Politechnika Białostocka

Wydział Elektryczny

Katedra Telekomunikacji i Aparatury Elektronicznej

Instrukcja do zajęć laboratoryjnych

Temat ćwiczenia:

Zarządzanie usługami w systemie telefonii VoIP

Część 1: Przygotowanie i konfiguracja środowiska sieciowego

Numer ćwiczenia: **6**

Laboratorium z przedmiotu:
Zarządzanie sieciami i usługami telekomunikacyjnymi

Kod przedmiotu: TS2D200012

Instrukcję opracował:
dr inż. Andrzej Zankiewicz

Białystok 2015

1. Ogólna charakterystyka technologii VoIP

VoIP (ang. *Voice over Internet Protocol*) bardzo często nazywany jest telefonią internetową. Jest to technologia, która poprzez łącza internetowe czy też sieci dedykowane zapewnia transmisję dźwięku w postaci pakietów przy użyciu protokołu IP. Dzięki temu, że dane transportowane są przy użyciu protokołu pakietowego, można wyeliminować znaczny okres trwania rozmowy, który stanowi ciszę. Mianowicie, kiedy przesyłamy głos w postaci analogowej, kanał rozmowny jest nam przydzielany na cały czas trwania rozmowy, stając się tym samym niemożliwym do wykorzystania przez innych użytkowników. W przypadku przesyłania mowy w formie cyfrowej, użytkownik zajmuje kanał jedynie w czasie wypowiadania słów. Stanowi to znaczną oszczędność, ponieważ współdzielone zasoby sieciowe mogą być lepiej wykorzystane przez inne połączenie bądź też inną aplikację.

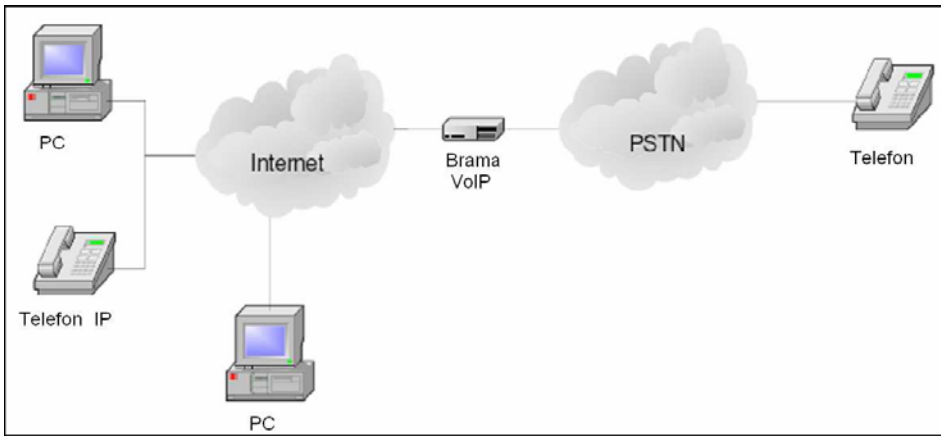
Technologia VoIP jest stosunkowo nowa. Pierwszy system telefonowania IP opracowany został w roku 1995 przez firmę VocalTec, pierwsza brama VoIP'owa ukazała się na rynku po upływie zaledwie roku. Obecnie, w czasach dynamicznego rozwoju technologii, połączenia VoIP odgrywają coraz większą rolę ze względu na stała poprawę ich jakości. Podstawowym zadaniem technologii VoIP jest integracja ruchu telefonicznego z transmisją danych oraz utworzenie jednej sieci, która będzie mogła transmitować wszelkiego rodzaju przekazy. Technologia ta wdrażana jest przez wiele firm, które produkują sprzęt i zajmują się oprogramowaniem dla telekomunikacji.

VoIP ma kilka zastosowań. Pierwsze, jakie możemy wyszczególnić to użycie tej technologii do prowadzenia rozmów telefonicznych zarówno międzymiastowych, jak również międzynarodowych. Połączenie może odbywać się bez zastosowania infrastruktury tradycyjnych operatorów telefonicznych. Sprawia to, iż uzyskuje się większą szybkość transmisji, niezawodność oraz znaczącą obniżkę kosztów. Wiąże się to jednak z szybkim dostępem do Internetu, a jak wiadomo nie w każdym zakątku świata taki dostęp istnieje. Kolejnym zastosowaniem jest integracja sieci korporacyjnych, mianowicie sieci transmisji głosu i danych, co powoduje obniżenie kosztów zarówno wdrożenia jak i późniejszej konserwacji.

Systemy VoIP mogą zostać wdrożone w celu realizacji usług telefonicznych w istniejącej już infrastrukturze, jednak muszą spełniać kilka warunków, a mianowicie:

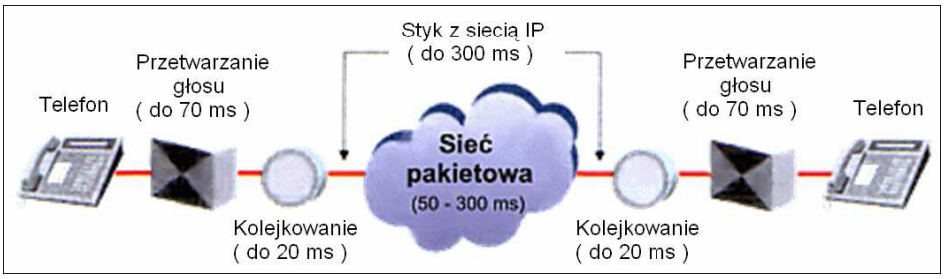
- wysoka wydajność przetwarzania zgłoszeń zarówno w sieci wewnętrznej jak i pomiędzy prywatnymi i publicznymi sieciami pakietowymi,
- skuteczne transmitowanie rozmów pomiędzy sieciami IP a sieciami z komutacją łączy w czasie rzeczywistym,
- skalowalność pod względem technicznym i ekonomicznym,
- akceptacja oraz implementacja standardów przez producentów sprzętu.

Ogólny schemat połączenia telefonii PSTN oraz technologii VoIP przedstawiono na rysunku 1.



Rys. 1. Schemat współpracy telefonii VoIP i PSTN [6].

Takie zestawienie wymaga użycia bramki VoIP, która łączy sieć PSTN z Internetem. W bramce następuje pakietyzacja i kompresja analogowego sygnału głosu oraz detekcja i usuwanie ciszy między słowami. Im stopień kompresji będzie wyższy, tym jakość po zdekodowaniu będzie niższa. Do najlepszych algorytmów kompresji głosu należą te, które generując najmniejszą ilość bitów po kompresji, nie powodują istotnych zmian przesyłanego głosu oraz zniekształceń, które uniemożliwiłyby odbiór takiego sygnału. Wypada także podkreślić fakt, że technologia VoIP ze względu na skończony czas kodowania i pakietyzacji oraz transfer za pośrednictwem zasobów systemu internetowego, przestała realizować transmisję głosu w czasie rzeczywistym wprowadzając opóźnienie głosu osiągające wartości rzędu nawet ok. 300 ms. Zostało to zilustrowane na rysunku 2



Rys. 2. Powstawanie opóźnień w telefonii IP [7].

