WIRTUALNE SIECI LAN

Mariusz Piwiński
Instytut Fizyki
Wydział Fizyki, Astronomii i Informatyki Stosowanej
Uniwersytet Mikołaja Kopernika w Toruniu
ul. Grudziądzka 5, 87-100 Toruń
Mariusz.Piwinski@fizyka.umk.pl

Abstract. The constant development of the network technologies and services results in growing number of devices connected to Internet. The increasing amount of generated and transferred data causes the need of optimization of computer networks. Moreover, due to security reasons the best practice is dividing users into separate groups with different privileges and rights to resources. Virtual Local Area Networks could be one of the solution of this problem. In this work the idea of VLANs is presented and discussed with typical topologies.

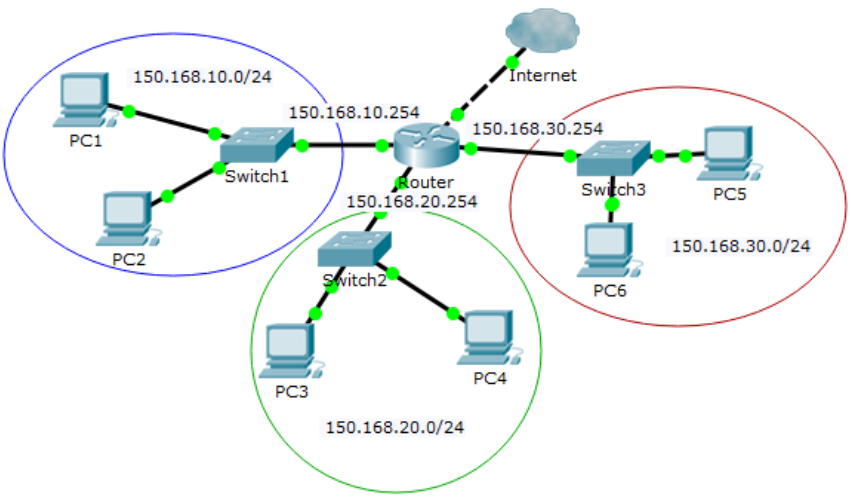
1. Wstęp

Globalna sieć teleinformatyczna nazywana potocznie Internetem stała się platformą wykorzystywaną do świadczenia wielu usług wykorzystywanych zarówno przez ludzi, systemy, jak i urządzenia. Zjawisko polegające na podłączaniu do sieci coraz większej liczby nowych urządzeń, które mogą ze sobą oddziaływać określa się mianem **Internetu Rzeczy** (*tzw.* ***IoT,*** *ang. Internet of Things*) [1]. Najczęściej dostęp do globalnej sieci realizowany jest za pośrednictwem dostawców usług internetowych (*tzw.* ***ISP,*** *ang. Internet Service Provider*), którzy w zależności od stawianych wymagań wykorzystują różne technologie dostępowe (np. Ethernet, DOCSIS, WiFi, DSL, WiMAX). Wybór zastosowanej technologii pociąga za sobą bezpośrednio ograniczenia dotyczące maksymalnego pasma dostępnego dla użytkownika końcowego, co czasami może być kluczowe z punktu widzenia wykorzystywanych usług. Jednocześnie wraz ze zwiększającą się liczbą urządzeń pracujących w sieci lokalnej pojawiają się problemy związane z wydajnością urządzeń sieciowych oraz zarządzaniem lokalny pasmem transmisji. Ze względu na wykorzystywane technologie wielodostępowe, bezpieczeństwo oraz rosnące wymagania aplikacji ważne jest wydajne zarządzanie zasobami poprzez tworzenie grup użytkowników posiadających odpowiednie priorytety i uprawnienia [7, 10].

Typowo stosowane podejście dotyczące optymalizacji sieci oparte jest na wydzielaniu grup użytkowników i przydzielaniu ich do indywidulanych podsieci. Takie rozwiązanie wymaga jednakże zastosowania wielu bram (interfejsów routera) oraz dedykowanych dla każdej podsieci przełączników. Wpływa to na podniesienie kosztów wykonania takiej sieci oraz ogranicza jej elastyczność. Rozwiązaniem tego problemu może być zastosowanie wirtualnych sieci **VLAN** (*ang. Virtual Local Area Networks*). Celem niniejszego opracowania jest przybliżenie tej technologii wraz z przykładami stosowanych typowych topologii oraz konfiguracji.

