

» Idź do

- Spis treści
- Przykładowy rozdział

» Katalog książek

- Katalog online
- Zamów drukowany katalog

» Twój koszyk

- Dodaj do koszyka

» Cennik i informacje

- Zamów informacje o nowościach
- Zamów cennik

» Czytelnia

- Fragmenty książek online

» Kontakt

Helion SA
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl
© Helion 1991-2010

Head First. Sieci komputerowe. Edycja polska

Autorzy: [Al Anderson](#), [Ryan Benedetti](#)

Tłumaczenie: Tomasz Walczak

ISBN: 978-83-246-2501-7

Tytuł oryginału: [Head First Networking](#)

Format: 200×230, stron: 536



Użytkowanie sieci komputerowych stało się co najmniej tak popularne jak posługiwanie się telefonem komórkowym. Jeśli Ty także chcesz obsługiwać swobodnie sieć komputerową, powinieneś sięgnąć po tę wyjątkową książkę. Z tego podręcznika, napisanego zgodnie z najnowszymi metodami skutecznej nauki, skorzystają zarówno amatorzy, którzy chcą sprawnie obsługiwać urządzenia sieciowe dla własnej wygody, jak i administratorzy pragnący poszerzać swoją wiedzę i sprawnie rozwiązywać trudne problemy.

W książce „Head First. Sieci komputerowe. Edycja polska” znajdziesz nie tylko odpowiedzi na nurtujące Cię pytania dotyczące sieci komputerowych, ale także ich klarowne i szczegółowe objaśnienie. Wyróżniającą cechą tego bogato ilustrowanego podręcznika jest przełożenie wiadomości teoretycznych na problemy koncentrujące się wokół praktyki obsługi sieci komputerowych, a więc opis rzeczywistych problemów, które spotykasz na co dzień w swojej pracy. W trakcie lektury niniejszej książki dowiesz się, jak zaplanować układ sieci, znajdziesz tu także praktyczne porady dotyczące wykrywania i rozwiązywania problemów z połączeniami, konfigurowania przełączników oraz routerów. Nauczysz się projektować sieć oraz sprawnie i bezpiecznie nią zarządzać.

- Naprawianie fizycznych uszkodzeń sieci
- Planowanie układu sieci
- Diagnostowanie i rozwiązywanie problemów
- Analizowanie pakietów
- Urządzenia i narzędzia
- Protokoły trasowania
- System nazw domen
- Sieci bezprzewodowe
- Bezpieczeństwo w sieci
- Projektowanie sieci

Zostań guru w dziedzinie sieci komputerowych!

Spis treści (skrótowy)

Wprowadzenie	25
1. Naprawianie fizycznych uszkodzeń sieci. <i>Spacer po przewodach</i>	37
2. Planowanie układu sieci. <i>Z sieciami w ciemnościach</i>	87
3. Narzędzia i rozwiązywanie problemów. <i>Do wnętrza kabla</i>	121
4. Analizowanie pakietów. <i>Na tropie ramek</i>	161
5. Urządzenia i ruch w sieci. <i>Jak inteligentna jest Twoja sieć?</i>	209
6. Łączenie sieci za pomocą routerów. <i>Łączenie różnych elementów</i>	239
7. Protokoły trasowania. <i>Protokół tego wymaga</i>	277
8. System nazw domen. <i>Przekształcanie nazw na numery</i>	325
9. Monitorowanie sieci i rozwiązywanie problemów. <i>Nasłuchuj, czy w sieci nie ma problemów</i>	363
10. Sieci bezprzewodowe. <i>Praca bez kabli</i>	397
11. Bezpieczeństwo w sieci. <i>Broń się!</i>	433
12. Projektowanie sieci. <i>Musisz mieć plan!</i>	471
A Pozostałości. <i>Dziesięć najważniejszych tematów (których nie poruszyliśmy)</i>	503
B Tabele kodów ASCII. <i>Sprawdzanie kodów</i>	513
C Instalowanie serwera BIND. <i>Serwer do obsługi systemu DNS</i>	519

Spis treści (na serio)



Wprowadzenie

Twój mózg a sieci. Podczas gdy Ty próbujesz się czegoś nauczyć, mózg wyświadcza Ci przysługę i dba o to, abyś *niczego nie zapamiętał*. Twój mózg myśli sobie: „Lepiej zostawić miejsce na ważniejsze informacje, na przykład o dzikich zwierzętach, których należy unikać, i o tym, dlaczego jeżdżenie nago na snowboardzie to zły pomysł”. Jak więc możesz przechytryć mózg i przekonać go, że Twoje życie zależy od umiejętności obsługi sieci?

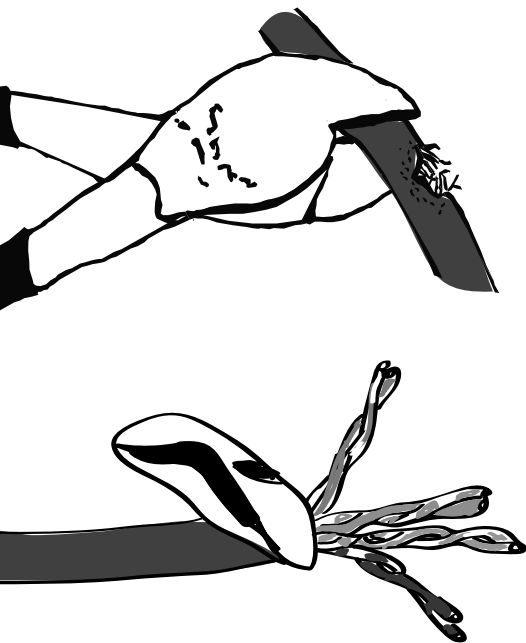
Dla kogo przeznaczona jest ta książka?	26
Wiemy, co sobie myślisz	27
Wiemy, co sobie myśli Twój mózg	27
Metapoznanie: myślenie o myśleniu	29
Oto, co MY zrobiliśmy	30
A oto, co TY możesz zrobić, aby zmusić mózg do posłuszeństwa	31
Przeczytaj koniecznie	32
Zespół recenzentów technicznych	34
Podziękowania	35

Naprawianie fizycznych uszkodzeń sieci

1

Spacer po przewodach

Wystarczy podłączyć kabel i sieć jest gotowa, prawda? Kable sieciowe po cichu wykonują swoje zadanie i błyskawicznie przesyłają dane. Co się jednak stanie, kiedy wystąpią problemy? Firmy w tak dużym stopniu polegają na sieciach, że ich awaria uniemożliwia funkcjonowanie organizacji. Dlatego umiejętność naprawy fizycznych uszkodzeń jest tak ważna. Z tego rozdziału dowiesz się, jak w łatwy sposób naprawić sieć i rozwiązać problemy. Wkrótce uzyskasz pełną kontrolę nad sieciami.



Linie lotnicze Kiwi mają problemy z siecią	38
Jak naprawiać kable?	41
Poznaj kable kat. 5	42
Kabel kat. 5 pod mikroskopem	43
Do czego służą kolory?	44
Naprawmy zepsuty kabel kat. 5	47
Bliższe spojrzenie na złącze RJ-45	48
Jakie operacje trzeba wykonać?	53
Naprawiłeś kabel kat. 5	55
Linie Kiwi mają kilka sieci	56
Poznaj kable koncentryczne	59
Sieci koncentryczne to sieci z magistralą	60
Czy potrafisz naprawić uszkodzony kabel?	61
Sieć wciąż nie działa	62
Co znajduje się w środku kabla koncentrycznego?	64
Do czego służą łączniki i terminatory?	65
Zastosuj zestaw generator-detektor do nasłuchiwania elektronów	66
Brak dźwięku oznacza brak elektronów	67
Naprawiłeś kabel koncentryczny	73
Wprowadzenie do światłowodów	74
Kabel linii Kiwi jest nadmiernie zgięty	75
Jak naprawić światłowód za pomocą spawarki światłowodowej?	76
Trzeba jeszcze zamocować złącze światłowodowe	78
Jesteś prawie gotowy do naprawienia złącza	80
Są dwa rodzaje włókien	81
Jakich włókien powinieneś użyć?	82
Umocuj złącze na światłowodzie	83
Linie Kiwi znów latają	85

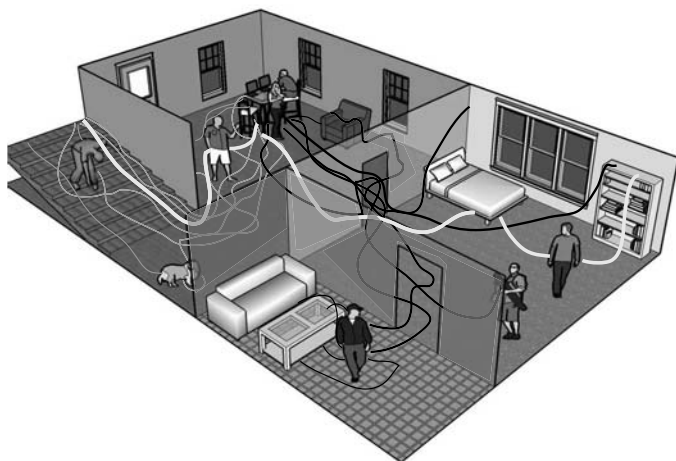
Planowanie układu sieci

2

Z sieciami w ciemnościach**Masz dość potykania się o przewody i ataków ze strony skrzynki elektrycznej?**

Jeśli zbudujesz sieć bez planu, powstanie bałagan — kable będą biegły we wszystkie strony i nie będziesz wiedział, do czego są podłączone. W tym rozdziale nauczysz się planować fizyczny układ sieci, co pozwoli Ci uniknąć późniejszych problemów. Dowiesz się też, jak używać odpowiedniego sprzętu do porządkowania przewodów i zarządzania nimi.

Zespół z programu „Poszukiwacze duchów” potrzebuje Twojej pomocy!	88
Przygotowywanie każdej dobrej sieci zaczyna się od dobrego planu	89
W jakim stopniu lista urządzeń pomoże w zaplanowaniu sieci?	90
Jak zaplanować układ sieci?	91
Zaplanuj układ kabli na podstawie projektów	92
Jesteś gotowy do zaplanowania układu kabli sieciowych?	96
Dokąd doszliśmy?	99
Musisz wybrać sprzęt do zarządzania okablowaniem	100
No tak! Okablowanie jest w zupełnym nieładzie	101
Poszukiwacze duchów potrzebują sprzętu do zarządzania okablowaniem	102
Nocne strachy...	104
Rzeczywiście pozbyłeś się odgłosów i uporządkowałeś WIEKSZOŚĆ kabli!	109
Zaczynij od dodania etykiet do kabli	110
W szafce nadal jest mnóstwo kabli	111
Czym jest panel krosowniczy?	112
Na zapleczu panelu krosowniczego	113
Przewody trafiają do bloku zaciskowego	114
Kamery na stanowiska!	119



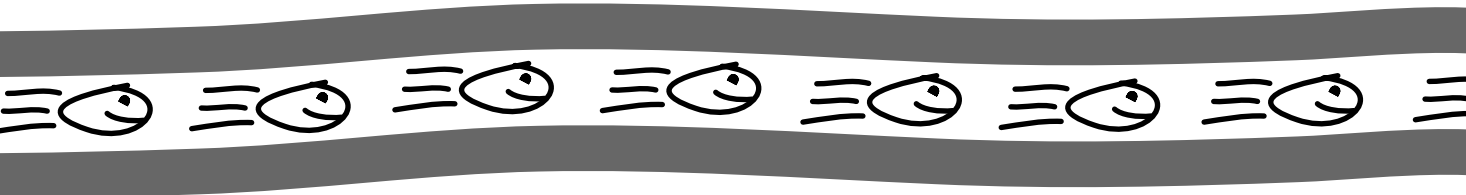
Narzędzia i rozwiązywanie problemów

3

Do wnętrza kabla

Skąd wiadomo, że kabel sieciowy nie przewodzi sygnału? Często dowiadujesz się o tym, kiedy sieć przestaje działać, jednak trudno określić przyczynę problemu tylko na podstawie wyglądu kabla. Na szczęście istnieją narzędzia, które pozwalają zajrzeć do wnętrza przewodu i przyrzec się samym sygnałom. W tym rozdziale dowiesz się, jak używać takich urządzeń do rozwiązywania problemów z sieciami i jak interpretować sekretny język sygnałów.

Firma Balonowe Łakocie otrzymała kontrakt na finał Ligi Mistrzów	122
Generator i detektor pozwalają sprawdzić obecność sygnału...	124
... ale nie jego jakość	124
Poznaj multimetr	128
Czym jest opór?	129
Jak przydatny okazał się multimetr?	135
Oscyloskop pokazuje zmiany napięcia	137
Napięcie to „ciśnienie” elektryczne	138
Skąd się bierze szum w kablach sieciowych?	139
Jak oscyloskop sprawdził się w Balonowych Łakociach?	144
Także analizator logiczny bada napięcie	146
Kiedy analizator logiczny jest przydatny?	151
Które narzędzie jest najlepsze?	151
Premię od dyrektora Balonowych Łakoci dostaje Julia	153
Analizator sieci LAN łączy funkcje wszystkich pozostałych narzędzi	154
Analizator sieci LAN wykrywa w sygnale dane przesyłane w sieci	155
Które urządzenie jest najlepsze?	156
Koniec problemów Balonowych Łakoci!	159

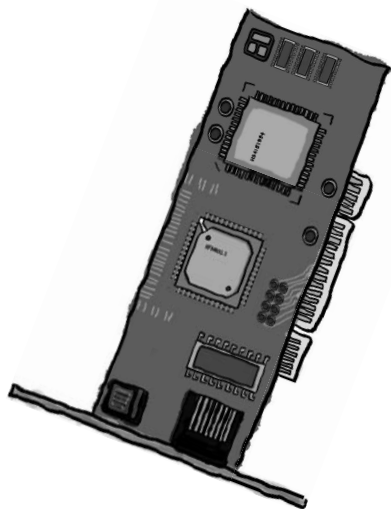


Analizowanie pakietów

4

Na tropie ramek

Czas zajrzeć pod maskę. Urządzenia sieciowe przesyłają informacje kablami, przekształcając dane na sygnały. Jak jednak to robią? Co oprócz informacji może ukrywać się w sygnale? Podobnie jak lekarz musi zbadać krew, aby wykryć choroby krwi, tak specjalista od sieci musi zobaczyć, co zawiera sygnał, żeby odkryć włamanie, przeprowadzić kontrolę i — ogólnie — zdiagnozować problem. Analiza pakietów to umożliwia. Czytaj dalej, aby dowiedzieć się, jak przyjrzeć się pod mikroskopem sygnałom przesyłanym w sieci.



