatego, że trudno jest wyśledzić źródło takiego ataku.

Każdy z wymienionych wyżej aspektów bezpieczeństwa musi być obsługiwany w inny sposób, ale zawsze trzeba mieć na uwadze pozostałe aspekty. Ochrona bezpieczeństwa systemu to działania bardzo zaawansowane. Metody wykorzystywane do zabezpieczenia systemu przed nieautoryzowanym dostępem nie mają wiele wspólnego z podsłuchiwaniem danych, tak samo jak ochrona przed podsłuchem niewiele ma wspólnego z ochroną przed nieautoryzowanym dostępem. Wykorzystując jednak te metody równolegle można zastosować rozwiązania, które się wzajemnie uzupełniają. Na przykład jedne z najbardziej chronionych w Twojej sieci dane to hasła użytkowników. Chroniąc pliki z tymi hasłami przed podsłuchaniem, zmniejszasz ryzyko występowania nieautoryzowanego dostępu do sieci. A ponieważ podsłuch sieci wymaga dostępu do jej segmentu, to ochrona przed nieautoryzowanym dostępem do maszyn pracujących w sieci pomoże ograniczyć możliwość podsłuchania komunikacji w sieci. W kilku kolejnych podrozdziałach omówię niektóre sposoby zapewnienia bezpieczeństwa.

Ocena wymagań dotyczących bezpieczeństwa

Zanim zaczniesz pracę nad zabezpieczeniami, powinieneś najpierw ocenić, jakie są Twoje wymagania odnośnie bezpieczeństwa. Większość administratorów komputerów i sieci nigdy nie zadaje sobie trudu, by pomyśleć o tych właśnie sprawach. Zaczynają od razu wprowadzać zabezpieczenia do swoich sieci, bez przemyślenia tego, co tak naprawdę powinno być w tych sieciach chronione. Choć szczegółowa analiza bezpieczeństwa może przekraczać Twoje kompetencje i zakres odpowiedzialności, to nawet pobieżne zastanowienie się nad tymi sprawami sprawi, że będziesz w stanie wskazać obszary, które wymagają szczególnej uwagi z Twojej strony. Na przykład, jeśli organizacja, w której pracujesz, ma coś wspólnego z bankowością lub finansami, to poufność danych klientów może być najważniejszym zadaniem z punktu widzenia bezpieczeństwa. Nie chcę *przez* to powiedzieć, że kontrola dostępu nie jest ważna. Omawiamy tu względny stosunek poszczególnych aspektów bezpieczeństwa do siebie. Uniwersytet, z drugiej strony, będzie prawdopodobnie zwracał mniejszą uwagę na podkradanie rekordów z danymi finansowymi ponieważ są one i tak, zgodnie z prawem, publiczną własnością. Jednak ochrona przed zmianą swoich ocen przez studentów lub uzyskaniem dostępu do plików zawierających kopie egzaminów końcowych może być priorytetem w zakresie bezpieczeństwa działającej tam sieci. Należy więc patrzeć na pełny obraz sieci i systemu i nie dać się pochłonąć przez szczegóły. Kiedy już zdecydujesz, jakie obszary w Twojej sieci wymagają zabezpieczeń, powinieneś dokonać realnej oceny podejmowanych działań zabezpieczających pracę tych obszarów. W niektórych przypadkach rezultatem może być spora irytacja użytkowników. Doskonałym słowem, które bardzo się przyda w czasie dokonywania tych analiz jest, *realistyczny*. Nie zakładaj, że jakaś sprawa nie jest poważnym zagrożeniem, ponieważ trudno ją dokładnie zdefiniować. Nie staraj się jednak także zabezpieczać za wszelką cenę czegoś, czego zabezpieczenie zajmie Ci sporo czasu, co i tak nie da się zabezpieczyć. Troska o ważne dane na maszynach w centrum administracyjnym przetwarzania danych na pewnym uniwersytecie doprowadziła do szybkiej decyzji o zainstalowaniu ściany ogniowej, która miała chronić te maszyny przed intruzami z sieci kampusowej. Nikt jednak nie zastanowił się, jak należy zabezpieczyć dane, które przesyłane są przez sieć kampusową do użytkowników, który mają do nich gwarantowany dostęp. Tak więc urządzenie zabezpieczające znalazło się w miejscu nieprzemyślanym i nie gwarantującym poprawnych wyników jego działania; jedyną zaletą tego rozwiązania było przekonanie kilku przewrażliwionych ludzi, że teraz ich dane są bezpieczne, choć w rzeczywistości tak nie było.

Na zakończenie trzeba podkreślić, że dla każdego typu luk w zabezpieczeniach, które zamierzasz usunąć, konieczne jest ich wcześniejsze oszacowanie. W dużym stopniu taki proces szacowania podobny jest do oszacowania kosztów i prawdopodobieństwa wystąpienia uszkodzeń, które oceniłeś podczas projektowania sieci (patrz rozdział 3, „Projektowanie sieci - część 2").

Tym razem jednak dokonujesz oceny prawdopodobieństwa pewnych działań wykonywanych przez użytkownika, a nie uszkodzeń występujących w urządzeniach, przez co Twoje przewidywania będą bardziej subiektywne. Kiedy już będziesz miał świadomość, jakie są koszty zabezpieczeń i prawdopodobieństwo naruszania pewnych zabezpieczeń, to będziesz znacznie lepiej przygotowany na skupienie swojej uwagi i środków na uchronieniu sieci przed występowaniem dziur w zabezpieczeniu lub uporaniu się z tymi, które już zostały zauważone. Powinieneś skupić swoje działania na problemach, których występowanie jest bardziej prawdopodobne, zanim zaczniesz się przejmować problemami drugorzędnymi.

Kontrola dostępu

Kontrolowanie dostępu do sieci i jej zasobów jest pierwszym i często jedynym zabezpieczeniem, o jakim myśli większość administratorów sieci i hostów. Być może wynika to z faktu, że mogą sobie dość łatwo wyobrazić cele, które są w stanie osiągnąć, stosując tę metodę zabezpieczeń. Poza tym łatwo jest mówić o zabezpieczeniach, jeśli oznaczają one hasła dostępu i są podobne do zabezpieczeń stosowanych poza światem komputerów. Zwykle nietrudno przekonać szefów do zastosowania tego typu kontroli dostępu. Bardzo łatwo jest w takich przypadkach zastosować porównanie niechcianego gościa buszującego po komputerze do takiego samego gościa, który rozgląda się po naszym domu. Niektórzy ludzie, pomimo tak oczywistych porównań, mają problem z uświadomieniem sobie, że zabezpieczenia takie są konieczne. Często można ich przekonać przedstawiając pełniejszy obraz sytuacji. Przecież nie chcianych gości trzymamy z dala od domu nie dlatego, że ich nie lubimy, lecz dlatego, że mogą wyrządzić jakieś szkody, jeśli tam się znajdą. Obawiamy się o to, co posiadamy, o naszą prywatność, a nawet o nasze życie.

W przypadku intruza komputerowego nie mamy co prawda takich samych obaw. Ktoś, kto wtargnie do naszych komputerów lub do sieci, nie będzie prawdopodobnie czyhał na nasze życie, i choć intruz taki może naruszyć bezpieczeństwo danych, to prawdopodobnie nie może skraść pamięci komputera, dysków, klawiatur lub innych części komputera. Choć kradzież danych jest tym, przed czym chcemy się uchronić, to większość przypadków włamań do komputera nie jest dokonywana w celu kradzieży danych lub oprogramowania. Intruzi chcą zwykle udowodnić sobie i innym, co potrafią (w poszukiwaniu silnych wrażeń) lub uszkodzić maszynę, w której się znajdują. Pamiętając o tym, możemy stwierdzić, że w większości przypadków nasze działania zabezpieczające przed wejściem do sieci lub hostów nie wynikają z obawy, że zrobią oni coś złego, kiedy już znajdą się w naszym systemie, lecz z faktu, że znajdą się tam bez naszej zgody. Choć jest to właściwy sposób myślenia, który uzasadnia starania zmierzające do trzymania intruzów z dala od sieci, gdzie mogą poważnie zagrażać prywatności danych lub je uszkodzić, to spojrzenie na te sprawy z pewnej perspektywy może zabezpieczyć administratorów przed utratą proporcji zagrożeń.

W swoich działaniach powinieneś być gorliwy, ale jednocześnie powinieneś być realistą.

Ściany ogniowe

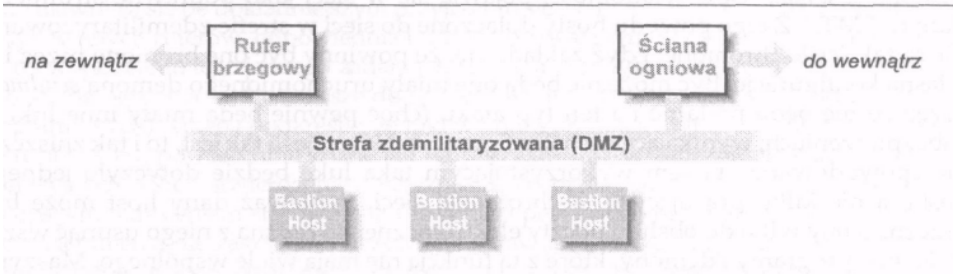
Jeśli zapytasz dziesięciu administratorów sieci o to, jak należy zabezpieczyć się przed niepowołanym dostępem do hostów i innych zasobów sieci, to każdy z nich natychmiast wspomni o zainstalowaniu ściany ogniowej. Czym jest takie urządzenie? Jego koncepcja pochodzi od rozwiązań, w których umieszczano barierę pomiędzy czymś niebezpiecznym, takim jak maszyna o dużej mocy, a czymś, co ma być za jej pomocą chronione, na przykład biurem. Jako rozwiązanie stosowane w sieciach komputerowych urządzenie takie umieszczane jest pomiędzy niebezpiecznym światem zewnętrznym a siecią wewnętrzną firmy. Pozwala ono na zdefiniowanie zestawu reguł, które określają, jaki rodzaj transmisji może, a jaki nie powinien, zostać przepuszczony przez ścianę ogniową i w którym kierunku może następować dany rodzaj transmisji.

Częściowo w związku z tym, że ściany ogniowe są tak popularne, łatwo jest zapomnieć o ich wadach. Największą z nich jest fakt, że takie urządzenie jest wąskim gardłem sieci. Choć utrata osiągów może być do pewnego poziomu uzasadniona ze względów bezpieczeństwa, to może się okazać, iż osiągi spadają poniżej minimalnej wartości, jaką jesteś w stanie zaakceptować. Szybka analiza każdego pojedynczego pakietu dokonywana przed przesłaniem go w którąkolwiek stronę przez ścianę ogniową wymaga dość szybkiego procesora. Choć ruter dokonuje zwykle takiej samej analizy, to nie zagląda on zbyt głęboko do wnętrza pakietu, lecz posługuje się zawartym w nim adresem docelowym. Procesor urządzenia tworzącego ścianę ogniową musi obsłużyć trochę dokładniejszą analizę pakietu. Drugim problemem jest to, że urządzenie takie można dość łatwo źle skonfigurować i pozostawić w nim szerokie przejście, które z łatwością wykorzysta intruz. Takie błędy w konfiguracji wyglądają trochę jak umieszczanie krat i zasuw we wszystkich drzwiach, stawiane uzbrojonej straży przy wszystkich drzwiach i przypadkowe pozostawienie szeroko otwartego okna. Oczywiście każde z urządzeń może być źle skonfigurowane, ale wpływ błędnej konfiguracji głównego urządzenia zabezpieczającego sieć może przynieść niespodziewane straty - zwłaszcza jeśli urządzenie to będzie dawało nadal fałszywe poczucie bezpieczeństwa. Każde urządzenie tego typu, które instalujesz, musi być proste w obsłudze, konfiguracji i procesie utrzymania i nadal gwarantować pewien wymagany w sieci poziom elastyczności. Po trzecie, ograniczenia nakładane przez ścianę ogniową mogą być zbyt duże. W zależności od tego, jak elastyczne są opcje konfiguracji, przy ich stosowaniu zezwolenie na pewną klasę usług przy jednoczesnym blokowaniu innej klasy może się okazać niemożliwe. Jeśli urządzenie takie jest zbyt restrykcyjne, Ty i użytkownicy zaczniecie szukać sposobów obejścia tych ograniczeń, co może doprowadzić do zmiany konfiguracji urządzenia kosztem zmniejszenia ogólnego poziomu zabezpieczenia sieci. Zanim zdecydujesz się na jego zastosowanie, powinieneś dokładnie przetestować każdy system ściany ogniowej i upewnić się, czy jest on na tyle elastyczny, aby zapewniał możliwość bardzo dokładnego określania reguł kontroli dostępu.

Kontrola dostępu

Wymienione wyżej wady mogą sprawić, że stwierdzisz, iż ściana ogniowa to kiepskie rozwiązanie. Nie jest to prawda. Jeśli dobrze zrozumiesz możliwości tego urządzenia i zaplanujesz konfigurację zabezpieczenia wykorzystującego je, to może stanowić ono wartościowy element systemu zabezpieczeń, jakim dysponujesz w sieci. Aby uniknąć lub ograniczyć wpływ wad tego urządzenia na pracę sieci, powinieneś po prostu zrozumieć sposób jego pracy; jego wady i zalety.

Rysunek 10-1 pokazuje typową konfigurację ściany ogniowej.* Zaczynając od lewej strony widzimy fizyczne łącze ze światem zewnętrznym, które jest dołączone do rutera brzegowego. Ten ruter może znajdować się pod kontrolą administratora sieci lokalnej lub może być obsługiwany przez inną organizację, taką jak ISP. Komunikacja przechodząca przez ten ruter nie podlega zwykle żadnym zabezpieczeniom.



Rysunek 10-1: Typowa konfiguracja ściany ogniowej

Tradycyjna sieć LAN, taka jak Ethernet, jest dołączona do rutera brzegowego. Jest ona określana jako strefa zdemilitaryzowana (DZM). Z punktu widzenia sieci lokalnej strefa DMZ traktowana jest jako część świata zewnętrznego; istnieje ona po to, by obsługiwać przyłączenie kolejnych komponentów, takich jak *bastion host,* który obsługuje zewnętrzne połączenia dla usług typu e-mail, WWW, FTP itd. Z punktu widzenia sieci lokalnych hosty te mają średni poziom ufności; są one administrowane lokalnie, ale nie są chronione przez ścianę ogniową i dlatego nie mogą być uważane za całkowicie bezpieczne. Najlepszym rozwiązaniem jest stosowanie oddzielnego hosta tego typu dla każdej z zewnętrznych usług. Takie rozwiązanie pozwala oddzielić problemy zabezpieczenia jednej usługi od pozostałych. Hosty tego typu nie powinny pozwalać na logowanie się w sieci, lecz powinny być zarządzane z bezpośrednio dołączonych do nich konsol lub przez łącza szeregowe. Dzięki wyeliminowaniu możliwości uzyskania dostępu do tych hostów przez sieć, możliwe jest stosowanie wyraźniejszych i prostszych zasad bezpieczeństwa, które łatwiej jest weryfikować.

* Więcej informacji na temat tworzenia zabezpieczeń z wykorzystaniem ścian ogniowych znajdziesz w książce „Building Internet Firewalls" autorstwa D. Brent Chapman i Elizabeth D. Zwicky (O'Reilly)

Dlaczego konieczne jest stosowanie takich hostów, dołączonych w strefie zdemilitaryzowanej? Dlaczego nie zezwolić na przepływ strumienia danych, generowanego przez daną usługę przez ścianę ogniową, do serwera który będzie chroniony przez tę ścianę? Hosty takie działają jak rodzaj serwera proxy, który w pewien sposób zabezpiecza komunikację ze światem zewnętrznym. Na przykład, dziury w zabezpieczeniach znajdowane są regularnie w demonie pocztowym systemu UNIX znanym pod nazwą *sendmail.* Jeśli taki program uruchomiony jest na wszystkich hostach UNIX pracujących w sieci, a ściana ogniowa będzie przepuszczała do sieci ruch generowany przy bezpośrednim dostępie do tego demona z zewnątrz sieci, to zastanów się, jaki będziesz miał poziom zabezpieczenia swojej sieci LAN? Absolutnie żaden! Stosowana ściana ogniowa nie będzie w stanie odróżnić poprawnej wiadomości email przesyłanej do jednego z Twoich komputerów od ataku przeprowadzanego na jedną z dziur demona *sendmail.* Obie wiadomości pojawią się w sieci jako poprawne strumienie danych SMTP. Z tego powodu hosty dołączone do sieci w strefie zdemilitaryzowanej nie są tak ściśle chronione, gdyż zakłada się, że powinny być one bronione przez ich własną konfigurację. Być może nie będą one miały uruchomionego demona *sendmail,* przez co nie będą podatne na ten typ ataku (choć pewnie będą miały inne luki w zabezpieczeniach, wynikające z ich konfiguracji). Nawet jeśli tak jest, to i tak zniszczenie spowodowane atakiem wykorzystującym taką lukę będzie dotyczyło jednego hosta, a nie kilku pracujących w chronionej sieci. Ponieważ dany host może być przeznaczony tylko do obsługi poczty elektronicznej, to można z niego usunąć wszystkie inne programy i demony, które z tą funkcją nie mają wiele wspólnego. Maszyna taka nie potrzebuje prawdopodobnie żadnych kompilatorów, obsługi klienta ani serwera Telnet, klienta i serwera FTP i tak dalej. Kiedy intruzowi uda się dostać na tę maszynę, nie będzie mógł na niej zbyt dużo zrobić.

Oczywiście taki wydzielony system obsługi poczty elektronicznej nadal powinien bezpiecznie przesyłać pocztę przez ścianę ogniową do wnętrza chronionej sieci. Jest wiele sposobów, aby to zrobić, każdy z nich zależy od tego, jak bardzo zależy Ci na szczegółach zabezpieczeń. Możliwe jest skonfigurowanie ściany ogniowej w taki sposób, aby przepuszczała połączenia SMTP do i z serwera obsługi poczty; w sieci chronionej możliwe jest skonfigurowanie serwera poczty elektronicznej, który się będzie zajmował jej wymianą z hostem umieszczonym w DMZ. Możliwe jest również rozwiązanie, w którym host obsługujący pocztę będzie ją przetrzymywał do czasu, aż nie zostanie z nim nawiązane połączenie z sieci chronionej, i serwer będzie mógł wtedy wymienić pocztę ze swoim odpowiednikiem pracującym w chronionej sieci. Takie podejście jest znacznie bezpieczniejsze, ponieważ *host bastion* nie może sam inicjować połączeń do wnętrza sieci, lecz musi czekać, aż takie połączenie zostanie zainicjowane z sieci chronionej. Oczywiście taka konfiguracja jest trochę trudniejsza do zrealizowania. W obu przypadkach ograniczono ruch przechodzący przez ścianę ogniową do dokładnie określonych adresów hostów, które mogą nawiązywać połączenia, co pozwala na ich dokładne monitorowanie. Dzięki temu możesz się skupić na kontrolowaniu zabezpieczeń tylko na hostach, które mogą zestawiać wymienione wyżej połączenia. Zastosowanie takiego układu podwójnych serwerów pozwala na stworzenie zaworu bezpieczeństwa, który zapobiega penetrowaniu luk z zewnątrz w systemie zabezpieczeń oprogramowania poczty na hostach w sieci przez użytkowników spoza tej sieci, co prowadzi z reguły do przełamania zabezpieczeń tych hostów.

Podobną konfigurację systemów można stworzyć dla usług takich jak Telnet, FTP, WWW. Każda usługa (idealnie) powinna korzystać z oddzielnego hosta typu *bastion, aby* problemy z bezpieczeństwem jednej z usług nie miały wpływu na pozostałe usługi.

Posuwając się na naszym rysunku w prawo, dochodzimy do samego urządzenia pełniącego funkcję ściany ogniowej. Może być to dedykowane urządzenie specjalnego zastosowania wyposażone w dwa interfejsy sieciowe lub więcej, które można programować w taki sposób, aby przepuszczało określone pakiety na podstawie kryteriów takich, jak adres IP źródłowy i docelowy, protokoły transportowe lub porty źródłowe TCP lub UDP i porty docelowe. Urządzenia specjalnie opracowane do pełnienia takich funkcji mają wiele zalet, które ujawniają się po dokładniejszym przyjrzeniu się ich pracy. Podobnie jak w przypadku dedykowanych ruterów, odpowiednia budowa pozwala tym urządzeniom skupić działanie na wypełnianiu tego jednego zadania. Dzięki temu dedykowane urządzenia, pracujące jako ściana ogniowa, są trudniejsze do spenetrowania od innych (na przykład rozwiązań programowych). Trzeba podkreślić, że luki w konfiguraqi tego typu urządzeń dedykowanych nie są tak powszechnie znane jak na przykład luki w zabezpieczeniach systemów operacyjnych. Choć stwierdzenie „zabezpieczanie przez zaciemnianie" nie zawsze jest najlepszym określeniem stosowanym dla funkcji pełnionych przez administratora, to trochę zaciemnienia nie zaszkodzi. Oczywiście sprawia to, że trudniej będzie Tobie i innym administratorom sieci obsługiwać to niezwykle istotne dla pracy systemu urządzenie, ponieważ jest to następne urządzenie, które ma własny język konfiguracji.

Inną opcją, na podstawie której można zbudować ścianę ogniową, jest wykorzystanie platformy sprzętowej ogólnego zastosowania, wyposażonej w wiele interfejsów. W takim komputerze należy wykorzystać specjalne oprogramowanie, które obsługuje funkcje filtrowania pakietów, podobnie jak dedykowane urządzenie opisywane wcześniej. Zaletą takiego rozwiązania jest to, że dzięki wykorzystywaniu typowego sprzętu całe urządzenie będzie łatwiej przyswajalne dla Ciebie i Twoich pracowników, co wiąże się z łatwiejszym zarządzaniem. Ponadto w miarę potrzeb możliwe jest przyspieszenie obsługi pakietów poprzez zainstalowanie oprogramowania na szybszej maszynie, bez konieczności czekania, aż producent dedykowanych urządzeń wypuści nowy model.

Trzecim typem ściany ogniowej, stosowanym najczęściej, jest wykorzystanie dedykowanego rutera, który wykorzystuje specjalne funkcje bezpieczeństwa. Bardzo często zdarza się, że masz już taki ruter, co oznacza, że obsługę filtrowania pakietów uzyskujesz niejako „za darmo". Niestety, takie rozwiązanie jest zwykle najmniej elastyczne i uważa się je za najgorsze z możliwych. Zadaniem rutera jest przełączanie pakietów i każde filtrowanie ma duży wpływ na jego osiągi. Możliwe również, że filtrowanie pakietów wpłynie na obsługę pakietów pomiędzy dwoma segmentami sieci wewnętrznej, które wcale nie są przesyłane przez skonfigurowaną na tym ruterze ścianę ogniową. Sprzęt dostarczany przez jednego z producentów ruterów ma kilka możliwych funkcji obsługi przełączanych pakietów, które mogą być wybrane w procesie konfiguracji systemu obsługującego ruter. Najlepsze osiągi można uzyskać stosując specjalne akceleratory sprzętowe i bufory pozwalające na osiągnięcie doskonałych wyników przełączania pakietów, które osiąga wartość 200000 pakietów na sekundę.

Niestety, te zaawansowane metody przełączania nie mogą być wykorzystywane, kiedy stosujemy na ruterze skomplikowane filtry pakietów.* Kiedy użyjemy zaawansowanych funkcji filtrowania, cała obsługa pakietów przechodzi przez CPU rutera i nie jest wspomagana akceleratorami sprzętowymi, co powoduje degradację osiągów do około 20000 pakietów na sekundę. Choć taka degradacja osiągów może dotyczyć jedynie pakietów, które muszą być przetworzone przez filtry, to należy pamiętać, że są takie filtry, które powodują że *wszystkie* pakiety przełączane przez ruter będą obsługiwane przez wolniejszy tryb pracy.

Podstawowy wpływ na pracę wykonywaną przez ruter, a nie związaną z filtrowaniem przetwarzania pakietów, to jeden z powodów, dla których ściana ogniowa powinna być skonfigurowana na ruterze, który obsługuje tylko te funkcje i nie zajmuje się niczym innym. Powinieneś starać się też, aby konfiguracja takiego systemu była jak najmniej skomplikowana. Prosty system bezpieczeństwa znacznie łatwiej się weryfikuje. Jeśli Twój system ściany ogniowej pracuje na hoście, który jednocześnie obsługuje pocztę elektroniczną, to czy możesz z całą pewnością stwierdzić, że demon pocztowy nie ma żadnych luk w zabezpieczeniach? Intruz może przecież wykorzystać obsługę poczty, by dostać się do konfiguracji ściany ogniowej i zmienić zabezpieczenia. Wszystkie pozostałe serwisy powinny być uruchamiane tylko na dedykowanych hostach.

