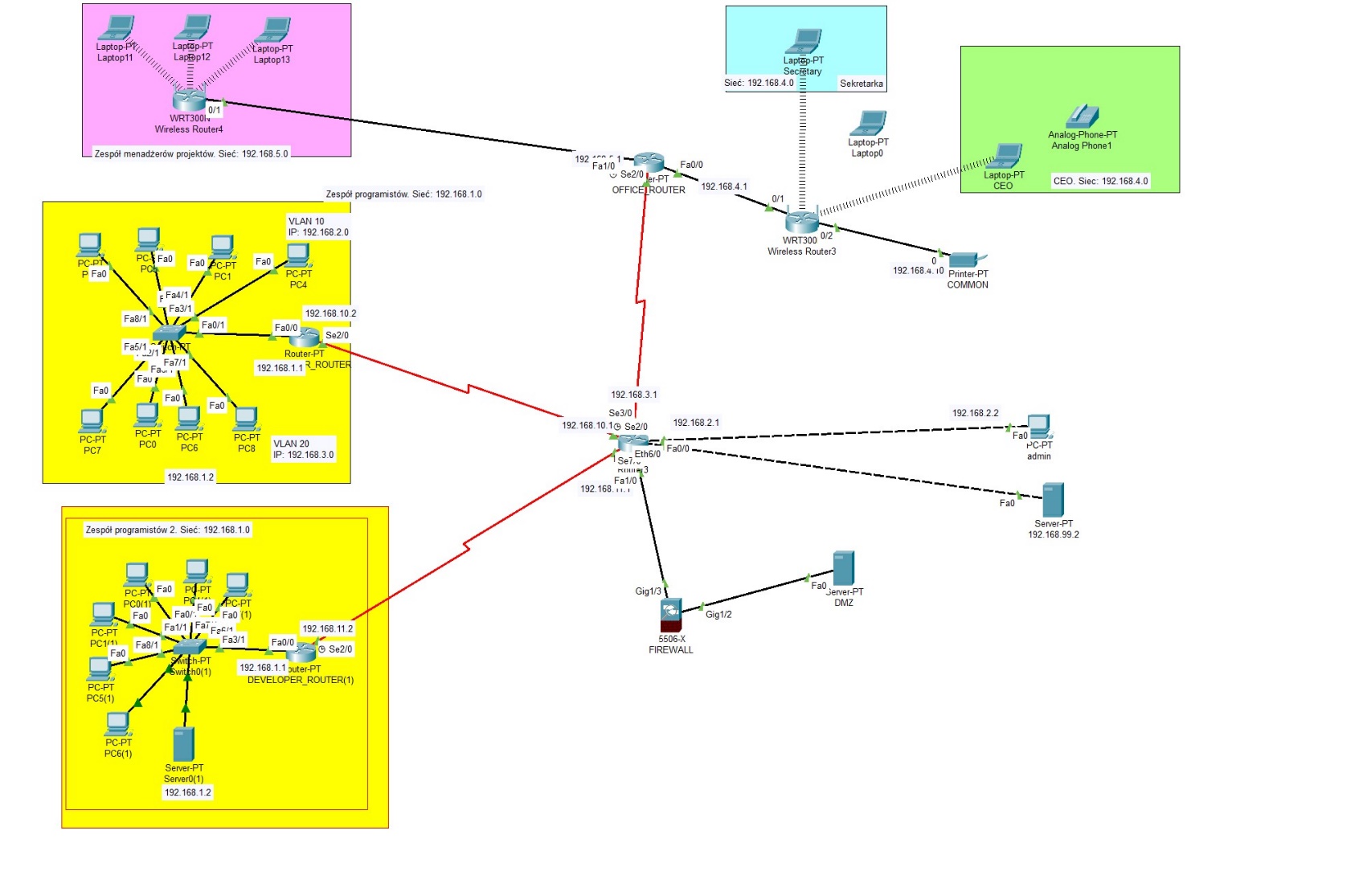
|  |  |
| --- | --- |
| Politechnika Świętokrzyska | |
| **Zespół:** Daniel Rogowski, David Salwa | **Grupa:** 1ID24B |
| **Projekt:** Pracownia Informatyczna |  |



Powyższe zdjęcie przedstawiania obraz zbudowanej przez zespół infrastruktury. Powyższa sieć odzwierciedla pracownię informatyczną, w której każdy „pokój” jest podzielony kolorem. Najważniejszym z punktu widzenia działalności pracowni jest „zielony” pokój. W tym pokoju swoją podsieć ma szef całej firmy, który jest podłączony do swojej podsieci (routera) za pomocą WI-FI. Jest tutaj włączone DHCP dla każdego urządzenia. Obok niego znajduje się sieć, w której pracuje seketarka/sekretarz (kolor niebieski), który również jest podłączony za pomocą WIFI i adres jest przypisane automatycznie (DHCP). Obie te sieci mają dostęp do drukarki o statycznym adresie *192.168.4.10*.

* konfiguracja serwera DHCP

Kolor „różowy” identyfikuje sieć (*192.168.5.0)* project managerów, osób zarządzającymi projektami. Tutaj również został zastosowany DHCP oraz podłączenie bezprzewodowe (WI-FI). W związku z tym, że przedstawiany pokój wymaga komunikacji z programistami (kolor żółty), została udostępniona możliwość komunikacji z tymi „pokojami”.

