Wyższa Szkoła Biznesu – National Louis University
w Nowym Sączu

Wydział Informatyki
Kierunek: informatyka
Specjalność: sieci komputerowe

Łukasz Pieczka
Numer albumu 7158

Wirtualne sieci LAN

Virtual LAN Networks

Praca licencjacka
Promotor: dr Henryk Telega

Nowy Sącz, 2006

Spis treści:

Streszczenie

Praca podzielona jest na część teoretyczna i praktyczną. Część teoretyczna to sześć pierwszych rozdziałów. W pierwszym rozdziale znajdują się podstawowe informacje o sieciach VLAN. Rozdział drugi koncentruje się na statycznych i dynamicznych sposobach tworzenia sieci wirtualnych uwzględniających różne kryteria. Rozdział trzeci opisuje takie zagadnienie, jak typy połączeń w sieciach VLAN. W rozdziale czwartym skupiono się na protokołach umożliwiających przesyłanie ruchu sieci VLAN w infrastrukturze sieciowej z uwzględnieniem protokołu standardu 802.1Q oraz InterSwitch Link. W rozdziale piątym znajduje się opis oraz przykładowe rozwiązania problemu rutowania ruchu między sieciami VLAN. Rozdział szósty składa się z dwóch wątków, pierwszy z nich to protokoły automatyzacji konfiguracji sieci VLAN takie jak VTP oraz GVRP, wątek drugi to opis przesyłania ruchu sieci wirtualnych na duże odległości z użyciem mechanizmu LANE w sieciach ATM. Rozdział VII to część praktyczna zawierająca postawienie problemu zaprojektowania infrastruktury sieciowej z wykorzystaniem sieci wirtualnych i przykładowe rozwiązanie tego problemu wraz z projektem sieci i opisem jej konfiguracji.

Wstęp

Tematem mojej pracy są wirtualne sieci LAN. Wybrałem ten temat, ponieważ uważam go za bardzo ciekawy i szczególnie ważny dla osoby specjalizującej się w sieciach komputerowych. Poza tym, muszę niestety przyznać, że moja dotychczasowa wiedza z tego zakresu była bardzo powierzchowna i chciałem to zmienić. Dzięki napisaniu tej pracy, poznałem szczegółowo wiele interesujących zagadnień dotyczących sieci wirtualnych i, co najważniejsze, zdobytą wiedzę jestem w stanie z powodzeniem zastosować w praktyce.

Celem pracy jest przedstawienie mechanizmu wirtualizacji w sieciach LAN, z uwzględnieniem jej najważniejszych elementów w technologii Ethernet oraz wykonanie projektu będącego ich praktycznym zastosowaniem. Początek części teoretycznej skupia się wokół informacji wstępnych, które mają na celu pomóc w zrozumieniu podstaw funkcjonowania sieci VLAN. W pracy postarano się by przedstawić różnorodność sposobów implementacji sieci wirtualnych, ze szczególnym naciskiem na najpopularniejsze mechanizmy tworzenia sieci dynamicznych. Dość dogłębnie zostało także przedstawione zagadnienie dotyczące przesyłania ruchu różnych sieci VLAN między przełącznikami w obrębie jednej infrastruktury sieciowej oraz kilku połączonych ze sobą na odległość. Zakończenie części teoretycznej to omówienie mechanizmów automatyzacji tworzenia sieci VLAN oraz usprawniania ich działania. Część praktyczna skupia się na zaprojektowaniu oraz wykonaniu statycznych jak i dynamicznych sieci VLAN w infrastrukturze sieciowej przedsiębiorstwa, które wykorzystują mechanizmy opisane w części teoretycznej pracy.

Rozdział I Podstawowe informacje

Pierwsze sieci komputerowe pojawiły się około pół wieku temu. Od tego czasu skok technologiczny sprawił, że stały się one niemal tak powszechne i naturalne jak telefony w naszych domach. Obecnie sieci komputerowe są podstawowym narzędziem wykorzystywanym w biznesie oraz różnego rodzaju instytucjach. To właśnie w tym obszarze powstaje większość dużych sieci nazywanych często korporacyjnymi. Duże sieci dają firmom ogromną zaletę, jaką jest możliwość połączenia wszystkich działów i pracujących tam ludzi w jedną komunikującą się ze sobą całość. Poprawia to wydajność i jakość pracy, ale powoduje też ogromne problemy w zarządzaniu takimi sieciami. W dużych korporacjach, gdzie wciąż muszą ze sobą współpracować setki, a nawet tysiące komputerów administracja siecią komputerową to wielkie wyzwanie. Trzeba zadbać o takie aspekty jak wydajność, skalowalność, a przede wszystkim bezpieczeństwo oraz utrzymywać wydatki na racjonalnym poziomie. Dla osiągnięcia tak postawionego celu powstało wiele różnych rozwiązań sieciowych, a jednym z nich są właśnie wirtualne sieci LAN.

1.1 Czym są wirtualne sieci LAN

Wirtualna sieć LAN (ang. VLAN – Virtual LAN) jest to grupa urządzeń w jednej lub większej liczbie połączonych ze sobą sieci LAN, która jest skonfigurowana w ten sposób, że wszystkie urządzenia należące do tej sieci VLAN mogą się ze sobą komunikować tak jakby były wpięte razem do jednego przełącznika (ang. *switch*) i odseparowane od reszty sieci. Dzieje się tak, mimo że w rzeczywistości znajdują się w różnych segmentach LAN, które często są od siebie bardzo oddalone. Uzyskanie takiego efektu jest możliwe, ponieważ wirtualne sieci LAN są strukturami logicznymi zbudowanymi na istniejącej infrastrukturze fizycznej i są od niej niezależne.

1.2 Spojrzenie z perspektywy historii

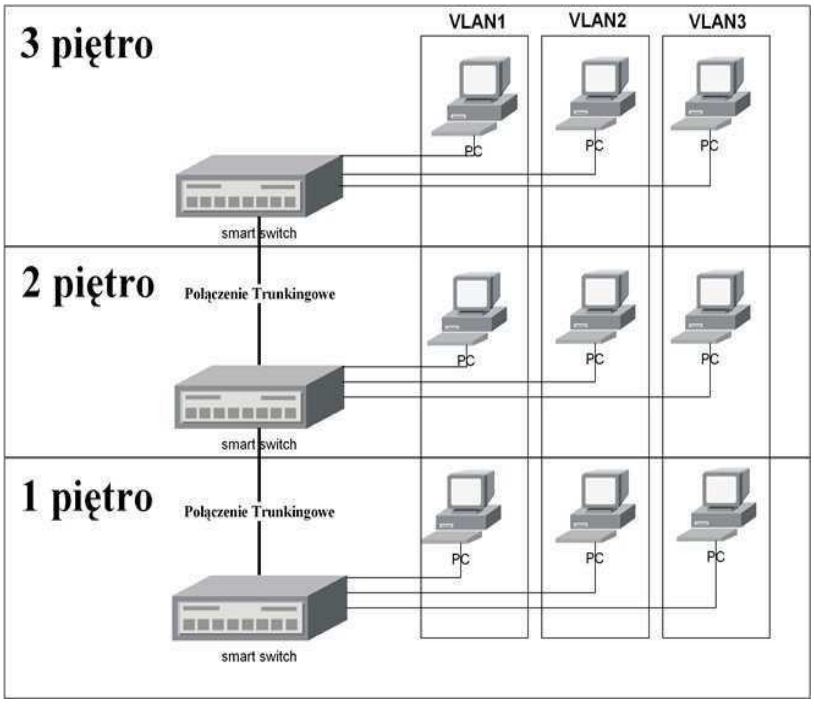
Wirtualne sieci LAN zaczęły pojawiać się w sieciach komputerowych na początku lat 90’ ubiegłego stulecia. Wtedy to firmy zaczynały wymieniać swój przestarzały sprzęt sieciowy, oparty głównie na koncentratorach (ang. hub), dwuportowych mostach (ang. *bridge*) i ruterach (ang. *router*). Podstawowym problemem w starych sieciach były

koncentratory i związane z nimi domeny kolizyjne, które uniemożliwiały wpięcie do jednego segmentu więcej niż 100 komputerów bez używania mostu. Problem ten rozwiązano zastępując je przełącznikami, które oprócz rozwiązania problemu kolizji (każdy port to oddzielna domena kolizyjna) dają dodatkowo dużo większą przepustowość (przepustowość nie dzieli się na wszystkie porty urządzenia tak jak w koncentratorach). Kiedy wprowadzono przełączniki segmenty sieci zaczęły się powiększać. Nie było to już 100, ale na przykład 500 komputerów. W wyniku takich działań bardzo rozrosły się domeny rozgłoszeniowe, które mógł ograniczyć tylko ruter. Dlatego, jeżeli chciano mieć więcej mniejszych, wydajniejszych i łatwiej zarządzanych segmentów musiano używać większej liczby ruterów, co generowało dosyć duże koszty. Jednak producenci sprzętu sieciowego szybko zaproponowali alternatywne rozwiązanie tego problemu, rozwiązaniem tym były wirtualne sieci LAN (VLAN), które nie dzieląc sieci fizycznie dzieliły ją logicznie na wiele domen rozgłoszeniowych. Stało się to możliwe głównie dzięki inteligentnym przełącznikom, które mają możliwość dzielenia segmentów sieci na poziomie warstwy trzeciej modelu OSI (warstwa sieciowa , ang. *network layer*) i nie pozwalają by ruch z jednej sieci VLAN przedostał się do innej. Aby możliwe było przekazywanie danych między sieciami VLAN niezbędny jest do tego ruter.

1.3 Zalety stosowania wirtualnych sieci LAN

Wirtualne sieci LAN posiadają kilka bardzo istotnych zalet, które zaważyły na ich szerokim stosowaniu przede wszystkim w dużych sieciach korporacyjnych. Stosowanie sieci VLAN bardzo poprawia wydajność sieci. Ma to szczególne znaczenie w sieciach z dużą ilością ruchu rozgłoszeniowego (ang. *broadcast*) i grupowego (ang. *multicast*). Rozwiązanie takie pozwala na odseparowanie urządzeń, dla których ruch ten jest przeznaczony, od reszty i przez to redukowanie niepotrzebnego krążenia pakietów. Inna ważną cechą sieci VLAN, która ma duże znaczenie dla poprawy parametrów sieci jest stosowanie inteligentnych przełączników zamiast ruterów do budowania domen rozgłoszeniowych. Rutery, ze względu na przeprowadzanie dość skomplikowanych operacji, powodują znacząco większe opóźnienia w przesyłaniu przychodzących pakietów niż przełączniki. Następną i chyba najważniejszą cechą sieci VLAN jest możliwość logicznego grupowania użytkowników sieci niezależnie od ich fizycznego położenia. Firmy dzięki sieciom VLAN mogą grupować swoich pracowników w zależności od tego, w jakim departamencie pracują a nie, w którym miejscu na obszarze

firmy się znajdują. Na przykład w firmie, w której pracownicy działu księgowość mają swoje biura w trzech różnych miejscach, zastosowanie sieci VLAN umożliwia połączenie ich wszystkich i komunikację między nimi, tak jakby pracowali w jednym miejscu wpięci do jednego przełącznika. To z kolei daje dwie kolejne zalety, pierwsza z nich to ułatwiona i szybsza administracja siecią, a druga to redukcja kosztów infrastruktury sieciowej. Ułatwiona administracja jest widoczna szczególnie w przypadku dużych firm, gdzie występuje rotacja użytkowników sieci. Chodzi tutaj przede wszystkim o dodawanie i przenoszenie pracowników. Nieocenione w takim przypadku są sieci VLAN zbudowane na zasadzie przynależności z użyciem adresów fizycznych MAC. W takim przypadku nie ma żadnego znaczenia, do którego przełącznika i na którym piętrze w firmie użytkownik wepnie swojego laptopa, bo zawsze będzie się on znajdował w tej samej sieci VLAN i będzie mógł korzystać z tych samych zasobów sieciowych. W sieciach, w których sieci VLAN nie są używane, takie przemieszczanie się użytkowników jest niemożliwe do zrealizowania w prosty i rozsądny finansowo sposób. Tak więc wirtualne sieci LAN dają możliwość zaoszczędzenia sporej ilości pieniędzy. Gdyby w firmie, w której są trzy departamenty, a budynek firmy ma trzy piętra, pozwolono pracownikom tak wędrować, to wymagało by to istnienia na każdym piętrze trzech przełączników. Trzy piętra razy trzy przełączniki daję nam dziewięć fizycznych urządzeń. Dokładnie to samo można osiągnąć tworząc w firmie trzy sieci VLAN i używając na każdym z pięter tylko jednego przełącznika (rysunek 1).



Rysunek 1. Sieć VLAN w firmie z trzema departamentami (opracowanie własne)

Koszty takiego rozwiązania są przynajmniej trzy razy mniejsze. Dodatkowym atutem tego rozwiązania jest to, że zwykle w takich sieciach nie trzeba używać tylu ruterów co w rozwiązaniu tradycyjnym. W wirtualny sieciach rutery są używane prawie wyłącznie do tworzenia łączności między różnymi VLANami.

Dzielenie sieci na segmenty znacząco poprawia jej bezpieczeństwo, ponieważ ruch między sieciami VLAN jest albo niemożliwy albo zarządzany i filtrowany. Redukuje to znacząco szanse przechwycenia przez potencjalnego włamywacza interesujących go danych, jeśli nie ma on praw do dostępu do sieci VLAN, w której one są dostępne. Z punktu widzenia bezpieczeństwa, sieci VLAN dają możliwość lepszej kontroli domen rozgłoszeniowych (ułatwia to walkę ze *sniffingiem*), ustawiania praw dostępu, filtrowania ruchu między sieciami VLAN za pomocą zapór (ang. *firewall*) i list ACL, a nawet informowania administratora o intruzach i wykrytych włamaniach.

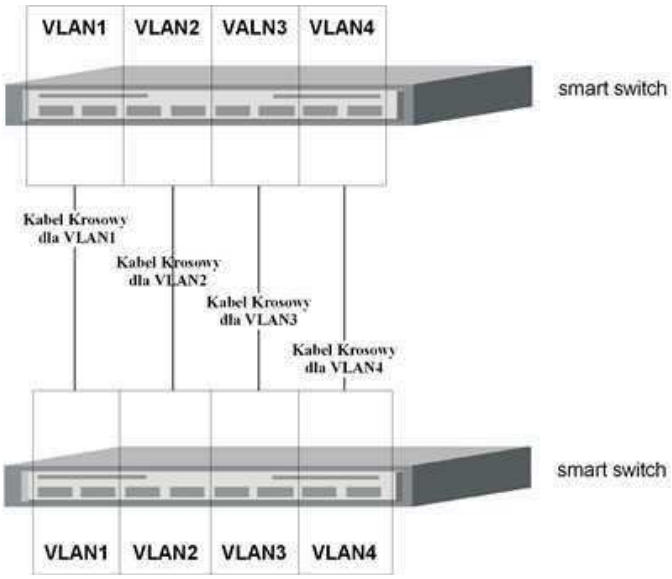
1.4 Rodzaje sieci VLAN i zarys ich działania

Sieci VLAN można podzielić na statyczne i dynamiczne. Podział ten wywodzi się od sposobu partycypowania przynależności do wirtualnych sieci przez podłączane urządzenia. W sieciach statycznych przynależność urządzenia do VLANa zależy od portu do jakiego zostało ono wpięte. Statyczne sieci VLAN są w całości ręcznie konfigurowane przez administratora. Konfiguracja ta polega na przypisaniu każdego portu przełącznika do odpowiedniej sieci VLAN na stałe. Oznacza to, że przynależność portu do wybranej sieci VLAN nie może się w żaden sposób zmienić podczas pracy przełącznika. Jedynym sposobem na przestawienie przynależności jest przekonfigurowanie przełącznika. W sieciach dynamicznych przypisanie portu przełącznika do sieci VLAN jest zmienne i zależy od właściwości urządzenia jakie zostało do niego wpięte. Do owych właściwości urządzenia mogą należeć między innymi: jego adres MAC, adres warstwy trzeciej modelu OSI (np. adres IP) lub rodzaj protokołu warstwy trzeciej. Przełącznik, dzięki poznaniu tych parametrów może przydzielić urządzenie do odpowiedniej sieci na podstawie konfiguracji własnej lub odpytać specjalny, wyznaczony serwer w sieci do jakiego VLANa powinno należeć to urządzenie. Serwerem ustalającym przynależność do sieci VLAN może być komputer z odpowiednim oprogramowanie i używający specjalnych protokołów (np. linux z oprogramowaniem OpenVMPS[1]). Jednak najczęściej funkcję serwera pełni wyznaczony przez administratora inteligentny switch, który

[1] Jest to oprogramowanie współpracujące z przełącznikami firmy Cisco umożliwiające budowanie sieci VLAN w oparciu o adresy MAC urządzeń.

na przykład posiada w pamięci mapę odwzorowań VLAN – MAC i na jej podstawie przydziela porty do VLANów.

Patrząc od strony technicznej, podstawową własnością, jaką posiadają sieci VLAN jest możliwość łączenia ze sobą kilku inteligentnych przełączników, w ten sposób że na każdym przełączniku są dostępne te same sieci VLAN. Takie działanie sieci można osiągnąć na dwa sposoby. Pierwszy sposób, jest możliwy do zastosowania tylko w statycznych sieciach VLAN bazujących na portach przełącznika i z założenia jest nie polecany, a nawet uważany za niepoprawny[2]. Polega on na łączeniu ze sobą tych samych sieci VLAN na każdym przełączniku za pomocą kabla krosowego (ang. *Cross-over*, rysunek 2) .



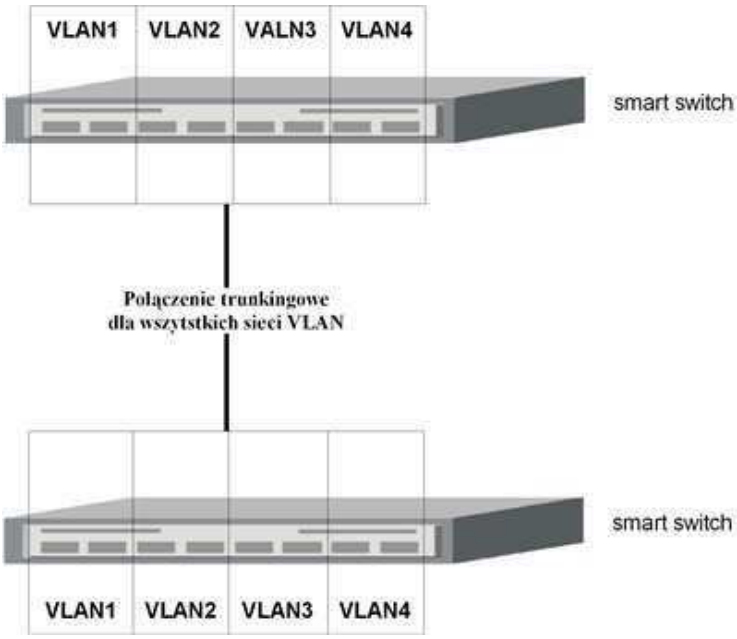
Rysunek 2. Połączenie każdej sieci VLAN kablem krosowym (opracowanie własne)

Rozwiązanie drugie to budowanie połączeń trunkingowych (rysunek 3). Połączenia trunkingowe polegają na tym, że na każdym przełączniku, na którym są wirtualne sieci, wybiera się jeden port[3] (zwany trunkingowym), konfiguruje go i przypisuje do niego odpowiednie sieci VLAN. Przy zestawianiu połączeń trunkingowych pomocny może być protokół DTP firmy Cisco, który między innymi potrafi tworzy takie połączenia automatycznie. Tak skonfigurowane połączenie służy do przesyłania ramek kilku sieci VLAN jakie istnieją na przełączniku. Jednak zanim ramka zostanie przesłana, musi ona zostać „oznaczona”, aby przełącznik, który odbierze tą ramkę po drugiej stronie łącza

[2] Ten sposób łączenia ze sobą sieci VLAN jest uważany za niepoprawny gdyż zupełnie omija podstawowe standardy sieci VLAN, jakimi są łącza trunkingowe oraz IEEE 802.1Q. Oczywistą rzeczą jest także, że zbudowana w ten sposób sieć nie ma większości zalet, które zostały opisane powyżej.

[3] Jeden port lub więcej, zależnie od ilości połączeń do innych przełączników, ruterów lub innych urządzeń VLAN-aware.

trunkingowego, wiedział, do którego VLANa ona należy. Zależnie od zastosowanego standardu, ramka ta może być „opisywana” za pomocą tagowania (ang. *tagging*) tak jak dzieje się to w standardzie i protokole IEEE 802.1q lub enkapsułowana. Enkapsulacja jest zastosowana na przykład w protokole ISL (ang. *InterSwitch Link*) firmy Cisco. Dzięki tak działającym łączom trunkingowym, możemy za pomocą jednego połączenia fizycznego tworzyć kilka połączeń logicznych. Używanie połączeń trunkingowych nie ogranicza się wyłącznie do przełączników, mogą one być także używane do połączenia przełączników z ruterami (mającymi zapewniać łączność między sieciami VLAN) lub innymi urządzeniami określanymi mianem „świadomych istnienia sieci VLAN” (ang. *VLAN-aware*).



Rysunek 3. Wykorzystanie łącza trunkingowego do połączenia VLANów na dwóch przełącznikach (opracowanie własne)

Rozdział II Sposoby implementacji sieci VLAN

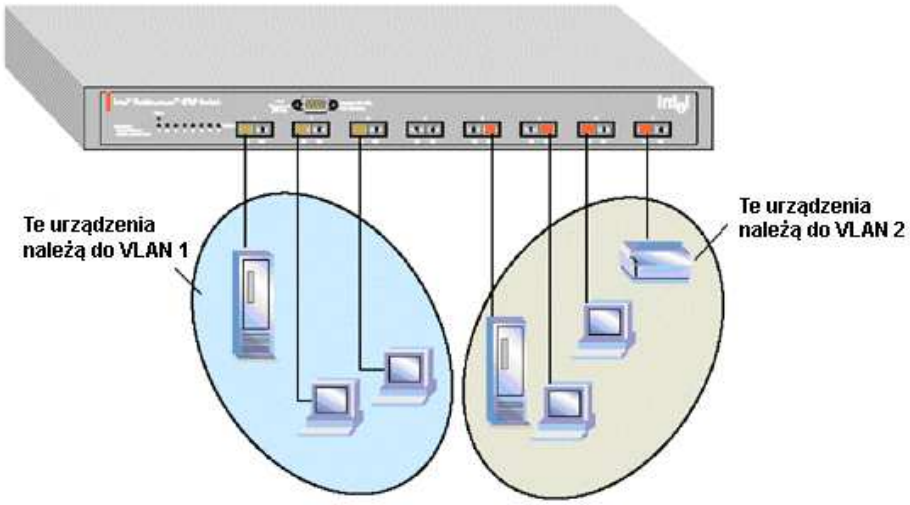
Wyróżnia się kilka możliwych sposobów implementacji sieci VLAN. Rodzaj wybranej implementacji najczęściej zależy od tego jak sieć ma być wykorzystywana i jakie udogodnienia oferowane przez wirtualne sieci są najbardziej pożądane. Najważniejsze typy sieci VLAN jakie się wyróżnia, ze względu na sposób implementacji to:

- Sieci VLAN oparte na portach przełącznika (ang. *Port-Based VLANs*)
- Sieci VLAN oparte na adresach MAC podłączonych urządzeń(ang. *MAC-Based VLANs*)
- Sieci VLAN oparte na warstwie trzeciej modelu OSI (ang. *layer-3 Based VLANs*)
- Sieci VLAN oparte o grupy multicastowe protokołu IP (ang. *IP Multicast Group-Based VLANs*)
- Sieci VLAN oparte o autentykację (ang. *Authenticated VLANs*)
- Sieci VLAN w sieciach ATM z wykorzystaniem systemu LANE
- Sieci VLAN bazujące na aplikacjach i usługach (ang. *Application-Based VLANs i Services-Based VLANs*)

Powyższa lista sposobów implementacji sieci VLAN ma trzy ważne właściwości, ponieważ kolejność wymieniania odzwierciedla ich popularność, skomplikowanie oraz cenę. Sieci VLAN oparte o porty przełącznika są najprostsze w implementacji (można je zbudować w kilka minut), co implikuje, że są one też najpopularniejsze. Także cena ich wdrożenia jest najniższa, gdyż są one możliwe do wykonania na wszystkich inteligentnych przełącznikach z „dolnej półki”. Na końcu listy są sieci wirtualne oparte na aplikacjach i usługach, w których wykorzystuje się takie wyrafinowane mechanizmy jak autoryzacja do sieci VLAN oraz zaawansowane zasady polityki. Aby budować tego typu wirtualne sieci trzeba być wyposażonym w sprzęt z górnej półki, ponieważ sieci te wymagają do działania dedykowanych i drogich urządzeń, które obsługują bardzo skomplikowane protokoły i są trudne w konfiguracji. Cena i skomplikowanie sieci wirtualnych bazujących na aplikacjach i usługach spowodowały, że są one najmniej popularne. Znajdują one zastosowanie przede wszystkim w sieciach korporacyjnych, gdzie mechanizmy przez nie oferowane są wymagane do wydajnej pracy (oraz administracji siecią), a ceny nie odstraszają.

2.1 Sieci VLAN oparte na portach przełącznika (Port-based VLANs)

Wirtualne sieci oparte na portach przełącznika są przykładem statycznych sieci VLAN, są one najbardziej popularne i zarazem najprostsze w implementacji. Konfiguracja tych sieci polega na ręcznym przypisaniu przez administratora każdego portu do jednego z VLANów. Oznacza to, że raz przypisany port, nie może zmienić swojej przynależności do sieci VLAN bez ingerencji administratora w wewnętrzne ustawienia przełącznika. Statyczne sieci VLAN nie potrzebują do działania żadnych zaawansowanych rozwiązań takich jak serwery określające przynależność. Cała konfiguracją sieci VLAN na przełączniku odbywa się tylko w obrębie tego, jednego przełącznika.



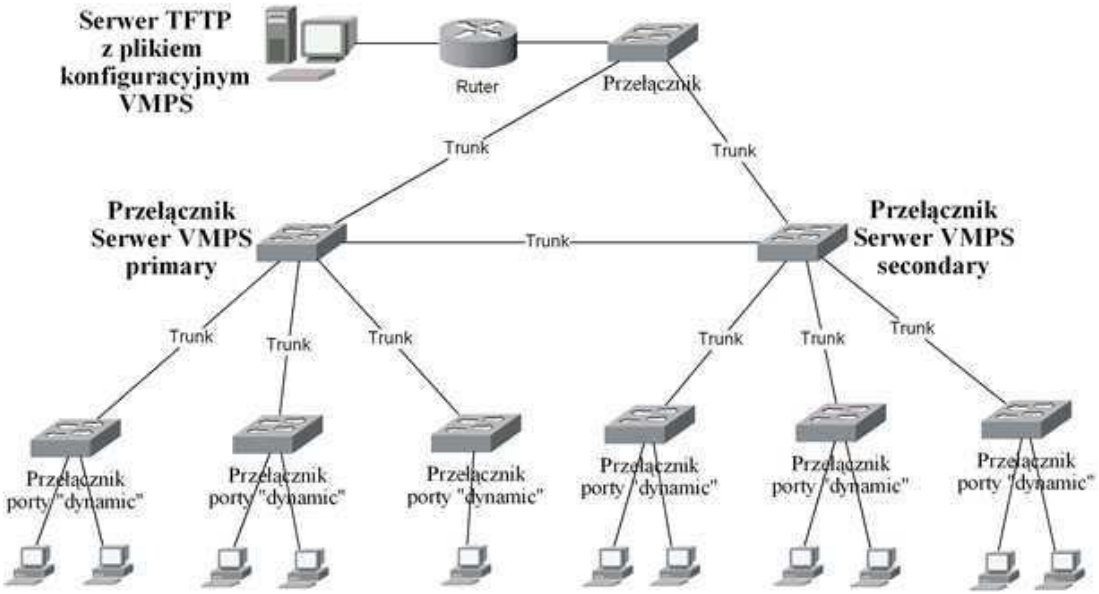
Rysunek 4.Dwie statyczne sieci VLAN bazujące na portach przełącznika(Źródło: www.intel.com, 15.06.2006)

Zgodnie z rysunkiem powyżej port 1, 2 i 3 na przełączniku został przydzielony do sieci VLAN 1, a porty od 5 do 8 do sieci VLAN 2. Tak stworzone statyczne wirtualne sieci zapewniają większe bezpieczeństwo dla komputerów, które się w nich znajdują, niż gdyby były wpięte w tradycyjny sposób do przełącznika bez VLANów. Komputery, które znajdują się w sieci VLAN 1 nie mogą z żaden sposób komunikować się z komputerami z sieci VLAN 2. Dzięki temu, atak polegający na próbie przechwycenia ruchu z sieci wirtualnej 1 za pomocą komputera znajdującego się w VLAN 2 jest z góry skazana na niepowodzenie. Innym, często wskazywanym przez administratorów, atutem statycznych sieci VLAN jest możliwość kontroli przemieszczania się użytkowników w obrębie infrastruktury sieciowej. Każdy użytkownik, chcący podpiąć się do swojej sieci VLAN w innym miejscu niż zostało mu pierwotnie wyznaczone, musi poprosić administratora, aby skonfigurował dostęp do jego

sieci VLAN na porcie przełącznika, do którego wpiął swój komputer. Jednak trzeba pamiętać, że ta zaleta w dużych sieciach, w których użytkownicy często zmieniają swoje miejsca może bardzo łatwo stać się ogromną wadą. W ekstremalnej sytuacji administrator musiałby wciąż biegać od przełącznika do przełącznika i rekonfigurować przynależność do VLANów. Aby ustrzec się takiej sytuacji powstały dynamiczne sieci VLAN.

