Programowa implementacja konfigurowalnego i zarządzanego przez interfejs WWW punktu dostępu do sieci standardu IEEE 802.11

Maciej Łabędź, Marek Natkaniec (e-mail: natkaniec@kt.agh.edu.pl)
Katedra Telekomunikacji Akademii Górniczo-Hutniczej, Kraków

STRESZCZENIE

Lokalne sieci bezprzewodowe WLANs (Wireless Local Area Networks) należą dzisiaj do najszybciej rozwijających się sieci transmisji danych. Obecnie mamy całą rodzinę standardów IEEE 802.11. Standard IEEE 802.11b jest dzisiaj de facto standardem dla sieci WLAN. Zapewnia on uzyskanie szybkości transmisji na poziomie 11 Mbit/s w paśmie ISM 2.4 GHz. Standard IEEE 802.11e wprowadza możliwość gwarancji jakości QoS świadczonych usług na poziomie warstwy MAC. Niestety, do dnia dzisiejszego standard ten nie został zaimplementowany w urządzeniach sieciowych. Artykuł przedstawia programowy sposób implementacji punktu dostępu. System operacyjny Linux wraz z interfejsem WLAN, opartym na układzie PRISM, pozwala na budowę taniego punktu dostępu o bardzo dobrych parametrach radiowych, zgodnego ze standardem IEEE 802.11b. W artykule poruszono również problem użycia mechanizmów QoS na poziomie warstwy sieciowej, który omówiono dla systemu operacyjnego Linux, posiadającego zaawansowane mechanizmy kontroli ruchu wejściowego i kształtowania ruchu wyjściowego.

ABSTRACT

The software implementation of configurable and manageable through www interface access point of IEEE 802.11 standard

Wireless Local Area Networks are one of the fastest growing areas of data transmission networks. Today we have a broad family of IEEE 802.11 WLAN standards. IEEE 802.11b has recently become the de facto standard for WLANs. It provides 11 Mb/s in the ISM 2.4 GHz band. IEEE 802.11e extends the MAC layer to improve QoS capabilities. Unfortunately this standard up to now was not implemented in real WLAN network devices. The possibility of software access point implementation is presented in this article. The Linux OS with the WLAN interface which is based on the Prism chipset let one create developed cheap access point devices with good radio parameters for IEEE 802.11b network. This study contains also problems related to servicing QoS mechanism in the network layer. These mechanisms are discussed on the basis of Linux OS, which provides advanced service of traffic policing and traffic shaping.

1. Wstęp

W ostatnich latach można zaobserwować wzrost znaczenia sieci Internet w różnych dziedzinach życia. Fakt ten wpływa na ciągle rosnące wymagania stawiane takim sieciom przez ich użytkowników. Nowo oferowane usługi często wymagają stosowania szerokopasmowych technik dostępu. Rosnące wymagania użytkowników wymuszają na operatorach konieczność stosowania mechanizmów gwarancji jakości usług QoS (*Quality of Service*). Mechanizmy QoS umożliwiają świadczenie niedostępnych dotąd usług, w tym aplikacji multimedialnych, a także pozwalają na kontrolę i lepsze zarządzanie ruchem generowanym w sieci. Użytkownicy sieci Internet często oczekują od operatorów możliwości swobodnego dostępu do sieci z dowolnego miejsca. Przykładem sieci zdobywających coraz większą popularność są lokalne sieci bezprzewodowe WLANs (*Wireless Local Area Networks*), oparte na rodzinie standardów IEEE 802.11 [7, 8, 9, 10, 11]. Sieci tego typu są obecnie coraz częściej dostępne jako publiczne sieci bezprzewodowe, tzw. *Hotspoty*, umożliwiając klientom dostęp do sieci Internet w miejscach, w których stosowanie technik przewodowych jest utrudnione lub niemożliwe.

Oprócz wielu zalet, sieci WLAN posiadają również kilka wad. Jedną z głównych wad sieci WLAN są problemy związane z zapewnieniem odpowiedniego poziomu bezpieczeństwa przesyłanych danych. Częściowe rozwiązanie tego problemu przynosi implementacja nowego standardu IEEE 802.11i [11]. Kolejną wadą sieci standardu IEEE 802.11 jest brak wsparcia dla zapewnienia odpowiedniego poziomu jakości świadczonych usług. Zaproponowane w pierwszej wersji standardu rozwiązania okazały się niewystarczające. Dopiero standard IEEE 802.11e pozwala na zapewnienie odpowiedniej jakości świadczonych usług na poziomie warstwy łącza danych [9]. Standard IEEE 802.11e został zatwierdzony na początku 2006 roku, jednak do dnia dzisiejszego nie został zaimplementowany w urządzeniach sieci WLAN.

Jednym z podstawowych urządzeń sieci WLAN, opartych na rodzinie standardów IEEE 802.11, jest punkt dostępu. Urządzenie to zapewnia scentralizowany

dostęp do infrastruktury sieciowej stacjom mobilnym pracującym w trybie BSS (*Basic Service Set*) [7]. Obecnie na rynku dostępnych jest wiele urządzeń tego typu, produkowanych przez różnych producentów. Urządzenia te, oprócz podstawowego dostępu do sieci, zapewniają użytkownikom wiele dodatkowych funkcji. Niestety punkty dostępu, zwłaszcza te o bardzo dobrych parametrach radiowych oraz rozbudowanych funkcjach, są dosyć kosztowne, a dodatkowo nie pozwalają na zapewnienie odpowiedniej jakości świadczonych usług. W niniejszym artykule przedstawiono przykład budowy takiego urządzenia opartego na karcie sieciowej standardu IEEE 802.11b dla systemu operacyjnego Linux, a rozbudowana obsługa mechanizmów QoS, na poziomie warstwy sieciowej, pozwoliła na dokładne kontrolowanie jakości przesyłanych strumieni ruchu.

2. Rodzina standardów IEEE 802.11

Pierwszy standard IEEE 802.11 opracowany został w 1997 roku. Zdefiniowane w nim zostały poszczególne elementy funkcjonalne oraz zasady działania sieci bezprzewodowych 802.11. Przedstawiona została również budowa oraz funkcje wykonywane przez warstwę MAC sieci 802.11. Standard określił również budowę trzech rodzajów warstw fizycznych przeznaczonych do współpracy z sieciami 802.11. Warstwy te różnią się między sobą technikami modulacji sygnału. Określono dwie szybkości transmisji sygnału: 1 oraz 2 Mbit/s. Jako pasmo pracy wybrano nielicencjonowane pasmo ISM 2,4 GHz oraz podczerwień.

