Przełączanie w sieciach lokalnych

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UMCS

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt „Programowa i strukturalna reforma systemu kształcenia na Wydziale Mat-Fiz-Inf”.
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Człowiek-najlepsza inwestycja

Uniwersytet Marii Curie-Skłodowskiej
Wydział Matematyki, Fizyki i Informatyki
Instytut Informatyki

Przełączanie w sieciach lokalnych

Karol Kuczyński
Waldemar Suszyński

Lublin 2012

Instytut Informatyki UMCS
Lublin 2012

Karol Kuczyński
Waldemar Suszyński
Przełączanie w sieciach lokalnych

Recenzent: Andrzej Bobyk

Opracowanie techniczne: Marcin Denkowski
Projekt okładki: Agnieszka Kuśmierska

Praca współfinansowana ze środków Unii Europejskiej w ramach
Europejskiego Funduszu Społecznego

Publikacja bezpłatna dostępna on-line na stronach
Instytutu Informatyki UMCS: informatyka.umcs.lublin.pl.

Wydawca
Uniwersytet Marii Curie-Skłodowskiej w Lublinie
Instytut Informatyki
pl. Marii Curie-Skłodowskiej 1, 20-031 Lublin
Redaktor serii: prof. dr hab. Paweł Mikołajczak
www: informatyka.umcs.lublin.pl
email: dyrii@hektor.umcs.lublin.pl

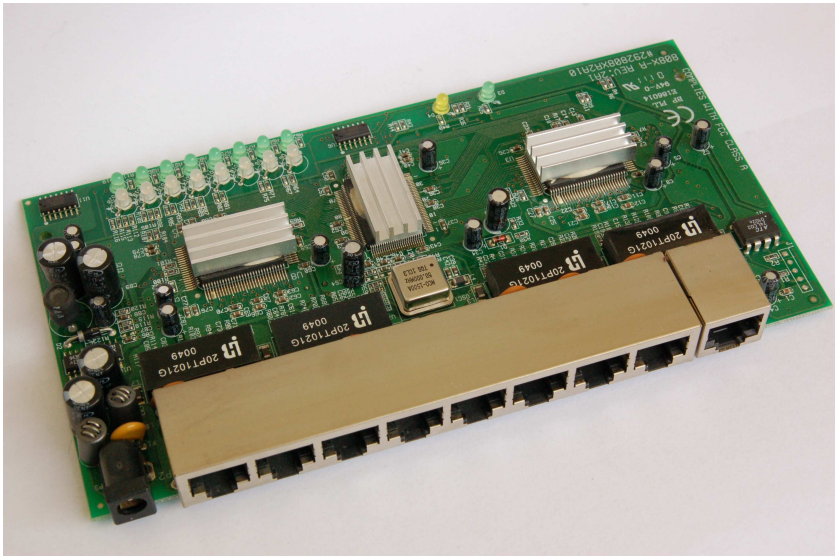
Druk
FIGARO Group Sp. z o.o. z siedzibą w Rykach
ul. Warszawska 10
08-500 Ryki
www: www.figaro.pl

ISBN: 978-83-62773-25-1

Spis treści

Przedmowa

Przełączanie we współczesnych sieciach lokalnych (LAN) jest technologią o zasadniczym znaczeniu. Pod pojęciem tym rozumiemy tu takie sterowanie ruchem, by w miarę możliwości docierał wyłącznie do adresata. Pożądane są szybkie rozwiązania sprzętowe. Prezentowane w dalszej części zagadnienia będą dotyczyły przede wszystkim przełączania w drugiej warstwie modelu OSI (rys. 1), jednak zostaną również przedstawione główne problemy przełączania w warstwie trzeciej i czwartej, jak również przełączania wielowarstwowego (ang. *Multilayer Switching*, MLS).



Rysunek 1. Wnętrze prostego przełącznika Ethernet

Sieci lokalne są obecnie zdominowane przez różne warianty technologii Ethernet (obok rozwiązań bezprzewodowych). Niegdyś konkurencyjne protokoły, takie jak Token Ring i FDDI mają już jedynie znaczenie historyczne. W związku z tym, technologia Ethernet została przedstawiona od strony teoretycznej (zasady funkcjonowania, ewolucja protokołu), jak też

praktycznej (podstawowa i bardziej zaawansowana konfiguracja przełączników Ethernet).

W kolejnych rozdziałach omówiono zagadnienia związane z budową wirtualnych sieci lokalnych (ang. *Virtual Local Area Network*, VLAN): podstawy teoretyczne, protokoły, metody konfiguracji i zarządzania, routing między sieciami VLAN.

Istotną kwestią jest zapewnienie niezawodności sieci lokalnej poprzez redundancję przełączników i połączeń między nimi, w sposób gwarantujący brak pętli w topologii logicznej (w 2. warstwie OSI). Jest to realizowane poprzez implementację protokołu drzewa rozpinającego (ang. *Spanning Tree Protocol*, STP). Protokół ten jest dość rozbudowany. Ocenia się, że znaczna część problemów występujących w skomplikowanych sieciach LAN wynika z jego niedostatecznej znajomości i niepoprawnej konfiguracji.

Ważne i jednocześnie bardzo często zaniedbywane przez administratorów są problemy bezpieczeństwa sieci związane z drugą warstwą modelu OSI. Kolejny rozdział przedstawia główne zagrożenia i sposoby zapobiegania im.

Większość prezentowanych treści znajduje się na liście zagadnień obowiązujących na egzaminie Cisco Certified Network Associate (640-802 CCNA) [1] lub stanowi ich rozszerzenie. Dodatkowe informacje można znaleźć w cytowanych źródłach literaturowych: dokumentach RFC (ang. *Request for Comments*), opisach standardów, dokumentach technicznych Cisco. Dostępna jest także literatura polskojęzyczna [1, 2, 3, 4], która jednak nie obejmuje wszystkich prezentowanych tu zagadnień.

Przedstawioną teorię uzupełniają propozycje ćwiczeń praktycznych (w znacznej części z kompletnymi rozwiązaniami lub wskazówkami), możliwych do wykonania w laboratorium sieciowym lub przy pomocy oprogramowania symulacyjnego. Do wykonania ćwiczeń zaleca się użycie trzech przełączników Cisco Catalyst 2960 lub 3560 z systemem IOS w wersji 12.2 (lub nowszej) oraz jednego lub dwóch dwóch routerów Cisco ISR 1841, 2801, 2811, 1941, 2901 lub 2911 (w przypadku innych modeli urządzeń wyposażonych w IOS, mogą wystąpić różnice w sposobie implementacji poszczególnych funkcji). Przedstawienie przykładów wykorzystujących rozwiązania konkretnego producenta sprzętu (Cisco Systems[1]) nie stanowi istotnego zawężenia ogólności prezentowanych rozważań, ponieważ opisywane technologie są (poza nielicznymi przypadkami, gdzie zostało to wyraźnie zaznaczone) powszechnie przyjętymi standardami. W przypadku dobrej ich znajomości, techniczne różnice w konfiguracji urządzeń różnych producentów nie powinny stanowić istotnego problemu.

Wymagania wstępne obejmują znajomość następujących zagadnień:
— modele OSI oraz TCP/IP,

[1] `http://www.cisco.com`

— podstawowe protokoły stosu TCP/IP,
— podstawy adresowania IPv4 i podziału na podsieci,
— konfigurowanie ustawień sieciowych hosta (w systemie Linux lub MS Windows),
— podstawy routingu statycznego i dynamicznego,
— podstawowa znajomość IOS oraz sposobu konfigurowania urządzeń Cisco,
— podstawy technologii Ethernet.

Polskojęzyczne odpowiedniki niektórych pojęć, użytych w podręczniku, mogą być kontrowersyjne, co jest nieuchronne przy tego typu publikacji. W związku z tym, w końcowej części znajduje się słownik angielsko-polski, w którym umieszczono przede wszystkim mniej oczywiste tłumaczenia.

Rozdział 1

Technologia Ethernet

1.1. Wstęp

Ethernet jest dominującą rodziną technologii wykorzystywanych do budowy sieci lokalnych. W zastosowaniach komercyjnych funkcjonuje od początku lat osiemdziesiątych XX wieku i jest nadal rozwijany, w przeciwieństwie do konkurencyjnych technologii, jak Token Ring (protokół IEEE 802.5 [5]), FDDI (ANSI X3T9.5 [6]) i ARCNET (ATA 878.1-1999 [7]), które mają już jedynie znaczenie historyczne. Ethernet definiuje protokoły warstwy fizycznej oraz warstwy łącza danych modelu OSI. Przy projektowaniu sieci lokalnej, jedyną wartą rozważenia alternatywą Ethernetu jest sieć bezprzewodowa WiFi. Jednak również w tym przypadku, jej szkielet (tzw. system dystrybucyjny) jest najczęściej realizowany w technologii Ethernet.

1.2. Historia

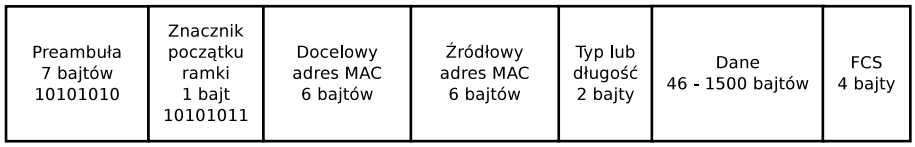
Inspiracją twórców technologii Ethernet była sieć radiowa ALOHAnet [8], łącząca bezprzewodowo komputery Uniwersytetu Hawajskiego, znajdujące się na kilku różnych wyspach. Nadawca mógł rozpocząć swoją transmisję w dowolnym momencie. Następnie oczekiwał na potwierdzenie odebrania od adresata. W razie braku potwierdzenia w określonym czasie, transmisja była ponawiana. Najczęstszym powodem niepowodzenia transmisji (skutkującego powtórną próbą) były kolizje, wynikające z jednoczesnej emisji dwóch lub większej liczby sygnałów.

Za głównego twórcę Ethernetu uznawany jest Robert Metcalfe z firmy Xerox, pracujący tam w latach siedemdziesiątych XX wieku [9]. Podstawową ideą jest dołączenie wielu węzłów do wspólnego medium (kabla miedzianego), przy czym każdy z nich ma równorzędne prawa i może rozpocząć transmisję w dowolnym momencie. W danej chwili transmitować może jednak tylko jeden węzeł. Równoczesna próba rozpoczęcia transmisji przez dwa węzły (które uprzednio stwierdziły, że medium jest dostępne) skutkuje kolizją i koniecznością retransmisji. Kolizja jest tu zatem zjawiskiem normalnym i, o ile nie występuje zbyt często (np. wskutek dołączenia zbyt dużej liczby urządzeń do segmentu sieci), nie wpływa istotnie na funkcjonalność sieci. Ten sposób realizacji dostępu do medium sieciowego w późniejszym okresie określono mianem *wielodostępu z badaniem stanu kanału i wykrywaniem kolizji* (ang. *Carrier Sense Multiple Access / with Collision Detection*, CSMA/CD).

Mechanizm ten jest prostszy niż w konkurencyjnych technologiach (Token Ring, FDDI), wykorzystujących przekazywanie żetonu (ang. *token passing*). Żeton jest specjalną ramką, która jest kolejno przekazywana do poszczególnych hostów w sieci. Posiadanie żetonu daje hostowi prawo do trans-

mitowania danych poprzez medium. Metoda przekazywania żetonu umożliwia zbudowanie sieci zachowującej się w sposób bardziej przewidywalny ("deterministyczny") niż w przypadku CSMA/CD i wydaje się bardziej bardziej zaawansowana technologicznie. W praktyce jednak "niedeterministyczne" technologie sieciowe, implementujące CSMA/CD, okazały się w większości sytuacji bardziej efektywne.

Dalsze prace nad protokołem Ethernet były prowadzone przez firmy Digital Equipment Corporation (DEC), Intel i Xerox. Standard DIX (od pierwszych liter nazw firm) definiował transmisję z szybkością 10 Mb/s oraz 48-bitowe adresy docelowe i źródłowe. Kolejna wersja, z roku 1982, nosiła oznaczenie Ethernet II. W roku 1980 IEEE[1] rozpoczęło prace nad standaryzacją technologii sieci lokalnych, w ramach projektu nr 802. Dotyczył on protokołu CSMA/CD, zaproponowanego przez DIX, oraz technologii konkurencyjnych. Ostatecznie, standard CSMA/CD został opublikowany jako IEEE 802.3.



Rysunek 1.1. Ramka Ethernet 802.3

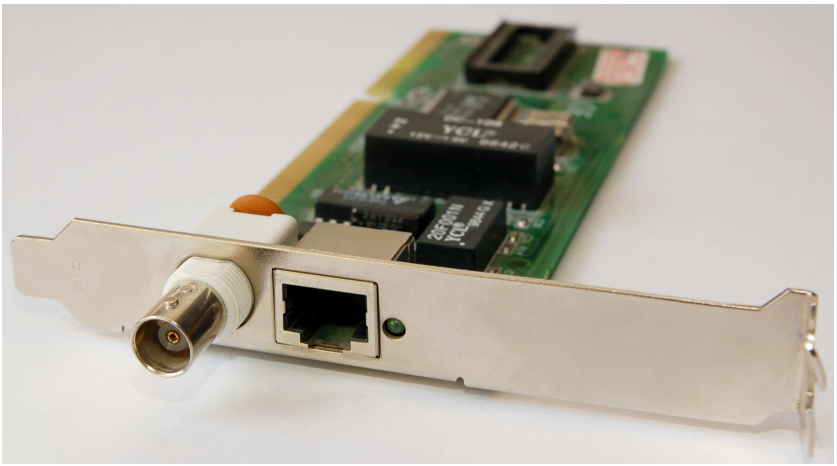
Rys. 1.1 przedstawia schemat ramki Ethernet, zgodnej z IEEE 802.3. W formacie ramki zaproponowanym przez DIX (Ethernet II), w miejscu pola *Typ lub długość* (ang. *EtherType or length*) występowało pole *Typ* (*EtherType*), informujące o protokole wyższej warstwy, którego dane są opakowane w ramkę. Ramka Ethernet II jest nadal najbardziej popularna. IEEE zamiast pola *Typ* wprowadziło początkowo pole *Długość* (*Length*), a informacja o typie danych była umieszczona w nagłówku 802.2, znajdującym się dalej. W kolejnej wersji standardu 802.3 (z 1997 roku) dopuszczono możliwość stosowania obu wariantów (jak na rys. 1.1). Wartość 1536 lub wyższa jest interpretowana jako typ, a mniejsza lub równa 1500 jako długość pola z danymi.

W początkowych implementacjach Ethernetu wykorzystywano kabel koncentryczny o impedancji 50 Ω i średnicy około 10 milimetrów (tzw. gruby Ethernet, ang. *thicknet*), zwykle koloru żółtego. Była to specyfikacja 10BASE5. 10 odnosi się do szerokości pasma, wyrażonej w Mb/s. BASE oznacza transmisję w paśmie podstawowym (ang. *baseband*), gdzie przez medium fizyczne transmitowany jest tylko jeden sygnał, w odróżnieniu od transmisji szerokopasmowej (BROAD), gdzie w medium fizycznym można wyodrębnić

[1] `http://www.ieee.org/`

wiele kanałów transmisyjnych (ang. *broadband*). Maksymalna długość kabla wynosiła 500 metrów ("5" w oznaczeniu).

Nowszym wariantem jest 10BASE2 – tzw. cienki Ethernet (ang. *thinnet*, *cheapernet*), wykorzystujący tańszy i łatwiejszy do instalacji kabel, jednak kosztem mniejszej maksymalnej długości (185 metrów, cyfra "2" oznacza tu "około 200 metrów").

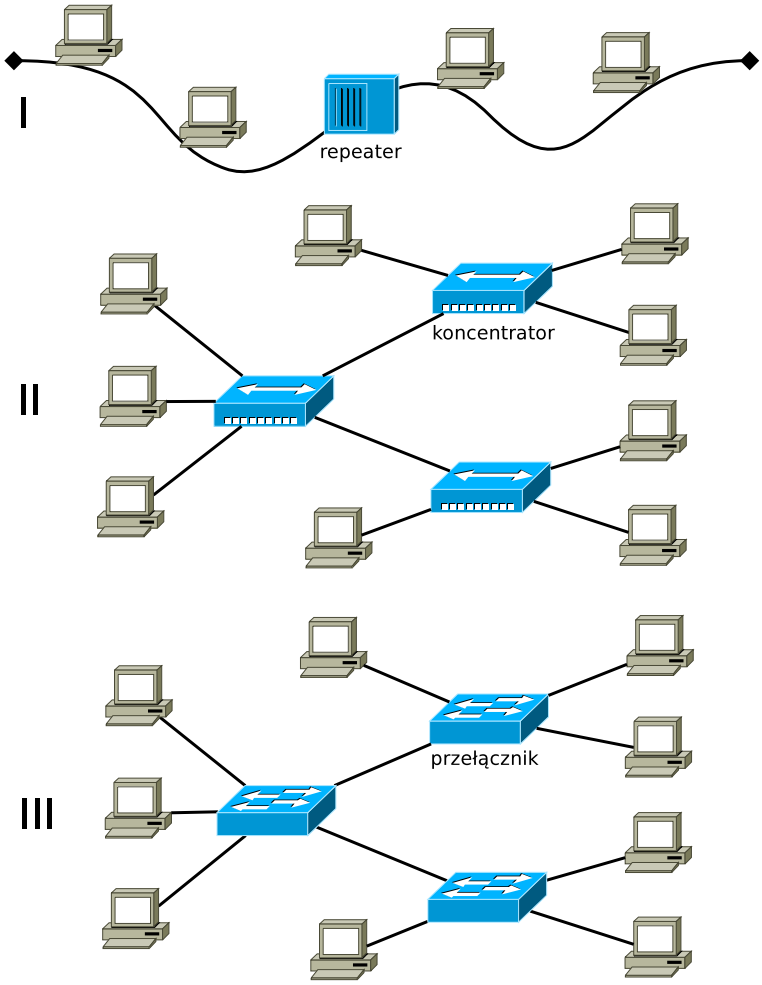


Rysunek 1.2. Karta sieciowa z okresu przejściowego, umożliwiająca podłączenie do kabla koncentrycznego lub skrętki

Ostatecznie kabel koncentryczny został zastąpiony tzw. skrętką, czyli kablem przeznaczonym do zastosowań telekomunikacyjnych, w którym znajdują się 4 pary skręconych wokół siebie przewodów (rys. 1.2). Pierwszym powszechnie przyjętym zastosowaniem skrętki w Ethernecie było 10BASE-T ("T" oznacza typ medium – skrętkę). 10BASE-T wymaga skrętki co najmniej 3 kategorii (im wyższa kategoria, tym bardziej rygorystyczne normy dotyczące własności elektrycznych, w określonym zakresie częstotliwości, musi spełniać kabel). Wykorzystuje się dwie z czterech par przewodów. W tym wariancie dwie pary przewodów pozostają niewykorzystane (wszystkie pary wykorzystuje dopiero Gigabit Ethernet). Stwarza to potencjalną możliwość użycia ich do dołączenia kolejnego hosta lub telefonu. Rozwiązania takie można spotkać w amatorskich instalacjach, jednak standard ich nie dopuszcza. Maksymalna długość kabla to 100 metrów.

Podstawowym urządzeniem sieciowym stał się koncentrator (ang. *hub*). Jest to wieloportowy repeater, czyli urządzenie warstwy fizycznej, przekazujące sygnał odebrany poprzez którykolwiek z portów, do wszystkich pozostałych portów. Umożliwił on budowanie sieci w topologii fizycznej gwiazdy

(rys. 1.3). Topologia logiczna pozostała natomiast identyczna jak w przypadku sieci wykorzystujących kabel koncentryczny.



Rysunek 1.3. Główne etapy ewolucji technologii Ethernet.

Przeznaczenie oddzielnych par przewodów do transmisji do i z karty sieciowej pozwoliło w przyszłości na ewolucję od modelu CSMA/CD do Ethernetu przełączanego, pracującego w trybie pełnego dupleksu. Przełomowym momentem w historii Ethernetu było wynalezienie w 1990 roku przełącznika (ang. *switch*), przypisywane firmie Kalpana (wchłoniętej później przez Cisco). Przełącznik Ethernet pracuje w warstwie łącza danych, tworząc oddzielne domeny kolizyjne dla poszczególnych portów. Jednocześnie, w sposób bezkolizyjny i z wykorzystaniem całej szerokości pasma, może

odbywać się wiele transmisji między urządzeniami dołączonymi do różnych interfejsów. Interfejs może jednocześnie wysyłać i odbierać dane.

Równolegle były i są nadal rozwijane technologie światłowodowe Ethernet. Dupleks uzyskuje się w nich poprzez użycie dwóch oddzielnych włókien światłowodowych do transmisji do i z karty sieciowej.

1.3. Współczesny Ethernet

Współcześnie, w typowych zastosowaniach, dominują technologie Fast Ethernet (100 Mb/s) oraz Gigabit Ethernet (1000 Mb/s). Koncentratory praktycznie całkowicie zostały wyparte przez przełączniki. O ile w przypadku technologii Fast Ethernet budowano początkowo sieci pracujące w półdupleksie (z użyciem koncentratorów), w sieciach Gigabit Ethernet zastosowanie znajdują wyłącznie przełączniki (chociaż standard dopuszcza także istnienie koncentratorów i tryb półdupleksu).

100BASE-T oznacza całą rodzinę technologii Fast Ethernet wykorzystujących skrętkę. Spośród nich stosowany jest jedynie wariant wykorzystujący dwie pary skrętki kategorii piątej lub wyższej – 100BASE-TX. Elementów technologii 100BASE-T4, wykorzystującej wszystkie pary, użyto później przy opracowywaniu 1000BASE-T. Dostępnych jest także kilka wariantów światłowodowych sieci Fast Ethernet: 100BASE-FX, 100BASE-SX, 100BASE-BX, 100BASE-LX10.

Gigabit Ethernet (IEEE 802.3-2008) był początkowo przeznaczony dla mocno obciążonych sieci szkieletowych. Coraz niższe ceny urządzeń sieciowych skutkują jednak stopniowym wypieraniem technologii Fast Ethernet przez Gigabit Ethernet również w segmentach sieci przeznaczonych dla urządzeń końcowych. Niemal wszystkie współcześnie produkowane komputery biurkowe i laptopy posiadają takie interfejsy.

Standard 1000BASE-TX, wymagający skrętki kategorii 6, został szybko wyparty z rynku przez 1000BASE-T (IEEE 802.3ab), akceptujący skrętkę kategorii 5. Inaczej niż w starszych technologiach, transmisja odbywa się poprzez wszystkie cztery pary przewodów, jednocześnie w obie strony. Standard 1000BASE-CX, zakładający użycie specjalnego kabla miedzianego ma teraz jedynie niszowe zastosowania. Do dyspozycji jest również kilka wariantów technologii światłowodowych: 1000BASE-LX, 1000BASE-SX, 1000BASE-LH, 1000BASE-ZX, a także 1000BASE-LX10 i 1000BASE-BX10.

W Ethernecie 10-gigabitowym (10 Gigabit Ethernet) początkowo zakładano wykorzystanie wyłącznie światłowodów lub specjalnego okablowania miedzianego. Jednak w 2006 roku opublikowano także standard 10GBASE-T (IEEE 802.3an-2006), umożliwiający użycie skrętki kategorii 6A, długości

maksymalnie 100 metrów, lub kategorii 6. dla mniejszych odległości. Standard nie przewiduje już półdupleksu i CSMA/CD.

Obecnie rozwijane są technologie światłowodowe 40 Gigabit Ethernet oraz 100 Gigabit Ethernet, chociaż wspomina się także o możliwości użycia kabli miedzianych. Niektóre rozwiązania są już dostępne komercyjnie. Pozwalają one na transmisję na odległość nawet do 40 km.

W celu ułatwienia zarządzania siecią, w której współistnieją urządzenia obsługujące różne generacje Ethernetu, opracowane zostały procedury autonegocjacji. Po raz pierwszy stało się to konieczne w celu zapewnienia zgodności technologii Fast Ethernet z 10BASE-T. Połączone ze sobą urządzenia powinny wynegocjować najwyższą akceptowalną dla obu szybkość i najlepszy tryb dupleksu (pełny dupleks jest preferowany przed półdupleksem). Niestety, w przypadku nowszych technologii Ethernet mogą występować niezgodności w sposobie implementacji autonegocjacji przez różnych producentów sprzętu. Mimo to, zaleca się korzystanie z autonegocjacji przynajmniej na portach dostępowych (tzn. przeznaczonych do podłączenia urządzeń końcowych).

Ewolucja technologii Ethernet nadal zmierza w kierunku coraz wyższych szybkości, jak również zwiększania odległości, na jaką może odbywać się transmisja. W związku z tym, Ethernet staje się nie tylko technologią sieci lokalnych, lecz również znajduje zastosowanie w sieciach metropolitalnych i rozległych. Przykładem jest coraz popularniejsza technologia Metro Ethernet.

Obok głównego nurtu rozwoju Ethernetu, wprowadzono także pewne dodatkowe usprawnienia. Wiele urządzeń sieciowych, np. bezprzewodowe punkty dostępowe, instaluje się w trudno dostępnych miejscach. Istotne utrudnienie stanowi wówczas konieczność doprowadzenia do nich zasilania. W technologiach 10BASE-T i 100BASE-TX można byłoby do tego celu wykorzystać wolne pary przewodów. Tego typu niestandardowe rozwiązania istniały zarówno w instalacjach amatorskich, jak również produktach dużych firm. Technologia dostarczania energii poprzez kabel Ethernet (ang. *Power over Ethernet*) doczekała się standaryzacji, najpierw jako IEEE 802.3af-2003, a następnie IEEE 802.3at-2009. Co ciekawe, do zasilania urządzeń wykorzystywane mogą być także przewody sygnałowe, co w przypadku technologii Gigabit Ethernet jest koniecznością.

Rozdział 2

Podstawowa konfiguracja przełącznika

2.1. Wstęp

Ogólne zasady konfiguracji przełącznika z systemem operacyjnym IOS są identyczne jak w przypadku routerów. Jedynie znak zgłoszenia:

```
Switch>
```

informuje z jakim urządzeniem pracujemy (przed nadaniem nazwy poleceniem `hostname`). W dalszej części rozdziału zakładamy, że czytelnikowi znany jest wiersz poleceń IOS w zakresie opisanym w [10] (rozdział 2). Przedstawione zostaną jedynie aspekty konfiguracji charakterystyczne dla funkcji przełączników, jak również kilka zagadnień nieomówionych w [10].

Przełącznik, w przeciwieństwie do routera, może pełnić swoje funkcje w sieci od razu po podłączeniu, z ustawieniami fabrycznymi. Jednak nawet jeżeli ustawienia fabryczne są wystarczające, warto włączyć przynajmniej podstawowe mechanizmy bezpieczeństwa.

Połączenie konsolowe z przełącznikiem Cisco zestawia się identycznie jak w przypadku routera. Przed rozpoczęciem wykonywania ćwiczeń laboratoryjnych zaproponowanych w kolejnych rozdziałach, zalecane jest przywrócenie ustawień fabrycznych. W tym celu, oprócz usunięcia pliku z konfiguracją startową, poleceniem:

```
erase startup-config
```

należy dodatkowo, jeżeli istnieje, skasować plik `vlan.dat`, zapisany w pamięci flash. Służy do tego celu polecenie:

```
delete flash:vlan.dat
```

Zawartość pamięci flash mozna przejrzeć przy pomocy polecenia:

```
show flash:
```

W pliku `vlan.dat` zapisywane są parametry konfiguracyjne dotyczące wirtualnych sieci LAN (VLAN). Należy zachować ostrożność, by usunąć tylko ten plik, a nie całą zawartość pamięci flash, wraz z obrazem systemu operacyjnego. Będzie wówczas konieczne przeprowadzenie procedury przywracania IOS, opisanej w Dodatku A. Po restarcie przełącznika poleceniem `reload`, bez zapisywania zmian w konfiguracji, będziemy dysponowali ustawieniami fabrycznymi. Następnie należy skonfigurować nazwę hosta i podstawowe mechanizmy zabezpieczające (hasła trybu uprzywilejowanego, konsoli i połączeń vty). Powinno to być czynnością rutynową.

2.2. Zdalny dostęp do przełącznika

Przełącznik jest urządzeniem 2. warstwy modelu OSI, w związku z czym nie potrzebuje do swojej pracy adresu IP. Ustawienia IP konfigurujemy jedynie gdy zamierzamy zdalnie łączyć się z urządzeniem, w celach administracyjnych. Adresu IP nie przypisujemy do interfejsu fizycznego, lecz wirtualnego w wybranej sieci VLAN. Pojęcie VLAN, czyli wirtualnej sieci lokalnej, zostanie wyjaśnione w dalszej części podręcznika; do tego momentu będziemy korzystać wyłącznie z VLAN 1 (co jednak jest niezalecane ze względów bezpieczeństwa, omówionych w dalszej części książki). Adres bramy domyślnej wprowadzamy w trybie konfiguracji globalnej. Sposób konfiguracji podstawowych ustawień ilsutruje poniższy listing:

```
configure terminal
 interface vlan 1
  ip address adres_IP maska_podsieci
  no shutdown
  exit
ip default-gateway adres_bramy
```

Połączenie wykorzystujące protokół telnet konfigurujemy tak samo, jak na routerach (poleceniem `line vty`). Jeżeli jednak zamierzamy zdalnie zarządzać przełącznikiem, protokół SSH oferuje znacznie większy poziom bezpieczeństwa, dzięki szyfrowaniu transmisji. Wymaga on dodatkowych czynności konfiguracyjnych i nie jest obsługiwany przez wszystkie wersje IOS. O obecności funkcji szyfrowania w IOS w wersji 12.2 lub nowszej informują znaki `k9` w nazwie pliku z obrazem.

W celu uruchomienia usługi serwera SSH na przełączniku (lub routerze) należy wykonać następującą sekwencję czynności [11]:

1. Urządzeniu należy nadać nazwę poleceniem `hostname` (o ile nie zostało to już zrobione wcześniej).
2. Należy skonfigurować nazwę domeny, poleceniem:

   ```
   ip domain-name nazwa_domeny
   ```

3. Należy wygenerować parę kluczy RSA, poleceniem:

   ```
   crypto key generate rsa
   ```

   wydanym w trybie konfiguracji globalnej. Jego niedostępność implikuje brak możliwości uruchomienia serwera SSH (należy zainstalować odpowiedni IOS). Ze względów bezpieczeństwa, zalecane jest wygenerowanie klucza o długości co najmniej 1024 bitów (urządzenie prosi o wprowadzenie tej wartości). W razie potrzeby, klucz można usunąć poleceniem:

```
crypto key zeroize rsa
```

co spowoduje również wyłączenie serwera SSH.

4. Musimy dysponować co najmniej jednym kontem użytkownika, który będzie mógł logować się poprzez SSH. Możemy stworzyć je lokalnie, poleceniem:

   ```
   username login privilege 15 secret hasło
   ```

   "15" oznacza maksymalny możliwy poziom uprawnień. Alternatywą dla lokalnych kont jest wykorzystanie zewnętrznego serwera do uwierzytelniania użytkowników (Radius lub TACACS+).
5. Ostatnim krokiem jest skonfigurowanie połączeń vty tak, aby korzystały z SSH:

   ```
   line vty 0 4
     login local
     transport input ssh
   ```

   W miejsce "4" można wpisać maksymalną możliwą liczbę dla danego urządzenia. `login local` uruchomi korzystanie z kont założonych uprzednio poleceniem `username`. Polecenie `transport input ssh` wymusi korzystanie z protokołu SSH (w konfiguracji domyślnej wpisane jest `transport input telnet`).
   Dalsze polecenia są opcjonalne. Polecenie:

   ```
   ip ssh
   ```

z odpowiednimi argumentami umożliwia skonfigurowanie także innych ustawień SSH, np. wersji, dopuszczalnej liczby prób logowania itp. Informacji o stanie serwera SSH dostarczają polecenia:

```
show ip ssh
```

oraz

```
show ssh
```

2.3. Konfiguracja interfejsów

Bardzo wiele ustawień konfiguracyjnych przełącznika dotyczy sposobu działania jego interfejsów fizycznych [12]. Interfejsy można konfigurować pojedynczo, np.:

```
interface fastethernet0/1
 shutdown
```

W tym miejscu warto zauważyć, że numeracja interfejsów zaczyna się od 1, a nie od 0, jak w przypadku routerów. Pracochłonnego konfigurowania tych samych ustawień dla wielu interfejsów można uniknąć korzystając z polecenia `interface range`. Przykładowo:

```
interface range fastethernet0/1 - 5
 shutdown
```

lub (w zależności od IOS):

```
interface range fastEthernet 0/1 - fastEthernet 0/5
 shutdown
```

spowoduje wyłączenie pięciu interfejsów.

Podstawowe ustawienia konfiguracyjne interfejsów przedstawione są w tabeli 2.1. Dopuszczalne wartości parametrów mogą różnić się w zależności od IOS i konfiguracji sprzętowej. Domyślnie (inaczej niż w routerach) interfejsy fizyczne są włączone.