* VLANy

Kolor „żółty” przedstawia dwa pokoje programistów. Tak jak wyżej zostało opisane przedstawiane pokoje muszą posiadać komunikację z kolorem różowym. Pokój przedstawiony wyżej posiada również 2 VLANy, o adresach VLAN10: *192.168.2.0* oraz VLAN20: *192.168.3.0*, obie te „podsieci” komunikują się ze „światem” za pomocą routera, którego domyślną bramą jest adres *192.168.1.1*, natomiast adresem komunikującym się ze światem (adres) routera to: *192.168.10.2.* Wszystkie urządzenia są podłączone „fizycznie” (przez kabel) oraz posiadają wedle swoich „podsieci” automatycznie nadane adres IP (DHCP). Dodatkowo switch działa jako „trunk”, tak aby mógł przepuszczać ruch z tych podsieci do routera.

Drugi pokój „Żółty”, który jest umiejscowiony niżej w odróżnieniu od powyższego nie posiada VLAN-ów oraz adresy DHCP są przydzielane nie z routera, tylko z serwera DHCP. Reszta funkcjonalności jest identyczna do wyżej opisanego pokoju. Różnice jakie posiada to inne adresy IP: *192.168.1.0*, natomiast serwer DHCP ma statyczny adres IP: *192.168.1.2,* bramą domyślną jest adres: *192.168.1.1*, natomiast adresem komunikacyjnym ze „światem” jest adres *192.168.11.2.*

* standardowe oraz rozszerzone listy dostępu ACL

Komputerem bez „koloru” po prawej stronie jest komputer serwisowy o adresie *192.168.2.2*. Ta sieć jest zarezerwowana tylko dla tego komputera. Dodatkowo żaden z innych komputerów nie ma możliwości komunikacji z tym komputerem, natomiast ten komputer ma możliwość komunikacji z innymi komputerami. Taka funkcja została wdrożona dzięki listów ACL.

* dostępy ssh

Komputer bez „koloru” jest również jedynym który ma dostęp do „głównego” routera (czyli tego który jest połączony do 5 innych urządzeń) po porcie 22 czyli ssh w celu możliwości konfiguracji ustawień oraz dostępów w sieci.

* zabezpieczenia przez atakami MAC

Obok pokoju „Niebieskiego” który jest obok pokoju CEO jest komputer który chce się włamać do sieci wi-fi, dzięki zabezpieczeniom adresacji MAC nie ma takiej możliwości. Aby mógł zostać dodany należy dodać jego adres MAC do routera który zezwoli na połączenia.

* konfiguracja syslogu

W serwerze Server0(1) dodaliśmy również usługę syslog która śledzi wydarzenia na routerach w zółtej sieci oraz w routerze głównym dzięki czemu można podejrzeć kiedy zostały wykonany zmiany na tych routerach. Co ułatwi nam monitorowanie zmian i ułatwi sprawdzenie kiedy ktoś mógł coś podejrzanego wykonać.

* konfiguracja AAA

W tym samym serwerze dodaliśmy usługę AAA która pozwala nam zalogować się za pomocą tych samych danych logowania na innych serwerach. Usługę tą wykorzystują routery na żółtym tle oraz główny.

* konfiguracja NTP

Dodatkowo, w ramach dalszego ulepszania naszej infrastruktury sieciowej, zaimplementowaliśmy protokół Network Time Protocol (NTP) na trzech wcześniej wspomnianych routerach wykorzystujących EIGRP. Decyzja ta wynika z potrzeby synchronizacji czasu w całej sieci, co jest kluczowe dla utrzymania właściwego porządku sekwencyjnego zdarzeń i logów systemowych. NTP zapewnia, że wszystkie urządzenia sieciowe, w tym routery, mają ustawiony dokładny i jednolity czas, co jest niezbędne dla efektywnego monitorowania i rozwiązywania problemów sieciowych. Ta integracja NTP z naszymi routerami EIGRP dodatkowo zwiększa efektywność naszej sieci, umożliwiając bardziej precyzyjne śledzenie i analizę danych sieciowych, co jest nieocenione w utrzymaniu wysokiej wydajności i niezawodności naszej infrastruktury sieciowej.

* Dynamiczne protokoły routingu.

W procesie projektowania naszej sieci korporacyjnej, zdecydowaliśmy się na wybór Enhanced Interior Gateway Routing Protocol (EIGRP) jako naszego protokołu dynamicznego routingu, głównie ze względu na jego zdecentralizowaną architekturę, szybką konwergencję i skalowalność. Każdy router w sieci przechowuje własną kopię tabeli routingu, co zapewnia odporność na zakłócenia i stabilność działania sieci. EIGRP wykorzystuje algorytm DUAL do efektywnego obliczania i aktualizowania ścieżek routingu, co jest kluczowe w dynamicznych środowiskach korporacyjnych. Jego zdolność do obsługi dużych sieci oraz kompatybilność z różnorodnym sprzętem sieciowym sprawiają, że jest to idealne rozwiązanie dla naszej rozrastającej się infrastruktury, umożliwiając łatwą integrację z istniejącymi komponentami sieciowymi i upraszczając zarządzanie siecią.