# VoIP

**Voice over Internet Protocol**, tiež nazývané **VoIP**, **IP Telefónia**, **Internetová telefónia**, je prenos komunikácie uskutočňovanej ľudským hlasom cez Internet alebo inú sieť založenú na protokole IP.

Protokoly, ktoré sa používajú na prenos hlasových signálov cez IP sieť sa zvyknú označovať ako **VoIP** protokoly. Dá sa na ne pozerať ako komerčnú realizáciu experimentálneho protokolu Network Voice Protocol (1973) navrhnutého pre sieť ARPANET. Vďaka použitiu jedinej siete na prenos dát aj hlasu je možné dosiahnuť isté finančné úspory, najmä ak je k dispozícii nevyužitá sieťová kapacita, ktorá sa dá využiť pre VoIP bez pridaných nákladov. Volania VoIP - VoIP sú prevažne zdarma, zatiaľ čo volania do verejných telekomunikačných sietí (tak pevných i mobilných) bezplatné v zásade nie sú.

Dva najhlavnejšie súperiace štandardy pre VoIP sú Session Initiation Protocol (SIP), vyvinutý pod hlavičkou organizácie IETF, a štandard ITU s označením H.323. Na počiatku bol populárnejším H.323, čo je štandard vychádzajúci z telekomunikačného prostredia, v súčasnosti je už v popredí SIP, s ktorým sa ráta už aj v ústredniach typu IMS.

VoIP dokáže zabezpečiť úlohy, ktoré môžu byť omnoho zložitejšie dosiahnuteľné pri použití klasických telekomunikačných technológií:

- Prichádzajúce telefónne hovory môžu byť automaticky smerované na VoIP telefón, nezávisle na tom, kde sa nachádzate.
- Vo viacerých krajinách (USA, Veľká Británia, atď.) sú k dispozícii bezplatne použiteľné telefónne čísla pre použitie vo VoIP.
- Pracovníci call centier môžu pri použití VoIP pracovať z ľubovoľného miesta, kde je k dispozícii dostatočne stabilné internetové pripojenie.
- Mnohé VoIP balíky služieb obsahujú funkcie verejných sietí, ktoré sú bežne spoplatňované osobitne, prípadne sú miestnym operátorom osobitne spoplatňované, ako napríklad konferenčné hovory, presmerovanie hovoru, automatické opakovanie vytáčania a pod.
- VoIP telefóny dokážu spájať viacero služieb dostupných cez Internet vrátane videokonferencií, prenosu dát popri hovore, správy telefónnych a adresových zoznamov a oznamovania online dostupnosti zvolených komunikačných partnerov.

## Problémy pri nasadení

**Fax**- ťažkosti pri odosielaní faxových správ kvôli softvérovým a sieťovým obmedzeniam vo väčšine domácich systémov. Existuje však snaha zadefinovať alternatívne riešenie prenosu faxov cez IP, menovite protokol T.38.

**Pripojenie k Internetu** - závislosť na ďalšej samostatnej službe - internetovom pripojení. Kvalita a celková spoľahlivosť telefonického spojenia cez VoIP je celkom závislá od kvality, spoľahlivosti a rýchlosti použitého internetového pripojenia. Mnohí používatelia VoIP stále prevádzkujú aj tradičné analógové telefónne linky, ktoré umožňujú volať na núdzové čísla, ako aj bez problémov používať tradičné faxové prístroje.

**Problémy s implementáciou** -Vzhľadom k tomu, že UDP neposkytuje mechanizmus, ktorý by zabezpečil, že dátové pakety budú doručené v správnom poradí, alebo poskytol garanciu kvality služby (Quality of Service), nasadenie VoIP čelí problémom s latenciou (oneskorením) a jitterom (kolísaním oneskorenia). Ďalšou starosťou je smerovanie prevádzky cez firewally a preklad adries. Zariadenia nazvané Session Border Controller sa používajú popri firewalloch na zabezpečenie VoIP hovorov do a z chránenej podnikovej siete. Skype využíva proprietárny protokol umožňujúci smerovať hovory cez iné uzly v sieti Skype, čím sa prekonáva symetrický NAT a firewally. Štandardné riešenia využívajú protokoly ako STUN a ICE.

**Nezáujem domácich používateľov -** VoIP nevyžaduje nutne širokopásmové pripojenie do Internetu + telefónnej služby

**Spoľahlivosť a kvalita služby** – výpadky hlasu, kvalita porovnateľná s GSM, spomalenie hlasu

**Núdzové volania** - Povaha protokolu IP prakticky znemožňuje presné geografické zameranie používateľov. Núdzové hovory preto nemôžu byť jednoducho presmerované na najbližšie operačné stredisko záchranného systému.