2.2 Sieci VLAN oparte na adresach MAC (MAC-based VLANs)

Każde urządzenie sieciowe, jakie można podpiąć do sieci komputerowej, posiada swój niepowtarzalny w skali globalnej adres fizyczny MAC (ang. *Media Access Control*). Jest to 48 bitowy numer nadany urządzeniu podczas produkcji, pierwsze 3 bajty oznaczają producenta, a pozostałe 3 bajty jego numer seryjny. Wykorzystanie tego unikatowego numeru pozwala na budowanie dynamicznych sieci VLAN zwanych MAC-based VLANs. Najważniejszą cechą takich sieci jest to, że przynależność urządzenia do odpowiedniej sieci administrator ustala w jednym centralnym urządzeniu, a wszystkie inteligentne przełączniki za pomocą połączeń sieciowych mając dostęp do tego urządzenia mogą je odpytywać zadając pytanie *„Do którego VLANa ma być zapisany nowo wpięty komputer?”*.



Rysunek 5. Topologia z dynamicznym uczestnictwem w sieciach VLAN oparta o usługi VMPS firmy Cisco (opracowanie własne)

Centralnym urządzaniem, które zarządza przynależnością do sieci wirtualnej jest zazwyczaj[4] inteligentny przełącznik wyposażony w specjalne usługi takie jak na przykład serwer VMPS (ang. *VLAN Member Policy Server*). Przełącznik będący serwerem zawiera w swojej pamięci tablicę odwzorowań MAC-do-VLAN i na jej podstawie odsyła odpowiedzi do przełączników odpytujących. Najczęściej taka mapa odwzorowań przygotowywana jest przez administratora w formie pliku tekstowego i umieszczana na serwerze TFTP, z którego przełącznik (pełniący funkcję serwera) może ją łatwo pobrać. Należy pamiętać, że w razie awarii przełącznika będącego serwera lub jego odłączenia od sieci, wszystkie przełączniki odpytujące, tracąc z nim łączność, nie będą w stanie ustalić przynależności urządzeń do VLANów. W rezultacie spowoduje to blokadę portów (tzw. tryb „*shutdown*”) lub przypisanie urządzeń do jednej domyślnej sieci VLAN. Aby zapobiec takiej sytuacji, w sieci są zazwyczaj 2 lub 3 inteligentne przełączniki, z których jeden pełni funkcję serwera głównego (ang. *primary server*), a pozostałe funkcję zapasową (ang. *secondary server*) w razie jego awarii.

Kolejną bardzo ważną zaletą sieci VLAN opartych na adresach MAC, która wynika z poprzedniej, jest możliwość przenoszenia się użytkowników w obrębie sieci bez potrzeby rekonfiguracji przełączników. Jest to rozwiązanie problemu, który pojawiał się w dużych sieciach, gdzie przynależność do sieci VLAN opierała się o statyczną konfigurację portów przełącznika.

Należy do VLAN		Adres MAC
2	→	5D:FF:68:DE:22:OA
4	→	23:DF:56:67:23:DA
4	→	32:AE:34:56:CB:23
12	→	AE:23:45:DF:78:65
4	→	56:13:FE:56:23:EF
4	→	42:54:AF:67:86:EA
12	→	43:79:ED:CB:23:67
2	→	23:DF:56:AE:34:98
2	→	42:54:AF:75:98:DE
12	→	5D:FF:68:65:76:DD

Rysunek 6. Przykładowa tablica przedstawiająca mapowanie adresów MAC na przyporządkowane im sieci VLAN, która znajduje się na przełączniku pełniącym rolę serwera przynależności (opracowanie własne)

[4] Urządzeniami tymi mogą być także komputery wyposażone w odpowiednie oprogramowanie (np. OpenVMPS)

Powyższa tabelka (rysunek 6) przedstawia przykładowe mapowanie MAC-do-VLAN jakie może się znajdować na urządzaniu ustalającym przynależność do sieci wirtualnych. Na jej podstawie można wywnioskować, że zostały zaprojektowane trzy sieci VLAN oznaczone jako VLAN 2 , VLAN 4 i VLAN 12. W chwili podpięcia do przełącznika dostępowego komputera o adresie MAC - AE:23:45:DF:78:65, przełącznik ten skieruje zapytanie do urządzenia zarządzającego o treści *„Do jakiej sieci VLAN ma przynależeć urządzenie sieciowe o adresie MAC AE:23:45:DF:78:65 ?”*. Urządzenie zarządzające sprawdzi swoją tablicę odwzorowań MAC-do-VLAN i wyśle do przełącznik dostępowego odpowiedź *„Urządzenie o adresie MAC AE:23:45:DF:78:65 ma znajdować się w sieci VLAN 12”*. Przełącznik dostępowy po otrzymaniu tej odpowiedzi ustawi port, do którego został wpięty komputer, jako członka sieci VLAN 12. Trzeba jednak pamiętać, że powyższy opis nie zapewnia, że nowo wpięty komputer będzie od razu mógł się bez przeszkód komunikować z resztą urządzeń w sieci VLAN 12. Dzieje się tak dlatego, że komputer do poprawnej komunikacji wymaga jeszcze skonfigurowanego adresu warstwy trzeciej. W sieciach TCP/IP wymagany jest adres IP i maska podsieci, dlatego, w szczególności, w dużych sieciach korporacyjnych (jeśli komputery w sieci nie mają przydzielonych adresów na stałe), przełącznik lub komputer pełniący funkcję zarządzania przynależnością do VLAN ma także zaimplementowaną usługę serwera DHCP[5]. Należy pamiętać także, że przełącznik dostępowy (klient dla serwera np. VMPS), który ma dawać możliwość dynamicznego zapisywania się do sieci VLAN po adresie MAC, wymaga odpowiedniej konfiguracji. Na przełączniku kliencie wymagane jest skonfigurowanie adresu IP serwera zarządzającego oraz ustawienie portów przełącznika, które mają być dynamicznie przypisywane do sieci VLAN na tryb dynamiczny.

W dynamicznych sieciach VLAN tworzonych na bazie adresów MAC, powstał pewien problem. Co zrobić z komputerami, których nie ma w tablicy odwzorowań MAC-do-VLAN. W niektórych przełącznikach, port, do którego zostało wpięte takie urządzenie zostaje po prostu wyłączony (tryb shutdown). Ale czasami, firmy, w których istnieją sieci VLAN chcą, aby była możliwość podpięcia takich komputerów do infrastruktury sieciowej i by na przykład miały one możliwość dostępu do Internetu. Aby rozwiązać ten problem producenci sprzętu sieciowego wymyślili specjalny typ sieci VLAN zwany *fallback* VLAN, do którego zapisywane jest każde urządzeni sieciowe, którego adres MAC nie ma odwzorowania w urządzeniu zarządzającym. Ten typ sieci VLAN można konfigurować dokładnie tak samo jak

[5] Funkcję serwera DHCP może oczywiście też pełnić inne, niezależne urządzenie sieciowe.

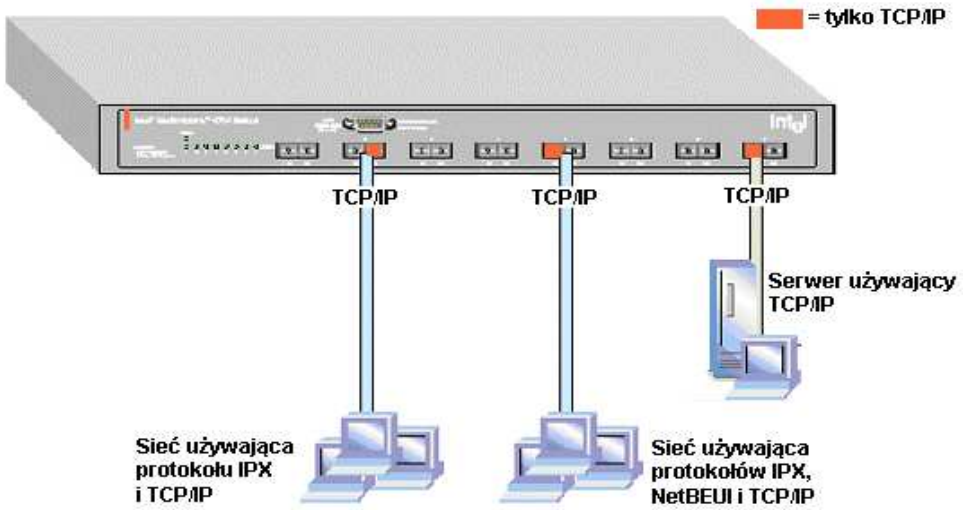
każdą inną, „normalną” sieć VLAN, a więc można na przykład użytkownikom tej sieci dać jedynie możliwość korzystania z Internetu.

2.3 Sieci VLAN oparte na warstwie trzeciej modelu OSI (Layer 3-based VLANs)

Można rozróżnić dwa typy sieci VLAN bazujących na warstwie trzeciej. Pierwszy typ to wirtualne sieci oparte na rodzaju protokołu warstwy trzeciej (ang. *protocol-based VLANs*), mogą one z założenia występować tylko w tych sieciach, w których korzysta się z kilku różnych protokołów takich jak na przykład IP, IPX i NetBEUI. Drugi typ wirtualnych sieci warstwy trzeciej bazuje na adresie sieci (ang. *network-layer address VLANs*), w przypadku sieci TCP/IP jest brany pod uwagą adres podsieci (ang. *subnet address*). W sieciach VLAN opartych na warstwie trzeciej znaczenie ramek nie jest wymagane. Jest ono niepotrzebne, ponieważ przełączniki potrafią rozpoznać sieci VLAN po rodzaju protokołu lub po numerze podsieci.

2.3.1 Wirtualne sieci bazujące na protokole (Protocol-based VLANs)

W sieciach, w których korzysta się z wielu różnych protokołów warstwy trzeciej można wydzielić osobne sieci VLAN bazujące na konkretnym typie protokołu. Konfiguracja tego typu wirtualnych sieci polega na przypisaniu do konkretnego portu na przełączniku typu protokołu, jaki ma on obsługiwać.

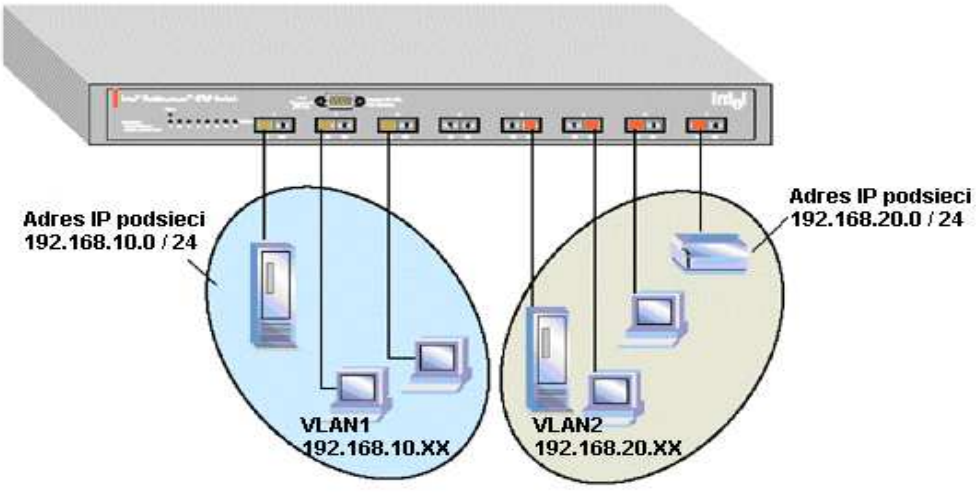


Rysunek 7. Przełącznik na którym port 2, 5 i 8 należą do VLANu z ruchem wyłącznie TCP/IP (opracowanie własne na podstawie www.intel.com, 15.06.2006)

Za pomocą takiego rozwiązania można w łatwy sposób filtrować ruch miedzy kilkoma sieciami VLAN tak, by na przykład przepuszczać tylko ruch TCP/IP, a pozostały blokować. Zgodnie z rysunkiem 7, do portu 2 i 5 na przełączniku podpięte są sieci, w których występuje ruch kilku protokołów, do portu 8 wpięty jest serwer komunikujący się za pomocą protokołu TCP/IP. Przełącznik został tak skonfigurowany, że porty 2,5 i 8 tworzą VLAN z ruchem wyłącznie TCP/IP. W tak skonfigurowanej sieci, VLAN pełni funkcję filtra, gdyż nie pozwala on, by ruch protokołów IPX i NetBEUI przedostał się przez port 2 i 5 na pozostałą część infrastruktury sieciowej. Natomiast wszystkie urządzenia sieciowe korzystające z protokołu TCP/IP mogą się ze sobą komunikować przez porty należące do tego VLANu bez przeszkód.

2.3.2 Wirtualne sieci bazujące na numerze sieci (Network-layer address VLANs)

W sieciach VLAN bazujących na adresie podsieci na przełącznikach konfigurowana jest mapa odwzorowań adresu sieci na odpowiedni VLAN. Switch, poznając numer sieci wpinanego urządzenia, jest w stanie zapisać go do odpowiedniej sieci VLAN. Taki sposób konfiguracji jest bardzo wygodny dla administratorów, ponieważ nie wymaga rekonfiguracji przełączników w razie przemieszczania się użytkowników w sieci i wpinania komputerów do innych portów, oraz przyjazny dla użytkowników, którzy nie muszą zmieniać adresów sieciowych. Ten typ wirtualnych sieci może być stosowany w sieciach TCP/IP, IPX, DECnet i AppleTalk. Nie można go natomiast stosować w sieci, w której występuje protokół NetBEUI ponieważ jest to protokół nierutowalny i nie występują w nim podsieci.

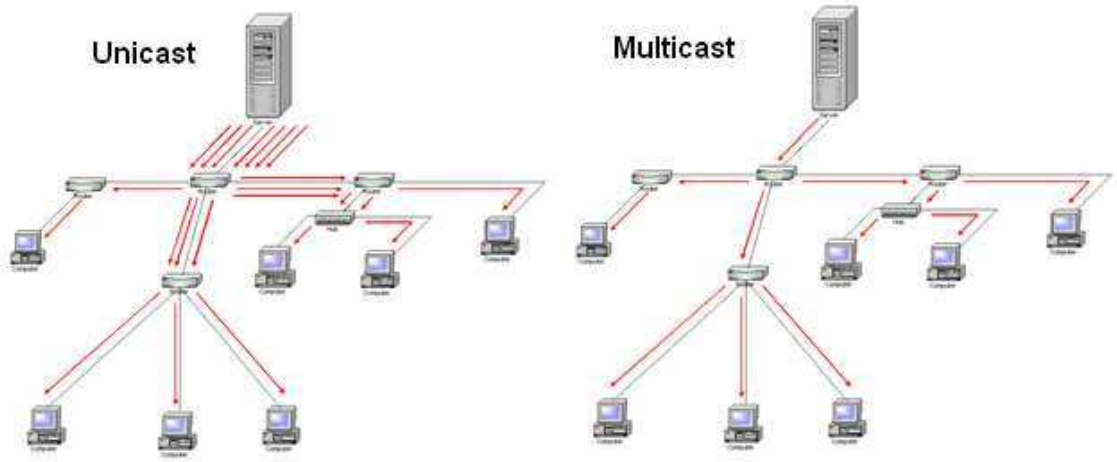


Rysunek 8. Sieci VLAN bazujące na adresie podsieci protokołu TCP/IP (opracowanie własne na podstawie www.intel.com, 15.06.2006)

Wirtualne sieci oparte o warstwę trzecią mają kilka dość ważnych zalet, które zostały opisane powyżej. Niestety, mają one też jedną dość poważną wadę, przełączanie w sieciach z VLANami warstwy trzeciej może być wolniejsze niż w przypadku VLANów bazujących na warstwie drugiej(np. *MAC-based VLAN*). Dzieje się tak, dlatego, że przełączniki z założenia są urządzeniami pracującymi w warstwie drugiej i sprawdzanie adresu MAC (który też funkcjonuje w warstwie drugiej) nie sprawi im problemu. Natomiast wydobycie z przesyłanego pakietu jego adresu warstwy trzeciej jest zadaniem zdecydowanie bardziej pracochłonnym. Dodatkowo opóźnienia przesyłania pakietów są także skorelowane z rodzajem protokołu warstwy trzeciej. Przełączniki o wiele lepiej radzą sobie z adresami pakietów protokołu TCP/IP niż z pozostałymi.

2.4 Sieci VLAN oparte o grupy multicastowe protokołu IP (IP multicast group-based VLANs)

Ruch multicastowy jest ruchem specyficznym, ponieważ nie jest on przeznaczony do jednego odbiorcy (tak jak ruch unicastowy), tylko do wielu. Grupy multicastowe protokołu IPv4 działają na adresach IP klasy D (zakres 224.0.0.0 - 239.255.255.255[6]), a w protokole IPv6 jest to zakres FF00::/8. W odróżnieniu od ruchu pojedynczego, w tym przypadku adres nie odnosi się do jednego konkretnego komputera, ale do całej sieci. Protokołem transportowym dla multicastu jest protokół UDP[7].

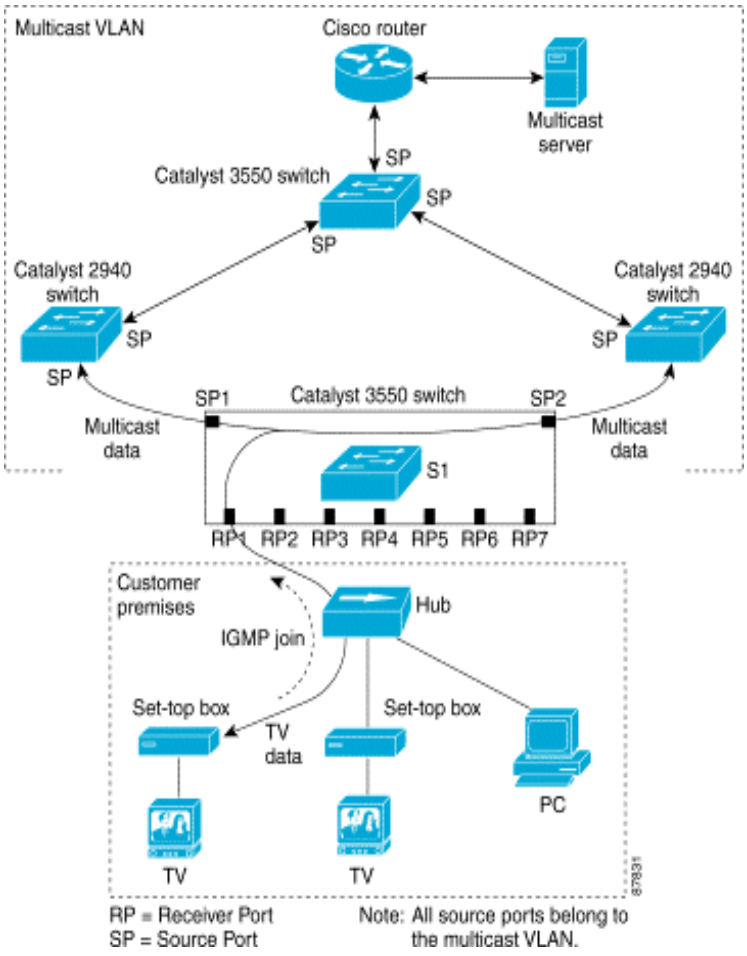


Rysunek 9. Na rysunkach została przedstawiona różnica między ruchem unicastowym a ruchem multicastowym (Źródło: http://www.surfnet.nl/publicaties/bulletin/01-2/h3.html, 16.06.2006)

[6] W zakresie tym występują adresy zarezerwowane których nie powinno się przypisywać, są to adresy od 224.0.0.0 do 224.0.0.255 oraz adres 224.0.0.1 który jest przypisany do wszystkich hostów w grupie.

[7] Protokół UDP nie zapewnia niezawodności tak jak TCP, utracone pakiety nie są wysyłane powtórnie, a te które dotrą nie w kolejności są odrzucane.

Najbardziej charakterystyczną cecha multicastu jest to, że ruch skierowany do grupy multicastowej jest wysyłany ze źródła w formie pojedynczych pakietów, które na węzłach sieci[8] ulegają skopiowaniu i rozpropagowaniu dalej na odpowiednie ścieżki. Ruch multicastowy wykorzystywany jest najczęściej do nadawania telewizji i radia internetowego oraz wszędzie tam, gdzie nadaje się w czasie rzeczywistym i istnieje wielu odbiorców. Tworzenie wirtualnych sieci VLAN na bazie grup multicastowych daje możliwość odseparowania wszystkich subskrybentów ruchu grupowego od pozostałej części sieci, a zatem dodatkowego zabezpieczenia go tak, by nie mógł on być przechwycony przez użytkowników, do których nie jest on skierowany. Rozwiązanie to polega na tym, że wszyscy użytkownicy zapisani do jednej grupy multicastowej, o konkretnym adresie, są członkami jednej sieci VLAN.



Rysunek 10 Przykład sieci wykorzystującej Multicast VLAN Registration wraz z IGMP (Źródło: www.cisco.com,20.06.2006)

[8] Chodzi o rutery i przełączniki.

Wirtualne sieci LAN tworzone za pomogą multicastu są dynamicznymi sieciami VLAN[9], charakteryzują się bardzo wysoką elastycznością i zmiennością. Podstawowymi zaletami, jakie daje stosowanie sieci VLAN do ruchu grupowego są bezpieczeństwo transmisji oraz możliwość ustawienia wybranemu ruchowi multicastowemu odpowiednich przepustowości i priorytetów podczas przesyłu pakietów. Najważniejsze protokoły, które zarządzają członkostwem grup multicastowych na przełącznikach to IGMP (ang. *Internet Group Management Protocol*) oraz GMRP (ang. *GARP Multicast Registration Protocol*). Do zarządzania członkostwem w sieciach VLAN zbudowanych na multicaście może służyć na przykład mechanizm MVR (ang. *Multicast VLAN Registration*) implementowany na inteligentnych przełącznikach firmy Cisco. MVR nie jest jednak niezależny, funkcjonuje on wraz z protokołem IGMP.

2.5 Sieci VLAN oparte o autentykację (Authenticated VLANs)

Sieci VLAN oparte o autentykację użytkowników i przypisywanie ich na taj podstawie do odpowiedniej sieci VLAN są odpowiedzią producentów sprzętu sieciowego na rosnące zapotrzebowania na bezpieczeństwo w sieciach komputerowych. Autentykowane sieci VLAN są oparte o protokół AAA (ang. *Authentication, Authorization and Accounting*). Oznacza to, że wpięty do przełącznika użytkownik, chcący dostać się do zasobów swojej sieci VLAN, musi najpierw podać hasło (ewentualnie użyć karty inteligentnej lub czytnika biometrycznego), następnie zostaje on autoryzowany na serwerze w sieci i jeżeli autoryzacja zakończyła się pomyślnie dostaje on dostęp do zasobów tej sieci VLAN[10], do której należy i w której się zalogował. Rozwiązania tego typu stają się coraz bardziej popularne i większość producentów dostarcza sprzęt, który umożliwia budowanie takich sieci VLAN.

Aby zbudować autentykowane sieci VLAN wymagane są:

- Protokół, który przenosi komunikaty podczas logowania się do sieci. Najczęściej wykorzystywanym protokołem jest protokół EAPOE (ang. *Extensible Authentication Protocol Over Ethernet*), będący specjalnie przystosowana do sieci Ethernet wersja protokołu EAP.

[9] Każdy użytkownik może się w dowolnej chwili zapisać do grupy multicastowej by otrzymywać jej ruch lub wypisać jeśli tylko posiada wymagane prawa dostępu.

[10] Przełącznik dostępowy dostaje sygnał od serwera, do której sieci VLAN ma przypisać port, na którym użytkownik jest wpięty.

- Serwer, który będzie pełnił funkcję autoryzacji użytkowników w sieci i wysyłał do przełącznika polecenie otwarcia lub zablokowania dostępu do zasobów na porcie, do którego wpięty jest użytkownik oraz zapisania go do odpowiedniej sieci VLAN. Najczęstszym wykonawcą tego zadania jest serwer RADIUS (ang. *Remote Authentication Dial-In Sernice*) lub serwer usług katalogowych LDAP.
- Oprogramowanie klienta, które jest w stanie współpracować z powyższymi elementami za pomocą używanego protokołu. W niektórych systemach, takich jak Windows XP lub 2003 Server, obsługa protokołu EAP znajduje się standartowo, natomiast większość pozostałych systemów operacyjnych wymaga zewnętrznego programowania klienckiego.

Dedykowanym standardem stworzonym do autentykacji i autoryzacji dostępu do sieci komputerowych jest standard 802.1X stworzony przez amerykańską organizację IEEE. W standardzie tym nie ma jednak sprecyzowanych specyfikacji co do sieci VLAN, jest on jednak na tyle elastyczny, że wszyscy producenci sprzętu bez problemu używają go do autentykacji do sieci VLAN. 802.1X w swej oryginalnej postaci składa się z protokołu komunikacyjnego EAP, serwera autoryzacji RADIUS, komputerów klienckich potrafiących korzystać z EAP oraz przełączników z zaimplementowanym w oprogramowanie standardem 802.1X. Istnieje też kilka rozwiązań, których autorami są producenci sprzętu sieciowego. Cisco proponuje swoje oprogramowanie User Registration Tool Server wraz z serwerem VPS (ang. *VLAN Policy Server*) i serwer usług katalogowych z zakresu LDAP, Active Directory lub Novell NDS. Alacatel oferuje rozwiązanie pod nazwą A-VLAN (ang. *Alcatel's Authenticated VLANs*), jest ono jednak, poza kilkoma dodatkami, prawie identyczne ze standardem 802.1X.

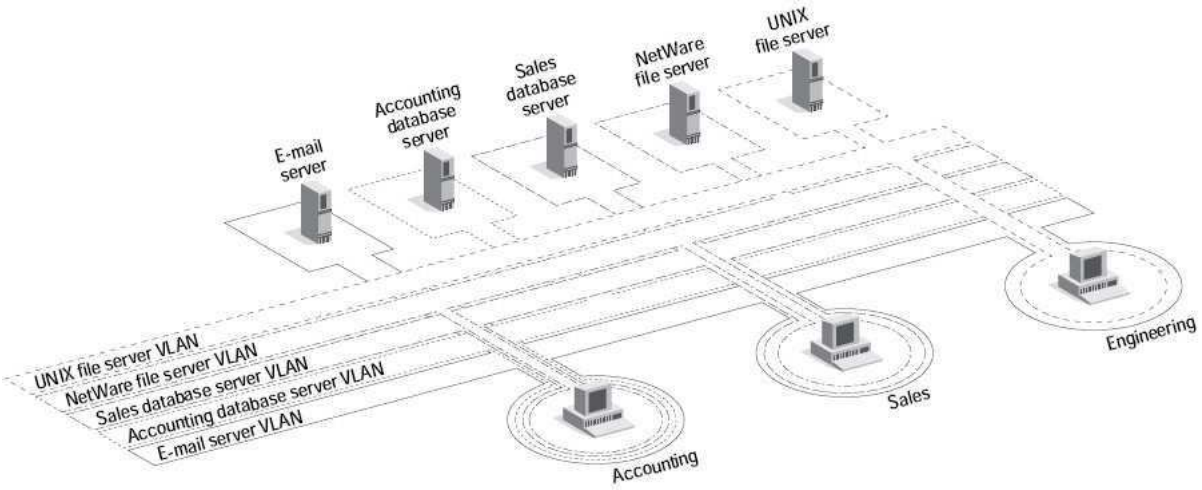
2.6 Sieci VLAN w sieciach ATM z wykorzystaniem systemu LANE

Sieci ATM (ang. *Asynchronous Transport Mode*) stosowane do łączenia urządzeń oddalonych od siebie na duże odległości także umożliwiają tworzenie sieci wirtualnych. Mimo ogromnej różnicy między funkcjonowaniem sieci ATM i Ethernet, dzięki stworzeniu systemu LANE (ang. *LAN Emulation*), możliwe stało się emulowanie sieci Ethernet na istniejącej infrastrukturze sieci ATM. LANE, oprócz budowania wirtualnych sieci LAN w samych sieciach ATM, daje możliwość łączenia ze sobą zwykłych sieci Ethernet wraz ze

zbudowanymi w nich VLANami, tak jak gdyby było to zwykłe połączenie trunkingowe między dwoma, niewiele oddalonymi od siebie inteligentnymi przełącznikami. Innymi słowy, dzięki rozwiązaniom LANE infrastruktura ATM staje się dla połączonych za jej pośrednictwem sieci Ethernet niewidoczna i są one całkowicie „nieświadome” jej istnienia.

Dokładniejszy opis możliwości tworzenia wirtualnych sieci LAN w sieciach ATM znajduje się w podrozdziale zatytułowanym „Sieci wirtualne w sieciach ATM” rozdziału VI.

2.7 Sieci VLAN bazujące na aplikacjach i usługach (ang. Application-Based VLANs i Service-Based VLANs)



Rysunek 11.Sieci VLAN bazujące na usługach. (Źródło: The Virtula Lan Technology Raport,1996, http://www.3com.com/other/pdfs/solutions/en_US/20037401.pdf, 22.06.2006)

Jest to najbardziej skomplikowany i zróżnicowany typ sieci wirtualnych, który trudno określić w jednoznaczny sposób. Podstawą do ich funkcjonowania są różnorodne aplikacje oraz usługi działające w sieciach komputerowych. Najprostszą formą tych sieci jest przypadek, kiedy każda z sieci VLAN odpowiada jednej usłudze uruchomionej w sieci lub dostępowi do konkretnego serwera z zasobami. Biorąc pod uwagę, że każdy użytkownik w sieci może wymagać dostępu do kilku serwerów lub korzystać z kilku usług, nieunikniona staje się sytuacja, w której konkretni użytkownicy lub grupy użytkowników stają się członkami wielu sieci VLAN równocześnie (sieci VLAN zachodzą na siebie lub w pewnych sytuacjach nawet się pokrywają). W typowej organizacji wielu użytkowników korzysta z takich usług sieciowych jak e-mail, HTTP lub VoIP oraz używa na przykład z serwera baz

danych i FTP. Jeśli każda z tych usług jest równoznaczna z istnieniem sieci VLAN to łatwo zauważyć, że sieci wirtualne bazując na aplikacjach i serwisach stają się wyjątkowo złożoną materią. Dlatego, sieci te, aby były praktyczne i możliwe do stosowania, wymagają wysokiej klasy rozwiązań uwzględniających w pełni automatyczną konfigurację urządzeń sieciowych i jedno centralne miejsce administracji siecią. W wirtualnych sieciach bazujących na aplikacjach i usługach, VLANy całkowicie tracą swój statyczny charakter w rozumieniu domeny rozgłoszeniowej definiowanej przez administratora. Stają się one swego rodzaju kanałem, do którego użytkownicy (mając odpowiednie prawa) mogą się dołączyć lub od niego odłączyć.

