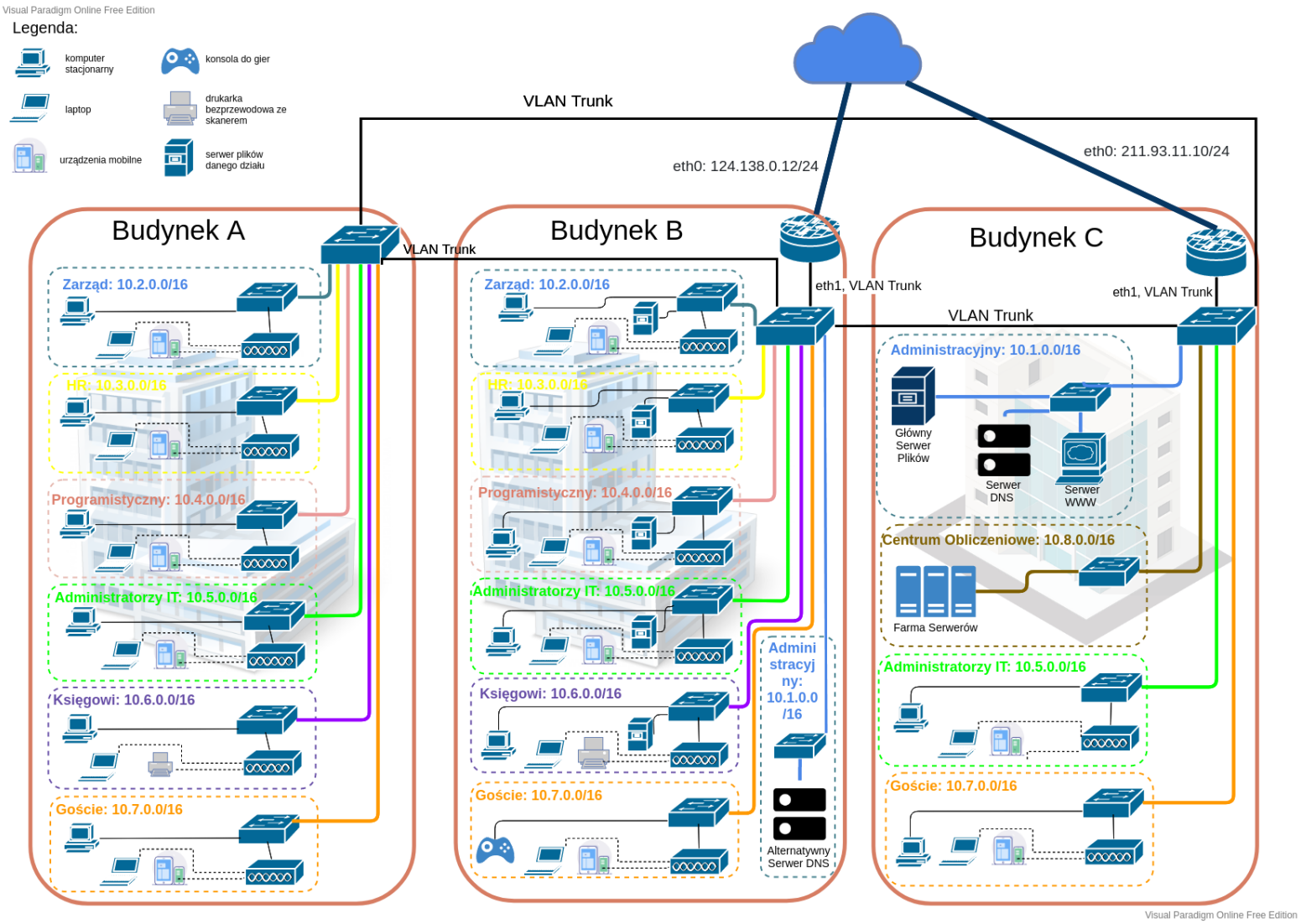
SIK - Zadanie 3

Jakub Zacharczuk jz418488

August 2021



Rysunek 1: Rysunek poglądowy przedstawiający konfigurację sieci, w oddzielnym pliku pdf znajduje się grafika w znacznie wyższej jakości

