*XXV Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – **PosTel 2007**, Beograd, 11. i 12. decembar 2007.*

PROTOKOLI ZA SIGNALIZACIJU KVALITETA SERVISA U NOVOJ GENERACIJI TELEKOMUNIKACIONIH MREŽA

Mirjana Stojanović[1,2], Slavica Boštjančič[1]
[1]Institut Mihajlo Pupin, Beograd, [2]Saobraćajni fakultet, Beograd

Sadržaj: *U radu je prvo prikazana klasifikacija mehanizama za signalizaciju kvaliteta servisa u mrežama zasnovanim na tehnologiji Internet protokola (IP). Sledi pregled osnovnih karakteristika protokola za rezervaciju resursa (Resource Reservation Protocol, RSVP) koji je standardizovan za podršku IETF arhitektura IP kvaliteta servisa. Zatim je prikazan pregled aktivnosti na standardizaciji protokola za signalizaciju kvaliteta servisa u novoj generaciji telekomunikacionih mreža, koji obuhvata ITU-T preporuku za zahteve za signalizaciju IP kvaliteta servisa i IETF okvirni rad za protokole za signalizaciju (Next Steps In Signaling, NSIS). Posebna pažnja posvećena je zahtevima i rešenjima za heterogene scenarije signalizacije, podršku mobilnosti čvorova i zašttne mehanizme.*

Ključne reči: *Internet, Kvalitet servisa, Rezervacija resursa, Signalizacija, Zaštita*

1. Uvod

Arhitektura nove generacije telekomunikacionih mreža (*Next Generation Network*, NGN) podrazumeva koncepciju prenosa svih informacija i servisa preko zajedničke mreže zasnovane na tehnologiji Internet protokola (IP). Obezbeđivanje različitih nivoa kvaliteta servisa (*Quality of Service*, QoS) od jednog do drugog kraja veze je jedan od ključnih zahteva za implementaciju NGN.

QoS arhitektura diferenciranih servisa (*Differentiated Services*, DiffServ) [1] je praktično usvojena kao osnov za implementaciju QoS u okosnici IP-bazirane mreže. Osnovna ideja DiffServ modela je da zaglavlje IP paketa sadrži 64-bitno polje koje označava kôd klase servisa – DSCP (*DiffServ Code Point*). Na osnovu vrednosti DSCP vrši se klasifikacija paketa i identifikacija tzv. *per-hop behavior* (PHB) koji određuje način opsluživanja i prioritet odbacivanja paketa u svakom čvoru mreže. Periferni ruteri konfigurišu se za veliki broj politika kondicioniranja pojedinačnih tokova ulaznog saobraćaja, koje obuhvataju merenje, kao i pravila markiranja, uobličavanja i odbacivanja paketa. Ruteri jezgra konfigurišu se za izvršavanje brzih i jednostavnih operacija opsluživanja paketa i upravljanja redovima, sa malim brojem klasa saobraćaja.

U mrežama za pristup mogu biti implementirane druge QoS arhitekture kao što su: integrisani servisi (*Integrated Services*, IntServ) [2], servisi definisani za UMTS (*Universal Mobile Telecommunication System*) [3], generička specifikacija servisa (*Generic Service Specification*, GSS) [4] i dr.

Obezbeđivanje QoS od jednog do drugog kraja veze zahteva implementaciju dodatnih mehanizama i algoritama u kontrolnoj ravni (rutiranje, signalizacija), kao i upravljanje resursima mreže. Iz tih razloga su razvoj i testiranje inoviranih QoS arhitektura, zasnovanih na modelu DiffServ u okosnici i njegovoj interoperabilnosti sa drugim QoS modelima, predmet brojnih naučno-istraživačkih projekata [4], [5], [6]. Okvir za dalji razvoj QoS arhitektura standardizovan je ITU-T preporukom Y.1291 [7]. Pristup se zasniva na implementaciji QoS preko skupa mehanizama distribuiranih u tri logičke ravni: korisničkoj, kontrolnoj i upravljačkoj. Neki od mehanizama (opsluživanje paketa, upravljanje redovima) odnose se na pojedinačne elemente mreže, dok se mehanizmi kao što su signalizacija, rutiranje i politika upravljanja odnose na grupu elemenata ili celu mrežu.

