Wprowadzenie

W dzisiejszych czasach, w dobie błyskawicznego rozwoju zarówno sprzętu, jak i oprogramowania, trudno wyobrazić sobie sieci komputerowe bez ich podstawowego elementów, jakimi są przełączniki. Przez lata użytkowania przełączniki niezwykle się rozwinęły, przejmując niektóre elementy pracy routerów, a z prostych urządzeń obsługujących warstwę łącza danych zmieniły się w „sieciowe kombajny" potrafiące wykorzystywać niektóre mechanizmy warstwy transportowej modelu ISO/OSI [1].

Historia przełączników w sieciach Ethernet wywodzi się w prostej linii od urządzeń zwanych koncentratorami, do zadań których należała replikacja sygnału do wszystkich urządzeń podłączonych bezpośrednio do niego. Na przestrzeni lat koncentratory zostały wyparte na rzecz przełączników ze względu swoją podstawową wadę, którą było rozsyłanie ramek w sposób rozgłoszeniowy. Taka praca, szczególnie w sieciach, w których występuje duże wykorzystanie zasobów łącza, jest bardzo utrudniona lub nawet niemożliwa ze względu na liczbę występujących kolizji, dodatkowo nasilającą się wraz z rozmiarem samej sieci. Przyczyną problemów, jakie wynikają z takiego działania, jest prostota wykonania samego urządzenia oraz to, że działa ono w warstwie fizycznej modelu ISO/OSI i bazuje na elektrycznej transmisji sygnałów, a nie ramek [2], [3].

Wspomniane wady koncentratorów doskonale eliminują przełączniki, które operują najczęściej na warstwie drugiej modelu ISO/OSI, tworząc głównie połączenia typu punkt-punkt, tym samym separując przesyłane ramki najczęściej do hostów, dla których zostały one przeznaczone. Aby dokładniej przybliżyć mechanizmy stojące za sukcesem przełączników, w następnym punkcie zostaną omówione rodzaje przełączników dostępnych na rynku [2], [3].

1. Klasyfikacja przełączników

1.1. Przełączniki L2

Jednymi z najprostszych, a zarazem najtańszych przełączników obecnie dostępnych na rynku, są urządzenia operujące na warstwie łącza danych. Stosuje się je głównie

z urządzenia od razu po wyjęciu go z pudełka. Mimo niewielkich rozmiarów przełączniki często wyposażone są w porty RJ45 o prędkościach 10/100/1000Mb/s oraz sloty na wkładki SFP. Z uwagi na głównie domowe zastosowanie, coraz częściej producenci w tym segmencie wdrażają różne mechanizmy oszczędzania energii, polegające na wykrywaniu i zasileniu tylko podłączonych urządzeń lub badaniu długości kabli do urządzeń końcowych i ograniczeniu napięcia podawanego na złącza [6].

Przełączniki zarządzane to najczęściej spotykana grupa urządzeń sieciowych, która znajduje swoje miejsce zarówno w małych firmach jak i dużych korporacjach, głównie z uwagi na dużo większy zestaw funkcji (patrz tabela 1), które gwarantują wysoką niezawodność oraz bezpieczeństwo.

1.2. Przełączniki L3

Ten rodzaj przełączników pojawił się głównie ze względu na rozpowszechnienie się sieci VLAN, w których ruch nie musiał być już trasowany za pomocą routerów. O ile duże firmy mogły pozwolić sobie na wykorzystanie osobnego sprzętu na potrzeby przełączania sieci VLAN, o tyle małe organizacje zmuszone były najczęściej do przesyłania całego ruchu między sieciami VLAN na router będący często na styku sieci lub zaraz za zaporą sieciową, co obciążało sieć i mogło prowadzić do zmniejszenia bezpieczeństwa. Przełącznik L3 jest urządzeniem specjalizującym się w routingu sieci VLAN i wykorzystuje do tego wirtualne interfejsy przełączania. Mimo, iż urządzenie to nie posiada wszystkich możliwości, jakie oferują obecnie routery, to w swoim wąskim zakresie pracy potrafi być wydajniejsze w przełączaniu pakietów [3].

