

DOI: [10.46793/CIGRE37.D2.14](https://doi.org/10.46793/CIGRE37.D2.14)**D2.14****РАЗМАТРАЊЕ МОГУЋНОСТИ РЕАЛИЗАЦИЈЕ РЕЗЕРВНОГ ПУТА
ЗА ПРЕНОС СИГНАЛА ТЕЛЕЗАШТИТЕ КОРИШЋЕЊЕМ MPLS ПРОТОКОЛА****FEASIBILITY ANALYSIS OF IMPLEMENTING A REDUNDANT TELEPROTECTION
LINK OVER MPLS****Iva Salom*, Milenko Kabović, Vladimir Čelebić, Anka Kabović, Jovana Vuleta-Radoičić,
Srđan Mitrović**

Кратак садржај – Распољивост преносног пута је један од кључних захтева за пренос сигнала телезаштите, који омогућава поуздан и брз пренос. Висока располољивост подразумева и увођење оптималног резервног пута узимајући у обзир нове комуникационе технологије и њихову примену у телекомуникационим системима електроенергетских компанија у свету и код нас. Последњих година развој нових комуникационих технологија доводи до преласка са SDH/SONET на пакетске мреже, које нуде флексибилније коришћење ресурса. Етернет протокол има ограничења у преносу критичних сигнала, па се MPLS (*Multi-Protocol Label Switching*) све више користи за ефикасно управљање телекомуникационим саобраћајем електроенергетских компанија. Овај рад, поред описа карактеристика IP-MPLS, MPLS-TE и MPLS-TP протокола, анализира ове протоколе као могућа решења за реализацију резервног преносног пута сигнала телезаштите, уз приказ искустава из неколико земаља, као и могућности имплементације у ЕМС АД у складу са постојећом телекомуникационом мрежом и плановима за реконструкцију.

Кључне речи – телезаштита, телекомуникациона мрежа, IP-MPLS, MPLS-TE, MPLS-TP

Abstract - The availability of the transmission path is one of the key requirements for teleprotection signal transmission, ensuring reliable and fast transmission. High availability also implies utilization of an optimized redundant link, considering new communication technologies and their application in the telecommunication systems of power utilities worldwide and in our region. In recent years, the development of new communication technologies has led to a transition from SDH/SONET to packet-switched networks, which offer more flexible resource utilization. The Ethernet protocol has limitations in transmitting critical signals, thus MPLS (*Multi-Protocol Label Switching*) is increasingly used for efficient traffic management in power utility telecommunications. This paper, in addition to describing the characteristics of IP-MPLS, MPLS-TE, and MPLS-TP protocols, analyzes these protocols as potential solutions for implementing a redundant teleprotection link.

* iva.salom@pupin.rs, Институт Михајло Пупин, Волгина 15, Београд

It also presents experiences from several countries and examines the possibilities of implementation within EMS JSC, in line with the existing telecommunication network and reconstruction plans.

Keywords – *teleprotection, telecommunication network, IP-MPLS, MPLS-TE, MPLS-TP*

1 УВОД

Телекомуникациони систем припада категорији инфраструктурних система електропривреде, који омогућава пренос података обезбеђујући различите телекомуникационе сервисе, који се деле на пословне (пословна телефонија, пренос пословних података и сл.) и оперативне (критичне) сервисе, који представљају специфичност електропривредних у односу на јавне системе. Имајући у виду строге захтеве за критичне сервисе пре свега у смислу поузданости и брзине преноса, телекомуникационе мреже електропривредних система су стандардно базиране на технологији комутације кола (*circuit switched*) са успостављањем фиксног пута кроз мрежу за повезивање уређаја, док се већи број сервиса истовремено преноси у посебним каналима у оквиру временског мултиплекса (TDM – *Time Division Multiplex*). Кроз успостављени комуникациони канал и дефинисане ресурсе у мрежи, TDM обезбеђује константан проток и константно кашњење. Са друге стране, овакво искоришћење ресурса је веома неефикасно, посебно у случајевима саобраћаја који се одвија спорадично. Типичне мреже овог типа које се користе у електропривредним системима су SDH/SONET мреже [1].

Како се мењају и повећавају захтеви система, посебно увођењем нових технологија (пре свега у контексту примене стандарда IEC 61850 [2]), а истовремено услед технолошке застарелости и скупог одржавања постојеће SDH/SONET опреме, електропривредни системи се глобално суочавају са неминовношћу миграције са TDM мрежне структуре на пакетске мреже [3]-[6]. Пакетска (*packet switched*) комуникација реализује се Етернет протоколом, који припада другом слоју OSI комуникационог модела (*Layer 2*). Етернет је у основи комуникација без успоставе везе (*connectionless*), и захваљујући томе омогућава ефикасније искоришћење ресурса. Међутим, за разлику од мрежа базираних на комутацији кола (SDH/SONET), који свакој апликацији додељују унапред одређени комуникациони капацитет и обезбеђују задато време преноса, изворни Етернет се заснива на систему прослеђивања пакета у датом тренутку доступним путањама у мрежи, чиме пре свега није загарантовано време преноса пакета, као ни поузданост (у случају загушења мреже). Унапређење пакетских мрежа, увођењем VLAN (*Virtual Local Area Network*) мрежа, које су омогућиле раздвајање саобраћаја и додељивање приоритета порука, омогућено је значајно смањење времена преноса пакета и већа поузданост, али фиксно кашњење и варијације кашњења и даље нису гарантовани [1].

