WYŻSZA SZKOŁA
INFORMATYKI i ZARZĄDZANIA
z siedzibą w Rzeszowie

KOLEGIUM INFORMATYKI STOSOWANEJ

Kierunek: INFORMATYKA

Grupa: 4IIZ/2022/IoT SP03

Michał Ziobro
Nr albumu w11111
Arkadiusz Swatek
Nr albumu w22222
Filip Walat
Nr albumu w67204

Infrastruktura sieci IoT

Prowadzący: dr inż. John Strong

Projekt

Rzeszów 2024

Spis treści

Wstęp

Celem projektu było zaprojektowanie topologii sieciowej dla organizacji, uwzględniając różne potrzeby i wymagania działów oraz zapewniając wydajność, bezpieczeństwo i skalowalność sieci. Przedstawiona topologia została zaplanowana w taki sposób, aby umożliwić separację ruchu sieciowego, kontrolę dostępu oraz zapewnienie wysokiej dostępności i redundancji. Projekt zakładał również zastosowanie różnych technologii sieciowych, takich jak VLAN, EtherChannel, STP, OSPF, HSRP, IPv6 oraz ACL, aby sprostać wymaganiom organizacji.

Na podstawie dostarczonego diagramu sieciowego, sieć została podzielona na kilka segmentów (VLAN-ów), które są przypisane do różnych działów i funkcji. Każdy segment ma swoje unikalne urządzenia i usługi, co pozwala na lepsze zarządzanie i kontrolę ruchu sieciowego. W projekcie uwzględniono również redundancję połączeń i urządzeń, co zapewnia wysoką dostępność sieci w przypadku awarii.

Liczba Urządzeń w Sieci

Na podstawie diagramu sieciowego, liczba urządzeń w sieci przedstawia się następująco:

- Przełączniki (Switch): 21
- Routery: 6
- Komputery (PC): 22
- Serwery: 9
- Inne urządzenia: 8
- Access Pointy: 2
- Inne elementy: 5

Rozdział 1

Podstawowe Założenia Sieci

1.1 Cel Projektu

Celem projektu było zaprojektowanie topologii sieciowej dla firmy produkującej oprogramowanie, uwzględniając potrzeby i wymagania różnych działów oraz zapewniając wydajność, bezpieczeństwo i skalowalność sieci. Projekt miał na celu stworzenie nowoczesnej, elastycznej i bezpiecznej infrastruktury sieciowej, która umożliwi sprawne funkcjonowanie wszystkich działów firmy.

1.2 Struktura Sieci

Sieć została zaprojektowana z myślą o separacji ruchu sieciowego, kontrolowaniu dostępu oraz zapewnieniu wysokiej dostępności i redundancji. Podstawowe założenia sieci obejmują segmentację za pomocą VLAN-ów, zastosowanie redundancji połączeń oraz wdrożenie różnych technologii sieciowych.

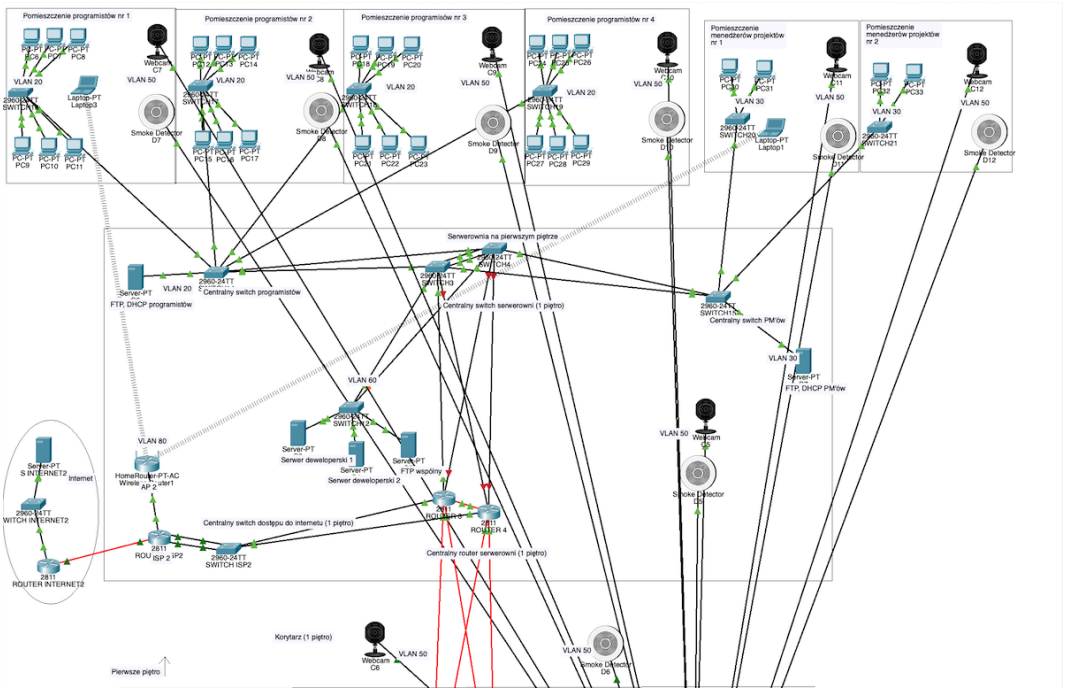
1.2.1 Segmentacja Sieci za Pomocą VLAN-ów

Segmentacja sieci została zrealizowana przy użyciu VLAN-ów (Virtual Local Area Network). Każdy dział w firmie, taki jak administracja, programiści, menedżerowie, ochrona, monitoring, serwery i goście, został przypisany do osobnego VLAN-u. Poniżej przedstawiono główne VLAN-y używane w sieci:

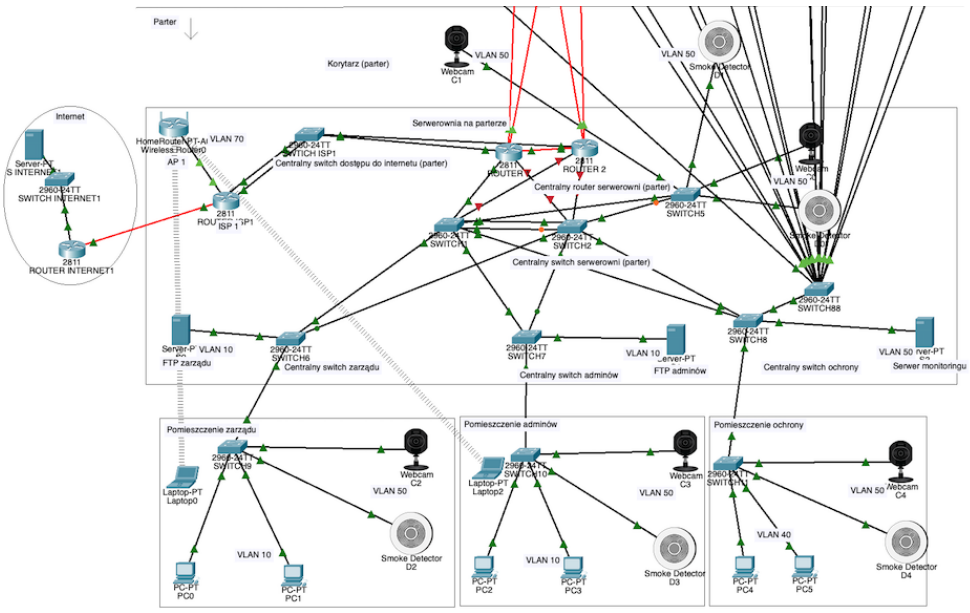
- **VLAN 10 (Admins)**: VLAN przypisany do zarządu i administracji, gdzie znajdują się komputery i serwery FTP zarządu oraz administracji.
- **VLAN 20 (Programmers)**: VLAN dla programistów, obejmujący komputery programistów oraz serwery FTP i DHCP.
- **VLAN 30 (Managers)**: VLAN dla menedżerów projektów, gdzie znajdują się komputery, serwer FTP i DHCP.
- **VLAN 40 (Security)**: VLAN dla ochrony, obejmujący komputery ochrony.
- **VLAN 50 (Monitoring)**: VLAN dla monitoringu, obejmujący kamery, serwer monitoringu oraz czujniki.
- **VLAN 60 (Servers)**: VLAN dla serwerów deweloperskich oraz wspólnego serwera FTP.
- **VLAN 70 (Guests)**: VLAN dla sieci Wi-Fi dla gości na parterze.
- **VLAN 80 (Guests2)**: VLAN dla sieci Wi-Fi dla gości na piętrze.
- **VLAN 95 (Black Hole)**: VLAN dla nieużywanych portów (black hole).