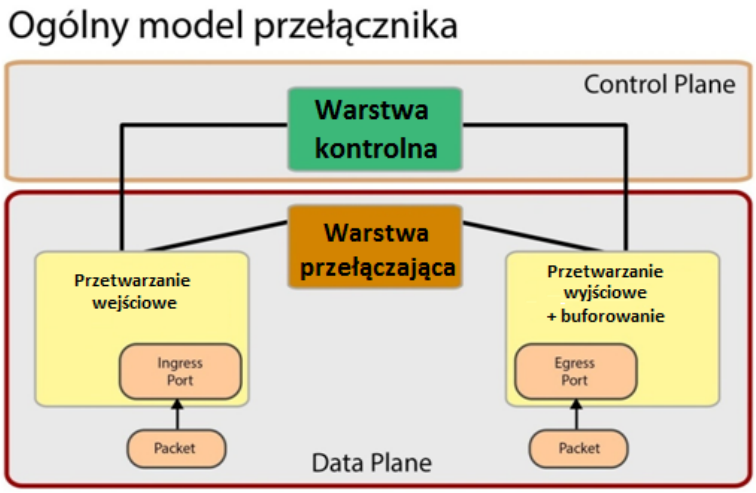
1.3. Przełączniki wielowarstwowe

Ten rodzaj przełączników jest rozwinięciem standardowych konstrukcji L3, lecz w porównaniu do nich zwykle przybiera wymiary powyżej 4U i ma konstrukcję modułową. Taka budowa zapewnia możliwość spersonalizowania urządzenia pod precyzyjne wymagania, jakie stawia specyfika sieci komputerowej. Przykładem takich konstrukcji może być cała seria urządzeń Cisco Nexus czy starsza konstrukcyjnie seria Catalyst. Dzięki temu, że urządzenia te mogą operować na warstwach wyższych

2. Idea przełączania ramek i pakietów

2.1. Ogólny model działania przełącznika

Generalnie sposób, w jaki działa przełącznik, można sprowadzić do kilku prostych kroków przedstawionych na rysunku 1. W pierwszym etapie pakiet trafia na porty wejściowe, na których wykonywane jest przetwarzanie wejściowe, w wyniku którego pakiet jest rozpoznawany i może zostać zmodyfikowany lub odrzucony. Później za pomocą warstwy przełączającej następuje umieszczenie pakietu w buforze. Końcowy proces to przeniesienie pakietu na porty wejściowe, w których wykonany jest proces przetwarzania wyjściowego. Taka droga pakietu określana jest często jako przekazywanie w warstwie (*ang. Data Plane)*. Jest to pożądany i najszybszy sposób przekazywania danych [7], [9].



Rysunek 1. Uproszczony schemat działania przełącznika [7]

Do sterowania przełącznikiem i jego pracą wykorzystywana jest warstwa kontrolna, do której zadań należy między innymi budowa tablic przełączania. Może się też zdarzyć, że pakiet zostanie skierowany do przetwarzania również przy pomocy tej warstwy. Dzieje się to tylko w wyjątkowych sytuacjach, gdy układy ASIC nie wiedzą co zrobić z danym pakietem lub jest to pakiet kontrolny. Tak zrealizowane przełączanie

Metoda	Opis
Fragment-free	Ulepszenie mechanizmu polegające na połączeniu zalet obu powyżej przedstawionych metod. Przełącznik pracujący w tym trybie odczytuje pierwsze 64 bajty i na podstawie tych informacji określa, czy przesyłana ramka jest poprawna. W przypadku kolizji przesyłany fragment jest mniejszy niż 64 bajty, co wskazuje na uszkodzenie. Metoda ta podobnie jak cut-through może zostać wykorzystana jedynie w połączeniach symetrycznych, kiedy oba interfejsy pracują z tą samą prędkością.

Ze względu na zastosowanie coraz wydajnych układów ASIC oraz pamięci typu TCAM, większość urządzeń firmy Cisco z serii Catalyst domyślnie przekazuje dane z wykorzystaniem metody store-and-forward. Urządzenia serii Nexus przeznaczone dla centrów przetwarzania danych z kolei wykorzystują domyślnie metodę cut-through.

Wspomniane ustawienia można dowolnie modyfikować, choć przyjęło się, że urządzenia pracujące w warstwie rdzenia powinny wykorzystywać metodę fast-forward ze względu na minimalizacje opóźnień. Z uwagi na różnorodność produkowanego przez firmę Cisco sprzętu zawsze należy sprawdzić w dokumentacji technicznej, czy dany tryb przełączania jest wspierany przez konkretne urządzanie [5].