Jak brzmi tajna wiadomość?	162
Za kodowanie odpowiadają karty sieciowe	166
Aby odebrać komunikat, należy odwrócić kodowanie	167
Sprzęt koduje dane na podstawie standardu Ethernet	168
Krótkie wprowadzenie do systemu dwójkowego	172
Ludzie czytają litery, a komputery — liczby	178
Z pomocą przybywa system szesnastkowy	180
Można uzyskać znaki ASCII na podstawie liczb szesnastkowych	181
Z powrotem w agencji szpiegowskiej...	188
Protokoły wyznaczają strukturę komunikatu	189
Ramki sieciowe mają wiele warstw	197
Przyjazny przewodnik po polach pakietu	198
Czy potrafisz odkodować tajny komunikat?	204
Mamy wszystkie potrzebne pakiety, ale niekoniecznie we właściwej kolejności	205
Pakiety informują o właściwej kolejności	206

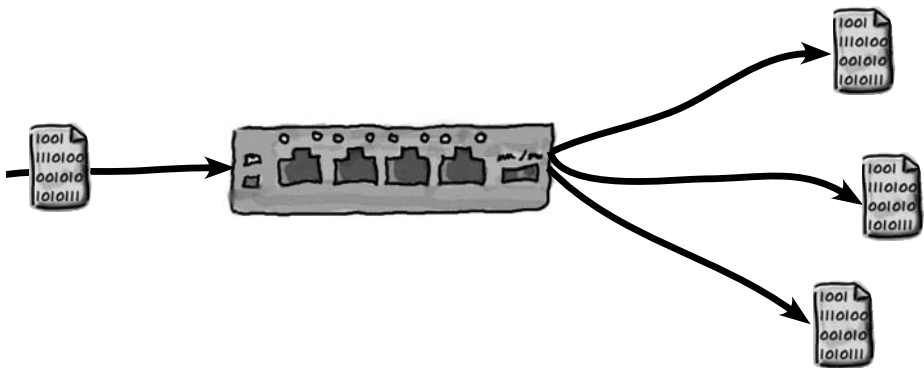
Urządzenia i ruch w sieci

5

Jak inteligentna jest Twoja sieć?

Sieć zawsze może być bardziej inteligentna. W sieć należy wbudować jak najwięcej inteligencji, jednak **z czego ona wynika?** Najważniejsze są urządzenia sieciowe. W tym rozdziale pokażemy, jak **koncentratory, przełączniki i routery** wykorzystują swoją naturalną **inteligencję** do przesyłania pakietów w sieci. Dowiesz się, w jaki sposób te narzędzia „**myślą**” i dlaczego są tak **przydatne**. Podejrzymy nawet dane przesyłane w sieci za pomocą **oprogramowania do analizowania pakietów**. Czytaj dalej, a zobaczysz, jak **włączyć turbodoładowanie sieci**.

Odkodowałeś tajną wiadomość...	210
Dane w pakiecie informują o jego pochodzeniu	213
Kto jest „wtyczką”?	214
Sieć to nie tylko komputery	215
Koncentratory nie są inteligentne	216
Koncentratory nie zmieniają adresu MAC	217
Koncentrator wysyła sygnały wszędzie	218
Które urządzenie przekazało sygnał do koncentratora?	219
Przełącznik wysyła ramki tylko do docelowej lokalizacji	220
Przełączniki przechowują adresy MAC w tablicy przeglądowej, co umożliwia płynne przesyłanie ramek	222
Przełącznik posiada cenne informacje	226
Można użyć oprogramowania do monitorowania pakietów	228
Podłącz program Wireshark do przełącznika	229
Program Wireshark udostępnia informacje o danych sieciowych	230
Także routery mają adresy MAC	233
Routery są naprawdę inteligentne	234
Zbliżamy się do celu!	235
Znalazłeś „wtyczkę”!	237

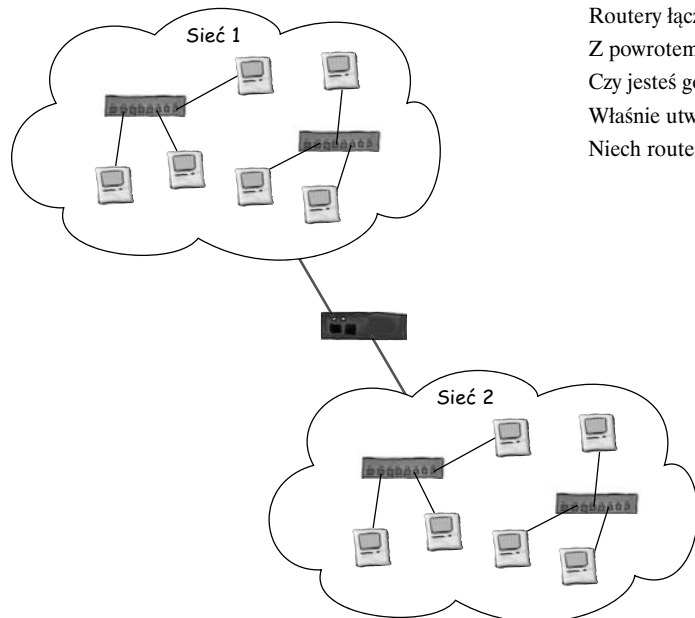


Łączenie sieci za pomocą routerów

6

Łączenie różnych elementów

Chcesz nawiązać połączenie sieciowe z bardzo odległym miejscem? Na razie pokazaliśmy, jak skonfigurować pojedynczą sieć. Co jednak zrobisz, kiedy zechcesz **udostępnić zasoby w innej sieci**? Potrzebne będą do tego routery. Te urządzenia służą do płynnego **przekazywania pakietów między sieciami**, a w tym rozdziale dokładnie opisujemy ten proces. Dowiesz się, jak **zaprogramować** router i jak urządzenie to może pomóc Ci **w rozwiązywaniu problemów**. Czytaj dalej, a zobaczysz, że routery to sprzęt nie z tego świata.



Z siecią po Księżycu	240
Trzeba połączyć dwie sieci ze sobą	243
Światła się świecą, ale nikogo nie ma w domu	244
Zobaczmy, jakie dane są przesyłane w sieci!	246
Adresy MAC i adresy IP	248
Adres IP umożliwia sieciom określanie lokalizacji, a węzłom sieciowym zapewnia przynależność do tej lokalizacji	249
Do pobierania adresów IP służy adres MAC i protokół ARP	250
Jaki problem ma baza Księżyc?	255
W jaki sposób można przekazywać pakiety między sieciami?	256
W jaki sposób router przekazuje dane między sieciami?	258
Wróćmy do problemów w bazie Księżyc	260
Sekret numerów IP tkwi w...	261
Routery łączą sieci przez wykonywanie obliczeń matematycznych...	262
Z powrotem w bazie Księżyc...	269
Czy jesteś gotowy do zaprogramowania routera?	270
Właśnie utworzyłeś poniższy plik konfiguracyjny routera!	272
Niech router określi, w czym tkwi problem	274

Protokoły trasowania

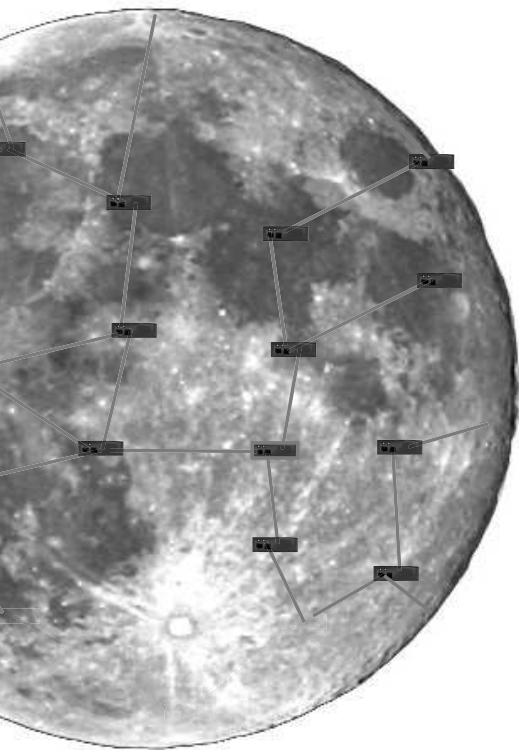
7

Protokół tego wymaga

Aby zbudować dużą sieć, musisz użyć komunikujących się ze sobą routerów.

Routerzy muszą przekazywać sobie trasy pakietów. Służą do tego różne protokoły trasowania. W tym rozdziale najpierw dowiesz się, jak ręcznie wprowadzić trasę, a następnie zobaczysz, jak zastosować prosty protokół trasowania RIP. W końcowej części opisujemy, jak skonfigurować zaawansowany protokół trasowania o nazwie EIGRP.

Houston, mamy problem	278
Tablice trasowania informują routery, gdzie należy przesłać pakiety	279
Każdy wiersz reprezentuje inną trasę	280
Jak można wprowadzić trasę?	282
Trasy pomagają routerom określić, gdzie należy przesłać dane sieciowe	283
Czy teraz bazy na Księżycu są połączone?	287
Z powrotem na Księżycu	289
Jak rozwiązywać problemy z nieprawidłowymi trasami?	290
Przydatne jest też polecenie traceroute	291
Na czym polega problem z połączeniem sieciowym?	295
Napływają informacje o zmianach adresów sieci	296
Zastosuj protokół RIP, aby router sam aktualizował trasy	298
Jak skonfigurować protokół RIP?	304
Problemy się nie skończyły	305
Liczba przeskoków jest za duża	306
Zoo z protokołami trasowania	310
Jak skonfigurować protokół EIGRP?	316
Wystartowaliśmy!	322



System nazw domen

8

Przekształcanie nazw na numery

Prawdopodobnie nigdy się nad tym nie zastanawiałeś, ale jak komputer znajduje adres IP serwera, kiedy wprowadzasz adres URL w przeglądarce?

W tym rozdziale odkryjesz świat domen internetowych. Dowiesz się, że istnieje 13 serwerów głównych, które zarządzają informacjami na temat nazw domen z całego Internetu. Ponadto zainstalujesz i skonfigurujesz własny serwer DNS.



Centrum Head First Health Club potrzebuje witryny	326
Witajcie, moja domena nazywa(m) się...	327
Kupmy nazwę domeny	328
No tak! Mamy kłopoty	330
Wprowadzenie do systemu DNS	332
System DNS oparty jest na serwerach nazw	332
W jaki sposób system DNS postrzega domenę?	333
Co ten system oznacza dla centrum Health Club?	338
Najpierw zainstaluj serwer nazw DNS...	340
... a następnie go skonfiguruj	341
Anatomia pliku strefy DNS	348
Jakie informacje o serwerach centrum Health Club zawiera plik strefy DNS?	349
Centrum Health Club nie może wysłać e-maili	351
W czym tkwi problem?	352
Serwery pocztowe korzystają z odwrotnej translacji do zwalczania spamu	352
Sprawdź nadawcę za pomocą odwrotnej translacji	353
Do odwrotnej translacji nazw DNS służy polecenie dig	354
Serwer nazw ma jeszcze jeden ważny plik strefy	356
Poczta elektroniczna działa!	361

Monitorowanie sieci i rozwiązywanie problemów

9

Nasłuchuj, czy w sieci nie ma problemów

Dzięki obserwowaniu sieci możesz uniknąć ataku serca! Skonfigurowałeś i uruchomiłeś sieć. Jednak — podobnie jak inne systemy — wymaga ona doglądania i konserwacji. Jeśli tego zaniedbasz, pewnego dnia sieć przestanie działać i nie będziesz wiedział, dlaczego tak się stało. W tym rozdziale poznasz różne narzędzia i techniki, które pomogą Ci obserwować sieć, a także zrozumieć, co się z nią dzieje. Dzięki temu będziesz mógł rozwiązać wszystkie problemy, zanim staną się naprawdę poważne.

Pizamy Apokalipsy znów ruszają w trasę	364
Od czego zaczniesz rozwiązywanie problemów z nie działającą siecią?	365
Zacznij rozwiązywanie problemów z siecią od sprawdzenia urządzeń sieciowych	367
Rozwiąż problemy z połączeniami za pomocą polecenia ping	368
Jeśli nie uzyskasz odpowiedzi, sprawdź kable	369
Zacznij od polecenia show interface	375
Sieć biura sprzedaży biletów wciąż nie działa	379
SNMP przybywa na ratunek!	380
SNMP to narzędzie do komunikowania się dla administratorów sieci	381
Jak skonfigurować SNMP w urządzeniach firmy Cisco?	382
Pozostała jedna godzina	387
Spraw, aby urządzenia przesyłały informacje o problemach	388
Jak skonfigurować demona syslogd dla urządzenia firmy Cisco?	389
Skąd wiadomo, co zawierają dzienniki?	390
Nadmiar informacji może być równie zły jak ich brak	393
Skąd wiadomo, które zdarzenia są ważne?	394
Bilety na Pizamy Apokalipsy zostały wyprzedane!	395



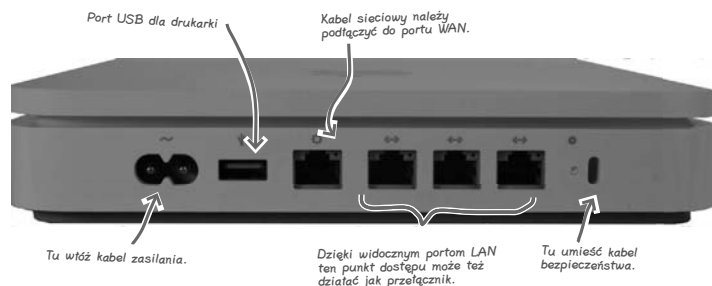
10

Sieci bezprzewodowe

Praca bez kabli

Bezprzewodowe surfowanie po Internecie jest wspaniałe! W tym rozdziale opisujemy wszystko, co powinieneś wiedzieć przy konfigurowaniu bezprzewodowego punktu dostępu. Najpierw musisz przemyśleć jego fizyczną lokalizację, ponieważ sygnał sieci radiowych może zostać zablokowany. Omawiamy też kilka nowych akronimów związanych z sieciami — NAT i DHCP. Nie martw się, wyjaśniamy ich znaczenie, dlatego zanim skończysz czytać ten rozdział, będziesz mógł korzystać z gotowej sieci bezprzewodowej.