Opisując proces przesyłania głosu miedzy rozmówcami przez sieć IP należy wspomnieć także o standardowych systemach telefonicznych, które zamieniają wypowiadane słowa na sygnał analogowy i transmitują go przez sieć. Takiemu sygnałowi towarzyszą szumy, które w przypadku jego wzmacniania również są wzmacniane, pogarszając tym samym jakość rozmowy. W przypadku usługi VoIP podczas przekształcenia mowy na sygnał cyfrowy, otrzymujemy ciąg danych binarnych (zer i jedynek), który nie zawiera żadnych informacji nadmiarowych (szumów) i który może być powielany dowolną ilość razy bez obawy o utratę jakości. Jest to podstawowa zaleta technologii cyfrowej.
Operacja zamieniająca mowę na postać cyfrową nosi nazwę modulacji impulsowo-kodowej PCM (ang. *Pulse Code Modulation*). PCM konwertuje mowę na

format cyfrowy próbkując sygnał analogowy 8 tysięcy razy na sekundę, czyli po 125 mikrosekund. Częstotliwość ta w zupełności wystarcza, gdyż słowa wypowiadane przez człowieka mieszczą się w częstotliwości poniżej 4 kHz. Standardowy system PCM do kodowania używa 8 bitów, więc mowę można transmitować przez łącze o przepustowości 64 kbps. Dodatkowo istnieje jeszcze 8-bitowy system kodowania, wykorzystujący adaptacyjną różnicową modulację impulsowo-kodową ADPCM (ang. *Adaptive Differential Pulse Code Modulation*). W tym przypadku wystarczy łącze o przepustowości 32 kbps. System ten zazwyczaj wykorzystywany jest przy połączeniach długodystansowych. Aby maksymalnie ograniczyć wymagane pasmo przenoszenia danych należy dążyć do tego, aby ilość bitów używana do kodowania była jak najmniejsza. Przy uŜyciu 8 bitów, system kodowania może rozróżnić 256 poziomów określających amplitudę sygnału, przy 4 bitach (jak w systemie ADPCM) amplituda sygnału porównywana jest do jednego z 64 poziomów. Do wyżej wymienionych systemów PCM oraz ADPCM dochodzą jeszcze standardy kompresji oparte na algorytmie kodowania z predykcją liniową LPC (ang. *Linear Predictive Coding*). Algorytm ten modeluje ludzki głos poprzez wykorzystanie powtarzających się elementów, wypowiadanych słów. W większości przypadków urządzenia oparte na algorytmie LPC pobierają do obróbki sygnały uformowane przy użyciu modulacji impulsowo-kodowej PCM.

2. Protokoły stosowane w technologii VoIP

Aby zapewnić prawidłową transmisję danych multimedialnych, w przypadku technologii VoIP – głosu, konieczne jest użycie specjalnych protokołów, a właściwie zestawu protokołów. Przesyłaniem głosu poprzez sieci oparte na protokole IP wiele firm zainteresowało się już na początku lat 90. w niedługim czasie na rynku pokazało się wiele rozwiązań realizujących przesyłanie danych audio przez sieć. Jednakże wszystkie aplikacje pracowały w oparciu o firmowe rozwiązania. Brak standardu w tej dziedzinie spowodował, iż niemożliwa była współpraca urządzeń różnych firm. Natychmiast zrodziła się potrzeba stworzenia uniwersalnego zestawu protokołów, która zaowocowała powstaniem zalecenia H.323, a niemalże równolegle z nim protokołu SIP (ang. *Session Initiation Protocol*). Pomimo tego, iż istnienia dwóch rozwiązań nie można określić mianem standardu, póki co obydwa mają swoich zwolenników i działają na rynku. Wyróżniamy protokoły należące do kilku grup, z których każda grupa pełni określone funkcje. Podział przedstawia się następująco:

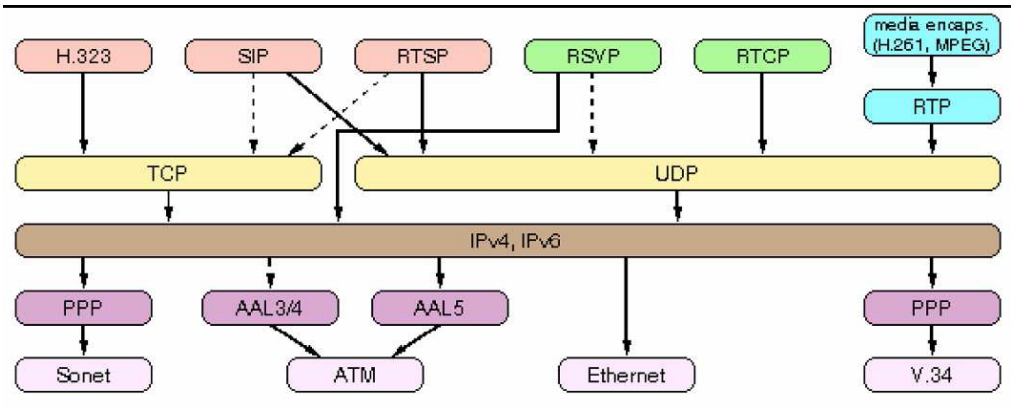
Sygnalizacja:
- SIP (*Session Initiation Protocol*)
- H.323
- SCCP (*Skinny Client Control Protocol*)
- MGCP (*Media Gateway Control Protocol*)
- RTSP (*Real Time Streaming Protocol*)

Transport w czasie rzeczywistym:
- RTP (*Real Time Protocol*)
- Kodeki

Transport pakietowy:

- TCP (*Transmission Control Protocol*)
- UDP (*User Datagram Protocol*)
- RTCP (*Real Time Transport Control Protocol*)