MPLS (*Multi-Protocol Label Switching*) протокол је врста пакетске комуникације [7]-[11], која захваљујући уведеним лабелама (ознакама) фиксне дужине у оквиру пакета, пре свега омогућава брже прослеђивање пакета кроз мрежу, али и ефикасно управљање саобраћајем избором путање, која не мора нужно бити најисплативија (*least cost path*), као код IP рутирања (*Internet Protocol, OSI Layer 3*), што омогућава максимално коришћење расположивог пропусног опсега између рутера [12]. Осим тога, MPLS може да каналише (тунелује) различите типове порука кроз мрежу, што помаже не само оптимизацији мреже већ и њеној безбедности [13]. Захваљујући овим карактеристикама, MPLS протокол је постао *de facto* нови стандард за телекомуникациону инфраструктуру у електропривредним системима [4], пре свега за пренос критичних сервиса. Како је у основи MPLS протокола изворно била IP технологија.

Овај протокол се често назива и IP-MPLS протокол [4], а касније су се издвојиле и друге врсте MPLS протокола, као што су MPLS-TE (MPLS *Traffic Engineering*) и MPLS-TP (MPLS *Transport Protocol*). MPLS-TP има потенцијала да директно одговори на сложене захтеве и техничке изазове преноса података у електропривреди.

Иако се у овом тренутку као главни телекомуникациони систем и даље користи SDH, у складу са поменутиим трендовима електропривредних компанија у свету, EMC АД је започео увођење DWDM (*Dense Wavelength Division Multiplexing*) система, а средином 2022. године је почела реализација прве фазе додатне DWDM опреме уз примену IP-MPLS технологије [13]. Уз то, очекује се примена доступних SDH/PDH мултиплексера и MPLS-TP опреме у оквиру пројеката прикључења објеката на преносни систем и изградње нових објеката [15].

Телезаштита представља један од критичних сервиса у електропривредном систему, којим се врши координација деловања заштите на крајевима појединих водова високог напона. Пренос сигнала телезаштите мора да испуни високе захтеве у погледу перформанси система телезаштите (висока поузданост, сигурност и расположивост, време преноса мање од 10 ms) према стандарду IEC 60834-1 [16]. Због захтева за високом расположивости намеће се потреба коришћења резервног пута за пренос телезаштитних порука. У складу са техничким нормативима EMC АД, главни пут преноса се реализује оптичким влакнима (превасходно OPGW – *Optical Ground Wire*), док се реализација резервног пута за пренос сигнала телезаштите може остварити на више начина. Имајући у виду унапређење пакетске комуникације, имплементиран је пренос сигнала Етернетом преко SDH (*Ethernet over SDH* – EoSDH) и постигнути су задовољавајући резултати по питању брзине преноса (око 4 ms) и преласка са главног на резервни пут, и обрнуто (испод 2 ms) [17].

У складу са поменутиим глобалним тенденцијама преласка на MPLS технологију у електропривредним системима, испитивање могућности примене MPLS протокола за пренос сигнала телезаштите је веома актуелно [3]-[5],[18]-[34]. Актуелна истраживања и имплементирани MPLS системи у свету, указују на потребу детаљног разматрања ове теме. У раду ће бити приказане основне карактеристике IP-MPLS протокола, као и две врсте MPLS-TE и MPLS-TP, као могућих протокола за реализацију резервног пута за сигнале телезаштите. Након теоријског увода, биће приказана основна испитивања у неколико земаља. На основу сагледавања свих резултата, као и реализоване телекомуникационе мреже у оквиру EMC АД, као и планова развоја, треба да буду разматране могућности имплементације резервног пута за пренос сигнала телезаштите коришћењем MPLS протокола у EMC АД.

