Marek Kopczyk, Paweł Kowalik

Zespół Szkół im. ks. S. Staszica w Tarnobrzegu

SERWER DHCP, IP STATYCZNE I DYNAMICZNE, BRAMA DOSTĘPOWA, MONITOROWANIE SIECI

Streszczenie

Dokument przedstawia podstawowe zagadnienia z zakresu działania i pracy w sieci lokalnej. W pierwszej sekcji zostanie omówiony protokół DHCP – do czego służy oraz jak porozumiewają się przez ten protokół serwer i klient w sieci. Wyjaśniona zostanie także różnica między statycznym a dynamicznym adresem IP, co również w dużym stopniu będzie nawiązaniem do protokołu DHCP. Kolejny rozdział poświęcony jest bramie dostępowej (sieciowej), czyli czym ona jest, do czego służy i w jaki sposób funkcjonuje. Na koniec opisane zostaną podstawowe techniki monitorowania sieci, czyli w jaki sposób podejrzeć działania urządzeń do niej podłączonych.

1. WSTĘP

Sieci komputerowe z biegiem czasu są coraz częściej wykorzystywane w wielu dziedzinach. Obecnie w domu, biurze, firmie, szkole czy w jakiejkolwiek instytucji nie można sobie wyobrazić pracy przy komputerze bez choćby najmniejszej i najprostszej sieci lokalnej. Jednak założenie i dalsza konserwacja takiej sieci wymaga znajomości pojęć, które zostaną poruszone w kolejnych rozdziałach, w celu ułatwienia konfiguracji, rozwiązywaniu ewentualnych problemów oraz lepszego poznania niektórych zagadnień z zakresu działania sieci lokalnej. Zacznijmy od poznania protokołu DHCP.

2. DHCP – ZASADA DZIAŁANIA, KONFIGURACJA

2.1. Opis protokołu

DHCP (Dynamic Host Configuration Protocol) jest protokołem konfiguracji sieci, który umożliwia uzyskanie informacji przez urządzenie pracujące w sieci. Jest to m.in. adres IP jaki zostanie przydzielony maszynie do komunikacji w sieci. DHCP funkcjonuje w architekturze klient-serwer, gdzie klient otrzymuje informacje konieczne do „zaistnienia" w sieci, zaś wysyłane są one przez serwer, który najczęściej jest zintegrowany razem z koncentratorem sieciowym. Szczegółową zasadę działania tego protokołu opisuje standard RFC 2131 [1].

2.2. Zasada działania

Nowo podłączone urządzenie do sieci musi posiadać pewne informacje, aby mogło ono współpracować z jej resztą. Pierwszą podstawową informacją jest adres IP, pod którym to urządzenie będzie widoczne w sieci. Do prawidłowego działania potrzebny jest także adres IP bramy sieciowej (rozdz. 4), serwer(y) DNS oraz maska podsieci. Takie informacje uzyskiwane są właśnie od **serwera** DHCP przez **klientów**, gdzie serwer jest aplikacją działającą na maszynie połączonej ze wszystkimi klientami, której zadaniem jest oczekiwanie od nich na połączenia i świadczenie im pewnych usług (w tym przypadku przydzielenie klientowi w/w informacji). Klientem zaś w tej sytuacji nazywamy każde inne urządzenie korzystające z usług serwera. Przyjrzyjmy się więc całej procedurze przydzielenia adresu IP klientowi przez serwer.

Serwer DHCP działa na porcie 67, natomiast klient chcąc się z nim połączyć korzysta z portu 68. Transmisja w obie strony opiera się na protokole UDP. Na samym początku urządzenie wysyła pakiet rozgłoszeniowy do wszystkich innych urządzeń znajdujących się w tej samej sieci w poszukiwaniu serwera DHCP (**DHCPDISCOVER**). Serwer DHCP otrzymuje pakiet i w odpowiedzi wysyła do urządzenia możliwy do przydzielenia adres IP (**DHCPOFFER**). W kolejnym etapie urządzenie akceptuje przydzielony adres, więc ponownie wysyła pakiet rozgłoszeniowy z „prośbą" o przydzielenie mu tego adresu (**DHCPREQUEST**). Serwer DHCP odsyła maszynie potwierdzenie (**DHCPACK**), po czym urządzenie może już skonfigurować swój interfejs sieciowy korzystając z otrzymanych danych. Mamy zatem 4 podstawowe rodzaje pakietów protokołu DHCP używanych do poprawnego skonfigurowania urządzenia w sieci.