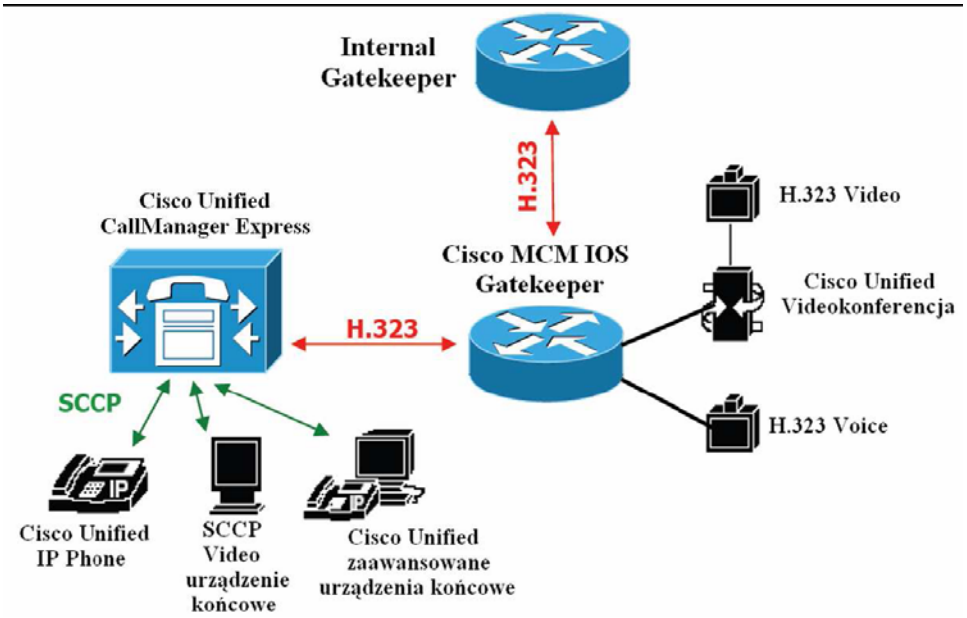
Rysunek 3 przedstawia zestawienie protokołów stosowanych w telefonii VoIP.



Rys. 3. Zestaw protokołów telefonii IP [8].

Protokół sygnalizacyjny Cisco SCCP

Protokół SCCP (ang. *Skinny Client Control Protocol*) jest standardowym protokołem firmy Cisco pozwalającym na prowadzenie rozmów w czasie rzeczywistym oraz umożliwia współpracę z innymi urządzeniami pracującymi w oparciu o działanie protokołu H.323. Rysunek 4 przedstawia przykładowe połączenie urządzeń wykorzystujących sygnalizację SCCP i H.323.



Rys. 4. Sygnalizacja urządzeń z wykorzystaniem protokołu SCCP i H.323 [4].

Klient komunikuje się z CallManager używając protokołu TCP/IP. Protokół SCCP wykorzystuje TCP/IP na porcie 2000 do komunikacji pomiędzy CallManager i telefonami IP. Numery portów TCP 2001 i 2002 wykorzystywane są do zarządzania QoS na routerach i switchach w celu zapewnienia wszystkim głosowym protokołom sygnalizacyjnym odpowiedniej przepustowości w sieci.

Protokół SCCP pozwala na korzystanie z takich funkcji jak: Call Hold, Call Park, Park Slot, Call Transfer Forward, Paging oraz Intercom, które mają na celu wstrzymywanie połączeń lub ich przekierowywanie. Konfiguracja wyżej wymienionych funkcji odbywa się na platformie CallManager.

Protokół SCCP wyposażony jest w narzędzie SmartDefense, które zapewnia całkowite połączenie w sieci pomiędzy urządzeniami oraz odpowiedni poziom bezpieczeństwa w komunikacji VoIP. Przesyłane pakiety są kontrolowane, zabezpieczane i odpowiednio grupowane. Protokół SCCP kontroluje zatem cały proces przesyłania danych i dzięki temu zwiększa poziom bezpieczeństwa.

Cisco Unified Communications Manager (CUCM) oraz Cisco Unified Communications Manager Express (CUCME) pozwalają na obsługę portów FXS, do których podłączą się urządzenia końcowe, głównie zwykłe telefony analogowe.

Protokół SCCP zarządza portami FXS oferując dodatkowe usługi, które nie są wspierane przez inne protokoły takie jak H.323, SIP czy MGCP, jednak może być także protokołem pośredniczącym w komunikacji z tymi protokołami ze względu na znacznie mniejsze zużywanie zasobów systemowych.

3. Cele i zakres ćwiczenia:

1. Zapoznanie się z podstawowymi informacjami teoretycznymi dotyczącymi wykorzystanych urządzeń i technologii.
2. Zapoznanie się ze sposobem łączenia urządzeń sieciowych wchodzących w skład systemu VoIP.
3. Konfiguracja urządzeń sieciowych:
   - Skonfigurowanie haseł: logowania z konsoli do trybu EXEC użytkownika, sesji terminala wirtualnego (Telnet), dostępu do trybu uprzywilejowanego EXEC.
   - Skonfigurowanie interfejsu szeregowego Serial 0 / Serial 1.
   - Utworzenie trasy statycznej i trasy domyślnej.
   - Zapoznanie się ze sposobem konfigurowania przełącznika.
   - Zdefiniowanie translacji NAT.
   - Skonfigurowanie interfejsów i podinterfejsów FastEthernet oraz pętli zwrotnej.
   - Zapoznanie się ze sposobem konfigurowania routera do obsługi protokołu DHCP (ang. *Dynamic Host Configuration Protocol*).
   - Poznanie mechanizmu dynamicznego przypisywania adresów podłączonym hostom.
4. Kopiowanie konfiguracji do pamięci NVRAM.

4. Plan wykonywania ćwiczenia laboratoryjnego

4.1 Ustawienia trybu konfiguracji routera

Wprowadzanie jakichkolwiek zmian w konfiguracji routera Cisco za pomocą interfejsu CLI jest możliwe po przejściu do trybu konfiguracji globalnej. Polecenia powodują zastosowanie instrukcji konfiguracyjnych w odniesieniu do całego systemu routera. Aby przejść do trybu konfiguracji globalnej należy użyć polecenia *configure terminal* i wówczas symbol zachęty ulegnie zmianie. Niektóre z trybów, do jakich można przejść z poziomu trybu konfiguracji globalnej, to:

- tryb interfejsu,
- tryb podinterfejsu,
- tryb linii,
- tryb konfiguracji protokołów routingu.

Po przejściu do jednego z tych trybów symbol zachęty routera zmienia się, wskazując na bieżący tryb konfiguracyjny. Wszelkie zmiany w konfiguracji będą dotyczyć tylko tych interfejsów lub procesów, które są objęte danym trybem. Aby powrócić z dowolnego z nich do trybu konfiguracji globalnej, należy wpisać polecenie *exit* bądź użyć kombinacji klawiszy *Ctrl-Z,* co spowoduje całkowite opuszczenie trybów konfiguracyjnych routera i powrót do trybu uprzywilejowanego. W celu uzyskania pomocy należy po znaku zachęty wstawić „?” i wybrać odpowiednią opcję.

4.2 Ustawienia i rodzaje haseł zabezpieczających urządzenia sieciowe

Aby użytkownicy mieli zdalny dostęp do routera przez połączenie Telnet, należy ustawić hasło dla jednej lub wielu linii terminali wirtualnych vty. Większość routerów Cisco obsługuje pięć linii vty o numerach od 0 do 4. Do ustawienia hasła dla linii vty używa się następujących poleceń:

```
Router(config)#line vty 0 4
Router(config-line)#password <hasło>
Router(config-line)#login
Router(config)#enable password <hasło>
Router(config)#enable secret <hasło>
```

Polecenia `enable password` i `enable secret` służą do ograniczania dostępu do trybu uprzywilejowanego. Polecenie `enable password` uzywane jest tylko wtedy, gdy nie zostało zastosowane polecenie `enable secret`. Zasadniczo należy korzystać z polecenia `enable secret`, ponieważ jest ono szyfrowane, podczas gdy polecenie `enable password` nie jest.