2 ПРИНЦИПИ MPLS ПРОТОКОЛА

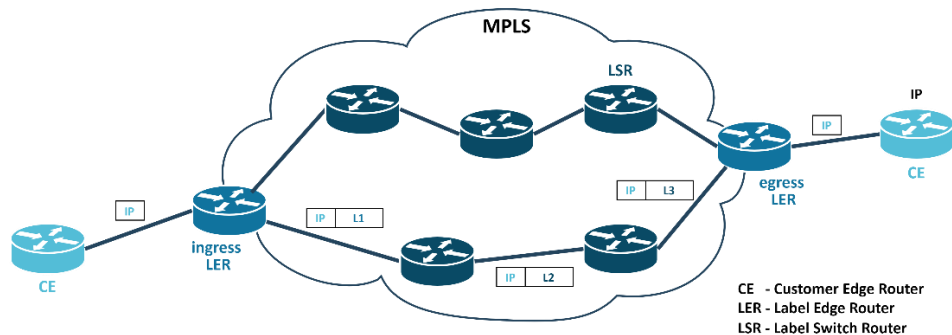
MPLS протокол је развијен 1990-тих година најпре због потребе да се повећа брзина прослеђивања IP пакета кроз мрежу на основу претраживања *lookup* табела рутирања, увођењем лабела фиксне дужине као кључног концепта у свету виртуелних мрежа [1],[9]-[11]. *Internet Engineering Task Force* (IETF) је објединио постављене захтеве у MPLS протокол [6],[8]. Иако су технологија и карактеристике хардвера напредовали у међувремену и брзине прослеђивања IP пакета су се готово изједначиле са брзинама прослеђивања пакета кроз MPLS мрежу, могућност контроле рутирања саобраћаја у мрежи ради управљања капацитетом, додељивања приоритета различитим сервисима и спречавања загушења MPLS протокола издвајају га као нови стандард у оквиру мрежних технологија. Посебно је значајно што је MPLS скалабилна технологија преноса са успоставом везе пре слања података (*connection-oriented*) [9].

Скалабилност подразумева једноставно проширење и надоградњу мреже повећањем капацитета линкова и/или додавањем нових чворова и линкова у мрежи.

Концепт MPLS протокола је приказан на слици 1. Рутери који представљају интерфејс ка MPLS мрежи називају се LER (*Label Edge Router*) рутери, и у зависности од смера слања пакета могу бити улазни (*ingress LER*) или излазни (*egress LER*). Улазни LER рутер прима пакет са одредишном IP адресом, додељује (*push*) лабелу (L1 на слици 1) и утврђује којој класи FEC (*Forwarding Equivalence Class*) припада. FEC је заправо скуп пакета који се прослеђују кроз MPLS мрежу истим путем (LSP – *Label-Switched Path*) иако им одредишне адресе не морају бити исте. LSP, дакле, одређује улазни LER рутер када утврди FEC класу. Захваљујући уведеној лабели, цела анализа путање прослеђивања пакета се врши само једном на улазу у MPLS мрежу, а даље унутар мреже врши се само прослеђивање на основу задате лабеле.

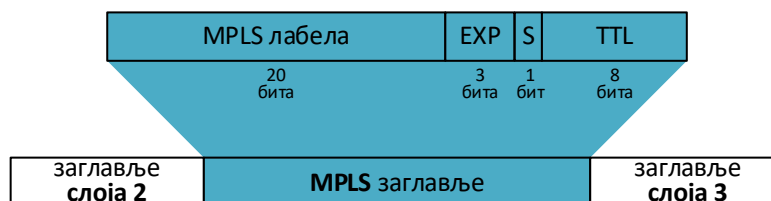
Рутери који прослеђују пакете са лабелама кроз MPLS мрежу називају се LSR (*Label Switch Router*) рутери. У примеру прослеђивања пакета, приказаном на слици 1, LSR рутер чита лабелу L1 коју је доделио LER рутер, мења (*swap*) лабелу другом лабелом (у примеру са слике, лабелом L2), која одређује следећи LSR рутер коме се пакет прослеђује. Овај процес се понавља све док пакет не стигне до излазног LER рутера, који одбацује (*pop*) лабелу из пакета и прослеђује га даље, користећи стандардну IP процедуру прослеђивања пакета. Сам LSR не складишти руте по IP шеми прослеђивања, чиме се побољшава скалабилност мреже. Додавање више лабела у стеку омогућава различите начине преноса пакета, на пример тунеловање. Различите врсте саобраћаја могу делити један LSP, а ако постоје довољни ресурси, један LSP може да преноси сав саобраћај без обзира на његов тип.