Nowe zadanie w Starbuzz Coffee	398
Sieci z bezprzewodowymi punktami dostępu są oparte na falach radiowych	399
Zainstalujmy bezprzewodowy punkt dostępu	400
Czy pamiętałeś o skonfigurowaniu sieci?	407
Czym jest DHCP?	408
Najpierw upewnij się, że po stronie klienta włączona jest obsługa DHCP...	410
Potem skonfiguruj bezprzewodowy punkt dostępu jako serwer DHCP	410
... a następnie określ przedział dostępnych adresów IP	411
Czy skonfigurowanie serwera DHCP rozwiązało problem?	412
Tym razem to sprawa osobista	413
Serwer wyczerpał pulę adresów IP	414
NAT działa przez realokację adresów IP	415
Jak przebiega konfigurowanie mechanizmu NAT?	416
Czy to rozwiązało problem?	419
Jest kilka protokołów bezprzewodowych	420
Centralny serwer firmy Starbuzz musi mieć dostęp do kasy fiskalnej	424
Wybawieniem jest mapowanie portów	426
Ustaw mapowanie portów dla punktu dostępu firmy Starbuzz	428
Uruchomienie bezprzewodowego punktu dostępu okazało się sukcesem!	432



Bezpieczeństwo w sieci

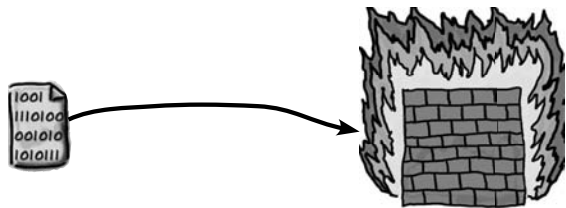
11

Broń się!

Sieć to niebezpieczne miejsce do zarabiania na życie. Niebezpieczeństwo czai się za każdym rogiem — rootkity, skrypciarze, boty... Musisz wzmocnić sieć, aby barbarzyńcy nie złamali zabezpieczeń. W tym rozdziale poznasz sieciowe podziemie, gdzie napastnicy fałszują adresy MAC, „zatruwają” pamięć ARP, infiltrują internety, wstrzykują pakiety do sieci i wyłudzą hasła od Twoich współpracowników. Broń się! Nie pozwól na to, aby dane wydostały się poza sieć lub by włamali się do niej intruzy.



„Źli chłopcy” są wszędzie	434
Szkody mogą nie ograniczać się do SIECI	435
Wielka czwórka zabezpieczeń sieci	436
Zabezpiecz sieć przed fałszowaniem adresów MAC	439
Jak można bronić się przed fałszowaniem adresów MAC?	444
Chroń sieć przed „zatrutowaniem” tablicy ARP	445
Jak można zapobiec atakom przez „zatrutowanie” tablicy ARP?	446
Tu chodzi o dostęp, mała!	448
Skonfiguruj w routerze listę kontroli dostępu, aby utrzymać napastników z dala od sieci	449
Jak skonfigurować listę kontroli dostępu?	451
Zapory filtrują pakiety przesyłane między sieciami	454
Filtrowanie pakietów rządzi!	455
Bądź sprytny — stosuj stanowe filtrowanie pakietów	460
Człowiek to najsłabsze ogniwo w łańcuchu zabezpieczeń	463
Jak działa socjotechnik?	464
Zwalczaj socjotechników za pomocą przejrzystej i zwięzłej polityki bezpieczeństwa	466
Wzmocniłeś sieć	469



12

Projektowanie sieci

Musisz mieć plan!

Przy budowaniu sieci najważniejszy jest dobry plan. Od pierwszego rozdziału nauczyłeś się już wielu rzeczy o sieciach komputerowych. Dowiedziałeś się, jak tworzyć fizyczne sieci przewodowe, jak działają bezprzewodowe punkty dostępu i jak wykorzystać wszystkie możliwości inteligentnych urządzeń sieciowych. Poznałeś też rozmaite techniki rozwiązywania problemów, które pomogą Ci wydostać się z najgorszych opałów. Teraz nadeszła pora na zastosowanie tej wiedzy w praktyce. Zobacz, jak daleko zaszedłeś w swoich podróżach z sieciami. Jesteśmy pewni, że sobie poradzisz!

Tym razem musisz zaplanować sieć od podstaw!	472
Przed przygotowaniem planu musisz poznać potrzeby	475
Przygotowałeś pytania — co dalej?	477
Przyjrzyj się planowi działań	478
Masz już fizyczny układ sieci. Co dalej?	481
Projekty przedstawiają wszystkie aspekty planowanego budynku	482
Możliwe, że będziesz musiał zmodyfikować plany sieci na podstawie projektów!	483
Opracowałeś już fizyczny układ sieci. Co dalej?	490
Na zakończenie musisz przygotować plan instalowania	498



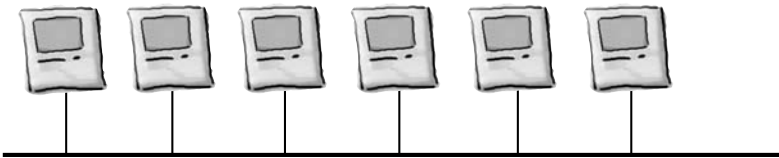
Pozostałości

A

Dziesięć najważniejszych tematów (których nie poruszyliśmy)

Sieci komputerowe to tak rozległe zagadnienie, że nie liczyliśmy nawet na to, iż opiszemy je całe w jednej książce. Jednak zanim wypuścimy Cię w wielki świat, chcemy dodać do Twojego przybornika kilka dodatkowych narzędzi. Niektóre z nich są opisane w każdej książce na temat sieci komputerowych, dlatego uznaliśmy, że możemy „upchnąć” je w tym miejscu. Inne punkty dotyczą kwestii wysokopoziomowych. Chcemy, abyś poznał przynajmniej terminologię i podstawowe pojęcia z tego obszaru. Dlatego zanim odłożysz książkę na półkę, zapoznaj się z tymi dodatkami.

Numer 1. Topologie sieci	504
Numer 2. Instalowanie programu Wireshark	506
Numer 3. Uruchamianie konsoli i terminalu	508
Numer 4. Stos TCP	509
Numer 5. Sieci VLAN	510
Numer 6. Symulatory systemu IOS firmy Cisco	510
Numer 7. Protokół BGP	511
Numer 8. Sieci VPN	511
Numer 9. Systemy wykrywania włamań	512
Numer 10. Certyfikaty firmy Cisco	512



Tabele kodów ASCII

B

Sprawdzanie kodów

Gdzie byś doszedł bez zaufanych tabel kodów ASCII? Nie zawsze wystarczy zrozumieć protokoły sieciowe. Wcześniej czy później będziesz musiał sprawdzić kody ASCII, aby ustalić, jakie sekrety są przesyłane przez sieć. W tym dodatku przedstawiamy zestaw kodów ASCII. Niezależnie od tego, czy preferujesz format dwójkowy, szesnastkowy, czy tradycyjny (dziesiętny) — w tym miejscu znajdziesz kody, których potrzebujesz.

Kody ASCII — od 0 do 31	514
Kody ASCII — od 32 do 63	515
Kody ASCII — od 64 do 95	516
Kody ASCII — od 96 do 127	517

Instalowanie serwera BIND

C

Serwer do obsługi systemu DNS

Każdy profesjonalista zajmujący się sieciami potrzebuje dobrego serwera DNS. Najpopularniejszym tego rodzaju serwerem w Internecie jest BIND. Proces jego instalowania jest prosty, jednak jeśli potrzebujesz pomocy, znajdziesz tu przydatne instrukcje.

Numer 1. Instalowanie serwera BIND w systemie Windows (XP, 2000 i Vista)	520
Numer 2. Instalowanie serwera BIND w systemie Mac OS X Server	521
Numer 3. Instalowanie serwera BIND w Linuksie i klienckiej wersji systemu Mac OS X	521

S

Skorowidz

523

5. Urządzenia i ruch w sieci

Jak inteligentna jest Twoja sieć?

Wszyscy w biurze uważają mnie za szaloną, a ja wiem, że ona nas obserwuje! Ostrzegałam ich, ale wkrótce sami się o tym przekonają. Ta sieć jest zbyt inteligentna!

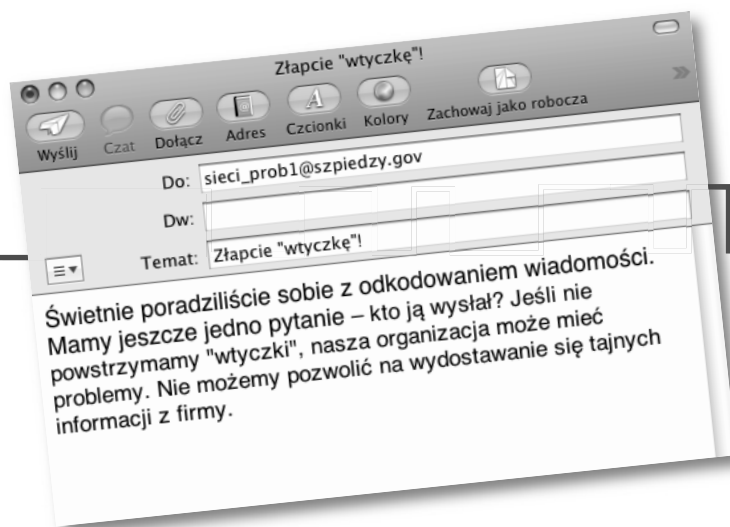


Sieć zawsze może być bardziej inteligentna. W sieć należy wbudować jak najwięcej inteligencji, jednak **z czego ona wynika?** Najważniejsze są urządzenia sieciowe. W tym rozdziale pokażemy, jak **koncentratory, przełączniki i routery** wykorzystują swoją naturalną **inteligencję** do przesyłania pakietów w sieci. Dowiesz się, w jaki sposób te narzędzia „**myślą**” i dlaczego są tak **przydatne**. Podejrzymy nawet dane przesyłane w sieci za pomocą **oprogramowania do analizowania pakietów**. Czytaj dalej, a zobaczysz, jak **włączyć turbodoładowanie sieci**.

Wróćmy do wiadomości...

Odkodowałeś tajną wiadomość...

Jesteś znakomitym pracownikiem technicznym agencji szpiegowskiej Head First. Udało Ci się odkodować tajną wiadomość z niebezpiecznego sygnału. Co dalej?



.. ale jak ustalić, kto ją wysłał?

Choć zdołałeś odkodować komunikat wysłany przez „wtyczkę”, nie wiadomo, kto nią jest. Jeśli nie wiemy, kto jest źródłem niebezpiecznych wiadomości, nie możemy zapobiec ich wysyłaniu.

Musimy wykryć, kto jest „wtyczką”. Jak to zrobić? Mamy tylko niebezpieczny sygnał, na podstawie którego odkodowałeś wiadomość. Czy pomoże to ustalić tożsamość „wtyczki”?



Ćwiczenie

Podpisz każdą część poniższej ramki i wyjaśnij, który fragment może pomóc w wykryciu „wtyczki”.



Uwagi:

.....

.....

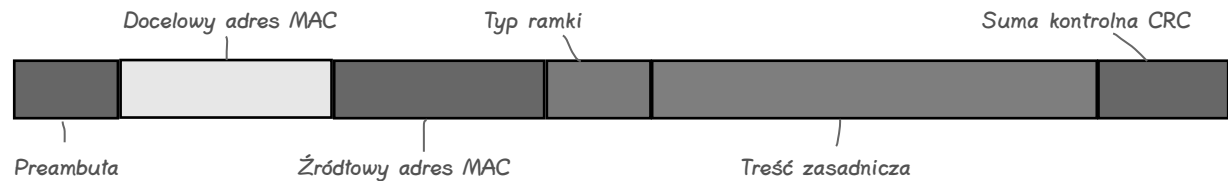
.....

.....



Ćwiczenie:
Rozwiązanie

Podpisz każdą część poniższej ramki i wyjaśnij, który fragment może pomóc w wykryciu „wtyczki”.



Uwagi: *Treść zasadnicza zawiera tajną wiadomość od „wtyczki”. Źródłowy adres MAC informuje, z którego urządzenia wystano komunikat. Pomoże to ustalić komputer, z którego korzysta „wtyczka”.*

Docelowy adres MAC określa, gdzie dane zostaną przesłane.

Dane w pakiecie informują o jego pochodzeniu

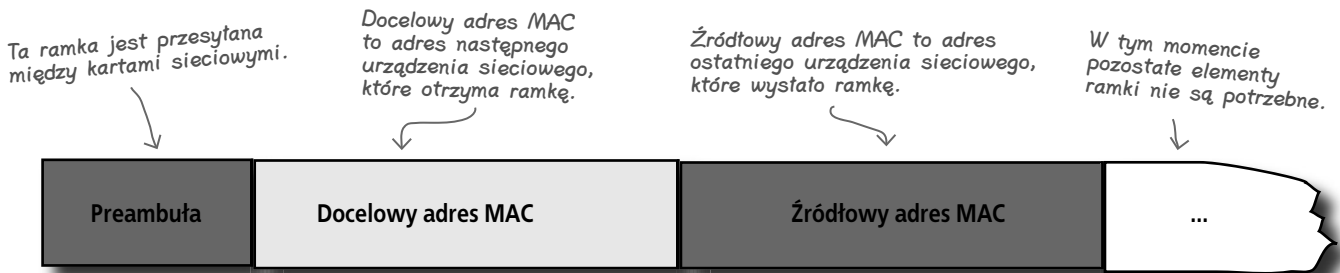
W czasie odkodowywania wiadomości dowiedziałeś się, że każdy pakiet zawiera źródłowy adres MAC. Oznacza to, że obejmuje adres MAC urządzenia, które wysłało dany pakiet.

Adres MAC jest zapisany na karcie sieciowej zainstalowanej w komputerze. Takie adresy mają sześć bajtów długości (48 bitów). Zwykle są zapisane w systemie szesnastkowym, a poszczególne bajty są rozdzielone dwukropkami lub myślnikami, na przykład 0f:2b:5d:e7:a3:eb.



Ciekawostki

Nie tylko komputery mają adresy MAC. Wiele systemów gier wideo z obsługą Internetu ma okno konsoli, które umożliwia sprawdzenie adresu MAC urządzenia.



Adres MAC urządzenia, z którego wysłano niebezpieczną wiadomość, to 00:1f:f3:53:fe:32. Jak na tej podstawie można określić, kto jest „wtyczką”?

To proste. Musimy znaleźć komputer o odpowiednim adresie MAC, a następnie sprawdzić, kto z niego korzysta. „Wtyczka” to prawdopodobnie użytkownik maszyny, z której wysłano komunikaty, prawda?

Zobaczmy, czy ta metoda okaże się skuteczna.



Który adres MAC?

Kto jest „wtyczką”?

