

Preporuke TM Foruma za ugovaranje SLA u slučaju VPN servisa

Srđan Bojičić

Funkcija za IT operativno upravljanje
Telekom Srbija
Beograd, Srbija
srdjan.bojicic@telekom.rs

Sažetak— U ovom radu prikazan je proces modelovanja SLA ugovora u slučaju pružanja VPN servisa, prema preporukama TM Foruma. Pažnja je usmerena na standardizaciju procesa ugovaranja, postavljanja i praćenja realizacije SLA. Na kraju je dat i jedan konkretan primer ponude, koji ukazuje na status do kog se u praksi stiglo prilikom definisanja SLA ponude za VPN servis.

Ključne riječi - SLA 1; VPN 2;

I. UVOD

Poslovanje se značajno promenilo u poslednjih nekoliko decenija. Kompanije sada razmišljaju u smislu globalnog prisustva, globalnog tržišta i logističke podrške. Većina kompanija ima filijale razgranate po različitim geografskim položajima na globusu. Gde god da ste locirani, sve ove filijale treba da imaju vezu sa centralom kompanije zbog razmene informacija. Sa promenom poslovne kulture i okruženja, zahtevi prodaje za vezom sa centralom kompanije bilo od kuće ili hotelske sobe su rastući i razmena podataka je postala potreba. Stoga postoji jedan zahtev koji sve kompanije traže od svojih mrežnih timova: brza, sigurna i pouzdana konekcija koja pruža mogućnost komunikacije sa svim kancelarijama filijala bilo gde da se one nalaze.

Kada kompanije žele da se mrežno povežu sa spoljnim partnerima, eksternim dobavljačima, outsource firmama, osobljem koje se bavi prodajom, postoje dva načina za to: iznajmljena linija koja služi samo za tu svrhu ili deoba propusnog opsega sa već postojećim linijama kao što je Internet. Iznajmljene linije iz opsega ISDN (144Kbps) do optičkog kabla (192Gbps) omogućuju kompanijama da poveću geografski razudene kancelarije. Na primer, X.25, Frame Relay, Asynchronous Transfer Mode (ATM), i MPLS (Multiprotocol Label Switching) su primeri privatnih WAN mreža. Za sigurnost konekcije preporuka je uvek imati svoju sopstvenu privatnu iznajmljenu liniju između različitih tačaka. Ipak, ova opcija je veoma skupa s obzirom da je potrebno povezati različita mesta pomoću različitih kablova, a postavljanje kablova je skupa radnja, a tek njihovo održavanje je još skuplje. Takođe, postavljanje kablova nije izvodljiva opcija s obzirom da se kancelarije premeštaju s vremena na vreme, ili za mobilnu radnu snagu koja je konstantno u pokretu. S druge strane, deoba linija sa drugima je jeftinije, ali nije uvek sigurno. Da bi se prevazišao ovaj problem, razvijen je

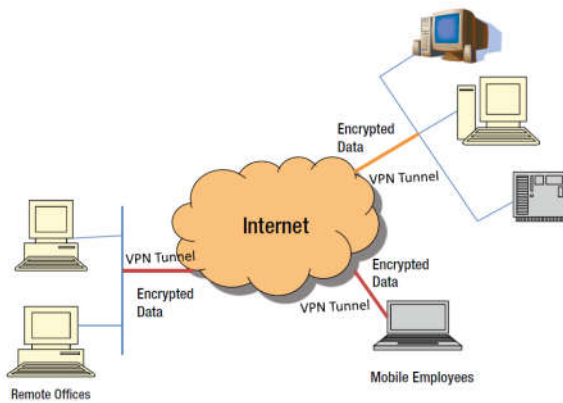
koncept virtuelne privatne mreže (VPN). U suštini, VPN kreira tunel između dve tačke kroz koji se podaci prenose sigurno kroz ovaj tunel, ali preko javno deljene mreže.

VPN je privatna mreža, kao što je prikazano na slici 1, ali koristi javnu mrežu (Internet) da poveže udaljene lokacije [1]. VPN kreira virtuelnu tunelsku konekciju rutiranu kroz Internet od kompanijine interne mreže do udaljene kancelarije ili mobilne radne snage. Sa VPN-om mogu se slati podaci preko javne mreže koja emulira privatni link između dve strane ili dve mreže. VPN mreža sigurnosno enkriptuje podatke pre nego što ih pošalje kroz tunel kako bi osigurala privatnost. Integritet podataka i autentifikacija se takođe osiguravaju pre slanja kroz tunel. Stoga, VPN štiti podatke kroz privatnost, integritet i autentifikaciju. Sa VPN-om, može se pružiti mnogo servisa kao što je Internet, email, aplikacije, servisi baza podataka, korisnicima na udaljenim lokacijama sa sigurnosno bezbednom komunikacijom.