Rosnące zapotrzebowanie na większe szybkości transmisji danych w sieciach bezprzewodowych doprowadziło do dalszych badań w tym zakresie. W ich wyniku w 1999 roku opublikowany został standard 802.11b [8], w którym przedstawiono nową warstwę fizyczną umożliwiającą pracę sieci z szybkościami do 11 Mbit/s. Standard ten został szybko przyjęty przez rynek i należy obecnie do najbardziej popularnych na świecie.

Alternatywne rozwiązanie, do przedstawionego w standardzie 802.11b, stanowi opublikowany w 1999 roku standard 802.11a. Przedstawiono w nim budowę warstwy fizycznej przeznaczonej do transmisji z szybkościami do 54 Mbit/s i korzystającej z pasma 5 GHz. Sieci w standardzie 802.11a nie zostały jednak tak szeroko rozpowszechnione, jak sieci 802.11b. Wpływ na to miało kilka czynników. Jednym z problemów, hamującym szerokie wdrożenie standardu 802.11a, były uregulowania prawne dotyczące pasma 5 GHz w różnych krajach świata. Urządzenia pracujące w standardzie 802.11a odznaczają się również mniejszym zasięgiem transmisji oraz większym poborem energii.

W 2003 roku opracowano standard 802.11g, w którym przedstawiona została kolejna wersja warstwy fizycznej dla pasma 2,4 GHz, umożliwiająca pracę z szybkościami do 54 Mbit/s. Urządzenia zgodne ze standardem 802.11g odznaczają się wsteczną kompatybilnością z wcześniejszymi standardami i umożliwiają współpracę w jednej sieci urządzeń standardu 802.11g, 802.11b oraz podstawowym 802.11.

W 2004 roku powołana została nowa grupa IEEE 802.11n mająca na celu opracowanie standardu umożliwiającego transmisję w sieci 802.11 z szybkościami dochodzącymi do 100 Mbit/s. Kolejnym założeniem, przyjętym w tym standardzie, ma być zwiększenie zasięgu działania sieci. Obecnie standard ten jest rozwijany, a jego publikacja oczekiwania jest na koniec 2007 roku.

Ze względu na szeroki dostęp do medium transmisyjnego w sieciach bezprzewodowych, ważnym aspektem stało się zapewnienie odpowiedniego poziomu bezpieczeństwa. Zaproponowana, w podstawowej wersji standardu 802.11, technika WEP (*Wired Equivalent Privacy*) okazała się być jednak mało skuteczna. Z tego względu konieczne było opracowanie nowych technik związanych z bezpieczeństwem. W połowie 2004 roku przedstawiono standard IEEE 802.11i wprowadzający nowe mechanizmy zapewnienia bezpieczeństwa w sieciach bezprzewodowych.

Ważną cechą współczesnych sieci jest możliwość zapewnienia właściwego poziomu świadczonych usług QoS. W sieciach bezprzewodowych, w porównaniu z sieciami stałymi, występuje znacznie więcej problemów związanych z transmisją w medium radiowym. Z tego względu zapewnienie odpowiedniego poziomu jakości przesyłanych usług staje się zadaniem bardziej skomplikowanym. Wprowadzone w pierwszej wersji standardu 802.11 w warstwie MAC (*Medium Access Control*) mechanizmy posiadały kilka wad, utrudniających właściwą realizację wymaganego poziomu usług. W celu zapewnienia lepszej współpracy z mechanizmami QoS opracowano standard IEEE 802.11e. Wprowadza on do warstwy MAC nowe rozwiązania w zakresie QoS, a w szczególności umożliwia realizację niezależnych kolejek pakietów, związanych z różnymi klasami ruchu na poziomie warstwy MAC.

Oprócz przedstawionych powyżej standardów, w całej rodzinie IEEE 802.11 dostępnych jest również kilka standardów wprowadzających do sieci dodatkowe funkcje oraz opisujących zagadnienia związane z sieciami 802.11. W standardzie 802.11c opisano sposób tworzenia bezprzewodowych mostów między sieciami bezprzewodowymi. Standard 802.11f wprowadził do komunikacji między punktami dostępu, należącymi do tego samego obszaru ESS, specjalny protokół IAPP (*Inter Access-Point Protocol*) [10]. Protokół ten jest używany do przyspieszenia procesu przełączania się stacji ruchomych podczas ich przemieszczania się między punktami dostępu.

3. Mechanizmy QoS w systemie operacyjnym Linux

Współcześnie oferowane usługi opierają swoje działanie na kontraktach z klientami końcowymi SLA (*Service Level Agreement*). Umowy zawarte między dwiema stronami często określają parametry związane z transmisją danych w sieci operatora TCA (*Traffic Conditioning Agreement*). Do głównych parametrów sieci pakietowych należą [12]:

- przepływność (*Bandwidth*),
- opóźnienie (*Delay*),
- zmienność opóźnienia (*Jitter*),
- prawdopodobieństwo utraty pakietów (*Packet Loss Rate*).

W celu kontroli i przestrzegania ustalonych w kontrakcie profilów ruchu w systemie operacyjnym Linux, stworzono dwa główne mechanizmy QoS:

1) mechanizm kontroli przepływności (*Traffic Policing*),
2) mechanizm kształtowania przepływności (*Traffic Shapping*).

Mechanizm kontroli przepływności analizuje przychodzący do rutera ruch pod względem zgodności z ustalonymi warunkami kontraktu. W sytuacji naruszenia warunków kontraktu pakiety są usuwane. Mechanizm kształtowania przepływności używany jest do generowania ruchu wyjściowego zgodnie z warunkami ustalonymi w kontrakcie.

System Linux, wśród wielu oferowanych przez jądro funkcji, posiada rozbudowany moduł związany z obsługą sieci pakietowych [1, 4, 5]. Przychodzące do węzła sieciowego ramki warstwy łącza danych przekazywane są przez sterownik interfejsu sieciowego do jądra systemu operacyjnego. Przetwarzanie odbieranych ramek w jądrze dokonywane jest przez funkcję *netif_rx()*, która umieszcza przychodzący pakiet w buforze *backlog*. Bufor ten jest wspólny dla wszystkich interfejsów dostępnych w systemie i przeznaczony do kolejkowania ramek oczekujących na dalsze przetworzenie przez jądro. Obsługa ramek oczekujących w kolejce jest dokonywana cyklicznie w funkcji *net_bh(),* wywoływanej przez system operacyjny. Funkcja ta kontroluje rodzaj protokołu warstwy sieciowej. Za odbiór pakietów IP odpowiedzialna jest funkcja *ip_recv()*, która dokonuje sprawdzenia poprawności nagłówka IP w odebranym pakiecie. W kolejnym etapie pakiet przekazywany jest do modułu *Netfilter* i reguły NF_IP_PREROUTING, przeprowadzających filtrację pakietów. W sytuacji, gdy pakiet nie zostanie usunięty, przez powyższy moduł jest on przekazywany do modułu kontroli ruchu, który odpowiada za obsługę mechanizmów QoS w jądrze systemu Linux. Wyjściowy pakiet z modułu jest przekazywany do funkcji *ip_route_input()*, która analizuje miejsce przeznaczenia pakietu.

