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

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
- Diagnozowanie 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 (skrócony)

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* przechytrzyć mózg i przekonać go, że Twoje życie zależy od umiejętności obsługi sieci?

Naprawianie fizycznych uszkodzeń sieci

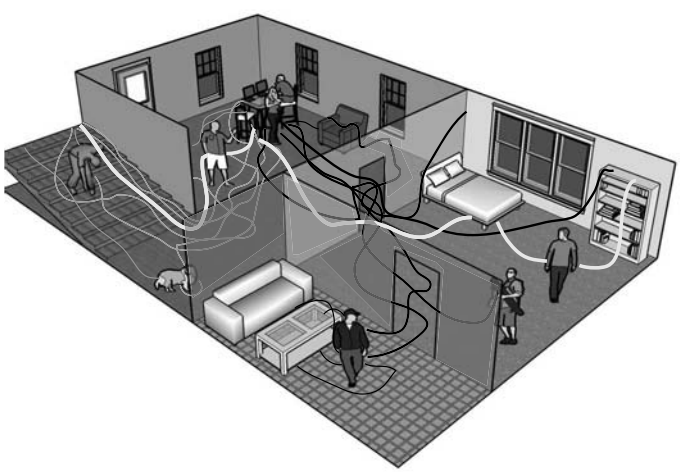
1 Spacer po przewodach

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.

Planowanie układu sieci

2 Z sieciami w ciemnościach

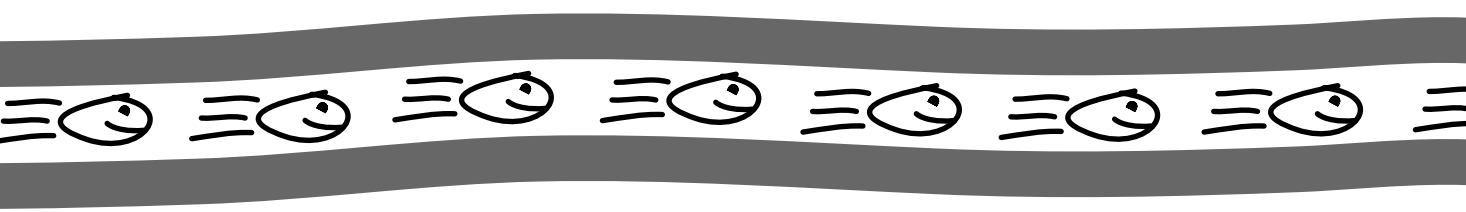
Masz dość potykania się o przewody i ataków ze strony skrzynki elektrycznej? Jeśli zbudujesz sieć bez planu, powstanie bałagan — kable będą biegły we wszystkie strony i nie będziesz wiedział, do czego są podłączone. W tym rozdziale nauczysz się planować fizyczny układ sieci, co pozwoli Ci uniknąć późniejszych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



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 przyjrzeć się samym sygnałom. W tym rozdziale dowiesz się, jak używać takich urządzeń do rozwiązywania problemów z sieciami i jak interpretować sekretny język sygnałów.

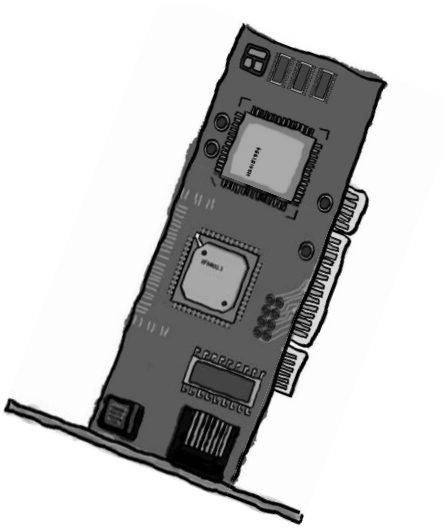


Analizowanie pakietów

4

Na tropie ramek

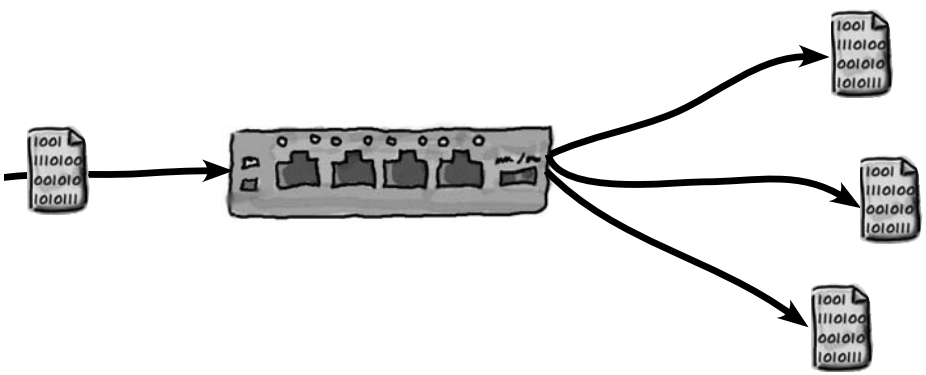
Czas zajrzeć pod maskę. Urządzenia sieciowe przesyłają informacje kablami, przekształcając dane na sygnały. Jak jednak to robią? Co oprócz informacji może ukrywać się w sygnale? Podobnie jak lekarz musi zbadać krew, aby wykryć choroby krwi, tak specjalista od sieci musi zobaczyć, co zawiera sygnał, żeby 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.



Urządzenia i ruch w sieci

5 Jak inteligentna jest Twoja sieć?

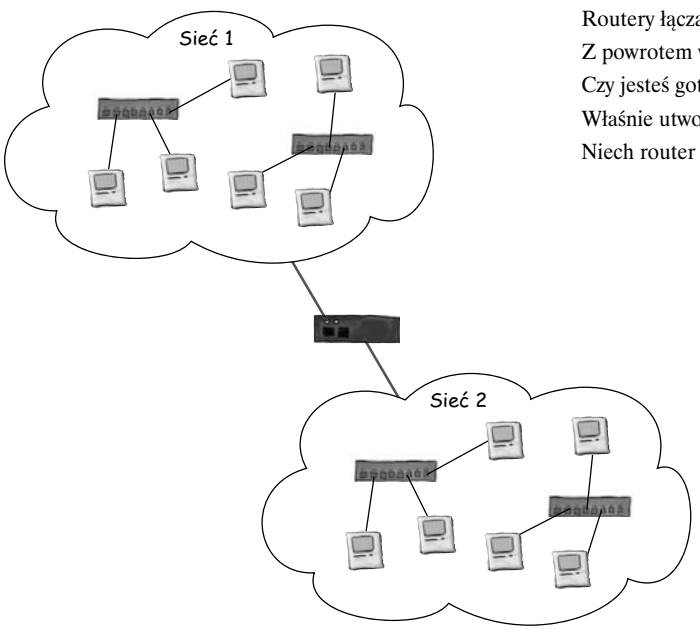
Sieć zawsze może być bardziej inteligentna. W sieć należy wbudować jak najwięcej inteligencji, jednak **z czego ona wynika**? Najważniejsze są urządzenia sieciowe. W tym rozdziale pokażemy, jak **koncentratory, przełączniki i routery** wykorzystują swoją naturalną **inteligencję** do przesyłania pakietów 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**.



Łączenie sieci za pomocą routerów

6 Łączenie różnych elementów

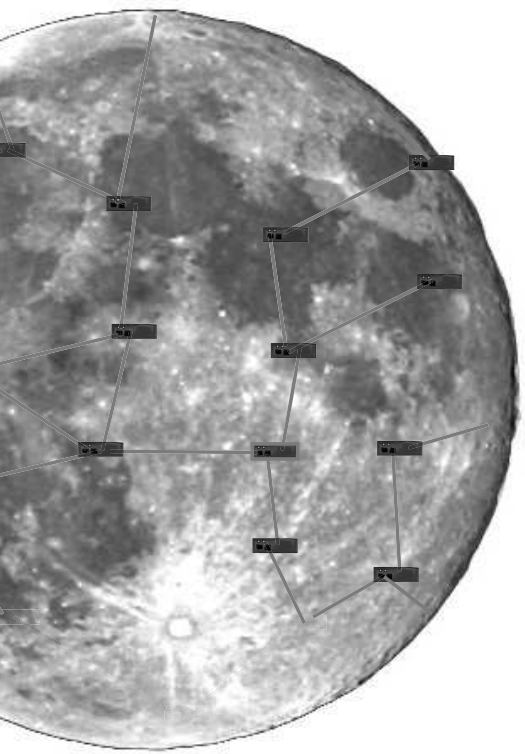
Chcesz nawiązać połączenie sieciowe z bardzo odległym miejscem? Na razie pokazaliśmy, jak skonfigurować pojedynczą sieć. Co jednak zrobisz, kiedy zechcesz **udostępnić zasoby w innej sieci**? Potrzebne będą do tego routery. Te urządzenia służą do płynnego **przekazywania pakietów między sieciami**, a 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.



Protokoły trasowania

7 Protokół tego wymaga

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



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.

Monitorowanie sieci i rozwiązywanie problemów

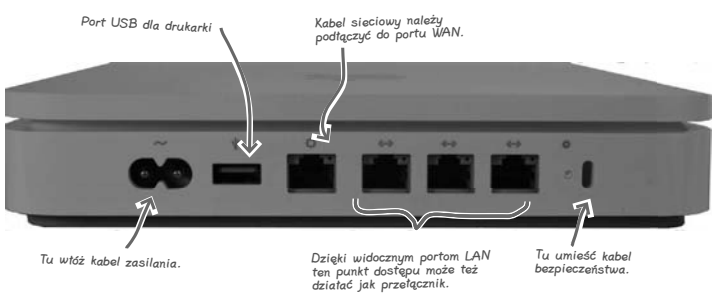
9 Nasłuchuj, czy w sieci nie ma problemów

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.