1.3 Opis Pomieszczeń i Urządzeń w Topologii Sieci

Diagram sieciowy przedstawia szczegółowy układ pomieszczeń w budynku firmy oraz urządzenia sieciowe przypisane do każdego pomieszczenia.



Rysunek 1.1: Diagram sieciowy - Pietro



Rysunek 1.2: Diagram sieciowy - Parter

1.3.1 Pomieszczenia Programistów

Pomieszczenia programistów są podzielone na cztery segmenty, z których każdy przypisany jest do VLAN 20. W każdym pomieszczeniu znajdują się komputery programistów oraz serwery FTP i DHCP. Dodatkowo, w każdym pomieszczeniu znajduje się smoke detector (czujnik dymu), co jest przykładem zastosowania urządzeń IoT (Internet of Things) do zwiększenia bezpieczeństwa w budynku.

1.3.2 Pomieszczenie Menedżerów Projektów

Pomieszczenie menedżerów projektów przypisane jest do VLAN 30. Znajdują się tam komputery menedżerów oraz serwery FTP i DHCP, które umożliwiają zarządzanie projektami i współpracę w ramach zespołu.

1.3.3 Pomieszczenia Zarządu i Administracji

Pomieszczenia zarządu i administracji są przypisane do VLAN 10. W tych pomieszczeniach znajdują się komputery i serwery FTP zarządu oraz administracji, co umożliwia zarządzanie firmą oraz administracyjne wsparcie dla innych działów.

1.3.4 Pomieszczenia Ochrony

Pomieszczenia ochrony są przypisane do VLAN 40. Znajdują się tam komputery ochrony oraz systemy monitoringu, które zapewniają bezpieczeństwo w budynku firmy.

1.3.5 Pomieszczenia Monitoringu

Pomieszczenia monitoringu przypisane są do VLAN 50. Znajdują się tam kamery monitoringu oraz serwery monitoringu, które rejestrują i przechowują dane wideo. W tych pomieszczeniach znajdują się również czujniki dymu, co jest kolejnym przykładem zastosowania urządzeń IoT.

1.3.6 Serwerownia

Serwerownia jest podzielona na dwa VLAN-y: VLAN 60 dla serwerów deweloperskich oraz VLAN 70 i VLAN 80 dla sieci Wi-Fi dla gości na parterze i piętrze. Serwerownia zawiera kluczowe serwery, takie jak serwery FTP i DHCP dla różnych działów oraz serwery deweloperskie, które wspierają pracę programistów.

1.3.7 Korytarze i Strefy Wspólne

W korytarzach i strefach wspólnych, takich jak pomieszczenia serwisowe, znajdują się przełączniki sieciowe oraz routery, które zapewniają łączność między różnymi segmentami sieci. Korytarze są również wyposażone w access pointy (AP) dla sieci Wi-Fi, które zapewniają bezprzewodowy dostęp do sieci dla gości.

1.3.8 Zastosowanie Urządzeń IoT

W całej topologii sieciowej zastosowano urządzenia IoT, takie jak kamery monitoringu i czujniki dymu. Kamery monitoringu są rozmieszczone w różnych pomieszczeniach i na korytarzach, zapewniając bezpieczeństwo i monitoring wizyjny. Czujniki dymu są zainstalowane w pomieszczeniach programistów oraz w pomieszczeniach monitoringu, co pozwala na szybkie wykrywanie pożarów i zwiększenie bezpieczeństwa w budynku.

1.4 Hasła do Urządzeń Sieciowych

W celu zapewnienia bezpieczeństwa sieciowego, każde urządzenie sieciowe zostało zabezpieczone hasłami. Poniżej znajduje się tabela z hasłami przypisanymi do poszczególnych urządzeń:

Tabela 1.1: Hasła do Urządzeń Sieciowych

Urządzenie	**Hasło**
Router1	Router1
Router2	Router2
Switch1	Switch1
Switch2	Switch2
Switch.ISP1	Switch.ISP1
Switch5	Switch5
Switch6	Switch6
Switch7	Switch7
Switch8	Switch8
Switch88	Switch88
Switch9	Switch9
Switch10	Switch10
Switch11	Switch11
Router3	Router3
Router4	Router4
Switch3	Switch3
Switch4	Switch4
Switch.ISP2	Switch.ISP2
Router.ISP2	Router.ISP2
Switch12	Switch12
Switch14	Switch14
Switch15	Switch15
Switch16	Switch16
Switch17	Switch17
Switch18	Switch18
Switch19	Switch19
Switch20	Switch20
Switch21	Switch21

1.5 SSID i Hasła do Sieci Wi-Fi

Sieci Wi-Fi w firmie zostały skonfigurowane z odpowiednimi SSID i hasłami, zapewniając dostęp dla gości na różnych poziomach budynku.

- **SSID: Parter, VLAN 70**
  - Hasło: *Parter!#$ (WPA2 Personal)*
- **SSID: Pietro, VLAN 80**
  - Hasło: *Pietro!#$% (WPA2 Personal)*

1.6 Podsumowanie

Projekt topologii sieciowej dla firmy produkującej oprogramowanie uwzględniał różnorodne potrzeby działów firmy oraz zapewniał wysoką wydajność, bezpieczeństwo i skalowalność sieci. Dzięki segmentacji za pomocą VLAN-ów, redundancji połączeń oraz zastosowaniu nowoczesnych technologii sieciowych, sieć jest elastyczna, bezpieczna i gotowa na przyszłe rozwinięcia. Wdrożenie urządzeń IoT dodatkowo zwiększa bezpieczeństwo i funkcjonalność infrastruktury sieciowej.

Rozdział 2

Opis Infrastruktury

Infrastruktura sieci składa się z wielu VLAN-ów, przełączników i routerów skonfigurowanych do zarządzania różnymi działami i funkcjami. VLAN-y są segmentowane w zależności od działu lub funkcji, takich jak administracja, programiści, menedżerowie, ochrona, monitoring, serwery i goście. Każdy VLAN ma przypisane konkretne urządzenia i usługi. Przełączniki są skonfigurowane z EtherChannel dla redundancji i poprawy wydajności, natomiast routery obsługują routing między VLAN-ami i zapewniają dostęp do sieci zewnętrznych.