1 Opis konfiguracji sieci

W budynkach B i C znajduję się router z firewallem podłączony do internetu. W każdym z budynków znajduje się jeden główny switch wyposażony w STP. Każdy główny switch jest bezpośrednio połączony z każdym innym głównym switchem VLAN Trunkiem. Dodatkowo główny switch B i C są połączone bezpośrednio z routerem wewnątrz swojego budynku. Nasza sieć zawiera 8 podsieci: po jednej dla każdego z 5 działów, podsieć administracyjną, odseparowana podsieć dostępna tylko dla gości oraz podsieć związaną z centrum obliczeniowym. Każdy dział w każdym z budynków dysponuje własnym switchem, podłączonym do głównego switcha w swoim budynku. Dodatkowo każdy dział w każdym budynku dysponuje punktem dostępu umożliwiającym bezprzewodowe podłączenie do sieci. Wszyscy pracownicy mają dostęp do wspólnego serwera plików. Aby zapewnić szczególną ochronę podsieci działu zarządu, dział ten dysponuje własnym serwerem plików. W tym projekcie, ze względu na nieograniczone fundusze, każdy dział dysponuje własnym serwerem plików znajdującym się w budynku B. Pozwoli to, w zależności od potrzeb, na np. postawienie własnego repozytorium w dziale programistycznym, czy własnej bazy danych w dziale księgowym. W celu zapewnienia bezpieczeństwa, dostęp do serwerów plików jest ograniczony hasłem.

1.1 Podsieci

Adres podsieci jest postaci: 10.X.0.0, gdzie X stanowi VLAN ID odpowiedniej sekcji.

Nazwa sekcji	VLAN ID	IP
Administracja	1	10.1.0.0/16
Zarząd	2	10.2.0.0/16
Dział HR	3	10.3.0.0/16
Programistyczny	4	10.4.0.0/16
Administratorzy IT	5	10.5.0.0/16
Księgowi	6	10.6.0.0/16
Goście	7	10.7.0.0/16
Centrum Obliczeniowe	8	10.8.0.0/16

2 Wymagany sprzęt

- 2 routery (wyposażone w DHCP, Firewall, NAT)
- 20 switchy
- 14 punktów dostępu
- 6 serwerów plików
- 2 serwery DNS
- 1 serwer WWW

3 Tablice tras

Poniżej przedstawię tablice tras dla obu routerów - podstawową, wykorzystywaną gdy router ma dostęp do internetu oraz alternatywną, gdy router nie ma dostępu do internetu. Przyjmijmy, że przyznany statycznie adres IP routera B w podsieci eth1 to 10.0.0.1 oraz routera C 10.0.0.2.

3.1 Router B

3.1.1 Gdy router ma dostęp do internetu

cel	maska	brama	interfejs
0.0.0.0	0.0.0.0	124.138.0.23	eth0
124.138.0.0	255.255.255.0	0.0.0.0	eth0
10.1.0.0	255.255.0.0	0.0.0.0	eth1/1
10.2.0.0	255.255.0.0	0.0.0.0	eth1/2
10.3.0.0	255.255.0.0	0.0.0.0	eth1/3
10.4.0.0	255.255.0.0	0.0.0.0	eth1/4
10.5.0.0	255.255.0.0	0.0.0.0	eth1/5
10.6.0.0	255.255.0.0	0.0.0.0	eth1/6
10.7.0.0	255.255.0.0	0.0.0.0	eth1/7
10.8.0.0	255.255.0.0	0.0.0.0	eth1/8

