

Matematički fakultet
Univerzitet u Beogradu



Seminarski rad iz Metodologije stručnog i naučnog rada

XMPP protokol

student:

Miloš Milaković
1063/2012

profesor:

Vladimir Filipović

Sadržaj

1	Uvod	2
2	Osnovni okvir XMPP-a	2
2.1	XMPP jezgro	2
2.2	Pregled bezbednosti	4
2.3	XMPP za servis za razmenu poruka i prisutnost	6
2.4	Softver	7
3	Proširenja	8
3.1	XEP-ovi	8
3.2	Proširenja interoperabilnosti	9
4	Zaključak	10

1 Uvod

Servis za slanje trenutnih poruka (en. instant messaging) je servis koji omogućava ljudima da komuniciraju jedni sa drugima u skoro realnom vremenu. On podržava različite stilove komunikacije kao što su unicast, multicast i mod za grupni razgovor. Priličan broj protokola i okvira (en. framework) koji podržavaju IM je napravljen do sada, na primer AIM, Yahoo Messenger i ICQ. Pored toga, protokol za pokretanje sesije (en. Session Instant Protocol, SIP), protokol za pokretanje sesije za trenutno slanje poruka i prisutnost (en. SIP for Instant Messaging and Presence Leveraging Extensions, SIMPLE) i IM proširenje koriste iste funkcionalnosti. Međutim, svaki od njih ima ozbiljne nedostatke. Komercijalni proizvodi su bazirani na vlasničkim protkolima koji blokiraju saradnju izmedju različitih implementacija i ograničavaju dalji razvoj. SIMPLE [1] [2] je veoma složen, jer je izgrađen na vrhu SIP arhitekture. Da bi se otklonili ovi problemi i olakšalo korišćenje IM-a pojavilo se novo rešenje.

Proširivi protokol za slanje poruka i prisutnost (en. eXtensible Messaging and Presence Protocol, XMPP) je standard za nošenje servisa IM koji je specifikovan od strane IETF (en. Internet Engineering Task Force). U pitanju je otvoreni XML protokol za slanje poruka u gotovo realnom vremenu, davanje informacija o prisutnosti i servis za primanje zahteva i za njihovo odgovaranje. XMPP je prvo predložila Jabber, zajednica otvorenog koda, a sada njegovim razvojem upravlja XSF (en. XMPP Standards Foundation). Tokom godina razvoja je formalno odobren i arhiviran od strane IETF u četiri Internet specifikacije [3] [4] [5] [6], a kasnije u još tri [12] [14] [13]. Zbog svojih dobrih karakteristika gorepomenuti problemi mogu biti lako rešeni korišćenjem XMPP protokola. Osim toga XSF radi na stalnom unapređenju ovog okvira.

2 Osnovni okvir XMPP-a

2.1 XMPP jezgro

Arhitektura XMPP-a se sastoji od tri elementa: XMPP klijenta, XMPP servera i kapija (en. gateways) ka stranim mrežama. XMPP server je odgovoran za upravljanje konekcijama i rutiranje poruka. Kapije služe kao mostovi izmedju različitih mreža i moraju da manipulišu sa najmanje dva protokola.

Osnovna veza između bilo koja dva XMPP elementa je TCP (en. Transmission Control Protocol). Prvo mora biti uspostavljena TCP konekcija za strimovanje XML-a. Jedna TCP veza može da nosi više veza koje su identifikovane po njihovim jedinstvenim adresama. Slično adresnoj šemi u SMTP (en. Simple Mail Transfer Protocol), identifikator za XMPP entitete, nazvan JID (Jabber ID) podseća na obrazac za e-mail adresu: user@example.com. Politika rutiranja aplikacionog nivoa je definisana na serverskoj strani, ali specifikacija [3] ostavlja detalje o procesu implementaciji. U XMPP-u ne postoji mogućnost otkrivanja rutiranja kao što je to navedeno u SIP okviru. U većini slučajeva direktni server-server tok (en. stream) između dva domena se usaglašava u početnoj fazi.