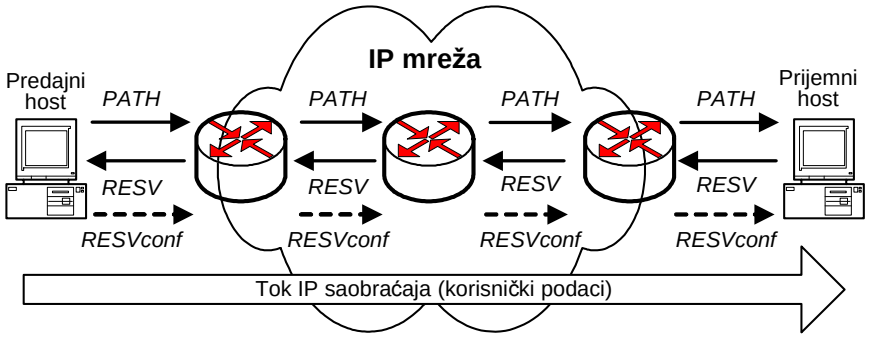
Predmet ovog rada je signalizacija kvaliteta servisa, a to je kontrolni mehanizam koji služi za ugovaranje QoS između provajdera i korisnika servisa [8], rezervaciju resursa mreže i određivanje putanja koje zadovoljavaju zahteve za QoS. U zavisnosti od toga da li je signalizaciona informacija pridružena korisničkom saobraćaju ili se prenosi posebnim protokolom, QoS signalizacija se može klasifikovati na signalizaciju u opsegu (*in-band*) i van opsega (*out-of-band*). QoS signalizacija u opsegu je tipično prisutna u odgovarajućem polju zaglavlja paketa, kao što je polje DSCP u arhitekturi DiffServ. Po svojoj prirodi, ovakav tip signalizacije nije pogodan za rezervaciju resursa ili QoS rutiranje, koji moraju da budu statički definisani pre faze prenosa korisničkih informacija. QoS signalizacija van opsega podrazumeva postojanje posebnog protokola, namenjenog za prenos signalizacionih informacija, što omogućava dinamičko rezervisanje resursa i QoS rutiranje. QoS signalizacija van opsega može da bude spregnuta sa putanjama kojima se prenose korisničke informacije (*path-coupled*) ili nezavisna od putanja korisničkih informacija (*path-decoupled*).

U radu su prvo prikazane osnovne karakteristike protokola za rezervaciju resursa (*Resource Reservation Protocol*, RSVP) koji je IETF prvobitno standardizovao za potrebe arhitekture IntServ, a zatim modifikovao i za DiffServ model. Inherentni nedostaci dizajna RSVP kao što su odsustvo podrške mobilnosti čvorova, odsustvo zaštitnih mehanizama i korišćenje nepouzdanog transportnog protokola, čine ovaj protokol nepodesnim za primenu u NGN. U radu je zatim prikazan pregled aktivnosti na standardizaciji protokola za signalizaciju IP kvaliteta servisa u NGN, koji obuhvata ITU-T preporuku za zahteve za signalizaciju IP QoS i IETF okvirni rad za protokole za signalizaciju u IP mrežama (*Next Steps In Signaling*, NSIS).

2. Protokol za rezervaciju resursa – RSVP

Protokol za rezervaciju resursa (RSVP) prvobitno je dizajniran za potrebe IntServ modela, odnosno rezervaciju resursa za pojedinačne tokove IP saobraćaja (RFC standard 2205 [9]). RSVP pripada klasi protokola koji su spregnuti sa putanjama korisničkih podataka, a projektovan je za podršku *multicast* rezervacija i komunikacije tipa *many-to-many*. Karakteriše se kontrolnim stanjima u ruterima koja nisu permanentna (*soft state*), odnosno koja će biti izbrisana ako nisu osvežena u definisanom intervalu

vremena. Na slici 1 su prikazane bazične operacije RSVP, koje se izvršavaju posredstvom kontrolnih poruka *PATH* i *RESV*.



Slika 1. *Osnovne operacije protokola za rezervaciju resursa (RSVP)*

Predajni host specificira karakteristike toka IP saobraćaja posredstvom poruke tipa *PATH*. Posle prijema poruke *PATH*, RSVP modul u svakom ruteru pamti adresu prethodnog RSVP rutera, kreira ili osvežava *path* stanje i prosleđuje poruku *PATH* prema prijemniku. Prijemni host odgovara porukom tipa *RESV*, kojom zahteva određeni tip i količinu resursa za dati tok IP saobraćaja. Svaki RSVP ruter koji primi poruku *RESV* kreira ili osvežava svoje stanje rezervacije (*resv*), a zatim prosleđuje poruku ka predajnom hostu. Poruke *RESV* opciono sadrže objekat koji označava zahtev za potvrdu rezervacije (*confirmation request*), koji uslovljava generisanje poruka tipa *RESVconf* od predajnog ka prijemnom hostu.