2.8 Podsumowanie rozdziału

Przedstawione w tym rozdziale sposoby tworzenia sieci VLAN są metodami najpopularniejszymi i najczęściej implementowanymi, więc także najlepiej ustandaryzowanymi. Trzeba jednak mieć na uwadze, że producenci sprzętu sieciowego wdrażają do swoich urządzeń ich autorskie rozwiązania, które dają często wiele nowych możliwości, ale najczęściej działają tylko na sprzęcie tego jednego producenta. Z tego powodu rozwiązania te są rzadko stosowane[11], ponieważ użytkownicy bardzo boją się braku kompatybilności między sprzętem różnych producentów (lub nawet starszym i nowszym tego samego). Stabilnie działająca sieć jest najważniejsza, dlatego odbiorcy sprzętu sieciowego, szczególnie ci korporacyjni, starają się korzystać tylko z najpopularniejszych mechanizmów i to najlepiej tych ustandaryzowanych przez amerykańską organizację IEEE (w przypadku sieci wirtualnych będzie to przede wszystkim standard 802.1Q). Takie postępowanie daje prawie całkowitą pewność, że urządzenia sieciowe różnych producentów będą ze sobą współpracowały i nie jest w stanie zmienić go kilka dodatkowych funkcji oferowanych przez jednego producenta.

Kolejną ważną rzeczą jest to, że producenci sprzętu sieciowego implementują do swoich urządzeń po kilka różnych metod tworzenia sieci VLAN. Na prawie wszystkich inteligentnych przełącznikach, nawet tych starszych, możliwe jest budowanie sieci

[11] Wyjątkiem od tej reguły jest firma Cisco, która wprowadziła do sieci komputerowych wiele swoich autorskich pomysłów i są one dość szeroko stosowane. Powodem tego zjawiska jest fakt, że firma ta jest potentatem i pionierem w dziedzinie sieci komputerowych.

wirtualnych opartych na portach, adresach MAC oraz na warstwie trzeciej modelu OSI[12]. Większość nowych, aktualnie produkowanych przełączników, używa także standardu 802.1X do autantykacji klientów oraz potrafi wydobywać z pakietów informacje warstwy czwartej, które potrzebne są do budowania sieci VLAN bazujących na usługach sieciowych. Inną tendencją jest to, że tworzy się wirtualne sieci za pomocą łączenia kilku metod. Na przykład *port-based/protocol-based/MAC-based* VLAN, w takim przypadku na konkretnym porcie przełącznika będzie mogła istnieć tylko taka sieć VLAN, która został przypisany do danego portu, ale pod warunkiem, że podpięte urządzenie sieciowe będzie używać określonego protokołu i dodatkowo jego MAC adres będzie zawierał się w sprecyzowanej puli adresów. Taki sposób budowania sieci wirtualnych, określany jako bazujący na zasadach (ang. *Police-Based VLAN*), dostarcza możliwość wyjątkowo precyzyjnego określania, które komputery mogą należeć do jakiej sieci VLAN.

[12] W przypadku VLANów bazujących na adresach MAC, gdzie wymagany jest serwer, przełączniki z „dolnej półki” mogą funkcjonować zazwyczaj tylko w formie klientów, a rolę serwera spełnia przełącznik z „wyższej półki”. Tak jest na przykład w mechanizmie VMPS firmy Cisco.

Rozdział III Połączenia urządzeń stosowane w sieciach wirtualnych

W sieciach VLAN wyróżniamy trzy typy połączeń służące do łączenia urządzeń znajdujących się w sieci. Rodzaje tych połączeń to Access Link, Trunk Link oraz Hybrid Link. Typ łącza zależy od rodzaju urządzeń nim połączonych oraz formy przesyłanych między nimi ramek.

W wirtualnych sieciach LAN rozróżniamy dwa typy urządzeń:

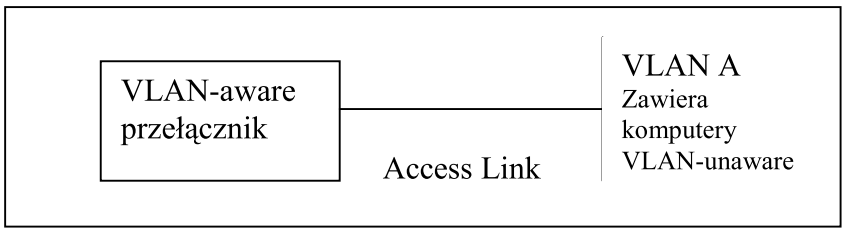
- Urządzenia świadome istnienia sieci VLAN (ang.VLAN-aware devices) są to urządzenia sieciowe, które „wiedzą” że odbierają i wysyłają ruch należący do różnych sieci VLAN. Potrafią one rozpoznać oznaczenia ramek (lub ich brak), które decydują o tym do którego VLANa one należą i gdzie powinny być przesłane. Potrafią one także znaczyć i odznaczać ramki używając jednego ze służących do tego protokołów[13]. Do tych urządzeń należą inteligentne przełączniki, rutery oraz komputery wyposażone w specjalne oprogramowanie i sterowniki karty sieciowej(najczęściej serwery).
- Urządzenia nieświadome istnienia sieci VLAN (ang. VLAN-unaware devices) są to urządzenia, które potrafią obsługiwać wyłącznie ruch nieoznaczony (standardowy, bez tagowania sieci VLAN). W wypadku otrzymania ramki oznaczonej, urządzenie takie uznaje ją za uszkodzoną ponieważ ma ona niestandardowy rozmiar (jest dla niego za duża). Do urządzeń VLAN-unaware należą koncentratory, standardowe przełączniki (nieinteligentne), oraz komputery podpięte do sieci.

3.1 Połączenia typu access (Access Links)

Połączenie typu access jest zwyczajnym połączeniem stosowanym w sieciach komputerowych do przesyłania ruchu tylko i wyłącznie jednej sieci VLAN. Access Link może być stosowany tylko jako połączenia między urządzeniami świadomymi i nieświadomymi istnienia sieci VLAN (między VLAN-aware i VLAN-unaware). Ruch sieciowy przesyłany przez Access link nie może być znakowany, dlatego z każdej ramki zanim opuści ona urządzenie świadome usuwane są wszystkie oznaczenia. W wypadku gdyby

[13] Więcej informacji o znaczeniu ramek i protokołach służących do tego znajduje się w dalszym rozdziale, który poświęcony jest temu zagadnieniu.

urządzenie nieświadome otrzymało ruch tagowany, cały zostanie on uznany za błędny (uszkodzony) i odrzucony ze względu na niestandardową wielkość ramek (oraz niezrozumiałe dodatki - tagi).

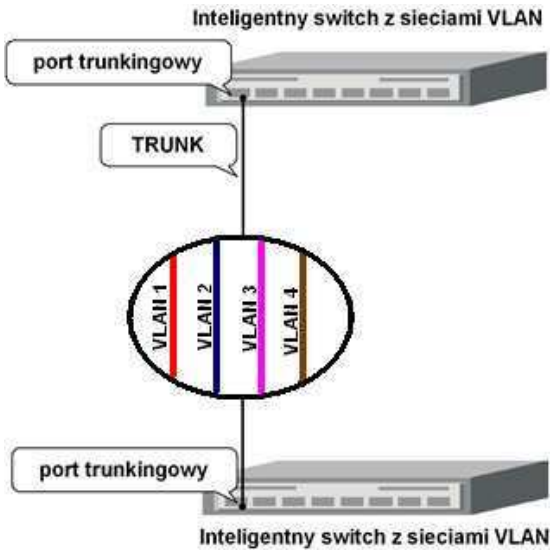


Rysunek 12. Połączenie typy Access Link (opracowanie własne)

Powyższy rysunek 13 przedstawia dwa urządzenia sieciowe połączone łączem typu Access link. Urządzeniem VLAN-aware jest najczęściej inteligentny przełącznik, a port do którego zostało podpięte łącze jest przydzielony do wirtualnej sieci VLAN A. Nieświadomym urządzeniem VLAN A może być jeden komputer, ale może też być nim cały segment sieci składający się z kilku komputerów złączonych razem koncentratorem, który wpięty jest do portu na przełączniku.

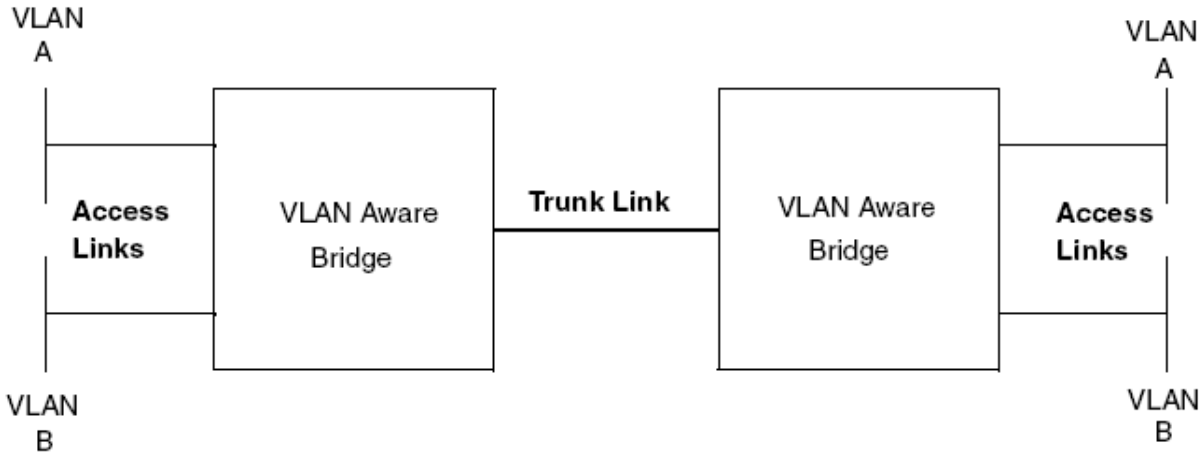
3.2 Połączenia trunkingowe (Trunk Links)

Połączenia trunkingowe, zwane też potocznie trunkami, są przeznaczone do przesyłania ruchu sieciowego należącego do wielu sieci VLAN. Za pomocą jednego fizycznego połączenia przesyłany jest logicznie ruch kilku oddzielnych sieci wirtualnych.



Rysunek 13. Połączenie trunkingowe między dwoma przełącznikami przenoszące ruch czterech sieci VLAN (opracowanie własne)

Trunkami można łączyć ze sobą tylko i wyłącznie urządzenia VLAN-aware, czyli świadome istnienia sieci VLAN. Wszystkie ramki, które są przesyłane takim łączem muszą być znaczone, aby spięte nim urządzenia były w stanie odczytać ich przynależność od sieci VLAN. Porty służące do budowania trunków także nazywają się portami trunkingowymi. Porty trunkingowe ze względu na charakter spełnianej funkcji powinny mieć większe pasmo przenoszenia danych niż porty standardowe do których przypięte są komputery. Dlatego jeżeli zwykłe porty typu access mają przepustowość 100Mbit/s to trunk powinien mieć 1Gbit/s. Innym rozwiązaniem, którego zadaniem jest zwiększenie przepustowości połączenia trunkingowego jest agregacja portów (standard 802.3ad lub EtherChanel firmy Cisco). Polega ona na użyciu nie jednego, a dwóch lub czterech fizycznych połączeń. Wtedy prędkość przesyłu danych jest dwu lub cztero krotnie większa (technika równoważenia obciążeń - *load balancing*), a dodatkowym atutem jest zwiększona niezawodność. W wypadku uszkodzenia jednego z połączeń pozostałe przejmują jego ruch na siebie i wszystko to dzieje się automatycznie.

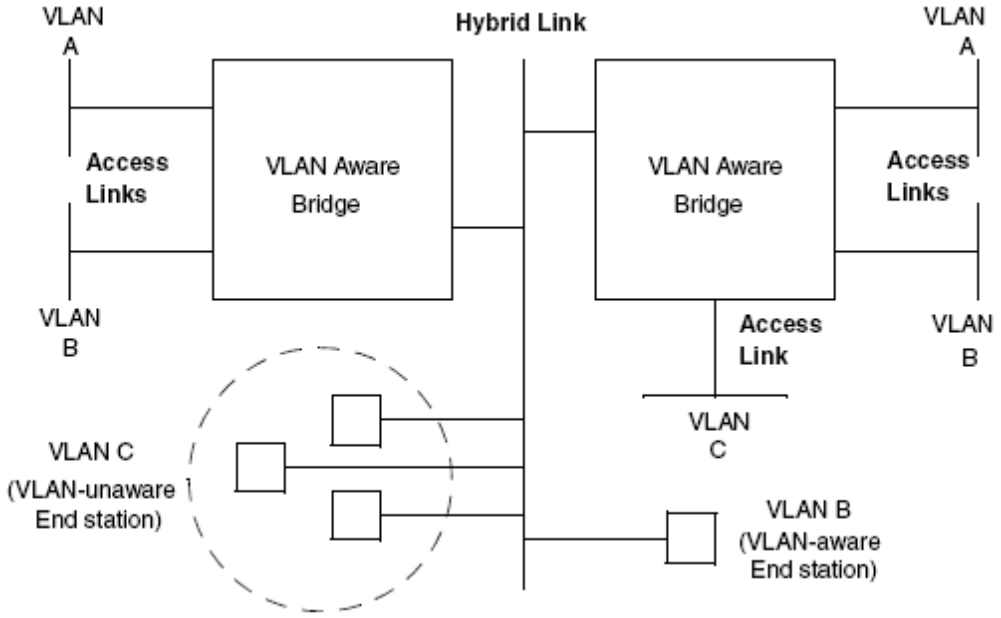


Rysunek 14. Typy połączeń między urządzeniami w sieciach VLAN (Źródło: opis standardu 802.1Q, wersja 2003, www.ieee.org)

3.3 Połączenia hybrydowe (Hybrid link)

Połączenie hybrydowe jest kombinacją połączeń typu access i trunk. Pojawia się ono kiedy segment sieci zawiera jednocześnie urządzenia świadome i nieświadome istnienia sieci VLAN. W wyniku takiego wymieszania urządzeń VLAN-aware i VLAN-unaware, połączenie to musi być zdolne do transportu ramek znaczonych i nieznaczonych jednocześnie. Inteligentne przełączniki mogę transportować ramki tagowane i nietagowane poprzez jeden

port bez większego problemu, jest to jedynie kwestia odpowiedniej konfiguracji przełącznika. Należy jednak pamiętać, że ramki należące do jednej sieci VLAN muszą wszystkie być znaczone albo nieznaczone. W sytuacji, gdyby część ruchu należącego do jednaj sieci VLAN była tagowana, a pozostała nie, przełącznik nie byłby w stanie połączyć go w jedną całość. Kolejną bardzo ważną rzeczą jest to, że wszystkie nieznaczone ramki mogą należeć tylko do jednej sieci VLAN. Powód jest taki sam jak wcześniej, nie da się ich rozróżnić. Dlatego bardzo ważne jest, aby na obu portach przełączników, do których wpięte jest łącze hybrydowe była ustawiona ta sama natywna sieć VLAN[14]. Gdyby doszło do takiej sytuacji, że na jednym porcie natywną siecią jest VLAN B, a na drugim VLAN C to ruch tych sieci zostałby nieświadomie połączony.



Rysunek 15. Połączenie hybrydowe w sieciach VLAN(Źródło: opis standardu 802.1Q, wersja 2003, www.ieee.org)

Rysunek nr 14 przedstawia przykładową sieć, w której występuje połączenie hybrydowe. Łączy ono ze sobą dwa inteligentne i świadome przełączniki oraz zawiera przyłączone dodatkowo kilka komputerów. Jeden z komputerów jest świadomy istnienia sieci wirtualnych i należy do VLAN B (tak też tagowane są wysyłane i odbierane przez niego ramki). Reszta komputerów to komputery[15] typu VLAN-unaware, ramki które one odbierają i

[14] Jest to ważne, ponieważ ramki nieznaczone wysyłane przez port mogą należeć tylko do natywnej sieci VLAN tego portu, czyli do tej, do której zapisany jest port (decyduje o tym identyfikator PVID).

[15] Grupa urządzeń nieświadomych istnienia sieci VLAN określana jest też po angielsku mianem „legacy segment”.

wysyłają są nieoznaczone. Aby wszystkie komputery[16], będące w wirtualnej sieci VLAN C, mogły się poprawnie komunikować, wymagana jest odpowiednia konfiguracja portów na przełącznikach, do których wpięte jest połączenie hybrydowe. Porty muszą być skonfigurowane do jawnego przenoszenia tagowanych ramek sieci VLAN A i B oraz do przenoszenia ramek standardowych (ang. *native*). W powyższym przypadku porty są ustawione tak by przyjmować ramki nieoznaczone i przypisywać je do sieci natywnej portu, którą musi być sieć VLAN C. Sieci natywna portu jest określana jako PVID (ang. *Port VLAN ID*).

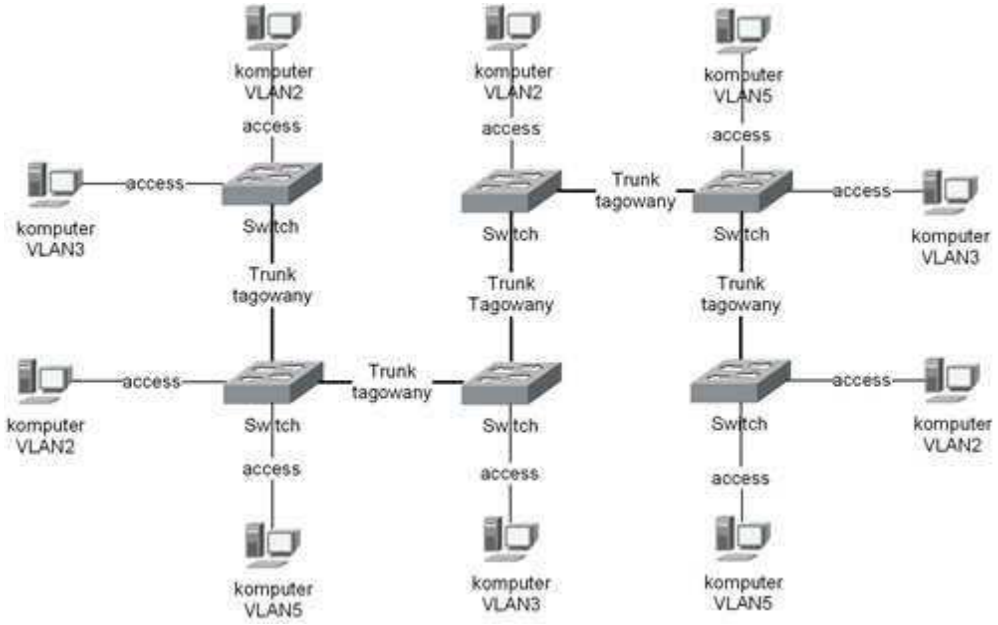
3.4 Podsumowanie rozdziału

Podział łączy przedstawiony w tym rozdziale, jest zgodny ze standardem 802.1Q. Niestety, w wyniku ciągłego, bujnego rozwoju sieci VLAN i dążenia to coraz większej elastyczności, podział ten uległ spłaszczeniu i częściowemu zatarciu. Aktualnie producenci rozróżniają już tylko połączenia Access i Trunk. Z tym, że obecnie połączenia określane jako Trunk są w rzeczywistości złożeniem połączeń trunkingowych i hybrydowych opisanych w tym rozdziale. Oznacza to, że połączenia typu Trunk służą do przenoszenia ruchu tagowanego i nietagowanego jednocześnie, zgodnie ze wszystkimi zasadami dotyczącymi łączy hybrydowych, które zostały wcześniej opisane.

[16] Chodzi tu szczególnie o pojedynczy komputer podpięty do przełącznika.

Rozdział IV Oznaczanie ramek w sieciach VLAN (VLAN Tagging lub Frame Tagging)

Oznaczanie ramek w sieciach VLAN jest jedną z najważniejszych podstaw ich istnienia, ponieważ bez tagowania nie możliwe jest budowanie połączeń trunkingowych między urządzeniami VLAN-aware. To dzięki tagowaniu ramek, przełączniki potrafią rozróżnić ruch należący do różnych sieci wirtualnych, który przychodzi do nich na port trunkingowy.



Rysunek 16. Dzięki połączeniom trunkingowym i tagowaniu komputery jednej sieci VLAN będące w różnych segmentach sieci mogą się ze sobą komunikować (opracowanie własne)

W sieciach VLAN wyróżnia się dwa typy ramek:

- Ramki nieoznaczone (nietagowane, ang. *untagged Frames*) – ramki te są standartowymi ramkami sieci Ethernet i nie zawierają one żadnych dodatkowych informacji, które mogły by posłużyć do ustalenia ich przynależności do sieci VLAN. Ten typ ramek może być przetwarzany przez urządzenia świadome oraz nieświadome istnienia sieci VLAN.
- Ramki oznaczone (tagowane, ang. *tagged Frames*) – są to ramki zawierające dodatkowe informacje, które pozwalają określić ich przynależność do sieci VLAN. Są one zrozumiałe tylko dla urządzeń VLAN-aware. Standard 802.1Q specyfikuje ponadto specjalny rodzaj ramek tagowanych, w których identyfikator VID równy jest 0. Ten typ ramek używany jest jedynie w celu nadania mi priorytetu (ang. *priority-tagged Frmes*)[17].

[17] Dokładniejszy opis ustawiania priorytetu w ramkach standardu 802.1Q znajduje w części pracy pod tytułem „Opis protokołu IEEE 802.1Q”.

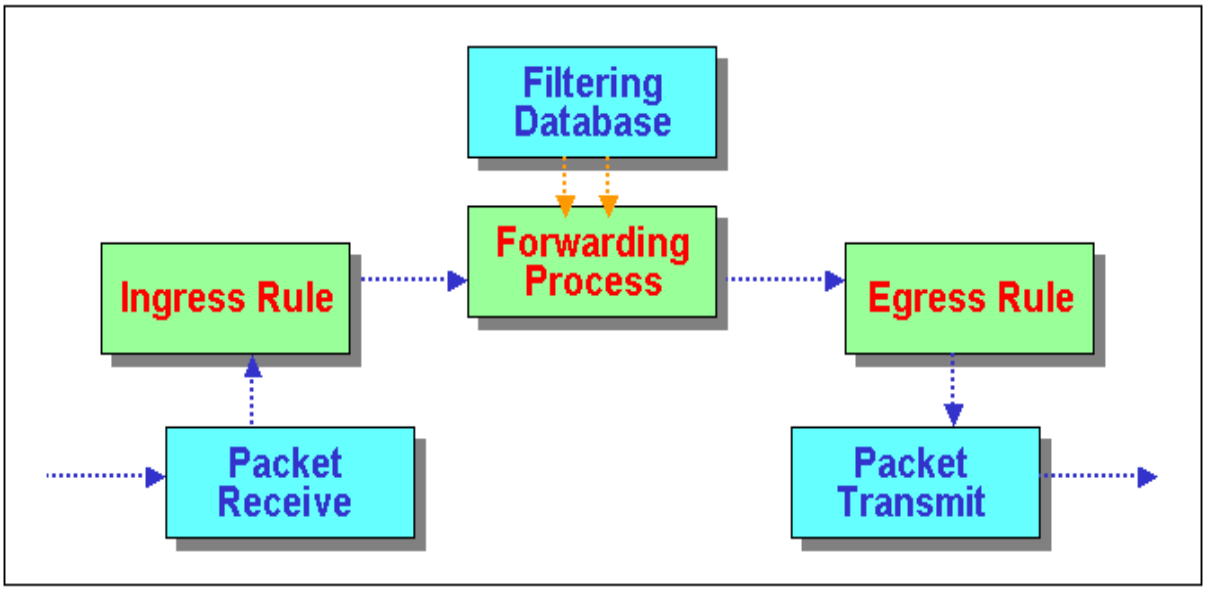
Z oznaczaniem ramek związane są dwa ważne skróty VID oraz PVID. VID (ang. *VLAN identifier*) jest identyfikatorem używanym do tagowania ramek w połączeniach trunkingowych i oznacza on, do której sieci VLAN należy konkretna ramka. PVID (ang. *Port VLAN identifier*) zwany także natywnym VID (ang. *native VLAN identifier*) jest identyfikatorem sieci VLAN na porcie przełącznika. PVID ustala do jakiej sieci VLAN należą ramki nieoznaczone[18] przychodzące na dany port. Każdy port na przełączniku musi mieć przypisany swój PVID. W przypadku sieci VLAN bazujących na portach przełącznika, kiedy administrator chce statycznie przypisać port od konkretnej sieci VLAN, robi to właśnie za pomocą identyfikatora PVID.

W początkowej fazie rozwoju sieci VLAN, kiedy nie było jeszcze sprecyzowanego, jednego standardu oznaczania ramek, producenci sprzętu tworzyli swoje własne protokoły i standardy służące do tagowania. Efektem tego była sytuacja, w której powstało wiele różnych protokołów wzajemnie ze sobą niezgodnych. Protokoły działały dobrze i spełniały swoje zadanie, ale tylko w homogenicznym środowisku na sprzęcie jednego producenta. Zaistniała potrzeba stworzenia jednego uniwersalnego standardu, który pozwoliłby na funkcjonowanie sieci VLAN w heterogenicznym środowisku z użyciem sprzętu sieciowego różnych producentów. Odpowiedzią na to zapotrzebowanie było stworzenie przez grupę amerykańskich inżynierów z IEEE standardu 802.1Q, który dokładnie specyfikuje sposób tagowania ramek. Obecnie protokół 802.1Q jest najczęściej wykorzystywanym protokołem w sieciach VLAN. Zasługą tego jest to, że protokół ten został bardzo dobrze przyjęty przez producentów sprzętu sieciowego i prawie wszyscy go zaimplementowali w swoje urządzenia. Drugim pod względem częstości występowania jest autorski protokół ISL firmy Cisco. Przyczyną takiego stany rzeczy jest to, że firma Cisco jest potentatem w dziedzinie urządzeń sieciowych i duża ilość istniejących sieci VLAN jest środowiskiem homogenicznym, zbudowanym wyłącznie na przełącznikach tej firmy.

4.1 Przetwarzanie ramek w sieciach VLAN

Proces przetwarzania ramek na urządzeniach VLAN-aware takich jak inteligentne przełączniki, składa się z trzech podstawowych etapów: procesu odbierania (ang. *ingress process*), procesu forwardownia (ang. *forwarding process*) i procesu wysyłania (ang. *egress process*).

[18] Dokładniej ramki nieoznaczone oraz ramki oznaczone identyfikatorem VID 0 z priorytetem (ang. *priority-tagged frames*)



Rysunek 17. Proces przetwarzania ramek w sieciach VLAN (Źródło: global.zyxel.com/support/supportnote/ies1000/app/8021q.htm, 1.07.2006)

W procesie forwardowania czynny udział bierze baza danych filtrowania (ang. *Filtering Database*). Baza danych filtrowania przechowuje informacje o zarejestrowanych sieciach VLAN i portach, które są z nimi skojarzone, przez co organizuje przesyłanie ruchu wirtualnych sieci na oraz z portów przełącznika. Baza filtrowania składa się z tablicy wpisów statycznych (ang. *SVLAN table*) oraz tablicy wpisów dynamicznych (ang. *DVLAN table*). Wpisy statyczne są wprowadzane ręcznie przez administratora, dynamiczne są natomiast dopisywane automatycznie z użyciem takich protokołów jak GVRP lub VTP i administrator nie może w nie ingerować. Baza filtrowania specyfikuje zachowanie się przełącznika w odniesieniu każdego jego portu. Znajdują się w niej między innymi takie informacje jak: sieć VLAN zapisana do portu, typ obsługiwanych ramek(znakowane, nieznakowane lub oba) oraz czy dany port może forwardować ramki sieci VLAN.

Proces przetwarzania ramek:

- Proces odbierania (ingress procrss) na konkretnym porcie przełącznika:
  a) Jeżeli odebrana ramka jest typu znaczonego (posiada VID) przełącznik sprawdza czy dany port może odbierać takie ramki. Jeżeli nie może o ramka jest odrzucana, a gdy może ramka jest przesyłana do procesu forwardowania.

b) Jeżeli odebrana ramka jest typu nieoznaczonego przełącznik sprawdza czy może przyjąć taką ramkę na danym porcie. Jeżeli nie może to ramka jest odrzucana. Jeżeli jednak może ją przyjąć to najpierw pobiera on identyfikator VLAN portu, na którym ramka została odebrana (PVID), a następnie tworzy z tej ramki ramkę znakowaną z VID równym PVID portu i przesyła ją do procesu forwardowania.

- Proces forwardowania (forwarding process) – w procesie tym, z użyciem bazy danych filtrowania, ustalane jest, na które pozostałe porty przełącznika ramka ma być rozesłana. Należy pamiętać, że tylko ustalone porty przełącznika należące do sieci VLAN służą do wysyłania ruchu na zewnątrz. Zazwyczaj są to tylko niektóre porty tunkingowe lub port docelowy, do którego wpięty jest adresat ramki.