2.1 Lista VLAN-ów

Tabela 2.1: Lista VLAN-ów

VLAN ID	Nazwa VLAN	Opis
10	VLAN_Admins	Zarząd i administracja, komputery i serwery FTP zarządu i administracji
20	VLAN_Programmers	Programiści, komputery programistów, serwer FTP i DHCP
30	VLAN_Managers	Menedżerowie projektów, komputery, serwer FTP i DHCP
40	VLAN_Security	Ochrona, komputery ochrony
50	VLAN_Monitoring	Monitoring, kamery, serwer monitoringu, czujniki
60	VLAN_Servers	Serwery deweloperskie 1 i 2, wspólny FTP
70	VLAN_Guests	Sieć Wi-Fi dla gości na parterze
80	VLAN_Guests2	Sieć Wi-Fi dla gości na piętrze
95	VLAN_Black_hole	VLAN dla nieużywanych portów (black hole)

2.2 Tabela Dostępu Między VLAN-ami

Poniższa tabela przedstawia dostępność między poszczególnymi VLAN-ami w sieci. "Pełny dostęp"oznacza, że VLAN źródłowy ma pełny dostęp do zasobów VLAN-u docelowego, "Ograniczony dostęp"oznacza, że dostęp jest ograniczony, a "Brak dostępu"oznacza, że dostęp jest zablokowany.

Tabela 2.2: Tabela Dostępu Między VLAN-ami (Część 1)

VLAN źródłowy	**VLAN docelowy**	**Typ dostępu**
VLAN 10 (Admins)	VLAN 20 (Programiści)	Pełny dostęp
VLAN 10 (Admins)	VLAN 30 (Menedżerowie)	Pełny dostęp
VLAN 10 (Admins)	VLAN 40 (Ochrona)	Brak dostępu
VLAN 10 (Admins)	VLAN 50 (Monitoring)	Pełny dostęp
VLAN 10 (Admins)	VLAN 60 (Serwery)	Pełny dostęp
VLAN 10 (Admins)	VLAN 70 (Goście)	Brak dostępu
VLAN 10 (Admins)	VLAN 80 (Goście2)	Brak dostępu
VLAN 10 (Admins)	VLAN 95 (Black Hole)	Brak dostępu
VLAN 20 (Programiści)	VLAN 10 (Admins)	Ograniczony dostęp
VLAN 20 (Programiści)	VLAN 30 (Menedżerowie)	Ograniczony dostęp
VLAN 20 (Programiści)	VLAN 40 (Ochrona)	Brak dostępu
VLAN 20 (Programiści)	VLAN 50 (Monitoring)	Ograniczony dostęp
VLAN 20 (Programiści)	VLAN 60 (Serwery)	Pełny dostęp
VLAN 20 (Programiści)	VLAN 70 (Goście)	Brak dostępu
VLAN 20 (Programiści)	VLAN 80 (Goście2)	Brak dostępu
VLAN 20 (Programiści)	VLAN 95 (Black Hole)	Brak dostępu
VLAN 30 (Menedżerowie)	VLAN 10 (Admins)	Ograniczony dostęp
VLAN 30 (Menedżerowie)	VLAN 20 (Programiści)	Ograniczony dostęp
VLAN 30 (Menedżerowie)	VLAN 40 (Ochrona)	Brak dostępu
VLAN 30 (Menedżerowie)	VLAN 50 (Monitoring)	Ograniczony dostęp
VLAN 30 (Menedżerowie)	VLAN 60 (Serwery)	Pełny dostęp
VLAN 30 (Menedżerowie)	VLAN 70 (Goście)	Brak dostępu
VLAN 30 (Menedżerowie)	VLAN 80 (Goście2)	Brak dostępu
VLAN 30 (Menedżerowie)	VLAN 95 (Black Hole)	Brak dostępu

Tabela 2.3: Tabela Dostępu Między VLAN-ami (Część 2)

VLAN źródłowy	VLAN docelowy	Typ dostępu
VLAN 40 (Ochrona)	VLAN 10 (Admins)	Brak dostępu
VLAN 40 (Ochrona)	VLAN 20 (Programiści)	Brak dostępu
VLAN 40 (Ochrona)	VLAN 30 (Menedżerowie)	Brak dostępu
VLAN 40 (Ochrona)	VLAN 50 (Monitoring)	Ograniczony dostęp
VLAN 40 (Ochrona)	VLAN 60 (Serwery)	Brak dostępu
VLAN 40 (Ochrona)	VLAN 70 (Goście)	Brak dostępu
VLAN 40 (Ochrona)	VLAN 80 (Goście2)	Brak dostępu
VLAN 40 (Ochrona)	VLAN 95 (Black Hole)	Brak dostępu
VLAN 50 (Monitoring)	VLAN 10 (Admins)	Pełny dostęp
VLAN 50 (Monitoring)	VLAN 20 (Programiści)	Ograniczony dostęp
VLAN 50 (Monitoring)	VLAN 30 (Menedżerowie)	Ograniczony dostęp
VLAN 50 (Monitoring)	VLAN 40 (Ochrona)	Ograniczony dostęp
VLAN 50 (Monitoring)	VLAN 60 (Serwery)	Pełny dostęp
VLAN 50 (Monitoring)	VLAN 70 (Goście)	Brak dostępu
VLAN 50 (Monitoring)	VLAN 80 (Goście2)	Brak dostępu
VLAN 50 (Monitoring)	VLAN 95 (Black Hole)	Brak dostępu
VLAN 60 (Serwery)	VLAN 10 (Admins)	Pełny dostęp
VLAN 60 (Serwery)	VLAN 20 (Programiści)	Pełny dostęp
VLAN 60 (Serwery)	VLAN 30 (Menedżerowie)	Pełny dostęp
VLAN 60 (Serwery)	VLAN 40 (Ochrona)	Brak dostępu
VLAN 60 (Serwery)	VLAN 50 (Monitoring)	Pełny dostęp
VLAN 60 (Serwery)	VLAN 70 (Goście)	Brak dostępu
VLAN 60 (Serwery)	VLAN 80 (Goście2)	Brak dostępu
VLAN 60 (Serwery)	VLAN 95 (Black Hole)	Brak dostępu
VLAN 70 (Goście)	VLAN 10 (Admins)	Brak dostępu
VLAN 70 (Goście)	VLAN 20 (Programiści)	Brak dostępu
VLAN 70 (Goście)	VLAN 30 (Menedżerowie)	Brak dostępu
VLAN 70 (Goście)	VLAN 40 (Ochrona)	Brak dostępu
VLAN 70 (Goście)	VLAN 50 (Monitoring)	Brak dostępu
VLAN 70 (Goście)	VLAN 60 (Serwery)	Brak dostępu
VLAN 70 (Goście)	VLAN 80 (Goście2)	Brak dostępu
VLAN 70 (Goście)	VLAN 95 (Black Hole)	Brak dostępu
VLAN 80 (Goście2)	VLAN 10 (Admins)	Brak dostępu
VLAN 80 (Goście2)	VLAN 20 (Programiści)	Brak dostępu
VLAN 80 (Goście2)	VLAN 30 (Menedżerowie)	Brak dostępu
VLAN 80 (Goście2)	VLAN 40 (Ochrona)	Brak dostępu
VLAN 80 (Goście2)	VLAN 50 (Monitoring)	Brak dostępu
VLAN 80 (Goście2)	VLAN 60 (Serwery)	Brak dostępu
VLAN 80 (Goście2)	VLAN 70 (Goście)	Brak dostępu
VLAN 80 (Goście2)	VLAN 95 (Black Hole)	Brak dostępu
VLAN 95 (Black Hole)	VLAN 10 (Admins)	Brak dostępu
VLAN 95 (Black Hole)	VLAN 20 (Programiści)	Brak dostępu
VLAN 95 (Black Hole)	VLAN 30 (Menedżerowie)	Brak dostępu
VLAN 95 (Black Hole)	VLAN 40 (Ochrona)	Brak dostępu
VLAN 95 (Black Hole)	VLAN 50 (Monitoring)	Brak dostępu
VLAN 95 (Black Hole)	VLAN 60 (Serwery)	Brak dostępu
VLAN 95 (Black Hole)	VLAN 70 (Goście)	Brak dostępu
VLAN 95 (Black Hole)	VLAN 80 (Goście2)	Brak dostępu