Nawet jeśli korzystasz z dedykowanych hostów, które obsługują różne usługi sieciowe i pracują w DMZ, to nadal nie jesteś w pełni zabezpieczony. Przypomnij sobie, że w zależności od konfiguracji dedykowany host może być w stanie zainicjować połączenie z dowolnym hostem znajdującym się po drugiej stronie ściany ogniowej. Niezależnie od tego, jak dobre jest oprogramowanie obsługujące ścianę ogniową, większość jego decyzji jest podejmowana na podstawie adresu IP hostów, które się ze sobą komunikują. Nie jest to idealne rozwiązanie, ponieważ oprogramowanie to pobiera adres IP z pakietu, który przetwarza, a wcale nie ma pewności, że nadawca tego pakietu mówi prawdę. IPv6 zabezpiecza się przed podmienianiem adresów w pakietach dzięki umieszczaniu cyfrowego podpisu, przez co odbiorca ma pewność, że tylko jedna maszyna mogła nadać taki pakiet. W IPv4 nie ma takiego mechanizmu, przez co protokół jest podatny na ataki typu *spoofing.* Co się będzie działo, jeśli intruz wyśle pakiet twierdzący, że nadesłano go z wydzielonego hosta? Czy Twoja ściana ogniowa będzie w stanie wykryć, że jest to pakiet oszukany i odrzucić go? Możliwe że tak, jeśli w konfiguracji ściany ogniowej podejmiesz odpowiednie środki ostrożności, ale w omawianym przypadku środki ostrożności powinny być konfigurowane na ruterze brzegowym.

*Za pomocą akceleratorów można obsługiwać tylko niektóre filtry podstawowe, co powoduje tylko niewielkie obniżenie osiągów. Te filtry są jednak naprawdę bardzo proste i nie mogą obsługiwać zadań filtrowania.

Kontrola dostępu

Aby uchronić się przed atakiem typu *spoofing,* możesz skonfigurować swój ruter brzegowy tak, by odrzucał wszystkie pakiety nadsyłane ze świata zewnętrznego, zawierające adres jednego z wydzielonych hostów znajdujących się w DMZ. Dzięki takiej konfiguracji próby przesłania pakietów zawierających *spoofing* nigdy nie zakończą się dotarciem pakietów do ściany ogniowej, która mogłaby je przepuścić jako pakiety pochodzące od hostów, którym ufamy. Takie filtrowanie pakietów na ruterze jest dość łatwo skonfigurować. W systemie Cisco IOS konieczne jest dodanie kilku poleceń do konfiguracji rutera brzegowego *Zwróć* uwagę, że s e r i a l 0 jest interfejsem, który obsługuje łącze ze światem zewnętrznym, a ethernet 0 obsługuje segment Ethernet będący strefą DMZ.

```
! our connection to the outside world - make sure that no one can
 ! masquerade as one of our bastion hosts on the DMZ from outside

 interface serial 0
  description Link to the Internet
  ip address 10.1.1.1 255.255.255.0
ip access-group 1 in
!
interface ethernet 0
description Connection to DMZ network
  ip address 192.168.1.1 255.255.255.0 i
! define an access-list that blocks addresses from our DMZ network
access-list 1 deny    192.168.1.0      0.0.0.255
access-list 1 permit 0.0.0.0           255.255.255.255
```

Lista dostępu nie pozwala na przejście do naszej sieci pakietów, których adresem źródłowym jest adres hostów ze strefy DMZ, pozwalając jednocześnie na przesłanie wszystkich pozostałych pakietów. Przypisując tę listę do filtra pakietów przychodzących na interfejsie szeregowym mówimy ruterowi, że ma odrzucić każdy pakiet, który udaje, że pochodzi od któregoś z wydzielonych hostów. Dzięki takiemu zabezpieczeniu konfiguracja ściany ogniowej nie musi uwzględniać oceny pakietów, które udają, że nadesłane są przez serwery pracujące w strefie DMZ.

Kiedy już stworzysz wyraźną granicę pomiędzy siecią wewnętrzną a hostami wydzielonymi do obsługi specjalnych zadań, nie ma potrzeby, abyś do adresowania hostów z sieci wewnętrznej używał adresów IP, które są ogólnie dostępne. Czyż to nie ściana ogniowa miała chronić Twoją sieć przed bezpośrednimi połączeniami ze światem zewnętrznym? Jedynymi hostami, do których powinien istnieć dostęp ze świata zewnętrznego, są wydzielone serwery. Dlatego też możesz zastanowić się nad użyciem w sieci wewnętrznej adresów prywatnych określonych w dokumencie RFC 1918. Takie rozwiązanie będzie miało dwie zalety: po pierwsze, pozwoli na zaoszczędzenie adresów sieci Internet, a po drugie, zapewni dodatkowe bezpieczeństwo hostom pracującym w sieci wewnętrznej. Użycie adresów prywatnych sprawia, że ewentualny intruz będzie miał utrudniony dostęp do maszyn w sieci, ponieważ ich adresy nie mają żadnego znaczenia poza Twoją siecią. Jeśli upewnisz się, że Twoja ściana ogniowa, hosty wydzielone i ruter brzegowy nie obsługują rutowania źródłowego IP, to maszyny pracujące wewnątrz sieci będą praktycznie nieosiągalne z zewnątrz w sposób bezpośredni, nawet jeśli ściana ogniowa ulegnie uszkodzeniu.

Aby wyłączyć nitowanie źródłowe, należy w konfiguracji Cisco dodać następujące polecenie:

```
no ip source-route
```

Czy zabezpieczenia hostów są rzeczywiście konieczne?

Jednym z powodów, dla których ludzie tak lubią ściany ogniowe zabezpieczające sieć i inne urządzenia, które obsługują całą sieć, jest to, że wydaje im się, iż mogą przestać zajmować się zabezpieczaniem hostów, skoro zabezpieczyli sieć jako całość. Powodem takiego podejścia do bezpieczeństwa sieci jest fakt, że znacznie łatwiej utrzymywać pojedyncze urządzenie pełniące funkcję ściany ogniowej i kilka publicznie dostępnych (zewnętrznych) maszyn w stanie wysokiego stopnia zabezpieczenia niż tysiąc lub więcej maszyn pracujących wewnątrz sieci. Takie podejście jest właściwe, ale jednocześnie popełnia się w nim jeden duży błąd.

Większość ogólnego bezpieczeństwa sieci powinna być osiągana przez odpowiednie zabezpieczenie hostów. Jeśli administratorzy hostów będą zakładali, że to ściana ogniowa powinna chronić ich hosty przed naruszaniem praw dostępu, to się bardzo mylą. Hosty powinny chronić się przed dostępem intruzów z zewnątrz tak samo, jak chronią się przed próbą dostępu z sieci wewnętrznej, albo jeszcze bardziej. Sieć może jedynie pomagać w zabezpieczeniu hostów, ale na pewno nie jest w stanie zastąpić systemu zabezpieczeń. Ochrona granic sieci przy jednoczesnym ignorowaniu zabezpieczeń stosowanych wewnątrz sieci sprawia, że podobna jest ona do twardego cukierka z miękkim nadzieniem. Kiedy zewnętrzna skorupa zostanie przełamana, to, co było w środku, po prostu wycieka na zewnątrz. Zastanów się, co będzie się działo, jeśli intruz przedrze się przez ścianę ogniową: będzie mógł łatwo przechodzić z maszyny na maszynę powodując ich uszkodzenia, utratę ważnych danych i przerwy w pracy systemu. Gdyby hosty pracujące w sieci zapewniały dodatkowe własne zabezpieczenia, to powodowane przez intruza zniszczenia mogłyby dotknąć mniejszą liczbę tych hostów i nie rozprzestrzeniać się w sieci.

Ściana ogniowa nie pomoże Ci również chronić sieci przed działaniami własnych użytkowników prowadzonymi z wnętrza sieci. Badania wykazują, że ponad 90 procent budżetu firm wydawanego na zabezpieczenia idzie na zabezpieczenie sieci przed dostępem z zewnątrz, podczas gdy 90 procent zniszczeń powodowanych jest przez pracowników i innych użytkowników prowadzących działania z wnętrza sieci. Choć znacznie łatwiej podejmować działania przeciwko własnym użytkownikom już po fakcie, to niestety uszkodzenie danych lub inne zaburzenia przecież już wystąpiły. Ponadto użytkownicy z wewnątrz często powodują problemy przez swoją ignorancję, a nie przez złośliwość. Dobre zabezpieczanie hostów pomaga uchronić się przed wpływem takich błędów, a także zamierzonych działań będących atakami na system zabezpieczeń sieci.

Na zakończenie należy jeszcze wspomnieć o tym, co się dzieje, kiedy użytkownik instaluje nieautoryzowany modem, przyłączając go do swojej stacji roboczej po to, by omijając ścianę ogniową mieć dostęp do tej stacji z domu. Taka dziura w zabezpieczeniach pozostaje niewykryta, aż do czasu, kiedy intruz znajdzie ją i w bardzo łatwy sposób uzyska dostęp do chronionej części sieci.

Kiedy zastanawiasz się nad potencjalnymi zagrożeniami bezpieczeństwa systemu wewnętrznego to odpowiedź na pytanie „Czy zabezpieczanie hostów jest nadal ważne, skoro mam ścianę ogniową?" brzmi „Tak!". Ściana ogniowa powinna być częścią większego systemu zabezpieczeń, a nie tylko jedynym zabezpieczeniem, jakiego używasz w sieci. Wszystkie hosty muszą brać na siebie ochronę własnego bezpieczeństwa. Co więc możesz zrobić? Zabezpieczenia hostów to temat wykraczający poza zakres tej książki, ale dostępnych jest wiele doskonałych książek opisujących te tematy, m.in. *Practical Unix and Internet Security, 2nd Edition* napisana przez Simsona Garfinkela i Gene Spafford (O'Reilly). Powinieneś zawsze pamiętać o kilku podstawowych sprawach, które przedstawiam poniżej.

- Instaluj wszystkie poprawki dotyczące bezpieczeństwa systemu, które są dostarczane przez producenta. Jest to jeden z najpewniejszych sposobów ochrony systemu. W momencie, kiedy producent wypuszcza poprawkę, to potencjalny intruz też o niej wie i może wykorzystać błąd systemu, którego nie załatałeś, spóźniając się z zainstalowaniem tej poprawki. Jeśli nie uaktualniasz swojego systemu o pojawiające się poprawki, to sam decydujesz o tym, że staniesz się potencjalnym celem ataków.
- Wyłącz wszelkie usługi, których obsługa nie jest konieczna. Na przykład stacja robocza UNIX nigdy nie będzie musiała odbierać poczty elektronicznej przesyłanej z innego hosta, prawdopodobnie dlatego, że cała poczta odbierana jest centralnie i dlatego nie ma powodu, abyś na stacji roboczej miał uruchomionego demona poczty. Wyłączenie tych nieużywanych usług pozwala wyeliminować luki w zabezpieczeniach systemu, które mogą być ukryte w tych usługach.
- Skonfiguruj maszyny tak, aby pozwalały na dostęp innych maszyn tylko wtedy, kiedy ich adresy są poprawnie zarejestrowane w DNS. „Poprawnie zarejestrowane" oznacza, że kiedy próbujesz rozwikłać nazwę hosta na jego adres IP i odwrotnie, to w obu przypadkach dostajesz ten sam adres IP lub listę adresów, na której ten adres się znajduje. Wymaganie dotyczące poprawnego zarejestrowania adresu hosta zmniejsza prawdopodobieństwo dokonania włamania do hostów z nielegalnie dołączonego do sieci urządzenia.
- Stosuj bezpieczny system haseł. Zachęcaj użytkowników (lub -jeśli to konieczne -zmuszaj ich do tego), aby wybierali dobre hasła i zmieniali je regularnie. Wytłumacz im potrzebę utrzymywania swoich haseł w tajemnicy i tego, że powinni zwracać się do administratorów za każdym razem, kiedy wydaje się im, że ich hasło zostało ujawnione i wykorzystane przez kogoś innego. Podkradanie haseł użytkowników jest nadal jednym z najszybszych i najwygodniejszych sposobów przeprowadzenia ataku. Zastanów się nad zasadnością wprowadzenia w firmie systemu haseł jednokrotnych opartych o karty elektroniczne, co jest najlepszym sposobem zabezpieczenia się przed podsłuchem prowadzącym do uzyskania poprawnego hasła. Przeanalizuj systemy takie jak Kerberos (z MIT), które wykonują autentykację bez przesyłania hasła przez sieć.

- Dokonuj regularnych audytów systemów używanych w sieci. Konieczne jest do tego poprawne skonfigurowanie tych systemów tak, aby zapisywały w plikach rejestrów wszystkie zdarzenia, które zdefiniowałeś jako ważne. Jako minimalną liczbę informacji systemy powinny zapisywać czas załogowania i wylogowania użytkownika oraz wykonania działań, które wymagają specjalnych przywilejów. Ponadto może się okazać przydatne skonfigurowanie jednej maszyny, na której zapisywane będą wszystkie próby uzyskania dostępu do sieci, niezależnie od tego, czy zakończyły się one powodzeniem, czy też nie. Kiedyś wyśledziłem studenta, który sprawdzał zabezpieczenie mojej sieci, korelując ciekawe formy nieudanych prób dostępu na kilku maszynach w sieci. Nawet jeśli takie audyty nie uchronią Cię przed włamaniem, dadzą Ci dowody na to, że włamanie takie miało miejsce, oraz kto go dokonał i co zrobił. Dane te mogą być szczególnie przydatne, jeśli konieczna będzie naprawa uszkodzeń, jakich dokonał intruz, lub kiedy podejmiesz działania prawne zmierzające do ukarania tego intruza.

Ochrona dostępu do rutera

Wszystkie hosty pracujące w sieci muszą się chronić - nie mogą polegać wyłącznie na sieci, zakładając, że obroni je ona przed nieuprawnionym dostępem. Jeśli Twoje urządzenia sieciowe mogą być zarządzane przez sieć za pomocą Telnet, SNMP, HTTP lub inną metodą, to należy je traktować tak samo jak hosty; muszą się one same bronić przed atakiem. Może nie myślisz o ruterze jako o potencjalnym celu ataków; przecież rutery nie zawierają żadnych ważnych danych. To jednak duży błąd. Oto, co może zrobić intruz, któremu uda się przejąć kontrolę nad Twoim ruterem:

- przebić dziury w konfiguracjach ścian ogniowych opartych na ruterach;
- przerwać poprawne działanie sieci;
- podjąć próbę ataku na inne maszyny używając klienta Telnet z rutera;
- wysyłać kopię każdego pakietu (lub tylko tych, które uzna za *interesujące)* na adres jakiejś maszyny, w której będzie je następnie analizował.

Pierwszy punkt może być jedną z większych wad systemu ściany ogniowej. Jeśli sama ściana ogniowa nie jest odporna na atak, to nie można gwarantować bezpieczeństwa całej sieci, którą ta ściana chroni. Jeśli stosowana przez Ciebie ściana ogniowa działa opierając się na filtrowaniu pakietów wykonywanym przez ruter, to ochrona tego rutera jest bezwzględnie konieczna. Drugi z wymienionych punktów powinien równie mocno interesować administratora sieci, może nawet bardziej niż punkt pierwszy. Co się stanie, jeśli intruz przejmie kontrolę nad Twoim ruterem znajdującym się w oddziale firmy, przerwie połączenie z centralą i zmieni hasło rutera? Będziesz miał wtedy sytuacja krytyczną, do której w żadnym wypadku nie powinno dojść. Sytuacja ta spowoduje straty finansowe firmy i będzie trwała do czasu, aż ktoś znajdujący się przy ruterze nie odzyska nad nim kontroli. Oczywiste jest, że takiego przypadku nie wolno tolerować.

Kontrola dostępu

Trzecia i czwarta możliwość to najpoważniejsze przypadki. Twój ruter jest prawdopodobnie traktowany jako wewnętrzny host, z punktu widzenia kontroli zabezpieczeń i może mieć łatwy dostęp do najbardziej wrażliwych systemów pracujących w sieci. Nawet jeśli tak nie jest, to przejmując kontrolę nad ruterem intruz może zamaskować się i - udając host o większym zaufaniu - uzyskać dostęp do innych systemów pracujących w całej organizacji, czasem nawet bez sprawdzania haseł i przechodzenia przez zabezpieczenia. Jeśli nie chronisz ruterów, dajesz intruzowi doskonałą okazję do spowodowania większych zniszczeń w sieci. Choć podsłuchiwanie ruchu w sieci lokalnej z dużej odległości nie jest możliwe, to jeśli intruz potrafi skonfigurować ruter tak, by przesyłał kopie pakietów z sieci lokalnej na inny adres systemy, gdzie dopiero zostaną one przeanalizowane, to możliwe będzie odkrycie haseł, informacji o opracowywanych w Twojej firmie projektach lub innych danych, które były przesyłane w sieci lokalnej. Możliwości założenia takiego podsłuchu ograniczone są jedynie umiejętnościami intruza i możliwościami stosowanych w Twojej sieci ruterów; zdaje się, że wybrałeś rutery o sporych możliwościach, nieprawdaż?

W przeciwieństwie do zapewniania wysokiego poziomu bezpieczeństwa systemom pracującym z podziałem czasu, zabezpieczanie rutera nie jest takie proste. To, co możesz zrobić z takim urządzeniem, jest ograniczone możliwościami zaimplementowanymi w nim przez dostawcę sprzętu; nie możesz uruchomić własnego oprogramowania zabezpieczającego wraz z oprogramowaniem obsługującym rutowanie pakietów. Zwykle dostęp do takiego urządzenia jest chroniony hasłem, ale należy pamiętać, że hasła są bezpieczne tylko wtedy, gdy nie można ich odgadnąć. Rzadko możliwa jest zamiana takiego systemu haseł na coś, co będzie bezpieczniejsze. Możesz np. ograniczyć dostęp do rutera z małej podsieci działającej wewnątrz sieci. Najlepiej, jeśli ruter dostępny będzie jedynie ze stacji roboczych personelu i ze stacji zarządzającej siecią. Jest to możliwe do wykonania przy użyciu możliwości filtrowania pakietów oferowanych przez ruter. Jeśli na przykład Twoi pracownicy mają stacje robocze pracujące w sieci 172.16.24.0/24 i są to jedyne maszyny pracujące w tej sieci, to możliwe jest skonfigurowanie Cisco IOS tak, by dostęp do rutera przez Telnet ograniczony był do tej sieci. Wykonuje się to poleceniem:

```
access-list 1 permit 172.16.24.0 0.0.0.255
!
line vty 0 4
 access-class 1 in
```

Taka konfiguracja informuje ruter, że wszelkie próby uzyskania dostępu do terminali wirtualnych (wykorzystywanych przez Telnet) o numerach od O do 4 muszą pochodzić od adresów źródłowych, które spełniają ograniczenia listy dostępu numer 1. Choć nadal możliwe jest wykonanie ataku na ruter za pomocą metody *address spoofing,* to posługując się listą dostępu obronisz się przed sporą liczbą intruzów. A propos, powinieneś upewnić się, że zastosowałeś tę samą listę dostępu dla wszystkich terminali wirtualnych na danym ruterze. Nie możesz przewidzieć, który z nich zostanie użyty do obsługi sesji Telnet nawiązywanej przez sieć.

Podobne zabezpieczenia można stosować w innym sprzęcie sieciowym.

Zastanów się również nad możliwością wykorzystania funkcji filtrowania pakietów obsługiwanej przez rutery dla kontroli dostępu do urządzeń, które nie mają takiej funkcji. Jako przykład takiej ochrony wykonywanej przez urządzenia trzecie w mojej sieci może służyć ochrona posiadanych przeze mnie przełączników, które nie są w stanie blokować niechcianych połączeń Telnet. Ponieważ mogę umieścić ich karty zarządzania w jednej podsieci IP, to mogę skorzystać z prostej listy dostępu założonej na interfejsie rutera, do którego dołączona jest ta podsieć. Takie rozwiązanie chroni wszystkie te przełączniki:

```
interface ethernet 0
 description Ethernet Switch Management Subnet
 ip address 172.16.243.1 255.255.255.0
 i

! define an access list that permits my network management subnet and
! my staff subnet access to the switches, routers, etc.
access-list 1 permit 172.16.11.0 0.0.0.255
access-list 1 permit 172.16.15.0 0.0.0.255
```

Lista kontroli dostępu zezwala na dostęp z sieci, w której pracują wszystkie moje hosty obsługujące zarządzanie siecią, a także z sieci, w której pracują stacje robocze personelu odpowiedzialnego za pracę sieci. Wszelkie inne próby uzyskania dostępu (włącznie z *ping)* są zabronione. Pamiętaj o tym, że choć użycie funkcji filtrowania pakietów przez ruter do ochrony tego rutera w niewielkim stopniu wpływa na jego osiągi (CPU tego rutera i tak przetwarza pakiety wysłane do rutera), to wykorzystanie tej funkcji do ochrony innych urządzeń może w dużym stopniu wpłynąć na osiągi.

Musisz również dokładnie przemyśleć, które maszyny powinny mieć dostęp do Twoich ruterów i innego sprzętu wykorzystywanego przez SNMP. Wersja I protokołu SNMP, która nadal jest powszechnie wykorzystywana, nie ma żadnych zabezpieczeń, a zabezpieczenia zastosowane w wersji 2 są uznane za niedoskonałe. Zezwolenie na czytanie lub zapis zmiennych konfiguracji systemu bazuje na sprawdzeniu prostego ciągu znaków, który dołączony jest do każdego zapytania i nie jest w żaden sposób zakodowany. Oznacza to, że jeśli korzystasz z protokołu SNMP do zarządzania posiadanym sprzętem sieciowym, powinieneś zastanowić się nad sposobami ograniczenia do minimum liczby hostów, które mają pozwolenie na zapis zmiennych, a ciągi znaków podawane jako *community string* powinny być chronione tak samo jak hasła. Liczbę maszyn, które mogą dokonywać zmian w konfiguracji ruterów, możesz ograniczyć za pomocą listy dostępu podobnej do tej, która została użyta do kontroli dostępu przez Telnet. Może to być nawet ta sama lista dostępu, która ograniczała dostęp przez Telnet:

```
! define the hosts permitted to make SNMP write requests to this router

access-list 1 permit 172.16.24.11  0.0.0.0

access-list 1 permit 172.16.131.57 0.0.0.0
```

Kontrola dostępu

```
! define all hosts in my network so I can restrict SNMP read requests,
! too
access-list 2 permit 172.16.0.0       0.0.255.255
i
!now apply the access lists to restrict SNMP access snmp-server
community secret RW 1 • • snmp-server community public RO 2
snmp-server trap-authentication snmp-server host
172.16.24.11 public
```

Po pierwsze, zabroniłem dostęp typu czytanie-zapis SNMP wszystkim maszynom oprócz dwóch. Jedną z nich będzie prawdopodobnie stacja zarządzania pracą sieci, a drugą prawdopodobnie Twoja stacja robocza, która jest zapasową stacją zarządzania. Należy ograniczyć do minimum listę maszyn, które mogą wysyłać zapytanie o zapis zmiennych SNMP. Po drugie, zabroniłem dostępu czytania zmiennych SNMP wszystkim oprócz hostów z sieci lokalnej. Choć może wydawać się to zbędne, to takie zabezpieczenie uniemożliwi intruzowi odczytanie pomocnych informacji o wewnętrznej strukturze sieci. Może to również ograniczyć działania „pomocnego" administratora, który - obserwując Twoją sieć z daleka - kieruje Twoim niedoświadczonym personelem i pomaga im usuwać problemy z siecią, których wcale nie ma.*

Niezależnie od tego, kto ma dostęp do Twoich ruterów poprzez SNMP i z jakimi przywilejami, powinieneś w konfiguracji umieścić polecenie, które w przypadku błędu autentykacji będzie generowało pułapkę SNMP wysyłaną na Twoją stację zarządzania. Taka konfiguracja pomoże Ci stwierdzić, że ktoś próbuje uzyskać dostęp do Twojego rutera przez SNMP pracując z niedozwolonego adresu lub posługując się niewłaściwym ciągiem znaków *community.* Nawet jeśli sam nie wykorzystujesz protokołu SNMP, powinieneś upewnić się, czy Twoje rutery i inne urządzenia sieciowe mają poprawną konfigurację tego protokołu lub czy obsługa SNMP, wykonana w tych urządzeniach została wyłączona. W mojej sieci regularnie znajdujemy koncentratory i przełączniki pracujące w sieciach działowych, które wykorzystują domyślną konfigurację SNMP, jaka jest wykonana w kupionym urządzeniu, co oznacza, że urządzenia te umożliwiają pełny dostęp po podaniu domyślnego, powszechnie znanego ciągu znaków. Zwykle takie wykryte sytuacje przekazujemy pracownikom tych działów, z prośbą o szybkie ich załatwienie, ale jeśli taką domyślną konfigurację znajdzie przed nami jakiś intruz, może ją wykorzystać.

