Zeszyty Naukowe WWSI, No 19, Vol. 12, 2018, s. 79-108
DOI: 10.26348/znwwsi.19.79

Zastosowanie przełączników we współczesnej infrastrukturze teleinformatycznej

Dariusz Chaładyniak, Paweł Niezgoda*

Warszawska Wyższa Szkoła Informatyki

Abstrakt

Artykuł przedstawia rolę przełączników we współczesnych systemach i sieciach teleinformatycznych. W części wstępnej omówiono klasyfikację przełączników sieciowych, mechanizmy przełączania ruchu ramek ethernetowych oraz procesy segmentacji i nadmiarowości. W części praktycznej przeprowadzono przykładową konfigurację sieci teleinformatycznej o architekturze warstwowej oraz omówiono wybrane mechanizmy bezpieczeństwa przesyłanych danych.

Słowa kluczowe – przełącznik, ramka ethernetowa, metody przełączania ramek, sieci VLAN, bezpieczeństwo

---

* E-mail: dchalad@wwsi.edu.pl, p_niezgoda@poczta.wwsi.edu.pl

Zgłoszono do druku 9 listopada 2018 r.

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

w warstwie dostępowej sieci, gdzie pełnią one rolę pierwszej linii sprzętu, z jakim spotykają się urządzenia końcowe, czyli drukarki, telefony VoIP, ale także zwykłe komputery i serwery. Wśród przełączników poziomu drugiego wyróżniamy dwa podstawowe typy urządzeń, czyli te, którymi można lub nie można zarządzać.

Tabela 1. Funkcjonalność przełączników L2. Opracowanie własne na podstawie [4], [8].

Funkcja	Opis
QoS	Kolejkowanie jest bardzo pomocne w przypadku wykorzystywania w sieci telefonii IP, w której bardziej niż dostarczenie wszystkich danych liczy się czas w jaki zostanie to zrobione. W przełącznikach ta funkcja jest implementowana w znacznie prostszym wydaniu niż na routerach. Sytuacja wygląda nieco inaczej w przypadku urządzeń wielowarstwowych.
STP/RSTP PVST/PVST+ MSTP	Protokoły drzewa rozpinającego odgrywają ważną rolę w budowaniu redundantnych sieci wykorzystujących nadmiarowe połączeń z innymi przełącznikami. Dzięki nim zapobiega się występowaniu, pętli przełączania, której wystąpienie kończy się przeważnie koniecznością restartu urządzenia.
EtherChannel	Agregacja łączy jest często wykorzystywana w celu zwiększenia niezawodności połączenia oraz rozłożenia obciążenia. Ze względu na powszechnie dostępne interfejsy 1 oraz 10 Gb/s coraz rzadziej stosowana.
VLAN	Możliwość utworzenia wirtualnych sieci, a tym samym łączenia urządzeń końcowych w łatwe do identyfikacji i zarządzania grupy, z których każda może mieć przydzieloną inną adresację IP.
SNMP	Protokół zarządzający i nadzorujący urządzenia pracujące w sieci, który potrafi dostarczyć cennych informacji o stanie infrastruktury sieciowej.
RADISU/ TACACS	Możliwość zabezpieczenia urządzeń zgodnie z modelem AAA za pomocą zewnętrznych bazy danych.
Listy ACL	Listy ACL są prostym sposobem na poprawę bezpieczeństwa dzięki możliwości sekwencyjnego filtrowania pakietów pochodzący od urządzeń końcowych jak i innych segmentów sieci. Są prostym sposobem na ograniczenie niechcianego ruchu.
Zarządzanie przez SSH i WWW	Możliwość bezpiecznego połączenia z konsolą i zarządzanie w trybie tekstowym lub po przez wygodny interfejs za udostępniany za pomocą strony internetowej.

Sprzęt niezarządzany to urządzenia niewielkich rozmiarów (mniejsze niż 1U), zasilane przez zasilacze 12/24V, które charakteryzują się niezwykłą prostotą obsługi dzięki wbudowanemu mechanizmowi *plug & play* pozwalającemu na korzystanie

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

modelu ISO/OSI, poza standardowym przełączaniem można instalować w nich moduły odpowiadające za [3]:

- łączność z sieciami WAN,
- zaporę ogniową,
- wykrywanie włamań (IDS),
- analizę ruchu sieciowego.

Aby wykorzystać wszystkie możliwości tych urządzeń inżynierowie poza mnogością dostępnych funkcji zwiększyli także prędkość magistrali łączących poszczególne moduły i dodali mechanizmy redundancji np. dodatkowe zasilacze, chłodzenia czy moduły sterowania.

