

ZESPÓŁ LABORATORIÓW TELEMATYKI TRANSPORTU
ZAKŁAD TELEKOMUNIKACJI W TRANSPORCIE
WYDZIAŁ TRANSPORTU
POLITECHNIKI WARSZAWSKIEJ

LABORATORIUM
SYSTEMY KOMUTACYJNE

INSTRUKCJA DO ĆWICZENIA NR 4

Telefonia internetowa VoIP

przygotował:
dr inż. Marek Sumiła

DO UŻYTKU WEWNĘTRZNEGO
WSZELKIE PRAWA ZASTRZEŻONE.

Warszawa 2016

1. Cel ćwiczenia

1. Zapoznanie z podstawową konfiguracją abonentów w centrali VoIP,
2. Zapoznanie z typami terminali VoIP,
3. Utworzenie podstawowej łączności VoIP z wykorzystaniem różnych typów terminali,
4. Zbadanie wybranych usług dodatkowych w sieci VoIP,
5. Testowanie łączności VoIP.

2. Stanowisko laboratoryjne

1. Stanowisko komputerowe PC,
2. Centrala VoIP,
3. Terminale VoIP: telefon sprzętowy, telefon software'owy, brama VoIP,
4. Oprogramowanie badawcze typu Wireshark.

3. Wprowadzenie teoretyczne

3.1. Telefonia internetowa

Voice over Internet Protocol (VoIP) jest ogólnym określeniem technologii stanowiącej połączenie różnego rodzaju protokołów i standardów pozwalających na transmisję głosu w sieci komputerowej. Początkowo technologia ta oznaczała połączenie dwóch terminali, jednak w wyniku rozwoju technologii możliwe stało się przesyłanie „pakietów głosowych” przez ogólnosiwiatową sieć Internet ze wskazaniem wywoływanego odbiorcy. Elementem niezbędnym do realizacji tej technologii jest odpowiednia brama (*gateway*) odpowiadająca za konwersję sygnału analogowego mowy na potrzeby transmisji w sieci pakietowej Internet.

VoIP jest poważnym konkurentem dla markowych systemów telekomunikacyjnych z uwagi na niższe koszty wdrożenia, możliwość integracji z innymi systemami telefonicznymi (bądź informatycznymi) oraz kosztami wsparcia technicznego.

W przeciwieństwie, bowiem do systemów komercyjnych centrale VoIP nie muszą być wyposażane w żadne drogie moduły sprzętowe – do poprawnej i niezawodnej pracy wystarczającym jest średniej klasy serwer. Najpopularniejsza wersja centrali VoIP – Asterisk nie wymaga zakupu licencji za wyjątkiem niektórych płatnych kodeków.

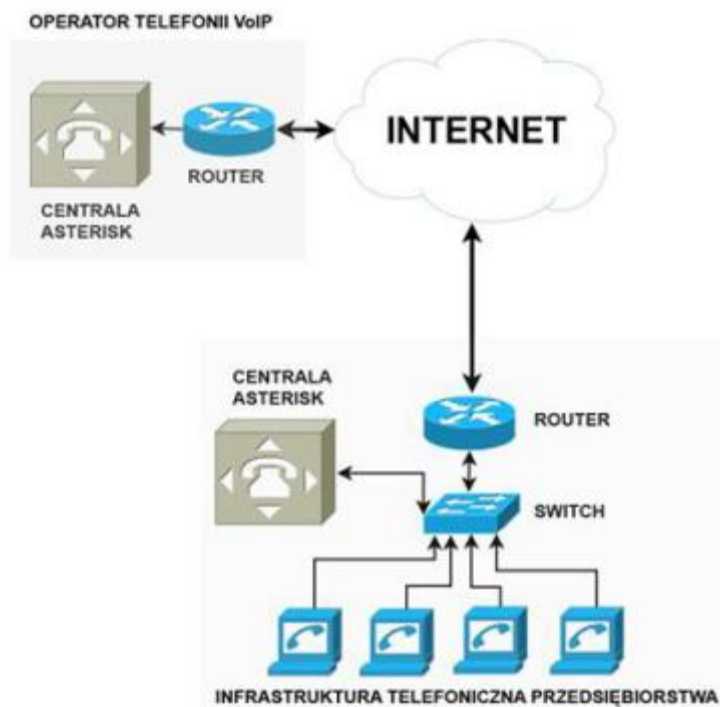
Ważnym atutem za VoIP jest brak konieczności instalacji dodatkowego okablowania telefonicznego, gdyż stacje telefoniczne mogą łączyć się z centralą przy użyciu już istniejącej w przedsiębiorstwie sieci LAN lub WAN. Nie bez znaczenia jest również fakt, iż centrale VoIP potrafią obsługiwać zarówno sprzętowe telefony, jak i tzw. softphone.

Poważnym biznesowym atutem Asteriska jest możliwość podłączenia stacji telefonicznych fizycznie zlokalizowanych poza główną siedzibą przedsiębiorstwa (np. w oddziałach) bez konieczności instalowania modułów wyniesionych, jak to miało miejsce w centralach komercyjnych. Koszt prowadzonych w ten sposób wewnętrznych rozmów telefonicznych jest zerowy, co niektórym spółkom potrafi przynieść oszczędności sięgające nawet do kilku tysięcy złotych miesięcznie.

Telefonia internetowa jest rozbudowaną formą technologii VoIP, w której uzupełniono znajdujące się na krańcach łącza gateway'e o elementy spełniające podobne zadania do tych, które dotychczas realizowały tradycyjne centrale telekomunikacyjne. Mowa tu o takich cechach jak odpowiednie adresowanie abonentów, nadzór nad procesami komutacyjnymi (zestawianie połączeń, likwidacja połączeń), zarządzanie siecią central, translacja numerów, itd.

Telefonia internetowa rozwinęła się (i nadal rozwija) głównie dlatego, że pozwala znacząco ograniczyć koszty realizowanych połączeń, zwłaszcza tych realizowanych na duże odległości. Inną korzyścią płynącą z zastosowania telefonii internetowej jest większa elastyczność w kreowaniu usług, szybkość dokonywania zmian w konfiguracji sieci VoIP, jednolita numeracja w ramach jednego przedsiębiorstwa, itd. Tym niemniej, VoIP wciąż nie zapewnia odpowiednich mechanizmów kontroli jakości połączenia (QoS), między innymi ze względu na fakt, że jakość ta jest uzależniona od aktualnego ruchu w danej sieci. Pewnym mankamentem jest też fakt, że korzystanie z telefonu internetowego wymaga stałego zasilania, w przeciwieństwie do tradycyjnej telefonii, gdzie aparat telefoniczny abonenta (CB – Centralna Bateria) jest zasilany, w podstawowym zakresie, wprost z centrali telekomunikacyjnej.

Przykładową infrastrukturę telefonii internetowej przedstawiono na poniższym rysunku.



Rys. 1. Przykładowa topologia połączeń sieci telefonii internetowej.

3.2. Zasada działania telefonii internetowej

3.2.1. Transmisja w sieci internetowej

Płaszczyzną na której jest realizowana telefonia VoIP jest sieć internetowa. Sieć ta funkcjonuje dzięki zastosowaniu **protokołu IP**, który wywodzi się z wojskowej sieci ARPANET stosowanej w USA w latach 1969-72. Obecnie stosowane są dwie wersje protokołu IP: czwarta i szósta. IPv4 jest obecnie powszechnie wykorzystywana. IPv4 została opracowana w roku 1981 przez IETF (*Internet Engineering Task Force*). Istotą działania sieci opartej na tym protokole jest podział informacji na mniejsze zbiory danych nazywane pakietami lub datagramami. **Pakiet** jest to usystematyzowany zbiór danych posiadający nagłówek, treść informacyjną oraz element potwierdzający poprawność danych w postaci sumy kontrolnej.

Stosowany mechanizm transmisji – „best effort” – oraz bezpołączeniowy charakter protokołu IP powodują, że urządzenie wysyłające pakiet IP nie ma żadnej gwarancji, że ten dotrze do miejsca przeznaczenia, a jeśli po drodze zostanie on usunięty (np. wskutek natłoku) to urządzenie zwrotnie nie otrzyma żadnej informacji o takim fakcie. W związku z tym

potwierdzanie poprawności transmisji musi być realizowane za pomocą innych protokołów znajdujących się w wyższych warstwach sterujących połączeniami (np. przez protokół TCP)¹.

Z punktu widzenia Voice over IP taki bezpołączeniowy charakter protokołu IP jest pewnym utrudnieniem, gdyż w przypadku komunikacji głosowej istotne jest uzyskanie przekazu informacji w czasie rzeczywistym, czyli z opóźnieniem nie przekraczającym 300 ms.

Stosowany powszechnie w sieci internetowej **protokół TCP** (*Transmission Control Protocol*) pozwala na uzyskanie wysokiej wierności przekazywania informacji poprzez mechanizmy kontroli zawartości przekazu. Niestety, weryfikacja każdego z pakietów w każdym z pośredniczących węzłów w sieci wiąże się z pewnym opóźnieniem, które utrudnia swobodną rozmowę komunikujących się abonentów sieci. Z tego też względu, jako protokół sterujący warstwą sieci często stosuje się protokół o mniejszej restryktywności integralności przekazu danych, jakim jest **UDP** (*User Datagram Protocol*). Cechą charakterystyczną tego protokołu jest brak narzutu na nawiązywanie połączenia i śledzenie sesji (w przeciwieństwie do TCP) oraz brak mechanizmów kontroli przepływu i retransmisji. Korzyścią płynącą z takiego uproszczenia budowy jest większa szybkość transmisji danych i brak dodatkowych zadań, którymi musi zajmować się węzeł propagujący pakiet tego protokołu. Oczywiście wadą jest tu możliwość gubienia, duplikowania lub zmiana kolejności przekazywanych przez sieć pakietów, jednak wszędzie tam gdzie dane muszą być przesyłane możliwie szybko jest on najskuteczniejszą metodą przekazu informacji w sieci IP. W takim przypadku poprawność przekazu i naprawianie ewentualnych błędów realizowane jest w innych, wyższych warstwach sterowania połączeniem, zgodnie z modelem OSI. UDP jest często używany w takich zastosowaniach jak strumień dźwięku i obrazu w Internecie (np. YouTube, radia internetowe, itp.).

Transmisja danych, które muszą być odtworzone w ściśle określonych momentach czasu wymaga dodatkowego mechanizmu sterującego połączeniami. Zarówno protokół IP, jak i UDP nie przenosi informacji o czasie przebywania pakietu w sieci. Konieczne zatem stało się zastosowanie dodatkowego protokołu umożliwiającego odpowiedni nadzór nad tym, tak ważnym elementem realizacji usługi. Do tego celu wykorzystano **protokół RTP** (*Real Time Protocol*). Służy on do transportu danych multimedialnych (głos, głos i wideo, inne) „od końca do końca” dla aplikacji używających tych danych w czasie rzeczywistym. Protokół ten podobnie, jak IP, został opracowany przez IETF i opisany w zaleceniu RFC3550. Wraz z RTP

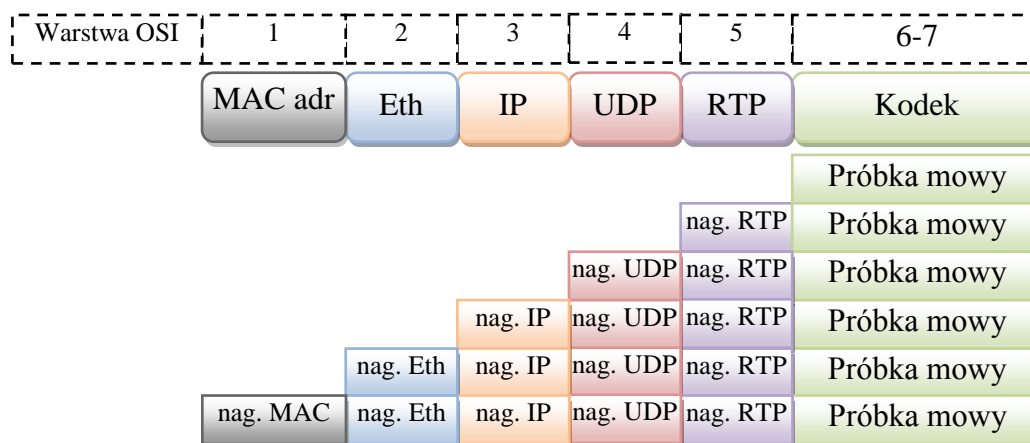
¹ Istnieje tu uzasadnione zaznaczenie, że „wyższe warstwy sterowania” są zdefiniowane w modelu siedmiowarstwowym OSI.

stosuje się dodatkowy **protokół RTCP** (*Real-time Transport Control Protocol*) umożliwiający monitorowanie oraz raportowanie bieżącej pracy protokołu RTP. Zasadnicze cele, jakie realizuje protokół RTP to:

- umiejscowienie przesyłanych próbek (mowy lub wideo) w czasie,
- numerowanie próbek danych, niezbędne do integralności danych,
- rozróżnianie różnych strumieni wychodzących z tego samego hosta,
- szyfrowanie transmisji (opcjonalnie).