Sieci bezprzewodowe

10 Praca bez kabli

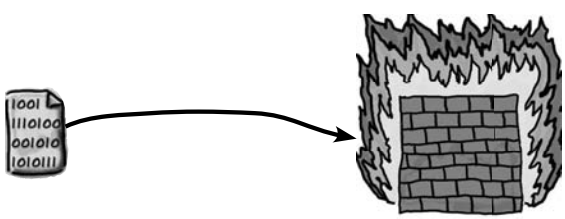
Bezprzewodowe surfowanie po Internecie jest wspaniałe! W tym rozdziale opisujemy wszystko, co powinieneś wiedzieć przy konfigurowaniu bezprzewodowego punktu dostępu. Najpierw musisz przemyśleć jego fizyczną lokalizację, ponieważ sygnał sieci radiowych może zostać zablokowany. Omawiamy też kilka nowych 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.



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 wyłudzają hasła od Twoich współpracowników. Broń się! Nie pozwól na to, aby dane wydostały się poza sieć lub by włamali się do niej intruzi.



Projektowanie sieci

12

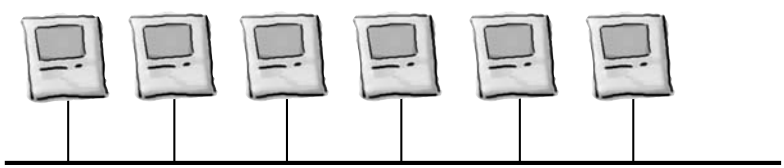
Musisz mieć plan!

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!

Pozostałości

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.



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.

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.

S

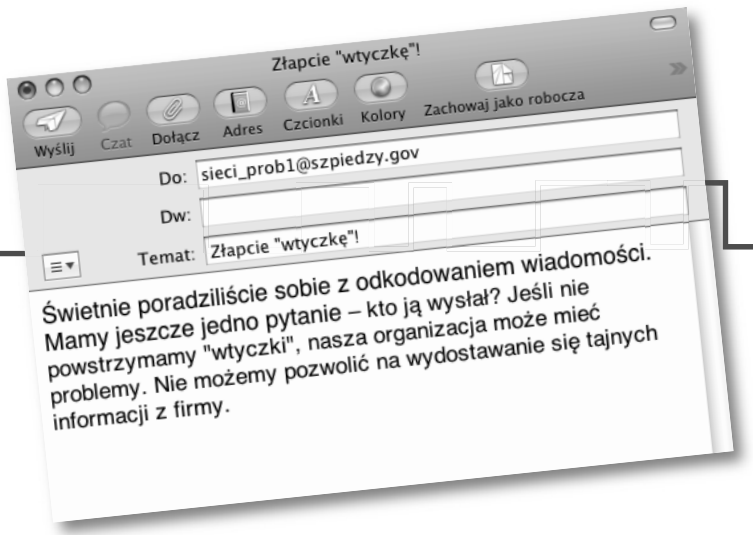
Skorowidz

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...

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: .....

.....

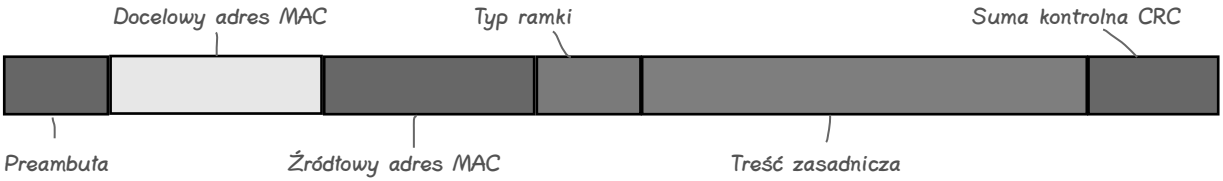
.....

.....

.....

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 wysłano komunikat. Pomoże to ustalić komputer, z którego korzysta „wtyczka".*

Docelowy adres MAC określa, gdzie dane zostaną przesłane.

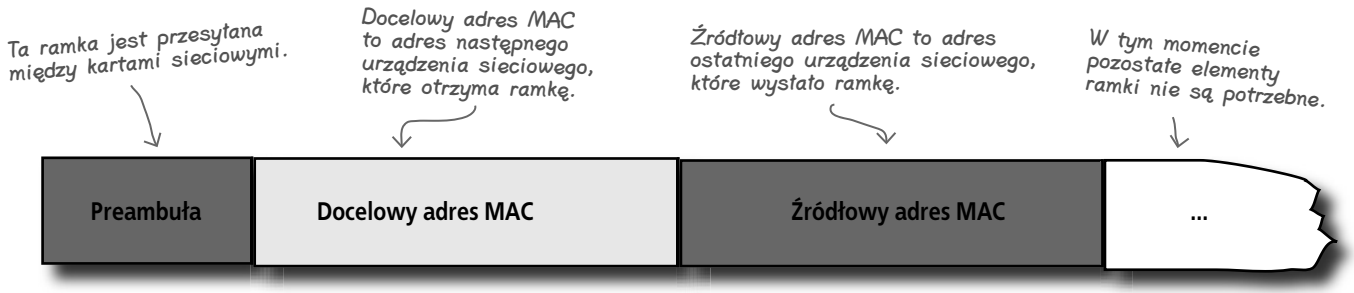
Dane w pakiecie informują o jego pochodzeniu

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

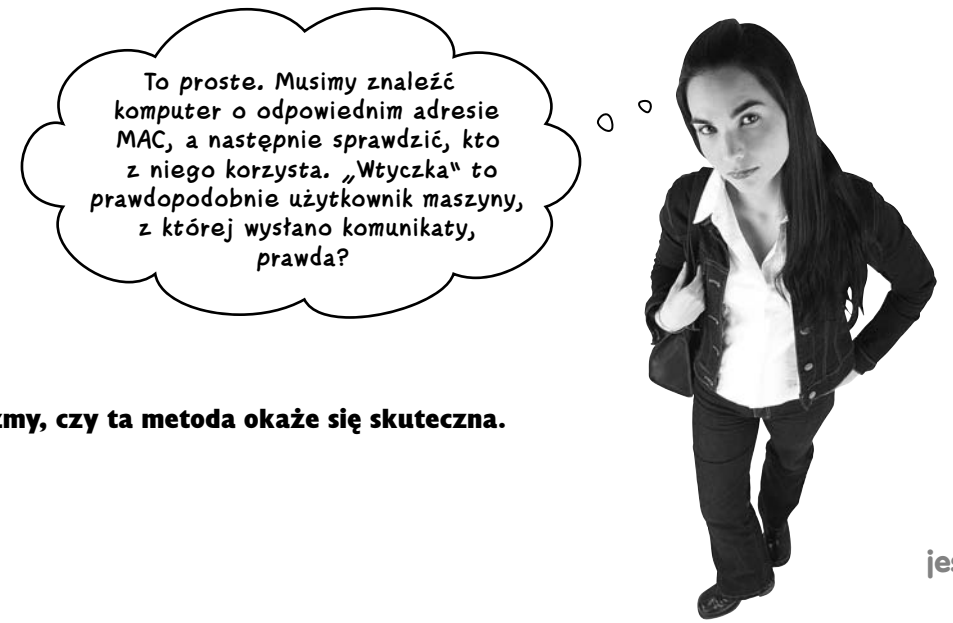
Adres MAC jest zapisany na karcie sieciowej zainstalowanej w komputerze. Takie adresy mają sześć bajtów długości (48 bitów). Zwykle są zapisane w systemie szesnastkowym, a poszczególne bajty są rozdzielone dwukropkami lub myślnikami, na przykład 0f:2b:5d:e7:a3:eb.

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”?



Zobaczmy, czy ta metoda okaże się skuteczna.

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.