Z uwagi na swoje wymiary, koszt oraz możliwości urządzenia tego typu znajdują zastosowanie w średniej lub dużej wielkości sieciach oraz centrach przetwarzania i dystrybucji danych. Podstawowe cechy wpływające na wybór urządzeń wielowarstwowych to między innymi [3], [4]:

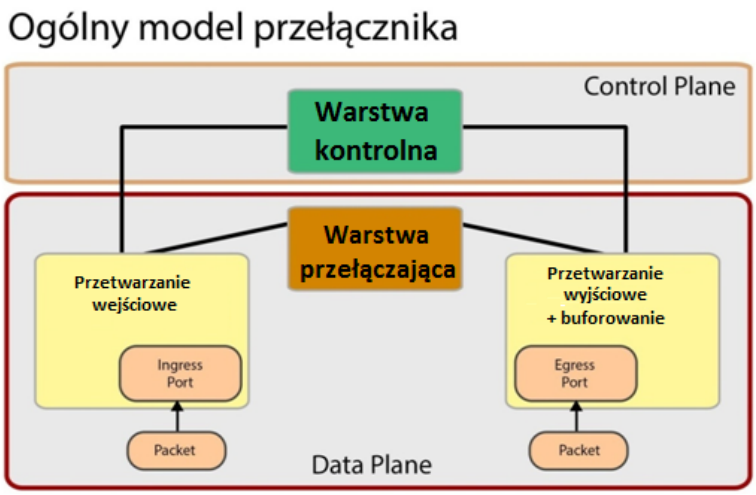
1. gwarancja ciągłości działania
    - wysoki współczynnik MTBF,
    - szybka zbieżność interfejsów,
    - architektura nieblokowana pod pełnym obciążeniem,
    - aktualizacja oprogramowania w trakcie pracy.
2. modularność
    - wymiana modułów sprzętowych w trakcie pracy urządzenia,
    - modułowa budowa oprogramowania,
    - uniwersalne porty sieciowe (Unified port).

Planując wdrożenie takiego przełącznika trzeba mieć też na uwadze zapewnienie wystarczającej ilości miejsca w szafie rack (nawet do 21 U), odpowiednio wydajnego przyłącza zasilania (złącza typu IEC-320 C20) oraz odpowiednio poprowadzonego okablowania, które nie utrudni lub uniemożliwi cyrkulację powietrza. Po spełnieniu powyższych wymagań otrzymujemy jednak wydajną platformę, na której można skonsolidować wiele usług, serwisów i protokołów, przy jednoczesnym zmniejszeniu liczby urządzeń w sieci [3].

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

nazywane jest przełączaniem w warstwie (*ang. Control Plane)* i nie jest ono pożądane z uwagi na małą wydajność i obciążenie procesora [7].

2.2. Tryby przekazywania pakietów L2

W przełącznikach na przestrzeni lat rozwinęły się różne metody przełączania ramek. Ich rozwój był w dużej mierze napędzany rozwojem technologii oraz zapotrzebowaniem na coraz większe przepustowości interfejsów. W związku z tym wśród rozwiązań firmy Cisco wyodrębniły się trzy podstawowe metody, które zostały przedstawione w tabeli 2.

Tabela 2. Metody przełączania ramek. Opracowanie własne na podstawie [4], [5], [9].

Metoda	Opis
Store-and-forward	Metoda polega na odebraniu od hosta całej przesyłanej przez niego ramki i umieszczeniu jej w buforze, po czym następuje wyliczenie sumy kontrolnej. Następnie wyliczona suma jest porównywana z wartością umieszczoną w polu FCS i sprawdzana jest długość ramki. W końcowym etapie przełącznik wyszukuje w tablicy MAC adres odbiorcy i dowiązany do niego numer interfejsu, na który należy przesłać ramkę. Opcjonalną czynnością może być filtrowanie przesyłanych danych oraz inne operacje modyfikujące przesyłaną ramkę. Jeżeli podczas procesu weryfikacji przełącznik znajdzie uszkodzoną ramkę (zły rozmiar lub błędne pole FCS), zostanie ona odrzucona. Takie działanie pozwala oszczędzać wykorzystanie dostępnego pasma transmisyjnego, ale generuje dodatkowe opóźnienia związane z liczbą operacji wykonywanych na przełączanej ramce. Metoda ta ma również zastosowanie, kiedy przełączanie następuje między interfejsami pracującymi z różnymi prędkościami (Fast Ethernet/ Gigabit Ethernet).
Cut-through/ Fast forward	Metoda pozwalająca na znaczne skrócenie czasu potrzebnego do przełączenia. Dzieje się tak, ponieważ przesłana do przełącznika ramka nie musi zostać odczytana w całości oraz nie jest wymagane obliczenie sumy kontrolnej dla ramki. Domyślnie operacja przełączania w tym przypadku jest realizowana zaraz po odczytaniu docelowego adresu MAC. Może się jednak zdarzyć, że przełącznik w celu wykonania dodatkowych operacji odczyta również pozostałe informacje z ramki np. docelowy MAC i typ ramki. Podobna sytuacja ma miejsce w metodzie store-and-forward z tą jednak różnicą, że w omawianej metodzie protokół dynamicznie decyduje, jaką część ramki musi odczytać. Z uwagi na brak mechanizmów kontroli wszystkie błędne przesłane ramki będą odrzucone dopiero przez kartę sieciową hosta. W przypadku licznie występujących błędów może to prowadzić do niepotrzebnego obciążenia sieci.