Niestety, wbrew swej nazwie, protokół RTP nie zawiera żadnego mechanizmu gwarancji jakości przekazu w czasie rzeczywistym.

Stos protokołów konieczny do transmisji głosu w sieci IP wymaga uwzględnienia również protokołów niższych warstw modelu referencyjnego OSI niezbędnych do zapewnienia prawidłowego dostępu terminali abonenckich do sieci IP. W klasycznym modelu dostępowym jest to protokół Ethernet w warstwie drugiej modelu oraz ICMP w warstwie pierwszej. Ogólny stos przedstawionych powyżej protokołów służących zapewnieniu transmisji głosu w czasie rzeczywistym w sieci internetowej przedstawiono na rysunku.

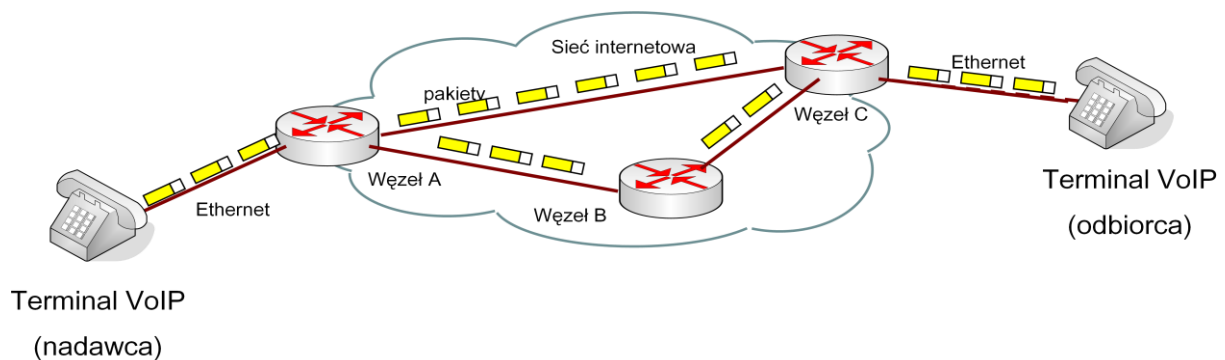


Rys. 2. Model warstwowy protokołów sieci internetowej oraz zawartość pakietu IP.

Odnosząc się do przedstawionego powyżej stosu protokołów należy podkreślić, że każdy protokół użyty w procesie transmisji głosu wymaga przekazania pewnych informacji dodatkowych zawartych najczęściej w nagłówku. Prowadzi to do powstania pewnej informacji nadmiarowej. Tą informację nadmiarową należy oszacować podczas planowania strumienia danych na łączy dostępowym. W tym celu należy uwzględnić wielkość każdego

nagłówka transmitowanego pakietu, a następnie obliczyć dla wybranego kodeka głosowego liczbę transmitowanych pakietów w czasie jednej sekundy. Obliczoną wartość należy następnie dodać do strumienia głosowego, uzyskując tym samym oczekiwaną szerokość strumienia danych. Sprawność wykorzystania łącza dla określonego kodeka głosowego należy obliczyć korzystając z wzoru:

Ogólną ideę transmisji głosu w sieci internetowej przedstawiono na rysunku 2.



Rys. 3. Transmisja pakietów zawierających próbki mowy w sieci IP

Kończąc omawiany poziom sieci internetowej warto zaznaczyć, że dzięki bogatej ofercie możliwych do wykorzystania technologii dostępnych do sieci internetowej, również telefonia VoIP może być osiągalna zarówno za pomocą łączy przewodowych (kabel miedziany, światłowód), jak i bezprzewodowych (Wi-Fi, GSM 3G, 4G, UMTS, Wi-Max).

Zatem, telefonia internetowa umożliwi abonentowi stałą łączność bez względu na to czy będzie on korzystać z komputera stacjonarnego, z telefonu VoIP, telefonu komórkowego, czy aplikacji webowej. Brak powiązania numeru abonenckiego z konkretnym łączem prowadzi do konieczności wykorzystania innych metod zapewniających prawidłowość procesu komutacyjnego.

3.2.2. Komutacja połączeń

Podobnie jak to ma miejsce w przypadku telefonii tradycyjnej, tak i w telefonii internetowej zanim dojdzie do połączenia między abonentami następuje proces sterujący mający na celu ustalenie abonenta żądanego i zestawienie do niego odpowiedniej drogi połączeniowej. Proces ten określa się mianem **komutacji połączeń**. W przypadku VoIP jest to ważny element funkcjonowania telefonii internetowej, gdyż abonent nie jest bezpośrednio związany z danym łączem fizycznym, czy lokalizacją. Abonent może zatem korzystać z tego

samego numeru VoIP zarówno w pracy, w domu, czy na wakacjach za granicą, będąc stale dostępny pod tym samym numerem lokalnym krajowym lub sieci wewnętrznej przedsiębiorstwa. W związku z tym, procesy komutacyjne w telefonii VoIP muszą zagwarantować:

1. **Lokalizację abonentów w sieci**, co gwarantuje dostępność atrybutu mobilności rozumianego jako możliwość przestrzennego przemieszczania się użytkowników, z zachowaniem dostępu do oferowanych przez system usług oraz udogodnień.
2. **Sterowanie dostępnością abonenta w sieci**, które ma zapewnić stronie wywoływanej możliwość różnicowania reakcji na wezwania do ustanowienia połączeń.
3. **Profilowanie sesji**, umożliwiające określenie typu wymienianych mediów w kategoriach schematu ich kodowania oraz parametrów szczegółowych.
4. **Obsługę połączeń**, obejmującą akcje właściwe komunikacji w trybie punkt-punkt oraz wielopunktowym, z uwzględnieniem właściwości uzgodnionego profilu.
5. **Zarządzanie sesją**, które stanowi zespół mechanizmów o zróżnicowanym przeznaczeniu. Ich zadaniem jest modyfikowanie profilu usługowego i wywoływanie dodatkowych usług w trakcie połączeń, a także przekazywanie istniejących sesji innym abonentom.

Taki stan rzeczy doprowadził do opracowania specyficznych protokołów komutacyjnych nazywanych popularnie protokołami sygnalizacyjnymi, które zapewniają realizację powyższych funkcji. Obecnie do najbardziej popularnych protokołów VoIP zapewniających komutację połączeń zalicza się: SIP, H.323 oraz Skype.

Ich szczegółowe omówienie wykracza swoim zasięgiem zakres przedmiotu Systemy Łączności w Transporcie, dlatego w dalszej części ograniczono się jedynie do syntetycznego zestawienia podstawowych cech wymienionych wcześniej protokołów (patrz Tabela 1).

Tab. 1. Ogólne porównanie protokołów komutacji VoIP

Cecha charakterystyczna	SIP	H.323	Skype
Organizacja, która opracowała protokół	IETF	ITU-T	J.Friis, N.Zennstrom (twórcy KaZaA)
Kodowanie komunikatów	Tekstowe	binarne	AES (komunikaty są zaszyfrowane)
Szyfrowanie sygnalizacji	Częściowo	nie (H.323v2)	tak, AES 256 bit

Wykorzystywany protokół do transmisji mowy	RTP	RTP	Własny
Wykorzystywany port (porty) dla sygnalizacji	5060, 5061	1719,1720, 1721	brak danych
Charakter sieci	klient-serwer	klient-serwer	peer-to-peer (P2P)
Elementy sieci	serwer proxy, serwer rejestrujący	gatekeeper, brama	Skype Super Node, inni użytkownicy
Liczba wykorzystywanych protokołów w sygnalizacji	mała (SIP, SDP)	duża (RAS, H.225, H.245, H.450)	brak danych

3.2.3. Transmisja głosu w sieci internetowej

Z uwagi na fakt pełnej cyfryzacji sieci internetowej, analogowy sygnał głosowy musi zostać przekształcony na postać cyfrową. Sposób tej zamiany i dokładność odwzorowania sygnału oryginalnego został opisany w specyfikacjach technicznych, np. serii G Światowej Unii Telekomunikacyjnej ITU-T.

Kodeki audio to inaczej programowe lub sprzętowe konwertery sygnałów akustycznych, umożliwiające zamianę sygnału mowy na postać cyfrową. W ten sposób możliwa jest ich transmisja w dowolnej sieci transmisji danych. Do podstawowych cech wszystkich kodeków zalicza się: metodę kodowania, pasmo kodowanych sygnałów audio, jakość odwzorowania, częstość próbkowania, wielkość strumienia danych, moc obliczeniową do realizacji procesu konwersji w czasie rzeczywistym oraz wielkość próbki lub pakietu. Do najpopularniejszych kodeków audio umożliwiających konwersję audio w paśmie telefonicznym (kodeki wąskopasmowe 4 kHz) zalicza się: G.711, G.726, G.722, G.723.1, G.729A, GSM, iLBC, Speer, LLC. Dostęp do części z nich jest ograniczony prawami autorskimi, a ich użytkowanie jest związane z wykupem licencji. Parametry wybranych kodeków przedstawione zostały w tabeli 2. Stosunkowo mało popularną grupą kodeków audio są kodeki szerokopasmowe umożliwiające kodowanie dźwięku w paśmie 0 – 7 kHz przy równoczesnej poprawie dynamiki przekazywanych sygnałów.

Tab. 2. Podstawowe parametrów popularnych kodeków audio

Nazwa kodeka	Przepływność nominalna [kbit/s]	Opóźnienie kodowania [ms]	Jakość (MOS)
G.711	64	0,125	4,1
G.726	16; 24; 32; 40	0,125	3,9
G.728	16	0,625	3,6
G.729	8	10	3,9
G.729a	8	10	3,7
G.723.1	6,3	37,5	3,9
G.723.1	5,3	37,5	3,6
GSM 6.10	13,2	20	3,7
iLBC	13,33; 15,2	30; 20	3,9
Speex	5,95; 8; 12; 15,2; 18,4; 24,8	20	b.d.

W tabeli 2, jako ostatni z wymienionych parametrów, wymienia się **parametr oceny jakości mowy**. Jakość sygnału mowy może być oceniana metodami subiektywnymi lub obiektywnymi. **Metody subiektywne** polegają na przeprowadzaniu testów odsłuchowych na specjalnie dobranej grupie słuchaczy. **Metody obiektywne** wykorzystują urządzenia, które wysyłają określony sygnał testowy a następnie odbierają sygnał i porównują z sygnałem pierwotnym.

W celu określenia poziomu jakości sygnału mowy zwykle wykorzystuje się skalę MOS (*Mean Opinion Score*). Zalecenie P.800 ITU-T określa średnią, subiektywną ocenę zrozumiałości przekazu dźwięków mowy ludzkiej. Skalę oceny MOS podzielono na pięć poziomów.

Tab. 3. Skala oceny zrozumiałości dźwięków mowy

Jakość/zrozumiałość przekazu	Ocena MOS
Doskonała	5
Dobra	4
Dostateczna	3
Mierna	2
Niedostateczna	1

Zawarte w tabeli wartości należy traktować jako wyjściowe przy ocenie poziomu zrozumiałości przekazu akustycznego.