Tabela 2.1. Podstawowe ustawienia konfiguracyjne interfejsów przełącznika

Funkcja	Polecenie	Dopuszczalne parametry	Ustawienie domyślne
szybkość	speed	10, 100, 1000, auto, nonegotiate	auto
dupleks	duplex	auto, full, half	auto
wykrywanie przeplotu kabla	mdix	auto	auto

Standardowo, gdy do interfejsu przełącznika podłączany jest interfejs sieciowy innego urządzenia, negocjowany jest najszybszy tryb pracy (tzn. szybkość i ustawienie dupleksu) obsługiwany przez oba urządzenia. W związku z tym, w typowych sytuacjach nie ma potrzeby zmieniania domyślnych ustawień.

W zależności od rodzaju łączonych urządzeń, powinno się używać kabla Ethernet typu prostego (ang. *straight-through*) lub z przeplotem (ang. *crossover*). Domyślnie włączona funkcja automatycznego wykrywania przeplotu (auto-MDIX) zwalnia z tego obowiązku. Użycie nieprawidłowego typu kabla zostanie automatycznie skorygowane. Funkcja ta wymaga do popraw-

nego działania domyślnych wartości szybkości i dupleksu, przynajmniej na jednym z interfejsów.

2.4. Tablica adresów MAC

Zarządzanie informacją o adresach MAC urządzeń podłączonych do poszczególnych interfejsów przełącznika należy do jego podstawowych funkcji. Dzięki tablicy adresów MAC, zapisywanej w pamięci CAM (ang. *Content Addressable Memory*), możliwe jest przesyłanie ramek tylko do odpowiedniego portu docelowego (lub zaniechanie transmisji, jeżeli okaże się, że host źródłowy i docelowy dołączone są do tego samego interfejsu). Tablica jest wypełniana dynamicznie, na podstawie adresów źródłowych odczytywanych z ramek przychodzących do przełącznika. Nieużywane wpisy są po pewnym czasie (domyślnie po 300 sekundach) usuwane, by zapewnić aktualność informacji. W tablicy adresów MAC mogą występować także wpisy statyczne, wprowadzone na stałe przez administratora (nieulegające przedawnieniu).

Zawartość tablicy adresów MAC można przejrzeć przy pomocy polecenia [13]:

```
show mac address-table
```

lub

```
show mac-address-table
```

w zależności od IOS (również w kolejnych poleceniach może być stosowana pisownia `mac address-table` lub `mac-address-table`). Wynik otrzymujemy w postaci:

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0c26.87b5    DYNAMIC     Fa0/4
   1    0002.1669.aa9c    DYNAMIC     Fa0/1
   1    0009.7ccb.d965    STATIC      Fa0/2
   1    00d0.58cd.9090    DYNAMIC     Fa0/3
```

Wynik można zawęzić do wpisów statycznych lub dynamicznych przy pomocy dodatkowych parametrów `static` lub `dynamic`, odpowiednio.

Dynamiczne wpisy w tablicy adresów MAC można usuwać poleceniem:

```
clear mac address-table dynamic
```

Można usunąć wszystkie lub tylko wybrane, podając dodatkowe opcje.

Wpis statyczny do tablicy można wprowadzić w trybie konfiguracji globalnej, poleceniem:

```
mac address-table static adresMAC vlan VLAN-ID
                                    interface interfejs
```

Statyczna konfiguracja adresów MAC może zwiększyć poziom bezpieczeństwa, jednak jest kłopotliwa i w związku z tym rzadko stosowana. Warto natomiast uruchomić mechanizm bezpieczeństwa portów, opisany w rozdziale 7.

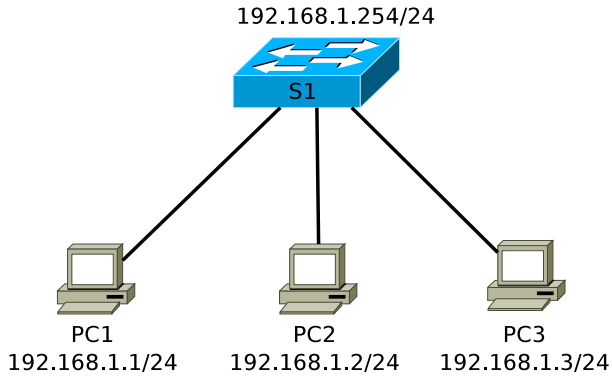
Czas, po którym wpisy dynamiczne w tablicy MAC ulegają przedawnieniu, definiuje się (w sekundach) poleceniem:

```
mac address-table aging-time
```

Jeżeli w sieci znajdują się hosty, które rzadko wysyłają dane, wpisy w tablicy MAC ulegają przedawnieniu i skutkuje to koniecznością wysyłania przeznaczonych dla nich ramek do wszystkich portów. Można wówczas rozważyć zwiększenie wartości tego parametru (domyślnie jest to 300 sekund).

2.5. Zadania

2.5.1. Zadanie 1



Rysunek 2.1. Schemat topologii logicznej sieci

1. Połącz sieć zgodnie ze schematem (rys. 2.1).

2. Nawiąż połączenie konsolowe z przełącznikiem i przywróć jego ustawienia fabryczne.
3. Skonfiguruj adresy IP komputerów PC1, PC2 i PC3. Upewnij się, że jest możliwa komunikacja między nimi, stosując polecenie `ping` (w razie potrzeby skoryguj ustawienia firewalla na PC).
4. Nadaj przełącznikowi nazwę. Zabezpiecz port konsolowy i dostęp do trybu uprzywilejowanego przełącznika. Włącz szyfrowanie haseł (poleceniem `service password encryption`, tak samo jak w przypadku routerów). Skonfiguruj adres IP przełącznika. Skonfiguruj i przetestuj zdalny dostęp do przełącznika poprzez telnet.
5. Zastąp telnet protokołem SSH (o ile jest to możliwe w przypadku posiadanej wersji IOS). Przetestuj połączenie SSH między jednym z komputerów a przełącznikiem (np. korzystając z programu PuTTY).
6. Sprawdź, czy dostępne są polecenia konfiguracyjne interfejsów, przedstawione w tabeli 2.1. Jakie są dopuszczalne opcje?
7. Przejrzyj zawartość tablicy adresów MAC przełącznika.
8. Skasuj zawartość tablicy adresów MAC i zaobserwuj ponowne, automatyczne jej wypełnianie.
9. Uruchom program Wireshark[1] lub inne narzędzie umożliwiające śledzenie pakietów w sieci (sniffer) na komputerze PC3. Wyczyść tablicę adresów MAC, wygeneruj ruch między PC1 i PC2 i postaraj się zaobserwować ramki docierające do PC3 ale zaadresowane do PC1 lub PC2 (przed ponownym, automatycznym wypełnieniem tablicy adresów MAC).
10. Wprowadź do tablicy adresów MAC adres jednego z komputerów jako wpis statyczny. Przejrzyj jej zawartość.

2.5.2. Rozwiązanie zadania 1

Listing 2.1. Istotne fragmenty pliku konfiguracyjnego przełącznika S1

```
1 [...]
  service password-encryption
3 !
  hostname S1
5 !
  enable secret 5 $1$qYl4$yPsrSeCcy8r0oJjEuEsvT.
7 !
  username admin privilege 15 secret 5 $1$5ATv$aGx [...]
9 no aaa new-model
  [...]
11 !
  ip domain-name umcs.pl
13 !
```

[1] `http://www.wireshark.org/`

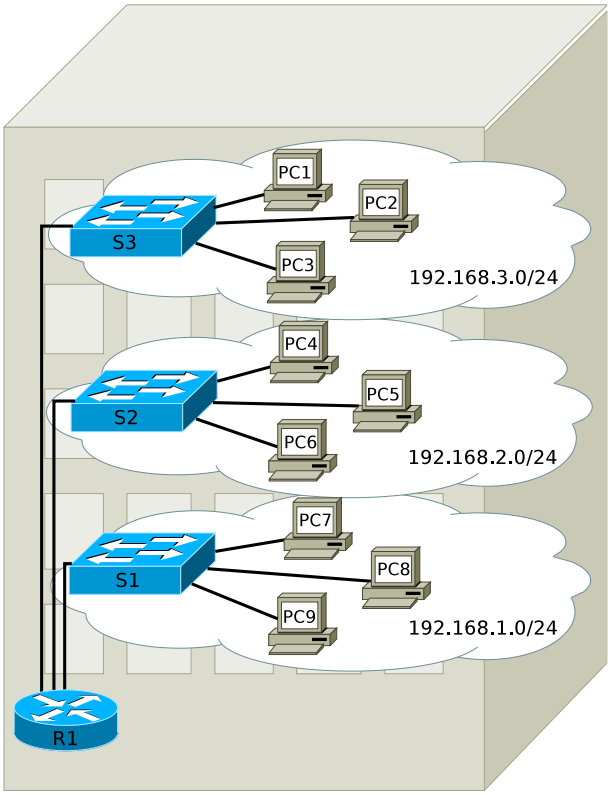
```
[...]
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
[...]
!
interface Vlan1
 ip address 192.168.1.254 255.255.255.0
 no ip route-cache
!
[...]
!
!
line con 0
 password 7 05080F1C2243
 login
line vty 0 4
 password 7 1511021F0725
 login local
 transport input ssh
line vty 5 15
 password 7 1511021F0725
 login local
 transport input ssh
!
mac-address-table static a4ba.dbc6.7054
                         vlan 1 interface FastEthernet0/9
end
```

Rozdział 3

Wirtualne sieci LAN (VLAN)

3.1. Wstęp

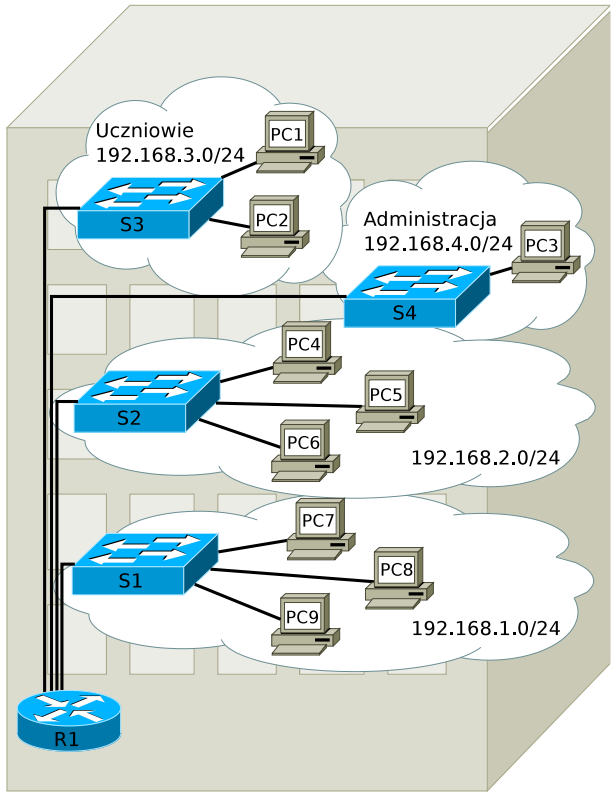
Rys. 3.1 przedstawia schemat topologii sieci LAN, zbudowanej w tradycyjny sposób. W sieci tej poszczególne hosty dołączane są do znajdującego się najbliżej przełącznika, co skutkuje koniecznością przydzielenia im adresu IP z sieci, do której należy interfejs routera połączony z przełącznikiem. Hosty, które znajdują się w danej lokalizacji fizycznej (np. na tym samym piętrze budynku) jednocześnie należą do tej samej domeny rozgłoszeniowej i sieci logicznej. Przeniesienie hosta do innej części budynku i podłączenie do innego przełącznika skutkuje koniecznością zmiany ustawień IP.



Rysunek 3.1. Sieć lokalna zbudowana w tradycyjny sposób

Załóżmy, że na najwyższym piętrze budynku znajduje się szkoła. Do przełącznika S3 dołączone są komputery przeznaczone dla uczniów oraz komputery pracowników administracji szkoły. Umieszczenie tych dwóch grup użytkowników w jednej domenie rozgłoszeniowej znacznie obniża poziom bezpieczeństwa – możliwości filtrowania ruchu między komputerami uczniów i administracji są bardzo ograniczone. Z drugiej strony, utrudniona jest także mobilność użytkowników. Przemieszczenie pracownika administracji

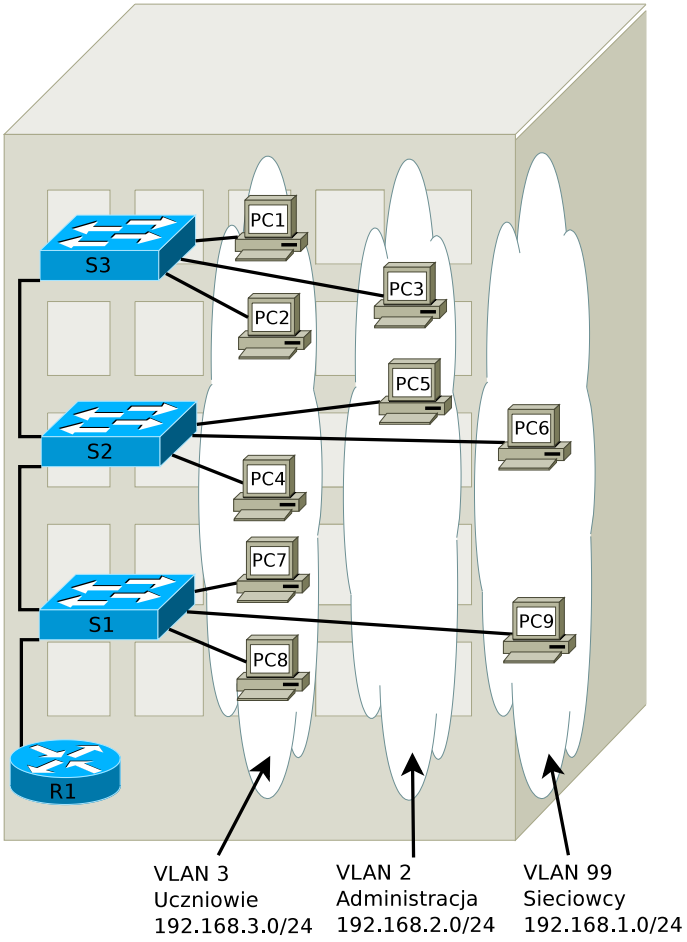
do innej części budynku (i podłączenie jego komputera do innego przełącznika) może utrudnić mu dostęp do zasobów udostępnianych w sieci 192.168.3.0/24.



Rysunek 3.2. Zmodyfikowana sieć lokalna

Rys. 3.2 przedstawia przykładowe rozwiązanie powyższego problemu. Stworzono dodatkowy segment LAN, w celu odseparowania uczniów i administracji poprzez urządzenie 3 warstwy (router). Rozwiązanie to jest jednak kłopotliwe, kosztowne i nieelastyczne. Wymaga zakupu dodatkowego przełącznika, poprowadzenia okablowania, a także potrzebny jest kolejny interfejs fizyczny routera. Nadal nierozwiązany pozostaje problem mobilności użytkowników.

Kolejny rysunek (3.3) przedstawia rekomendowane rozwiązanie, z wykorzystaniem nowego mechanizmu – wirtualnych sieci lokalnych (ang. *Virtual Local Area Network*, VLAN). Tak jak poprzednio, chmury oznaczają odrębne domeny rozgłoszeniowe, które w tym przypadku są równoważne wirtualnym sieciom lokalnym. Komputery PC1 i PC3 należą teraz do odrębnych domen rozgłoszeniowych, mimo że są dołączone do tego samego



Rysunek 3.3. Rozwiązanie z wykorzystaniem VLAN

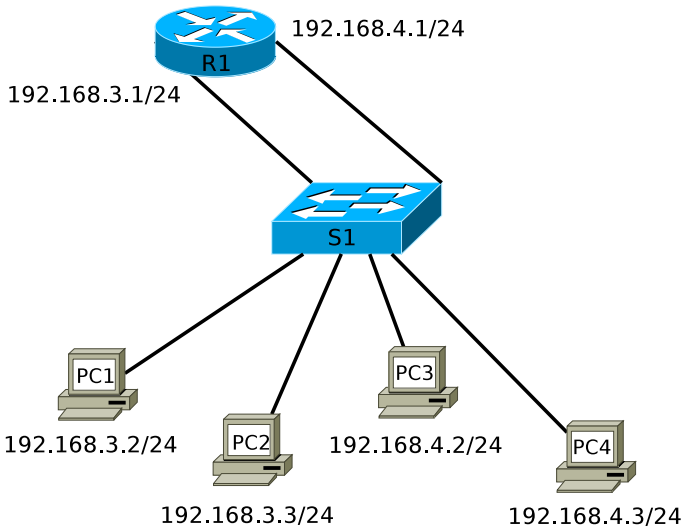
przełącznika. Jakakolwiek komunikacja między nimi możliwa jest wyłącznie za pośrednictwem urządzenia 3 warstwy (routera R1). W związku z tym, każda sieć VLAN powinna być odrębną siecią IP (lub podsiecią). Komputer PC3 mógłby zostać podłączony do przełącznika S2 lub S1, nadal pozostając w tej samej domenie rozgłoszeniowej, a więc także sieci logicznej, przeznaczonej dla administracji. Fizyczne przemieszczenie hosta nie wymaga zmiany jego adresu IP. Należy zwrócić uwagę także na sposób połączenia urządzeń pośrednich. Wykorzystany jest tylko jeden interfejs fizyczny routera. Oprócz sieci VLAN przeznaczonych dla uczniów i administracji, zaplanowano jeszcze kolejną (VLAN 99, Sieciowcy), przeznaczoną do zarządzania siecią przez administratorów.

Podsumowując, wirtualne sieci lokalne (VLAN) są mechanizmem umoż-

liwiającym tworzenie domen rozgłoszeniowych na pojedynczym przełączniku lub wielu połączonych przełącznikach. To z kolei pozwala na logiczne grupowanie użytkowników, którzy nie muszą znajdować się w tym samym miejscu.

3.2. Działanie sieci VLAN

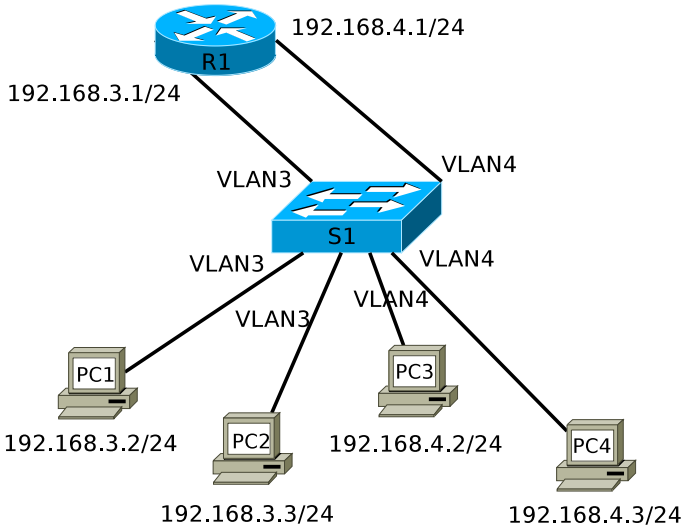
Rys. 3.4 przedstawia dwie sieci logiczne (192.168.3.0/24 i 192.168.4.0/24), dołączone do jednego przełącznika. Ze względu na sposób przypisania adresów IP, komputery PC1 i PC3 będą mogły komunikować się ze sobą tylko za pośrednictwem routera (pod warunkiem odpowiedniego jego skonfigurowania oraz poprawnego określenia adresów bram domyślnych).



Rysunek 3.4. Próba separacji dwóch sieci logicznych

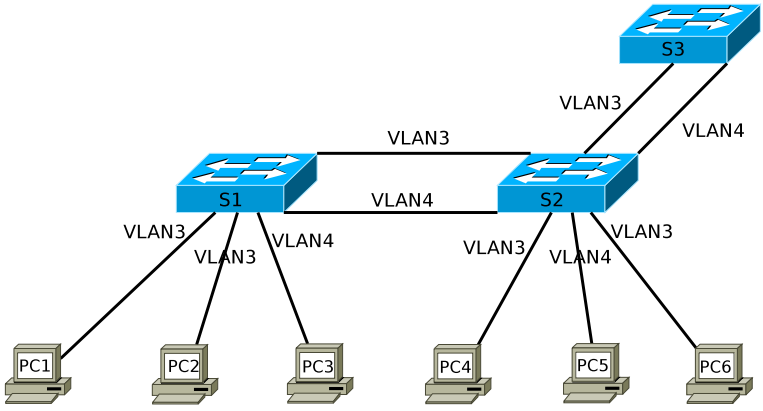
Separacja między dwiema sieciami nie jest jednak pełna. Wszystkie komputery należą do tej samej domeny rozgłoszeniowej i ramki rozgłoszeniowe (np. zapytania ARP) są rozsyłane poprzez wszystkie porty przełącznika. Podobnie przełącznik postępuje z ramkami adresowanymi do nieznanych hostów. Ponadto, użytkownik może łatwo przenieść swój komputer do innej sieci, modyfikując jego adres IP.

W sieci z rys. 3.5 na przełączniku stworzono dwie sieci VLAN (3 i 4) i odpowiednio przypisano do nich interfejsy. W tym momencie dysponujemy dwiema domenami rozgłoszeniowymi, całkowicie odseparowanymi wewnątrz przełącznika. Komunikację między nimi (ang. *inter-VLAN routing*) może zapewnić tylko router (lub przełącznik trzeciej warstwy). Poprzednie



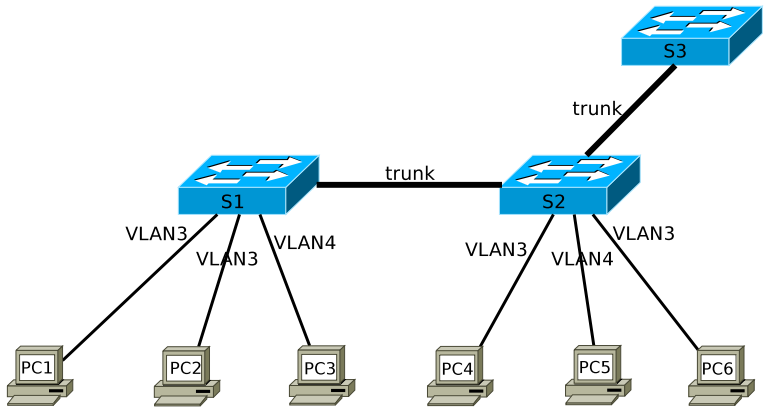
Rysunek 3.5. Separacja sieci przy pomocy VLAN

rozwiązanie, przedstawione na rys. 3.4 jest nierekomendowane i niezgodne z dobrymi praktykami.



Rysunek 3.6. Sieci VLAN na kilku przełącznikach

Kolejnym problemem jest stworzenie sieci VLAN obejmującej swoim zasięgiem więcej niż 1 przełącznik. Przykład jest przedstawiony na rys. 3.6. Komputery należące do tej samej sieci VLAN mogą komunikować się ze sobą również wtedy, gdy są dołączone do różnych przełączników. Należy jednak zwrócić uwagę na fakt, że przedstawione rozwiązanie jest słabo skalowalne. Każda sieć VLAN wymaga oddzielnego połączenia między przełącznikami. Pomimo niewielkiej liczby liczby sieci VLAN, przełącznik S2 stracił aż 4



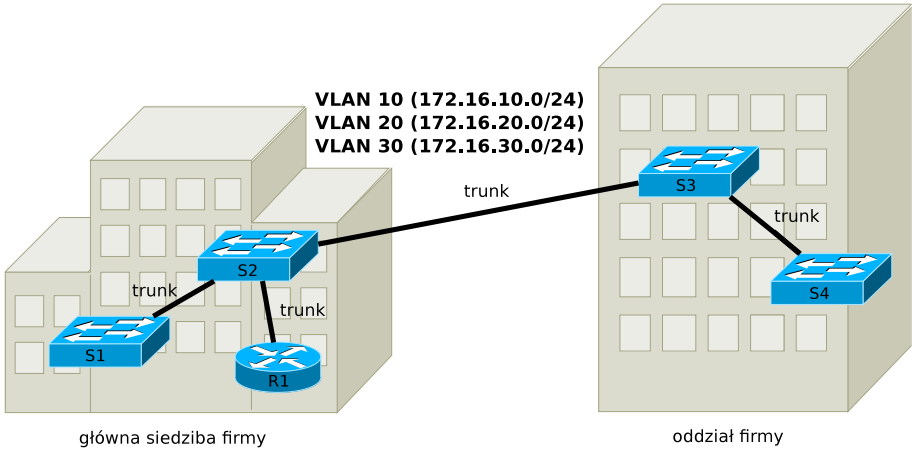
Rysunek 3.7. Połączenie trunk między przełącznikami

interfejsy. Ten sam problem dotyczy połączenia między routerem a przełącznikiem na rys. 3.5.

W sieci z rys. 3.7 skonfigurowano połączenia typu trunk między przełącznikami. Trunk jest połączeniem wspólnym dla wielu sieci VLAN. Transmitowane ramki są oznaczane identyfikatorem sieci VLAN, do której należą. Przełącznik wysyłający ramkę poprzez połączenie trunk jest odpowiedzialny za jej oznakowanie (ang. *VLAN tagging*), natomiast odbierający usuwa znakowanie, doprowadzając ramkę do pierwotnej postaci, i przekazuje do odpowiedniego portu. Powszechnie przyjętym standardem połączeń trunk jest obecnie IEEE 802.1Q (w ustawieniach konfiguracyjnych przełączników określany jako `dot1q`). W przypadku niektórych, zwłaszcza starszych urządzeń Cisco, można spotkać także protokół ISL [14]. Proces znakowania ramek jest niewidoczny dla hostów, a sieci VLAN nadal pozostają odseparowane (pod warunkiem zabezpieczenia przed zestawieniem połączenia trunk między przełącznikiem a urządzeniem użytkownika końcowego). Połączenie trunk można skonfigurować także między przełącznikiem a routerem.

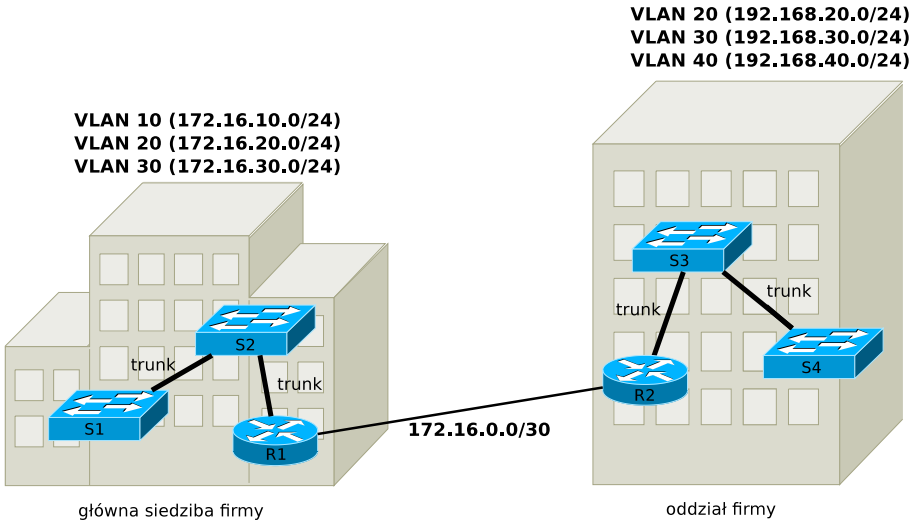
Takie rozwiązanie spełnia warunek skalowalności, umożliwiając stworzenie wielu sieci VLAN przy pojedynczych połączeniach między przełącznikami. Jest natomiast wskazane zapewnienie przepustowości połączeń trunk adekwatnej do ich obciążenia. Zasadniczo, połączenia trunk powinny mieć przepustowość co najmniej 100Mb/s (Fast Ethernet), chociaż istnieją także urządzenia z wolniejszymi interfejsami, umożliwiającymi włączenie tej funkcji. Jeżeli przełącznik jest wyposażony w interfejsy o różnej przepustowości, np. Fast Ethernet i Gigabit Ethernet, do zestawienia połączeń trunk należy użyć szybszych.

W dużych sieciach korporacyjnych należy rozważyć kwestię zasięgu sieci VLAN. Pierwszy przykład jest przedstawiony na rys. 3.8. Dzięki połącze-

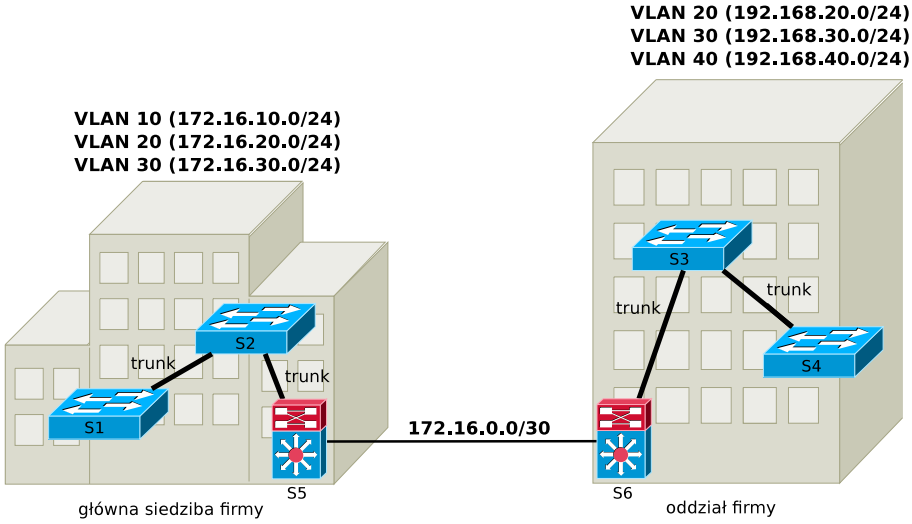


Rysunek 3.8. VLAN typu *end-to-end*

niom typu trunk, sieci VLAN obejmują swoim zasięgiem główną siedzibę firmy oraz jej oddział. Ten scenariusz, określany mianem sieci VLAN typu *end-to-end*, ma zastosowanie w sytuacji, gdy członkowie poszczególnych grup roboczych, dla których stworzono sieci VLAN, pracują w różnych miejscach, ale korzystają głównie z zasobów swojej grupy roboczej (np. serwera aplikacji lub współdzielonych plików). Mówi się tu o charakterystyce przepływu 80/20, gdzie około 80% ruchu sieciowego odbywa się wewnątrz sieci VLAN. Ponieważ wszystkie sieci VLAN są dostępne we wszystkich lokalizacjach, łatwe jest przemieszczanie użytkowników wraz z ich komputerami. Jednak model 80/20 rzadko obecnie znajduje zastosowanie, ponieważ pracownicy zwykle intensywnie korzystają również z zasobów spoza swojej grupy roboczej (w tym z Internetu), co skutkuje koniecznością transmisji za pośrednictwem urządzeń warstwy trzeciej (w naszym przypadku – routera R1). Charakterystyka przepływu może być zbliżona do 20/80, gdzie zdecydowana większość ruchu wykracza poza VLAN. W takim przypadku tworzenie rozbudowanych sieci VLAN traci sens. Co więcej, rozbudowana struktura sieci VLAN z połączeniami trunk jest trudna do zarządzania. Ponadto, chociaż przełączanie w drugiej warstwie modelu OSI odbywa się szybciej niż w trzeciej, obecnie różnica nie jest na tyle znacząca, by było celowe unikanie przełączania w trzeciej warstwie za wszelką cenę. Rozwiązanie sugerowane w takiej sytuacji przedstawia rys. 3.9. Mówimy tu o lokalnych sieciach VLAN lub sieciach VLAN typu geograficznego. Zasięg sieci VLAN jest ograniczony do niewielkiego obszaru, np. jednego budynku. Podział na sieci VLAN niekoniecznie dokładnie odpowiada wówczas podziałowi pracowników na grupy robocze. W przykładzie z rys. 3.9, sieci VLAN w siedzibie firmy i jej oddziale działają zupełnie niezależnie. W przedstawionej tu sy-



Rysunek 3.9. VLAN typu geograficznego



Rysunek 3.10. VLAN typu geograficznego z przełącznikami 3 warstwy

tuacji, w siedzibie firmy i w oddziale występuje VLAN 20. Mimo takiego samego identyfikatora, są to dwie oddzielne sieci VLAN (zbieżność identyfikatorów jest bez znaczenia). Komunikacja miedzy dwiema lokalizacjami odbywa się poprzez sieć 172.16.0.0/30 i routery R1 i R2. Zamiast routerów można zastosować przełączniki 3 warstwy, jak na rys. 3.10 (S5 i S6).

3.3. Konfiguracja sieci VLAN

3.3.1. Tworzenie i modyfikacja sieci VLAN

W domyślnej konfiguracji wszystkie interfejsy fizyczne przełącznika są przypisane do nieusuwalnej sieci VLAN 1 (tzw. domyślny VLAN, ang. *default VLAN*). Inne sieci VLAN można tworzyć i modyfikować poleceniem:

```
vlan vlan-id
```

wydanym w trybie konfiguracji globalnej. Uruchamia ono tryb edycji ustawień sieci VLAN o podanym numerze (*vlan-id*).

W starszych urządzeniach, w trybie użytkownika uprzywilejowanego, dostępne było polecenie:

```
vlan database
```

uruchamiające tryb edycji konfiguracji sieci VLAN. Ustawienia wydawane w trybie *vlan database* były uruchamiane przy wychodzeniu z tego trybu, a nie tak jak jest to w przypadku innych konfiguracji, od razu po wydaniu komendy. Ten sposób konfigurowania sieci VLAN jest obecnie uważany za przestarzały i w dalszej części ograniczymy się do pierwszej metody.

Ustawienia konfiguracyjne dotyczące VLAN zapisywane są w pamięci flash, w pliku `vlan.dat`. Wspomniano o nim już, przedstawiając sposób przywracania fabrycznych ustawień przełącznika.

Sieć VLAN można stworzyć lub zmodyfikować korzystając z poleceń [15]:

```
vlan vlan-id
 name nazwa
 end
```

Sieci VLAN ze zwykłego zakresu (ang. *normal-range VLANs*) mają identyfikatory (VLAN ID) od 1 do 1005, przy czym identyfikatory od 1002 do 1005 są zarezerwowane dla TokenRing i FDDI. Identyfikatory od 1006 do 4094 należą do rozszerzonego zakresu (ang. *extended-range VLANs*). W kolejnych przykładach wykorzystywany będzie tylko zwykły zakres. W poleceniu `vlan`, podanie niewykorzystywanego dotychczas identyfikatora skutkuje utworzeniem nowej sieci VLAN, w przeciwnym razie można modyfikować ustawienia istniejącej sieci VLAN. Polecenie `name` jest opcjonalne (podobnie jak pozostałe polecenia dostępne w trybie konfiguracji sieci VLAN) i służy do nadania nazwy informującej administratora o przeznaczeniu sieci VLAN. Nie ma natomiast wpływu na jej funkcjonowanie. Domyślna nazwa ma postać *VLANxxxx*, gdzie *xxxx* jest numerem VLAN ID. Sieci VLAN można też nadać adres IP, w sposób już przedstawiony w podrozdziale 2.2, dla VLAN

1. Będzie można łączyć się korzystając z niego z przełącznikiem poprzez wszystkie jego interfejsy fizyczne, należące do tej sieci VLAN. Ze opcji tej należy korzystać tylko wtedy, gdy rzeczywiście potrzebny jest zdalny dostęp do przełącznika. Polecenie

```
no vlan vlan-id
```

usuwa sieć VLAN o podanym identyfikatorze.

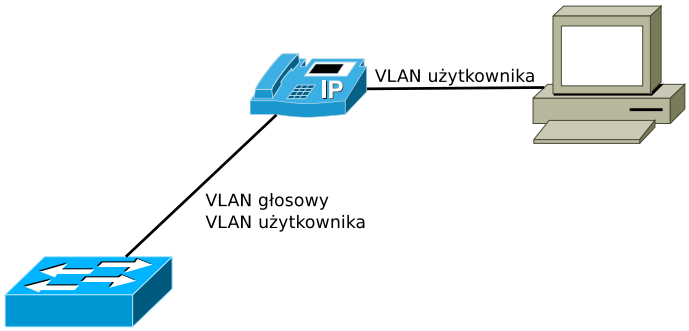
3.3.2. Przypisywanie interfejsów do sieci VLAN

Kolejnym zadaniem jest przypisanie portów przełącznika do poszczególnych sieci VLAN. Domyślnie wszystkie interfejsy fizyczne należą do sieci VLAN 1. Interfejs może zostać skonfigurowany jako statyczny port dostępowy (ang. *static-access*), tzn. przeznaczony do podłączenia urządzeń końcowych. Należy on wówczas do jednej sieci VLAN, zgodnie z zapisem w pliku konfiguracyjnym przełącznika, wprowadzonym przez administratora. Jest to najczęściej stosowane rozwiązanie. Jeżeli do interfejsu zostanie dołączone więcej niż jedno urządzenie (poprzez kolejny przełącznik lub koncentrator), wszystkie znajdą się w tej samej sieci VLAN.

Port dynamicznego dostępu (ang. *dynamic-access*) również należy do jednej sieci VLAN. Przypisanie jest realizowane (inaczej niż w przypadku statycznych portów dostępowych) na podstawie informacji uzyskanych z serwera VMPS (ang. *VLAN Management Policy Server*). Przypisanie portu do sieci VLAN odbywa się na podstawie adresu MAC dołączonego hosta (który można łatwo sfałszować) lub zgodnie z procedurami uwierzytelniania 802.1x. Mechanizm ten zwalnia administratora z obowiązku zmiany przypisań portów do sieci VLAN w razie przemieszczania komputerów (jak w przypadku statycznych portów dostępowych). Wymaga jednak odpowiedniego sprzętu, oprogramowania i dodatkowych czynności na etapie początkowej konfiguracji. To rozwiązanie jest zalecane dla dużych sieci.

Port może też zostać przeznaczony do obsługi specjalnej sieci VLAN, służącej do transmisji głosu (VoIP) [16]. Obsługuje wówczas dwie sieci VLAN – "głosową" (ang. *voice* VLAN), umożliwiającą dołączenie telefonu IP, oraz kolejną – zwykłą, do podłączenia komputera. Schemat połączeń jest przedstawiony na rys. 3.11. Dzięki takiej konfiguracji, VoIP jest obsługiwany przez dedykowaną sieć VLAN, a do stanowiska użytkownika (z komputerem i telefonem IP) doprowadzony jest tylko jeden kabel. Telefon posiada dwa interfejsy sieciowe i odpowiednie układy rozdzielające ruch.

Interfejs typu trunk (w odróżnieniu od portu dostępowego) domyślnie obsługuje wszystkie sieci VLAN. Można też samodzielnie określić listę sieci VLAN, z których ruch będzie przesyłany.



Rysunek 3.11. Wykorzystanie sieci VLAN dla VoIP

Aby statycznie przypisać interfejs do sieci VLAN o identyfikatorze *vlan-id*, należy w trybie konfiguracji globalnej wydać następujące polecenia:

```
interface nazwa-interfejsu
 switchport mode access
 switchport access vlan vlan-id
 end
```

Aby jednocześnie w identyczny sposób skonfigurować wiele interfejsów, można użyć polecenia `interface range`. Polecenie `switchport mode access` konfiguruje interfejs jako statyczny port dostępowy. Uniemożliwia to zestawienie poprzez niego połączenia typu trunk, podnosząc poziom bezpieczeństwa. W większości współczesnych systemów IOS, próba przypisania interfejsu do nieistniejącej sieci VLAN spowoduje automatyczne jej stworzenie. Problem może wystąpić w razie usunięcia sieci VLAN, ponieważ skutkuje to wyłączeniem przypisanych do niej interfejsów, aż do czasu gdy zostanie odtworzona, lub interfejsy zostaną przypisane do innej sieci VLAN.

Podstawowym poleceniem do weryfikacji konfiguracji VLAN jest

```
show vlan
```

Fragment generowanej informacji przedstawia poniższy listing.

Listing 3.1. Fragment informacji wyświetlanej w wyniku działania polecenia show vlan

```
1 VLAN Name                             Status    Ports
  ---- -------------------------------- --------- -------------------------------
3 1    default                          active    Fa0/12, Fa0/13, Fa0/14,
                                                  Fa0/16, Fa0/17, Fa0/18,
5                                                 Fa0/20, Fa0/21, Fa0/22,
                                                  Fa0/24, Gig1/1, Gig1/2
7 10   ksiegowosc                       active    Fa0/1, Fa0/2, Fa0/3,
```

```
   20   kadry                 active    Fa0/5, Fa0/6, Fa0/7
 9 25   dyrekcja              active    Fa0/8, Fa0/9, Fa0/10,
   70   VLAN0070              active
11 1002 fddi-default          act/unsup
   1003 token-ring-default    act/unsup
13 1004 fddinet-default       act/unsup
   1005 trnet-default         act/unsup
```

Uzyskujemy tu informacje o sieciach VLAN dostępnych na przełączniku, ich nazwach oraz o przypisaniu interfejsów. Dodatkowe, opcjonalne parametry umożliwiają uzyskanie bardziej szczegółowych informacji. Ponadto, dostępne jest polecenie:

```
show interfaces vlan vlan-id
```

wyświetlające m.in. adres IP nadany sieci VLAN.

3.3.3. Konfiguracja połączeń trunk

Połączenie między dwoma przełącznikami może być zwykłym połączeniem dostępowym lub połączeniem typu trunk. Zależy to od wyniku negocjacji przy wykorzystaniu protokołu DTP (ang. *Dynamic Trunking Protocol*) [15], który z kolei zależy od sposobu skonfigurowania sąsiednich interfejsów. Możliwe są następujące opcje (dla przełącznika 2960):

— `switchport mode access` – port może pracować wyłącznie jako dostępowy,
— `switchport mode trunk` – port zawsze pracuje jako trunk,
— `switchport mode dynamic auto` – ustawienie domyślne, port może pracować jako trunk, jeżeli sąsiedni interfejs jest skonfigurowany jako `trunk` lub `desirable`,
— `switchport mode dynamic desirable` – port stara się wymusić połączenie trunk, gdy sąsiedni interfejs jest skonfigurowany jako `trunk`, `desirable` lub `auto`,
— `switchport nonegotiate` – powoduje, że interfejs nie generuje komunikatów DTP, a tryb portu dostępowego lub trunk musi być ręcznie skonfigurowany na obu interfejsach.

Niektóre kombinacje powyższych ustawień mogą prowadzić do nieprzewidywalnych wyników. W typowych sytuacjach można poprzestać na skonfigurowaniu interfejsów przełącznika jako dostępowe (`switchport mode access`), przeznaczone do podłączenia hostów, lub trunk (`switchport mode trunk`).

Typ enkapsulacji połączenia trunk (802.1q lub ISL) można skonfigurować poleceniem:

```
switchport trunk encapsulation dot1q|isl
```

Jeżeli przełącznik obsługuje tylko jeden typ enkapsulacji (obecnie zwykle 802.1q), polecenie może być niedostępne.

Połączenie trunk domyślnie obsługuje wszystkie sieci VLAN. Można jednak listę obsługiwanych sieci stworzyć samodzielnie, przy pomocy polecenia:

```
switchport trunk allowed vlan lista-sieci-vlan
```

lub

```
switchport trunk allowed vlan add|all|except|remove
                                                lista-sieci-vlan
```

w ustawieniach interfejsu skonfigurowanego jako trunk. *lista-sieci-vlan* może zawierać pojedyncze identyfikatory VLAN ID rozdzielane przecinkami lub zakresy zdefiniowane poprzez podanie pierwszego i ostatniego, rozdzielonych myślnikiem.

Jak już wspomniano, ramki transmitowane poprzez łącze trunk są znakowane identyfikatorem sieci VLAN, do której należą. Jednak w protokole 802.1q jest jeden wyjątek. Ramki pochodzące z tzw. natywnej sieci VLAN (ang. *native* VLAN) są przesyłane w niezmienionej postaci. Domyślnie jest to VLAN 1. Zmiany można dokonać poleceniem:

```
switchport trunk native vlan vlan-id
```

po obu stronach łącza trunk (z tą sama wartością *vlan-id*).

Komplet informacji o połączeniach trunk można uzyskać dzięki poleceniom:

```
show interfaces trunk
```

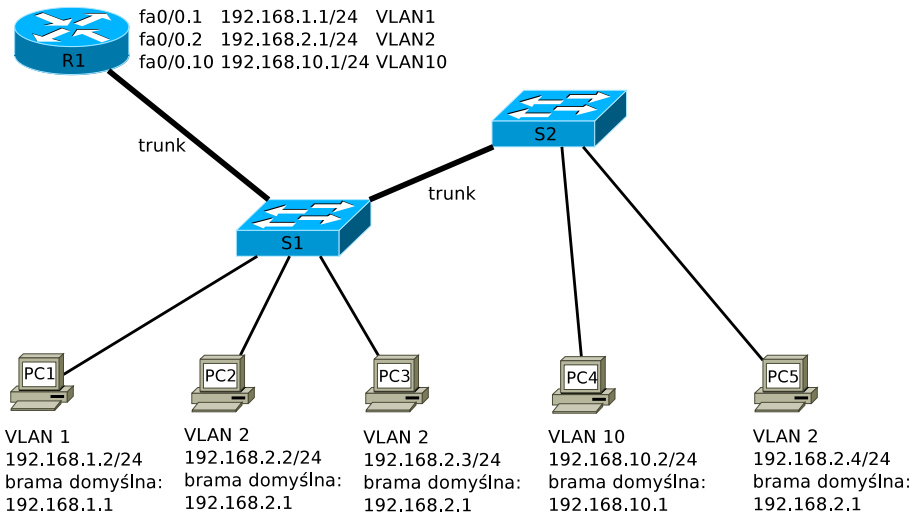
oraz

```
show interfaces nazwa-interfejsu switchport
```

3.3.4. Routing między sieciami VLAN

Komunikacja między sieciami VLAN może odbywać się tylko za pośrednictwem urządzenia 3 warstwy. Router można dołączyć do przełącznika z sieciami VLAN w sposób pokazany na rys. 3.5. Router musi mieć wtedy tyle interfejsów fizycznych, ile sieci VLAN należy skomunikować. Dlatego lepszym rozwiązaniem jest zastosowanie między routerem a przełącznikiem połączenia trunk. Przykładowa konfiguracja jest przedstawiona na rys. 3.12. Pokazany sposób dołączenia routera realizującego routing między sieciami

VLAN (ang. *inter-VLAN routing*) bywa określany mianem routera na patyku (ang. *router-on-a-stick*).



Rysunek 3.12. Routing między sieciami VLAN z wykorzystaniem podinterfejsów

Interfejs przełącznika połączony z routerem powinien być skonfigurowany jako trunk:

```
switchport mode trunk
```

Interfejs fizyczny routera (fa0/0 na rys. 3.12) powinien być włączony i skonfigurowany bez adresu IP:

```
interface nazwa-interfejsu
 no ip address
 no shutdown
```

Następnie można stworzyć na nim tzw. podinterfejsy (ang. *subinterfaces*) – po jednym dla każdej sieci VLAN. Podinterfejs tworzy się dopisując jego numer (tzn. dowolnie wybraną liczbę) do oznaczenia interfejsu fizycznego, po kropce. Każdy podinterfejs powinien zostać powiązany z odpowiednią siecią VLAN i mieć skonfigurowany należący do niej adres IP. Służą do tego celu instrukcje:

```
interface nazwa-interfejsu.numer-podinterfejsu
 encapsulation dot1q vlan-id [native]
 ip address adres-IP maska
```

Parametr `native` może być potrzebny do poinformowania routera o na-

tywnej sieci VLAN. W przypadku enkapsulacji ISL, należy użyć słowa `isl` zamiast `dot1q`. Adres podinterfejsu powinien zostać wpisany jako brama domyślna hostów w sieci VLAN.

W sieci z rys. 3.12 numer sieci VLAN pojawia się w trzecim oktecie adresu IP oraz w numerach podinterfejsów. Stosowanie takiej konwencji nie jest konieczne, ponieważ powiązanie podinterfejsu routera z siecią VLAN jest realizowane wyłącznie poprzez podanie jej numeru jako drugiego parametru polecenia `encapsulation`. Jest ona jednak zgodna z dobrymi praktykami i ułatwia zarządzanie sieciami VLAN.

Wynikiem przedstawionej powyżej konfiguracji powinno być pojawienie się w tablicy routingu routera tras do bezpośrednio dołączonych do niego sieci VLAN, co można sprawdzić w standardowy sposób (poleceniem `show ip route`).

3.4. Sieci VLAN specjalnego przeznaczenia

Bieżący podrozdział zawiera podsumowanie i uzupełnienie informacji o typach sieci VLAN, które wyróżnia się ze względu na ich przeznaczenie. Przedstawione są tu rekomendowane praktyki związane w wykorzystywaniem sieci VLAN, zwłaszcza w kontekście bezpieczeństwa.

Wyróżniamy następujące typy sieci VLAN:

— VLAN 1 jest jednocześnie domyślną siecią VLAN, ponieważ przy ustawieniach fabrycznych należą do niej wszystkie interfejsy przełącznika. W połączeniach trunk, z sieci VLAN 1 korzystają protokoły takie jak CDP (*Cisco Discovery Protocol*), VTP (*Virtual Trunk Protocol*), PAgP (*Port Aggregation Protocol*), w niektórych sytuacjach STP (*Spanning Tree Protocol*). Ze względu na bezpieczeństwo i stabilność działania, zalecane jest pozostawienie sieci VLAN 1 wyłącznie na potrzeby protokołów, które standardowo z niej korzystają.

— Natywna sieć VLAN (ang. *native* VLAN) jest jedyną siecią, z której ramki nie są znakowane przy transmisji poprzez połączenia trunk. Domyślnie jest to VLAN 1. W razie modyfikacji, ważne jest skonfigurowanie tej samej natywnej sieci VLAN po obu stronach połączenia trunk. Natywna sieć VLAN nie powinna być wykorzystywana, jeżeli nie jest to niezbędne, np. ze względu na konieczność dołączenia przełączników nieobsługujących 802.1q.

— Sieci VLAN użytkowników (ang. *user* VLAN) są przeznaczone dla urządzeń końcowych zwykłych użytkowników sieci i powinny by wykorzystywane wyłącznie do tego celu.

— Zarządzająca sieć VLAN (ang. *management* VLAN) jest wykorzystywana przez administratora do zdalnego łączenia się z urządzeniami siecio-

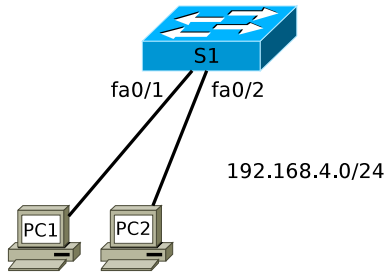
wymi, w celu zarządzania nimi. Może mieć dowolny identyfikator. Powinna być niedostępna dla zwykłych użytkowników i zawierać wyłącznie zaufane urządzenia. W razie wystąpienia takich problemów jak burze rozgłoszeń (podrozdział 7.4), dysponowanie dedykowaną siecią VLAN może umożliwić administratorowi dostęp do urządzeń i rozwiązanie problemu. Odseparowanie sieci zarządzającej i sieci użytkowników jest szczególnie ważne w sytuacji, gdy nie jest możliwe nawiązanie połączenia szyfrowanego (SSH) z urządzeniem sieciowym i administrator korzysta z takich protokołów jak telnet lub TFTP. Nadawanie przełącznikom adresów IP jest zasadne tylko w zarządzającej sieci VLAN.

— Głosowa sieć VLAN (ang. *voice* VLAN) jest przeznaczona dla komunikacji VoIP. Jej zastosowanie ułatwia implementację mechanizmów jakości usług (QoS) w odniesieniu do telefonii internetowej.

3.5. Zadania

3.5.1. Zadanie 1 – podstawowa konfiguracja sieci VLAN i połączeń trunk

1. Zbuduj sieć zgodnie z poniższym schematem (rys. 3.13).

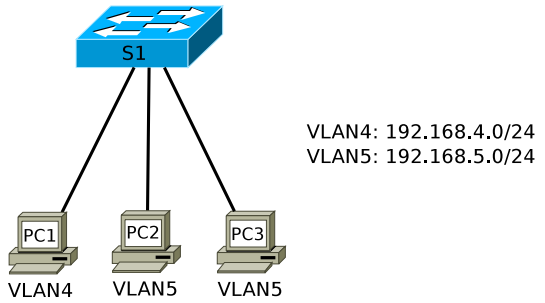


Rysunek 3.13. Schemat topologii logicznej sieci – 1. etap

2. Upewnij się, że przełącznik ma ustawienia fabryczne. Przywróć je w razie potrzeby (pamiętając również o usunięciu pliku vlan.dat). Nadaj urządzeniu nazwę i skonfiguruj podstawowe zabezpieczenia (jak w ćwiczeniu 2.5.1).
3. Nadaj komputerom adresy IP z sieci 192.168.4.0/24, pozostawiając pierwszy możliwy adres dla routera, którego dołączenie jest planowane w przyszłości. Upewnij się, że możliwa jest komunikacja między komputerami (`ping`).
4. Stwórz sieci VLAN 4 i 5. Nadaj im dowolne nazwy. Interfejsy przeznaczone do podłączenia hostów skonfiguruj jako dostępowe (statycznie, po-

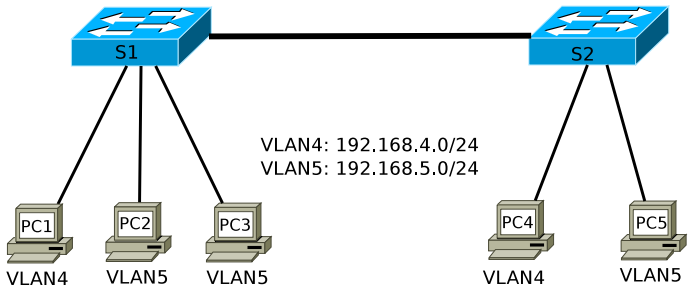
leceniem `switchport mode access`). Przypisz interfejs fa0/1 do VLAN 4, a fa0/2 do VLAN 5. Upewnij się, że sieci wirtualne są od siebie odseparowane i nie jest teraz możliwa komunikacja między nimi (mimo że hosty mają nadane adresy IP z tej samej sieci).

5. Dołącz do sieci kolejny komputer (rys. 3.14). Przypisz go do sieci VLAN 5. Skoryguj ustawienia IP tak, aby komputer należący do VLAN 4 miał adres z sieci 192.168.4.0/24, natomiast komputery należące do VLAN 5 – z sieci 192.168.5.0/24 (również z pozostawieniem pierwszego użytecznego adresu dla routera dołączonego w przyszłości). Upewnij się, że komputery należące do tej samej sieci VLAN (czyli PC2 i PC3) mogą się komunikować. W przeciwnym razie znajdź i usuń błędy konfiguracji.



Rysunek 3.14. Schemat topologii logicznej sieci – 2. etap

6. Dołącz kolejny przełącznik oraz komputery (rys. 3.15). Połączenie między przełącznikami wykonaj korzystając z najszybszych dostępnych interfejsów, np. Gigabit Ethernet. Przeprowadź podstawową konfigurację S2 (analogicznie jak w punkcie 2.).



Rysunek 3.15. Schemat topologii logicznej sieci – 3. etap

7. Połączenie między przełącznikami skonfiguruj jako trunk.
8. Na przełączniku S2 stwórz sieci VLAN 4 i 5, identycznie jak na S1.

9. Skonfiguruj adresy IP komputerów PC4 i PC5 i przypisz je do sieci VLAN, zgodnie z rys. 3.15.
10. Upewnij się, że komputery należące do tej samej sieci VLAN mogą komunikować się ze sobą, również gdy są dołączone do różnych przełączników (połączonych ze sobą łączem trunk).
11. Zapisz konfigurację urządzeń (będzie punktem startowym kolejnego ćwiczenia).

3.5.2. Rozwiązanie zadania 1

Ustawienia konfiguracyjne sieci VLAN są zapisywane w pliku vlan.dat w pamięci flash, a nie w running-config ani startup-config. W związku z tym, prezentowane listingi plików konfiguracyjnych nie stanowią kompletnego rozwiązania.

Listing 3.2. Istotne fragmenty pliku konfiguracyjnego przełącznika S1

```
[...]
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
interface FastEthernet0/1
 switchport access vlan 4
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 5
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 5
 switchport mode access
!
[...]
!
interface GigabitEthernet1/1
 switchport mode trunk
!
[...]
!
interface Vlan1
 no ip address
 shutdown
!
```

```
!
line con 0
 password 7 0822455D0A16
 login
!
[...]
!
end
```

Listing 3.3. Istotne fragmenty pliku konfiguracyjnego przełącznika S2

```
[...]
service password-encryption
!
hostname S2
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
interface FastEthernet0/1
 switchport access vlan 4
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 5
 switchport mode access
!
[...]
!
interface GigabitEthernet1/1
 switchport mode trunk
!
[...]
!
interface Vlan1
 no ip address
 shutdown
!
!
line con 0
 password 7 0822455D0A16
 login
!
[...]
!
end
```

Listing 3.4. Wynik działania polecenia show vlan na przełączniku S1

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, [...]
                                                Fa0/8, Fa0/9, [...]
                                                Fa0/12, Fa0/13, [...]
                                                Fa0/16, Fa0/17, [...]
                                                Fa0/20, Fa0/21, [...]
                                                Fa0/24, Gig1/2
4    czworka                          active    Fa0/1
5    piatka                           active    Fa0/2, Fa0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
[...]
```

Listing 3.5. Wynik działania polecenia show vlan na przełączniku S2

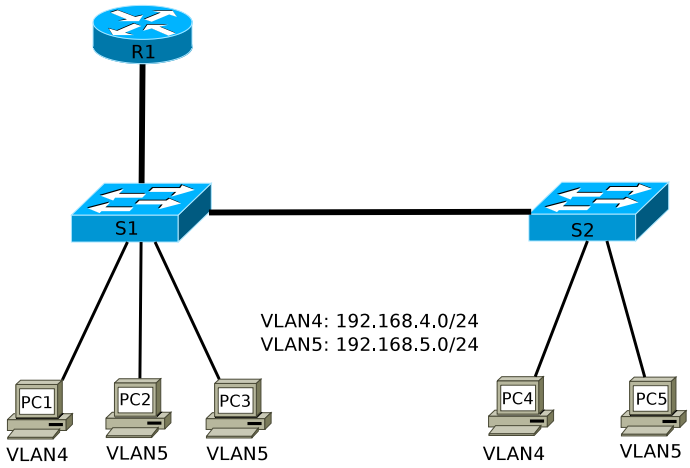
```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, [...]
                                                Fa0/7, Fa0/8, [...]
                                                Fa0/11, Fa0/12, [...]
                                                Fa0/15, Fa0/16, [...]
                                                Fa0/19, Fa0/20, [...]
                                                Fa0/23, Fa0/24, [...]
4    czworka                          active    Fa0/1
5    piatka                           active    Fa0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
[...]
```

Listing 3.6. Informacja o stanie interfejsów trunk (wynik działania polecenia show interfaces trunk) na S1 i S2

```
Port        Mode         Encapsulation  Status        Native vlan
Gig1/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig1/1      1-1005

Port        Vlans allowed and active in management domain
Gig1/1      1,4,5

Port        Vlans in spanning tree forwarding state and
```

```
11              not pruned
   Gig1/1       1,4,5
```

3.5.3. Zadanie 2 – routing miedzy sieciami VLAN



Rysunek 3.16. Schemat topologii logicznej sieci

1. Do sieci zbudowanej i skonfigurowanej w poprzednim zadaniu dołącz router, którego zadaniem będzie zapewnienie komunikacji między sieciami VLAN 4 i 5 (rys. 3.16).
2. Przeprowadź podstawową konfigurację routera (nazwa, hasła).
3. Skonfiguruj połączenie trunk między przełącznikiem S1 a routerem.
4. Na routerze skonfiguruj podinterfejsy dla VLAN 4 i VLAN 5.
5. Przejrzyj zawartość tablicy routingu. Upewnij się, że możliwa jest komunikacja między wszystkimi komputerami (także z różnych sieci VLAN).

3.5.4. Rozwiązanie zadania 2

Listing 3.7. Istotne fragmenty pliku konfiguracyjnego routera R1

```
   [...]
2  !
   hostname R1
4  !
   !
6  !
   enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
8  !
```

```
[...]
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet0/0.5
 encapsulation dot1Q 5
 ip address 192.168.5.1 255.255.255.0
!
[...]
!
ip classless
!
[...]
!
line con 0
 password 7 0822455D0A16
 login
[...]
!
end
```

Listing 3.8. Dodatkowa konfiguracja przełącznika S1

```
!
interface FastEthernet0/4
 switchport mode trunk
!
```

Listing 3.9. Zawartość tablicy routingu routera R1

```
C    192.168.4.0/24 is directly connected, FastEthernet0/0.4
C    192.168.5.0/24 is directly connected, FastEthernet0/0.5
```

Listing 3.10. Przykładowe ustawienia sieciowe hosta PC1

```
Adres IP:              192.168.4.10
Maska podsieci:        255.255.255.0
Brama domyślna:        192.168.4.1
```

Listing 3.11. Przykładowe ustawienia sieciowe hosta PC2

```
Adres IP:           192.168.5.10
Maska podsieci:     255.255.255.0
Brama domyślna:     192.168.5.1
```

Listing 3.12. Przykładowe ustawienia sieciowe hosta PC3

```
Adres IP:           192.168.5.11
Maska podsieci:     255.255.255.0
Brama domyślna:     192.168.5.1
```

Rozdział 4

Protokół VTP

4.1. Wstęp

VLAN Trunk Protocol (VTP) [17] jest, w przeciwieństwie do większości prezentowanych tu standardów, protokołem własnościowym Cisco. Wbrew sugestii zawartej w nazwie, VTP nie jest niezbędny do zestawienia połączeń typu trunk ani skonfigurowania wirtualnych sieci LAN. Jest natomiast narzędziem w znacznym stopniu ułatwiającym administrowanie sieciami VLAN, zwłaszcza w przypadku rozbudowanych konfiguracji, z wieloma przełącznikami.

Standardowo, jeżeli sieci VLAN mają funkcjonować w obrębie kilku przełączników połączonych poprzez łącza trunk, muszą zostać skonfigurowane oddzielnie na każdym przełączniku. Każdy przełącznik przechowuje swoje własne informacje konfiguracyjne i nie są one współdzielone. Gdy sieć jest zbudowana z wielu przełączników, na których skonfigurowano wiele sieci VLAN, administrowanie nią, a zwłaszcza modyfikacje i rozbudowywanie stają się kłopotliwe. Problemem mogą być nawet pozornie proste aspekty konfiguracji, takie jak zapewnienie by sieci VLAN o danym identyfikatorze miały skonfigurowane identyczne nazwy na wszystkich przełącznikach. Implementacja VTP zmienia tę sytuację. Dzięki działaniu VTP, stworzenie, usunięcie lub modyfikacja ustawień sieci VLAN (np. nazwy), przeprowadzona na jednym urządzeniu, może być automatycznie powielona na pozostałe przełączniki, w obrębie domeny VTP. Dzięki temu uzyskujemy spójność całej konfiguracji.

Analizując zalety protokołu VTP należy mieć świadomość, że przypisywanie interfejsów fizycznych do sieci VLAN odbywa się tak samo, niezależnie od działania protokołu VTP lub jego braku. W przypadku statycznych sieci VLAN jest to zatem nadal jeden z bardziej czasochłonnych obowiązków administratora, wymagający łączenia się z poszczególnymi przełącznikami.

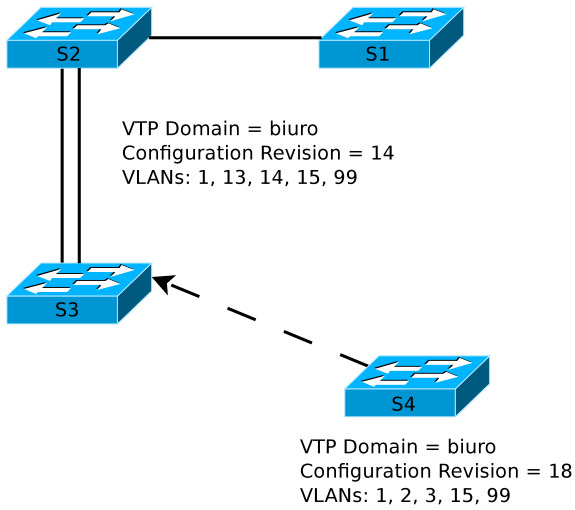
Informacje podane w dalszej części rozdziału odnoszą się przede wszystkim do protokołu VTP w wersji 1 lub 2. Wersja 3 [18] jest obecnie obsługiwana tylko przez niektóre urządzenia (np. nieco przestarzałe już przełączniki z systemem Catalyst OS (CatOS) od wersji 8.1(1) oraz Catalyst 6500, począwszy od IOS 12.2(33)SXI).

Konkurencyjnym dla VTP rozwiązaniem jest *Multiple Registration Protocol* (MRP) – standard 802.1ak [19], który jest następcą *Generic Attribute Registration Protocol* (GARP). Można uruchomić go także na urządzeniach Cisco [20], jednak zagadnienie to wykracza poza zakres tego podręcznika.

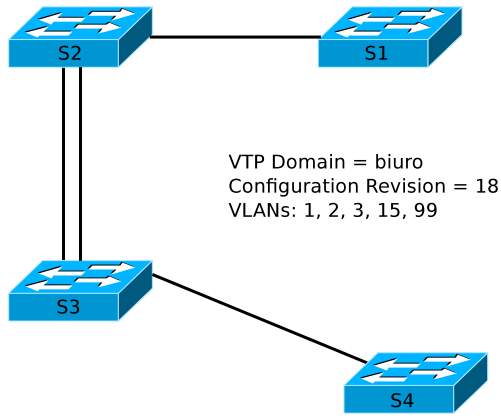
4.2. Działanie VTP

VTP jest protokołem drugiej warstwy modelu OSI. Komunikacja odbywa się wyłącznie poprzez połączenia trunk (ISL lub IEEE 802.1Q). Domena VTP (ang. *VTP domain*, *VLAN management domain*) jest grupą przełączników, które współdzielą te same ustawienia konfiguracyjne dotyczące sieci VLAN. Przełącznik może należeć tylko do jednej domeny VTP. Nazwa domeny VTP jest podstawowym parametrem konfiguracyjnym tego protokołu. Domyślnie jest ona pustym łańcuchem, aż do chwili gdy zostanie ręcznie skonfigurowana przez administratora lub przełącznik otrzyma komunikat VTP poprzez połączenie trunk. Wówczas nazwa domeny zostanie automatycznie ustawiona na zgodną z zawartą w komunikacie. Po ustaleniu nazwy swojej domeny VTP, przełącznik będzie ignorował komunikaty VTP pochodzące z innych domen.