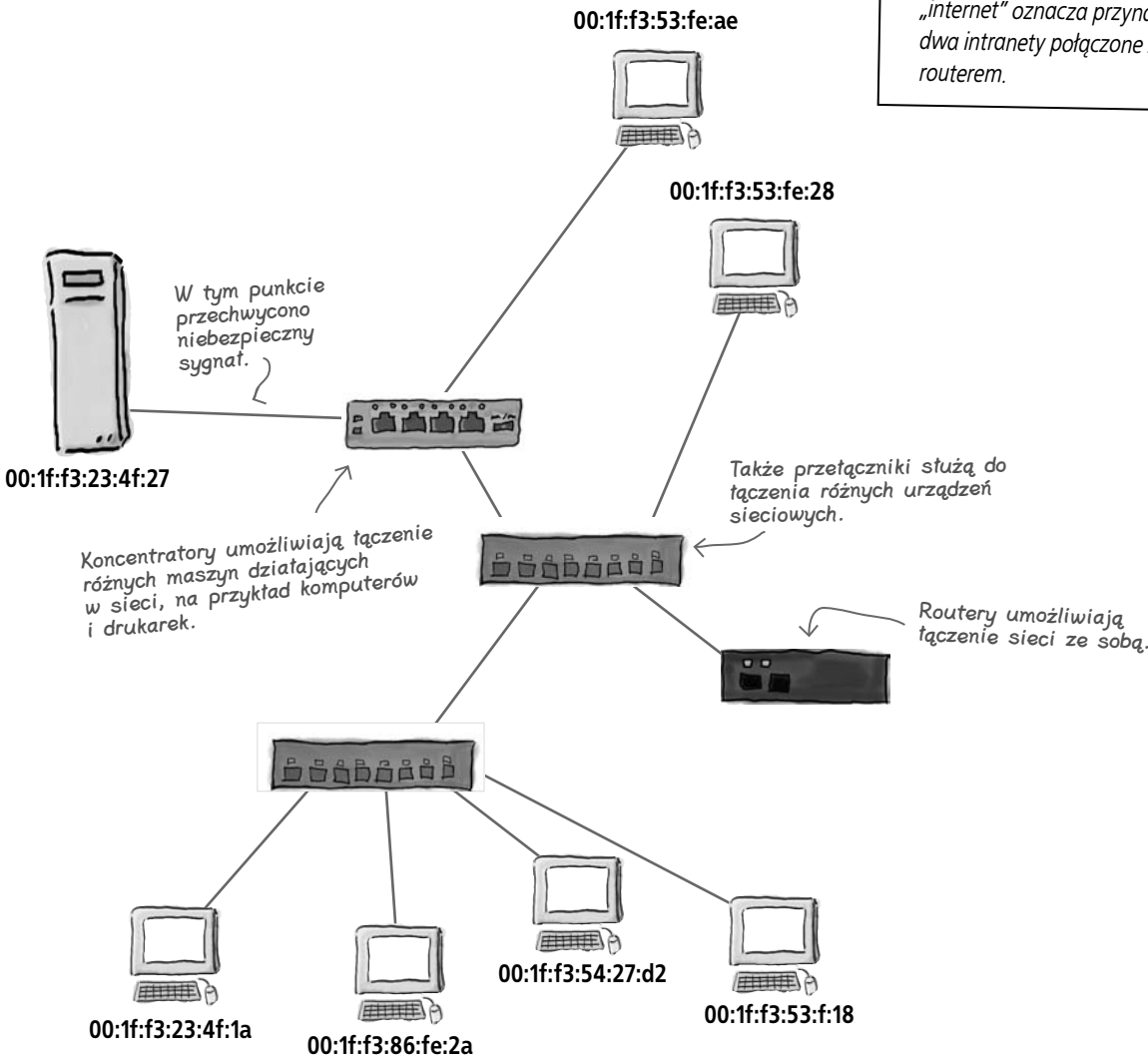
Sieć to nie tylko komputery

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.

Uwaga!

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

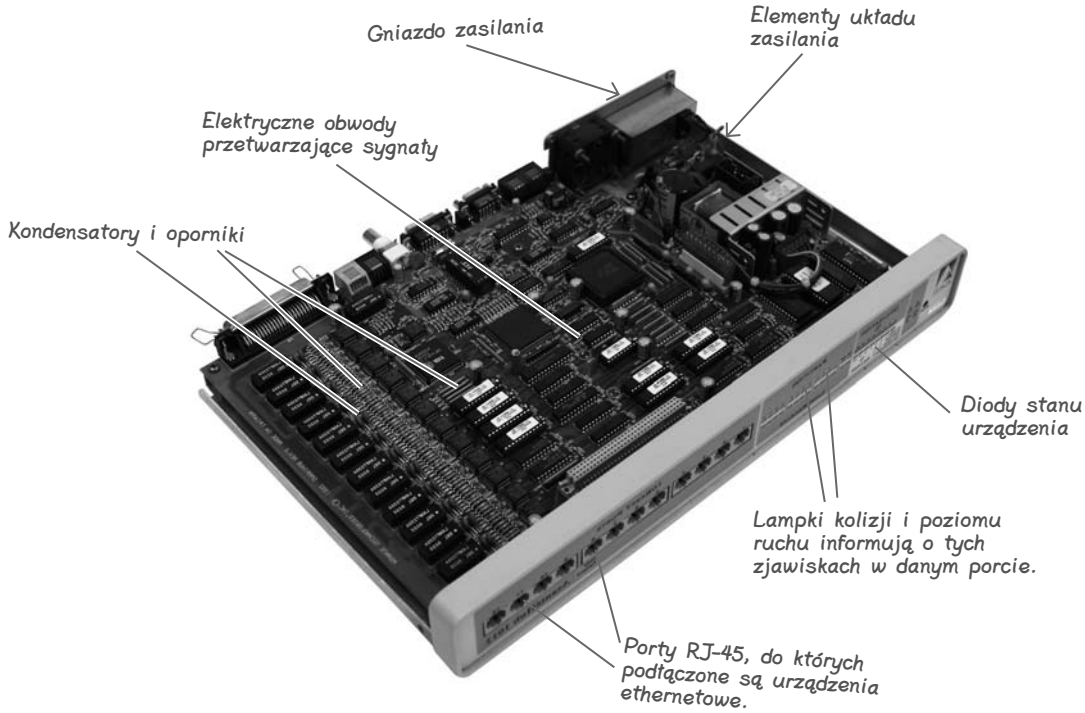
Słowo „Internet" określa dużą przestrzeń pełną powiązań, umożliwiającą przesyłanie danych po całym świecie. Pojęcie „internet" oznacza przynajmniej dwa intranety połączone ze sobą routerem.



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

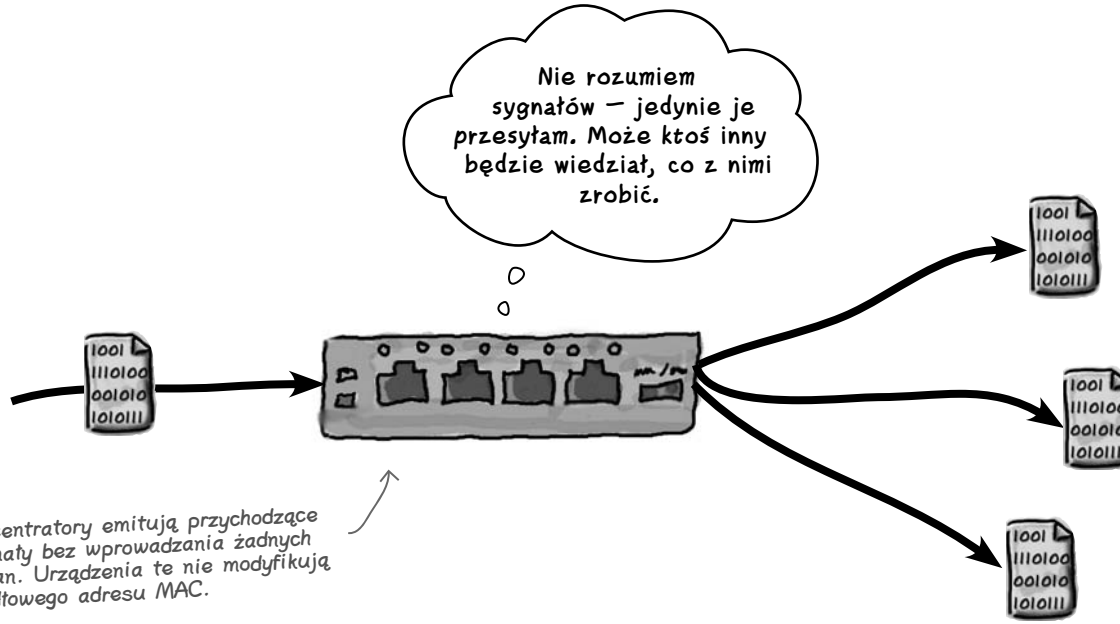
W jaki sposób ma to pomóc w wyśledzeniu źródła niebezpiecznego sygnału?

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?

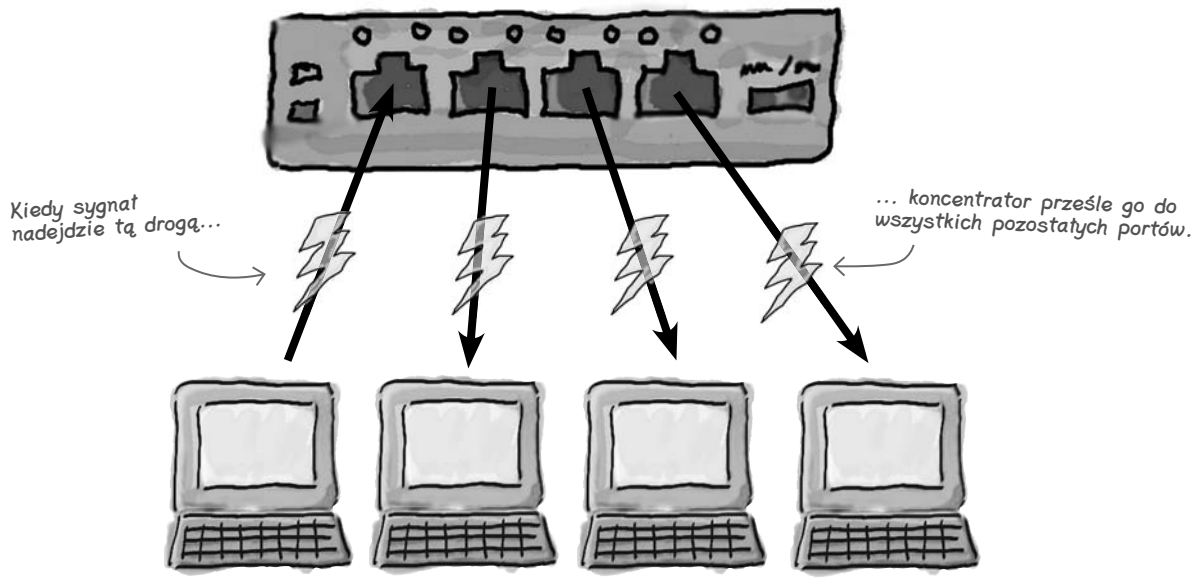
Ponieważ koncentrator nie modyfikuje źródłowego adresu MAC, adres ten musi należeć do urządzenia, które przekazało sygnał do koncentratora. Trzeba spojrzeć poza koncentrator, aby wykryć „wtyczkę”.