Jeśli Twój ruter obsługuje inne mechanizmy pozwalające na zarządzanie jego pracą poprzez sieć, takie jak protokół HTTP, powinieneś ograniczyć dostęp również do nich. Niestety, system Cisco IOS nie obsługuje jeszcze tego samego poziomu kontroli dostępu do interfejsu konfiguracyjnego pracującego z wykorzystaniem HTTP. Dlatego lepiej wyłączyć obsługę tej funkcji, jeśli chcesz mieć pewność, że ruter jest bezpieczny i poczekać przynajmniej do czasu, kiedy Cisco wyposaży rutery w taki sam system kontroli dostępu, jaki zastosowano dla obsługi Telnet i SNMP.

*Tak, tak, to się zdarza.

Obsługa HTTP domyślnie jest wyłączona; jeśli ją włączyłeś lub chcesz upewnić się, czy jest wyłączona, powinieneś użyć w konfiguracji następującego polecenia:

```
no ip http server
```

Jeśli jednak poprzestaniesz na kontroli dostępu, to prosisz się o kłopoty. Powszechnie stosuje się rozwiązania polegające na tym, że pliki konfiguracyjne urządzeń przechowywane są w hostach w sieci i kopiowane do rutera lub innego urządzenia za pomocą protokołu TFTP. Takie rozwiązanie jest bardzo wygodne i w poprzednich rozdziałach nawet zalecałem ich stosowanie. Powinieneś jednak ostrożnie używać protokołu TFTP. Domyślnie pliki konfiguracyjne Cisco zawierają wszystkie hasła zapisane w postaci nie zakodowanego tekstu, a sam protokół TFTP nie obsługuje żadnej kontroli dostępu. Jeśli stwierdzisz, że tak jest w przypadku Twojego rutera, i wykorzystasz TFTP do skopiowania plików konfiguracyjnych, to powinieneś zastanowić się nad ewentualnym użyciem oprogramowania, które będzie kontrolowało dostęp do wspomnianych plików konfiguracyjnych na serwerze TFTP. Innym wyjściem jest zastosowanie jakiejś metody kodowania haseł proponowanej przez dostawcę sprzętu. Dodanie przedstawionego niżej polecenia do pliku konfiguracyjnego powoduje zakodowanie haseł przechowywanych z konfiguracji rutera:

```
service password-encryption
```

Wyświetlenie takiej konfiguracji powoduje pokazanie w niej zakodowanego hasła, które następnie wraz z resztą konfiguracji można umieścić w pliku na hoście TFTP i zabezpieczyć się przed możliwością zdobycia hasła przez intruza, który uzyskał dostęp do plików konfiguracyjnych przechowywanych na tym hoście. Należy pamiętać, że stosowane w takim przypadku kodowanie jest odwracalne, nie jest to więc metoda całkowicie bezpieczna. Aby włączyć funkcję własnego hasła (tego, które umożliwia uzyskanie uprzywilejowanego dostępu) należy użyć polecenia:

```
enable secret my-password
```

Schemat kodowania stosowany w takim przypadku jest nowszy i znacznie bardziej skomplikowany.

Lokalne hasła chroniące dostęp Telnet i dostęp do poleceń uprzywilejowanych mają również swoje wady. A oto niektóre z nich:

- Konieczne jest utrzymywanie haseł na wielu ruterach i jednoczesne uaktualnienie wszystkich przy dokonywaniu zmiany.
- Konieczne jest bezpieczne przekazywanie nowych haseł wszystkim użytkownikom, którzy mają się nimi posługiwać.
- Bardzo trudno określić różne poziomy dostępu różnym pracownikom.
- W sieci hasła te nadal przesyłane są w postaci tekstu.

Aby poradzić sobie z tymi problemami, Cisco IOS pozwala na zastosowanie kilku różnych metod służących do sprawdzania praw dostępu do rutera i do uprzywilejowanych poleceń w tym ruterze. W skrócie metody te są następujące:

Terminal Access Controller Access Control System (TACACS)

TAC ACS zapewnia scentralizowaną obsługę autentykacji haseł i minimalne funkcje obsługi kont użytkowników. Za każdym razem, kiedy użytkownik podejmuje jakieś działanie, ruter wysyła nazwę użytkownika i jego hasło do centralnego serwera. Serwer sprawdza w swojej bazie kontroli dostępu przesłane zapytanie i wysyła zgodę lub zakaz wykonanie danego działania. TACACS jest najstarszym mechanizmem kontroli zdalnego dostępu stosowanym przez Cisco i ma najwięcej ograniczeń spośród wszystkich stosowanych mechanizmów tego typu. Jeśli wykorzystujesz TACACS do kontroli dostępu do rutera, a także do kontroli dostępu do uprzywilejowanych poleceń, to każdy użytkownik, który ma dostęp do rutera, będzie miał również dostęp do poleceń konfiguracyjnych, ponieważ TACACS nie jest w stanie rozróżnić zapytań kierowanych do niego z prośbą o potwierdzenie prawa dostępu przy użyciu tych dwóch poziomów zabezpieczenia.

Extended TACACS *(XTACACS)*

XTACACS pomyślano jako sposób na poprawę niektórych ze znanych ograniczeń systemu TACACS, co realizowane jest poprzez bardziej szczegółowe informowanie serwera o podejmowanych przez użytkownika działaniach. Podczas gdy TACACS nie potrafi np. rozróżnić prób uzyskania dostępu do różnych poziomów funkcji rutera, to XTACACS potrafi dokonać takiego rozróżnienia. XTACACS zapewnia również większą liczbę informacji umieszczanych w plikach rejestrów, co pozwala na lepsze śledzenie podejmowanych przez użytkowników prób uzyskania dostępu i zbieranie danych o wykorzystaniu konta dostępowego.

TACACS+

TACACS+ jest częścią nowego modelu autentykacji stosowanego przez Cisco, którego pełna nazwa brzmi *Authentication, Authorization and Accounting (AAA)*. AAA tworzy środowisko, w którym pracuje kilka różnych protokołów zapewniających usługi wymagane przez rutery do autentykacji użytkowników, autoryzowania podejmowanych przez nich działań i zapisywania ich w plikach rejestrów. TACACS+ był pierwszym protokołem wbudowanym w system operacyjny obsługujący rutery i jest rozszerzeniem wcześniejszych wersji protokołów TACACS. W przeciwieństwie do systemów TACACS, TACACS+ koduje szczególnie ważne informacje przed przesłaniem ich przez sieć. Spośród wszystkich trzech wariantów TACACS ten ostami zapewnia największą elastyczność i najwyższy poziom kontroli, ale jest też najbardziej skomplikowany.

Remote Access Dial In User Services (RADIUS)

Podczas gdy oryginalne rozwiązanie protokołu TACACS było otwartym standardem stosowanym w sieci Internet, to późniejsze jego wersje tworzone przez Cisco sprawiły, że stał się on bardziej firmowym protokołem Cisco. RADIUS jest kolejną, podjętą przez społeczność Internetową, próbą opracowania protokołu kontrolującego zdalny dostęp, który będzie w stanie obsługiwać wszelkie typy zapytań o dostęp kierowane z sieci i będzie zapewniał odpowiedni poziom bezpieczeństwa.

Bezpieczeństwo protokołu RADIUS osiągnięte zostało przez zastosowanie szyfru, który znany jest zarówno klientowi, jak i serwerowi. Szyfr ten (w rzeczywistości to klucz, którym wykonywane jest kodowanie) jest wykorzystywany przez klienta i serwer do kodowania ważniejszych informacji przesyłanych w sieci, co uniemożliwia ich podsłuchiwanie. Choć nie jest to jeszcze w pełni standard sieci Internet, to obsługa protokołu RADIUS została już zaimplementowana w produktach wielu dostawców.

Kerberos wersja 5

Jako część projektu Athena na uniwersytecie MIT opracowano system autentykacji Kerberos. System Kerberos opracowano tak, że hasło nigdy nie jest w nim przesyłane przez sieć w postaci jawnego tekstu. Zamiast tego dla każdej operacji Kerberos generuje ciąg znaków *ticket,* który jest następnie szyfrowany przy użyciu prywatnego klucza użytkownika. Kiedy system klienta odbierze przesłaną mu zakodowaną informację, wykorzystuje do jej dekodowania klucz publiczny, który został wcześniej dostarczony przez tego użytkownika. Jeśli dekodowanie zakończy się pomyślnie, to użytkownik uzyskuje dostęp. Kerberos nie jest standardem sieci Internet, ale w wielu miejscach sieci znajdują się spore instalacje tego systemu, wykorzystywane do kontrolowania dostępu do maszyn wielodostępnych i do stacji roboczych, a także do pracujących w tych sieciach ruterów.

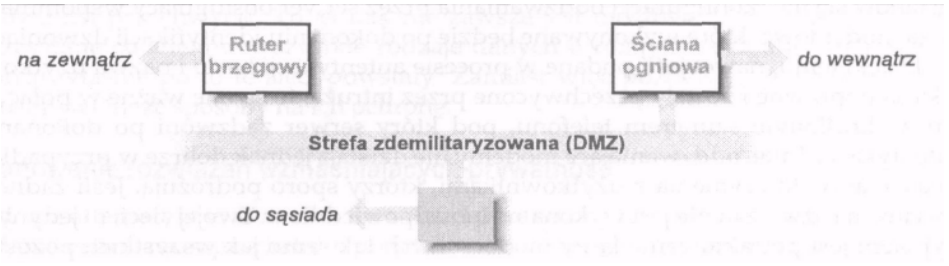
Niezależnie od tego, który z tych systemów wybierzesz, będziesz potrzebował odpowiedniego serwera do jego obsługi. Serwer ten może być zbudowany na podstawie systemu dostępnego na rynku lub możesz stworzyć go sam, co pozwoli Ci na stosowanie zaawansowanych technik zabezpieczeń, takich jak karty generujące jednorazowe hasła użytkowników. Konieczne jest wtedy stosowanie centralnego serwera. Dodatkową wadą takich zaawansowanych zabezpieczeń jest to, że w przypadku niedostępności tego serwera nie będziesz mógł dostać się do obsługiwanych przez Ciebie ruterów. Konieczne jest więc dobre wyważenie ryzyka stosowania zaawansowanych systemów i wybór zabezpieczeń najodpowiedniejszych dla danej sieci. Niestety, ponieważ szczegóły konfiguracji poszczególnych usług zdalnej autentykacji uzależnione są od wybranego przez Ciebie systemu i konkretnej implementacji, to zaprezentowanie konkretnych przykładów wykracza poza zakres tematyczny tej książki.

Efekt stosowania zewnętrznych połączeń

Prawie każdy zdaje sobie sprawę z tego, że połączenie z siecią Internet ma ogromny wpływ na bezpieczeństwo sieci lokalnej. Internet ma miliony użytkowników, z których każdy jest potencjalnym intruzem. Niestety, istnieją jeszcze inne niebezpieczeństwa związane z każdym rodzajem połączenia wychodzącego z Twojej sieci na zewnątrz. Zastanów się nad prywatnym łączem prowadzącym do innej organizacji. Łącze takie może stać się powodem obniżenia bezpieczeństwa sieci - spowodowanego na przykład przez atak jednego z użytkowników sąsiedniej sieci lub atak jakiegoś intruza, który do niej przeniknął. Częściej jednak takie łącze prywatne będzie ścieżką, po której w Twojej sieci będą się rozprzestrzeniały wirusy komputerowe.

Kontrola dostępu

To, że w sieci sąsiedniej organizacji pracuje mniej użytkowników niż w Internecie, nie znaczy, że powinieneś mniej uwagi zwracać na zabezpieczenie tego połączenia. Nie na wiele zda się zastosowanie ściany ogniowej chroniącej Twoją sieć od strony Internetu, skoro sieć sąsiednia ma tylne wejście do Twojej sieci i jednocześnie sama jest kiepsko zabezpieczona. Jeśli nie jesteś w stanie zapewnić tego samego stopnia ochrony wszystkim połączeniom zewnętrznym za pomocą ścian ogniowych, to powinieneś zastanowić się nad rozwiązaniem połączeń sieci sąsiadów do Twojej strefy DMZ, jak pokazano na rysunku 10-2.



Rysunek 10-2: Dołącz sieć sąsiedzką do DMZ, a nie bezpośrednio do swojej sieci

Główną wadą takiego połączenia jest to, że nie będziesz mógł nadać sieci sąsiedzkiej innego poziomu dostępu niż poziom, który zastosowałeś w stosunku do całego świata. Możliwość taka zależy od elastyczności zastosowanego systemu ściany ogniowej, ale jeśli chodzi o poziom zabezpieczeń, to dobrze jest dołączyć sąsiadów do tego samego miejsca, w którym dołączone są pozostałe łącza prowadzące z Twojej sieci w świat.

Najczęściej zapomina się jednak nie o zabezpieczeniach źródeł zagrożenia, jakimi są łącza stałe, lecz o łączach komutowanych. Pierwsze miejsce w źródłach naruszania zabezpieczeń mają komutowane łącza telefoniczne obsługiwane przez modemy. Często są one umieszczane w samym sercu sieci i mają niewielkie zabezpieczenia stosowane pomiędzy hostami, które je obsługują, a siecią. Kiedy zdasz sobie sprawę, że na świecie jest znacznie więcej maszyn wyposażonych w modem niż tych dołączonych bezpośrednio do Internetu, to powinieneś zrozumieć, dlaczego tego typu modemy są głównym problemem bezpieczeństwa sieci. W jednej ze znanych mi sieci podjęto zaawansowane działania zmierzające do ochrony pewnych ważnych maszyn przed możliwością dostępu z zewnątrz - z sieci publicznej, ale jednocześnie pozostawiono tam zestaw modemów, który obsługiwał pełny dostęp do tych maszyn bez żadnej autentykacji. W takim przypadku miejsca w sieci publicznej były mniej niebezpieczne dla tej sieci od wspomnianych modemów, ponieważ dostęp z sieci publicznej byłby przynajmniej za każdym razem odnotowany, co posłużyłoby za dowód takiej próby dostępu.

Aby zabezpieczyć się przed naruszeniem systemu zabezpieczeń stosowanego w sieci powinieneś stosować następujące zasady. Po pierwsze, *nigdy* nie pozwalaj na używa nie modemów dla uzyskania dostępu bez konieczności autentykacji. Jako minimum każ dodzwaniającemu się użytkownikowi identyfikować się przez podanie jego nazwy i hasła, nawet jeśli nigdy nie będą one weryfikowane. Takie podejście daje przynajmniej świadomość istnienia zabezpieczeń i może odstraszyć przypadkowych intruzów. Lepszym rozwiązaniem jest stosowanie serwera obsługującego takie połączenia modemowe, który jednocześnie sprawdza poprawność podanej nazwy użytkownika i hasła, przy zastosowaniu jednego z opisanych wcześniej protokołów autentykacji. Takie rozwiązanie może być jednak czasami niewystarczające. Jeśli tak jest, zastanów się nad konfiguracją oddzwaniania przez serwer obsługujący wspomniane łącza modemowe, które wykonywane będzie po dokonaniu identyfikacji dzwoniące go. Dzięki temu, nawet jeśli podane w procesie autentykacji hasło i nazwa użytkownika są poprawne i zostały przechwycone przez intruza, to są one ważne w połączeniu z określonym numerem telefonu, pod który serwer zadzwoni po dokonaniu autentykacji. Takie oddzwaniające modemy nie działają jednak dobrze w przypadku, kiedy mamy do czynienia z użytkownikami, którzy sporo podróżują. Jeśli żadne z opisanych rozwiązań nie jest wykonalne lub odpowiednie w Twojej sieci, to jedynym wyjściem jest potraktowanie łączy modemowych tak samo jak wszystkich pozostałych łączy prowadzących do świata zewnętrznego i umieszczenie ich poza ścianą ogniową. Choć rozwiązanie takie będzie niewygodne dla użytkowników, to umieszczenie zestawu modemów za ścianą ogniową zabezpiecza Twoją sieć przed poważnym zagrożeniem.

Wzmacnianie prywatności

Pierwszą rzeczą, na jaką powinieneś zwrócić uwagę w tej części książki, jest jej tytuł. Tytuł nie brzmi *Zapewnianie prywatności* ani *Dostarczanie prywatności.* Wybrałem tu słowo *wzmacnianie,* ponieważ doskonale podkreśla ono fakt, że zapewnienie prywatności jest zadaniem bardzo trudnym. Jest prawie niemożliwe - dysponując budżetem rozsądnej wielkości - doprowadzenie do tego, aby sieć była całkiem odporna na próby naruszenia prywatności. Zrozumienie i zaakceptowanie takiej rzeczywistości jest dla wielu osób jednym z najtrudniejszych aspektów tematu bezpieczeństwa sieci. Będzie bardzo źle, jeśli pozwolisz użytkownikom Twojej sieci wierzyć, że przesyłane przez nich w sieci dane są wyłącznie ich prywatną tajemnicą. Powinni oni od samego początku zrozumieć, że prywatność w większości sieci przypomina bardziej prywatność karty pocztowej niż rozmowy telefonicznej: kiedy pakiet opuszcza maszynę użytkownika, to nie można określić, ile par oczu będzie go oglądało i czytało jego zawartość, zanim dotrze on do miejsca przeznaczenia.

Druga sprawa to fakt, że społeczność sieci lokalnej jest większym zagrożeniem prywatności niż ludzie pracujący w sieci poza Twoją organizacją. Podsłuchiwanie danych przesyłanych w sieci wymaga dostępu do tej sieci. Użytkownicy znajdujący się poza Twoją siecią muszą najpierw uzyskać do niej dostęp, aby ją podsłuchiwać, a Twoi użytkownicy dostęp ten już mają.

Oprogramowanie pozwalające podsłuchiwać przesyłane w sieci dane jest dostępne bezpłatnie na wiele platform sprzętowych. Niektóre systemy sprzedawane są nawet wraz z takim oprogramowaniem. Oczywiście podsłuchiwanie danych przesyłanych w sieciach publicznych to zupełnie inna sprawa i pomówimy o niej krótko w dalszej części książki.

Co więc możesz zrobić, aby podnieść poziom prywatności danych w sieci? Jednym z najlepszych sposobów zapewnienia prywatności danych w sieci jest upewnienie się, że nie jest w niej przesyłane nic, co mogłoby zostać łatwo przechwycone. Może to oznaczać, że najważniejsze dane (na przykład informacje finansowe) nigdy nie powinny być przesyłane w tej sieci. Jeśli dane nigdy nie pojawią się w sieci, to nie można będzie ich przechwycić. To jednak nie zawsze jest możliwe. W sieci powinny być przesyłane codziennie wszystkie rodzaje danych o różnym poziomie ważności. W końcu właśnie po to te sieci powstały. Zamiast więc pozbywać się danych z sieci musimy znaleźć sposoby na ich ochronę.

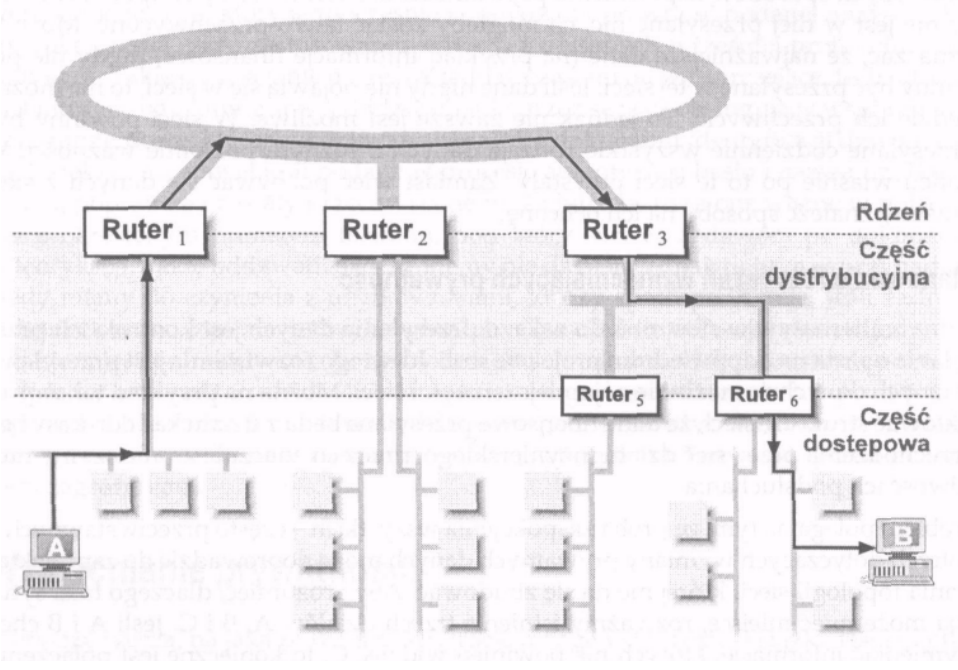
Planowanie rozwiązań wzmacniających prywatność

Jedną z alternatyw w stosunku do zakazu przesyłania danych jest kontrola ich przesyłania oparta na odpowiednim projekcie sieci. Ideą tego rozwiązania jest przesyłanie ważnych danych w możliwie najmniejszej części sieci. Można na przykład tak zaprojektować strukturę sieci, że dane finansowe przesyłane będą z działu kadr do kasy bez przechodzenia przez sieć działu inżynierskiego, przez co znacznie zmniejszymy możliwość ich podsłuchania.

Problem polega na tym, że próba zaspokojenia wszystkich - często przeciwstawnych -potrzeb dotyczących wymiany prywatnych danych może doprowadzić do zaprojektowania topologii sieci, której nie da się zbudować. Aby zrozumieć, dlaczego taka sytuacja może mieć miejsce, rozważmy istnienie trzech działów A, B i C. Jeśli A i B chcą wymieniać informacje, których nie powinien widzieć C, to konieczne jest połączenie sieci w tych działach ścieżką, która nie prowadzi przez sieć działu C. Jednym ze sposobów osiągnięcia takiego stanu jest połączenie sieci A i B, a następnie dołączenie sieci C do sieci działu A. Co się będzie jednak działo, kiedy C zechce wymieniać informacje z B, których nie powinien widzieć dział A? W porządku, wystarczy tylko przenieść połączenie z sieci C i dołączyć je do B, a nie do sieci A. Problem został rozwiązany. Ale powróci, kiedy dział A będzie chciał wysłać prywatne dane do C. No dobrze, można dodać dodatkowe łącze pomiędzy A i C, ale połączenie typu „każdy z każdym" nie będzie się dobrze skalowało, jeśli sieć będzie łączyła kilkadziesiąt takich działów, z których każdy będzie chciał wymieniać z pozostałymi jakieś prywatne dane.

W większości sieci topologia wielopoziomowej gwiazdy (opisanej w rozdziale 2, zatytułowanym „Projektowanie sieci - część I") najrozsądniej znaleźć kompromis pomiędzy zachowaniem prywatności a praktycznym podejściem do budowy sieci. W topologii wielopoziomowej gwiazdy (patrz rysunek 10-3) jedyną siecią, przez którą muszą przechodzić dane przesyłane pomiędzy każdą dowolną parą działów, są komponenty sieci tworzące jej rdzeń i część dystrybucyjną. Komponenty te przede wszystkim nie powinny składać się z włączonych do nich maszyn użytkowników, przez co sprawa zabezpieczeń będzie dotyczyła tylko grupy personelu zajmującego się siecią.

Grupa taka jest zwykle niewielka i (miejmy nadzieję) składa się z profesjonalistów. Jeśli nie możesz zaufać swojemu personelowi, to - niezależnie od tego, jak zaprojektujesz sieć - nie będziesz mógł zapewnić w niej prywatności.



Rysunek 10-3: Wielopoziomowa gwiazda umożliwiająca zachowanie prywatności komunikacji

Kiedy sprawdzasz ścieżki, po których w sieci przesyłane są ważne dane, nie zapomnij o sprawdzeniu zapasowych ścieżek i redundantnych połączeń, które dodałeś w celu zwiększenia niezawodności sieci. Choć podstawowa ścieżka może przesyłać dane z dala od miejsc, w których nie powinny się one znaleźć, to zapasowa ścieżka może je właśnie w takie miejsca wysyłać. Choć można to zaakceptować, gdy sieć znajduje się w trybie pracy stosowanym w czasie uszkodzenia, to powinieneś przynajmniej zdawać sobie sprawę z ryzyka i ostrzec użytkowników o możliwości naruszenia prywatności danych przesyłanych po sieci w tym czasie.