2.3 Tabela Przełączników z Zastosowanymi Technologiami

Poniższa tabela przedstawia listę przełączników używanych w sieci oraz technologie, które są na nich zastosowane. EtherChannel jest używany do zwiększenia przepustowości

Tabela 2.4: Tabela Przełączników z Zastosowanymi Technologiami

Przełącznik	Zastosowane Technologie	EtherChannel
Przełącznik 1	VLAN, Spanning-Tree, PortFast, Trunk, EtherChannel	Tak
Przełącznik 2	VLAN, Spanning-Tree, PortFast, Trunk, EtherChannel	Tak
Przełącznik 3	VLAN, Spanning-Tree, PortFast, Trunk, EtherChannel	Tak
Przełącznik 4	VLAN, Spanning-Tree, PortFast, Trunk, EtherChannel	Tak
Przełącznik 5	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 6	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 7	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 8	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 9	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 10	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 11	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 12	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 14	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 15	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 16	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 17	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 18	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 19	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 20	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 21	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie
Przełącznik 88	VLAN, Spanning-Tree, PortFast, Port Security, Trunk	Nie

2.4 Tabela Routerów z Zastosowanymi Technologiami

Poniższa tabela przedstawia listę routerów używanych w sieci oraz technologie, które są na nich zastosowane. Routery obsługują m.in. protokoły routingu OSPF i HSRP, a także routing między VLAN-ami oraz IPv6.

Tabela 2.5: Tabela Routerów z Zastosowanymi Technologiami

Router	Zastosowane Technologie
Router 1	OSPF, HSRP, Routing statyczny, Routing między VLAN-ami, IPv6, ACL
Router 2	OSPF, HSRP, Routing statyczny, Routing między VLAN-ami, IPv6, ACL
Router 3	OSPF, HSRP, Routing statyczny, Routing między VLAN-ami, IPv6, ACL
Router 4	OSPF, HSRP, Routing statyczny, Routing między VLAN-ami, IPv6, ACL
Router ISP1	Routing statyczny, IPv6, ACL
Router ISP2	Routing statyczny, IPv6, ACL

Rozdział 3

Opis Zastosowanych Technologii

3.1 VLAN (Virtual Local Area Network)

VLAN (Virtual Local Area Network) to technologia umożliwiająca logiczne segmentowanie sieci na mniejsze części, co poprawia zarządzanie, bezpieczeństwo i wydajność. W obecnej topologii sieciowej VLAN-y są używane do separacji różnych działów, takich jak administracja, programiści, menedżerowie, ochrona, monitoring, serwery i goście.

3.1.1 Zalety

- Poprawa bezpieczeństwa poprzez segmentację sieci.
  - Separacja ruchu sieciowego: Dzięki VLAN-om ruch sieciowy z jednego działu (np. administracji) jest oddzielony od ruchu z innych działów (np. programistów). To oznacza, że nawet jeśli jeden dział zostanie zainfekowany złośliwym oprogramowaniem, inne działy pozostaną bezpieczne.
  - Kontrola dostępu: VLAN-y umożliwiają bardziej precyzyjną kontrolę dostępu do zasobów sieciowych. Na przykład, pracownicy administracji mogą mieć dostęp do zasobów, do których programiści nie mają dostępu, co zwiększa bezpieczeństwo danych.
- Redukcja ruchu broadcastowego.
  - Ograniczenie zasięgu broadcastu: W tradycyjnej sieci, komunikaty typu broadcast są przesyłane do wszystkich urządzeń. Dzięki VLAN-om, broadcasty są ograniczone tylko do urządzeń w tym samym VLAN-ie. To zmniejsza ilość niepotrzebnego ruchu sieciowego i poprawia wydajność.
  - Poprawa wydajności sieci: Mniej broadcastów oznacza mniej zakłóceń dla urządzeń w sieci, co prowadzi do lepszej wydajności i szybszej komunikacji między urządzeniami.
- Lepsze zarządzanie siecią.
  - Łatwiejsza administracja: VLAN-y pozwalają na logiczne grupowanie urządzeń, co ułatwia zarządzanie siecią. Administratorzy mogą łatwo przypisywać urządzenia do odpowiednich VLAN-ów i zarządzać politykami sieciowymi.
  - Skalowalność: Sieć z VLAN-ami jest bardziej skalowalna, ponieważ nowe urządzenia mogą być łatwo dodawane do odpowiednich VLAN-ów bez konieczności zmian w fizycznej topologii sieci.
- Ułatwienie zarządzania politykami sieciowymi.

  - Centralizacja kontroli: Dzięki VLAN-om, polityki sieciowe mogą być łatwiej wdrażane i zarządzane z jednego centralnego punktu. Na przykład, polityki bezpieczeństwa mogą być stosowane tylko do określonych VLAN-ów.
  - Elastyczność: Administratorzy mają większą elastyczność w konfigurowaniu reguł dostępu, priorytetów ruchu i innych ustawień sieciowych w zależności od potrzeb poszczególnych działów.

3.1.2 Wady

- Złożoność konfiguracji i zarządzania.
  - Potrzebna wiedza specjalistyczna: Konfiguracja VLAN-ów wymaga wiedzy na temat sieci i doświadczenia w pracy z przełącznikami sieciowymi. Błędy w konfiguracji mogą prowadzić do problemów z dostępnością sieci.
  - Utrzymanie i aktualizacje: Utrzymanie VLAN-ów i wprowadzanie zmian w konfiguracji mogą być czasochłonne, szczególnie w dużych sieciach.
- Potrzeba wsparcia ze strony urządzeń sieciowych.
  - Kompatybilność sprzętu: Wszystkie przełączniki i routery w sieci muszą obsługiwać VLAN-y, co może wymagać modernizacji starszego sprzętu.
  - Koszty: Zakup nowego sprzętu, który obsługuje VLAN-y, może być kosztowny, szczególnie w dużych sieciach.
- Możliwość błędnej konfiguracji prowadząca do problemów z dostępnością sieci.
  - Ryzyko błędów: Nieprawidłowa konfiguracja VLAN-ów może prowadzić do problemów z komunikacją między urządzeniami, co może skutkować przestojami w pracy sieci.
  - Trudności w diagnostyce: Diagnostyka problemów związanych z VLAN-ami może być skomplikowana i czasochłonna, co może opóźniać rozwiązanie problemów sieciowych.