Kolejnym istotnym parametrem jest numer zmiany konfiguracji VTP (ang. *VTP configuration revision number*). Jest to 32-bitowa liczba, której wartość jest zwiększana o 1 przy każdej modyfikacji konfiguracji VLAN. Numer zmiany konfiguracji jest umieszczany w każdym ogłoszeniu VTP, periodycznie wysyłanym jako multicast, przez każdy przełącznik, przez wszystkie porty trunk. Otrzymanie przez przełącznik komunikatu VTP z wyższą wartością numeru zmiany konfiguracji niż wartość, którą aktualnie posiada oznacza, że istnieje nowsza konfiguracja VLAN i należy ją pozyskać z innego przełącznika. W przeciwnym razie ogłoszenie jest ignorowane.



Rysunek 4.1. Dodawanie nowego przełącznika do domeny VTP



Rysunek 4.2. Sytuacja po dołączeniu przełącznika S4 do domeny VTP

Z mechanizmem tym związane jest pewne zagrożenie. Przeanalizujmy scenariusz z rys. 4.1. Początkowo w sieci pracowały 4 przełączniki, połączone poprzez łącza trunk, należące do domeny VTP "biuro". Stworzono sieci VLAN nr 13, 14, 15 i 99. Następnie przełącznik S4 został odłączony i zabrany do testów. Podczas jego testów, zmodyfikowano konfigurację VLAN: utworzono VLAN 2 i 3, usunięto 13 i 14. W wyniku tego działania, wzrosła wartość numeru zmiany konfiguracji VTP. Po ponownym dołączeniu przełącznika S4 do sieci, pozostałe przełączniki przejęły jego ustawienia (rys. 4.2), ponieważ wartość numeru zmiany konfiguracji przełącznika S4 była wyższa niż ich własna. Sieci VLAN nr 13 i 14 przestały istnieć. Jak już wspomniano wcześniej, jeżeli zostanie usunięty VLAN, do którego przypisane są interfejsy przełącznika, interfejsy te przestają działać. Przedstawiony problem nie posiada prostego rozwiązania. W celu przywrócenia działania interfejsów przypisanych do VLAN 13 i 14, konieczne jest ponowne ich utworzenie lub przypisanie portów do innych sieci VLAN. Jeżeli VLAN nr 2 i 3 nie są potrzebne, należy je usunąć.

Widać tu, że przy dołączaniu przełączników do istniejącej domeny VTP należy zachować szczególną ostrożność. Ryzyko nie występuje, gdy dołączany jest przełącznik z ustawieniami fabrycznymi (brak nazwy domeny VTP, zerowa wartość numeru zmiany konfiguracji). W przeciwnym razie, należy zwrócić uwagę na numer zmiany konfiguracji. Nie ma możliwości bezpośredniej modyfikacji jej wartości. Można ją natomiast wyzerować poprzez zmianę nazwy domeny VTP na inną, a następnie przywrócenie pożądanej. Po dołączeniu takiego przełącznika do sieci, powinien on pobrać ustawienia VLAN od innych przełączników (pod warunkiem posiadania zgodnej nazwy domeny).

Kolejnym problemem jest bezpieczeństwo. Jeżeli potencjalnemu włamy-

waczowi uda się wymusić połączenie typu trunk między przełącznikiem w sieci a przełącznikiem dostarczonym przez siebie, może wprowadzić do domeny VTP praktycznie dowolne ustawienia VLAN i sparaliżować działanie sieci. Dlatego porty przełączników przeznaczone dla urządzeń końcowych powinny być na stałe skonfigurowane jako dostępowe (przy pomocy znanego już polecenia `switchport mode access`). Kolejnym zabezpieczeniem jest skonfigurowanie hasła domeny VTP (przekształcanego automatycznie na 16-bajtową wartość MD5). To samo hasło powinno zostać ręcznie skonfigurowane na wszystkich przełącznikach w domenie i tylko te przełączniki będą mogły komunikować się w protokole VTP. Pomimo tych mechanizmów, jeżeli bezpieczeństwo sieci ma krytyczne znaczenie, należy rozważyć rezygnację z protokołu VTP.

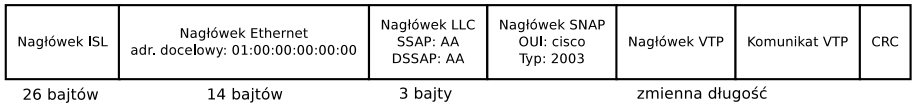
W protokole VTP przełącznik może pracować w jednym z następujących trybów:
— serwer VTP (ang. *VTP server*),
— klient VTP (ang. *VTP client*),
— tryb przezroczysty (ang. *VTP transparent*),
— wyłączony (ang. *off*).

Tryb serwera umożliwia przeprowadzanie wszelkich operacji związanych z konfiguracją VLAN (tworzenie, modyfikacja, usuwanie) uraz ustalanie parametrów protokołu VTP dla całej domeny. Serwer rozsyła komunikaty VTP informujące o konfiguracji VLAN, jak również odbiera je od innych przełączników i w razie dostępności nowszej konfiguracji, dostosowuje się do niej. Jest to domyślny tryb. W sieci może jednocześnie pracować wiele serwerów VTP.

Zachowanie klienta VTP jest zbliżone do serwera, z tą różnicą, że nie jest na nim możliwe dodawanie, modyfikacja ani usuwanie sieci VLAN (odpowiednie polecenia są niedostępne).

Przełącznik w trybie przezroczystym ignoruje otrzymywane komunikaty VTP (w 2. wersji VTP są one jednak przekazywane dalej poprzez połączenia trunk) i nie generuje własnych. Tworzenie, modyfikacja i usuwanie sieci VLAN jest możliwe lokalnie i nie ma wpływu na konfigurację pozostałych przełączników.

Tryb wyłączony można skonfigurować tylko na przełącznikach z systemem CatOS. Działa on podobnie jak tryb przezroczysty, jednak komunikaty VTP nie są w ogóle przekazywane.



Rysunek 4.3. Format komunikatu VTP w enkapsulacji ISL [17]

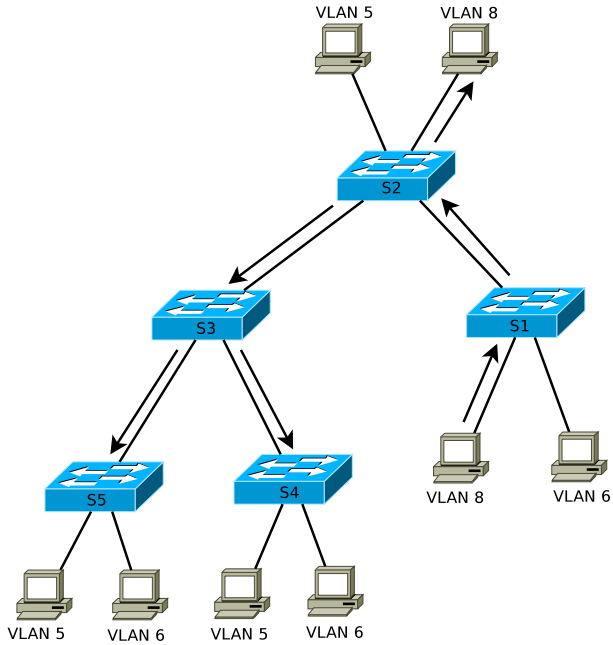
Komunikacja między przełącznikami w protokole VTP jest realizowana przy pomocy następujących typów wiadomości (rys. 4.3):
— sumaryczne ogłoszenie (ang. *summary advertisements*),
— częściowe ogłoszenie (ang. *subset advertisement*),
— żądanie ogłoszenia (ang. *advertisement requests*),
— wiadomość o dołączeniu do VTP (ang. *VTP join messages*).

Sumaryczne ogłoszenia domyślnie wysyłane są co 5 minut. Służą one do informowania sąsiednich przełączników o aktualnej wartości numeru zmiany konfiguracji. W odpowiedzi na sumaryczne ogłoszenie z wyższą wartością numeru zmiany konfiguracji, niż aktualna na danym przełączniku, przełącznik wysyła żądanie przesłania mu szczegółowych informacji (żądanie ogłoszenia). Częściowe ogłoszenia służą do przekazywania informacji o sieciach VLAN. W przypadku istnienia wielu sieci VLAN, do przesłania kompletu informacji może być potrzebnych kilka takich komunikatów. Wiadomość o dołączeniu do VTP jest podobna do żądania ogłoszenia, przy czym informuje także o dodaniu nowego urządzenia do domeny.

VTP domyślnie uruchamia się w 1. wersji. Wersja 2. posiada kilka dodatkowych funkcji, w szczególności wsparcie dla Token Ring. Jeżeli nie jest ono potrzebne, zwykle wersja 1. jest wystarczająca. Wersje 1. i 2. nie są zgodne, więc w całej domenie VTP powinna być skonfigurowana ta sama. W wersji 3. dodano szereg rozszerzeń, np. obsługę rozszerzonego zakresu sieci VLAN, bezpieczne sieci VLAN (*Private VLAN*), zabezpieczenia bazy danych przed wymazaniem zawartości po dołączeniu nowego przełącznika. Wersja 3. jest zgodna wstecz z 2., jednak zaleca się, by w miarę możliwości stosować jednorodną konfigurację.

Użyteczną funkcją może być przycinanie VTP (ang. *VTP pruning*). W przykładzie z rys. 4.4 komputer należący do sieci VLAN nr 8 wysłał ramkę rozgłoszeniową. Musi on zostać przekazany do wszystkich portów przypisanych tej sieci VLAN. Zostanie więc rozesłany poprzez połączenia trunk do wszystkich przełączników. W naszym scenariuszu jednak urządzenia należące do VLAN 8 są dołączone tylko do przełączników S1 i S2, w związku z czym przekazywanie ramki do przełączników S3, S4 i S5 jest bezcelowe i niepotrzebnie obciąża sieć. Połączenie trunk domyślnie obsługuje wszystkie sieci VLAN. Można byłoby wyłączyć obsługę VLAN 8 przez trunk między S2 i S3, jednak w razie uaktywnienia portu przełącznika S3, S4 lub S5 należącego do VLAN 8, ustawienie to należałoby cofnąć. Lepszym rozwiązaniem jest włączenie funkcji przycinania VTP. Eliminuje ona w sposób automatyczny zbędną część ruchu rozgłoszeniowego. W sytuacji z rys. 4.4 obszar rozsyłania ramki rozgłoszeniowej zostałby ograniczony do przełączników S1 i S2.

Włączenie przycinania na dowolnym serwerze VTP skutkuje aktywacją



Rysunek 4.4. Przekazywanie ramki rozgłoszeniowej (między przełącznikami są połączenia trunk)

tej funkcji w całej domenie. Przycinanie nie działa dla sieci VLAN 1, 1002 – 1005 oraz całego zakresu rozszerzonego (powyżej 1005).

4.3. Konfiguracja VTP

Domyślna konfiguracja protokołu VTP zawiera następujące ustawienia:
— nazwa domeny VTP (*VTP Domain Name*): *Null*,
— tryb VTP (*VTP Operating Mode*): *Server*,
— wersja VTP v2 (*VTP V2 Mode*): *Disabled* (wyłączona),
— hasło VTP: brak,
— przycinanie VTP (*VTP Pruning Mode*): *Disabled* (wyłączone).
Konfiguracja VTP może zostać przeprowadzona w trybie konfiguracyjnym VLAN (po wpisaniu polecenia `vlan database`) lub w trybie konfiguracji globalnej. Przedstawiona zostanie druga możliwość. W wariancie minimalistycznym wystarczy skonfigurować nazwę domeny VTP na jednym z przełączników (pozostałe przełączniki, dołączone poprzez łącza trunk, powinny przyjąć ją automatycznie):

```
vtp domain nazwa
```

Tryb VTP można skonfigurować poleceniem:

```
vtp mode client|server|transparent
```

Domenę VTP warto zabezpieczyć hasłem, wpisując w ustawieniach wszystkich przełączników polecenie:

```
vtp password hasło
```

Wersję 2. VTP można włączyć poleceniem:

```
vtp version 2
```

Polecenie wystarczy wydać na jednym z serwerów. Pozostałe przełączniki powinny przejąć to ustawienie, o ile są w stanie obsługiwać 2. wersję.

Przycinanie VTP włącza polecenie:

```
vtp pruning
```

wydane na jednym z serwerów.

4.4. Weryfikacja działania VTP

Skutkiem działania VTP powinna być dostępność tych samych sieci VLAN z identycznymi nazwami na wszystkich przełącznikach połączonych poprzez łącza trunk, co można sprawdzić znanym już poleceniem:

```
show vlan
```

Podstawowym poleceniem diagnostycznym samego VTP jest natomiast:

```
show vtp status
```

Przykładowy wynik działania tego polecenia przedstawia poniższy listing.

Listing 4.1. Przykładowy wynik działania polecenia show vtp status

```
1 VTP Version                     : 2
  Configuration Revision          : 4
3 Maximum VLANs supported locally : 255
  Number of existing VLANs        : 8
5 VTP Operating Mode              : Server
  VTP Domain Name                 : biuro
7 VTP Pruning Mode                : Disabled
  VTP V2 Mode                     : Disabled
9 VTP Traps Generation            : Disabled
  MD5 digest                      : 0x60 0xB3 0x0C 0xF5
```

```
11                                    0x40 0xD4 0x76 0x65
   Configuration last modified by 0.0.0.0 at 3-1-93 00:28:15
13 Local updater ID is 192.168.1.1 on interface Vl1 (lowest
                                numbered VLAN interface found)
```

Pierwszy wiersz powyższego listingu informuje, że przełącznik jest w stanie obsługiwać VTP v2 (jak również wersję wcześniejszą). Jednak w tym momencie obsługuje wersję 1., zgodnie z zapisem w wierszu nr 8. W przypadku niektórych urządzeń i nowszych wersji IOS, informacja ta może mieć mniej enigmatyczną postać, np:

```
VTP Version              : running VTP1 (VTP2 capable)
[...]
VTP V2 Mode              : Disabled
[...]
```

lub:

```
VTP Version capable              : 1 to 3
VTP version running              : 1
[...]
```

W stabilnym stanie sieci powinniśmy zaobserwować te same wartości *Configuration Revision* (wiersz 2. listingu 4.1) na wszystkich przełącznikach.

Informacji o liczbie wysłanych i odebranych komunikatów VTP dostarcza polecenie:

```
show vtp counters
```

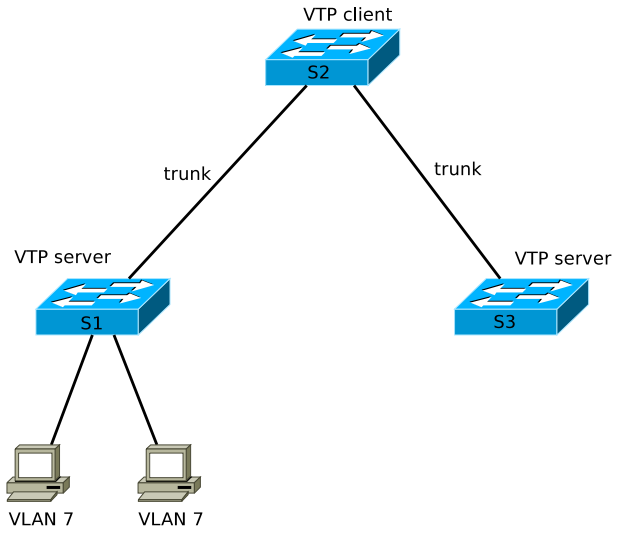
Przykładowy wynik jego działania przedstawia kolejny listing.

Listing 4.2. Przykładowy wynik działania polecenia show vtp counters

```
1 VTP statistics:
  Summary advertisements received    : 12
3 Subset advertisements received     : 7
  Request advertisements received    : 3
5 Summary advertisements transmitted : 15
  Subset advertisements transmitted  : 10
7 Request advertisements transmitted : 0
  Number of config revision errors   : 0
9 Number of config digest errors     : 0
  Number of V1 summary errors        : 0
11

13 VTP pruning statistics:
   [...]
```

4.5. Zadania

4.5.1. Zadanie 1 – podstawowa konfiguracja VTP



Rysunek 4.5. Schemat topologii logicznej sieci

1. W razie potrzeby przywróć fabryczną konfigurację przełączników. Zbuduj sieć zgodnie ze schematem (rys. 4.5).
2. Przeprowadź podstawową konfigurację przełączników (nazwy, hasła zabezpieczające, VLAN zarządzający).
3. Porty łączące przełączniki skonfiguruj jako trunk, natomiast pozostałe jako dostępowe (możesz użyć polecenia `interface range`). Zweryfikuj działanie połączenia trunk (np. poleceniem `show interface trunk` lub `ping` między przełącznikami).
4. Skonfiguruj nazwę domeny VTP na przełączniku S1. Upewnij się, że nazwa pojawiła się również na pozostałych przełącznikach.
5. Skonfiguruj hasło zabezpieczające VTP.
6. Przełącznik S2 skonfiguruj jako klienta VTP.
7. Na jednym z serwerów stwórz kilka sieci VLAN (np. 2, 3, 7) i nadaj im nazwy. Upewnij się, że te same sieci VLAN pojawiły się automatycznie na pozostałych przełącznikach. Przypisz porty do sieci VLAN.
8. Zweryfikuj działanie protokołu VTP poleceniami `show vtp status` oraz `show vtp counters`. Zwróć uwagę na numer zmiany konfiguracji i jego inkrementację przy modyfikacji konfiguracji VLAN.
9. Włącz funkcję `vtp pruning`. Zweryfikuj jej działanie, jak w poprzednim punkcie.

4.5.2. Rozwiązanie zadania 1

Ustawienia konfiguracyjne protokołu VTP są zapisywane w pliku vlan.dat w pamięci flash, a nie w running-config ani startup-config. W związku z tym, prezentowane listingi plików konfiguracyjnych nie stanowią kompletnego rozwiązania.

Listing 4.3. Istotne fragmenty pliku konfiguracyjnego przełącznika S1

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 7
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 7
 switchport mode access
!
interface FastEthernet0/4
 switchport mode access
!
interface FastEthernet0/5
 switchport mode access
!

[...]

!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login
```

```
   line vty 5 15
44  login
   !
46 !
   end
```

Listing 4.4. Istotne fragmenty pliku konfiguracyjnego przełącznika S2

```
 1 version 12.2
   no service timestamps log datetime msec
 3 no service timestamps debug datetime msec
   service password-encryption
 5 !
   hostname S2
 7 !
   enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
 9 !
   !
11 interface FastEthernet0/1
    switchport mode trunk
13 !
   interface FastEthernet0/2
15  switchport mode trunk
   !
17 interface FastEthernet0/3
    switchport mode access
19 !
   interface FastEthernet0/4
21  switchport mode access
   !
23 interface FastEthernet0/5
    switchport mode access
25 !

27 [...]

29 !
   interface Vlan1
31  ip address 192.168.1.2 255.255.255.0
   !
33 !
   line con 0
35  password 7 0822455D0A16
    login
37 !
   line vty 0 4
39  login
   line vty 5 15
41  login
   !
```

```
!
end
```

Listing 4.5. Przykładowy wynik działania polecenia show vtp status dla przełącznika S1

```
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : biuro
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x61 0x64 0xDD 0x42
                                  0x80 0x9A 0xF7 0x55
Configuration last modified by 192.168.1.3
                          at 3-1-93 00:49:21
Local updater ID is 192.168.1.1 on interface Vl1
            (lowest numbered VLAN interface found)
```

Listing 4.6. Przykładowy wynik działania polecenia show vtp status dla przełącznika S2

```
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : biuro
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x61 0x64 0xDD 0x42
                                  0x80 0x9A 0xF7 0x55
Configuration last modified by 192.168.1.3 at
                                3-1-93 00:49:21
```

Listing 4.7. Przykładowy wynik działania polecenia show vlan dla przełącznika S1

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------
1    default                           active    Fa0/4, [...]
                                                 Fa0/8, [...]
                                                 Fa0/12,[...]
```

```
                                                  Fa0/16,[...]
7                                                 Fa0/20,[...]
                                                  Fa0/24,[...]
9 2    dwojka                          active
  3    trojka                          active
11 7   siodemka                        active     Fa0/2, Fa0/3
  1002 fddi-default                    act/unsup
13 1003 token-ring-default              act/unsup
  1004 fddinet-default                 act/unsup
15 1005 trnet-default                   act/unsup

17 [...]
```

Listing 4.8. Przykładowy wynik działania polecenia show vlan dla przełącznika S3

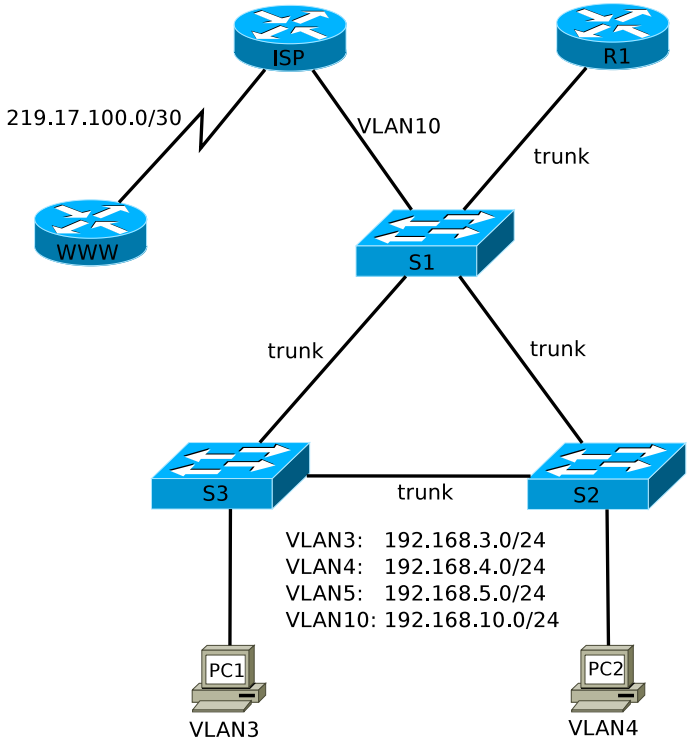
```
1 VLAN Name                             Status    Ports
  ---- -------------------------------- --------- -------
3 1    default                          active    Fa0/2, [...]
                                                  Fa0/6, [...]
5                                                 Fa0/10,[...]
                                                  Fa0/14,[...]
7                                                 Fa0/18,[...]
                                                  Fa0/22,[...]
9                                                 Gig1/2
  2    dwojka                          active
11 3   trojka                          active
  7    siodemka                        active
13 1002 fddi-default                    act/unsup
  1003 token-ring-default               act/unsup
15 1004 fddinet-default                 act/unsup
  1005 trnet-default                    act/unsup
17
  [...]
```

Listing 4.9. Przykładowy wynik działania polecenia show vtp counters dla przełącznika S2

```
  VTP statistics:
2 Summary advertisements received    : 6
  Subset advertisements received     : 4
4 Request advertisements received    : 1
  Summary advertisements transmitted : 7
6 Subset advertisements transmitted  : 4
  Request advertisements transmitted : 1
8 Number of config revision errors   : 0
  Number of config digest errors     : 0
10 Number of V1 summary errors       : 0
```

```
12
   VTP pruning statistics:
14
   Trunk   Join Transmitted Join Received  Summary advts
16                                         received from
                                           non-pruning-capable
18                                         device
   ------  ----------------- -------------  ---------------------
20 Fa0/1          33              32              0
   Fa0/2          32              33              0
```

4.5.3. Zadanie 2 – VTP i routing między sieciami VLAN



Rysunek 4.6. Schemat topologii logicznej sieci.

Początkowo w sieci przedstawionej na rys. 4.6 znajdowały się tylko przełączniki oraz router R1. R1 był odpowiedzialny za routing między sieciami VLAN 3, 4 i 5. Następnie uzyskano połączenie z Internetem, za pośrednictwem routera ISP. Ponieważ R1 nie posiadał wolnego interfejsu fizycznego, stworzono VLAN 10 i ISP dołączono do przełącznika. Celem zadania jest

skonfigurowanie routingu statycznego w taki sposób, aby była możliwa komunikacja między wszystkimi urządzeniami.

1. Połącz urządzenia zgodnie ze schematem (rys. 4.6).
2. Zaplanuj adresowanie IP, zgodnie z rysunkiem. Dla interfejsów routerów zarezerwuj najniższe możliwe adresy.
3. Przeprowadź podstawową konfigurację wszystkich urządzeń (nazwy, hasła, itp.).
4. Połączenia między przełącznikami oraz między przełącznikiem S1 a routerem R1 skonfiguruj jako trunk.
5. Skonfiguruj adresy IP interfejsów, które tego wymagają.
6. Stwórz sieci VLAN 3, 4, 5, 10. Skorzystaj z protokołu VTP do zapewnienia spójności konfiguracji.
7. Skonfiguruj router R1 tak, aby realizował routing między sieciami VLAN.
8. Na routerze WWW włącz usługę serwera HTTP.
9. Na routerach R1, ISP i WWW skonfiguruj trasy statyczne tak, aby była możliwa komunikacja między wszystkimi urządzeniami w sieci.
10. Przetestuj działanie sieci, a w szczególności upewnij się, że jest możliwe połączenie przeglądarką internetową między komputerami PC a routerem WWW.
11. Wykonaj kopie zapasowe konfiguracji routerów i przełączników.
12. Przywróć standardową konfigurację urządzeń.

4.5.4. Rozwiązanie zadania 2

W celu umożliwienia komunikacji między sieciami VLAN, na routerze R1 wystarczy odpowiednio skonfigurować podinterfejsy, jak pokazano w wierszach 5–24 listingu 4.13. Pakiety przeznaczone dla adresatów spoza bezpośrednio dołączonych sieci (VLAN 3, 4, 5 i 10) należy przekazywać do interfejsu Fast Ethernet routera ISP. Odpowiednia instrukcja definiująca trasę domyślną dla R1 znajduje się w wierszu 29. Kompletną zawartość tablicy routingu przedstawia listing 4.18.

Router dostawcy Internetu – ISP automatycznie uzyska w tablicy routingu wpisy dotyczące bezpośrednio dołączonych sieci, tzn. 219.17.100.0/30 i 192.168.10.0/24 (VLAN 10). Konieczne jest zatem zdefiniowanie tras do sieci VLAN 3, 4, 5, co pokazują wiersze 21–23 listingu 4.14. Pakiety przeznaczone dla tych sieci należy przekazać routerowi R1, do podinterfejsu dołączonego do VLAN 10. Kompletną tablicę routingu ISP pokazuje listing 4.19.

Konfiguracja routingu na routerze WWW wymaga tylko zdefiniowania trasy domyślnej poprzez jego interfejs szeregowy, poleceniem pokazanym w 13. wierszu listingu 4.15.

Listing 4.10. Istotne fragmenty pliku konfiguracyjnego przełącznika S1

```
[...]
!
hostname S1
!
!
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
[...]
!
interface FastEthernet0/24
 switchport access vlan 10
 switchport mode access
!
[...]
!
interface Vlan1
 no ip address
 shutdown
!
[...]
!
end
```

Listing 4.11. Istotne fragmenty pliku konfiguracyjnego przełącznika S2

```
[...]
!
hostname S2
!
!
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 4
 switchport mode access
!
```

```
   [...]
18 !
   interface Vlan1
20  no ip address
    shutdown
22 !
   [...]
24 !
   end
```

Listing 4.12. Istotne fragmenty pliku konfiguracyjnego przełącznika S3

```
1  [...]
   !
3  hostname S3
   !
5  !
   !
7  interface FastEthernet0/1
    switchport mode trunk
9  !
   interface FastEthernet0/2
11  switchport mode trunk
   !
13 interface FastEthernet0/3
    switchport access vlan 3
15  switchport mode access
   !
17 [...]
   !
19 interface Vlan1
    no ip address
21  shutdown
   !
23 !
   [...]
25 !
   !
27 end
```

Listing 4.13. Istotne fragmenty pliku konfiguracyjnego routera R1

```
1  [...]
   !
3  hostname R1
   !
5  interface FastEthernet0/0
    no ip address
7   duplex auto
```

```
 speed auto
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet0/0.5
 encapsulation dot1Q 5
 ip address 192.168.5.1 255.255.255.0
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.2 255.255.255.0
!
[...]
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
[...]
!
end
```

Listing 4.14. Istotne fragmenty pliku konfiguracyjnego routera ISP

```
[...]
!
hostname ISP
!
[...]
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
[...]
!
interface Serial1/0
 ip address 219.17.100.1 255.255.255.252
 clock rate 128000
!
[...]
!
ip classless
ip route 192.168.3.0 255.255.255.0 192.168.10.2
```

```
ip route 192.168.4.0 255.255.255.0 192.168.10.2
ip route 192.168.5.0 255.255.255.0 192.168.10.2
!
[...]
!
end
```

Listing 4.15. Istotne fragmenty pliku konfiguracyjnego routera WWW

```
[...]
!
hostname WWW
!
[...]
!
interface Serial1/0
 ip address 219.17.100.2 255.255.255.252
!
[...]
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial1/0
!
[...]
!
ip http server
no ip http secure-server
!
[...]
!
end
```

Listing 4.16. Konfiguracja VLAN przełącznika S3

```
S3#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, [...]
                                                Fa0/8, [...]
                                                Fa0/12,[...]
                                                Fa0/16,[...]
                                                Fa0/20,[...]
                                                Fa0/24,[...]
3    VLAN0003                         active    Fa0/3
4    VLAN0004                         active
5    VLAN0005                         active
10   VLAN0010                         active
[...]
```

Listing 4.17. Konfiguracja VTP przełącznika S3

```
S3#show vtp status
VTP Version                     : 2
Configuration Revision          : 4
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Server
VTP Domain Name                 : LAB
[...]
```

Listing 4.18. Tablica routingu routera R1

```
Gateway of last resort is 192.168.10.1 to network 0.0.0.0

C   192.168.3.0/24 is directly connected, FastEthernet0/0.3
C   192.168.4.0/24 is directly connected, FastEthernet0/0.4
C   192.168.5.0/24 is directly connected, FastEthernet0/0.5
C   192.168.10.0/24 is directly connected, FastEthernet0/0.10
S*  0.0.0.0/0 [1/0] via 192.168.10.1
```

Listing 4.19. Tablica routingu routera ISP

```
S     192.168.3.0/24 [1/0] via 192.168.10.2
S     192.168.4.0/24 [1/0] via 192.168.10.2
S     192.168.5.0/24 [1/0] via 192.168.10.2
C     192.168.10.0/24 is directly connected, FastEthernet0/0
      219.17.100.0/30 is subnetted, 1 subnets
C        219.17.100.0 is directly connected, Serial1/0
```

Listing 4.20. Przykładowe ustawienia sieciowe hosta PC1

```
Adres IP:           192.168.3.10
Maska podsieci:     255.255.255.0
Brama domyślna:     192.168.3.1
```

Listing 4.21. Przykładowe ustawienia sieciowe hosta PC2

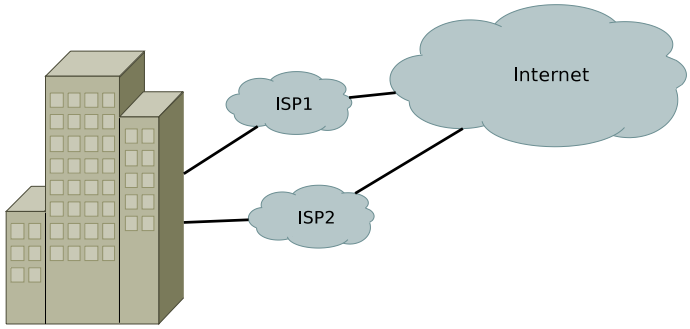
```
Adres IP:           192.168.4.10
Maska podsieci:     255.255.255.0
Brama domyślna:     192.168.4.1
```

Rozdział 5

Podstawy projektowania sieci lokalnych

5.1. Wstęp

Współczesne sieci komputerowe są narzędziem biznesowym. Jakiekolwiek przerwy w ich funkcjonowaniu skutkują wymiernymi stratami dla firmy. Dąży się zatem do jak najwyższego poziomu niezawodności i dostępności sieci dla użytkowników. W sytuacji, gdy praktycznie każdy komponent sieci może ulec awarii, niezbędne jest wprowadzenie urządzeń nadmiarowych, które mogłyby automatycznie przejąć zadania urządzeń uszkodzonych.

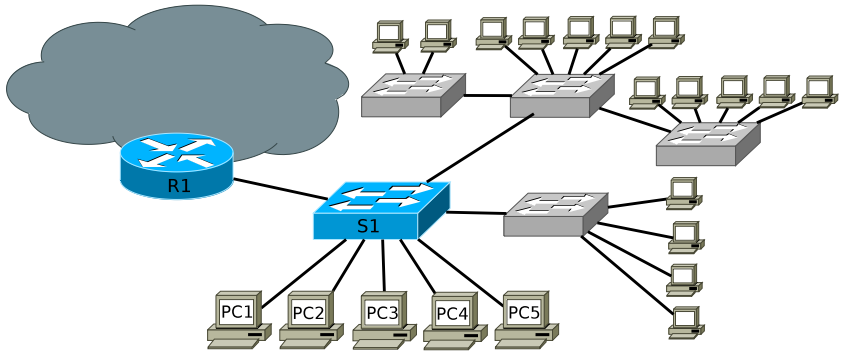


Rysunek 5.1. Redundancja dostępu do Internetu

Załóżmy, że hipotetyczna firma, której siedziba jest przedstawiona na rys. 5.1, ma dostęp do Internetu zapewniany przez jednego operatora – ISP1. Operator ten jest bardzo zawodny i połączenie z Internetem jest dostępne tylko przez około 90% czasu. Firma znajduje zatem kolejnego operatora – ISP2 (niezależnego od ISP1), również gwarantującego połączenie z Internetem przez 90% czasu. Prosty rachunek pozwoli stwierdzić, że dzięki dwóm operatorom, połączenie z Internetem będzie dostępne już przez 99% czasu.