Zdarzają się sytuacje, kiedy nie możesz zabezpieczyć prywatności poprzez odpowiednie zaprojektowanie sieci. Może będziesz musiał np. zabezpieczyć prywatność danych przesyłanych pomiędzy dwoma hostami pracującymi w tym samym segmencie sieci; nie jest to jednak akceptowane przez inne hosty, a z jakichś powodów nie możesz wydzielić hostów wymagających prywatności. W takiej sytuacji należy roz*ważyć* dwa rozwiązania.

Pierwsze wynika z charakteru sieci przełączanych, w którym dane przesyłane z hosta A do B nie będą przesyłane na połączenie prowadzące do hosta C, co skutecznie uchroni host C przed możliwością podsłuchiwania tego ruchu generowanego w sieci. Choć rozwiązanie takie może być dość drogie, to może się okazać znacznie tańsze od innych rozwiązań. Drugie rozwiązanie jest odmianą pierwszego. Wielu dostawców oferuje funkcje bezpieczeństwa w swoich koncentratorach sieci Ethernet. Rozwiązania tego typu polegają na tym, że koncentrator uczy się lub ma w trakcie konfiguracji podane informacje o tym, jakie maszyny dołączone są do jego portów, a następnie nie dopuszcza do przesyłania poprawnych informacji na łącza, które tej informacji nie powinny otrzymywać. Takie rozwiązanie zapewnia poziom prywatności podobny do tego, który oferowany jest *przez* przełączniki Ethernet, z wyjątkiem tego, że wykorzystanie pasma sieci jest takie jak z sieci Ethernet. Rozwiązanie opierające się na koncentratorach jest zwykle znacznie tańsze niż to opisane, bazujące na przełącznikach sieci Ethernet.

Szyfrowanie danych

Projektowanie sieci z uwzględnieniem prywatności danych jest podejściem dobrym w przypadku, kiedy projektujesz nową sieć lub dokonujesz znacznej zmiany projektu sieci używanej dotychczas. Co można jednak zrobić, kiedy mamy do czynienia z siecią już pracującą, której struktury nie można zmieniać, albo - w jeszcze trudniejszym przypadku - kiedy prywatne dane muszą opuścić sieć organizacji i zostać przesłane przez sieć Internet? Jedynym rozsądnym rozwiązaniem jest wtedy szyfrowanie danych. Szyfrowanie danych może następować w kilku miejscach procesu trasy, w której przesyłane są dane; każdy z tych punktów ma pewne zalety. Generalna zasada mówi, że im wyżej w stosie komunikacyjnym następuje to szyfrowanie, tym rozwiązanie jest elastyczniejsze, ale jednocześnie jest ujawniana większa liczba informacji dotyczących natury systemu komunikacji.

- Zaczynając od dołu stosu protokołów komunikacyjnych, szyfrowanie może być wykonywane na poziomie warstwy łącza: wszystkie dane przesyłane przez łącze fizyczne są szyfrowane. Może to oznaczać szyfrowanie całych pakietów lub tylko przesyłanych w nich danych, podczas gdy nagłówki warstwy łącza pozostają nie szyfrowane. Niezależnie od tego, która metoda jest używana, rozszyfrowanie informacji musi być wykonane przez odbiorcę na poziomie warstwy łącza danych, bez względu na to, czy będzie to host, czy też ruter. Dopiero na podstawie takiej zdekodowanej informacji podejmowana jest decyzja o rutowaniu. Z tego względu szyfrowanie tego typu stosuje się głównie na łączach typu punkt-punkt lub w komunikacji pomiędzy dwoma hostami pracującymi w tej samej podsieci.
- Drugim miejscem, gdzie może być dokonywane szyfrowanie danych, jest warstwa sieciowa. W tym rodzaju szyfrowania nagłówki IP są nadal nie szyfrowane, a szyfrowane są tylko dane kierowane na określony adres komputera. Ponieważ ta metoda nie obejmuje nagłówków IP, możliwe jest rutowanie szyfrowanych pakietów w sieci bez konieczności rozszyfrowania każdego z nich, podejmowania decyzji o rutowaniu i kolejnego szyfrowania pakietów przed przesłaniem dalej.

Takie rozwiązanie zwiększa bezpieczeństwo danych, ponieważ są one tylko raz rozszyfrowywane przez odbiorcę, do którego zostały przesłane. Rozwiązanie to ma jednak swoją cenę: informacja o tym, kto z kim się komunikuje, widoczna jest dzięki nie zaszyfrowanym nagłówkom IP. Możliwe jest więc stwierdzenie, że maszyna *merlin* komunikuje się z *arthur,* nawet jeśli nie wiadomo, jakie dane przesyłają. W niektórych sytuacjach istnieje potrzeba ukrycia nawet takich informacji.

- Posuwając się w górę stosu komunikacyjnego, możemy zastosować szyfrowanie w warstwie transportowej. W takim przypadku aplikacja przekazuje niezaszyfrowane dane do oprogramowania sieciowego, które dokonuje szyfrowania strumienia danych z warstwy transportowej przed przesłaniem go w dół do IP. W niektórych przypadkach takie rozwiązanie ma swoje zalety: szyfrowanie danych w warstwie transportowej skraca czas, przez jaki niezaszyfrowane dane dostępne są w systemie końcowym, przesuwając szyfrowanie bliżej aplikacji. Znacznie trudniej jest przeszukiwać bufory systemu operacyjnego w celu znalezienia danych, które nie są jeszcze zaszyfrowane. Wadą jest jednak to, że jeszcze więcej przesyłanych informacji jest dostępnych w formie niezaszyfrowanej. Jeśli wiemy, że *merlin* wysyła dane na port TCP 25 hosta *arthur,* to oczywiste jest, że są to dane poczty elektronicznej.
- Możliwe jest zastosowanie szyfrowania na poziomie aplikacji, która dokona ich szyfrowania jeszcze przed przekazaniem do systemu. Na przykład program obsługi e-mail może szyfrować zawartość wiadomości e-mail, pozostawiając jednocześnie niezaszyfrowane nagłówki, dzięki czemu wiadomość ta może być obsługiwana przez pośredniczące w jej przekazywaniu serwery poczty elektronicznej. Taka wiadomość może być nawet przesyłana przez sieci pracujące z protokołem innym niż IP, w których nie jest możliwe stosowanie żadnej metody szyfrowania z niższej warstwy. Szyfrowanie danych na poziomie aplikacji jest odporne na ujawnianie na hostach, które obsługują wielu użytkowników, ale jednocześnie przy przesyłaniu informacji widać jeszcze więcej szczegółów. Wiadomo, że przesyłane są wiadomości poczty elektronicznej, i wiadomo, do kogo są one przesyłane.

Dla wykonania szyfrowania można użyć specjalnego wyposażenia wewnątrz komputera lub wyposażenia umieszczonego pomiędzy siecią a komputerem albo można zastosować oprogramowanie. Rozwiązania sprzętowe wymuszają stosowanie szyfrowania na poziomie niższych warstw stosu protokołów komunikacyjnych, a rozwiązania programowe stosowane są zwykle na wyższych warstwach. Rozwiązania sprzętowe pracują zwykle szybciej, ponieważ nie wykorzystują mocy CPU hosta, i mogą pracować solidniej, ponieważ błędy występujące w systemie operacyjnym nie wpływają na poziom bezpieczeństwa. Sprzętowe szyfrowanie jest również droższe od szyfrowania programowego. Wynika to z faktu, że każdy host, który ma uczestniczyć w wymianie prywatnych danych, wymaga zastosowania wymienionego wyposażenia. Jeśli w sieci pracuje tysiąc maszyn, które muszą się bezpiecznie komunikować ze sobą, to konieczne będzie zastosowanie tysiąca urządzeń szyfrujących. Rozwiązanie takie może się więc okazać dość kosztowne. Rozwiązania programowe mają tę zaletę, że nie wszystkie informacje przesyłane przez host muszą podlegać szyfrowaniu.

Wzmacnianie prywatności

Można wybiórczo szyfrować informacje za pomocą urządzenia, ale musi być ono znacznie inteligentniejsze. Host musi wtedy w jakiś sposób przekazać informację do urządzenia szyfrującego, które pakiety mają być szyfrowane. W przypadku stosowania oprogramowania szyfrującego system po prostu nie szyfruje danych, które tego nie wymagają.

Być może nie potrzebujesz szyfrowania komunikacji pomiędzy hostami. Zamiast tego możesz chcieć szyfrować dane przesyłane pomiędzy Twoją siecią a siecią innej organizacji (być może oddziału firmy), ponieważ łącze pomiędzy tymi dwiema sieciami jest łączem publicznym. W takim przypadku rozwiązanie sprzętowe jest idealne. Wystarczy umieścić takie urządzenie pomiędzy Twoją siecią a Internetem i to samo zrobić w sieci, z którą się komunikujesz. Następnie należy zaprogramować urządzenia, aby szyfrowały wszelkie dane przesyłane pomiędzy sieciami i tworzyły w ten sposób wirtualną sieć prywatną. Urządzenia pozwalające na tworzenie takich połączeń stają się coraz bardziej popularne, w miarę jak Internet coraz częściej wykorzystywany jest do komunikacji pomiędzy sieciami komercyjnymi.

Szyfrowanie danych zapewnia prywatność przesyłanych danych i zabezpiecza przed ich podsłuchiwaniem. Metoda ta ma jednak również pewne wady. Konieczne jest wyważenie ograniczeń elastyczności sieci, stopnia jej zabezpieczenia, szybkości pracy i poniesionych kosztów. Ponadto szyfrowanie danych nie jest rozwiązaniem całkowicie bezpiecznym. Mając dostatecznie dużo czasu i mocy przetwarzania można złamać każdy klucz szyfrujący. Zadaniem szyfrowania nie jest jednak całkowite zabezpieczenie danych przed ich odczytaniem. Chodzi o upewnienie się, czy dane, które zostaną odszyfrowane, nie będą już miały większej wartości lub znaczenia lub czy koszty poniesione na ich rozszyfrowanie będą wyższe od wartości samych danych. Jeśli np. szpiegom przemysłowym rozszyfrowanie podsłuchanych danych zajmie dwa lata i wtedy dopiero odkryją formułę super kleju produkowanego przez Twoją firmę, którego wprowadzenie na rynek zajęło wam jeden rok, to oczywiste staje się, że tak późno rozszyfrowana formuła nie będzie miała dla nich żadnej wartości.

Nawet szyfrowanie, które można złamać po tygodniu, ma wartość. Twoim potencjalnym wrogiem w tej grze o prywatność danych jest pracownik wewnątrz firmy. Ludzie ci zwykle nie są na tyle złośliwi, aby chcieć sprzedawać sekrety firmy konkurencji. Są oni częściej zainteresowani poznaniem nowinek lub zdobyciem informacji o tym, co się działo na spotkaniu zarządu firmy. Stosując nawet najprostsze metody szyfrowania, zapobiegniesz zdobywaniu tematów do plotek. Takie zabezpieczenie powinno wtedy w zupełności wystarczyć; i w rezultacie zabezpieczysz się przed przypadkowymi próbami podsłuchiwania danych przesyłanych w sieci.

Powinieneś jednak pamiętać, że wiele rządów różnych krajów traktuje techniki szyfrowania jako zagrożenie państwa. W niektórych krajach zakazano stosowania systemów szyfrowania, których służby państwowe nie mogą łatwo złamać. W innych, jak na przykład w Stanach Zjednoczonych, wprowadzono bardzo szczegółowe regulacje prawne dotyczące szyfrowania sprzętowego i programowego. Choć fakty te nie muszą mieć wpływu na działanie firmy obsługującej określony rejon, to są one ważne w przypadku firm mających siedziby w wielu krajach na świecie. Firmy takie muszą bardzo dokładnie zapoznać się z lokalnymi przepisami i stosować tylko dozwolone metody szyfrowania, nawet jeśli używane są one do szyfrowania wewnętrznej wymiany danych w firmie.

Wirtualne sieci prywatne

Wirtualne sieci prywatne (VPN) stają się ostatnio coraz popularniejsze. Sieć taka jest łączem pomiędzy dwoma (lub więcej) miejscami przebiegającym przez publiczną sieć transmisji danych, taką jak Internet, i mającym taki sam poziom zabezpieczenia prywatności danych co prywatna sieć. Połączenie takie odpowiada dzierżawionemu łączu prywatnemu przebiegającemu pomiędzy dwoma miejscami i pozwala na zapewnienie tego samego poziomu prywatności sieci, bez konieczności ponoszenia kosztów na faktyczną dzierżawę łącza. Urządzenia umieszczone na obu końcach takiego połączenia tworzą szyfrowane tunele pomiędzy sobą, a następnie traktują te tunele tak, jakby były one prywatnymi łączami typu punkt-punkt. Pakiety, które muszą zostać bezpiecznie przesłane do drugiego miejsca obsługiwanego przez VPN, są wysyłane do lokalnego urządzenia. Urządzenie to dokonuje szyfrowania pakietów tak, jakby były to zwykłe dane, i umieszcza je wewnątrz innych pakietów, które przesyłane są *przez* sieć publiczną do urządzenia pracującego w odległym miejscu. Urządzenie to dokonuje ekstrakcji zaszyfrowanych danych z odebranych pakietów i rozszyfrowuje te dane tworząc oryginalne pakiety, a następnie przesyła je do miejsca przeznaczenia.

Zalety stosowania VPN są oczywiste. W żadnym miejscu sieci publicznej ważne dane, które są w niej przesyłane, nie pojawiają się jako niezaszyfrowany tekst. Dane przesyłane przez te łącza są zawsze zakodowane; są one widoczne jedynie w obu prywatnych sieciach - podobnie jak w dedykowanym łączu prywatnym! Rozwiązanie to ma również sporo wad, z których największą jest konieczność zakupienia odpowiedniego urządzenia (lub oprogramowania) dla obu końców tunelu. Choć w przypadku stosowania wielu łączy wirtualnych może to oznaczać dość duży wydatek, to nadal rozwiązanie to może być tańsze od dzierżawionych łączy prywatnych.

Drugą wadą łączy VPN jest to, że obydwa miejsca, które chcemy połączyć, wymagają stosowania kompatybilnego wyposażenia lub oprogramowania tworzącego tunele. Choć nie jest to problem dla dużej korporacji, która może wysłać kilkadziesiąt identycznych urządzeń do każdego z biur w poszczególnych krajach, to w przypadku mniejszych firm, które wymieniają dane z różnymi partnerami, może to oznaczać konieczność posiadania różnych urządzeń VPN dla każdego z biur firmy. Jest to nie tylko rozwiązanie kosztowne, ale też bardzo niewygodne, jeśli chodzi o zarządzanie pracą tego sprzętu. Mimo to, jeśli wymagania dotyczące prywatności danych są dosyć wysokie, a koszty takich rozwiązań są niższe niż w przypadku stosowania prywatnych łączy danych, VPN mogą być właściwym rozwiązaniem komunikacyjnym.

Na zakończenie należy zaznaczyć, że kiedy rozważasz użycie VPN przebiegających przez publiczną sieć Internet, musisz pamiętać o tym, że generowany przez Ciebie ruch będzie wykorzystywał pasmo sieci, do której jesteś podłączony, wraz z publicznym ruchem generowanym przez Twoją sieć do Internetu. Choć prawie zawsze możliwe jest kupienie szybszego łącza dzierżawionego, to pasmo w sieci Internet jest ograniczone. To, co uzyskasz, jest częścią pasma dzielonego pośród wielu użytkowników i wiele miejsc w sieci, a dokładna wartość dostępnego pasma prawie nigdy nie może być przez Ciebie kontrolowana.

Utrzymywanie integralności danych

Większości ludzi wydaje się, że nic się nie może stać ich danym w czasie pomiędzy ich wysłaniem a odebraniem przez adresata. Czy tak jest rzeczywiście? Skąd można mieć pewność, że dane, które zostały wysłane do sieci są tymi samymi danymi, które zostały odebrane przez adresata? Protokoły sieciowe dbają o to, by przesyłane dane nie miały błędów, stosując do tego celu sumy kontrolne umieszczane w ramkach sprzętowych, nagłówkach pakietów i samych danych, ale nie są one w stanie zagwarantować, że na drugim końcu jakiegoś odcinka sieci, po którym przesyłane są dane, nie nastąpiła manipulacja nimi. Na przykład wiadomość e-mail może zostać zmieniona, zanim opuści maszynę, która ją wysyła, po tym jak dotrze do maszyny docelowej lub gdy czeka w kolejce w jednej z maszyn pośredniczących w przekazywaniu poczty w sieci. Taka manipulacja danymi nie jest ograniczana przez system ochrony wbudowany w protokół sieciowy. Nie ma także żadnego sposobu, aby maszyna odbierająca wiadomość mogła potwierdzić, że jej nadawca jest faktycznie tym, za kogo się podaje. Niektóre przypadki fałszerstwa mogą być wykryte przez ludzi po dokładnym przejrzeniu zawartości przesłanej wiadomości, ale niewielu użytkowników wie, czego należy szukać, zwłaszcza że fałszerz może być całkiem sprytny.

Najlepszym sposobem zapewnienia integralności danych jest stosowanie techniki określanej jako *cyfrowy podpis.* Podobnie jak podpis tradycyjny, podpis cyfrowy jest czymś dodawanym do przesyłanych danych, takich jak wiadomość poczty elektronicznej, który odbiorca może sprawdzić w celu potwierdzenia autentyczności nadawcy tej wiadomości. W przeciwieństwie do tradycyjnego podpisu, podpis cyfrowy znacznie trudniej podrobić i dlatego daje on większą pewność, że osoba podająca się za autora wiadomości rzeczywiście ją podpisała. Stosowanie podpisów cyfrowych ma jeszcze jedną ważną zaletę. Ponieważ podpis taki tworzony jest na podstawie tekstu, który jest podpisywany, każda zmiana dokonana w tekście spowoduje, że algorytm sprawdzający poprawność podpisu na pewno to wykryje. W przypadku wiadomości poczty elektronicznej podpis cyfrowy nie tylko upewnia odbiorcę, że nadawca jest tym, za kogo się podaje, ale również że wiadomość nie uległa zmianie od czasu, kiedy została podpisana.

Na szczęście oprogramowanie pozwalające generować cyfrowe podpisy jest szeroko dostępne na wiele platform sprzętowych i systemów operacyjnych. *Pretty Good Privacy (PGP)* jest programem pracującym w systemie UNIX, Microsoft Windows, Macintosh, VMS i innych systemach,* który jest dostępny za darmo. Poświęcając jedynie czas na zdobycie programu, zainstalowanie go i przeszkolenie użytkowników, będziesz mógł weryfikować zawartość i pochodzenie plików, wiadomości poczty i innych danych. Oprogramowanie to zostało opisane w książce FGP: *Pretty Good Privacy* napisanej przez Simsona Garfinkela (O'Reilly).

*Komercyjne wersje programu dostępne są w firmie PGP Inc. Aby dowiedzieć się o ceny i dostępność oprogramowania na inne platformy, zajrzyj na stronę *http://www.pgp.com.*

PGP jest doskonałym narzędziem służącym do podpisywania i szyfrowania danych na poziomie aplikacji, ale nie pomaga w weryfikowaniu danych przesyłanych pomiędzy maszynami. Niestety, protokół IPv4 nie ma jeszcze możliwości obsługi cyfrowego podpisu przy zastosowaniach do obsługi typowej komunikacji w sieci. Protokół ten dodaje jednak cyfrowy podpis do niektórych protokołów dynamicznego rutowania, podczas wymieniania przez nie informacji o rutowaniu. Aby zrozumieć, dlaczego stosowanie podpisów w wymianie informacji o rutowaniu jest takie ważne, zastanów się, co będzie się działo, kiedy złośliwy (albo nieostrożny) użytkownik zacznie wysyłać do Twojej sieci uaktualnienia protokołu rutowania dynamicznego zawierające fałszywe informacje. W najlepszym wypadku w Twojej sieci powstaną czarne dziury, w których pakiety - zamiast podróżować w wyznaczonym kierunku - będą znikać. W najgorszym przypadku pakiety kierowane do niektórych albo do wszystkich maszyn wysyłane będą do innego miejsca przeznaczenia, wybranego przez intruza, gdzie mogą zostać poddane analizie. Technologia podpisu cyfrowego może pomóc w takich przypadkach, pozwalając ruterowi upewnić się, czy uaktualnienia, które otrzymuje pochodzą od autentycznego nadawcy, jakim jest jeden ze współpracujących ruterów.

Jeśli wybrany przez Ciebie protokół rutowania obsługuje uaktualnienia przesyłane z podpisem, powinieneś poważnie rozważyć użycie tej funkcji. Konfiguracja jest prosta. Należy podać ruterowi klucz autentykacji, którym będzie się on posługiwał przy przesyłaniu uaktualnień przez dany interfejs lub do określonego sąsiada. Na przykład aby wykorzystać klucze autentykacji w protokole OSPF, wystarczy dodać:

```
interface ethernet 0
 ip address 192.168.1.100 255.255.255.0
 ip ospf authentication-key mysecret

router ospf 1
 network 172.16.0.0 0.0.255.255 area 1
 network 0.0.0.0 255.255.255.255 area 0
 area 0authentication
```

Ten fragment konfiguracji informuje ruter, że ma on uruchomić proces OSPF, umieścić interfejs 172.16.0 .0/16 w obszarze 1 a wszystkie pozostałe - w obszarze 0. następnie zdefiniowany został klucz autentykacji dla interfejsu ethernet 0(każdy interfejs może mieć inny klucz). Na zakończenie kazano ruterowi wykorzystywać funkcję autentykacji w obszarze 0. Pozostałe obszary, takie jak l, nie są obsługiwane przez tę funkcję. Ponieważ interfejs ethernet 0 najduje się w obszarze O, wszystkie uaktualnienia tras dotyczące obszaru 0 będą wykorzystywały klucz mysecret. Jeśli uaktualnienie zostanie nadesłane na ten interfejs i nie będzie posiadało takiego klucza, to ruter je odrzuci.

Dlatego wszystkie urządzenia pracujące w jednym obszarze OSPF muszą stosować klucze autentykacji lub nie stosować ich wcale. Nie można mieszać tych dwóch rozwiązań.

Konfigurowanie autentykacji dla uaktualnień przesyłanych przez protokół BGP jest również proste. Wystarczy powiedzieć procesowi rutowania BGP, jakiego hasła ma używać do komunikowania się z każdym z sąsiadów:

```
router bgp 101

network 172.16.0.0
 neighbor 192.168.23.4 remote-as 102
 neighbor 192.168.23.4 password my-secret
 neighbor 10.23.4.109 remote-as 103
 neighbor 10.23.4.109 password his-secret
```

Każdy z sąsiadów może stosować różne hasła, podobnie jak w OSPF; każdy interfejs może stosować różne klucze autentykacji. Możliwe jest ponadto określenie niektórych sąsiadów, którzy nie wykorzystują haseł; wtedy wymiana uaktualnień z tymi sąsiadami nie będzie podlegała autentykacji.

Niestety, większość dynamicznych protokołów rutowania nie obsługuje żadnego ze sposobów autentykacji. Wtedy jedyną obroną jest takie skonfigurowanie ruterów, aby wymieniały one uaktualnienia tylko wtedy, gdy to konieczne, i głównie z maszynami, które znajdują się pod Twoją bezpośrednią kontrolą. Konfiguracja powinna ponadto odfiltrować niechciane uaktualnienia tras, stosując ograniczenie nakładane na dystans administracyjny i filtrować je pod względem ich zawartości, która powinna być rozsądna. Jeśli wiesz np. że informacja o trasie domyślnej może być nadesłana z niewielkiej grupy ruterów, to powinieneś odfiltrować taką informację z innych uaktualnień nadsyłanych z każdego innego rutera, nawet jeśli znajduje się on pod Twoją kontrolą. Wszystkie te sposoby zostały opisane w rozdziale 6.

Zapobieganie atakowi denial of service

Czwartym aspektem bezpieczeństwa sieci, o którym powinieneś pamiętać, jest atak typu *denial of service*. W przypadku tego typu ataku osoba atakująca Twój system dąży nie do przeniknięcia do jego wnętrza, lecz do zablokowania możliwości pracy w systemie jego prawowitych użytkowników. Na przykład program zabierający całą moc CPU w systemie, w którym pracuje kilku użytkowników, może doprowadzić do tego, że nie będą mogli oni wykonywać swoich zadań. Każdy zasób komputera może być przedmiotem ataku, ale sieć otwiera możliwości przeprowadzania takiego ataku z zewnątrz. Zastanów się, co się stanie, kiedy grupa maszyn będzie bombardowała inną maszynę w sieci z maksymalną szybkością, z jaką mogą one generować pakiety IP. Jeśli maszyna będąca adresatem tych pakietów nie będzie w stanie ich obsłużyć, może przestać pracować w sieci lub nawet ulec uszkodzeniu w wyniku całkowitego wykorzystania zasobów.