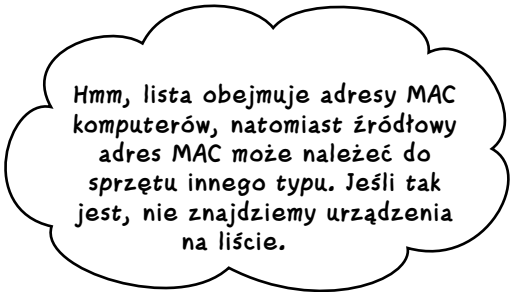
Oto lista wszystkich adresów MAC w firmie, którą badasz.
Kto korzysta z komputera, z którego wysłano niebezpieczny sygnał?

Adres MAC maszyny, z której wysłano niebezpieczny sygnał, to 00:1f:f3:53:fe:32. Dlaczego nie ma go na liście?



Osoba	Lokalizacja	Adres IP	Adres MAC
Marek D.	Administracja	192.168.100.34	00:1f:f3:53:fe:ae
Ola T.	Obsługa klienta	192.168.100.45	00:1f:f3:53:fe:28
Piotr G.	Dział dostaw	192.168.100.32	00:1f:f3:53:f:18
Jan M.	Dział IT	192.168.100.2	00:1f:f3:54:27:d2
Diana Z.	Dział IT	192.168.100.3	00:1f:f3:86:fe:2a
Karolina C.	Administracja	192.168.100.4	00:1f:f3:23:4f:1a
Serwer	Dział IT	192.168.100.100	00:1f:f3:23:4f:27

Niestety, źródłowego adresu MAC sygnału nie ma na liście komputerów, choć jest ona aktualna. Jak to możliwe?



Także urządzenia innego typu mają adresy MAC.

Przyjrzyj się sieci i sprawdź, czy uda Ci się zrozumieć, co się w niej dzieje.

Sieć to nie tylko komputery

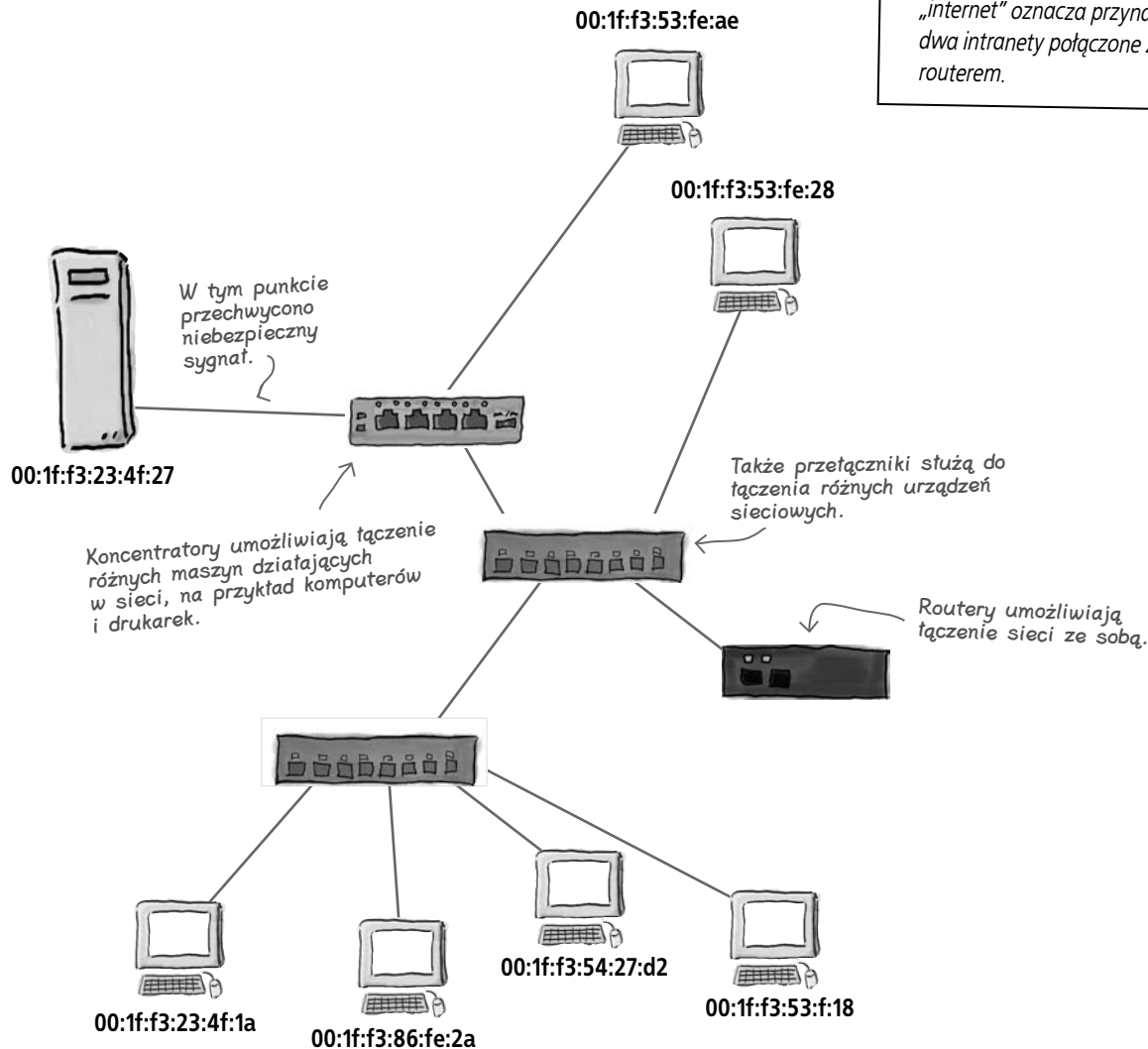
Firmowa sieć składa się nie tylko z komputerów i serwerów, ale też z urządzeń sieciowych, takich jak koncentratory, przełączniki i routery. Koncentratory i przełączniki działają w sieciach LAN oraz intranetach, natomiast routery umożliwiają budowanie sieci WAN i internetów.



Nazwy „Internet” i „internet” oznaczają co innego.

Uwaga!

Słowo „Internet” określa dużą przestrzeń pełną powiązań, umożliwiającą przesyłanie danych po całym świecie. Pojęcie „internet” oznacza przynajmniej dwa intranety połączone ze sobą routerem.

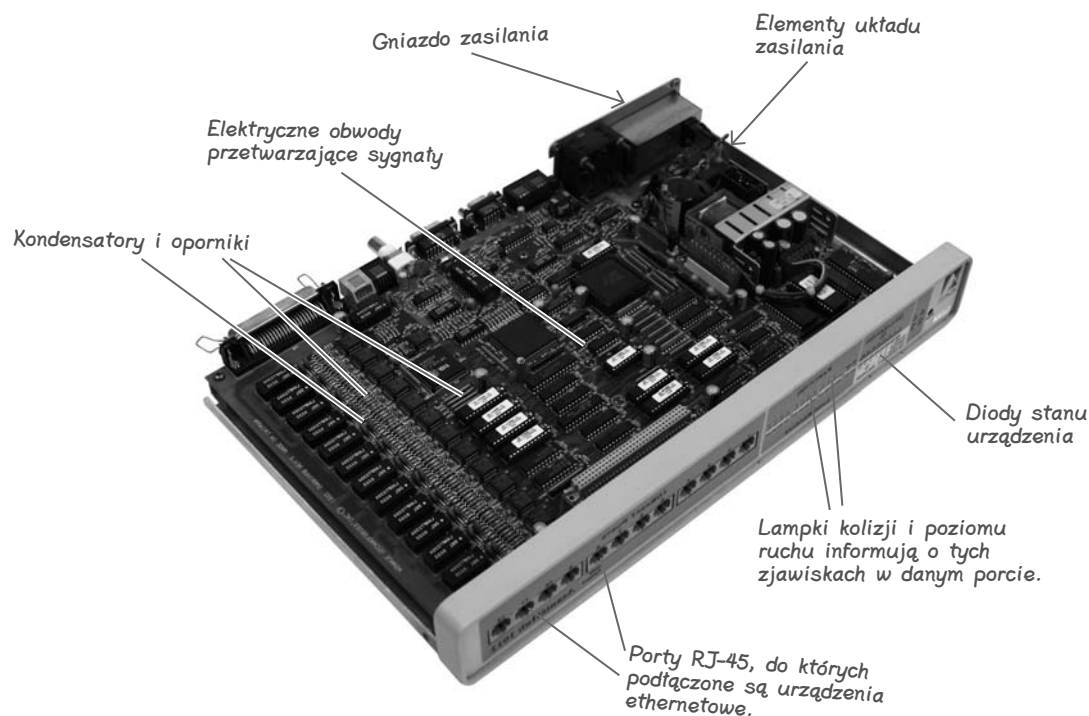




Koncentrator pod lupą

Jak wyjaśniliśmy to wcześniej, koncentratory (inaczej huby) umożliwiają podłączanie do sieci różnych maszyn, na przykład komputerów i drukarek. Koncentrator przyjmuje przychodzący sygnał, kopiuje go do wszystkich portów i emituje. Koncentrator jest nazywany czasem repeaterem (czyli „powtarzaczem”), ponieważ powtarza odebrany sygnał bez korzystania z cyfrowej „inteligencji”, na przykład pamięci lub procesora.

Tak wygląda wnętrze koncentratora:



Koncentratory nie są inteligentne

Koncentrator to proste urządzenie, które nie rozumie danych przesyłanych w sieci, nie zna adresów MAC i ich nie przechowuje. Jego jedyne zadanie to przekazywanie przychodzących sygnałów do wszystkich portów bez wprowadzania żadnych zmian.

Koncentratory nie zmieniają adresu MAC

W jaki sposób ma to pomóc w wysledzeniu źródła niebezpiecznego sygnału?

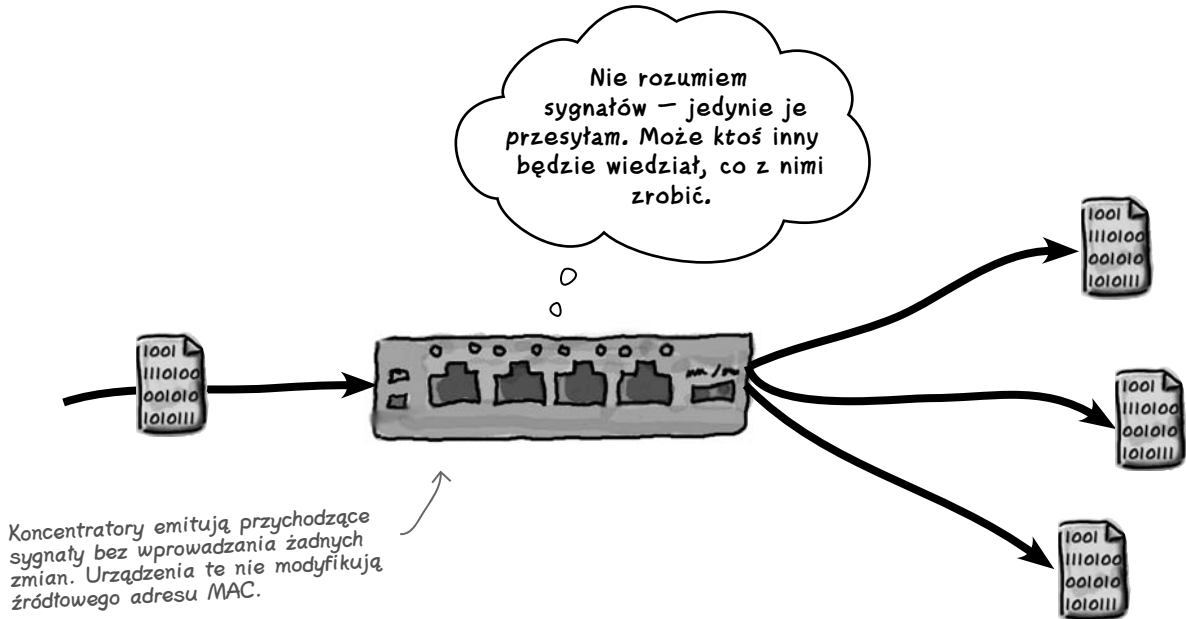
Ostatnim urządzeniem, przez które przeszedł pakiet przed jego przechwyceniem, był koncentrator. Ponieważ to narzędzie jedynie przesyła sygnał i nie rozumie danych sieciowych, nie wprowadza żadnych zmian w źródłowym adresie MAC. Koncentrator pozostawia ten adres w takiej samej postaci, w jakiej go otrzymał.



Uwaga!

Nie można wykryć, że pakiet został wysłany przez koncentrator.

Aby to ustalić, musisz znać układ sieci i węzłów podłączonych do koncentratorów.



Które urządzenie wysłało pakiet do koncentratora?

Ponieważ koncentrator nie modyfikuje źródłowego adresu MAC, adres ten musi należeć do urządzenia, które przekazało sygnał do koncentratora. Trzeba spojrzeć poza koncentrator, aby wykryć „wtyczkę”.

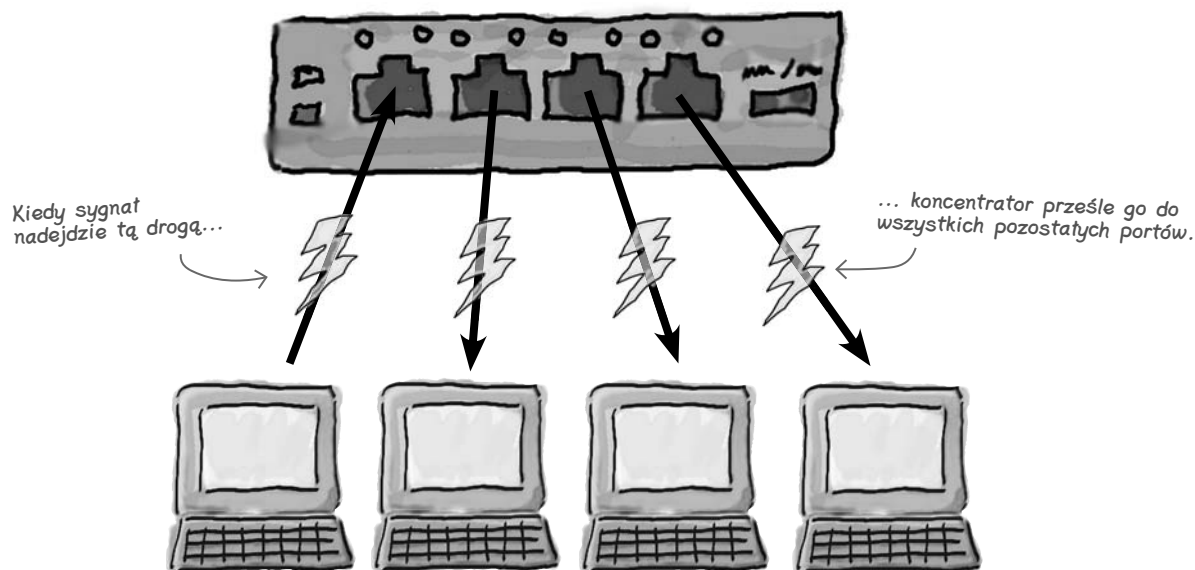


WYSIL SZARE KOMÓRKI

Koncentratory nie mają procesorów. Jakie wnioski na temat przetwarzania sygnału przez koncentratory możesz wysnuć na tej podstawie?