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

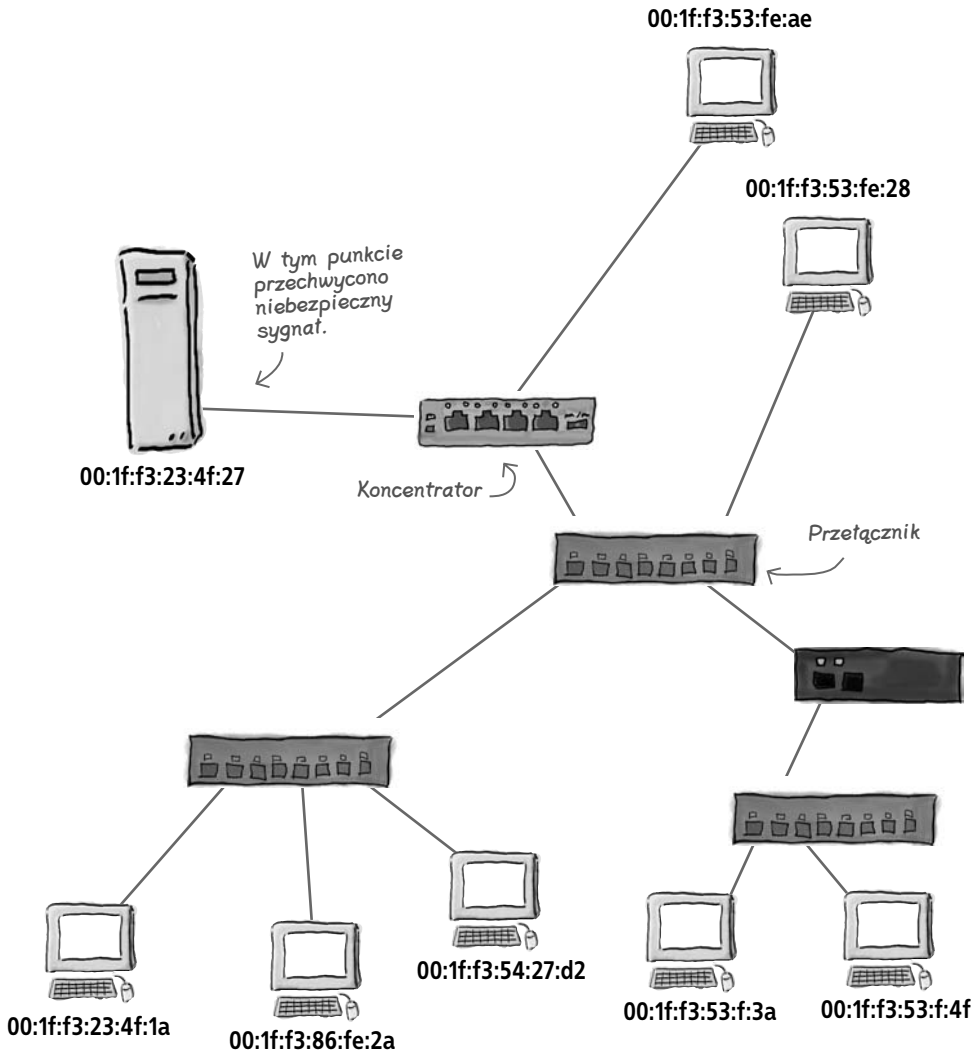
Koncentratory nie mają procesorów, co oznacza, że nie rozumieją danych sieciowych, na przykład adresów MAC lub ramek. Traktują przychodzący sygnał sieciowy jako zjawisko czysto elektryczne i przekazują go.

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.

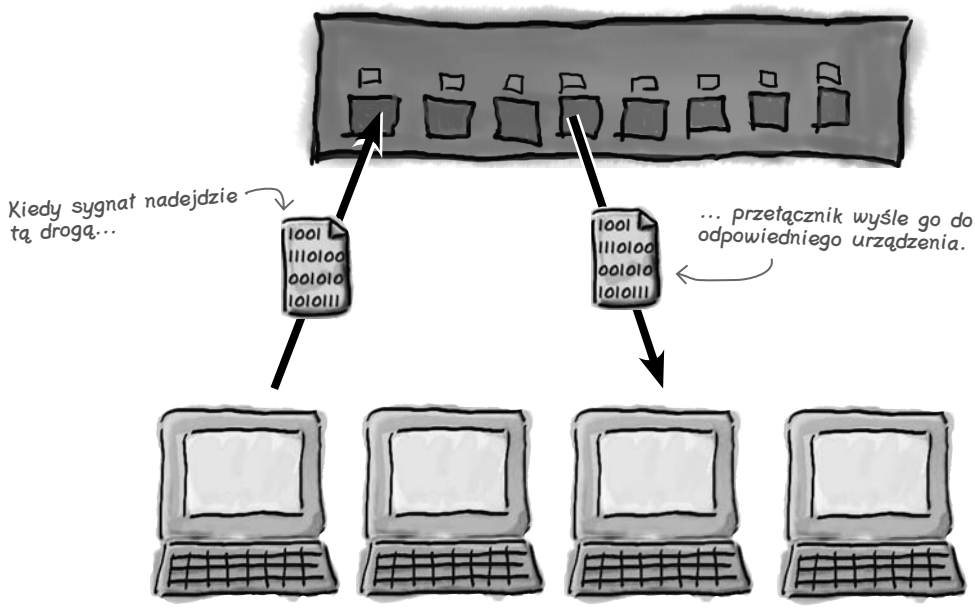


Do koncentratora podłączone są dwa urządzenia, które mogą być źródłem sygnału — komputer i przełącznik. Ponieważ adres MAC komputera nie pasuje do szukanego adresu, wiadomo, że to nie z tej maszyny wysłano dane. Oznacza to, że źródłem sygnału jest przełącznik.

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

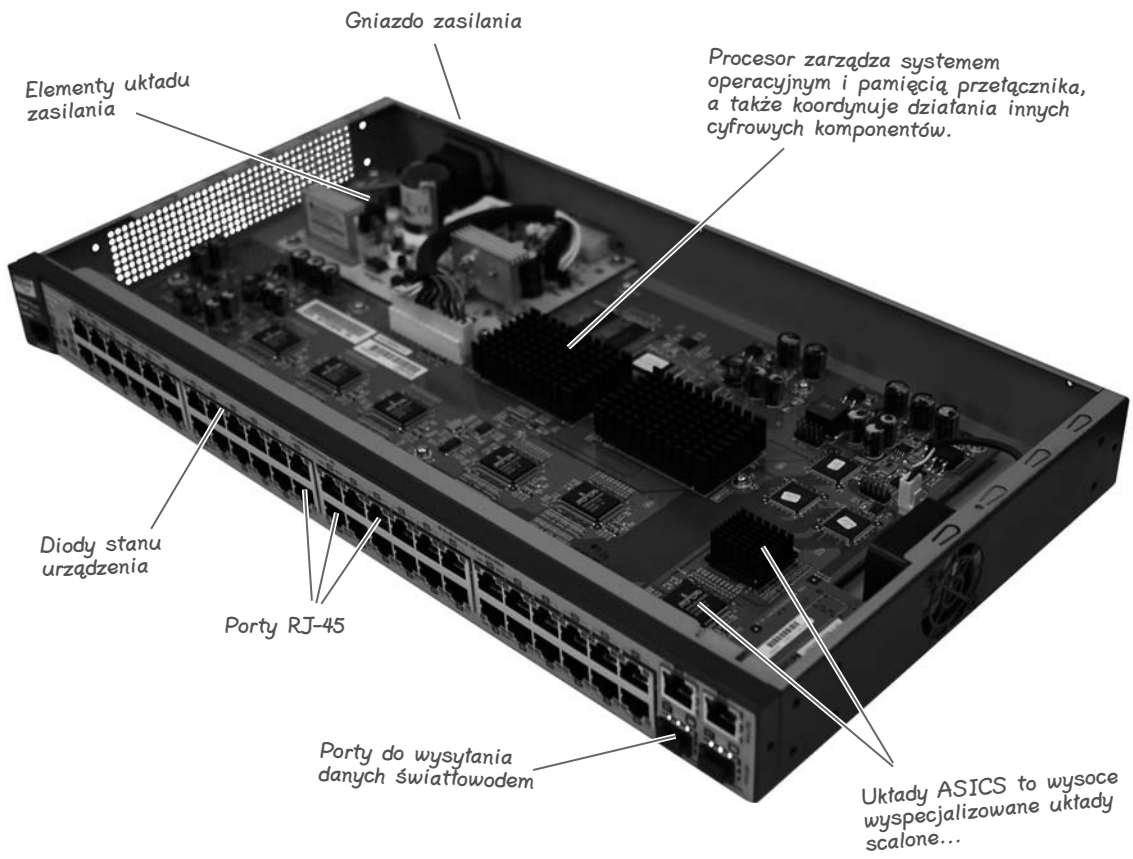
Przełączniki zawierają procesory, pamięć RAM i układy ASICS, co powoduje, że mogą przetwarzać dane sieciowe. Te urządzenia rozumieją adresy MAC i ramki, dlatego w inteligentny sposób obsługują przychodzące sygnały sieciowe. Przełączniki potrafią określić docelową lokalizację sygnału i dostosować do tego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

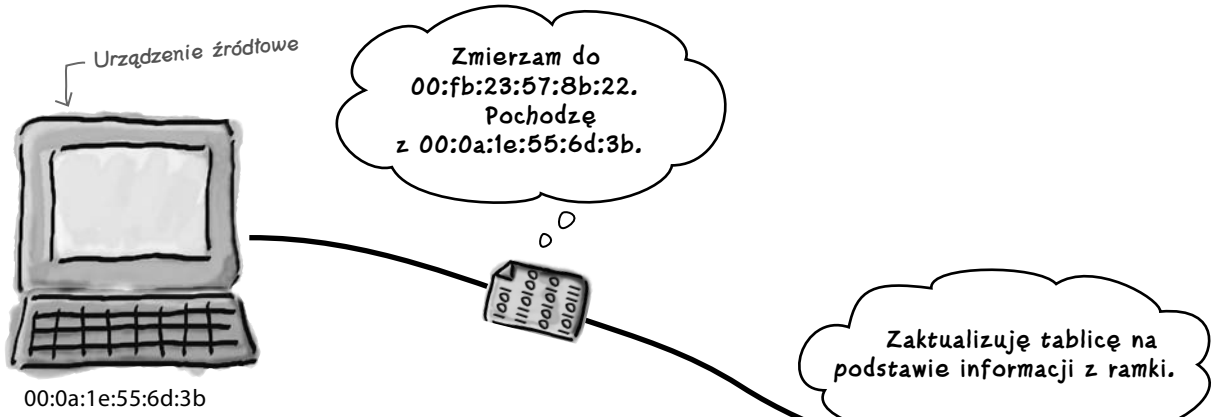
Obsługiwanie sygnału przez koncentratory i przełączniki przebiega zupełnie inaczej. Przełącznik potrafi przetwarzać sygnały jako ramki i rozpoznaje adresy MAC. Zamiast przesyłać przychodzące sygnały do wszystkich portów, przełącznik może zapisać pakiety i przekazać je do docelowych urządzeń.