У складу са стандардном мрежном архитектуром, улога контролне равни код MPLS мреже је додељивање лабела, креирање табела прослеђивања лабела и успостављање и уклањање LSP путања. Раван података за пренос података користи OSI слој 2, и одговорна је за додавање и уклањање лабела, као и прослеђивање пакета на основу LFIB (*Label Forwarding Information Base*) [12]. У равни података, лабеле се додељују сваком LER и LSR рутеру ради проналажења најбоље LSP путање. Контролна равна дистрибуира информације о лабелама. Постоји више приступа за извлачење информација из MPLS заглавља [9]. Први приступ користи протокол за дистрибуцију лабела (*Label Distribution Protocol* – LDP). LDP користи информације за рутирање, али не зависи ни од једног протокола за рутирање [35]. Други приступ је врста проширеног LDP протокола, протокол за резервацију ресурса (*Resource Reservation Protocol* – RSVP) на чворовима дуж пута [35]. RSVP ради на транспортном нивоу, али не учествује у преносу апликативних података [35]. LDP омогућава једноставну конфигурацију, одржавање сесија и поуздан пренос пакета. У оквиру RSVP протокола, LDP је проширен како би омогућио креирање и одржавање LSP путања и резервисање пропусног опсега. LDP је пожељнији у погледу почетне конфигурације и скалабилности. Међутим, RSVP је бољи за миграцију са OSI слоја 2 на MPLS мрежу. Трећи приступ је MP-BGP (*Multiprotocol Border Gateway Protocol*), проширена верзија BGP протокола, који представља скуп правила који одређују најбољу руту за пренос података у мрежи. MP-BGP се користи за размену VPN (*Virtual Private Network*) лабела.



Слика 1: Концепт MPLS протокола

MPLS заглавље, које садржи лабелу MPLS протокола, његову главну карактеристику, уведено је између заглавља OSI слоја 2 (*Layer 2*) и слоја 3 (*Layer 3*), због чега се често каже да MPLS припада слоју 2,5 [12]. На слици 2 приказан је изглед MPLS заглавља са пољима од којих се састоји [8]. MPLS лабела је величине 20 бита. EXP је поље величине 3 бита за експерименталну употребу, које је тренутно везано за организацију редова за чекање и специфицира класу сервиса (CoS – *Class-of-Service*) пакета, информацију која је круцијална за постизање задатог квалитета сервиса QoS (*Quality-of-Service*). S бит (*Bottom-of-Stack*) има вредност 0 ако иза тренутне лабеле постоји још лабела, односно 1, ако је тренутна лабела последња на стеку. TTL (*Time to Live*) је поље од 8 бита, чија је главна функција избегавање заглављивања пакета у рутинаној путањи, а и када се то деси захваљујући овом пољу зна се место (рутер) на коме је настао проблем. Наиме, IP пакет иницијално, на месту генерисања пакета, обично поставља вредност TTL поља на 255, и затим се декрементира при сваком скоку. Када IP пакет уђе у MPLS мрежу на улазном LER рутеру вредност TTL поља из IP пакета се стандардно декрементира и копира у TTL поље MPLS заглавља. Када пакет стигне са TTL вредношћу 0, LSR који га је примио одбацује пакет и шаље поштом IP пакета ICMP (*Internet Control Message Protocol*) поруку „време је истекло“ (тип 11, код 0). Генерално, рутер у мрежи се понаша на исти начин када прими IP пакет са вредношћу 0 у TTL пољу. Опционо, корисник може да конфигурише LSR тако да не декрементира MPLS TTL вредност при сваком пролазу.



Слика 2: MPLS заглавље у пакету [9]

2.1 MPLS-TE

Управљање саобраћајем (TE – *Traffic Engineering*) је скуп метода којима се оптимално искоришћавају ресурси мреже, са основном идејом да се омогући прослеђивање пакета на основу топологије мреже, скупа ограничења и расположивих ресурса. Примарни циљ управљања саобраћајем је минимизација загушења. Загушење најчешће настаје из два разлога: недовољни мрежни ресурси и неефикасно мапирање саобраћаја на доступне ресурсе. Проблем загушења мреже може се решити проширењем капацитета мреже или коришћењем класичних техника контроле загушења, као што су ограничавање брзине преноса података, контрола токова и сл. Управљање саобраћајем се врши током преусмеравања саобраћаја како би се осигурало да се подаци ефикасно прослеђују [9].

У MPLS мрежи управљање саобраћајем је уведено као посебна технологија MPLS-TE како би се избегла загушења мреже и побољшао QoS, кроз минимизацију губитка пакета и кашњења, максимизацију пропусног опсега и подршка спровођењу SLA (*Service Level Agreement*) [36].