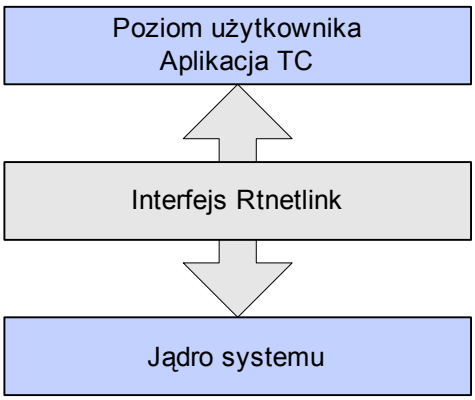
W przypadku, gdy przetwarzany pakiet przeznaczony jest dla danego węzła sieciowego, jest on przekazywany do funkcji odpowiedzialnej za lokalne dostarczenie pakietu. W przypadku protokołu IP wykonywana jest funkcja *ip_local_deliver()* przekazująca pakiet do warstwy transportowej.

Jeżeli pakiet powinien zostać przekazany do innego węzła sieciowego, to wywoływana jest funkcja *ip_forward()*. Funkcja ta jest odpowiedzialna m.in. za dobór odpowiedniego interfejsu wyjściowego zgodnie z tablicą tras (*routing table)* i adresem docelowym pakietu. Sprawdzane i ustawiane są również niektóre pola w nagłówku IP, jak np. pole TTL.

W następnym kroku pakiet jest przekazywany do modułu *Netfilter* i reguły NF_IP_FORWARD. W sytuacji, gdy pakiet zostanie zaakceptowany przez reguły filtrujące, jest on przekazywany do funkcji *ip_forward_finish()*. Jeżeli konieczne jest ustawienie dodatkowych opcji w pakiecie IP, to wywoływana jest funkcja *ip_forward_options()*. Następnie pakiet jest przekazywany do funkcji *ip_send()*. Jeżeli pakiet wymaga dokonania fragmentacji, to funkcja ta przekazuje pakiet do funkcji *ip_fragment()*. W kolejnym etapie pakiet przekazywany jest do modułu *Netfilter* i reguły NF_IP_POSTROUTING. Następnie pakiet trafia do modułu kontroli ruchu i reguły kolejkowania, przypisanej do interfejsu wyjściowego. Moduł kontroli ruchu jest odpowiedzialny za dalsze przekazanie pakietu do interfejsu wyjściowego.

W przypadku, gdy lokalnie generowane pakiety mają zostać wysłane do odległej maszyny, są one przekazywane do funkcji *ip_forward()* obsługującej wysyłanie pakietów zgodnie z procesem opisanym powyżej.

Na rysunku 1 przedstawiono ogólną architekturę obsługi mechanizmów QoS w systemie Linux.



Rys. 1. Architektura obsługi mechanizmów QoS w systemie Linux

Obsługa kontroli ruchu podzielona została na dwa poziomy użytkowe:

1) poziom użytkownika,
2) poziom systemu.

Na poziomie użytkownika dostępne jest oprogramowanie odpowiedzialne za konfigurację i diagnostykę parametrów kontroli ruchu. Zasadnicza kontrola ruchu

odbywa się na poziomie jądra systemu. Dla komunikacji między modułem kontroli ruchu w jądrze i aplikacjami z poziomu użytkownika stworzony został interfejs *Rtnetlink*, dostępny w postaci biblioteki z odpowiednimi funkcjami.

Właściwa kontrola i kształtowanie ruchu odbywa się na poziomie jądra systemu. W tym celu stworzono w jądrze systemu moduł kontroli ruchu TC (*Traffic Control*) o trzech głównych elementach:

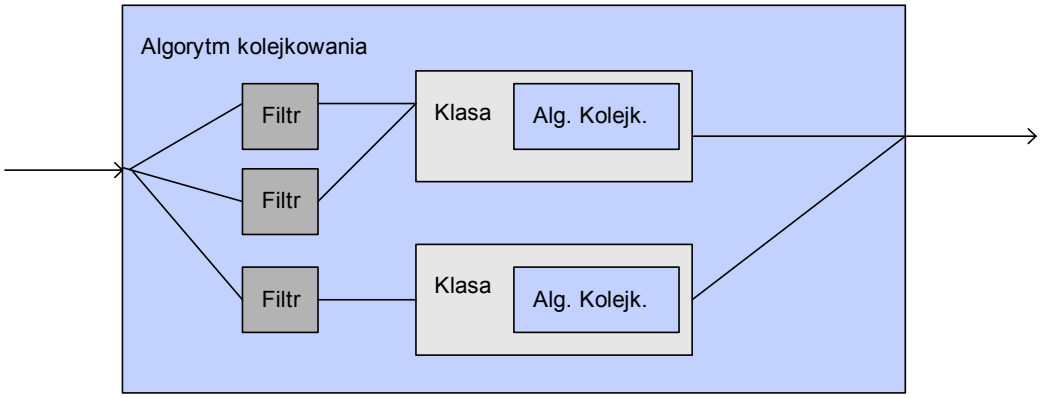
1) algorytmach kolejkowania,
2) klasach,
3) filtrach.

Powyższe trzy elementy umożliwiają tworzenie kolejek pakietów o zróżnicowanym stopniu złożoności. Na rysunku 2 przedstawiono zależność między tymi elementami.

Na poziomie użytkownika systemu dostępne jest oprogramowanie przeznaczone do konfiguracji i diagnostyki parametrów kontroli ruchu. Głównym narzędziem przeznaczonym do tego celu jest aplikacja *tc* z pakietu IPRoute2.

W opracowanym punkcie dostępu używane są istniejące w systemie Linux mechanizmy QoS, których działanie rozszerzono o możliwość automatycznego dokonywania zmian ich konfiguracji w czasie. Funkcjonalność ta wraz z klasowymi algorytmami kolejkowania umożliwia tworzenie rozbudowanych kontraktów ruchu TCA dla różnych klientów.

Dostępne dla systemu operacyjnego Linux oprogramowanie umożliwia również zarządzanie punktem dostępu przez interfejs WWW.