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].

Aby w pełni zaprezentować potrzebę stosowania sieci wirtualnych, posłużmy się następującym przykładem. Załóżmy, że w firmie jest sala konferencyjna, gdzie często przebywają osoby niebędące pracownikami, które potrzebują połączenia z siecią Internet. Administrator nie ma wpływu na to, jaki sprzęt zostanie wpięty do lokalnej sieci, ani jakie oprogramowanie będzie zawierał, dlatego już ze względów bezpieczeństwa korzystne będzie odseparowanie ruchu sieciowego osób trzecich od pracowników i zasobów sieciowych firmy.

Chcąc wykorzystać sieci wirtualne w infrastrukturze sieciowej trzeba posiadać urządzenia i techniki, które zapewnią wzajemną komunikację między wydzielonymi sieciami. Pierwsze obecnie niewykorzystywane rozwiązania wymagały osobnego interfejsu sieciowego na routerze dla każdej utworzonej sieci VLAN. Było to niezwykle kłopotliwe, dlatego opracowano specjalny tryb określany mianem trunk oraz metody znakowania pakietów danej w sieci. Najpopularniejszym obecnie standardem jest IEEE 802.1Q, który zakłada rozszerzenie standardowej ramki Ethernet o dodatkowe informacje, między innymi numer VLAN [2], [8].

3.2. Nadmiarowość w sieciach LAN

Nadmiarowość, zwana też redundancją, jest bardzo istotną cechą, która umożliwia nieprzerwane działanie danej sieci i usług w niej świadczonych nawet w przypadku awarii lub uszkodzenia pewnych jej elementów. Istotne jest, aby już na poziomie projektowym ustalić akceptowalny poziom niezawodności i odpowiednio dobrać rozwiązania redundantne. W dobrze zaprojektowanej sieci wystąpienie awarii powinno być niezauważalne dla zwykłych użytkowników.

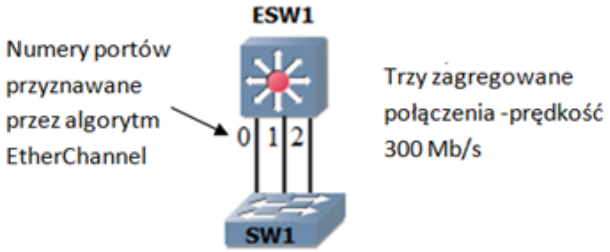
Oczywiście każdy administrator dąży do jak najwyższego współczynnika bezawaryjności swojej sieci, lecz liczba i jakość użytych rozwiązań w dużej mierze zależy od funduszy przeznaczonych w fazie projektowej.

Redundancję można zapewniać przez zdublowane połączenie sieciowe od dostawców ISP, drzewiastą strukturę przełączników, zdublowane karty sieciowe w serwerach lub całe serwery. Najczęściej stosowanym rozwiązaniem jest zdublowanie medium transmisyjnego łączącego urządzenia sieciowe. Jedną z podstawowych praktyk jest zastosowanie nadmiarowych połączeń dla przełączników i routerów. To działanie może jednak doprowadzić do pętli przełączania, a tym samym zakłócić

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.

W przypadku powyższego przykładu rozkład obciążenia poszczególnych interfejsów będzie przedstawiać się następująco: dla połączenia 0 oraz 1 obciążenie powinno wynosić około 37, 5% obciążenia całego łącza, natomiast dla interfejsu 2 będzie to 25%. Dokładny rozkład obciążeń z uwzględnieniem ilości połączeń przedstawia rysunek 3 [3].

Liczba łączy fizycznych	8	7	6	5	4	3	2
1	12,5 %	25%	25%	25%	25%	37,5%	50%
2	12,5 %	12,5 %	25%	25%	25%	37,5%	50%
3	12,5 %	12,5 %	12,5 %	25%	25%	25%	
4	12,5 %	12,5 %	12,5 %	12,5 %	25%		
5	12,5 %	12,5 %	12,5 %	12,5 %			
6	12,5 %	12,5 %	12,5 %				
7	12,5 %	12,5 %					
8	12,5 %						

Rysunek 3. Procentowy rozkład obciążenia łączy EtherChannel [3]

4. Projekt sieci i przykładowa konfiguracja urządzeń

4.1. Charakterystyka firmy MŚP

Firma MŚP w Warszawie zajmuje się profesjonalnym doradztwem personalnym oraz świadczy usługi audytu personalnego z ukierunkowaniem na branżę IT:

1. IT Administratorzy – sieci, systemy, helpdesk, audyt, bazy danych;
2. IT Oprogramowanie – programiści, testerzy, analitycy biznesowi.

Do zadań firmy należy realizowanie projektów związanych z doborem najlepszej kadry na określone specjalistyczne stanowiska. Metodologia pracy oparta jest o bezpośrednie poszukiwanie kandydatów dysponujących umiejętnościami z zakresu IT.