2. Podstawy sieci VLAN

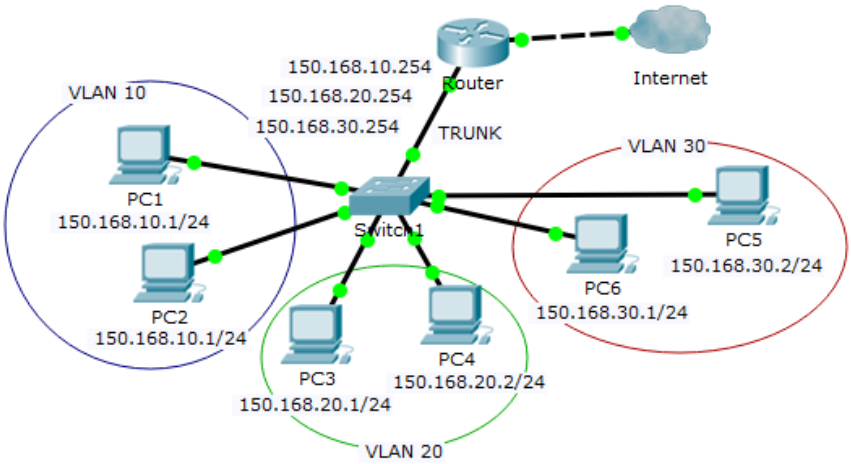
Idea przyświecająca tworzeniu sieci VLAN polega na możliwości wydzielenia ruchu należącego do różnych grup użytkowników przy wykorzystaniu urządzeń warstwy 2 modelu OSI (*ang. Open System Interconnection*) [11]. W rozwiązaniach niewykorzystujących wirtualnych sieci taki podział realizowany jest za pomocą urządzeń warstwy 3, czyli routerów, co przedstawiono na Rysunku 1. W rezultacie oznacza to, iż każda podsieć musi być obsługiwana przez indywidualny interfejs routera.



Rysunek 1 Podział sieci 150.168.0.0./16 na trzy podsieci (150.168.10.0/24, 150.168.20.0/24, 150.168.30.0/24) w celu lepszego zarządzania użytkownikami.

Stworzenie VLAN'ów przy użyciu przełącznika sieciowego oznacza możliwość wydzielenia grup użytkowników i oddzielenia od siebie generowanego przez nie ruchu sieciowego (Rysunek 2). W efekcie jest to równoważne z sytuacją, w której każda grupa hostów byłaby podłączona do dedykowanego przełącznika sieciowego (Rysunek 1). W skrócie można stwierdzić, iż każdy stworzony VLAN stanowi od-

dzielną domenę rozgłoszeniową. O ile z VLAN'ami związane będą bezpośrednio podsieci, oznaczać to będzie, iż komunikacja pomiędzy użytkownikami należącymi do różnych grup będzie możliwa jedynie za pośrednictwem urządzenia warstwy 3, czyli routera. Ze względu na fakt, iż przydział użytkownika do danej grupy związany jest z odpowiednią konfiguracją przełącznika, a nie z fizycznymi połączeniami, takie rozwiązanie zapewnia znacznie większą elastyczność niż klasyczne zarządzanie podsieciami. Należy zauważyć, iż urządzenia końcowe pracujące w różnych VLAN'ach (należące do różnych podsieci) będą musiały posiadać różne adresy bramy domyślnej. Oznacza to, iż nadal w celu zapewnienia pełnej obsługi urządzeń końcowych wymagane jest zastosowanie wielu interfejsów routera, co przy wydzieleniu wielu grup użytkowników stanowić będzie istotny problem. Ostateczne rozwiązanie może być oparte na technologii wykorzystującej logiczne podinterfejsy zdefiniowane na jednym fizycznym interfejsie routera. Z punktu widzenia routingu realizowanego przez urządzenie warstwy 3, są one pełnoprawnymi interfejsami mogącymi obsługiwać ruch należący do różnych grup użytkowników. Topologia taka często określana jest, jako „router na patyku" (*ang. router on a stick*), co ma związek z wykorzystywanym pojedynczym interfejsem sieciowym routera (Rysunek 2). Przykładowa konfiguracja podinterfejsów routera została przedstawiona na Rysunku 3.



