STUDIA INFORMATICA 2001
Volume 22 Number 2 (44)

Sławomir JASEK
PWPT WASKO Sp. z.o.o., Zakład Systemów Telekomunikacyjnych

TRANSMISJA VOIP W SIECIACH KONWERGENTNYCH

Streszczenie. Artykuł pt. „Transmisja VoIP w sieciach konwergentnych" poświęcony jest zagadnieniom transmisji danych typu „voice" w sieciach IP, a także integracji tych sieci z tradycyjnymi sieciami telefonicznymi. Opisane w nim zostały trzy najczęściej spotykane standardy: H.323 ITU-T, SIP IETF oraz MGCP IETF. Poszczególne standardy zostały scharakteryzowane pod względem architektury, podstawowych komponentów działających w sieci i funkcjonalności. Przedstawione zostały też przykładowe procedury zestawiania połączeń.

VOIP TRANSMISSION IN CONVERGENCE NETWORK

Summary. The article „VoIP transmission in convergence network" describes most popular protocols used for transmission voice in IP network and transmission voice between Public Switched Telecommunication Network and IP network. It provides detalied description three most frequently used protocols H.323 ITU-T, SIP IETF, MGCP IETF.

1. Wstęp

Rozwój sieci komputerowych, szczególnie opartych na protokole IP, spowodował konieczność zwiększenia stopnia integracji sieci IP z tradycyjnymi sieciami PTSN (Public Switched Telecommunication Network). Powstanie nowych technologii związanych z przesyłaniem dźwięku i obrazu przez sieci pakietowe umożliwiło tworzenie sieci konwergentnych. Integracja tych sieci umożliwia przesyłanie danych w trybie pakietowym, jak i w trybie komutacji kanałów czasowych.

Najczęściej połączenie sieci IP z siecią PSTN tworzy się przy wykorzystaniu konwerterów mediów tzw. Media Gateway. Są to urządzenia, które dokonują konwersji danych

przesyłanych pakietowo do postaci zdatnej do przesłania w sieci opartej na technice TDM (sieć z komutacją kanałów). Stosowanie takich połączeń jest bardzo korzystne przy połączeniu sieci opartej na technologii VoIP (Voice over IP) z siecią PSTN. Zwiększa to atrakcyjność sieci IP umożliwiając integrację w niej usług związanych z przesyłaniem danych, głosu i obrazu oraz obustronną komunikację z użytkownikami sieci PSTN. Przedstawione w opracowaniu protokoły omówione są pod kątem zastosowania do przesyłania danych multimedialnych w sieciach IP oraz pomiędzy sieciami IP i sieciami telefonicznymi (PSTN). W większości wypadków standardy te dają możliwość tworzenia takich połączeń w sieciach opartych na innych protokołach transportowych.

2. Technologie przesyłania głosu stosowane w sieciach IP

2.1. Standard H.323

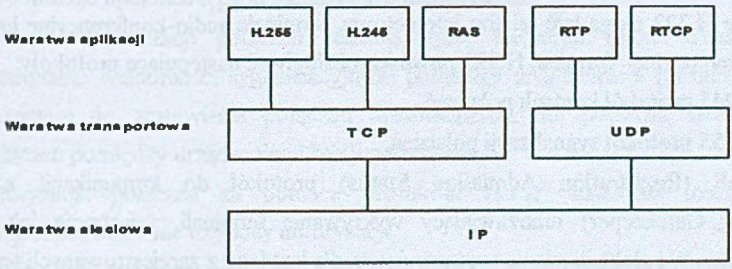
Aktualnie wielu producentów wyposażenia używa różnych standardów protokołów w sieciach VoIP, zaznacza się jednak tendencja do stosowania protokołu H.323 ITU-T.

Standard ten umożliwia przesyłanie danych wąskopasmowej telefonii oraz obrazów video w sieciach LAN i WAN (w tym w sieciach opartych na protokole IP). Określa urządzenia uczestniczące i kontrolujące połączenia multimedialne H.323 oraz urządzenia współpracujące z innymi sieciami np. siecią telefoniczną komutowaną (Switched Circuit Network).

Standard H.323 obejmuje całą rodzinę protokołów, na którą składają się m.in.:

- H.225 ITU-T - protokół definiujący zestaw wiadomości umożliwiający zestawianie połączeń medialnych (tzn. transmisja danych audio, video) w sieci, rejestrację i zezwalanie na połączenia. Wiadomości sygnalizacyjne stanowią podzbiór wiadomości określonych w protokole Q.931 dla sieci ISDN,
- H.245 ITU-T - protokół kontroli połączeń tworzy kanał połączeniowy pomiędzy elementami środowiska H.323, np. terminale, jednostka kontrolna MCU (ang. Multipoint Control Unit), nadzorca (ang. Gatekeeper); protokół ten umożliwia m. in. przesyłanie informacji dotyczących zdolności urządzeń do wzajemnej komunikacji (np. typ stosowanego kodeka wg zaleceń, G.723.1 ITU-T audio, G.728 ITU-T audio, czy CIF H.263 ITU-T video), rozwiązywanie sytuacji konfliktów przy dostępie terminali do tych samych zasobów, przesyłanie sygnalizacji DTMF,
- RTP IETF (Real Time Protocol) - protokół służący do transportu danych multimedialnych w sieci IP (dźwięku, video). Umożliwia tworzenie połączeń typu Multicast,
- RTCP IETF (Real Time Control Protocol) - protokół kontrolujący połączenia RTP, zarządzający jakością połączeń.