Najlepszym sposobem zapobiegania większości ataków typu *denial of service* jest odcięcie atakujących od dostępu do zasobów atakowanego systemu. Jeśli pomiędzy Twoją siecią a światem zewnętrznym znajduje się ściana ogniowa, to atak skierowany przeciwko maszynom znajdującym się wewnątrz Twojej sieci musi być wykonywany przy użyciu usług przechodzących *przez* ścianę ogniową.

Żadna usługa, która nie jest przepuszczana przez ścianę ogniową, nie będzie mogła być wykorzystana do przeprowadzenia tego typu ataku. Atakujący może oczywiście obciążyć ścianę ogniową tak, że nie będzie mogła ona spełniać swoich zadań lub wykorzystać całe dostępne pasmo Twoich zewnętrznych łączy.

Innym ważnym sposobem obrony jest wykorzystanie funkcji oferowanych przez dostawcę sprzętu. Wielu atakom *denial of service* można łatwo zaradzić, stosując dostarczane przez dostawcę łaty programowe nakładane na atakowane systemy. Będąc na bieżąco z oferowanymi przez dostawcę łatami możesz łatwo zapobiec zaatakowaniu systemu lub ograniczyć wpływ tego ataku na pracę urządzenia.

Powinieneś wyłączyć wszystkie usługi, których nie potrzebujesz, gdyż nie będą mogły być one wtedy użyte jako punkt przeprowadzenia ataku. W rozdziale 8, zatytułowanym „Techniczna strona *zarządzania pracą* sieci", napisałem, że TCP i UDP mają małe usługi, takie jak *echo* i *daytime,* które są powszechnie wykorzystywane do przeprowadzania ataków opisywanego tu typu. Domyślnie usługi te są uruchomione na Twoim ruterze i prawdopodobnie na większości hostów pracujących w sieci. Musisz więc podjąć decyzję, czy przydatność tych usług w diagnozowaniu pracy sieci jest taka, że trzeba je pozostawić i umożliwić wykorzystanie dla przeprowadzenia ataku. Wyłączenie tych usług w systemie Cisco IOS jest bardzo proste i wymaga podania:

```
no service tcp-small-servers
no service udp-small-servers
```

Zawsze jednak będą ataki typu *denial of service,* którym nie będzie można zapobiec, niezależnie od tego, jak gorliwym jesteś administratorem. Wtedy jedynym sposobem obrony jest wyśledzenie źródła ataku lub znalezienie sposobu powstrzymania go. Proces ten będzie przebiegał znacznie sprawniej, jeśli będziesz utrzymywał dobre stosunki z inżynierami pracującymi u dostawcy usług. Na szczęście naprawdę niebezpieczne ataki tego typu należą do rzadkości. Większość ludzi pracujących w sieci ma zbyt małe zasoby sprzętowe, aby skutecznie przeprowadzić taki atak. Jeśli Twoja sieć jest dołączona do Internetu łączem TI, to atakujący, który chce zapchać takie połączenie, musi dysponować łączem TI. Większość ludzi, którzy mają tyle pieniędzy, że stać ich na takie łącze, ma z reguły lepsze *rzeczy* do roboty niż ataki na Twój system.

Są jeszcze inne, mniej oczywiste sposoby przerwania usług oferowanych w Twojej sieci. Dość łatwo jest wysłać do rutera pakiet ICMP, który spowoduje zmianę informacji o trasach (nawet statycznych) i przesyłanie pakietów niewłaściwymi trasami. Ponieważ ruter powinien być urządzeniem, które decyduje o tym, jakie informacje o nitowaniu rozsyłane są w sieci, to nie powinien przetwarzać żadnych pakietów przekierowania ICMP, które odbiera z sieci. Na szczęście większość dostawców ruterów domyślnie ignoruje obsługę tego typu przekierowań (nie myl pojęcia „wysyłanie przekierowań" z pojęciem „przetwarzanie przekierowań"), a w niektórych nie ma nawet opcji, która pozwala je obsługiwać. Aby się upewnić, sprawdź posiadane rutery.

Zapobieganie atakowi denial of service

Czasami ruter może zostać zaatakowany przy wykorzystaniu metod i protokołów, których obsługę w nim umieściliśmy w celu zarządzania jego pracą. Zastanów się np., jakie efekty będzie miała próba przejrzenia całej zawartości SNMP MIB na jednym z ruterów. W zależności od tego, jak ruter będzie w danej chwili obciążony, może to potrwać chwilę, ale może też spowodować dodatkowe obciążenie, które sprawi, że ruter ulegnie uszkodzeniu. Nawet jeśli tak się nie stanie, to ruter spędzi mnóstwo czasu na obsługiwaniu SNMP, który normalnie powinien być przeznaczony do obsługi podstawowego zadania rutera, jakim jest trasowanie pakietów. Jest to kolejny powód, dla którego powinieneś ograniczyć dostęp do procesów SNMP działających w ruterach i innych urządzeniach sieciowych. Jeśli ograniczysz liczbę maszyn, które mogą próbkować sieć za pomocą SNMP, to ograniczysz tym samym liczbę osób, których powinieneś się obawiać.

W rozdziale 1, zatytułowanym „Podstawy sieci IP", napisałem, że maszyna w sieci może wysyłać pakiet typu broadcast do sieci, do której nie jest dołączona. Można tego dokonać wykorzystując odpowiedni adres sieci lub podsieci odległej i przesyłając go przez rutery w pakiecie typu *unicast*. W takim przypadku ostami ruter wyśle pakiet broadcast do odległej sieci, która była przeznaczeniem tego pakietu. Ten rodzaj skierowanego pakietu typu broadcast może być bardzo przydatny. Należy jednak pamiętać o tym, że możliwość ta może prowadzić do wielu błędów w użyciu tej funkcji lub zamierzonego jej nadużywania. Każdy taki pakiet broadcast przerywa pracę wszystkich maszyn w segmencie sieci, do której został skierowany; nawet maszyn, które nie pracują z protokołem IP. Każda z tych maszyn musi taki pakiet odebrać i przeanalizować jego zawartość, aby stwierdzić, czy powinna go przetwarzać, a jeśli okaże się, że tak, to przetworzyć odebrany pakiet.

Zastanów się teraz, co się będzie działo, jeśli jakaś maszyna będzie wysyłała wiele pakietów broadcast. Maszyna o średniej mocy może zająć w ten sposób sporą część pasma sieci, do której pakiety te są kierowane, przerywając niepotrzebnie pracę wszystkich maszyn w tej sieci, bez przerywania pracy samej sobie. Czy rzeczywiście chcesz, aby jakiś złośliwy osobnik mógł przerywać pracę Twojej sieci siedząc przy komputerze na drugim końcu świata? Zalecam, abyś wyłączył przetwarzanie skierowanych pakietów broadcast na niektórych, a nawet na wszystkich ruterach w swojej sieci, jeśli nie musisz koniecznie stosować tego typu pakietów. (Wyłączenie obsługi skierowanych pakietów broadcast nie oznacza wyłączenia obsługi lokalnych pakietów tego typu, które są bardzo ważne w pracy sieci.) W Cisco IOS wystarczy dodać następującą instrukcję w konfiguracji każdego z interfejsów:

```
no ip directed-broadcast
```

Instrukcja ta jest częścią mojej domyślnej konfiguracji interfejsów. Jak dotąd nie znalazłem aż tyle ważnych powodów, abym musiał podjąć ryzyko i włączyć obsługę skierowanych pakietów broadcast.

Inne sprawy związane z bezpieczeństwem

Kontrola dostępu, ochrona prywatności danych, utrzymywanie integralności danych i zapobieganie atakom powodującym zablokowanie usług to najczęściej rozważane tematy związane z bezpieczeństwem sieci. Nie są to jednak jedyne sprawy, którymi powinieneś się zainteresować. Omówię teraz kilka problemów, które nie są bezpośrednio związane z bezpieczeństwem sieci komputerowych, ale które powinny być uwzględnione w planie zabezpieczeń danych opracowanym dla całej firmy.

Wirusy komputerowe

Jednym ze szczególnie powszechnie spotykanych sposobów ataków powodujących zablokowanie usług jest wirus komputerowy. Wirusy to małe programy komputerowe opracowane tak, by mogły się same powielać i „infekować" kolejne maszyny. Mogą to robić przez dołączanie się do kodu binarnego programów, plików zawierających dokumenty lub ukrywając się w początkowych sektorach dysków. Efektem działania wirusów może być proste wyświetlanie komunikatu na ekranie komputera, który został zainfekowany, lub tak poważne, jak wykasowanie wszystkich danych z dysku twardego. Odmiana wirusów określana koniami trojańskimi może również przechwytywać informacje takie jak hasła lub pakiety przesyłane w sieci, a następnie przesyłać je do autora wirusa w celu późniejszego wykorzystania. Niestety, wirusy komputerowe i konie trojańskie są częścią życia zarówno użytkowników komputerów, jak i administratorów sieci. Obecnie znanych jest kilka tysięcy wirusów i ich modyfikacji, a kolejne są cały czas tworzone. Powinieneś przedsięwziąć pewne kroki w celu ochrony swojej sieci przed zainfekowaniem lub w celu usunięcia wirusa po zainfekowaniu komputera.

Przede wszystkim należy uzyskać program antywirusowy dla systemów, które są najbardziej narażone na zainfekowanie. Są to zwykle komputery typu PC lub Macintosh, ale mogą to być również inne systemy, które znajdują się w Twojej sieci. Program antywirusowy pracuje zwykle w dwóch trybach. Pierwszy tryb pracy skanuje pliki i systemy, zanim jeszcze wirus ma szansę się rozmnożyć. Drugi tryb pozwala na wykrycie zainfekowanych plików i usunięcie z nich wirusa, kiedy infekcja ta następuje. Na przykład, skoro niektóre wirusy próbują zmienić zawartość bootsektora dysku systemowego, to program antywirusowy może przechwytywać takie próby i wyświetlać odpowiednie komunikaty użytkownikowi. Jeśli zmiana, która następuje, wynika z działania użytkownika, to może on pozwolić na jej dokończenie. W pozostałych przypadkach następuje identyfikacja wirusa i zatrzymanie jego działania. Niektóre programy antywirusowe mogą pomagać w usuwaniu wirusów po wystąpieniu infekcji. Jeśli jakiś wirus nie może być usunięty bezpiecznie, to może się okazać konieczne odtworzenie kopii systemu z medium, na którym wykonana została kopia zapasowa, lub - jeśli ta kopia jest niedostępna lub została zainfekowana - być może konieczna będzie powtórna instalacja systemu z zabezpieczonej przed zapisem kopii instalacyjnej. Obydwa rozwiązania oznaczają sporo pracy.

Inne sprawy związane z bezpieczeństwem

Na razie najlepszą bronią przeciwko wirusom komputerowym jest szkolenie użytkowników i szczegółowo opracowane procedury. Należy przygotować zakaz instalowania i wykorzystywania w pracy jakiegokolwiek oprogramowania, które użytkownicy ściągają z sieci, przynoszą z domu lub dostają od przyjaciół. Oprogramowanie takie powinno najpierw przejść dokładne testy na obecność wirusów i innych ukrytych funkcji. Takie testy powinny być wykonywane na maszynie odłączonej od sieci i mającej zainstalowane różne programy antywirusowe. Tylko po przejściu testów można zastanowić się, czy oprogramowanie to może zostać zainstalowane na pozostałych maszynach.

Nawet pusta dyskietka może zawierać wirusa. W niektórych przypadkach samo włożenie zainfekowanej dyskietki może spowodować zainfekowanie maszyny, a włożenie czystej dyskietki do maszyny, która jest zainfekowana, może spowodować zainfekowanie tej dyskietki. Z tego powodu wszystkie dyskietki, które były używane w zainfekowanych maszynach lub są nieznanego pochodzenia, powinny być dokładnie sprawdzone. Można powiedzieć, że są „czyste" dopiero po przeprowadzeniu pełnego procesu kasowania ich zawartości, ale ponieważ dyskietki są coraz tańsze, to zainfekowane dyskietki łatwiej zniszczyć i użyć nowych.

Kradzież przez pracownika

Zbyt często administratorzy komputerów i sieci męczą się nad zabezpieczeniem swoich systemów tylko po to, aby tajemnice firmy zostały wyniesione z firmy w teczkach jej pracowników. Choć nie jest to zabezpieczenie sieci z technicznego punktu widzenia nie należy go ignorować. Kiedy myślimy o prywatności danych, to użytkownicy pracujący w sieci stają się potencjalnymi wrogami. Nie doprowadzaj do sytuacji, w której poprosisz wilka, aby popilnował Twoich owiec! Jedynym sposobem zabezpieczenia się przed wykradaniem danych z sieci przez jej użytkowników jest dobry system zapewniający prywatność danych oraz system kontroli dostępu. Jeśli złodziej nie będzie mógł uzyskać danych, to nie będzie ich mógł również ukraść. Dochodzimy więc do tego, że personel, któremu musimy zaufać, powinien być dokładnie sprawdzany.

Niezależnie od zaimplementowanych rozwiązań musisz pamiętać, że zawsze trzeba je wdrażać, zanim będą faktycznie potrzebne. Idealnie powinieneś opracować zabezpieczenia sieci już w czasie jej tworzenia i skoordynować je z planem bezpieczeństwa całej firmy. Niestety, prawie nikt tak nie postępuje. Większość administratorów sieci nie zajmuje się jej bezpieczeństwem do chwili wystąpienia problemu. Następnie w wielkim pośpiechu instalują oni różne rozwiązania zabezpieczające sieć przed powtórzeniem się ataku w przyszłości. Spośród tych, którzy zabezpieczają sieć, zanim jeszcze wystąpią problemy z jej bezpieczeństwem, większość wydaje się być postrzegana jak ludzie, którzy mają urojenia. Skupiają się oni zwykle na jednym aspekcie bezpieczeństwa, takim jak kontrola dostępu, i kompletnie ignorują inne potencjalne możliwości naruszenia bezpieczeństwa systemu. Albo też zajmują się głównie zabezpieczeniem sieci przed dostępem z zewnątrz, podczas gdy kompletnie ignorowane są próby naruszenia bezpieczeństwa *przez* własnych użytkowników.

Staraj się nie dołączyć do którejś z opisanych wyżej grup. Dobrze opracowany plan bezpieczeństwa sieci *musi* brać pod uwagę wszystkie możliwe zabezpieczenia i wszystkie aspekty związane z implementacją tych zabezpieczeń, *zanim* wystąpi ich naruszenie. Choć może Ci się wydawać, że Twój system i przechowywane w nim informacje nie jest ważne i warte ataku, to ktoś może mieć inne zdanie, a Ty możesz się przekonać, jaka była wartość tych danych, kiedy będzie już za późno.

Konfigurowanie interfejsów

A

Bez interfejsów nie byłoby czego rutować w sieciach IP. Ile czasu zajmuje konfigurowanie numerów IP na interfejsach Twojego rutera? Naprawdę niewiele. Skonfigurowanie IP na interfejsie rutera Cisco przybiera zwykle następującą formę:

```
interface type number ip address 172.16.52.34 255.255.255.0
  optional IP configuration statements such as proxy ARP
  interface-specific configuration statements
```

Parametr *type* w instrukcji `interface` jest zdefiniowaną w systemie nazwą przypisaną do typu interfejsów taką, jak ethernet, fddi lub `serial` , a parametr *number* jest numerem, który określa konkretny interfejs danego typu. System IOS numeruje interfejsy poczynając od zera, tak więc pierwszy interfejs sieci Ethernet będzie się nazywał `ethernet` O, a trzeci interfejs szeregowy - `serial` 2. W dużych ruterach numer interfejsu może przybierać formę zapisu *slot/number,* gdzie *slot* oznacza kolejny moduł rozszerzenia umieszczony w ruterze (numerowany od zera), a *number* określa numer konkretnego interfejsu znajdującego się w tym module rozszerzeń. Tak więc drugi interfejs Ethernet, znajdujący się na karcie modułu umieszczonego w pierwszym słocie rutera Cisco 75XX, będzie nazywany `ethernet 0/1`. Nowsze wersje ruterów z serii Cisco 75XX mogą stosować trzyczęściowy schemat numerowania interfejsów polegający na zapisie *slot/sub-slot/number.*

Po podaniu nazwy interfejsu następuje przypisanie temu interfejsowi adresu IP i maski sieci. Wykonywane jest to instrukcją `i p address`. Instrukcja ta zawiera minimalną liczbę informacji wymaganych przez IP do pracy z tym interfejsem, ale możliwe jest jeszcze dodanie innych instrukcji związanych z konfiguracją IP. Przykładem takich instrukcji mogą być polecenia włączające lub wyłączające obsługę proxy ARP, skierowane pakiety broadcast, pakiety IP multicast, itd. Żadna z tych instrukcji nie jest wymagana do uruchomienia rutowania IP, ale niektóre z nich mogą zmieniać zachowanie dynamicznego protokołu rutowania. Instrukcje te zostały omówione w odpowiednich rozdziałach tej książki.

Można więc stwierdzić, że konfiguracja każdego interfejsu może zawierać instrukcje, które są albo opcjonalne, albo wymagane do uruchomienia tego interfejsu. W mediach sieci LAN, takich jak Ethernet, Token Ring i FDDI, nie jest zwykle wymagana żadna dodatkowa konfiguracja interfejsów. Natomiast szeregowe interfejsy rutera mogą wymagać ustawienia parametrów enkapsulacji na poziomie protokołu łącza takiego jak PPP lub Frame Relay. Interfejsy skonfigurowane do pracy na żądanie wymagają konfiguracji określającej, kiedy mają nawiązywać połączenie, kiedy mają je rozłączać i jak mapować adresy protokołów na numery telefonów docelowych miejsc, pod które ruter ma dzwonić. Konfiguracja interfejsu do pracy z sieciami Frame Relay lub ATM jest jeszcze bardziej skomplikowana; konieczne jest określenie połączeń wirtualnych i powiązanie tych połączeń wirtualnych z adresami protokołów, które mają obsługiwać. Na zakończenie trzeba wspomnieć o interfejsach specjalnego przeznaczenia, takich jak połączenie z kanałem danych mainframe, których konfiguracja musi obsługiwać ścisłą współpracę rutera i hosta mainframe. Najlepszym miejscem, gdzie można uzyskać informacje o konfigurowaniu interfejsów, jest dokumentacja rutera, ale poniżej zaprezentuję kilka podstawowych instrukcji i zasad konfiguracji najczęściej wykorzystywanych interfejsów.

Tradycyjne media LAN - Ethernet, Token Ring i FDDI

Tradycyjne media sieci lokalnych, takich jak Ethernet, Token Ring i FDDI, pozwalają na dokonanie wyboru kilku parametrów konfiguracji. Dzieje się tak dlatego, że są to wszystko dość stare standardy i tak powszechnie stosowane, że domyślne wartości ustawiane przez ruter są prawie zawsze poprawne. Wynika to również z faktu, że są to standardy znacznie mniej elastyczne i nie wymagają takiej złożoności funkcji jak np. ATM.

Sieć Ethernet pozwala na dokonanie kilku wyborów. Jedyną ważną decyzją, którą musisz podjąć, jest metoda enkapsulacji datagramów IP stosowana w sieci. Masz do wyboru następujące metody:

- standardowa metoda ARPA Ethernet Version 2.0, która stosuje 16-bitowy kod typu protokołu. Jest to metoda domyślna i prawie zawsze jest tą, której powinieneś używać;
- SAP IEEE 802.3, w której kod typu staje się długością ramki dla enkapsulacji IEEE 802.2 LLC;
- metoda SNAP, zgodnie z definicją zawartą w RFC 1042, która pozwala protokołom sieci Ethernet pracować po mediach IEEE 802.2.

Domyślnie stosowane są ramki sieci Ethernet w wersji 2 i wynika to z jednego powodu - większość urządzeń obsługuje tylko ten standard ramki. Tak więc prawie nigdy nie będziesz musiał zmieniać metody enkapsulacji. Jeśli jednak zajdzie taka potrzeba, to w konfiguracji interfejsu Ethernet powinieneś użyć jednej z przedstawionych poniżej instrukcji `encapsulation`:

```
interface ethernet O ip address 172.16.52.34
  255.255.255.0
! for ARPA Ethernet Version 2.0 encapsulation (the default)
encapsulation arpa ! for IEEE 802.3 encapsulation
encapsulation sap
! for RFC 1042 SNAP encapsulation
encapsulation snap
```

Sieć Token Ring daje wybór pomiędzy większą liczbą opcji, ale i tak ich liczba jest dość ograniczona. Token Ring może pracować z szybkością 4 Mbps lub 16 Mbps; niektóre interfejsy sprzętowe wymagają podania, jaka szybkość stosowana jest w sieci. Aby to zrobić, należy użyć instrukcji `ring-speed`:

```
interface tokenring 1
  ip address 172.16.52.34 255.255.255.0 !
specify 4 Mbps speed
  ring-speed 4 ! or specify 16 Mbps
speed
  ring-speed 16
```

Możliwe jest również podanie parametru umożliwiającego wcześniejsze zwolnienie żetonu. Zwykle maszyna nie generuje żetonu, dopóki nie dostanie z powrotem z sieci swojej własnej ramki, co rozumiane jest jako zakończenie podróży ramki przez sieć. Wcześniejsze zwolnienie żetonu pozwala maszynie generować żeton natychmiast po wysłaniu ramki, ale zanim ramka ta zostanie z powrotem odebrana z sieci. Takie funkcjonowanie może doprowadzić do lepszego wykorzystania pasma sieci uzyskanego jednak kosztem kilku zabezpieczeń przed występowaniem w sieci błędów transmisji. Aby umożliwić wcześniejsze zwolnienie należy w konfiguracji interfejsu użyć następującej instrukcji:

```
early-token-release
```

Sieć FDDI udostępnia największą liczbę opcji do konfiguracji, ale prawie wszystkie z nich służą do kontroli czasów wykorzystywanych przez protokoły niższych warstw. Jeśli nie wiesz dokładnie, jakie są funkcje każdego z tych czasów i jaki wynik przyniesie ich zmiana, nie powinieneś dotykać tych wartości bez uzyskania wskazówek od zespołu technicznego Cisco. Bardzo łatwo zatrzymać pracę pierścienia FDDI. Jedyną wartością, którą kiedykolwiek zmieniałem, był czas TL-min, który kontroluje sterowanie sygnalizacją w warstwie fizycznej. Kiedy dodałem ruter Cisco do mojej sieci FDDI, w skład której wchodzą urządzenia innej firmy, musiałem ją zwolnić o kilka milisekund, aby kolejny ruter znajdujący się za Cisco miał więcej czasu na podniesienie pierścienia. Konfiguracja pokazana niżej podnosi wartość tego czasu do 200 mikrosekund, co jest wystarczającym czasem, aby cały pierścień pracował poprawnie:

```
interface fddi 2
  ip address 172.16.52.34 255.255.255.0
```

```
! slow down some low-level processing to allow the other routers to
\ keep up
fddi tl-min-time 200
```

Stałe łącza szeregowe

Stałe łącza szeregowe są trochę bardziej złożone niż tradycyjne media sieci LAN. Pierwszą decyzją jest wybór metody enkapsulacji, jaka będzie stosowana na takim łączu. Trzy najczęściej stosowane rozwiązania to: *Point to Point Protocol (PPP), High-level Data Link Control (HDLC)* i *Frame Relay.* Konfigurowanie łącza *Frame Relay* jest na tyle skomplikowane, że na jego opis przeznaczyłem oddzielną część tego rozdziału. Najważniejszą różnicą pomiędzy PPP i HDLC jest to, że PPP jest standardem otwartym, zdefiniowanym przez społeczność internetową, podczas gdy HDLC jest wykonaną przez ISO modyfikacją protokołu *Synchronous Data Link Control (SDLC),* opracowanego przez IBM. Każdy z tych dwóch protokołów potrafi obsługiwać kilka protokołów wyższych warstw i każdy ma niewielkie zalety. Prawdopodobnie największą zaletą PPP jest fakt, że protokół ten jest stosowany przez większość producentów, gdyż jest standardem sieci Internet. Jeśli pracujesz tylko i wyłącznie na sprzęcie Cisco, to nie ma żadnego powodu, aby wybierać tylko jeden z tych protokołów. HDLC jest domyślnie stosowanym protokołem w ruterach Cisco, ale zawsze możesz wybrać PPP za pomocą instrukcji encapsulation:

```
interface serial 0
 ip address 172.16.52.34 255.255.255.0
 ! select PPP as the encapsulation protocol on this interface
 encapsulation ppp
```

Jeśli zdecydujesz się na użycie PPP, to prawdopodobnie będziesz chciał lub musiał uruchomić protokół autentykacji. Protokołu takiego nie musisz stosować na stałych łączach szeregowych, ponieważ druga strona połączenia jest dobrze znana, ale konfiguracja PPP jest taka sama, niezależnie od tego, czy protokół jest wykorzystywany do obsługi łącza dzierżawionego, czy też łącza zestawianego na żądanie. Pomijam tu sytuację, kiedy administrator sieci, z którą się łączysz, nalega na stosowanie autentykacji po to, by się zabezpieczyć przed przerwaniem łącza i włączeniem w nie kogoś, kto ma złe zamiary. W celu wykonania autentykacji możliwe jest zastosowanie jednej z dwóch metod obsługiwanych przez PPP (żadna z nich nie jest obsługiwana przez HDLC): protokół *Password Authentication Protocol (PAP)* oraz *Challenge Handshake Authentication Protocol (CHAP).* Protokół PAP jest starszy, mniej skomplikowany i nadal częściej stosowany. Korzystający z PAP ruter, który nawiązuje połączenie, wysyła do drugiego rutera nazwę użytkownika i jego hasło w celu „załogowania się" do łącza. Odbierający prośbę o zestawienie połączenia ruter stwierdza ważność przekazanych informacji, akceptuje połączenie lub je odrzuca. Protokół CHAP działa inaczej, zapobiegając przesyłaniu hasła przez łącze. Pracujący z protokołem CHAP ruter, który odbiera połączenie, wysyła inicjujący ciąg znaków do rutera, który chce się z nim połączyć. Inicjujący połączenie ruter odbiera te dane i szyfruje je za pomocą

swojego hasła, a następnie odsyła powstały ciąg znaków z powrotem. Ruter ten stosuje również kodowanie ciągu znaków za pomocą hasła rutera, który chce nawiązać połączenie. Jeśli zakodowane w tym procesie ciągi znaków pasują do siebie, to ruter nawiązujący połączenie zostaje uwierzytelniony. Aby skonfigurować obsługę protokołu PAP lub CHAP na swoim ruterze, powinieneś użyć polecenia:

```
interface serial O
 ip address 172.16.52.34 255.255.255.0
 encapsulation ppp ! or use ppp authentication pap

 ppp authentication chap
 user-name name1 password secret1
 user-name name2 password secret2
```

Konieczne jest podanie nazwy użytkownika i jego hasła dla każdego z ruterów, który będzie nawiązywał połączenie z naszym ruterem lub z którym my będziemy się łączyli. Oczywiście możesz nie używać żadnej autentykacji. Wybór należy do Ciebie, ale jeśli łącze zestawiane na żądanie skonfigurujesz bez żadnej autentykacji, to stworzysz w ten sposób dziurę w zabezpieczeniach swojej sieci.