W przypadku systemów informatycznych, których działanie jest szczególnie istotne, mówi się o pożądanej dostępności na poziomie "pięciu dziewiątek" (ang. *five nines*), tzn. system powinien być dostępny przez 99,999% czasu. Średni czas niedostępności w ciągu roku wynosi wówczas około $5\frac{1}{2}$ minuty. Wiąże się to oczywiście z kosztami zakupu, konfiguracji i utrzymania dodatkowych urządzeń. Należy rozważyć także kwestię stabilnego zasilania, również w razie problemów z dostarczaniem energii elektrycznej. Duże systemy informatyczne, np. centra danych, potrzebują także wody do chłodzenia urządzeń. Znalezienie dwóch niezależnych dostawców może być jeszcze trudniejsze niż w przypadku energii elektrycznej lub połączeń internetowych. Jednocześnie, kwestia dużego zużycia wody przez takie systemy jest często przemilczana.

Kolejny problem jest przedstawiony na rys. 5.2. Początkowo sieć składała się z routera R1, przełącznika S1 i było do niej dołączonych pięć hostów



Rysunek 5.2. Problem rozbudowy sieci

(PC1 – PC5). Wraz z rozwojem firmy, siec była stopniowo rozbudowywana, poprzez dołączanie kolejnych przełączników. Jest to typowy i często spotykany (chociaż nie polecany) model ewolucji sieci lokalnych. W pewnym momencie jej wydajność drastycznie spadła wskutek dużej liczby rozgłoszeń oraz znacznego obciążenia niektórych segmentów (np. między R1 i S1). Problem dotyczył także komputerów PC1 – PC5, które początkowo funkcjonowały w sieci bezproblemowo. Został tu przedstawiony brak pożądanej cechy sieci, jaką jest skalowalność. Polega ona na takim zaprojektowaniu sieci, by była możliwa jej rozbudowa w celu dodania nowych użytkowników, bez pogarszania komfortu pracy dotychczasowych użytkowników.

Wraz z rozbudową sieci, coraz bardziej złożonym zadaniem staje się zarządzanie nią. Przy niewielkiej liczbie urządzeń sieciowych, można łączyć się z każdym z nich, w celu uzyskania informacji o ich stanie i wykonania czynności administracyjnych. W dużych sieciach niezbędne stają się narzędzia dające całościowy obraz sytuacji.

Należy przewidzieć także sposób postępowania w sytuacjach kryzysowych, np. awarii poszczególnych komponentów sieci. Wskazane, chociaż nie zawsze możliwe, jest przewidzenie przyszłych możliwości migracji w kierunku nowych, szybszych technologii. Dobrym przykładem z historii Ethernetu były sieci zbudowane z wykorzystaniem skrętki UTP i koncentratorów. Ich modernizacja była łatwa do przeprowadzenia poprzez wymianę koncentratorów na przełączniki, bez konieczności dokonywania głębszych zmian (przy założeniu, że okablowanie było dobrej jakości, wykonane zgodnie ze standardami). Wskazane jest też, by prace modernizacyjne w jak najmniejszym stopniu zakłócały pracę użytkowników sieci.

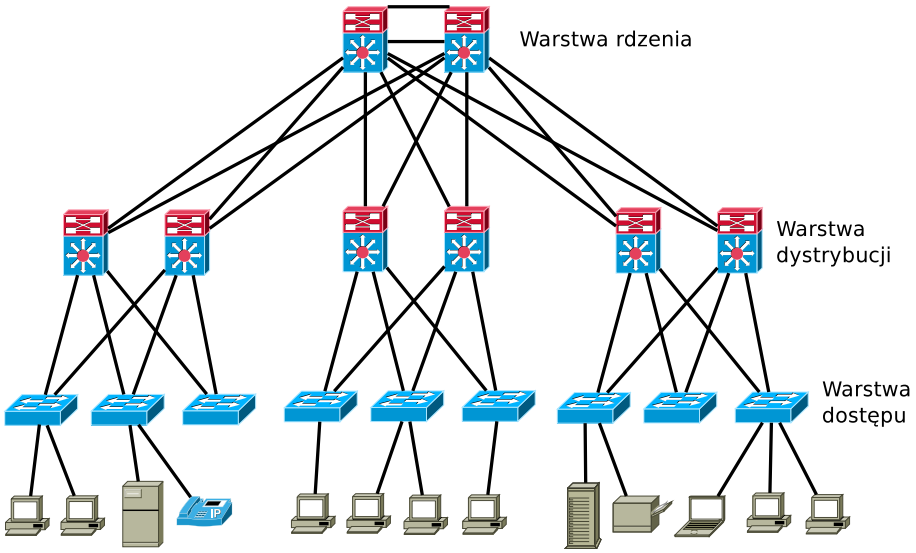
Podsumowując zatem, siec powinna charakteryzować się następującymi cechami:

— odpowiedni poziom dostępności usług dla użytkowników (niezawodność

osiągnięta dzięki nadmiarowym komponentom, wydajność adekwatna do potrzeb),
— skalowalność,
— możliwość sprawnego zarządzania siecią,
— możliwość sprawnego usuwania usterek, wprowadzania zmian, modernizacji,
— bezpieczeństwo (szerzej omówione w rozdziale 7.).

5.2. Hierarchiczny model sieci

Hierarchiczny, trójwarstwowy model sieci (rys. 5.3) powstał w odpowiedzi na problemy przedstawione powyżej. Został on zaproponowany przez Cisco [21], jednak obecnie jest powszechnie przyjęty. Jego zastosowanie służy ułatwieniu projektowania dużych sieci, spełniających między innymi warunek skalowalności.



Rysunek 5.3. Trójwarstwowy, hierarchiczny model sieci

Głównym zadaniem warstwy dostępu (ang. *access layer*) jest umożliwienie dołączenia do sieci urządzeń końcowych: komputerów PC, drukarek sieciowych, telefonów IP, kamer, a także bezprzewodowych punktów dostępowych (WiFi). Stosuje się tu przede wszystkim przełączniki warstwy drugiej (OSI), jednak można spotkać także urządzenia warstwy trzeciej (przełączniki trzeciej warstwy lub routery). Warstwa dostępu powinna zapewniać komunikację w obrębie grupy roboczej. Pakiety przeznaczone do wysłania

poza grupę roboczą są przekazywane wyżej – do warstwy dystrybucji (ang. *distribution layer*). W warstwie dostępu uruchamia się podstawowe mechanizmy bezpieczeństwa, np. zabezpieczenia portów przełącznika (rozdział 7). Mają tu również zastosowanie mechanizmy QoS, a także technologia *Power over Ethernet* (np. do zasilania bezprzewodowych punktów dostępowych). Raczej nie stosuje się natomiast pełnej nadmiarowości. Urządzenia końcowe zwykle są wyposażone w pojedyncze interfejsy sieciowe. Awaria przełącznika, do którego podłączone jest dane urządzenie, prowadzi oczywiście do utraty połączenia sieciowego. Tego typu problemy dotyczą jednak ograniczonej liczby użytkowników, a ponadto powinny być łatwe do wykrycia i szybkiego usunięcia.

Znajdująca się wyżej warstwa dystrybucji zapewnia komunikację pomiędzy grupami użytkowników oraz połączenie z głównym szkieletem sieci (rdzeniem). Jest tu realizowane przełączanie w drugiej i trzeciej warstwie OSI. Konieczne jest zapewnienie odpowiedniej przepustowości, np. poprzez agregację połączeń (skonfigurowanie kilku połączeń fizycznych w jedno logiczne, np. w technologii *EtherChannel* [22], przedstawionej w dalszej części podręcznika). Implementuje się tu również większość mechanizmów bezpieczeństwa, np. listy ACL, firewalle. Istotna jest także kwestia jakości usług (QoS). Ponieważ ewentualna awaria urządzenia z tej warstwy będzie odczuwalna dla dużego obszaru sieci i znacznej liczby użytkowników, niezbędne są nadmiarowe komponenty.

Warstwa rdzenia (ang. *core layer*) stanowi główny szkielet sieci. Jej struktura jest bardzo prosta (w porównaniu z dwiema niższymi warstwami), natomiast prawidłowe funkcjonowanie ma kluczowe znaczenie dla całego przedsiębiorstwa. Warstwa rdzenia zapewnia komunikację np. między poszczególnymi częściami kampusu uniwersyteckiego lub oddziałami firmy, zwykle na poziomie 3 warstwy modelu OSI. Priorytetem jest tu szybkość transmisji oraz niezawodność. Niezbędne są zatem nadmiarowe łącza i urządzenia. Rezygnuje się natomiast, polegając na warstwie dystrybucji, z filtrowania ruchu i innych mechanizmów bezpieczeństwa (chociaż nadal korzysta się z QoS), by nie spowalniać transmisji.

W przypadku sieci niewielkich przedsiębiorstw, wdrożenie pełnego, trójwarstwowego modelu może być bezcelowe i zbyt kosztowne. Można wówczas połączyć funkcje warstwy rdzenia i dystrybucji. Z drugiej strony, w przypadku dużych korporacji (wykorzystujących technologie sieci LAN, ale też WAN, SAN[1]), trójwarstwowa struktura może okazać się niewystarczająca. Rozszerzeniem przedstawionego modelu, dla najbardziej rozbudowanych sieci, jest np. Cisco Enterprise Composite Network Model (ECNM) [23, 24].

[1] ang. *Storage Area Network*, sieć pamięci masowej

5.3. Przełączanie w wyższych warstwach i przełączanie wielowarstwowe

Tradycyjnie termin *przełącznik* odnosi się do urządzenia pracującego w drugiej warstwie modelu OSI. Dzięki sprzętowej realizacji przełączania, przy pomocy wyspecjalizowanych układów elektronicznych (ang. *application-specific integrated circuit*, ASIC), jest ono bardzo wydajne. Ponadto, transmitowany pakiet nie jest w żaden sposób modyfikowany. Przy tzw. przełączaniu przezroczystym (ang. *transparent switching*), nie jest modyfikowana również ramka. W ten sposób działa Ethernet. Zmiana formatu ramki (translacja) występuje tylko w miejscu styku różnych technologii, np. Ethernetu i Token Ring lub WiFi. Największym ograniczeniem technologii przełączania w warstwie drugiej jest brak możliwości segmentacji domen rozgłoszeniowych.

Klasyczny router jest z kolei urządzeniem pracującym w trzeciej warstwie. Ze względu na dużą złożoność i różnorodność wykonywanych operacji (obsługa protokołów routingu, list kontroli dostępu, serwera DHCP i wielu innych funkcji), są one realizowane przez oprogramowanie routera, wykonywane przez typowy mikroprocesor (a więc wolniej niż w przypadku wyspecjalizowanych układów). Tradycyjny routing zapewnia lepszą skalowalność sieci niż przełączanie (w szczególności dzięki separacji domen rozgłoszeniowych), jednak kosztem niższej wydajności.

Celem przełączania w warstwie trzeciej jest połączenie zalet obu powyższych technologii. Przełącznik warstwy trzeciej posiada funkcjonalność routera, lecz operacje przekazywania pakietów są realizowane sprzętowo. Dzięki temu uzyskuje się znacznie lepszą wydajność. Inną korzyścią jest np. możliwość stworzenia sieci VLAN i skonfigurowania routingu między nimi, bez potrzeby stosowania do tego celu oddzielnego routera. Przełączniki warstwy trzeciej zwykle nie posiadają natomiast interfejsów WAN i związanych z tym funkcji. Liczba oferowanych możliwości i sposób ich implementacji różnią się w różnych modelach urządzeń, a jednoznaczne ich sklasyfikowanie bywa problematyczne. Niewątpliwie jednak stopniowo zacierają się różnice między routerami a przełącznikami trzeciej warstwy.

Router, podejmując decyzje o sposobie postępowania z pakietami, może brać pod uwagę również informacje z czwartej warstwy modelu OSI (warstwy transportowej), np. numery portów. Mogą do tego celu być wykorzystywane rozszerzone listy kontroli dostępu (*extended* ACL). Pod pojęciem przełączania w warstwie czwartej rozumiemy sprzętowo zrealizowane przełączanie w warstwie trzeciej, z uwzględnieniem informacji z warstwy czwartej. Znajduje to zastosowanie przy implementacji mechanizmów QoS. Istnieją również przełączniki korzystające z informacji aż do warstwy siódmej.

Bywają one nazywane przełącznikami warstw 4–7 i są stosowane np. do rozdzielania przychodzącego ruchu sieciowego na grupę serwerów.

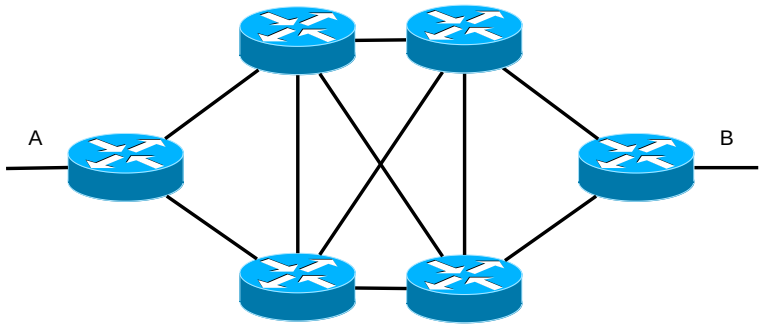
Połączenie powyższych technologii, czyli przełączania w 2, 3 i 4 warstwie, jest określane mianem przełączania wielowarstwowego (ang. *multi-layer switching*, MLS). Dzięki temu uzyskuje się dobrą skalowalność, połączoną z dużą wydajnością i niewielkimi opóźnieniami w sieci. Administrator otrzymuje niezwykle rozbudowane możliwości filtrowania i nadawania priorytetów określonym typom ruchu w sieci, na podstawie wielu kryteriów. Dzięki rozwiązaniom sprzętowym, duża złożoność tego typu operacji nie skutkuje istotnym spadkiem wydajności.

Rozdział 6

Nadmiarowość w sieciach lokalnych

6.1. Wstęp

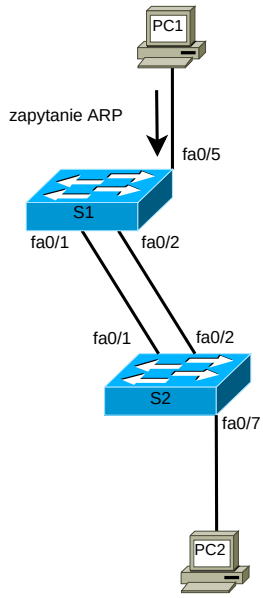
Zgodnie z rozważaniami przedstawionymi w poprzednim rozdziale, w celu zapewnienia odpowiedniego poziomu niezawodności sieci, konieczne jest zastosowanie nadmiarowych komponentów. Przykładowa sytuacja jest przedstawiona na rys. 6.1.



Rysunek 6.1. Nadmiarowe routery w sieci

Po odpowiednim skonfigurowaniu protokołu routingu, wybrana zostanie optymalna trasa między sieciami A i B. Jeżeli stanie się ona nieosiągalna wskutek awarii, automatycznie zastąpi ją trasa alternatywna. W razie popełnienia błędów w konfiguracji lub wystąpienia niekorzystnego zbiegu okoliczności, może wystąpić zjawisko pętli routingu – pakiety będą krążyć między routerami, nigdy nie docierając do celu. Zjawisko to jest oczywiście niepożądane. Istnieje jednak w protokole IP mechanizm umożliwiający eliminowanie z sieci pakietów, które znalazły się w pętli. Przy każdym przejściu przez router, wartość wpisana w nagłówku pakietu, w polu *time to live* (TTL w IPv4) lub *hop limit* dla IPv6 jest zmniejszana o 1. Gdy osiągnie zero, pakiet jest odrzucany.

Inaczej sytuacja wygląda w przypadku segmentu sieci zbudowanego z wykorzystaniem urządzeń 2. warstwy modelu OSI, np. przełączników Ethernet. W sieci z rys. 6.2 przełączniki S1 i S2 zostały połączone dwoma kablami. Załóżmy, że komputer PC1 wyśle ramkę rozgłoszeniową, np. zawierającą zapytanie ARP. Przełącznik S1 wyśle ją poprzez wszystkie aktywne interfejsy, oprócz źródłowego (tzn. poprzez fa0/1 i fa0/2). Przełącznik S2 ramkę otrzymaną poprzez swój interfejs fa0/1 przekaże do fa0/2 i fa0/7, natomiast ramkę otrzymaną poprzez fa0/2 – do fa0/1 i fa0/7. W ten sposób przełącznik S1 otrzyma z powrotem dwie kopie ramki nadanej przez PC1, a następnie roześle je ponownie. Ramki te będą cały czas przesyłane między przełącznikami, z maksymalną możliwą szybkością, utrudniając lub całkowicie uniemożliwiając jakikolwiek inny ruch w sieci. Zjawisko takie nazywamy bu-



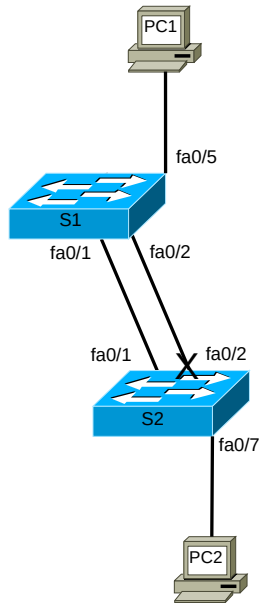
Rysunek 6.2. Nadmiarowe połączenie między przełącznikami

rzą rozgłoszeń. Protokół Ethernet nie ma wbudowanego mechanizmu, który mógłby zatrzymać ten proces. W ramce nie ma odpowiednika pola *time to live*. Konieczne jest przerwanie pętli poprzez rozłączenie jednego z połączeń między przełącznikami, ręcznie lub wskutek zadziałania dodatkowych mechanizmów zaimplementowanych przez producenta urządzenia (mechanizm kontroli burz w przełącznikach Cisco opisany jest w rozdziale 7.).

W przedstawionej sieci problematyczne będzie również przekazywanie ramek unicastowych. Nie będzie możliwe poprawne i jednoznaczne wypełnienie tablic adresów MAC przełączników. Ramki mogą docierać do hostów nieoptymalną drogą, docierać w kilku kopiach, lub nie docierać wcale. Przestawione problemy mogą wystąpić nawet gdy dysponujemy tylko jednym przełącznikiem i zostaną ze sobą połączone dwa jego interfejsy.

Z powyższych przesłanek wynika, że warunkiem poprawnego działania sieci przełączanej jest brak pętli. Wówczas między dwoma dowolnymi miejscami istnieje tylko jedna trasa. Jest to jednak sprzeczne z postulatem posiadania w sieci nadmiarowych połączeń i urządzeń.

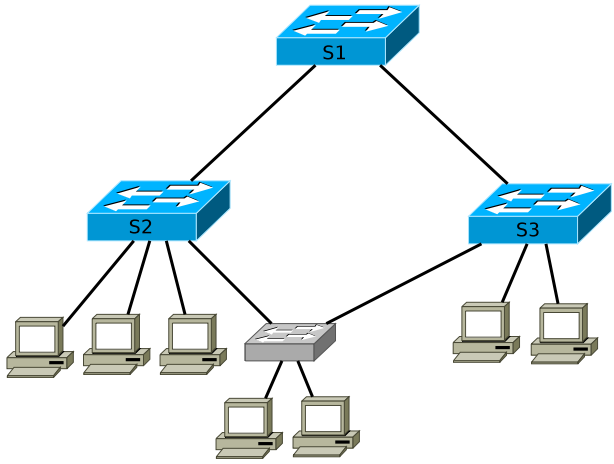
Rozwiązaniem problemu jest skorzystanie z protokołu drzewa rozpinającego (ang. *Spanning Tree Protocol*, STP) [25]. W sieci z nadmiarowymi połączeniami fizycznymi powoduje on automatyczne wyłączenie niektórych interfejsów i stworzenie topologii logicznej bez pętli. W razie awarii działających połączeń lub wystąpienia innej zmiany, topologia jest automatycznie przebudowywana.



Rysunek 6.3. Efekt działania protokołu STP

Wynik działania protokołu STP w sieci z rys. 6.2 przedstawia rys. 6.3. Interfejs fa0/2 przełącznika S2 został zablokowany. Jednak w razie rozłączenia działającego łącza, zostanie on odblokowany, udostępniając alternatywną trasę.

W większości urządzeń obsługujących protokół STP (w tym w przełącznikach Cisco) jest on domyślnie włączony. Zatem, aby zaobserwować opisany powyżej efekt burzy rozgłoszeń, na czas przeprowadzania doświadczenia, STP należy wyłączyć. Protokół ten jest niezwykle skomplikowany. W implementacjach poszczególnych producentów sprzętu występują także dodatkowe funkcje wykraczające poza standard. Wiele problemów występujących w sieciach lokalnych wynika z błędów w konfiguracji lub niezrozumienia niuansów protokołu STP. Mimo to, z STP nie należy rezygnować, nawet mając pewność, że w danej sieci połączenia nadmiarowe nie występują. Połączenie takie może zostać przypadkowo zestawione przez administratora, lecz także użytkowników sieci, np. poprzez połączenie dwóch gniazd Ethernet kablem lub w sposób przedstawiony na rys. 6.4. Mały przełącznik bez oznaczenia został zainstalowany przez użytkowników, bez wiedzy administratora.



Rysunek 6.4. Ryzyko powstania pętli wskutek niekontrolowanej działalności użytkowników

6.2. Podstawy działania protokołu STP

STP jest protokołem warstwy łącza danych. Podstawową i najpopularniejszą jego odmianę opisywał standard IEEE 802.1d (przed zastąpieniem STP protokołem RSTP) [25], chociaż występuje wiele innych implementacji. Działanie opiera się na algorytmie drzewa rozpinającego, stworzonym przez Radię Perlman [26], podczas pracy dla Digital Equipment Corporation (DEC). Połączone ze sobą przełączniki traktowane są jak węzły grafu. W kontekście protokołu STP, zwykle używa się pojęcia mostu (*bridge*) a nie przełącznika, ze względów historycznych (i w bieżącym rozdziale można traktować je zamiennie). Celem algorytmu jest wyznaczenie wolnych od pętli tras prowadzących od poszczególnych przełączników, do jednego wybranego, stanowiącego korzeń drzewa, charakteryzujących się minimalną wartością kosztu. Połączenia, które są nadmiarowe zostają wyłączone.

Każdy przełącznik obsługujący protokół STP musi posiadać swój ośmiobajtowy identyfikator – *bridge ID* (BID), którym podpisywane są komunikaty BPDU (ang. *Bridge Protocol Data Unit*) wymieniane między przełącznikami. Na dwóch najbardziej znaczących bajtach zakodowany jest priorytet przełącznika (*bridge priority*). Zgodnie z konwencją przyjętą w STP, niższa wartość liczbowa oznacza wyższy stopień preferencji. Kolejnych sześć bajtów wypełnia podstawowy adres MAC przełącznika.

Tabela 6.1 przedstawia format komunikatu konfiguracyjnego BPDU (*Configuration BPDU*, CBPDU), wykorzystywanego przy budowie drzewa (z oryginalnymi, anglojęzycznymi nazwami pół). Komunikaty BPDU wysyłane są na zarezerwowany dla STP adres multicastowy 01:80:C2:00:00:00. Komuni-

Tabela 6.1. Format konfiguracyjnego komunikatu BPDU [25]

Nazwa pola	Bajty
Protocol Identifier	1 2
Protocol Version Identifier	3
BPDU Type	4
Flags	5
Root Identifier	6 7 8 9 10 11 12 13
Root Path Cost	14 15 16 17
Bridge Identifier	18 19 20 21 22 23 24 25
Port Identifier	26 27
Message Age	28 29
Max Age	30 31
Hello Time	32 33
Forward Delay	34 35

katy BPDU typu TCN (ang. *Topology Change Notification*) służą do informowania o zmianie topologii sieci, natomiast TCA (ang. *Topology Change Notification Acknowledgment*) są wysyłane jako potwierdzenie otrzymania wiadomości TCN. Komunikaty BPDU domyślnie wysyłane są co 2 sekundy (*hello time*).

Budowa wolnej od pętli topologii odbywa się jest w trzech etapach:

1. Spośród wszystkich przełączników wybierany jest główny most (ang. *root bridge*).
2. Każdy przełącznik, oprócz mostu głównego, spośród swoich interfejsów wybiera jeden port główny (ang. *root port*), poprzez który ramki będą wysyłane w kierunku mostu głównego.
3. Dla każdego segmentu sieci wybierany jest port desygnowany, poprzez który ramki z tego segmentu będą wysyłane w kierunku mostu głównego.

Początkowym i kluczowym dla optymalnego działania sieci etapem działania protokołu STP jest wybór przełącznika (mostu) głównego, stanowiącego korzeń drzewa – centralny punkt sieci (STP *root*). Staje się nim przełącznik posiadający najniższy co do wartości identyfikator *bridge ID*. W przypadku identycznych wartości priorytetów, o wyborze decyduje adres MAC, czyli praktycznie wybór jest przypadkowy. Początkowo każdy przełącznik uważa samego siebie za korzeń i w rozsyłanych komunikatach BPDU umieszcza swój identyfikator w polu *Root Identifier*. Po otrzymaniu od sąsiednich przełączników informacji o istnieniu przełącznika z niższą wartością identyfikatora, jest to weryfikowane i już po chwili przełącznik główny powinien być poprawnie rozpoznany. W kolejnych krokach poszukiwane będą optymalne trasy prowadzące od poszczególnych przełączników do głównego, a nadmiarowe zostaną zablokowane.

Koszt trasy jest sumą algebraiczną kosztów poszczególnych odcinków i zależy od przepustowości łącz. Tabela 6.2 przedstawia domyślne wartości. Ulegały one zmianom ze względu na ewolucję technologii sieciowych i pojawienie się przepustowości, których wcześniej nie przewidziano.

Wybór mostu głównego ma istotne znaczenie. Rys. 6.5 przedstawia przykładową sytuację. Skutkiem wybrania przełącznika S1 jako głównego jest zablokowanie bezpośredniego połączenia między S2 i S3, ponieważ ten segment nie jest elementem najkrótszej (w sensie kosztu) trasy od S2 do S1 ani od S3 do S1. Na rys. 6.6 przełącznikiem głównym jest S3. Wyłączone zostało połączenie między S1 i S2. Wskutek tego, dane wysyłane poza własną sieć przez komputery dołączone do S2, są transmitowane nieoptymalną trasą poprzez trzy przełączniki.

Rolę przełącznika głównego powinno pełnić urządzenie faktycznie znajdujące się w centrum sieci. Najlepiej, jeżeli jest to jeden z przełączników stanowiących szkielet sieci, do którego nie są dołączone urządzenia końco-

Tabela 6.2. Domyślne wartości kosztu w protokole STP

Szybkość łącza	Koszt 802.1d – 1998	Koszt 802.1d – 2004
4 Mb/s	250	5000000
10 Mb/s	100	2000000
16 Mb/s	62	1250000
100 Mb/s	19	200000
1 Gb/s	4	20000
2 Gb/s	3	10000
10 Gb/s	2	2000
100 Gb/s		200
1 Tb/s		20
10 Tb/s		2

we. Administrator przesądza o wyborze przełącznika głównego konfigurując priorytet o wartości niższej niż priorytety pozostałych urządzeń.

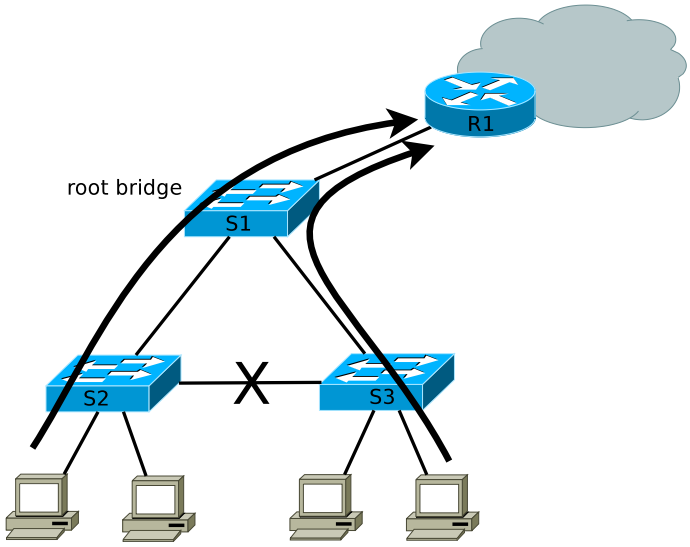
W drugim etapie każdy przełącznik, oprócz głównego, poszukuje najkrótszej (tzn. charakteryzującej się najniższą wartością kosztu) trasy prowadzącej do przełącznika głównego. Port, poprzez który prowadzi ta trasa uzyskuje rolę portu głównego (ang. *root port*, RP).

W sytuacji przedstawionej na rys. 6.7, wszystkie przełączniki mają identyczne wartości priorytetu, więc głównym przełącznikiem stał się S1, natomiast przełączniki S2 i S3 muszą wybrać swoje porty główne. S3 dysponuje połączeniem bezpośrednim z S1 (niższy koszt) oraz trasą poprzez S2 (wyższy koszt), więc wybór portu głównego jest oczywisty. Spośród trzech tras do S1, którymi dysponuje przełącznik S2, dwie charakteryzują się jednakowym kosztem. Potrzebne są więc dodatkowe kryteria wyboru portów.

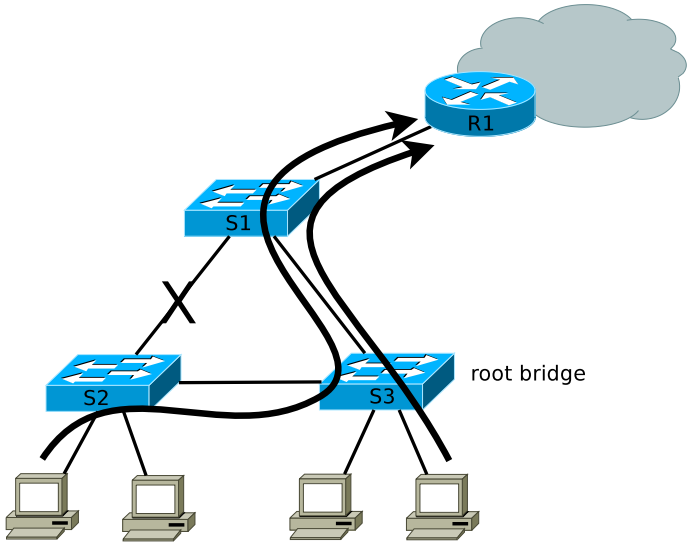
Ogólna sekwencja podejmowania decyzji w protokole STP jest następująca:

1. Najniższa wartość BID.
2. Najniższy koszt trasy do przełącznika głównego.
3. Najniższy BID nadawcy.
4. Najniższy priorytet portu.
5. Najniższy identyfikator portu.

Wracając do przykładu z rys. 6.7 i problemu wyboru portu głównego przez S2, pierwszy krok sekwencji podejmowania decyzji nie ma tu zastosowania (był użyty wcześniej, przy wyborze przełącznika głównego). Krok drugi pozwolił wyeliminować port łączący z S3, ze względy na wyższy koszt trasy. Najniższy BID nadawcy (krok trzeci) również nie rozwiąże problemu, ponieważ w przypadku obu tras nadawcą jest ten sam przełącznik S1. W piątym kroku o wyborze portu głównego przez S2 mogą zdecydować priorytety portów STP skonfigurowane przez administratora na przełączniku S1. Jeżeli



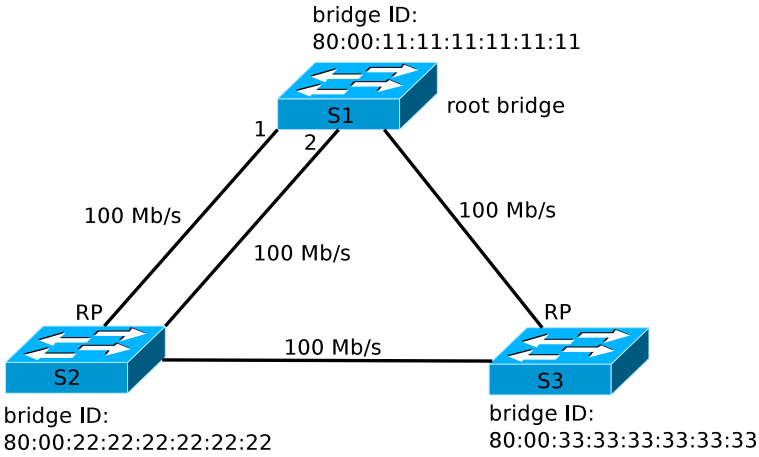
Rysunek 6.5. Poprawny wybór przełącznika – korzenia



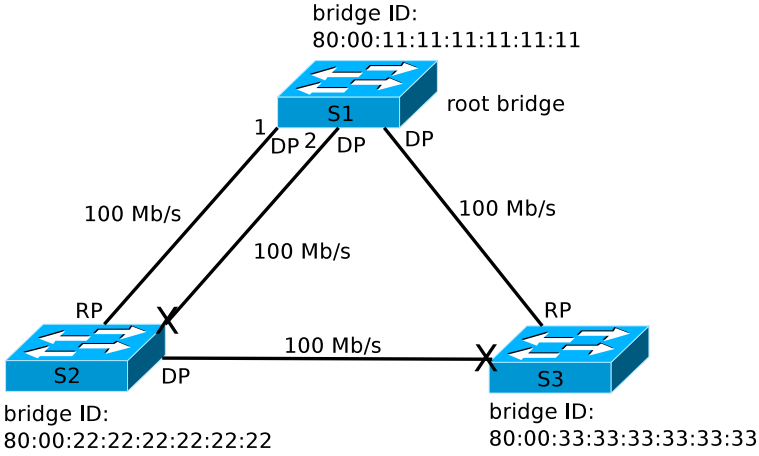
Rysunek 6.6. Nieoptymalny wybór przełącznika – korzenia

ich wartości są jednakowe (np. domyślne), preferowane są porty o niższych identyfikatorach, czyli fa0/1 zostanie wybrany przed fa0/2. Przełącznik S2 jako port główny wybierze ostatecznie interfejs, który połączy go z portem przełącznika S1 o niższym identyfikatorze.