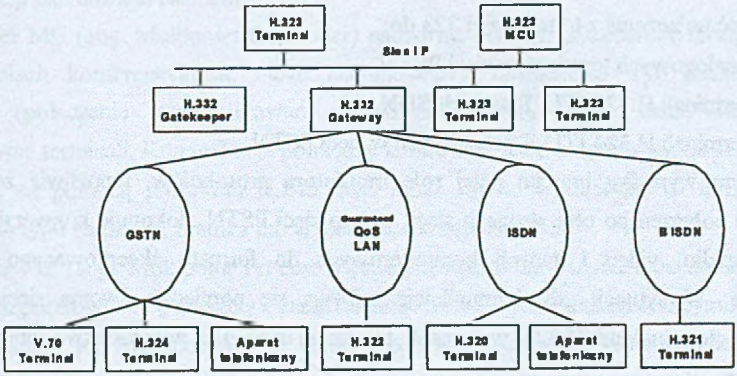
W warstwie transportowej sieci IP protokoły H.323 wykorzystują dwa rodzaje protokołów TCP (Transport Control Protocol) i UDP (User Datagram Protocol). Protokół TCP, zapewniający dużą wiarygodność transmisji pakietów i korekcję błędów, używany jest do przesyłania sygnalizacji i stanowi warstwę transportową dla protokołów H.225 i H.245. Protokół UDP tworzący proste i szybkie usługi połączeniowe z minimalnym narzutem nagłówka protokołu służy do transportu protokołów RTP przenoszącego dane multimedialne i protokołu RTCP. Zgodnie z przedstawionym na rys. 1 modelem warstwowym protokoły H.323 umiejscowione są w warstwie aplikacji w stosie protokołów sieci IP.



Rys.1. Protokoły warstwy aplikacji
Fig. 1. Application layer protocols

2.1.1. Elementy składowe systemu H.323

Przedstawiona na rys. 2 architektura systemu H.323 składa się z kilku komponentów tworzących środowisko systemu; niektóre z tych komponentów mogą występować opcjonalnie.



Rys. 2. Środowisko H.323
Fig. 2. H.323 Environment

W zaleceniu H.323 określone zostały następujące elementy: terminale H.323, bramka (ang. Gateway), nadzorca (ang. Gatekeeper), jednostka kontrolna MCU (ang. Multipoint Control Unit) oraz kontroler MC (ang. Multipoint Controller), procesor MP (ang. Multipoint Procesor).

Terminal H.323 jest urządzeniem, które umożliwia komunikację w czasie rzeczywistym z innymi terminalami H.323, bramką lub jednostką kontrolną MCU. Komunikacja obejmuje przesyłanie informacji audio, video oraz sygnalizacji i informacji sterujących. Terminal H.323 może być w zależności od aplikacji terminalem przesyłającym dane typu voice (dźwięk), voice i video, lub voice video oraz dane komputerowe. Przykładowymi terminalami pracującymi w standardzie H.323 mogą być telefon internetowy, terminale audio-konferencyjne lub aplikacje video-konferencyjne. Terminal H.323 powinien obsługiwać następujące protokoły:

- H.245 protokół kontroli połączeń,
- H.255 protokół sygnalizacji połączeń,
- RAS (Registration Admission Status) protokół do komunikacji z nadzorcą (ang. Gatekeeper) umożliwiający wykrywanie terminali, rejestracje ich w strefie nadzorcy i alokacji pasma transmisyjnego dla każdego z zarejestrowanych terminali,
- RTP/RTCP transmisja pakietów z danymi audio i video,

oraz opcjonalnie może spełniać funkcje kodowania video, obsługi protokołu T.120 ITU-T dla połączeń konferencyjnych, lub spełniać funkcję jednostki MCU i bramki.

Bramka jest opcjonalnym elementem w systemie H.323; pełni rolę urządzenia pośredniczącego w komunikacji pomiędzy terminalami H.323 i innymi typami terminali określonymi w zaleceniach ITU-T znajdującymi się w różnych sieciach typu LAN, WAN, PSTN (Public Switching Telphone Network) itp. (rys. 2). Bramka jest niezbędna, gdy chcemy realizować połączenia z terminala H.323 do:

- analogowych terminali w sieci PSTN,
- terminali H.320 ITU-T w sieci ISDN,
- terminali H.324 ITU-T pracujących w sieci PSTN.

W tym wypadku bramka pełni rolę translatora protokołów, umożliwia zestawianie i zrywanie połączeń po obu stronach sieci, w tym sieci PSTN, dokonuje konwersji strumienia danych audio, video i danych komputerowych do formatu akceptowanego przez sieć docelową. W sytuacji gdy komunikacja odbywa się pomiędzy dwoma sieciami IP lub pomiędzy terminalami H.323 w ramach tej samej sieci IP, pośrednictwo bramki nie jest konieczne.