Originalna varijanta RSVP protokola modifikovana je za potrebe diferencijacije servisa po agregatnim tokovima saobraćaja (DiffServ). RFC standard 3175 [10] definiše pristup dinamičkom kreiranju RSVP rezervacija za agregate saobraćaja za IPv4 i IPv6 protokolske stekove, kao i principe klasifikacije saobraćaja na koji se primenjuju agregatne rezervacije i način određivanja propusnog opsega potrebnog za agregatni saobraćaj. Ovaj dokument takođe sadrži preporuke za algoritme i politike predikcije potrebnih resursa. RFC standard 3209 [11] specificira ekstenzije RSVP poruka i procedura protokola za potrebe distribucije labela i eksplicitno rutiranje saobraćaja u mreži sa multiprotokolskom komutacijom labela (*Multi-Protocol Label Switching*, MPLS). Pored toga, uveden je mehanizam koji omogućava detekciju ispada bilo kog susednog čvora.

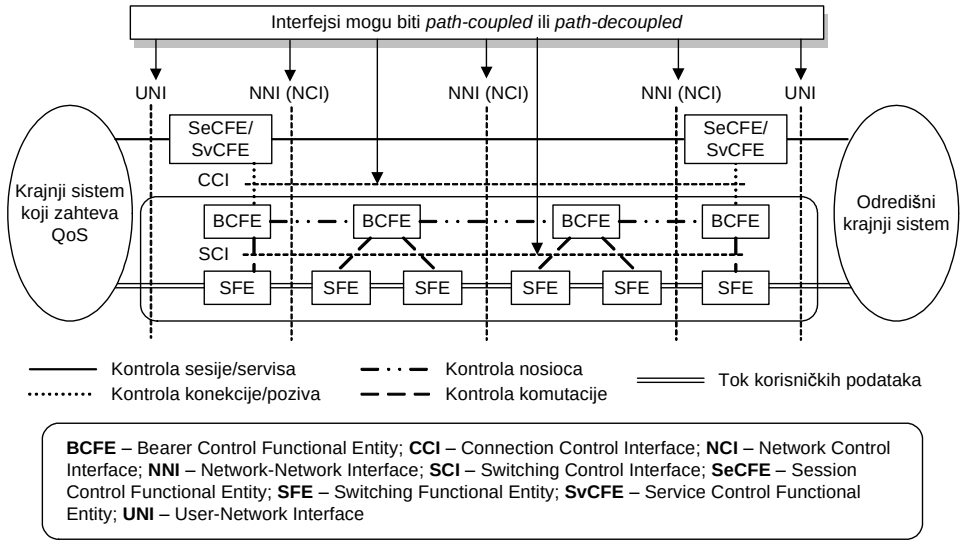
U nastavku će biti navedeni glavni nedostaci koji čine RSVP nepodesnim za primenu u NGN, a iscrpna analiza može se pronaći u [12]. Pre svega, RSVP je projektovan u vreme kada su mobilne komunikacije bile u začetku i ne podržava mobilnost čvorova. Korišćenje nekonektivnog transportnog mehanizma (*User Datagram Protocol*, UDP) bez mogućnosti segmentiranja poruka unosi ograničenja za mrežne arhitekture i signalizacione aplikacije. RSVP ne predviđa okvir za mehanizme zaštite, prvenstveno autentifikaciju i upravljanje kriptografskim ključevima. Generalna potreba *path-coupled* signalizacije je da otkriva lanac signalizacionih čvorova po principu *hop-by-hop*, duž putanje korisničkih podataka. U RSVP su otkrivanje čvorova i isporuka signalizacionih poruka objedinjeni u zajedničkom koraku. Takvo svojstvo značajno otežava i primenu postojećih bezbednosnih mehanizama (npr. *IP Security*), što je

posebno nepovoljno za poruke koje se prenose od jednog do drugog kraja mreže, kao šro je *PATH*.

3. Zahtevi za signalizaciju IP QoS

ITU-T SG 11 je specificirala zahteve za QoS signalizaciju od jednog do drugog krajnjeg korisnika dodatkom 51 preporuka Q serije [13]. Zahtevi obuhvataju interfejs korisnik-mreža (*User-Network Interface*, UNI) i međumrežni interfejs (*Network-Network Interface*, NNI). Specifikacija obaveznih i opcionih parametara QoS u signalizacionim porukama obuhvata:

- ciljne numeričke vrednosti mera performansi za datu klasu servisa kao što su procenat izgubljenih paketa, najveće kašnjenje i dr.;
- parametre kojima se opisuje tok saobraćaja, kao što su: vršni i/ili prosečan protok, vršna i/ili prosečna eksplozivnost saobraćaja, najveća dozvoljena veličina paketa;
- PHB kôd, tj. vrednost polja DSCP u zaglavlju IP paketa (opciono);
- parametre kojima se specificira prioritet i pouzdanost servisa.



