Podaci o interfejsima elektronskih komunikacionih mreža A1 Srbija u terminalnim tačkama mreže A1 Srbija

Na osnovu Pravilnika o načinu objavljivanja podataka o interfejsima elektronskih komunikacionih mreža u terminalnim tačkama mreže („Službeni glasnik RS", broj 50/2024), A1 Srbija d.o.o. Beograd (u daljem tekstu: „**A1 Srbija**"), objavljuje tehničke specifikacije postojećih interfejsa u terminalim tačkama mreže, a kako sledi:

---

1. Pojmovi

1.1. **Ethernet** – Data Link sloj tehnologija specificirana IEEE 802.3 specifikacijom koja omogućava povezivanja opreme u lokalnoj mreži.
1.2. **Cat6** – Standardni kabl sa upredenim bakarnim paricama za potrebe Ethernet veza preporučen za povezivanje uređaja u lokalnim kućnim mrežama na rastojanjima od 50-100m gde se garantuju brzine do 1Gbps.
1.3. **CPE** – Customer Premisses Equipment (A1 oprema koja se nalazi kod korisnika).
1.4. **L3 CPE** – Layer 3 CPE – Ruter na lokaciji korisnika.
1.5. **L2 CPE** – Layer 2 CPE – data link sloj uređaj na lokaciji korisnika, u ovom slučaju ONT funkcionalnost gde se obezbeđuje terminacija optičkog dela mreže i omogućava Ethernet LAN pristup ka Layer 3 uređaju.
1.6. **PON** – Passive Optical Network (Pasivna Optička Mreža).
1.7. **GPON** – Gigabit-per-second-capable Passive Optical Network (Gigabitna pasivna optička mreža).
1.8. **PPP** – Point To Point Protocol.
1.9. **PPPoE** – Point To Point over Ethernet.
1.10. **ODN** – Optical Distribution Network (Optička distributivna mreža).
1.11. **ONT** – Optical Network Terminal (Optički mrežni terminal).
1.12. **ONU** – Optical Network Unit (Optička mrežna jedinica).
1.13. **OLT** – Optical Line Terminal (Optička linijska terminacija).
1.14. **FTTH** – Fiber To The Home (Optika do kuće).
1.15. **IPv4** – Internet Protocol version (Internet protokol versija).
1.16. **VLAN** – Virtual Local Area Network (Virtuelna lokalna privatna mreža).
1.17. **VLANID** – Virtual Local Area Network Identifier (Identifikator virtuelne lokalne privatne mreže).
1.18. **MTU** – Maximum Transmission Unit.
1.19. **802.1p bit** – IEEE specification for adding traffic class expediting to 802.1D standard.
1.20. **DSCP** – Differented Services Code Point.
1.21. **QoS** – Quality Of Service (Kvalitet usluge).
1.22. **WAN** – Wide Area Network.
1.23. **3rd party** – Third Party (Oznaka uglavnom za ruter koji je korisnik samostalno nabavio i povezuje ga opciono sa A1 Srbija CPE opremom).
1.24. **ISO OSI model** – International Organization for Standardization Open System Interconnection model.
1.25. **Bridge mode** – podešavanje A1 Srbija CPE uređaja gde se isključuju funkcionalnosti trećeg sloja ISO OSI modela (uređaj transparentno prosleđuje saobraćaj od/ka A1 mreže ka 3rd party ruteru korisnika i ne obavlja više fukcije rutiranja gde se ta funkcionalnost ostavlja 3rd party korisničkom ruteru).

---

2. Polje primene

Tehničke specifikacije postojećih interfejsa u terminalim tačkama mreže A1 Srbija se odnose na A1 usluge pristupa internetu, koje se pružaju preko fiksne javne komunikacione mreže.