Nadzorca jest również elementem opcjonalnym w strukturze H.323 służącym do kontroli połączeń pomiędzy elementami systemu H.323. W sieci może równocześnie pracować kilka

nadzorców, którzy mogą się komunikować z pozostałymi elementami systemu, terminalami, jednostkami MCU i z innymi nadzorcami. Nadzorca spełnia w systemie takie funkcje, jak:

- translacja adresów, np. dokonuje translacji numerów telefonicznych na adresy IP,
- kontrola dostępu, polega na autoryzacji dostępu do sieci przy użyciu protokołu H.255,
- kontrola pasma, odbiera polecenia żądania, potwierdzenia i zwolnienia dodatkowego pasma wysyłane przez terminale,
- zarządzanie strefami, rejestruje wszystkie urządzenia pracujące w strefie działania nadzorcy i podlegające jego kontroli.

Dodatkowe funkcje opcjonalne, jakie może, pełnić nadzorca, to:

- kontrola sygnalizacji połączeń telefonicznych; nadzorca może uczestniczyć w przesyłaniu wiadomości sygnalizacyjnych pomiędzy urządzeniami (terminal, bramka) służącymi do zestawiania połączeń telefonicznych, lub pozwolić na zestawianie połączeń pomiędzy urządzeniami bez jego udziału,
- autoryzacja połączeń za pomocą protokołu H.255; nadzorca może odrzucić połączenia, które nie uzyskały autoryzacji,
- zarządzanie pasmem; nadzorca kontroluje liczbę terminali H.323, które mają jednoczesny dostęp do sieci. Używając sygnalizacji H.255 może nie zezwolić na połączenia terminalom w wypadku zbyt dużej liczby istniejących połączeń. Funkcja zarządzania pasmem jest realizowana również w czasie aktywnych połączeń, gdy terminale wysyłają żądanie o przydzielenie dodatkowego pasma,
- zarządzanie połączeniami, utrzymanie listy aktywnych połączeń H.323, określa w ten sposób zajętość poszczególnych terminali. Informacja ta jest również użyteczna dla funkcji zarządzania pasmem.

Kontroler MC (ang. Multipoint Controller) nadzoruje urządzenia końcowe biorące udział w połączeniach konferencyjnych, może negocjować z terminalami tryb realizowanego połączenia (połączenie scentralizowane lub zdecentralizowane) oraz właściwości komunikacyjne terminali. Komunikacja pomiędzy kontrolerem MC a urządzeniami końcowymi odbywa się za pomocą protokołu H.245. MC może być umiejscowiony w terminalu, w urządzeniach typu nadzorca, bramka lub w jednostce kontrolnej MCU.

Procesor MP (ang. Multipoint Procesor) przesyła strumienie danych typu audio, video i danych komputerowych pomiędzy urządzeniami końcowymi uczestniczącymi w sesji (scentralizowane lub hybrydowej). MP może przetwarzać jeden lub kilka strumieni danych dokonując ich miksowania, przełączania pomiędzy poszczególnymi urządzeniami, a nawet konwersji sposobu kodowania danych lub prędkości bitowych.

Jednostka kontrolna MCU (ang. Multipoint Control Unit) obsługuje połączenia konferencyjne pomiędzy trzema lub więcej urządzeniami końcowymi. Zgodnie z zaleceniem

H.323 MCU składa się z kontrolerów MC i opcjonalnie z procesorów MP. Zwykle MCU realizuje połączenia multikonferencyjne scentralizowane, gdzie kontroler MC spełnia funkcje kontroli połączeń, a procesor MP przetwarzania strumieni danych. Jednostka kontrolna MCU może również uczestniczyć w realizacji połączeń zdecentralizowanych za pomocą kontrolera MC tylko w zakresie kontroli połączeń (protokół H.245).

Połączenia scentralizowane polegają na komunikowaniu się urządzeń końcowych z kontrolerami MC będącymi częścią MCU poprzez kanał kontrolny (H.245) oraz przesyłaniu danych audio-video do procesorów MP. MC pełni funkcje kontrolne dla połączeń konferencyjnych, a MP umożliwia przełączanie i miksowanie danych.

W połączeniach zdecentralizowanych urządzenia końcowe przejmują rolę przetwarzania strumienia danych i przesyłania ich w trybie multicast, natomiast kontrola połączeń odbywa się tak jak w poprzednim przypadku za pośrednictwem kontrolera MC.

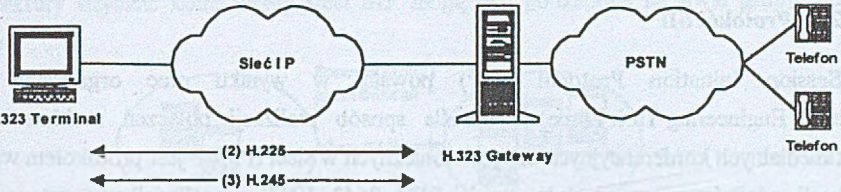
Istnieją również połączenia hybrydowe tzw. mieszane ze scentralizowane połączeniami tylko dla danych typu audio lub video.