Przyjrzyjmy się bliżej działaniu przełączników.

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

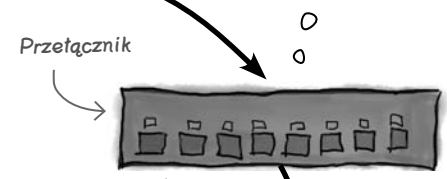
1 Źródłowa stacja robocza wysyła ramkę.

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.



Port to miejsce połączenia węzła sieciowego z przełącznikiem.

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

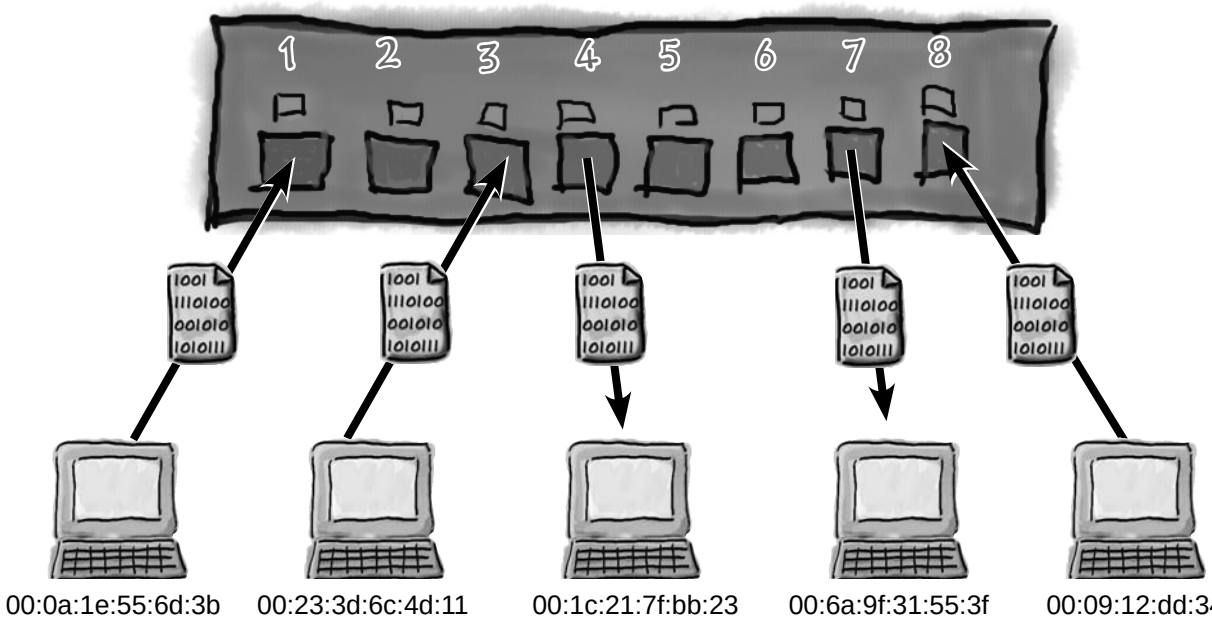
Przełącznik używa tablicy do śledzenia informacji z ramek.

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

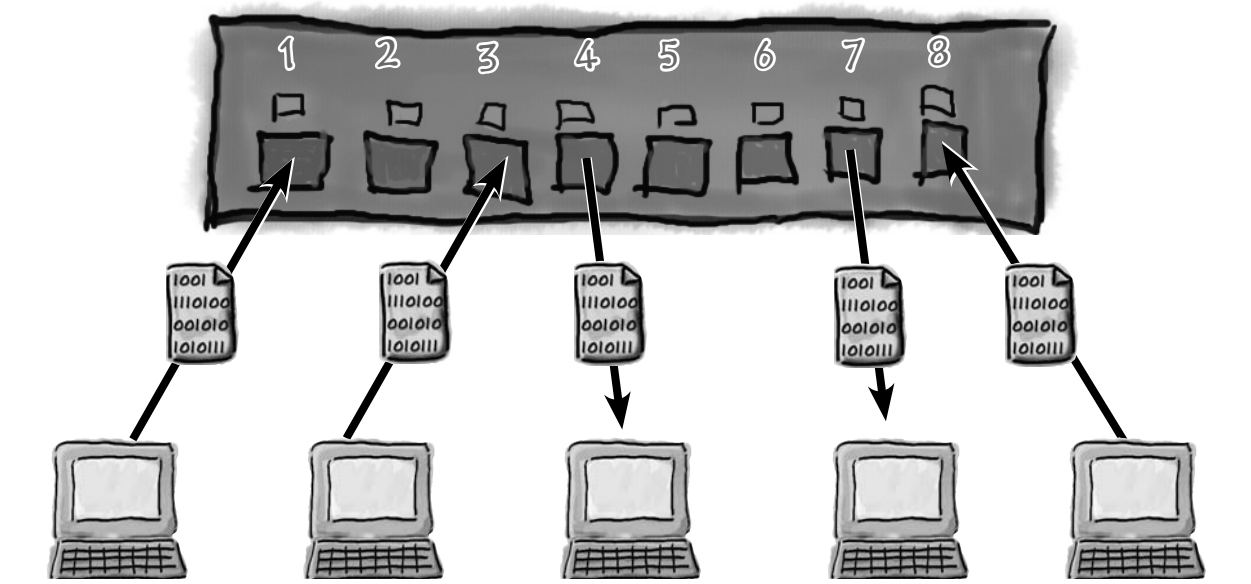
Wciel się w rolę przełącznika i zaktualizuj tablicę na podstawie dostępnych informacji z ramek. Strzałki pomogą Ci powiązać adresy MAC z portami. Pierwszy wiersz uzupełniliśmy za Ciebie.



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

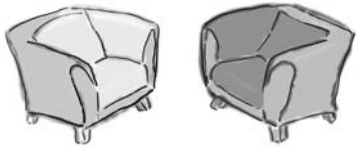
ZOSTAŃ przełącznikiem. Rozwiązanie

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:

Słuchaj, 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: Sądzisz 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?

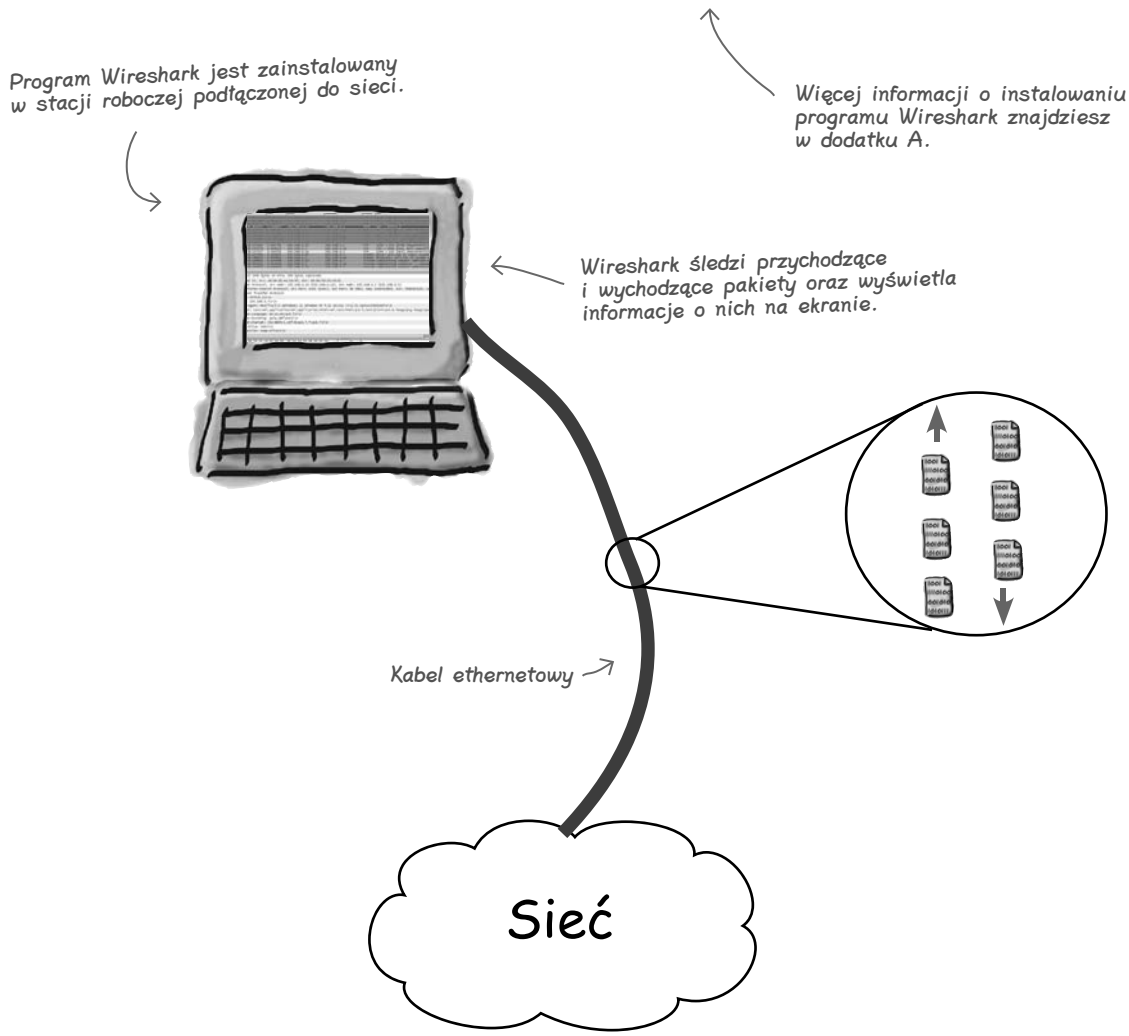
Kuba: Uważam, że musimy zacząć przechwytywać dane i poszukać tych z odpowiednim źródłowym adresem MAC. Następnie możemy wrócić do przełącznika i znaleźć ten adres, aby zawęzić poszukiwania do określonego portu.