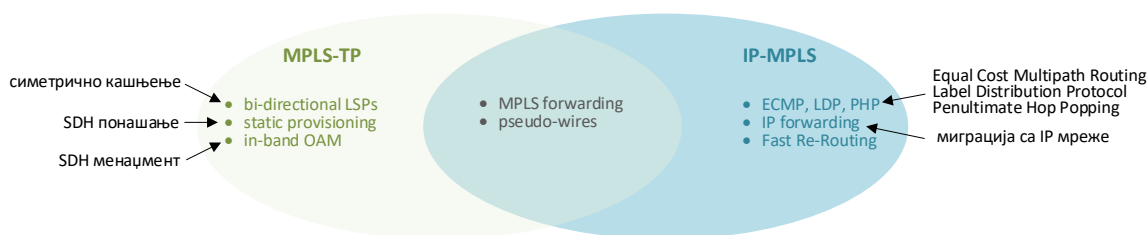
MPLS-TE врши анализу топологије мреже и расположивих ресурса, а затим на основу тога мапира токове саобраћаја кроз успостављање LSP путања и транспарентно преноси саобраћај кроз њих. У случају недостатка ресурса, LSP са вишим приоритетом (што је специфицирано у MPLS заглављу) може преузети пропусни опсег LSP са нижим приоритетом како би се задовољили захтеви сервиса са већим приоритетом. Поред тога, у случају отказивања LSP или загушења у мрежном чвору, MPLS-TE обезбеђује заштиту применом технике брзе промене путање (FRR – *Fast Reroute*) и резервне путање.

2.2 MPLS-TP

MPLS-TP је варијанта MPLS технологије прилагођена транспортним мрежама, која обезбеђује унапред дефинисане тунеле између приступних тачака сервиса. Ова адаптација MPLS технологије, уведена од стране IETF и ITU [37], подржава традиционалне захтеве транспортних мрежа, као што су висока расположивост и QoS, који су до сада били испуњени SDH/SONET технологијама [1],[6],[9]. Фокусирањем на транспортни домен, MPLS-TP користи само подскуп MPLS технологије, задржавајући предности, као што је прослеђивање пакета на основу додељених лабела, елиминишући непотребне функције и њихову сложеност и додајући недостајуће механизме неопходне за транспортне мреже. Један од тих механизма је OAM (*Operations, Administration, and Maintenance*) сигнализација на различитим нивоима повезаности, слична оној у SDH/SONET мрежама [1].

MPLS-TP раздваја мрежу између крајњих корисника на два сегмента: корисничку (апликативну) мрежу и транспортну мрежу. Транспортна мрежа обезбеђује услуге тачка-тачка познате као „псеудо-жице“ (*pseudo-wires*), које преносе Етернет сервисе (*E-line* или *E-LAN Carrier Ethernet* услуге) и традиционални TDM преко мреже са пакетском комутацијом (*TDM Pseudowire Emulation*) [1].

Иако MPLS-TP технологија због фиксне структуре тунела није погодна за велике телекомуникационе операторе који покривају крајње кориснике, што постаје непрактично за велики број крајњих тачака и услуга, за електропривредне системе MPLS-TP представља обећавајућу технологију, јер обезбеђује све функционалности постојећих SDH/SONET система, компатибилан је са корпоративним мрежама, као што је IP-MPLS, и уводи нове могућности уз коришћење сличних процеса управљања, које електропривредне компаније већ поседују [1]. Поређење IP-MPLS и MPLS-TP технологија приказано је на слици 3.



Слика 3: Поређење IP-MPLS и MPLS-TP технологија [1],[9]

3 MPLS ПРОТОКОЛИ У ЕЛЕКТРОПРИВРЕДИ

Иако постоји све већа тежња ка преласку на MPLS технологије, ипак је примена ове технологије у електропривредним системима и даље предмет расправа. Док је IP-MPLS технологија зрелија, и чак примењена у неким сегментима, тежи се ка што безболнијем преласку на MPLS-TP технологију због свих наведених предности. У оквиру електропривредних система увођење MPLS технологија није потпуно нов задатак, већ је постао део плана трансформације мреже. Као што је већ речено, већина телекомуникационих мрежа је у овом тренутку базирана на SDH/SONET мрежама, пре свега због временски критичних сервиса, као што је телезаштита. Синхрони протоколи, који се користе у овим мрежама, као што је E12 протокол, морају бити емулирани у новим пакетским мрежама. Управљање телекомуникационом мрежом у електропривредним компанијама се спроводи кроз централизоване платформе, које су прилагођене постојећим мрежама. У том контексту, MPLS-TP се чини као прикладнија технологија од IP-MPLS, чак укључујући и управљање саобраћајем (TE) [1]. Овде ће бити сумиране главне предности MPLS-TP технологије.

- **Потпуна контрола над мрежом** – Код MPLS-TP мрежа лабеле генерише централни систем за управљање мрежом (NMS – *Network Management System*), омогућавајући дефинисање главних и алтернативних путања између крајњих тачака, као у SDH/SONET мрежама. Код IP-MPLS мрежа исправан рад мреже зависи од комуникације у контролној равни. Ако је неопходно детерминистичко понашање за одређене токове података, мора се увести одговарајуће управљање саобраћајем како би се регулисале одлуке у чворовима у мрежи.
- **Квалитет услуге и детерминистичко понашање.**
- **Величина мреже и тип саобраћаја** – MPLS-TP, због свог понашања сличног SDH/SONET мрежама, испуњава све постојеће захтеве за сервисе, али и омогућава нове пакетске услуге у мрежама, на нивоу величине електроенергетских компанија.
- **Могућности у односу на сложеност** – IP-MPLS пружа бројне техничке могућности, али уз повећану сложеност. Имплементација QoS кроз динамичку резервацију ресурса (RSVP) може се реализовати у IP-MPLS мрежи, али није једноставан задатак применити га на великом броју конекција.
- **Миграција са SDH/SONET мрежа** – Прелазак на пакетске мреже за електропривредне компаније које имају обимну SDH/SONET инфраструктуру, алате за управљање и знања скоро је безболан у случају MPLS-TP мреже, јер се уклапа у постојећи систем управљања. С друге стране, IP-MPLS представља потпуно другачији модел рада, што захтева значајније промене у начину управљања мрежом.