4.3 Zapoznanie się z wykorzystaniem polecenia „show”, służącego do sprawdzania konfiguracji urządzeń sieciowych.

W celu sprawdzenia konfiguracji istniejącej na urządzeniu bądź dokonanej samodzielnie należy korzystać z polecenia `show`. Poniżej przedstawiono kilka przydatnych i najczęściej używanych komend:

- **`show interfaces`**: wyświetla dane statystyczne dotyczące wszystkich interfejsów routera. Aby wyświetlić dane statystyczne dotyczące określonego

interfejsu, należy wpisać polecenie *show interfaces* wraz z nazwą określającą typ interfejsu oraz numerem gniazda/portu.
- **show clock**: wyświetla godzinę ustawioną w routerze.
- **show hosts**: wyświetla przechowywaną w pamięci podręcznej listę nazw i adresów hostów.
- **show users**: wyświetla nazwy wszystkich uzytkowników podłączonych do routera.
- **show history**: wyświetla historię wprowadzonych poleceń.
- **show flash**: wyświetla informacje o pamięci flash oraz o plikach IOS w niej przechowywanych.
- **show version**: wyświetla informacje o załadowanej w danym momencie wersji oprogramowania wraz z danymi o sprzęcie i urządzeniach.
- **show protocols**: wyświetla status wszystkich skonfigurowanych protokołów warstwy 3 w ujęciu globalnym i z uwzględnieniem konkretnych interfejsów.
- **show startup-config**: wyświetla zawartość pamięci NVRAM, jeśli istnieje i jest poprawna, lub prezentuje plik konfiguracyjny wskazywany przez zmienną środowiskową CONFIG_FILE.
- **show running-config**: wyświetla zawartość wykorzystywanego w danym momencie pliku konfiguracyjnego lub konfigurację dla konkretnego interfejsu bądź informacje o klasie odwzorowania.

4.4 Zarządzanie systemem plików.

W przypadku routera lub przełącznika Cisco aktywny plik konfiguracyjny znajduje się w pamięci RAM, a domyślna lokalizacja konfiguracji początkowej to pamięć NVRAM. Należy utworzyć kopię zapasową konfiguracji początkowej na wypadek utraty danych konfiguracyjnych. Jedna z kopii zapasowych konfiguracji może zostać zapisana na serwerze TFTP. Do utworzenia takiej kopii może zostać użyte polecenie *copy running-config tftp*. Etapy procesu kopiowania zostały opisane poniżej:
- Wprowadź polecenie *copy running-config tftp*.
- Wpisz adres IP serwera TFTP, na którym ma zostać zapisany plik konfiguracyjny.
- Podaj nazwę pliku.
- Potwierdź wybrane opcje.

W celu odtworzenia konfiguracji routera możliwe będzie załadowanie kopii zapasowej pliku konfiguracyjnego z serwera TFTP. Poniżej opisano poszczególne etapy tego procesu:
- Wprowadź polecenie *copy tftp running-config*.
- W wierszu poleceń wybierz plik konfiguracyjny na hoście lub w sieci.
- Wpisz adres IP serwera TFTP, na którym znajduje się plik konfiguracyjny.
- Podaj nazwę pliku.
- Potwierdź wyświetloną przez system nazwę pliku konfiguracyjnego oraz adres serwera.

4.4 Ustawienia interfejsu szeregowego (Serial 0 / Serial 1).

Każdy podłączony interfejs szeregowy musi mieć zdefiniowany adres IP i maskę podsieci, aby mógł przesyłać pakiety IP. Adres IP konfiguruje się za pomocą następujących poleceń:

```
Router(config)#interface serial 0/0
Router(config-if)#ip address <adres_ip> <maska_podsieci>
```

Synchroniczne interfejsy szeregowe (np.: V.35) wymagają sygnału zegarowego sterującego komunikacją. W większości środowisk sygnał zegarowy dostarczany jest przez urządzenie DCE, takie jak CSU/DSU. Domyślnie routery Cisco są urządzeniami DTE, ale można je skonfigurować jako urządzenia DCE. W przypadku bezpośrednio połączonych ze sobą łączy szeregowych, na przykład w laboratorium, jedna ze stron musi być traktowana jako urządzenie DCE i dostarczać sygnał zegarowy. Polecenie `clock rate` powoduje włączenie zegara i określenie jego szybkości. Dostępne szybkości w bitach na sekundę to: 1200, 2400, 9600, 19 200, 38 400, 56 000, 64 000, 72 000, 125 000, 148 000, 500 000, 800 000, 1 000 000, 1 300 000, 2 000 000 i 4 000 000. W przypadku niektórych interfejsów szeregowych pewne szybkości mogą nie być dostępne. Zależy to od przepustowości interfejsu. Domyślnie interfejsy są wyłączone lub nieaktywne. Aby włączyć lub uaktywnić interfejs, należy użyć polecenia `no shutdown`. Jeśli zachodzi potrzeba administracyjnego wyłączenia interfejsu w celu przeprowadzenia czynności serwisowych lub rozwiązania problemu, należy użyć polecenia *shutdown,* jak pokazano poniżej:

```
Router(config)#interface serial 0/0
Router(config-if)#shutdown
```

4.5 Ustawienia interfejsu FastEthernet.

Każdy interfejs FastEthernet musi mieć zdefiniowany adres IP i maskę podsieci, aby mógł przesyłać pakiety IP. Domyślnie interfejsy są wyłączone lub nieaktywne. Aby włączyć lub uaktywnić interfejs, należy użyć polecenia `no shutdown` w trybie konfiguracji danego interfejsu.