Koncentrator wysyła sygnały wszędzie

Koncentrator otrzymuje sygnały i rozsyła je wszystkimi pozostałymi portami. Kiedy kilka urządzeń zaczyna wysyłać dane, bezładne powielanie sygnału przez koncentrator prowadzi do nadmiernego ruchu w sieci i kolizji. Kolizja ma miejsce, kiedy dwa sygnały „wpadną” na siebie, co prowadzi do błędu. Nadawca musi wtedy odczekać odpowiedni czas, aby ponownie wysłać sygnał.



Podstawą działania koncentratorów jest elektryczność

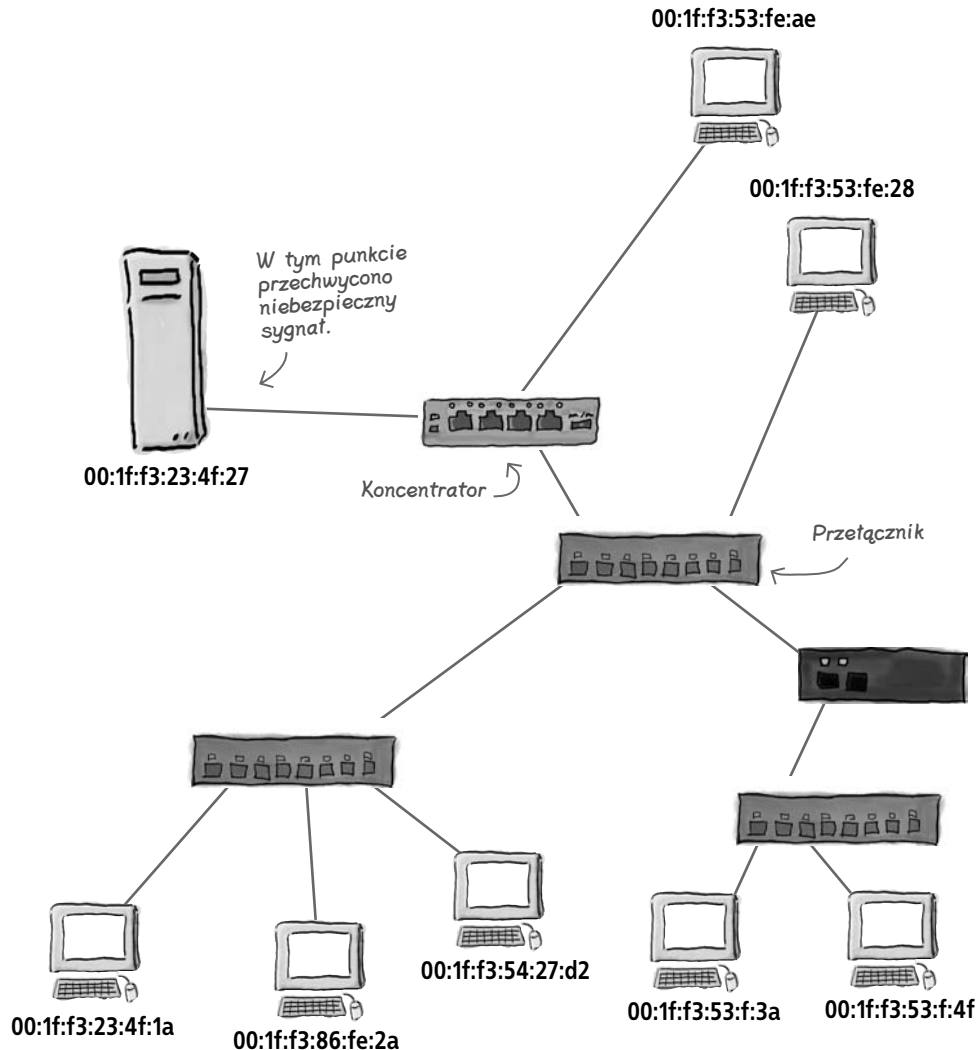
Koncentratory nie mają procesorów, co oznacza, że nie rozumieją danych sieciowych, na przykład adresów MAC lub ramek. Traktują przychodzący sygnał sieciowy jako zjawisko czysto elektryczne i przekazują go.

Co dalej?

Koncentrator to urządzenie elektryczne, które służy tylko do przekazywania danych. Przyjmuje dowolny sygnał i wysyła go do wszystkich pozostałych portów.

Które urządzenie przekazało sygnał do koncentratora?

Wiesz już, że sygnał przeszedł przez koncentrator. Nadal jednak nie wiadomo, które urządzenie sieciowe wysłało dane. Wróćmy do diagramu sieci. Tym razem zwróć uwagę na to, które urządzenia są podłączone do koncentratora.

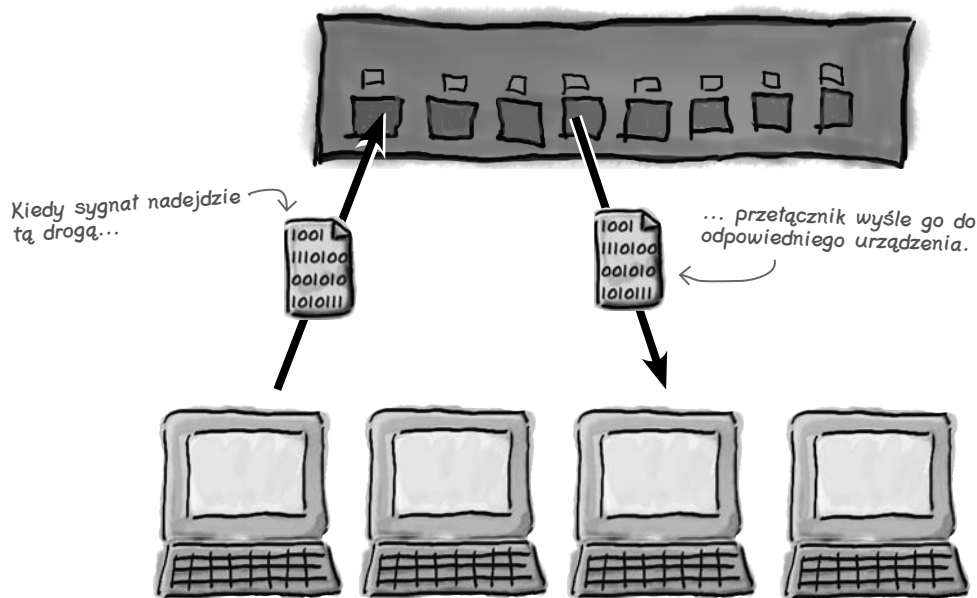


Do koncentratora podłączone są dwa urządzenia, które mogą być źródłem sygnału — komputer i przełącznik. Ponieważ adres MAC komputera nie pasuje do szukanego adresu, wiadomo, że to nie z tej maszyny wysłano dane. Oznacza to, że źródłem sygnału jest przełącznik.

Jak działają przełączniki?

Przełącznik wysyła ramki tylko do docelowej lokalizacji

Przełączniki pozwalają uniknąć kolizji, ponieważ rejestrują i przekazują ramki w intranecie. Te urządzenia wykorzystują do tego adres MAC zapisany w ramce. Zamiast powtarzać ten sam sygnał we wszystkich portach, przełączniki przekazują go tylko do docelowego odbiorcy.



Działanie przełączników oparte jest na ramkach

Przełączniki zawierają procesory, pamięć RAM i układy ASICs, co powoduje, że mogą przetwarzać dane sieciowe. Te urządzenia rozumieją adresy MAC i ramki, dlatego w inteligentny sposób obsługują przychodzące sygnały sieciowe. Przełączniki potrafią określić docelową lokalizację sygnału i dostosować do tego swoje działanie.

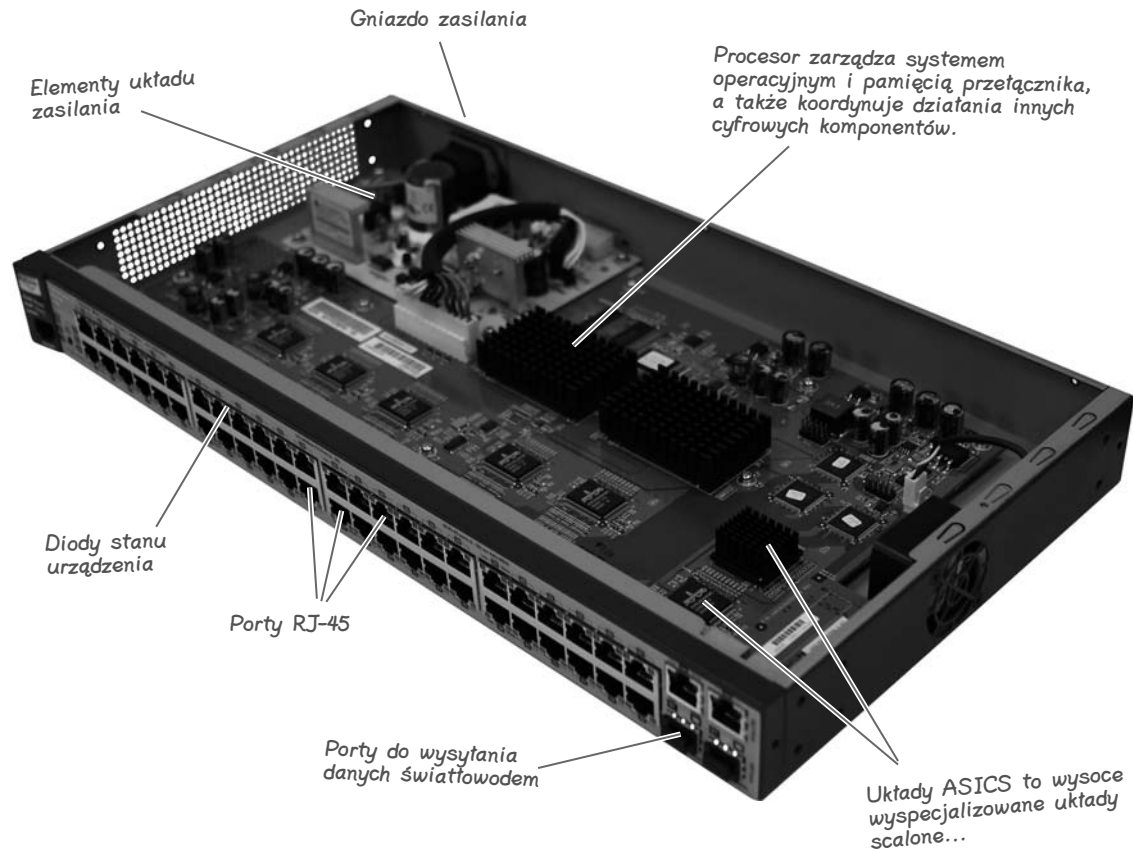
Przełącznik odczytuje sygnał jako ramkę i używa zapisanych w niej informacji do wysłania danych do odpowiedniego urządzenia.

Przełączniki pod lupą



Przełącznik — podobnie jak koncentrator — umożliwia podłączenie do sieci różnych maszyn, na przykład komputerów i drukarek.

Oto wnętrze przełącznika:



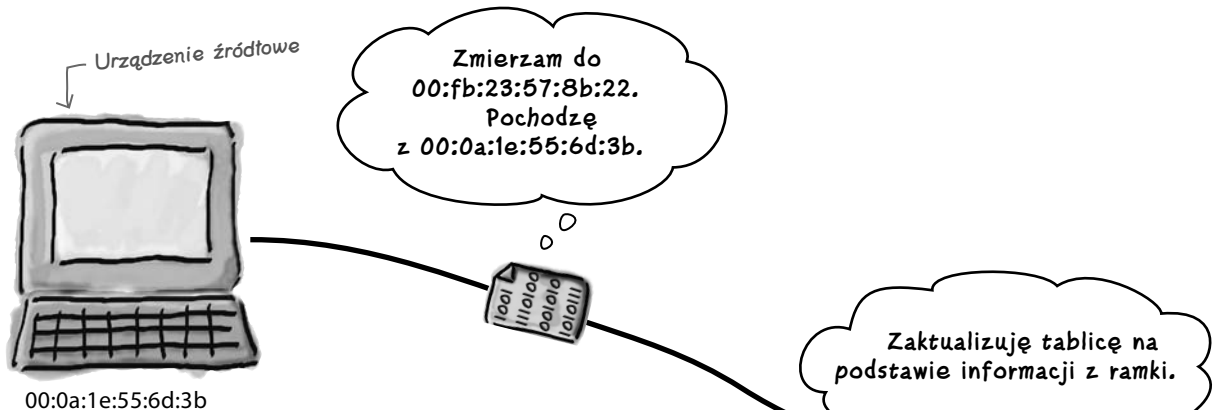
Przełączniki są inteligentne

Obsługiwanie sygnału przez koncentratory i przełączniki przebiega zupełnie inaczej. Przełącznik potrafi przetwarzać sygnały jako ramki i rozpoznaje adresy MAC. Zamiast przysyłać przychodzące sygnały do wszystkich portów, przełącznik może zapisać pakiety i przekazać je do docelowych urządzeń.

Przyjrzyjmy się bliżej działaniu przełączników.

Przełączniki przechowują adresy MAC w tablicy przeglądowej, co umożliwia płynne przesyłanie ramek

- 1 Źródłowa stacja robocza wysyła ramkę.
Ramka obejmuje treść zasadniczą i czas wysłania danych, a także źródłowy i docelowy adres MAC.