3.3. Problematyka jakości połączeń w telefonii internetowej

„Jakość świadczenia usług stanowi miarę satysfakcji użytkownika konkretnej usługi oferowanej przez system telekomunikacyjny”.² Terminem określającym tą jakość jest parametr QoS (*Quality of Service*) odzwierciedlający zdolność operatora, a więc i sieci do realizacji powierzonych im zadań. Podstawowymi czynnikami wpływającymi na jakość przekazywanej mowy są:

- **Opóźnienia** – stanowiące sumę opóźnień wprowadzonych przez kodeki audio, związanych z rozmiarami pakietów, czasami buforowania po stronie odbiorczej i czasu transmisji pakietu przez sieć.
- **Zjawisko echa** – Echo powstaje z powodu przenikania energii sygnału przez elementy składowe urządzenia krańcowego. Najczęściej przyczyną echa jest niedopasowanie rozgałęźnika przy przejściu z toru nadawczego i odbiorczego (4-przewodowego) na linię 2-przewodową.
- **Utrata pakietów w sieci lub ich przekłamanie** – spowodowane zastosowaniem szybkiego protokołu UDP.

Operator sieci wykorzystując dodatkowe środki techniczne zapewniające nadzorowanie QoS oraz sterowanie zasobami technicznymi jest w stanie efektywnie zarządzać pasmem transmisyjnym, jitterem oraz opóźnieniami wynikającymi z dynamicznego routingu w sieci internetowej. Ponadto, istnieje możliwość:

- efektywnego nadzorowania i sterowania zasobami sieci,
- lepszej administracji siecią, co jest szczególnie ważne w przypadku sieci oferujących usługi zintegrowane,
- efektywniejsze dopasowania świadczonych usług do oczekiwań klienta,
- oraz elastyczne sterowanie jakością oferowanych usług.

Z punktu widzenia klienta, oczekiwanym efektem wdrożonych do sieci jest na pewno dostępność usług, jakość połączeń głosowych oraz tolerowane opóźnienia w przekazie głosu. Jest to wciąż trudne zadanie ze względu na występujące:

- niejednorodne sieci teletransmisyjne,
- dużą dynamikę obciążenia kanałów teletransmisyjnych,
- brak gwarancji na wymagane pasmo transmisyjne,

² Collins D.: Carrier Grade voice over IP. McGraw-Hill Professional. 2002.

- różne wydajności węzłów w sieci,
- różnorodne systemy zabezpieczeń utrudniające przepływ informacji,
- ograniczenia technologii dostępowych do abonenta,

Poziom świadczonych usług jest ostatecznie miarą oceny operatora sieci VoIP.

3.4. Centrala VoIP

Podobnie jak to się dzieje w klasycznej sieci PSTN, telefonia internetowa VoIP wymaga elementów/urządzeń umożliwiających komutację połączeń. W przypadku klasycznych sieci z komutacją łączy tymi elementami są centrale telefoniczne, w przypadku telefonii internetowej są to serwery komutacji VoIP, nazywane popularnie centralami VoIP. Centralą VoIP może być dowolny serwer lub komputer PC pracujący pod kontrolą systemu operacyjnego Linux. Centrala VoIP jest połączona z siecią Internet za pośrednictwem stałego, szerokopasmowego łącza symetrycznego o przepływności adekwatnej do spodziewanego ruchu telekomunikacyjnego oraz zastosowanych kodeków audio – video. Typowa centrala VoIP zazwyczaj bazuje na rdzeniu centrali opracowanej przez Marka Spencera i firmę Dignum – Asterisk. Do cech charakterystycznych centrali VoIP należy zaliczyć:

- komutację połączeń głosowych i wideogłosowych,
- obsługę bram sieci PSTN,
- tele i wideokonferencje,
- pocztę głosową,
- Music on Hold, czyli muzyka na czas oczekiwania,
- kolejgowanie połączeń (również z powiadomieniami głosowymi),
- zapowiedzi głosowe,
- realizację usług dodatkowych zgodnych ze standardami tradycyjnych central cyfrowych.

Dzięki prawie nieograniczonym możliwościom integracji z aplikacjami zewnętrznymi, możliwe jest także zwiększenie funkcjonalności centrali o niektóre usługi, do których należą między innymi:

- interaktywne menu głosowe (IVR),
- fax to e-mail,
- poczta głosowa na e-mail,
- Click to Call,
- Text to Speech (syntezator mowy),
- Voice recognition (rozpoznawanie mowy),
- integracja z systemem CRM,
- automatyczny dialer do połączeń wychodzących.

- obsługę LCR (*Least Cost Routing*) – wybór najtańszego operatora docelowego sieci stacjonarnej.

Istnieje również możliwość pisania skryptów AGI, dzięki którym można w sposób praktycznie nieograniczony modyfikować pracę centrali telefonicznej.

Programowanie centrali z poziomu kodu źródłowego jest zajęciem stosunkowo uciążliwym. Wszelkie błędy w składni poleceń prowadzą do błędów, które będą powodować nieprawidłowe lub niepełne funkcjonowanie abonenta i często nie są od razu możliwe do wykrycia. W związku z tym, istnieje duża liczba „nakładek” graficznych (GUI) na rdzeń centrali Asterisk. Jedną z popularniejszych jest rozszerzenie FreePBX i jej wersja TRIKBOX. W takim przypadku obsługę centrali przeprowadza się poprzez typową przeglądarkę internetową stron internetowych. Na potrzeby tego ćwiczenia uruchomiono w laboratorium centralę VoIP w wersji TRIKBOX.

3.4.1. Charakterystyka centrali TRIKBOX

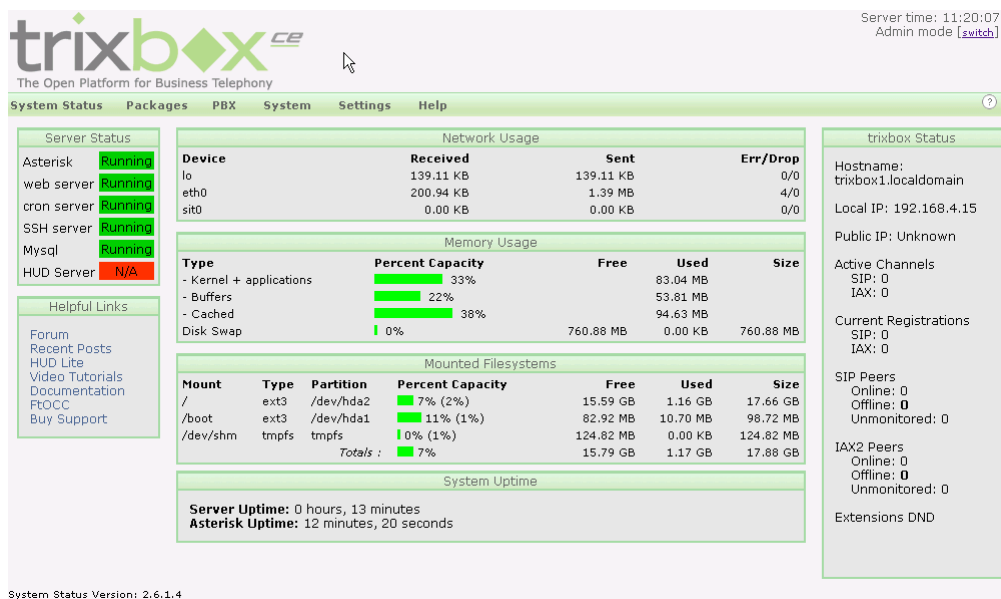
Trixbox jest centralą VoIP bazującą na oprogramowaniu Open Source. Początkowo znana była pod nazwą Asterisk@home, jednakże od 2006 roku znana jest pod nazwą TRIKBOX. Obecnie występuje w dwóch wersjach: bezpłatnej CE oraz komercyjnej Pro. W przypadku komercyjnej wersji istnieje możliwość zakupu centrali w postaci gotowego rozwiązania sprzętowego (patrz rysunek).



Rys. 4. Sprzętowa wersja centrali TRIKBOX

Oprogramowanie sterujące połączeniami opiera się na dystrybucji Linuksa CentOS. System zawiera nie tylko preinstalowaną centralę Asterisk, lecz także inne narzędzia ułatwiające rozpoczęcie pracy z systemem oraz wspomagające jego administrację. Podczas korzystania z TRIKBOX nie jest wymagana znajomość systemu Linux. Zasadniczą konfigurację można

realizować poprzez interfejs GUI. Poniższy rysunek przedstawia główne okno uruchomionej centrali.



Rys. 5. Główne okno centrali TRIXBOX

3.4.2. Usługi dodatkowe centrali

Centrala TRIXBOX podobnie, jak każda nowoczesna centrala cyfrowa sieci publicznej, pozwala na realizację wielu usług dodatkowych. Abonent centrali może samodzielnie aktywować i wyłączyć usługi wprowadzając odpowiednie kody sterujące wprost z klawiatury swojego terminala. Przykładowe usługi prezentuje tabela 4.

Tab.4 Kody usług dodatkowych centrali Asterisk

Nazwa usługi	Nazwa angielska	Kod
Lista połączeń złośliwych		
numer listy złośliwych wywołań	<i>Black list a number</i>	*30
usuwanie numeru z listy złośliwych wywołań	<i>Remove a number from the blacklist</i>	*31
dopisanie do listy złośliwych wywołań ostatnio wywołującego abonenta	<i>Blacklist the last caller</i>	*32
Przekazywanie połączeń (Call Forward)		
aktywacja przekierowania połączenia w przypadku nieobecności abonenta	<i>Call Forward No Answer/Unavailable Activate</i>	*52
wyłączenie przekierowania połączenia w	<i>Call Forward No</i>	*53

przypadku nieobecności abonenta	<i>Answer/Unavailable</i> <i>Deactivate</i>	
aktywacja przekierowania wszystkich połączeń przychodzących	<i>Call Forward All Activate</i>	*72
wyłączenie przekierowania wszystkich połączeń przychodzących	<i>Call Forward All Deactivate</i>	*73
aktywacja przekierowania w przypadku zajętości abonenta	<i>Call Forward Busy Activate</i>	*90
deaktywacja przekierowania w przypadku zajętości abonenta	<i>Call Forward Busy Deactivate</i>	*91
Połączenia oczekujące (Call Waiting)		
aktywacja połączeń oczekujących	<i>Call Waiting Activate</i>	*70
wyłączenie usługi połączeń oczekujących	<i>Call Waiting Deactivate</i>	*71
Usługa nie przeszkadzać (Do-Not-Disturb)		
włączenie usługi „nie przeszkadzać”	<i>DND Activate</i>	*78
wyłączenie usługi „nie przeszkadzać”	<i>DND Deactivate</i>	*79
Usługi informacyjne (Info services)		
Test pogłosu	<i>Echo test</i>	*43
Sprawdzenie własnego numeru katalogowego	<i>Speak Your Exten Number</i>	*65
Sprawdzenie ostatnio wybieranego numeru	<i>Call Trace</i>	*69
Zegarynka	<i>Speaking Clock</i>	*60
Poczta głosowa	<i>Voicemail</i>	*97