Rys. 2. Zależność między elementami kontroli ruchu

Główny element kontroli ruchu stanowi algorytm kolejkowania, który decyduje o sposobie kolejkowania i kontroli przetwarzanych pakietów. Każdemu interfejsowi sieciowemu dostępnemu w systemie można przypisać unikalny algorytm kolejkowania. Ze względu na budowę, algorytmy kolejkowania można podzielić na dwie główne grupy:

1) algorytmy kolejkowania bezklasowe (m.in. FIFO, RED, TBF),
2) algorytmy kolejkowania klasowe (CBQ, HTB, INGRESS).

Bezklasowe algorytmy kolejkowania są odpowiedzialne za właściwy proces kolejkowania pakietów i nie dają możliwości klasyfikowania pakietów ze względu na ich parametry. Algorytmy klasowe umożliwiają klasyfikowanie pakietów na podstawie ich parametrów i ich przydział do kolejek o różnych priorytetach obsługi. Pakiety można klasyfikować według różnych parametrów, opierając się na:

- adresach źródłowych i docelowych,
- portach źródłowych i docelowych,
- protokołach warstwy transportowej,
- wartościach pola TOS.

4. Programowa implementacja punktu dostępu

Jednym z głównych celów niniejszej pracy było zaprojektowanie i wykonanie urządzenia będącego punktem dostępu do sieci standardu 802.11b. Dodatkowymi zadaniami postawionymi przed projektowanym urządzeniem było:

- zarządzanie nim przez interfejs WWW,
- wsparcie dla mechanizmów QoS,
- zbieranie statystyk i ich prezentacja przez interfejs WWW,
- łatwa instalacja urządzenia

Praktyczne wykonanie konfigurowanego i zarządzanego przez interfejs WWW punktu dostępu oparto na systemie operacyjnym Linux. System ten, wśród wielu oferowanych funkcji, posiada rozbudowany moduł obsługi sieci pakietowych. W obecnej serii jądra 2.6 systemu Linux możliwa jest współpraca z kartami bezprzewodowymi wielu producentów [14]. W tym celu wprowadzono w jądrze systemu Linux mechanizmy określane jako *Wireless Extension*. Mechanizmy te od-

powiadają za komunikację między jądrem systemu, sterownikami interfejsów bezprzewodowych i aplikacjami pracującymi w przestrzeni użytkownika.

Jednym z przykładów sterownika dla kart bezprzewodowych jest moduł *HostAP* [6]. Jest on przeznaczony do współpracy z kartami opartymi na układzie *Prism* w wersji 2, 2.5 oraz 3 firmy *Intersil*. Układ ten jest zgodny z sieciami standardu 802.11b. Ważną zaletą sterownika *HostAP* i układu *Prism* jest możliwość pracy interfejsu bezprzewodowego w trybie punktu dostępu. Do funkcji oferowanych przez sterownik *HostAP* w czasie pracy w trybie punktu dostępu należą m.in.:

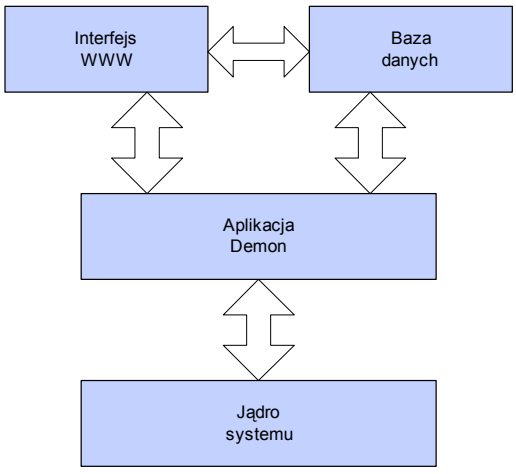
- kontrola dostępu klientów do sieci,
- obsługa przyłączania klientów do sieci,
- zapewnienie komunikacji między stacjami końcowymi,
- wsparcie dla stacji końcowych korzystających z trybu oszczędzania energią,
- komunikacja z innymi punktami dostępu przez protokół IAPP.

Sterownik *HostAP* umożliwia również pracę karty bezprzewodowej w standardowych trybach pracy i zapewnia współpracę z sieciami BSS oraz IBSS (*Independent Basic Service Set*). Ważną cechę sterownika *HostAP* stanowi możliwość współpracy z następującymi standardami bezpieczeństwa:

- WEP,
- WPA (*Wi-Fi Protected Access*),
- 802.11i.

Należy zaznaczyć, iż sterownik *HostAP* stanowi jedną z pierwszych pełnych implementacji standardu 802.11i.

Dostępne dla systemu operacyjnego Linux oprogramowanie umożliwia stworzenie interfejsu WWW, pozwalającego na zarządzanie urządzeniem punktu dostępu do sieci WLAN opartym na układzie Prism i sterowniku HostAP. Na rysunku 3 przedstawiono ogólną architekturę takiego punktu dostępu.



Rys. 3. Architektura zaprojektowanego punktu dostępu

Do obsługi interfejsu WWW wybrano serwer HTTP Apache. Serwer ten charakteryzuje się wieloma rozbudowanymi funkcjami, do których należy m.in. możliwość współpracy z różnymi językami programowania. Interfejs WWW zaimplementowano w języku PHP. Język ten oferuje m.in. funkcje obsługi komunikacji z bazą danych, oraz umożliwia korzystanie z programowania obiektowego, które ułatwia wprowadzanie zmian i łatwą rozbudowę interfejsu.

Do przechowywania parametrów konfiguracji punktu dostępu i zbierania statystyk wybrano bazę danych PostgreSQL. Baza PostgreSQL, oprócz zalet oferowanych przez relacyjne bazy danych SQL, umożliwia tworzenie funkcji w języku PLpgSQL. Język ten pozwala na tworzenie rozbudowanych i zarazem wydajnych funkcji przetwarzania danych bezpośrednio w bazie SQL. W projektowanym punkcie dostępu tego typu funkcje odpowiedzialne są za właściwy proces kontroli i przetwarzania danych. Przechowywane informacje podzielono na następujące grupy danych związane z:

- konfiguracją interfejsów,
- konfiguracją mechanizmów QoS,
- konfiguracją klientów i kontroli dostępu,
- gromadzeniem statystyk,
- pozostałymi parametrami konfiguracyjnymi.

Na rysunku 4 przedstawiono tabele bazy danych wraz z istniejącymi między nimi relacjami.

