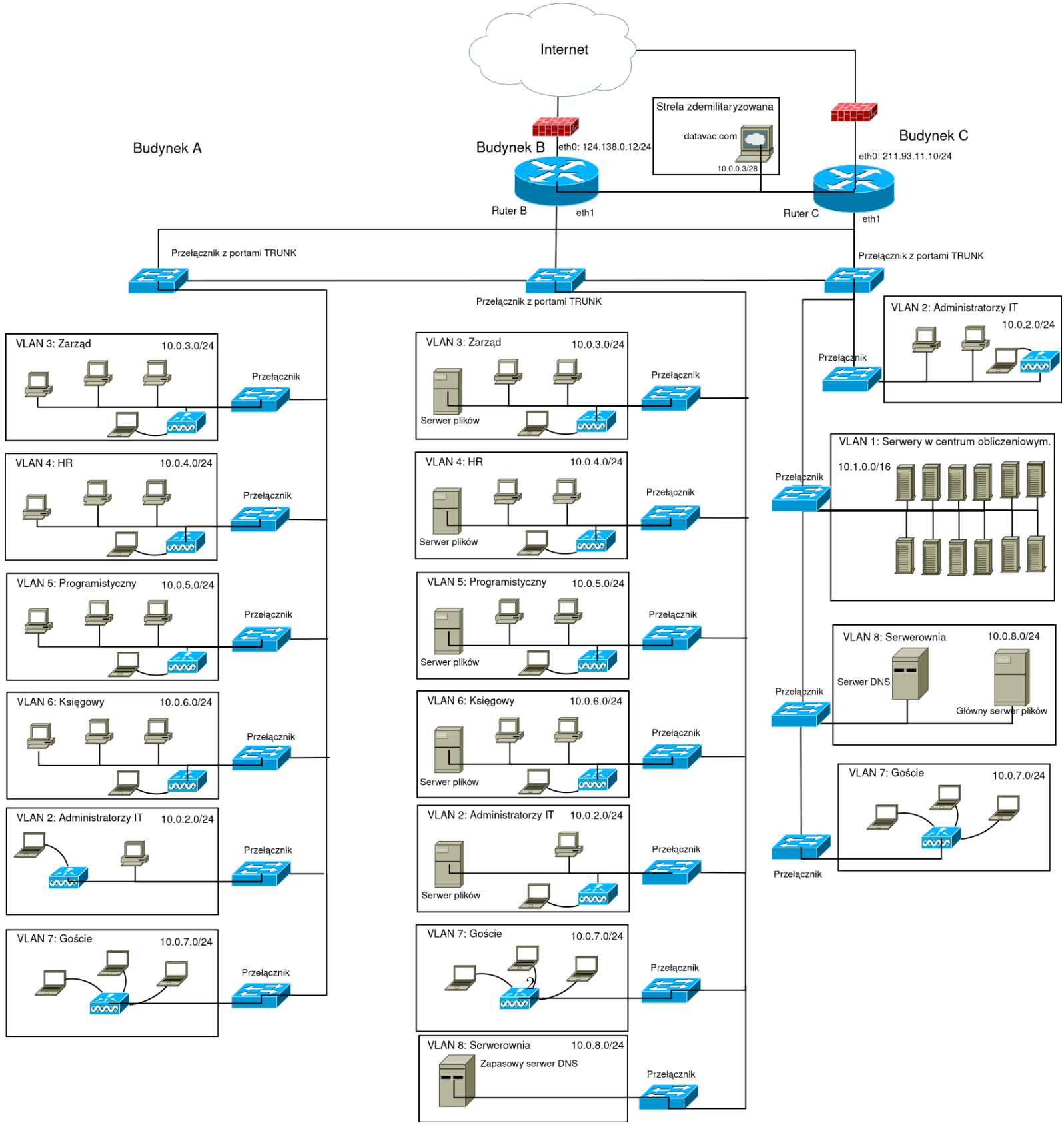
# Sieci komputerowe, zadanie 3

Adam Boguszewski, nr albumu: 417730

Czerwiec 2021

# Projekt sieci



## Podział na sieci

Sieć została podzielona w sumie na 9 wirtualnych podsieci. Własną podsieć ma każdy z wymienionych w treści zadania dział, istnieją również sieć dla gości, serwerownia oraz mała sieć dla strefy zdemilitaryzowanej. Sieci połączone są przełącznikami, pomiędzy budynkami występuje tzw. trunking w celu połączenia hostów z różnych budynków w tę samą sieć wirtualną. Przełączniki układają się w cykl, ale rozwiązują ten problem za pomocą algorytmu drzewa rozpinającego. Zgodnie z poleceniem, do połączeń przewodowych między budynkami wykorzystano światłowód.
Domyślne rutery powinny być konfigurowane następująco: hosty z budynku A i B jako domyślny ruter mają ruter B, a hosty z budynku C jako domyślny ruter mają ruter C. Na rysunku oznaczenie eth1 przy ruterach zbiorczo oznacza interfejsy eth1.0, eth1.1, ..., eth1.9.