Tri osnovne primitive koje se nazivaju XML strofe (en. stanzas) su definisane u XMPP-u. Pored toga, postoji pet osnovnih atributa za strofe (kome, odKoga, id, tip, xml:lang). Tri ključne strofe su opisane ispod:

- poruka (en. message): izvodi se uz pomoć skladišti i gurni (en. store and push) mehanizma preko kojeg jedan entitet šalje informacije drugom. Na primer, razmena poruka između dve krajnje tačke.

```
<message 'alice@example.com  
to=bob@example.com />  
<body>Hello</body>  
</message>
```

- prisutnost (en. presence): to je emitovanje preko kojeg više entiteta dobijaju informacije o drugom entitetu na koji su prijavljeni, npr informacija može biti o dostupnosti entiteta.

```
<presence from=alice@example.com  
to=bob@example.com />
```

- iq: to je zahtev/odgovor mehanizam sličan HTTP-u (en. HyperText Transfer Protocol), koji omogućava entitetima da zahtevaju i dobijaju odgovore među sobom. Na primer prenos datoteka.

```
<iq type=get  
from=alice@example.com>  
<query xmlns=jabber:roster/>  
</iq>
```

Sve primitive XML strofa moraju se nalaziti u `<stream/>` bloku. To znači da ove strofe treba tretirati kao sadržaj XML toka. Sve greške na nivou toka se smatraju nepopravljivim i `<error/>` strofa sa opisom se šalje od strane detektora. Spisak stanja grešaka je definisan u specifikaciji [12]. Kao rezultat ovih karakteristika, XMPP ima pet pozitivnih mogućnosti:

1. Kutija sa porukama (en. message box): Poruke se skladište pre nego što budu prosledjene. XMPP implementacija može zadržati poruke radi kasnije isporuke ako je primalac nedostupan (en. offline).
2. Servis otkrivanja (en. service discovery): sa `<iq/>` strofom za upit, usluga otkrivanja je moguća. DNS SRV je podržan da pronadje mrežne servise.
3. Povezivanje resursa (en. resource binding): podaci o resursu su u dodati u adresi da bi se razlikovali različiti uređaji jednog korisnika. Nema potrebe za dodatnim protokolom koji bi rukovao ovim problemom.
4. Internacionalizacija: `<xml:lang>` zajednički atribut omogućava laku internacionalizaciju.
5. Pouzdana komunikacija: TCP veza za obavljanje sesije nudi garanciju isporuke, što se ne može postići sa UDP (en. User Datagram Protocol) prenosom.

Ipak, zbog toga što su formata lako čitljivog ljudima, XMPP poruke su veće od onih u binarnom formatu i to dovodi do zagušenja. Osim toga, u nekim slučajevima TCP veza može biti skupa, a UDP veza pravi manji saobraćaj i efikasnija je. To se može desiti u slučaju samo povremene komunikacije između dva čvora.

2.2 Pregled bezbednosti

Bezbednost komunikacije je takodje specificovana u jezgru XMPP [13]. Dva mehanizma su zadužena da obezbede poverljivost: integritet podataka i uzajamna autentikacija. Prvi protokol je TLS (en. Transport Layer Security) [7]. On kriptuje XML tokove da bi osigurao poverljivost i integritet podataka između dva entiteta. Drugi je SASL protokol (en. Simple Authentication and Security Layer) [8] koji može da obezbedi pouzdan mehanizam za potvrđivanje identiteta entiteta. Oba protokola moraju biti podržani za klijent-server i server-server komunikaciju.

XMPP koristi TLS da zaštiti kanal od ometanja i prisluškivanja. Klijenti bi trebali da koriste TLS da osiguraju tokove pre pokušaja završetka SASL pregovora. On se pokreće od strane STARTTLS proširenja i ima svoj prostor imena `"urn:ietf:params:xml:ns:xmpp-tls"`. SASL definiše uopšteni metod za dodavanje podrške za autentikaciju za protokole bazirane na konekcijama. I XMPP koristi generički prostor imena `"urn:ietf:params:xml:ns:xmpp-sasl"` za profilisanje SASL koji je u skladu sa zahtevima profilisanja. Podržani mehanizmi su objavljeni u `<mechanism/>` elementu. Opšta procedura uspešnog TLS+SASL pregovora je sledeća:

1. Klijent uspostavlja TCP vezu sa serverom i inicira XML tokove.
2. Server šalje STARTTLS proširenje klijentu, uključujući podržani mehanizam za autentikaciju.
3. Klijent odgovara na STARTTLS komandu.
4. Server obaveštava klijenta da je u redu da nastavi sa radom.
5. Klijent i server završavaju podešavanje TLS konekcije.
6. Uspešnim završetkom prethodnog koraka, klijent pokreće novi tok ka serveru.
7. Server odgovara slanjem glave toka (en. stream header) zajedno sa svim dostupnim funkcijama toka (SASL autentikacija).
8. Klijent uzima odgovarajući mehanizam za autentikaciju.
9. Server šalje Base64-šifrovan izazov klijentu.
10. Klijent odgovara na izazov sa akreditivima.
11. Server šalje još jedan izazov klijentu, kao sesija tokena.
12. Klijent ponovo odgovara na izazov.
13. Server obaveštava klijent o uspešnoj potvrdi identiteta.
14. Klijent inicira novi tok ka serveru za komunikaciju.