3.4.3. Obsługa centrali TRIBOX

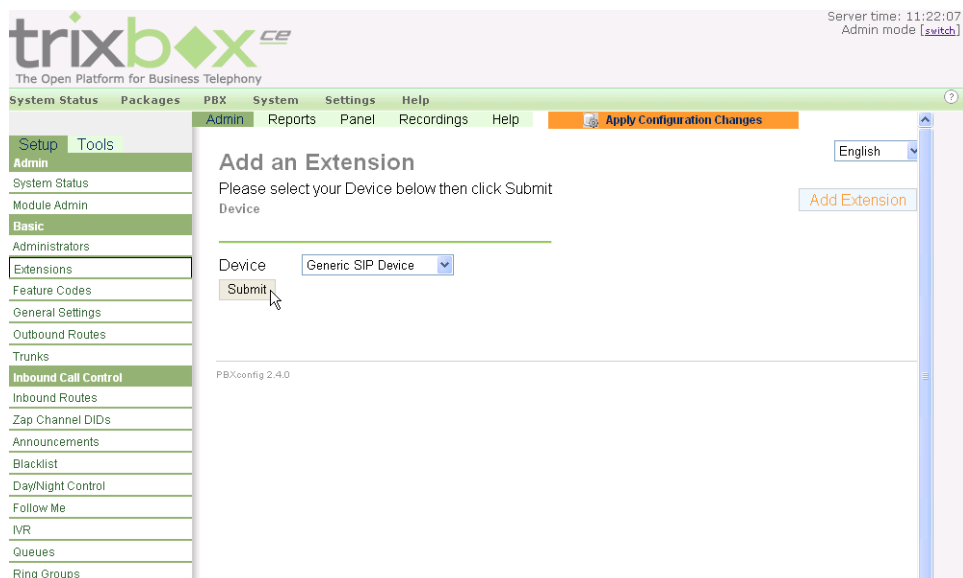
Do obsługi centrali TRIBOX wystarczy przeglądarka internetowa zainstalowana na dowolnym komputerze pracującym w tej samej sieci, co centrala. Dostęp sieciowy do centrali zainstalowanej w laboratorium jest możliwy po wpisaniu adresu **192.168.11.100**. W dalszej kolejności należy wykonać następujące czynności:

- przełączyć profil abonenta na administratora centrali wybierając opcję: **User mode [switch]**, a następnie wpisać użytkownika: **maint**, hasło: **password**,
- na listwie górnej okna głównego rozwinąć zakładkę: **PBX**, a następnie wybrać opcję: **PBX Settings**, aby otworzyć okno konfiguracji centrali,

- W celu edycji ustawień abonentów należy wybrać z menu bocznego: **Setup -> Basic -> Extensions**,
- Aby stworzyć nowego abonenta w centrali należy wybrać z listy: **Generic SIP Device** i potwierdzić przyciskiem **Submit**.

UWAGA: Zmiana ustawień w centrali (po zatwierdzeniu zmian – przycisk Done) wymaga jej restartu. Komunikat o potrzebie restartu jest również wyświetlany w postaci napisu w pomarańczowej ramce w górnej części okna centrali „Apply Configuration Changes”.

Po wykonaniu powyższych czynności powinno zostać wyświetlone okno zarządzania abonentami SIP³ (patrz rysunek 5).



Rys. 6. Okno Extensions centrali VoIP

3.4.4. Procedura tworzenia nowego abonenta VoIP

Konfiguracja centrali do potrzeb stworzenia nowego abonenta wymaga wprowadzenia zestawu parametrów w formie tekstowej. Standardowa składnia jest zależna od stosowanego protokołu komutacji VoIP. Dla najpopularniejszego protokołu SIP, konfiguracji nowych abonentów dokonuje się w pliku `/etc/asterisk/sip.conf` centrali, a opis abonenta będzie miał następującą postać:

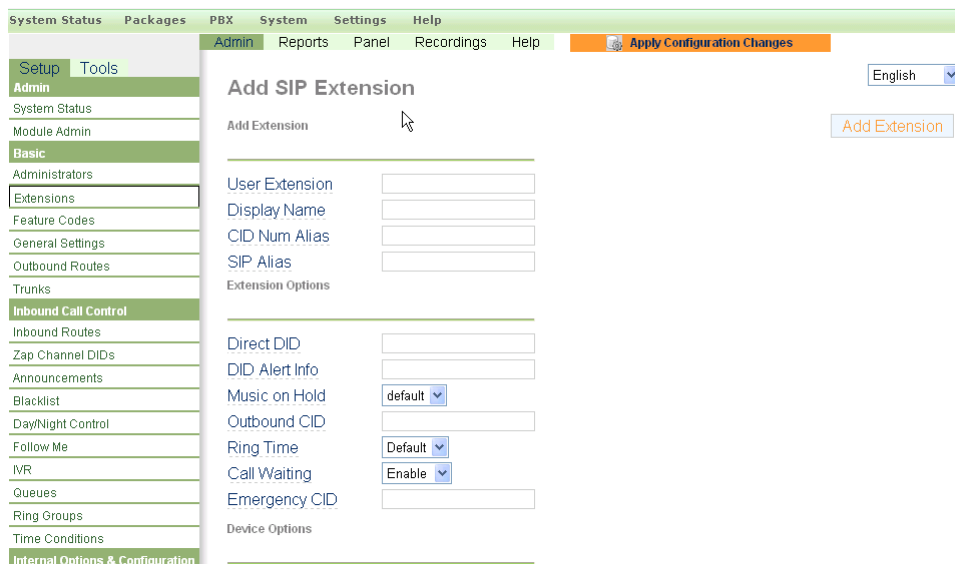
³ SIP oznacza protokół komutacji VoIP za pośrednictwem którego będzie komunikował się terminal abonenta.

[general]	- fragment ustawień ogólnych
port=5060	- ustawienie portu sygnalizacji SIP
bindaddr=192.168.0.10	- adres, pod którym centrala nasłuchuje komunikatów sygnalizacji
context=default	- standardowe ustawienie dla abonentów SIP
[abonent]	- definicja (nazwa) nowego abonenta
type=friend	- rodzaj abonenta (inne opcje: peer, user)
secret=haslo	- hasło uwierzytelniające abonenta w centrali
host=dynamic	- sposób nadawania adresu IP abonentowi
defaultip=192.168.0.15	- alternatywny adres IP dla host=dynamic
dtmfmode=rfc2833	- pozwolenie na transmisję kodów DTMF
disallow=all	- zerowanie ustawień kodeków A/V
allow=ulaw	- zezwolenie użycia kodeka u PCM
allow=gsm	- zezwolenie użycia kodeka GSM
allow=ilbc	- zezwolenie użycia kodeka ilbc
language=pl	- narodowość abonenta
mailbox=1000@internal	- adres skrzynki pocztowej
itd.	

Utworzenie nowego abonenta w centrali TRIKBOX jest o wiele prostsze, gdyż wykonywane jest poprzez GUI nakładki graficznej centrali w oknie przeglądarki. Standardowa konfiguracja wymaga wprowadzenia co najmniej trzech podstawowych parametrów identyfikujących nowego abonenta, tj.:

1. **User Extension** – numer katalogowy abonenta SIP w centrali,
2. **Display Name** – nazwa abonenta, np. imię i nazwisko, które będzie wyświetlane na wyświetlaczu abonenta wywoływanego,
3. **Secret** – unikalne hasło uwierzytelniające abonenta w centrali.

Po wpisaniu wymienionych wyżej parametrów należy operację zatwierdzić naciskając przycisk **Submit**. Aby zmiany zostały przyjęte przez centralę należy zmienioną konfigurację zatwierdzić naciskając czerwony przycisk **Apply Configuration Changes**. Po wykonaniu tej operacji centrala jest przygotowana do obsługi abonenta w sieci VoIP. Potwierdzeniem poprawności przeprowadzonej operacji utworzenia abonenta VoIP jest wyświetlenie jego danych w panelu aktywności abonentów centrali (górną belką opcja **Panel**).



Rys. 7. Okno edycji nowego abonenta w centrali VoIP

Poza standardową konfiguracją każdego nowego abonenta w centrali, warto zwrócić uwagę na **usługę poczty głosowej (Voicemail & Directory)**. Jej konfiguracja wymaga wprowadzenia odrębnego hasła złożonego z samych cyfr. Usługa poczty głosowej umożliwia abonentom pozostawienie wiadomości głosowej dla abonenta, jak również obsługę konta abonenckiego w sieci komputerowej po wcześniejszym zalogowaniu z użyciem numeru katalogowego jako loginu i hasła do poczty głosowej.

Konfigurację tej części usług abonenta definiuje między innymi:

1. **Status – Disabled** (wyłączona poczta) / **Enabled** (włączona poczta),
2. **Voicemail Password** – unikalne hasło do poczty głosowej,
3. **Email Address** – w tym miejscu można wprowadzić adres e-mail, na który ma być wysyłana wiadomość o nadchodzącej poczcie głosowej,
4. **Email Attachment** – do poczty e-mail dołączany jest załącznik z nagraniem poczty,
5. **Play CID** – umożliwia w trakcie odsłuchiwania poczty głosowej odczytanie numeru katalogowego nadawcy wiadomości,
6. **Delete Voicemail** – opcja umożliwia kasowanie wiadomości ze skrzynki głosowej.

Menu skrzynki wiadomości, dostępne dla użytkownika, prezentowane jest w języku angielskim. Znaczenie poszczególnych komunikatów przedstawia tabela 5.

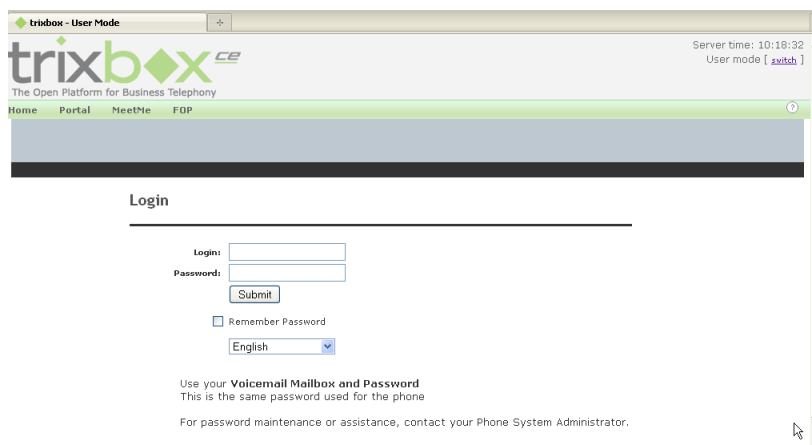
Tab.5 Menu poczty głosowej

kod	funkcja	kod	funkcja	kod	funkcja
1	Stare wiadomości	3	Opcje zaawansowane	1	Wyślij odpowiedź
				2	Oddzwoń
				3	Nagłówek wiadomości
				4	Rozmowa wychodząca
				5	Zostaw wiadomość
				*	Powrót do menu głównego
		4	Odtwórz poprzednią wiadomość		
		5	Powtórz bieżącą wiadomość		
		6	Odtwórz następną wiadomość		
		7	Skazuj bieżącą wiadomość		
		8	Przełącz wiadomość do skrzynki mailowej		
		9	Zachowaj wiadomość		
		*	Pomoc		
#	wyjście				
2	Zmiana folderu				
3	Opcje zaawansowane				
0	Opcje skrzynki głosowej	1	Nagraj wiadomość w przypadku niedostępności		
		2	Nagraj wiadomość w przypadku zajętości		
		3	Nagraj imię		
		4	Zmień hasło		
		*	Powrót do menu głównego		
*	Pomoc				
#	Wyjście				

3.4.5. Panel abonencki w centrali TRIXBOX

Zarządzanie częścią usług z poziomu terminala abonenta (telefonu) często jest niewygodne, gdyż wymaga skupienia na komunikatach oraz znajomości kodów usług dodatkowych. W przypadku central VoIP istnieje możliwość kontroli własnego konta poprzez

sieć internetową za pośrednictwem tzw. **panelu abonenckiego**. Przykład takiego panelu przedstawia rysunek 7.



Rys. 8. Okno logowania do Panelu abonenckiego centrali VoIP

Procedura logowania do Panelu abonenckiego wygląda następująco:

1. Przełączyć profil abonenta z administratora centrali na użytkownika wybierając opcję: **Admin mode [switch]**, tak aby pojawiło się **User mode [switch]**,
2. Na liście górnej okna głównego wybrać opcję **Portal**,
3. W oknie logowania jako **Login** wpisać numer abonenta, jako **Password** hasło do poczty głosowej.