3. Segmentacja sieci i nadmiarowość

3.1. Koncepcja sieci wirtualnych – VLAN

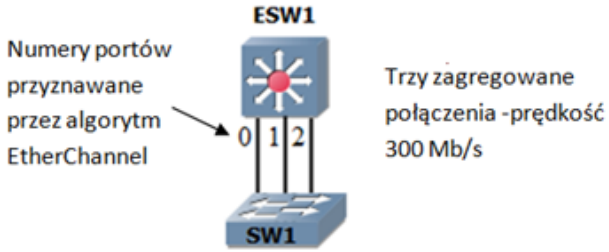
Sieci VLAN to sieci logiczne, które są tworzone w obrębie jednej sieci fizycznej. Dzięki tej technologii można w obrębie jednego fizycznego urządzenia skonfigurować kilka sieci logicznych. Taka konfiguracja może odbywać się na poziomie przełącznika lub – rzadziej – routera, dzięki czemu dla każdego połączonego do interfejsu sieciowego urządzenia można utworzyć własną izolowaną podsieć [3], [10].

Wykorzystanie VLAN-ów pozwala w sposób efektywny segmentować sieć, czyli podzielić ją na mniejsze elementy, które w sposób logiczny są od siebie odseparowane. Taki podział wpływa również na zmniejszenie domen rozgłoszeniowych, uporządkowanie ruchu, a przez to większą wydajność sieci [10].

działanie sieci. Aby temu zapobiec wykorzystuje się specjalne protokoły takie jak np. protokół STP.

Zapewnienie nadmiarowości w postaci kilku fizycznych połączeń, nad którymi czuwa protokół drzewa rozpinającego, w niektórych przypadkach nie jest wystarczające, bowiem cały czas występuje ograniczenie maksymalnej prędkości połączenia. W przypadku standardu Fast Ethernet jest to szybkość 100Mb/s. Do komunikacji można również wykorzystać szybsze połączenia, lecz wiąże się to z dodatkowymi kosztami lub wymianą sprzętu sieciowego. W takich przypadkach z powodzeniem można wykorzystać funkcjonalność zwaną EtherChannel.

Jej założenia opierają się na zgrupowaniu do ośmiu fizycznych łączy w jedno logiczne, których prędkość równa jest sumie wszystkich przyłączonych fizycznych połączeń. Jak widać na rysunku 2, połączenie między przełącznikami realizowane jest za pomocą trzech fizycznych połączeń zgrupowanych w jedno logiczne. W tym przypadku prędkość takiego połączenia to teoretycznie 300 Mb/s, jednak pojedynczy host transmitujący dane do przełącznika ESW1 ma prędkość ograniczoną do 100 Mb/s [3].



Rysunek 2. Agregacja połączeń między przełącznikami

Dzieje się tak, ponieważ każdy z przesyłanych pakietów musi umieścić informację o źródłowym i docelowym adresie MAC. Jako, że w zagregowanych połączeniach każdy interfejs ma nadal swój przydzielony adres MAC, to transmisja osiąga prędkość pojedynczego interfejsu. Aby ruch poszczególnych hostów odbywał się różnymi interfejsami wchodzącymi w skład połączenia EtherChannel, algorytm haszujący każdemu z nich przydziela cyfrę z zakresu od 0 do 7. Omawiany algorytm również wpływa na rozdzielenie obciążenia między poszczególnymi połączeniami.

Firma prowadzi własną bazę danych, w której przechowywane są listy CV, życiorysy oraz listy motywacyjne kandydatów poszukujących zatrudnienia.

4.1.1. Lokalizacja

Siedziba MŚP zlokalizowana jest w obrębie jednego trzypiętrowego budynku znajdującego się pod adresem: 00-131 Warszawa, ul. Grzybowska 57/69 lok. 350.

4.1.2. Struktura firmy MŚP

Headhunters 1, 2 – działy prowadzące poszukiwania kandydatów na wybrane stanowiska. Odpowiadają również za nawiązywanie kontaktu z klientami biznesowymi w celu rozpoczęcia lub zakończenia naboru .

