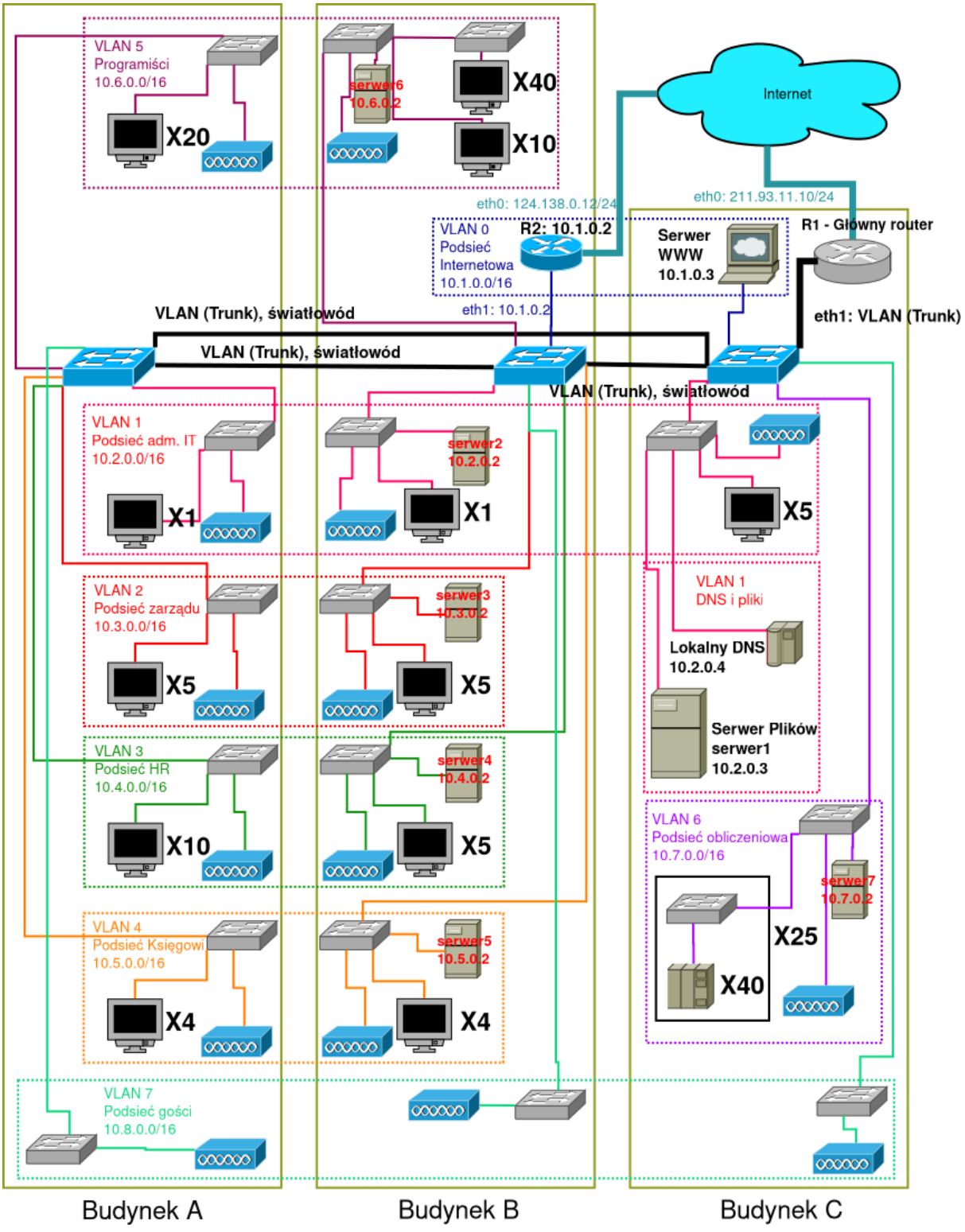