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.

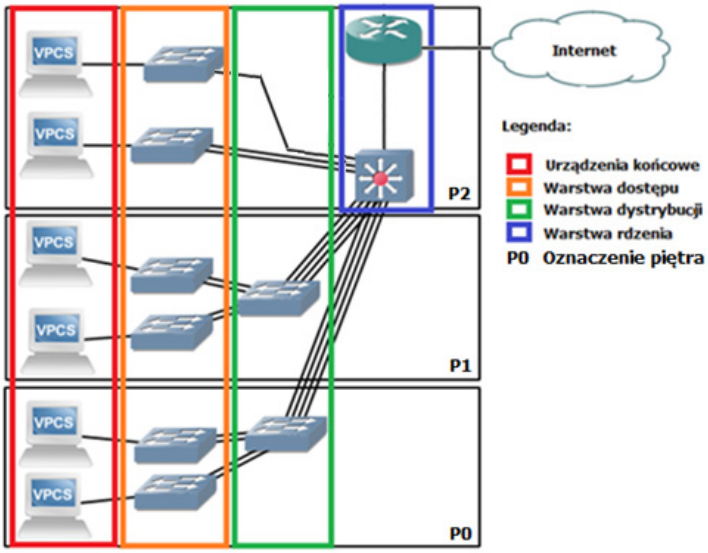
Tabela 3. Struktura okablowania

Nazwa warstwy	Opis
Rdzenia	Główny punkt dystrybucyjny (serwerownia) znajduje się na piętrze nr 2. Tu zbiega się okablowanie całego budynku.
Dystrybucyjna	Okablowanie pionowe zapewniające połączenia między głównym punktem dystrybucyjnym, a pośrednimi punktami rozdzielczymi wykorzystuje po cztery kable miedziane kategorii 6 na punkt rozdzielczy, w przypadku piętra nr 0 i 1, natomiast piętro nr 2 połączone jest za pomocą dwóch kabli.
Dostępu	Okablowanie poziome w tej warstwie zapewnia połączenie gniazd abonenckich z pośrednim punktem rozdzielczym.

Z uwagi na zastosowaną strukturę okablowania, sieć będzie posiadać topologię gwiazdy rozszerzonej. Główny punkt dystrybucji zlokalizowany jest w pomieszczeniu serwerowni, do którego zbiera się okablowanie sieciowe z całego budynku. Przeprowadzone jest ono przepustami technicznymi w aluminiowych korytach kablowych. W takiej formie realizowane są połączenia między serwerownią umieszczoną na piętrze nr 2, a innymi piętrami. Na piętrach numer 0 i 1 z głównego punktu biegną po cztery kable na piętro (warstwa dystrybucyjna). Kable schodzą pionowo przepustem do szaf telekomunikacyjnych a następnie w korytach aluminiowych w suficie podwieszanym rozprowadzone są do pomieszczenia z punktami abonenckimi. Tam z podwieszanego sufitu pionowo do dołu przebiegają koryta natynkowe typu DLP wykonane z aluminium. Między urządzeniami w warstwie dystrybucyjnej a dostępowej doprowadzono dwa kable sieciowe, którymi ma być realizowane połączenie. Schemat podziału okablowania między poszczególnymi warstwami przedstawia rysunek 4.

Zaletą takiego warstwowego rozwiązania jest fakt, iż długość okablowania do wszystkich pomieszczeń nie przekracza 100 metrów, co przekłada się na oszczędności, możliwość prostej rozbudowy i zwiększenia liczby punktów abonenckich.

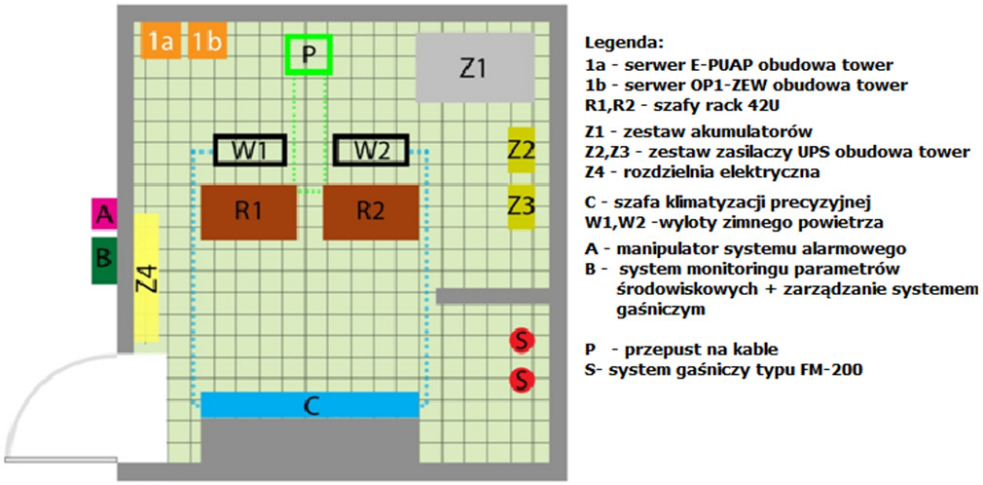
Możliwe jest również odłączenie dowolnego punktu abonenckiego, a w przypadku awarii jednego z punktów dystrybucyjnych odcięte jest jedynie jedno piętro.