Kada se govori o VPN mrežama najčešće se misli na Layer 3 ili Layer 4 VPN mreže (iz OSI modela). Glavna mana ovih VPN mreža je interoperabilnost i osetljivost na DoS napade. Najčešće su VPN konekcije vezane za jednog vendedora ili jednog ISP (Internet Servis Provajder). Mnoga od IP baziranih VPN rešenja zahtevaju enkapsulaciju IP sadržaja ili čak i duplu enkapsulaciju. Ovo zahteva dodatnu obradu na ulazu i izlazu iz ISP mreže. Takođe, ove mreže najčešće koriste javne gateway-e za povezivanje. Time su one izložene DoS (Denial of Service) napadima, koji smanjuju brzinu i iskorišćeni propusni opseg. Ova pitanja mogu biti rešena ako se VPN konekcija prebaci na Layer 2. VPN konekcija na Layer 2, poznatija pod imenom IP VPN ili MPLS VPN, izbegava javni Internet putujući na privatnoj konekciji na svaki udaljeni sajt. Takođe, kao Layer 2 servis IP VPN koristi mogućnosti MPLS-a za prioritizacijom kompanijskog saobraćaja, tako da kritične aplikacije poput video konferencije i digitalnog prenosa govora imaju zagantovani propusni opseg koji im je potreban za prenos. Prenosni MPLS svičevi ne obrađuju IP zaglavljia, destinacione IP adrese u paketima se ne ispituju, i još uz to bolja je kontrola mrežnih parametara kao što su kašnjenje, propusni opseg i raspoloživost. MPLS baziran VPN, ili IP VPN, omogućuje povezivanje geografski razudjenih kancelarija ili privatnih mreža korišćenjem LSP-a (Label Switch Path).

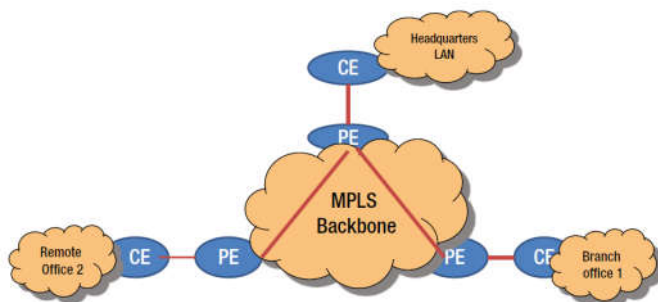
Na slici 2 je prikazana osnovna arhitektura MPLS baziranog VPN-a. Postoje dve komponente u arhitekturi, CE

korisnička oprema (Customer Equipment) i oprema servis provajdera (Provider Equipment).



Slika 1. VPN mrežni scenario.

CE može biti ruter, svič ili host. PE su deo backbone mreže. PE je odgovoran za kontrolu VPN konektivnosti, VPN korisnike, uspostavljanje MPLS LSP konekcije (VPN tunel) između PE-ova i dodeljenih ruta među raznim kancelarijama istog VPN-a.



Slika 2. MPLS baziran VPN (IP VPN ili L2 VPN).

II. END-TO-END SLA MENADŽMENT

SLA se definiše kao ugovor sa dogovorenim nivoom kvaliteta usluge. SLA služi kao sredstvo formalnog dokumentovanja očekivanih performansi servisa, odgovornosti pojedinih ugovornih strana i tački razgraničenja između servis provajdera i njihovih korisnika. Tipičan SLA opisuje nivoe servisa korišćenjem različitih atributa, poput: raspoloživost, dostupnost, operativnost, penali koji su pridruženi atributima u slučaju kršenja SLA. U SLA se definišu Business Level Objectives tj. nivoi poslovnih ciljeva, koji se ne odnose na servise već na poslovne zahteve korisnika poput disaster recovery, data privacy itd. BLO formiraju poslovnu politiku koja određuje vrednosti servisnih parametara. Najčešće se BLO baziraju na subjektivnim „soft“ merenjima, poput: Visok, Nizak, itd. Definišu se i Service Level Objectives tj. nivoi servisa koji predstavljaju specifične merljive karakteristike servisa koji se monitoriše. SLO se sastoje od jednog ili više Quality of Service indikatora ili servisnih metrika.