2.3. Przykładowa konfiguracja klienta i serwera DHCP w systemach UNIX

Najczęściej oprogramowanie zarówno w postaci klienta jak i serwera DHCP dostarczane jest przez **ISC (Internet System Consortium)** [4]. Na nim więc została oparta poniższa konfiguracja.

Całość sprowadza się do zmodyfikowania zaledwie dwóch plików. Pierwszy z nich to /etc/dhcpd.conf, jego przykładowa treść wygląda następująco:

```
subnet 192.168.0.0 netmask 255.255.255.0 {

option routers                  192.168.0.1;
option subnet-mask                    255.255.255.0;
option domain-name                    "domain.org";
option domain-name-servers      192.168.1.1;

range dynamic-bootp 192.168.0.128 192.168.0.255;
default-lease-time 21600;
max-lease-time 43200;
}
```

Przykład 1: Konfiguracja /etc/dhcpd.conf

Na początku określamy podsieć oraz jej maskę, w której nasz serwer będzie pracował, następnie pomiędzy nawiasami klamrowymi uzupełniamy dalszą konfigurację. Linie rozpoczynające się od option oznaczają parametry, które zostaną wysłane do klienta w celu skonfigurowania swojego interfejsu:

- **routers** - adres domyślnej bramy sieciowej
- **subnet-mask** - maska podsieci (najczęściej ta sama jak dla serwera)
- **domain-name** - nazwa domeny
- **domain-name-servers** - adresy serwerów DNS oddzielonych przecinkiem

Kolejne opcje dotyczą ustawień samego serwera DHCP:

- **range dynamic-bootp** - zakres możliwych do przydzielenie adresów IP, w powyższym przykładzie serwer może przydzielić adresy od 192.168.0.128 do 192.168.0.255
- **default-lease-time** - domyślny czas dzierżawy w sekundach
- **max-lease-time** - maksymalny czas dzierżawy w sekundach

Większość parametrów nie powinno przysporzyć problemów za wyjątkiem dwóch ostatnich. Odnoszą się one do kolejnego rodzaju pakietów protokołu DHCP jakim jest czas dzierżawy. Mianowicie urządzenie otrzymujące swoją konfigurację dostaje także swój czas dzierżawy. Po upływie tego czasu musi ono wysłać potwierdzenie do serwera, aby nadal mogło korzystać z przydzielonego adresu. Z reguły serwer odpowiada twierdząco i przedłuża czas dzierżawy. Jeśli klient chce zrezygnować z przydzielonego mu adresu wysyła pakiet (**DHCPRELEASE**) w celu zwolnienia adresu, który będzie mógł zostać przydzielony innemu urządzeniu.

Teraz wystarczy już tylko wybrać interfejs sieciowy, na którym będzie działał serwer DHCP i uruchomić usługę. W tym celu edytujemy plik `/etc/sysconfig/dhcpd` i w linijce `DHCP_INTERFACES=""` wewnątrz cudzysłowów podajemy nazwę interfejsu, np. `eth0`. Następnie uruchamiamy usługę DHCPD.

Konfiguracja zarówno statycznego jak i dynamicznego adresu IP po stronie klienta sprowadza się do co najmniej jednego pliku `/etc/network/interfaces`:

```
auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet static
 address     192.168.11.100
 netmask     255.255.255.0
 gateway     192.168.11.1
 dns-nameservers    192.168.11.1
```

Przykład 2: Konfiguracja statycznego i dynamicznego adresu IP w systemie UNIX

Plik zawiera przykładowe konfiguracje interfejsów sieciowych **eth0** i **eth1**. Przejdźmy zatem do jego omówienia. Linia **auto** oznacza, że dany interfejs będzie uruchamiany przy starcie systemu. Słowem **iface** rozpoczynamy konfigurację dla danego interfejsu. Następnie podajemy rodzinę adresów, zazwyczaj jest to **inet**, czyli standardowe adresy IPv4 (cztery 8-bitowe liczby oddzielone kropkami). Kolejna opcja definiuje w jaki sposób chcemy uzyskać adres. Jak widać w pierwszym przypadku **dhcp** oznacza, że adres przydzielany będzie dynamicznie poprzez DHCP, natomiast słowem **static** konfigurujemy go ręcznie podając w kolejnych liniach parametry (kolejno: adres IP, maska podsieci, brama sieciowa, serwer(y) DNS).