### Sieć ruterów

W celu trasowania do siebie nawzajem, rutery tworzą dodatkową, niezaznaczoną na rysunku sieć VLAN 9 o adresie 10.0.9.0/28. Są one jedynymi urządzeniami w tej podsieci, dzięki czemu przesyłane informacje nie mogą zostać podsłuchane.

### Sieć centrum obliczeniowego

Składa się ona z serwerów w centrum obliczeniowym. Nie zostało wyspecjalizowane, czy serwery w centrum obliczeniowym także potrzebują bazy danych, repozytorium oraz systemu do zarządzania projektem, jeśli tak, to należałoby skonfigurować dodatkowy serwer w tym celu. Założono też, że w tym dziale połączenie będzie odbywać się jedynie przewodowo, zatem nie umieszczono w nim punktu dostępu Wi-Fi.

### Sieci poszczególnych działów

Każdy dział ma hosty w przynajmniej dwóch budynkach, w związku z tym prawie wszyscy dodatkowe serwery (baza danych, repozytorium, system zarządzania projektem) zostały umieszczone na jednej fizycznej maszynie w budynku B. Wyjątkiem jest sieć zarządu, która te serwery mieści na osobnej maszynie ze względów wyższego bezpieczeństwa. Na rysunku szara maszyna w podsieciach w budynku B symbolizuje te maszyny logiczne. Każdy dział ma punkt dostępowy Wi-Fi (na rysunku niebieskie urządzenie wewnątrz działów) w celu zapewnienia komunikacji bezprzewodowej oraz podłączone do sieci fizyczne komputery. Sieci są zabezpieczone w warstwie aplikacji za pomocą haseł oraz innych ograniczeń tej warstwy jak np. role w aplikacji.

### Sieć gościnna

Sieć dla gości składa się jedynie z punktów dostępowych Wi-Fi. Ruter blokuje dostęp urządzeń z tej sieci do pozostałych sieci w firmie, w związku z czym np.

korzysta ona z zewnętrznego serwera DNS, a nie wewnętrznego. Jest chroniona hasłem, które można uzyskać od pracowników firmy.

#### Sieć serwerowni

Sieć serwerowni jest dodatkową siecią administracyjną. W budynku C znajduje się w niej jedna fizyczna maszyna, na której znajdują się wewnętrzny serwer DNS oraz serwer plików, służący do wymiany informacji pomiędzy działami. W budynku B znajduje się jedynie zapasowy serwer DNS, działający na tej samej fizycznej maszynie co serwery dla innych działów.

#### Strefa zdemilitaryzowana

W strefie zdemilitaryzowanej o adresie 10.0.0.0/28 znajduje się serwer WWW kryjący się pod adresem datavac.com. Fizyczna maszyna, na której działa ten serwer znajduje się w budynku C (na osobnej maszynie lub na tej samej co ruter C, więcej informacji w sekcji Potrzebny sprzęt).

### Ochrona

Zapory ogniowe na ruterach B i C blokują dostęp z zewnątrz, jedynie zezwalają na dostęp do serwera WWW znajdującego się w strefie zdemilitaryzowanej. Wszystkie sieci są chronione hasłami, a dodatkowo rutery blokują dostęp między siecią gości a pozostałymi sieciami. Sieć zarządu potrzebuje szczególnej ochrony, zatem na swój serwer plików dostaje osobną maszynę fizyczną, a także jest znacznie mocniej zabezpieczona w warstwie aplikacji niż pozostałe sieci.

## Potrzebny sprzęt

- 2 maszyny na rutery
- 3 przełączniki obsługujące tzw. trunking za pomocą światłowodu
- 17 zestawów przełączników zwykłych, po jednym dla każdej podsieci w każdym budynku, ilość wyjść w zestawach powinna być różna, np. serwery w centrum obliczeniowym potrzebują zestawu obsługującego w sumie 1000 wyjść, natomiast w pozostałych działach wystarczy kilkadziesiąt wyjść
- 1 maszyna na serwery plików dla działów oraz zapasowy serwer DNS
- 1 maszyna na serwer plików dla zarządu
- 1 maszyna na główny serwer DNS oraz serwer plików do wymiany między działami
- 1 maszyna serwerowa na serwer WWW
- 13 punktów dostępowych