Po zalogowaniu do Panelu istnieje możliwość wyświetlenia listy:

- **Voicemail** - odsłuchanie poczty głosowej,
- **Call Monitor** – lista połączeń wychodzących,
- **Phone Features** – usługi dodatkowe:
 - **Call Waiting** – połączenie oczekujące,
 - **Do No Disturb** – funkcja „nie przeszkadzać”,
 - **Call Forwarding** (przekierowanie połączenia w przypadku):
 - **Unconditional** - bezwarunkowe
 - **Unavailable** – abonent niedostępny,

Busy – abonent w trakcie rozmowy,

3.5. Terminale VoIP

Praktyczne użycie technologii VoIP wymaga zastosowania terminali abonenckich VoIP oraz innych urządzeń wspomagających proces komutacyjny. Terminale VoIP najogólniej można podzielić na dwie charakterystyczne grupy: programowe (*softphone*) oraz sprzętowe (*hardware phone equipment*).

3.5.1. Terminale software'owe

Do pierwszej z wymienionych obecnie można zaliczyć różnorodne aplikacje instalowane w postaci samodzielnych programów przeznaczonych na komputery PC oraz aplikacje pozwalające na uruchomienie telefonu VoIP na platformie mobilnej telefonu komórkowego, smartfonu lub tabletu. Do specyficznej podgrupy **softphone'ów** należą tzw. **webphone'y**. Pozwalają one na komunikację VoIP bezpośrednio przez strony internetowe. Rozwiązanie typu *webphone*, w odróżnieniu od *softphone'a*, nie jest związane z żadną platformą programową czy sprzętową. Do uruchomienia *webphone'a* potrzebna jest jedynie przeglądarka internetowa z odpowiednio zainstalowanym plug-in'em. Brak konieczności bezpośredniej instalacji na dysku komputera PC niezależnego oprogramowania daje możliwość korzystania z takiego telefonu niemalże na każdym terminalu internetowym posiadającym przeglądarkę internetową. Wadą takiego rozwiązania może być jednak brak plug-ina dla konkretnej przeglądarki internetowej.

Jednym z rozwiązań typu *softphone* jest, wykorzystywany w trakcie realizacji ćwiczenia, bezpłatny program X-Lite. Jego zaawansowane możliwości umożliwiają obsługę do czterech niezależnych numerów, posiada książkę telefoniczną, udostępnia zaawansowaną analizę historii połączeń, funkcję połączeń konferencyjnych oraz wideokonferencyjnych. Softphone jest dostępny bezpłatnie, a udostępniony kod źródłowy aplikacji jest przyczyną dużej popularyzacji programu wśród operatorów VoIP, którzy mogą umieścić w aplikacji swoje logo, wprowadzić standardowe ustawienia swoich serwerów VoIP, jak również wzbogacić program o dodatkową funkcjonalność, np. możliwość szyfrowania połączeń. Aplikacja pozwala na pracę z protokołem sygnalizacyjnym SIP. Okno główne programu X-Lite zostało przedstawione na rys. 8.



Rys. 9. Terminale software'owe VoIP. Od lewej: X-Lite, Linphone, tpad

Zastosowanie softphone'ów ma duże praktyczne zastosowanie w firmach transportowych. Jako dedykowane miejsca tej technologii wskazuje się różnego rodzaju centra zarządzania i dystrybucji informacji typu *Call Center*. Użycie aplikacji terminala VoIP oferuje większe możliwości działania użytkownika z innymi aplikacjami komputerowymi takimi, jak na przykład bazy danych, informacja GIS, dokumentacja elektroniczna klienta. Dodatkową zaletą telefonu w postaci aplikacji komputerowej jest stosunkowo prosta możliwość rejestracji prowadzonych rozmów bezpośrednio na twardym dysku komputera, na którym zainstalowany został softphone. W klasycznych centralach PBX jedyną możliwością jest zastosowanie urządzeń zewnętrznych, które zawsze są kosztowne i trudne w administracji.

Wadą rozwiązań software'owych jest konieczność zastosowania platformy sprzętowej, na której softphone mógłby zostać uruchomiony. Dodatkowo, by terminal mógł w pełni spełniać swoje zadania, maszyna na której został zainstalowany musi być cały czas uruchomiona. Takie rozwiązanie może okazać się dość uciążliwe w przypadku abonentów indywidualnych, pragnących mieć stały dostęp do telefonu we własnym domu. Innym ograniczeniem może być również system operacyjny, na którym zainstalowany jest terminal oraz jego wewnętrzne mechanizmy zarządzania i kontroli uruchomionych aplikacji.

Do niewątpliwych zalet trzeba natomiast zaliczyć stosunkowo małe wymagania odnośnie wydajności procesora oraz karty dźwiękowej, możliwość utworzenia książki telefonicznej i korzystanie z usług więcej niż jednego operatora telefonii internetowej.

3.5.2. Terminale hardware'owe

Rozwiązania hardware'owe należą do grupy urządzeń nie wymagających komputera jako elementu pośredniczącego w procesie inicjacji i germinacji połączeń VoIP. Urządzenia te można podzielić na dwie grupy: **telefony VoIP** oraz **bramy VoIP**.

Telefony VoIP stanowią kompleksowe rozwiązania przypominające wyglądem nowoczesne telefony stacjonarne. Występują w wersji:

- **przewodowej** – podłączanej do lokalnej sieci Ethernet przy pomocy skrętki,
- **bezprzewodowej** – zawierającej bezprzewodową słuchawkę DECT i podłączaną do sieci lokalnej bazę systemu.

Bramy VoIP są elementami pośredniczącymi pomiędzy tradycyjnymi urządzeniami (telefony, faxy, modemy) podłączanymi bezpośrednio do tradycyjnych sieci telekomunikacyjnych, a siecią internetową. Ich konfiguracja pozwala na optymalne wykorzystanie istniejącego sprzętu i nowoczesnej technologii. Przykładowe urządzenia przedstawiono na rysunku 9.



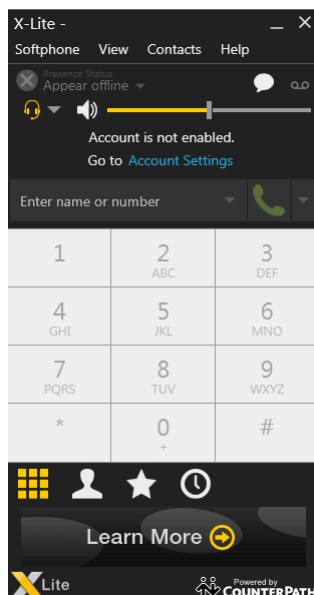
Rys. 10. Terminale hardware'owe VoIP. Od lewej: telefon przewodowy i bezprzewodowy AASTRA, brama AVM

3.6. Procedury konfiguracji wybranych terminali VoIP

Bez względu na to czy abonent centrali VoIP korzysta z telefonu zainstalowanego w formie aplikacji na swoim komputerze, czy używa telefonu sprzętowego musi dokonać jego konfiguracji. Prawidłowa konfiguracja telefonu VoIP powinna zawierać: unikalny **login** i **hasło** abonenta uwierzytelniające abonenta w centrali, **domenę operatora** (adres IP centrali VoIP). W zależności od typu urządzenia i jego funkcjonalności, proces konfiguracji może obejmować szerokie spektrum dodatkowych opcji.

3.6.1. Procedura konfiguracji wybranego Softphone'a (X-Lite)

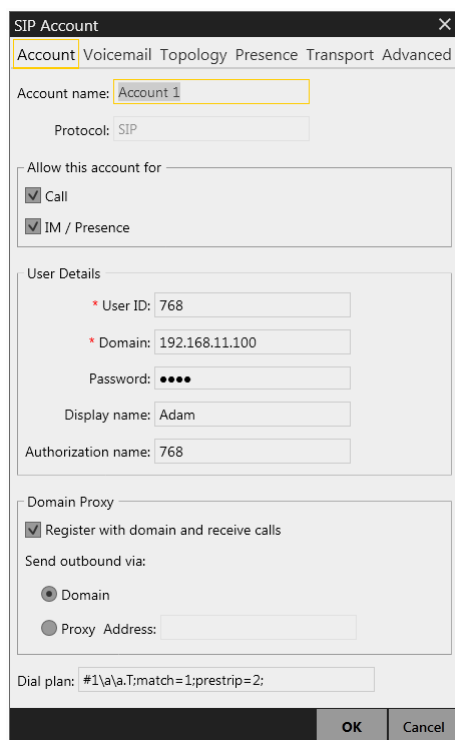
Spośród wielu różnych typów programów typu softphone, na potrzeby laboratorium został wybrany program firmy CounterPath o nazwie X-Lite. Okno główne programu zostało przedstawione na rysunku (Rys. 11).



Rys. 11. Widok okna głównego terminala VoIP typu X-Lite

Skrótowy opis podstawowej konfiguracji aplikacji X-Lite dla OS MS Windows 10 został zamieszczony poniżej. Ze względu na objętość niniejszej instrukcji ograniczono się do przedstawienia procedury konfiguracji nowego abonenta VoIP.

1. Kliknij przyciskiem myszy górną część okna oznaczoną jako **Softphone**. Po rozwinięciu menu wybierz opcję **Accounts Settings**.
2. W nowym oknie (patrz Rys. 12), w zakładce Account wypełnij kolejne pola:
 - a. **Account name**: - dowolna nazwa przypisana do konta,
 - b. **User ID**: - nr katalogowy abonenta,
 - c. **Domain**: - adres IP centrali VoIP,
 - d. **Password**: - unikalne hasło uwierzytelniające abonenta w centrali,
 - e. **Display name**: - dowolna nazwa, która będzie się wyświetlała przy wywołaniach,
 - f. **Authorization name**: - nr katalogowy abonenta,
3. Zmiany w ustawieniach terminal zatwierdzamy przyciskiem **OK** w dolnej części okna konfiguracyjnego.



Rys. 12. Okno konfiguracji ustawień abonenta w aplikacji X-Lite

Pozostałe opcje ustawień nie są wymagane w podstawowej konfiguracji telefonu. Zakończenie procesu konfiguracji dostępu do konta VoIP w centrali powoduje zamknięcie okna przedstawionego na rysunku (Rys. 12). Należy jednak sprawdzić poprawność zalogowania telefonu do centrali. W przypadku wystąpienia błędów dokonać niezbędnej korekty wpisanych parametrów. Po zalogowaniu do centrali na wyświetlaczu aplikacji powinien pojawić się komunikat: **Ready Your username is: xxxx**. Od tej chwili możemy wykonywać połączenia głosowe za pośrednictwem softphone X-Lite do innych abonentów sieci VoIP.

3.6.2. Konfiguracja telefonu Yealink SIP-T23P

Telefon Yealink SIP-T23P charakteryzuje się intuicyjnym interfejsem użytkownika oraz bogatą funkcjonalnością. Jest ceniony za swoją wysoką wydajność oraz łatwość w obsłudze. Dzięki wykorzystaniu technologii Yealink HD, umożliwia różnorodną i czystą komunikację głosową, opcję zdalnego zarządzania oraz możliwość korzystania z aplikacji komunikacyjnych innych firm. Wygląd urządzenia przedstawiono na rysunku.