Slika 2. *Funkcionalni model zahteva za signalizaciju IP QoS* [13]

ITU-T funkcionalni model zahteva za signalizaciju IP QoS prikazan je na slici 2. Funkcionalni elementi su struktuirani u dva sloja: sloj poziva/sesije i transportni sloj. Transportni sloj je podeljen na kontrolnu ravan nosioca i transportnu ravan.

Krajnji korisnik zahteva određeni servis posredstvom **funkcionalnog entiteta za kontrolu sesije** (*Session Control Functional Entity*, SeCFE) ili **funkcionalnog entiteta za kontrolu servisa** (*Service Control Functional Entity*, SvCFE). SeCFE kontroliše poziv/sesiju, vrši ekstrakciju zahteva za QoS za servisnu konekciju i generiše zahteve za QoS funkcionalnom entitetu za kontrolu nosioca (*Bearer Control Functional Entity*,

BCFE) na transportnom sloju, posredstvom odgovarajućeg interfejsa (*Connection Control Interface*, CCI). SeCFE se može implementirati kao *soft switch*, multipoint kontrolna jedinica (MCU), kontrolni server za video na zahtev i dr. SvCFE proširuje generičke mogućnosti SeCFE za ugovaranje i kontrolu QoS kako bi se obezbedila podrška za specifične servise krajnjih korisnika (prvenstveno mobilnih korisnika).

Funkcionalni entiteti za kontrolu nosioca (BCFE) su odgovorni za uspostavljanje, modifikaciju i oslobađanje resursa mreže koji su neophodni za obezbeđivanje ugovorenog nivoa QoS. BCFE mora imati informaciju o topologiji mreže i stanju resursa kako bi ocenio zahtev za QoS, dodelio resurse i generisao odgovarajuće podatke za konfigurisanje elemenata mreže. Priroda takve informacije prvenstveno zavisi od tehnologije transportnog sloja. BCFE prosleđuje rezultate analize putanja komutacionom funkcionalnom entitetu (SFE, *Switching Functional Entity*), posredstvom odgovarajućeg interfejsa (*Switching Control Interface*, SCI). Direktna komunikacija BCFE parnjaka obavlja se posredstvom interfejsa za kontrolu mreže (*Network Control Interface*, NCI).

Komutacioni funkcionalni entiteti (SFE) vrše prospajanje virtuelne veze na jednom portu sa virtuelnom vezom na drugom portu. Karakteristike virtuelne veze zasnivaju se na parametrima poziva ugovorenog na SeCFE/SvCFE nivou i putanjama određenim na BCFE nivou.

4. NSIS model

NSIS model [14] je usmeren ka specifikaciji protokola koji su spregnuti sa putanjama korisničkih podataka i namenjeni za komunikaciju tipa "tačka – tačka". Tako postavljen problem signalizacije je u suštini blizak specifikaciji RSVP, ali NSIS ima za cilj generalizaciju koncepta RSVP u smislu: (1) primenljivosti komponenata NSIS protokolskog steka u različitim delovima Interneta, za različite potrebe – pristupna signalizacija, signalizacija između krajnjih korisnika, signalizacija između graničnih rutera mreže i (2) mogućnosti interakcija između signalizacije i drugih funkcija mrežnog sloja, kao što su prevođenje adresa, rutiranje i mobilnost.

NSIS model razdvaja funkcije kao što su pouzdanost, upravljanje zagušenjem i integritet podataka od signalizacionih poruka koje potiču od odgovarajućih aplikacija, uvođenjem dvoslojne arhitekture koju sačinjavaju transportni sloj i sloj signalizacije, što je u saglasnosti sa ITU-T funkcionalnim modelom opisanim u poglavlju 3.

Protokol transportnog sloja (*NSIS Transport Layer Protocol*, NTLP) je odgovoran za prenos signalizacionih poruka između aplikacija. Iako je u [14] predviđena opcija dizajna monolitnog protokola na NTLP sloju, preporučen je pristup da NSIS specifične funkcije budu obuhvaćene generalnim transportnim protokolom za signalizaciju u Internetu (*General Internet Signaling Transport*, GIST [15]). GIST koristi standardne nekonektivne i konektivne transportne protokole i mehanizme zaštite.