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.



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

Podłącz program Wireshark do przełącznika

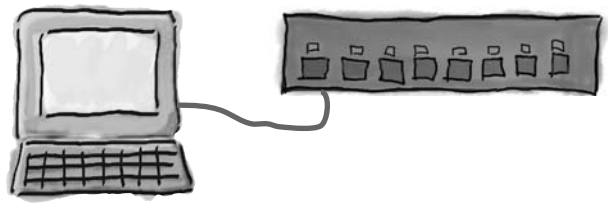
Jak można wykorzystać program Wireshark do monitorowania danych przechodzących przez przełącznik? Wystarczy zastosować się do poniższych instrukcji.

1. **Podłącz komputer do przełącznika kablem szeregowym.**
   Wykorzystasz ten kabel do komunikowania się z przełącznikiem.

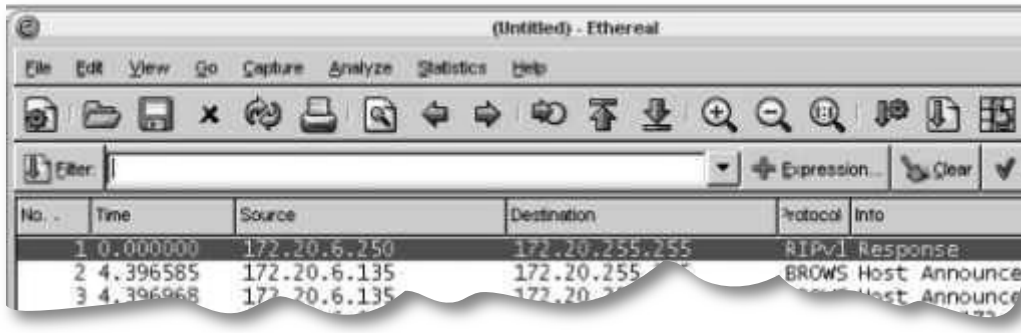
2. **Otwórz terminal (na przykład Hyperterminal) i uruchom wiersz polecenia przełącznika. Wpisz poniższe instrukcje.**

```
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 przechwyć dane sieciowe.**