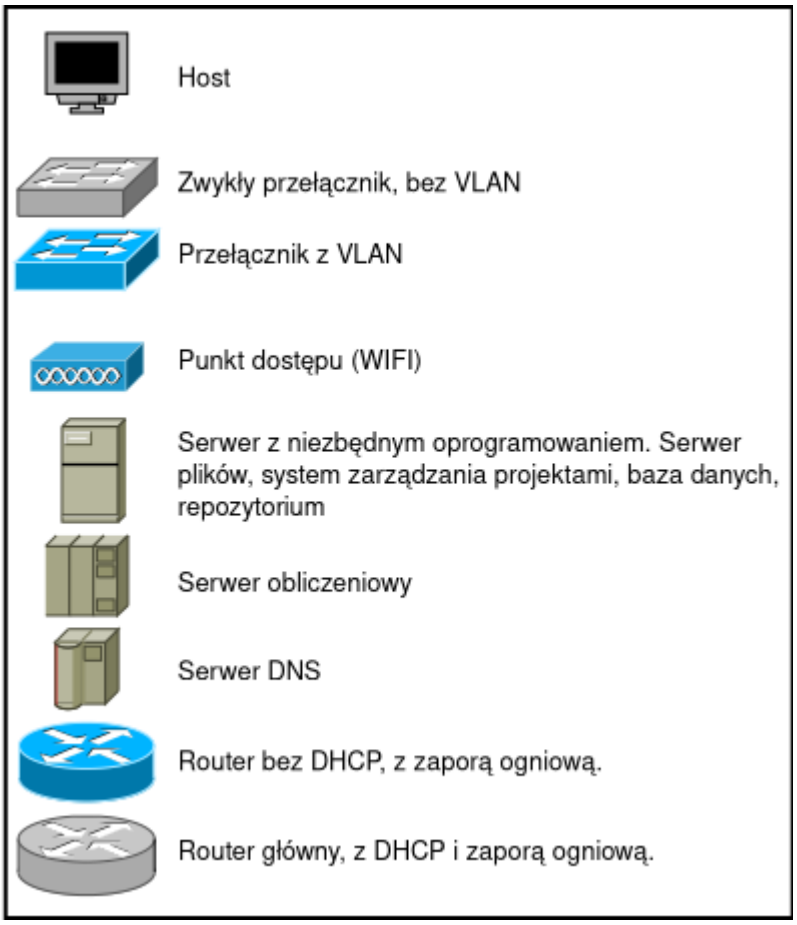
Sieci Komputerowe - Zadanie 3