Protokoli sloja signalizacije (*NSIS Signaling Layer Protocols*, NSLPs) izvršavaju funkcije signalizacije koje su specifične za konkretne aplikacije, što obuhvata formate i pravila procesiranja signalizacionih poruka. Primeri NSLP su QoS NSLP za signalizaciju sa rezervacijom resursa, NSLP za konfigurisanje merne opreme i dr.

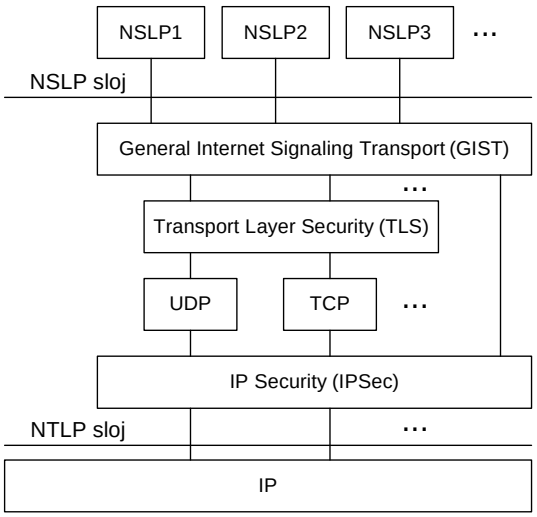
Kao i RSVP, NSIS protokoli se zasnivaju na principu *soft* kontrolnih stanja. NSIS uvodi koncept **signalizacionih sesija** sa jedinstvenim **identifikatorima** i pridruženim stanjima. Sesija se može preslikati u pojedinačni tok saobraćaja po principu

1:1, ali postoji i mogućnost uspostavljanja fleksibilnijih relacija sa tokovima saobraćaja u smislu podrške mobilnosti učesnika (tokom procedure *handover*-a), preslikavanja više tokova saobraćaja u jednu sesiju (*multihoming*) i transparentnosti identifikatora sesije u odnosu na tunelske mehanizme ili IPv4/IPv6 rutiranje između domena.

4.1 Transportni sloj – principi dizajna GIST protokola

GIST je zadužen za efikasnu isporuku signalizacionih poruka, u različitim mrežnim scenarijima. Ključni mehanizam GIST-a je otkrivanje parnjaka (*peer discovery*), a to je lociranje i/ili izbor NTLP parnjaka sa kojim će biti vršena razmena signalizacionih poruka za konkretan tok IP saobraćaja. Komponenta za otkrivanje paranjaka može se zasnivati na opciji *router alert* (RAO) ili tabelama rutiranja. Razdvajanje otkrivanja parnjaka od mehanizma prenosa poruke je ključna karakteristika koja omogućava da GIST koristi postojeće transportne protokole, kao i protokole zaštite na mrežnom i transportnom sloju.

Logička struktura NTLP sloja i uloga GIST protokola ilustrovani su na slici 3.



Slika 3. *Logička struktura NTLP sloja i uloga GIST protokola*

GIST funkcioniše u dva režima rada: (1) **datagram mod**, koji koristi nepouzdane, nekonektivne transportne mehanizme sa UDP protokolom kao prvim izborom i (2) **konektivni mod**, koji koristi pouzdane, konektivne transportne mehanizme, sa TCP (*Transmission Control Protocol*) kao prvim izborom. GIST može koristiti protokole zaštite na mrežnom sloju, kao što je IP *Security* (IPSec) ili na transportnom sloju, npr. *Transport Layer Security* (TLS).

GIST kreira i održava sledeće vrste *soft* stanja:

- Stanje rutiranja poruke po toku (*per-flow message routing state*) za procesiranje odlaznih poruka, koje tipično obuhvata identifikator toka, tip NSLP i identifikator sesije;
- Stanje pridruživanja poruke (*message association state*) za upravljanje stanjima parnjaka u konektivnom modu, koje se sastoji od adrese odredišnog

signalizacionog entiteta, brojeva protokola i porta, interne konfiguracije protokola i informacije o stanju.

GIST poruka se sastoji od zajedničkog zaglavlja i niza specifičnih *type-length-value* objekata. Zaglavlje sadrži informaciju o režimu rada, smeru poruke (*upstream/downstream*), vrsti NSLP i brojač *hop*-ova sa ciljem da se izbegne formiranje beskonačnih petlji. Pored toga, GIST koristi kratke poruke tipa upit/odziv (*cookies*) kao bezbednosni mehanizam za zaštitu od napada koji mogu prouzrokovati odbijanje servisa (*Denial of Service*, DoS).