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

Tabela 4. Wyposażenie serwerowni

Nazwa	Opis
Listwy zasilania	Listwy dystrybucji zasilania 4x po 5 gniazd typu IEC 320 C13 oraz 1 gniazdo IEC 320 C-19.
System zasilania rezerwowego	2x zasilacz UPS moc 6000W z zestawem akumulatorów 18x 12V/9Ah Złącza: 8x IEC 320 C-13, 1x IEC 320 C19 2x IEC Jumpers (kable do podłączenia dodatkowych baterii), gniazda wejściowe IEC 320 C20.
Szafa rack 42U	2x szafa o wymiarach 800x2000x1000mm, przepusty kablowe w podłodzie, perforowane drzwi przednie i tylne, możliwość demontażu drzwi bocznych, 3 dedykowane półki, dedykowany system zarządzania okablowaniem.
Zestaw baterii do zasilaczy UPS	10 x akumulator AGM 12V o pojemności 200Ah.
System chłodzenia	Chłodzenie pomieszczenia oparte o szafę klimatyzacji precyzyjnej w konfiguracji z nawiewem dołem (wykorzystana podłoga techniczna i utworzone kanały powietrzne).
System gaśniczy	W skład systemu wchodzą elementy wczesnego ostrzegania oraz gaśnicze, oparte na technice gaszenia gazem naturalnym typu „FM-200”.
System alarmowy	W skład systemu wchodzą czujki ruchu, styczniki zamontowane na drzwiach, zamek magnetyczny otwierany za pomocą manipulatora lub panelu wewnątrz serwerowni.
Rozdzielnia elektryczna	Rozdzielnia elektryczna z przyłączem trójfazowym.
Panele krosowe	3x Modułowe panele krosowe o wysokości 2U pozwalające na podłączenie 24 portów z systemem zarządzania kablami.

Na potrzeby chłodzenia serwerowni zainstalowano system oparty o szafę klimatyzacji precyzyjnej z nawiewem zimnego powietrza od dołu. System przeciwpożarowy oparty jest o system gaszenia gazem obojętnym. Dzięki swoim właściwościom nie przewodzi prądu elektrycznego oraz nie powoduje korozji, dzięki czemu jest bezpieczny dla urządzeń sieciowych i innych elementów pomieszczenia serwerowni.

Nadzór nad czynnikami środowiskowymi w serwerowni pełni system, którego sterowanie odbywa się z panelu dotykowego zainstalowanego na zewnątrz 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

trasą domyślną. Pozostałe wytyczne dotyczące konfiguracji zostały przedstawione w tabeli 6.

Tabela 6. Wytyczne administratora sieci

Nazwa	Opis
Nazewnictwo	Zastosować nazewnictwo zgodnie z tabelą 7.
Hasła	Zastosować hasła zgodnie z tabelą 8.
Podsieci	Zastosować podział podsieci zgodnie z tabelą 9. Wszystkie bramy domyślne mają zostać skonfigurowane na adresy IP X.X.X.254.
VLAN	Skonfigurować sieci VLAN zgodnie z tabelą 9.
Routing	Zapewnić routing w warstwie trzeciej za pomocą przełącznika L3.
VTP	Skonfigurować serwer VTP na przełączniku Cisco 3560.
Rapid-PVST	Skonfigurować protokół RSTP tak, aby przełącznik C3560 umożliwił przenoszenie VLAN z zakresu 10-100 oraz pełnił funkcję przełącznika głównego.
EtherChannel	Wykorzystać całe dostępne okablowanie między warstwą rdzenia, a warstwą dystrybucyjną (piętro nr 0 oraz piętro nr 1) po 4 kable oraz między warstwą dystrybucyjną, a dostępową po 2 kable.
Zabezpieczenia	Skonfigurować następujące zabezpieczenia: - przypisać adresy MAC stacji końcowych do przełącznika; - zabezpieczyć sieć przed przebudową drzewa rozpinającego; - odrzucić każdy ruch z nieznanej stacji i wyświetlić stosowne informacje w logach; - skonfigurować na przełącznikach dostęp do linii konsolowej z najwyższym możliwym poziomem uprawnień i zabezpieczyć go za pomocą haseł z szyfrowaniem algorytmem typu 7. Wyłączyć czas bezczynności; - wymusić zdalne połączenia do urządzeń jedynie po protokole SSH, zabezpieczyć je hasłem, ustawić długość sesji na 5 minut oraz przypisać najwyższy możliwy poziom uprawnień; - zabezpieczyć hasłem serwer VTP oraz zdalny dostęp do przełączników; - wszystkie niewykorzystane interfejsy wyłączyć administracyjnie i ustawić w trybie dostępowym, przypisać do VLAN 80 oraz informować o próbie włączenia portu; - ustawić na przełącznikach raportowanie zdarzeń do serwera SYSLOG skonfigurowanego pod adresem IP 192.10.52.253.