2.1.2. Realizacja połączeń w środowisku H.323

W praktyce możliwe jest wiele scenariuszy zestawiania połączeń w środowisku H.323. Zależy to od zastosowanej konfiguracji systemu. Jako przykład podane zostaną dwa typowe sposoby realizacji połączeń przy użyciu nadzorcy oraz połączenia bez udziału nadzorcy.

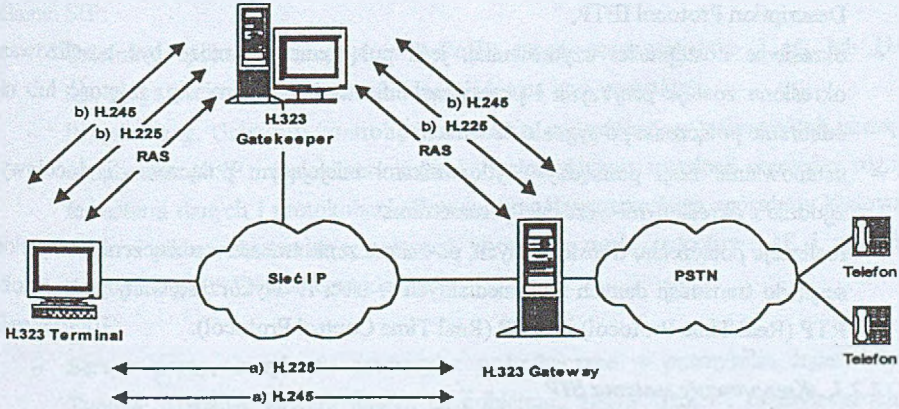
Zestawianie połączeń H.323 bez udziału nadzorcy przedstawia rys. 3. W przedstawionym przykładzie połączenie jest realizowane pomiędzy terminalem H.323 znajdującym się w sieci IP a aparatem telefonicznym analogowym w sieci PSTN. Połączenie to ustanawiane jest pomiędzy terminalem H.323 a bramką pośredniczącą pomiędzy siecią IP i PSTN.

Po wybraniu przez terminal H.323 określonego numeru abonenta w sieci PSTN oprogramowanie terminala dokonuje jego translacji na numer IP i rozpoczyna procedurę zestawiania połączenia (protokół H.255) do bramki. Bramka dokonuje translacji numerów IP, na numer abonenta w sieci PSTN. Następnie ustanawiany jest kanał kontrolny H.245 pomiędzy terminalem i bramką w celu wymiany informacji o kompatybilności zastosowanego sposobu kodowania. Bramka rozpoczyna wymianę sygnalizacji z urządzeniem znajdującym się po stronie sieci PSTN (centrala, PBX) i zestawia do niego połączenie. Po zakończeniu procedury zestawiania połączenia zostaje ustanowiony logiczny kanał kontrolny H.245.



Rys. 3. Zestawianie połączenia bez udziału nadzorcy w środowisku H.323
Fig. 3. H.323 Call setup without Gatekeeper

Analogiczne połączenie może być realizowane za pośrednictwem nadzorcy, co przedstawia rys. 4. Terminal H.323 rejestruje się w strefie działania nadzorcy przy użyciu protokołu RAS. Po pomyślnej rejestracji i otrzymaniu potwierdzenia ze strony nadzorcy może być przeprowadzona dalsza część procedury. Przesyłanie wiadomości sygnalizacyjnych H.255 oraz poleceń H.245 pomiędzy terminalem a bramką może być realizowane z udziałem nadzorcy lub bezpośrednio pomiędzy urządzeniami końcowymi. Jeżeli sygnalizacja jest przesyłana przez nadzorcę, kanał sygnalizacyjny może być otwarty w trakcie połączenia i przeznaczony do realizacji dodatkowych usług, np. przekierowanie połączeń. Końcowym etapem ustanawiania połączenia jest potwierdzenie dotyczące zgodności pracy urządzeń końcowych (protokół H.245).



Rys. 4. Zestawianie połączenia z udziałem nadzorcy w środowisku H.323: a) sygnalizacja przesyłana bezpośrednio, b) sygnalizacja przesyłana za pośrednictwem nadzorcy
Fig. 4. H.323 Call setup with Gatekeeper: a) signalling routed directly, b) signalling routed through Gatekeeper

2.2. Protokół SIP

Session Initiation Protocol (SIP) powstał w wyniku prac organizacji IETF (Internet Engineering Task Force) i określa sposób realizacji połączeń multimedialnych, multimedialnych konferencyjnych oraz telefonicznych w sieci IP. SIP jest protokołem warstwy aplikacji zdefiniowanym w dokumencie RFC 2543 IETF umożliwiającym ustanawianie, utrzymywanie i zakończenie połączeń pomiędzy dwoma lub więcej uczestnikami.