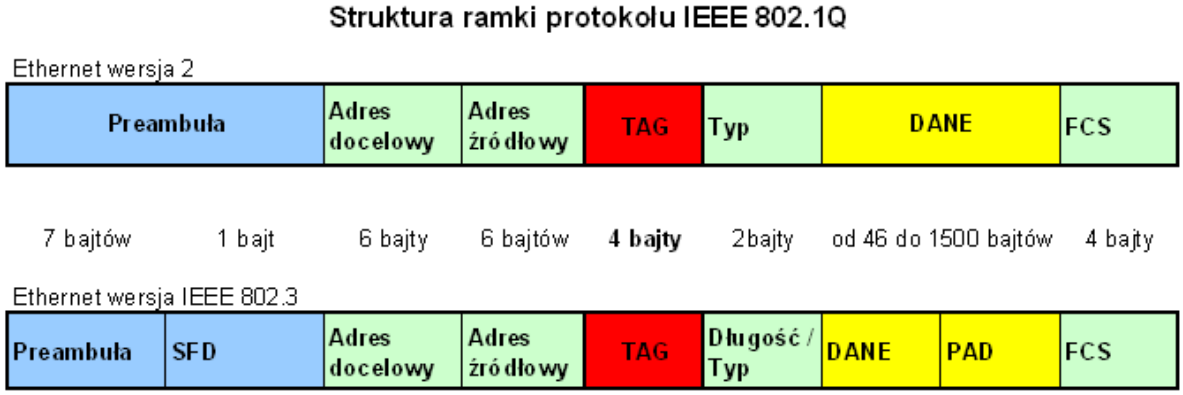
- Proces wysyłania (egress process) na konkretny porcie przełącznika:
  a) Jeżeli w bazie filtrowania znajduje się wpis, że dla konkretnej sieci VLAN na danym porcie ramka ma być wysłana bez oznaczeń, to z ramki przed wysyłką usuwane jest tagowanie po czym zostaje ona wysłana.
  b) Jeżeli w bazie filtrowania znajduje się wpis, że dla konkretnej sieci VLAN na danym porcie ramka ma być wysyłana w formie oznaczonej, to ramka zostaje wysłana razem z tagowaniem.

4.2 Opis protokołu IEEE 802.1Q

Standard 802.1Q został stworzony przez grupę amerykańskich inżynierów z organizacji IEEE (ang. *Institute of Electrical and Electronics Engineers*). Standard ten dokładnie specyfikuje działanie protokołu, który nosi taką samą nazwę - 802.1Q. 802.1Q jest jedynym uniwersalnym standardem w całości specyfikującym działanie sieci wirtualnych, który został zaakceptowany przez wszystkich producentów sprzętu sieciowego i zaimplementowany do ich urządzeń. Efektem tego jest możliwość budowania heterogenicznych, wirtualnych sieci komputerowych, opartych o urządzenia wielu producentów.

Protokół 802.1Q jest protokołem, tagowania wewnętrznego. Oznacza to, że do wnętrza standardowej ramki Ethernet dodawana jest dodatkowa paczka informacji zwana

nagłówkiem 802.1Q. Ramki, które mogą być tagowane przy użyciu tego standardu to Ethernet , Token-Ring oraz FDDI.



Rysunek 18. Struktura ramki Ethernet tagowanej według standardu IEEE 802.1Q (opracowanie własne)

Jak widać na rysunku 19 nagłówek protokołu 802.1Q (zwany tagiem) zostaje dołożony do ramki Ethernet między pola „Adres źródłowy” i „Długość/Typ”. Wielkość nagłówka jest stosunkowo mała i wynosi jedynie 4 bajty[19] (dla porównania, protokół ISL dokłada aż 30bajtów). Minimalny i maksymalny rozmiar ramki, w wyniku dodania nowego elementu, zwiększają się i wynoszą odpowiednio 68 i 1522 bajty. Należy jednak pamiętać, że dołożenie do ramki oznaczenia, powoduje więcej zmian niż tylko wzrost jej rozmiaru. Dodatkowy element powoduje, że 32 bitowe pole FCS (ang. *Frame Check Sequence*) staje się nieaktualne (posiada błędną wartość) i należy od nowa policzyć wartość sumy kontrolnej ramki, która się w nim znajduje. Czynność ta jest automatycznie wykonywana przez przełącznik po każdym ściągnięciu i dołożeniu oznaczenia do ramki, ale niestety powoduje ona pewne opóźnienia w przesyłaniu ruchu.

Standard 802.1Q, poza ramkami tagowanymi i nietagowanymi, specyfikuje jeszcze jeden rodzaj ramek, są to ramki tagowane priorytetem (ang. *priority-tagged Frame*). Ramki tego typu są identyczne, w swej strukturze, ze zwykłymi rakami znaczonymi standardu 802.1Q, ale w miejscu identyfikatora sieci VLAN (VID) znajduje się wartość 0. Taki typ ramek, pod względem przynależności do sieci VLAN, jest przetwarzany tak jak ramki nieoznaczone[20]. Pole priorytetu w ramkach tagowanych oraz tagowanych priorytetem zostało stworzone by zapewnić ramkom Ethernet w sieciach VLAN zgodność z protokołem 802.1p.

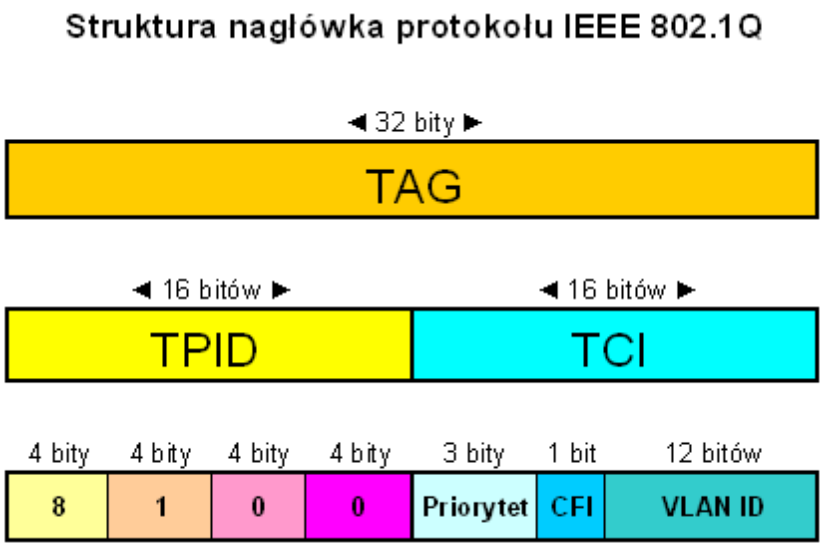
[19] Tylko gdy jest to ramka Ethernet. W przypadku ramki Token-Ring jest to 10 bajtów, a w przypadku FDDI długość jest zmienna i może dojść do 40 bajtów.

[20] Gdy wchodzą do przełącznika dodawany jest do nich identyfikator sieci zgodnym z natywnym VLANem portu (PVID).

Jest to protokół, który powstał w celu wprowadzenia do sieci Ethernet zaawansowanego sterowania[21] ruchem na poziomie warstwy drugiej modelu OSI i jest on bardzo ważnym elementem serwisu zapewnienia niezawodności usług QoS (ang. *Quality of Service*). Priorytetowanie ramek jest wykorzystywane na przykład w usłudze VoIP (ang. *Voice over IP*), w której opóźnienie dochodzenia ramek do celu ma wyjątkowo negatywny wpływ na jej jakość.

4.2.1 Analiza nagłówka protokołu 802.1Q dla ramek Ethernet

Nagłówek protokołu 802.1Q w przypadku ramki Ethernet ma wielkość 32 bity i jest to rozmiar całkowicie wystarczający do tego, by pomieścić w nim wszystkie niezbędne informacje dotyczące sieci wirtualnych oraz jej priorytet.



Rysunek 19. Struktura nagłówka protokołu IEEE 802,1Q w ramkach Ethernet (opracowanie własne)

Nagłówek składa się z dwóch podstawowych pół TPID oraz TCI. Pole TPID (ang. Tag Protocol Identifier) ma 16 bitów i rozkłada się dodatkowo na cztery koleje pola po 4 bity każde. W polu TPID zapisana jest stała wartość równa 0x8100, która oznacza ramkę znaczoną według standardu IEEE 802.1Q.TCI (ang. Tag Control Information) składa się z trzech pól, których znaczenie zostało opisane poniżej.

[21] W sensie priorytetownia ruchu.

Pole Priorytet (ang. *Priority*) – jest polem 3 bitowym i daje możliwość ustawienia priorytetu na ośmiu poziomach ważności od 0 do 7. Pole ma za zadanie zapewnić ramkom Ethernet w sieciach VLAN zgodność z protokołem 802.1p i usługą QoS.

User priority	Acronym	Purpose
0 (default)	BE	best effort
1	BK	background
2	-	spare
3	EE	excellent effort
4	CL	controlled load
5	VI	“video” < 100 ms latency and jitter
6	VO	“voice” < 10 ms latency and jitter
7	NC	network control

Rysunek 20. Tabela przedstawiająca priorytet ramki wraz typem ruchu do jakiego powinien być on stosowany (Źródło: http://www.cesnet.cz/doc/techzpravy/2003/l2qos/l2qos.pdf, 5.07.2006)

Pole CFI (ang. *Canonical Format Indicator*) – to 1 bitowe pole dające możliwość określenia czy adres MAC ramki Ethernet jest w formie kanonicznej czy niekanonicznej. Jeżeli wartość jest równa 0 to adres jest w formie kanonicznej. Wartość 1 w tym polu oznacza, że za polem „Długość/Typ” w ramce Ethernet znajduje się dodatkowe pole E-RIF (ang. Embedded RIF) o rozmiarze od 2 do 30 bajtów, a w nim 1 bitowy znacznik NCIF, w którym 0 oznacza adres kanoniczny, a 1 adres niekanoniczny.

Pole VLAN ID – pole to determinuje do jakiej sieci VLAN należy ramka. Pole jest 12 bitowe, więc daje możliwość obsługi 4096 sieci VLAN. Wartość 0 oznacza jednak, że jest to ramka tagowana priorytetem i należy ją przetwarzać tak jak ramkę nieoznaczoną.

4.2.2 Problem drzewa rozpinającego w standardzie 802.1Q

Protokół 802.1Q, według swojej specyfikacji, jest w stanie obsłużyć 4096 sieci VLAN. Jest to jednak tak ogromna liczba sieci wirtualnych, że prawdopodobnie nikt do tej pory jej nie osiągnął nawet w ramach sieci korporacyjnej[22]. Aby możliwe było wydajne działanie sieci komputerowych z taką liczbą sieci wirtualnych, poza sprzętem z górnej półki,

[22] Wykluczone są w tym stwierdzeniu warunki laboratoryjne, w których prawdopodobnie przetestowano ten wariant.

wymagane jest istnienie odpowiednich, wspomagających wirtualizację protokołów. Niestety, dwa najczęściej używane (już stosunkowo stare) i do niedawna jedyne protokoły budowania drzewa rozpinającego (ang. *Spinning Tree*) nijak się mają do tego postulatu. Protokoły STP (ang. *Spinning Tree Protocol*, IEEE 802.1d) i nowszy RSTP (ang. *Rapid Spinning Tree Protocol*, IEEE 802.1w), których zadaniem jest blokowanie nadmiarowych połączeń sieciowych w celu uniknięcia tworzenia się pętli, nienajlepiej współpracują ze standardem 802.1Q. Problemem tych protokołów jest to, że budują one tylko jedno drzewo rozpinające, ponieważ postrzegają całą topologię jako jedną logiczną sieć i nie widzą istniejących w niej sieci wirtualnych. Powoduje to, w najlepszym wypadku, całkowite blokowanie nadmiarowych połączeń trunkingowych, a co za tym idzie wykluczone jest rozkładanie między nie obciążeń (ang. *load balancing*). Przepustowość sieci, w których występuje kilkanaście lub nawet kilkadziesiąt sieci wirtualnych, przy tych protokołach drzewa rozpinającego, drastycznie spada. Innym częstym zjawiskiem jest doprowadzenie do tego, że jedna sieć wirtualna zostaje rozłączona na dwie części w wyniku zablokowania połączenia trunkingowego między nimi. Jednym rozwiązaniem tego problemu, które zresztą jest bardzo często stosowane, jest wyłączenie protokołów typu STP lub RSTP i dbanie przez administratora o nie występowanie pętli w sieciach VLAN we własnym zakresie. Innym, też stosowanym rozwiązaniem, jest konfigurowanie ręcznie wielu kopii protokołu STP dla każdej sieci VLAN. Metoda ta jednak jest mało wydajna, ponieważ bardzo mocno obciąża przełącznik przetwarzaniem informacji generowanych przez wszystkie kopie STP.

Firma Cisco bardzo szybko zauważyła problem współdziałania protokołów STP i RSTP ze standardem 802.1Q. Dlatego, aby wyjść mu na przeciw, stworzyła protokół PVST+[23], który dla każdej sieci VLAN buduje oddzielną instancję drzewa rozpinającego. Pozwala to na rozkładanie ruchu różnych sieci VLAN między różne połączenia trunkingowe, nie powoduje tworzenia się pętli[24], a przy tym nie obciąża przełącznika przetwarzaniem nadmiernej ilości danych. Należy jednak pamiętać, że protokół ten działa tylko na urządzeniach firmy Cisco i przez to nie rozwiązuje problemu na sprzęcie innych producentów.

Problem drzewa rozpinającego w standardzie 802.1Q został całkowicie rozwiązany dopiero, gdy organizacja IEEE stworzyła protokół MSTP (ang. *Multiple Spinning Tree Protocol*). Protokół ten najpierw został wyspecyfikowany jako oddzielny standard IEEE

[23] Jest to protokół stworzony na bazie protokołu PVST, który spełnia to samo zadanie ale w sieciach VLAN wykorzystujących protokół InterSwitch Link.

[24] Oznacza to, że ruch jednej sieci VLAN będzie przechodził zawsze tymi samymi połączeniami trunkingowymi, a ruch kolejnej innymi, ale też zawsze tymi samymi.

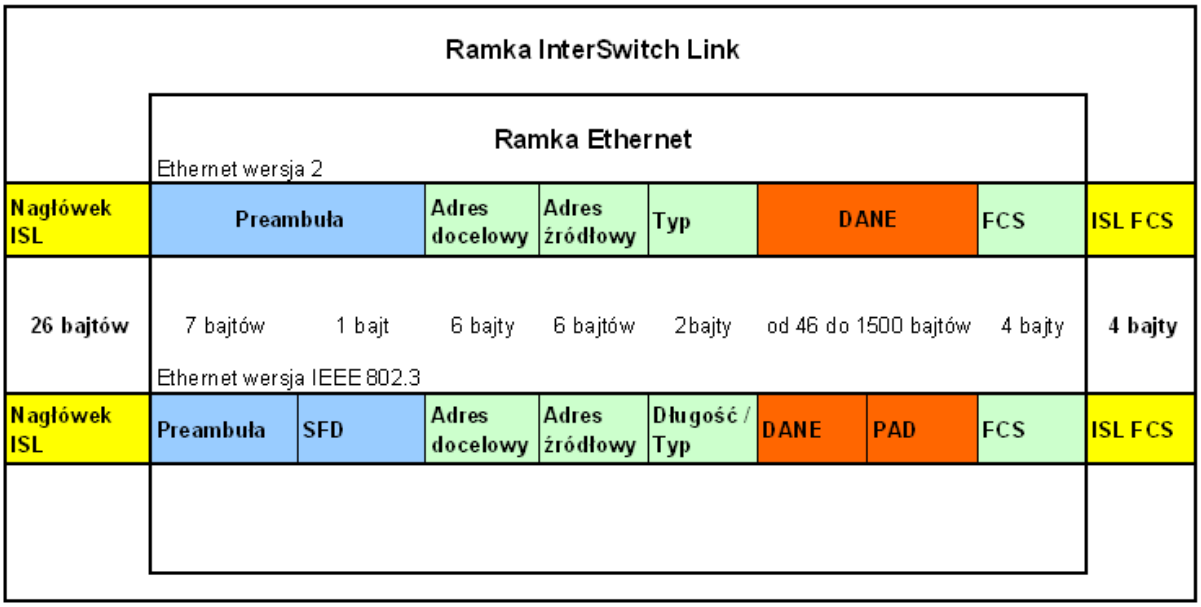
802.1s, a w 2003 roku został w całości włączony do standardu 802.1Q jako jego część. Pomysł na działanie MSTP jest, w ogólności, bardzo podobny do protokołu RVST+ firmy Cisco. Dla każdej sieci VLAN budowana jest oddzielna instancja drzewa rozpinającego. Jednak protokół ten pod względem wykorzystywanych mechanizmów i wydajności jest dużo bardziej zaawansowany niż produkt firmy Cisco i daje większe możliwości konfiguracyjne. Protokół MSTP jest protokołem otwartym i darmowym, więc wszyscy producenci sprzętu sieciowego korzystają z niego i implementują go w swoich urządzeniach.

4.3 Opis protokołu InterSwitch Link

Protokół ISL (ang. *InterSwitch Link*) jest protokołem stworzonym przez firmę Cisco, dlatego może on być używany tylko w sieciach komputerowych opartych o przełączniki tej firmy. ISL jest protokołem, który używa tzw. zewnętrznego tagowania ramek. Oznacza to, że do wnętrza ramek, przesyłanych połączeniem trunkingowym, nie są dodawane żadne nowe informacje, a jedynie są one enkapsułowane w ramkach ISL. Według firmy Cisco protokół ISL jest w stanie obsłużyć do 1000 sieci VLAN jednocześnie na połączeniach trunkingowych i nie powoduje to żadnych opóźnień w przesyłaniu danych. ISL współpracuje z protokołem PVST (ang. *Per VLAN Spanning Tree*), który także należy do firmy Cisco. Protokół ten działa w ten sposób, że dla każdej sieci VLAN tworzona jest osobna instancja drzewa rozpinającego (ang. *Spinning Tree*). Dzięki temu możliwe jest takie zarządzanie infrastrukturą sieci VLAN, że ruch należący do różnych sieci wirtualnych jest rozkładany między różne połączenia trunkingowe[25] (ang. *load balancing*) i nie tworzą się przy tym negatywne pętle.

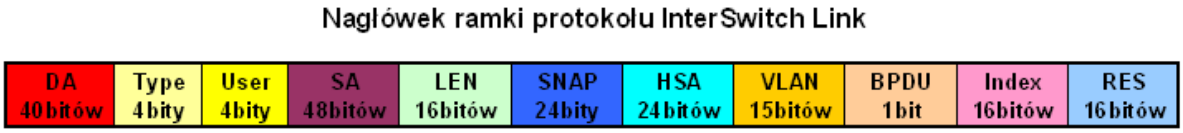
Rysunek 22 przedstawia przykładowe ramki ISL, które enkapsulują ramki Ethernet w wersji 2 i IEEE802.3 . Jedynymi elementami dodawanymi przez protokół ISL jest nagłówek ISL oraz pole ISL FCS, które zawiera informacje potrzebne do sprawdzania spójności przesłanej ramki (32 bitowa wartość CRC). Rozmiar ramki w stosunku do oryginalnej ramki Ethernet wzrasta zawsze o 30 bajtów, bo tyle zajmują informacje protokołu ISL. Te dodatkowe informacje są powodem, dla którego urządzenia VLAN-unaware od razu je odrzucają. Z drugiej strony, nawet gdyby zdołały je odebrać to nie byłyby w stanie nic odczytać z takiej ramki.

[25] Działa to na tej zasadzie, że dla jednych sieci VLAN pewne połączenia trunkingowe są zablokowane, a dla innych odblokowane. Fizycznie pętle połączeń trunkingowych istnieją, ale licznie już nie. Ruch sieci VLAN jest rozkładany miedzy te połączenia pół na pół.



Rysunek 21. Struktura ramki ISL (opracowanie własne)

4.3.1 Analiza nagłówka ramki protokołu InterSwitch Link



Rysunek 22. Struktura nagłówka ramki ISL (opracowanie własne)

Nagłówek ramki protokołu ISL składa się aż z jedenastu pół i ma rozmiar 26 bajtów, ponieważ musi on zawierać, oprócz informacji o sieci VLAN, także adres odbiorcy, typ enkapsułowanej ramki, priorytet oraz kilka dodatkowych informacji. Opis pól znajduje się poniżej.

Pole DA - adres docelowy (ang. *destination address*) – jest to pole o wielkości 40 bitów, które zawiera adres multicastowy „0x01-00-0C-00-00” lub „0x03-00-0C-00-00” informujący urządzenia VLAN-aware, że jest to ramka protokołu ISL.

Pole Frame Type – typ ramki – jest polem wielkości 4 bity i służy ono do identyfikacji typu enkapsułowanej ramki. Wartość 0000 oznacza ramkę Ethernet, 0001 ramkę Token-Ring, 0010 ramkę FDDI, a 0011 ramkę ATM.

Pole User Define Bits – bity priorytetu – jest to 4 bitowe, opcjonalne pole nadające ramce priorytet, które jest używane jako rozszerzenie pola Frame Type, w przypadku gdy enkapsułowaną ramką jest ramka typu Ethernet. Dzięki temu ramka z wyższym priorytetem może osiągnąć cel dużo szybciej niż ramki pozostałe. Istnieją cztery możliwe wartości pola: XX00 – priorytet normalny, XX01 – priorytet 1, XX10 – priorytet 2, XX11 – najwyższy priorytet.

Pole SA – adres źródła – (ang. *source address*) – jest to 48 bitowy adres MAC portu urządzenia wysyłającego (zwykle przełącznika), z którego ramka została wysłana.

Pole Length – rozmiar ramki – jest to 16 bitowe pole przedstawiające rozmiar całej ramki ISL z wyłączeniem pół: DA, Frame Type, User, SA, Lenght and FCS. Całkowity rozmiar wyłączonych pól to 18 bajtów, więc wielkość tam wpisana to zawsze rozmiar całej ramki ISL minus 18 bajtów.

Pole SNAP – jest to pole o wielkości 24 bitów, które zawiera stałą wartość „0xAAAA03”

Pole HSA – starsze bity adresu źródłowego (ang. *high bits source addess*) – jest to pole wielkości równej połowie wielkości adresu MAC (24 bity) i zawiera część adresu MAC identyfikującą producenta sprzętu, z którego została wysłana ta ramka. Równa się ono pierwszej połowie pola SA. Ma ono stała wartość „0x00-00-0C” ponieważ jest to identyfikator firmy Cisco, a tylko na takim sprzęcie działa protokół ISL.

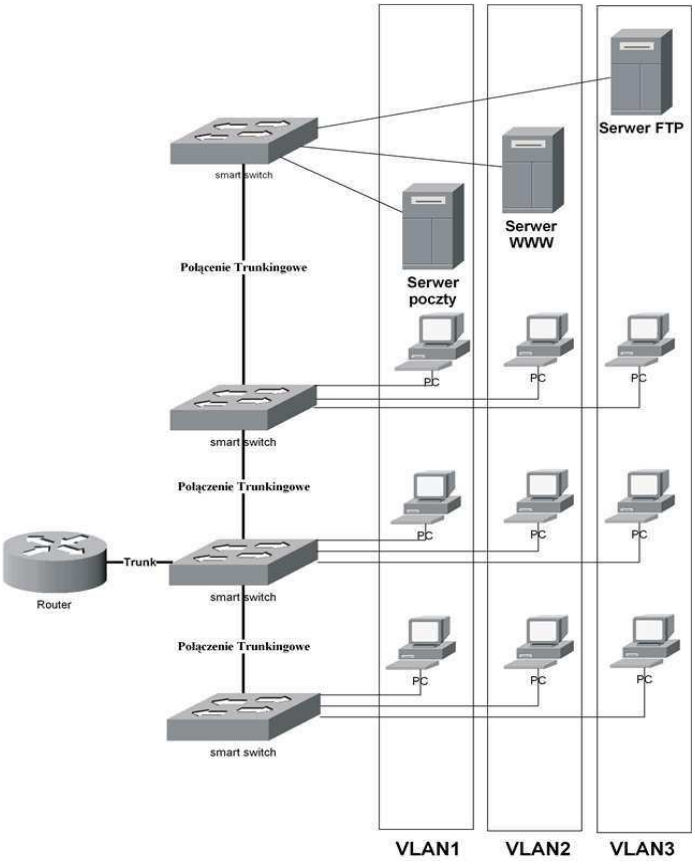
Pole VLAN – jest to pole identyfikujące sieć VLAN, do której należy enkapsułowana ramka. Pole to ma wielkość 15 bitów.

Pole BPDU (ang. Bridge Protocol Data Unit and Cisco Discovery Protocol Indicator) – jest to pole o wielkości tylko jednego bitu, ale informuje ono o tym, że ramka przenosi enkapsułowany pakiet BPDU (używany przez protokół STP do przenoszenia informacji o topologii sieci), pakiet CDP lub pakiet protokołu VTP.

Pole Index – jest to 16 bajtowa wartość, która określa numer portu źródłowego pakietu na switchu. Jest ono używane do celów diagnostycznych.
Pole RES – zarezerwowane (ang. *reserved*) – jest to 16 bitowe pole zarezerwowane dla ramek Token-Ring i FDDI enkapsułowanych w pakietach ISL. Na przykład, jeżeli jest to ramka Token-Ring to w tym miejscu są zapisane wartości pół Access Control i Frame Control z oryginalnej ramki. Dla ramek Ethernet pole to jest równe 0.

Rozdział V Trasowanie w sieciach wirtualnych

Trasowanie, czyli rutowanie (ang. *routing*), jest w sieciach VLAN tak samo ważne jak w każdych innych sieciach komputerowych. Jest to podstawowy sposób pozwalający na komunikowanie się między sobą urządzeń sieciowych znajdujących się w różnych podsieciach. W przypadku sieci wirtualnych, takimi podsieciami są domeny rozgłoszeniowe każdej sieci VLAN wraz z ich adresacją. Najczęstsza sytuacja jaka pojawia się w sieciach wirtualnych i wymaga rutingu została przedstawiona na rysunku 24. Każda z sieci VLAN zawiera jeden serwer, który jej użytkownicy wykorzystują do codziennej pracy. Ale czasami pojawia się potrzeba, aby osoby z innej sieci VLAN mogły skorzystać z nie swojego serwera (np. WWW dla sieci VLAN1 i VLAN3). Sieci wirtualne są jednak całkowicie hermetyczne i nie pozwalają na jakiekolwiek „przeciekanie” ruchu jednej sieci do drugiej. Dlatego jedynym rozwiązaniem tego problemu jest wykorzystanie rutera, który otworzy użytkownikom każdej z sieci VLAN dostęp do pozostałych serwerów[26].



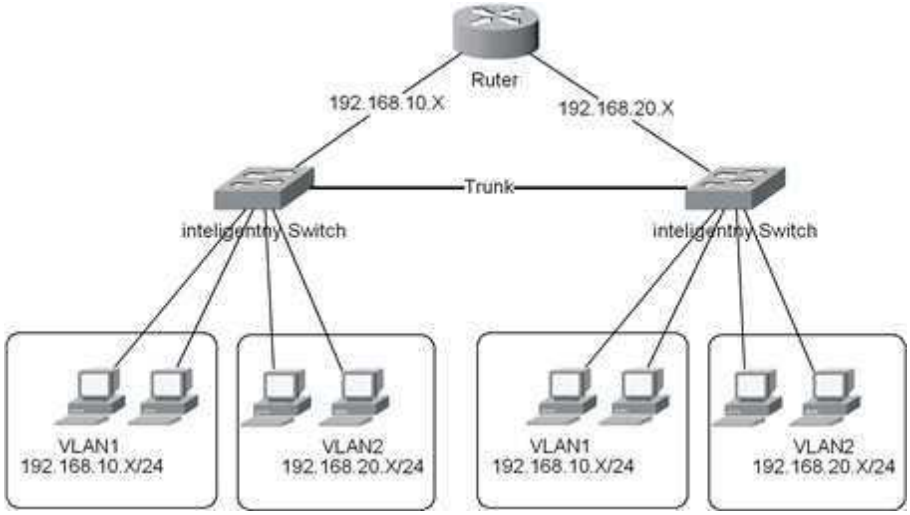
Rysunek 23. Infrastruktura trzech sieci wirtualnych wraz z ruterem, który umożliwia przesyłanie ruchu sieciowego miedzy nimi (opracowanie własne)

[26] Otworzy także dostęp do wszystkich innych urządzeń pozostałych sieci VLAN, ale w tym wypadku zmartwieniem administratora sieci jest zbudowanie takich list ACL lub innych zabezpieczeń by użytkownicy mieli dostęp tylko do wybranych zasobów sąsiadujących sieci.

Poniżej zostały opisane trzy najpopularniejsze metody rutowania w sieciach wirtualnych. Każda z tych metod ma swoje zasadnicze wady i zalety, które należy brać pod uwagę podczas projektowania sieci wirtualnych.

5.1 Ruter z oddzielnym interfejsem dla każdej sieci VLAN

Rozwiązanie to polega na tym, że każda sieć wirtualna dołączona jest do rutera na jednym własnym fizycznym interfejsie tak jak ma to miejsce między standardowymi sieciach, gdzie wirtualność nie występuje.



Rysunek 24. Ruter z oddzielnym interfejsem dla każdej sieci VLAN(opracowanie własne)

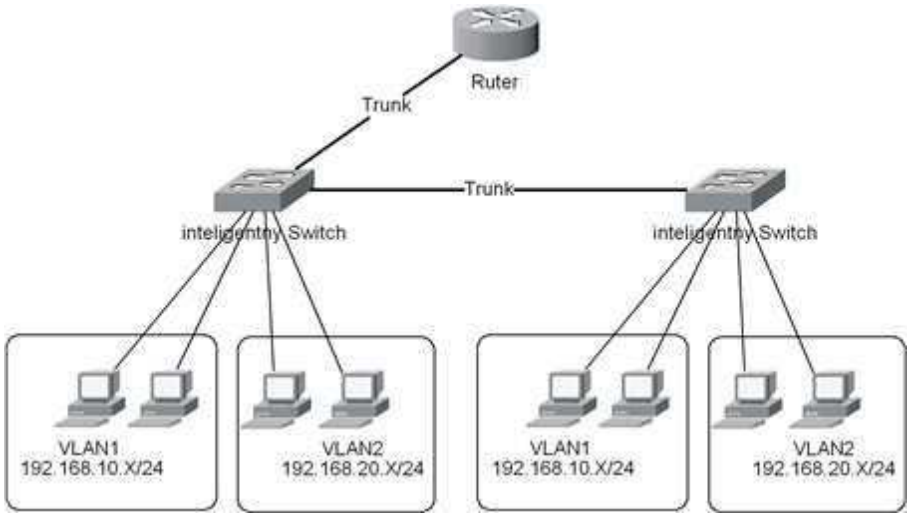
Na rysunku 25 przestawiono ruter, który pozwala na przesyłanie ruchu między sieciami VLAN1 i VLAN2. Obie sieci wirtualne są podłączone z ruterem za pomocą oddzielnych interfejsów, które posiadają adresy do niech należące. Interfejs, z adresem należącym do podsieci 192.168.10.X, doprowadza do rutera ruch sieci VLAN1. Natomiast interfejs, z adresem należącym do podsieci 192.168.20.X, przesyła ruch sieci VLAN2.