Niezależnie od tego, czy wybierzesz PPP czy też HDLC, możliwe będzie zastosowanie kompresji w warstwie łącza, która poprawi wykorzystanie dostępnego pasma. Dostępne algorytmy kompresji *zależą* od wybranej enkapsulacji. Protokół PPP może wykorzystywać zarówno schemat kompresji oparty na przewidywaniu (algorytm RAND) lub schemat kompresji Stacker, opracowany przez firmę STAĆ Inc. W przypadku protokołu HDLC wybór ograniczony jest do algorytmu Stacker. Aby włączyć kompresję w warstwie łącza należy w konfiguracji umieścić jedną z podanych niżej instrukcji:

```
interface serial 0
 ip address 172.16.52.34 255.255.255.0
 encapsulation ppp
 compress predictor
! or
 compress stac
!
interface serial 1
 ip address 172.16.53.17 255.255.255.0
 encapsulation hdlc
 compress stac
```

Obie strony połączenia muszą używać tego samego typu kompresji lub żadnego. Większość ruterów Cisco nie ma wbudowanej żadnej obsługi kompresji sprzętowej -główny procesor CPU musi obsługiwać algorytm kompresji. Jeśli więc zdecydujesz się na włączenie kompresji, to powinieneś dokładnie monitorować wykorzystanie CPU rutera. Jeśli obciążenie procesora będzie przekraczało stale 65 procent to należy, bezzwłocznie wyłączyć obsługę kompresji.

Łącza zestawiane na żądanie

Łącza zestawiane na żądanie mogą używać kilku technologii telekomunikacyjnych. Spośród nich najczęściej stosowane są przełączane synchroniczne łącza szeregowe, modemy analogowe oraz technologia ISDN. Wszystkie wymienione technologie mają więcej cech wspólnych niż różnic, tak więc będę omawiał je wszystkie razem. Z punktu widzenia protokołu IP lub każdego innego protokołu sieciowego, łącza zestawiane na żądanie wyglądają tak samo jak interfejs szeregowy, jeśli tylko są one w użyciu. Konfiguracja protokołu IP jest prosta i łatwa do wykonania. Kłopoty zaczynają się wtedy, kiedy chcemy powiązać adres IP z odpowiednimi numerami telefonów, które ruter ma wybierać,* kiedy chcemy określić, jak i kiedy ruter ma zestawiać połączenie i kiedy ma je rozłączyć.

Mapowanie adresów IP na numery telefonów wykonywane jest zwykle za pomocą statycznego odwzorowania odpowiednich wartości, przechowywanego w każdym z ruterów. Może to oznaczać konieczność wpisywania wielu danych, jeśli korzystasz z wielu połączeń zestawianych na żądanie. Ponieważ jednak większość informacji może być wymieniana pomiędzy ruterami, po wykonaniu tego odwzorowania poza ruterem możliwe jest wykonanie prostego przetwarzania tych danych i dołączenie ich do konfiguracji wielu ruterów w postaci wspólnego pliku. Mapy można skonfigurować, dodając do konfiguracji interfejsu instrukcje d i a l e r ma p:

```
dialer map ip 192.168.100.1 5551212
dialer map ip 192.168.100.17 5558891
```

Zapisy te informują ruter, że adres IP 192 .168.100 . l można osiągnąć łącząc się z numerem 555-1212, natomiast adres 192.168.100.1 pod numerem 555-8891. Jeśli interfejs obsługujący połączenia zestawiane na żądanie dołączony jest do linii ISDN, możliwe jest dodanie opcjonalnego parametru określającego szybkość połączenia, która dla niektórych połączeń może wynosić 56 kbps, a dla innych 64 kbps:

```
dialer map ip 192.168.100.1 5551212 speed 56 dialer map ip
192.168.100.17 5558891 speed 64
```

Najtrudniejszą częścią procesu konfiguracji jest poinformowanie rutera o tym, w jaki sposób należy zestawiać połączenie. W przypadku łącza ISDN podaje się informację o tym, do jakiego przełącznika ISDN jest on dołączony i jak ma się identyfikować przy łączeniu z tym przełącznikiem. Na przykład aby poinformować ruter, że dołączony jest do przełącznika Northern Telecom DMS-100, konfiguracja musi wyglądać następująco:

*W związku z brakiem lepszego określenia, nazwa „numer telefonu" będzie oznaczała ciąg znaków używany do identyfikowania części sieci, z którą chcemy nawiązać połączenie. Nie należy zakładać, że chodzi tu o zwykłe połączenia telefoniczne.

```
isdn switch-type basic-dms100
interface bri 0
 ip address 172.16.52.34 255.255.255.0
 isdn spidl 888555121201
 isdn spid2 888555121301
```

Zwróć uwagę na to, że typ przełącznika podany jest *poza* konfiguracją samego interfejsu. Jest to globalna instrukcja konfiguracji rutera; wszystkie interfejsy ISDN pracujące na jednym ruterze muszą być dołączone do tego samego typu przełącznika ISDN. Przedstawiona konfiguracja zawiera również wartość parametrów o nazwie *Senńce Profile Identifiers (SPIDs)* dla moich łączy ISDN przyłączonych do interfejsu. W zależności od rodzaju usługi ISDN, jaką otrzymujesz, liczba tych wartości może być równa zero, jeden lub dwa. Informację tę musi przekazać Ci firma telekomunikacyjna - NIE WOLNO wpisywać tu żadnych własnych liczb! Jeśli wpisane wartości tych parametrów będą błędne, to sieć ISDN nie będzie z Tobą rozmawiała.

W przypadku stosowania łączy obsługiwanych przez modemy analogowe skonfigurowanie sposobu wybierania numeru jest znacznie trudniejsze. Najpierw musisz powiedzieć ruterowi, że ma obsługiwać interfejs łącza na żądanie, używając do tego instrukcji `dialer in-band`, pokazanej poniżej. Taka instrukcja informuje ruter, że może on komunikować się z modemem przesyłając do niego polecenia umieszczone wraz z danymi. Polecenia te należy wyszczególnić w skrypcie *chat,* który poinformuje ruter o ich wykorzystywaniu, robiąc to w sposób następujący: „Jeśli modem wysyła do ciebie *to,* to ty w odpowiedzi masz do niego wysłać *to."* Skrypt *chat* przedstawiony w dokumentacji systemu IOS Cisco, jest następujący:. . . . . .

```
chat-script dial ABORT ERROR "" "AT Z" OK "ATDT \T" TIMEOUT 30 CONNECT \c
```

Instrukcje te tworzą skrypt o nazwie `dial`, a następnie definiują pary *expect-send.* Są dwie wartości specjalne typu *expect.* ABORT mówi ruterowi, aby przerwał wykonywanie skryptu, jeśli tekst występujący po ABORT pojawi się w strumieniu wejściowym nadsyłanym z modemu. Liczba skonfigurowanych warunków ABORT może być dowolna. Kolejną wartością specjalną jest TIMEOUT. Ustawia ona zegar, który będzie określał czas, przez jaki ruter będzie oczekiwał na nadejście odpowiedniego ciągu znaków, zanim nie zgłosi komunikatu o błędzie. Domyślną wartością jest pięć sekund. We wszystkich innych przypadkach pary wartości tworzą ciąg, który ma być krok po kroku wykonywany przez ruter. Tak więc w tym skrypcie ruter najpierw spodziewa się usłyszeć cokolwiek (pusty ciąg znaków), a następnie wysyła do modemu komendę AT *I.* Po jej wysłaniu powinien odebrać ciąg OK; odpowiada na niego ATDT, po którym umieszczany jest numer, z jakim należy nawiązać połączenie (parametr \T zamieniany jest na odpowiedni numer telefonu). Następnie ruter dostaje polecenie zwiększenia czasu oczekiwania do 30 sekund, co daje urządzeniu, do którego zestawiamy połączenie, czas na wysłanie odpowiedzi. Jeśli kolejnym ciągiem znaków, jaki zobaczy ruter, będzie C O N N E C T, to ma wysłać pusty ciąg znaków (parametr \ c oznacza nie wysyłanie niczego), i skrypt kończy zadanie pomyślnie. Oczywiście stosowany w rzeczywistości skrypt *chat* będzie prawdopodobnie bardziej szczegółowy niż ten przykład. Istnieje wiele specjalnych ciągów, które zdefiniowane są do obsługi różnych sytuacji.

Przy tworzeniu takich skryptów najlepiej posługiwać się dokumentacją modemu, a także dokumentacją Cisco. Zawsze konieczne będzie wykonanie kilku testów i usunięcie pojawiających się w przygotowanym skrypcie błędów.

Kiedy już stworzysz odpowiedni skrypt *chat,* musisz przypisać go do interfejsu obsługującego połączenie na żądanie, do którego dołączony jest modem:

```
interface async O
 ip address 172.16.52.34 255.255.255.0
 dialer in-band
 script dialer dial
```

Polecenia te informują ruter, że kiedy będzie chciał użyć tego interfejsu, do rozmowy z modemem powinien użyć skryptu o nazwie dial.* Jest jeszcze wiele innych opcji stosowanych w skryptach nawiązujących połączenie; dostępne są nawet polecenia pozwalające tworzyć skrypty logowania dla odległych miejsc w sieci. Nie będę tu podawał szczegółów tych wszystkich poleceń. Jeśli chcesz konfigurować modem analogowy obsługujący łącze zestawiane na żądanie, powinieneś zajrzeć do dokumentacji IOS.

Po wykonaniu opisanych wyżej poleceń mamy odwzorowane numery telefonów na adresy IP i powiedzieliśmy ruterowi, w jaki sposób ma zestawiać połączenia. Pozostało jeszcze skonfigurowanie parametrów zestawiania połączenia i rozłączania go. Aby móc kontrolować, kiedy połączenie jest zestawiane, konieczne jest zastosowanie listy kontroli dostępu, która będzie określała pakiety na tyle *interesujące, aby* połączenie było nawiązane. Może to być nieskomplikowana lista dostępu lub lista rozszerzona. Podstawowa lista dostępu, która będzie powodowała zestawienie połączenia za każdym razem, kiedy pakiet nadesłany zostanie z podsieci 172.16.25.0/24 lub 172.16.80.0/23, będzie wyglądała następująco:

```
interface async O
 ip address 172.16.52.34 255.255.255.0
 dialer in-band
 script dialer dial
 dialer-group 1
! define uhat we consider interesting packets
access-list 27 permit 172.16.25.0 0.0.0.255
access-list 27 permit 172.16.80.0 0.0.1.255
! associate the access list of interesting packets with a dialer group
dialer-list 1 list 27
```

Nazwa skryptu jest wyrażeniem regularnym, które pozwala zdefiniować grupę skryptów zachowujących się podobnie i następnie wybierać z niej ten skrypt, który spełnia określone warunki. Ponieważ ciąg znaków jest wyrażeniem regularnym, które odpowiada samemu sobie, zawsze możliwe jest użycie nazwy skryptu *chat,* jeśli tylko taki skrypt jest przygotowany.

Łącza zestawiane na żądanie

Po poinformowaniu rutera o tym, że interfejs obsługuje zestawiane na żądanie połączenie, co zostało wykonane za pomocą instrukcji d i a l er i n-demand, musimy jeszcze poinformować ten ruter, do której grupy ten interfejs należy. Możliwe jest stworzenie najwyżej dziesięciu takich grup (o numerach od l do 10). Następnie konfiguracja mówi ruterowi, jaki ruch powinien być uznany za interesujący, wykorzystując do tego celu listę dostępu 27. Lista ta zostaje przypisana do grupy wybierania numerów za pomocą instrukcji d i a 1 er -1 i s t. Kiedy jakikolwiek pakiet zgodny z listą dostępu 27 będzie wysyłany na ten interfejs, ruter wybierze numer miejsca przeznaczenia pakietu i wyśle ten pakiet po nawiązaniu połączenia. Lista dostępu, którą definiujesz, może być tak złożona, jak tylko uznasz to za stosowne. Na przykład dzięki temu, że możliwe jest użycie rozszerzonych list dostępu, możesz filtrować ruch z uwzględnieniem protokołu TCP lub UDP, adresów źródłowego i docelowego lub dowolnej kombinacji tych parametrów. Na przykład lista dostępu, która będzie chroniła przed zestawianiem połączenia przez pakiety ICMP (chyba że są one przesyłane z maszyny o adresie 172.16.27.34)1 będzie przesyłała ruch z dowolnego komputera z podsieci 172.16.98.0/24, będzie wyglądała następująco:

```
access-list 127    permit ip 172.16.27.34 0.0.0.0              172.16.98.0 0.0.0.255
access-list 127    deny icmp 0.0.0.0 255.255.255.255           0.0.0.0 255.255.255.255
access-list 127    permit ip 0.0.0.0 255.255.255.255           0.0.0.0 255.255.255.255
```

Pierwsza instrukcja access-list mogłaby również specyfikować ICMP, ale metoda rozdzielenia protokołów, jaką tu zastosowałem, sprawia, że przetwarzanie listy dostępu wykonywane jest szybciej, jeśli adres spełnia jej warunki; przypomnij sobie, że analiza listy kończona jest przy pierwszym trafieniu. Należy pamiętać o tym, że lista dostępu obsługująca zestawianie połączeń nie nakłada żadnych ograniczeń na to, jaki ruch przesyłany jest tymi połączeniami, lecz decyduje tylko o tym, co jest interesujące na tyle, aby spowodowało nawiązanie połączenia. Kontrola dostępu zapewniana jest przez instrukcję ip access-group, o której mowa w rozdziale 10, „Bezpieczeństwo sieci".

Wszystko, co jeszcze musimy zrobić, to przekazać ruterowi informację o tym, kiedy ma rozłączać nawiązane połączenie. W systemie IOS rozłączanie obsługiwane jest przez licznik mierzący czas, kiedy łącze nie jest aktywne. Za każdym razem, kiedy ruter przesyła jakiś pakiet, który jest na tyle interesujący, aby podnieść interfejs, to pakiet taki powoduje wyzerowanie licznika. Jeśli licznik, odliczając czas braku aktywności łącza, osiągnie wartość graniczną, podaną w konfiguracji (domyślnie jest to 120 sekund), to łącze jest rozłączane. Dla każdego interfejsu można określać czas oczekiwania przed rozłączeniem, dodając w konfiguracji interfejsu następującą instrukcję:

```
! set the idle timeout for this interface to 5 minutes (300 seconds) dialer idle-timeout 300
```

Jeśli interfejs pracuje w stanie połączenia, ponieważ odebrał żądanie nawiązania tego połączenia z zewnątrz, a interesujący pakiet powinien być wysłany do innego miejsca, to ruter użyje innego licznika, który ma zwykle krótszy czas nieaktywności.

Licznik ten konfigurowany jest za pomocą instrukcji `dialer fast-i die`, a jego domyślna wartość to 20 sekund. Jeśli ten szybszy licznik jest wywoływany zbyt często, to powinieneś zastanowić się nad dodaniem większej liczby modemów do rutera. Takie ciągłe przełączanie się z jednego połączenia na drugie może w znacznym stopniu ograniczyć przepustowość sieci i w efekcie więcej kosztować.

Kiedy połączenie zostaje nawiązane, dalsza jego konfiguracja wygląda dokładnie tak samo jak w przypadku łącza stałego. Konieczne jest więc skonfigurowanie opcji określających typ wykorzystywanej enkapsulacji, wykorzystania PAP lub CHAP dla protokołu PPP oraz rodzaju kompresji warstwy łącza. Aby dowiedzieć się, jak wykonać konfigurację wspomnianych wyżej parametrów, przeczytaj opis konfiguracji stałych łączy szeregowych. Jest wiele sposobów dostrojenia zachowania łączy zestawianych na żądanie. Opcje te wykraczają jednak poza zakres tematów poruszanych w tej książce i więcej informacji na ten temat znajdziesz w dokumentacji IOS.

Frame Relay

Frame Relay nie jest specjalnym rodzajem interfejsu w sensie sprzętowym: jest to metoda enkapsulacji, która może pracować nad prawie każdym typem interfejsu szeregowego. Technologia ta jest najczęściej stosowana na stałych szeregowych łączach synchronicznych. Ruter lub host pracujący na łączu szeregowym łączy się zwykle z przełącznikiem, który jest własnością prywatną lub jest obsługiwany przez firmę telekomunikacyjną. *Frame Relay* jest technologią przełączania pakietów, która pozwala na multipleksowanie kilku logicznych strumieni danych do postaci jednego łącza fizycznego. Te logiczne strumienie danych nazywane są kanałami wirtualnymi (logicznymi) i identyfikowane są przez *Data-Link Connection Identifier (DLCI).* Wartość DLCI ma jedynie znaczenie na poziomie logicznej obsługi kanałów we *Frame Relay.* Nie może ono mieć (i zwykle nie ma) żadnego wpływu na pracę każdego z fizycznych łączy działających w sieci *Frame Relay.*

Możliwa jest obsługa dwóch typów kanałów wirtualnych. Stały kanał wirtualny (PVC) jest tworzony przez administratora przełącznika i będzie istniał w sieci do czasu, kiedy nie zostanie z niej przez administratora usunięty. Taki kanał jest zasadniczo odpowiednikiem stałego łącza szeregowego. Innym typem kanałów logicznych jest przełączany kanał logiczny (SVC). Kanał SVC tworzony jest na żądanie przez oprogramowanie i trwa w sieci tylko tyle, na ile został zestawiony, i zostaje usunięty przez oprogramowanie, podobnie jak to ma miejsce w przypadku połączeń telefonicznych. Choć sieci *Frame Relay* zostały ostatnio rozwinięte i można w nich wykorzystywać oba typy kanałów, to większość sieci *Frame Relay* nadal zapewnia obsługę jedynie kanałów PVC. Z tego powodu nie będę w tej książce omawiał metod konfigurowania kanałów SVC w sieci *Frame Relay.*

Ponieważ poszczególne kanały są w sieci *Frame Relay* multipleksowane do postaci jednego łącza fizycznego, interfejs *Frame Relay* może pracować w dwóch trybach. Jednym z nich jest tryb obsługi połączenia punkt-punkt, kiedy interfejs pracuje jak tradycyjne łącze szeregowe. Tak skonfigurowany interfejs rozmawia z jednym urządzeniem pracującym po drugiej stronie jednego kanału logicznego, co znacznie upraszcza konfigurację łącza *Frame Relay.*

W takim przypadku mapowanie pomiędzy adresami sieciowymi a kanałami logicznymi jest bezpośrednie - druga strona kanału wirtualnego powinna być obsługiwana przez ruter lub host, którego się spodziewasz w konfiguracji swojego rutera. W trybie obsługi wielu kanałów urządzenie może komunikować się jednocześnie z kilkoma różnymi odległymi urządzeniami, z których każde dołączone będzie do jednego z kanałów logicznych. Nadal jednak każdy z tych kanałów można traktować jak połączenie punkt-punkt. Choć tak skonfigurowane urządzenie może rozmawiać po kolei ze wszystkimi urządzeniami dołączonymi do logicznych kanałów, nie może ono wysłać pakietu typu broadcast jednocześnie na wszystkie te kanały, lecz musi taki pakiet wysyłać po kolei do każdego z kanałów logicznych. Ten rodzaj pakietów *pseudo broadcast* jest dość drogim rozwiązaniem, zarówno pod względem mocy potrzebnej do ich obsługi, jak i zajętości pasma sieci -każdy pakiet broadcast wysyłany jest kilka razy przez łącze.

Zanim zaczniemy omawiać konfigurację *Frame Relay,* powinieneś zrozumieć ideę interfejsów logicznych. Niektóre technologie, zwłaszcza *Frame Relay* i ATM, pozwalają na równoczesną obsługę kilku interfejsów logicznych na tym samym interfejsie fizycznym. Każdy z tych logicznych interfejsów może mieć własny adres IP, maskę sieci i tak dalej. Na tym właśnie polega różnica pomiędzy powyższym rozwiązaniem a multipleksowaniem, które wykonywanie jest w kanałach logicznych. Każdy interfejs logiczny może obsługiwać jeden lub kilka kanałów logicznych, które są z nim skojarzone, ale zwykle każdy taki kanał logiczny skojarzony jest tylko z jednym interfejsem logicznym. Aby pozwolić na niezależną konfigurację wielu interfejsów logicznych, IOS stosuje rozwiązanie o nazwie pod-interfejsy (sub-interface). Nazwa takiego pod-interfejsu jest taka sama jak nazwa interfejsu podstawowego z dodaną po niej kropką i numerem tego pod-interfejsu. Na przykład nazwa `serial 2.3` oznacza trzeci pod-interfejs podstawowego interfejsu o nazwie `serial 2`. Zwróć uwagę na to, że nie jest to czwarty pod-interfejs, ponieważ w tym systemie oznaczeń pod-interfejs O oznacza to samo, co interfejs podstawowy. Posługiwanie się takim systemem nazw interfejsów wymaga trochę doświadczenia, zwłaszcza kiedy okazuje się, że niektóre polecenia konfiguracyjne można stosować tylko przy konfigurowaniu pod-interfejsów, a inne tylko przy konfigurowaniu interfejsów podstawowych. W praktyce koncepcja ta staje się dość szybko łatwa w użyciu, a IOS jest dość przyjaznym systemem dzięki kontekstowej pomocy dokładnie informującej, które instrukcje gdzie można stosować. Niestety większość konfiguracji *Frame Relay* nie może działać bez wykorzystywania tych logicznych interfejsów. W poniższym opisie będę stosował określenie „interfejs" dla nazwania właśnie takich pod-interfejsów. Mam nadzieję, że takie uproszczenie nie będzie zbyt mylące.