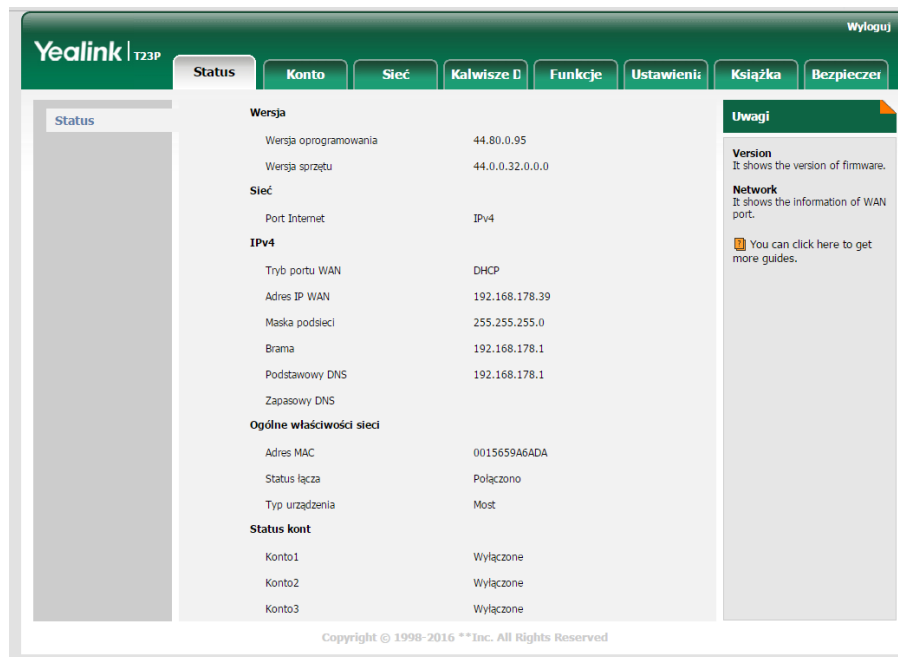
Rys. 13. Telefon Yealink SIP-T23

Wśród wielu funkcji oferowanych przez ten terminal należy zwrócić uwagę na:

- wstrzymanie połączenia, wyciszenie, tryb „Nie przeszkadzać” (DND)
- szybkie wybieranie (za jednym dotknięciem), Hotline
- połączenia anonimowe, odrzucanie połączeń anonimowych,
- przekierowanie połączeń, połączenia oczekujące, przekazywanie połączeń
- pocztę głosową, parkowanie połączeń, przejmowanie połączeń,
- grupowe odsłuchiwanie, SMS
- lokalną trójstronną konferencję,
- interkom, paging, muzyka dla połączenia oczekującego,
- zakończenie połączenia, nagrywanie połączeń, hot-desking,
- bezpośrednie połączenia IP bez użycia SIP Proxy,
- Dial plan, automatyczne wybieranie numeru po podniesieniu słuchawki, przeglądarka XML, action URL/URI, zrzuty ekranu LCD,
- wskaźnik zajętości linii (BLF),
- wskaźnik wiadomości oczekującej (MWI).

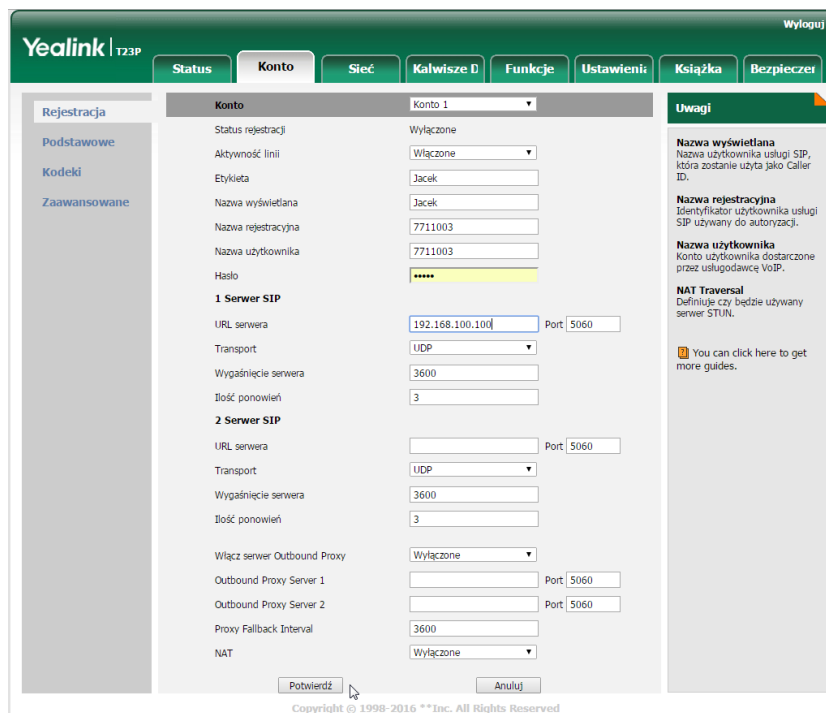
Konfiguracja terminala jest możliwa na dwa sposoby. Poprzez klawiaturę urządzenia lub poprzez wbudowany serwer WWW. W tym drugim przypadku konfiguracja polega na zmianie ustawień poprzez komputer z przeglądarką internetową znajdujący się w tej samej podsieci co telefon. Lokalizacja telefonu w sieci jest możliwa po ustaleniu jego adresu IP. Najprostszym sposobem takiej identyfikacji jest sprawdzenie adresu IP na wyświetlaczu w **Menu -> Status**.

Dostęp do konfiguracji jest chroniony hasłem (login: **admin**, hasło: **admin**). Po wpisaniu danych uwierzytelniających możliwa jest dalsza konfiguracja urządzenia. Okno główne przedstawiono na rysunku.



Rys. 14. Okno statusu telefonu Yealink SIP-T23

Konfiguracja parametrów uwierzytelniających konto abonenta w telefonie przeprowadza się w zakładce **Konto**, pod zakładce **Rejestracja**.



Rys. 15. Widok okna rejestracji nowego abonenta w telefonie SIP-T23

W tym miejscu należy wprowadzić ustawienia w polach:

- Aktywność linii – włączona,
- Etykieta – dowolna nazwa,
- Nazwa wyświetlana – dowolna nazwa,
- Nazwa rejestracyjna – zazwyczaj numer katalogowy abonenta,
- Nazwa użytkownika – numer katalogowy abonenta,
- Hasło – ciąg znaków uwierzytelniających abonenta w centrali VoIP,
- URL serwera – adres IP centrali VoIP.

Zmiany w konfiguracji kont należy zatwierdzić przyciskiem „**Potwierdź**”.

3.6.3. Konfiguracja telefonu GRANDSTREAM GXP 2000

Telefon sprzętowy typu GRANDSTREAM GXP 2000 należy do grupy nowoczesnych i zaawansowanych technologicznie urządzeń do głosowej komunikacji w sieci internetowej. Dzięki zaawansowanej funkcjonalności, z dodatkowym modulem sygnalizacyjnym, może posłużyć jako pulpit dyspozytorski lub urządzenie typu AWIZO. Zdjęcie urządzenia przedstawiono na rysunku 11.



Rys. 16. Telefon VoIP GRANDSTREAM GXP 2000

Konfiguracja stacjonarnego telefonu VoIP jest możliwa na dwa sposoby. Pierwszy jest wykorzystanie klawiatury i wyświetlacza będących częścią urządzenia. Drugim, wygodniejszym jest wykorzystanie wbudowanego serwera WWW i zdalna konfiguracja za pośrednictwem przeglądarki internetowej komputera podłączonego do tej samej sieci co telefon. Lokalizacja telefonu w sieci jest możliwa po ustaleniu jego adresu IP. Najprostszym

sposobem takiej identyfikacji jest sprawdzenie adresu IP wyświetlającego się na wbudowanym ekranie telefonu.

UWAGA: Zespół wykonujący ćwiczenie w danej sali ma prawo do konfiguracji urządzeń znajdujących się na stanowisku. W przypadku stwierdzenia ingerencji sieciowej w urządzenia z sąsiedniej sali Zespół będzie ukarany utratą zdobytych punktów z wejściówki.

Właściwa konfiguracja telefonu jest możliwa po zalogowaniu się na stronie wyświetlanej przez wbudowany serwer WWW (hasło: **admin**). W odpowiedniej zakładce (np. **Konto 1 (Account 1), Konto 2, ...**) należy wprowadzić parametry niezbędne do prawidłowej konfiguracji abonenta w centrali, zgodnie z wcześniejszą konfiguracją abonenta w centrali.

The screenshot shows the 'Konfiguracja urządzenia Grandstream' window. At the top, there is a navigation bar with tabs: 'STATUS', 'USTAWIENIA PODSTAWOWE', 'USTAWIENIA ZAAWANSOWANE', 'KONTO 1', 'KONTO 2', 'KONTO 3', 'KONTO 4', 'EXT 1', and 'EXT 2'. The 'KONTO 1' tab is selected. The main area contains various configuration fields:

- Konto aktywne:** Radio buttons for 'Nie' and 'Tak' (selected).
- Nazwa konta:** Text input with 'Stanowisko 2' and a hint '(np. MojaFirma)'. Below it is the **Server SIP:** field with '192.168.4.15' and hint '(np. sip.mycompany.com, lub adres IP)'. Below that is the **Outbound Proxy:** field with '192.168.4.15' and hint '(np. proxy.myprovider.com, lub adres IP, jeśli występuje)'. Below that is the **SIP User ID:** field with '1592' and hint '(część adresu SIP określająca użytkownika)'. Below that is the **Authenticate ID:** field with '1592' and hint '(może być taki sam bądź różny od)'. Below that is the **Authenticate Password:** field with '***' and hint '(celowo nie wyświetlany dla bezpieczeństwa)'. Below that is the **Nazwa:** field with 'Stanowisko 2' and hint '(opcjonalnie, np. Jan Kowalski)'. Below that is the **Użyj serwera DNS:** radio buttons for 'Nie' (selected) and 'Tak'.
- User ID jest numerem telefonu:** Radio buttons for 'Nie' (selected) and 'Tak'.
- Rejestracja SIP:** Radio buttons for 'Nie' and 'Tak' (selected).
- Wyrejestruj przy restarcie:** Radio buttons for 'Nie' (selected) and 'Tak'.
- Rejestracja wygasa:** Text input with '60' and hint '(w minutach, domyślnie 1 godzina, max 45 dni)'. Below it is the **lokalny port SIP:** field with '5060' and hint '(domyślnie 5060)'. Below that is the **Czas opóźnienia dla nieudanej rejestracji SIP:** field with '20' and hint '(w sekundach. Pomiedzy 1-3600, domyślna wartość 20)'. Below that is the **SIP T1 Timeout:** dropdown menu with '1 sek' selected. Below that is the **SIP T2 Interval:** dropdown menu with '4 sek' selected.

Rys. 17. Okno konfiguracji ustawień konta abonenta w telefonie GrandStream GXP 2000

UWAGA: Zmiany ustawień muszą zostać potwierdzone przyciskiem Update oraz restartem urządzenia – przycisk Restart

3.6.4. Konfiguracja bramy VoIP Linksys Cisco PAP2T

Brama Linksys PAP2T jest wygodnym rozwiązaniem dla osób pragnących zachować dotychczas wykorzystywane terminale telefoniczne sieci analogowej. Dotyczy to zarówno urządzeń telefonicznych, modemowych, faksowych oraz specjalnego przeznaczenia. Zdjęcie urządzenia przedstawiono na rysunku 13.



Rys. 18. Brama VoIP Linksys PAP2T

Pomimo braku zewnętrznego interfejsu, konfiguracja bramy jest możliwa bez użycia dodatkowego komputera lub podobnie, jak to miało miejsce we wcześniej opisywanych terminalach poprzez interfejs WWW. Pierwsza metoda konfiguracji jest realizowana za pomocą telefonu CB podłączonego do gniazda **Phone 1** i polega na zastosowaniu specjalnych kodów wprowadzanych poprzez klawiaturę telefonu. Niektóre z dostępnych kodów zostały umieszczone w tab. Odpowiedzi bramy na zadany kod – komendę są przekazywane głosowo (w języku angielskim) do słuchawki telefonu.

Druga metoda jest o wiele wygodniejszym sposobem konfiguracji. Użycie przeglądarki internetowej zainstalowanej na komputerze znajdującym się w tej samej sieci co brama.

Adres IP bramy Linksys PAP2T można ustalić jedynie poprzez wbudowany system IVR, osiągalny po wprowadzeniu odpowiedniej kombinacji znaków z telefonu podłączonego do portu (gniazda) 1 konfigurowanej bramy.

UWAGA: Zespół wykonujący ćwiczenie w danej sali ma prawo do konfiguracji urządzeń znajdujących się na swoim stanowisku.

Konfiguracja urządzenia jest możliwa bezpośrednio po wpisaniu jego adresu w pasku adresu przeglądarki internetowej (brak założonego hasła). W celu konfiguracji należy wykonać w kolejności:

1. Zmienić **User Login** na **Admin Login**.
2. Zmienić **Basic View** na **Advanced View**.
3. Wybrać linię (zakładkę), która ma być skonfigurowana (aparat telefoniczny powinien być podłączony do gniazda linii pierwszej (**Line 1**)).