Kilka serwerów logicznych można umieścić na jednej maszynie, zatem wszystkie działy poza zarządem mogą uruchomić specjalne oprogramowanie (repozytorium, baza danych, system zarządzania projektami) na jednej maszynie. Nie znamy dokładnego planu budynku, więc zakładamy, że jeden punkt dostępowy dla każdej podsieci (poza serwerami w centrum obliczeniowym) w każdym budynku wystarczy. W celu zaoszczędzenia pieniędzy lub miejsca można umieścić też wszystkie te serwery (poza serwerem plików dla zarządu) na tych samych maszynach, co routery. Wówczas w sumie wystarczyłyby nam trzy maszyny.

# Tablice trasowania

Poniżej dostawca B oznacza operatora, który dostarcza połączenie z internetem do budynku B, a dostawca C jest operatorem dla budynku C. W przypadku awarii dostawcy C, ruter w budynku B musi jedynie usunąć z tablicy trasowania wpis o sieci tamtego dostawcy (211.93.11.0), analogicznie dla awarii dostawcy B i rutera w budynku C.

### Tablica trasowania rutera B

| cel | maska | interfejs | brama |
|---|---|---|---|
| 10.0.0.0 | 255.255.255.240 | eth1.0 | 0.0.0.0 |
| 10.1.0.0 | 255.255.0.0 | eth1.1 | 0.0.0.0 |
| 10.0.2.0 | 255.255.255.0 | eth1.2 | 0.0.0.0 |
| 10.0.3.0 | 255.255.255.0 | eth1.3 | 0.0.0.0 |
| 10.0.4.0 | 255.255.255.0 | eth1.4 | 0.0.0.0 |
| 10.0.5.0 | 255.255.255.0 | eth1.5 | 0.0.0.0 |
| 10.0.6.0 | 255.255.255.0 | eth1.6 | 0.0.0.0 |
| 10.0.7.0 | 255.255.255.0 | eth1.7 | 0.0.0.0 |
| 10.0.8.0 | 255.255.255.0 | eth1.8 | 0.0.0.0 |
| 10.0.9.0 | 255.255.255.240 | eth1.9 | 0.0.0.0 |
| 124.138.0.0 | 255.255.255.0 | eth0 | 0.0.0.0 |
| 211.93.11.0 | 255.255.255.0 | eth1.9 | 10.0.9.2 |
| 0.0.0.0 | 0.0.0.0 | eth0 | 124.138.0.23 |

**Tablica trasowania rutera B w przypadku awarii łącza dostawcy B**

| cel | maska | interfejs | brama |
|---|---|---|---|
| 10.0.0.0 | 255.255.255.240 | eth1.0 | 0.0.0.0 |
| 10.1.0.0 | 255.255.0.0 | eth1.1 | 0.0.0.0 |
| 10.0.2.0 | 255.255.255.0 | eth1.2 | 0.0.0.0 |
| 10.0.3.0 | 255.255.255.0 | eth1.3 | 0.0.0.0 |
| 10.0.4.0 | 255.255.255.0 | eth1.4 | 0.0.0.0 |
| 10.0.5.0 | 255.255.255.0 | eth1.5 | 0.0.0.0 |
| 10.0.6.0 | 255.255.255.0 | eth1.6 | 0.0.0.0 |
| 10.0.7.0 | 255.255.255.0 | eth1.7 | 0.0.0.0 |
| 10.0.8.0 | 255.255.255.0 | eth1.8 | 0.0.0.0 |
| 10.0.9.0 | 255.255.255.240 | eth1.9 | 0.0.0.0 |
| 0.0.0.0 | 0.0.0.0 | eth1.9 | 10.0.9.2 |

**Tablica trasowania rutera C**

| cel | maska | interfejs | brama |
|---|---|---|---|
| 10.0.0.0 | 255.255.255.240 | eth1.0 | 0.0.0.0 |
| 10.1.0.0 | 255.255.0.0 | eth1.1 | 0.0.0.0 |
| 10.0.2.0 | 255.255.255.0 | eth1.2 | 0.0.0.0 |
| 10.0.3.0 | 255.255.255.0 | eth1.3 | 0.0.0.0 |
| 10.0.4.0 | 255.255.255.0 | eth1.4 | 0.0.0.0 |
| 10.0.5.0 | 255.255.255.0 | eth1.5 | 0.0.0.0 |
| 10.0.6.0 | 255.255.255.0 | eth1.6 | 0.0.0.0 |
| 10.0.7.0 | 255.255.255.0 | eth1.7 | 0.0.0.0 |
| 10.0.8.0 | 255.255.255.0 | eth1.8 | 0.0.0.0 |
| 10.0.9.0 | 255.255.255.240 | eth1.9 | 0.0.0.0 |
| 124.138.0.0 | 255.255.255.0 | eth1.9 | 10.0.9.1 |
| 211.93.11.0 | 255.255.255.0 | eth0 | 0.0.0.0 |
| 0.0.0.0 | 0.0.0.0 | eth0 | 211.93.11.224 |