3.1.3 Zastosowanie w Topologii

W obecnej topologii VLAN-y są używane do separacji ruchu sieciowego między różnymi działami firmy. Dzięki temu każdy dział działa w oddzielnej przestrzeni, co zwiększa bezpieczeństwo i wydajność sieci. Na przykład, VLAN 10 jest przypisany do administracji, VLAN 20 do programistów, a VLAN 30 do menedżerów, co pozwala na lepsze zarządzanie zasobami sieciowymi i kontrolę dostępu.

3.2 Spanning-Tree Protocol (STP)

Spanning-Tree Protocol (STP) to protokół zapobiegający powstawaniu pętli w sieciach z redundancją połączeń. STP automatycznie wykrywa i blokuje redundantne ścieżki, utrzymując jednocześnie dostępność sieci.

3.2.1 Zalety

- Zapobieganie powstawaniu pętli w sieci.
  - Eliminacja pętli: Pętle w sieci mogą powodować nadmierne przesyłanie tych samych pakietów, co prowadzi do zakłóceń i obciążeń sieci. STP wykrywa i eliminuje pętle, utrzymując sieć stabilną.
  - Stabilność sieci: Dzięki eliminacji pętli, STP zapewnia stabilność i niezawodność sieci, co jest kluczowe dla utrzymania ciągłości działania.
- Automatyczne przywracanie ścieżek w przypadku awarii.
  - Redundancja połączeń: STP pozwala na tworzenie redundantnych połączeń, które są automatycznie aktywowane w przypadku awarii głównej ścieżki. To zapewnia ciągłość działania sieci.
  - Szybka reakcja: STP szybko reaguje na zmiany w topologii sieci, automatycznie przełączając ruch na alternatywne ścieżki, co minimalizuje przerwy w działaniu.
- Poprawa niezawodności sieci.
  - Redukcja ryzyka przestojów: Dzięki STP, ryzyko przestojów w sieci jest znacznie mniejsze, ponieważ protokół automatycznie zarządza połączeniami i eliminuje pętle.
  - Lepsze zarządzanie: STP umożliwia lepsze zarządzanie połączeniami sieciowymi, co prowadzi do bardziej przewidywalnego i stabilnego działania sieci.

3.2.2 Wady

- Opóźnienia w konwergencji sieci.
  - Czas konwergencji: Proces konwergencji STP, podczas którego sieć dostosowuje się do zmian topologii, może trwać kilka sekund do minut, co może prowadzić do krótkich przestojów.
  - Wpływ na wydajność: Dłuższy czas konwergencji może wpływać na wydajność sieci, szczególnie w przypadku częstych zmian topologii.
- Złożoność konfiguracji.
  - Zaawansowane ustawienia: Konfiguracja STP wymaga zaawansowanej wiedzy na temat sieci, co może być wyzwaniem dla mniej doświadczonych administratorów.
  - Potencjalne błędy: Błędna konfiguracja STP może prowadzić do problemów z dostępnością sieci i trudności w diagnostyce.
- Możliwość nieprawidłowej konfiguracji prowadzącej do problemów z dostępnością sieci.
  - Ryzyko pętli: Nieprawidłowa konfiguracja STP może prowadzić do powstania pętli w sieci, co może powodować poważne problemy z dostępnością i wydajnością sieci.
  - Trudności w diagnostyce: Problemy związane z nieprawidłową konfiguracją STP mogą być trudne do zdiagnozowania i naprawienia, co może wydłużać czas przestoju.

3.2.3 Zastosowanie w Topologii

W obecnej topologii STP jest używany na przełącznikach, aby zapobiec powstawaniu pętli i zapewnić redundancję połączeń. Dzięki temu sieć jest bardziej niezawodna, a ewentualne awarie są automatycznie wykrywane i naprawiane. STP umożliwia tworzenie redundantnych połączeń między przełącznikami, co zapewnia ciągłość działania sieci nawet w przypadku awarii jednego z połączeń.

3.3 PortFast

PortFast to funkcja Spanning-Tree Protocol, która umożliwia szybkie aktywowanie portów przełączników podłączonych do końcowych urządzeń sieciowych. Dzięki temu urządzenia końcowe mogą szybciej uzyskać połączenie z siecią.

3.3.1 Zalety

- Szybsze połączenie urządzeń końcowych z siecią.
  - Skrócony czas aktywacji portu: PortFast omija standardowy proces STP, który może trwać do 50 sekund, co pozwala na natychmiastowe aktywowanie portu. Dzięki temu urządzenia końcowe szybciej uzyskują połączenie z siecią.
  - Poprawa doświadczenia użytkownika: Szybsze połączenie z siecią oznacza, że użytkownicy nie muszą długo czekać na dostęp do zasobów sieciowych po podłączeniu swoich urządzeń.
- Zmniejszenie opóźnień przy uruchamianiu urządzeń.
  - Szybszy dostęp do zasobów: Urządzenia końcowe, takie jak komputery i drukarki, mogą szybciej uzyskać dostęp do sieci i zasobów sieciowych, co poprawia wydajność pracy.
  - Ułatwienie diagnostyki: Dzięki szybszemu uruchamianiu urządzeń, administratorzy sieci mogą szybciej zdiagnozować i rozwiązać ewentualne problemy z połączeniem.
- Ułatwienie konfiguracji sieci dla urządzeń końcowych.
  - Prostsza konfiguracja: PortFast umożliwia łatwiejszą konfigurację portów przełączników dla urządzeń końcowych, co redukuje złożoność zarządzania siecią.
  - Redukcja błędów: Dzięki prostszej konfiguracji, ryzyko popełnienia błędów jest mniejsze, co prowadzi do bardziej stabilnej i niezawodnej sieci.

3.3.2 Wady

- Potencjalne ryzyko pętli sieciowych, jeśli PortFast zostanie błędnie skonfigurowany na portach trunk.
  - Ryzyko pętli: Jeśli PortFast zostanie przypadkowo włączony na portach trunk, może to prowadzić do powstania pętli w sieci, co może powodować poważne problemy z dostępnością i wydajnością sieci.
  - Trudności w diagnostyce: Problemy związane z błędną konfiguracją PortFast mogą być trudne do zdiagnozowania i naprawienia, co może wydłużać czas przestoju.

3.3.3 Zastosowanie w Topologii

W obecnej topologii PortFast jest używany na portach przełączników podłączonych do komputerów i innych urządzeń końcowych. Dzięki temu urządzenia te mogą szybciej uzyskać dostęp do sieci. PortFast jest skonfigurowany tylko na portach, które są bezpośrednio podłączone do urządzeń końcowych, aby uniknąć ryzyka pętli sieciowych.

3.4 Trunking

Trunking to technologia umożliwiająca przesyłanie ruchu sieciowego z wielu VLAN-ów przez jedno połączenie między przełącznikami. Trunking jest używany do łączenia przełączników w celu zapewnienia komunikacji między różnymi VLAN-ami.