Glavni izazov prilikom upravljanja SLA ugovorima s kraja na kraj (end-to-end) je kako uraditi agregaciju SLA kroz

različite servise, servisne domene i njihove odgovarajuće metrike, kako na pojedinačnom servisu, tako i na kompozitnom i agregacionom nivou. U literaturi [2] se definiše rola SLA integratora kao odgovorna za agregaciju SLA-ova različitih dobavljača i njihovo predstavljanje kao jedinstvenog SLA od strane servis provajdera ka korisniku. SLA integracija je agregacija, koja se vrši preko transformacije i kombinacije metrika od nižih SLA ka višem jedinstvenom SLA.

Ovde je potrebno napraviti rezime i usaglašavanje termina koji se koriste za metrike kod SLA, s obzirom da oni nisu jedinstveno definisani kroz literaturu. Metrike uglavnom upadaju u dve velike grupe. To su biznis metrike (koje se i definišu kroz SLA) i tehničke metrike (monitoring metrike) koje omogućavaju proračun biznis metrika. Na primer response time može biti specificiran u SLA, dok druga tehnička merenja kao što su hop-ovi i bandwidth mogu biti korišćeni za dinamičku alokaciju resursa omogućavajući ispunjenje response time-a. Metrike bazirane na iskorišćenosti resursa su generalno podkategorija biznis metrika i predstavljaju glavnu komponentu ugovora o usluzi, koje mogu a i ne moraju biti deo SLA ugovora. Neki primeri metrika iskorišćenosti resursa su broj korisnika usluge, iskorišćenje: instance, CPU-a, storage-a, memorije. Metrike koštanja su bazirane na novcu po iskorišćenosti resursa (npr. novčana_valuta/instance_minutes). SLA se pre svega zasniva na service assurance-u, dakle metrike korišćenja resursa tj. biling nije u scope-u SLA. Slede definicije metrika koje su u širokoj upotrebi u SLA:

- metrika – nešto što je merljivo
- mera – broj sa relativnom vrednošću (novčana valuta, litri, gigabajti storage-a, kilovati)
- merenja – SLM (T) se odnosi na SLA i predstavlja skup izmerenih vrednosti u trenutku T za sve KQI u odgovarajućem SLA
- KQI – u SLA kontekstu su metrike razumljive za korisnika. U telekom kontekstu su metrike razumljive za netehničko osoblje. KQI se koristi u Service Level Specifikaciji, s obzirom da korisnici u praksi nisu svesni tehnologije kojom se servis pruža
- KPI – u SLA kontekstu su metrike razumljive za servis provajdera. U telco kontekstu to su metrike bliske tehnologiji i uređajima

S obzirom na različite tipove metrika/merenja koji doprinose proračunu SLA, takve biznis metrike, performance metrike, storage metrike itd. zahtevaju metamodel koji daje konzistentan opis. Detaljan opis ovakvog metamodela je dat u literaturi [3]. Framework je definisan u UML-u i značajne su definicije: MetricDefinition, MetricDefMeasure i MetricDefinitionDeterminationMethod.

III. PRIMER SLA PARAMETARA U SLUČAJU L3 VPN SERVISIA

U literaturi [4] je naveden primer implementiranog modela SLA ugovora za jednog velikog nacionalnog provajdera fiksne telefonije i interneta. Rešenje je iskorišćeno za monitoring stanja 4 VPN mreže i proračun SLA parametara. Svaki čvor pojedine VPN mreže je povezan različitim interfejsima core

mreže rutera i monitorisan je nezavisno. Monitoring VPN čvora je izvedeno Service Assurance agentima koji su ugrađeni deo operativnog sistema Cisco rutera. Agent periodično šalje određeni paket podataka, čija je veličina unapred konfigurisana, prema CPE (Customer Premises Equipment) opremi, gde je instaliran agent koji odgovara na ove upite. Stoga, agent pruža sledeće metrike linka:

- Raspoloživost (0 znači link je raspoloživ, 1 znači da nije),
- Prosečno vreme kašnjenja [ms] (Average Round Trip Time),
- Varijaciju kašnjenja [ms] (Round Trip Time Jitter),
- Gubitak paketa [%] (Packet Loss),
- Dolazni saobraćaj [kb/s] (Incoming traffic),
- Odlazni saobraćaj [kb/s] (Outgoing traffic).