Po wybraniu portów głównych, dla każdego segmentu sieci (tzn. odcin-



Rysunek 6.7. Wybór portów głównych

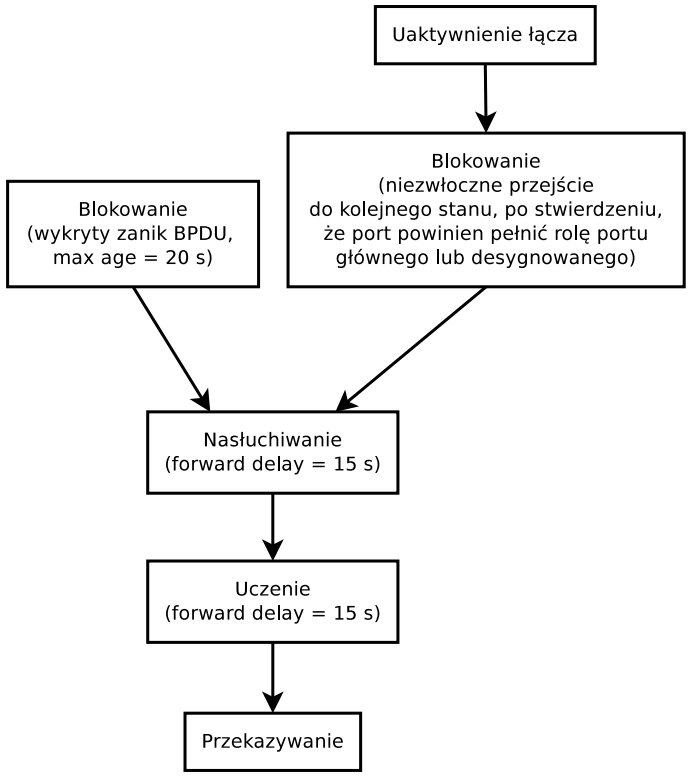


Rysunek 6.8. Wybór portów desygnowanych

ka łączącego przełączniki lub przełącznik i urządzenie końcowe) wybierany jest jeden port desygnowany (ang. *designated port*, DP), poprzez który ramki z tego segmentu będą przesyłane w kierunku portu głównego (rys. 6.8). Przy wyborze obowiązuje podana powyżej sekwencja podejmowania decyzji. W przypadku segmentów łączących S1 i S2 oraz S1 i S3, o wyborze przesądza kryterium najniższego kosztu trasy do S1. W segmencie łączącym S2 i S3, oba porty zapewniają identyczny koszt trasy do przełącznika głównego. Zgodnie z trzecim krokiem sekwencji decyzyjnej, preferowana będzie trasa prowadząca przez przełącznik o niższym identyfikatorze BID (czyli S2).

Porty, które nie uzyskały roli głównych ani desygnowanych zostają za-

blokowane – nie transmitują ramek użytkowników. Na na rys. 6.8 zostały oznaczone znakiem `X`. Sytuacja jest jednak stale monitorowana przy pomocy periodycznie rozsyłanych ramek BPDU i w razie potrzeby topologia zostanie przebudowana.



Rysunek 6.9. Diagram przejść między stanami portów w STP, od blokowania do przekazywania

Port przełącznika nie może przystąpić do przekazywania ramek natychmiast po jego uaktywnieniu, gdyż groziłoby to powstawaniem pętli. Konieczne jest przejście przez sekwencję kolejnych stanów, zgodnie ze schematem z rys. 6.9.

1. W stanie blokowania (ang. *blocking*) port nie przekazuje ramek użytkowników. Odbiera jedynie komunikaty BPDU, nie wysyłając własnych. Podczas stabilnej pracy sieci w tym stanie znajdują się porty, które nie uzyskały roli portów głównych ani desygnowanych. Ze stanem blokowania związany jest parametr czasowy *max age* (domyślnie 20 sekund). Jest to maksymalny czas przechowywania komunikatu BPDU, po którym jest on odrzucany. Jeżeli port przestanie otrzymywać komunikaty BPDU z danego źródła, oznacza to, że nastąpiła zmiana topologii sie-

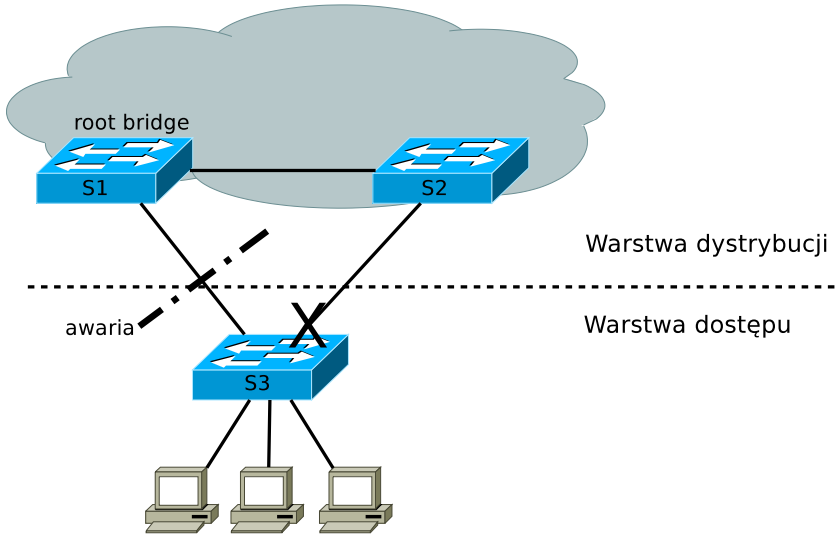
ci, na którą musi odpowiednio zareagować protokół STP. Port przebywa w stanie blokowania przez czas *max age* w przypadku awarii w odległych segmentach sieci. W razie zmian dotyczących bezpośrednio jego interfejsów, przejście ze stanu blokowania do kolejnego następuje natychmiast.
2. W stanie nasłuchiwania (ang. *listening*) przełącznik nadal przetwarza komunikaty BPDU i w razie wystąpienia stosownych przesłanek może powrócić do stanu blokowania. Po czasie określonym parametrem *forward delay* (domyślnie 15 sekund) port przechodzi do kolejnego stanu.
3. W stanie uczenia (ang. *learning*) port przygotowuje się do przekazywania ramek użytkowników poprzez prowadzenie nasłuchu i wypełnianie tablicy adresów MAC. Czas przebywania w tym stanie, podobnie jak w poprzednim, określa parametr *forward delay*.
4. W stanie przekazywania (ang. *forwarding*) port przekazuje ramki użytkowników. Jednocześnie wysyła własne i monitoruje przychodzące komunikaty BPDU, by w razie potrzeby powrócić do stanu blokowania, zapobiegając powstaniu pętli. Jest to docelowy stan dla portów pełniących role portów głównych lub desygnowanych.
5. Porty, które nie działają z powodu działań administratora (w przypadku urządzeń Cisco, zostały wyłączone poleceniem `shutdown`), z punktu widzenia protokołu STP znajdują sie w stanie wyłączonym (ang. *disabled*).

6.3. Rapid Spanning Tree Protocol (RSTP)

Domyślne wartości parametrów czasowych STP (*hello time*, *max age*, *forward delay*) zostały tak dobrane, by zapewnić stabilną pracę sieci o średnicy nie większej niż 7 [27]. Pod pojęciem średnicy (ang. *diameter*) rozumiemy maksymalną liczbę przełączników, które musi przebyć ramka na drodze między dwoma dowolnymi punktami sieci. Ze schematu przedstawionego na rys. 6.9 wynika, że osiąganie stanu konwergencji może trwać niemal minutę. W tym czasie transmisja ramek użytkowników może nie być możliwa. Problematyczne może być np. korzystanie przez hosty z protokołu DHCP. Jeżeli przez 30 sekund od chwili włączenia komputera port przełącznika będzie niedostępny (w stanie nasłuchiwania i uczenia), host może nie uzyskać adresu IP od serwera DHCP. W przełącznikach Cisco dostępna jest funkcja *PortFast* [28], której włączenie dla interfejsu przeznaczonego do podłączenia urządzeń końcowych skutkuje natychmiastowym przejściem do stanu przekazywania. Jednocześnie jednak, ze względów bezpieczeństwa, powinien zostać uruchomiony mechanizm weryfikacji, czy faktycznie do portu dołączony jest host, a nie kolejny przełącznik (np. zainstalowany bez wiedzy administratora, w sposób pokazany wcześniej na rys. 6.4). Przełączniki Cisco oferują funkcję BPDU *guard* (strażnik BPDU) [29], która w razie wykrycia

komunikatu BPDU wchodzącego do interfejsu z włączonym mechanizmem *PortFast* spowoduje jego zablokowanie.

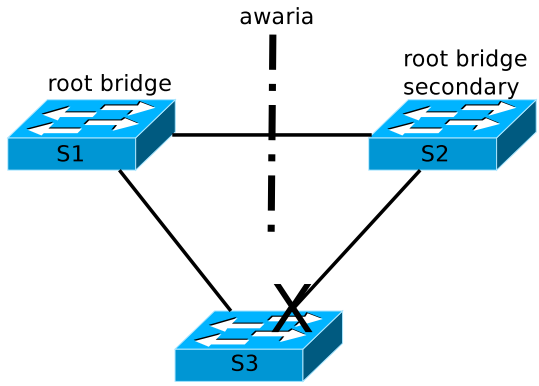
Problem protokołu DHCP ma zatem stosunkowo proste rozwiązanie, jednak również w innych sytuacjach kilkudziesięciosekundowe przerwy w poprawnym działaniu sieci mogą być nieakceptowalne (chociaż w czasie gdy standard powstawał, zapewne nie stanowiło to problemu). W sieci o mniejszej średnicy można zmniejszyć wartości parametrów czasowych, by przyspieszyć osiąganie stanu konwergencji [30], ale dobranie optymalnych wartości wymaga doświadczenia. Uzyskane czasy konwergencji, rzędu kilkunastu sekund, nadal mogą być nieakceptowalne.



Rysunek 6.10. Przykład zastosowania funkcji *Uplink Fast*

Kolejną funkcją dodatkową, wprowadzoną do STP przez Cisco jest *Uplink Fast* [31]. W sytuacji przedstawionej na rys. 6.10, przełącznik warstwy dostępu S3 dysponuje dwoma połączeniami z warstwą dystrybucji. Połączenie nadmiarowe, oznaczone znakiem `X`, zostało zablokowane przez protokół STP. W razie gdy przełącznik S3 stwierdzi utratę dotychczas wykorzystywanego połączenia, mając uruchomioną funkcję *Uplink Fast*, może natychmiast (w czasie poniżej 1 sekundy) uruchomić port zapewniający najlepszą spośród dostępnych tras do przełącznika głównego, łamiąc procedury STP poprzez pominięcie standardowej sekwencji stanów. W tej sytuacji problemem przedłużającym faktyczny czas osiągania stanu konwergencji, może być zawartość tablic adresów MAC przełączników S1 i S2, adekwatna do sytuacji sprzed awarii. Dlatego przełącznik S3 wyśle specjalne ramki multicastowe

z podstawionymi adresami źródłowymi dołączonych do niego hostów, by wymusić aktualizację tablic.



Rysunek 6.11. Przykład zastosowania funkcji *Backbone Fast*

Funkcja *Uplink Fast* ma zastosowanie tylko gdy awaria dotyczy łącza bezpośrednio dołączonego do przełącznika (ang. *direct link failure*). Z kolei funkcja *Backbone Fast* (również autorstwa Cisco) [32] przyspiesza osiąganie stanu konwergencji w przypadku awarii odległych łącz (ang. *indirect link failure*). Przykładową sytuację przedstawia rys. 6.11. S1 pełni rolę przełącznika głównego. W razie jego ewentualnej awarii, stałby się nim S2. W wyniku awarii łącza zaznaczonego na rysunku, przełącznik S2 przestanie otrzymywać komunikaty BPDU od przełącznika głównego, ponieważ zablokowany port przełącznika S3 ich nie wysyła. W związku z tym, S2 stwierdzi, że powinien przejąć rolę głównego przełącznika i informacja o tym pojawi się w komunikatach BPDU wysyłanych przez niego do S3 (jak wcześniej wspomniano, w stanie blokowania port odbiera komunikaty BPDU ale ich nie wysyła). S3 będzie w tej sytuacji otrzymywał sprzeczne komunikaty BPDU – oba sąsiednie urządzenia będą podawać się za główny przełącznik. Przy standardowej implementacji STP, S3 będzie ignorował komunikaty STP pochodzące od S2 przez czas określony parametrem *max age*. Po upłynięciu tego czasu, S3 przełączy dotychczas zablokowany port do stanu nasłuchiwania, co umożliwi komunikatom BPDU z poprawnym *Root Id* dotarcie do S2, który z kolei natychmiast zrezygnuje z roli przełącznika głównego. Port przełącznika S3 po przejściu przez stan nasłuchiwania i uczenia, co potrwa dwukrotną wartość parametru *forward delay*, przełączy się do stanu przekazywania. Przy domyślnych ustawieniach, sieć będzie potrzebowała 50 sekund do osiągnięcia stanu konwergencji.

Funkcja *Backbone Fast* wprowadza mechanizm wykrywania awarii odległych łącz poprzez śledzenie specjalnego typu komunikatów BPDU, informujących o awarii bezpośrednio przyłączonych łącz innych przełączników

oraz poprzez mechanizm pozwalający na sprawdzenie poprawności przechowywanych informacji BPDU przy pomocy wysłanych zapytań (ang. *Root Link Query*, RLQ). Pozwala to "zaoszczędzić" przełącznikowi czas równy parametrowi *max age* (zwykle 20 sekund), wskutek zaniechania pasywnego oczekiwania w stanie blokowania.

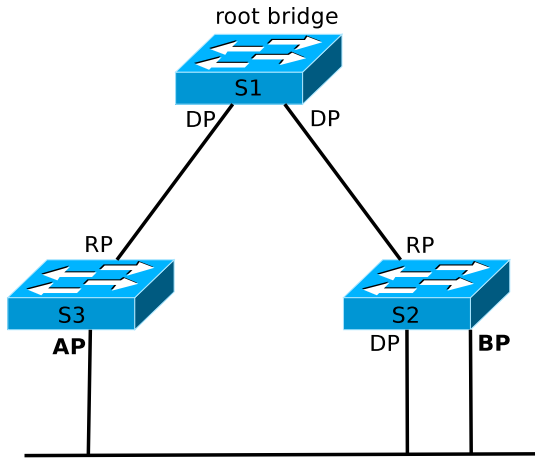
W 2001 roku został opublikowany standard 802.1w – *Rapid Spanning Tree Protocol*, następca zwykłego STP opisanego w 802.1d-1998. Główne zasady funkcjonowania protokołu pozostały niezmienione, podobnie jak znaczenie większości parametrów konfiguracyjnych. Wprowadzone modyfikacje o charakterze ewolucyjnym miały na celu skrócenie czasu osiągania stanu konwergencji, do co najwyżej kilku sekund. Modyfikacje te w większości przypadków sprowadzały się do zaadaptowania rozszerzeń uprzednio wprowadzonych przez producentów sprzętu, np. *Uplink Fast*, *Backbone Fast* i *Port Fast* [33]. Dzięki wprowadzeniu ich do standardu, stały się uniwersalne. Uproszczono również, lub nawet wyeliminowano całkowicie, potrzebę ich konfigurowania. Zachowano też wsteczną zgodność z STP, w celu umożliwienia współpracy nowych urządzeń ze starymi, która oczywiście wiąże się z utratą korzyści wynikających z nowszego protokołu. W roku 2004 standard 802.1w został włączony do nowej wersji 802.1d-2004 i RSTP oficjalnie zastąpił STP.

Tabela 6.3. Stany portów w STP i RSTP

STP	RSTP
wyłączony (*disabled*)	odrzucanie (*discarding*)
blokowanie (*blocking*)	odrzucanie (*discarding*)
nasłuchiwanie (*listening*)	odrzucanie (*discarding*)
uczenie (*learning*)	uczenie (*learning*)
przekazywanie (*forwarding*)	przekazywanie (*forwarding*)

Najważniejsze modyfikacje wprowadzone w RSTP dotyczą przedefiniowania stanów i ról portów. W STP wyróżnia się pięć stanów, przy czym analizując funkcjonalne działanie sieci, porty w stanie blokowania i nasłuchiwania zachowują się identycznie, tzn. nie przekazują ramek użytkowników i nie uczą się adresów MAC urządzeń. W RSTP pozostawiono tylko trzy stany: odrzucania, uczenia i przekazywania. Ilustruje to tabela 6.3. W urządzeniach Cisco, w odniesieniu do stanu odrzucania, nadal jest używane pojęcie blokowania [33].

W RSTP dodano nowe role portów. Porty główne i desygnowane funkcjonują identycznie jak w STP i są wybierane zgodnie z tymi samymi zasadami (tzn. omówioną już sekwencją decyzji STP). Dokonano natomiast dodatkowego rozróżnienia ról portów blokowanych. Porty, które nie uzyskały roli głównych ani desygnowanych, pełnią rolę zapasowych (ang. *backup*) albo alternatywnych (ang. *alternate*).



Rysunek 6.12. Role portów w RSTP (DP – desygnowany, RP – główny, BP – zapasowy, AP – alternatywny)

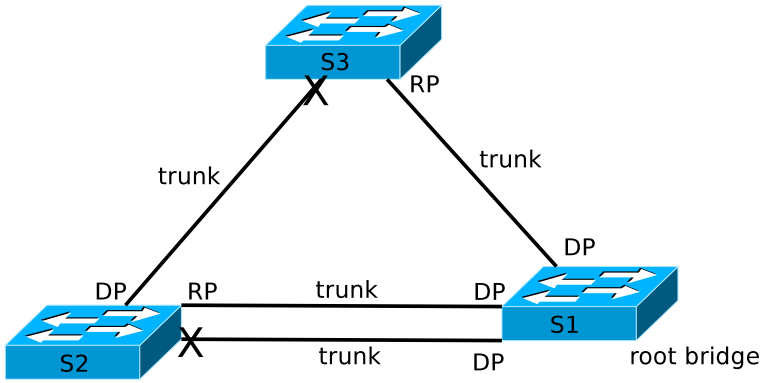
W sieci z rys. 6.12, porty główne (RP) i desygnowane (DP) zostały wybrane identycznie jak w STP. Port zapasowy (BP) i port desygnowany dolnego segmentu sieci oferują tę samą trasę do przełącznika głównego i są to porty tego samego przełącznika. Port desygnowany został wybrany zgodnie ze standardową sekwencją wyboru, więc musiał charakteryzować się niższą wartością priorytetu lub niższym identyfikatorem. W razie awarii portu desygnowanego, port zapasowy powinien przejąć jego rolę. Trasa oferowana przez port zapasowy byłaby jednak bezużyteczna w razie utraty połączenia S1–S2. Wówczas należy uruchomić port alternatywny (AP), oferujący alternatywną (mniej preferowaną) trasę z dolnego segmentu sieci do przełącznika głównego.

Przyspieszenie procesu przechodzenia portów do docelowego stanu przekazywania jest związane z pojęciem portów brzegowych (ang. *edge ports*) oraz typu łącza (ang. *link type*). Port brzegowy jest to port, do którego dołączony jest host, w związku z czym możne on natychmiast przejść do stanu przekazywania, bez ryzyka powstania pętli. Mechanizm ten jest bezpośrednim odpowiednikiem funkcji *PortFast*, wprowadzonej do STP przez Cisco.

Pod pojęciem typu łącza w kontekście RSTP, kryją się połączenia typu punkt-punkt (ang. *point-to-point*) lub współdzielone (ang. *shared*). Jedynie połączenia typu punkt-punkt są kandydatami do szybkiego przejścia do stanu przekazywania. Typ łącza można skonfigurować samodzielnie. Domyślnie połączenia pracujące w trybie pełnego dupleksu traktowane są jako punkt-punkt, natomiast pracujące w trybie półdupleksu – jako współdzielone.

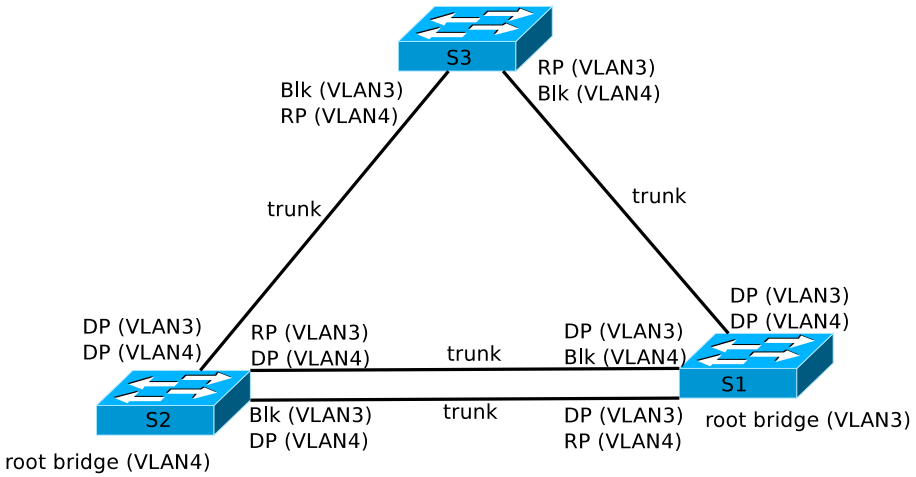
6.4. Inne rozszerzenia STP

Wspominany już standard 802.1q definiuje nie tylko opisany w poprzednich rozdziałach sposób komunikacji poprzez połączenia trunk. Przewiduje także funkcjonowanie jednego, wspólnego drzewa rozpinającego (*Common Spanning Tree*, CST), niezależnie od liczby sieci VLAN. Rozwiązanie to nie obciąża w dużym stopniu procesorów przełączników, jednak ma istotne wady. Załóżmy, że w przełącznikach z rys. 6.13 wykorzystywanych jest kilka sieci VLAN. Rozwiązanie, w którym przy dostępności dwóch połączeń trunk między przełącznikami S1 i S2, wszystkie sieci VLAN korzystają z jednego, jest zdecydowanie nieoptymalne.



Rysunek 6.13. Wspólne drzewo rozpinające dla wszystkich sieci VLAN (CST)

Cisco wprowadziło własne rozszerzenie protokołu – *Per-VLAN Spanning Tree* (PVST lub PVSTP). Polega ono na tym, że dla każdej sieci VLAN budowane jest oddzielne drzewo. Możliwe jest zatem stworzenie konfiguracji, w której te same porty pełnią różne role STP w różnych sieciach VLAN, lepiej wykorzystując dostępne łącza (rys. 6.14). PVST korzysta z połączeń trunk z enakpsulacją ISL. Nowszy wariant – PVST+ (lub PVSTP+) oferuje tę samą funkcjonalność co PVST, korzystając z 802.1q (co nie zmienia faktu, że pozostaje protokołem własnościowym Cisco). Ten wariant STP



Rysunek 6.14. Przykładowa implementacja PVSTP

jest ustawieniem domyślnym większości przełączników Cisco. Bazuje on na starej wersji 802.1d z rozszerzeniami Cisco (*BackboneFast*, *UplinkFast*, *PortFast*). Oczywistą kontynuacją rozwoju rozwiązań Cisco jest *rapid* PVST+, zbudowany na bazie IEEE 802.1w [34].

Przy dużej liczbie sieci VLAN i budowaniu oddzielnego drzewa dla każdej z nich, może wystąpić problem skalowalności. Poza tym, zazwyczaj nie ma sensu budowanie więcej niż kilku topologii logicznych. Można więc zdefiniować grupy sieci VLAN i uruchomić oddzielne instancje STP dla każdej grupy (a nie dla każdej sieci VLAN, jak poprzednio). Implementacja Cisco nosi nazwę *Multiple Instances Spanning Tree Protocol* (MISTP) [35]. Podobny mechanizm, opracowany następnie przez IEEE – MST (*Multiple Spanning Tree*) lub MSTP (*Multiple Spanning Tree Protocol*) jest standardem 802.1s, włączonym następnie do IEEE 802.1q-2005 [36]. MST zachowuje zgodność z RSTP. Przełącznik RSTP, odbierając komunikat MSTP BPDU interpretuje go jak zwykły komunikat RSTP BPDU, traktując grupę przełączników obsługujących MSTP jak pojedynczy przełącznik.

Kolejnym rozszerzeniem Cisco, związanym z bezpieczeństwem STP, jest funkcja *root guard* [37]. Administrator sieci, w której działa STP, powinien świadomie wpłynąć na wybór przełącznika głównego, poprzez odpowiednie ustawienie priorytetów. Jednak w razie pojawienia się w sieci przełącznika z niższą wartością priorytetu (lub identycznym priorytetem jak przełącznik główny, lecz niższą wartością adresu MAC), może on w niekontrolowany sposób przejąć rolę przełącznika głównego. Funkcja *root guard* umożliwia uniknięcie takiej sytuacji. Port przełącznika, na którym została ona uruchomiona może być tylko portem desygnowanym (typowo wszystkie porty

przełącznika głównego są desygnowane). W razie otrzymania komunikatu BPDU informującego o istnieniu przełącznika bardziej preferowanego, port taki jest przełączany do stanu *root-inconsistent*, podobnego do stanu nasłuchiwania, uniemożliwiając zmianę lokalizacji przełącznika głównego.

Celem publikacji kolejnych wersji standardów IEEE, dotyczących protokołu STP/RSTP, jest (jak w przypadku każdego standardu) zapewnienie bezproblemowej współpracy urządzeń różnych producentów (ang. *interoperability*). Rozwój STP w ostatnich latach był dość dynamiczny. Poszczególni producenci wprowadzali i nadal wprowadzają własne modyfikacje. Następnie niektóre z nich, w oryginalnej lub zmodyfikowanej formie, stają się częścią standardu. Należy wziąć to pod uwagę w razie konieczności łączenia przełączników różnych producentów, lub nawet tego samego producenta, ale różnych generacji. O ile podstawowe mechanizmy powinny działać, skonfigurowanie bardziej zaawansowanych funkcji może być problematyczne. Należy zatem zapoznać się z dokumentacją odnośnie implementacji istotnych elementów standardu.

6.5. Podstawowa konfiguracja STP

Jak już wspomniano powyżej, protokół STP jest domyślnie włączony i działa w wariancie PVST+ (Cisco). W razie potrzeby wyłącza się go poleceniem [38]:

```
no spanning-tree vlan vlan-id
```

wydanym w trybie konfiguracji globalnej. Powyższe polecenie oraz znaczna część prezentowanych dalej, odnosi się do konfiguracji STP dla konkretnej sieci VLAN i wymaga podania jej identyfikatora (*vlan-id*) jako parametru.

Tryb pracy STP można zmienić poleceniem:

```
spanning-tree mode pvst | mst | rapid-pvst
```

Alternatywne opcje: `pvst`, `mst` lub `rapid-pvst` oznaczają PVST+, MSTP i rapid PVST+, odpowiednio. Zagadnienie dotyczące MSTP wykraczają poza zakres tego podręcznika.

Wartość priorytetu przełącznika (*bridge priority*, domyślnie 32768) zmienia się poleceniem:

```
spanning-tree vlan vlan-id priority wartość
```

Jednak, aby samodzielnie wymusić określone położenie przełącznika głównego, znacznie wygodniejsze od bezpośredniego modyfikowania priorytetów jest użycie polecenia:

```
spanning-tree vlan vlan-id root primary
```

na przełączniku, który ma pełnić role głównego oraz:

```
spanning-tree vlan vlan-id root secondary
```

na przełączniku, który miałby przejąć tę rolę w razie awarii głównego. Użycie powyższych dwóch poleceń spowoduje automatyczne dobranie odpowiednich wartości priorytetów (o ile jest to możliwe i priorytety pozostałych przełączników nie mają już zbyt niskich wartości).

Wartość priorytetu portu dla danej sieci VLAN można zmienić w trybie konfiguracji interfejsu poleceniem:

```
spanning-tree vlan vlan-id port-priority wartość
```

Wartością domyślną jest 128. Może ona być zmieniana w zakresie od 0 do 240 co 16, tzn. 0, 16, 32, ..., 240.

Funkcję *PortFast* włącza się w trybie konfiguracji globalnej dla wszystkich portów dostępowych poleceniem:

```
spanning-tree portfast default
```

Można oczywiście również użyć odpowiednich poleceń w ustawieniach konfiguracyjnych poszczególnych interfejsów, tak by funkcja ta była aktywna tylko na wybranych interfejsach przeznaczonych dla urządzeń końcowych. Domyślnie wyłączoną funkcję *BPDU guard* dla portów, na których uruchomiono *PortFast* aktywuje się poleceniem:

```
spanning-tree portfast bpduguard default
```

Podstawowym poleceniem diagnostycznym STP jest:

```
show spanning-tree {vlan vlan-id}
```

W razie niepodania opcjonalnego parametru `vlan`, wyświetlone zostaną informacje o konfiguracji STP we wszystkich sieciach VLAN. Ponadto, dostępne są polecenia:

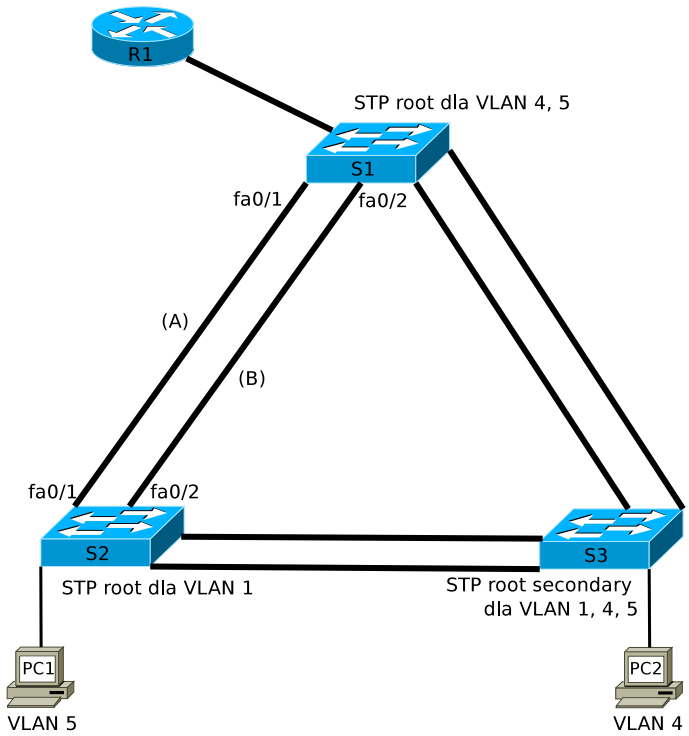
```
show spanning-tree active
```

wyświetlające tylko informacje dotyczące aktywnych interfejsów oraz:

```
show spanning-tree detail
show spanning-tree interface interface-id
show spanning-tree summary
```

6.6. Zadania

6.6.1. Zadanie 1



Rysunek 6.15. Schemat topologii logicznej sieci

Celem zadania jest uruchomienie sieci przedstawionej na rys. 6.15) i skonfigurowanie protokołu STP zgodnie z zaleceniami podanymi na rysunku oraz poniżej.

1. Połącz sieć zgodnie ze schematem (rys. 6.15).
2. Wszystkie połączenia między przełącznikami oraz między przełącznikiem i routerem skonfiguruj jako trunk.
3. Stwórz sieci VLAN nr 4 i 5 i nadaj im dowolne nazwy. Skorzystaj z protokołu VTP w celu zachowania spójności konfiguracji VLAN.
4. Skonfiguruj router R1 tak, aby była możliwa komunikacja między VLAN 4 i VLAN 5. Sprawdź łączność między PC1 i PC2.
5. Skonfiguruj STP tak, by S1 był przełącznikiem głównym dla VLAN 4 i 5, S2 dla VLAN 1, a S3 – zapasowym przełącznikiem głównym dla VLAN 1, 4 i 5.