Rysunek 2 Topologia sieci wykorzystującej wirtualne sieci VLAN (10, 20 i 30) oraz podinterfejsy logiczne routera.

```
Router(config)#int g0/0.10
Router(config-subif)#encapsulation dot1Q 10 native
Router(config-subif)#ip address 150.168.10.254 255.255.255.0
Router(config-subif)#int g0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 150.168.20.254 255.255.255.0
Router(config-subif)#int g0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 150.168.30.254 255.255.255.0
Router#
%SYS-5-CONFIG_I: Configured from console by console
sh ip int brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     unassigned      YES manual up
up
GigabitEthernet0/0.10  150.168.10.254  YES manual up
up
GigabitEthernet0/0.20  150.168.20.254  YES manual up
up
GigabitEthernet0/0.30  150.168.30.254  YES manual up
```

Rysunek 3 Konfiguracja logicznych podinterfejsów routera w systemie Cisco IOS wraz z weryfikacją ich stanu.

3. Standardy znakowania ramek VLAN

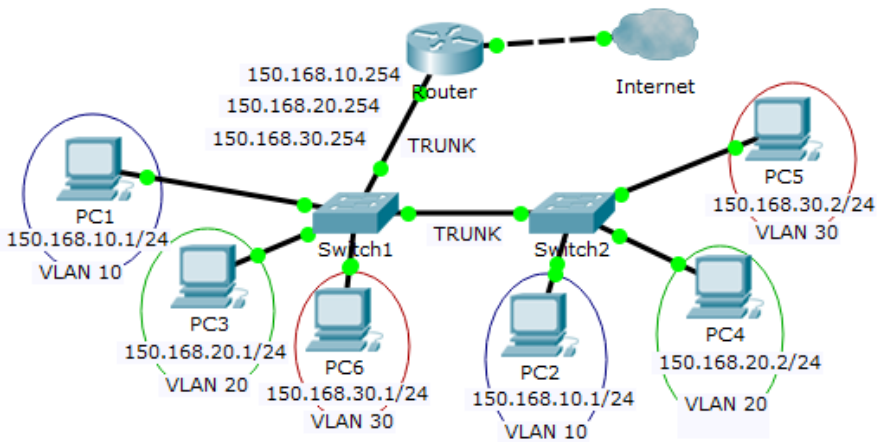
Przedstawione podejście wymaga jednakże przesyłania do routera danych ze wszystkich VLAN'ów poprzez jedno fizyczne łącze, które pełni funkcję magistrali (*ang. trunk*). Niestety ramka Ethernet'owa nie zawiera pola, które mogłoby zostać użyte do przekazania informacji, z którego VLAN'u pochodzą przesyłane dane. W związku z powyższym takie rozwiązanie wymaga specjalnego oznakowania ramki. Istnieje wiele sposobów, które mogą zostać wykorzystane w tym celu. Ze względu na brak początkowej standaryzacji, producenci urządzeń sieciowych stosowali swoje rozwiązania, które jednak nie były obsługiwane przez urządzenia innych firm. Powodowało to, iż szeroka implementacja sieci VLAN była bardzo utrudniona. Rysunek 4 przedstawia dwa sposoby znakowania ramek Ethernet II. Pierwszy z nich, definiowany jako **ISL** (*ang. InterSwitch Linking Protocol*) polega na enkapsulacji przesyłanej ramki w nową ramkę. Posiada ona nagłówek, w którym umieszczono informację na temat obsługiwanego VLAN'u (między innymi jego numer) oraz stopkę zawierającą sumę kontrolną [4]. Urządzenie sieciowe odbierające taką ramkę otrzymuje komplet informacji potrzebny do prawidłowej obsługi przesyłanych danych. Następnie ramka ISL jest rozpakowywana, a do urządzenia końcowego należącego do odpowiedniego VLAN'u przesyłana jest oryginalna ramka Ethernet II. Jak widać znakowane ramki będą zupełnie niezrozumiałe dla urządzeń nieobsługujących protokół ISL, co stanowi dużą wadę tego rozwiązania. Metoda ta została opracowana przez firmę Cisco i jako taka wykorzystywana była w urządzeniach tego producenta.