**Konkurencia mobilných telefónov**

**Bezpečnosť** - šifrovanie

**Zobrazenie čísla účastníka** – ano aj nie

**Integrácia do celosvetového číslovacieho systému** - Tradičné telefónne siete využívajú na identifikáciu účastníkov telefónne čísla podľa štandardu E.164. Používatelia VoIP sú identifikované primárne pomocou URI (napríklad v tvare *sip:jozef@firma.com*). Aby bolo možné smerovanie hovorov medzi klasickými a VoIP sieťami, existujú určité technológie na preklad telefónnych čísel a URI. Najrozšírenejšou technológiou je ENUM, čo je služba založená na DNS (základná služba Internetu na preklad doménových mien počítačov a IP adries. V databáze ENUM je pre telefónne číslo zapísaný jeden alebo viac kontaktov, na ktorých je účastník daného čísla dosiahnuteľný (môžu byť aj na rôznych technológiách, ako SIP, H.323, či dokonca klasický e-mail).

**Nasadenie na spotrebiteľskom trhu** – výhodná cena hovoru na veľké vzdialenosti

**Využitie u telekomunikačných operátorov** – z hľadiska konvergencie sietí, NGN (IP)

**Právne problémy** – zatiaľ nie je právne podchytená

**Výpadky elektriny**

# H.323

Štandard H.323 (rodina protokolov H.323) bol v prvej verzii uvedený medzinárodnou telekomunikačnou štandardizačnou organizáciou ITU-T v roku 1996. Označenie dodržuje konvenciu ITU-T - veľké písmeno, nasledované bodkou a číslom.

Prvé písmeno označuje oblasť činnosti, ktorej sa štandard týka (napr. G - prenosové systémy, médiá, digitálne systémy a siete, I - ISDN, V - dátové prenosy cez telefónnu sieť, H - audiovizuálne a multimediálne systémy).

Slovne je štandard (odporúčanie) H.323 nazvaný Packet-based multimedia communications systems (multimediálne komunikačné systémy na paketovom základe), teda zahŕňa multimediálne prenosy cez paketové siete bez všeobecnej garancie QoS. Prvá verzia tohto odporúčania bola zameraná predovšetkým na videokonferencie, ďalšie verzie sú už viac prispôsobené pre VoIP. Štandard H.323 patrí ku skupine odporučení H.32x, ktoré sa týkajú multimediálnej komunikácie cez rôzne druhy sietí:

- H.324 - cez klasickú telefónnu sieť s prepínaním okruhov
- H.320 - cez ISDN
- H.321 a H.310 - cez širokopásmové ISDN (B-ISDN)
- H.322 - cez LAN siete s garanciou QoS

Ako štandard vychádzajúci z telekomunikačného prostredia (na rozdiel od SIP-u, ktorý bol inšpirovaný klasickým internetovým prostredím dátových prenosov) je H.323 relatívne komplikovaný a zahŕňa prevažnú väčšinu aspektov multimediálnej komunikácie (signalizácia, transport multimediálnych dát, kodeky, prenos všeobecných dát). Nezahŕňa samotnú lokálnu sieť ani transportnú vrstvu použitú na prepojenie s inými sieťami, s výnimkou rozhrania do okruhovo prepínanej telefónnej siete. Signalizácia v protokolovej rodine H.323 vychádza z telekomunikačného prostredia. H.323 obsahuje časti:

- H.225.0-RAS
- Q.931-H.245
- RTP-RTCP
- audio (G.711, G.723, G.729, atd.), video (H.261, H.263) a dátové kodeky (T.120).

Hovor je prenášaný na RTP/RTCP protokolom. RTP prenáša konkrétny hovor a RTCP prenáša stavové a riadiace informácie. Signalizácia, s výnimkou RAS, je prenášaná spoľahlivo cez TCP. Nasledujúce protokoly sa zaoberajú signalizácie:

- RAS –riadi registráciu, prístup a stav
- Q.931 -riadi nastavenie volania a jeho ukončenia
- H.245 -určí využitie kanálu a jeho kapacitu

Nasledujúce protokoly zaisťujú voliteľné prostriedky v rámci H.323:

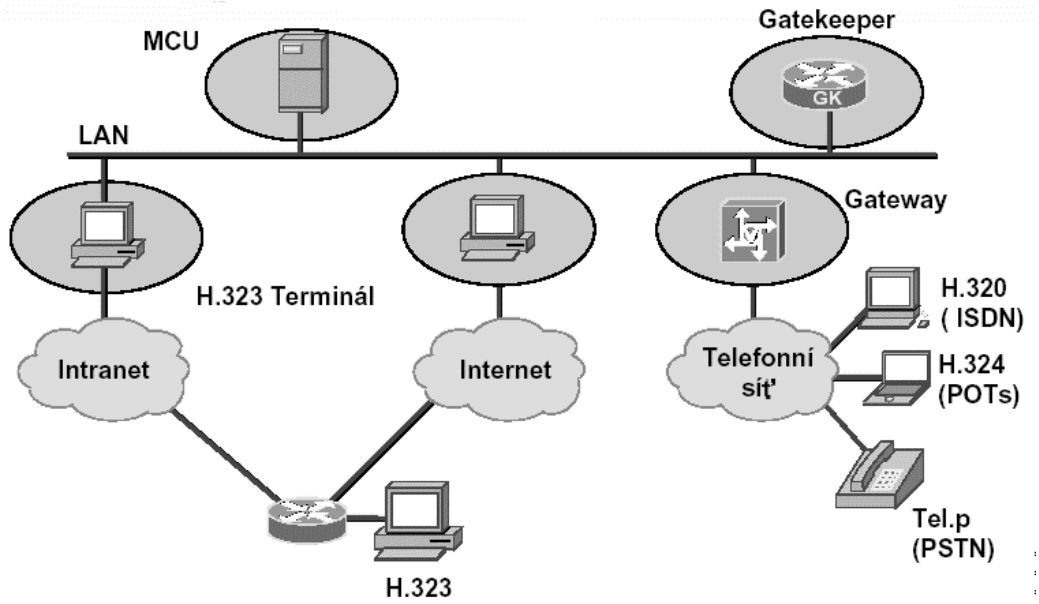
- H.235 -zabezpečenie a identifikácie
- H.450 -doplnkové služby

V prípade H.323 sú signalizačné informácie k hovoru dané odporúčaním H.225.0, ktoré využíva oba protokoly UDP i TCP, štandardne riadiaci prvok siete (Gatekeeper) naslúcha

signalizácii H.225.0/RAS na porte UDP 1719 a prípadne aj na 1718 (pre multicast 224.0.1.41), hovorová signalizácia spojenia H.225.0/Q.931 sa prenáša na porte TCP 1720. Okrem toto tu je ďalšia časť signalizácie podľa ITU-T H.245 na dojednanie parametrov audia/videa, ktorá je postavená na TCP, od verzie H.323v2 je pomocí metódy *Fast Connect* schopná väčšinu informácií preniesť v H.225.0/Q.931.

## Stavebné prvky H.323 a ich vlastnosti

Na Obr. 1 sú zobrazené komponenty H.323. Prvky siete H.323 tvoria koncové body EP (endpoints) a riadiace prvky (gatekeepers). Množina EP registrovaná k rovnakému GK tvoria tzv. *zónu*, ktorú môžeme chápať ako logickú oblasť spravovanú GK, v jednej zóne nemôže byť viacero GK. Existuje spôsob zálohovania GK, kde viacero GK sa môže postarať o EP, avšak niektoré EP sú prihlásené vždy v danej chvíli len k jednému GK. Zálohovanie je uskutočnené na princípe preregistrácie EP a opakovania smerovacích tabuliek, ktoré viacero GK medzi sebou zdieľa. Napríklad budeme mať dva identické GK, jeden v bode A, druhý v bode B, EP geograficky ležiace v oblasti bodu A budú prihlásené na GK v bode A, zvyšné budú registrované na GK v bode B. Oba GK si medzi sebou synchronizujú smerovacie informácie (susedné GK a hlasové brány k výstupu z H.323 siete). V prípade vypnutia GK v bode A, pošle tento GK všetkým EP v jeho zóne požiadavku na preregistrovanie do GK v bode B, pokiaľ by došlo k nekorektnému vypnutiu a GK by už nemal možnosť komunikovať s EP, tak aj tento prípad je ošetrený, keďže už pri prvej registrácií EP na GK, je predaný zoznam s alternatívnymi GK zoradenými podľa priority, pre prípad výpadku. Keďže registrácia EP na GK platí obmedzenú dobu, je zaistené, že mŕtva zóna vždy nakoniec skonverguje do inej, pokiaľ však má kam.




