SIP, to protokół tekstowy, warstwy aplikacji. Komunikaty SIP są wysyłane za pośrednictwem TCP lub UDP. Używany jest do ustanowienia, utrzymywania i zrywania sesji multimedialnych. W systemie SIP mamy do czynienia z dwoma komponentami:

1. agenci użytkowników (aplikacje systemu końcowego klienta)

* UAC (ang. User – Agent Client),
* UAS (ang. User – Agent Server, UAS )

1. serwery sieciowe

* Serwer Proxy SIP – może równolegle próbować adresów, aż do pomyślnego nawiązania połączenia.
* Serwer przekierowań – serwer przekazuje pełną listę lokalizacji i pozwala klientowi zlokalizować użytkownika bezpośrednio;

Komunikaty tymczasowe:

* informacyjne; 100 – próbowanie (ang. Trying) 180 – dzwonienie (ang. Ringing)
* pomyślne: 200 – OK. 305 – użyj proxy
* błąd klienta: 400 – błędne żądanie 484 – niepełny adres
* błąd serwera 502 – błędna brama 503 – usługa niedostępna
* ogólne awarie: 600 – wszystko zajęte 606 – brak akceptacji

Ocena jakości usług przesyłania danych **QoS** (ang. Quality of Service) jest niezwykle ważna dla skuteczności VoIP. Zwyczajowo akustyczną jakość połączeń mierzy się za pomocą skali **MOS** (ang. Mean Opinion Score). QoS określa się często wszystkie środki, jakie są stosowane w celu polepszenia funkcjonowania głosu w sieciach. Dwa kluczowe standardy, to:

* **RSVP** (ang. Resource Reservation Protocol) jest zalecanym protokołem sygnalizacji dla **IntServ** (jest zaleceniem dla dostarczonego, przypisanego pasma dla kanałów multimedialnych w sieci IP. Wszystkie routery, czy na brzegu, czy w sieci podstawowej, odgrywają aktywną rolę w procesie decydowania o polityce przyznawania pasma.) Ten standard jest dobrym wyborem dla sieci z ograniczonym pasmem podstawowym. Protokół dodaje warstwę sygnalizowania wstępnego do sieci IP. Zadaniem protokołu jest zapewnienie wystarczającego pasma przepustowości, zanim dane multimedialne zostaną przesłane przez kanał.
* **MPLS** (ang. Multipoint Label Switching) jest najbardziej zaawansowanym środkiem QoS dostępnym w dużych sieciach VoIP. MPLS wykorzystuje się w sieciach transportowych i bardzo dużych sieciach korporacyjnych. Etykiety MPLS mają za zadanie zidentyfikować ścieżki i priorytety związane z każdym pakietem. Ścieżki odnoszą się do kanału multimedialnego połączenia VoIP, a priorytety odpowiadają poziomowi usługi QoS wynegocjowanemu dla tych kanałów.

**Opóźnienie VoIP – to czas jaki jest potrzebny na wymówienie słów i dotarcie ich do uszu słuchacza**. W sieci telefonicznej mamy do czynienia z trzema rodzajami opóźnień. Badania wykazały, że opóźnienie do 150 ms jest niezauważalne, a powyżej 150 ms znacznie utrudniają komunikację. Opóźnienia powyżej 300 ms są nieakceptowane.

Rodzaje opóźnień:

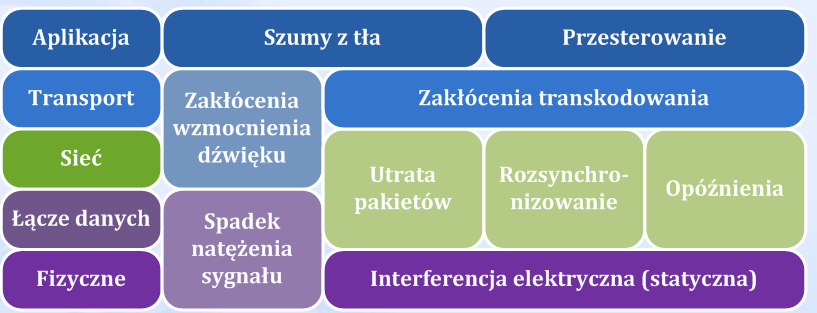
* opóźnienie propagacji - prędkość światła
* opóźnienie obsługi - próbki co 10 ms
* opóżnieni kolejkowania - kolejki pakietów

**Strata pakietów** jest niezwykle szkodliwa dla połączeń w sieci VoIP. Ich główną przyczyną jest przeciążenie sieci. Może ona prowadzić do rozsynchronizowania.

**Rozsynchronizowanie** jest to brak synchronizacji w czasie transmisji pakietów. Powoduje, że pakiety przychodzą nie po kolei, pozostawiając luki w sekwencji ramkowania sygnału głosowego. Brak synchronizacji w pojawia się, gdy pakiety głosowe muszą przejść przez kilka routerów w sieci. Im więcej routerów tym rozsynchronizowanie może być większe.