4. W oknie Line 1 należy wprowadzić niezbędne parametry konfiguracji abonenta, zgodne z wcześniejszą konfiguracją abonenta w centrali. Ustaw parametry:

- **Enable Line: Yes**
- **NAT Keep Alive Enable: Yes**
- **Register: Yes**
- **Register Expires: 3600**
- **SIP Port: 5060**
- **Proxy: 192.168.100.100** (adres centrali)
- **User ID i AuthID:** nazwa konta SIP (SSDMGGN)
- **Password:** hasło do konta SIP
- **Preferred Codec: G.711**

Poniższy rysunek przedstawia okno konfiguracji bramy wraz z zaznaczonymi ważniejszymi elementami konfiguracji konta abonenta VoIP.

The screenshot displays the Linksys configuration web interface for a PAP2T phone adapter. The 'Voice' section is active, and the 'Line 1' tab is selected. The 'Basic View' is shown. Several configuration fields are highlighted with red boxes, corresponding to the parameters listed in the text above:

- Line Enable:** set to 'yes'.
- SIP Port:** set to '5060'.
- Proxy:** (empty field).
- Register:** set to 'yes'.
- Register Expires:** set to '3600'.
- User ID:** set to '9876543210'.
- Password:** (empty field).

The interface also shows various supplementary services and audio configuration options, all of which are currently set to 'yes'.

Rys. 19. Okno konfiguracji bramy Linksys PAP2T

UWAGA: Bramka Linksys jest urządzeniem, które ma domyślnie włączoną funkcję dynamicznego nadawania adresu IP w sieci (DHCP). Wiąże się z tym ograniczona możliwość wpłynięcia na przydzielony adres IP i brak możliwości weryfikacji tego przydziału z poziomu wyświetlacza, gdyż urządzenie go nie posiada. W tej sytuacji producent urządzenia zaimplementował specjalny system IVR umożliwiający konfigurację i diagnostykę wybranych cech urządzenia poprzez podłączony do bramy terminal analogowy. W tabeli 6 umieszczono zestaw instrukcji sterujących IVR pomocnych podczas konfiguracji bramy.

Tab. 6. Lista kodów IVR bramki Linksys

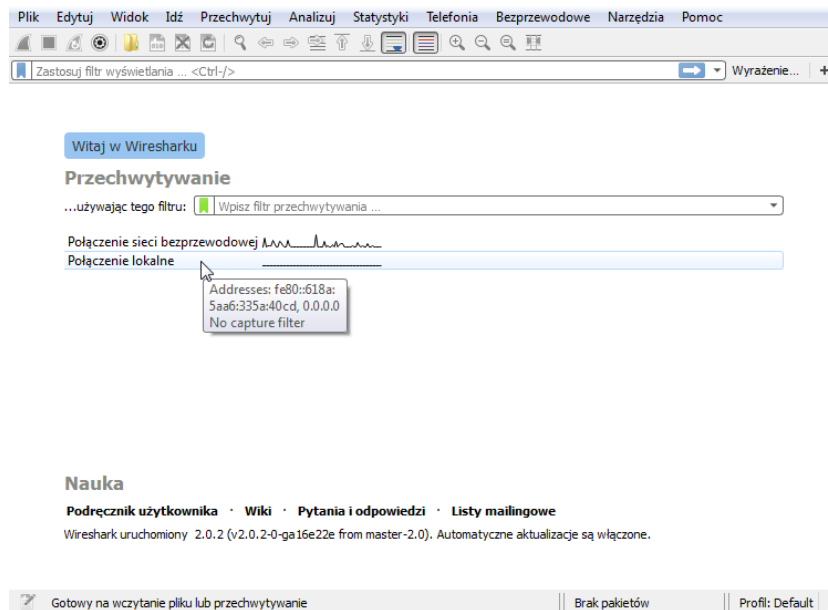
Operacja	Kod z klawiatury	Parametry	Uwagi
Wejście do menu IVR	* * * *	Brak	
Wyjście z menu IVR	*3948#	Brak	
Stan DHCP	*100#	Brak	
Wł/Wył DHCP	*101#	Naciśnij 1 aby włączyć, naciśnij 0 aby wyłączyć	Wymaga hasła
Aktualny adres IP	*110#	Brak	
Nowy statyczny adres IP	*111#	Adres IP wprowadzamy: 192*168*2*215#	Wymaga hasła
Aktualna maska sieci	*120#	Brak	
Nowa maska sieci	*121#	Adres maski wprowadzamy: 255*255*255*0#	Wymaga hasła
Aktualna brama sieci	*130#	Brak	
Nowy adres IP bramy sieci	*131#	Adres IP wprowadzamy: 192*168*2*215#	Wymaga hasła
Adres MAC	*140#	Brak	
Wersja firmware	*150#	Brak	
Factory reset	*73738#	1 – potwierdzenie, * - anulowanie operacji	

4. Wireshark

Wireshark jest darmowym programem pozwalającym na podgląd oraz analizę protokołów przesyłanych pomiędzy komputerem a siecią. Działanie programu odbywa się w dwóch etapach:

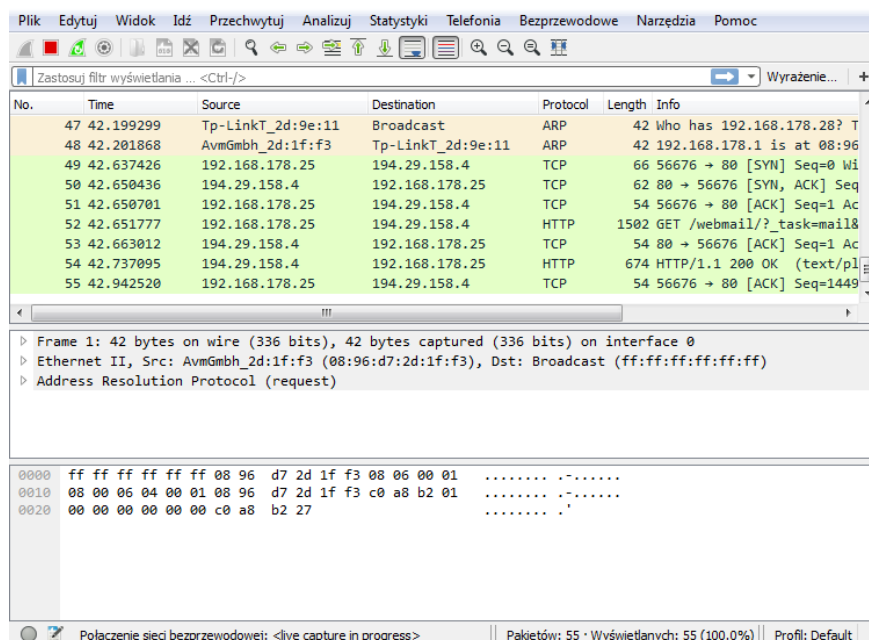
- Nasłuch wybranej karty sieciowej oraz przechwytywanie wszystkich przechodzących przez nią protokołów (zarówno przychodzących jak i wychodzących)
- Po zakończeniu nasłuchu analiza zebranych danych.

Po uruchomieniu programu następuje skanowanie dostępnych interfejsów sieciowych komputera, a następnie wyświetlona ich lista.



Rys. 20. Okno główne programu WireShark

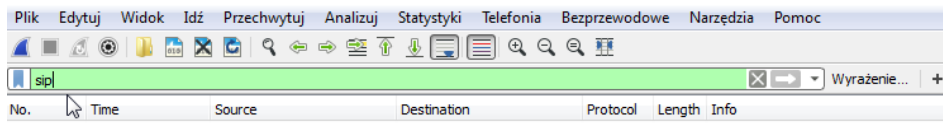
Aby rozpocząć nasłuch danej karty należy najechać myszką na wybrany interfejs sieciowy i kliknąć na niego. W wyniku wykonania tych czynności uruchomione zostanie nowe okno przechwytywania danych.



Rys. 21. Widok okna przechwytywania pakietów

Podczas wykonywania ćwiczenia narzędzie WireShark będzie służyło do obserwacji i analizy wiadomości sygnalizacyjnych komunikujących się stron VoIP, dlatego wśród

wszystkich zarejestrowanych pakietów odfiltrować te związane z sygnalizacją SIP. Wpisanie i uruchomienie filtru jest możliwe po wpisaniu jego nazwy w górnej części okna. Nazwy filtrów wpisujemy małymi literami, np.: sip, udp, tcp, itd.

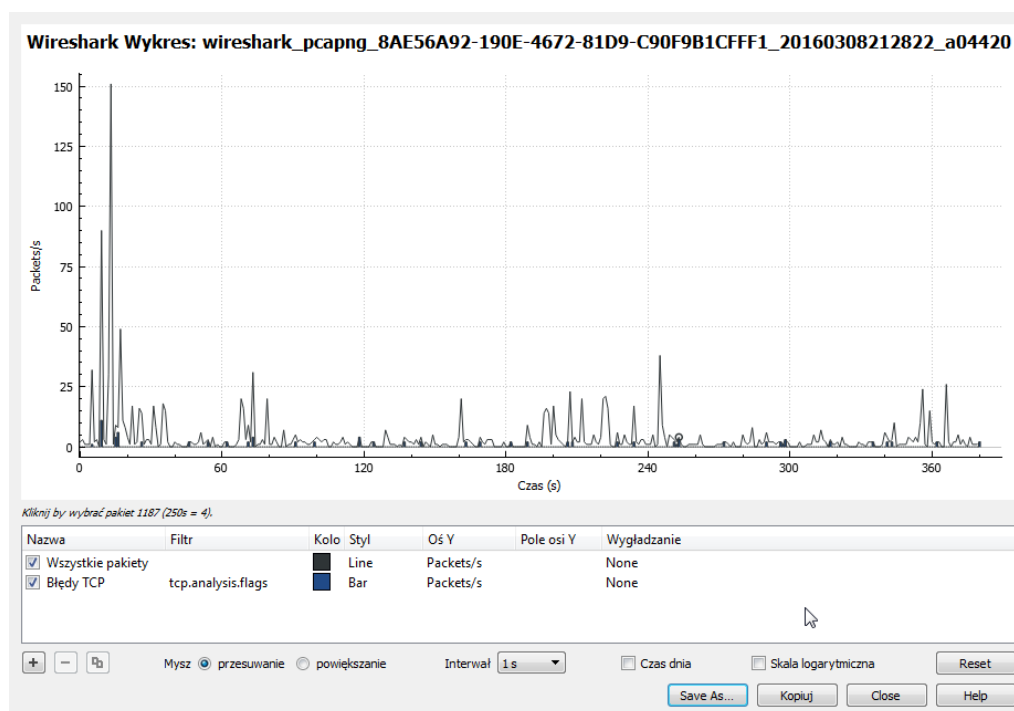


Rys. 22. Widok okna filtrowania wiadomości

Po zakończeniu przechwytywania automatycznie przechodzimy do analizy pakietów. Ukazą nam się wtedy tylko protokoły związane z sygnalizacją SIP. Aby móc przejrzeć treść pojedynczego protokołu SIP należy rozwinąć go (widoczna jest jego cała nazwa – *Session Initiation Protocol*). Zapis protokołów jest możliwy dzięki wydrukowaniu do pliku za pomocą programu PDF Creator. Nie należy zapisywać całego procesu a jedynie interesujące nas elementy (po użyciu filtra podczas drukowania zaznaczamy *Displayed*)

UWAGA: Podczas sygnalizacji często dochodzi do niekontrolowanych błędów w transmisji lub nieprawidłowej rejestracji w serwerze Asterisk. Kod tej błędnej wiadomości to 407 i nie ma ona znaczącego wpływu na przebieg sygnalizacji.