**Obr. 1** Komponenty v H.323

H.323 infraštruktúra je logicky rozdelená do zón. Zóna je množina zariadení riadených jedným GK. V H.323 rozpoznávame nasledujúce komponenty:

- *Endpoin*t (koncový bod, zariadenie), tým môže byť MCU, brána GW alebo terminál TE
- *Gatekeeper* (riadiaci prvok siete)

*MCU (Multipoint Control Unit)* je multikonferenčná jednotka, ktorá má za úlohu podporovať konferencie medzi 3 alebo viacerými koncovými body, ide spravidla o najdrahšiu časť siete, aj keď nepovinnou, podstatnou výhodou MCU pre audio je, že vie transkódovať, čiže prepojiť terminály i s rôznymi kodekmi. MCU obsahuje riadiacu jednotku MC (media controller) a procesorovou jednotku alebo audio mixér MP (media processor).

*GW (Gateway)* je brána zabezpečujúca prepojenie s telefónnou sieťou, obsahuje teda spravidla aj ISDN rozhranie (prípadne iné) a DSP procesory na podporu viacerých kodekov, podľa výkonu, kapacity, typu rozhrania a podporovaných kodekov sa odvíja aj cena.

*TE (Terminal)* je typické koncové zariadenie, buď je realizované na báze SW pre Windows/Linux (softphone) alebo ako HW terminál (IP telefon), trh je pomerne dobre zásobený stovkami typov IP telefónov, cena pochopiteľne záleží na výkonu zariadení (implementované funkcie, podpora kodekov, NAT, 802.1Q, diffserv, napájania 803.af, miniswitch vo vnútri, apod..).

*Gatekeeper* je riadiacim prvkom H.323 koncových bodov (terminál, gateway, MCU). Podľa štandardu H.323 musí zaisťovať nasledujúce funkcie:

- podpora signalizácie RAS (Registration/Administration/Status). Pomocou signalizácie RAS sa realizuje riadenie prístupu k prostriedkom siete
- riadenie prístupu (Addission Control), zaisťuje autorizovaný prístup pomocou správ ARQ/ACF/ARJ (Admission Request/Confirm/Reject) definovaných v signalizácií RAS (Registration, Admissions and Status Signaling)
- preklad adries (Address Translation) medzi E.164 číslom a IP sieťovou adresou. Preklad na IP adresy koncových bodov z prijatých adries typu „alias“ (jmeno@domena) allebo „E.164“ (štandardné tel. č.)
- riadenie prideľovania kapacity pásma (Bandwidth Control). Riadenie pásma podľa požiadaviek z koncových bodov pomocí správ BRQ/BCF/BRJ signalizácia RAS
- riadenie spojení (Call Control), spracovanie správ alebo ich smerovanie
- riadenie zón (Zone Management), zaisťuje riadiace funkcie pre všetky registrované koncové body H.323 zóny. Koncové terminály a VoGW sú rozdelené do zón, ktoré predstavujú distribuovanú štruktúru GK.

GK ďalej obvykle podporujú autorizáciu volaní (Call authorization). Autorizácia jednotlivých volaní sa uskutočňuje podľa identifikačných kódov a umožňuje zaviesť hovorový kredit. GK môže zaisťovať *Least Cost routing*, optimalizáciu smerovaní cestou najnižších nákladov a možnosti nastavení záložného GK (standby GK).

# SIP

Na rozdiel od protokolovej rodiny H.323 zastrešuje jeho vývoj a uvádzanie do praxe organizácia IETF, aj preto je celá protokolová rodina SIP protokolu zložená z protokolov definovaných touto organizáciou. SIP nie je tak komplexným štandardom ako H.323, nešpecifikuje totiž klasické telekomunikačné služby, ale skôr len súbor primitív používaných pre uskutočňovanie komunikácie.

Špecifikácia SIP protokolu je dostupná vo forme niekoľkých doporučení RFC, najdôležitejší je RFC 3261, ktorý obsahuje jadro protokolu. Protokol je určený k zostaveniu, modifikácií a ukončeniu spojenia s jedným alebo viacerými účastníkmi. SIP nie jediný protokol, ktorý je potrebný pre komunikujúce zariadenie. V spojení so SIP protokolom sú najčastejšie používané ešte dva ďalšie protokoly, RTP a SDP. RTP protokol je používaný k prenosu multimédií v reálnom čase (real-time), tento protokol umožňuje prenášať hlas alebo video v paketoch pomocou IP. Ďalším dôležitým protokolom je SDP, ktorý je požívaný k popisu vlastností účastníkov spojenia. Tento popis je potom použitý k dojednaniu parametrov spojenia všetkých zariadení účastníkov (vyjednání kodeků transportního protokolu).