Dodatkowo w przypadku braku zainstalowanego pakietu **resolvconf,** który odpowiada za uzyskiwanie informacji na temat aktualnie dostępnych serwerów DNS, należy je umieścić ręcznie w pliku `/etc/resolv.conf` po jednym na każdą linię w postaci `nameserver adres_dns1`.

2.4. Adresy IP zakończone 0 lub 255

Podczas konfiguracji statycznego adresu IP należy od razu wykluczyć możliwość przydzielenia sobie adresu zakończonego 0 lub 255. Są one zarezerwowane dla pewnych funkcji. Pierwszą z nich (adres 0) jest odwołanie się do całej podsieci, np. adres 192.168.1.0 oznacza całą podsieć od 192.168.1.0 do 192.168.1.255. Z takim odwołaniem spotkaliśmy się podczas konfiguracji serwera DHCP (2.3), gdzie ustawialiśmy, w jakiej podsieci ma on działać. Oznaczenia całych sieci stosowane są też często w

regułach sieciowych, dzięki czemu możemy przykładowo blokować lub zezwalać na połączenia z całych sieci zamiast podawania pojedynczych adresów IP.

Adres z końcówką 255 jest zarezerwowany jako adres rozgłoszeniowy. Również jest on wykorzystywany w protokole DHCP. Dzięki niemu w danej sieci możemy wysłać pakiet do wszystkich urządzeń w niej znajdujących się (patrz rozdz. 2.2 - DHCPDISCOVER).

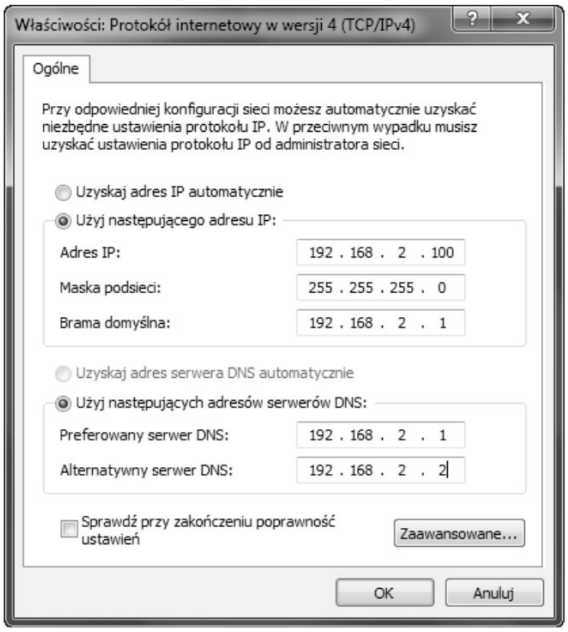
2.5. Podsumowanie

Serwer DHCP bez wątpienia jest przydatną rzeczą w sieci lokalnej. Już dzięki prostej konfiguracji możemy bez problemu dołączać kolejne urządzenia do naszej sieci bez konieczności ich ręcznej konfiguracji, wystarczy bowiem że będą posiadały klienta DHCP. Ponadto mamy pewność, że kilka urządzeń, które korzystają z DHCP nie przydzieli sobie tego samego adresu IP, co spowodowałoby konflikt w naszej sieci. Za pomocą takiego serwera możemy także kontrolować jaki konkretny adres IP ma zostać przydzielony konkretnemu klientowi (przypisywanie adresów IP konkretnym adresom MAC), czy też ograniczać pulę dostępnych do wykorzystania adresów.