Oprócz poinformowania rutera o istnieniu kanałów logicznych zasadniczym przedmiotem konfiguracji jest odwzorowanie adresów IP na numery DLCI. Sposób, w jaki jest to wykonywane, zależy od tego, czy interfejs pracuje w trybie punkt-punkt, czy wielokierunkowo. Interfejsy punkt-punkt mogą pracować z wykorzystaniem jednego z dwóch trybów: *implicit* lub *explicit.* W pierwszym trybie ruter zakłada po prostu, że urządzenie znajdujące się po drugiej stronie kanału logicznego musi dopasować się do adresu IP, który jest wysyłany.

Jest to koncepcja zbliżona do stosowania nienumerowanych łączy punkt-punkt, a interfejsy punkt-punkt pracujące w sieci *Frame Relay* mogą być konfigurowane jako interfejsy nienumerowane. W obu przypadkach konieczne jest jedynie przypisanie numeru DLCI do danego interfejsu:

```
interface serial O
! configure the main interface for Frame Relay encapsulation
 encapsulation frame-relay ietf
! now create a point-to-point sub-interface and give it an IP address
Interface serial 0.1 point-to-point
 ip address 172.16.52.34 255.255.255.252
! finally, associate DLCI 192 with this sub-interface
! the mapping from IP address to DLCI will be implicit
 frame-relay interface-dlci 192
```

Drugą opcją jest wykonanie dokładnego mapowania adresu IP na numer DLCI sieci *Frame Relay*. W takim przypadku z kolei zamiast informować ruter o tym, że DLCI ma być powiązane z danym interfejsem, umieszczana jest instrukcja, która mapuje adres IP na numer DLCI:

```
interface serial O
! configure the main interface for Frame Relay encapsulation
 encapsulation frame-relay ietf
! now create a point-to-point sub-interface and give it on IP address interface serial
0.1 point-to-point
 ip address 172.16.52.34 255.255.255.252     '
! explicitly map the remote IP address to DLCI 192                    >
 frame-relay map 172.16.52.35 192
```

Rzadko będziesz używał opcji mapowania *explicit;* mapowanie *implicit* (bezwarunkowe) jest łatwiejsze w obsłudze, ponieważ adres IP odległego miejsca nie musi być w nim wyraźnie skonfigurowany.

Kiedy interfejs pracuje w trybie obsługi wielu połączeń, jego konfiguracja staje się jeszcze ciekawsza. Ruter nie może na podstawie DLCI wnioskować, jaki jest adres IP odległego urządzenia, ponieważ jego interfejs skojarzony jest z wieloma DLCI i wieloma adresami IP. Tu także istnieją dwie opcje konfiguracji. Tak jak możliwe było wyraźne skonfigurowanie mapowania pomiędzy adresem IP a DLCI na interfejsie punkt-punkt, można to zrobić tak samo (statycznie) mapując kilka adresów IP z podsieci na numery DLCI na interfejsie. Wykonuje się to za pomocą kilka razy powtórzonej instrukcji frame- reley map:

```
interface serial O
! configure the main interface for Frame Relay encapsulation
 encapsulation frame-relay ietf
! now create a multipoint sub-interface and give it an IP address interface serial
0.1 multipoint
 ip address 172.16.52.34 255.255.255.0 ! explicitly map each remote
 IP address to the correct DLCI
```

```
frame-relay map 172.16.52.35 192 frame-relay map
172.16.52.109 314 broadcast frame-relay map
172.16.52.212 789 broadcast
```

Słowo kluczowe `broadcast` informuje ruter, że na tym DLCI należy rozsyłać pakiet pseudo broadcast. Domyślnie na żadnym DLCI nie są rozsyłane pakiety broadcast. *Zwróć* uwagę na to, że nie musimy informować rutera, które numery DLCI są dostępne. Informacja ta wynika z wykonanego mapowania adresów IP na DLCI. Konieczne jest jednak umieszczenie w konfiguracji mapowania dla każdej odległej pary tworzonej przez adres IP i DLCI, co może powodować konieczność wykonania dość dużej pracy w przypadku używania dużej sieci *Frame Relay.* Wykorzystujemy tu alternatywną metodę mapowania. Jeśli poinformujemy ruter o wszystkich DLCI, ale nie powiemy, które adresy IP należy skojarzyć z tymi numerami, to ruter będzie wysyłał odwrotne zapytanie ARP do odległego urządzenia i otrzymywał w odpowiedzi jego adres IP. Na podstawie uzyskanej w ten sposób tabeli odpowiedzi ruter będzie budował mapowanie dynamicznie:

```
interface serial O
! configure the main interface for Frame Relay encapsulation
 encapsulation frame-relay ietf
! now create a multipoint sub-interface and give it an IP address interface serial 0.1
multipoint
 ip address 172.16.52.34 255.255.255.0
! dynamically map each remote IP address to the correct DLCI using ! inverse ARP
on these DLCIs
 frame-relay interface-dlci 192
 frame-relay interface-dlci 314
 frame-relay interface-dlci 789
```

Statyczne odwzorowanie adresów daje większą kontrolę kosztem konieczności wykonywania tego przyporządkowania na każdym z ruterów (a jest ono inne na każdym z ruterów). Natomiast dynamiczne odwzorowanie pozwala zepchnąć więcej pracy na rutery. To, którą z metod powinieneś zastosować w swojej sieci *Frame Relay,* zależy od jej wielkości, częstości zmian konfiguracji kanałów logicznych i zakresu kontroli nad siecią, jaki chcesz sobie zostawić.

Teraz kilka ostatnich uwag dotyczących interfejsów Frame Relay. Po pierwsze, wszystkie logiczne interfejsy tworzone na podstawie interfejsu podstawowego muszą stosować taką samą enkapsulację. Nie ma sensu konfigurowanie interfejsu serial 0.1 do pracy z *Frame Relay,* a interfejsu serial 0.2 do pracy z PPP. Z tego powodu instrukcja opisująca wybrany typ enkapsulaqi jest stosowana tylko w konfiguracji interfejsu podstawowego. Po drugie, nie ma powodu, aby nie mieszać logicznych interfejsów punkt-punkt i interfejsów *multipoint w* jednym interfejsie fizycznym. Należy jednak pamiętać, że będą one traktowane jako różne interfejsy i nie będą nawzajem widziały generowanego w sobie ruchu. Na zakończenie należy podkreślić, że choć większość opcji określonych dla interfejsu podstawowego ma wpływ na jego interfejsy logiczne, to nie dotyczy to wszystkich skonfigurowanych parametrów. Niektóre z wartości parametrów skonfigurowanych dla interfejsu podstawowego mogą być ponadto zmieniane przez parametry konfiguracji jego pod-interfejsów. Jeśli będziesz miał

wątpliwości co do parametrów konfiguracji interfejsów, zajrzyj do dokumentacji IOS, porozmawiaj z kimś bardziej doświadczonym i poeksperymentuj na swojej sieci testowej.

Asynchronous Transfer Mode (ATM)

W wielu aspektach działanie ATM podobne jest do technologii *Frame Relay.* Wiele / podstawowych założeń, określeń i metod stosowanych w technologii ATM zostało zapożyczonych z *Frame Relay.* Na przykład ATM działa w oparciu o kanały wirtualne. Nie chcę przez to powiedzieć, że ATM jest następcą *Frame Relay* (choć niektórzy tak myślą). Należy raczej stwierdzić, że każda z tych technologii ma swoje zalety, obsługuje różne sieci i ma inne zadania. *Frame Relay* jest rozpatrywany jako technologia sieci WAN i stara się optymalnie wykorzystywać łącza, na których pracuje. Natomiast ATM jest pomyślany jako technologia zarówno sieci LAN, jak i WAN, pozwalająca na ich łączenie. Głównym celem w technologii ATM jest szybkość pracy, zapewnienie kontroli usług sieciowych i gwarancji pasma.

Są jeszcze inne różnice pomiędzy *frame Relay* a ATM. Na przykład *Frame Relay* opiera się na ramkach zmiennej długości, podobnie jak tradycyjne media sieci LAN, ATM natomiast na *komórce* stałej długości, która wynosi 53 oktety. Tak mały rozmiar komórki wybrany został po to, by można było szybko i wydajnie przełączać komórki. Niestety w związku z małym rozmiarem komórki pojedynczy pakiet IP musi być dzielony i przesyłany w wielu takich komórkach. Jeśli którakolwiek z nich zostanie utracona, to odrzucany jest cały pakiet. Dlatego sieci ATM muszą być projektowane tak, aby utrata komórek była możliwie najmniejsza.

W przeciwieństwie do *Franie Relay,* interfejs ATM jest specjalnie zaprojektowanym do tego celu interfejsem rutera; technologia *Frame Relay* wykorzystywała każdy odpowiedni interfejs szeregowy. Taki interfejs ATM jest dołączony do przełącznika sieci ATM za pomocą jednego z kilku dostępnych mediów fizycznych obsługujących różne szybkości. Powszechnie stosowane kombinacje medium i szybkości pracy są następujące:

- światłowód 622 Mbps (OC-12);
- światłowód 155 Mbps (OC-3);
- miedziana skrętka kablowa kat. 5 155Mbps;
- światłowód 100 Mbps (TAXI);
- kabel koncentryczny 45 Mbps (DS-3).

Istnieje również standard o przepustowości 25 Mbps, pracujący po miedzianej skrętce kablowej, ale nie wydaje się, żeby wzbudzał on szczególne zainteresowanie na rynku. Być może wynika to z faktu, że nie jest on znacznie szybszy od przełączanego Ethernetu, a jednocześnie jest znacznie droższy od technologii Fast Ethernet 100 Mbps. Niezależnie od rodzaju użytego medium i szybkości pracy, konfiguracja rutera jest zawsze taka sama.

Wirtualne kanały w sieci ATM identyfikowane są za pomocą dwóch numerów. Pierwszy z nich, określany jako *virtual path identifier* (VPI), identyfikuje grupę kanałów logicznych, które mogą być razem przełączane przez działające w sieci przełączniki. Większość oprogramowania i systemów spodziewa się, że dla większości aplikacji wartość VPI będzie wynosiła O, i powinieneś stosować tę wartość, chyba że dokładnie wiesz, co chcesz osiągnąć, stosując inną wartość. Drugim numerem jest *virtual channel identifier* (VCI). Definiuje on kanał wewnątrz grupy opisanej numerem VPI. Numery VCI poniżej 32 są zarezerwowane przez organizację ATM Forum dla obsługi specjalnych, dobrze znanych usług, która jest organizacją zajmującą się opracowaniem standardów sieci ATM. W dalszej części tego opisu zetkniemy się z dwoma takimi kanałami. Numery VPI/VCI pozwalają na jednoznaczne określenie kanałów logicznych, podobnie jak to było w przypadku DLCI w sieci *Frame Relay* i mają znaczenie tylko dla jednego fizycznego łącza w sieci - zestawionego pomiędzy hostem a przełącznikiem lub pomiędzy dwoma przełącznikami. Numery te mogą się zmieniać (i zwykle tak się dzieje) w każdym z łączy fizycznych. Oznacza to, że kiedy ruter A identyfikuje kanał prowadzący do rutera B jako 0/32, to ruter B może ten sam kanał widzieć jako 0/67, ale nadal jest to ten sam kanał wirtualny.

Wirtualne kanały stosowane w sieciach ATM również mają dwie odmiany - stałe kanały o nazwie *permanent virtual circuits* (PVC) i przełączane kanały o nazwie *switched virtual circuits* (SVC). PVC są przeważnie stosowane w ATM w sieciach rozległych, choć można je spotkać również w lokalnych sieciach wykorzystujących technologię ATM. Podobnie jak w przypadku sieci *Franie Relay,* kanały te muszą być ręcznie konfigurowane na każdym z przełączników ATM przez administratora i pozostają w sieci do czasu, aż nie zostaną w taki sam sposób usunięte. SVC są częściej stosowane w lokalnych sieciach ATM. Są wygodne, ponieważ mogą być tworzone przez oprogramowania na żądanie i usuwane, kiedy przestaną być wykorzystywane. Takie automatyczne tworzenie kanałów zwalnia administratora z konieczności tworzenia ciągle zmieniającej się tablicy kanałów i dopasowywania jej do potrzeb wynikających z aktualnego wykorzystania sieci. Niektóre rozwiązania ATM stosowane w sieciach rozległych również obsługują kanały SVC.

Dobrze, wystarczy już tych podstaw. Zajrzyjmy do konfiguracji. ATM może (i zwykle to robi) wykorzystywać pod-interfejsy w celu obsługi wielu logicznych podsieci pracujących w jednej sieci ATM obsługiwanej przez jedno fizyczne łącze z ruterem. Jeden z moich ruterów w sieci ma obecnie skonfigurowanych ponad 60 pod-interfejsów, które zostały zdefiniowane na bazie jednego z jego interfejsów ATM. Każdy z takich interfejsów logicznych ma własny adres IP i każdy z nich może używać PVC lub SVC, niezależnie od innych interfejsów. Pokażę przykłady takich rozwiązań. Technologia ATM definiuje również dwa sposoby przesyłania datagramów IP w sieci ATM. Pierwszy z tych sposobów (rozwiązanie starsze) to *Clasical IP over ATM,* zdefiniowany w RFC 1577. Drugim jest standard ATM Forum, nazwany jest LAN Emulation (LANE). Opiszę obie metody.

Clasical IP może być używane zarówno w kanałach PVC, jak i SVC. Kiedy metoda ta używana jest z PVC, konieczne jest poinformowanie rutera o kanałach logicznych, które skonfigurowane są w sieci, a także o sposobie przypisania adresów IP do tych kanałów. Aby poinformować ruter o istnieniu kanałów logicznych, należy do konfiguracji interfejsu dodać następujące polecenia:

```
interface atm l
  ip address 172.16.52.34 255.255.255.0 ! create the PVCs to be used by this
interface - one line for each
  atm pvc 1 0 32 aalSsnap
  atm pvc 2 0 45 aa!5snap
```

Każda instrukcja `atm pvc` informuje ruter o jednym kanale PVC. Pierwszy numer występujący w tej instrukcji pozwala na późniejsze odwoływanie się do tego kanału logicznego w dowolnym miejscu konfiguracji. Musi być on unikatowy, ale może być obierany arbitralnie. Drugi i trzeci numer określają parę PVC/SVC dla danego kanału. W przedstawionym przykładzie kanał wirtualny o numerze l przypisany jest do VPI/VCI0/32 a kanał 2 do 0/45. Ostatnie słowo kluczowe w definicji każdego z PVC informuje ruter/ jakiego rodzaju enkapsulacji należy używać w tym kanale. Wymieniana w przykładzie enkapsulacja `aa!5snapjest` stosowana najczęściej; obydwie strony kanału wirtualnego muszą stosować ten sam rodzaj. Kiedy już stworzymy wszystkie kanały, należy poinformować ruter o mapowaniu adresów IP na kanały logiczne. Aby to zrobić, należy stworzyć listę mapowania i skojarzyć ją z interfejsem:

```
interface atm l
  ip address 172.16.52.34 255.255.255.0 ! create the PVCs to be used by this
interface - one line for each
  atm pvc 1 0 32 aa!5snap
  atm pvc 2 0 45 aalSsnap
  map-group my-map
! define a mapping between protocol addresses and virtual circuits map-list my-map
  ip 172.16.52.77 atm-vc 1
  ip 172.16.52.198 atm-vc 2 broadcast
```

Instrukcja `map-list` i występujące po niej instrukcje definiują listę mapowania o nazwie my-map. Pierwsza instrukcja IP mówi, że adres `172 .16. 52 . 77` można osiągnąć przez kanał wirtualny l, który jest przypisany do VPI/VCI0/32. Druga instrukcja zawiera dokładnie takie same informacje, lecz dla sieci `172.16.52.198`, ale jednocześnie informuje ruter, że do tego urządzenia należy wysyłać pakiety broadcast. Ponieważ ATM nie jest technologią broadcast, to ruter obsługuje tego typu pakiety, kopiując je na każdy z kanałów wirtualnych, który oznaczony został tym parametrem. Takie rozsyłanie pakietów pseudo broadcast jest niekorzystne z punktu widzenia CPU rutera i pasma sieci.

Kanały PVC i mapowanie statyczne działają poprawnie, jeśli w sieci znajduje się kilka hostów. Jeśli jednak pojawi się więcej hostów, to konieczne jest mapowanie dużej liczby adresów IP na wiele kanałów PVC. Jednym z alternatywnych rozwiązań, które sprawia, że taka konfiguracja staje się bardziej dynamiczna, jest użycie odwrotnego ARP dla wykonania mapowania.

Zamiast wpisywać do rutera statyczne mapowanie pomiędzy adresami a kanałami wirtualnymi, każemy mu, aby zapytał urządzenie pracującego na drugim końcu kanału wirtualnego PVC, jaki jest jego adres:

```
interface atm 1
 ip address 172.16.52.34 255.255.255.0
! create the PVCs to be used by this interface and set them for inverse arp
atm pvc 1 0 32 aa!5snap inarp 5
atm pvc 2 0 45 aalSsnap inarp 5
```

W tym przykładzie, podobnie jak wcześniej, poinformowaliśmy ruter o kanałach wirtualnych. Tym razem jednak kazałem mu również używać odwrotnego ARP na każdym z kanałów i wysyłać zapytanie co pięć minut. Na podstawie uzyskanych odpowiedzi ruter może zbudować mapowanie adresów IP na kanały wirtualne, a nawet nadążać za zmianą adresów IP skojarzonych z wirtualnymi kanałami. Mimo to duża liczba kanałów wirtualnych może oznaczać konieczność wykonywania długotrwałej konfiguracji, a jeśli kanały ulegają częstym zmianom, to konfigurowanie tego mapowania może stać się koszmarem.

W takich przypadkach z pomocą przychodzą kanały SVC. SVC są tworzone programowo, na żądanie współpracujących w sieci urządzeń. Nie jest więc możliwe mapowanie adresów IP na przełączane kanały wirtualne. Zamiast tego ruter musi wykonać mapowanie adresów IP na odpowiedniki tych adresów w sieci ATM. Tym równoważnikiem adresu IP jest *Network Service Access Point Address (NSAPA),* Jest to wartość szesnastkowa o długości 20 oktetów. Kiedy urządzenie tworzy kanał wirtualny, zgłasza do sieci ATM numer NSAPA punktu przeznaczenia i czeka, aż sieć zestawi połączenie i zwróci informację o jego gotowości do transmitowania danych. Procedura zestawiania takiego kanału obsługiwana jest przez specjalnie do tego celu przeznaczony kanał sygnalizacyjny PVC, który ma numer VPI/VCI 0/5 i musi istnieć w każdej konfiguracji SVC. Ponadto sieć potrzebuje jakiegoś sposobu określenia, gdzie każdy z NSAPA się znajduje. W tym celu każde urządzenie musi wykonać krótkie uzgodnienia z przełącznikiem w momencie, kiedy jest do niego dołączane. Pyta ono przełącznik, jaka powinna być wartość pierwszych 13 oktetów NSAPA, pozostałe 7 dołącza na podstawie własnej konfiguracji, a następnie przekazuje do przełącznika utworzony w ten sposób numer. Agregowanie NSAPA jest wykonywane automatycznie, ponieważ każdy z przełączników ma swoją unikatową wartość 13-oktetowego prefiksu. Wymiana tych informacji następuje przez kolejny kanał PVC specjalnego przeznaczenia, który ma numer VPI/VCI 0/16. Obydwa wspomniane PVC pojawią się we wszystkich przykładach konfigurowania SVC.

Są dwa sposoby mapowania adresów IP na ATM NSAPA. Pierwszy z nich wykorzystuje mapowanie statyczne, podobne do tego, które zastosowano w przykładzie z PVC. Taka konfiguracja będzie wyglądała następująco:

```
interface atm 0
 atm pvc 1 0 5 qsaal
 atm pvc 2 O 16 ilmi

interface atm 0.1
 ip address 172.16.52.34 255.255.255.0
 atm es1-address 0987.1189.0034.13
 atm map-group my-svc-map
\create a mapping from IP address to NSAPA - circuits will be created \on-demand map-
list my-svc-map
 ip 172.16.52.77 atm-nsapBC.CDEF.01.234567.890A.BCDE.F01 2.3456.7890.1334.13
 ip 172.16.52.198 atm-nsapBC.CDEF.OI.234567.890A.HCDE.F012.3456.7890.1224.12
```

W podanym przykładzie jest sporo nowych poleceń. Po pierwsze, dwa PVC wymagane do sygnalizacji oraz ILMI zostały odpowiednio zdefiniowane i oznaczone do wykorzystania właściwego protokołu. Enkapsulacja QSAAL mówi ruterowi, że ten kanał wirtualny jest wykorzystywany do sygnalizowania, że przełącznik chce zestawić SVC do tego rutera. Enkapsulacja ILMI mówi ruterowi, że powinien wykorzystywać kanał wirtualny do wymiany z przełącznikiem informacji zarządzających, takich jak rejestrowanie NSAPA. Kanały te skojarzone są z podstawowym interfejsem -wszystkie interfejsy logiczne, które powinny używać sygnalizacji lub wymieniać ILMI z przełącznikiem, będą je wykorzystywały. Następnie dla interfejsu atm 0.1 określono ESI *(End Station Identifier),* wskazujący ten właśnie interfejs. Wartość ta to ostatnie 7 oktetów NSAPA rutera i powinna być ona przypisana przez lokalnego administratora ATM, aby zapewnić niepowtarzalność tej wartości we wszystkich urządzeniach dołączonych do jednego przełącznika ATM. Ruter będzie wykorzystywał kanał wirtualny ILMI do uzyskania 13-oktetowego prefiksu przełącznika i będzie go dołączał do swojego ESI tak, by utworzyć 20-oktetowy NSAPA dla tego rutera, a następnie zarejestrować tę wartość w przełączniku powtórnie wykorzystując kanał ILMI. Powstały w opisanym wyżej procesie NSAPA *musi być* unikatowy w sieci.* Nie powtarzanie się adresów jest gwarantowane przez przydzielanie unikatowego prefiksu dla każdego przełącznika ATM, a także unikatowego ESI dla każdego z urządzeń dołączonych do przełącznika. Prefiks przełącznika, którego wartość konfigurowana jest przez administratora ATM, może być przydzielany organizacji przez ISO lub dostawcę usług ATM lub, w przypadku prywatnych sieci ATM, może być ustalany arbitralnie. Na zakończenie utworzyłem nową listę mapowania o nazwie my - s v c - ma p, która mapuje adresy IP na NSAPA, i przypisałem ją do interfejsu logicznego. Oznacza to, że każdy taki interfejs będzie miał własne mapowanie. •

Choć zastosowanie kanałów SVC znacznie pomaga uporządkować konfigurację, to nadal musimy ją wykonywać ręcznie. Każdy ruter nadal wymaga konfiguracji uwzględniającej NSAPA wszystkich urządzeń działających w sieci ATM. Byłoby znacznie wygodniej, gdyby rutery nie tylko tworzyły kanały wirtualne na żądanie,

*Właściwie to tylko pierwsze 19 oktetów musi być unikatowych, ponieważ oktet numer 20 ma jedynie znaczenie dla urządzenia lokalnego i nie jest wykorzystywany przez przełączniki w procesie zestawiania połączeń.

ale też dokonywały dynamicznego wykrycia NSAPA skojarzonego z takim kanałem. Ponieważ ATM nie jest technologią *broadcast,* ruter nie może po prostu wysłać zapytania ARP w sieć i oczekiwać na odpowiedzi. Technologia ta musi opierać wyszukiwanie adresów na serwerze ARP. Kiedy taki serwer ATM ARP wykorzystywany jest w sieci, to każdy ruter, który w tej sieci pracuje, zna jego NSAPA. Następnie urządzenia otwierają SVC do serwera i informują go o swoich adresach IP i NSAPA. Informacja ta odświeżana jest co 20 minut. Kiedy jakiekolwiek urządzenie w sieci chce rozmawiać z innym urządzeniem, to zapytuje ono serwer ARP o to, jaki NSAPA skojarzony jest z IP tego urządzenia. Jeśli serwer odpowie, przekazując odpowiednią informację, to na jej podstawie zestawiany jest kanał SVC i nadawca może przesłać pakiety. Jeśli kanał taki pozostaje niewykorzystany przez 20 minut, jest on automatycznie zamykany. Poniżej przedstawiono konfigurację serwera ATM ARP:

```
! the configuration for an ATM ARP server
interface atm 1
  atm pvc 1  0  5  qsaal
 atm pvc 2 0 16 1lmi i
interface  atm 0 . 1
  ip address  172.16.52.34  255.255.255.0
  atm esi-address  0987.1189.0034.13 atm arp-
  server  self
```

Nadal konieczna jest obsługa sygnalizacji i ILMI PVC. Nadal także musimy przekazać ruterowi informację o jego adresie ESI, dzięki któremu będzie się on mógł poprawnie zarejestrować w przełączniku (a później w serwerze ARP). Aby jednak uruchomić serwer, należy poinformować jeden z ruterów, że jest on serwerem ATM ARP dla tej podsieci. Wykonałem to, używając instrukcji a tm arp-server sel f. Poniżej przedstawiam konfigurację klienta ARP:

```
! the configuration for an ATM ARP client
interface atm 1
  atmpvc 1  0  5  qsaal
 atm pvc 2 0 16 i lmi
interface atm 0 . 1
  ip address 172.16.52.34 255.255.255.0
  atm esi-address 0987.1189.0034.13
  atm arp-server nsap BC.CDEF.01.234567.890A.BCDE.F012.3456.7890.1334.13
```

Musimy powiedzieć klientowi, gdzie znajduje się serwer, używając do tego celu polecenia instrukcji arm arp-server nsap. Podczas gdy NSAPA serwera ATM ARP musi być cały czas przekazywane każdemu urządzeniu w sieci, to przynajmniej nie trzeba już przekazywać NSAPA innych urządzeń i wykonywać ich mapowania. W związku z tym, że serwer ATM ARP jest konfigurowany dla każdego interfejsu logicznego, możliwe jest, aby jeden ruter był serwerem ARP dla jednej z podsieci dołączonej do interfejsu logicznego i jednocześnie klientem ARP w innej podsieci dołączonej do innego interfejsu logicznego. Możliwe jest nawet, aby ruter posiadał

kolejny interfejs logiczny, na którym obsługiwany jest kanał PVC. Wszystko zależy od potrzeb każdej wykorzystywanej podsieci.