Podstawowymi zaletami tego rozwiązania są: prostota konfiguracji oraz duża przepustowość, dzięki zastosowaniu oddzielnych połączeń. Każdy z interfejsów może transportować ruch sieci VLAN do niego należącej ze swoją maksymalną szerokością pasma. Największą wadą tej metody jest ograniczona ilość obsługiwanych sieci VLAN. Ruter może

trasować ruch tylko tylu sieci wirtualnych ile interfejsów posiada[27]. Ten typ rutowania w sieciach VLAN jest najstarszym stosowanym sposobem i nadal najpopularniejszym w małych topologiach.

5.2 Ruter na patyku (Ruter on the stick)

Topologia znana pod nazwą „ruter na patyku” stała się popularna, gdy w sieciach komputerowych zaczęła powstawać duża liczba sieci wirtualnych. Rozwiązanie to polega na przyłączeniu rutera do istniejącej infrastruktury sieciowej za pomocą tylko jednego[28] z jego interfejsów i uczynienie tego połączenia połączeniem typu Trunk. Następnie na użytym interfejsie konfiguruje się wirtualne podinterfejsy – po jednym dla każdej sieci VLAN. W wyniku takiej konfiguracji rutera, każda sieć wirtualna posiada swój własny logiczny interfejs z adresem do niej należącym.



Rysunek 25. Topologia "ruter na patyku" (opracowane własne)

Zgodnie z rysunkiem 26 ruter jest połączony z siecią za pomocą jednego fizycznego połączenia. Jednak liczba faktycznych logicznych łączy zależy tylko od liczby wirtualnych sieci. W tym przypadku są tylko dwie.

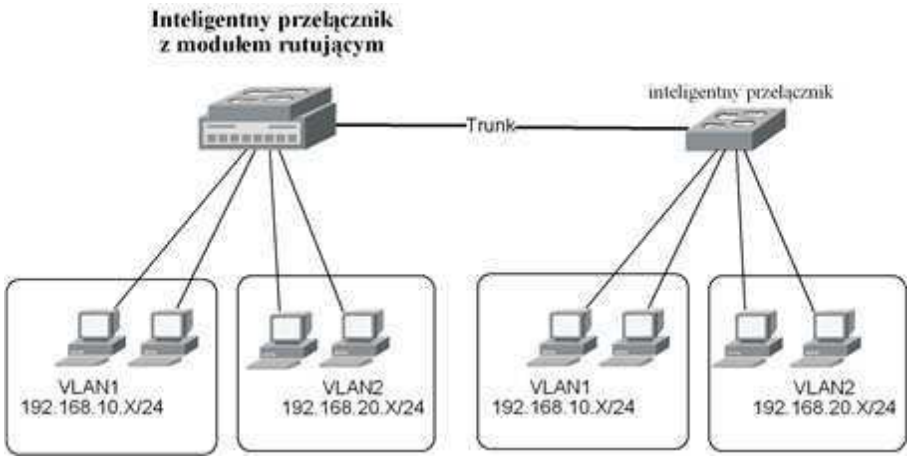
Zaletą topologii „ruter na patyku” jest możliwość obsługi przez jeden ruter dużej liczby sieci wirtualnych. Nie istnieje tutaj ograniczenie związane z ilością fizycznych interfejsów rutera. Charakter tego połączenia powoduje jednak, że pojawia się wada związana

[27] Standardowo rutery posiadają do dziesięciu różnych interfejsów, ale można dokupić specjalne moduły z dodatkowymi portami, jest to jednak bardzo drogie.
[28] Jednego lub więcej, istotą rozwiązania jest to, że pozwala na istnienie wirtualnych interfejsów.

w przepustowością łącza pełniącego funkcję połączenia Trunk. Na niewiele się zda możliwość połączenia wielu sieci wirtualnych za pomocą jednego połączenia jeżeli jego przepustowość będzie niewielka. Dlatego w przypadku większej ilości sieci VLAN, ich ruch należy rozkładać równomiernie na wszystkie interfejsy rutera[29] i tworzyć na nich podinterfejsy.

5.3 Przełącznik z modułem rutującym

Przełączniki umożliwiające rutowanie, dzięki zamontowanemu w nich modułowi rutującemu są jednym z najnowszych technologicznie rozwiązań w sieciach komputerowych. Urządzenia te są swego rodzaju hybrydami przełącznika i rutera w jednym. Dzięki temu, że dwa logiczne urządzenia są zintegrowane w jednym fizycznym, są one w stanie zapewnić dużo większą wydajność niż oddzielny przełącznik i ruter spięte ze sobą łączem nawet o dużej przepustowości.



Rysunek 26. Inteligentny przełącznik z modułem rutującym (opracowanie własne)

Konfiguracja zintegrowanego rutera polega na odpowiedniej konfiguracji wirtualnych interfejsów, które mają takie same oznaczenia jak sieci VLAN. Na przykład, jeżeli w sieci istnieje sieć wirtualna VLAN 2 to interfejs rutera też będzie nazywał się VLAN 2. Reszta konfiguracji przebiega dokładnie tak samo jak na standardowym ruterze zewnętrznym.

Przełączniki zawierające moduły rutujące są urządzeniami z górnej półki i zazwyczaj pełnią one funkcje przełącznika głównego w całej sieci. Przełączniki takie, oprócz rutowania, mogą spełniać na przykład funkcję serwera VMPS, DHCP lub VTP.

[29] W taki sposób, że jedna sieć VLAN może znajdować się tylko na jednym z interfejsów. Nie mogą istnieć dwa logiczne połączenia jednej sieci.

Rozdział VI Protokoły i mechanizmy wykorzystywane w wirtualnych sieciach LAN

6.1 Protokoły wspomagające automatyczną konfigurację sieci wirtualnych

Konfiguracja sieci wirtualnych w dużej sieci komputerowej, w której wykorzystywanych jest kilkadziesiąt przełączników jest dużym wyzwaniem dla administratora. Nie byłoby to tak wielki problem, gdyby sprzęt sieciowy konfigurowało się statycznie raz na długi czas, a w sieci nie byłoby żadnych zmian. Niestety takie sytuacje nie zdarzają się prawie nigdy. W sieci zawsze następują jakieś zmiany. Najczęściej użytkownicy zmieniają swoje miejsca pracy (zatem także przełączniki do których są wpięci) lub dodawane są nowe sieci i usuwane stare już niepotrzebne. Zmartwieniem administratora jest śledzić przemieszczanie się użytkowników i tak konfigurować sieć komputerową by wciąż mieli oni dostęp do swoich sieci VLAN. W ekstremalnej sytuacji mogłoby dojść do tego, że jedynym zajęciem administratora byłoby bieganie od przełącznika do przełącznika i konfigurowanie sieci VLAN tak by ich ruch mógł być przesyłany przez szkielet sieci[30]. W sieciach zdarzają się też awarie urządzeń sieciowych, ich konfiguracja zazwyczaj wtedy jest tracona i trzeba ją stworzyć od nowa.

Aby zapobiec sytuacji przedstawionej powyżej, zostały stworzone protokoły, które umożliwiają automatyczne konfigurowanie sieci VLAN na urządzeniach sieciowych w obrębie całej topologii. Do protokołów automatycznej konfiguracji należą między innymi: protokół GVRP (ang. *GARP(Generic Atribute Registration Protocol) VLAN Registration Protocol*) oraz protokół VTP (ang. *VLAN Trunk Protocol*).

Protokół GVRP został stworzony przez amerykańską organizację IEEE i jest zdefiniowany w standardzie 802.1P. GVRP jest protokołem z rodziny protokołów bazujących na protokole GARP, a jego komunikaty są przesyłane tylko i wyłącznie w ramkach znaczonych z użyciem protokołu 802.1Q. Protokół ten umożliwia automatyczne, dynamiczne konfigurowanie się sieci VLAN na przełącznikach, dzięki temu, że każdy przełącznik rozgłasza do przełączników sąsiadujących swoje sieci VLAN za pomocą wiadomość GVRP PDU (ang. GVRP Protocol Data Unit). Pozostałe przełączniki odbierając te wiadomości

[30] Należy pamiętać, że aby ruch sieci VLAN mógł być przesłany do jednego przełącznika do drugiego, wszystkie przełączniki pośredniczące też muszą posiadać te sieci VLAN w swoich bazach.

„uczą się” tych sieci wirtualnych, poprzez konfigurowanie siebie do ich obsługi. Drugim bardzo istotnym mechanizmem oferowanym przez protokół GVRP jest „*pruning*”. Działanie „*pruningu*” polega na blokowaniu ruchu rozgłoszeniowego, konkretnej sieci VLAN, przesyłanego przez połączenia trunkingowe na przełączniki, które w danej chwili nie posiadają wpiętych urządzeń w niej operujących. Dzięki temu poprawia się wydajność sieci, bo oszczędzana jest przepustowość łączy przez „wycinanie” niepotrzebnego ruchu. Protokół GVRP może przesyłać swoje wiadomości tylko za pomocą połączeń trunkingowych, w których ruch jest znaczony z użyciem protokołu 802.1Q. Wszystkie urządzenia z włączonym protokołem GVRP mają w sieci równorzędny status, oznacza to, że nie ma tam podziału na serwer i klientów. Protokół GVRP przewiduje także możliwość niestandardowej konfiguracji swoich mechanizmów. Niektóre przełączniki mogą mieć wyłączone „uczenie się” GVRP (nie konfigurują się one wtedy automatycznie) lub „reklamowanie” GVRP (nie rozsyłają informacji o swoich sieciach VLAN).

Protokół VTP jest protokołem firmy Cisco i może on być używany tylko na przełącznikach tej firmy. Działa on tylko na przełącznikach spiętych ze sobą za pomocą łączy trunkingowych, a ruch w tych połączeniach może być znaczony za pomocą protokołu 802.1Q, jak również enkapsułowany protokołem InterSwitch Link[31]. VTP, tak jak GVRP, oferuje mechanizm automatycznej, dynamicznej konfiguracji sieci VLAN na przełącznikach oraz blokowanie niepotrzebnego ruchu rozgłoszeniowego (*VTP pruning*). „Pruning” działa w protokole VTP tak samo jak w GVRP, natomiast mechanizm automatycznej konfiguracji operuje w sposób odmienny. W mechanizmie VTP administrator wybiera w sieci jeden główny przełącznik (ang. *core switch*), który konfiguruje do obsługi sieci VLAN i czyni serwerem VTP. Pozostałe przełączniki w sieci są konfigurowane jako klienci przełącznika serwera i od niego uczą się konfiguracji sieci VLAN. Na przełącznikach klientach VTP, manualna konfiguracja sieci VLAN[32] jest niemożliwa. W VTP, oprócz serwera i klienta, istnieje także trzeci tryb pracy przełącznika zwany przeźroczystym (ang. *transparent mode*), przełączniki tak skonfigurowane pozwalają na przekazywanie otrzymanych komunikatów VTP do innych przełączników (są pośrednikami), same natomiast maja własną konfigurację (nie pobieraną z serwera VTP), której nie rozgłaszają.

[31] Może również być znaczony za pomocą standardu 802.10 dla sieci Fiber Distributed Data Interface (FDDI) oraz mechanizmu LANE w sieciach ATM.
[32] Czyli ich dodawanie, usuwanie, zmienianie nazw lub innych parametrów (np. MTU lub stanu).

6.1.1 Analiza protokołu automatycznej konfiguracji sieci VLAN na podstawie protokołu VTP firmy Cisco.

Protokół VTP firmy Cisco ma trzy wersje, z których wersja pierwsza jest wersją najczęściej używaną w sieciach wirtualnych Ethernet. Wersja druga różni się od pierwszej jedynie obsługą sieci Token-Ring i innym zachowaniem się przełącznika w trybie transparent, natomiast pozostałe funkcje są identyczne. Wersja trzecia jest najnowsza, dostarcza nowe mechanizmy i różni się w dużym stopniu od wersji pierwszej i drugiej, ale potrafi z nimi częściowo współpracować. Wersje pierwsza i druga nie współpracują ze sobą, dlatego wszystkie przełączniki jednej domeny VTP muszą być skonfigurowane do obsługi tej samej wersji tego protokołu. Poniższy opis dotyczy działania wersji pierwszej i drugiej protokołu VTP w sieciach Ethernet.

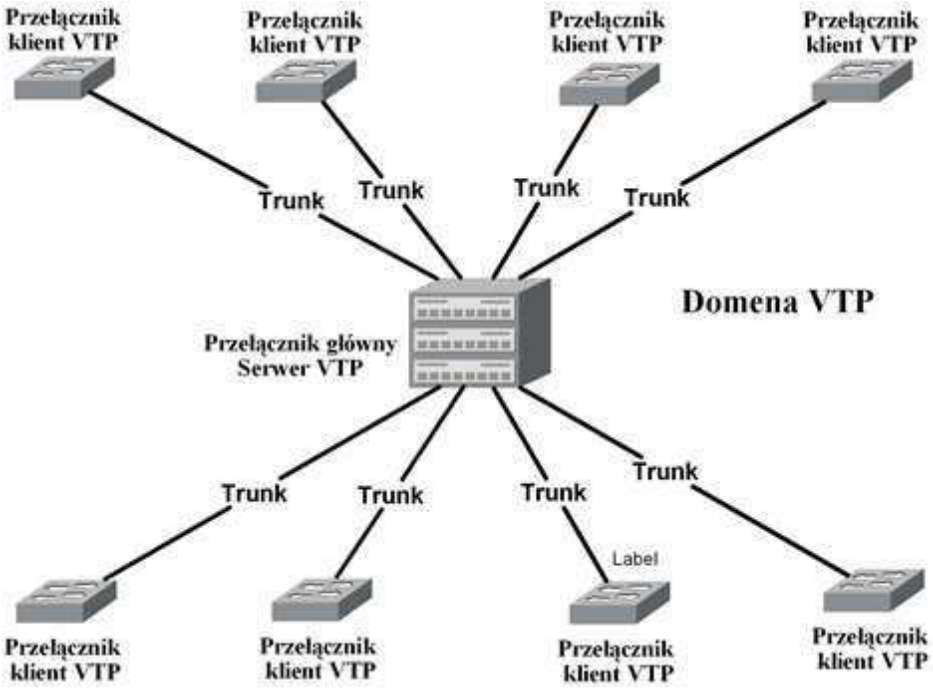
Przełączniki, z uruchomionym protokołem VTP, mogą pracować w trzech trybach: tryb serwera VTP, tryb klienta VTP oraz tryb przeźroczysty.

Tryb serwera (ang. VTP serwer mode) – na przełączniku pracującym w trybie serwera wszystkie sieci VLAN są zawsze dodawane, usuwane lub zmieniane ręcznie przez administratora. Konfiguracja jest zapisywana do pamięci NVRAM. Ustawiana jest także nazwa domeny VTP, której ten przełącznik jest serwerem. Serwer VTP ogłasza konfigurację sieci VLAN na połączeniach trunkingowych i synchronizuje w ten sposób konfigurację wszystkich przełączników klientów. Wszystkie przełączniki firmy Cisco przy pierwszym uruchomieniu domyślenie pracują w trybie serwera, ale nie mają ustawionej nazwy domeny.

Tryb klienta (ang. VTP client mode)– przełącznik pracujący w trybie klienta odbiera od serwera VTP, za pomocą połączeń trunkingowych, komunikaty o istniejących sieciach VLAN. Na ich podstawie, buduję on taką samą bazę danych sieci wirtualnych jaką posiada serwer. Jeżeli przełącznik klient jest połączony z innymi przełącznikami za pomocą połączeń trunkingowych, to przesyła on automatycznie do nich otrzymaną konfigurację.

Tryb przeźroczysty (ang. VTP transparent mode) – w wersji pierwszej VLAN Trunk Protocol przełącznik pracujący w trybie transparent ignoruje wszystkie komunikaty VTP po prostu je odrzucając. W drugiej wersji natomiast, przełączniki z trybem przeźroczystym ignorują komunikaty VTP ale ich nie odrzucają tylko przesyłają na pozostałe połączenia

trunkingowe tak jak ma to miejsce w trybie klienta. Tryb transparent pozwala przełącznikom posiadać swoją własną, niezależną konfigurację sieci VLAN, która nie jest ogłaszana.



Rysunek 27. VLAN Trunk Protocol (opracowanie własne)

W sieci może istnieć więcej niż jedna domena VTP. Ogłoszenia różnych domeny rozróżniane są po ich nazwach. Wszystkie przełączniki, które mają synchronizować konfigurację w wybranym serwerem VTP, muszą mieć skonfigurowana tą samą nazwę domeny co on.

6.1.1.1 Budowa pakietu protokołu VTP

Pakiety VTP są przesyłane łączami trunkingowymi tylko w postaci znaczonej z identyfikatorem VLAN równym 1[33] i mogą być oznaczane za pomocą protokołu ISL, 802.1Q lub LANE. Pakiety składają się z nagłówka VTP oraz wiadomości VTP.

Nagłówek pakietu protokołu VTP może mieć różną budowę i zależy to od typu wiadomości jaką niesie on ze sobą. Każdy pakiet zawiera jednak cztery obowiązkowe pola, są to: wersja protokołu VTP, typ wiadomości transportowanej przez pakiet, długość nazwy domeny zarządzania oraz nazwa domeny zarządzania. Najważniejsze z tych pól to typ

[33] Sieci VLAN 1 jest siecią zarządzania, z pomocą której komunikują się ze sobą między innymi przełączniki. Nie da się jej usunąć z przełącznika.

przenoszonej wiadomości. Protokół VTP obsługuje cztery typy wiadomości i należą do nich: ogłoszenie skonsolidowane, ogłoszenie szczegółowe, żądanie ogłoszeń, ogłoszenie przyłączenia się.

Ogłoszenie skonsolidowane (ang. *Sumary Advertisement Message*) – jest wysyłane przez każdy serwer VTP co 5 minut. Zwiera ono między innymi pola: nazwa domeny VTP, wersja ogłaszanej konfiguracji, stempel czasu, hash MD5 hasła domeny oraz ilość ogłoszeń szczegółowych, które należą do tego ogłoszenia zbiorowego. Bardzo ważnym polem jest wersja ogłaszanej konfiguracji, zawiera ono numer konfiguracji. Im liczba w tym polu jest wyższa tym przesyłana konfiguracja jest nowsza. Numer ten pomaga dowiedzieć się przełącznikom czy zawierają aktualną konfigurację. Ogłoszenie skonsolidowane samo w sobie nie zawiera konfiguracji, jest ona wysyłana dopiero w ogłoszeniach szczegółowych. Kiedy przełącznik odbiera ogłoszenie skonsolidowane, w pierwszej kolejności, sprawdza on nazwę domeny. Jeżeli nazwa domeny jest inna to ignoruje je i przesyła dalej do pozostałych przełączników, jeżeli natomiast nazwa domeny się zgadza to zaczyna przetwarzać ogłoszenie. Pierwszym krokiem przetwarzania jest sprawdzenie wersji przesyłanej konfiguracji, jeżeli jest ona taka sama lub starsza niż na przełączniku to przetwarzanie zostaje zakończone. Zazwyczaj jednak wersja ta jest nowsza i w takiej sytuacji przełącznik wysyła żądanie ogłoszeń.

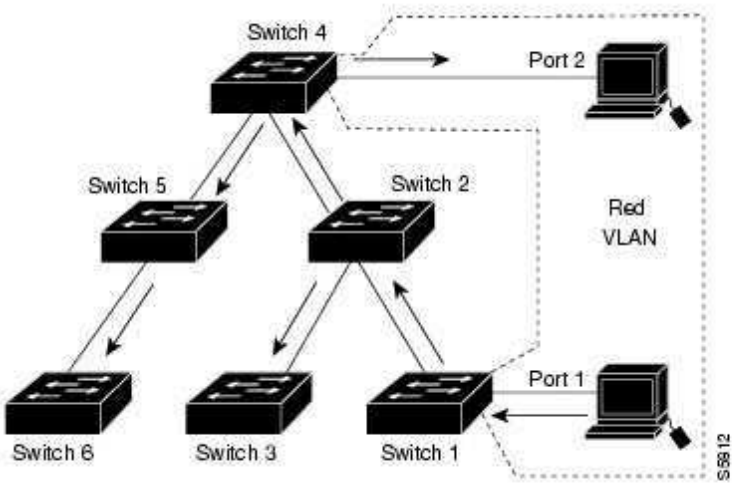
Ogłoszenie szczegółowe (ang. Subset Advertisement) – jest to ogłoszenie zawierające konfigurację pojedynczej sieci VLAN i jest ono wysyłane do przełącznika jako odpowiedź na żądanie ogłoszeń. Ilość przesyłanych do przełącznika ogłoszeń szczegółowych jest taka jak było to zapisane w ogłoszeniu skonsolidowanym, do którego przełącznik wysłał żądanie ogłoszeń i odpowiada ona zazwyczaj ilości sieci VLAN, które zostały dodane, usunięte lub ich konfiguracja się zmieniła.

Żądanie ogłoszeń (ang. *Advertisement Request*) – jest to prośba wysyłana przez przełącznik o dostarczenie mu ogłoszeń szczegółowych. Zapytanie to jest wysyłane w trzech przypadkach: przełącznik został zresetowany, nazwa domeny na przełączniku kliencie została zmieniona na inną, lub gdy konfiguracja na przełączniku jest starsza niż ta ogłaszana za pomocą ogłoszenia skonsolidowanego.

Ogłoszenie przyłączenia się (ang. *VTP Join Message*) – jest to ogłoszenie wysyłane przez przełącznik klienta VTP, gdy przyłącza się on do nowej domeny VTP, w którym informuje on serwer VTP o swoim istnieniu.

6.1.1.2 VTP pruning

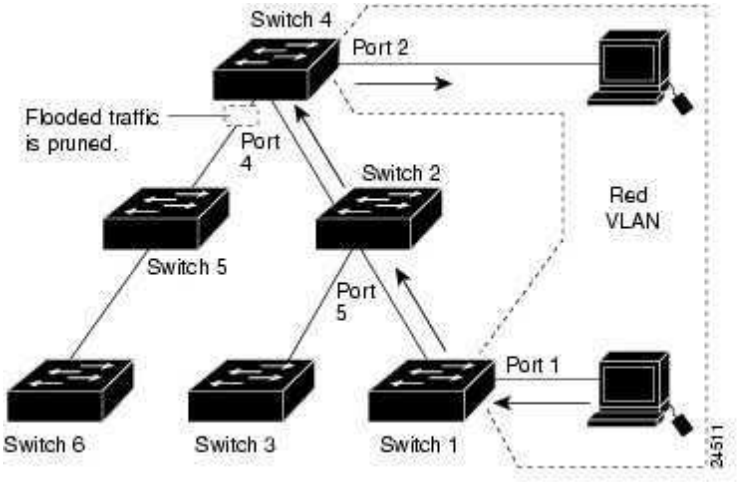
Zasada działania połączeń trunkingowych w sieciach VLAN zakłada, że ruch rozgłoszeniowy wysyłany w jednej sieci VLAN jest przesyłany za ich pomocą do wszystkich przełączników w sieci, które posiadają w bazię tą sieć VLAN, niezależnie od tego czy potrzebują one otrzymać ten ruch czy nie. W małych sieciach nie jest to duża wada, ale w sieciach korporacyjnych urasta do sporego problemu. W sieci, w której funkcjonuje kilkanaście przełączników, a jedna z sieci VLAN ma użytkowników tylko na dwóch przełącznikach, wysyłanie rozgłoszenia takiej sieci VLAN na wszystkie przełączniki jest ogromnym marnowaniem przepustowości łączy. Niech w sieci znajdzie się kilka takich sieci VLAN, to tworzony przez nie ruch rozgłoszeniowy może okazać się przyczyną „zapychania się sieci”.



Rysunek 28. Rozgłoszenie w sieci bez mechanizmu VTP pruning (Źródło: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008019f048.html, 8.07.2006)

Zgodnie z tym, co zostało opisane już wcześniej, mechanizmem wymyślonym by rozwiązać ten problem jest VTP pruning. Służy on do blokowania przesyłania przez przełączniki ruchu rozgłoszeniowego sieci VLAN na te części infrastruktury sieciowej, w których nie ma odbiorców tego ruchu. Mówiąc inaczej, ruch rozgłoszeniowy sieci VLAN jest przesyłany tylko między tymi przełącznikami, które bezpośrednio pośredniczą w

przekazywaniu ruchu sieci VLAN z przełącznika źródłowego do przełącznika docelowego (lub przełączników docelowych)[34].



Rysunek 29. Rozgłoszenie w sieci z mechanizmem VTP pruning (Źródło: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008019f048.html, 8.07.2006)

VTP pruning jest domyślnie wyłączone na przełącznikach firmy Cisco i aby działało należy go włączyć. VTP pruning działa na podstawie tego samego protokołu VTP, który został opisany powyżej i obsługuje go dodatkowy typ wiadomości. Funkcjonowanie VTP pruning polega na przesłaniu przez przełącznik ogłoszenia do przełączników sąsiadujących, że dana sieci VLAN stała się na nim aktywna lub jest nadal nieaktywna. Przełączniki sąsiadujące zapisują tą informację i wykorzystują ją później, gdy decydują którymi łączami trunkingowymi przesłać ruch rozgłoszeniowy dalej. Po włączeniu mechanizmu VTP pruning na przełączniku, domyślnie działa on dla wszystkich istniejących sieci VLAN oprócz sieci VLAN 1. Sieć VLAN 1 jest siecią specjalnego znaczenia i nazywa się ją siecią zarządzania. Jest to sieć VLAN, którą komunikują się ze sobą urządzenia VLAN-aware i włączenie w niej mechanizmu VTP pruning jest niemożliwe. Zakres sieci VLAN, które są objęte działaniem VTP pruning można konfigurować ręcznie za pomocą polecenia „*set vtp pruneeligible zakres_sieci_vlan*”[35].

[34]Przełącznik źródłowy oznacza przełącznik, w którym znajduje się komputer wysyłający rozgłoszenie, a przełączniki docelowe to te, do których wpięci są odbiorcy tego ruchu. Wszystkie komputery są w jednym VLANie.

[35] Dla przełącznika Cisco Catalyst 6500 z oprogramowaniem Cisco Operating System w wersji 8.1

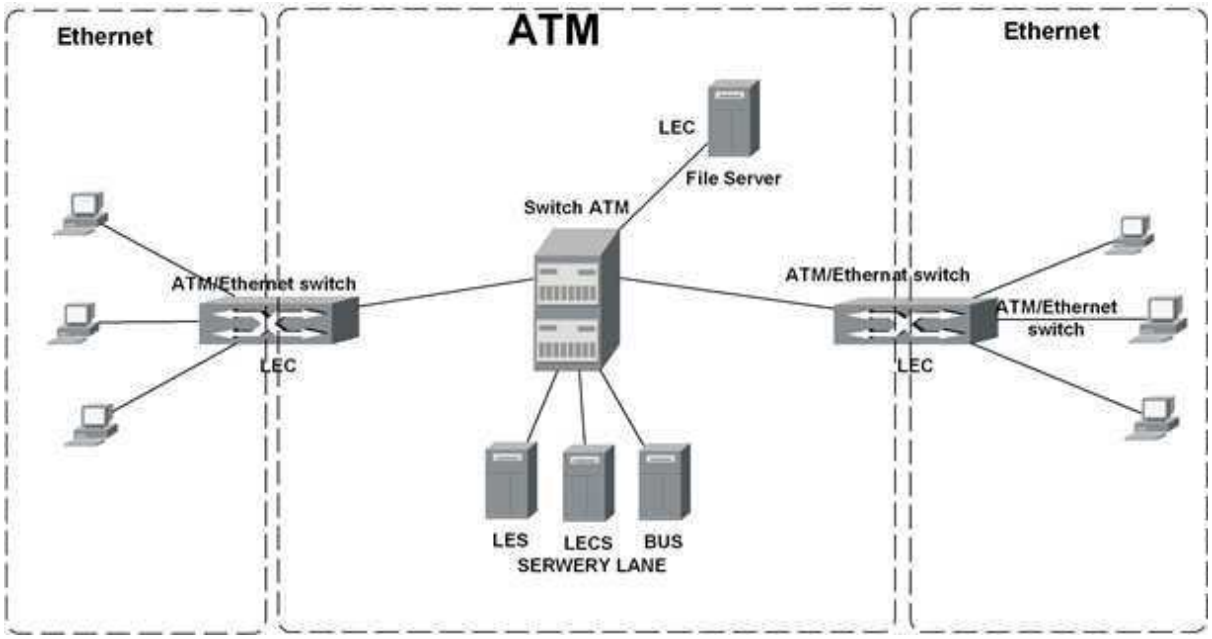
6.2 Sieci wirtualne w sieci ATM

Sieci ATM (ang. *Asynchronous Transfer Mode*) są sieciami komputerowymi stosowanymi do łączenia ze sobą urządzeni rozmieszczonych na dużych obszarach geograficznych, takich jak województwo, kraj lub kontynent[36]. W Polsce sieci ATM są wykorzystywane między innymi jako szkielet sieci Internet. W pierwszej połowie lat 90-tych ubiegłego stulecia, kiedy istniała już duża liczba lokalnych sieci, pojawiła się potrzeba łączenia ze sobą w łatwy sposób dwóch lub więcej znacznie oddalonych od siebie sieci LAN w jedną sieć (np. w firmach ogólnokrajowych lub międzynarodowych). Jedyną możliwością łączenia tych sieci ze sobą było wykorzystanie istniejącej infrastruktury ATM. Jednak integracja technologii ATM z sieciami LAN nie jest prosta, ponieważ sieci ATM są sieciami połączeniowymi typu punkt-punkt[37], których ramki zwane komórkami (ang. *cells*) mają stałą wielkość - 53 bajty. Natomiast sieci LAN są bezpołączeniowe, typu jeden do wiele, a ramki mają zmienną wielkość. Aby rozwiązać problem integracji sieci ATM i LAN w 1995 roku organizacja ATM Forum stworzyła LANE (ang. *LAN Emulation*). Jest to system emulujący protokół warstwy drugiej (łącza danych) modelu OSI, którego działanie polega na emulowaniu sieci LAN w sieciach ATM w taki sposób, że aplikacje działające na bazie sieci LAN funkcjonują bez żadnych zmian i nie są świadome istnienie kanału ATM, którym przekazywane są ich pakiety. LANE pozwala na automatyczne zestawienie tzw. wirtualnego kanału na życzenie SVC (ang. *Switched Virtual Circuit*) między klientami LANE[38] oraz prostą enkapsulację pakietów protokołów warstw wyższych bez ich modyfikacji (między innymi TCP/IP i IPX/SPX) w komórkach ATM i przesyłanie ich przez szkielet sieci ATM. Pojedyncza wirtualna sieć składająca się z kilku klientów LANE oraz dodatkowych elementów systemowych LANE ponad siecią ATM jest nazywana ELAN (ang. *Emulated LAN*). W sieciach ATM można tworzyć wiele ELANów, które pełnią funkcję sieci wirtualnych.