3.1 Телезаштита преко MPLS протокола

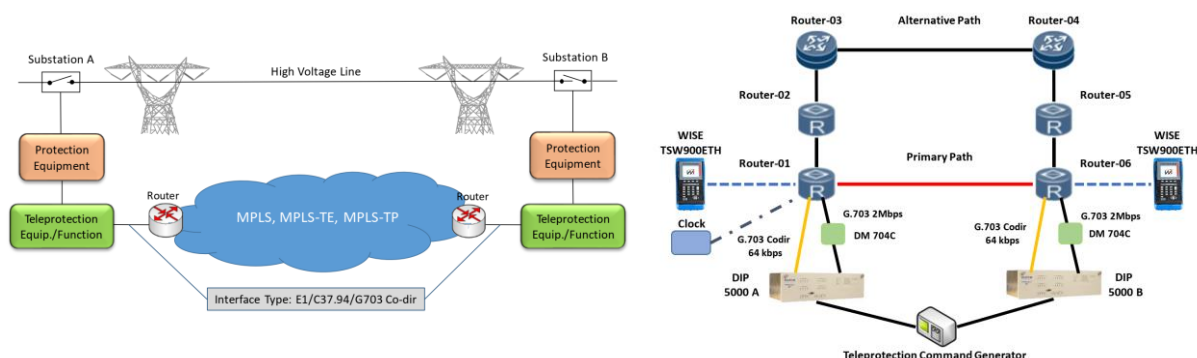
Пренос сервиса у електропривреди историјски је пратио развој телекомуникационих технологија. Еволуција телекомуникационих мрежа данас укључује мрежне протоколе засноване на пакетској комутацији, са имплементацијом функционалности неопходних за критичне сервисе, што је посебно изражено код имплементације MPLS-TP и MPLS-TE протокола. Недавни тестови, објављени литератури, показују да MPLS-TP и MPLS-TE имају значајне предности у односу на стандардни MPLS када је у питању телезаштита [21].

4 ИСКУСТВА И ТЕСТИРАЊА ПРЕНОСА ТЕЛЕЗАШТИТЕ КОРИШЋЕЊЕМ МРЕЖЕ СА MPLS ПРОТОКОЛОМ

У више земаља су обављена испитивања могућности преноса сигнала телезаштите и диференцијалне заштите коришћењем мреже са MPLS протоколом. У овом поглављу су приказани начини мерења и основни резултати добијени тестирањем неколико одабраних испитивања.

4.1 Бразил

У [21] су приказани резултати научно-истраживачког пројекта оператора преносног система Бразила у циљу испитивања преноса сервиса телезаштите преко IP-MPLS мреже у истраживачкој лабораторији овог оператора. Испитивања су спроведена због миграције са TDM на пакетске мреже. Тестови су обухватили практичне имплементације мрежне топологије (прстен и звезда), са различитим процентом загушености мреже, различите сценарије и врсте команди телезаштите (са директним искључењем – *direct tripping*, и са условљеним даљинским искључењем – *permissive tripping*) и испитивање преноса сигнала телезаштите са главним и резервним путем, кроз параметре као што су проток, време преноса и грешке у преносу. Тестови су спроведени са два произвођача мрежне опреме (кодирекциони и E1 интерфејс), који подржавају MPLS-TE и MPLS-TP протоколе. На слици 4 приказани су генерална архитектура мреже за пренос сигнала телезаштите (слика 4a) и конфигурација тест система за испитивање преноса сигнала телезаштите (слика 4b). Резултати тестова су сумирани у табели Табела I.