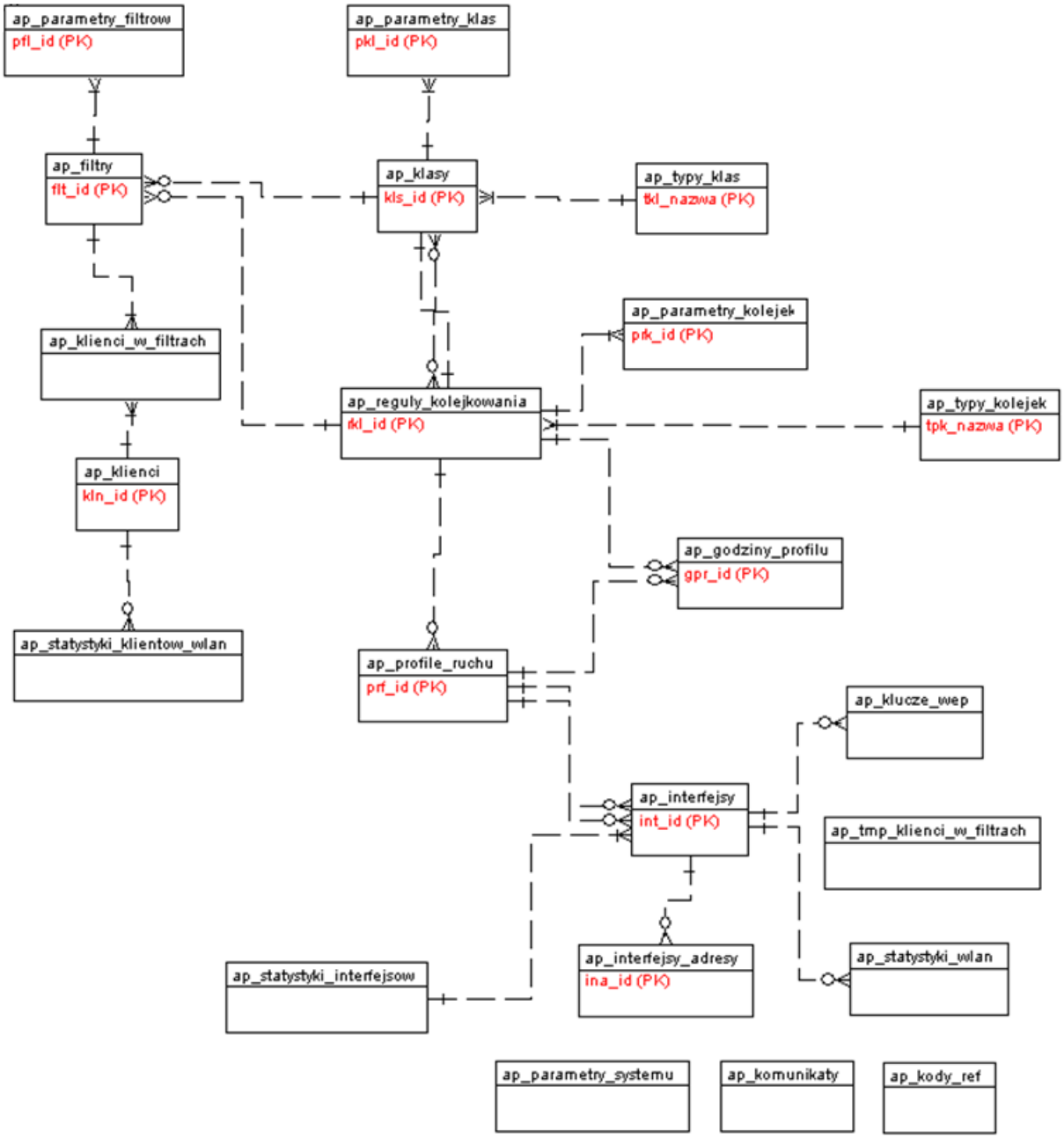
Konieczne okazało się też stworzenie dodatkowej aplikacji demona pracującego w przestrzeni użytkownika. Aplikacja ta, napisana w języku C, umożliwia komunikację między interfejsem WWW i jądrem systemu. Głównymi funkcjami aplikacji demona są:

- Wprowadzanie zmian w konfiguracji systemu na podstawie zmian dokonywanych przez interfejs WWW,
- Odczytywanie z jądra systemu statystyk i przekazywanie ich do bazy danych.

Komunikacja między interfejsem WWW a aplikacją demona dokonywana jest przez regułę obsługi plików FIFO, dostępną w systemie Linux. Aplikacja demona posiada również interfejs komunikacyjny z bazą danych PostgreSQL. Na podstawie wprowadzanych przez użytkownika zmian w konfiguracji, z poziomu interfejsu WWW przekazywane są komendy do aplikacji demona. Korzystając z komend, aplikacja demona odczytuje wymaganą konfigurację systemu z bazy danych i dokonuje wymaganych zmian w konfiguracji systemu operacyjnego.

Opracowane oprogramowanie pozwala na obsługę z poziomu użytkownika następujących elementów:

- zarządzanie klientami,
- zarządzanie mechanizmami QoS,



Rys. 4. Architektura bazy danych punktu dostępu

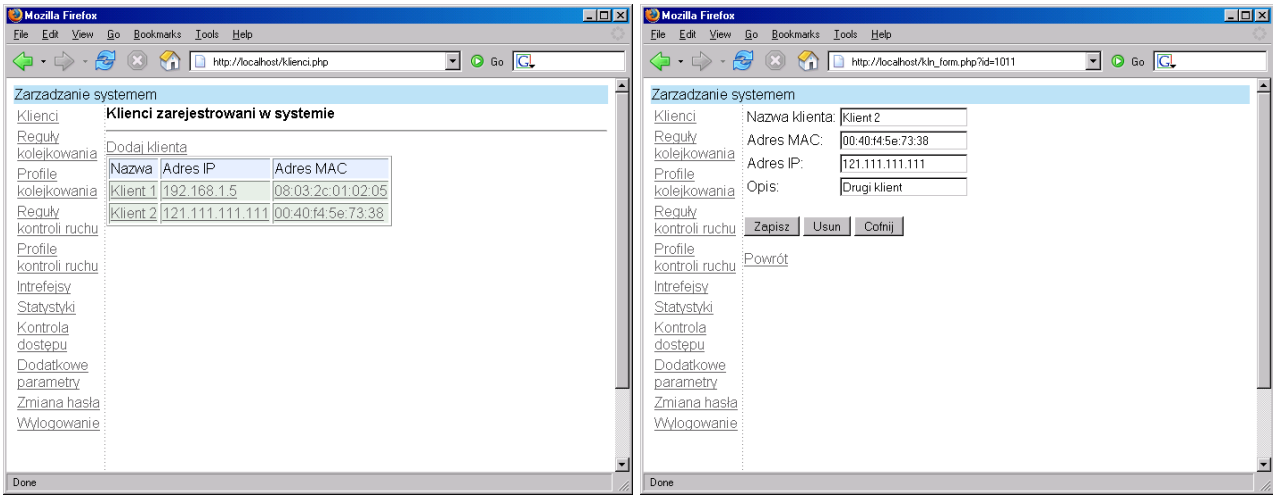
- zarządzenie interfejsami sieciowymi,
- konfigurowanie dodatkowych parametrów sieciowych,
- przeglądanie statystyk ruchu.