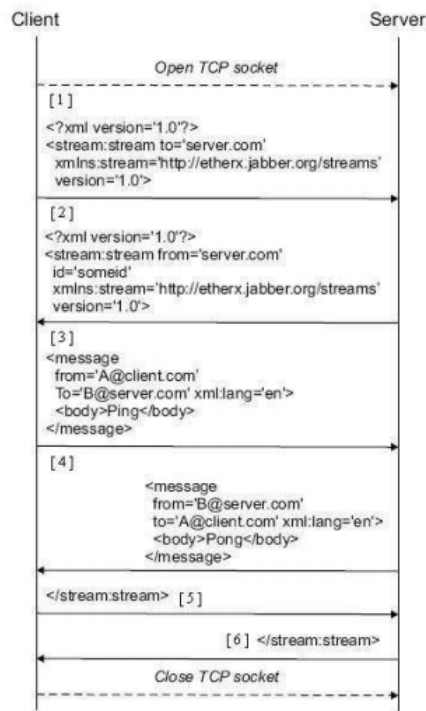


Figure 1: Komunikacija izmedju klijenta i servera

2.3 XMPP za servis za razmenu poruka i prisutnost

Kao što mu i samo ime kaže, primarna svrha XMPP/Jabber tehnologija su poruke u realnom vremenu i davanje informacija o prisutnosti. Da bi se opisali proširenja i mogućnosti jezgra XMPP-a razvijena je još jedna specifikacija [13] kao dopuna za osnovni dokument.

Slika broj 1 opisuje jednostavni proces komunikacije sa jedne strane izmedju klijenta A i servera. Skoro ista situacija je i sa druge strane. Prve dve poruke iniciraju XML tok. U ovom koraku, neki od ključnih parametara toka, kao npr. tag "id" i bezbednosni mehanizmi (TLS i SASL) treba da se dogovore izmedju dva entiteta. Zatim, prenos sadržaja može početi. Treća poruka se šalje od klijenta A na udaljeni čvor B koji je u "server.com" domenu. Jezik je postavljen na engleski ("english"). Četvrta poruka je odgovor od pozvane strane. Na kraju konverzacije klijent A prekida konekciju slanjem `/stream:stream` na server. Server potvrđuje akciju slanjem iste XML strofe

kako bi prekinuo XML tok. Na kraju se završava TCP konekcija.

U stvarnosti scenario opisan gore može biti dosta komplikovaniji. Postoji pet tipova poruka u XMPP-u: ćaskanje (en. chat, unicast), grupno ćaskanje (en. multichat, multicast), emitovanje (en. headline, broadcast), normalna poruka i greška. Svaka vrsta je napravljena da odgovara specifičnom okruženju. Pored toga XMPP IM definiše skup podređenih elemenata (naslov - subject, telo - body, nit - thread) za poruke u realnom vremenu.

Kod prisutnosti je definisano sedam tipova stanja koji opisuju informacije o prisutnosti. To su: nedostupan (en. unavailable), prijaviti se (en. subscribe), prijavljen (en. subscribed), odjaviti se (en. unsubscribed), ispitivanje i greška (en. error). Strofa o prisutnosti ima tri podređena elementa: prikaži, status i prioritet. Element prikaži opisuje četiri statusa (odsutan, dostupan, ne uznemiravaj i mirovanje). Status sadrži bilo koje reči koje je korisnik definisao za stanja, a koje će biti prikazane kontaktima iz liste kontakata. Servis o prisutnosti ima problem sa politikom privatnosti. Zbog toga neka podešavanja o prisutnosti treba prepustiti klijentskoj strani kako bi korisnici mogli sami da upravljaju podacima o prisutnosti.

Lista kontakata može biti skladištena i na klijentskoj i na serverskoj strani. Iako se povećava opterećenje na serveru kada se lista nalazi na njemu, preporučeno je da se baš čuva na serverskoj strani. Razlog za to je taj što lista kontakata može biti izgubljena ako se čuva lokalno npr. slučajnim brisanjem ili prekidom rada diska.

2.4 Softver

Prema XMPP arhitekturi prikazanoj na slici 2 trebala bi postojati tri vrste softvera: klijent, server i kapija. Prva dva formiraju osnovu XMPP mrežu. Oba softvera imaju različite verzije za različite operative sisteme (Windows, Linux i Macintosh) i različite uređaje.