Z czasem coraz większe wykorzystanie technologii VLAN spowodowało jej standaryzację w postaci standardu IEEE **802.1Q** (nazywanego również **Dot1q**), który obecnie stosowany jest przez większość urządzeń sieciowych [6]. Protokół ten jest cały czas rozwijany przez grupę roboczą IEEE 802.1 [2], w wyniku czego powstało wiele jego rozszerzeń. Do protokołu tego został między innymi włączony protokół Multiple Registration Protocol (**MRP**) IEEE 802.1ak, który umożliwia przełącznikom wymianę informacji o obsługiwanych sieciach VLAN oraz o przynależności hostów do grup typu multicast [5]. Ogólny format ramki Ethernet II oznakowanej w protokole IEEE 802.1Q przedstawiono na Rysunku 4. Należy zauważyć, iż w tym przypadku ramka nie została opakowana w nową ramkę, ale bezpośrednio za polem opisującym adres źródłowy zdefiniowano pole opisujące obsługiwany VLAN (zwierające 16-bitowy numer VLAN). Takie rozwiązanie umożliwia (w pewnych przypadkach) obsługę oznakowanych ramek również przez urządzenia sieciowe niewspierające bezpośrednio tej technologii. Wynika to bezpośrednio z faktu, iż struktura ramki wraz z polami adresowymi, standardowo analizowanymi przez przełączniki sieciowe, nie została zmieniona. Analogicznie jak w poprzednim przypadku, urządzenie sieciowe obsługujące wirtualne sieci po odczytaniu informacji o VLAN'ie, z którego pochodzą dane, usuwa to pole, a następnie do urządzenia końcowego przesyła ramkę zgodną z formatem Ethernet. Należy podkreślić, iż prawidłowo skonfigurowany przełącznik ethernetowy nie może przesyłać oznakowanych ramek do urządzeń końcowych, gdyż te nie posiadając skonfigurowanego protokołu IEEE 802.1Q nie będą w stanie ich poprawnie interpretować. W takim przypadku pole 802.1Q może być błędnie interpretowane jako pole Typ.

Rysunek 4 Struktura ramki Ethernet II, ramki protokołu ISL oraz standardu znakowania IEEE 802.1Q.

4. Rozszerzone topologie VLAN

Opisywany protokół znakowania ramek pozwala na przesyłanie informacji nie tylko pomiędzy routerem a przełącznikiem, a także pomiędzy samymi przełącznikami sieciowymi. Oznacza to, iż definiując łącze magistrali pomiędzy przełącznikami możemy za pomocą pojedynczego połączenia przenosić dane ze wszystkich obsługiwanych VLAN'ów. Zatem wydzielona grupa użytkowników nie musi być ograniczona do pojedynczego urządzenia. Granicę stosowalności takiego rozwiązania określa interfejs routera, który stanowi bramę domyślną dla poszczególnych podsieci. Topologia wykorzystująca dwa przełączniki sieciowe została przedstawiona na Rysunku 5.



Rysunek 5 Topologia sieci VLAN wykorzystującej dwa przełączniki sieciowe.

Jak już wspomniano, dane wysyłane przez łącze magistrali identyfikowane są z odpowiednim VLAN'em na podstawie numeru zapisanego w polu 802.1Q. W związku z powyższym, aby umożliwić bezpośrednią komunikację pomiędzy użytkownikami należącymi do tej samej grupy, a podłączonymi do różnych przełączników wystarczy zadbać o spójną numerację wirtualnych sieci na wszystkich wykorzystywanych przełącznikach sieciowych.

Stosując wiele urządzeń do budowy sieci, naturalną potrzebą jest możliwość zdalnego zarządzania tymi urządzeniami. W przypadku przełączników sieciowych wymaga to skonfigurowania wirtualnego interfejsu oraz nadania mu odpowiedniego adresu IP. Ze względów bezpieczeństwa dobrą praktyką jest ograniczenie dostępu do tego typu urządzeń sieciowych dla wybranej grupy użytkowników. W efekcie oznacza to, iż urządzenia te mają skonfigurowane adresy sieciowe należące do specjalnego VLAN'u (podsieci) służącego do administrowania urządzeń. Restrykcje

dotyczące dostępu do tej specjalnej sieci najczęściej definiowane są w postaci list kontroli dostępu ACL (*ang. Access Control List*).