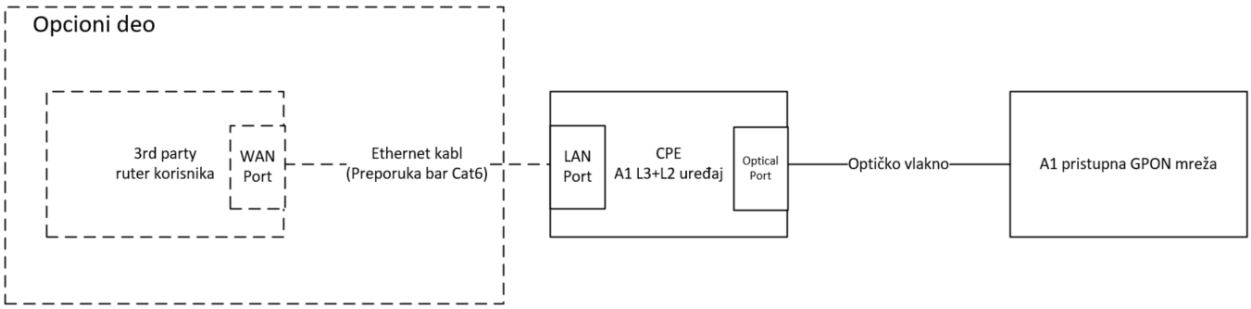
3. Opis tehničkih specifijacija

A1 Srbija za pružanje usluge pristupa interneta preko fiksne javne komunikacione mreže, na fizičkom sloju (ISO OSI Layer1 – Physical) i na data link sloju (ISO OSI Layer2 – Data Link) koristi pasivnu optičku mrežu na bazi GPON tehnologije specificirane ITU-T G.984.x specifikacijama.

GPON sistem se sastoji od OLT-ova na lokacijama A1 Srbija, ONU/ONT-ova na lokaciji krajnjeg korisnika, odnosno Pretplatnika i optičke distributivne mreže.

Tačke razgraničenja opreme krajnjeg korisnika i A1 pristupne opreme se nalaze na sledećim slikama:

Scenario 1:
A1 CPE L3+L2 (Inegrisana ONT funkcionalnost i ruter funkcionalnost (Layer 3) u jednom A1 Srbija uređaju)



Slika 1

U ovom scenariju u slučaju da krajnji korisnik, odnosno Pretplatnik želi da poveže svoj Layer3 uređaj (*3rd party* kućni ruter), potrebno da podnese na zahtev ka A1 Srbija i zatražiti daljinsku izmenu konfiguracije gde se A1 Srbija uređaj prebacuje u *„brigde*" mode i obezbeđuje Ethernet vezom povezivanje Layer3 korisničkog rutera sa bilo kojim LAN ethernet portom na A1 Srbija CPE uređaju.

Optička/GPON terminacija ka mreži ostaje na A1 Srbija CPE-u.

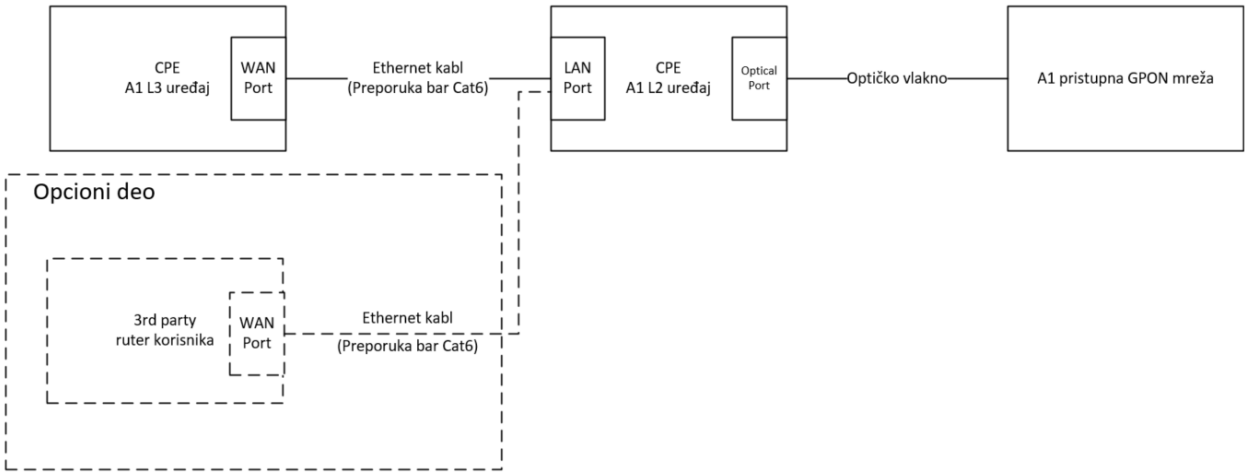
U ovom slučaju ruter kranjeg korisnika, odnosno Pretplatnika (*3rd party* ruter) treba da ispuni sledeće zahteve:

1.	Podrška za podešavanje PPP jedinstvenog korisničkog naloga – korisničko ime i šifra (na zahtev se u ovom slučaju može dostaviti korisniku na siguran način)
2.	Mogućnost VLAN tag-ovanja sa unosom odgovarajućih VLANID-jeva koji će A1 na zahtev korisnika dostaviti
3.	MTU size: 1492 (bytes)
4.	Link Type: PPP
5.	PPP Transfer Type: PPPoE
6.	IP verzija: IPv4

Tabela 1

Opciono: Podrška za podešavanje 802.1p bita i DSCP QoS parametara.