4.2 Signalizacija kvaliteta servisa – QoS NSLP

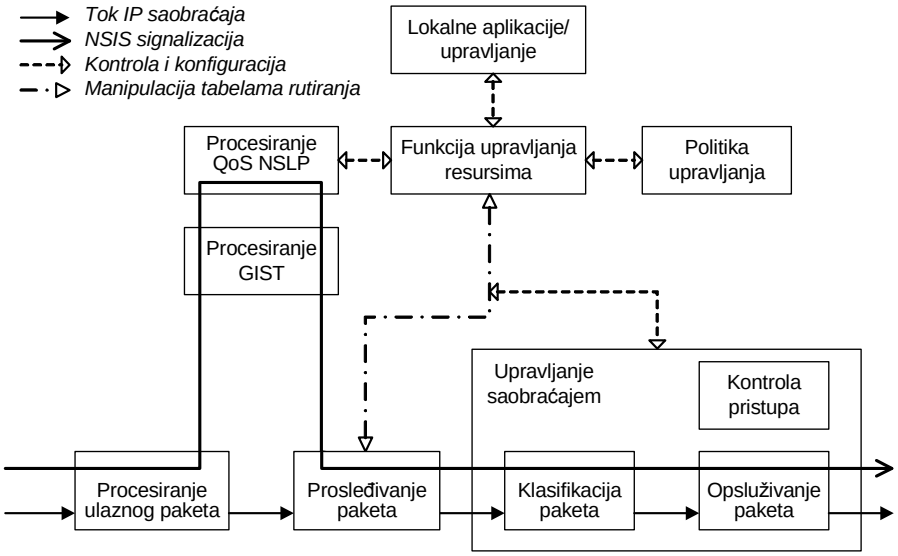
U slučaju signalizacije kvaliteta servisa pretpostavlja se da je proces signalizacije, koji rezultuje uspostavljanjem odgovarajućeg signalizacionog toka, usmeren od jednog do drugog krajnjeg korisnika. Inicijator (*QoS NSIS Initiator*, QNI) je entitet koji generiše zahtev za resurs, tipično kao posledicu zahteva korisničke aplikacije. Responder (*QoS NSIS Responder*, QNR) je entitet koji predstavlja krajnju tačku signalizacije i opciono može stupati u interakcije sa aplikacijom. Tranzitni signalizacioni entiteti (*QoS NSIS Forwarders*, QNFs) prosleđuju signalizacione poruke između QNI i QNR, kroz mrežu. Uzimajući u obzir smer toka korisničkih informacija, QoS signalizacija može biti orijentisana ka predajniku ili ka prijemniku (*sender-oriented/ receiver-oriented*). Semantika QoS NSLP poruka prikazana je u tabeli 1.

Tabela 1. *Pregled QoS NSLP poruka* [15]

Poruka	Smer	Operacija
Request	QNI→ QNR	Kreiranje nove rezervacije za tok saobraćaja
Modify	QNI↔ QNR	Modifikacija postojeće rezervacije
Release	QNI↔ QNR	Brisanje postojeće rezervacije
Accept/ Reject	QNI→ QNR	Potvrda ili odbijanje zahteva za rezervaciju
Notify	QNI↔ QNR	Izveštaj o događaju detektovanom u mreži
Refresh	QNI→ QNR	Upravljanje *soft* stanjem

Logički funkcionalni model QoS NSLP u čvoru prikazan je na slici 4. Iz perspektive čvora, zahtev za QoS može poticati od lokalne aplikacije (iniciran od korisničke aplikacije ili sistema za nadzor i upravljanje) ili dolazne QoS NSLP poruke. U slučaju dolazne NSLP poruke, neophodno je da NSIS poruke budu izdvojene tokom procesiranja ulaznog paketa i prosleđene entitetu GIST. QoS NSLP modul procesira samo poruke koje se tiču obezbeđivanja QoS, nezavisno od primenjenog QoS modela (IntServ, DiffServ, UMTS, GSS, drugi modeli). Parametri koji se odnose na rezervaciju resursa (npr. raspoloživi propusni opseg, parametri kondicionera saobraćaja) enkapsulirani su u NSLP i prenose se između QoS NSLP čvorova. U svakom čvoru, zahtev za QoS procesira se u sklopu funkcije upravljanja resursima. Lokalni QoS model propisuje način interpretacije zahteva za QoS iz signalizacione poruke, kao i način obezbeđivanja i konfigurisanja resursa. Obezbeđivanje resursa obuhvata dva dodatna

lokalna procesa – proceduru kontrole pristupa i politiku upravljanja. Na kraju, QoS NSLP čvor generiše indikaciju da su zahtevani resursi konfigurisani, tj. potvrdu zahteva. Čvor takođe može proslediti zahtev za QoS po odgovarajućoj putanji do prijemne strane.