SIP bol navrhnutý v súlade s modelom Internetu. Ide teda o end-to-end orientovaný signalizačný protokol, čo znamená, že všetka logika je uložená v koncových zariadeniach (s výnimkou smerovania SIP správ), koncové zariadenie pozná aj jednotlivé stavy komunikácie, čím je zvýšená odolnosť komunikácie voči chybám. Cena, ktorá sa musí zaplatiť za decentralizáciu a dostupnosť služby, je vyššia réžia v hlavičkách správ (správy sú posielané end-to-end).

Nepochybne stojí za zmienku, že end-to-end koncept SIP protokolu je významná odlišnosť od klasického riešenia PSTN (Public Switched Telephone Network), kde logika je uložená v sieti a koncové zariadenia sú primitívne. Cieľ SIP protokolu je zaistiť rovnakú funkcionalitu akú majú klasické PSTN, ale end-to-end návrh umožní SIP sieťam vyššiu výkonnosť a otvorí možnosti implementácie nových služieb, ktoré môžu byť len ťažko nasadené v klasických PSTN.

Inšpiráciou pre formu protokolu SIP boli protokoly HTTP (Hypertext Transfer Protocol - základ súčasného World Wide Webu) a SMTP (Simple Mail Transfer Protocol - prenos elektronickej pošty). Jeho jednoduchosť je jednou z jeho výhod. Na rozdiel od binárne kódovaného H.323 je založený na správach vo forme čistého textu a je transportne nezávislý (môže byť použitý na prakticky ľubovoľnom transportnom protokole).

SIP entity sú identifikované použitím *SIP URI* (Uniform Resource Identifier). SIP URI má formát:

*sip:username@domain*

Ako je možné vidieť, SIP URI sa skladá z časti *username* a z časti *domain* , obe časti sú oddelené znakom @. SIP URI je podobná e-mailovej adrese, tzn. , že rovnaká adresa môže byť použitá pre e-mail i SIP, takže URI môže byť ľahko zapamätateľná.

## Prvky SIP

V najjednoduchšej konfigurácií je možné použiť dva UA (usser agents) posielajúce si navzájom SIP správy, typická SIP sieť bude obsahovať viac než jeden typ prvkov. Základnými SIP prvkami sú:

- user agents,
- proxies, registrars, and redirect servers.

Koncové body siete Internet, ktoré používajú SIP k vzájomnému spojeniu sú nazývané *user agents (UA)*. UA sú obvykle predstavované koncovými terminálmi vo forme HW SIP telefónu nebo aplikácie, SIP UA môžu byť aj mobilné telefóny, PSTN brány (GW), PDA, IVR systémy atd.

SIP umožňuje vytvoriť infraštruktúru siete hostiteľov nazývaných ako *proxy servers*. Koncové terminály UA môžu odosielať správy na proxy server. Proxy servery sú dôležité entity v SIP infraštruktúre, zaisťujú smerovanie žiadostí o spojení podľa aktuálneho umiestnenia adresáta, autentizáciu, účtovanie a mnoho ďalších dôležitých funkcií. Najdôležitejšou úlohou proxy serveru je smerovať žiadosti o zostavenie spojení "bližšie" k volanému. Pri inicializácií zostavenia spojenia bude obvykle prehľadávať radu proxy serverov, pokiaľ nenájde taký, ktorý pozná aktuálne umiestnenie volaného. Takže proxy bude presmerovávať žiadosť o spojení priamo k volanému a volaný akceptuje alebo odmietne žiadosť o spojenie. Poznáme dva základní typy SIP proxy serverov:

- *stateless (bezstavový)*
- *stateful (s informáciou o stavoch)*

Stateless servery sú pomerne jednoduché a iba preposielajú správy nezávisle na ich vzájomných väzbách. Správy sú väčšinou v poriadku z hľadiska súvislosti a významu v signalizácií, bezstavové proxy servery nevedia kontrolovať ich výmenu z hľadiska zmysluplnosti, takže môže výnimočne dochádzať k nekorektným stavom, ktoré musia byť ošetrené na úrovni koncového zariadenia. Bezstavové proxy servery sú jednoduché, ale rýchlejšie než proxy servery s informáciou o stavoch. Využitie nachádzajú napr. na zníženie záťaže, na jednoduché prekladanie správ a smerovania. Jedna z nevýhod bezstavových proxy serverov je, že nie sú schopné zachytiť opakovanie správ a prevádzkovať dokonalejšie smerovanie, napr. vetvenie alebo predanie.