4.6 Sieci VLAN.

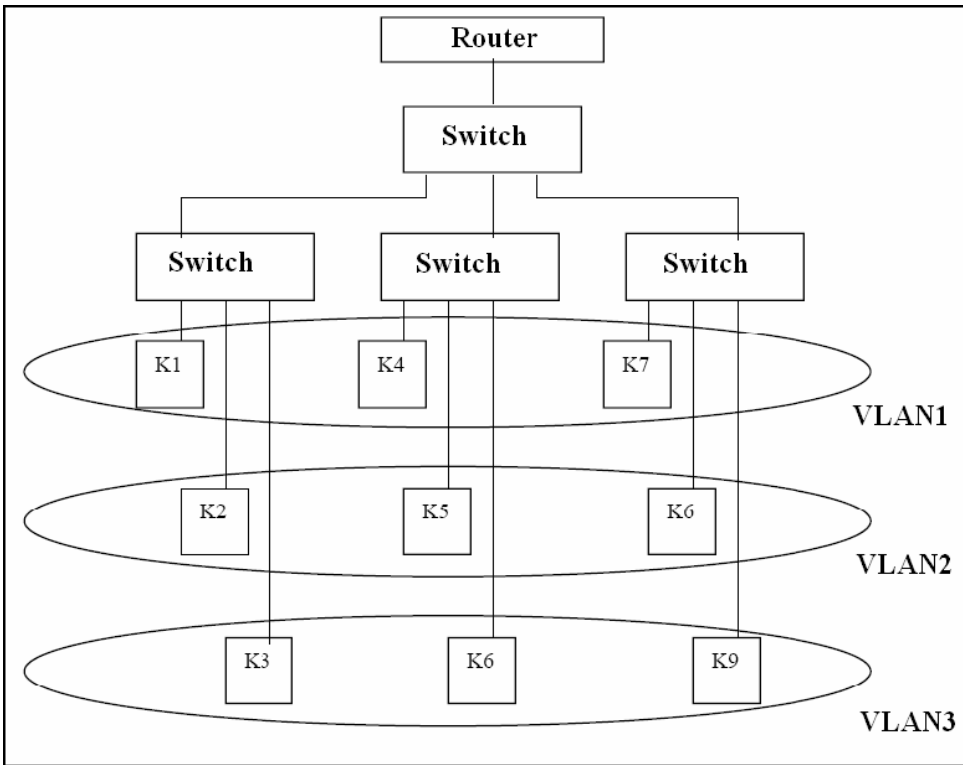
Istotną cechą przełączania w sieciach Ethernet jest możliwość tworzenia wirtualnej sieci, czyli sieci VLAN, która jest logiczną grupą stacji i urządzeń sieciowych. Ruch między sieciami VLAN jest ograniczony. Innymi słowy, urządzenia w sieci VLAN komunikują się tylko z urządzeniami znajdującymi się w tej samej sieci VLAN, a połączenie pomiędzy tymi sieciami zapewniają routery. Sieci VLAN zwiększają ogólną wydajność sieci poprzez logiczne grupowanie użytkowników i zasobów. Firmy często używają sieci VLAN w celu logicznego grupowania określonych użytkowników niezależnie od ich fizycznego rozmieszczenia.

Właściwie zaprojektowane i skonfigurowane sieci VLAN stanowią bogate w możliwości narzędzie dla administratorów. Sieci VLAN zwiększają także bezpieczeństwo sieci i pomagają sterować rozgłaszaniem w warstwie 3. Jednakże niepoprawnie skonfigurowana sieć VLAN może zaburzyć funkcjonowanie sieci lub całkowicie je uniemożliwić. Sieci VLAN dzielą sieci przełączane na segmenty

logiczne w oparciu o pełnione funkcje, niezależnie od fizycznego rozmieszczenia użytkowników lub fizycznych podłączeń do sieci.

Konfigurowanie sieci VLAN odbywa się na drodze programowej, dlatego nie wymaga ono fizycznego przenoszenia lub podłączania sprzętu sieciowego.

Stacja robocza w grupie VLAN może komunikować się tylko z serwerami plików, które znajdują się w tej samej grupie VLAN. Sieci te logicznie dzielą sieć na wiele domen rozgłoszeniowych, dlatego pakiety są przesyłane tylko między portami przypisanymi do danej sieci VLAN. Porty przypisane do sieci VLAN odbierają i przekazują te same pakiety rozgłoszeniowe. Zwiększa to wydajność sieci, ponieważ zmniejsza się ilość zbędnych pakietów rozgłoszeniowych. Na rysunku 5 przedstawiono przykładową sieć VLAN.



Rys.5. Przykładowa sieć VLAN [9].

Dzięki sieci VLAN komunikaty typu *broadcast* z urządzenia z jednej z sieci VLAN trafiają jedynie do urządzeń będących w tej samej sieci VLAN i nie będą transmitowane do innych stacji, nawet przyłączonych do tego samego przełącznika, np. na rysunku 5 komunikat typu *broadcast* ze stacji K1 trafi jedynie do stacji K4 i K7. Dzięki temu cała sieć działa znacznie wydajniej.

Sieci VLAN dzieli się na statyczne i dynamiczne. W sieciach statycznych skład sieci VLAN stanowi statyczny zbiór wybranych wcześniej portów. Przynależność danego portu do sieci VLAN nie może ulec zmianie, dopóki administrator nie zmieni konfiguracji. Natomiast w sieciach dynamicznych, przełącznik automatycznie ustala do jakiej sieci VLAN przypisać dany port, na przykład na podstawie nazwy użytkownika, który rejestruje się w sieci komputerowej.

Domyślną siecią VLAN dla każdego portu przełącznika jest sieć zarządzania VLAN 1. Sieci tej nie można usunąć. Aby móc zarządzać przełącznikiem, do sieci

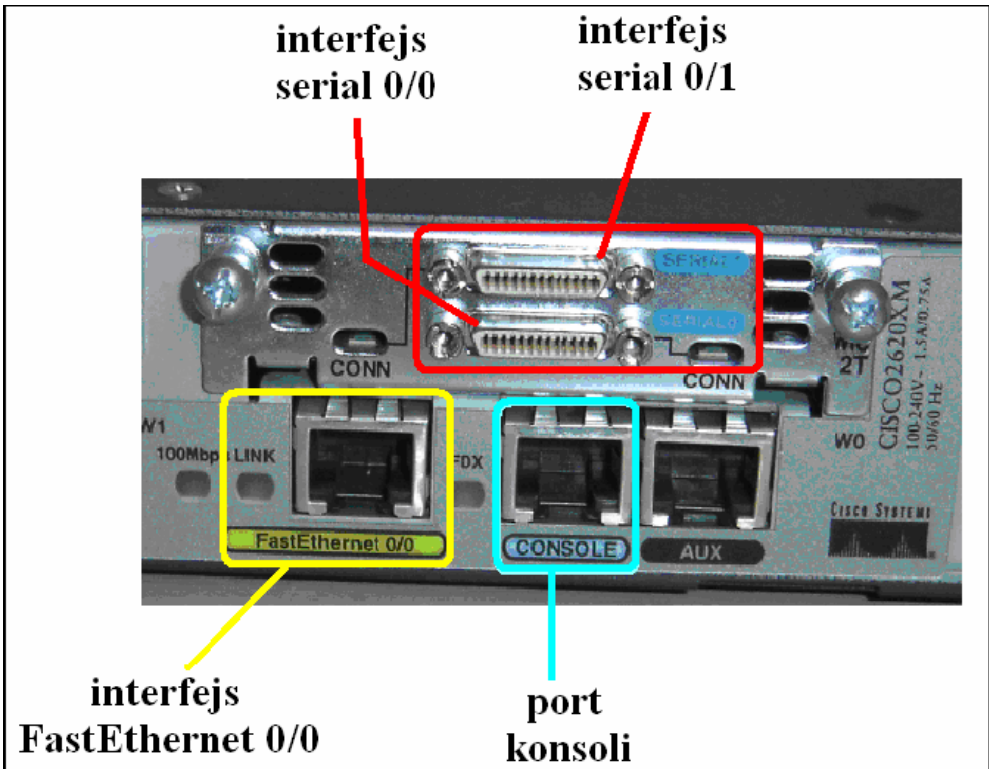
VLAN 1 musi być przypisany co najmniej jeden port. Wszystkie inne porty przełącznika mogą być przypisane do innych sieci VLAN.