Autor: Andrzej Stalke

Indeks: ****

1. **Rysunek przedstawiający konfigurację sieci.**





1.5. Ogólny opis

Podstawą całej sieci są 3 główne przełączniki, po jednym na budynek, pozwalające na utworzenie wielu sieci VLAN. Połączone są ze sobą przy pomocy światłowodów (z trunkingiem). Przy ich pomocy budujemy 8 sieci VLAN, które połączone są ze sobą za pośrednictwem routera znajdującego się w budynku C (dalej nazywanego **R1** lub **Routerem głównym**). W budynku B znajduje się router **R2.** Szczegółowy opis routerów w dalszej części dokumentu.

Dla każdego działu zapewniona jest osobna sieć VLAN. Ponadto utworzona jest sieć zawierająca serwer WWW i router **R2** oraz osobna sieć dla gości w celu odseparowania ich od sieci firmowej. Goście mogą łączyć się przy pomocy zabezpieczonej hasłem sieci bezprzewodowej. Ewentualny dostęp przewodowy jest możliwy przez wybrane przełączniki. Adresy, maski i nazwy poszczególnych sieci zapisane są na rysunku.

Każdy dział posiada w swojej sieci własny lokalny serwer. Każdy z nich znajduje się w budynku **B** (wyjątek: centrum obliczeniowe ma w budynku **C**). Każda z tych maszyn ma adres **10.X.0.2** w swojej podsieci i nazwę domenową **serwerX**, gdzie **X** to stosowny numer. Ponadto pozwalają na logowanie tylko pracowników z działu w którego sieci się znajdują i udostępniają usługi: współdzielenie danych między pracownikami danego działu, system zarządzania projektami, baza danych, repozytorium. Jeśli dana usługa na to pozwala, to komunikacja jest prowadzona bezpiecznym, szyfrowanym kanałem. Oprócz serwerów lokalnych, w podsieci administratorów IT pod adresem IP **10.2.0.3** o nazwie domenowej

serwer1 dostępny jest serwer globalny, który zapewnia te same usługi co serwery lokalne, ale dla wszystkich pracowników firmy.
W każdym z budynków zajmowanych przez dział, oprócz hostów znajduje się: co najmniej jeden zwykły przełącznik podłączony do głównego przełącznika oraz punkt dostępu zapewniający dostęp do zabezpieczonej silnym hasłem sieci bezprzewodowej (**WI-FI).**
Jako, że największy przełącznik jaki byłem w stanie znaleźć w Internecie miał 48 portów Ethernet, to część sieci wymagało więcej niż jednego przełącznika. Taka sytuacja wystąpiła między innymi w dziale programistów w budynku **B** oraz w centrum obliczeniowym.

Wszystkie sieci VLAN połączone są za pomocą routera **R1**, który jest wyposażony w zaporę sieciową, NAT i serwer DHCP. Zajmuje on pierwszy dostępny adres IP w każdej z podsieci i służy jako brama domyślna. Router **R2** (adres **10.1.0.2)** służy jako zapasowy dostęp do Internetu w przypadku awarii łącza z którego korzysta **R1** (domyślnie cały ruch idzie przez łącze **R1**).
Zapory obu routerów zapewniają podstawową ochronę strefy DMZ i blokują ruch inicjowany z zewnątrz, który nie jest skierowany do serwera WWW.
Zapora routera **R1** ponadto pozwala gościom komunikować się tylko z innymi gośćmi, serwerem WWW oraz Internetem. Szczególnie chroni podsieć zarządu: nie pozwala na połączenia z serwerem plików zarządu spoza podsieci, a sam ruch jest ściśle analizowany i monitorowany pod kątem podejrzanych pakietów.

2. Potrzebny sprzęt:

- router z zaporą sieciową, NATem, serwerem DHCP i obsługą VLAN
- router z zaporą sieciową i NATem
- 3 przełączniki zdolne do utworzenia co najmniej 8 sieci VLAN do których można podłączyć światłowody i ethernet (lub jeśli takich nie ma, to należy uzyskać sprzęt, który to umożliwi).
- Co najmniej 15 punktów dostępu (więcej w razie potrzeby, to zależy od topologii budynku).
- 6 serwerów na lokalne serwery dla każdego działu.
- 1 serwer na serwer dla całej firmy.
- 1 serwer DNS
- 1 serwer WWW
- 41 zwykłych przełączników, z czego 26 musi mieć co najmniej 48 portów. Pozostałe zależnie od potrzeb.

3. Tablice tras routerów:

Tablica tras routera głównego R1			
Cel	**Brama**	**Maska**	**Interfejs**
0.0.0.0	211.93.11.224	0.0.0.0	eth0
211.93.11.0	0.0.0.0	255.255.255.0	eth0
10.1.0.0	0.0.0.0	255.255.0.0	eth1.0
10.2.0.0	0.0.0.0	255.255.0.0	eth1.1
10.3.0.0	0.0.0.0	255.255.0.0	eth1.2
10.4.0.0	0.0.0.0	255.255.0.0	eth1.3
10.5.0.0	0.0.0.0	255.255.0.0	eth1.4
10.6.0.0	0.0.0.0	255.255.0.0	eth1.5
10.7.0.0	0.0.0.0	255.255.0.0	eth1.6
10.8.0.0	0.0.0.0	255.255.0.0	eth1.7

Awaryjna tablica tras routera głównego R1			
Cel	**Brama**	**Maska**	**Interfejs**
0.0.0.0	10.1.0.2	0.0.0.0	eth1.0
10.1.0.0	0.0.0.0	255.255.0.0	eth1.0
10.2.0.0	0.0.0.0	255.255.0.0	eth1.1
10.3.0.0	0.0.0.0	255.255.0.0	eth1.2
10.4.0.0	0.0.0.0	255.255.0.0	eth1.3
10.5.0.0	0.0.0.0	255.255.0.0	eth1.4
10.6.0.0	0.0.0.0	255.255.0.0	eth1.5
10.7.0.0	0.0.0.0	255.255.0.0	eth1.6
10.8.0.0	0.0.0.0	255.255.0.0	eth1.7