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	

Tabela 9. Dane do logowania na urządzeniach sieciowych

Typ urządzenia	Typ połączenia	Login	Hasło
Przełącznik	Konsola		ad-[Nazwa urządzenia](2018)
	SSH	AD001MSP	#$[Nazwa urządzenia]$#2018
	VTP Serwer/Client	MSP	#$%MSP2018

Wszystkie adresy sieciowe na hostach będą ustawiane w sposób ręczny bez wykorzystania protokołu DHCP. Taki przydział został narzucony odgórnie i związany jest z lokalnymi procedurami firmy MŚP.

4.4. Konfiguracja przełącznika warstwy rdzeniowej

4.4.1. Nadanie nazw i konfiguracja połączenia konsolowego

W celu identyfikacji urządzenia i spełnienia wymagań konwencji nazewniczej skonfigurowano nazwę „C_ML_SW_1”. Dalsze polecenia służą do zabezpieczenia dostępu poprzez linię konsolową. Połączenie takie wymaga fizycznego dostępu do urządzenia. Według wytycznych wyłączono funkcję zamknięcia połączenia konsolowego po upływie standardowego czasu oraz nadano maksymalne uprawnienia użytkownika.

Następne polecenie, czyli „logging synchronous” zapewnia wygodną pracę, ponieważ podczas wpisywania poleceń nie są one przerywane przez komunikaty płynące z systemu IOS. Dalsza część poleceń odpowiada bezpośrednio na ustawienie hasła, wymuszenie jego stosowania, włączenie wyświetlania komunikatu informacyjnego, który skonfigurowany będzie później oraz szyfrowanie.

```
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.

```
C_ML_SW_1(config)#username AD001MSP privilege 15 secret
#$C_ML_SW_1$#2018
C_ML_SW_1(config)#ip domain-name siec.MSP.inside
C_ML_SW_1(config)#crypto key generate rsa
The name for the keys will be: C_ML_SW_1.siec.MSP.inside
Choose the size of the key modulus in the range of 360 to 2048
for your
  General Purpose Keys. Choosing a key modulus greater than 512
may take a few minutes.
How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK]
C_ML_SW_1(config)#ip ssh version 2
*mar 1 0:1:51.312:  %SSH-5-ENABLED: SSH 1.99 has been enabled
C_ML_SW_1(config)#ip ssh authentication-retries 3
C_ML_SW_1(config)#ip ssh time-out 90
C_ML_SW_1(config)#line vty 0 15
C_ML_SW_1(config-line)#exec-timeout 5
C_ML_SW_1(config-line)#transport input none
C_ML_SW_1(config-line)#transport input ssh
C_ML_SW_1(config-line)#transport output none
C_ML_SW_1(config-line)#transport output ssh
C_ML_SW_1(config-line)#login local
C_ML_SW_1(config-line)#exit
```

Rysunek 7. Konfiguracja SSH dla przełącznika warstwy rdzeniowej

4.4.3. Konfiguracja VTP

Przełącznik umieszczony w warstwie rdzeniowej będzie pełnić rolę serwera VTP. Dzięki takiej konfiguracji zarządzanie sieciami VLAN odbywać będzie się jedynie na tym przełączniku. W znaczny sposób przyspieszy to pracę administratora i wyeliminuje ryzyko popełnienia błędu (literówki). W celu automatycznego pobierania ustawień sieci VLAN, przełączniki wykorzystują protokół VTP wersji drugiej. Kolejnym etapem jest podanie nazwy serwera VTP oraz hasła dostępu.

```
C_ML_SW_1(config)#vtp version 2
C_ML_SW_1(config)#vtp mode server
Device mode already VTP SERVER.
C_ML_SW_1(config)#vtp domain MSP
C_ML_SW_1(config)#vtp password #$%MSP2018
```

Rysunek 8. Konfiguracja serwera VTP

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

4.4.5. Konfiguracja interfejsów sieciowych

Jako pierwsze skonfigurowano interfejsy pracujące w trybie trunk, które będą przenosić ruch etykietowany za pomocą protokołu IEEE 802.1Q. W celu wykorzystania dostępnego okablowania użyto mechanizm agregujący połączenia sieciowe.

Za pomocą pierwszego polecenia wybrany jest zakres konfigurowanych portów a następnie określany jest VLAN domyślny (natywny). Przypisany został VLAN 70, ponieważ zastąpił on domyślnie ustawiony VLAN 1. Konfiguracja taka jest istotna ze względów bezpieczeństwa, gdyż istnieją ataki sieciowe, które wykorzystują domyślne ustawienia wszystkich przełączników firmy Cisco.

Kolejne polecenia definiują, jaki zakres sieci wirtualnych ma zostać przesyłany przez interfejsy pracujące w trybie trunk. Dalej określony jest tryb znakowania ramek oraz tryb, w jakim działa interfejs.

Polecenie „channel-group" służy do zdefiniowania nowej grupy zagregowanych portów. Tryb agregacji jest ręcznie ustawiany na „desirable", dzięki czemu przełącznik sam inicjuje utworzenie takiego połączenia. Dla utworzonego w ten sposób kanału również konfigurowany jest protokół znakowania, tryb działania kanału, VLAN domyślny oraz zakres przenoszonych sieci wirtualnych.