5. Konfiguracja sieci VLAN

Ze względu na różne implementacje, sposoby konfiguracji sieci VLAN na urządzeniach różnych producentów mogą różnić się od siebie, jednakże w większości przypadków będą one wymagały wykonania następujących czynności:

- Stworzenie sieci VLAN

Podczas konfiguracji na urządzeniu tworzona jest baza danych sieci VLAN określająca numery oraz opisy sieci. Na Rysunku 6 przedstawiono konfigurację sieci VLAN w systemie Cisco IOS. Po wykonaniu komendy weryfikacyjnej ***show vlan*** oprócz utworzonych sieci widoczny jest również domyślny VLAN 1, do którego przydzielone są domyślnie wszystkie porty przełącznika. System IOS uniemożliwia usunięcie tego VLAN'u, zatem dobrą praktyką związaną z bezpieczeństwem jest usunięcie wszystkich portów z sieci VLAN 1.

```
Switch(config)#vlan 10
Switch(config-vlan)#name Admin
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Studenci
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name Pracownicy
Switch(config-vlan)#do sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -
--------------------------------
1    default                           active    Fa0/1, Fa0/2,
Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6,
Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10,
Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14,
Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18,
Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22,
Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   Admin                             active
20   Studenci                          active
30   Pracownicy                        active
```

Rysunek 6 Konfiguracja sieci VLAN na przełączniku sieciowym.

- Przydział portów przełącznika do poszczególnych sieci VLAN

W niniejszym opracowaniu omawiane jest przyporządkowanie statyczne portu przełącznika do określonego VLAN'u. Konfiguracja ta zakłada, iż cały ruch generowany przez określonego hosta (podłączonego do tego portu) będzie należał do jednej wirtualnej sieci. Istnieją inne metody pozwalające na przydział hosta (lub jego danych) do odpowiedniego VLAN'u na podstawie jego identyfikacji, lub analizy generowanego przez niego ruchu. Jednakże ze względu na znaczną złożoność takiego podejścia zagadnienia te stanowczo wychodzą poza ramy niniejszego opracowania. Przykładowy statyczny przydział portów do sieci VLAN wraz z weryfikacją konfiguracji (komenda ***sh vlan***) został przedstawiony na Rysunku 7.

```
Switch(config)#int fa 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int fa 0/3
Switch(config-if)#switchport access vlan 30
Switch(config-if)#switchport mode access
Switch# sh vlan

10   Admin                            active    Fa0/1
20   Studenci                         active    Fa0/2
30   Pracownicy                       active    Fa0/3
```

Rysunek 7 Przykładowa konfiguracja przydziału portów do sieci VLAN w systemie Cisco IOS wraz z weryfikacją konfiguracji.