3.4.1 Zalety

- Efektywne wykorzystanie połączeń między przełącznikami.
  - Większa przepustowość: Trunking pozwala na przesyłanie ruchu z wielu VLAN-ów przez jedno połączenie, co zwiększa efektywność wykorzystania dostępnych zasobów sieciowych.
  - Zmniejszenie liczby połączeń: Dzięki trunkingowi można zmniejszyć liczbę fizycznych połączeń między przełącznikami, co upraszcza topologię sieci.
- Umożliwienie komunikacji między różnymi VLAN-ami.
  - Elastyczność: Trunking umożliwia łatwą komunikację między VLAN-ami, co jest kluczowe dla aplikacji i usług wymagających dostępu do wielu segmentów sieci.
  - Centralizacja zasobów: Dzięki trunkingowi można centralizować zasoby, takie jak serwery i urządzenia sieciowe, co upraszcza zarządzanie i poprawia wydajność.
- Skalowalność i łatwość zarządzania.
  - Łatwa rozbudowa: Trunking ułatwia rozbudowę sieci, ponieważ nowe VLAN-y mogą być dodawane bez konieczności zmiany fizycznej topologii.
  - Prostsze zarządzanie: Zarządzanie połączeniami trunkowymi jest prostsze i bardziej efektywne niż zarządzanie wieloma pojedynczymi połączeniami między VLAN-ami.

3.4.2 Wady

- Złożoność konfiguracji.
  - Wymagana wiedza: Konfiguracja trunkingu wymaga zaawansowanej wiedzy na temat sieci i VLAN-ów, co może być wyzwaniem dla mniej doświadczonych administratorów.
  - Możliwość błędów: Błędna konfiguracja trunkingu może prowadzić do problemów z dostępnością i wydajnością sieci, co może być trudne do zdiagnozowania.
- Możliwość błędnej konfiguracji prowadząca do problemów z dostępnością sieci.
  - Ryzyko przerw w działaniu: Nieprawidłowa konfiguracja trunkingu może prowadzić do przerw w działaniu sieci, co może mieć poważne konsekwencje dla działalności biznesowej.
  - Trudności w diagnostyce: Problemy związane z trunkingiem mogą być trudne do zdiagnozowania i naprawienia, co może wydłużać czas przestoju.

3.4.3 Zastosowanie w Topologii

W obecnej topologii trunking jest używany do łączenia przełączników, co umożliwia przesyłanie ruchu z wielu VLAN-ów przez jedno połączenie. Dzięki temu sieć jest bardziej efektywna i łatwiejsza w zarządzaniu. Trunking pozwala na centralizację zasobów sieciowych i ułatwia komunikację między różnymi segmentami sieci.

3.5 EtherChannel

EtherChannel to technologia umożliwiająca połączenie kilku fizycznych łączy w jedno logiczne łącze w celu zwiększenia przepustowości i zapewnienia redundancji. EtherChannel jest używany na przełącznikach do łączenia wielu portów.

3.5.1 Zalety

- Zwiększenie przepustowości połączeń.
  - Większa przepustowość: EtherChannel łączy kilka fizycznych łączy w jedno logiczne łącze, co zwiększa przepustowość i pozwala na przesyłanie większej ilości danych.
  - Lepsze wykorzystanie zasobów: Dzięki EtherChannel, sieć może efektywniej wykorzystywać dostępne zasoby, co prowadzi do lepszej wydajności.
- Redundancja i większa niezawodność.
  - Redundancja połączeń: EtherChannel zapewnia redundancję, co oznacza, że w przypadku awarii jednego łącza, pozostałe łącza nadal działają, zapewniając ciągłość działania sieci.
  - Poprawa niezawodności: Dzięki redundancji, sieć jest bardziej niezawodna i mniej podatna na awarie, co jest kluczowe dla utrzymania ciągłości działania.
- Łatwiejsze zarządzanie połączeniami.
  - Prostsza konfiguracja: EtherChannel upraszcza zarządzanie połączeniami sieciowymi, ponieważ administratorzy muszą zarządzać jednym logicznym łączem zamiast kilku fizycznych.
  - Elastyczność: EtherChannel umożliwia łatwe dodawanie i usuwanie fizycznych łączy bez wpływu na działanie logicznego łącza, co ułatwia zarządzanie i rozbudowę sieci.

3.5.2 Wady

- Złożoność konfiguracji.
  - Wymagana wiedza: Konfiguracja EtherChannel wymaga zaawansowanej wiedzy na temat sieci, co może być wyzwaniem dla mniej doświadczonych administratorów.
  - Możliwość błędów: Błędna konfiguracja EtherChannel może prowadzić do problemów z dostępnością i wydajnością sieci, co może być trudne do zdiagnozowania.
- Potencjalne problemy z kompatybilnością.
  - Kompatybilność sprzętu: Wszystkie przełączniki i routery muszą obsługiwać EtherChannel, co może wymagać modernizacji starszego sprzętu.
  - Koszty: Zakup nowego sprzętu, który obsługuje EtherChannel, może być kosztowny, szczególnie w dużych sieciach.

3.5.3 Zastosowanie w Topologii

W obecnej topologii EtherChannel jest używany do łączenia przełączników w celu zwiększenia przepustowości i zapewnienia redundancji połączeń. Dzięki temu sieć jest bardziej wydajna i niezawodna. EtherChannel pozwala na łączenie wielu fizycznych łączy w jedno logiczne łącze, co poprawia przepustowość i niezawodność sieci.

3.6 OSPF (Open Shortest Path First)

OSPF (Open Shortest Path First) to protokół routingu używany do znajdowania najkrótszych ścieżek w sieci IP. OSPF jest stosowany w dużych sieciach, gdzie dynamiczne trasowanie jest kluczowe dla utrzymania wydajności.

3.6.1 Zalety

- Szybka konwergencja.
  - Krótszy czas konwergencji: OSPF szybko dostosowuje się do zmian w topologii sieci, co minimalizuje czas przestoju i zapewnia ciągłość działania sieci.
  - Zwiększona niezawodność: Szybka konwergencja OSPF oznacza, że sieć jest bardziej niezawodna i mniej podatna na awarie.
- Skalowalność i wsparcie dla dużych sieci.
  - Obsługa dużych sieci: OSPF jest zaprojektowany do pracy w dużych sieciach, co czyni go idealnym rozwiązaniem dla korporacji i dostawców usług internetowych.
  - Hierarchiczna struktura: OSPF wykorzystuje hierarchiczną strukturę z obszarami, co ułatwia zarządzanie i skalowanie sieci.
- Wykorzystanie metryk do znajdowania optymalnych tras.
  - Metryki kosztów: OSPF wykorzystuje metryki kosztów do oceny i wyboru optymalnych tras, co zapewnia efektywne wykorzystanie zasobów sieciowych.
  - Dynamiczne trasowanie: Dzięki dynamicznemu trasowaniu, OSPF automatycznie dostosowuje trasy w zależności od zmieniających się warunków sieciowych.

3.6.2 Wady

- Złożoność konfiguracji.
  - Wymagana wiedza: Konfiguracja OSPF wymaga zaawansowanej wiedzy na temat sieci, co może być wyzwaniem dla mniej doświadczonych administratorów.
  - Możliwość błędów: Błędna konfiguracja OSPF może prowadzić do problemów z dostępnością i wydajnością sieci, co może być trudne do zdiagnozowania.
- Wymagania dotyczące zasobów sprzętowych.
  - Wymagania sprzętowe: OSPF może wymagać więcej zasobów sprzętowych niż inne protokoły routingu, co może zwiększać koszty.
  - Koszty operacyjne: Utrzymanie sieci opartej na OSPF może być bardziej kosztowne ze względu na wymagania dotyczące zasobów i zarządzania.

3.6.3 Zastosowanie w Topologii

W obecnej topologii OSPF jest używany do dynamicznego trasowania w sieci. Dzięki temu sieć może szybko dostosowywać się do zmian i znajdować optymalne trasy dla przesyłanych danych. OSPF zapewnia skalowalność i niezawodność, co jest kluczowe dla dużych sieci korporacyjnych.