Protokół SIP realizuje funkcje przesyłania sygnalizacji i zarządzania połączeniami w sieci pakietowej. Protokół ten umożliwia też obsługę użytkowników ruchomych dzięki połączeniom typu proxy i przekierowywaniu połączeń do miejsca lokalizacji użytkownika (użytkownik ma możliwość rejestracji w systemie własnego położenia). Protokół SIP został zaprojektowany jako zupełnie niezależny od protokołów transportowych niższych warstw i może być rozszerzany o nowe właściwości.

SIP określa kilka faz w zestawianiu i rozłączaniu sesji multimedialnych:

- lokalizacja użytkownika końcowego SIP umożliwia określanie adresów, mapowanie nazw i przekierowywanie połączeń,
- określenie parametrów połączenia (kompatybilność terminali), jakie może realizować użytkownik końcowy; w tym celu wykorzystywany jest protokół SDP Session Description Protocol IETF,
- określenie dostępności użytkownika, jeśli połączenie nie może być zrealizowane; określona zostaje przyczyna i przesyłana informacja zwrotna, np. zajętość lub nieodebranie połączenia po sygnale dzwonienia,
- ustanowienie sesji pomiędzy użytkownikami inicjującym połączenie i docelowym zgodnie z określonymi wcześniej parametrami,
- realizacja połączenia, transfer danych, po zakończeniu transferu rozłączenie wszystkich sesji; do transmisji danych multimedialnych w sieci IP wykorzystywany jest protokół RTP (Real Time Protocol) i RTCP (Real Time Control Protocol).

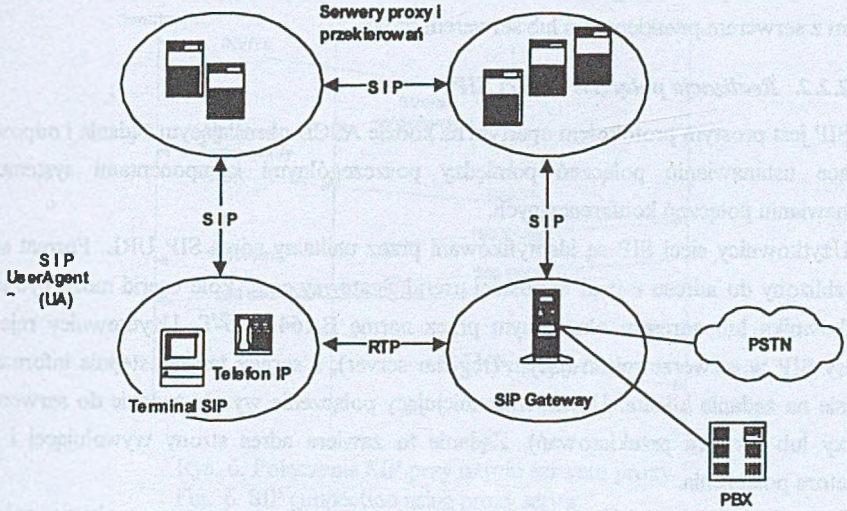
2.2.1. Komponenty systemu SIP

SIP jest rodzajem protokołu peer-to-peer realizującym połączenia pomiędzy tzw. User Agents. User Agent może funkcjonować jako:

- User agent client (UAC) - aplikacja klienta inicjująca połączenie SIP.
- User agent server (UAS) - aplikacja serwera łącząca się z użytkownikiem po zainicjowaniu przez niego połączenia i zwracająca odpowiedź, akceptująca, odrzucająca lub przekierowująca połączenie.

Zwykle elementy systemu SIP w czasie jednej sesji połączeniowej mogą funkcjonować jako UAC lub UAS, co zależy od agenta inicjującego połączenie. Z punktu widzenia

architektury fizyczne komponenty sieci SIP mogą być podzielone na dwie grupy: klient i serwer.



Rys. 5. Architektura SIP
Fig. 5. SIP Architecture

Klienci SIP:

- Telefony, aplikacje komputerowe VoIP, mogą pracować jako UAS lub UAC, tzn. mogą inicjować połączenie i odpowiadać na inne wywołania.
- Bramka (ang. Gateway) kontroluje połączenia, pośredniczy w połączeniach pomiędzy urządzeniami SIP i innymi terminalami. Spełnia funkcje translacji pomiędzy różnymi formatami danych i protokołami. Bramka umożliwia translację sposobów kodowania audio i video, zestawianie połączeń pomiędzy siecią pakietową IP i np. siecią telefoniczną (PSTN) lub centralą PBX.

Serwery SIP:

- Serwer proxy, urządzenie mediacyjne pośredniczące w przesyłaniu żądań klienta. Typowe działanie serwera polega na odbieraniu żądań klienta i przesyłaniu ich do innego serwera SIP. Serwer proxy może także dokonywać autentykacji, autoryzacji, kontroli dostępu do sieci.
- Serwer przekierowań (redirects server) dostarcza klientowi informacji o tym, jak ma być kierowane połączenie w sieci, aby połączyć się z klientem końcowym lub serwerem.

Serwer rejestrujący (registar server) przetwarza żądania wysyłane z aplikacji klienta UAC w celu rejestracji aktualnego położenia klienta. Serwer rejestrujący jest często umiejscowiony razem z serwerem przekierowań lub serwerem proxy.