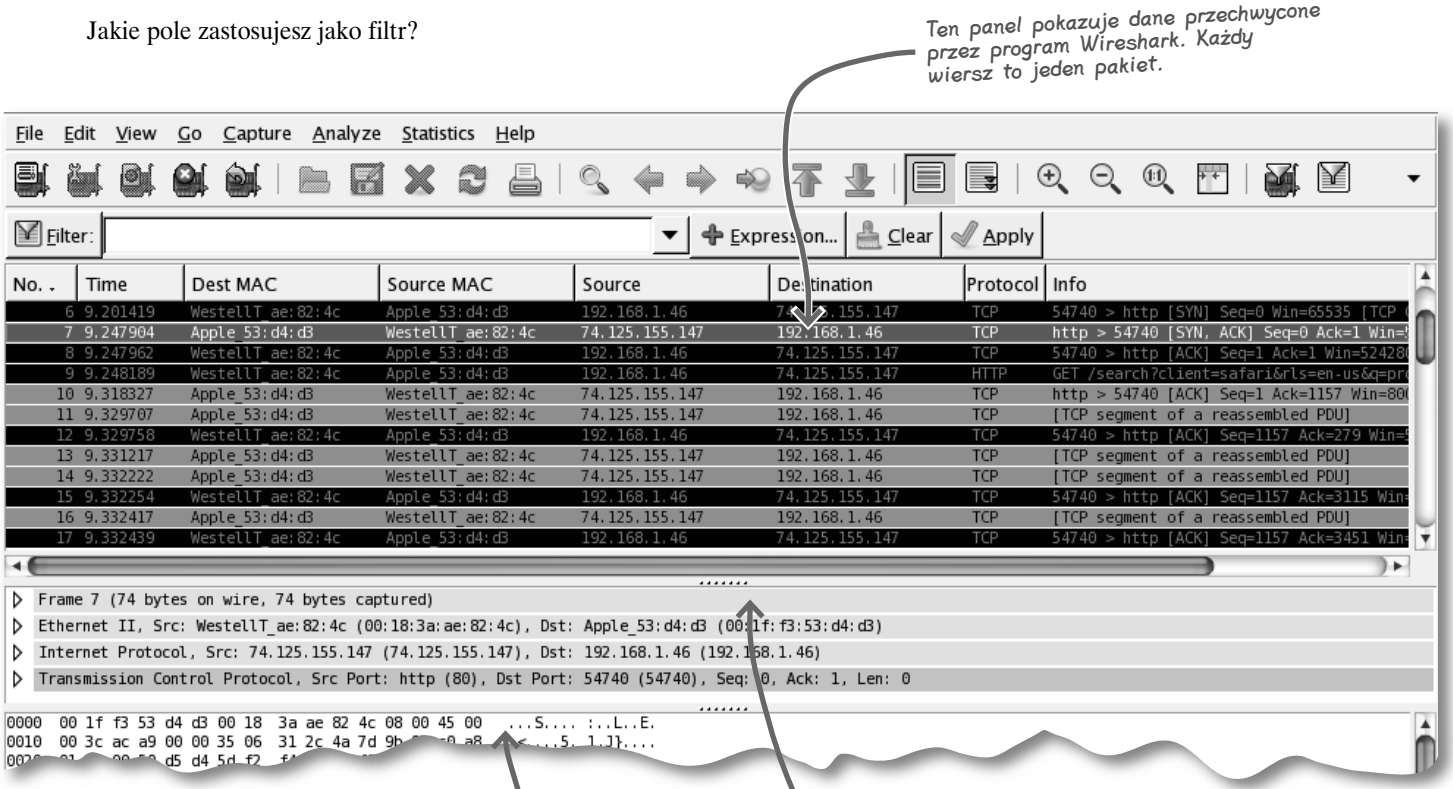


Jakie informacje udostępnia program Wireshark?

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?



Ciekawostki

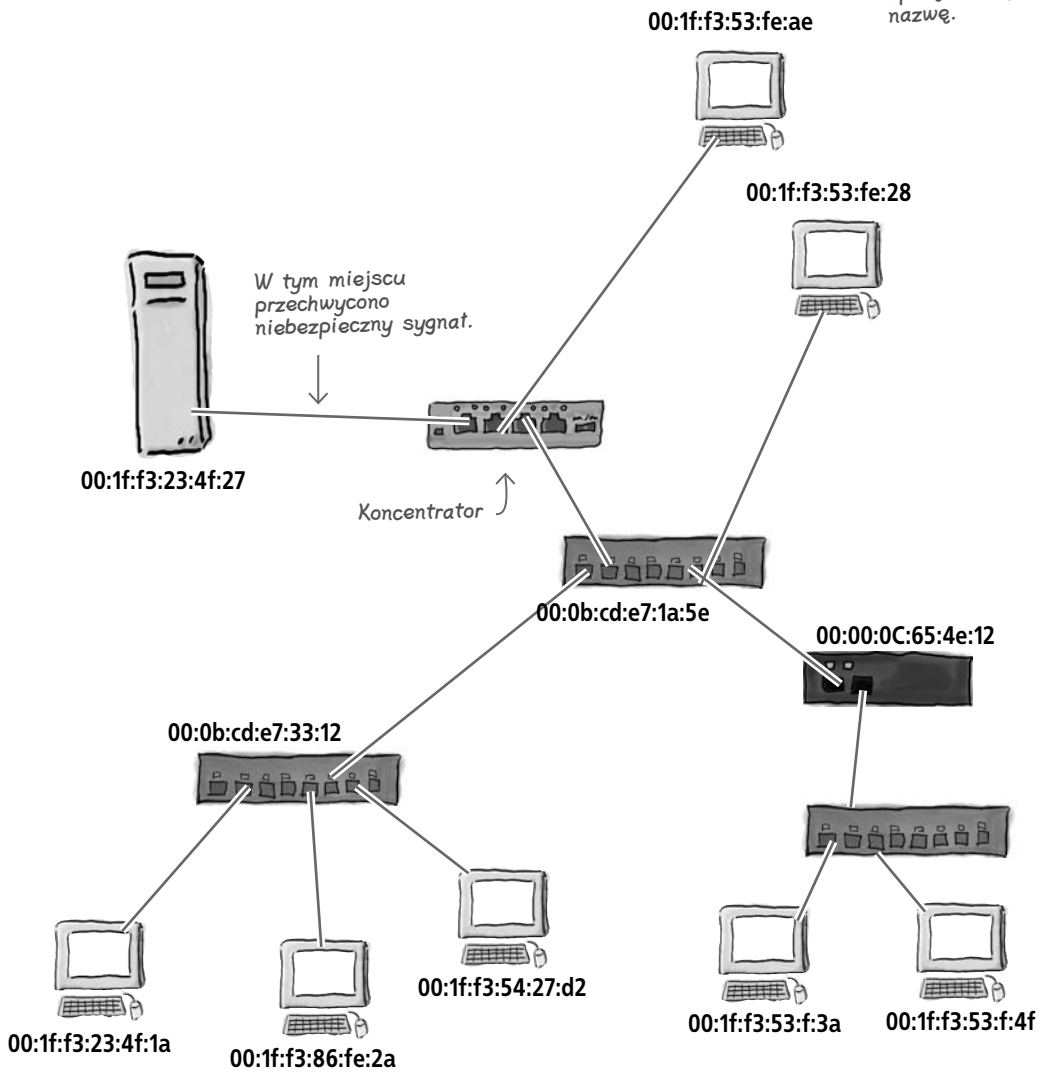
Oficjalnie Wireshark jest „analizatorem protokołów".

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

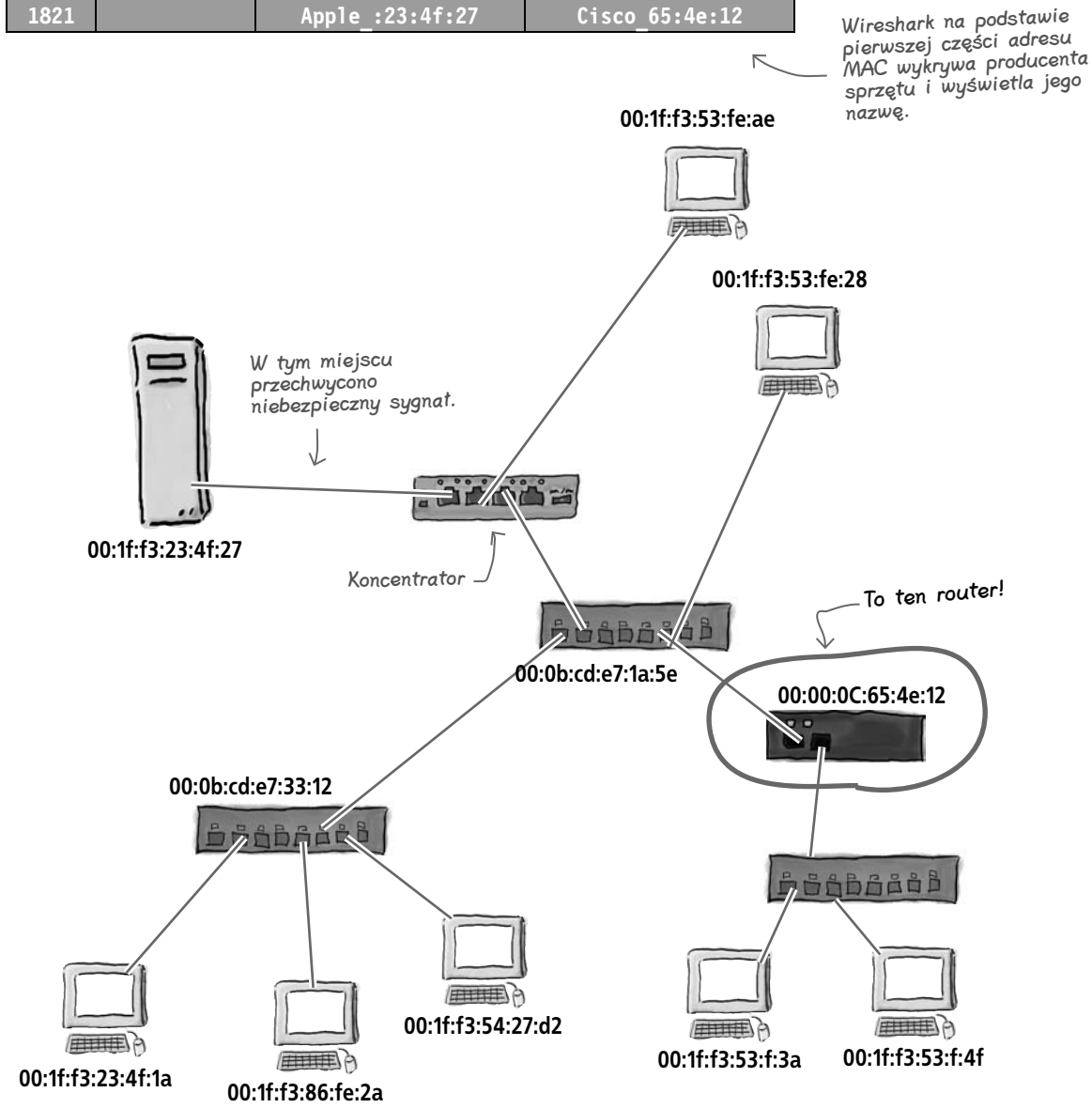
Wireshark na podstawie pierwszej części adresu MAC wykrywa producenta sprzętu i wyświetla jego nazwę.



Zaostrz ołówek: Rozwiązanie

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

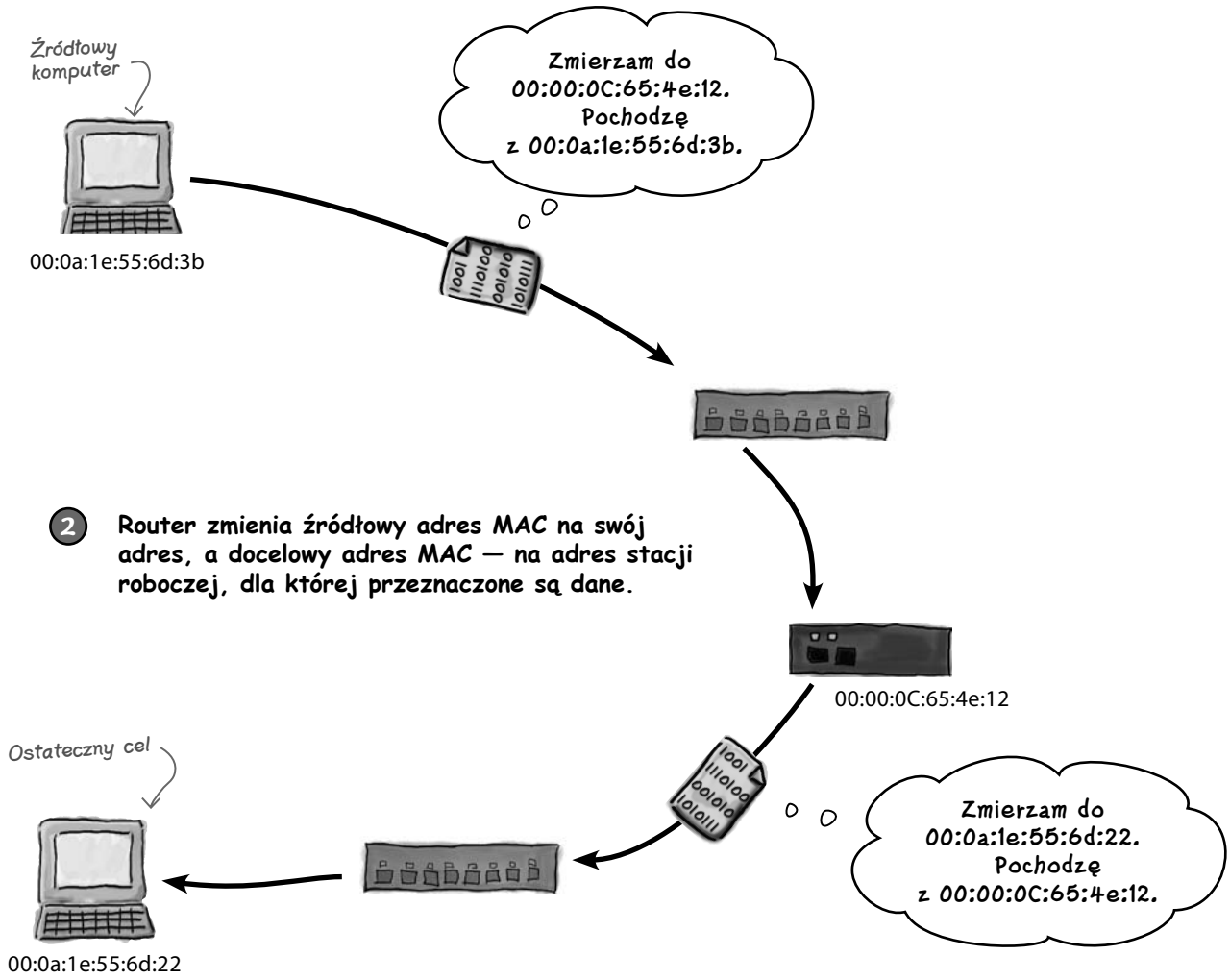
No.	Time	Dest MAC	Source MAC
1821		Apple_:23:4f:27	Cisco_65:4e:12