Izmerenim vrednostima se pristupa pomoću SNMP protokola, prikupljaju se sa rutera na svakih 5 minuta i čuvaju u txt fajlovima od strane eksterne aplikacije. Periodično (svakog sata) fajlovi sa performansnim podacima se učitavaju u dve baze: produkcionu i razvojnu. Zahtevi su razvijani tako da se prate samo performansni podaci, a ne i podaci sa fault-a. Definirano je više pragova za raspoloživost i performansne parametre, i razvijene su formule za obračun penala prema zahtevima provajdera.

Sistem za medijaciju uzima podatke iz navedenih baza pomoću 2 procesa:

- proces koji radi upite nad bazom
- proces koji predstavlja adapter između SLM sistema i podataka koje dovlači prvi proces direktno iz baze

Kada se jednom uzmu podaci iz baze, proces ih šalje ka Performance Management modulu gde se podaci obrađuju (proračunavaju se KPI i skladište u internu bazu odakle iz koristi SLM sistem).

S obzirom da SLA filozofija traži da se prvo kreiraju templejti, a zatim da se popunjavaju konkretnim podacima, definisano je 6 templejta. Jedan SAP (Service Access Point) templejt, koji definiše link ka VPN čvoru i specificira koji KPI se šalju ka servisnom nivou. Jedan servisni templejt, koji koristi prethodni SAP templejt, ali ima i specifikaciju koji KPI-evi su dostupni na SLA nivou. Jedan produkcionni templejt (koji sadrži prethodno definisani servisni templejt) i tri SLA templejta.

Zatim se određene instance objekata i SLA ugovora kreiraju na osnovu prethodno definisanih templejta. Kada se pojavi alarm na osnovu prekoračenja nekog PM praga, preuzima se određena akcija na bazi definisanog korelacionog mehanizma. Ova vrsta alarma obaveštava korisnika da je prekoračeno iskorišćenje dozvoljenog propusnog opsega i da se neće obračunati penali za KPI-eve.

Funkcionalnost izveštavanja omogućuje korisnicima:

- prikaz trenutne vrednosti KPI grafički,

- praćenje statusa servisa i SLA ugovora u “near real time” vremenu pomoću alarmne liste i dodeljenih view-ova u SLM-u,
- obračun penala za prekoračenje SLA na osnovu predefinisanih izveštaja.

Na ovaj način je SLM sistem uspešno implementiran u realnom okruženju. Ispunjeni su svi predefinisani zahtevi klijenta i sistem je evaluiran iz biznis perspektive.

IV. PRIMER SLA PARAMETARA U SLUČAJU L2 VPN SERVISA

L2 VPN servis se pruža korisniku [3] kao skup pristupa sa CPE rutera ka IP backbone mreži. Stoga se ovde mogu identifikovati dva tipa servisnih elemenata: pristup i konektivnost IP backbone mreže. Važno je monitorisati SLA potrebe na korisničkom sajtu tj. na geografskoj lokaciji na kojoj se nalazi krajnja tačka L2 VPN-a. Stoga se SLA parametri za jedan L2 VPN servis mogu definisati na sledeći način:

- IP Packet Loss za jednu pristupnu tačku, na tački razgraničenja prema VPN konekciji,
- s obzirom da jedan korisnički sajt može imati više pristupnih tačaka (više SAP-ova), KPI se mogu agregirati kako bi se dobila vrednost za tu lokaciju (kao što je njena dostupnost na primer),
- za konekciju između dve pristupne tačke, može se definisati broj izgubljenih IP paketa i kašnjenje u prenosu IP paketa između njih,
- za višestruke instance istog tipa pristupa može se definisati srednja raspoloživost za sve pristupe,
- servis bundle parametri, agregirani za celokupan IP VPN servis, kao što je raspoloživost servisa i MTTR (Mean Time to Restore).

Primer L2 VPN SLA parametara dat je u Tabeli I, pri čemu je MTTR (Mean Time to Restore), MTBF (Minimum Time between Failure) i MTTP (Mean Time to Provision).