Slika 4. *Funkcionalni model QoS NSLP u čvoru mreže* [15]

5. Zaštita NSIS protokola

Zaštita NSIS protokola je složen zadatak zbog toga što je NSIS namenjen za podršku velikog broja heterogenih mrežnih scenarija, u koje može biti uključen veliki broj signalizacionih entiteta, veliki broj različitih uređaja – od servera visokih performansi u korporativnim mrežama do mobilnih uređaja, kao i različiti kriptografski mehanizmi i protokoli za autentifikaciju. Mogući napadi na NSIS protokole obuhvataju opšte napade koji su zajednički za većinu kontrolnih protokola i napade specifične za NSIS [16], [17].

S obzirom da je protokolski stek podeljen na dva sloja, mehanizmi zaštite obuhvataju rešenja za NTLP i za NSLP. Zahtevi za zaštitu NSIS [18] obuhvataju:

- Sposobnost izvršavanja autentifikacije i protokola za razmenu ključeva između susednih NSIS parnjaka;
- Uspostavljanje zaštitne asocijacije sa ciljem obezbeđivanja integriteta, poverljivosti i zaštite od replikacije signalizacionih poruka koje razmenjuju susedni parnjaci;
- Zaštita od odbijanja servisa (DoS);
- Osnovna zaštita mehanizma otktivanja parnjaka;
- Autorizacija NTLP signalizacionih parnjaka;
- Fleksibilna autorizacija na NSLP sloju koja podrazumeva interoperabilnost sa postojećom infrastrukturom za autentifikaciju, autorizaciju i tarifiranje (*Authentication, Authorization and Accounting*, AAA).

Veoma je teško projektovati novi protokol zaštite koji bi ispunio sve navedene zahteve. Kao što je ranije istaknuto, NSIS model pretpostavlja integraciju sa standardnim protokolima zaštite na mrežnom i transportnom sloju, kao što su IPSec i TLS. Ti protokoli u određenoj meri obezbeđuju autentifikaciju, uspostavljanje zaštitnih asocijacija i zaštitu od DoS napada, ali na račun uvođenja značajnog kašnjenja pri uspostavljanju veze. Ako se NSIS sesije uspostavljaju samo između čvorova koji implementiraju isti NSLP, parnjaci mogu da provere identitet i izvše autorizaciju. Autorizacija GIST-a na transportnom sloju treba da osigura legitimitet inicijatora GIST veze. Međutim, u najvećem broju slučajeva, teško je da GIST entitet sam izvrši autorizaciju i neophodna je njegova komunikacija sa entitetom NSLP sloja. Pored toga, razmena poruka za otkrivanje parnjaka je bezbednosno vrlo osetljiv proces u kome se može primeniti mehanizam baziran na kratkim porukama (*cookies*) [18]. U velikom broju slučajeva, NSIS čvor nije u mogućnosti da sam donese ispravnu odluku o autorizaciji, posebno u mobilnom okruženju, već za te potrebe mora da sarađuje sa AAA infrastrukturom.

6. Zaključak

Signalizacija je danas jedan od najsloženijih problema u istraživanju arhitektura i mehanizama implementacije kvaliteta servisa u Internetu i IP baziranim mrežama. Iako je RSVP protokol godinama razvijan i usavršavan za potrebe signalizacije u okruženju različitih IP QoS arhitektura, on nije implementiran u operativnim mrežama. S obzirom da RSVP ne podržava mobilnost čvorova i ne poseduje mehanizme zaštite, ovaj protokol nije podesan za signalizaciju u NGN.