Stateful Servery sú Proxy servery s informáciou o stavoch sú omnoho komplexnejšie. Po prijatí požiadavky, si server vytvorí záznam stavu a tento stav drží, pokiaľ nedôjde k ukončeniu transakcie. Niektoré transakcie, obzvlášť vytvorené správou INVITE, môžu trvať pomerne dlho (pokiaľ volaný nedvihne alebo sa neukončí volanie). Pretože proxy servery s informáciou o stavoch musí udržiavať stav po celú dobu danej transakcie, je ich výkon limitovaný. Schopnosť priradzovať SIP správy do transakcií dáva serveru niektoré zaujímavé vlastnosti, napríklad môže prevádzkovať vetvenie, na prijatie jednej správy, môže byť odoslaných viacero správ. Proxy server s informáciou o stavoch môže zachytiť opakovanie správ, pretože zo stavu transakcie vie, či bola rovnaká správa už prijatá (bezstavový proxy nemôže overovať, pretože nedrží stav). Môže prevádzkovať komplikovanejšie metódy objavenia užívateľa, napríklad možnosť skúsiť volať na telefón v zamestnaní a v prípade neohlásenia volania presmerovať na mobilní telefón. Bezstavová proxy to nemôže, pretože nemá informáciu, či bol dosiahnutý cieľ alebo nie. Väčšina SIP proxy serverov je s informáciou o stavoch, často poskytuje účtovanie, vetvenie, niektoré podporujú i NAT.

Na podporu služieb spojenia popisuje RFC 3261 pre SIP prtokol päť aspektov správy multimediálnych spojení:

- umiestnenie používateľa (User location) - určenie, s ktorým koncovým systémom sa komunikuje.
- dostupnosť používateľa (User availability) - určenie, či sa volaný účastník chce zúčastniť komunikácie alebo nie
- možnosti používateľa (User capabilities) - určene média a jeho parametrov, ktoré budú použité pri komunikácii
- zriadenie spojenia (Session setup) - "vyzváňanie", stanovenie parametrov spojenia na oboch jeho stranách
- správa spojenia (Session management) - zahŕňa prenos a ukončenie spojenia, zmenu parametrov spojenia a vyvolanie ďalších služieb

## SIP signalizácia

SIP je protokol typu klient-server. Klient nadväzuje spojenie so serverom. Jedno zariadenie môže pracovať súčasne ako klient aj server. Napríklad telefón pracuje ako klient pre odchádzajúce hovory a ako server pre prichádzajúce hovory. Hovor, ktorý môže byť hlasový alebo multimediálny, môže prebiehať medzi viacerými účastníkmi. Multimediálne dáta sú pri tom prenášané naraz pre všetkých účastníkov spojením typu multicast, spojením typu unicast od každého účastníka cez prepojovaciu bránu, spojením unicast medzi každou dvojicou účastníkov alebo kombináciou týchto dvoch metód.

Správy protokolu SIP sú dvojakého druhu:

- žiadosti
- odpovede.

Žiadostiam sa tiež hovorí metódy a sú nasledujúcich typov:

INVITE – žiadosť o nadviazanie spojenia alebo o zmenu parametrov existujúceho spojenia
BYE – žiadosť o ukončenie spojenia
ACK – žiadosť, ktorou klient potvrdzuje, že dostal odpoveď na žiadosť INVITE
REGISTER – žiadosť o registráciu klienta na registrar serveri
CANCEL – žiadosť o zrušenie prebiehajúcej žiadosti INVITE
OPTIONS – žiadosť o zaslanie podporovaných funkcií na serveri
INFO – prenos informácií behom hovoru

Odpovede na SIP metódy sú správy uvedené číselným kódom. Systém kódov je prevzatý z HTTP protokolu. Číselné kódy odpovedí sú členené do ž skupín:

• 1xx – informačné správy (napr. “100 Trying”, “180 Ringing”)
• 2xx – úspešné ukončenie žiadosti (“200 OK”)
• 3xx – presmerovanie, požiadavku je potrebné smerovať inde (“305 Use Proxy”)
• 4xx – chyba, požiadavka by sa nemala v rovnakej podobe opakovať (“403 Forbidden”)
• 5xx – chyba servera (“500 Server Internal Error”)
• 6xx – globálne zlyhanie (“606 Not Acceptable”)