Слика 4: а) Архитектура мреже за пренос сигнала телезаштите, и б) конфигурација тест система [21]

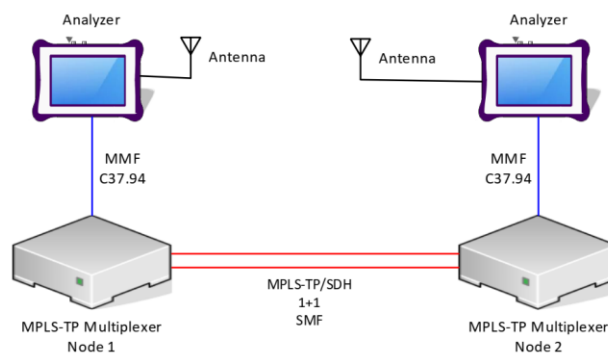
Табела I: Резултати тестова из [21]

Тест	Сценарио	Произвођач	Кашњење [ms] <i>direct tripping</i>	Кашњење [ms] <i>permissive trip</i>	Коментар
1	IP мрежа интерфејс 64 kbps без додатог саобраћаја	A	9,96	7,52	1 ms кашњење G.703 64kbps → E1 (произвођач Б)
		Б	10,96	8,50	
2	IP мрежа интерфејс 64 kbps са додатим саобраћајем	A	9,42	7,48	1 ms кашњење G.703 64kbps → E1 (произвођач Б)
		Б	11,42	8,94	
3	IP мрежа интерфејс 64 kbps без додатог саобраћаја	A	5,75	5,49	1 ms кашњење V.35 → E1 (произвођач А)
		Б	4,61	4,33	
4	IP мрежа интерфејс 64 kbps са додатим саобраћајем	A	5,82	5,55	1 ms кашњење V.35 → E1 (произвођач А)
		Б	4,80	4,50	
5	IP мрежа прекид главног линка	A	~ 0	~ 0	
		Б	~ 0	~ 0	
6	IP мрежа асиметрија преноса	A	0,07	0,08	
		Б	0,03	0,035	

Генерални закључак истраживања је да су добијени резултати упоредиви са преносом сервиса телезаштите TDM мрежама, са препоруком да се испитивања наставе у реалним условима, укључујући специфичности сваке електроенергетске инфраструктуре и шеме заштите.

4.2 Панама и Перу

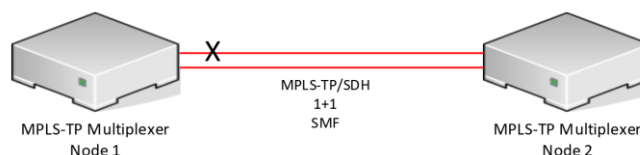
У [28] су приказани резултати лабораторијских и теренских испитивања кашњења у преносу сигнала телезаштите преко хибридне мреже (TDM и пакетска мрежа симултано преко истог оптичког кабла) у конфигурацији са резервним путем, поредећи пренос C37.94 протокола преко SDH и MPLS-TP мреже, као и GOOSE (*Generic Object Oriented Substation Event*) порука диференцијалне заштите. Сprovedени тестови и резултати су приказани на сликама 5 - 7 и табелама Табела II и Табела III. У закључку је истакнуто да тестирани MPLS-TP уређај у испитиваној хибридној конфигурацији омогућава пренос критичних сервиса, као што су телезаштита, диференцијална заштита и пренос GOOSE порука, иако су измерена кашњења нешто већа него у случају SDH мреже. У раду нису експлицитно дати детаљи о томе ко је покренуо истраживање. Један аутор је испред компаније *Grid Resources Inc* (Панама) [38], која се бави решењима у сектору телекомуникационих мрежа за електропривредне системе, укључујући и пренос критичних сервиса преко MPLS-TP мрежа, и обухвата више земаља Централне и Јужне Америке. Други аутор је испред компаније *Nakama Soluciones* (Перу) [39], специјализоване за пружање опреме и услуга за разводна постројења и мреже средњег и високог напонског нивоа.



Слика 5: Мерење кашњења и асиметрије кашњења C37.94 протокола у [28]

Табела II: Резултати тестова кашњења и асиметрије кашњења из [28]

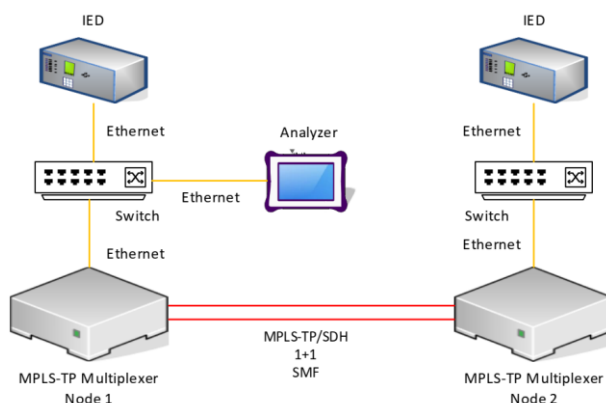
Параметар	SDH			MPLS-TP		
	тренутно	min	max	тренутно	min	max
round-trip кашњење	922 μ s	920 μ s	922 μ s	4.174 ms	4.166 ms	4.187 ms
Tx кашњење	431 μ s	430 μ s	431 μ s	2.182 ms	2.174 ms	2.182 ms
Rx кашњење	491 μ s	490 μ s	491 μ s	1.992 ms	1.992 ms	2.005 ms
Асиметрија	-60 μ s	-60 μ s	-59 μ s	190 μ s	177 μ s	190 μ s