Innym sposobem przesyłania IP przez sieć ATM jest *LAN Emulation (LANE).* Rozwiązanie LANE stara się ukryć sieć ATM przed protokołem stosowanym w sieci, a także przed końcowymi urządzeniami brzegowymi, takimi jaki przełączniki LAN dołączone do ATM. Wykonuje to przez enkapsulację całych ramek LAN, niezależnie od tego, jakie medium jest emulowane (na razie zdefiniowane są Ethernet i Token Ring), i przesyła tak powstałe komórki przez sieć ATM, zamiast przesyłać surowe pakiety warstwy sieciowej. Zaletą takiego rozwiązania jest przezroczysta obsługa protokołów innych niż IP. Jest jednak trochę więcej zadań związanych z emulowaniem sieci Token Ring lub Ethernet niż tylko samo przesyłanie ramek LAN przez sieć ATM. Jednym z największych problemów jest obsługa pakietów typu broadcast. ATM nie jest, jak już wcześniej stwierdziłem, technologią broadcast; wykorzystuje połączenia wirtualne w relacji punkt-punkt. Natomiast media sieci LAN to technologie typu broadcast i pracujące w nich protokoły sieciowe spodziewają się, że będą mogły wysyłać w sieć pakiety typu broadcast. LANE musi ponadto zdecydować, gdzie należy przesyłać ramki unicast, jeśli takie zostaną odebrane. Możliwe byłoby ich rozesłanie wszędzie po sieci, ale jest to zwykłe marnowanie pasma. Lepiej, gdyby w sieci wy stępo wał jakiś mechanizm określający, które urządzenia ATM chcą otrzymywać takie ramki, i dopiero wtedy rozsyłać je do zainteresowanych. Urządzenia pracujące w środowisku LANE musiałyby być w stanie dokonać odwzorowania adresu MAC sieci Ethernet lub Token Ring na kanał wirtualny NSAPA.

Rozwiązaniem obu opisanych wyżej problemów jest utworzenie zestawu serwerów. Pierwszym i najważniejszym serwerem zdefiniowanym w LANE jest *LAN Emulation Configuration Server (LEGS).* LEGS jest centralnym zbiorem informacji o całej konfiguracji LANE. Jednocześnie w sieci ATM może więc pracować tylko jeden taki serwer LECS (choć w kolejnej wersji standardu pomyślano o redundantnym serwerze LECS). Kiedy urządzenie LANE uruchamia po raz pierwszy swój interfejs ATM, to nawiązuje ono połączenie z LECS, aby dowiedzieć się, gdzie w sieci pracują serwery Emulated LAN (E-LAN). LECS odpowiada wtedy przesyłając z powrotem informację o NSAPA serwera *LAN Emulation Server (LES),* o który urządzenie zapytało, lub wartość domyślną, jeśli serwera takiego nie ma w sieci.

LES odpowiedzialny jest za kontrolowanie uczestnictwa w E-LAN i za przechowywanie informacji o tym, kto i gdzie jest przyłączony do sieci. W rezultacie staje się on miejscem kontrolującym prawo przystąpienia do sieci, jak również serwerem ARP dla sieci E-LAN. Dla każdej sieci E-LAN działającej w ATM istnieje jeden LES. Jeśli kiedykolwiek jakieś urządzenie pracujące w E-LAN chce wiedzieć, gdzie jest określony adres MAC w sieci, to wysyła LANE ARP do serwera LES w celu otrzymania informacji o właściwym NSAPA. W czasie, kiedy czeka na uzyskanie odpowiedzi, zamiast odrzucić lub po prostu przetrzymać ramkę, którą chce wysłać, przekazuje ją do trzeciego serwera działającego w sieci LANE, który nazywa się *Broadcast and Unknown Server (BUS).* Serwer ten jest odpowiedzialny za obsługę zarówno ramek typu broadcast, które powinny docierać do wszystkich części E-LAN, jak i ramek, dla których mapowanie pomiędzy LAN MAC a NSAPA nie jest jeszcze znane. Te ostatnie ramki są również rozsyłane w sieci.

Zamiast jednak stosować kosztowne rozwiązanie obsługi pseudo broadcast BUS ma cały czas otwarty kanał wirtualny typu *point-multipoint.* Taki kanał wirtualny ma jednego nadawcę i wielu odbiorców. Kiedy wysyłany jest nim pakiet, to przełączniki pracujące w sieci powielają komórki i rozsyłają je do wszystkich słuchaczy, a także dbają o to, żeby pakiet nie był dwa razy przesyłany tym samym łączem. Ponieważ funkcje tego serwera są silnie powiązane z LES, to zwykle LES i BUS tworzą jedno urządzenie serwera i jako takie są konfigurowane przez aktualną wersję IOS. •,-.- v'.f rJ'n'!"f::, **;:• •>

Ostatnim elementem sieci LANE jest *LAN Emulation Client (LEC).* Choć w sieci ATM jest tylko jeden LEGS, również tylko jeden LES/BUS dla każdej sieci E-LAN, to LEC działa na każdym urządzeniu w sieci E-LAN, a urządzenia biorące udział w kilku sieciach E-LAN mają po kilka klientów LEC (proszę nie mylić tego z LEGS). Zwykle klient LEC zajmuje się wymianą informacji pomiędzy urządzeniem a serwerami obsługującymi sieć E-LAN, a także dzięki temu, że zna mapowanie adresów LAN MAC na ATM NSAPA może otwierać kanały wirtualne bezpośrednio z innymi klientami LEC. W takim przypadku pakiety będą przesyłane bezpośrednio pomiędzy dwoma LEC, z pominięciem serwerów LES/BUS.

Jest w tym wszystkim wiele tematów i koncepcji, w których łatwo się zaplątać i utknąć na dobre. Należy jednak powiedzieć, że konfiguracja sieci LANE nie jest wcale skomplikowana. Po pierwsze, jakieś urządzenie pracujące w sieci (może to być Twój ruter) musi być skonfigurowane jako LECS. Ponieważ takie urządzenie musi posiadać informację o tym, gdzie znajduje się każdy LES, będzie zawierało dość długą listę NSAPA, którą będzie musiało obsługiwać. Na szczęście adresy te zapisywane są w konfiguracji tylko tego jednego rutera:

```
/ define the NSAPA of the LES for each E-LAN
lane database my-lane
  name elan1 server-atm-address 47.00918100000000613E5D0301.00603EODE841.01
  name elan2 server-atm-address 47.00918100000000613E5D0301.008876EF0356.08
  name elan3 server-atm-address 47.00918100000000613E5D0301.0060344982DB.01
  name elan4 server-atm-address 47.00918100000000613E5D0301.00E4409DE642.0C
  d

interface atm0
  atm pvc 1  0  5   qsaal
  atm pvc 2 0 16 ilmi
\ attach the LANE database to this interface, and use the default LANE
i addresses
' lane config my-lane
   lane  auto-config-atm-address
```

Jest to przykładowa konfiguracja, w której widać istnienie czterech sieci E-LAN w bazie danych LEGS o nazwie my-1 ane. Nazwy tych sieci to e1 ani, e1 an2, e1 an3 i e l a n4. Każda z nich ma podany NSAPA dla swoich serwerów LES. Domyślną siecią E-LAN dla każdego z klientów, który nie wie, do której sieci powinien się przyłączyć, jest sieć elan1. W tym przykładzie pozostawiłem członkostwo w poszczególnych sieciach E-LAN nieograniczone żadnymi prawami dostępu. Jeśli chcesz nałożyć pewne ograniczenia na członkostwo w sieciach, to powinieneś zajrzeć do dokumentacji IOS, aby dowiedzieć się, jak to konfigurować.

Takie zaawansowane konfiguracje oznaczają *znacznie* większe bazy danych LECS, ale jeśli uważasz, że powinieneś skorzystać z tego dodatkowego zabezpieczenia, to można to zrobić. Po utworzeniu bazy danych konieczne jest jej przypisanie do interfejsu ATM, a *nie* do pod-interfejsu. Operacja ta wykonywana jest za pomocą instrukcji lane config. Na zakończenie za pomocą instrukcji lane auto-config-atm-address informujemy ruter, aby do określenia NSAPA dla każdego interfejsu logicznego wykorzystywał domyślny algorytm Cisco.

Mając skonfigurowany serwer LECS możemy zająć się serwerami LES/BUS i klientami LEC. Zamiast pokazywać te konfiguracje oddzielnie w kolejnym przykładzie pokazałem dwa interfejsy logiczne i ich konfigurację. Pierwszy interfejs atm O . l jest skonfigurowany do pracy jako LES/BUS dla sieci e l ani. Ma on również uruchomionego klienta dla tej sieci E-LAN, ponieważ chcemy, by w pełni brał udział w pracy sieci. Gdybyśmy nie dołączyli konfiguracji LEC, to serwery LES/BUS funkcjonowałyby normalnie, ale ruter nie byłby członkiem sieci E-LAN i dlatego nie mógłby wykonywać rutowania w tej sieci. Drugi interfejs logiczny ma jedynie LEC dla e 1 a n 2; serwery LES/BUS pracują na innym urządzeniu w sieci. Obie sieci E-LAN emulują pracę sieci Ethernet, choć bez problemu mogłyby emulować Token Ring. Nie informujemy rutera, gdzie znajduje się LES/BUS. Zamiast tego spodziewamy się, że zapyta on serwer LECS (który tu pracuje na tym samym ruterze, choć wcale nie musi tak być zawsze), gdzie jest serwer LES.

```
! this sub-interface has both the LES/BUS and on LEC for elan1
interface atm 0.1
  ip address 172.16.52.34 255.255.255.0
  lane server-bus ethernet elan1
  lane client ethernet elanl
! this sub-interface only has an LEC for elan2 - the LES/BUS is
! elsewhere
interface atm 0.2
  ip address 172.16.87.3255.255.254.0                    . . . . . .
  lane client ethernet elan2
```

Żaden z interfejsów logicznych nie otrzymał informacji o tym, jakiego NSAPA ma używać dla siebie. Ponieważ w konfiguracji interfejsu podstawowego umieściłem instrukcję l ane auto-config-atm-address, to każdy z tych interfejsów wygeneruje dla siebie unikatowy adres, korzystając z algorytmu obsługiwanego przez IOS. Jest to znacznie łatwiejszy sposób uzyskiwania unikatowych numerów NSAPA niż ręczne ich wpisywanie.

Czy powinieneś w swojej sieci ATM stosować rozwiązanie Classical IP, czy też LANE? To zależy. LANE z natury jest wieloprotokołowe. Ponieważ ramki medium sieci LAN są przesyłane przez sieć ATM bez analizy ich zawartości, to nie jest ważne, czy ramka taka zawiera pakiety protokołu IP, AppleTalk, IPX, czy innego, stosowanego w sieciach LAN. Rozwiązanie to pozwala ponadto zintegrować tradycyjne media sieci LAN z sieciami ATM i może posłużyć jako pośrednie rozwiązanie na drodze z sieci LAN do ATM.

Asynchronous Transfer Mode (ATM)

Rozwiązanie Classical IP jest z drugiej strony rozwiązaniem, którego zaletą jest możliwość stosowania większego MTU niż to, które stosowane jest w LANE. Ponieważ LANE emuluje sieć Ethernet lub Token Ring, wartość MTU została określona z uwzględnieniem tych mediów. MTU w Classical IP ma wielkość 9180 oktetów, co prowadzi do lepszych parametrów pracy sieci. Ponadto w związku z tym, że LANE stara się ukrywać sieć ATM przed dołączonymi do niej urządzeniami, nie jest możliwe wykorzystanie dostępności usług, gwarantowanej w technologii ATM. Classical IP może mieć dostęp do wszystkich funkcji technologii ATM. I na zakończenie: najlepszą odpowiedzią na postawione wyżej pytanie jest zawsze „obydwie". W podsieciach, w których wszystkie interfejsy wykorzystują funkcje ATM, możesz używać rozwiązania Classical IP - na przykład przy łączeniu ruterów do szkieletu sieci ATM. Technologii LANE możesz natomiast użyć w podsieciach (i logicznych interfejsach), gdzie obsługiwane są przełączniki LAN dołączone do ATM. Obydwa rozwiązania będą zgodnie współpracować. Należy tylko pamiętać, że każda podsieć lub interfejs logiczny może używać tylko jednego z tych rozwiązań.

Gdzie i jak uzyskać nowe dokumenty RFC B

Dokumenty RFC to oficjalne dokumenty zawierające definicje standardów protokołów z rodziny IP. Są one dostępne w wielu składnicach dokumentów i można je pobierać przy użyciu prawie każdej z dostępnych obecnie technik: WWW, FTP, email i tak dalej. Prawdopodobnie najwygodniejszym sposobem uzyskania kopii dokumentów RFC jest wykorzystanie strony WWW, utrzymywanej przez wydawcę RFC. Adres URL tego miejsca to: *http://ivww.isi.edu/rfc-editor/.* Oprócz zbioru samych dokumentów miejsce to wyposażone jest również w (czasem niestaranny) indeks przeszukiwania. Innym miejscem WWW, które obsługiwane jest przez lepszą wyszukiwarkę, jest *http://ds.internic.net/ds/dspglintdoc.htmL*

Dwa powszechnie znane miejsca, gdzie można uzyskać RFC za pomocą FTP to: *ftp://ftp.isi.edn/in-notes/rfcnnnn.txtorazftp://ds.internic.net/rfc/rfcnnnn.txt,* gdzie *nnnn* to numer dokumentu RFC, którego poszukujesz. Zawsze należy stosować numer czterocyfrowy.

Wygodnie jest również pozyskiwać dokumenty RFC za pomocą poczty elektronicznej. Aby uzyskać RFC z serwera *isi.edu* za pomocą email, należy wysłać wiadomość na adres *rfc-info@isi.edu,* której zawartość będzie następująca:

```
Retrieve:RFC Doc-
ID: RFCnnnn
```

gdzie *nnnn* odpowiada numerowi dokumentu RFC (zawsze należy stosować 4 cyfry -zapis DOC-ID dla RFC 822 to RFC0822). Serwer *rfc-info@isi.edu* obsługuje również inne metody pozwalające na wybranie dokumentów RFC w oparciu o słowa kluczowe i inne tego typu wyznaczniki. Aby uzyskać więcej informacji na ten temat, należy wysłać pocztą elektroniczną wiadomość do *rfc-info@isi.edu,* zawierającą następującą treść:

```
help: help
```

Aby za pomocą poczty elektronicznej otrzymać dokumenty RFC z *ds.internic.net,* należy wysłać wiadomość na adres *mailserv@ds.intemic.net* i umieścić w niej jedną z następujących instrukcji:

document-by-name rfcnnnn gdzie *nnnn* jest

numerem dokumentu RFC;

file /ftp/rfc/rfcnnnn.yyy gdzie *nnnn* jest numerem dokumentu RFC, a yyy - rozszerzeniem

nazwy txt lub ps;

help

aby uzyskać informacje o korzystaniu z serwera poczty elektronicznej.

W sieci jest jeszcze wiele innych miejsc, które zawierają w swych zbiorach dokumenty RFC. Część z nich może być znacznie łatwiej osiągalna poza terenem USA. Aby uzyskać pełną listę takich miejsc należy pobrać plik*ftp://ftp.isi.edu/in-notes/rfc-retrie-val.txt.*

Otrzymywanie dokumentów roboczych C

Dokumenty o nazwie *Internet Drafts* są roboczymi dokumentami opracowywanymi przez *Internet Engineering Task Force.* Powinny być one traktowane jako dokumenty opisujące działania, które dopiero trwają, i tylko jako takie mogą być cytowane. Większość dokumentów *Internet Drafts* nigdy nie wyjdzie poza fazę dokumentu roboczego. Zawarte są w nich idee, które nie wzbudziły zainteresowania, jakiego spodziewał się ich autor lub zostały przez większość społeczności uznane za niepożądane. Pozostałe dokumenty robocze, które zainteresują społeczność, stają się w efekcie dalszych prac nad ich zawartością dokumentami *Internet Request for Comment* (RFC) i będą zawierały informacje lub propozycje standardów, które z czasem w końcu staną się standardami w sieci Internet.

We wszystkich opisanych wyżej przypadkach każdy z dokumentów Internet Drafts ważny jest tylko przez sześć miesięcy od daty jego opublikowania. W tym czasie musi być on ponownie wydany (w wyniku uwzględnienia zgłoszonych poprawek), przekazany do rozpatrzenia jako RFC lub wycofany. Jeśli więc otrzymałeś do czytania dokument *Internet Drafts,* zawsze pamiętaj, że zawarte w nim informacje nie są standardem, nie reprezentują proponowanego standardu i mogą nigdy nie wyjść poza fazę dokumentu roboczego. Nadal jednak propozycje te należy uważać za wartościowe, jeśli chcesz zorientować się, jakie tematy są obecnie rozpatrywane przez IETF, i być może przekazać swoje komentarze autorowi takiego dokumentu.

Dokumenty z serii *Internet Drafts* dostępne są w różnej formie. Aby uzyskać takie dokumenty przez anonimowe FTP konieczne jest nawiązanie połączenia FTP z jednym z niżej podanych miejsc i załogowanie się jako anonymous. Następnie trzeba wykonać *cd* do katalogu */internet-drafts.* W katalogu tym oprócz samych dokumentów Internet Drafts znaleźć można plik o nazwie *lid-abstract.txt,* w którym znajduje się lista dokumentów rozpatrywanych w danej chwili z podaniem ich tytułów, ścieżek dostępu, nazwisk autorów, dat opublikowania wraz z krótkimi streszczeniami. W katalogu tym jest również plik o nazwie *lid-index.txt,* w którym znajduje się skrócona lista dokumentów *Internet Drafts* (tytuł dokumentu, nazwa pliku i data opublikowania).

Region	*Host*	*Adres IP*
Afryka Europa Rejon Pacyfiku USA Wybrzeże Wschodnie USA Wybrzeże Zachodnie	*ftp.is.co.za nic.nordu.net* *munnari.oz.au ds.internic.net* *ftp.isi.edu*	196.4.160.8 192.36.148.17 128.250.1.21 198.49.45.10 128.9.0.32

* Dokumenty Internet Drafts znajdujące się na tej maszynie są przechowywane w skompresowanym formacie systemu UNIX (tzn. z rozszerzeniem .Z)

Internet Drafts dostępne są również za pomocą poczty elektronicznej z serwera *ds.in-ternic.net.* Aby pobrać taki plik, należy wysłać wiadomość email z odpowiednim zapytaniem na adres *mailserv@ds.internic.net,* w której to, co będzie znajdowało się w polu tematu, zostanie zignorowane. Zawartość tej wiadomości powinna być następująca:

```
FILE /internet-drafts/lid-abstracts.txt PATH
jdoe@somedomain.edu
```

gdzie PATH jest .adresem poczty elektronicznej, na który ma być wysłana odpowiedź. Jeśli masz na swoim hoście obsługę *mpack* lub Twój program obsługi poczty jest zgodny ze standardem MIME, możliwe jest użycie dodatkowego polecenia:

```
ENCODING mime
```

Polecenie to sprawi, że informacje zwrócone zostaną w postaci wiadomości w formacie MIME.

Dokumenty *Internet Drafts* dostępne są również z WWW. Sama organizacja IETF twierdzi, że usługa ta jest ciągle zmieniana, należy ją więc sprawdzać dość często. Adres URL, pod którym znajdują się *Internet Drafts,* to: *http://www.ietf .org/lid-abs-tracts.html* oraz strona domowa IETF, którą można znaleźć pod adresem *http://www.ietf.org.html.*

D

Uzyskiwanie adresów IP

Przestrzeń adresową IP dla swojej sieci powinieneś otrzymać od swojego dostawcy usług lub powinieneś zastosować adresy z prywatnych bloków zdefiniowanych w RFC 1918. Przestrzeń adresową należy traktować jak nagrodę i jest to najlepszy sposób pozwalający na rozdzielanie odpowiedniej wielkości grup adresów przy jednoczesnym pozostawieniu ich części na przyszłość. Jeśli zdecydujesz, że musisz mieć przestrzeń adresową, która jest przenośna, powinieneś zrozumieć, że nie ma żadnych gwarancji na to, iż przestrzeń taka *będzie rutowana. Gwarancji takich nie daje Internet Assigned Numbers Authority* (JANA) ani żaden z rejestratorów IP. Może się nawet zdarzyć, że dostawca usług internetowych postanowi nie rutować tych adresów i będzie nalegał, abyś w swojej sieci wykorzystywał przestrzeń adresową, którą on Ci wyznaczy.

To, z kim powinieneś skontaktować się, jeśli będziesz chciał uzyskać przenośną grupę adresów, zależy od tego, w której części świata się znajdujesz. Powinieneś przeczytać informacje zawarte w części poniżej, wybierając tę, która opisuje Twoją lokalizację.

Rejon Azji i Pacyfiku

Regionalnym biurem rejestracji adresów w rejonie Azji i Pacyfiku jest *Asian Pacific Network Information Center (APNIC).* Powinieneś pobrać plik */apnic/docs/Contents z* anonimowego serwera FTP o *nazwieftp.apnic.net* i przejrzeć go, by dowiedzieć się, które szablony powinieneś pobrać z katalogu */apnic/docs,* znajdującego się na tym serwerze. Kiedy wypełnisz odpowiedni formularz, powinieneś wysłać go na adres: *ip-request@rs.apnic.net.* Możliwe jest również złożenie formularza wysyłając go na numer faksu: +81-3-5500-0481 lub na adres pocztowy:

Asia Pacific Network Information Center

Tokyo Central Post Office Box 351

Tokyo,100-91, Japan

Organizaq'a APNIC przyznaje, że preferowany jest sposób składania formularzy przez pocztę elektroniczną, a adres pocztowy powinien być wykorzystany w ostateczności. Nie są akceptowane zgłoszenia wykonywane za pomocą telefonu. Jeśli masz jakieś pytania odnośnie wypełnianego formularza, powinieneś kontaktować się z APNIC wysyłając wiadomość pocztą elektroniczną na adres *hostmaster@apnic.net* (preferowany), wysyłając pytania faksem na podany wyżej numer lub pocztą na podany wyżej adres, a w ostateczności telefonując pod numer +81-3-5500-0480.

Europa

Europejskie adresy IP przydzielane są przez RIPE NCC. Powinieneś ściągnąć plik */ripe/forms/netnum-appl.txt* poprzez anonimowe FTP z *seiweraftp.ripe.net* lub od swojego dostawcy usług internetowych. Ponadto powinieneś pobrać kopię pliku */ri-pe/forms/netnum-support.txt.* Oba pliki powinieneś bardzo uważnie przeczytać, a następnie wypełnić je, posługując się zawartą w nich instrukcją.

Z RIPE NCC można się skontaktować pod adresami:

RIPE NCC

Kruislaan409

1098 SJ Amsterdam

The Netherlands

tel.:+31205925065

fax:+3120 592 5090

email: hostmaster@ripe.ne