4.7 Połączenia urządzeń sieciowych i telefonów

Poniżej na rysunku przedstawiona jest tylna ścianka routera Cisco 2620XM oraz zdjęcie z uwzględnieniem interfejsów szeregowych i FastEthernet oraz portu konsoli.

Rys. 6. Tylna ścianka routera Cisco 2620XM.

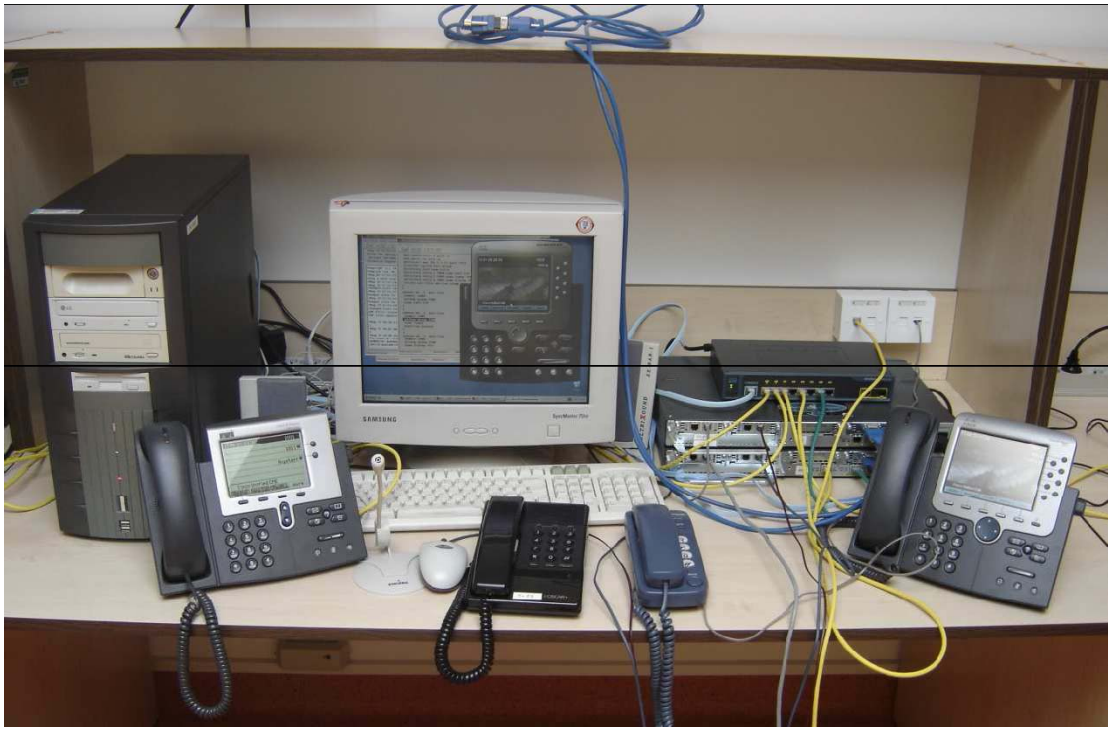
Interfejs szeregowy Serial służy głównie do połączeń pomiędzy routerami. Router 2 w zestawionym połączeniu posiada tylko jeden interfejs FastEthernet, za pomocą którego zostało nawiązane połączenie ze switchem kablem prostym zakończonym z obu stron wtyczkami RJ-45. Natomiast w routerze 1 są dwa interfejsy FastEthernet, z czego jeden z nich został wykorzystany do połączenia z Internetem takżŜe kablem prostym.



Rys. 7. Interfejsy szeregowe i FastEthernet oraz port konsoli na tylnej ściance routera Cisco 2620XM

Port konsoli służy do bezpośredniego połączenia stacji roboczej z routerem, co umożliwia jego konfigurację bezpośrednio z komputera poprzez oprogramowanie terminalowe.

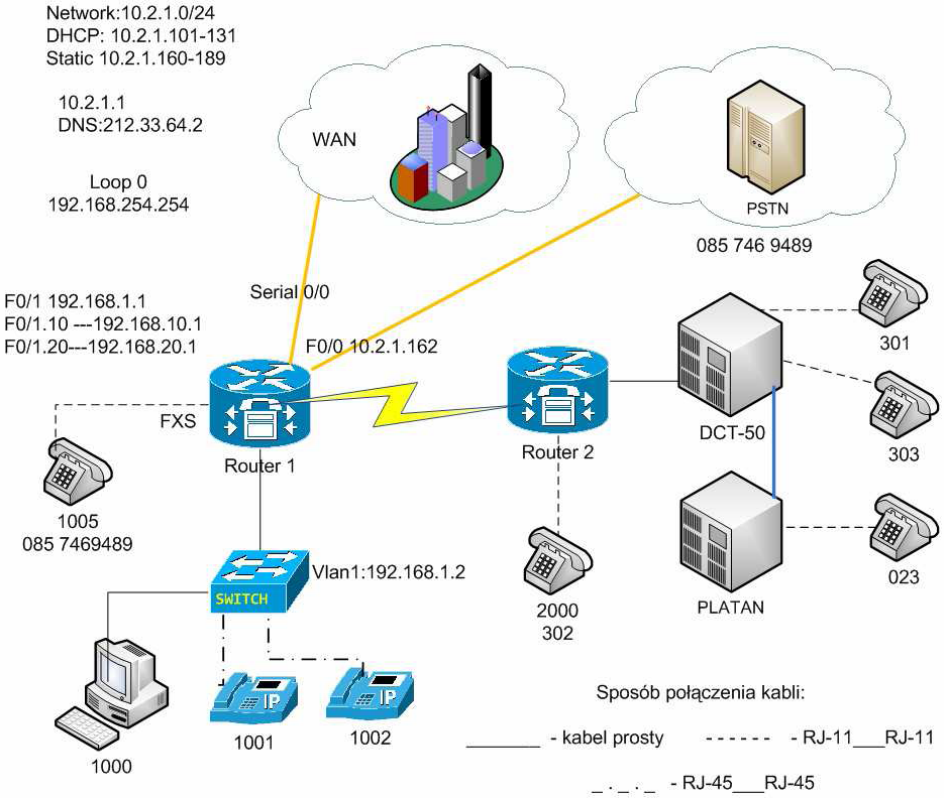
Ogólne zestawienie urządzeń sieciowych oraz zastosowanych telefonów IP i zwykłych aparatów analogowych przedstawione jest na rysunku 8.



Rys. 8 Stanowisko laboratoryjne przeznaczone do badania systemu VoIP.

dSchemat struktury stanowiska laboratoryjnego wraz z opisem interfejsów oraz

Schemat struktury stanowiska laboratoryjnego wraz z opisem interfejsów oraz stosowanych przewodów przedstawiono na rysunku 9.