Administracja – jej zadaniem jest zapewnienie i organizacja sprawnej pracy firmy, kierowanie i nadzorowanie pracy działów Headhunters 1, 2, rejestrowanie zarządzeń i ustaleń szefa MŚP oraz prowadzenie wykazu realizowanych prac.

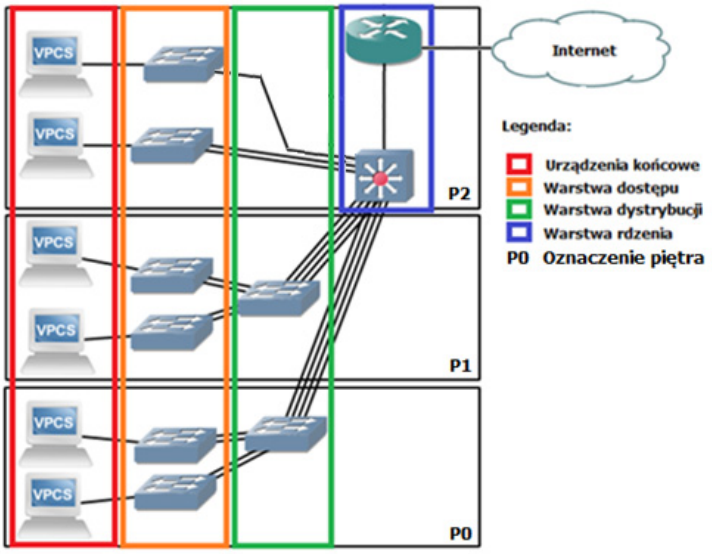
Finanse – dział ten odpowiada za dokumentowanie w formie elektronicznej i pisemnej przychodów i wydatków z budżetu MŚP, konsultacja wydatków z szefem i organizowanych inwestycji MŚP oraz prowadzenie księgowości MŚP.

Kadry – dział zajmujący się zarządzaniem personelem pracującym na potrzeby MŚP poprzez prowadzenie dokumentacji w zakresie szkolenia, zatrudniania i zwalniania pracowników.

IT – dział, który zajmuje się utrzymaniem infrastruktury sieciowej, nadzorowaniem systemów wspierających pracę pracowników MŚP, przygotowaniem sprzętu do pracy (instalacją i konfiguracją oprogramowania), prowadzeniem dokumentacji prowadzonych prac oraz zmian zachodzących w infrastrukturze sieciowej .

4.2. Struktura okablowania budynku i zainstalowane wyposażenie

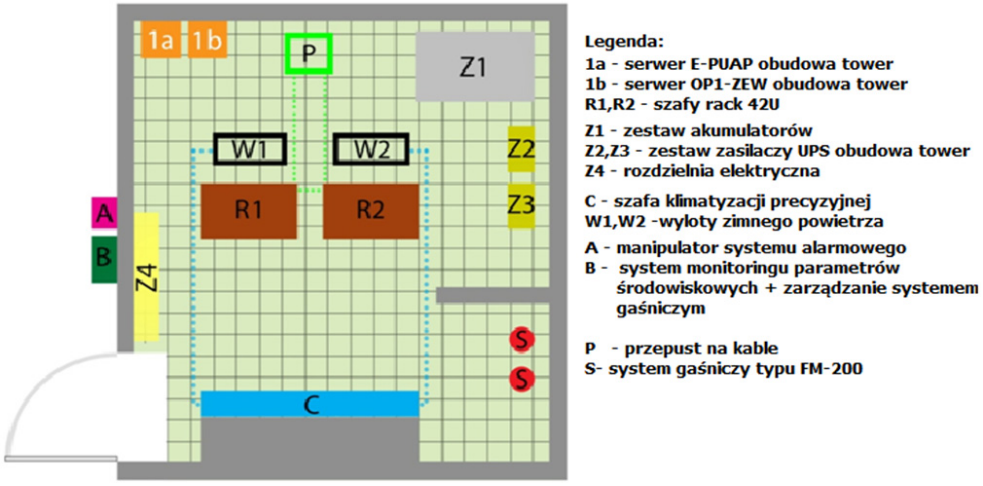
W omawianym budynku istnieje już infrastruktura kablowa, która ma zostać zaimplementowana w projekcie sieci komputerowej. Opiera się ona na nieekranowanej skrętce miedzianej UTP kategorii 6, dostosowanej do przesyłania danych z prędkością 1Gb/s. Konstrukcja okablowania bazuje na trójwarstwowym schemacie, który przedstawia tabela 3.