XMPP klijent je bilo koji softver ili aplikacija koja omogućava konekciju na XMPP. Primeri klijentskih aplikacija su Agile Messenger, Candy, iChat, Jeti, Kopete, Miranda, Pidgin, Psi. Od 2005. godine kada je Google predstavio Google Talk, kombinaciju VoIP i IM sistema, ta aplikacija je koristila XMPP protokol, a od 2006. godine Talk je stupio u federaciju sa javnom Jabber mrežom. Ipak, Google je u maju 2013. godine najavio da će ukinuti kompatibilnost Google Talk-a sa XMPP protokolom. [17]

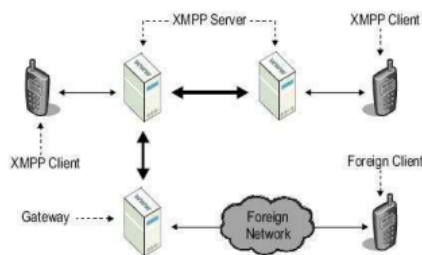


Figure 2: XMPP arhitektura

XMPP serveri obezbeđuju osnovne mogućnosti kao što su slanje i primanje poruka i informacija o prisutnosti i XML rutiranje. Primeri XMPP servera su CommuniGate Pro, Apache Vysper, iChat Server, Openfire, Jerry Messenger, Siemens OpenScope, Tigase, Wokkel. [18]

3 Proširenja

XMPP proširenja se sastoje od dve glavne grane. Prvi deo su XEP-ovi (en. XMPP Extension Protocols, ranije JEP-ovi) kojim upravlja XMPP Standards Foundation (XSF). Oni su najveći izvor XMPP proširenja i pruža značajnu podršku funkcionalnim poboljšanjima i generičkim standardima. Drugi izvor potiče od raznih istraživanja i implementacija, od kojih se najviše njih fokusira na interoperabilnost aplikacija baziranih na XMPP-u. Primer je IM servis baziran na XMPP-u a koji je izveden od SMS servisa (en. Short Message Service).

3.1 XEP-ovi

XSF razvija proširenja za XMPP kroz standardni proces baziran na JEP-ovima. Procesom upravlja JEP editor i uključuje intenzivnu diskusiju na mejling listi, formalna razmatranja i glasanja od strane Jabber saveta, kao i eventualno uključivanje seta odobrenih protokola. Spisak svih detalja svakog predloga je dostupan na Jabber-ovoj veb prezentaciji www.jabber.org.

Pored odbijenih i zastarelih XEP-ova, kao i onih koji su pod aktivnim razmatranjem, postoji i pet vrsta statusa za svako odobreno proširenje Jabber/XMPP protokola. Oni su navedeni ispod:

1. Konačna verzija - Definisani protokol se može smatrati stabilnim za implementaciju i primenu.
2. Nacrtna verzija - Definisani protokol se preporučuje kao odgovarajući za primenu u proizvodnji sistema, ali su moguće neke izmene pre nego što postane konačna verzija.
3. Eksperimentalna verzija - Nema odobrenih garancija za XEP. Korišćenje u proizvodnji sistema se ne preporučuje dok ne dobije status nacrtna verzije.
4. Predložena verzija - Ovaj XEP je trenutno u fazi poslednjeg razmatranja od strane Jabber saveta. Razmatra se da li treba da dobije naredni nivo u procesu JSF standardizacije.
5. Aktivna verzija - Definisani proces ili aktivnost je odobrena. Trenutno radi i radiće sve dok XEP ne zastari.

Zahvaljujući do sada napravljenim XEP-ovima mnoge nove funkcije i poboljšanja su dodane u programe zasnovane na XMPP-u. Neki od tih primera su lični avatar, transfer fajlova, interakcija između kapija, HTTP povezivanje, Jingle protokol za slanje glasa i videa kao i podrška za višekorisničko ćaskanje. Rezultat toga je da su XMPP aplikacije postale moćnije i popularnije.

3.2 Proširenja interoperabilnosti

Da bi se aplikacijama baziranim na XMPP-u omogućilo da rade sa drugim protokolima ili mrežama, proširenja moraju biti sposobna da koordinišu različitim protokolima i da ih povežu neprimetno. XMPP kapije kao komercijalnim protokolima kao što su MSN, Yahoo i AIM su takodje dostupne. Ovde je izložena kratka analiza XMPP baziranog IM servisa kombinovanog sa SMS servisom.