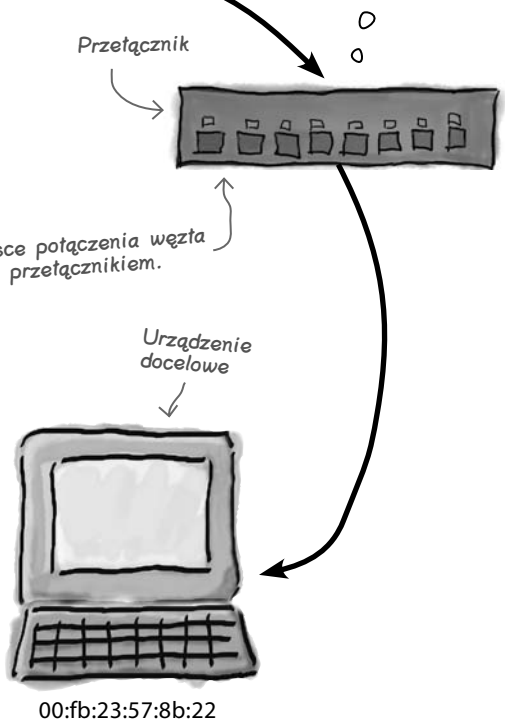
- 2 Przełącznik aktualizuje tablicę adresów MAC na podstawie adresu MAC urządzenia i portu, do którego jest ono podłączone.
Przełączniki przechowują tablice adresów MAC. Kiedy przełącznik odbiera ramkę, uzyskuje nowe informacje o ruchu w sieci i łączy porty z adresami MAC.

Adres MAC docelowej maszyny	Port
00:fb:23:57:8b:22	49

Przełącznik używa tablicy do śledzenia informacji z ramek.

Port to miejsce połączenia węża sieciowego z przełącznikiem.

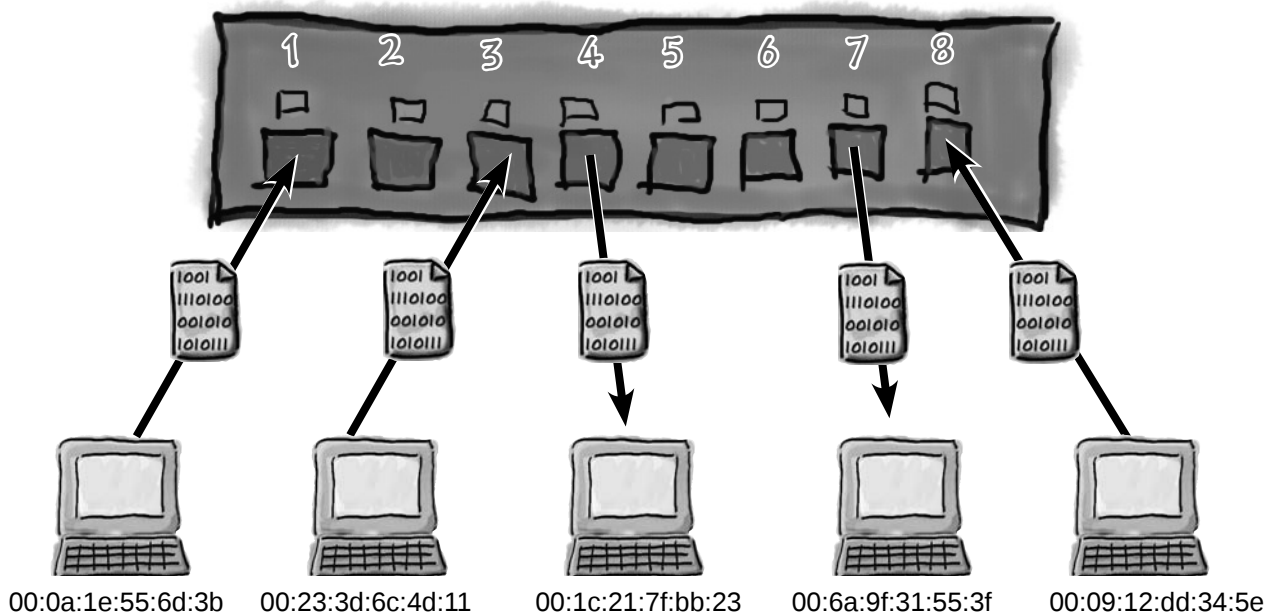
- 3 Przełącznik przekazuje ramkę pod docelowy adres MAC na podstawie informacji z tablicy.
Przełącznik robi to przez wysłanie ramki przez port powiązany w tablicy z danym adresem MAC.



ZOSTAŃ przełącznikiem



Wciel się w rolę przełącznika
i zaktualizuj tablicę na podstawie
dostępnych informacji
z ramek. Strzałki pomogą
Ci powiązać adresy MAC
z portami. Pierwszy wiersz
uzupełniłmy za Ciebie.

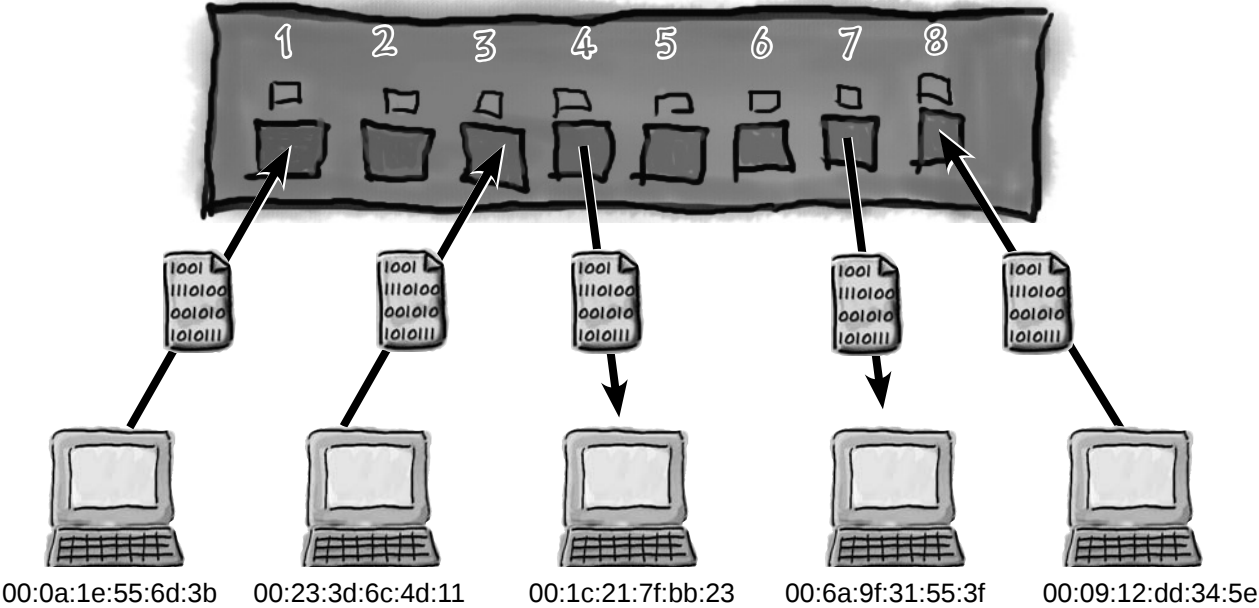


Adres MAC	Port
00:0a:1e:55:6d:3b	1

ZOSTAŃ przełącznikiem.
Rozwiązanie

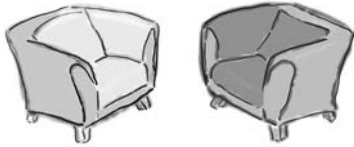


Wciel się w rolę przełącznika i zaktualizuj
tablicę na podstawie
dostępnych informacji
z ramek. Strzałki pomogą
Ci powiązać adresy MAC
z portami. Pierwszy wiersz
uzupełniliśmy za Ciebie.



Adres MAC	Port
00:0a:1e:55:6d:3b	1
00:23:3d:6c:4d:11	3
00:1c:21:7f:bb:23	4
00:6a:9f:31:55:3f	7
00:09:12:dd:34:5e	8

Pogawędki przy kominku



Dziś w programie: koncentrator i przełącznik

Koncentrator:

Śłuchaj, przełączniku, mam już dość żartów na temat mojej inteligencji.

Mam już dość... Czy znowu sobie ze mnie żartujesz?

Rzeczywiście, nazywają mnie repeaterem, i co z tego?

W porządku, powtarzam sygnały, ale poza tym działamy całkiem podobnie.

Wolę prąd niż dane. Dlatego operuję wyłącznie na elektryczności.

Natomiast ja łączę komputery ze sobą.

Chcę mieć pewność, że wszystkie urządzenia w sieci dowiedzą się o danych.

Ja jednak jestem tańszy. Nie pokonasz mnie pod tym względem.

Przełącznik:

Czy możesz to powtórzyć?

To tylko mały żart na temat twojej drugiej nazwy.

W tym właśnie kryje się problem. Ponieważ WSZYSTKO, co odbierzesz w jednym porcie, powtarzasz w każdym pozostałym, sieć działa bardzo powoli.

Nieprawda. Ty działasz na podstawie sygnałów, a ja korzystam z ramek.

Ja działam jak komputer i mam własny system operacyjny.

Jednak nie robisz tego wydajnie. Niepotrzebnie kierujesz dane sieciowe do wszystkich portów.

Prowadzi to do zbędnego szumu informacyjnego. Ja przesyłam ramki dokładnie tam, gdzie są potrzebne. Mam wbudowaną logikę cyfrową i potrafię odczytywać informacje z ramek oraz używać ich do precyzyjnego przekazywania danych.

Jestem wart każdej ceny. Jeśli ktoś doda mnie do sieci, w której działają same koncentratory, błyskawicznie zwiększę jej przepustowość.

Przełącznik posiada cenne informacje

Ponieważ przełącznik przechowuje adresy MAC, możliwe powinno być połączenie się z tym urządzeniem i przyjrzenie się zawartości jego tablic.

Czy w ten sposób uzyskamy informacje potrzebne do znalezienia „wtyczki”?

- 1 Podłącz komputer do przełącznika kablem szeregowym.

Użyjesz tego kabla do komunikowania się z przełącznikiem.

Tańsze przełączniki zwykle nie mają portów szeregowych.

- 2 Otwórz terminal (na przykład Hyperterminal) i przejdź do wiersza polecenia przełącznika. Wpisz poniższą instrukcję:

```
Plik Edycja Okno Pomoc KtóryPrzełącznik?  
  
switch# show mac-address  
  
Status and Counters - Port Address Table  
  
MAC Address   Located on Port  
-----  
000074-a23563 49  
0001e6-70f1bb 44  
0001e6-7673f6 42  
0001e6-800044 37  
0001e6-81cb6b 5  
0001e6-8f0a86 12  
#
```

Adres MAC komputera lub innego urządzenia sieciowego podłączonego do przełącznika.

Numer portu, do którego podłączone jest dane urządzenie.



WYSIL SZARE KOMÓRKI

Jak sądzisz, jak długo przełącznik przechowuje adresy MAC w tablicy?



Uwaga!

Powyższa instrukcja jest przeznaczona dla przełącznika HP ProCurve.

Aby wyświetlić tablicę adresów MAC w przełącznikach innych marek, możesz potrzebować nieco odmiennych instrukcji.



Franek: Sądysz więc, że przełączniki nie rejestrują tego adresu MAC?

Kuba: Nie — problem polega na tym, że przełącznik usuwa zawartość tablicy adresów MAC po mniej więcej trzech minutach.

Franek: Usuwa zawartość?

Kuba: Tak — kiedy urządzenie sieciowe zakończy przesyłanie danych, przełącznik usuwa wpisy z tablicy, aby jej rozmiar pozostał niewielki.

Franek: Jak wpływa to na możliwość znalezienia niebezpiecznej maszyny?

Kuba: No cóż, sprawdziłem wszystkie komputery i nie znalazłem niebezpiecznego adresu.

Franek: Co teraz?

Kuba: Uważam, że musimy zacząć przechwytywać dane i poszukać tych z odpowiednim źródłowym adresem MAC. Następnie możemy wrócić do przełącznika i znaleźć ten adres, aby zawęzić poszukiwania do określonego portu.

Franek: To wygląda na dobry plan. W jaki sposób chcesz przechwytywać dane?

Kuba: Muszę poszukać odpowiedniego programu...

Można użyć oprogramowania do monitorowania pakietów

Jeśli chcesz śledzić ruch w sieci i przechwytywać informacje z pakietów, możesz zastosować doskonały program, działający dokładnie tak, jak tego potrzebujesz. Jest to aplikacja Wireshark. Aby monitorować dane, wystarczy zainstalować program w stacji roboczej, a następnie podłączyć ją do sieci w miejscu, które chcesz obserwować. Aplikacja zacznie udostępniać informacje o pakietach docierających do stacji roboczej.

Program Wireshark jest zainstalowany w stacji roboczej podłączonej do sieci.

Więcej informacji o instalowaniu programu Wireshark znajdziesz w dodatku A.

Wireshark śledzi przychodzące i wychodzące pakiety oraz wyświetla informacje o nich na ekranie.

Kabel ethernetowy

Sieć

Użyj programu Wireshark do śledzenia pakietów na poziomie przełącznika. W ten sposób możesz przechwycić następane sygnały wysyłane przez „wtyczkę” i dowiedzieć się, jakie urządzenie sieciowe przekazuje te dane do przełącznika.

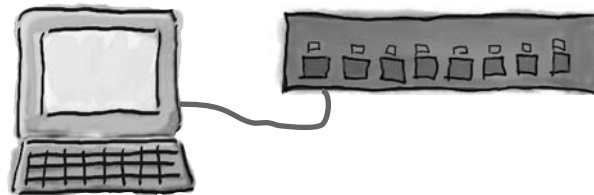
Podłącz program Wireshark do przełącznika

Jak można wykorzystać program Wireshark do monitorowania danych przechodzących przez przełącznik? Wystarczy zastosować się do poniższych instrukcji.

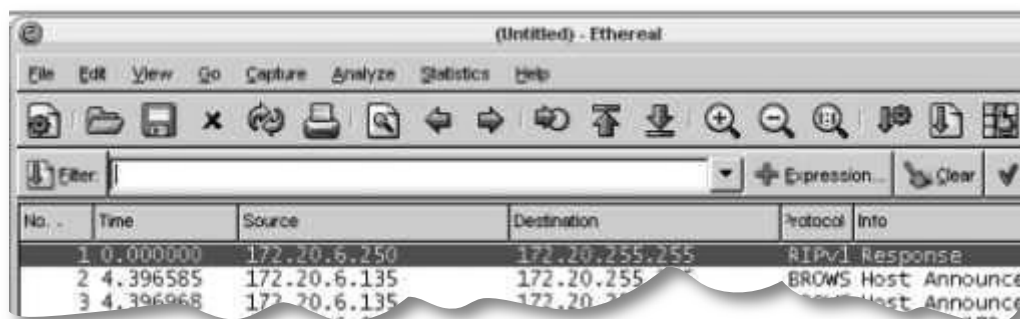
- 1 Podłącz komputer do przełącznika kablem szeregowym. Wykorzystasz ten kabel do komunikowania się z przełącznikiem.
- 2 Otwórz terminal (na przykład Hyperterminal) i uruchom wiersz polecenia przełącznika. Wpisz poniższe instrukcje.

```
Plik Edycja Okno Pomoc NieWchodźDoWody
switch> enable
switch# port monitor 1 2,3,4,5,6
```

- 3 Podłącz komputer do portu 1 przełącznika za pomocą kabla ethernetowego. To połączenie posłuży do przechwytywania danych sieciowych.