Rysunek 4. Schemat podziału okablowania

4.2.1. Serwerownia

Pomieszczenie zagospodarowane na potrzeby serwerowni zlokalizowane jest na piętrze nr 2 i odpowiednio przystosowane. Schemat serwerowni zawiera rysunek 5, a systemy wspomagające pracę serwerowni i jej wyposażenie przedstawia tabela 4.



Rysunek 5. Schemat pomieszczenia serwerowni

Instalacja alarmowa oparta jest na czujnikach ruchu (PIR), styczniku informującym o nieuprawnionym otwarciu drzwi oraz panelu manipulatora służącemu do aktywacji i dezaktywacji systemu.

4.2.2. Sprzęt sieciowy

Firma MŚP na potrzeby stworzenia infrastruktury sieciowej zakupiła sprzęt sieciowy firmy Cisco. Sprzęt ten został wybrany z uwagi na swoją niezawodność, wysoką wydajność, łatwość w konfiguracji oraz wsparcie producenta w zakresie serwisu i oprogramowania. Liczbę zakupionego sprzętu i jego rodzaj przedstawia tabela 5.

Tabela 5. Zakupiony sprzęt sieciowy

Nazwa /model	Opis
Przełącznik Cisco C2960	5 x przełącznik posiadający 24 porty FastEthernet oraz 2 porty GigabitEthernet i 2x przełącznik posiadający 48 porty FastEthernet oraz 2 porty GigabitEthernet.
Przełącznik Cisco C3560	1 x przełącznik warstwy trzeciej posiadający 24 porty FastEthernet oraz 2 porty GigabitEthernet.

4.3. Wytyczne do konfiguracji sieci

W celu zapewnienia dostępu do sieci, lokalny operator internetowy dostarczył dwa publiczne adresy IP oraz router. Komunikacja z siecią ISP ma odbywać się przez adres IP 91.189.56.251, natomiast adres 91.189.57.248 pozostaje do indywidualnego wykorzystania. Operator internetowy zastrzega sobie wyłączne prawo do konfiguracji tego urządzenia.

Przedmiotem wdrożenia w myśl podpisanej z MŚP umowy zostaje stworzenie projektu trójwarstwowej struktury sieci opartej wyłącznie o zakupiony sprzęt.

Administrator lokalny w kolejnych etapach rozbudowy infrastruktury planuje dołożenie w warstwie rdzenia zaporę sieciową Cisco ASA 5506 dlatego wymaga, aby na przełączniku Cisco C3650 utworzona została sieć o adresie IP 192.10.0.252 z maską 255.255.255.252 na interfejsie Fast Ethernet 0/21. Ponadto ma ona być

Tabela 7. Nazewnictwo wykorzystywane w infrastrukturze sieci

Symbol	Typ urządzenia	Opis
C_ML_SW_[X]	Przełącznik L3	Urządzenia będące w warstwie rdzenia posiadające funkcję przełączania L3.
C_SW_[X]	Przełącznik L2	Urządzenia będące w warstwie rdzenia posiadające funkcję przełączania L2.
C_T[X]	Terminal	Terminal do zarządzania infrastrukturą sieciową.
DS_SW_[X]	Przełącznik	Urządzenia będące w warstwie dystrybucyjnej.
AC_SW_[X]	Przełącznik	Urządzenia będące w warstwie dostępowej.
SE[X]_[N]	Serwery	Serwer nie wysyłający dane poza sieć lokalną.

[X] – symbol oznaczający kolejny numer urządzenia, zaczynając od cyfry 1.

[N] – Dowolny ciąg znaków

Tabela 8. Podział sieci wirtualnych i wykaz sprzętu

Nr	Wydział/Nazwa VLAN	Adresacja
21	Headhunters1	IP 192.10.21.0 /24
22	Headhunters2	IP 192.10.22.0 /24
31	Administracja	IP 192.10.31.0 /24
41	Finanse	IP 192.10.41.0/24
42	Kadry	IP 192.10.42.0/24
50	SE1	IP 192.10.50.253 /30
51	SE2	IP 192.10.51.253 /30
52	SE3	IP 192.10.52.253 /30
53	SE4	IP 192.10.53.253 /30
70	IT i NATIVE	IP 192.10.70.100 /24
80	BLACK_HOLE	