3.1.2 Gdy router nie ma dostępu do internetu

Zamieniamy pierwszy wiersz na przekierowanie do routera C

cel	maska	brama	interfejs
0.0.0.0	0.0.0.0	10.0.0.2	eth1

3.2 Router C

3.2.1 Gdy router ma dostęp do internetu

cel	maska	brama	interfejs
0.0.0.0	0.0.0.0	211.93.11.224	eth0
211.93.11.0	255.255.255.0	0.0.0.0	eth0
10.1.0.0	255.255.0.0	0.0.0.0	eth1/1
10.2.0.0	255.255.0.0	0.0.0.0	eth1/2
10.3.0.0	255.255.0.0	0.0.0.0	eth1/3
10.4.0.0	255.255.0.0	0.0.0.0	eth1/4
10.5.0.0	255.255.0.0	0.0.0.0	eth1/5
10.6.0.0	255.255.0.0	0.0.0.0	eth1/6
10.7.0.0	255.255.0.0	0.0.0.0	eth1/7
10.8.0.0	255.255.0.0	0.0.0.0	eth1/8

3.2.2 Gdy router nie ma dostępu do internetu

Zamieniamy pierwszy wiersz na przekierowanie do routera C

cel	maska	brama	interfejs
0.0.0.0	0.0.0.0	10.0.0.1	eth1

4 NAT, Firewall

Router C ma otwarte porty HTTP i HTTPS (80 i 443), które są mapowane na odpowiednie porty serwera WWW. Router z Firewallem oraz NAT uniemożliwia inicjację z zewnątrz połączenia z lokalnymi urządzeniami. Dodatkowo ze względów bezpieczeństwa firewall i NAT odseparowują ruch w sieci uniemożliwiając między innymi: komunikację ze sobą między działami o VLAN ID ze zbioru 2-6, 8 (natomiast każdy z tych działów ma dostęp do

działu administracji). NAT blokuje również pakiety wysyłane z podsieci gości, które nie są skierowane do internetu. Ponadto serwer WWW, również ze względów bezpieczeństwa, nie ma dostępu do serwerów plików.

5 Przydział adresów IP

Dynamicznym przydzielaniem adresów IP zajmują się oba routery wyposażone w DHCP. Konfigurujemy dwa serwery DHCP, gdyż awaria jedynego serwera DHCP może doprowadzić do całkowitej zapaści sieci. Hostom będziemy przydzielać adres IP dynamicznie. Aby uniknąć sytuacji gdzie router przyzna dwóm urządzeniom ten sam adres, wskazujemy aby router w budynku B, przyznając adres urządzeniu z działu X, dysponował adresami od 10.X.0.1 do 10.X.127.255 natomiast router w budynku C od 10.X.128.0 do 10.X.128.254. Statycznie możemy przydzielić adresy dla: routerów (wewnątrz interfejsu eth1), serwerów DNS, głównego serwera plików, lokalnych serwerów plików każdym z działów, serwera WWW.

6 DNS

Schemat przydzielania wewnętrznych nazw, sposób rozwiązywania nazw - czy będzie używany wewnętrzny serwer DNS, czy zewnętrzna usługa. Konfiguracja DNS (plik strefy). Należy wziąć pod uwagę, że tylko serwer WWW powinien być widoczny z zewnątrz. Nasza firma dysponuje dwoma serwerami DNS, podstawowym i alternatywnym. Serwery będą odpowiedzialne za odwzorowanie nazw na adresy IP wewnętrznych hostów podsieci np. przykładowy host działu HR, może mieć adres hr5.corp.datavac.pl, natomiast baza danych działu księgowego to: db.acc.corp.datavac.pl . Ponadto serwery będą również odpowiedzialne za pamiętanie i odwzorowanie nazw zewnętrznych adresów na adres IP. Strona WWW ma zarejestrowaną nazwę domenową www.datavac.pl u zewnętrznej firmy i jest kierowana na IP routera C - 211.93.11.10/24. Sieć dostępna dla gości nie ma dostępu do wewnętrznego serwera DNS, zatem będzie ona korzystała z usług firmy zewnętrznej.