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.

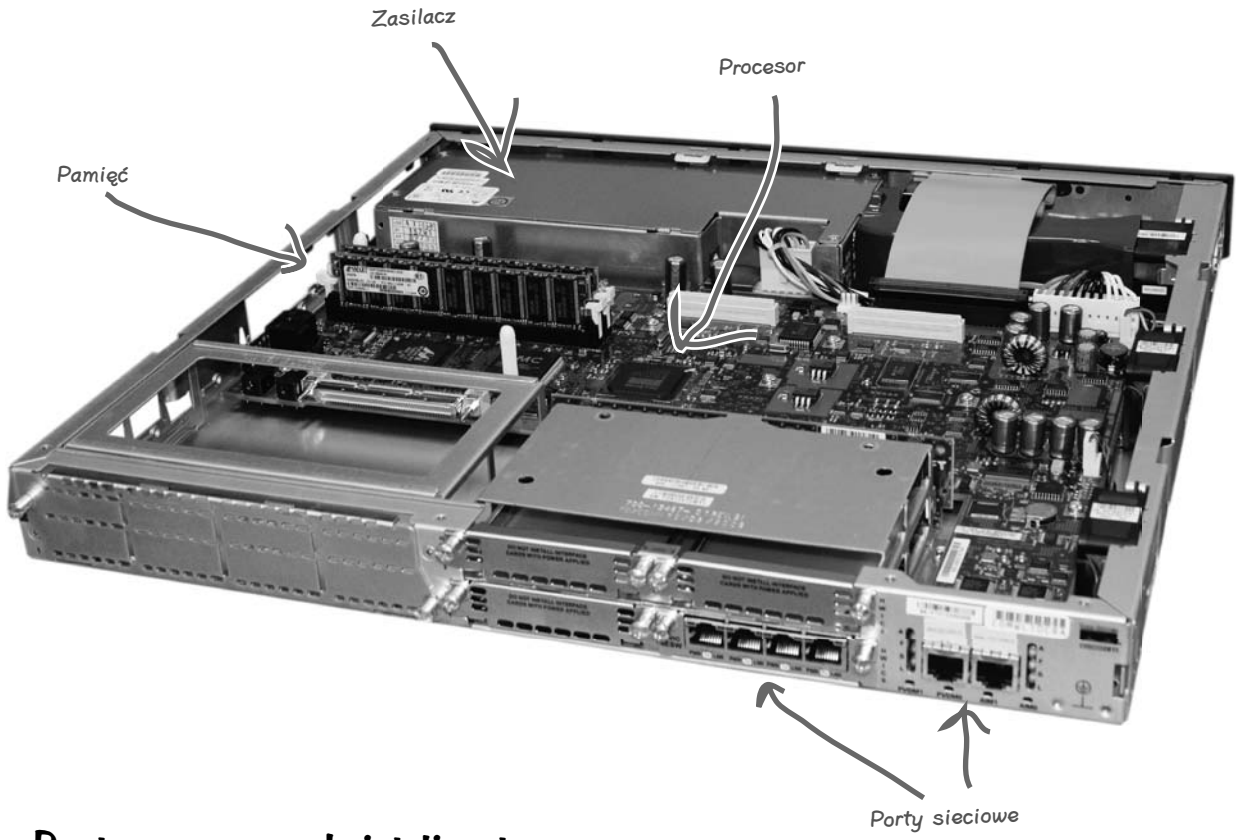


2 **Router zmienia źródłowy adres MAC na swój adres, a docelowy adres MAC — na adres stacji roboczej, dla której przeznaczone są dane.**

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

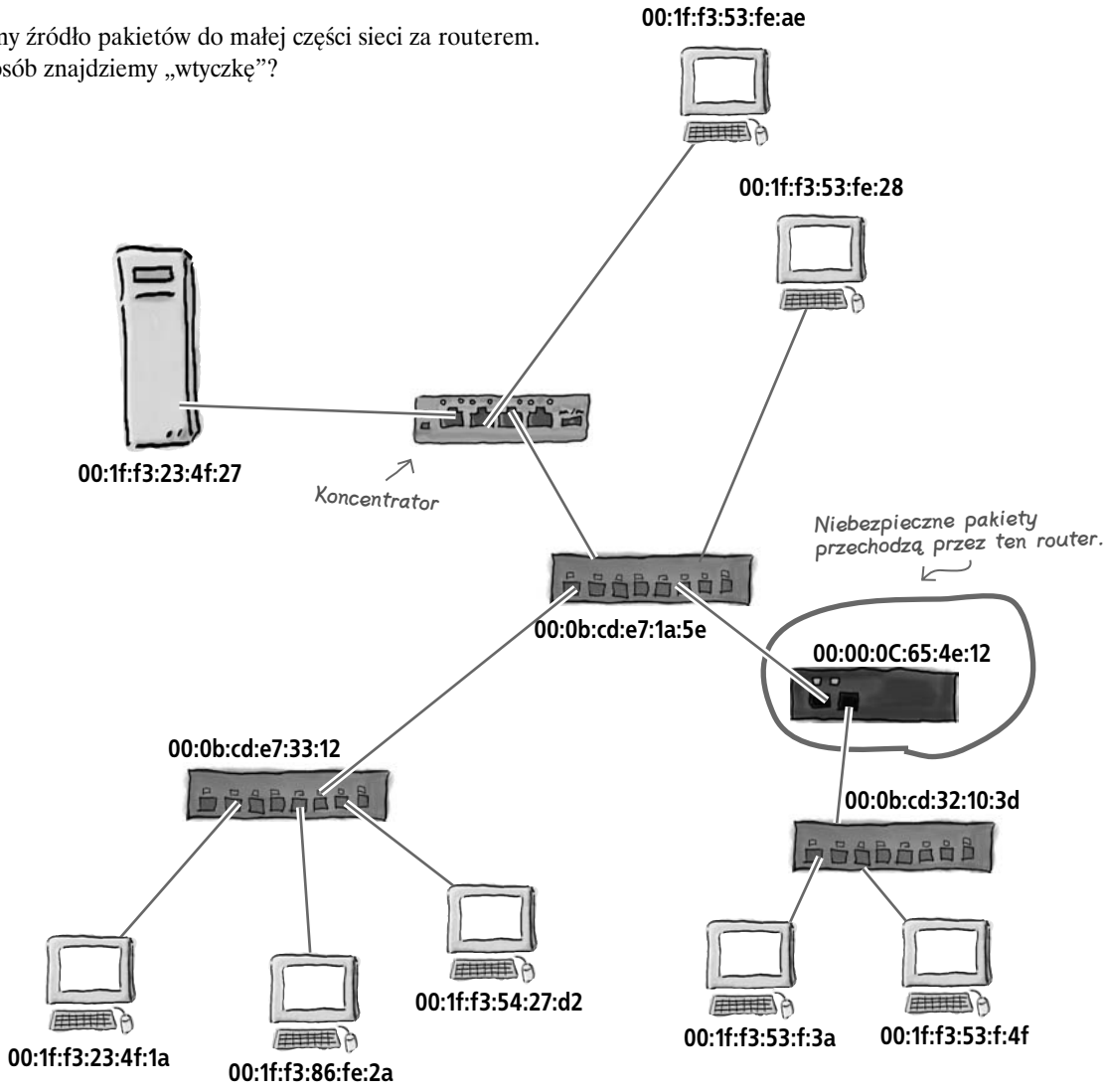
Te urządzenia muszą być naprawdę inteligentne, ponieważ stosują adresy IP do przekazywania pakietów w sieci. Wykonanie tego zadania wymaga sporej mocy procesora.

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

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.

.....

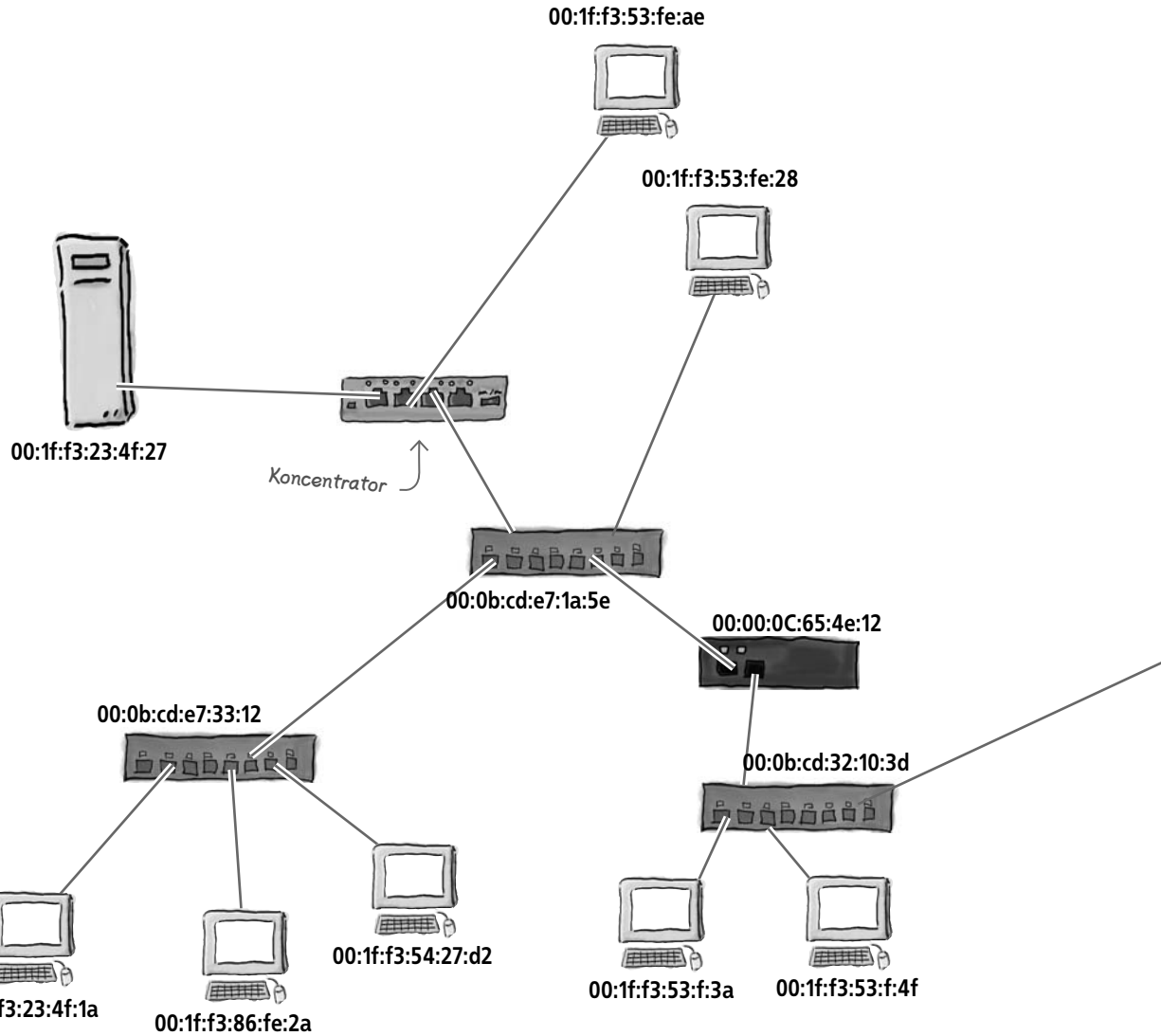
.....

.....

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!