3. STATYCZNY I DYNAMICZNY ADRES IP

3.1. Różnica między statycznym a dynamicznym adresem

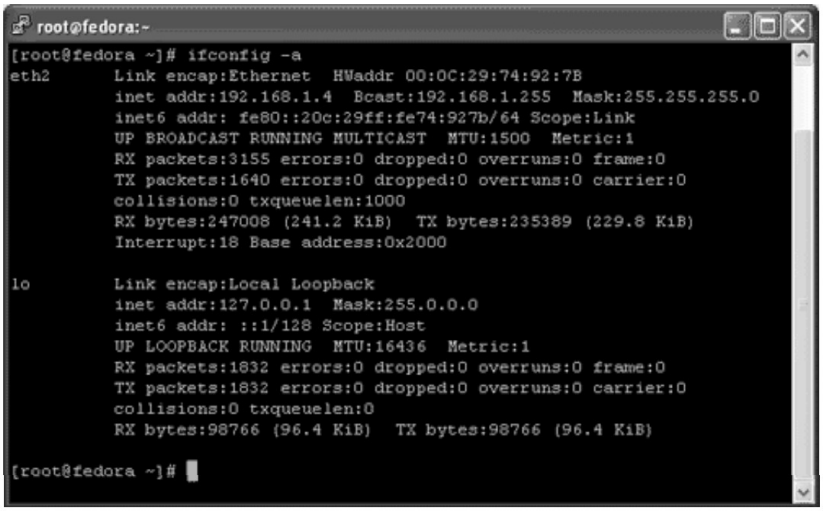
Dynamiczne adresy IP zostały niejako opisane w poprzednim rozdziale. Takim bowiem adresem nazywamy ten przypisany nam poprzez serwer DHCP, czy to w sieci lokalnej czy też poprzez naszego **ISP (Internet Service Provider)** jako nasz publiczny adres widoczny w sieci Internet. Z kolei statyczny adres IP ustawiany jest ręcznie razem z innymi potrzebnymi informacjami tj. maska podsieci, brama i serwery DNS i pozostaje niezmieniony dopóki ręcznie go nie zmodyfikujemy. Poniżej przedstawiono przykład konfiguracji statycznego adresu w sieci lokalnej na przykładzie systemu Microsoft Windows:



Rysunek 1: Konfiguracja statycznego adresu IP w systemie Windows

Analogicznie w celu uzyskania dynamicznego adresu należy zaznaczyć opcje uzyskiwania adresu automatycznie. Jak zatem widać w przypadku ręcznej konfiguracji sami decydujemy, jaki adres IP chcemy sobie przydzielić. Oczywiście jednak nie jesteśmy w stanie przypisać sobie dowolnego adresu, zwłaszcza publicznego, jeśli jest już on w użyciu.

Aby sprawdzić czy poprawnie skonfigurowaliśmy połączenie możemy skorzystać z narzędzia *ipconfig* w wierszu poleceń w systemie Windows lu *ifconfig* w systemie UNIX.



Rysunek 2: Wynik polecenia ifconfig w systemie UNIX (rys. linuxogren.com)

3.2. Podsumowanie

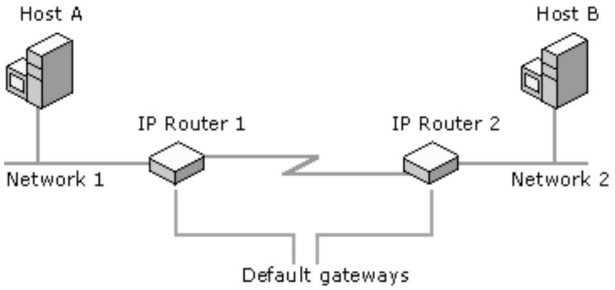
Pracując w sieci lokalnej lub w Internecie posługujemy się adresem IP, który możemy skonfigurować ręcznie lub jest on nam przydzielony dynamicznie przez serwer DHCP. Oba rozwiązania mają swoje wady i zalety. Jeśli chodzi o prostotę i szybkość konfiguracji, najlepszym rozwiązaniem jest adres dynamiczny. Należy jednak pamiętać, że taki sposób w dużym stopniu utrudnia nam publikowanie treści z naszego komputera w formie strony WWW, czy też udostępniania plików przez serwer FTP, ponieważ nie mamy gwarancji stałego IP. Statyczny adres IP wymaga konfiguracji, ale w zamian otrzymujemy kontrolę nad naszym adresem i możliwość uruchamiania wszelkiego rodzaju aplikacji serwerowych dostępnych pod jednym niezmiennym adresem.