- Konfiguracja portów pracujących w trybie magistrali

W kolejnym kroku należy skonfigurować porty obsługujące połączenie magistrali (trunk) z przełącznikiem lub routerem. W konfiguracji takiego portu pojawia się zapis o VLAN'ie natywnym określający sieć domyślną, do której kierowane są nieznakowane ramki pojawiające się na łączu magistrali. W celu prawidłowego działania łącza magistrali, należy po obu jego stronach skonfigurować taki sam VLAN natywny. Przykładowa konfiguracja wraz z weryfikacją ustawień została przedstawiona na Rysunku 8.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int g0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 10
Switch(config-if)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      10
```

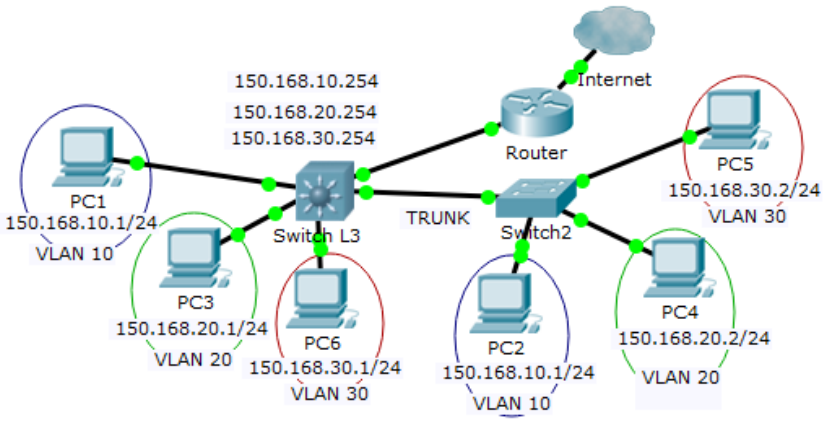
Rysunek 8 Przykładowa konfiguracja portu w trybie magistrali VLAN w systemie Cisco IOS.

- Konfiguracja podinterfejsów routera

W celu zapewnienia komunikacji użytkowników z innymi urządzeniami znajdującymi się poza VLAN'em wymagane jest skonfigurowanie bram domyślnych dla obsługiwanych podsieci. Podczas konfiguracji podinterfejsów obsługujących wirtualne sieci, należy zdefiniować numer VLAN, z którym ma zostać stowarzyszony dany interfejs. Ponadto należy również wskazać, który z VLAN'ów będzie traktowany jako natywny. Najczęściej jest to VLAN wykorzystywany do zarządzania urządzeniami sieciowymi. Przykładowa konfiguracja podinterfejsów routera do obsługi sieci VLAN została przedstawiona na Rysunku 3.

6. Konfiguracja sieci VLAN w oparciu o przełącznik L3

Przedstawiona na Rysunku 5 topologia posiada dosyć istotną wadę polegającą na znacznym obciążeniu łącza pomiędzy routerem a przełącznikiem. Jest ono wykorzystywane zarówno podczas wysyłania danych poza LAN jak i w komunikacji między hostami należącymi do różnych VLAN'ów. Problem ten można rozwiązać stosując przełącznik warstwy 3, którego celem będzie routowanie danych między VLAN'ami (podsieciami). Tym samym urządzenie to będzie również odpowiedzialne za definiowanie reguł określających prawa dostępu do różnych zasobów dla poszczególnych grup lub indywidualnych hostów. Reguły takie mogą być określane w oparciu o adresację IP, a w bardziej zaawansowanych przypadkach również bazując na adresach MAC. Ze względu na fakt, iż jest to przełącznik warstwy 3, urządzenie to jest zoptymalizowane pod kątem przełączana ramek i posiada ograniczone funkcje w stosunku do typowych routerów. Również jego konfiguracja jest nieco odmienna od typowej konfiguracji przełącznika i routera. Jak widać na Rysunku 9 przełącznik ten posiada interfejsy logiczne, które pełnią rolę bram domyślnych dla podsieci VLAN, a w przedstawianej topologii router pełni jedynie funkcję urządzenia brzegowego.



Rysunek 9 Topologia sieci VLAN wykorzystującej przełącznik warstwy 3.

Opisywane rozwiązania dotyczące obsługi wirtualnych sieci mogą być również stosowane w połączeniu sieciami bezprzewodowymi IEEE 802.11 [9]. W tym przypadku znakowanie ramek realizowane jest przez punkt dostępowy obsługujący klienta radiowego i przesyłający dane za pomocą sieci kablowej do przełącznika lub kolejnego punktu dostępowego. Należy jednakże pamiętać, iż ze względu na obsługę pasma radiowego komunikacja ta jest znacznie bardziej skomplikowana. Wszyscy klienci radiowi należący do różnych VLAN'ów obsługiwani są na tym samym kanale radiowym, a zatem fizyczne rozdzielenie transmisji (tak jak dzieje się to w sieci kablowej) nie jest możliwe. W związku z powyższym w takich przypadkach najczęściej sieci VLAN stowarzyszone są z różnymi sieciami bezprzewodowymi (rozgłaszającymi różne SSID). Takie rozwiązanie w połączeniu z różnymi sposobami autoryzacji klientów zapewnia izolowanie ruchu należącego do różnych sieci VLAN. Ze względu na przedstawioną implementację maksymalna liczba obsługiwanych w ten sposób wirtualnych sieci w sieciach radiowych jest mocno ograniczona. Jest ona bezpośrednio związana z maksymalną liczbą obsługiwanych sieci radiowych pracujących równocześnie na jednym kanale radiowym.