[36] Chodzi tutaj przede wszystkim o sieci WAN (ang. Wide Area Network)
[37] Przed rozpoczęciem przesyłania musi istnieć zestawiony wirtualny kanał między nadawcą a odbiorcą. Kanał ten określany jest skrótem VCC, co po angielsku oznacza Virtual Channel Connection
[38] Zanim powstało LANE zestawianie takich połączeń wymagało ręcznego ustawienia przez administratora. Połączenia tez nazywane są PVC (ang. Permanent Virtual Circuit).

6.2.1 Jednostki systemowe LANE

System LANE, oprócz samych klientów, do działania wymaga kilku elementów spełniających funkcje konfiguracyjne, sygnalizacyjne i rozgłoszeniowe. Są to aplikacje, będące serwerami zarządzającymi pojedynczym ELANem, które są niezbędne do budowania automatycznych wirtualnych połączeń na żądanie (SVC), bez których LANE nie mogłoby funkcjonować. Każda z tych jednostek może istnieć jako osobne urządzenie (na przykład komputer z kartą ATM i odpowiednim oprogramowaniem) jak również wszystkie one mogą być zaimplementowane w jednym urządzeniu (najczęściej wysokiej klasy przełączniku ATM).



Rysunek 30. Przykład konfiguracji systemu LANE z jedną siecią ELAN (opracowanie własne)

Elementami systemu LANE są:

- Klient LANE - LEC (ang. *LAN Emulation Client*) jest to aplikacja będąca interfejsem łączącym sieć LAN siecią ATM, której zadaniem jest przesyłanie danych oraz rozpoznawanie i wiązanie adresów urządzeń. Funkcję LEC spełnia zwykle switch, ale może to też być inne urządzenie sieciowe wyposażone w interfejs ATM (na rysunku 30 takim urządzeniem jest serwer plików)
- Serwer LANE – LES (ang. *LAN Emulation Server*) jest to aplikacja spełniająca funkcje sterujące w emulowanej sieci LAN. Najważniejszymi funkcjami serwera jest rejestrowanie adresów ATM klientów LANE (i adresów MAC podpiętych do nich

urządzeń końcowych) oraz pozostałych elementów systemu LANE, odwzorowywanie adresów MAC i ATM, a także wyznaczanie tras przesyłania komórek ATM. Każda emulowana sieć LAN (ELAN) musi posiadać swój własny serwer LES.

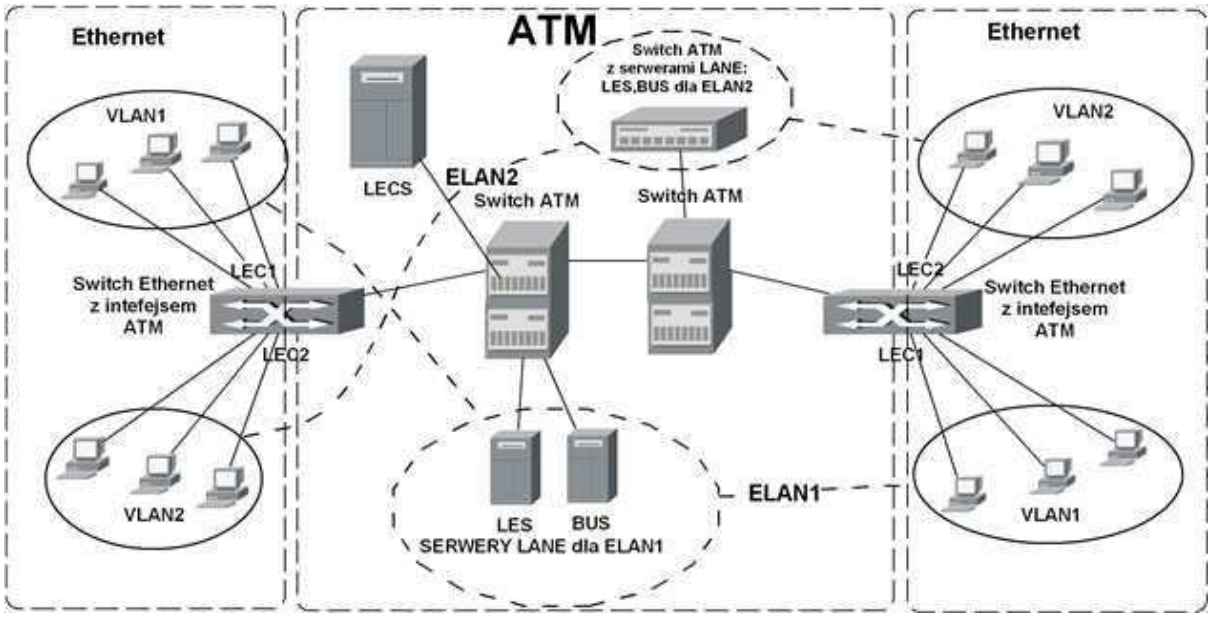
- Serwer konfiguracyjny LANE – LECS (ang. *LAN Emulation Configuration Server*) jest aplikacją odpowiedzialną za przypisywanie klientów LANE do odpowiednich sieci ELAN (wirtualnych sieci), polega to na łączeniu klientów z odpowiednim serwerem LANE (LES). Podstawę do funkcjonowania serwera konfiguracyjnego stanowi baza danych konfiguracyjnych stworzona przez administratora oraz informacje otrzymywane od klientów LAC. W każdej sieci ATM może mieć tylko jeden serwer konfiguracji, niezależnie od ilości emulowanych sieci.
- Serwer rozgłoszeniowy – BUS (ang. *Broadcast and Unknown Server*) odpowiada za rozsyłanie informacji na adresy multicastowe oraz broadcastowe MAC oraz przekazywanie rozkazów inicjujących generowanych w przypadku nieznajomości adresu ATM celu (ruch „*unknown”*). Każda sieć ELAN musi posiadać własny serwer BUS.

6.2.2 Sieci wirtualne ELAN/VLAN

W obrębie jednej sieci ATM może istnieć wiele emulowanych sieci LAN (ELAN), które są sieciami wirtualnymi. Należy pamiętać, że każda sieć ELAN musi posiadać osobne, własne serwery LES i BUS. Natomiast w każdej wydzielonej sieci ATM może być tylko jeden serwer konfiguracji LECS, który podaje klientom LEC (podczas ich inicjalizacji) adres ATM serwera LES sieci ELAN, do której powinni przynależeć. W sieci ATM mogą istnieć serwery wyposażone w interfejsy ATM, które należą do wielu lub wszystkich sieci ELAN, w takim przypadku użytkownicy kilku wirtualnych sieci mają dostęp do tych serwerów. Rutowanie między sieciami ELAN jest możliwy do wykonania tylko za pomocą zewnętrznego lub programowego rutera oraz standardu MPOA (ang. *Multiprotocol over ATM*), który tak jak LANE został stworzony przez ATM Forum.

Rysunek 31 przedstawia dwie sieci VLAN połączone ze sobą za pomocą sieci szkieletowej ATM. Jak widać, każda sieć VLAN zbudowana na przełączniku brzegowym wyposażonym w interfejs ATM musi posiadać swojego własnego klienta LANE (LEC). W sieci ATM oba VLANy pozostają oddzielnymi wirtualnymi sieciami ELAN1 oraz ELAN2. Każdy z tych emulowanych VLANów musi posiadać swoje własne serwery LES oraz BUS.

Sieć ELAN1 ma serwery w postaci dwóch osobnych urządzeń, natomiast serwery sieci ELAN2 są zaimplementowane w oprogramowanie jednego przełącznika ATM. Serwer konfiguracji LANE (LECS) może być tylko jeden na całą sieć ATM. Jego zadaniem jest odpowiadać wszystkim klientom LEC, na podstawie bazy konfiguracyjnej stworzonej przez administratora, do której sieci ELAN należą. Serwery wykonują to zadanie poprzez odsyłanie do LEC adresu ATM serwera LES, na którym powinni zarejestrować się.



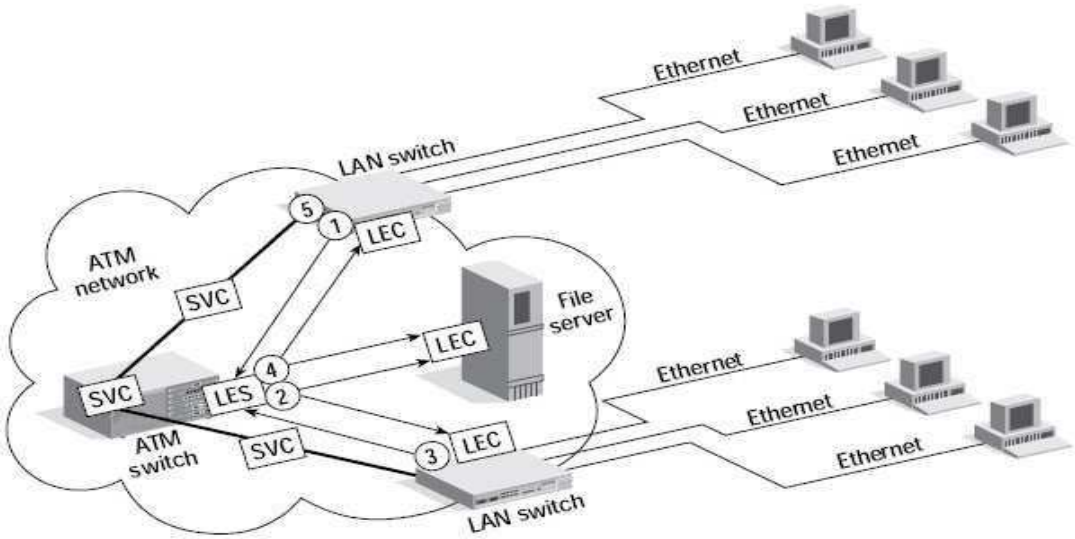
Rysunek 31. Dwie wirtualne sieci LAN emulowane w sieci ATM przy użyciu systemu LANE (opracowanie własne)

6.2.3 Rejestrowanie się klientów LEC w sieci ELAN oraz przesyłanie pakietów między nimi

Rejestracja klientów LEC do emulowanej sieci jest kilkuetapowa i wymaga łączenia się ze wszystkimi serwerami LANE. Oto jej przebieg:

1. Klient LEC chcący się dowiedzieć, do której sieć ELAN ma należeć musi zapytać o to serwer konfiguracji LANE (LECS). W tym celu LEC pyta przełącznik ATM, do którego jest bezpośrednio przypięty o adres serwera LECS i w odpowiedzi go otrzymuje.
2. LEC wysyła do LECS zapytanie „Do której sieci ELAN powinienem należeć?”. Serwer LECS, na postawie adresu ATM posiadanego przez LEC i skonfigurowanej przez administratora bazy odwzorować LEC do LES, odpowiada klientowi odsyłając mu adres przypisanego mu serwera LES.

3. Następnie LEC kontaktuje się z LES w celu zarejestrowania się. LES łączy się z LECS i sprawdza czy LEC na pewno może należeć do obsługiwanej przez niego sieci ELAN. Jeżeli weryfikacja powiedzie się to LES odsyła do LEC jego numer ID w sieci, po którym będzie on rozpoznawał wiadomości do niego kierowane w formie broadcastów, oraz adres należącego do ELAN serwera BUS.
4. Na końcu LEC kontaktuje się z BUS i przyłącza się do grupy broadcastowej.



Rysunek 32. Przesyłanie danych w systemie LANE, dokładny opis poniżej. (Źródło: The Virtula Lan Technology Raport,http://www.3com.com/other/pdfs/solutions/en_US/20037401.pdf,18.06.2006)

Przebieg przesyłania pakietów w emulowanych sieciach ELAN(opis do rysunku 32):

1. Klient LEC otrzymuje ramki z danymi z komputera znajdującego się w sieci Ethernet przypiętej do niego, które mają zostać przesłane do komputera znajdującego się w sieci Ethernet po „drugiej stronie” sieci ATM. LEC pobiera z ramek docelowy adres MAC i pyta serwer LES o adres ATM klienta LEC, do którego przypięta jest sieć Ethernet zawierająca komputer o takim adresie (LEC, jeżeli już wcześniej wysyłał dane do tego komputera, może posiadać niezbędny adres ATM w wewnętrznej tablicy i wtedy przechodzi od razu do punktu 5 poniższego opisu).
2. Jeżeli LES zna adres ATM klienta LEC, do którego podpięty jest adresat ramek to odsyła go do LEC pytającego(od razu przejście do kroku 5). W przypadku, gdy go nie zna, wysyła on za pośrednictwem serwera BUS multicast do wszystkich klientów LEC z zapytaniem: *„Kto ma podpięty komputer z takim adresem MAC?”*.

3. Tylko klient LEC, który ma w sieci Ethernet docelowy MAC adres odpowiada do LES.
4. LES odsyła adres otrzymany w odpowiedzi do LEC, który zadawał pytanie.
5. Wysyłający LEC otrzymuje adres ATM klienta LEC, do którego ma skierować pakiety i buduje z nim wirtualne połączenie na życzenie (SVC), przez które następnie zostają przesłane ramki.

Ramki Ethernet, które mają zostać przesłane przez sieć ATM, nie są przesyłane w oryginalnej formie[39]. W sieciach ATM przesyłane są ramki zwane komórkami (lub „celkami”,ang. *cells*), których wielkość jest stała i wynosi 53 bajty. Natomiast w sieciach Ethernet ramki mają wielkość zmienną od 64 do 1536 bajtów[40]. Do przesyłania ramek w sieciach ATM używana jest specjalna warstwa adaptacyjna zwana AAL (ang. *ATM Adaptation Layer*). Jest więc ona też używana do przesyłania ramek Ethernet w sieci ATM. Zadaniem AAL jest budowanie pakietów danych (mogą być różnej długości, aż do 64kB) z danych przeznaczonych do wysyłki, które następnie są dzielone na komórki o wielkość 53 bajtów, z których każda zawiera 48bajtów danych (w przypadku typu AAL5, pozostałe 5 bajtów to nagłówek). Komórki są przesyłane przez sieć ATM, a w miejscu docelowym składane z powrotem do postaci pakietów AAL. Dopiero z tak powstałych pakietów otrzymywane są oryginalne dane, które były przesyłane. W dużym uproszczeniu wygląda to tak, że w miejscu wejścia ramki Ethernet do sieci ATM jest budowany pakiet AAL, potem jest on cięty na kawałki po 48bajtów, które następnie są enakapsułowane w komórkach ATM i przesyłane do miejsca przeznaczenia. W miejscu przeznaczenia to 48bajtów jest wyciągane z każdej celki i sklejane w pakiet ALL, potem z tego wydzielane są ramka Ethernet, które oryginalnie przesyłano.

6.2.4 Podsumowanie wirtualnych sieci w sieciach ATM

System LANE jest mechanizmem mocno skomplikowanym i powyższy opis jest jedynie ogólnym przybliżeniem jego działania nakierowanym na przedstawienie wirtualności samego LANE, a także sieci VLAN, które w nim funkcjonują.

[39] Oryginalnej formie, czyli takiej, w jakiej otrzymał je klient LEC.
[40] Są to wartości graniczne dla sieci Ethernet w ogólności, w zależności od konkretnej implementacji takich jak Ethernet I, Ethernet II lub IEEE 802.2 LLC minimalny i maksymalny rozmiar ramki może być różny.

Rozdział VII Projekt sieci komputerowej wykorzystującej wirtualne sieci LAN

7.1 Postawienie problemu

Pewna, dynamicznie rozwijająca się firma zatrudniająca około 200 pracowników, która wytwarza sprzęt elektroniczny, wybudowała niedawno nową siedzibę. Firma ma zamiar w najbliższym czasie przenieść swoją działalność ze starego miejsca bytowania do nowych budynków. Nowa siedziba firmy nie ma jednak jeszcze wykonanej infrastruktury sieciowej, którą trzeba zaprojektować i skonfigurować.

7.1.1 Założenia i wymagania stawiane sieci

Kluczową sprawą w nowej sieci, jest wykorzystanie w niej zalet jakie dają sieci wirtualne. Jest to bardzo istotne, ponieważ w firmie istnieje kilka działów, które powinny być wydzielonymi, w obrębie infrastruktury sieciowej, logicznymi jednostkami. Sieć ma także być w miarę prosta w swojej fizycznej budowie (firma chce zakupić jedynie ten sprzęt, który jest całkowicie wymagany do jej funkcjonowania), niezawodna oraz wydajna. Możliwość wpięcia się do konkretnej sieci VLAN w wybranym pomieszczeniu firmy ma podlegać pewnym restrykcjom, a ruch sieciowy między różnymi działami firmy ma być dopuszczony, z możliwością jego ograniczania za pomocą nakładania zasad.

W firmie istnieją takie oto działy, w które mają posiadać swoje własne sieci VLAN: Administracja, dział IT, dział Zarządzania, dział Księgowości, dział Produkcji, dział Projektowania oraz dział Sprzedaży. Poza tym na hali produkcyjnej ma być dostępna osobna lokalna sieć VLAN dla maszyn wykorzystywanych podczas produkcji, która nie ma dostępu do zewnętrznych zasobów. Ciekawostką jest to, że w firmie w każdym pomieszczeniu ma istnieć drukarka sieciowa, aby pracownicy różnych działów, mając do nich dostęp sieciowy, mogli drukować dokumenty od razu w pomieszczeniu osoby, do której są one skierowane. Dzięki temu pracownicy działów nie muszą chodzić do siebie z dokumentami. Wymagane jest jednak, aby wszystkie tak działające drukarki sieciowe, także znajdowały się w osobnej sieci VLAN. Przedsiębiorstwo posiada też serwery, które muszą zostać przeniesione ze starych budynków do nowych. W firmie istnieją trzy serwery ogólnie dostępne, są to serwer WWW (firmowy intranet), serwer pocztowy oraz serwer z usługami katalogowymi (LDAP) i usługą DNS. Poza serwerami ogólnej dostępności, istnieją także serwery przeznaczone dla

pracowników określonych działów. Dział Księgowości oraz Sprzedaży posiadają serwery aplikacji, dział Projektowania serwer plików (FTP). Pracownicy firmy pracują w dużej mierze na komputerach stacjonarnych, jednak istnieje także duża liczba pracowników różnych działów posiadających komputery przenośne, którzy często zmieniają pomieszczenie, w którym pracują.

Nowa siedziba firmy składa się z dwóch budynków. Jednego większego (budynek A), trzypiętrowego z czterema dużymi pomieszczeniami na każdym z pięter. Drugiego mniejszego (budynek B), także trzypiętrowego, w którym na drugim i trzecim piętrze znajdują się po dwa pomieszczenia, a na pierwszej kondygnacji jest hala produkcyjna. Firma ma już zaplanowane wykorzystanie tych pomieszczeń oraz ich oznaczenia. Rysunki 33 i 34 przedstawiają zaplanowany, przez zarząd firmy, podział budynku na działy, którego należy przestrzegać przy projektowaniu sieci wirtualnych.

Budynek A

3 PIĘTRO	A1 Dział Projektowania	A2 Ogólny	A3 Dział Księgowości	A4 Dział Zarządzania
2 PIĘTRO	Centrum Komputerowe	B1 Dział IT	B2 Ogólny	B3 Dział Księgowości
1 PIĘTRO	C1 Dział Sprzedaży	C2 Ogólny	C3 Administracja	C4 Dział Projektowania

Rysunek 33. Podział budynku A na działy (opracowanie własne)

Budynek B

3 PIĘTRO	D4 Dział Projektowania	D5 Administracja
2 PIĘTRO	D1 Dział Sprzedaży	D2 Dział Produkcji
1 PIĘTRO	D1 Hala Produkcji	

Rysunek 34. Podział budynku B na działy (opracowanie własne)

Ja widać na rysunkach, na przykład pomieszczenia A1 i C4 w budynku A oraz D4 w budynku B przeznaczone są dla Działu Projektowania. Natomiast pomieszczenia A2,B2 i C2 nie są przypisane do żadnego działu i mogą w nich pracować osoby z różnych działów firmy. Pomieszczenie nazwane Centrum Komputerowe przeznaczono na serwery firmowe.

Firma, w założeniach do projektu sieci, określiła także dokładnie czy pracownicy innych działów mogą się wpinać do sieci w pomieszczeniu konkretnego działu, a jeśli tak to w jakiej ilości. Jest to ważne, ponieważ jak już wcześniej określono, firma posiada dużą ilość pracowników mobilnych, wyposażonych w komputery przenośne, a różne działy do pewnego stopnia ze sobą współpracują przy wykonywaniu projektów. We wszystkich pomieszczeniach firmy, które należą do jakiegoś działu (z wyłączeniem działu IT i hali produkcji) maksymalna ilość pracowników z innych działów jaka może być wpięta do sieci wynosi sześć. W pomieszczeniu B1, które należy do działu IT zabronione jest wpinanie się pracowników z działu innego. Na hali produkcji mogą pracować tylko pracownicy działu produkcji. W pomieszczeniach „ogólnych”, bez przydzielonego działu, czyli A2,B2 i C2 mogą pracować osoby ze wszystkich działów oprócz działu Księgowości i Produkcji. Wszystkie wymagane reguły zostały dokładnie przedstawione na rysunku numer 35.

Nazwa Działu i maks. z innego		Maksymalna ilość pracowników z konkretnego innego działu (ograniczenia)						
		administracja	it	zarządzanie	księgowość	produkcja	projektowanie	sprzedaż
administracja	6	*	6	6	0	0	0	0
it	0	0	*	0	0	0	0	0
zarządzanie	6	6	6	*	6	0	6	6
księgowość	6	0	0	6	*	0	0	6
produkcja	6	0	0	0	0	*	6	0
projektowanie	6	0	0	0	0	6	*	0
sprzedaż	6	0	0	6	6	0	0	*
pom. Ogólne	*	*	*	*	0	0	*	*
hala produkcji (produkcja)	0	0	0	0	0	*	0	0

" * " - oznacza ograniczenie jedynie ilością portów przełącznika, "0" oznacza dostęp zabroniony

Rysunek 35. Możliwa ilość pracowników innego działu w pomieszczeniu działu (opracowanie własne)

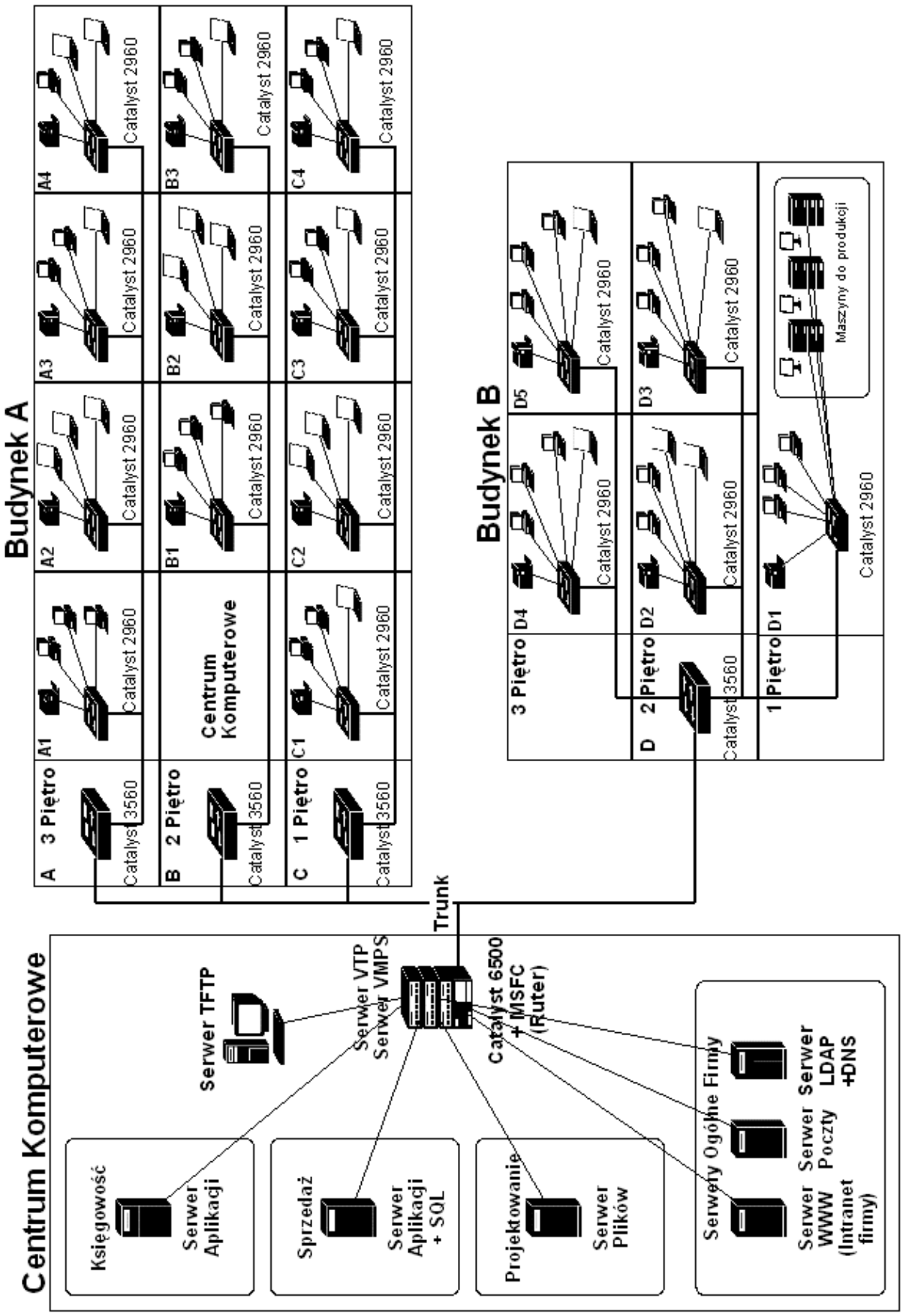
7.2 Proponowane rozwiązanie - zastosowane mechanizmy sieci VLAN

Aby sprostać wymaganiom sieci przedstawionym powyżej, postanowiono wykorzystać statyczne oraz dynamiczne przypisanie do sieci VLAN. Przypisanie statyczne bazuje na portach przełącznika i wymaga ręcznej konfiguracji na każdym przełączniku dostępowym. Przypisanie dynamiczne bazuje na adresach MAC wpinanych komputerów. Aby możliwe było dynamiczne przypisywanie portów przełączników do sieci VLAN zastosowano mechanizm VMPS (ang. *VLAN Member Policy Server*) firmy Cisco. Dzięki takiemu rozwiązaniu, oprócz przypisywania portów do sieci VLAN po adresie MAC, możliwe jest także ustalanie reguł, które umożliwiają ograniczenie możliwości istnienia pewnych sieci VLAN na wybranych przełącznikach. W przypadku wpięcia do przełącznika komputera należącego do zabronionej na nim sieci VLAN, port przechodzi w stan zablokowany „shutdown”. W sieci postanowiono zastosować tryb VMPS security, wyklucza to uruchomienie potencjalnie niebezpiecznych sieci fallback VLAN. Dzięki temu, gdy w bazie danych VMPS adres MAC urządzenia nie istnieje lub jest on zabroniony port przełącznika od razu przechodzi w stan zablokowany.

Drugim zastosowanym mechanizmem jest protokół VTP (ang. *VLAN Trunk Protocol*) w wersji 2. Dzięki niemu, konfigurowanie istniejących sieci VLAN następuje na jednym fizycznym urządzeniu, a pozostałe przełączniki uczą się tej konfiguracji za pomocą połączeń trankingowych. Należy też pamiętać, że mechanizm VTP jest wymagany przez serwer VMPS. Postanowiono także zastosować mechanizm VTP pruning, który będzie podnosił wydajność sieci dzięki blokowaniu niepotrzebnego ruchu rozgłoszeniowego.

W sieci nie został przewidziany osobny ruter. Funkcję rutowania ruchu między sieciami VLAN będzie spełniał moduł MSFC (ang. *Multilayer Switch Feature Card*), który jest wewnętrznym modułem rutującym dla przełącznika Cisco Catalyst 6500. Dzięki takiemu rozwiązaniu rutowanie między sieciami VLAN jest dużo bardziej wydajne niż stosowanie zewnętrznego rutera.

Jako serwer dla mechanizmów VTP i VMPS postanowiono zastosować przełącznik Cisco Catalyst serii 6500. Klientami VTP będą pozostałe przełączniki zastosowane w sieci, a klientami VMPS przełączniki dostępowe, na których ma działać dynamiczne przydzielanie sieci VLAN.



Rysunek 36. Topologia sieci rozrysowana na budynkach przedsiębiorstwa (opracowanie własne)

7.3 Opis zastosowanych urządzeń oraz topologia sieci

Sieć postanowiono wykonać w oparciu o sprzęt i rozwiązania firmy Cisco. Firma Cisco jest pionierem oraz światowym liderem w dziedzinie produkcji sprzętu sieciowego, dlatego można polegać na jej urządzeniach. Zastosowane urządzenia to:

Przełącznik Cisco Catalyst serii 6500 z modułem wewnętrznego rutowania – jest to przełącznik który będzie mógł zapewnić wysoką wydajność sieci dzięki posiadaniu dużej ilości portów o przepustowności 1Gigabit/s oraz długą bezawaryjną pracę dzięki technice redundancji[41]. Przełącznik ten pełni w zaprojektowanej sieci funkcję przełącznika głównego i zarządzającego, na nim działają serwery VTP oraz VMPS. Przełącznik dostarcza też sieci mechanizm rutowania dzięki zastosowaniu dodatkowego modułu MSFC (ang. Multilayer Switch Feature Card). Zastosowane oprogramowanie to Cisco Operating System w wersji 8.1

Rysunek 37. Przełączniki z rodziny Cisco Catalyst 6500
(Źródło: www.cisco.com, 10.07.2006)

Przełączniki Cisco Catalyst serii 3560 – przełączniki te zostały zastosowane jako przełączniki szkieletowe, gdyż posiadają one 24 porty pracujące z przepustowością 1Gigabita/s. Pełnią funkcję klientów VTP. Zastosowany model to 3560G-24TS z oprogramowaniem Cisco IOS 12.1 EA1 (w sieci wykorzystano 4 przełączniki tego typu).