4. BRAMA SIECIOWA

4.1 Zadania bramy sieciowej

Brama sieciowa (ang. *default gateway*) pełni bardzo ważną rolę w sieci lokalnej. Dzięki niej jesteśmy w stanie połączyć się z innymi podsieciami (także Internetem). Brak jej ustawienia pozwala nam na komunikację jedynie z naszą podsiecią. Podobnie jak serwer DHCP, brama sieciowa najczęściej występ uje razem z routerem.

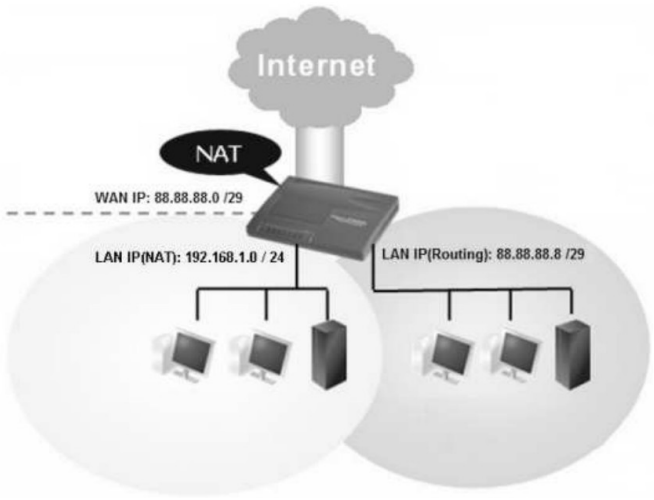
Każdy pakiet wysyłany do innej podsieci trafia najpierw do bramy sieciowej. To ona dalej decyduje dokąd go wysłać dzięki tablicom trasowania



Rysunek 3: Rola bramy sieciowej na przykładzie dwóch sieci lokalnych (rys. technet.microsoft.com [6])

Host A chcąc połączyć się z Hostem B, sprawdza w swojej tablicy czy posiada bezpośrednie połączenie do tego hosta. Ten jednak znajduje się w innej podsieci (Network 2) niż on sam (Network 1), więc Host A kieruje połączenie do swojej domyślnej bramy sieciowej, która przekazuje połączenie do odpowiedniej podsieci.

Komunikacja pomiędzy różnymi sieciami odbywa się za pomocą technologii **NAT (Network Address Translation)**. Służy ona do tłumaczenia adresów lokalnych, tak aby możliwa była komunikacja z innymi podsieciami.



Rysunek 4: Sieć lokalna z wykorzystaniem NAT (rys. draytek.pl)

Powyższy rysunek przedstawia 2 podsieci utworzone przy pomocy jednego przełącznika. Załóżmy, że dostawca przydzielił nam pulę adresów **88.88.88.0 /28**, co teoretycznie daje nam 16 adresów. Technologia NAT pozwala nam na utworzenie sieci z wieloma urządzeniami, gdzie każde z nich w Internecie widoczne będzie pod jednym publicznym adresem, np. **88.88.88.1**, natomiast między sobą będą komunikowały się lokalnymi adresami sieciowymi (w tym przypadku z zakresu 192.168.1.0 /24). Taką opcję zastosowano w podsieci po lewej stronie rysunku. Nic jednak nie stoi na przeszkodzie, aby utworzyć podsieć, w której urządzenia otrzymywać będą publiczne adresy IP (sieć po prawej stronie). W takim wypadku nie korzystamy z technologii NAT, ponieważ każde urządzenie korzysta z unikatowego publicznego adresu IP, a przełącznik w takiej sieci pełni wyłącznie rolę routingu.

4.2 Podsumowanie

Brama sieciowa pozwala na ustanowienie połączenia między różnymi podsieciami. Innymi słowy, stanowi punkt wejściowy i wyjściowy danej sieci. Koniecznie jest więc jej skonfigurowanie u klienta w celu nawiązania takiego połączenia. Najczęściej jest ona także koncentratorem, więc posiada t en sam adres IP.