TABELA I. PRIMER L2 VPN SLA PARAMETARA

Servis perspektiva	SLA Parametri		
	<i>Tehnološki specifično</i>	<i>Servisno specifično</i>	<i>Tehnološki/Servisno nezavisno</i>
Pristupna tačka	Brzina	- max kašnjenje - max gubitak paketa - max jitter	- max vreme neraspoloživosti linije - MTTR - MTBF
Agregirani zahtevi	Neraspoloživost	- max kašnjenje za sve pristupe - srednje kašnjenje za određenu lokaciju - srednje kašnjenje za određeni pristup - srednji jitter - srednji protok	- max vreme neraspoloživosti za lokaciju - max vreme neraspoloživosti za sve pristupne linije - MTBF - MTTR - MTTP

V. JEDAN PRIMER IZ PRAKSE ZA L2 I L3 VPN SERVIS

Ovde će biti prikazan jedan primer iz prakse ponude SLA za L2 i L3 VPN servis. U ovom primeru se nude 4 KQI koji su zajednički i za L2 i za L3 VPN SLA ugovor:

- Uspostavljanje servisa (Provisioning)
- Vreme odziva (Response time)
- Vreme za otklanjanje smetnji (Restore time)
- Raspoloživost (Availability)

Ovo su parametri kvaliteta servisa, koji imaju različite vrednosti u zavisnosti od izabranog SLA paketa. Pri tome su u ponudi dati sledeći paketi: Standard SLA, Standard SLA+, Silver SLA, Gold SLA i Gold SLA+. U ponudi je i varijanta u kojoj provajder obezbeđuje CE ruter na lokaciji korisnika, ili to čini sam korisnik. U slučaju da to učini sam korisnik, onda mu se nude samo dve opcije SLA paketa: Standard SLA i Standard SLA+.

U slučaju L2 VPN servisa definisane su sledeće vrednosti SLA parametara ugovora u slučaju Standard SLA paketa sa direktnim pristupom:

TABELA II. PRIMER L2 VPN SLA PARAMETARA

SLA parametar	Vrednost
Raspoloživost	99,25%
Provisioning time	25 radnih dana
Response time	90 minuta
Restore time	48h

U slučaju L3 VPN servisa definisane su sledeće vrednosti SLA parametara ugovora za Silver paket (u pitanju je pristup bakrom):

TABELA III. PRIMER L3 VPN SLA PARAMETARA ZA SILVER PAKET

SLA parametar	Vrednost
Raspoloživost	99%
Provisioning time	20 radnih dana
Response time	60 minuta
Restore time	16h

U slučaju L3 VPN servisa u ponudi su i sledeći QoS parametri kvaliteta po klasama servisa (Voice i Business klase):

- Kašnjenje (Round Trip Time)
- Varijacija kašnjenja (Jitter)
- Gubitak paketa (Packet loss)

Recimo, za Voice klasu u ponudi su sledeće vrednosti za FastEthernet/GigabitEthernet pristup:

TABELA IV. PRIMER QoS PARAMETARA ZA L3 VPN SILVER PAKET

QoS parametar	Vrednost
Round Trip Time	25ms
Jitter	6ms
Packet loss	0,05%

VI. ZAKLJUČAK

Cilj ovog rada je da pokaže kako je za kreiranje SLA ugovora u slučaju VPN servisa, potrebno razmotriti zahteve svih učesnika u korišćenju i pružanju ove usluge. Iz perspektive krajnjeg korisnika ovo znači da mu je potrebno obezbediti one parametre usluge koji znatno utiču na njegovo celokupno zadovoljstvo pri korišćenju usluge (QoE). Na kraju je dat primer ponude iz prakse jednog konkretnog provajdera iz okruženja.

LITERATURA

- [1] U. Nayak, U. Rao, "The Infosec Handbook", Apress, 2014
- [2] GB917: „SLA Management Handbook“, TM Forum, Novembar 2012
- [3] GB 922, „Information Framework Suite - Metric“, TM Forum, Mart 2015
- [4] J. Kosinski, P. Nawrocki, D. Radziszowski, K. Zielinski, S. Zielinski, "SLA monitoring and management framework for Telecommunication services", Fourth International Conference on Networking and Services (icns 2008)

ABSTRACT

In this paper SLA for VPN service, according to TM Forum recommendations is presented. Attention is focused on the standardization of negotiation process, deployment and operations of SLA. In the end, an example of the offer for SLA VPN service is shown. This example reveals how far SLA VPN has come in practice.

PREPORUKE TM FORUMA ZA UGOVARANJE SLA U SLUČAJU VPN SERVISIA

Srđan Bojičić