- 4 Uruchom program Wireshark i przechwyc dane sieciowe.



Jakie informacje udostępnia program Wireshark?

Program Wireshark udostępnia informacje o danych sieciowych

Wireshark wyświetla wszystkie dane sieciowe wykryte przez komputer w przełączniku, do którego jest podłączony. Jeśli chcesz, możesz odfiltrować dane wyjściowe i poszukać określonych ramek.

Jakie pole zastosujesz jako filtr?

Ten panel pokazuje dane przechwycone przez program Wireshark. Każdy wiersz to jeden pakiet.

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No. .	Time	Dest MAC	Source MAC	Source	Destination	Protocol	Info
6	9.201419	WestellT ae:82:4c	Apple 53:d4:d3	192.168.1.46	74.125.155.147	TCP	54740 > http [SYN] Seq=0 Win=65535 [TCP ...]
7	9.247904	Apple 53:d4:d3	WestellT ae:82:4c	74.125.155.147	192.168.1.46	TCP	http > 54740 [SYN, ACK] Seq=0 Ack=1 Win=...
8	9.247962	WestellT ae:82:4c	Apple 53:d4:d3	192.168.1.46	74.125.155.147	TCP	54740 > http [ACK] Seq=1 Ack=1 Win=52428...
9	9.248189	WestellT ae:82:4c	Apple 53:d4:d3	192.168.1.46	74.125.155.147	HTTP	GET /search?client=safari&rls=en-us&q=pr...
10	9.318327	Apple 53:d4:d3	WestellT ae:82:4c	74.125.155.147	192.168.1.46	TCP	http > 54740 [ACK] Seq=1 Ack=1157 Win=800...
11	9.329707	Apple 53:d4:d3	WestellT ae:82:4c	74.125.155.147	192.168.1.46	TCP	[TCP segment of a reassembled PDU]
12	9.329758	WestellT ae:82:4c	Apple 53:d4:d3	192.168.1.46	74.125.155.147	TCP	54740 > http [ACK] Seq=1157 Ack=279 Win=...
13	9.331217	Apple 53:d4:d3	WestellT ae:82:4c	74.125.155.147	192.168.1.46	TCP	[TCP segment of a reassembled PDU]
14	9.332222	Apple 53:d4:d3	WestellT ae:82:4c	74.125.155.147	192.168.1.46	TCP	[TCP segment of a reassembled PDU]
15	9.332254	WestellT ae:82:4c	Apple 53:d4:d3	192.168.1.46	74.125.155.147	TCP	54740 > http [ACK] Seq=1157 Ack=3115 Win=...
16	9.332417	Apple 53:d4:d3	WestellT ae:82:4c	74.125.155.147	192.168.1.46	TCP	[TCP segment of a reassembled PDU]
17	9.332439	WestellT ae:82:4c	Apple 53:d4:d3	192.168.1.46	74.125.155.147	TCP	54740 > http [ACK] Seq=1157 Ack=3451 Win=...

▶ Frame 7 (74 bytes on wire (74 bytes captured))

▶ Ethernet II, Src: WestellT ae:82:4c (00:18:3a:ae:82:4c), Dst: Apple_53:d4:d3 (00:1f:f3:53:d4:d3)

▶ Internet Protocol, Src: 74.125.155.147 (74.125.155.147), Dst: 192.168.1.46 (192.168.1.46)

▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 54740 (54740), Seq: 0, Ack: 1, Len: 0

0000 00 1f f3 53 d4 d3 00 18 3a ae 82 4c 08 00 45 00 ...S... :...L...E.
0010 00 3c ac a9 00 00 35 06 31 2c 4a 7d 9b 00 00 a8 ...C...5...1...J...
0020 01 00 00 d5 d4 5d f2 f4 00 00 00 00 00 00 00

To okno przedstawia przesłane w pakietach nieprzetworzone dane w systemie szesnastkowym.

Ten panel wyświetla informacje na temat każdego pakietu.



Ciekawostki

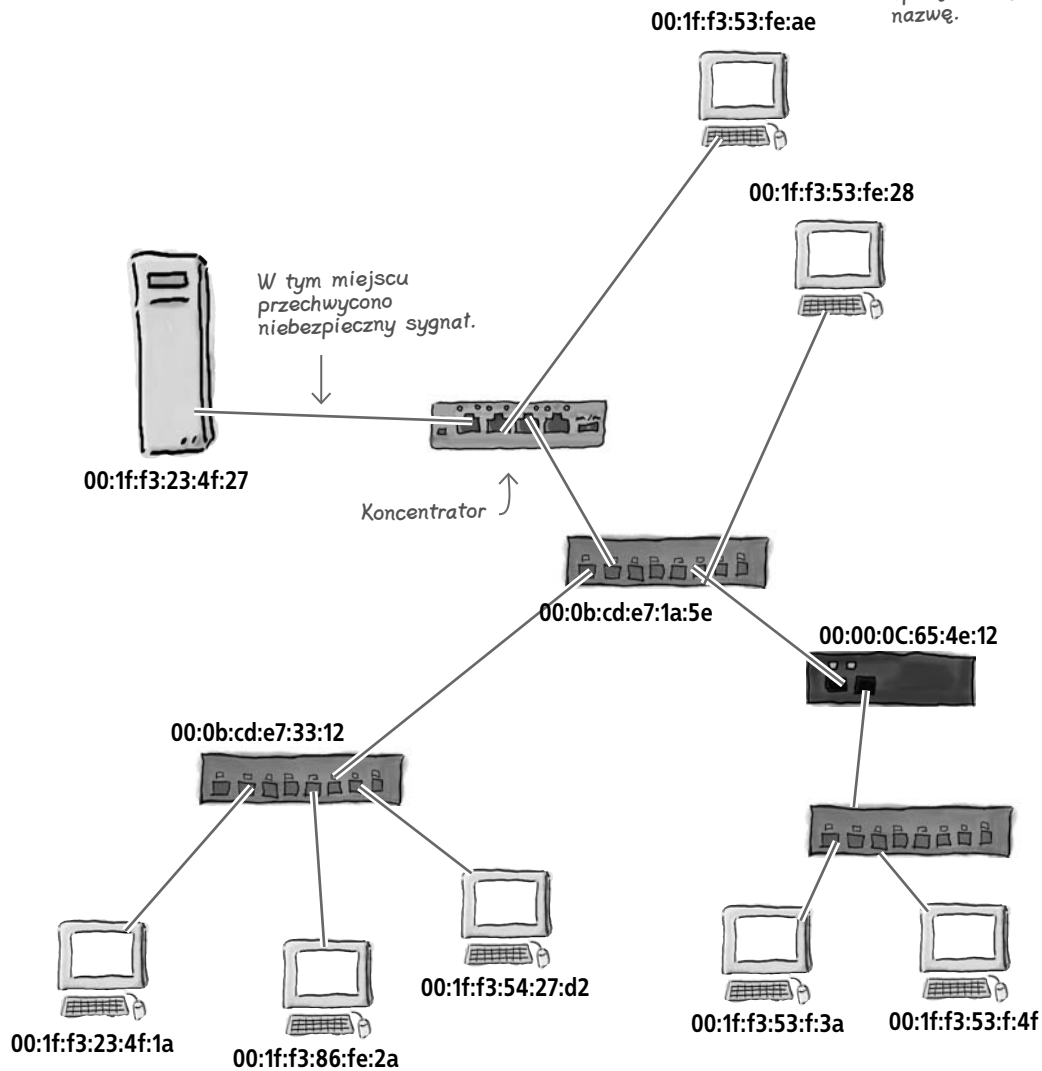
Oficjalnie Wireshark jest „analizatorem protokołów”.

Zaostrz ołówek

Poniżej znajduje się fragment informacji na temat pakietu wyświetlonych w programie Wireshark. Zaznacz urządzenie, które wysłało ten pakiet.

No.	Time	Dest MAC	Source MAC
1821		Apple_23:4f:27	Cisco_65:4e:12

Wireshark na podstawie pierwszej części adresu MAC wykrywa producenta sprzętu i wyświetla jego nazwę.



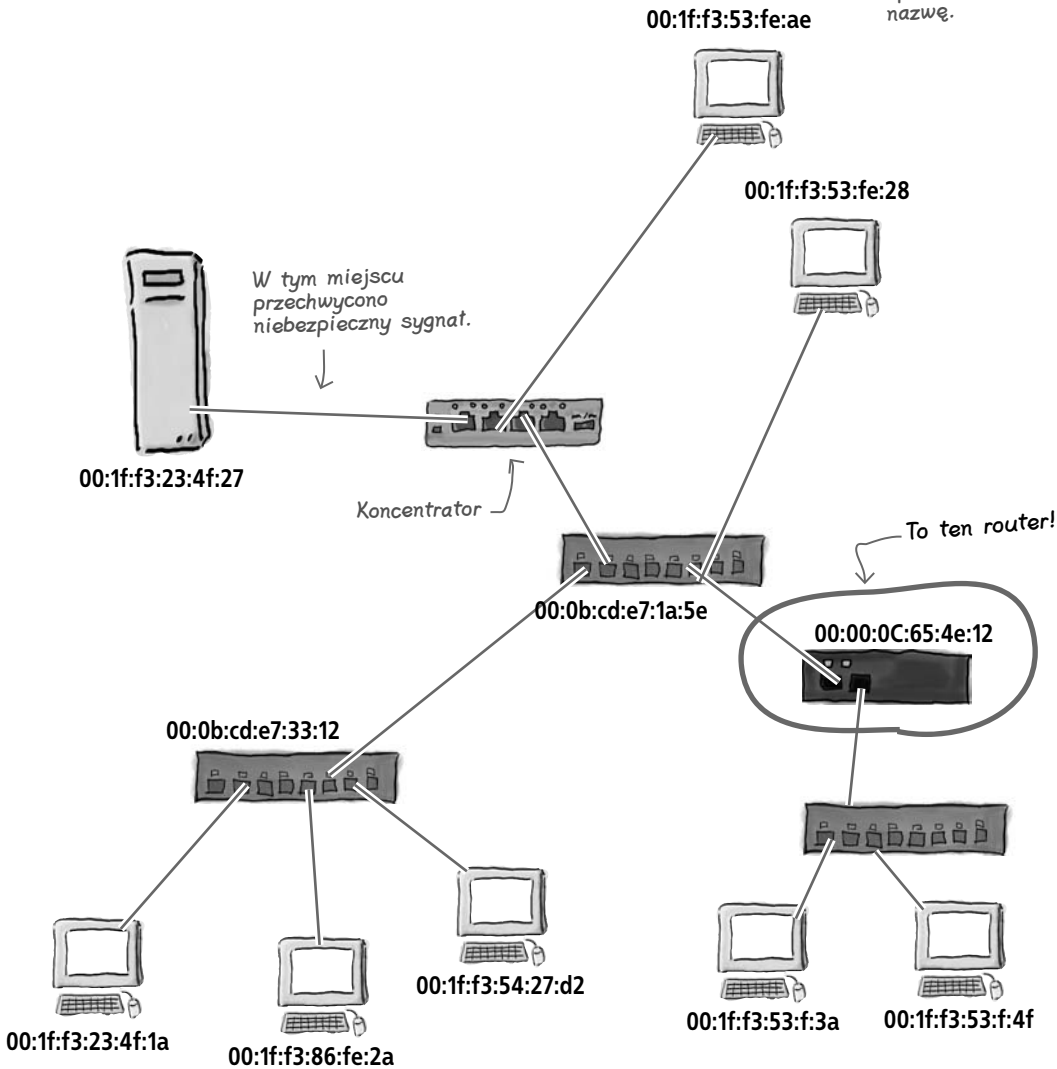


Zaostrz ołówek:
Rozwiązanie

Poniżej znajduje się fragment informacji na temat pakietu wyświetlonych w programie Wireshark. Zaznacz urządzenie, które wysłało ten pakiet.

No.	Time	Dest MAC	Source MAC
1821		Apple_23:4f:27	Cisco_65:4e:12

Wireshark na podstawie pierwszej części adresu MAC wykrywa producenta sprzętu i wyświetla jego nazwę.

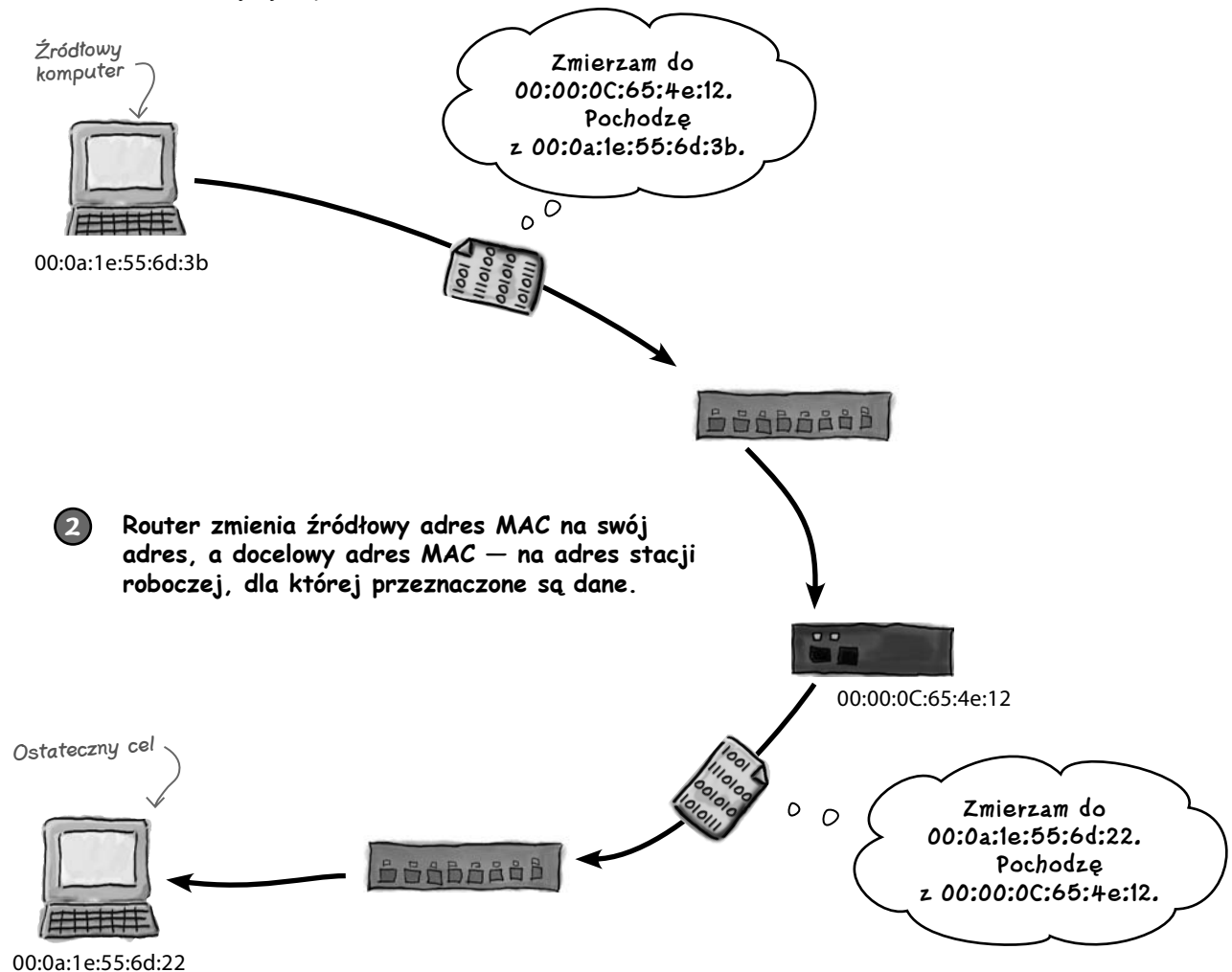


Także routery mają adresy MAC

Jeśli pakiety pochodzą z routera, widoczny będzie adres MAC tylko tego urządzenia. Wszystkie stacje robocze podłączone do routera składają się na tak zwaną podsieć IP. Przełącznik, aby przekazać ramki do docelowej lokalizacji, musi tylko sprawdzić adres MAC. Router określa adres IP na podstawie informacji z przychodzących pakietów i przekazuje dane dalej, jeśli są przeznaczone do stacji roboczej zlokalizowanej w innej sieci.