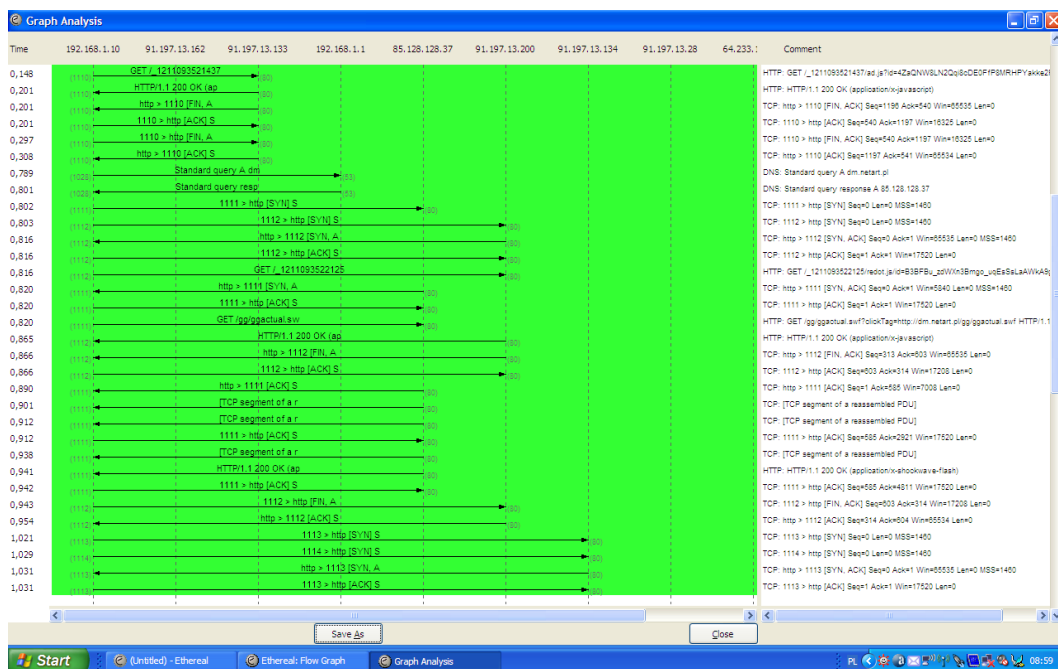
Poza analizą treści protokołu możemy obejrzeć wykres wiadomości danego typu wiadomości. Jest on dostępny w zakładce Statystyki (*Statistics*), opcja Wykres.



Rys. 23. Widok wykresu utworzonego na podstawie określonych danych

Przedstawiony powyżej wykres można dowolnie adaptować poprzez określenie typu wyświetlanych wiadomości. W tym celu należy zmienić wartość w kolumnie *Filtr* znajdującej się pod wykresem. Wykres można zapisać w postaci bitmapy lub pliku PDF wybierając przycisk *Save as...*

Następną bardzo pomocną funkcją programu jest graf wymiany wiadomości SIP. Pozwala on na wizualizację kolejno pojawiających się wiadomości, wskazania ich kierunku i treści. Dostęp do tego narzędzia jest możliwy po wybraniu z zakładki *Telefonia* opcji *Przepływy SIP (Flow Graph)*.



Rys. 21. Program Ethereal. Wymiana komunikatów

Uwaga: Program WireShark nie posiada funkcji zapisu grafów w postaci zewnętrznej. (Zapis możliwy jest w postaci danych odczytywalnych przez sam program). Dlatego też zapis grafu należy wykonywać za pomocą polecenia „Print Screen” a następnie wklejenie ich do Paint’ a.

PRAKTYCZNE UWAGI NA TEMAT REALIZACJI WYBRANYCH ZADAŃ

Przed przystąpieniem do ćwiczenia należy zapoznać się ze stanem procesów w centrali. Następnie należy ustalić adresy IP terminali hardware’owych i bramki Linksys znajdujących się na stanowisku. Adresy te **należy zanotować w protokole z ćwiczeń.**

5. Przebieg ćwiczenia

1. Uruchom na stanowisku laboratoryjnym komputer, a następnie dowolną przeglądarkę internetową.

2. Konfiguracja Centrali VoIP

2.1. Zaloguj się zdalnie do centrali VoIP znajdującej się pod adresem IP: 192.168.11.100.

2.2. Przejdź w tryb administratora centrali: maint, hasło: password,

2.3. Korzystając z menu Extensions rozwiń listę istniejących abonentów centrali.

2.4. Utwórz w centrali trzech nowych abonentów o numerach wg zasady SSDDGGN (gdzie: SS – numer sali, DD – dzień miesiąca wykonywania ćwiczenia, GG – godzina rozpoczęcia zajęć, N – numer kolejny, tj.: 1 – X-Lite, 2 – Yealink SIP-T23 lub Grandstream GXP 2000, 3 – Linksys PAP2T, 4 – Yealink SIP-T23). Display name – dowolny tekst, Secret – dowolny tekst alfanumeryczny, poczta głosowa – dowolny zestaw cyfr.

2.5. Uruchom panel abonencki (user mode w oknie startowym centrali) i zaloguj się na konto każdego z abonentów wykorzystując numer katalogowy, jako login i hasło do poczty głosowej jako password.

3. Konfiguracja terminali VoIP i podstawowe usługi telefonii internetowej

3.1. Uruchom telefon software'owy X-Lite na komputerze stanowiskowym.

3.2. Dokonaj konfiguracji aplikacji zgodnie z parametrami kodowania dla zaprogramowanego przez zespół pierwszego abonenta centrali SSDDGG1.

3.3. Sprawdź czy aplikacja X-Lite została zarejestrowana w centrali (Status: Ready).

3.4. Korzystając z przeglądarki internetowej zaloguj się do telefonu Yealink SIP-T23 na stanowisku (login i hasło: admin).

3.5. Dokonaj konfiguracji urządzenia zgodnie z parametrami konta utworzonego wcześniej drugiego konta w centrali. W przypadku poczty głosowej możliwość korzystania z wybierania DTMF wymaga zaznaczenia transmisji poprzez protokół RTP!

3.6. Wykonaj operację aktualizacji ustawień terminala. Prawidłowa konfiguracja terminala sygnalizowana jest pogrubioną czcionką wyświetlanego na ekranie urządzenia numeru katalogowego (Grandstream GXP 2000).

3.7. Wykonaj operację konfiguracji bramy Linksys PAP2T (brak ustanowionego hasła).

3.8. Prawidłowo przeprowadzona konfiguracja jest sygnalizowana odpowiednią diodą na obudowie bramy.

- 3.9. Przeprowadź rozmowę testową pomiędzy abonentami softphone'a i każdym z urządzeń hardware'owym. Jak można ocenić jakość rozmowy?
- 3.10. Sprawdź, czy połączenie pomiędzy telefonem Yealink i bramą Linksys pozwala na uzyskanie lepszej jakości połączenia?
- 3.11. Wykonaj operację nagrania wiadomości na poczcie głosowej terminala o numerze 3, a następnie odsłuchaj wiadomość za pośrednictwem terminala (należy najpierw zadzwonić na pocztę głosową w centrali i podać hasło zgodnie z tym, które zostało wprowadzone podczas tworzenia abonenta w centrali).
- 3.12. Włącz usługę dodatkową w terminalu numer 2 – „nie przeszkadzać” (Do Not Disturb). Sprawdź jej działanie tej usługi z innego dostępnego terminala. Co słyszy abonent wywołujący terminal nr 2?
- 3.13. Zamów usługę przekierowania rozmowy abonenta nr 1, gdy abonent ten jest niedostępny na nr 3. Jaka jest reakcja centrali? Z czego ona wynika? Zapisz spostrzeżenia.
- 3.14. Sprawdź działanie usług informacyjnych i zapisz spostrzeżenia (wszystkie komunikaty są wypowiedane w jęz. angielskim):
 - Test pogłosu (Echo Test),
 - Mój numer (Speak Your Exten Number),
 - Moje ostatnie połączenie (Call Trace),
 - Zegarynka (Speaking Clock).
- 3.15. Przeprowadź telekonferencję między wszystkimi abonentami, tj. nr 1, nr 2 i nr 3. Sprawdź jej działanie. Zapisz spostrzeżenia.
- 3.16. Przygotuj sprawozdanie z ćwiczenia.

4. Analiza sygnalizacji SIP

- 4.1. Uruchom program do analizy protokołów Wireshark, następnie przechwytywanie pakietów przesyłanych przez kartę sieciową komputera (Capture Interface's -zakładka Capture).
- 4.2. Zadzwonź za pomocą aplikacji X-Lite na telefon Grandstream.
- 4.3. Odbierz połączenie i przeprowadź rozmowę telefoniczną. Podczas trwającej rozmowy zaobserwuj, który z protokołów generuje największą liczbę pakietów. Zakończ rozmowę, a następnie zanotuj liczbę pakietów każdego z protokołów. Po przeprowadzonej rozmowie zakończ przechwytywanie (klawisz stop).
- 4.4. W okienku Filter uruchom filtrowanie pakietów SIP. Przeprowadź analizę kolejnych pakietów pod kątem protokołów kolejnych warstw modelu OSI. Jakie protokoły są

- wykorzystywane w każdej z warstw do transmisji wiadomości SIP? Zanotuj wyniki pomiarów.
- 4.5. Przeanalizuj wiadomości sygnalizacyjne poczynając od wiadomości o metodzie INVITE, a skończywszy na wiadomości BYE i OK. W tym celu dla każdej z nich rozwiń element "Session Initiation Protocol", a następnie nagłówek wiadomości "Message Header". Zwróć uwagę, które z pól: Contact, To, From, CSeq, są charakterystyczne dla konkretnych wiadomości, a które występują we wszystkich typach. Zapisz adresy IP komunikujących się stron. Narysuj graf przepływu wiadomości pomiędzy stronami. Zaznaczając kierunki i nazwy metod pakietów.
 - 4.6. Z zakładki Statistics wybierz graf przepływu pakietów IO Graphs. Zastosuj filtrację wykresu: Graph1 – udp, Graph2 – sip, Graph4 – sdp. Zmień rozdzielczość na większą. Sprawdź jakiej długości są pojedyncze pakiety głosowe. Zapisz graf (Print Screen). Jaka jest charakterystyka uzyskanych przebiegów? Kiedy pojawiają się pakiety sygnalizacyjne? Dlaczego tak jest?
 - 4.7. Za pomocą polecenia Flow Graph przeanalizuj kierunki przepływu pakietów. Czy kierunki przepływu informacji są zgodne z polami From i To w wiadomościach? Jeżeli nie to, z czego to wynika? Porównaj otrzymany graf z wcześniej opracowanym wykresem. Zapisz go (Print Screen).
 - 4.8. W nowych sesjach przechwyć pakiety sygnalizacyjne i zbuduj odpowiadające im grafy przepływu dla następujących przypadków:
 - 4.9. Nieodebrane połączenie przychodzące na aplikację X-Lite,
 - 4.10. Błędnie wybierany numer abonenta z aplikacji X-Lite,
 - 4.11. Odrzucenie połączenia przez abonenta X-Lite.
 - 4.12. Odebranie połączenia na skrzynce głosowej.
 - 4.13. Zapisz i przeanalizuj testowane przypadki zachowania sygnalizacji.
 - 4.14. Podczas każdej z rozmowy testowej sprawdź prędkość transmisji wychodzącą z komputera na stanowisku. Czy prędkość ta jest w każdym przypadku identyczna?
 - 4.15. Przygotuj sprawozdanie z ćwiczenia.

Literatura

- [1] Bromski M.: *Telefonia VoIP. Multimedialne sieci IP*, Wydawnictwo BTC, Warszawa 2006 r.
- [2] Kabaciński W., Żal M.: *Sieci telekomunikacyjne*, WKiŁ, Warszawa 2008 r.
- [3] Meggelen J.V., Smith J., Madsen L.: *Asterisk. The Future of The Telephony*, O'Reilly, Sebastopol 2005 r.
- [4] Surgut K., *Tania telefonia internetowa VoIP*, Wydawnictwo Helion, Gliwice 2006 r.
- [5] Wallingford T.: *VoIP. Praktyczny przewodnik po telefonii internetowej*, Wydawnictwo Helion, Gliwice 2007 r.