**Tablica trasowania rutera C w przypadku awarii łącza dostawcy C**

| cel | maska | interfejs | brama |
|---|---|---|---|
| 10.0.0.0 | 255.255.255.240 | eth1.0 | 0.0.0.0 |
| 10.1.0.0 | 255.255.0.0 | eth1.1 | 0.0.0.0 |
| 10.0.2.0 | 255.255.255.0 | eth1.2 | 0.0.0.0 |
| 10.0.3.0 | 255.255.255.0 | eth1.3 | 0.0.0.0 |
| 10.0.4.0 | 255.255.255.0 | eth1.4 | 0.0.0.0 |
| 10.0.5.0 | 255.255.255.0 | eth1.5 | 0.0.0.0 |
| 10.0.6.0 | 255.255.255.0 | eth1.6 | 0.0.0.0 |
| 10.0.7.0 | 255.255.255.0 | eth1.7 | 0.0.0.0 |
| 10.0.8.0 | 255.255.255.0 | eth1.8 | 0.0.0.0 |
| 10.0.9.0 | 255.255.255.240 | eth1.9 | 0.0.0.0 |
| 0.0.0.0 | 0.0.0.0 | eth1.0 | 10.0.9.1 |

# Reguły NAT

Przychodzące z zewnątrz pakiety przysyłane na port 80 (HTTP) lub 443 (HTTPS) routerów zostają przekierowane do serwera WWW znajdującego się w strefie zdemilitaryzowanej. Pozostałe porty są zamknięte na nowe połączenia, aby sieć była niedostępna ze świata zewnętrznego. Tabela funkcji NAT rutera B wygląda następująco:

| adres zewnętrzny | adres wewnętrzny |
|---|---|
| 124.138.0.12:80 | 10.0.0.3:80 |
| 124.138.0.12:443 | 10.0.0.3:443 |

Natomiast dla rutera C:

| adres zewnętrzny | adres wewnętrzny |
|---|---|
| 211.93.11.10:80 | 10.0.0.3:80 |
| 211.93.11.10:443 | 10.0.0.3:443 |

# Przydzielanie adresów IP

Maszyny serwerowe w podsieciach działów otrzymują stałe adresy, według schematu: 10.0.<id sieci>.3, na przykład w sieci działu programistycznego będzie to 10.0.5.3. Stałe adresy IP można przydzielić też maszynom w serwerowni (10.0.8.3 dla serwera plików, 10.0.8.4 dla serwera DNS, 10.0.8.5 dla zapasowego serwera DNS) oraz serwerowi WWW (10.0.0.3). Ruter B w odpowiednich sieciach ma adres 10.0.<id sieci>.1, a ruter C ma adresy 10.0.<id sieci>.2 dla odpowiednich interfejsów (dla przykładu, w sieci serwerów w centrum obliczeniowym te adresy to odpowiednio 10.1.0.1 i 10.1.0.2). Pozostałe adresy IP mogą być przydzielane dynamicznie przy pomocy serwera DHCP, którego agenty działają na

tych samych maszynach co rutery (a sam serwer jest umiejscowiony na maszynie routera C).

## Schemat przydzielania nazw

Nazwa serwera WWW datavac.com jest obsługiwana przez zewnętrzną usługę, powinna ona być w stanie kierować na oba rutery, ponieważ oba mają określone reguły NAT przekierowujące na ten serwer.
Firma skorzysta z wewnętrznego serwera DNS. Adresem serwera głównego jest 10.0.8.4, zaś nazwą domeny datavac.com. Jedną z rozpoznawalnych nazw jest exchange-server wskazujące na adres 10.0.8.3, które jest nazwą serwera służącego do wymiany informacji pomiędzy działami. Dodatkowo własne nazwy posiadają serwery plików w każdym dziale według schematu <nazwa działu>-fileserver, np. nazwa zarzad-fileserver jest mapowana na adres 10.0.3.3. Domyślnie nie jest planowane nazywanie każdego hosta, jednak serwer DHCP w połączeniu z serwerem DNS powinny zaradzić temu problemowi w razie potrzeby.
W ramach potrzeb firmy można też skonfigurować np. adres pocztowy.