Rys.9 Schemat struktury stanowiska laboratoryjnego.

4.8 Konfiguracja urządzeń sieciowych.

Krok 1. Zalogowanie się do routera w uprzywilejowanym trybie EXEC oraz zmiana nazwy routera.

Na samym początku po włączeniu, router znajduje się w trybie użytkownika. Żeby przejść do trybu uprzywilejowanego należy użyć polecenia *enable*, tak jak to zostało pokazane poniżej:

Router>**enable**

Następnie wpisując polecenie *configure terminal* router przechodzi do trybu konfiguracji globalnej:

```
Router#configure terminal
```

W tym momencie można już konfigurować router. Pierwszym prostym zadaniem będzie zmiana nazwy routera wykorzystując polecenie *hostname* i wpisując nazwę routera, np. „Router1".

```
Router1(config)#hostname <nazwa>
```

Krok 2. Skonfigurowanie hasła konsoli, hasła linii terminala wirtualnego i hasła dostępu do uprzywilejowanego trybu EXEC.

```
Router1 (config)#line console 0
Router1 (config-line)#password <hasło>
Router1 (config-line)#login
Router1 (config-line)#exit
Router1(config)#line vty 0 4
Router1(config-line)#password <hasło>
Router1(config-line)#login
Router1 (config-line)#exit
Router1(config)#enable password <hasło>
Router1(config)#enable secret <hasło>
Router1(config)#exit
```

Krok 3. Konfiguracja interfejsu szeregowego Serial 0 na routerze 1.

Po przejściu do trybu konfiguracji interfejsu, należy ustawić adres IP tego interfejsu oraz maskę podsieci. Polecenie *no shutdown* powoduje włączenie interfejsu. Stan *shutdown* oznacza jego wyłączenie. W nawiasie należy podać adres IP oraz maskę podsieci oddzielone od siebie spacją w postaci: xxxx.xxxx.xxxx.xxxx xxxx.xxxx.xxxx.xxxx (maska podsieci może być klasy C, np.: 255.255.255.0).

```
Router1 (config)#interface serial 0/0
Router1 (config-if)#ip address <adres_ip maska_podsieci>
Router1 (config-if)#no shutdown
Router1 (config-if)#exit
Router1 (config)#exit
```

W taki sam sposób należy skonfigurować interfejs szeregowy na routerze 2. W celu sprawdzenia poprawności połączenia naleŜy wykonać polecenie *ping* z jednego routera do drugiego podając odpowiedni adres IP routera.

Krok 4. Utworzenie trasy statycznej.

Utwórz trasę statyczną prowadzącą od urządzenia po stronie dostawcy usług internetowych (router 2) do routera 1.

```
Router2(config)#ip route <adres_ip maska_podsieci> serial 0/0
```

Krok 5. Utworzenie trasy domyślnej.

Używając polecenia *ip route*, utwórz trasę domyślną (oznaczaną jako: 0.0.0.0 0.0.0.0) prowadzącą od routera 1 do routera 2. Spowoduje to, że cały ruchu kierowany do nieznanych adresów zostanie przekazany do urządzenia po stronie dostawcy usług internetowych.

```
Router1(config)#ip route 0.0.0.0 0.0.0.0 <adres_ip>
```

Krok 6. Skonfigurowanie na switchu dostępu do warstwy 3.

Operację tę należy wykonać na wewnętrznym interfejsie wirtualnym sieci VLAN 1.

```
Switch(config)#interface VLAN 1
Switch(config-if)#ip address <adres_ip maska_podsieci>
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

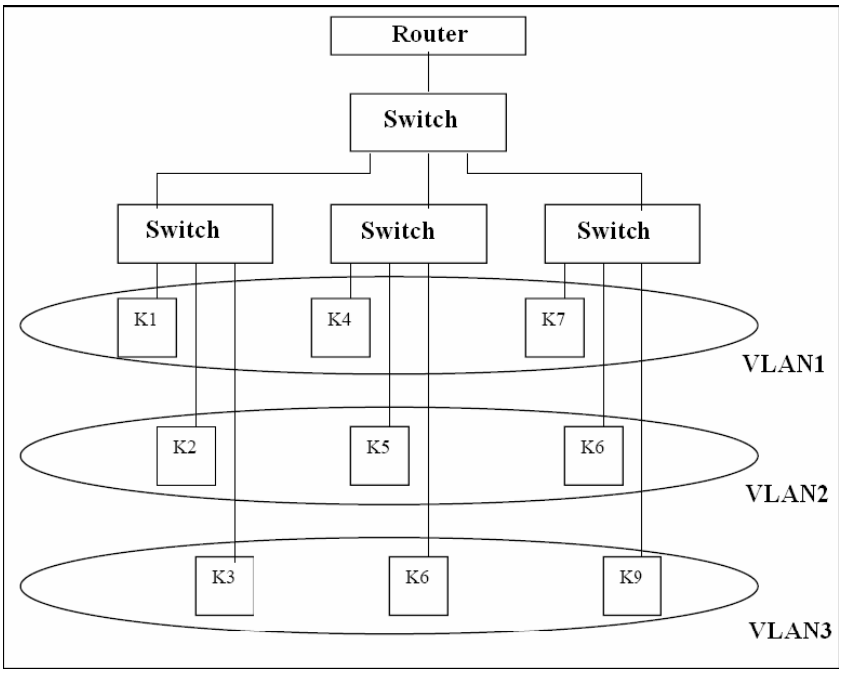
Dla bramy domyślnej przełącznika i domyślnej sieci VLAN służącej do zarządzania także należy ustawić adres IP.

```
Switch (config)#ip default-gateway <adres_ip>
Switch (config)#exit
```

Krok 7. Utworzenie dwóch sieci VLAN i nadanie im nazw.

Należy utworzyć dwie sieci VLAN (np.: *Voice* oraz *Data*) aby zagwarantować pełną separację przesyłanych danych, w celu zachowania większego bezpieczeństwa oraz wyszczególnienia domen rozgłoszeniowych i związanym z tym przesyłem pakietów. Przykładowe sieci VLAN przedstawia poniższa konfiguracj i rysunek 10.

```
Switch #vlan database
Switch (vlan)#vlan <numer> name <nazwa>
Switch (vlan)#vlan <numer> name <nazwa>
Switch (vlan)#exit
```



Rys. 10. Przykładowa sieć VLAN [9].

Krok 8. Przypisywanie portów do sieci VLAN

Przypisywanie portów do sieci VLAN musi zostać dokonane w trybie interfejsu.