Rysunek 38. Przełączniki z rodziny Cisco Catalyst 3560
(Źródło: www.cisco.com, 10.07.2006)

Przełączniki Cisco Catalyst serii 2960 – w sieci pełnią one funkcję przełączników brzegowych (dostępowych), bezpośrednio do nich są wpinane komputery pracowników

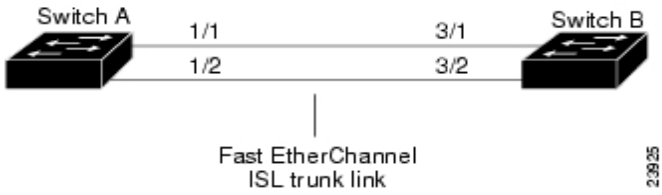
[41] Przełącznik posiada między innymi dwa niezależne zasilania

firmy. Przełączniki w większości pełnią funkcję klientów VTP oraz VMPS. Dzięki posiadaniu przez nie dwóch portów 1Gigabit/s mogą się one wydajnie komunikować z przełącznikami szkieletowymi. Zastosowany model to 2960-24TT-L z oprogramowaniem Cisco ISO w wersji 12.2 SEE (w sieci wykorzystano 16 przełączniki tego typu).

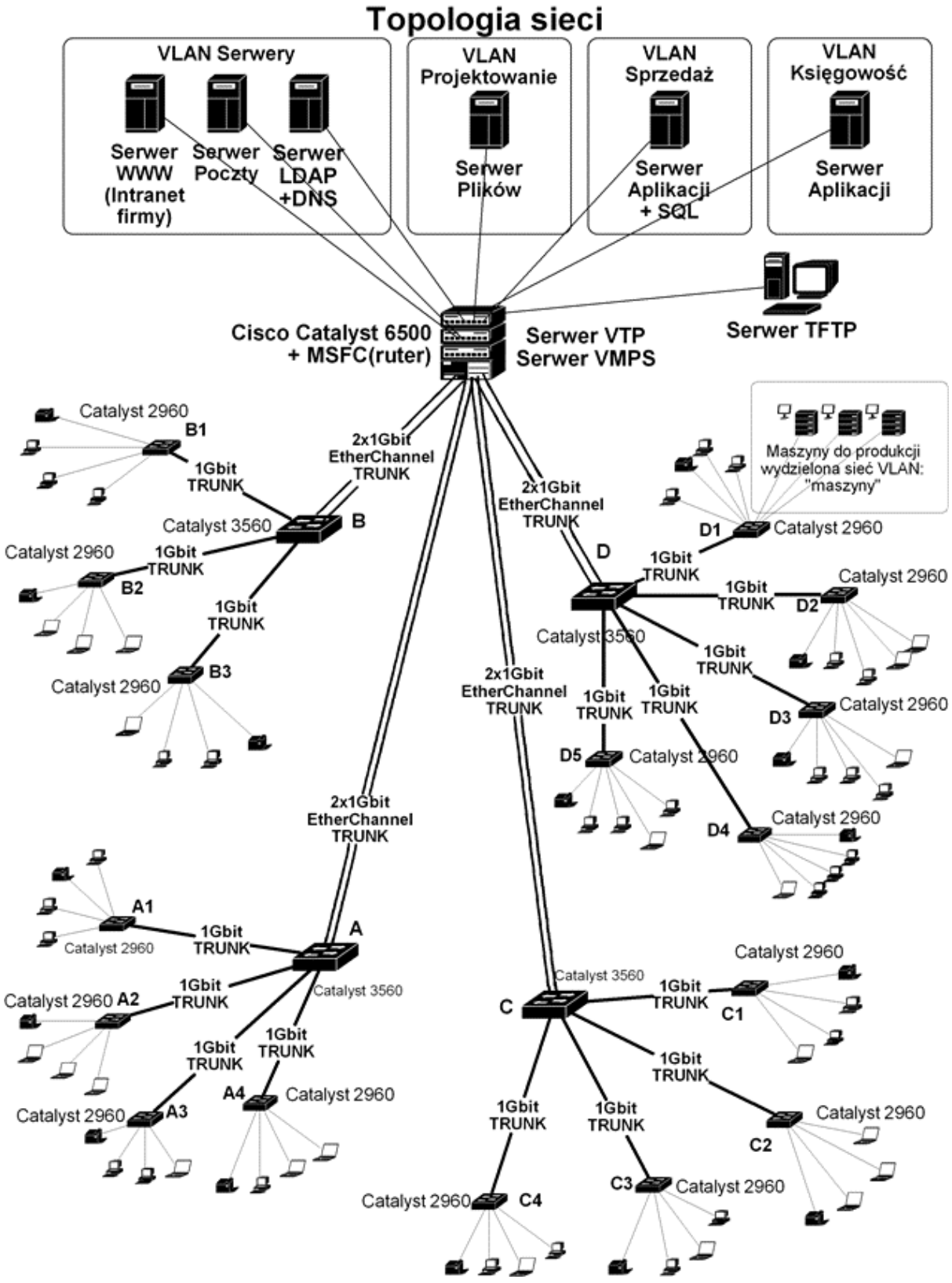
Rysunek 39. Przełączniki z rodziny Cisco Catalyst 2960 (Źródło: www.cisco.com, 10.07.2006)

Serwer TFTP – jest to komputer z oprogramowaniem serwera TFTP. Na nim jest umiejscowiony plik konfiguracyjny mechanizmu VMPS, który pobiera przełącznik będący serwerem VMPS.

W sieci zastosowano dwa typy połączeń. Połączenia Access Link wykorzystywane są między komputerami i innymi urządzeniami końcowymi, a przełącznikami dostępowymi w pomieszczeniach firmy (100Mbitów/s) oraz między przełącznikiem głównym Catalyst 6500, a serwerami przedsiębiorstwa (1Gbit/s). Połączenia Trunk Link zastosowano między przełącznikiem głównym Catalyst 6500 i przełącznikami Catalyst 3560 oraz między przełącznikami dostępowymi Catalyst 2960 i przełącznikami Catalyst 3560. W celu podniesienia prędkości przesyłania danych oraz niezawodności sieci , połączenia trunkingowe między przełącznikiem głównym Catalyst 6500 i przełącznikami szkieletowymi Catalyst 3560 wykorzystują technologię EtherChannel firmy Cisco. Dzięki temu jedno logiczne połączenie trunkingowe, o łącznej przepustowości 2Gbity/s, składa się z dwóch połączeń fizycznych o przepustowości 1Gbit/s każde.



Rysunek 40. Przykład połączenia Trunk Link z wykorzystaniem techologi EtherChannel (Źródło:http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008019f00f.html,10.07.2006)



Rysunek 41. Topologia sieci wraz z opisanymi połączeniami. (opracowanie własne)

7.4 Założenia dotyczące konfiguracji sieci VLAN

7.4.1 Podział na sieci VLAN oraz ich adresacja

Podstawą do wydzielenia w firmie osobnych sieci VLAN są jej działy, jednak oprócz sieci VLAN, odpowiadającym departamentom, zastosowano także określoną w wymaganiach do projektu sieć VLAN dla drukarek sieciowych - „drukarki”. Kolejną zastosowana siecią wirtualną jest osobna sieć dla serwerów ogólnych firmy, nazwano ją „serwery”. Trzy serwery dedykowane do obsługi w działach Księgowości, Projektowania oraz Sprzedaży znajdują się w sieciach VLAN tych działów. Na przełączniku dostępowym D1 umiejscowionym w hali produkcji skonfigurowano dodatkowo wydzieloną sieć VLAN „maszyny”, w której znajdują się urządzenia wykorzystywane przy produkcji. Sieć ta jest skonfigurowana tylko i wyłącznie na tym przełączniku[42]. W całej firmie funkcjonuje dziesięć sieci wirtualnych, poniżej znajduje się ich spis (rysunek 42), który zawiera nazwy sieci w bazach danych przełączników, ich numery, podstawę adresacji urządzeń w nich się znajdujących oraz adresy bram (ang. *gateway*) wymagane do działania rutowania.

Nazwa Działu	Nazwa sieci VLAN	numer sieci VLAN	adresacja urządzeń	adres bramy
-------	drukarki	VLAN 5	192.168.5.X / 24	192.168.5.1
Administracja	administracja	VLAN 10	192.168.10.X / 24	192.168.10.1
IT	it	VLAN 20	192.168.20.X / 24	192.168.20.1
Zazadzanie	zarzadzanie	VLAN 30	192.168.30.X / 24	192.168.30.1
Księgowość	ksiegowosc	VLAN 40	192.168.40.X / 24	192.168.40.1
Produkcja	produkcja	VLAN 50	192.168.50.X / 24	192.168.50.1
Projektowanie	projektowanie	VLAN 60	192.168.60.X / 24	192.168.60.1
Sprzedaż	sprzedaz	VLAN 70	192.168.70.X / 24	192.168.70.1
--------	serwer	VLAN 80	192.168.80.X / 24	192.168.80.1
--------	maszyny	VLAN 100	192.168.100.X / 24	192.168.100.1

Rysunek 42. Spis wszystkich sieci VLAN w przedsiębiorstwie (opracowanie własne)

7.4.2 Adresy MAC komputerów

Do sieci VLAN, które mogą być dynamicznie przydzielane na przełącznikach dostępowych, należą tylko sieci VLAN odpowiadające działom w firmie. Jedynie pracownicy, którzy posiadają komputery przenośnie mogą uzyskać dostęp do swojej sieci w

[42] Przełącznik pracuje w trybie VTP transparent.

sposób dynamiczny za pomocą adresu MAC. Każdy dział zawiera różną liczbę użytkowników mobilnych, którzy posiadają komputery przenośnie. Odwzorowanie wszystkich adresów MAC do działów, z których one pochodzą przedstawia rysunek 43.

Odwzorowanie adresów MAC komputerów przenośnych na działy do których należą

Administracja	IT	Zazadzanie	Księgowość	Produkcja	Projektowanie	Sprzedaż
AA:BB:CC:10:00:01	AA:BB:CC:20:00:24	AA:BB:CC:30:00:56	AA:BB:CC:40:00:87	AA:BB:CC:50:00:34	AA:BB:CC:60:00:38	AA:BB:CC:70:00:03
AA:BB:CC:10:00:02	AA:BB:CC:20:00:25	AA:BB:CC:30:00:57	AA:BB:CC:40:00:88	AA:BB:CC:50:00:35	AA:BB:CC:60:00:39	AA:BB:CC:70:00:04
AA:BB:CC:10:00:03	AA:BB:CC:20:00:26	AA:BB:CC:30:00:58	AA:BB:CC:40:00:89	AA:BB:CC:50:00:36	AA:BB:CC:60:00:40	AA:BB:CC:70:00:05
AA:BB:CC:10:00:04	AA:BB:CC:20:00:27	AA:BB:CC:30:00:59	AA:BB:CC:40:00:90	AA:BB:CC:50:00:37	AA:BB:CC:60:00:41	AA:BB:CC:70:00:06
AA:BB:CC:10:00:05	AA:BB:CC:20:00:28	AA:BB:CC:30:00:60	AA:BB:CC:40:00:91	AA:BB:CC:50:00:38	AA:BB:CC:60:00:42	AA:BB:CC:70:00:07
AA:BB:CC:10:00:06	AA:BB:CC:20:00:29	AA:BB:CC:30:00:61	AA:BB:CC:40:00:92		AA:BB:CC:60:00:43	AA:BB:CC:70:00:08
AA:BB:CC:10:00:07	AA:BB:CC:20:00:30	AA:BB:CC:30:00:62	AA:BB:CC:40:00:93		AA:BB:CC:60:00:44	AA:BB:CC:70:00:09
AA:BB:CC:10:00:08	AA:BB:CC:20:00:31	AA:BB:CC:30:00:63			AA:BB:CC:60:00:45	AA:BB:CC:70:00:10
AA:BB:CC:10:00:09	AA:BB:CC:20:00:32	AA:BB:CC:30:00:64			AA:BB:CC:60:00:46	AA:BB:CC:70:00:11
AA:BB:CC:10:00:10	AA:BB:CC:20:00:33				AA:BB:CC:60:00:47	
	AA:BB:CC:20:00:34				AA:BB:CC:60:00:48	
	AA:BB:CC:20:00:35				AA:BB:CC:60:00:49	
					AA:BB:CC:60:00:50	
					AA:BB:CC:60:00:51	
					AA:BB:CC:60:00:52	
					AA:BB:CC:60:00:53	

Rysunek 43. Odwzorowanie adresów MAC na działy firmy. (opracowanie własne)

7.4.3 Zastosowane ustawienia mechanizmów VTP i VMPS

Zdecydowano, że nazwą domeny VTP oraz VMPS jest słowo „firma”. Protokół VTP został skonfigurowany do działania w wersji 2, hasłem domeny jest słowo „haslo”, VTP pruning jest uruchomiony dla wszystkich sieci VLAN skonfigurowanych na serwerze VTP. Serwer VTP oraz VMPS działa na przełączniku głównym Cisco Catalyst 6500. Wszystkie pozostałe przełączniki działają w trybie klienta VTP za wyjątkiem przełącznika D1, który działa w trybie przeźroczystym VTP ze względu na lokalnie działającą sieć VLAN „maszyny”. Nazwa pliku konfiguracyjnego VMPS to „vmps_conf.db”. Aby w sieci było możliwe korzystanie z VMPS, wszystkie przełączniki, na których działa ta usługa, wymagają posiadania swoich adresów IP oraz skonfigurowanego adresu serwera VMPS. Komputer, na którym działa serwer TFTP z plikiem konfiguracyjnym VMPS, też musi posiadać adres IP. Adres ten musi być znany serwerowi VMPS. Adresacja przełączników wykorzystujących VMPS oraz serwera TFTP została przedstawiona na rysunku 44. Nazwy przełączników dostępowych pokrywają się nazwami pomieszczeń, w których się one znajdują. Przełączniki B1 oraz D1 nie są klientami VMPS i nie mają możliwości przydzielania sieci VLAN dynamicznie, ponieważ w tych pomieszczeniach jest to zabronione.

Nazwa przełącznika	Adres IP	Adres serwera VMPS	Adres TFTP
przełącznik główny	172.20.20.100	nie dotyczy	172.20.20.150
A1	172.20.20.1	172.20.20.100	nie dotyczy
A2	172.20.20.2	172.20.20.100	nie dotyczy
A3	172.20.20.3	172.20.20.100	nie dotyczy
A4	172.20.20.4	172.20.20.100	nie dotyczy
B1	172.20.20.5	dynamiczne sieci VLAN są zabronione	
B2	172.20.20.6	172.20.20.100	nie dotyczy
B3	172.20.20.7	172.20.20.100	nie dotyczy
C1	172.20.20.8	172.20.20.100	nie dotyczy
C2	172.20.20.9	172.20.20.100	nie dotyczy
C3	172.20.20.10	172.20.20.100	nie dotyczy
C4	172.20.20.11	172.20.20.100	nie dotyczy
D1	172.20.20.12	dynamiczne sieci VLAN są zabronione	
D2	172.20.20.13	172.20.20.100	nie dotyczy
D3	172.20.20.14	172.20.20.100	nie dotyczy
D4	172.20.20.15	172.20.20.100	nie dotyczy
D5	172.20.20.16	172.20.20.100	nie dotyczy

Rysunek 44. Parametry konfiguracyjne przełączników wymagane do działania usługi VMPS (opracowanie własne)

7.4.4 Sposób przypisania portów przełączników do sieci VLAN

Bardzo istotną rzeczą jest sposób konfiguracji portów na przełącznikach dostępowych. Aby sprostać potrzebom przedstawionym w założeniach do projektu, postanowiono, na wszystkich przełącznikach dostępowych, porty 1 i 2 przypisać statycznie do sieci VLAN drukarki. Na przełącznikach znajdujących się w pomieszczeniach działów firmy porty od 3 do 18 zostały statycznie przypisane do sieci VLAN tych działów, a porty od 19 do 24 ustawione na dostęp dynamiczny. W pomieszczeniach ogólnych porty od 3 do 24 są ustawione na dostęp dynamiczny. W dziale IT sieci dynamiczne są niedozwolone, dlatego porty od 3 do 24 na przełączniku B1 są ustawione statycznie na sieć VLAN 20 należącą do tego działu. Przełącznik D1 znajdujący się w hali produkcji jest w całości skonfigurowany na dostęp statyczny, jego porty od 3 do 12 należą do sieci VLAN działu Produkcji, a porty od 13 do 24 do lokalnej sieci „maszyny”. Pozostałe ograniczenia, nałożone na możliwość dynamicznego wpinania się do określonych sieci VLAN na określonych przełącznikach (zawarte na rysunku 35), zostały skonfigurowane dzięki zastosowaniu zasad *„VLAN port Policies”* w pliku

konfiguracyjnym serwera VMPS. Dokładna konfiguracja sieci VLAN na przełącznikach dostępowych w przedsiębiorstwie została przedstawiona na rysunkach 45.

	A1		A2		A3		A4	
Administracja	X	X	D 3-24	D 3-24	X	X	D 19-24	X
Drukarki	S 1-2	S 1-2	S 1-2	S 1-2	S 1-2	S 1-2	S 1-2	S 1-2
It	X	S 3-24	D 3-24	D 3-24	X	X	D 19-24	X
Zarządzanie	X	X	D 3-24	D 3-24	D 19-24	D 19-24	S 3-18*	X
Księgowość	X	X	X	X	S 3-18*	S 3-18*	D 19-24	X
Produkcja	D 19-24	X	X	X	X	X	X	S 3-12
Projektowanie	S 3-18 *	X	D 3-24	D 3-24	X	X	D 19-24	X
Sprzedaż	X	X	D 3-24	D 3-24	D 19-24	D 19-24	D 19-24	X
Serwery	X	X	X	X	X	X	X	X
maszyny(lok.)	X	X	X	X	X	X	X	S 13-24
		B1		B2		B3		D1

" * " - oznacza, że ta sieć VLAN dostąpna jest także w sposób dynamiczny na portach od 19 do 24
„S” – oznacza statyczne przypisanie „D”- oznacza dynamiczne przypisanie

	C1		C2		C3		C4	
Administracja	X	X	D 3-24	X	S 3-18*	X	X	S 3-18*
Drukarki	S 1-2	S 1-2	S 1-2	S 1-2	S 1-2	S 1-2	S 1-2	S 1-2
It	X	X	D 3-24	X	D 19-24	X	X	D 19-24
Zarządzanie	D 19-24	D 19-24	D 3-24	X	D 19-24	X	X	D 19-24
Księgowość	D 19-24	D 19-24	X	X	X	X	X	X
Produkcja	X	X	X	S 3-18*	X	D 19-24	D 19-24	X
Projektowanie	X	X	D 3-24	D 19-24	X	S 3-18*	S 3-18*	X
Sprzedaż	S 3-18*	S 3-18*	D 3-24	X	X	X	X	X
Serwery	X	X	X	X	X	X	X	X
maszyny(lok.)		X	X	X	X	X	X	X
		D2		D3		D4		D5

Rysunek 45. Konfiguracja VLAN na portach przełączników (opracowanie własne)

W celu funkcjonowania sieci wirtualnych w całej infrastrukturze sieciowej wymagane są połączenia trunkingowe. Jak już wcześniej było wspomniane, w sieci między przełącznikiem głównym, a przełącznikami szkieletowymi występują połączenia Trunk Link z wykorzystaniem technologii EtherChannel, dlatego na tych przełącznikach do budowy pojedynczego połączenia trunkingowego wykorzystane są po dwa porty na jednym przełączniku. Porty wykorzystane do budowy połączeń trunkingowych na każdym

przełączniku są przedstawione na rysunku numer 46. Znakowanie ramek za pomocą protokołu 802.1q (na urządzeniach Cisco protokół ten ma oznaczenie „*dot1q*”).

Przełącznik	Port/y 1Gbit	Typ połączenia	Port/y 1Gbit	Przełącznik
główny	0/1 - 0/2	EtherChannel Trunk (grupa 1)	0/1 - 0/2	A
główny	0/3 - 0/4	EtherChannel Trunk (grupa 2)	0/1 - 0/2	B
główny	0/5 - 0/6	EtherChannel Trunk (grupa 3)	0/1 - 0/2	C
główny	0/7 - 0/8	EtherChannel Trunk (grupa 4)	0/1 - 0/2	D
A	0/3	Trunk	0/1	A1
A	0/4	Trunk	0/1	A2
A	0/5	Trunk	0/1	A3
A	0/6	Trunk	0/1	A4
B	0/3	Trunk	0/1	B1
B	0/4	Trunk	0/1	B2
B	0/5	Trunk	0/1	B3
C	0/3	Trunk	0/1	C1
C	0/4	Trunk	0/1	C2
C	0/5	Trunk	0/1	C3
C	0/6	Trunk	0/1	C4
D	0/3	Trunk	0/1	D1
D	0/4	Trunk	0/1	D2
D	0/5	Trunk	0/1	D3
D	0/6	Trunk	0/1	D4
D	0/7	Trunk	0/1	D5

Rysunek 46. Połączenia trunkingowe w sieci. (opracowanie własne)

Ostatni rysunek (numer 47), w tym rozdziale, przedstawia do jakich sieci VLAN należą porty przełącznika głównego, do których wpięte są serwery firmy. Przepustowość połączenia jest negocjowana i zależy do możliwości karty sieciowej serwera. Wszystkie serwery posiadają karty 1Gbit/s, więc porty przełącznika będą działać z taką prędkością.

Serwer	Sieć VLAN	port przełącznika
Serwer WWW	VLAN 80	0/10
Serwer Poczty	VLAN 80	0/11
Serwer LADP+DNS	VLAN 80	0/12
Serwer Aplikacji działu Księgowość	VLAN 40	0/15
Serwer Aplikacji działu Sprzedaż	VLAN 70	0/16
Serwer Plików działu Projektowanie	VLAN 60	0/17
Serwer TFTP	VLAN 1	0/20

Rysunek 47. Porty przełącznika głównego i ich przynależność do sieci VLAN, do których wpięte są serwery firmy (opracowanie własne)

7.5 Praktyczne konfigurowanie przedstawionej sieci

Nazwy urządzeń, stosowane w tym rozdziale, pokrywają się z nazwami przedstawionymi na rysunkach topologii sieci. Nazwa przełącznika głównego to „glowny” i znajduje się na nim oprogramowanie Cisco Operating System w wersji 8.1, na pozostałych przełącznikach działa oprogramowanie Cisco IOS w wersji 12. Przebieg konfiguracji został podzielony na części, które obrazują chronologię tego procesu.

7.5.1 Konfigurowanie sieci VLAN na przełącznikach

Dodawanie nowych sieci VLAN na przełączniku głównym.

```
glowny> enable
glowny# set vlan 5 name drukarki
Vlan 5 configuration successful
glowny# set vlan 10 name administracja
Vlan 10 configuration successful
glowny# set vlan 20 name it
Vlan 20 configuration successful
glowny# set vlan 30 name zarzadzanie
Vlan 30 configuration successful
glowny# set vlan 40 name ksiegowosc
Vlan 40 configuration successful
glowny# set vlan 50 name produkcja
Vlan 50 configuration successful
glowny# set vlan 60 name projektowanie
Vlan 60 configuration successful
glowny# set vlan 70 name sprzedaz
Vlan 70 configuration successful
glowny# set vlan 80 name serwery
Vlan 80 configuration successful
```

Dzięki protokołowi VTP pozostałe przełączniki automatycznie skonfigurują się do obsługi tych sieci (poza D1 pracującym w trybie transparent). Sprawdzenie konfiguracji przełącznika poleceniem „*show vlan*” zostało przedstawione na rysunku 48(pozostałe widoczne sieci VLAN są sieciami ustawionymi domyślnie na wszystkich przełącznikach firmy Cisco):

```
switch#show 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
5    drukarki                          active
10   administracja                     active
20   it                                active
30   zarzadzanie                       active
40   ksiegowosc                        active
50   produkcja                         active
60   projektowanie                     active
70   sprzedaz                          active
80   serwery                           active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
50   enet  100050     1500  -      -      -        -    -        0      0
60   enet  100060     1500  -      -      -        -    -        0      0
70   enet  100070     1500  -      -      -        -    -        0      0
80   enet  100080     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------


switch#_
```

Rysunek 48. Sieci VLAN skonfigurowane na przełączniku głównym (opracowanie własne)

Dodawanie nowych sieci VLAN na przełączniku dostępowym D1.

```
D1> enable
D1# vlan database
D1(vlan)# vlan 5 name drukarki
D1(vlan)# vlan 50 name produkcja
D1(vlan)# vlan 100 name maszyny
D1(vlan)# exit
```

7.5.2 Konfigurowanie połączeń trunkingowych w sieci

Trunk Link z wykorzystaniem technologii EtherChannel między przełącznikiem głównym i przełącznikiem A:

Przełącznik główny:

```
glowny> enable
glowny# set port channel 0/1-2 desirable
glowny# set trunk 0/1 desirable dot1q
```

Przełącznik A:

```
A> enable
A# configure terminal
A(config)# interface range gigabitethernet0/1 - 2
A(config-if-range)# switchport mode trunk
A(config-if-range)# switchport trunk encapsulation dot1q
A(config-if-range)# channel-group 1 mode desirable
A(config-if-range)# end
```

Trunk Link z wykorzystaniem technologii EtherChannel między przełącznikiem głównym i przełącznikiem B:

Przełącznik główny:

```
glowny> enable
glowny# set port channel 0/3-4 desirable
glowny# set trunk 0/3 desirable dot1q
```

Przełącznik B:

```
B> enable
B# configure terminal
B(config)# interface range gigabitethernet0/1 - 2
B(config-if-range)# switchport mode trunk
B(config-if-range)# switchport trunk encapsulation dot1q
B(config-if-range)# channel-group 1 mode desirable
B(config-if-range)# end
```

Połączenia trunkingowe z wykorzystaniem technologii EtherChannel między przełącznikiem głównym, a przełącznikami C i D zostały wykonane analogicznie zgodnie z rysunkiem 46, który określa porty trunkingowe przełączników.

Trunk Link między przełącznikiem A i przełącznikiem A1:

Przełącznik A:

```
A> enable
A# configure terminal
A(config)# interface gigabitethernet0/3
A(config-if-range)# switchport mode trunk
A(config-if-range)# switchport trunk encapsulation dot1q
A(config-if-range)# end
A(config)#
```

Przełącznik A1:

```
A1> enable
A1# configure terminal
A1(config)# interface gigabitethernet0/1
A1(config-if-range)# switchport mode trunk
A1(config-if-range)# switchport trunk encapsulation dot1q
A1(config-if-range)# end
A1(config)#
```

Trunk Link między przełącznikiem A i przełącznikiem A1:

Przełącznik A:

```
A> enable
A# configure terminal
A(config)# interface gigabitethernet0/3
A(config-if-range)# switchport mode trunk
A(config-if-range)# switchport trunk encapsulation dot1q
A(config-if-range)# end
A(config)#
```

Przełącznik A1:

```
A1> enable
A1# configure terminal
A1(config)# interface gigabitethernet0/1
A1(config-if-range)# switchport mode trunk
A1(config-if-range)# switchport trunk encapsulation dot1q
A1(config-if-range)# end
A1(config)#
```

Połączenia trunkingowe między przełącznikami A, B, C, D i przełącznikami dostępowymi do nich podpiętymi (A3,A4,B1,B2,B3,C1,C2,C3,C4,D1,D2,D3,D4,D5) zostały wykonane analogicznie zgodnie z rysunkiem 46, który określa porty trunkingowe przełączników.

7.5.3 Konfigurowanie protokołu VTP

Konfigurowanie przełącznika głównego jako serwer protokołu VTP oraz uruchomienie mechanizmu VTP pruning.

```
glowny> enable
glowny# set vtp domain firma
glowny# set vtp version 2
glowny# set vtp mode server
glowny# set vtp password haslo
glowny# set vtp pruning enable
```

Mechanizm VTP pruning włączony jest tylko na serwerze VTP, ponieważ klienci dziedziczą to ustawienie.

Konfigurowanie przełącznika A jako klienta VTP.

```
A> enable
A# configure terminal
A(config)# vtp domain firma
A(config)# vtp version 2
A(config)# vtp mode client
A(config)# vtp password haslo
A(config)# end
```

Konfigurowanie pozostałych przełączników jako klientów VTP jest analogiczna. Wyjątkiem jest przełącznik D1, który pracuje w trybie przeźroczystym.