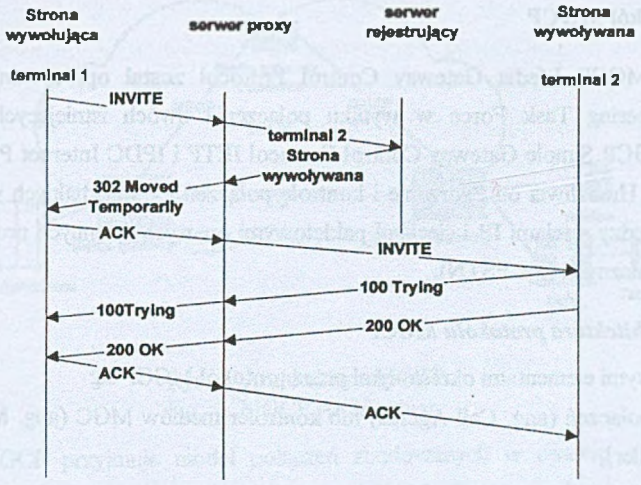
2.2.2. Realizacja połączeń w sieci SIP

SIP jest prostym protokołem opartym na kodzie ASCII określającym żądania i odpowiedzi służące ustanawianiu połączeń pomiędzy poszczególnymi komponentami systemu lub ustanawianiu połączeń konferencyjnych.

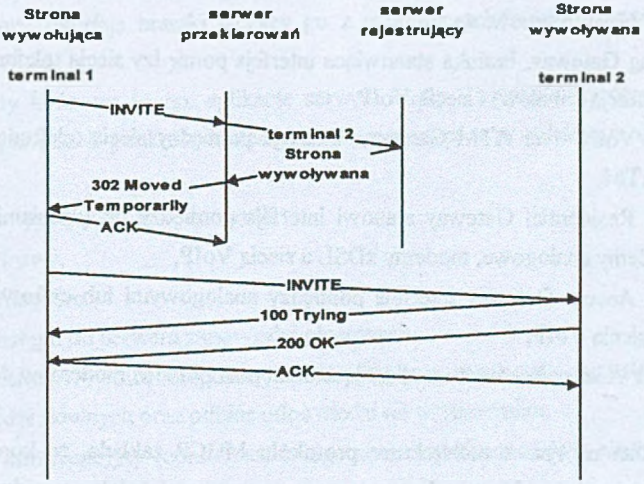
Użytkownicy sieci SIP są identyfikowani przez unikalny adres SIP URL. Format adresu jest zbliżony do adresu e-mail w postaci userid@gateway.com. Pole userid może być nazwą użytkownika lub adresem określonym przez normę E.164 ITU-T. Użytkownicy rejestrują adresy SIP w serwerze rejestrującym (registar server), a serwer ten udostępnia informacje o adresie na żądanie klienta. Użytkownik inicjujący połączenie wysyła żądanie do serwera SIP (proxy lub serwera przekierowań). Żądanie to zawiera adres strony wywołującej i adres inicjatora połączenia.

Połączenia SIP w trybie proxy przestawia rys. 6. Serwer proxy przyjmuje polecenie INVITE zawierające adres strony wywoływanej i wywołującej, następnie łączy się z serwerem rejestrującym (registar server) w celu precyzyjnego określenia lokalizacji strony wywoływanej (terminal 2). Serwer proxy zwraca do terminala 1 kod odpowiedź 302 Moved Temporarily (oznacza to konieczność nawiązania połączenia pod wskazanym w odpowiedzi adresem) i przesyła polecenie INVITE pod wskazany przez serwer rejestrujący adres. Strona wywoływana zwraca do serwera odpowiedź 100 Trying (ozn. próba nawiązania połączenia) i następnie 200 ok (ozn. pomyślne nawiązanie połączenia), a serwer proxy przesyła je do terminala 1. Na zakończenie przesłane zostają potwierdzenia otrzymania odpowiedzi ACK.

Połączenia SIP w trybie przekierowania przedstawia rys. 7. Strona wywołująca przesyła polecenie INVITE do serwera przekierowań (redirects server), następnie określony zostaje dokładny adres strony wywoływanej za pomocą serwera rejestrującego. Informacja o tym adresie przekazana zostaje przez serwer przekierowań do strony wywołującej. Strona wywołująca rozpoczyna połączenie bezpośrednio ze stroną wywoływaną.



Rys. 6. Połączenie SIP przy użyciu serwera proxy
Fig. 6. SIP connection using proxy server



Rys. 7. Połączenie SIP przy użyciu serwera przekierowań
Fig. 7. SIP connection using redirect server

2.3. Protokół MGCP

Protokół MGCP Media Gateway Control Protocol został opracowany przez IETF Internet Engineering Task Force w wyniku połączenia dwóch istniejących do tej pory protokołów SGCP Simple Gateway Control Protocol IETF i IPDC Internet Protocol Device Control IETF. Umożliwia on tworzenie i kontrolę połączeń multimedialnych w sieci IP oraz połączeń pomiędzy sieciami IP i sieciami pakietowymi opartych na innych protokołach, jak i sieciami telefonicznymi (np. PSTN).