1 Źródłowa stacja robocza wysyła ramkę do routera.

Dane są przesyłane do routera, ponieważ docelowa stacja robocza znajduje się za nim.



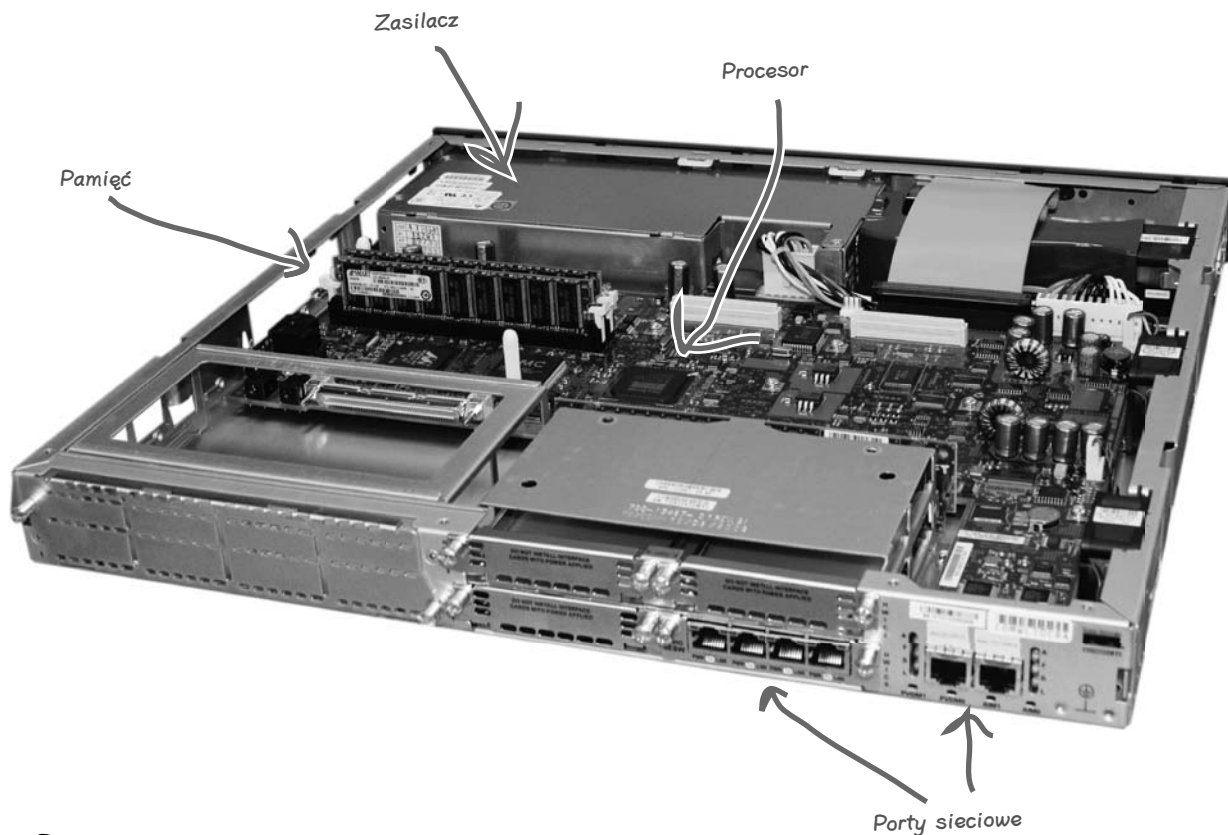
2 Router zmienia źródłowy adres MAC na swój adres, a docelowy adres MAC — na adres stacji roboczej, dla której przeznaczone są dane.



Routery pod lupą

Routery to zaawansowane urządzenia sieciowe. Służą do łączenia ze sobą poszczególnych sieci. Internet jest oparty na routerach, takich jak poniższy.

Zobacz, co znajduje się wewnątrz takiego urządzenia.



Routery są naprawdę inteligentne

Te urządzenia muszą być naprawdę inteligentne, ponieważ stosują adresy IP do przekazywania pakietów w sieci. Wykonanie tego zadania wymaga sporej mocy procesora.

Ponadto routery mają dużo mniej portów sieciowych, ponieważ zwykle są podłączone do innych routerów lub do przełączników. Komputery zazwyczaj nie są bezpośrednio podłączone do routerów.

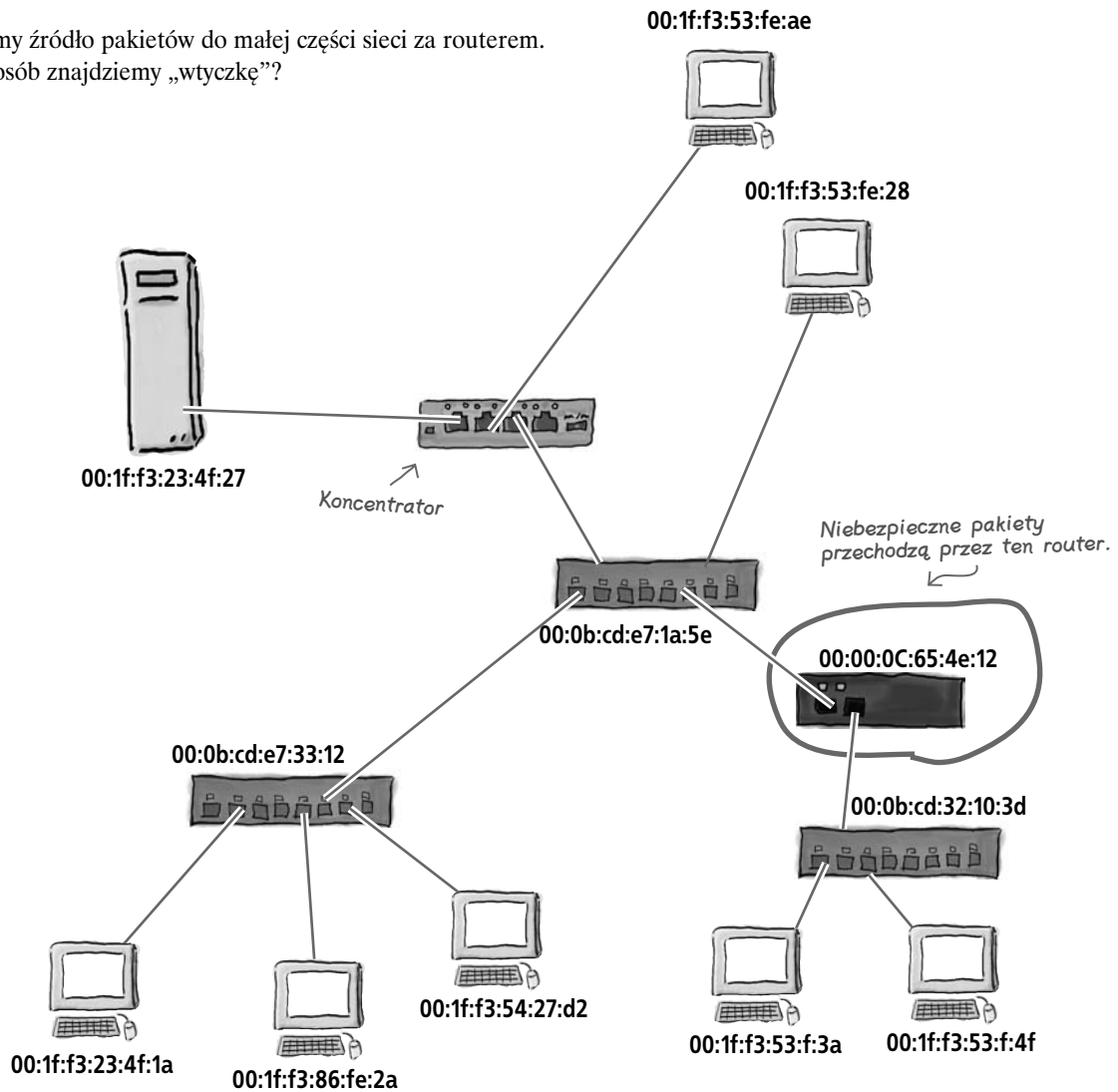


Spokojnie

Routery opisujemy szczegółowo w dwóch następnych rozdziałach.

Zbliżamy się do celu!

Zawęziliśmy źródło pakietów do małej części sieci za routerem.
W jaki sposób znajdziemy „wtyczkę”?



Ćwiczenie

Zapisz następne kroki potrzebne do znalezienia stacji roboczej, z której wysyłane są niebezpieczne pakiety.

.....

.....

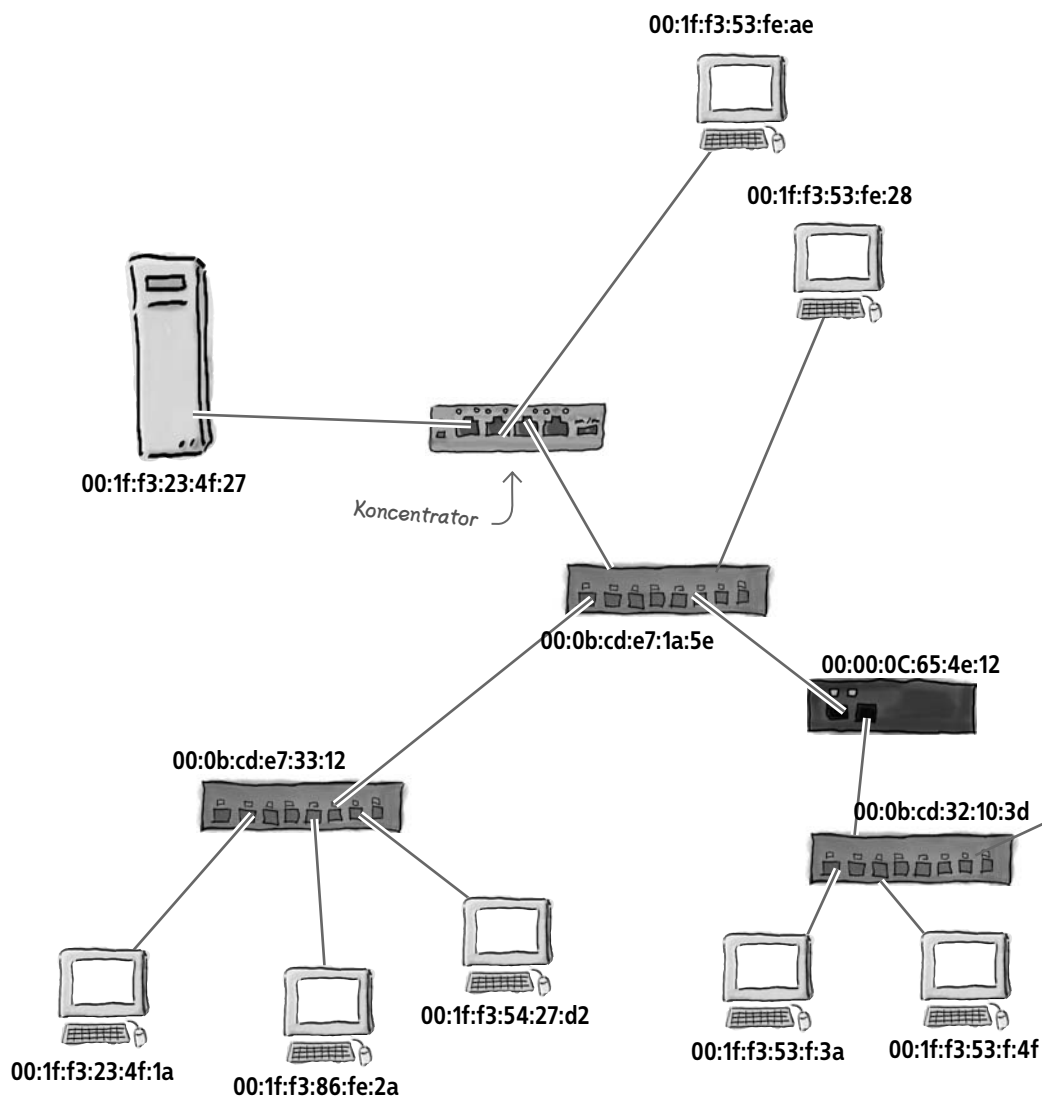
.....



Ćwiczenie: Rozwiązanie

Zapisz następne kroki potrzebne do znalezienia stacji roboczej, z której wysyłane są niebezpieczne pakiety.

Należy podłączyć się do przełącznika za routerem i znaleźć niebezpieczny adres MAC w tablicy. W ten sposób znajdziemy port, do którego podłączona jest niebezpieczna maszyna, co doprowadzi nas do „wtyczki”.



Znalazłeś „wtyczkę”!

Dzięki wiedzy na temat sieci znalazłeś „wtyczkę”. Szpieg podłącza laptop do przełącznika za routerem. Dobra robota!