Inne rozwiązanie polega na podłączeniu wszystkich klientów do jednej sieci radiowej oraz indywidualnego szyfrowania każdej transmisji w oparciu o dane autoryzacyjne klienta. Spowoduje to, iż klienci nie będą w stanie odszyfrować danych przeznaczonych dla innych użytkowników. Punkt dostępowy po otrzymaniu takiej ramki od klienta radiowego, dokonuje weryfikacji do którego VLAN'u powinna ona trafić, a następnie przesyła ją jako oznakowaną ramkę Ethernet II po łączu magistrali do kolejnego przełącznika.

W przypadku sieci bezprzewodowych wykorzystujących kontrolery **WLAN** (*ang. Wireless Local Area Network)* sytuacja jest jeszcze bardziej skomplikowana. W tym przypadku dane odebrane od klienta przez tzw. „*cieńki punkt dostępowy*" (*ang. Thin Access Point*) wysyłane są za pomocą sieci przewodowej do kontrolera przy wykorzystaniu specjalnego protokołu **LWAPP** (*ang. Lightweight Access Point Protocol*) [3]. Kontroler po otrzymaniu danych podejmuje decyzję o wysłaniu ich do odpowiedniej sieci VLAN [12]. Obecnie wszystkie te rozwiązania są szeroko implementowane w sieciach LAN.

Opisywane w niniejszym opracowaniu wirtualne sieci zostały przedstawione w połączeniu z protokołem IPv4. Jednakże ze względu na fakt, iż dotyczą one warstwy 2 modelu OSI, mogą współpracować z różnymi protokołami warstwy 3, w tym również z protokołem IPv6 [8]. Zastosowanie takiego rozwiązania nie wymaga zmiany opisywanych topologii, a jedynie zapewnienia odpowiedniej konfiguracji urządzeń.

7. Podsumowanie

Niniejsze opracowanie miało na celu przybliżenie technologii VLAN wykorzystywanych do optymalizacji i zarządzania zasobami sieci LAN. Przedstawiono typowe topologie wykorzystujące router oraz przełączniki, w tym również przełącznik warstwy 3. Niniejsze opracowanie może stanowić wstęp do implementacji wirtualnych sieci w administrowanej sieci LAN oraz być zachętą do dalszego studiowania zagadnień związanych z zarządzaniem sieciami LAN.

Literatura

1. Ashton K, That 'Internet of Things' Thing, http://www.rfidjournal.com/articles/view?4986
2. https://1.ieee802.org
3. https://tools.ietf.org/html/rfc5412
4. https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html
5. http://www.ieee802.org/1/pages/802.1ak.html
6. http://www.ieee802.org/1/pages/802.1Q-2014.html
7. Piwiński. M, Internet - wybrane aspekty bezpieczeństwa, Informatyka w Edukacji, red. A.B. Kwiatkowska, Wydawnictwa Naukowe UMK, Toruń, 2013, http://repozytorium.umk.pl/handle/item/1712

8. Piwiński M., Komunikacja sieciowa z wykorzystaniem protokołu IPv6, Informatyka w Edukacji, Kształcenie informatyczne i programowanie dla wszystkich uczniów, A.B. Kwiatkowska, M.M. Sysło, Wydawnictwo Naukowe UMK, 380-398, Toruń, 2016 ISBN 978-83-231-3585-2, http://repozytorium.umk.pl/handle/item/3700
9. Piwiński M., Sieci bezprzewodowe IEEE 802.11, „Informatyka w Edukacji, Wokół nowej podstawy informatyki", A.B. Kwiatkowska, M.M Sysło, Wydawnictwo Naukowe UMK, 388-407, Toruń, 2017, http://repozytorium.umk.pl/handle/item/4427
10. Piwiński M., Sieci komputerowe, konfiguracja i bezpieczeństwo, Informatyka w Edukacji, Nauczyciel przewodnik i twórca, red. A.B. Kwiatkowska, M.M. Sysło, Wydawnictwo Naukowe UMK, ISBN 978-83-231-3411-4, Toruń, 85-99, Toruń, 2015, https://repozytorium.umk.pl/handle/item/2759
11. Piwiński M., Praktyczna analiza sieci komputerowych z wykorzystaniem programu Wireshark, Informatyka w Edukacji V, A.B. Kwiatkowska, M.M. Sysło, Wydawnictwo Naukowe UMK, 277-285, Toruń, 2008, http://repozytorium.umk.pl/handle/item/1686
12. Piwiński M., Marczak G., Sieci bezprzewodowe wykorzystujące technologie wirtualnej komórki i wirtualnego portu na przykładzie Meru Networks, Informatyka w Edukacji, Informatyka dla wszystkich od najmłodszych lat, A.B. Kwiatkowska, M.M Sysło, Wydawnictwo Naukowe UMK, Toruń, 2014 ISBN 978-83-231-3251-6 https://repozytorium.umk.pl/handle/item/2101