Interfejs WWW umożliwia tworzenie listy klientów wraz z przypisanymi im adresami MAC oraz IP. Na podstawie listy klientów możliwe jest automatyczne konfigurowanie klientów przez wbudowany w urządzeniu serwer DHCP. Urządzenie punktu dostępu pozwala również na kontrolę dostępu do sieci na podstawie adresów MAC klientów (rys. 5).

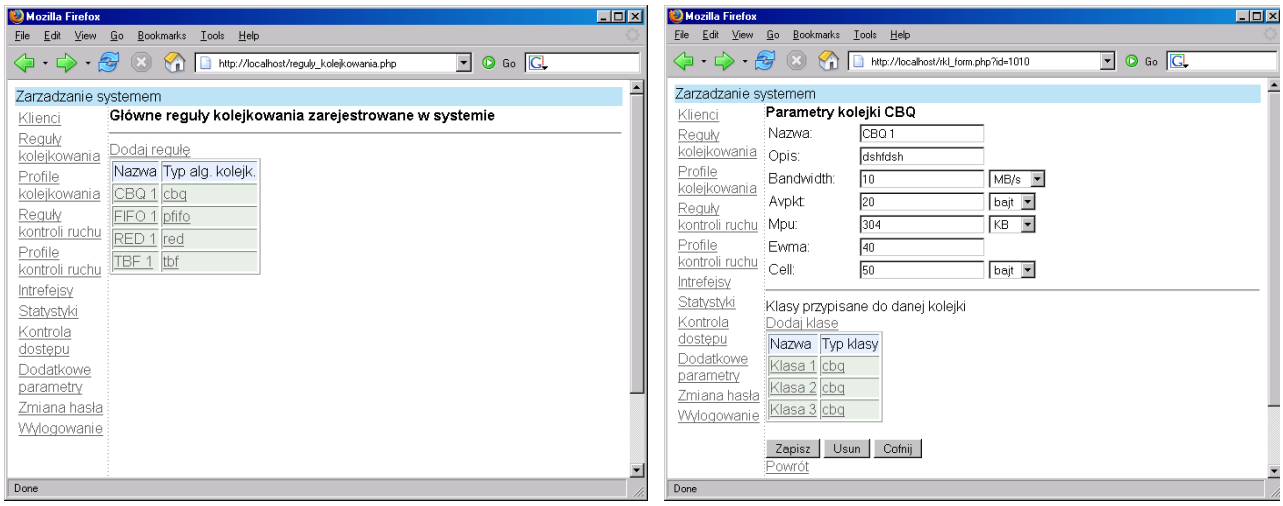
Zarządzanie mechanizmami QoS jest realizowane na drodze konfiguracji następujących elementów:

- reguł kolejkowania,
- profili kolejkowania,
- reguł kontroli ruchu,
- profili kontroli ruchu.

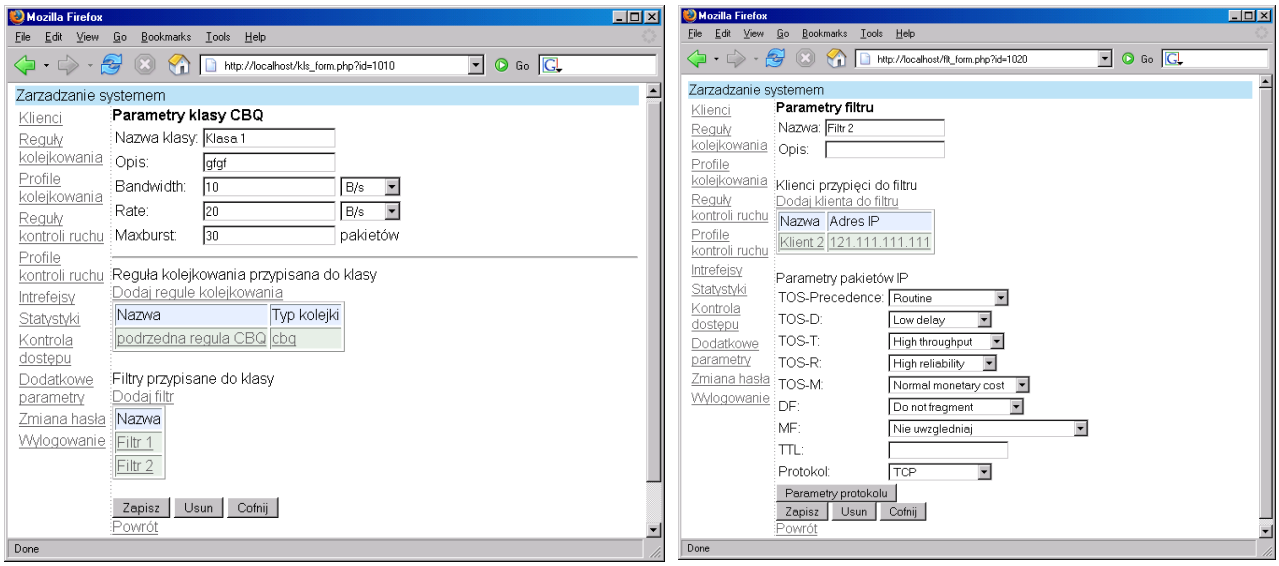
Reguły kolejkowania pozwalają na tworzenie różnych konfiguracji algorytmów kolejkowania związanych z kształtowaniem przepływności. W przypadku korzystania z klasowych algorytmów kolejkowania możliwe jest przypisywanie zarejestrowanych klientów do różnych klas i ich obsługa z różnymi priorytetami. Stworzone oprogramowanie pozwala również na klasyfikację ruchu na podstawie parametrów pakietów IP, a opracowana reguła kolejkowania – na tworzenie profili kolejkowania. Każdy z tych profili pozwala na podzielenie tygodnia na dowolną liczbę okresów, w których obowiązują wybrane reguły kolejkowania. Analogiczne reguły i profile kontroli są stosowane do kontroli ruchu wejściowego (rys. 6 i 7).