Scenario 2:
A1 CPE L3 + A1 CPE L2



Slika 2

U ovom scenariju ONT funkcionalnost je odvojena od ruter (Layer 3) funkcionalnosti prema slici 2. U slučaju da krajnji korisnik korisnik, odnosno Pretplatnik želi da koristi svoj *3rd party* ruter, krajnji korisnik, odnosno Pretplatnik bi se povezivao u ovom slučaju Ethernet kablom/vezom sa LAN portom A1 L2 uređaja a na strani *3rd party* korisničkog rutera to bi bio WAN port. A1 Srbija L3 CPE se u ovom slučaju ne bi koristio. Konfiguracija 3rd party rutera krajnjeg korisnika, odnosno Pretplatnika bi bila u skladu sa instrukcijama iz Tabele 1 i odgovarajući parametri bi se dostavili na zahtev krajnjeg korsnika, odnosno Pretplatnika na siguran način.

---

4. Zaštita podataka o ličnosti

4.1. Predmet i pravni okvir

Ovaj odeljak definiše tehničke i organizacione mere zaštite podataka o ličnosti koji se obrađuju putem interfejsa u fiksnoj terminalnoj mreži (terminalna tačka mreže – NTP). Mere su usklađene sa važećim propisima o zaštiti podataka o ličnosti (Zakon o zaštiti podataka o ličnosti, "Sl. glasnik RS", br. 87/2018, Zakon o elektronskim komunikacijama, "Sl. glasnik RS", br. 35/2023) i sa preporukama iz standarda SRPS TR 101 730 i SRPS TR 101 731.

4.2. Vrste podataka o ličnosti na interfejsu

Kroz interfejs u fiksnoj terminalnoj mreži mogu se prenositi i/ili obrađivati sledeće kategorije podataka o ličnosti Pretplatnika:

- identifikacioni i kontakt podaci (npr. pretplatnički broj, identifikatori korisničke opreme: MAC adresa, IP adresa, korisničko ime za pristup usluzi);
- podaci o saobraćaju (npr. datum i vreme uspostavljanja i prekida veze, trajanje veze, obim prenesenih podataka, odredišni i izvorišni brojevi/adrese);
- sadržaj komunikacije, u meri u kojoj se prenosi preko interfejsa (npr. govorna komunikacija, podaci, multimedija), pri čemu operator nema pravo uvida u sadržaj, osim u slučajevima izričito propisanim zakonom.

4.3. Tehničke mere zaštite

4.3.1. *Logičko odvajanje i zaštita saobraćaja*

Na interfejsu se obezbeđuje logičko odvajanje saobraćaja različitih korisnika (npr. primenom VLAN-ova, PPPoE sesija i drugih mehanizama segmentacije), tako da nije moguće neovlašćeno presretanje ili pristup saobraćaju drugih korisnika. Konfiguracija interfejsa se vrši na način koji sprečava nenamerno mešanje saobraćaja više korisnika u istu broadcast ili kolizionu domenu, osim kada je takav rad izričito definisan uslugom i odgovarajuće zaštićen posebnim mehanizmima.

1.3.2 Kontrola pristupa i autentifikacija
Pristup mreži preko interfejsa uslovljen je autentifikacijom korisnika i/ili krajnje opreme, u skladu sa vrstom usluge i arhitekturom mreže (npr. autentifikacija putem PPPoE naloga, 802.1X, sistemskih naloga ili drugih prihvaćenih mehanizama). Parametri autentifikacije se čuvaju i obrađuju kao poverljivi i ne smeju se prenositi u otvorenom obliku preko nezaštićenih kanala ukoliko je raspoloživ bezbedniji mehanizam.

4.3.2. Poverljivost i integritet podataka

Interfejs je projektovan tako da omogući primenu kriptografskih i drugih bezbednosnih mehanizama na višim slojevima, čime se korisniku omogućava da obezbedi poverljivost i integritet svojih podataka o ličnosti. Operator, u skladu sa SRPS TR 101 730 i SRPS TR 101 731, obezbeđuje da implementacija interfejsa ne sprečava ili ne ograničava neophodnu primenu ovih mehanizama, izuzev u slučajevima kada je za to postojanje ograničenje izričito definisano i obrazloženo (npr. specifične tehničke usluge).