Konfigurowanie przełącznika D1 do pracy w trybie przeźroczystym VTP.

```
D1> enable
D1# configure terminal
D1 (config)# vtp domain firma
D1 (config)# vtp version 2
```

```
D1 (config)# vtp mode transparent
D1 (config)# vtp password haslo
D1 (config)# end
```

7.5.4 Konfigurowanie mechanizmu VMPS

Budowanie pliku konfiguracyjnego VMPS (nazwa pliku „vmps_conf.txt”)

Wszystkie linijki zaczynające się od „ ! ” oznaczają komentarz. Opis pliku został zawarty w jego komentarzach.

```
!vmps domain <domain-name>
!oznacza nazwę domeny VMPS, musi być zgodna z VTP
!vmps mode { open | secure }
!tryb pracy: otwarty lub zabezpieczony,domyślny tryb to "open", jeżeli
!wybrano zabezpieczony to fallback vlan nie jest dozwolony
!vmps fallback <vlan-name>
!nazwa sieci VLAN, której będą przypisywane komputery bez odwzorowania
!adresu MAC w bazie, działa tylko gdy tryb pracy VMPS to "open"
!vmps no-domain-req { allow | deny }
!określa czy serwer VMPS może obsługiwać także przełączniki z innej domeny
!VTP niż ustawiono, domyślna wartość to "allow"
!
!zastosowane ustawienia są poniżej, nazwa domeny to firma, tryb pracy
!zabezpieczony oraz wykluczone obsługiwanie komputerów z innej domeny VTP
vmps domain firma
vmps mode secure
vmps no-domain-req deny
!
!Odwzorowania adresów MAC komputerów przenośnych w firmie na ich sieci VLAN
vmps-mac-addrs
!
! address <addr> vlan-name <vlan_name>
!
address aabb.cc10.0001 vlan-name administracja
address aabb.cc10.0002 vlan-name administracja
address aabb.cc10.0003 vlan-name administracja
address aabb.cc10.0004 vlan-name administracja
address aabb.cc10.0005 vlan-name administracja
address aabb.cc10.0006 vlan-name administracja
address aabb.cc10.0007 vlan-name administracja
address aabb.cc10.0008 vlan-name administracja
address aabb.cc10.0009 vlan-name administracja
address aabb.cc10.0010 vlan-name administracja
!
address aabb.cc20.0024 vlan-name it
address aabb.cc20.0025 vlan-name it
address aabb.cc20.0026 vlan-name it
address aabb.cc20.0027 vlan-name it
address aabb.cc20.0028 vlan-name it
address aabb.cc20.0029 vlan-name it
address aabb.cc20.0030 vlan-name it
address aabb.cc20.0031 vlan-name it
address aabb.cc20.0032 vlan-name it
address aabb.cc20.0033 vlan-name it
address aabb.cc20.0034 vlan-name it
```

```
address aabb.cc20.0035 vlan-name it
!
address aabb.cc30.0056 vlan-name zarzadzanie
address aabb.cc30.0057 vlan-name zarzadzanie
address aabb.cc30.0058 vlan-name zarzadzanie
address aabb.cc30.0059 vlan-name zarzadzanie
address aabb.cc30.0060 vlan-name zarzadzanie
address aabb.cc30.0061 vlan-name zarzadzanie
address aabb.cc30.0062 vlan-name zarzadzanie
address aabb.cc30.0063 vlan-name zarzadzanie
address aabb.cc30.0064 vlan-name zarzadzanie
!
address aabb.cc40.0087 vlan-name ksiegowosc
address aabb.cc40.0088 vlan-name ksiegowosc
address aabb.cc40.0089 vlan-name ksiegowosc
address aabb.cc40.0090 vlan-name ksiegowosc
address aabb.cc40.0091 vlan-name ksiegowosc
address aabb.cc40.0092 vlan-name ksiegowosc
address aabb.cc40.0093 vlan-name ksiegowosc
!
address aabb.cc50.0034 vlan-name produkcja
address aabb.cc50.0035 vlan-name produkcja
address aabb.cc50.0036 vlan-name produkcja
address aabb.cc50.0037 vlan-name produkcja
address aabb.cc50.0038 vlan-name produkcja
!
address aabb.cc60.0038 vlan-name projektowanie
address aabb.cc60.0039 vlan-name projektowanie
address aabb.cc60.0040 vlan-name projektowanie
address aabb.cc60.0041 vlan-name projektowanie
address aabb.cc60.0042 vlan-name projektowanie
address aabb.cc60.0043 vlan-name projektowanie
address aabb.cc60.0044 vlan-name projektowanie
address aabb.cc60.0045 vlan-name projektowanie
address aabb.cc60.0046 vlan-name projektowanie
address aabb.cc60.0047 vlan-name projektowanie
address aabb.cc60.0048 vlan-name projektowanie
address aabb.cc60.0049 vlan-name projektowanie
address aabb.cc60.0050 vlan-name projektowanie
address aabb.cc60.0051 vlan-name projektowanie
address aabb.cc60.0052 vlan-name projektowanie
address aabb.cc60.0053 vlan-name projektowanie
!
address aabb.cc70.0004 vlan-name sprzedaz
address aabb.cc70.0005 vlan-name sprzedaz
address aabb.cc70.0006 vlan-name sprzedaz
address aabb.cc70.0007 vlan-name sprzedaz
address aabb.cc70.0008 vlan-name sprzedaz
address aabb.cc70.0009 vlan-name sprzedaz
address aabb.cc70.0010 vlan-name sprzedaz
address aabb.cc70.0011 vlan-name sprzedaz
!
!Port Groups
!Grupy portów zostały wykorzystanie do określenia portów przełączników,
!które mogą obsługiwać dynamiczne przypisywanie do sieci VLAN
!Nazwy skonstruowano według klucza „nazwaPrzełącznika_portOd_portDo”
!
!vmps-port-group <group-name>
! device <device-id> { port <port-name> | all-ports }
!
!adresy ip są adresami przełączników
```

```
!
vmps-port-group A1_19_24
device 172.20.20.1 port fa0/19
device 172.20.20.1 port fa0/20
device 172.20.20.1 port fa0/21
device 172.20.20.1 port fa0/22
device 172.20.20.1 port fa0/23
device 172.20.20.1 port fa0/24
!
vmps-port-group A2_3_24
device 172.20.20.2 port fa0/3
device 172.20.20.2 port fa0/4
device 172.20.20.2 port fa0/5
device 172.20.20.2 port fa0/6
device 172.20.20.2 port fa0/7
device 172.20.20.2 port fa0/8
device 172.20.20.2 port fa0/9
device 172.20.20.2 port fa0/10
device 172.20.20.2 port fa0/11
device 172.20.20.2 port fa0/12
device 172.20.20.2 port fa0/13
device 172.20.20.2 port fa0/14
device 172.20.20.2 port fa0/15
device 172.20.20.2 port fa0/16
device 172.20.20.2 port fa0/17
device 172.20.20.2 port fa0/18
device 172.20.20.2 port fa0/19
device 172.20.20.2 port fa0/20
device 172.20.20.2 port fa0/21
device 172.20.20.2 port fa0/22
device 172.20.20.2 port fa0/23
device 172.20.20.2 port fa0/24
!
vmps-port-group A3_19_24
device 172.20.20.3 port fa0/19
device 172.20.20.3 port fa0/20
device 172.20.20.3 port fa0/21
device 172.20.20.3 port fa0/22
device 172.20.20.3 port fa0/23
device 172.20.20.3 port fa0/24
!
vmps-port-group A4_19_24
device 172.20.20.4 port fa0/19
device 172.20.20.4 port fa0/20
device 172.20.20.4 port fa0/21
device 172.20.20.4 port fa0/22
device 172.20.20.4 port fa0/23
device 172.20.20.4 port fa0/24
!
vmps-port-group B2_3_24
device 172.20.20.6 port fa0/3
device 172.20.20.6 port fa0/4
device 172.20.20.6 port fa0/5
device 172.20.20.6 port fa0/6
device 172.20.20.6 port fa0/7
device 172.20.20.6 port fa0/8
device 172.20.20.6 port fa0/9
device 172.20.20.6 port fa0/10
device 172.20.20.6 port fa0/11
device 172.20.20.6 port fa0/12
device 172.20.20.6 port fa0/13
```

```
device 172.20.20.6 port fa0/14
device 172.20.20.6 port fa0/15
device 172.20.20.6 port fa0/16
device 172.20.20.6 port fa0/17
device 172.20.20.6 port fa0/18
device 172.20.20.6 port fa0/19
device 172.20.20.6 port fa0/20
device 172.20.20.6 port fa0/21
device 172.20.20.6 port fa0/22
device 172.20.20.6 port fa0/23
device 172.20.20.6 port fa0/24
!
vmps-port-group B3_19_24
device 172.20.20.7 port fa0/19
device 172.20.20.7 port fa0/20
device 172.20.20.7 port fa0/21
device 172.20.20.7 port fa0/22
device 172.20.20.7 port fa0/23
device 172.20.20.7 port fa0/24
!
vmps-port-group C1_19_24
device 172.20.20.8 port fa0/19
device 172.20.20.8 port fa0/20
device 172.20.20.8 port fa0/21
device 172.20.20.8 port fa0/22
device 172.20.20.8 port fa0/23
device 172.20.20.8 port fa0/24
!
vmps-port-group C2_3_24
device 172.20.20.9 port fa0/3
device 172.20.20.9 port fa0/4
device 172.20.20.9 port fa0/5
device 172.20.20.9 port fa0/6
device 172.20.20.9 port fa0/7
device 172.20.20.9 port fa0/8
device 172.20.20.9 port fa0/9
device 172.20.20.9 port fa0/10
device 172.20.20.9 port fa0/11
device 172.20.20.9 port fa0/12
device 172.20.20.9 port fa0/13
device 172.20.20.9 port fa0/14
device 172.20.20.9 port fa0/15
device 172.20.20.9 port fa0/16
device 172.20.20.9 port fa0/17
device 172.20.20.9 port fa0/18
device 172.20.20.9 port fa0/19
device 172.20.20.9 port fa0/20
device 172.20.20.9 port fa0/21
device 172.20.20.9 port fa0/22
device 172.20.20.9 port fa0/23
device 172.20.20.9 port fa0/24
!
vmps-port-group C4_19_24
device 172.20.20.11 port fa0/19
device 172.20.20.11 port fa0/20
device 172.20.20.11 port fa0/21
device 172.20.20.11 port fa0/22
device 172.20.20.11 port fa0/23
device 172.20.20.11 port fa0/24
!
vmps-port-group D2_19_24
```

```
device 172.20.20.13 port fa0/19
device 172.20.20.13 port fa0/20
device 172.20.20.13 port fa0/21
device 172.20.20.13 port fa0/22
device 172.20.20.13 port fa0/23
device 172.20.20.13 port fa0/24
!
vmps-port-group D3_19_24
device 172.20.20.14 port fa0/19
device 172.20.20.14 port fa0/20
device 172.20.20.14 port fa0/21
device 172.20.20.14 port fa0/22
device 172.20.20.14 port fa0/23
device 172.20.20.14 port fa0/24
!
vmps-port-group D4_19_24
device 172.20.20.15 port fa0/19
device 172.20.20.15 port fa0/20
device 172.20.20.15 port fa0/21
device 172.20.20.15 port fa0/22
device 172.20.20.15 port fa0/23
device 172.20.20.15 port fa0/24
!
vmps-port-group D5_19_24
device 172.20.20.16 port fa0/19
device 172.20.20.16 port fa0/20
device 172.20.20.16 port fa0/21
device 172.20.20.16 port fa0/22
device 172.20.20.16 port fa0/23
device 172.20.20.16 port fa0/24
!
!VLAN groups
!oznacza sieci VLAN połączone w jedną grupę,zastosowano do VLAN
!administracja oraz it, ponieważ zasady dotyczące możliwości ich
!występowania na określonych przełącznikach są identyczne
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmps-vlan-group admin_it
vlan-name administracja
vlan-name it
!
!VLAN port Policies
!określają zasady występowania określonych sieci VLAN na określonych
!portach wybranych przełączników. VLAN port polices zostały wykorzystane do
!ustawienia na serwerze VMPS reguł ustalonych w „założeniach do projektu”
!(rysunek 35 oraz 45)
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
!
!przykładowo: sieci VLAN administracja i it mogą być dynamicznie
!przydzielane tylko na grupach portów przełączników wypisanych poniżej
!
vmps-port-policies vlan-group admin_it
port-group A2_3_24
port-group B2_3_24
port-group C2_3_24
port-group A4_19_24
port-group C3_19_24
```

```
port-group D5_19_24
!
vmps-port-policies vlan-name zarzadzanie
port-group A2_3_24
port-group A3_19_24
port-group A4_19_24
port-group A4_19_24
port-group B2_3_24
port-group B3_19_24
port-group C1_19_24
port-group C2_3_24
port-group C3_19_24
port-group D5_19_24
!
vmps-port-policies vlan-name ksiegowosc
port-group A3_19_24
port-group B3_19_24
port-group A4_19_24
port-group C1_19_24
port-group D2_19_24
!
vmps-port-policies vlan-name produkcja
port-group A1_19_24
port-group D3_19_24
port-group D4_19_24
port-group D5_19_24
!
vmps-port-policies vlan-name produkcja
port-group A1_19_24
port-group A2_3_24
port-group B2_3_24
port-group A4_19_24
port-group C2_19_24
port-group D3_19_24
port-group D4_19_24
port-group C4_19_24
!
vmps-port-policies vlan-name sprzedaz
port-group A2_3_24
port-group B2_3_24
port-group A3_19_24
port-group B3_19_24
port-group A4_19_24
port-group C1_19_24
port-group D2_19_24
port-group C2_3_24
```

Plik został zapisany pod nazwą „vmps_conf.txt” i umieszczony na serwerze TFTP podpiętym do przełącznika głównego.

Konfigurowanie przełącznika głównego jako serwera VMPS

```
glowny> enable
glowny# configure terminal
glowny(config)# interface vlan1
```

```
glowny(config-if)# ip address 172.20.20.100 255.255.255.0
glowny(config-if)#exit
glowny(config)# set vmps tftpserwer 172.20.20.150 vmps_conf.txt
glowny(config)# set vmps state enable
glowny(config)# exit
```

Najpierw ustawiany jest wymagany przez VMPS adres IP przełącznika. Przełączniki domyślnie komunikują się między sobą w sieci VLAN1, która jest określana siecią zarządzania, dlatego adres IP został ustawiony na interfejsie VLAN1.

7.5.5 Konfigurowanie portów przełączników do działania w statycznych i dynamicznych sieciach VLAN

Konfigurowanie statycznego przypisania portów przełącznika głównego, do których podpięte są serwery w firmie do sieci VLAN

```
glowny> enable
glowny# configure terminal
glowny(config)# set vlan 80 0/10 - 12
glowny(config)# set vlan 40 0/15
glowny(config)# set vlan 70 0/16
glowny(config)# set vlan 60 0/17
glowny(config)# set vlan 1 0/20
glowny(config)# exit
```

Konfigurowanie przełączników dostępowych

Przed konfiguracją portów ustawiany jest adres IP przełącznika oraz adres IP serwera VMPS, jeżeli przełącznik jest przewidziany do obsługi dynamicznych sieci VLAN.

Przełącznik A1:

```
A1> enable
A1# configure terminal
A1(config)# interface vlan1
A1(config-if)# ip address 172.20.20.1 255.255.255.0
A1(config-if)# exit
A1(config)# vmps server 172.20.20.100 primary
A1(config-if)# interface fa0/1 - 2
A1(config-if-range)# switchport mode access
A1(config-if-range)# switchport access vlan 5
A1(config-if-range)# interface fa0/3 - 18
A1(config-if-range)# switchport mode access
A1(config-if-range)# switchport access vlan 60
A1(config-if-range)# interface fa0/19 - 24
A1(config-if-range)# switchport mode access
A1(config-if-range)# switchport access vlan dynamic
A1(config-if-range)# exit
```

Przełącznik A2:

```
A2> enable
A2# configure terminal
A2(config)# interface vlan1
```

```
A2(config-if)# ip address 172.20.20.2 255.255.255.0
A2(config-if)# exit
A2(config)# vmps server 172.20.20.100 primary
A2(config-if)# interface fa0/1 - 2
A2(config-if-range)# switchport mode access
A2(config-if-range)# switchport access vlan 5
A2(config-if-range)# interface fa0/3 - 24
A2(config-if-range)# switchport mode access
A2(config-if-range)# switchport access vlan dynamic
A2(config-if-range)# exit
```

Przełącznik A3:

```
A3> enable
A3# configure terminal
A3(config)# interface vlan1
A3(config-if)# ip address 172.20.20.3 255.255.255.0
A3(config-if)# exit
A3(config)# vmps server 172.20.20.100 primary
A3(config-if)# interface fa0/1 - 2
A3(config-if-range)# switchport mode access
A3(config-if-range)# switchport access vlan 5
A3(config-if-range)# interface fa0/3 - 18
A3(config-if-range)# switchport mode access
A3(config-if-range)# switchport access vlan 40
A3(config-if-range)# interface fa0/19 - 24
A3(config-if-range)# switchport mode access
A3(config-if-range)# switchport access vlan dynamic
A3(config-if-range)# exit
```

Przełącznik A4:

```
A4> enable
A4# configure terminal
A4(config)# interface vlan1
A4(config-if)# ip address 172.20.20.4 255.255.255.0
A4(config-if)# exit
A4(config)# vmps server 172.20.20.100 primary
A4(config-if)# interface fa0/1 - 2
A4(config-if-range)# switchport mode access
A4(config-if-range)# switchport access vlan 5
A4(config-if-range)# interface fa0/3 - 18
A4(config-if-range)# switchport mode access
A4(config-if-range)# switchport access vlan 30
A4(config-if-range)# interface fa0/19 - 24
A4(config-if-range)# switchport mode access
A4(config-if-range)# switchport access vlan dynamic
A4(config-if-range)# exit
```

Przełącznik B1 (bez vmps):

```
B1> enable
B1# configure terminal
B1(config-if)# interface fa0/1 - 2
B1(config-if-range)# switchport mode access
B1(config-if-range)# switchport access vlan 5
B1(config-if-range)# interface fa0/3 - 24
B1(config-if-range)# switchport mode access
B1config-if-range)# switchport access vlan 20
B1(config-if-range)# exit
```

Przełącznik B2:

```
B2> enable
B2# configure terminal
```

```
B2(config)# interface vlan1
B2(config-if)# ip address 172.20.20.6 255.255.255.0
B2(config-if)# exit
B2(config)# vmps server 172.20.20.100 primary
B2(config-if)# interface fa0/1 - 2
B2(config-if-range)# switchport mode access
B2(config-if-range)# switchport access vlan 5
B2(config-if-range)# interface fa0/3 - 24
B2(config-if-range)# switchport mode access
B2(config-if-range)# switchport access vlan dynamic
B2(config-if-range)# exit
```

Przełącznik B3:

```
B3> enable
B3# configure terminal
B3(config)# interface vlan1
B3(config-if)# ip address 172.20.20.7 255.255.255.0
B3(config-if)# exit
B3(config)# vmps server 172.20.20.100 primary
B3(config-if)# interface fa0/1 - 2
B3(config-if-range)# switchport mode access
B3(config-if-range)# switchport access vlan 5
B3(config-if-range)# interface fa0/3 - 18
B3(config-if-range)# switchport mode access
B3(config-if-range)# switchport access vlan 40
B3(config-if-range)# interface fa0/19 - 24
B3(config-if-range)# switchport mode access
B3(config-if-range)# switchport access vlan dynamic
B3(config-if-range)# exit
```

Przełącznik C1:

```
C1> enable
C1# configure terminal
C1(config)# interface vlan1
C1(config-if)# ip address 172.20.20.8 255.255.255.0
C1(config-if)# exit
C1(config)# vmps server 172.20.20.100 primary
C1(config-if)# interface fa0/1 - 2
C1(config-if-range)# switchport mode access
C1(config-if-range)# switchport access vlan 5
C1(config-if-range)# interface fa0/3 - 18
C1(config-if-range)# switchport mode access
C1(config-if-range)# switchport access vlan 70
C1(config-if-range)# interface fa0/19 - 24
C1(config-if-range)# switchport mode access
C1(config-if-range)# switchport access vlan dynamic
C1(config-if-range)# exit
```

Przełącznik C2:

```
C2> enable
C2# configure terminal
C2(config)# interface vlan1
C2(config-if)# ip address 172.20.20.9 255.255.255.0
C2(config-if)# exit
C2(config)# vmps server 172.20.20.100 primary
C2(config-if)# interface fa0/1 - 2
C2(config-if-range)# switchport mode access
C2(config-if-range)# switchport access vlan 5
C2(config-if-range)# interface fa0/3 - 24
C2(config-if-range)# switchport mode access
C2(config-if-range)# switchport access vlan dynamic
```

```
C2(config-if-range)# exit
```

Przełącznik C3:

```
C3> enable
C3# configure terminal
C3(config)# interface vlan1
C3(config-if)# ip address 172.20.20.10 255.255.255.0
C3(config-if)# exit
C3(config)# vmps server 172.20.20.100 primary
C3(config-if)# interface fa0/1 - 2
C3(config-if-range)# switchport mode access
C3(config-if-range)# switchport access vlan 5
C3(config-if-range)# interface fa0/3 - 18
C3(config-if-range)# switchport mode access
C3(config-if-range)# switchport access vlan 10
C3(config-if-range)# interface fa0/19 - 24
C3(config-if-range)# switchport mode access
C3(config-if-range)# switchport access vlan dynamic
C3(config-if-range)# exit
```

Przełącznik C4:

```
C4> enable
C4# configure terminal
C4(config)# interface vlan1
C4(config-if)# ip address 172.20.20.11 255.255.255.0
C4(config-if)# exit
C4(config)# vmps server 172.20.20.100 primary
C4(config-if)# interface fa0/1 - 2
C4(config-if-range)# switchport mode access
C4(config-if-range)# switchport access vlan 5
C4(config-if-range)# interface fa0/3 - 18
C4(config-if-range)# switchport mode access
C4(config-if-range)# switchport access vlan 60
C4(config-if-range)# interface fa0/19 - 24
C4(config-if-range)# switchport mode access
C4(config-if-range)# switchport access vlan dynamic
C4(config-if-range)# exit
```

Przełącznik D1 (bez vmps, VTP transparent):

```
D1> enable
D1# configure terminal
D1(config-if)# interface fa0/1 - 2
D1(config-if-range)# switchport mode access
D1(config-if-range)# switchport access vlan 5
D1(config-if-range)# interface fa0/3 - 12
D1(config-if-range)# switchport mode access
D1config-if-range)# switchport access vlan 50
D1(config-if-range)# interface fa0/13 - 24
D1(config-if-range)# switchport mode access
D1config-if-range)# switchport access vlan 100
D1(config-if-range)# exit
```

Przełącznik D2:

```
D2> enable
D2# configure terminal
D2(config)# interface vlan1
D2(config-if)# ip address 172.20.20.13 255.255.255.0
D2(config-if)# exit
D2(config)# vmps server 172.20.20.100 primary
D2(config-if)# interface fa0/1 - 2
D2(config-if-range)# switchport mode access
D2(config-if-range)# switchport access vlan 5
```

```
D2(config-if)# interface fa0/3 - 18
D2(config-if-range)# switchport mode access
D2(config-if-range)# switchport access vlan 70
D2(config-if-range)# interface fa0/19 - 24
D2(config-if-range)# switchport mode access
D2(config-if-range)# switchport access vlan dynamic
D2(config-if-range)# exit
```

Przełącznik D3:

```
D3> enable
D3# configure terminal
D3(config)# interface vlan1
D3(config-if)# ip address 172.20.20.14 255.255.255.0
D3(config-if)# exit
D3(config)# vmps server 172.20.20.100 primary
D3(config-if)# interface fa0/1 - 2
D3(config-if-range)# switchport mode access
D3(config-if-range)# switchport access vlan 5
D3(config-if)# interface fa0/3 - 18
D3(config-if-range)# switchport mode access
D3(config-if-range)# switchport access vlan 50
D3(config-if-range)# interface fa0/19 - 24
D3(config-if-range)# switchport mode access
D3(config-if-range)# switchport access vlan dynamic
D3(config-if-range)# exit
```

Przełącznik D4:

```
D4> enable
D4# configure terminal
D4(config)# interface vlan1
D4(config-if)# ip address 172.20.20.15 255.255.255.0
D4(config-if)# exit
D4(config)# vmps server 172.20.20.100 primary
D4(config-if)# interface fa0/1 - 2
D4(config-if-range)# switchport mode access
D4(config-if-range)# switchport access vlan 5
D4(config-if)# interface fa0/3 - 18
D4(config-if-range)# switchport mode access
D4(config-if-range)# switchport access vlan 70
D4(config-if-range)# interface fa0/19 - 24
D4(config-if-range)# switchport mode access
D4(config-if-range)# switchport access vlan dynamic
D4(config-if-range)# exit
```

Przełącznik D5:

```
D5> enable
D5# configure terminal
D5(config)# interface vlan1
D5(config-if)# ip address 172.20.20.16 255.255.255.0
D5(config-if)# exit
D5(config)# vmps server 172.20.20.100 primary
D5(config-if)# interface fa0/1 - 2
D5(config-if-range)# switchport mode access
D5(config-if-range)# switchport access vlan 5
D5(config-if)# interface fa0/3 - 18
D5(config-if-range)# switchport mode access
D5(config-if-range)# switchport access vlan 10
D5(config-if-range)# interface fa0/19 - 24
D5(config-if-range)# switchport mode access
D5(config-if-range)# switchport access vlan dynamic
D5(config-if-range)# exit
```

7.5.6 Konfigurowanie rutowania w sieci

Poniższe polecenia, wykonane po zalogowaniu się do modułu rutującego MSFC przełącznika głównego, umożliwiają włączenie trasowania ruchu między sieciami VLAN w firmie. Wykorzystane adresy bram w poszczególnych sieciach zostały przedstawiona na rysunku 42. Protokołem rutowania jest RIP.

```
router> enable
router# configure terminal
router(config)# ip routing
router(config)# interface vlan 5
router(config-if)# ip address 192.168.5.1 255.255.255.0
router(config)# interface vlan 10
router(config-if)# ip address 192.168.10.1 255.255.255.0
router(config)# interface vlan 20
router(config-if)# ip address 192.168.20.1 255.255.255.0
router(config)# interface vlan 30
router(config-if)# ip address 192.168.30.1 255.255.255.0
router(config)# interface vlan 40
router(config-if)# ip address 192.168.40.1 255.255.255.0
router(config)# interface vlan 50
router(config-if)# ip address 192.168.50.1 255.255.255.0
router(config)# interface vlan 60
router(config-if)# ip address 192.168.60.1 255.255.255.0
router(config)# interface vlan 70
router(config-if)# ip address 192.168.70.1 255.255.255.0
router(config)# interface vlan 80
router(config-if)# ip address 192.168.80.1 255.255.255.0
router(config-if)# router rip
router(config-router)# network 192.168.5.0
router(config-router)# network 192.168.10.0
router(config-router)# network 192.168.20.0
router(config-router)# network 192.168.30.0
router(config-router)# network 192.168.40.0
router(config-router)# network 192.168.50.0
router(config-router)# network 192.168.60.0
router(config-router)# network 192.168.70.0
router(config-router)# network 192.168.80.0
router(config-router)# exit
```

7.6 Podsumowanie projektu

Projektowaną sieć udało się skonfigurować tak, by spełniała ona wszystkie wymagania sformułowane w założeniach do projektu. Dodatkowo sieć zapewnia wymaganą niezawodność, wydajność oraz bezpieczeństwo. Zastosowanie serwera VMPS do zarządzania sieciami dynamicznymi daje ogromną elastyczność konfiguracji zasad przynależności do sieci VLAN. Rutowanie wewnętrzne na przełączniku głównym powoduje, że w sieci nie ma opóźnień przesyłania ruchu między sieciami wirtualnymi, a dzięki zastosowaniu list ACL może on być w łatwy sposób restrykcjonowany. Patrząc w przyszłość, gdyby firma rozrosła się jeszcze bardziej i otworzyła filię lub kilka filii, dzięki zastosowanie techniki LANE wszystkie części firmy będzie można ze sobą połączone wraz z istniejącym odwzorowaniem sieci wirtualnych ponad infrastrukturą ATM sieci Internet.

Rozdział VIII Zakończenie

Cel pracy, którym było przedstawienie technologii wirtualnych sieci LAN oraz zaprojektowanie z ich udziałem infrastruktury sieciowej został w pełni osiągnięty. Rozdziały od I do VI, będące częścią teoretyczną, zawierają przystępnie przedstawione najistotniejsze informacje oraz opisy mechanizmów z dziedziny sieci VLAN. Rozdział VII natomiast przedstawia praktyczne użycie większości mechanizmów, o których była mowa wcześniej. Trzeba jednak pamiętać, że praca opisuje jedynie najważniejsze elementy „świata” sieci wirtualnych i nie jest możliwe zawarcie całego, niezwykle szerokiego jego spektrum w ramach pracy licencjackiej. Ze względu na brak polskiej literatury na temat sieci wirtualnych LAN, w czasie pisania pracy korzystałem głównie z dokumentu opisującego standard IEEE 802.1Q w wersji z roku 2003 oraz innych anglojęzycznych materiałów znajdujących się na stronach internetowych, pomocne były także materiały akademii sieciowej firmy Cisco CCNA oraz CCNP.

Bibliografia

1. Dokumenty opisujące standard 802.1Q w wersji z roku 2003, http://standards.ieee.org/getieee802/download/802.1Q-2003.pdf, 24.04.2006
2. Materiały CCNA w wersji 3.1PL oraz CCNP akademii sieciowej firmy Cisco,2006
3. „Cisco Catalyst LAN Switching” Louis R. Rossi i Louis D. Rossi, Cisco Press 2002
4. „Cisco LAN Switching” Kennedy Clark i Kelvin Hamilton, Cisco Press, 1999
5. „The Virtual LAN Technology Report”,1996, http://www.3com.com/other/pdfs/solutions/en_US/20037401.pdf, 18.06.2006
6. Materiały o sieciach VLAN na stronie http://www.firewall.cx/vlans-intro.php, 5.05.2006
7. „Virtual LANs”, http://scitec.uwichill.edu.bb/cmp/online/cs23l/vlans.pdf, 1.06.2006
8. “Virtual Local Area Networks” Alcatel, http://faculty.capitol-college.edu/~wbutler/IA%20712/Week%204/Asynch/alcatelwpvlans.pdf, 4.06.2006
9. “LANE(LAN Emulation)” Linktionary, http://www.linktionary.com/l/lane.html, 23.06.2006
10. Opis systemu Cisco Operating System w wersji 8.1 przeznaczonego na przełączniki z rodziny Cisco Catalyst 6500, http://www.cisco.com/application/pdf/en/us/guest/products/ps708/c2001/ccmigration_09186a00801d2ef4.pdf, 1.07.2006
11. Opis systemu IOS w wersji 12.1 przeznaczonego na przełączniki z rodziny Cisco Catalyst 3560, http://www.cisco.com/application/pdf/en/us/guest/products/ps5528/c2001/ccmigration_09186a00801e85be.pdf, 1.07.2006
12. Opis systemu IOS w wersji 12.1 przeznaczonego na przełączniki z rodziny Cisco Catalyst 2960, http://www.cisco.com/en/US/products/ps6406/products_configuration_guide_book09186a00805f80e4.html, 1.07.2006

Spis ilustracji