Slično ćaskanju u realnom vremenu, SMS je još jedan popularni servis za tekstualnu komunikaciju u realnom vremenu. Ali, za razliku od IM-a koji radi u mrežama baziranim na IP adresama, SMS servis radi u mobilnim mrežama poput GSM mreže. Danas postoji zajednički, jedinstveni i otvoreni

standard koji je dostupan. [11] Infrastruktura bazirana na XMPP-u može da poveže IM sisteme sa SMS sistemima.

Zahvaljujući arhitekturi prikazanoj na slici 2 XMPP klijent može vršiti konverzaciju sa spoljašnjim čvorom preko XMPP servera koji se povezuje na stranu mrežu uz pomoć kapija. U ovom dizajnu kapija se ponaša kao prevodilac i most. Osnovni protokol u SMS sistemima je SMPP (en. Short Message Peer-to-Peer). U pitanju je binarni format, različit od XML-a koji je čitljiv ljudima. Kapija mora da bude sposobna da obavi svoje dve glavne funkcije. Jedna je konverzacija između XML paketa i SMPP jedinica podataka, a druga je upravljanje sesijama.

Pored toga, trebalo bi da postoji način da se uvede red u isporuke. Na osnovu gornje analize predložen je dizajn kapije između IM sistema i SMS sistema. [11] Da bi zadovoljila drugi zahtev, upravljanje sesijama, modul sesija XMPP, kapija stvara pseudo XMPP server. Deluje da odgovarajući SMS korisnik vrši funkcije poput prijavljivanja na sistem, prenosa podataka itd.

Filozofija ovog dizajna može se primeniti na premošćavanje XMPP sistema i drugih mreža. Detalji zavise od atributa ne-XMPP protokola i interfejsa obezbeđenih od strane vlasnika protokola.

4 Zaključak

XMPP/Jabber tehnologija je postigla veliki uspeh, pogotovo od kada je IETF odobrio osnovne protokole. To je dovelo do značajnih implementacija i velikog napretka u razvoju. Nove opcije i mogućnosti su ugrađene u okvir, što je i dovelo do toga da taj protokol dnevno koristi više desetina miliona korisnika. Po mom mišljenju u pitanju je dobro napisan i poprilično dobro implementiran protokol.

References

- [1] Robert Sparks and Hisham Khartabil. SIP for Instant Messaging and Presence Leveraging Extensions (simple). At <http://www.ietf.org/html.charters/simple-char>

- [2] Simone Leggio. SIP for Instant Messaging and Presence Leveraging Extensions. At https://www.cs.helsinki.fi/u/kraatika/Courses/IPsem04s/SIMPLE_Leggio.pdf University of Helsinki, Department of Computer Science, 2004.
- [3] Peter Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Core. IETF RFC 3920, oktobar 2004.
- [4] Peter Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence. IETF RFC 3921, oktobar 2004.
- [5] Peter Saint-Andre. Mapping the Extensible Messaging and Presence Protocol (XMPP) to Common Presence and Instant Messaging (CPIM). IETF RFC 3922, oktobar 2004.
- [6] Peter Saint-Andre. End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP). IETF RFC 3923, oktobar 2004.
- [7] T. Dierks and C. Allen. The TLS Protocol Version 1.0. IETF RFC 2246, januar 1999.
- [8] J. Myers. Simple Authentication and Security Layer (SASL). IETF RFC 2222, oktobar 1997.
- [9] Jabber Community. Jabber Client At <http://jajc.ksn.ru/download.php?id=4>
- [10] JiveSoftware Organization. XMPP server wildre. At <http://www.jivesoftware.org/wildfire/>
- [11] Heng-Te Chu, Wen-Shiung Chen, Yi-Hung Huang and Jeng-Yueng Chen. A novel design of instant messaging service extended from short message service with XMPP. Fifth IEE International Conference on 3G Mobile Communication Technologies, 2004 Page(s):504- 508, IEEE Computer Society Press.
- [12] Peter Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Core. IETF RFC 6120, mart 2011. <http://tools.ietf.org/html/rfc6120>
- [13] Peter Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence. IETF RFC 6121, mart 2011. <http://tools.ietf.org/html/rfc6121>

- [14] Peter Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Address Format. IETF RFC 6122, mart 2011. <http://tools.ietf.org/html/rfc6122>
- [15] <http://xmpp.org/xmpp-software/clients/>
- [16] <http://xmpp.org/xmpp-software/servers/>
- [17] <http://www.h-online.com/open/news/item/Google-s-chat-client-drops-Jabber-compatibility-1866129.html>
- [18] <http://en.wikipedia.org/wiki/XMPP>