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z
Switch(config)#hostname C_ML_SW_1
C_ML_SW_1(config)#line console 0
C_ML_SW_1(config-line)#exec-timeout 0 0
C_ML_SW_1(config-line)#privilege level 15
C_ML_SW_1(config-line)#logging synchro
C_ML_SW_1(config-line)#password ad-C_ML_SW_1(2018)
C_ML_SW_1(config-line)#login
C_ML_SW_1(config-line)#exit
C_ML_SW_1(config)#service password-encryption
```

Rysunek 6. Konfiguracja nazw i linii konsolowej dla przełącznika warstwy rdzeniowej

4.4.2. Konfiguracja zdalnego połączenia SSH

W celu ułatwienia zarządzania i konfiguracji sieci skonfigurowano zdalne połączenia z przełącznikami za pomocą protokołu SSH. Jest to obecnie najbezpieczniejszy sposób połączenia, jaki oferuje to urządzenie sieciowe.

W pierwszym etapie tworzony jest nowy użytkownik „AD001MSP" z najwyższymi dostępnymi uprawnieniami oraz hasłem szyfrowanym za pomocą algorytmu MD5. Później ustalana jest nazwa domeny niezbędna do wygenerowania klucza publicznego, po czym generowany jest sam klucz o długości 2048-bitów, czyli najwyższą oferowaną przez ten przełącznik.

W dalszej części konfiguracji ustawiana jest wersja protokołu SSH, która będzie używana przy zdalnym połączeniu oraz czas oczekiwania długości 90 sekund po trzykrotnej nieudanej próbie logowania.

Następnie ustawiany jest dla wszystkich dostępnych linii wirtualnych czas bezczynności długości 5 minut oraz wymuszane są połączenia przy pomocy protokołu SSH dla całego ruchu wchodzącego i wychodzącego.

Dalsze polecenia odpowiadają za uwierzytelnianie użytkownika odbywające się za pomocą danych lokalnie zapisanych na przełączniku oraz wyświetlenie komunikatu informacyjnego.

Rolę klientów tak skonfigurowanej domeny VTP będą pełniły wszystkie przełączniki w warstwie dystrybucyjnej i dostępowej. Na chwilę obecną w sieci nie będzie żadnego przełącznika działającego w trybie transparentnym.

Podczas ostatecznego wdrożenia ruch VTP zostanie jeszcze dodatkowo ograniczony mechanizmem VTP Pruning. Dzięki temu zmniejszy się wykorzystanie łączy i propagacja pakietów wysyłanych przez protokół VTP do obszarów, w których nie występują hosty z danej sieci VLAN.

4.4.4. Tworzenie VLAN

Sieci VLAN zostały utworzone i nazwane według wytycznych zawartych w tabeli 9. Pracownicy każdego z wydziałów zostaną przydzieleni do swojej sieci wirtualnej. Dzięki takiej konfiguracji zapewniona jest separacja użytkowników i serwerów oraz zmniejszone domeny rozgłoszeniowe.

Ze względów bezpieczeństwa domyślny VLAN1 został wyłączony.

```
C_ML_SW_1(config)#vlan 22
C_ML_SW_1(config-vlan)#name Headhunters2
C_ML_SW_1(config-vlan)#vlan 21
C_ML_SW_1(config-vlan)#name Headhunters1
C_ML_SW_1(config-vlan)#vlan 31
C_ML_SW_1(config-vlan)#name Administracja
C_ML_SW_1(config-vlan)#vlan 41
C_ML_SW_1(config-vlan)#name Finanse
C_ML_SW_1(config-vlan)#vlan 42
C_ML_SW_1(config-vlan)#name Kadry
C_ML_SW_1(config-vlan)#vlan 50
C_ML_SW_1(config-vlan)#name SE1
C_ML_SW_1(config-vlan)#vlan 51
C_ML_SW_1(config-vlan)#name SE2
C_ML_SW_1(config-vlan)#vlan 52
C_ML_SW_1(config-vlan)#name SE3
C_ML_SW_1(config-vlan)#vlan 53
C_ML_SW_1(config-vlan)#name SE4
C_ML_SW_1(config-vlan)#vlan 70
C_ML_SW_1(config-vlan)#name NATIVE
C_ML_SW_1(config-vlan)#vlan 80
C_ML_SW_1(config-vlan)#name BLACK_HOLE
C_ML_SW_1(config-vlan)#exit
C_ML_SW_1(config)#interface vlan 1
C_ML_SW_1(config-if)#shutdown
C_ML_SW_1(config-if)#exit
```

Rysunek 9. Tworzenie sieci wirtualnych