6. Uruchom funkcje *PortFast* i *BPDU guard* dla wszystkich portów dostępowych.
7. Zweryfikuj wprowadzone ustawienia konfiguracyjne. W jakim trybie działa STP? Jakie są priorytety poszczególnych przełączników? Które porty są blokowane?
8. W przedstawionym scenariuszu wszystkie sieci VLAN wykorzystują połączenie (A) między przełącznikami S1 i S2, natomiast (B) jest zablokowane. Upewnij się, że faktycznie tak jest.
9. Zmodyfikuj priorytety portów STP na przełączniku S1 tak, aby sieć VLAN 5 do komunikacji między S1 i S2 wykorzystywała połączenie (B).[1]
10. Spróbuj przerwać wybrane połączenia między przełącznikami i zaobserwować proces rekalkulacji STP. Ile czasu potrzeba na przywrócenie komunikacji w sieci (np. między PC1 i PC2)? Przywróć układ połączeń zgodny ze schematem (rys. 6.15).
11. Zastąp STP (PVST+) protokołem rapid STP (rapid PVST+) na wszystkich przełącznikach. Powtórz eksperyment z poprzedniego punktu. Czy faktycznie sieć szybciej osiąga stan konwergencji?
12. Wykonaj kopie konfiguracji przełączników.
13. Przywróć ustawienia fabryczne.

6.6.2. Rozwiązanie zadania 1

Konfiguracja routera została przeprowadzona analogicznie jak w poprzednich zadaniach (listing 6.1). Kolejne listingi (6.2, 6.3, 6.4) zawierają fragmenty plików konfiguracyjnych przełączników, przedstawiające rozwiązanie zadania, do 8. punktu włącznie. Odpowiedzi na postawione pytania można znaleźć analizując wyniki działania polecenia `show spanning-tree`. Przed rozpoczęciem konfigurowania bardziej zaawansowanych mechanizmów STP, warto zweryfikować poprawność funkcjonowania wszystkich połączeń trunk (listing 6.5) oraz protokołu VTP (poleceniem `show vtp status`).

W sieciach VLAN 4 i VLAN 5 przełącznik S1 jest mostem głównym (zapis `This bridge is the root`). W związku z tym, wszystkie jego aktywne interfejsy pełnią role desygnowanych (`Desg`) i znajdują się w stanie przekazywania (`FWD`) – listing 6.6. Przełącznik S2, dysponując podwójnym łączem z S1 ((A) i (B)), wybierze połączenie z interfejsem przełącznika S1 o niższym identyfikatorze (przy identycznych wartościach priorytetów interfejsów, domyślnie 128). Dlatego interfejs Fa0/1 przełącznika S2 jest portem głównym (`Root`) w stanie przekazywania (`FWD`), a Fa0/2 został zablokowany (`BLK`) –

[1] Ruch między S1 i S2 można rozdzielić na 2 połączenia trunk również korzystając z polecenia *switchport trunk allowed vlan*. Wyższość rozwiązania polegającego na modyfikacji priorytetów portów STP polega na tym, ze w razie awarii jednego z połączeń trunk, drugie będzie mogło automatycznie przejąć jego funkcje.

listing 6.7. Zatem VLAN 4 i VLAN 5 faktycznie korzystają z połączenia (A).

Listing 6.1. Istotne fragmenty pliku konfiguracyjnego routera R1

```
[...]
!
hostname R1
!
[...]
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet0/0.5
 encapsulation dot1Q 5
 ip address 192.168.5.1 255.255.255.0
!
[...]
!
end
```

Listing 6.2. Istotne fragmenty pliku konfiguracyjnego przełącznika S1 do 8. punktu włącznie

```
!
[...]
!
hostname S1
!
[...]
!
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 4-5 priority 24576
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
```

```
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode trunk
!
interface FastEthernet0/5
 switchport mode trunk
!
[...]
!
interface Vlan1
 no ip address
 no ip route-cache
!
[...]
!
end
```

Listing 6.3. Istotne fragmenty pliku konfiguracyjnego przełącznika S2 do 8. punktu włącznie

```
!
[...]
!
hostname S2
!
!
[...]
!
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
```

```
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 5
 switchport mode access
!
[...]
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
[...]
!
end
```

Listing 6.4. Istotne fragmenty pliku konfiguracyjnego przełącznika S3 do 8. punktu włącznie

```
!
[...]
!
hostname S3
!
[...]
!
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1,4-5 priority 28672
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 4
 switchport mode access
```

```
!
[...]
!
interface Vlan1
 no ip address
 no ip route-cache
!
[...]
!
end
```

Listing 6.5. Weryfikacja poprawności działania połączeń trunk przełącznika S1

```
S1#sh interfaces trunk

Port      Mode      Encapsulation  Status        Native vlan
Fa0/1     on        802.1q         trunking      1
Fa0/2     on        802.1q         trunking      1
Fa0/3     on        802.1q         trunking      1
Fa0/4     on        802.1q         trunking      1
Fa0/5     on        802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094
Fa0/2       1-4094
Fa0/3       1-4094
Fa0/4       1-4094
Fa0/5       1-4094

[...]
```

Listing 6.6. Wynik działania polecenia show spanning-tree na przełączniku S1 w 8. kroku zadania

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0022.9182.e880
              Cost        19
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec
                                  Forward Delay 15 sec

  Bridge ID   Priority    32769 (priority 32768 sys-id-ext 1)
              Address     0022.91dd.fc00
              Hello Time   2 sec  Max Age 20 sec
                                  Forward Delay 15 sec
```

```
                Aging Time 300
15
  Interface          Role Sts Cost      Prio.Nbr Type
17 ------------------ ---- --- --------- -------- --------------------
  Fa0/1              Root FWD 19        128.1    P2p
19 Fa0/2              Altn BLK 19        128.2    P2p
  Fa0/3              Altn BLK 19        128.3    P2p
21 Fa0/4              Altn BLK 19        128.4    P2p
  Fa0/5              Desg FWD 19        128.5    P2p
23

25 VLAN0004
     Spanning tree enabled protocol ieee
27   Root ID     Priority    24580
                 Address     0022.91dd.fc00
29               This bridge is the root
                 Hello Time   2 sec  Max Age 20 sec
31                                   Forward Delay 15 sec

33   Bridge ID   Priority  24580  (priority 24576 sys-id-ext 4)
                 Address   0022.91dd.fc00
35               Hello Time   2 sec  Max Age 20 sec
                                     Forward Delay 15 sec
37               Aging Time 300

39 Interface          Role Sts Cost      Prio.Nbr Type
------------------ ---- --- --------- -------- --------------------
41 Fa0/1              Desg FWD 19        128.1    P2p
  Fa0/2              Desg FWD 19        128.2    P2p
43 Fa0/3              Desg FWD 19        128.3    P2p
  Fa0/4              Desg FWD 19        128.4    P2p
45 Fa0/5              Desg FWD 19        128.5    P2p


47
  VLAN0005
49   Spanning tree enabled protocol ieee
     Root ID     Priority    24581
51               Address     0022.91dd.fc00
                 This bridge is the root
53               Hello Time   2 sec  Max Age 20 sec
                 Forward Delay 15 sec
55
     Bridge ID   Priority  24581  (priority 24576 sys-id-ext 5)
57               Address   0022.91dd.fc00
                 Hello Time   2 sec  Max Age 20 sec
59                                   Forward Delay 15 sec
                 Aging Time 300
61
  Interface          Role Sts Cost      Prio.Nbr Type
63 ------------------ ---- --- --------- -------- --------------------
  Fa0/1              Desg FWD 19        128.1    P2p
```

```
Fa0/2           Desg FWD 19        128.2    P2p
Fa0/3           Desg FWD 19        128.3    P2p
Fa0/4           Desg FWD 19        128.4    P2p
Fa0/5           Desg FWD 19        128.5    P2p
```

Listing 6.7. Wynik działania polecenia show spanning-tree na przełączniku S2 w 8. kroku zadania

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0022.9182.e880
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec
                                  Forward Delay 15 sec

  Bridge ID   Priority  24577  (priority 24576 sys-id-ext 1)
              Address   0022.9182.e880
              Hello Time   2 sec  Max Age 20 sec
                                  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p


VLAN0004
  Spanning tree enabled protocol ieee
  Root ID     Priority    24580
              Address     0022.91dd.fc00
              Cost        19
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec
                                  Forward Delay 15 sec

  Bridge ID   Priority  32772  (priority 32768 sys-id-ext 4)
              Address   0022.9182.e880
              Hello Time   2 sec  Max Age 20 sec
                                  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

```
Fa0/4               Desg FWD 19        128.4     P2p
44

46 VLAN0005
   Spanning tree enabled protocol ieee
48 Root ID     Priority    24581
               Address     0022.91dd.fc00
50             Cost        19
               Port        1 (FastEthernet0/1)
52             Hello Time   2 sec  Max Age 20 sec
                                   Forward Delay 15 sec
54
   Bridge ID   Priority  32773  (priority 32768 sys-id-ext 5)
56             Address   0022.9182.e880
               Hello Time   2 sec  Max Age 20 sec
58                                 Forward Delay 15 sec
               Aging Time 300
60
Interface          Role  Sts  Cost       Prio.Nbr Type
62 ---------------- ----  ---  ---------- -------- --------------------------------
Fa0/1              Root FWD  19         128.1    P2p
64 Fa0/2           Altn BLK  19         128.2    P2p
Fa0/3              Altn BLK  19         128.3    P2p
66 Fa0/4           Altn BLK  19         128.4    P2p
Fa0/5              Desg FWD  19         128.4    P2p
```

W 9. kroku, na przełączniku S1 należy wydać polecenia konfiguracyjne:

```
interface FastEthernet0/2
 spanning-tree vlan 5 port-priority 112
```

Skonfigurowana wartość priorytetu (np. 112) powinna być niższa od domyślnej. Efekt ilustrują dwa poniższe listingi, pokazujące wynik działania polecenia `show spanning-tree`. Należy zwrócić uwagę na wiersz 20. listingu 6.8 oraz wiersze 7, 8, 18, 19 listingu 6.9. Role i stany portów Fa0/1 i Fa0/2 przełącznika S2 w sieciach VLAN 4 i 5 zostały zróżnicowane, zgodnie z założeniami zadania.

Listing 6.8. Fragment wyniku działania polecenia show spanning-tree na przełączniku S1 po wykonaniu 9. kroku zadania

```
[...]
2 VLAN0004
[...]
4
Interface          Role  Sts  Cost       Prio.Nbr Type
6 ---------------- ----  ---  ---------- -------- --------------------------------
Fa0/1              Desg FWD  19         128.1    P2p
8 Fa0/2            Desg FWD  19         128.2    P2p
```

```
Fa0/3           Desg FWD 19        128.3    P2p
Fa0/4           Desg FWD 19        128.4    P2p
Fa0/5           Desg FWD 19        128.5    P2p

VLAN0005
[...]

Interface       Role Sts Cost      Prio.Nbr Type
--------------- ---- --- --------- -------- --------------------------------
Fa0/1           Desg FWD 19        128.1    P2p
Fa0/2           Desg FWD 19        112.2    P2p
Fa0/3           Desg FWD 19        128.3    P2p
Fa0/4           Desg FWD 19        128.4    P2p
Fa0/5           Desg FWD 19        128.5    P2p
```

Listing 6.9. Fragment wyniku działania polecenia show spanning-tree na przełączniku S2 po wykonaniu 9. kroku zadania

```
[...]
VLAN0004
[...]

Interface       Role Sts Cost      Prio.Nbr Type
--------------- ---- --- --------- -------- --------------------------------
Fa0/1           Root FWD 19        128.1    P2p
Fa0/2           Altn BLK 19        128.2    P2p
Fa0/3           Altn BLK 19        128.3    P2p
Fa0/4           Altn BLK 19        128.4    P2p

VLAN0005
[...]

Interface       Role Sts Cost      Prio.Nbr Type
--------------- ---- --- --------- -------- --------------------------------
Fa0/1           Altn BLK 19        128.1    P2p
Fa0/2           Root FWD 19        128.2    P2p
Fa0/3           Altn BLK 19        128.3    P2p
Fa0/4           Altn BLK 19        128.4    P2p
Fa0/5           Desg FWD 19        128.4    P2p
```

STP można zastąpić protokołem rapid STP, wydając na każdym przełączniku polecenie:

```
spanning-tree mode rapid-pvst
```

Wśród informacji wyświetlanych przez `show spanning-tree` powinniśmy zaobserwować zmianę zapisu

```
Spanning tree enabled protocol ieee
```

na:

```
Spanning tree enabled protocol rstp
```

Rozdział 7

Bezpieczeństwo sieci LAN

7.1. Wstęp

Problem bezpieczeństwa sieci na poziomie drugiej warstwy modelu OSI jest często niedoceniany i w konsekwencji zaniedbywany. W związku z tym, warstwa łącza danych bywa najsłabszym ogniwem, obniżającym poziom bezpieczeństwa całego systemu.

Wiele zagadnień dotyczących zabezpieczeń przełączników zostało już omówionych lub zasygnalizowanych w poprzednich rozdziałach. Bieżący rozdział zawiera ich podsumowanie, jak również prezentuje kilka kolejnych. Należy jednak zaznaczyć, że implementacja przedstawionych tu mechanizmów nie gwarantuje pełnego bezpieczeństwa. Zapewnia jego podstawowy poziom i jest punktem wyjściowym do dalszego, ciągłego zabezpieczania, monitorowania i ulepszania. Dalsze wskazówki dotyczące zabezpieczania urządzeń wyposażonych w system IOS można znaleźć w przewodniku Cisco [39].

7.2. Podstawowe mechanizmy bezpieczeństwa przełączników

Podstawowe mechanizmy bezpieczeństwa, z których większość już została przedstawiona w poprzednich rozdziałach lub przy okazji omawiania konfiguracji routerów w [10], to:

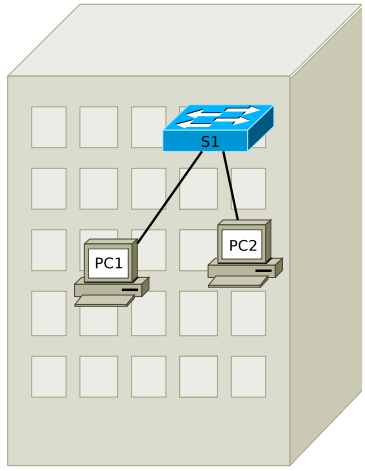
— umieszczenie urządzeń w bezpiecznym miejscu, niedostępnym dla osób nieuprawnionych (np. ze względu na możliwość łatwego przejęcia kontroli nad urządzeniem, w sposób opisany w Dodatku A), zapewniającym odpowiednie warunki pracy – stabilne zasilanie, temperaturę, wilgotność (ang. *Heating, Ventilation, Air Conditioning*, HVAC),
— zabezpieczenie odpowiednio skomplikowanym hasłem dostępu do trybu uprzywilejowanego i portu konsolowego, zabezpieczenie lub wyłączenie dostępu poprzez port AUX i zdalnie (vty), automatyczne wylogowywanie po określonym czasie nieaktywności,
— w miarę możliwości stosowanie haseł przechowywanych w postaci zaszyfrowanej (np. `enable secret` zamiast `enable password`),
— w przypadku rozbudowanych sieci i wielu administratorów – założenie administratorom oddzielnych kont z odpowiednimi uprawnieniami, implementacja AAA (ang. *Authentication, Authorization, and Accounting* – uwierzytelnianie, autoryzacja, ewidencjonowanie)
— przechowywanie logów systemowych na dedykowanym serwerze *syslog*,
— przechowywanie w bezpiecznym miejscu kopii plików konfiguracyjnych i obrazów IOS,
— aktualizacja oprogramowania systemowego, zwłaszcza w razie ujawnienia informacji o błędach,

— synchronizacja zegarów czasu rzeczywistego urządzeń, przy pomocy protokołu NTP, w celu łatwiejszego odtworzenia sekwencji zdarzeń w sieci, na podstawie logów,
— dostęp zdalny poprzez odpowiednio skonfigurowane SSH w możliwie najnowszej wersji, a nie telnet,
— w razie potrzeby stosowania transmisji nieszyfrowanej (np. protokołu TFTP), korzystanie z segmentów sieci dostępnych tylko dla administratora,
— nadanie adresu IP przełącznikowi tylko w jednej sieci VLAN (o ile w ogóle jest potrzebny), niedostępnej dla użytkowników i przeznaczonej wyłącznie na potrzeby administratora,
— skonfigurowanie portów przeznaczonych dla użytkowników jako portów dostępowych (`switchport mode access`) w celu uniemożliwienia zestawienia połączeń typu trunk,
— wyłączenie nieużywanych interfejsów sieciowych,
— wyłączenie protokołu CDP (*Cisco Discovery Protocol*) oraz innych niewykorzystywanych usług,
— odpowiednie zabezpieczenie protokołu SNMP, o ile jest wykorzystywany,
— zdefiniowanie sieci VLAN dla poszczególnych grup użytkowników i ich skonfigurowanie zgodnie ze wskazówkami zawartymi w podrozdziale 3.4,
— zabezpieczenie domeny VTP hasłem, ewentualnie rezygnacja z protokołu VTP,
— odpowiednia konfiguracja STP, zgodnie z zaleceniami przedstawionymi w rozdziale 6.

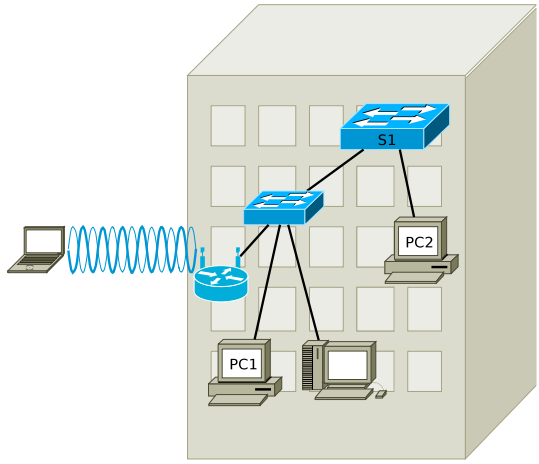
7.3. Bezpieczeństwo portów

Typowy przykład złamania zasad polityki bezpieczeństwa sieci jest przedstawiony na rys. 7.1 i 7.2. Początkowo (rys. 7.1) do przełącznika dołączone były dwa firmowe komputery PC. Następnie użytkownicy, zamiast jednego z nich, bez wiedzy i zgody administratora, podłączyli własny przełącznik (ang. *rogue switch*), kolejne komputery oraz router bezprzewodowy (rys. 7.2). Urządzenia te są całkowicie poza kontrolą administratora. Szczególne zagrożenie stwarza router bezprzewodowy (lub bezprzewodowy punkt dostępowy), ponieważ może udostępniać wszystkim znajdującym się w pobliżu użytkownikom urządzeń WiFi zasoby sieci korporacyjnej.

Innym zagrożeniem jest przepełnienie tablicy adresów MAC przełącznika, przechowywanej w pamięci CAM. Jest oczywiste, że ma ona ograniczoną pojemność. W przypadku jej przekroczenia, przełącznik zaczyna zachowywać się podobnie jak koncentrator, tzn. przychodzące ramki są przekazywane do wszystkich interfejsów. Można do takiej sytuacji doprowadzić



Rysunek 7.1. Fragment sieci korporacyjnej



Rysunek 7.2. Fragment sieci korporacyjnej samodzielnie rozbudowanej przez użytkowników

generując duża liczbę ramek ze sfałszowanymi adresami źródłowymi. Atak tego typu (*CAM Table Overflow*) jest łatwy do przeprowadzenia, przy pomocy dostępnego oprogramowania. Skutkiem jest spadek wydajności sieci (tracimy korzyści wynikające z zastosowania przełączników) oraz możliwość podsłuchiwania (ang. *sniffing*) całego ruchu przechodzącego przez przełącznik.

Takim nadużyciom można zapobiegać (ale nie wyeliminować całkowicie) stosując mechanizmy tzw. bezpieczeństwa portów (ang. *port security*)[40]. Umożliwiają one zdefiniowanie adresów MAC "bezpiecznych" urządzeń, któ-

re mogą być podłączane do danego interfejsu, oraz określenie maksymalnej liczby adresów MAC, które mogą być jednocześnie obsługiwane przez interfejs. Ramki z adresami źródłowymi spoza zdefiniowanej grupy są odrzucane, a ich pojawienie się traktowane jest jako złamanie zasad bezpieczeństwa i skutkuje wykonaniem działań zdefiniowanych przez administratora. Podobnie traktowana jest sytuacja, gdy urządzenie zdefiniowane jako bezpieczne na danym interfejsie zostanie podłączone do innego interfejsu, na którym także włączono mechanizm bezpieczeństwa portów.

Mechanizm bezpieczeństwa portów domyślnie jest wyłączony (w ustawieniach konfiguracyjnych interfejsu fizycznego). Zwykle stosuje się go dla portów dostępowych, do których mogą być podłączane urządzenia użytkowników (chociaż można również w przypadku interfejsów trunk). Tryb pracy interfejsu (dostępowy lub trunk) musi być skonfigurowany statycznie (w razie pozostawienia domyślnej opcji `dynamic auto`, bezpieczeństwa portów włączyć się nie da), np.:

```
switchport mode access
```

Mechanizm bezpieczeństwa danego interfejsu uruchamia się poleceniem:

```
switchport port-security
```

Maksymalną liczbę bezpiecznych adresów MAC można określić poleceniem:

```
switchport port-security maximum liczba
```

Domyślną wartością jest 1, co jest wartością odpowiednią w typowej sytuacji, gdy do portu dołączona jest jedna stacja robocza (zakładając, że nie występują protokoły stosujące wirtualne adresy MAC, np. HSRP[1]).

Wyróżnia się trzy rodzaje bezpiecznych adresów MAC:

— Adresy statyczne są konfigurowane przez administratora poleceniem:

```
switchport port-security mac-address adresMAC
```

— Adresy dynamiczne dodawane są automatycznie, gdy pojawiają się ramki z nowym adresem źródłowym i są tracone w momencie restartu urządzenia.

— Adresy "przylepne" (ang. *sticky*) dodawane są automatycznie (jak dynamiczne) i dopisywane do bieżącej konfiguracji (która z kolei może zostać zapisana jako konfiguracja startowa), co zwalnia administratora z konieczności ręcznego wpisywania adresów MAC urządzeń. Mechanizm ten włącza się poleceniem:

[1] *Hot Standby Router Protocol* [41]

```
switchport port-security mac-address sticky
```

Można jednocześnie korzystać z adresów statycznych i dodawanych automatycznie, oczywiście pod warunkiem skonfigurowania odpowiednio dużej maksymalnej liczby bezpiecznych adresów.

W razie złamania zdefiniowanych zasad bezpieczeństwa, podejmowana jest jedna z trzech akcji, określonych poleceniem:

```
switchport port-security violation
                                    protect | restrict | shutdown
```

`protect` skutkuje jedynie odrzucaniem ramek posiadających adres źródłowy spoza dozwolonej puli. Administrator nie otrzymuje żadnej informacji. W wariancie `restrict` dodatkowo generowany jest komunikat SNMP typu *trap*, wpis w logu, oraz zwiększana jest wartość licznika naruszeń bezpieczeństwa. Domyślną opcją jest `shutdown`. Oprócz działań jak w przypadku `restrict`, interfejs zostaje wyłączony (o czym informuje także zgaśnięcie lub zmiana koloru diody LED portu, z zielonego na pomarańczowy) i pozostaje w tym stanie aż do ingerencji administratora.

Wyłączenie z powodu błędu (*err-disabled* lub *error-disabled*) [42] jest stanem, w którym interfejs jest w sposób automatyczny całkowicie zablokowany przez oprogramowanie przełącznika. Kilka kolejnych, spośród wielu sytuacji, w których port jest przełączany do stanu *err-disabled* zostanie przedstawionych w dalszej części rozdziału. Działanie wyłączonych w ten sposób interfejsów można przywrócić poleceniami konfiguracyjnymi interfejsu:

```
shutdown
no shutdown
```

Możliwe jest również takie skonfigurowanie przełącznika, by port w stanie *err-disabled* był ponownie włączany, po zadanym czasie od usunięcia problemu, który spowodował wyłączenie. Służy do tego celu polecenie

```
errdisable recovery cause ?
```

z odpowiednimi parametrami (znak "?" spowoduje wyświetlenie opcji, które udostępnia dany IOS). Wynik konfiguracji można zweryfikować poleceniem:

```
show errdisable recovery
```

W przypadku zablokowania portu z powodu naruszenia skonfigurowanych reguł bezpieczeństwa portów, automatyczne włączenie możliwe jest przy pomocy polecenia:

```
errdisable recovery cause psecure-violation
```

w trybie konfiguracji globalnej.

Podstawowym poleceniem diagnostycznym mechanizmu bezpieczeństwa portów jest natomiast

```
show port-security
```

z opcjonalnym parametrem – nazwą interfejsu.

7.4. Burze ramek

Burza rozgłoszeń (ang. *broadcast storm*) jest to sytuacja gdy sieć jest "zalewana" bardzo dużą liczbą rozgłoszeń, co prowadzi do radykalnego spadku wydajności lub nawet całkowitego uniemożliwienia komunikacji. Pojęcie burzy stosuje się także w odniesieniu do nadmiernego ruchu multicastowego i unicastowego. Powodem burzy może być błąd w implementacji niektórych protokołów, błędy w konfiguracji sieci lub atak typu DoS (ang. *denial of service* – odmowa usługi). Atak tego typu jest bardzo prosty do przeprowadzenia, przy pomocy powszechnie dostępnych narzędzi.

Mechanizm obronny może polegać na zliczaniu ramek poszczególnych typów (broadcast, multicast, unicast), otrzymywanych poprzez poszczególne interfejsy fizyczne w jednostce czasu (w przypadku przełączników Cisco, domyślnie 1 sekundzie). W razie przekroczenia uprzednio zdefiniowanej wartości progowej dla określonego typu ruchu, zostaje on zablokowany aż do chwili gdy ruch zmaleje poniżej progu odblokowania [40].

Natężenie poszczególnych typów ruchu może być mierzone poprzez zliczanie ramek otrzymywanych w ciągu sekundy, zliczanie bitów otrzymywanych w ciągu sekundy lub jako procent wykorzystania dostępnego pasma. W ostatnim przypadku, ustalenie progu na poziomie 100% oznacza brak limitów dla danego typu ruchu, natomiast 0% – całkowitą blokadę.

W przełącznikach Cisco mechanizm kontroli burz (ang. *storm control*) dla poszczególnych interfejsów jest domyślnie wyłączony. Włączenie następuje poprzez ustalenie progów działania, w trybie konfiguracji interfejsu, przy pomocy polecenia:

```
storm-control broadcast|multicast|unicast level
                                    poziom [poziom-dolny]
```

Parametr *poziom* jest liczbą z zakresu od 0.00 do 100.00, określającą procent wykorzystania pasma przez ruch określonego typu (broadcast, multicast lub unicast), powyżej którego nastąpi zablokowanie tego ruchu. Opcjonalny pa-

rametr *poziom-dolny* określa natężenie ruchu, przy którym blokada zostanie wyłączona. Jego wartość nie może być większa niż *poziom*. Aby zdefiniować progi w bitach lub ramkach na sekundę, zamiast procentowo, należy w powyższym poleceniu użyć parametrów `bps` lub `fps`, odpowiednio.

Jak już wspomniano, w razie wykrycia burzy, domyślną akcją jest filtrowanie ruchu określonego typu. Przykładowo, jeżeli zostanie przekroczony próg dla ruchu multicastowego, blokowany jest cały ruch multicastowy, oprócz kontrolnego (np. BPDU, CDP). Przy pomocy polecenia:

```
storm-control action shutdown|trap
```

można wymusić inne działania, tzn. przełączanie portu do stanu *err-disabled* (parametr `shutdown`) lub generowanie komunikatu SNMP trap (parametr `trap`).

7.5. Porty chronione i blokowane

W pewnych sytuacjach dobrym rozwiązaniem, zwiększającym poziom bezpieczeństwa, może być zablokowanie komunikacji (na poziomie 2. warstwy modelu OSI) między portami tego samego przełącznika. Przykładowo, w sieci kawiarni internetowej moglibyśmy przyjąć, że komputery klientów mogą komunikować się z Internetem (za pośrednictwem routera), natomiast nie będą wymieniać żadnych komunikatów między sobą. W przypadku przełączników Cisco można osiągnąć to włączając funkcję portów chronionych (ang. *protected ports*)[40].

Pomiędzy portami skonfigurowanymi jako chronione nie są przekazywane żadne ramki (unicastowe, multicastowe ani rozgłoszeniowe, poza kontrolnymi, związanymi z pracą przełącznika). Możliwa jest natomiast komunikacja za pośrednictwem urządzenia warstwy trzeciej. Komunikacja między portami chronionymi i niechronionymi odbywa się w sposób standardowy. Port konfiguruje się jako chroniony poleceniem:

```
switchport protected
```

Domyślnie opcja jest wyłączona.

Jeżeli przełącznik otrzyma ramkę z nieznanym adresem MAC (lub ramkę multicastową), rozsyła ją do wszystkich interfejsów. W pewnych sytuacjach (np. w razie korzystania z portów chronionych) może to stanowić lukę w systemie bezpieczeństwa. Wydanie poleceń:

```
switchport block multicast
```

oraz

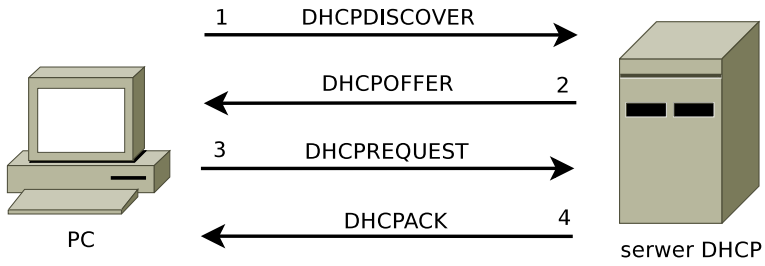
```
switchport block unicast
```

w ustawieniach interfejsu (chronionego lub niechronionego) spowoduje, że ramki multicastowe i unicastowe z nieznanym docelowym adresem MAC (tzn. gdy w tablicy adresów MAC przełącznika brakuje odpowiedniego wpisu) nie będą do niego przesyłane.

Jeżeli host docelowy przez dłuższy czas nie będzie wysyłał żadnych ramek, jego adres MAC może zostać usunięty z tablicy przełącznika wskutek przedawnienia (domyślnie po 300 sekundach). Wówczas skutkiem wydania powyższych poleceń będzie brak możliwości transmisji do "milczącego" hosta. Jednak, w przypadku współczesnych systemów operacyjnych i aplikacji, 300-sekundowe milczenie jest zjawiskiem mało prawdopodobnym.

7.6. Protokół DHCP

DHCP (*Dynamic Host Configuration Protocol*)[43] jest protokołem, który automatyzuje proces konfiguracji hostów do pracy w sieci. Najczęściej wykorzystuje się go do przydzielania urządzeniom końcowym adresu IP wraz z maską, adresu bramy domyślnej i adresów serwerów DNS. Protokół istotnie upraszcza zarządzanie siecią i jest obecnie powszechnie stosowany.



Rysunek 7.3. Komunikacja w protokole DHCP.

Rys. 7.3 ilustruje najbardziej typowy sposób działania protokołu DHCP. W pierwszym kroku klient poszukuje serwera DHCP, który mógłby przypisać mu ustawienia konfiguracyjne. Komunikat DHCPDISCOVER jest wysyłany jako rozgłoszenie. Jeżeli serwer DHCP znajduje się w innej sieci (co jest częste), odpowiednio skonfigurowany router (*DHCP relay agent*) może przekazywać te komunikaty w odpowiednie miejsce. Serwer DHCP w odpowiedzi wysyła pakiet DHCPOFFER z propozycją konfiguracji (krok 2.). Jeżeli klient je akceptuje, wysyła kolejne rozgłoszenie z komunikat DHCPREQUEST – prośbą o przydzielenie zaproponowanych ustawień. Serwer

potwierdza ten fakt komunikatem DHCPACK, zezwalając klientowi na skonfigurowanie swojego interfejsu sieciowego.

Przedstawiony mechanizm może wydawać się nadmiernie skomplikowany. Należy jednak zauważyć, że w sieci może być dostępnych kilka serwerów DHCP i host może otrzymać więcej niż jedną propozycję DHCPOFFER. Informacja o wyborze jednej z nich i odrzuceniu pozostałych (DHCPREQUEST) powinna dotrzeć do wszystkich serwerów.

Ze względu na charakter ustawień konfiguracyjnych realizowanych przy pomocy DHCP oraz sposób działania protokołu, jego stosowanie może obniżyć poziom bezpieczeństwa sieci. W razie braku odpowiednich mechanizmów zabezpieczających, każdy użytkownik może uruchomić własny serwer DHCP, przydzielający ustawienia IP hostom w jego domenie rozgłoszeniowej. Jeżeli legalny serwer DHCP znajduje się w innej sieci, wzrasta prawdopodobieństwo, że hosty pobiorą ustawienia konfiguracyjne z podstawionego, ponieważ zwykle host korzysta z pierwszej propozycji DHCPOFFER, która do niego dotrze. Można w ten sposób przeprowadzić mało wyrafinowany atak polegający na przydzielaniu bezsensownych adresów, skutkujący paraliżem sieci. Można również, modyfikując adres bramy domyślnej, przechwytywać ruch między siecią LAN a światem zewnętrznym lub przeprowadzić atak typu "człowiek pośrodku" (ang. *man in the middle*). Konfigurując z kolei adres nielegalnego serwera DNS, można np. przekierować połączenia z bankiem internetowym do podstawionego serwera, służącego do kradzieży tożsamości. Z powodu przedstawionych zagrożeń, niekiedy administratorzy rezygnują z protokołu DHCP, np. w sieciach o znaczeniu militarnym. Nie ulega wątpliwości, że w przypadku korzystania z DHCP, w sieci powinny zostać zaimplementowane odpowiednie zabezpieczenia.

W przypadku przełączników Cisco, eliminowanie komunikatów DHCP pochodzących od niezaufanych serwerów zapewnia funkcja "podglądania" DHCP (ang. *DHCP snooping*) [44]. Pod pojęciem niezaufanych interfejsów rozumiemy te, do których dołączone są hosty użytkowników. Interfejsy zaufane służą z kolei do podłączenia serwerów DHCP lub innych przełączników. Mechanizm jest dość rozbudowany i zostanie tu przedstawiony tylko podstawowy wariant konfiguracji [44]:

1. Należy globalnie włączyć DHCP *snooping*:

   ```
   ip dhcp snooping
   ```

2. Należy określić sieci VLAN, w których ma działać mechanizm:

   ```
   ip dhcp snooping vlan zakres-sieci-VLAN
   ```

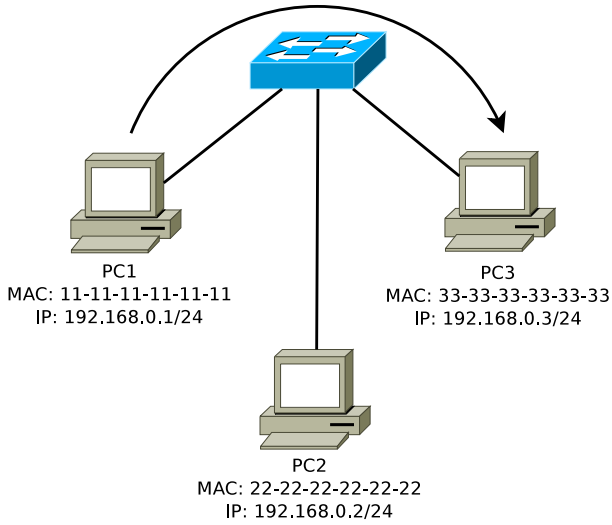
3. Od tego momentu wszystkie interfejsy są traktowane jako niezaufane.

Interfejs staje się zaufany po wydaniu w jego ustawieniach konfiguracyjnych polecenia:

```
ip dhcp snooping trust
```

7.7. Protokół ARP

Protokół ARP (ang. *Address Resolution Protocol*) [45] umożliwia automatyczne przypisanie znanym adresom IP nieznanych adresów drugiej warstwy modelu OSI, wewnątrz domeny rozgłoszeniowej. Jest wykorzystywany w praktycznie każdej sieci Ethernet, lecz także Token Ring, FDDI, WiFi. Ze swojej natury protokół ten jest podatny na różnego typu nadużycia. Teoretycznie możliwa jest rezygnacja z ARP, poprzez zastosowanie statycznych wpisów w tablicach ARP, jednak w sieciach liczących więcej niż kilka hostów wiązałoby się to z olbrzymimi komplikacjami.



Rysunek 7.4. Przykładowa sieć LAN.

W sieci z rys. 7.4 host PC1 musi wysłać pakiet do PC3. Nie zna jednak jego adresu MAC. W związku z tym, wyśle jako rozgłoszenie zapytanie ARP o adres fizyczny hosta posiadającego adres IP 192.168.0.3. Na zapytanie to powinien zareagować wyłącznie PC3, wysyłając do PC1 informację o swoim adresie MAC. W tablicy ARP hosta PC1 powinien pojawić się wpis postaci:

```
Address         HWtype  HWaddress           Flags Mask  Iface
192.168.0.3     ether   33:33:33:33:33:33   C             eth0
```

Powyżej pokazany jest wynik działania polecenia `arp` (z odpowiednim parametrem, w zależności od systemu operacyjnego). PC2 może jednak wysłać do sieci sfałszowane komunikaty ARP, twierdząc, że posiada adres IP 192.168.0.3 i adres MAC 22:22:22:22:22:22. Jest to jeszcze łatwiejsze dzięki mechanizmowi grzecznościowego ARP (ang. *gratuitous ARP*), zgodnie z którym host może rozgłaszać odpowiedzi ARP, także bez uprzedniego zapytania. Odbierając te rozgłoszenia, pozostałe hosty aktualizują swoje tablice ARP informacjami, które mogły zostać sfałszowane. Host PC1, dysponując w tablicy ARP wpisem:

```
Address         HWtype  HWaddress           Flags Mask  Iface
192.168.0.3     ether   22:22:22:22:22:22   C           eth0
```

będzie wysyłał ramki przeznaczone dla hosta PC3 do hosta PC2, który z kolei, znając prawdziwy obraz sieci, może je przeglądać, modyfikować, a następnie wysyłać do prawdziwego adresata. Jest to kolejny przykład ataku typu "człowiek pośrodku".

Obronę przed atakami na protokół ARP zapewnia mechanizm dynamicznej inspekcji ARP (ang. *dynamic ARP inspection* [46]). Polega on na śledzeniu komunikatów ARP i automatycznym odrzucaniu tych, które zawierają nieprawdziwe przypisania adresów MAC do IP. Podobnie jak w przypadku *DHCP snooping*, rozróżnia się interfejsy zaufane i niezaufane. Komunikaty ARP generowane przez urządzenia dołączone do zaufanych interfejsów są zawsze akceptowane, natomiast pozostałe podlegają filtrowaniu. W typowym przypadku, porty do których dołączone są urządzenia końcowe, konfiguruje się jako niezaufane, natomiast porty łączące z innymi przełącznikami jako zaufane. Nieprzestrzeganie tej reguły może prowadzić do przerwania komunikacji lub powstania luk bezpieczeństwa.

Dynamiczna inspekcja ARP domyślnie jest wyłączona. Sposób konfiguracji zależy od tego, czy adresy hostów w sieci są przydzielane dynamicznie (DHCP) czy statycznie. W przypadku sieci z serwerem DHCP, inspekcja ARP korzysta z danych generowanych przez DHCP *snooping* i funkcja ta musi zostać włączona. Następnie należy użyć następujących poleceń:

1. W trybie konfiguracji globalnej należy włączyć inspekcję ARP dla poszczególnych sieci VLAN:

   ```
   ip arp inspection vlan zakres-sieci-VLAN
   ```

2. Następnie interfejsy stanowiące połączenia między przełącznikami należy skonfigurować jako zaufane (domyślnie są niezaufane), wpisując w ich ustawieniach polecenie:

   ```
   ip arp inspection trust
   ```

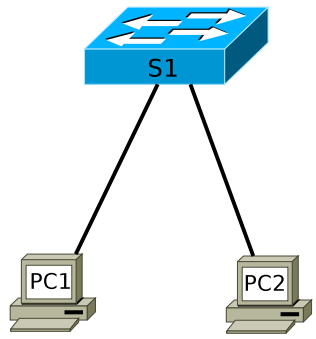
3. Wprowadzone ustawienia można zweryfikować poleceniami:

```
show ip arp inspection interfaces
show ip arp inspection vlan zakres-sieci-VLAN
```

Więcej przykładów konfiguracyjnych (m.in. dla sieci bez DHCP) oraz opis zaawansowanych opcji można znaleźć w dokumentacji [46].

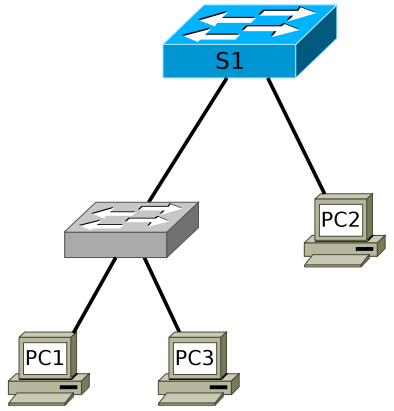
7.8. Zadania

7.8.1. Zadanie 1 – bezpieczeństwo portów



Rysunek 7.5. Schemat topologii logicznej sieci

1. Połącz sieć zgodnie ze schematem (rys. 7.5). Upewnij się, że komputery mogą komunikować się między sobą.
2. Wyłącz nieużywane porty. Na wykorzystywanych interfejsach włącz mechanizmy bezpieczeństwa portów. Ustal maksymalną liczbę bezpiecznych adresów MAC na 1.
3. Spróbuj złamać zdefiniowane zasady bezpieczeństwa, np. w sposób przedstawiony na rys. 7.6.
4. Przywróć topologię sieci z rys. 7.5. Uruchom zablokowany interfejs.
5. Adres MAC komputera PC1 skonfiguruj jako bezpieczny adres statyczny. Na interfejsie, do którego dołączony jest PC2, włącz mechanizm adresów "przylepnych". Upewnij się, że działa komunikacja między hostami.
6. Przejrzyj ustawienia dotyczące bezpieczeństwa portów w bieżącym pliku konfiguracyjnym oraz informacje, których dostarcza polecenie diagnostyczne `show port-security` (również z parametrem – nazwą interfejsu).



Rysunek 7.6. Próba złamania polityki bezpieczeństwa

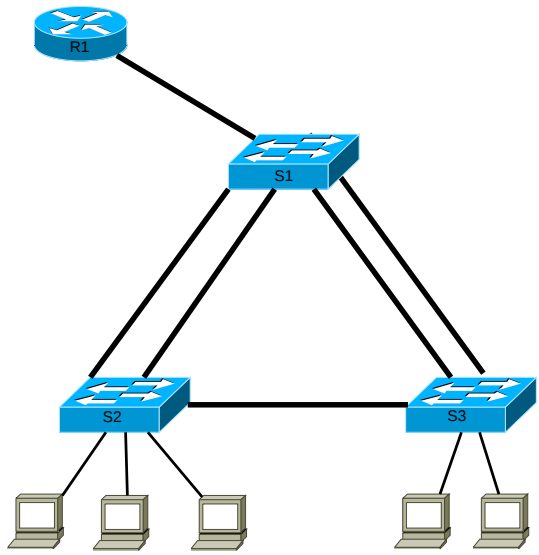
7.8.2. Rozwiązanie zadania 1

Wpis w 16. wierszu pliku konfiguracyjnego został wygenerowany automatycznie.

Listing 7.1. Istotne fragmenty pliku konfiguracyjnego przełącznika S1

```
[...]
!
hostname S1
!
!
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address 0006.2A4B.5B3A
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.7026.9BA8
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
[...]
!
end
```

7.8.3. Zadanie 2 – studium przypadku



Rysunek 7.7. Schemat topologii logicznej sieci

Zbuduj i skonfiguruj sieć zgodnie ze schematem (rys. 7.7). Stwórz 3 sieci VLAN: dla 2 grup użytkowników oraz zarządzającą. Router powinien zapewniać komunikację między sieciami VLAN, jak również pracować jako serwer DHCP dla hostów. Zaplanuj, zaimplementuj i przetestuj strategię bezpieczeństwa dla sieci LAN, uwzględniając wskazówki zawarte w bieżącym rozdziale, jak również rozdziałach dotyczących wirtualnych sieci LAN oraz protokołu STP.

Dodatek A

Procedura odzyskiwania kontroli nad przełącznikiem

A.1. Odzyskiwanie hasła

W przypadku konfigurowalnego urządzenia sieciowego, może zaistnieć konieczność przejęcia nad nim kontroli, w razie zabezpieczenia go nieznanym hasłem. Odpowiednie procedury zwykle są udokumentowane przez producentów sprzętu, a ich przeprowadzenie wymaga fizycznego dostępu do urządzenia. Istnienie takich procedur może stanowić istotne zagrożenie dla bezpieczeństwa sieci, o ile nie zostaną wprowadzone odpowiednie fizyczne zabezpieczenia przed dostępem osób niepowołanych.

Ogólne informacje o odzyskiwaniu haseł zabezpieczających urządzenia Cisco można znaleźć w [47]. Opis procedury dla routerów serii 2600 i 2800 znajduje się w [48] lub [10]. W przypadku przełączników Cisco, procedura przebiega nieco inaczej. Poniższy opis procedury dotyczy urządzeń serii 2900XL/3500XL, 2940, 2950/2955, 2960, 2970 oraz 3550, 3560 i 3750 [49].

Należy wykonać następującą sekwencję czynności:

1. Należy uruchomić połączenie konsolowe z przełącznikiem (standardowe ustawienia: 9600 baud, 8 bitów danych, brak parzystości, 1 bit stopu, kontrola przepływu: Xon/Xoff).
2. Przełącznik musi zostać uruchomiony w trybie ROMmon (znak zgłoszenia: `switch:`), umożliwiającym niskopoziomowe rozwiązywanie problemów. W tym celu należy odłączyć kabel zasilający, a następnie włączyć go ponownie (przełączniki zwykle nie posiadają wyłączników sieciowych), jednocześnie trzymając wciśnięty przycisk `MODE`. Przycisk może zostać zwolniony po kilku – kilkunastu sekundach, w zależności od wersji urządzenia. W przypadku przełączników Catalyst 2955, zamiast naciskania przycisku, należy wysłać z konsoli znak Break (kombinacja klawiszowa `Ctrl + Break` lub inna, w zależności od systemu operacyjnego i programu emulatora terminala).
3. Gdy ukaże się znak zgłoszenia postaci `switch:`, należy wydać polecenie:

   ```
   flash_init
   ```

   a następnie:

   ```
   load_helper
   ```

4. Poleceniem:

   ```
   dir flash:
   ```

   można wylistować pliki zapisane w pamięci flash urządzenia. Powinien wśród nich znajdować się plik `config.text`, w którym zapisana jest konfiguracja startowa (`startup-config`), wraz z nieznanymi hasłami. Aby

przejąc kontrolę nad przełącznikiem, a jednocześnie nie stracić zapisanych uprzednio ustawień konfiguracyjnych, należy zmienić nazwę pliku `config.text` na inną, np.:

```
rename flash:config.text flash:config.old
```

Wykonanie powyższego polecenia nie powiedzie się, w razie gdy plik `config.old` już istnieje. Należy wówczas wybrać inną nazwę. Gdyby natomiast nie zależało nam na zachowaniu ustawień konfiguracyjnych, plik konfiguracyjny można od razu usunąć poleceniem:

```
delete flash:config.text
```

5. Poleceniem

```
boot
```

uruchamiamy proces wczytywania systemu operacyjnego. Udzielamy następnie odpowiedzi odmownej na pytanie o uruchomienie dialogu konfiguracyjnego (`Continue with configuration dialog? [yes/no]: n`).
6. W tym momencie powinno być możliwe uruchomienie trybu uprzywilejowanego:

```
enable
```

i wykonanie wszelkich innych operacji. Procedurę można na tym zakończyć. Jeżeli jednak zależy nam na przywróceniu wcześniejszych ustawień konfiguracyjnych (zapisanych obecnie w pliku `config.old`, jeżeli zmieniliśmy nazwę zgodnie ze wskazówkami z 4. punktu bieżącej procedury), należy wykonać kolejne kroki.
7. Polecenie

```
copy flash:config.text system:running-config
```

uruchomi uprzednio zapisaną konfigurację. Należy teraz w standardowy sposób zmodyfikować hasła zabezpieczające przełącznik, a następnie zapisać konfigurację:

```
copy running-config startup-config
```

A.2. Przywracanie IOS

W razie gdy w przełączniku jest zainstalowany działający obraz systemu operacyjnego, operacje archiwizacji IOS oraz instalacji nowego można przeprowadzić standardowymi poleceniami:

```
copy flash tftp
copy tftp flash
```

Potrzebny jest serwer TFTP. Czynności te wykonuje się identycznie jak w przypadku routerów.

W razie braku działającego IOS, np. wskutek przypadkowego wykasowania zawartości pamięci flash, należy przeprowadzić procedurę jego przywrócenia. Zostanie ona przedstawiona na przykładzie przełącznika Catalyst 2960 [50].

1. Oprogramowanie systemowe przełącznika Catalyst jest oryginalnie dostarczane w postaci archiwum .tar. Należy je rozpakować celem pozyskania pliku z obrazem IOS, z rozszerzeniem .bin (przykładowa nazwa: c2960-lanbase-mz.122-25.FX.bin).
2. Podobnie jak w procedurze odzyskiwania hasła, należy nawiązać połączenie konsolowe z przełącznikiem, korzystając z programu obsługującego protokół Xmodem. Jeżeli nie będzie możliwe wczytanie IOS, przełącznik automatycznie uruchomi się w trybie ROMmon, zatem nie jest konieczne włączanie go z wciśniętym przyciskiem `MODE`.
3. Gdy ukaże się znak zgłoszenia postaci `switch:`, należy wydać polecenie:

   ```
   flash_init
   ```

   a następnie:

   ```
   load_helper
   ```

4. Obraz IOS będzie przesyłany poprzez port konsolowy. Domyślnie pracuje on z szybkością 9600 baud, co będzie skutkowało długim czasem transmisji. Szybkość tę można zwiększyć poleceniem:

   ```
   set BAUD 115200
   ```

   o ile w danej wersji urządzenia jest dostępne. Konieczne jest wówczas również odpowiednie zmodyfikowanie parametrów połączenia konsolowego w programie emulującym terminal.
5. Należy wydać polecenie:

   ```
   copy xmodem: flash:image_filename.bin
   ```

gdzie *image_filename.bin* jest nazwą pliku z obrazem IOS.

6. Należy uruchomić wysyłanie pliku obrazu w protokole Xmodem, w sposób zgodny z dokumentacją programu emulującego terminal.
7. Po zakończeniu transmisji należy przywrócić standardową szybkość portu konsolowego:

   ```
   set BAUD 9600
   ```

   jeżeli została wcześniej zmieniona. Analogicznie należy przywrócić poprzednie ustawienie portu w programie emulującym terminal.
8. Uruchomienie nowego IOS powinno być teraz możliwe poprzez restart urządzenia lub poleceniem:

   ```
   boot flash:image_filename.bin
   ```

9. Po załadowaniu IOS przełącznik powinien już poprawnie funkcjonować. Jego oprogramowanie systemowe nie jest jednak jeszcze kompletne. Przykładowo, brakuje plików HTML wykorzystywanych przez serwer HTTP przełącznika. Pełne oprogramowanie systemowe można zainstalować przy pomocy polecenia

   ```
   archive download-sw
   ```

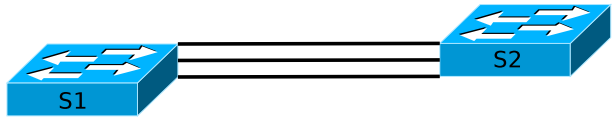
   wydanego w trybie uprzywilejowanym (zakładając, że dysponujemy odpowiednim archiwum .tar). Jeżeli nowo zainstalowane oprogramowanie będzie działać prawidłowo po restarcie przełącznika, wówczas można usunąć plik uprzednio przesłany poprzez Xmodem (*image_filename.bin*).

Dodatek B

Konfiguracja mechanizmu EtherChannel

B.1. Wstęp

Jeżeli przepustowość łącza między dwoma przełącznikami jest niesatysfakcjonująca, a mają one niewykorzystywane interfejsy, istnieje możliwość skonfigurowania kilku łącz fizycznych jako jedno połączenie logiczne, korzystając z technologii EtherChannel.



Rysunek B.1. Wielokrotne połączenie między przełącznikami

Przy domyślnej konfiguracji, w sytuacji przedstawionej na rys. B.1, dwa z trzech połączeń zostałyby wyłączone wskutek działania protokołu STP (rozdział 6).

B.2. Konfigurowanie EtherChannel

Do wyboru mamy dwa protokoły wykorzystywane do automatycznego tworzenia łącza typu EtherChannel. Pierwszy z nich (wykorzystany w przykładzie) to PAgP (*Port Aggregation Protocol*) – protokół własnościowy CISCO. Drugim jest LACP (*Link Aggregate Control Protocol*) – standard IEEE 802.3ad. Oba wykorzystywane są w procesie negocjacji formowania kanału przesyłu informacji poprzez EtherChannel. Można również zrezygnować z autonegocjacji, wybierając opcję `on`.

Przykładowy sposób konfiguracji przedstawia poniższy listing B.1. Jak widać, ustawienia konfiguracyjne wprowadzane są w trybie konfiguracji wybranego zakresu interfejsów (`interface range`).

Listing B.1. Konfiguracja EtherChannel

```
S2(config-if-range)#channel-group 1 mode ?
  active      Enable LACP unconditionally
  auto        Enable PAgP only if a PAgP device is detected
  desirable   Enable PAgP unconditionally
  on          Enable Etherchannel only
  passive     Enable LACP only if a LACP device is detected

S2(config-if-range)#channel-group 1 mode desirable
S2(config)#int port-channel 1
S2(config-if)#switchport mode trunk
```

Podstawowym poleceniem do weryfikacji poprawności skonfigurowania kanału jest `show etherchannel summary` (listing B.2).

Listing B.2. Przykładowy wynik działania polecenia show etherchannel summary

```
Flags: D - down        P - bundled in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3      S - Layer2
       U - in use      f - failed to allocate aggregator

       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
1      Po1(SU)         PAgP      Fa0/22(P)   Fa0/23(P)
                                 Fa0/24(P)
```

Informacje o EtherChannel pojawiają się także w wyniku działania znanych już poleceń: `show interface trunk` oraz `show spanning-tree`.

Istnieje możliwość wybrania jednego z kilku algorytmów równoważenia ruchu (rozdzielania ruchu na dostępne w ramach kanału łącza fizyczne). Domyślnym kryterium jest źródłowy adres MAC (`src-mac`):

```
S2# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-mac
```

Dostępne są następujące opcje:

```
S2(config)#port-channel load-balance ?
  dst-ip          Dst IP Addr
  dst-mac         Dst Mac Addr
  src-dst-ip      Src XOR Dst IP Addr
  src-dst-mac     Src XOR Dst Mac Addr
  src-ip          Src IP Addr
  src-mac         Src Mac Addr
```

Słownik angielsko-polski

access control list (ACL)	lista kontroli dostępu
alternate port	port alternatywny
authentication, authorization, accounting (AAA)	uwierzytelnianie, autoryzacja, ewidencjonowanie
autonegotiation	autonegocjacja
backup port	port zapasowy
bandwidth	szerokość pasma
blocking state	stan blokowania
BPDU guard	strażnik BPDU
bridge	most
broadcast	rozgłoszenie
broadcast storm	burza rozgłoszeń
Carrier Sense Multiple Access / with Collision Detection	wielodostęp z badaniem stanu kanału i wykrywaniem kolizji
configuration revision number	numer zmiany konfiguracji
convergence	zbieżność
data link layer	warstwa łącza danych
denial of service	odmowa usługi
designated port	port desygnowany
DHCP snooping	podglądanie DHCP
diameter	średnica
direct link failure	awaria łącza bezpośrednio przyłączonego
disabled state	stan wyłączony
edge port	port brzegowy
extended-range VLANs	sieci VLAN z rozszerzonego zakresu
flapping link	niestabilne łącze
forwarding state	stan przekazywania
frame	ramka
full duplex	pełny dupleks
gratuitous ARP	grzecznościowy ARP

half duplex	półdupleks
hub	koncentrator
indirect link failure	awaria odległego łącza
inter-VLAN routing	routing między sieciami VLAN
layer 3 switch	przełącznik warstwy 3
learning state	stan uczenia
link type	typ łącza
listening state	stan nasłuchiwania
local area network (LAN)	sieć lokalna
loopback	pętla zwrotna
MAC address table	tablica adresów MAC
man in the middle	człowiek pośrodku
management frame	ramka zarządzająca
multilayer switching (MLS)	przełączanie wielowarstwowe
network diameter	średnica sieci
normal-range VLANs	sieci VLAN ze zwykłego zakresu
physical layer	warstwa fizyczna
point-to-point	punkt-punkt
Power over Ethernet	zasilanie poprzez kabel Ethernet
quality of service	jakość usług
redundancy	nadmiarowość
rogue switch/router/access point	przełącznik/router/punkt dostępowy zainstalowany bez wiedzy administratora
root bridge	przełącznik główny
root port	port główny
router	router
routing	routing, trasowanie
routing loop	pętla routingu
Spanning Tree Protocol, STP	protokół drzewa rozpinającego
Storage Area Network	sieć pamięci masowej
subinterface	podinterfejs
switch	przełącznik
switching	przełączanie
switching loop	pętla w sieci przełączanej
TCP/IP stack	stos TCP/IP
thicknet	gruby Ethernet
thinnet	cienki Ethernet
token	żeton
token passing	przekazywanie żetonu
transparent switching	przełączanie przezroczyste
user EXEC mode	tryb EXEC użytkownika

virtual local area network, VLAN	wirtualna sieć lokalna
VLAN tagging	znakowanie ramek
VTP pruning	przycinanie VTP
Wide Area Network (WAN)	sieć rozległa

Bibliografia

[1] W. Lewis, *Akademia sieci Cisco. CCNA Exploration. Semestr 3. Przełączanie sieci LAN i sieci bezprzewodowe*, PWN, 2011.

[2] B. Sosinsky, *Sieci komputerowe. Biblia*, Helion, 2011.

[3] R. Breyer, S. Riley, *Switched, Fast i Gigabit Ethernet*, Helion, 2000.

[4] K. Krysiak, *Sieci komputerowe. Kompendium. Wydanie II*, Helion, 2005.

[5] IEEE, *IEEE 802.5 Web Site*, `http://www.ieee802.org/5/www8025org/`.

[6] ANSI X3T9.5 Committee, *FDDI Station Management (SMT)*, Rev. 6.1, March 15 1990.

[7] ARCNET Trace Association, *ATA 878.1 - 1999 Local Area Network: Token Bus*, 1999, `http://www.arcnet.com`.

[8] N. Abramson, The ALOHA System – Another Alternative for Computer Communications, *Proc. 1970 Fall Joint Computer Conference*, AFIPS Press, 1970.

[9] R.M. Mercalfe, D.R. Boggs, Ch.P. Thacker, B.W. Lampson, Multipoint data communication system (with collision detection), U.S. Patent 4,063,220, 1977.

[10] K. Kuczyński, R. Stęgierski, *Routing w sieciach IP*, UMCS, Lublin 2011.

[11] Cisco Systems, Configuring Switch-Based Authentication, *Catalyst 2960 Switch Software Configuration Guide, 12.2(25)SED*, `http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_sed/configuration/guide/2960SCG.pdf`.

[12] Cisco Systems, Configuring Interface Characteristics, *Catalyst 2960 Switch Software Configuration Guide, 12.2(25)SED*, `http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_sed/configuration/guide/2960SCG.pdf`.

[13] Cisco Systems, Catalyst 2960 Switch Cisco IOS Commands, *Catalyst 2960 Switch Command Reference, 12.2(46)SE*, `http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_46_se/command/reference/2960CR.pdf`.

[14] Cisco Systems, *Inter-Switch Link and IEEE 802.1Q Frame Format*, Document ID: 17056, `http://www.cisco.com/application/pdf/paws/17056/741_4.pdf`.

[15] Cisco Systems, Configuring VLANs, *Catalyst 2960 Switch Software Configuration Guide, 12.2(25)SEE*, `http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_see/configuration/guide/2960SCG.pdf`.

[16] Cisco Systems, Configuring Voice VLAN, *Catalyst 2960 Switch Software Configuration Guide, 12.2(25)SEE*, `http://www.cisco.com/en/US/`

docs/switches/lan/catalyst2960/software/release/12.2_25_see/configuration/guide/2960SCG.pdf.

[17] Cisco Systems, *Understanding VLAN Trunk Protocol (VTP)*, Document ID: 10558, http://www.cisco.com/application/pdf/paws/10558/21.pdf.

[18] Cisco Systems, Understanding How VTP Version 3 Works, *Catalyst 6500 Series Software Configuration Guide, 8.7*, http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/6000_cfg.pdf.

[19] IEEE, *802.1ak – Multiple Registration Protocol*, 2007, http://www.ieee802.org/1/pages/802.1ak.html.

[20] Cisco Systems, *IEEE 801.ak – MVRP and MRP*, 2008, http://www.cisco.com/en/US/docs/ios/lanswitch/configuration/guide/lsw_cfg_mvrp.pdf.

[21] Cisco Systems, *Enterprise Campus 3.0 Architecture: Overview and Framework*, http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html.

[22] Cisco Systems, *Understanding EtherChannel Load Balancing and Redundancy on Catalyst Switches*, Document ID: 12023, http://www.cisco.com/image/gif/paws/12023/4.pdf.

[23] Cisco Systems, *Cisco SAFE*, http://www.cisco.com/go/safe.

[24] B. Stewart, *CCNP BSCI Official Exam Certification Guide* (4th Edition), Cisco Press, 2008.

[25] IEEE, *802.1D IEEE Standard for Local and metropolitan area networks, Media Access Control (MAC) Bridges*, http://standards.ieee.org/getieee802/download/802.1D-2004.pdf.

[26] R. Perlman, An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN, *ACM SIGCOMM Computer Communication Review*, 15(4): 44–53, 1985.

[27] Cisco Systems, *Spanning Tree Protocol Problems and Related Design Considerations*, Document ID: 10556, http://www.cisco.com/image/gif/paws/10556/16.pdf.

[28] Cisco Systems, *Using PortFast and Other Commands to Fix Workstation Startup Connectivity Delays*, Document ID: 10553, http://www.cisco.com/image/gif/paws/10553/12.pdf.

[29] Cisco Systems, *Spanning Tree PortFast BPDU Guard Enhancement*, Document ID: 10586, http://www.cisco.com/application/pdf/paws/10586/65.pdf.

[30] Cisco Systems, *Understanding and Tuning Spanning Tree Protocol Timers*, Document ID: 19120, http://www.cisco.com/application/pdf/paws/19120/122.pdf.

[31] Cisco Systems, *Understanding and Configuring the Cisco UplinkFast Feature*, Document ID: 10575, http://www.cisco.com/application/pdf/paws/10575/51.pdf.

[32] Cisco Systems, *Understanding and Configuring Backbone Fast on Catalyst Switches*, Document ID: 12014, http://www.cisco.com/image/gif/paws/12014/18.pdf.

[33] Cisco Systems, *Understanding Rapid Spanning Tree Protocol (802.1w)*, Do-

cument ID: 24062, http://www.cisco.com/application/pdf/paws/24062/146.pdf.

[34] Cisco Systems, *Spanning Tree from PVST+ to Rapid-PVST Migration Configuration Example*, Document ID: 72836, http://www.cisco.com/image/gif/paws/72836/rapidpvst-mig-config.pdf.

[35] Cisco Systems, *Understanding Multiple Spanning Tree Protocol (802.1s)*, Document ID: 24248, http://www.cisco.com/application/pdf/paws/24248/147.pdf.

[36] IEEE, *802.1Q IEEE Standard for Local and metropolitan area networks, Virtual Bridged Local Area Networks*,http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf.

[37] Cisco Systems, *Spanning Tree Protocol Root Guard Enhancement*, Document ID: 10588, http://www.cisco.com/application/pdf/paws/10588/74.pdf.

[38] Cisco Systems, Configuring STP, *Catalyst 2960 and 2960-S Software Configuration Guide, 12.2(53)SE1*, http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_53_se/configuration/guide/2960scg.pdf.

[39] Cisco Systems, *Cisco Guide to Harden Cisco IOS Devices*, Document ID: 13608, http://www.cisco.com/image/gif/paws/13608/21.pdf.

[40] Cisco Systems, Configuring Port-Based Traffic Control, *Catalyst 2960 Switch Software Configuration Guide, 12.2(25)SEE*, http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_see/configuration/guide/2960SCG.pdf.

[41] T. Li, B. Cole, P. Morton, D. Li, *Cisco Hot Standby Router Protocol (HSRP)*, Request for Comments: 2281 Network Working Group, 1998, http://tools.ietf.org/html/rfc2281.

[42] Cisco Systems, *Errdisable Port State Recovery on the Cisco IOS Platforms*, Document ID: 69980, http://www.cisco.com/image/gif/paws/69980/errdisable_recovery.pdf.

[43] R. Droms, *Dynamic Host Configuration Protocol*, Request for Comments: 2131 Network Working Group, 1997, http://tools.ietf.org/html/rfc2131.

[44] Cisco Systems, Configuring DHCP Features, *Catalyst 2960 Switch Software Configuration Guide, 12.2(25)FX*, http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_fx/configuration/guide/2960SCG.pdf.

[45] D.C. Plummer, *An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*, Request For Comments: 826, Network Working Group, 1982, http://tools.ietf.org/html/rfc826.

[46] Cisco Systems, Configuring Dynamic ARP Inspection, *Catalyst 2960 Switch Software Configuration Guide, Rel. 12.2(50)SE*, http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_50_se/configuration/guide/2960SCG.pdf.

[47] Cisco Systems, *Password Recovery Procedures*, Document ID: 6130, http://www.cisco.com/image/gif/paws/6130/index.pdf.

[48] Cisco Systems, *Password Recovery Procedure for the Cisco 2600 and 2800*

Series Routers, Document ID: 22188, http://www.cisco.com/image/gif/paws/22188/pswdrec_2600.pdf.

[49] Cisco Systems, *Password Recovery – Cisco Catalyst Fixed Configuration Layer 2 and Layer 3 Switches*, Document ID: 12040, http://www.cisco.com/image/gif/paws/12040/pswdrec_2900xl.pdf.

[50] Cisco Systems, *Troubleshooting – Catalyst 2960 Switch Software Configuration Guide, Rel. 12.2(46)SE [Cisco Catalyst 2960 Series Switches]*, http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_46_se/configuration/guide/2960SCG.pdf.

Skorowidz