```
C_ML_SW_1(config)#interface range fastEthernet 0/1-4
C_ML_SW_1(config-if-range)#switchport trunk native vlan 70
C_ML_SW_1(config-if-range)#switchport trunk allowed vlan 10-100
C_ML_SW_1(config-if-range)#switchport trunk encapsulation dot1q
C_ML_SW_1(config-if-range)#switchport mode trunk
C_ML_SW_1(config-if-range)#channel-group 3 mode desirable
C_ML_SW_1(config-if-range)#int port-channel 3
C_ML_SW_1(config-if)#switchport trunk encapsulation dot1q
C_ML_SW_1(config-if)#switchport mode trunk
C_ML_SW_1(config-if)#switchport trunk native vlan 70
C_ML_SW_1(config-if)#switchport trunk allowed vlan 10-100
```

Rysunek 10. Konfiguracja interfejsów trunk i agregacji portów przełącznika warstwy rdzeniowej

Do omawianego przełącznika podłączone są również serwery świadczące swoje usługi na potrzeby sieci. Poniższa konfiguracja prezentuje interfejs, do którego został podłączony serwer SE1, na którym będzie działał serwer FTP.

```
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

przełącznik będzie pełnił funkcję nadrzędną. Następnie włączono mechanizm „portfast” domyślnie ustawiony na wszystkich portach pracujących w trybie „access”.

```
C_ML_SW_1(config)#spanning-tree mode rapid-pvst
C_ML_SW_1(config)#spanning-tree vlan 10-100 root primary
C_ML_SW_1(config)#spanning-tree vlan 10-100 priority 0
C_ML_SW_1(config-if-range)#spanning-tree portfast default
C_ML_SW_1(config)#interface range fastEthernet 0/1-10
C_ML_SW_1(config-if-range)#spanning-tree portfast disable
C_ML_SW_1(config-if-range)#spanning-tree guard root
C_ML_SW_1(config-if-range)#spanning-tree link-type point-to-point
C_ML_SW_1(config-if-range)#spanning-tree vlan 10-100
C_ML_SW_1(config)#interface port-channel 3
C_ML_SW_1(config-if)#spanning-tree portfast disable
C_ML_SW_1(config-if)#spanning-tree guard root
C_ML_SW_1(config-if)#spanning-tree link-type point-to-point
C_ML_SW_1(config-if)#spanning-tree vlan 10-100
C_ML_SW_1(config-if)#exit
C_ML_SW_1(config)#port-channel load-balance src-dst-ip
```

Rysunek 14. Konfiguracja STP dla połączeń trunk przełącznika warstwy rdzeniowej

Dla wszystkich interfejsów przenoszących sieci VLAN, czyli „interface range FastEthernet 0/1-10”, wyłączony jest tryb „portfast”, gdyż jego wykorzystanie nie jest zalecane na portach pracujących w trybie trunk. Następnie użyty jest mechanizm zapobiegający zmianie struktury drzewa rozpinającego. Jest to istotne z punktu widzenia bezpieczeństwa, gdyż wpięcie do sieci nieautoryzowanego przełącznika nie jest w stanie zaburzyć pracy sieci.

Połączenia wykorzystywane do transportu ramek STP ustawione są w trybie „point to point”. Jest to tryb połączenia zalecany podczas stosowania protokołu RSTP. Zakres przenoszonych sieci wirtualnych ustawiony jest również między 10 a 100.

Analogiczne ustawienia wykorzystuje „port channel 3” oraz inne skonfigurowane na tym przełączniku porty „channel 2 i 4”. Ze względu na obszerny listing został tu przedstawiony jedynie wycinek z konfiguracji. Na koniec w celu optymalizacji działania zagregowanych połączeń i równomiernego rozkładu obciążenia pomiędzy wszystkie dostępne interfejsy ustawiono mechanizm zwany „pory-channel load-balance”.