Tablica tras routera R2 (awaryjna taka sama)			
Cel	**Brama**	**Maska**	**Interfejs**
0.0.0.0	124.138.0.23	0.0.0.0	eth0
124.138.0.0	0.0.0.0	255.255.255.0	eth0
10.1.0.0	0.0.0.0	255.255.0.0	eth1
10.2.0.0	10.1.0.1	255.255.0.0	eth1
10.3.0.0	10.1.0.1	255.255.0.0	eth1
10.4.0.0	10.1.0.1	255.255.0.0	eth1
10.5.0.0	10.1.0.1	255.255.0.0	eth1
10.6.0.0	10.1.0.1	255.255.0.0	eth1
10.7.0.0	10.1.0.1	255.255.0.0	eth1
10.8.0.0	10.1.0.1	255.255.0.0	eth1

4. Reguły NAT

Oba routery zapewniają dostęp do serwera WWW poprzez przekierowanie portu 80 (HTPP) i 443 (HTTPS) do maszyny znajdującej się w strefie **DMZ** pod adresem **10.1.0.3.**

5. Przydział adresów IP

Sieć dla gości otrzymuje adresy IP dynamicznie, a pozostałe podsieci statycznie (adres IP przypisany do adresu MAC). Adresy są przydzielane przez serwer DHCP na routerze **R1**.

6. Rozwiązywanie nazw

Pod adresem **10.2.0.4** znajduje się lokalny serwer **DNS**, który tłumaczy nazwy domenowe serwerów plików. Za tłumaczenie nazwy serwera WWW odpowiada zewnętrzny serwer DNS.

7. Podsumowanie

a. “Należy zapewnić bezpieczny transfer i swobodne współdzielenie danych w obrębie poszczególnych działów.” - zapewnione poprzez lokalny serwer zapewniony dla każdego działu, z którym komunikacja jest zabezpieczona. Ponadto hosty są w jednej sieci VLAN i mogą się komunikować.
b. “Należy zapewnić szczególną ochronę podsieci działu zarządu.” - dodatkowe reguły zapory sieciowej oraz analiza i monitoring ruchu pozwalają wykryć zagrożenia bezpieczeństwa.
c. “W każdym budynku należy zapewnić dostęp do Internetu także dla gości firmy (w taki sposób, aby goście nie mieli dostępu do zasobów firmowych).” - goście mają własną sieć, która jest odgrodzona od sieci firmowej przy pomocy zapory i w każdym budynku mają co najmniej jeden punkt dostępu.
d. “W każdym budynku powinna być zainstalowana sieć przewodowa zbudowana na bazie Ethernetu i sieć bezprzewodowa zbudowana na bazie

Wi-Fi.” - w każdym dziale, w każdym budynku zapewniona jest sieć przewodowa i bezprzewodowa.

e. “Każdy z działów powinien mieć możliwość udostępniania danych wyłącznie pracownikom swojego działu (dla innych działów te dane nie powinny być dostępne).” - zapewnione przez lokalne serwery.
f. “Powinna być także możliwość udostępniania pewnych danych wszystkim pracownikom firmy w taki sposób, by nie były one dostępne bezpośrednio z sieci zewnętrznej.” - zapewnione przez główny serwer, który jest niewidoczny z sieci zewnętrznej, ale widoczny w wewnętrznej.
g. “Firma będzie chciała udostępniać własny serwis WWW.” - dostępny jest serwer WWW, który znajduje się w strefie DMZ i dostęp do niego z sieci zewnętrznej jest możliwy dzięki zewnętrznej usłudze DNS i zmienionym ustawieniom NAT.
h. “Poszczególne działy firmy potrzebują serwerów z różnego rodzaju oprogramowaniem: systemem zarządzania projektami, bazą danych, repozytorium.” - usługi zapewnione przez lokalny serwer.