**Jitter, to różnica pomiędzy czasem w jakim pakiet jest oczekiwany a czasem rzeczywistego nadejścia pakietu.**

W sieci telefonicznej **echo** jest zwykle powodowane błędem impedancji na przejściu z sieci czteroprzewodowej na dwuprzewodową. **Echo** w standardowej sieci PSTN jest regulowane za pomocą tłumików echa i kontroli błędów impedancji. **Rodzaje szumów**: addytywne - niepożądane sygnały które są przy transmisji dźwięku, subtraktywne - przerwy lub zmniejszenia transmijsi dźwięku



Systemy **CoS** (ang. Class of Service) nadają priorytety przepływowi danych na pojedynczym kanale transmisji danych. CoS odnosi się jedynie do pojedynczego kanału. Celem CoS jest dostarczenie priorytetowych pakietów danych, zgodnie z zachowaniem ustalonym przez administratora. Rozwiązania takie sprawdzają się w takich kanałach, gdzie pakiety głosowe stanowią mniej niż 30% ruchu sieciowego. Dwa standardy obsługujące CoS, to:

* **802.1p/ToS**. wykorzystuje 3-bitową część nagłówka pakietu ethernetowego. Określa ona zachowanie się pakietu na **lokalnym łączu danych**. Metoda ta polega na nadaniu priorytetu, określeniu rodzaju usługi (ang. Traffic of Service, **ToS**). Metoda ta nazywana jest również **priorytetem IP**. Zaleca się zdefiniować klasę 5 dla ruchu akustycznego.
* **DiffServ** jest używany do obsługi routowanych sieci WAN. Używa on, podobnie jak 802.1p tagów ToS. Kiedy pakiet dociera do węzła brzegowego sieci, to nadawany jest mu priorytet, zgodnie z ustawioną przez administratora „polityką”. Ważne jest to, aby wszystkie „przeskoki” utrzymały priorytet pakietu, nadany przez router brzegowy. Routery podstawowe nie zmieniają kolejności czy priorytetów pakietów. Jedynie przesyłają je, podporządkowując się „polityce nadawania priorytetów” na brzegu sieci.

Bezpieczeństwo w sieciach IP oznacza wymuszenie ustalonej polityki bezpieczeństwa: rejestrowanie przypadków nadużyć dla celów sądowych, kodowanie lub inne zabezpieczanie tajnych informacji w czasie transportu, wspieranie odporności systemów na ataki i wirusy komputerowe, zabezpieczanie granic dostępu do sieci VoIP.

* Stare routery i switche mogą nie obsługiwać ustanowionych polityk zapenienia QoS;
* Administrator powinien uzyskać poparcie ustanowionych polityk zapewnienia QoS wszystkich podległych oddziałów;
* Jeśli przepływ danych w sieci stanowi 70% całego ruchu, w stosunku do pakiet audio, korzystaj z technik nadawania priorytetów, takich jak **DiffServ** czy **802.1p**;
* Jeśli sieć jest obciążona, należy wykorzystać **DiffServ**;
* Jeśli sieć jest wyjątkowo przeciążona lub bardzo duża (tysiące węzłów audio), należy wykorzystać **RSVP**.
* Odmowa dostępu: Ataki DoS które zmniejszają lub naruszają funkcjonalność systemu oprogramowania poprzez przekroczenie buforu czy przepustowości lub przez wykorzystanie błędu w zabezpieczeniu. Z zasady ataki DoS zwalcza się za pomocą kontroli dostępu.
* Interferencja człowieka: To grupa ataków pozwalających osobom trzecim na monitorowanie, zapisywanie, bloków, czy nawet wprowadzanie zmian w transmisji danych. Wiąże się to zwykle z przechwytywaniem pakietów na łączu danych. Zabezpiecza przed nimi szyfrowanie i wymóg autoryzacji.
* Trojany: Autonomiczne procesy zaprojektowane dla przemieszczania się po Internecie i sieciach IP infekujące hosty a następnie podlegające replikacji. Zabezpiecza przed nimi specjalne oprogramowanie antywirusowe i typu spyware.

SNMP jest łatwą metodą gromadzenia danych o ruchu i aktywności urządzeń sieciowych, takich jak serwery i switche. Różne rodzaje danych korzystają z różnych schematów parametrów, zwanych bazami informacji zarządzania MIB (ang.Management Information Bases).

Poprawne używanie standardów:

* W ustawieniach protokołu DiffServ należy nadać głosowemu ruchowi IP klasę EF;
* W ustawieniach 802.1p należy nadawać priorytet 5;
* Warto używać kodek G.711, tak często, jak to możliwe;
* Należy unikać transkodowania – jeśli jest to absolutnie konieczne warto używać kodeków GSM;
* Należy używać łączy o dużych prędkościach – warto zrezygnować zupełnie z wolnych łączy
* Nie jest zalecane uruchamianie sesji VoIP na VPN;
* Warto używać cyfrowych obwodów lub kanałów logicznych IP dla połączeń z firmą telefoniczną;