Przełącznik oferuje kilka trybów rozkładu obciążenia, jednak na potrzeby tego projektu została wybrana opcja „src-dst-ip”. Dzięki takiej konfiguracji pakiety

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”.

```
C_ML_SW_1(config)#interface Vlan21
C_ML_SW_1(config-if)#ip address 192.10.21.254  255.255.255.0
C_ML_SW_1(config-if)#interface Vlan22
C_ML_SW_1(config-if)#ip address 192.10.22.254  255.255.255.0
C_ML_SW_1(config-if)#interface Vlan31
C_ML_SW_1(config-if)#ip address 192.10.31.254  255.255.255.0
C_ML_SW_1(config-if)#interface Vlan41
C_ML_SW_1(config-if)#ip address 192.10.41.254  255.255.255.0
C_ML_SW_1(config-if)#interface Vlan42
C_ML_SW_1(config-if)#ip address 192.10.42.254  255.255.255.0
C_ML_SW_1(config-if)#interface Vlan50
C_ML_SW_1(config-if)#ip address 192.10.50.254  255.255.255.252
C_ML_SW_1(config-if)#interface Vlan51
C_ML_SW_1(config-if)#ip address 192.10.51.254  255.255.255.252
C_ML_SW_1(config-if)#interface Vlan52
C_ML_SW_1(config-if)#ip address 192.10.52.254  255.255.255.252
C_ML_SW_1(config-if)#interface Vlan53
C_ML_SW_1(config-if)#ip address 192.10.53.254  255.255.255.252
C_ML_SW_1(config-if)#interface Vlan70
C_ML_SW_1(config-if)#ip address 192.10.70.254  255.255.255.0
C_ML_SW_1(config-if)#exit
C_ML_SW_1(config)#ip routing
```

Rysunek 16. Przydzielanie adresacji dla sieci VLAN

4.4.8. Ustawienie routingu na przełączniku L3

W przełączniku L3 na potrzeby komunikacji z zaporą sieciową, która ma zostać wprowadzona w drugim etapie budowy sieci skonfigurowano trasę domyślną z adresem IP zapory ogniowej Cisco ASA.

```
C_ML_SW_1(config)#ip route 0.0.0.0 0.0.0.0 192.10.0.254
```

Rysunek 17. Trasa domyślna skonfigurowana na przełączniku

4.5. Konfiguracja przełączników warstwy dostępowej i dystrybucyjnej

Z uwagi na powtarzającą się treść listingów i analogiczną konfigurację zostaną przedstawione jedynie nowe elementy konfiguracji urządzeń warstwy dostępowej i dystrybucyjnej.

Mechanizm VTP na tych urządzeniach skonfigurowano w trybie klienta, który pobiera informacje o skonfigurowanych sieciach VLAN z przełącznika warstwy rdzeniowej.

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.

Podsumowanie

We współczesnej infrastrukturze telekomunikacyjnej przełączniki są nieodzowną częścią prawie każdego projektu sieciowego. Taką sytuację doskonale widać na rynku urządzeń teleinformatycznych, na którym liczni producenci w swojej ofercie dostarczają sprzęt z różnorodnym wachlarzem funkcji dostosowany do potrzeb użytkowników. Dlatego przy tworzeniu współczesnej sieci komputerowej baczną uwagę należy poświęcić na odpowiednie zaprojektowanie infrastruktury sieciowej i dostosowanie jej do własnych wymagań oraz usług jakie będą świadczone przez dane środowisko. Dużą uwagę w momencie projektowania sieci LAN należy przywiązać do przełączników, które mogą pełnić liczne funkcjonalności, a w niektórych przypadkach z powodzeniem zastąpić routery i bezpośrednio przyczynić się do optymalizowania wydajności projektowanej sieci.

W małych niewyspecjalizowanych środowiskach dominują rozwiązania opierające się o warstwę drugą (L2). Rozpatrując większe sieci, przełączniki dodatkowo zyskują na swoim znaczeniu pełniąc funkcję urządzeń szkieletowych czy też łączników pomiędzy sieciami opierającymi się o protokoły np. Ethernet (LAN) lub Fibre Channel (SAN) [5].

Jednymi z najważniejszych cech jakie decydują o silnej pozycji przełączników jako nieodzownego elementu sieci są m.in.:

- szybkość interfejsów (40Gb lub nawet 100 Gb),
- niskie lub bardzo niskie opóźnienia (przekazywanie ruchu sprzętowo – ASIC),
- modularność i elastyczność (możliwość łączenia sieci LAN i SAN),
- bogaty zestaw funkcjonalności (rozwijanie podejścia SDN).

W najbliższym czasie przełączniki raczej nie stracą na swoim znaczeniu, a ich pozycja może się nawet umocnić ze względu na rozwijany trend budowania sieci konwergentnych. Dobrym dowodem na to są coraz częściej wdrażane przez firmę Cisco rozwiązania hiperkonwergentne Hyperflex, łączące w obrębie jednego środowiska zarówno warstwę sieciową jak i serwery oraz macierze dyskowe.

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.

Application of Switches in Contemporary ICT Systems and Networks

Abstract

The article presents the role of switches in contemporary ICT systems and networks. The introductory part presents the classification of network switches, mechanisms of switching the Ethernet frames as well as segmentation and redundancy processes. In the practical part, an exemplary configuration of ICT network with a layered architecture was carried out, and selected security mechanisms of transmitted data were discussed.

Keywords – switch, Ethernet frame, store-and-forward switching, cut-through switching, fragment-free switching, VLAN networks, security