3.7 HSRP (Hot Standby Router Protocol)

HSRP (Hot Standby Router Protocol) to protokół zapewniający wysoką dostępność poprzez umożliwienie skonfigurowania grupy routerów jako zapasowych dla siebie nawzajem. W przypadku awarii głównego routera, zapasowy router przejmuje jego funkcje.

3.7.1 Zalety

- Zapewnienie wysokiej dostępności.
  - Redundancja: HSRP zapewnia redundancję, co oznacza, że w przypadku awarii głównego routera, zapasowy router automatycznie przejmuje jego funkcje, zapewniając ciągłość działania sieci.
  - Zmniejszenie przestojów: Dzięki HSRP, ryzyko przestojów w sieci jest znacznie mniejsze, co jest kluczowe dla utrzymania ciągłości działania.
- Automatyczne przełączanie w przypadku awarii.
  - Szybka reakcja: HSRP automatycznie przełącza ruch na zapasowy router w przypadku awarii głównego routera, co minimalizuje przerwy w działaniu sieci.
  - Prostsze zarządzanie: Automatyczne przełączanie zmniejsza konieczność ręcznego zarządzania awariami, co ułatwia pracę administratorów sieci.
- Łatwość konfiguracji.
  - Prosta konfiguracja: Konfiguracja HSRP jest stosunkowo prosta i nie wymaga zaawansowanej wiedzy, co ułatwia wdrożenie tej technologii w sieci.
  - Dokumentacja i wsparcie: HSRP jest dobrze udokumentowany i szeroko wspierany przez producentów sprzętu, co ułatwia jego konfigurację i zarządzanie.

3.7.2 Wady

- Dodatkowe wymagania dotyczące sprzętu.
  - Koszty sprzętu: Konfiguracja HSRP wymaga dodatkowego sprzętu (zapasowych routerów), co może zwiększać koszty.
  - Zasoby sieciowe: HSRP może zwiększać zapotrzebowanie na zasoby sieciowe, co może prowadzić do wyższych kosztów operacyjnych.
- Możliwość problemów z synchronizacją.
  - Problemy z synchronizacją: Synchronizacja stanów między głównym a zapasowym routerem może czasami sprawiać problemy, co może wpływać na niezawodność sieci.
  - Trudności w diagnostyce: Problemy z synchronizacją mogą być trudne do zdiagnozowania i naprawienia, co może wydłużać czas przestoju.

3.7.3 Zastosowanie w Topologii

W obecnej topologii HSRP jest używany do zapewnienia wysokiej dostępności routerów. Dzięki temu w przypadku awarii głównego routera, zapasowy router automatycznie przejmuje jego funkcje, zapewniając ciągłość działania sieci. HSRP jest skonfigurowany na routerach, aby zapewnić redundancję i minimalizować ryzyko przestojów.

3.8 Routing Między VLAN-ami

Routing między VLAN-ami umożliwia komunikację między różnymi VLAN-ami w sieci. Jest to realizowane za pomocą routerów lub przełączników warstwy 3.

3.8.1 Zalety

- Umożliwienie komunikacji między różnymi segmentami sieci.
  - Łatwiejsza komunikacja: Routing między VLAN-ami umożliwia łatwą komunikację między różnymi segmentami sieci, co jest kluczowe dla aplikacji i usług wymagających dostępu do wielu VLAN-ów.
  - Centralizacja zasobów: Dzięki routingowi między VLAN-ami można centralizować zasoby, takie jak serwery i urządzenia sieciowe, co upraszcza zarządzanie i poprawia wydajność.
- Centralizacja zarządzania politykami sieciowymi.
  - Prostsze zarządzanie: Routing między VLAN-ami umożliwia centralne zarządzanie politykami sieciowymi, co ułatwia wdrażanie i egzekwowanie zasad bezpieczeństwa.
  - Skuteczniejsza kontrola: Dzięki centralizacji, administratorzy mają lepszą kontrolę nad dostępem do zasobów sieciowych i mogą łatwiej monitorować ruch sieciowy.
- Poprawa bezpieczeństwa i kontroli dostępu.
  - Precyzyjna kontrola dostępu: Routing między VLAN-ami umożliwia dokładniejszą kontrolę dostępu do zasobów sieciowych, co zwiększa bezpieczeństwo danych.
  - Izolacja ruchu: Dzięki izolacji ruchu między VLAN-ami, można lepiej chronić dane przed nieautoryzowanym dostępem i złośliwym oprogramowaniem.

3.8.2 Wady

- Złożoność konfiguracji.
  - Wymagana wiedza: Konfiguracja routingu między VLAN-ami wymaga zaawansowanej wiedzy na temat sieci, co może być wyzwaniem dla mniej doświadczonych administratorów.
  - Możliwość błędów: Błędna konfiguracja routingu między VLAN-ami może prowadzić do problemów z dostępnością i wydajnością sieci, co może być trudne do zdiagnozowania.
- Wymagania dotyczące sprzętu.
  - Koszty sprzętu: Routing między VLAN-ami wymaga routerów lub przełączników warstwy 3, co może zwiększać koszty sprzętu.
  - Zasoby sieciowe: Routing między VLAN-ami może zwiększać zapotrzebowanie na zasoby sieciowe, co może prowadzić do wyższych kosztów operacyjnych.

3.8.3 Zastosowanie w Topologii

W obecnej topologii routing między VLAN-ami jest realizowany przez routery, które umożliwiają komunikację między różnymi VLAN-ami, zapewniając jednocześnie bezpieczeństwo i kontrolę dostępu. Dzięki temu sieć może efektywnie zarządzać ruchem między różnymi segmentami, poprawiając wydajność i bezpieczeństwo.

3.9 IPv6

IPv6 to najnowsza wersja protokołu internetowego, która zapewnia większą przestrzeń adresową i poprawę funkcji w porównaniu do IPv4. IPv6 jest używany w nowoczesnych sieciach, aby zapewnić skalowalność i wydajność.

3.9.1 Zalety

- Większa przestrzeń adresowa.
  - Rozwiązanie problemu wyczerpania adresów IPv4: IPv6 oferuje znacznie większą przestrzeń adresową (2^{128} adresów), co pozwala na unikanie problemów związanych z wyczerpaniem adresów IP.
  - Możliwość podłączania większej liczby urządzeń: Dzięki większej przestrzeni adresowej, IPv6 umożliwia podłączenie znacznie większej liczby urządzeń, co jest kluczowe dla Internetu Rzeczy (IoT).
- Lepsze wsparcie dla mobilności i bezpieczeństwa.
  - Mobilność: IPv6 wspiera lepsze mechanizmy mobilności, co umożliwia płynne przemieszczanie się urządzeń między różnymi sieciami bez utraty połączenia.
  - Bezpieczeństwo: IPv6 ma wbudowane wsparcie dla IPsec, co zapewnia lepsze mechanizmy szyfrowania i uwierzytelniania, zwiększając bezpieczeństwo komunikacji.
- Uproszczony nagłówek pakietu.
  - Efektywność przetwarzania: Uproszczony nagłówek IPv6 pozwala na szybsze przetwarzanie pakietów przez routery, co poprawia wydajność sieci.
  - Redukcja obciążenia: Mniejsza liczba pól w nagłówku IPv6 zmniejsza obciążenie urządzeń sieciowych, co prowadzi do lepszej wydajności i mniejszego zużycia zasobów.