2.3.1. Architektura protokołu MGCP

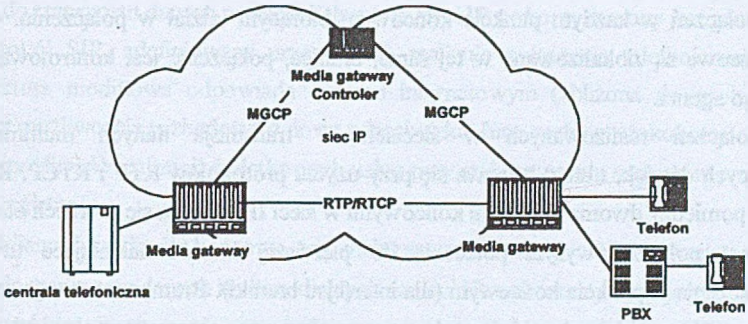
Podstawowymi elementami określonymi przez protokół MGCP są:

- agent połączeń (ang. Call Agents) lub kontroler mediów MGC (ang. Media Gateway Controller),
- bramka (ang. Gateway).

MGCP jest protokołem służącym do komunikacji pomiędzy elementami kontrolnymi zwanymi kontrolerami MGC lub agentami połączeń a bramką. Bramka jest elementem sieciowym, który jest odpowiedzialny za realizacje połączeń i wymianę informacji pomiędzy sieciami transmisyjnymi różnych typów, np.:

- Trunking Gateway, bramka stanowiąca interfejs pomiędzy siecią telefoniczną cyfrową (z komutacją kanałów) i siecią VoIP,
- bramka Voice over ATM Gateway, interfejs pomiędzy siecią telefoniczną cyfrową a siecią ATM,
- bramka Residential Gateway stanowi interfejs pomiędzy urządzeniami analogowymi np. modemy analogowe, modemy xDSL a siecią VoIP,
- bramka Access Gateway interfejs pomiędzy analogowymi lub cyfrowymi centralami PBX a siecią VoIP,
- Network Access Servers umożliwiające dostęp za pomocą modemów do sieci Internet itp.

Przedstawiona na rys. 8 architektura protokołu MGCP zakłada, że kontrola połączeń realizowanych przez bramki jest realizowana poza nim przez niezależne urządzenia kontrolne, tzn. agentów połączeń lub kontrolery MGC. MGCP jest protokołem typu master/slave, gdzie bramka wykonuje polecenia otrzymywane od agentów połączeń oraz wysyła potwierdzenia wykonania poleceń.



Rys. 8. Architektura MGCP
Fig. 8. MGCP Architecture

Protokół MGCP przyjmuje model połączeń zbudowanych w oparciu o tzw. punkty końcowe (ang. endpoints) i połączenia (ang. connections). Punkty końcowe są to, inaczej mówiąc, „źródła danych" i można wśród nich wyróżnić punkty końcowe fizyczne lub wirtualne. Przykładem fizycznych punktów końcowych są:

- Interfejs bramki łączący go z siecią PSTN (centralą telefoniczną),
- Analogowy Interfejs bramki łączący go z aparatem telefonicznym analogowym lub centralą PBX.

Wirtualne punkty końcowe to np. aplikacje serwera audio. Bramka w ogólnym przypadku składa się z wielu takich punktów końcowych różnych typów w zależności od wymaganej funkcjonalności.

Podstawowe typy punktów końcowych to:

- kanał cyfrowy,
- łącze analogowe,
- punkt dostępu do serwera zapowiedzi głosowych,
- IVR interactive voice response umożliwiający generowanie sygnałów tonowych, zapowiedzi słownych oraz odbiór odpowiedzi od użytkownika,
- mostek konferencyjny (conference bridge acess point) umożliwia realizację połączeń konferencyjnych,
- pakietowy np. IP, ATM,
- wiretap - połączenie z serwerem umożliwiającym nagrywanie i odtwarzanie połączeń.

Połączenia (ang. connections) mogą być typu punkt-punkt lub wielopunktowymi (np. połączenia konferencyjne). Połączenie punkt-punkt zachodzi pomiędzy dwoma punktami końcowymi i umożliwia transmisję danych pomiędzy nimi. W tym wypadku punkty końcowe mogą należeć do tej samej lub mieścić się w różnych bramkach. Połączenia są tworzone przez

agentów połączeń w każdym punkcie końcowym biorącym udział w połączeniu. Gdy oba punkty końcowe są zlokalizowane w tej samej bramce, połączenie jest kontrolowane przez tego samego agenta.

Dla połączeń realizowanych w sieciach IP transmisja danych multimedialnych (przenoszących dźwięk, obraz) odbywa się przy użyciu protokołów RTP i RTCP. Realizacja połączenia pomiędzy dwoma punktami końcowymi w sieci IP odbywa się w trzech etapach.