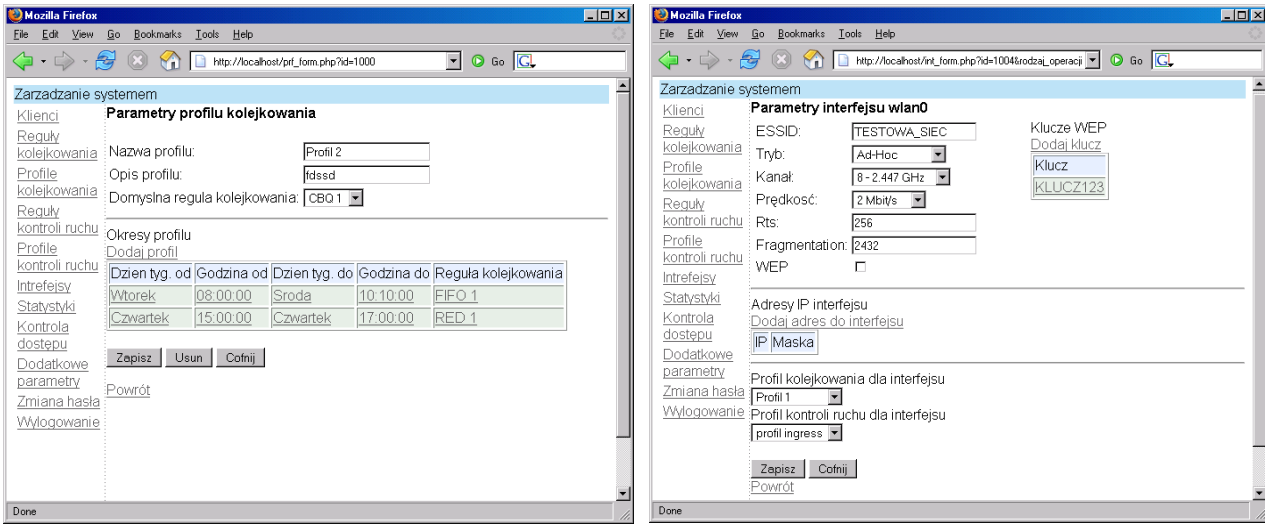
Rys. 5. Strona umożliwiająca przeglądanie zarejestrowanych w systemie klientów oraz formularz modyfikacji i usuwania klientów



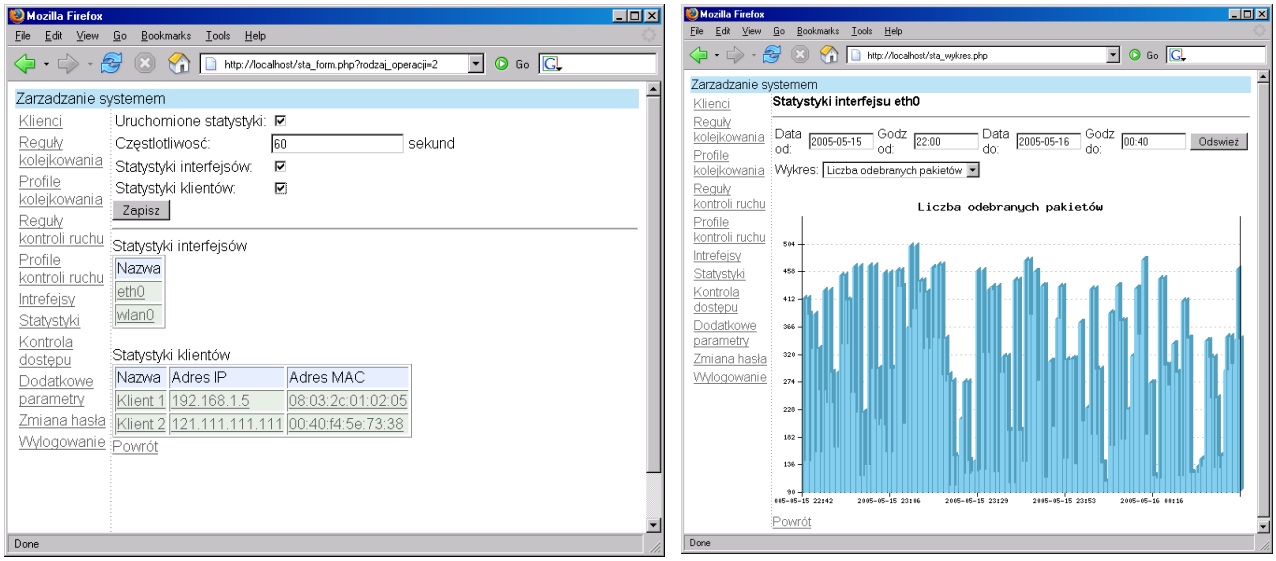
Rys. 6. Strona umożliwiająca przeglądanie reguł kolejkowania oraz formularz modyfikacji klasowego algorytmu kolejkowania



Rys. 7. Strona umożliwiająca modyfikację parametrów klasy oraz formularz z parametrami filtru



Rys. 8. Strona do modyfikacji profilu kolejkowania oraz formularz do modyfikacji parametrów interfejsów



Rys. 9. Strona do konfiguracji statystyk oraz formularz prezentujący statystyki interfejsu

W celu zarządzania interfejsami sieciowymi z poziomu menu administrator sieci może przypisywać adresy IP oraz maski podsieci. Możliwe jest również włączenie maskowania adresów IP na adres interfejsu wyjściowego. Każdemu z interfejsów sieciowych użytkownik może przypisać profile kolejkowania i kontroli pakietów związanych z mechanizmami QoS. Dodatkowo, dla interfejsów bezprzewodowych możliwe jest konfigurowanie takich ich parametrów (rys. 8), jak:

- tryb pracy interfejsu,
- numer kanału,
- szybkość transmisji,
- próg *RTS threshold*,
- próg *Fragmentation threshold*,
- kodowanie WEP.

Ponadto interfejs WWW pozwala również na konfigurowanie takich dodatkowych parametrów, jak:

- adresy IP serwerów DNS,
- adres IP domyślnej bramy sieciowej.

Zaprojektowane w ramach pracy urządzenie punktu dostępu umożliwia zbieranie i przeglądanie statystyk ruchu w sieci. Zbierane przez urządzenie statystyki podzielić można na dwie grupy:

1) statystyki interfejsów sieciowych,
2) statystyki dotyczące ruchu generowanego przez klientów.