5. MONITOROWANIE SIECI

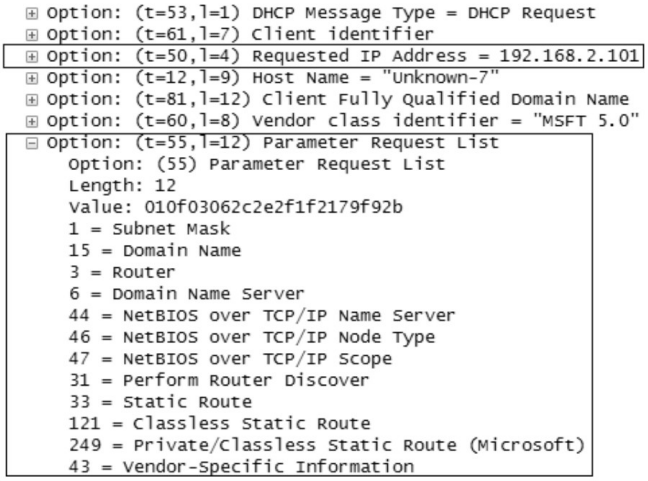
Podczas pracy w sieci nasze urządzenie nawiązuje wiele połączeń, poprzez które przesyłane s ą dane od nas i do nas, czy to poprzez przeglądarkę WWW, komunikator, klient poczty, na grach sieciowych kończąc. Z pomocą odpowiednich narzędzi jesteśmy w stanie podejrzeć wszystko, co przechodzi przez naszą kartę sieciową.

5.2. Monitorowanie połączeń w programie WireShark

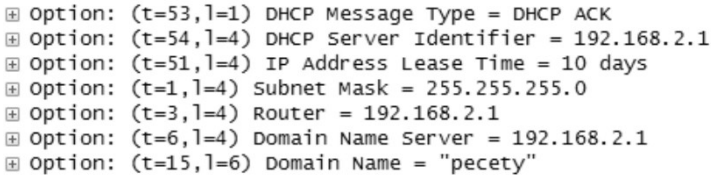
WireShark [7] jest wieloplatformowym (Windows, Unix) narzędziem pozwalającym na monitorowanie przesyłanych przez nasz komputer danych w sieci w czasie rzeczywistym. Każde połączenie jest dokładnie analizowanie przez program, który dokładnie przedstawia nam szczegółowe informacje na jego temat. Rozpoznawany jest protokół, adres i port źródłowy i docelowy, przesłane dane i wiele innych informacji dot. danego połączenia. Jako przykład działania aplikacji przeanalizujmy pakiety protokołu DHCP:

```
468 18.173854   0.0.0.0          255.255.255.255    DHCP     350 DHCP Request  - Transaction ID 0x14fddd99
469 18.176162   192.168.2.1      255.255.255.255    DHCP     590 DHCP ACK      - Transaction ID 0x14fddd99
```

Rysunek 5: Pakiety DHCP wykryte przez program WireShark



Rysunek 6: Szczegółowe dane pakietu DHCPREQUEST



Rysunek 7: Szczegółowe dane pakietu DHCPACK

Powyższe pakiety (rys. 5) zostały „wyłapane" przez program WireShark tuż po podłączeniu kabla sieciowego do komputera. Jako pierwszy został wysłany pakiet DHCPREQUEST. Przeglądając go szczegółowo, możemy dostrzec dane jakie są w nim umieszczone (rys. 6). Oprócz żądanego adresu IP (Requested IP Address), możemy także sprawdzić jakich innych parametrów oczekujemy od serwera DHCP (jak widać oprócz standardowych takich jak maska, brama i serwery DNS, możemy napotkać inne, w tym przypadku dołączone przez system Windows, nie oznacza to jednak, że otrzymamy je wszystkie). Na rysunku 7 mamy natomiast szczegóły dotyczące odpowiedzi od serwera DHCP na wcześniej wysłany pakiet. W tym przypadku otrzymaliśmy potwierdzenie żądanego przez nas adresu IP na okres 10 dni, poza tym oczywiście adresy maski, bramy, serwera DNS oraz nazwę domeny.