```
C_ML_SW_1(config)#interface range fastEthernet 0/24
C_ML_SW_1(config-if-range)#switchport access vlan 50
C_ML_SW_1(config-if-range)#switchport mode access
C_ML_SW_1(config-if-range)#switchport port-security mac-address sticky
C_ML_SW_1(config-if-range)#switchport port-security violation restrict
```

Rysunek 11. Konfiguracja interfejsów dostępowych przełącznika warstwy rdzeniowej

Na omawianym urządzeniu sieciowym w celu komunikacji z zaporą ogniową, skonfigurowano port numer 21 na przełączniku Cisco 3560. Dzięki temu istnieje możliwość routowania pakietów.

```
C_ML_SW_1(config)#interface fastEthernet 0/21
C_ML_SW_1(config-if)#no switchport
C_ML_SW_1(config-if)#ip address 192.10.0.253 255.255.255.252
```

Rysunek 12. Konfiguracja interfejsu do routingu pakietów

Wszystkie interfejsy, które nie są aktualnie wykorzystywane, zostały wyłączone i przypisane do VLAN 80. Dzięki temu nie ma możliwości, aby hosty w sposób przypadkowy dostały się do wirtualnej sieci domyślnej, która jest zastrzeżona jedynie dla administratora i urządzeń sieciowych.

```
C_ML_SW_1(config)#interface range fastEthernet 0/11-19,
gigabitEthernet 0/2
C_ML_SW_1(config-if-range)#switchport access vlan 80
C_ML_SW_1(config-if-range)#switchport mode access
C_ML_SW_1(config-if-range)#shutdown
C_ML_SW_1(config-if-range)#exit
```

Rysunek 13. Konfiguracja nieprzydzielonych portów

4.4.6. Konfiguracja STP

Kierując się wytycznymi przekazanymi przez administratora na przełączniku musi być skonfigurowany protokół Rapid-PVST. Dzięki niemu skróci się czas osiągania zbieżności sieci, co jest szczególnie istotne np. w czasie awarii.

Na rysunku 14 przedstawiono etapy ustawiania protokołu STP dla poszczególnych portów przełącznika. Na początku ustawiony został typ wykorzystanego protokołu „Rapid-PVST", po czym przydzielony jest zakres sieci wirtualnych, dla których

przeznaczone dla jednego hosta mogą być wysłane przez różne interfejsy wchodzące w skład zagregowanych połączeń.

W przypadku połączeń dla serwerów przyłączonych do konfigurowanego urządzenia ustawienie portów będzie przebiegało jak na rysunku 15.

```
C_ML_SW_1(config)#interface fastEthernet 0/24
C_ML_SW_1(config-if)#spanning-tree guard root
C_ML_SW_1(config-if)#spanning-tree bpduguard enable
C_ML_SW_1(config-if)#switchport nonegotiate
C_ML_SW_1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/24 but will only
have effect when the interface is in a non-trunking mode.
```

Rysunek 15. Konfiguracja STP dla połączeń „access" dla przełącznika warstwy rdzeniowej

Port działa domyślnie w trybie dostępowym, lecz na wypadek jego zmiany i podłączenia innego przełącznika wprowadzona została ochrona przed przebudową drzewa STP. Ponadto wprowadzono również mechanizm bpduguard chroniący przed pojawieniem się ramek BPDU na tym interfejsie oraz wyłączono auto negocjacje połączeń trunk, którą zapewnia protokół DTP. Następna pozycja, czyli „spanning-tree portfast" skraca czas konfiguracji portu. Powinno się ją wykorzystywać jedynie w połączeniach z hostami końcowymi w trybie dostępowym „access", o czym świadczy komunikat na poniższym rysunku.

4.4.7. Przydzielanie adresów IP

Aby możliwe było przełączanie ruchu w warstwie sieci, konieczne jest przypisanie adresów sieciowych do VLAN-ów oraz wydanie na przełączniku polecenia „ip routing".

Dla urządzeń końcowych w celu zabezpieczenia przed nieuprawnionym dostępem do sieci ustawiono mechanizm chroniący porty poprzez przypisanie adresu MAC pierwszego podłączonego urządzenia. Funkcja ta jest wykorzystana z uwagi na wewnętrzne procedury dopuszczające stosowanie takiego rozwiązania. Jeżeli do portu z tak zapamiętanym adresem sprzętowym zostanie podłączona inna stacja wówczas połączenie zostanie przerwane, a stosowny komunikat wyświetli się w konsoli przełącznika. Za takie działanie odpowiada komenda „violation restrict". Dodatkowo na wypadek nieumyślnego przełączenia portów w tryb trunk dodano mechanizm ochrony drzewa STP.

Kolejne polecenia dotyczą protokołu RSTP ustawiając szybsze nawiązanie połączenia za pomocą funkcji „portfast" oraz zabraniając transmisji ramek BPDU do urządzeń końcowych. Jest to dobry sposób zapobiegający wpięciu nieautoryzowanego przełącznika do infrastruktury sieciowej.