```
Switch #configure terminal
Switch (config)#interface fastethernet 0/1
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access vlan
<numer_utworzonego_vlanu>
Switch (config-if)#end
```

Wszystkie porty FastEthernet na switchu (zdjęcie switcha przedstawiono poniżej), które będą wykorzystywane, należy skonfigurować w sposób przedstawiony powyżej zmieniając odpowiednio numer portu FastEthernet oraz numer VLAN w zależności, który port zostaje przypisany do konkretnego VLANu.

Rys. 11. Switch Cisco Catalyst 2960.

Krok 9. Zdefiniowanie puli uŜytecznych adresów IP.

W nawiasie należy wstawić adres IP początku puli i adres IP końca puli.

```
Router1(config)#ip nat pool out <adres_ip adres_ip> netmask
<maska_podsieci>
```

Krok 10. Zdefiniowanie listy dostępowej zgodnej z wewnętrznymi prywatnymi adresami IP.

Konfiguracja list dostępowych pozwala na przepuszczanie ruchu (komenda *permit*) lub blokowanie ruchu (komenda *deny*). Listy dostępowe, zwane *Access List* konfiguruje się w zależności od potrzeb.

```
Router1(config)#access-list 1 permit <adres_ip maska_podsieci>
```

Krok 11. Zdefiniowanie translacji NAT między listą wewnętrzną a pulą zewnętrzną.

```
Router1(config)#ip nat inside source list 1 interface
fastethernet 0/1 overload
```

Krok 12. Konfiguracja interfejsów i podinterfejsów FastEthernet, pętli zwrotnej oraz mechanizmu NAT na routerze 1.

Pierwszy interfejs Ethernet w routerze może być różnie oznaczony. W zależności od typu routera może to być: ethernet 0, fastethernet 0 lub fastethernet 0/0.

```
Router1 (config)#interface loopback 0
Router1 (config-if)#ip address <adres_ip maska_podsieci>
Router1 (config-if)#exit
Router1 (config)#interface fastethernet 0/0
Router1 (config-if)#ip address <adres_ip maska_podsieci>
Router1 (config-if)#ip nat inside
Router1 (config-if)#duplex auto
Router1 (config-if)#speed auto
Router1 (config-if)#no shutdown
Router1 (config-if)#exit
Router1 (config)#interface fastethernet 0/1
Router1 (config-if)#ip address dhcp
Router1 (config-if)#ip nat outside
Router1 (config-if)#duplex auto
Router1 (config-if)#speed auto
Router1 (config-if)#no shutdown
Router1 (config-if)#exit
Router1 (config)#interface fastethernet 0/0.10
Router1 (config-if)#encapsulation dot1Q 10
Router1 (config-if)#ip address <adres_ip maska_podsieci>
Router1 (config-if)#ip nat inside
Router1 (config-if)#exit
Router1 (config)#interface fastethernet 0/0.20
Router1 (config-if)#encapsulation dot1Q 20
Router1 (config-if)#ip address <adres_ip maska_podsieci>
Router1 (config-if)#ip nat inside
Router1 (config-if)#exit
```

Należy dokonać konfiguracji interfejsów, trasy statycznej i domyślnej oraz pętli zwrotnej na routerze 2. Należy jednak pamiętać o podaniu odpowiednich adresów IP jak również maski podsieci. W konfiguracji routera 2 ustawia się częstotliwości

zegara używając polecenia *clock rate* i podając odpowiednią prędkość, tak jak poniżej:

```
Router2 (config)#interface serial 0/0
Router2 (config-if)#clock rate 2000000
```

W celu sprawdzenia poprawności połączenia należy wykonać polecenie *ping* z jednego routera do drugiego podając odpowiedni adres IP routera.

Krok 13. Konfiguracja protokołu DHCP na routerze 2.

```
Router2 (config)#ip dhcp pool <nazwa puli>
Router2 (dhcp-config)#network <adres_ip maska_podsieci>
Router2 (dhcp-config)#default-router <adres_ip>
Router2 (dhcp-config)#dns-server <adres_ip>
Router2 (dhcp-config)#option 150 ip <adres_ip>
```

Krok 14. Wykluczenie adresów z puli.

Aby zdefiniować zakres adresów, które mają zostać wykluczone przez serwer DHCP z operacji dynamicznego przydzielania adresów, należy użyć poniższych poleceń. W nawiasach należy podać adresy IP (w kolejności: adresy w podsieci 1 i adresy w podsieci 2, które mogą być przydzielone do innych urządzeń sieciowych oraz adresy w VLAN1 i VLAN2, które mogą być przydzielone np. dla IP Phone).

```
Router2 (config)#ip dhcp excluded-address <adres_ip adres_ip>
Router2 (config)#ip dhcp excluded-address <adres_ip adres_ip>
Router2 (config)#ip dhcp excluded-address <adres_ip adres_ip>
Router2 (config)#ip dhcp excluded-address <adres_ip adres_ip>
```

Krok 15. Kopiowanie konfiguracji do pamięci NVRAM.

Skopiuj konfigurację do pamięci NVRAM w sposób przedstawiony poniżej. Dzięki wykonaniu tego komendy wszystkie zmiany będą dostępne dla danego urządzenia sieciowego, jeśli nastąpi ponowne załadowanie lub awaria zasilania. Instrukcja zostanie przedstawiona na przykładzie routera 1. Należy ją także wykonać dla routera 2 oraz switcha.

```
Router1 #copy running-config startup-config
Destination filename [startup-config]? (Nazwa pliku docelowego
[startup-config]?)
Building configuration... (Tworzenie pliku
konfiguracyjnego...)
[OK]
Router1 #
```

Kopiowanie konfiguracji należy także wykonać dla routera 2 oraz switcha.

5. Sprawozdanie

W sprawozdaniu należy zamieścić opis przygotowanego w ramach ćwiczenia środowiska sieciowego ze szczegółowym uwzględnieniem adresów przypisanych do poszczególnych interfejsów oraz utworzonych sieci VLAN.

6. Wymagania BHP

Zgodnie z podanymi na pierwszych zajęciach i potwierdzonymi przez studentów zasadami obowiązującymi w pomieszczeniu, w którym odbywają się ćwiczenia. Stosowny regulamin BHP jest też wywieszony w pomieszczeniu laboratorium.

7. Literatura

1. Theodore Wallingford: VoIP, praktyczny przewodnik po telefonii internetowej. Helion, Gliwice, 2007.
2. Krzysztof Surdut: Tania telefonia internetowa VoIP. Helion, Gliwice, 2006.
3. Marek Bromirski: Telefonia VoIP. Multimedialne sieci VoIP. BTC, Warszawa, 2006.
4. Jonathan Davidson: Deploying Cisco Voice over IP Solution. CiscoPress.
5. Jonathan Davidson, James Peters: Voice over IP Fundamentals. CiscoPress, 2000
6. Ciarkowski A., Żyromski M.: Wprowadzenie do telefonii VoIP – teoria vs real life. Materiały konferencji InfoShare 2007.
7. Witryna www.itpedia.pl
8. Witryna www.protocols.com
9. Dokumentacja techniczna *Cisco* (dostępna w laboratorium na CD-ROM oraz w witrynie *www.cisco.com*)