5.3. Monitorowanie sieci lokalnej

Analiza pakietów przechodzących przez nasz komputer nie sprawia wielu kłopotów i najczęściej sprowadza się do instalacji odpowiedniego oprogramowania. Co jednak w sytuacji gdy chcemy monitorować całą sieć? W przypadku sieci opartej na koncentratorze typu HUB również nie jest to trudne zadanie, gdyż pakiety przechodzące przez HUB-a trafiają do wszystkich maszyn w sieci, przez co łatwo je podsłuchać. Sprawa komplikuje się gdy sieć jest oparta na przełączniku, który przekazuje pakiety tylko do urządzenia, dla którego są przeznaczone. W takiej sytuacji jedynym wyjściem jest instalacja sniffera na tym przełączniku, co wiązałoby się z koniecznością podmiany całego oprogramowania przełącznika lub uzyskaniem hasła do jego interfejsu (przełączniki zarządzane często posiadają proste sniffery dostępne z panelu WWW). Coraz częściej jednak możemy spotkać przełączniki posiadające specjalne dedykowane gniazdo służące do nasłuchiwania ruchu w sieci. Podłączając się pod nie, wszystkie pakiety przechodzące przez sieć będą trafiać do naszego urządzenia, niezależnie od tego czy zostały skierowane do nas czy gdziekolwiek indziej (podobnie jak w hubie).

5.4. Podsumowanie

Dzięki odpowiedniemu oprogramowaniu (np. WireShark) możemy z łatwością analizować w czasie rzeczywistym pakiety odbierane oraz wysyłane przez naszą kartę sieciową w celu sprawdzenia ich poprawności oraz kontroli nad danymi przesyłanymi przez aplikacje, do których nie mamy dostępu podczas normalnej pracy przy komputerze. Analizowanie pakietów w całej sieci lokalnej jest trudniejsze do zrealizowania chociażby ze względu na konieczność ingerencji w oprogramowanie routera. Nie znaczy to jednak, że nie jest możliwe do zrealizowania.

6. ZAKOŃCZENIE

Każde urządzenie podłączone do jakiejkolwiek sieci posiada swój adres IP. Może on być przydzielony statycznie lub dynamicznie (poprzez serwer DHCP) w zależności od potrzeb. Dodatkowo w celu nawiązania połączenia z inną siecią, każde urządzenie w powinno posiadać poprawnie skonfigurowany adres bramy sieciowej, do której przesyłane będą pakiety zaadresowane do zewnętrznych sieci a także z innych sieci do sieci tego urządzenia. Ilość bram sieciowych nie jest ograniczona, dzięki czemu mamy możliwość tworzenia rozległych i rozgałęzionych sieci, które bez problemu będą mogły się ze sobą komunikować. Z pomocą odpowiednich narzędzi możemy także analizować ruch sieciowy w danej maszynie w sieci lub też całej sieci, jeżeli w odpowiedni sposób skonfigurujemy przełącznik tworzący tą sieć.

BIBLIOGRAFIA

[1]RFC 2131 - http://www.ietf.org/rfc/rfc2131.txt, 1997
[2]What is DHCP Client? Animation - http://www.learningocean.com/view.php?cid=1026&protocol=DHCP&title=1.%20DHCP%20Basics&ctype=1, 2012
[3]DHCPD Deamon - http://pl.docs.pld-linux.org/uslugi_dhcpd.html, 2011
[4]Internet System Consortium – http://www.isc.org, 2012
[5]
[6]Default gateway - http://technet.microsoft.com/en-us/library/cc779696(v=ws.10).aspx, 2005
[7]WireShark - http://www.wireshark.org/, 2012
[8]Debian Manual – Network Setup - http://www.debian.org/doc/manuals/debian-reference/ch05.en.html, 2012

DHCP SERVER, STATIC AND DYNAMIC IP ADDRESS, DEFAULT GATEWAY, NETWORK MONITORING

Summary

This document describes basics issues of the local network. First section explains the DHCP protocol and communications between it's client and server in the network. Next section shows the difference between dynamic and static IP address which also points to the DHCP protocol. Next section is dedicated to the default gateway - what is it, how it works and what is the purpose. At the end there is explained the basic techniques of network monitoring like analysing packets of all devices connected to one network.