```
AC_SW_1(config)#interface range fastEthernet 0/1-4
AC_SW_1(config-if-range)#switchport mode access
AC_SW_1(config-if-range)#switchport access vlan 21
AC_SW_1(config-if-range)#switchport port-security mac-address sticky
AC_SW_1(config-if-range)#switchport port-security violation restrict
AC_SW_1(config-if-range)#spanning-tree guard root
AC_SW_1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast will be configured in 4 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.
AC_SW_1(config-if-range)#spanning-tree bpduguard enable
AC_SW_1(config-if-range)#no shutdown
```

Rysunek 18. Konfiguracja interfejsów dostępowych dla przełączników warstwy dostępowej

Interfejsy przesyłające ruch VLAN-ów podobnie jak w przypadku przełącznika warstwy trzeciej są w trybie trunk, lecz na tym etapie nie trzeba już określać sposobu enkapsulacji. Do wszystkich przełączników w tej warstwie przypisane są adresy IP wchodzące w skład wirtualnej sieci o numerze 70. Dzięki temu możliwe jest zdalne zarządzanie.

Bibliografia

[1] J. Hofmokl, *Internet jako nowe dobro wspólne*, Wydawnictwa Akademickie i Profesjonalne, 2009.

[2] A. Józefiok, *CCNA 200-120. Zostań administratorem sieci komputerowych CISCO*, Wydawnictwo Helion, 2015.

[3] G.A. Donahue, *Wojownik sieci*, Wydawnictwo Helion, 2012.

[4] Ch.E. Spurgeon, J. Zimmerman, *Ethernet. Biblia administratora*, Wydawnictwo Helion, 2014.

[5] http://www.ciscopress.com/article.asp?p=357103&seqNum=4

[6] http://www.tp-link.com/pl/products/details/cat-5072_TL-SG1008D.html

[7] J. Gawron, *Diagnostyka przełączników Catalyst czyli Tips & Tricks by Cisco TAC*, Materiały z konferencji naukowej PLNOG 2015, Zakopane, 2015.

[8] CISCO, *CCNA Routing and Switching*: *Podstawy routingu i przełączania*, Kurs Sisco NetAcademy [Online]

[9] J. Menga, *CCNP Self-Study CCNP Practical Studies: Switching*, Cisco Press, 2004.

[10] A. Józefiok, *Budowa sieci komputerowych na przełącznikach i routerach Cisco*, Wydawnictwo Helion, 2009.

The Comparison of the Native Function Execution Times for Mobile Application Implemented Using Native and Hybrid Approaches

Abstract

This paper presents the performance evaluation of the mobile native and hybrid applications. The comparison of application performance was carried out assuming a native function execution time (e.g. an access to the hardware, an access to the network, writing or reading files or contacts) as a main criteria.

The measurements were conducted by preparing two functionally identical applications for Android OS, one written in Java language (native methodology) the other written in JavaScript and HTML languages with the aid of PhoneGap bridge (hybrid methodology), that were later used to call selected native functions and measure their execution time. The evaluation was performed for three versions of Android OS in order to have a broader perspective on the analysed issue.

Keywords – Hybrid applications, native applications, Android OS, PhoneGap