3.9.2 Wady

- Złożoność migracji z IPv4.
  - Trudności migracyjne: Migracja z IPv4 do IPv6 może być skomplikowana i czasochłonna, wymagająca dokładnego planowania i koordynacji.
  - Koszty: Proces migracji może wiązać się z kosztami związanymi z aktualizacją sprzętu i oprogramowania oraz szkoleniem personelu.
- Wymagania dotyczące wsparcia sprzętowego.
  - Kompatybilność sprzętu: Wiele starszych urządzeń sieciowych może nie obsługiwać IPv6, co może wymagać ich wymiany lub modernizacji.
  - Koszty: Zakup nowego sprzętu, który obsługuje IPv6, może być kosztowny, szczególnie w dużych sieciach.

3.9.3 Zastosowanie w Topologii

W obecnej topologii IPv6 jest używany obok IPv4, co zapewnia skalowalność i przyszłościową kompatybilność sieci. Dzięki temu sieć może obsługiwać większą liczbę urządzeń i lepiej zarządzać zasobami. Wdrażanie IPv6 zapewnia również lepsze wsparcie dla mobilności i bezpieczeństwa, co jest kluczowe w nowoczesnych sieciach.

3.10 ACL (Access Control List)

ACL (Access Control List) to technologia używana do kontrolowania dostępu do zasobów sieciowych na podstawie adresów IP i innych kryteriów. ACL są stosowane na routerach i przełącznikach warstwy 3.

3.10.1 Zalety

- Precyzyjna kontrola dostępu.
  - Granularność: ACL umożliwiają bardzo precyzyjne definiowanie, które urządzenia lub użytkownicy mogą mieć dostęp do określonych zasobów sieciowych, co zwiększa bezpieczeństwo.
  - Elastyczność: ACL pozwalają na tworzenie różnych reguł dostępu w zależności od potrzeb, co umożliwia elastyczne zarządzanie dostępem.
- Poprawa bezpieczeństwa sieci.
  - Blokowanie nieautoryzowanego dostępu: ACL mogą blokować ruch z nieautoryzowanych adresów IP, co chroni sieć przed atakami z zewnątrz.
  - Monitorowanie ruchu: ACL umożliwiają monitorowanie i logowanie ruchu sieciowego, co pomaga w wykrywaniu i analizowaniu potencjalnych zagrożeń.
- Możliwość definiowania szczegółowych polityk dostępu.
  - Polityki bezpieczeństwa: ACL pozwalają na wdrażanie szczegółowych polityk bezpieczeństwa, które określają, kto i w jaki sposób może korzystać z zasobów sieciowych.
  - Zarządzanie ruchem: Dzięki ACL można zarządzać ruchem sieciowym, priorytetować pewne typy ruchu lub ograniczać przepustowość dla innych, co poprawia wydajność sieci.

3.10.2 Wady

- Złożoność konfiguracji.
  - Wymagana wiedza: Konfiguracja ACL wymaga zaawansowanej wiedzy na temat sieci, co może być wyzwaniem dla mniej doświadczonych administratorów.
  - Możliwość błędów: Błędna konfiguracja ACL może prowadzić do problemów z dostępnością i bezpieczeństwem sieci, co może być trudne do zdiagnozowania.
- Możliwość degradacji wydajności przy dużej liczbie reguł.
  - Obciążenie zasobów: Duża liczba reguł ACL może obciążać zasoby sprzętowe, co może prowadzić do degradacji wydajności sieci.
  - Koszty operacyjne: Zarządzanie dużą liczbą reguł ACL może być czasochłonne i kosztowne, wymagając regularnych aktualizacji i monitorowania.

3.10.3 Zastosowanie w Topologii

W obecnej topologii ACL są używane do kontrolowania dostępu do różnych części sieci. Dzięki temu sieć jest bardziej bezpieczna, a dostęp do zasobów jest precyzyjnie kontrolowany. ACL są skonfigurowane na routerach i przełącznikach warstwy 3, aby zapewnić granularną kontrolę dostępu i poprawić bezpieczeństwo sieci.

3.11 Port Security

Port Security to funkcja przełączników, która umożliwia ograniczenie dostępu do portów na podstawie adresów MAC urządzeń. Dzięki temu można zapobiec nieautoryzowanemu dostępowi do sieci.

3.11.1 Zalety

- Poprawa bezpieczeństwa sieci poprzez ograniczenie dostępu.
  - Ochrona przed nieautoryzowanymi urządzeniami: Port Security pozwala na ograniczenie liczby urządzeń, które mogą być podłączone do portu, co zapobiega podłączaniu nieautoryzowanych urządzeń.
  - Kontrola dostępu: Port Security umożliwia przypisanie konkretnych adresów MAC do portów, co pozwala na precyzyjną kontrolę dostępu do sieci.
- Ochrona przed atakami typu MAC flooding.
  - Zapobieganie atakom: Port Security chroni sieć przed atakami typu MAC flooding, które polegają na zalewaniu przełącznika fałszywymi adresami MAC w celu wyczerpania jego tablicy MAC.
  - Zwiększenie stabilności sieci: Dzięki ochronie przed atakami, Port Security przyczynia się do zwiększenia stabilności i niezawodności sieci.
- Łatwość konfiguracji i zarządzania.
  - Prosta konfiguracja: Konfiguracja Port Security jest stosunkowo prosta i może być łatwo wdrożona przez administratorów sieci.
  - Monitorowanie i alarmowanie: Port Security umożliwia monitorowanie nieautoryzowanych prób dostępu i generowanie alarmów, co ułatwia zarządzanie bezpieczeństwem sieci.

3.11.2 Wady

- Możliwość blokowania autoryzowanych urządzeń.
  - Ryzyko fałszywych alarmów: Port Security może czasami blokować autoryzowane urządzenia, jeśli ich adresy MAC nie zostały poprawnie skonfigurowane.
  - Utrudnienia w diagnostyce: Problemy związane z Port Security mogą być trudne do zdiagnozowania i naprawienia, co może prowadzić do przestojów.
- Konieczność regularnej aktualizacji konfiguracji.
  - Zmiany w sieci: W miarę dodawania nowych urządzeń do sieci, konfiguracja Port Security musi być regularnie aktualizowana, co może być czasochłonne.
  - Koszty operacyjne: Regularne aktualizacje konfiguracji mogą zwiększać koszty operacyjne, szczególnie w dużych sieciach.

3.11.3 Zastosowanie w Topologii

W obecnej topologii Port Security jest używany na przełącznikach, aby ograniczyć dostęp do portów na podstawie adresów MAC urządzeń. Dzięki temu sieć jest bardziej bezpieczna i chroniona przed nieautoryzowanym dostępem. Port Security jest skonfigurowany na portach przełączników, które są podłączone do komputerów i innych urządzeń końcowych.

Bibliografia

[1] https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/layer2/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide_Release_5-x_chapter4.html z dnia 10.05.2024

[2] https://community.cisco.com/t5/networking-knowledge-base/cisco-access-control-lists-acl/ta-p/4182349 z dnia 10.05.2024

[3] https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8651-21.html z dnia 10.05.2024

[4] https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_digital_building_series_switches/software/15-2_5_ex/configuration_guide/b_1525ex_consolidated_cdb_cg/b_1525ex_consolidated_cdb_cg_chapter_0110101.html z dnia 10.05.2024

[5] https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html z dnia 10.05.2024