4.3.3. Zaštita od zloupotrebe i neovlašćenog pristupa

Na interfejsu i odgovarajućim mrežnim elementima primenjuju se mere zaštite od tipičnih oblika zloupotrebe (npr. spoofing, neovlašćeno preuzimanje identiteta, pokušaji presretanja komunikacije), u skladu sa smernicama iz SRPS TR 101 730 i SRPS TR 101 731. Saobraćaj koji ukazuje na pokušaje neovlašćenog pristupa, manipulacije signalizacijom ili narušavanje integriteta mreže može biti ograničen ili blokiran, uz vođenje odgovarajuće evidencije u svrhu analize i reagovanja na bezbednosne incidente.

A1 ne garantuje krajnjem korisniku, odnosno Pretplatniku:

a) da prilikom pružanja Usluga datoteke preuzete sa interneta ne sadrže neki od računarskih virusa („trojanci", worms, rootkits, spyware, bots, backdoors i sl.) ili elemente drugih malicioznih računarskih programa, koji uzrokuju loše funckonisanje uređaja i/ili Usluge, niti je A1 odgovoran Pretplatniku za bilo kakvu pričinjenu eventualnu štetu;
b) sigurnost i tačnost informacija, koje Pretplatnik razmenjuje sa ostalim korisnicima Interneta.

A1 nije odgovoran krajnjem korisniku, odnosno Pretplatniku:

a) za povredu prava na privatnost i sigurnost Pretplatnika, koju preko Interneta učini treće lice;
b) za štetu, pričinjenu Pretplatniku ili trećem licu usled povrede obaveze Pretplatnika na čuvanje tajnosti podataka o svom korisničkom nalogu, kao ni za štetu koju Pretplatnik svojim ponašanjem na internetu prouzrokuje trećima licima;
c) ako je kvalitet pružene Usluge manji od ugovorenog zbog toga što Pretplatnik nije zaštitio svoj pristup Mreži od neovlaščenog pristupa trećih lica.

4.3.4. Evidentiranje (logovanje) i zadržavanje podataka

Sistemi koji upravljaju terminalnim interfejsom vode tehničke evidencije o relevantnim događajima (npr. uspostavljanje i prekid sesija, neuspele autentifikacije, neuobičajen saobraćaj), u meri neophodnoj za:

- obezbeđivanje ispravnog funkcionisanja usluge,
- otkrivanje i rešavanje incidenata bezbednosti,
- ispunjenje zakonom propisanih obaveza zadržavanja podataka o saobraćaju.

Obim i rokovi čuvanja ovih podataka definišu se internim politikama operatora i važećim propisima, pri čemu se primenjuje načelo minimizacije i ograničenja rokova čuvanja.

4.4. Organizacione mere zaštite

4.4.1. Ograničenje pristupa i poverljivost

Pristup konfiguraciji interfejsa i povezanim podacima o ličnosti dozvoljen je isključivo ovlašćenim licima operatora, u skladu sa definisanim ulogama i nivoima ovlašćenja. Sva ovlašćena lica imaju

obavezu čuvanja poverljivosti u skladu sa zakonom, internim aktima operatora i preporukama iz SRPS TR 101 730 i SRPS TR 101 731. Administratorski pristup mrežnim elementima vrši se isključivo preko zaštićenih kanala (npr. SSH, VPN) uz upotrebu personalizovanih naloga.

4.4.2. Svrha obrade i minimizacija

Podaci o ličnosti koji se obrađuju putem interfejsa koriste se isključivo za jasno definisane svrhe: pružanje i održavanje usluge, naplata, obezbeđivanje kvaliteta i bezbednosti usluga, ispunjenje zakonskih obaveza i postupanje po zahtevima nadležnih organa u skladu sa zakonom. U skladu sa SRPS TR 101 730 i SRPS TR 101 731, primenjuje se načelo minimizacije podataka: operator obrađuje samo one podatke koji su nužni za ostvarenje navedenih svrha.

4.5. Postupanje u slučaju bezbednosnih incidenata

U slučaju otkrivanja bezbednosnog incidenta na interfejsu koji može dovesti do povrede podataka o ličnosti (npr. neovlašćen pristup, presretanje ili izmene saobraćaja), operator primenjuje definisane procedure:

- hitna tehnička stabilizacija i ograničavanje posledica,
- evidentiranje incidenta i analiza uzroka,
- preduzimanje korektivnih i preventivnih mera,
- postupanje u skladu sa važećim propisima o obaveštavanju nadležnog nadzornog organa, kao i, po potrebi, informisanje korisnika na koje se incident odnosi.