ITU-T SG 11 je specificirala zahteve za QoS signalizaciju od jednog do drugog krajnjeg korisnika, kao i odgovarajuće funkcionalne elemente, struktuirane u dva sloja (sloj poziva/sesije i transportni sloj). IETF definiše dvoslojni NSIS protokolski stek, koji je u osnovi kompatibilan sa ITU-T specifikacijama. Skalabilnost, interoperabilnost sa postojećim transportnim protokolima i protokolima zaštite, kao i podrška mobilnih korisnika su prednosti NSIS protokola koje bi trebalo da doprinesu njihovoj bržoj implementaciji u operativnim mrežama. Iako je NSIS implementiran u jednom broju nezavisnih eksperimentalnih mreža, još uvek nije izvršena kompletna validacija i verifikacija NSIS protokola, posebno u domenu mobilnih IP mreža. Neka od otvorenih pitanja obuhvataju nove mehanizme za otkrivanje parnjaka na transportnom sloju, integraciju sa AAA infrastrukturom sa posebnim naglaskom na tarifne mehanizme i interoperabilnost sa RSVP protokolom.

Literatura

[1] S. Blake et al., "An Architecture for Differentiated Services", RFC 2475 (Informational), IETF, 1998.

[2] R. Braden, D. Clark, S. Shenker, "Integrated Services in the Internet Architecture: an Overview", RFC 1633 (Informational), IETF, 1994.

[3] "End to End Quality of Service Concept and Architecture", 3rd Generation Partnership Project TS 23.207, Release 5, June 2003. [Online]. Available: http://www.3gpp.org.

[4] S. Maniatis, E. Nikolouzou, I. Venieris, "End-to-End QoS Specification Issues in the Converged All-IP Wired and Wireless Environment", *IEEE Communications Magazine*, vol. 42, no. 6, June 2004, pp. 80-86.

[5] S. Giordano et al., "Advanced QoS Provisioning in IP Networks: The European Premium IP Projects", *IEEE Communications Magazine*, vol. 41, no. 1, January 2003, pp. 30-36.
[6] M. Stojanović, V. Aćimović-Raspopović, *Inženjering telekomunikacionog saobraćaja u multiservisnim IP mrežama*, naučna monografija, Saobraćajni fakultet Univerziteta u Beogradu, oktobar 2006.
[7] ITU-T Recommendation Y.1291, "An Architectural Framework for Support of Quality of Service (QoS) in Packet Networks", May 2004.
[8] V. Aćimović-Raspopović, M. Stojanović, D. Teodorović, "Quality of Service Negotiation in Next Generation Networks", invited paper, *Proceedings of the TELSIKS 2007*, vol.1, pp. 77-86, Niš, September 2007.
[9] R. Braden et al., "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification", RFC 2205 (Standards Track), IETF, 1997.
[10] F. Baker et al., "Aggregation of RSVP for IPv4 and IPv6 Reservations", RFC 3175 (Standards Track), IETF, 2001.
[11] D. Awduche et al., "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209 (Standards Track), IETF, 2001.
[12] J. Manner, X. Fu, "Analysis of Existing Quality-of-Service Signaling Protocols", RFC 4904 (Informational), IETF, 2005.
[13] Supplement 51 to ITU-T Q-series Recommendations, "Signalling Requirements for IP-QoS", December 2004.
[14] R. Hancock et al., "Next Steps in Signaling (NSIS): Framework", RFC 4080 (Informational), IETF, 2005.
[15] X. Fu et al., "NSIS: A New Extensible IP Signaling Protocol Suite", *IEEE Communications Magazine*, vol. 43, no. 10, October 2005, pp. 133-141
[16] H. Tschofenig, D. Kroeselberg, "Security Threats for Next Steps in Signaling (NSIS)", RFC 4081 (Informational), IETF, 2005.
[17] D. Paunović, "Zaštita NSIS protokola u telekomunikacionim mrežama zasnovanim na Internet tehnologiji", *Zbornik radova TELFOR 2007 (CD)*, Beograd, 2007.
[18] H. Tschofenig, X. Fu, "Securing the Next Steps in Signaling (NSIS) Protocol Suite", *Inernational Journal of Internet Protocol Technology*, vol. 1, no. 4, August 2006, pp. 271-282.

Abstract: *In this paper, we first provide taxonomy of quality of service (QoS) signaling mechanisms in Internet Protocol (IP) based networks. Further, an overview of Resource Reservation Protocol (RSVP) is presented. RSVP has been standardized by IETF to support different QoS architectures. We particularly address activities in standardization of QoS signaling protocols in next generation networks, i.e., ITU-T recommendations for IP QoS signaling requirements and IETF framework for signaling protocols – Next Steps in Signaling (NSIS). Important issues encompass support of heterogeneous network scenarios, support of mobile users and security mechanisms.*
Keywords: *Internet, Quality of service, Resource reservation, Security, Signaling*

QUALITY OF SERVICE SIGNALING PROTOCOLS IN NEXT GENERATION NETWORKS

Mirjana Stojanović, Slavica Boštjančič