- Agent połączeń wysyła polecenie do pierwszej bramki nakazujące utworzenie połączenia w punkcie końcowym (dla interfejsu bramki). Bramka rezerwuje zasoby dla tego połączenia i odpowiada poleceniem opisującym parametry połączenia (session description zawierającym np. adres IP port UDP).
- Agent wysyła polecenie utworzenia połączenia do drugiej bramki. W poleceniu tym zawarte są parametry połączenia otrzymane wcześniej. Bramka rezerwuje zasoby i przesyła własne parametry połączenia.
- Agent połączeń przekazuje otrzymane parametry do pierwszej bramki, po czym połączenie może być zrealizowane.

3. Podsumowanie

Technologia VoIP jest jedną z najnowszych, jaka rozwinęła się w ostatnich latach. Szybka ekspansja sieci IP (Internet), jej otwarta architektura, rozwój nowych usług (np. e-commerce), a często względy ekonomiczne powodują, że telefonia IP staje się coraz bardziej popularna. Przedstawione w opracowaniu protokoły H.323, SIP, MGCP są najczęściej stosowanymi standardami przez producentów oprogramowania i sprzętu sieciowego. Oprócz nich istnieją jeszcze inne protokoły wprowadzane niezależnie przez producentów sprzętu sieciowego.

Protokół H.323 ITU-T, jako opracowany wcześniej, zyskał duże poparcie ze strony producentów. Reprezentuje architekturę zbliżoną do tradycyjnych sieci telefonicznych, połączenia realizowane są w oparciu o protokół sygnalizacyjny sieci ISDN Q.931 (Integrated Service Digital Network). Do transportu sygnalizacji w sieci IP wykorzystywany jest protokół TCP, co powoduje, że czas zestawiania połączeń jest dłuższy niż np. sieci SIP wykorzystującej protokół UDP. Problem ten został zniwelowany w zaproponowanej kolejnej trzeciej wersji protokołu H.323 v3, gdzie do przesyłania sygnalizacji dopuszcza się protokół UDP.

Protokół ten cechuje ponadto:

- możliwość realizacji dodatkowych usług telefonicznych przy wykorzystaniu nadzorcy,
- klienci H.323 (urządzenia końcowe, terminale) są urządzeniami inteligentnymi posiadającymi dużą funkcjonalność, obsługującymi wiele protokołów,

– do transportu danych multimedialnych w sieci IP wykorzystywany jest protokół RTP.

Protokół SIP, zdefiniowany przez IETF, realizuje połączenia telefoniczne w sieci IP. Architektura modułowa odpowiada sieciom internetowym (zbliżona do protokołu HTTP IETF), z możliwością rozbudowy o nowe właściwości. Inne cechy protokołu to:

– możliwość realizacji dodatkowych usług przy wykorzystaniu serwerów proxy, redirect, registar,
– klienci (urządzenia końcowe, terminale) są urządzeniami inteligentnymi,
– do transportu danych multimedialnych w sieci IP wykorzystywany jest protokół RTP,
– szybkie zestawianie połączeń przy wykorzystaniu protokołu UDP lub innego protokołu.

Protokół MGCP umożliwia kontrolę bramek VoIP za pomocą zewnętrznych urządzeń kontrolnych. Architektura protokołu typu master/slave, MGCP jest wewnętrznym protokołem działającym pomiędzy elementami rozproszonymi, agentami połączeń, kontrolerami MGC i bramkami. Do transportu danych multimedialnych w sieci IP używany jest, tak jak w poprzednich przypadkach, protokół RTP.

LITERATURA

1. „Deploying H.323 Applications in Cisco Networks" White paper Sam Kotha,1998 Cisco Sytems, Inc.
2. ITU-T Recommendation H.323 „Packet-based multimedia communications systems" ITU-T Study Group 16 (1997-2000).
3. RFC 2705 „Media Gateway Control Protocol (MGCP) Version 1.0" IETF Internet Engineering Task Force October 1999.
4. RFC 2705 „Media Gateway Control Protocol Architecture and Requirements" IETF Internet Engineering Task Force April 2000.
5. RFC 2543 „SIP: Session Initiation Protocol" IETF Internet EngineeringTask Force March 1999.

Recenzent: Dr inż. Bartłomiej Zieliński

Wpłynęło do Redakcji 30 marca 2001 r.

Abstract

The article describes Internet Protocol (IP) telephony as one of the most important technologies in the telecommunications. This article provides detailed description of three commonly used standard communication protocol in voice over IP network. There are H.323 ITU-T, Session Initiation Protocol (SIP) IETF and Media Gateway Control Protocol (MGCP) IETF. This document describes architecture, functional components and gives examples of voice over IP connection setup in each of these standards.

H.323 protocols are the ITU-T multimedia communication standard for packet–switched networks. Main architecture of this standard is shown at fig 1. It consists many components, which allow to setup H.323 voice session in IP network, interact with switched circuit network and establish multipoint conference connections.

Session Initiation Protocol (SIP) defined by IETF Internet Engineering Task Force allow to setup, maintain, and release voice connection in IP network. The main components shown at fig 5 are: SIP clients (terminal, gateway), proxy severs, redirect server, registar server.

MGCP IETF is protocol for controlling Voice over IP (VoIP) Gateways from external call control elements (Call Agents or Media Gateway Controller). MGCP assumes a call control architecture where the call control „intelligence" is outside the gateways and handled by external call control elements.