W przypadku interfejsów sieciowych gromadzone są informacje o liczbie przesłanych i odebranych bajtów oraz pakietów. W przypadku interfejsów bezprzewodowych dodatkowo gromadzone są statystyki, do których należą:

- liczba ramek z błędnym ESSID,
- liczba błędnie zakodowanych ramek,
- liczba niepoprawnych fragmentów,
- liczba zagubionych ramek *Beacon*,
- liczba przekroczonych prób retransmisji ramek,
- szybkość transmisji interfejsu sieciowego.

Statystyki dotyczące ruchu generowanego przez klientów zawierają informacje o liczbie przesłanych i odebranych bajtów oraz pakietów, jak również o poziomie mocy sygnału i szumu dla poszczególnych klientów punktu dostępu. Zgromadzone statystyki mogą być prezentowane w formie wykresów lub tabel (rys. 9).

W celu uproszczenia instalacji urządzenia, system operacyjny Linux wraz ze stworzonym w ramach pracy oprogramowaniem został zrealizowany w postaci płyty startowej CD.

5. Podsumowanie

W ramach pracy wykonano oprogramowanie umożliwiające budowę urządzenia – punktu dostępu dla sieci bezprzewodowych standardu 802.11, wykorzystującego komputer klasy PC. Oprogramowanie oparto na systemie operacyjnym Linux. System ten umożliwia współpracę z wieloma rodzajami interfejsów sieciowych, do których należą m. in. interfejsy bezprzewodowe standardu 802.11. Urządzenie przystosowane zostało do współpracy z interfejsem opartym na układzie Prism. Układ ten, jako jeden z nielicznych, daje możliwość pracy interfejsu bezprzewodowego w trybie punktu dostępu dla sieci standardu 802.11b, zapewniając obsługę wielu funkcji wykonywanych przez tego rodzaju urządzenia.

Opracowane urządzenie może być w łatwy sposób konfigurowane i zarządzane przez wbudowany interfejs WWW. Pozwala on na zarządzanie interfejsami sieciowymi, sieciami IP oraz klientami korzystającymi z punktu dostępu. Zapis i analiza różnego rodzaju statystyk pozwalają na monitorowanie stanu sieci i ułatwiają wykrywanie problemów w niej występujących. Urządzenie wyposażone zostało również w obsługę mechanizmów WEP związanych z bezpieczeństwem sieci standardu IEEE 802.11. Dzięki zastosowaniu sterownika *HostAP*, istnieje możliwość łatwej rozbudowy urządzenia o obsługę standardu IEEE 802.11i. Pełne wprowadzenie tego standardu w sieci wymaga jednak jego implementacji w stacjach klientów.

Ważną funkcją, w jaką wyposażone zostało urządzenie, niespotykaną nawet w komercyjnych urządzeniach klasy „enterprise", jest rozbudowana obsługa mechanizmów QoS. Przedstawiony w standardzie IEEE 802.11 tryb PCF (*Point Coordination Function*) obsługi mechanizmów QoS w warstwie łącza danych posiada pewne wady. Tryb ten jako opcjonalny nie jest szeroko stosowany w sieciach standardu 802.11. Nowy standard IEEE 802.11e, wprowadzający rozszerzoną obsługę QoS w warstwie łącza danych w sieciach IEEE 802.11, nie został jeszcze zaimplementowany w urządzeniach sieciowych. Z tych względów konieczne okazało się zastosowanie alternatywnego rozwiązania. Zaimplementowany w systemie operacyjnym Linux moduł umożliwia obsługę różnego rodzaju algorytmów kolejkowania pakietów. Pozwala to na tworzenie rozbudowanych kontraktów ruchu wejściowego i wyjściowego. Dodatkowo, mechanizmy QoS systemu Linux zostały rozszerzone o możliwość zmiany ich konfiguracji w czasie.

Należy zaznaczyć, że stworzone w ramach pracy oprogramowanie pozwala także na projektowanie i rozbudowę innych urządzeń sieciowych. Architektura poszczególnych elementów oprogramowania pozwala na wprowadzanie w takich urządzeniach nowego rodzaju funkcjonalności dostarczanej przez system Linux. Powyższe zalety systemu pozwoliły na opracowanie na jego podstawie rozbudowanego urządzenia punktu dostępu do sieci WLAN, którego możliwości wyraźnie przewyższają obecnie dostępne rozwiązania komercyjne.

Literatura

[1] Almesberger W.: *Linux Network Traffic Control – Implementation Overview*. 1999

[2] Frank O.: *Wi-Fi Handbook: Building 802.11b Wireless Networks*. 2003

[3] Gast M.: O'Reilly – 802.11 Wireless Networks: The Definitive Guide

[4] Hubert B.: Linux Advanced Routing & Traffic Control, 2003 (http://lartc.org)

[5] Krawczyk P.: *Sterowanie przepływem danych w Linuxie*. 2001

[6] Malinen J.: *Host AP driver for Intersil Prism2/2.5/3* http://hostap.epitest.fi/

[7] Standard IEEE 802.11: IEEE Standards for Information Technology – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,1999

[8] Standard IEEE 802.11b: Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band, 1999

[9] Standard IEEE 802.11e: IEEE Standard for Information technology – Local and metropolitan area networks – Specific requirements Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Quality of Service (QoS) Enhancements, 2005

[10] Standard IEEE 802.11f: IEEE Recommended Practice for Multi-Vendor Access Point Interoperability via

an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, 2003

[11] Standard IEEE 802.11i: IEEE Standard for Information technology – Local and metropolitan area networks. Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements, 2004

[12] Stankiewicz R., Jajszczyk A.: *Sposoby zapewnienia gwarantowanej jakości usług w sieciach IP*. Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne nr 2/2002

[13] Vegesna S.: *IP Quality of Service*. Cisco Press, 2001

[14] Weeks R., Dumbill E.: *Linux Unwired*

Marek Natkaniec - otrzymał tytuł magistra inżyniera oraz doktora telekomunikacji na Wydziale Elektrotechniki Automatyki i Elektroniki Akademii Górniczo-Hutniczej w Krakowie w latach 1997 i 2002. Obecnie pracuje jako adiunkt w Katedrze Telekomunikacji Akademii Górniczo-Hutniczej. Jego zainteresowania obejmują: lokalne sieci bezprzewodowe, projektowanie protokołów komunikacyjnych, zagadnienia QoS, usługi multimedialne, modelowanie oraz analiza wydajności pracy sieci teleinformatycznych. Pracuje aktywnie w projektach europejskich. Uczestniczy również w realizacji projektów badawczych finansowanych przez Ministerstwo Nauki i Szkolnictwa Wyższego. Marek Natkaniec jest współautorem czterech książek oraz ponad sześćdziesięciu publikacji.