Слика 6: Мерење пребацивања на и са резервног пута у [28]

Табела III: Резултати тестова кашњења и асиметрије кашњења из [28]

Параметар	SDH		MPLS-TP	
	прекид линка	успостава линка	прекид линка	успостава линка
бр. прекида сервиса	1	2	4	3
укупно	1,3 ms	0,6 ms	1,1 ms	1,3 ms
просечно	1,3 ms	0,3 ms	0,3 ms	0,4 ms
min	1,3 ms	0,1 ms	0,1 ms	0,4 ms
max	1,3 ms	0,5 ms	0,8 ms	0,5 ms



Слика 7: Мерење кашњења преноса GOOSE порука у [28];
 приоритет порука је 6, просечно кашњење 809,6 μ s, а максимално кашњење 1,2 ms

4.3 Венецуела

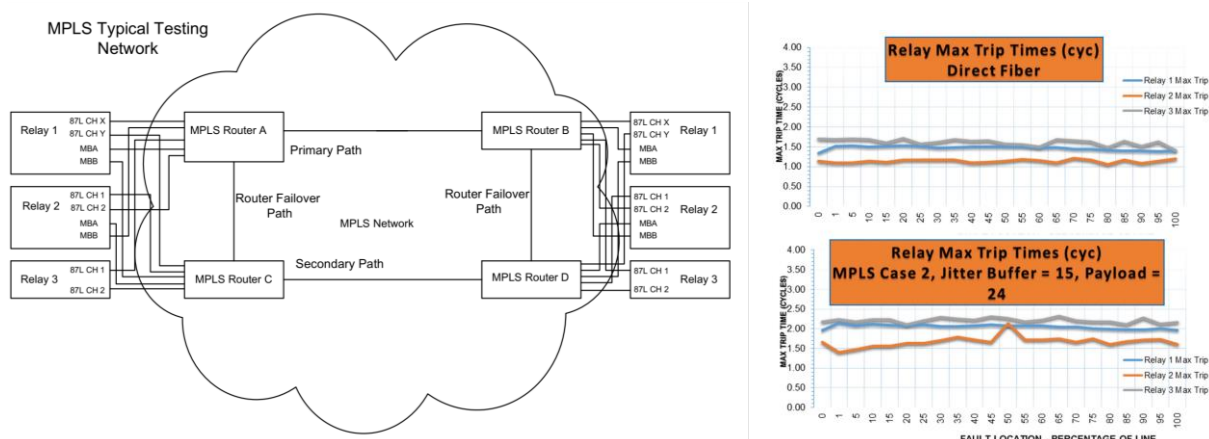
Рад [19] је објављен 2016. године и представља теоријско разматрање примене MPLS-TP протокола за критичне сервисе, као и једноставно лабораторијско поређење преноса сигнала телезаштите уређаја (C37.94) који су директно повезани оптичким каблом (4 ms) и MPLS-TP протоколом преко оптичког кабла (7,5 ms). У закључку је истакнуто да MPLS-TP опрема, која ће бити инсталирана, треба да подржи и постојеће интерфејсе попут E1, STM-1 и C37.94, емулацијом TDM прстенова коришћењем *pseudo-wires* технологије. На тај начин биће створена снажна окосница и приступне могућности за постепену надоградњу постојећих инвестиција до краја њиховог животног века. У међувремену није било информација докле се са овом надоградњом стигло.

4.4 САД

4.4.1 Сан Дијего

San Diego Gas & Electric (SDG&E) [40] је компанија која обезбеђује природни гас и електричну енергију за округ Сан Дијего и јужни део округа Оринџ у југозападној Калифорнији. Да би испитала могућности примене MPLS технологије у електропривреди за пренос сигнала заштите и припремила се за миграцију са T1 протокола преко SONET мреже на MPLS мрежу, SDG&E је спровела лабораторијске тестове са дигиталним симулатором у реалном времену RTDS (*Realtime Digital Simulator*) са заштитиним релеима, MPLS рутерима и MPLS мрежом конфигурисаном за пренос сигнала телезаштите [33]. У извештају [33] су разматрани утицаји асиметрије канала, кашњење, расположивост, пребацивање на резервни пут, и MPLS алати за анализу и отклањање грешака. Приказани лабораторијски тестови су један корак у плану миграције на MPLS мрежу, а следећи корак су инсталације и испитивања у реалним системима, са крајњим циљем да се пренос сигнала телезаштите остварује преко главног пута (наменска оптичка влакна), и резервног пута (MPLS).

На слици 8а приказана је лабораторијска тестна конфигурација, која је обухватила три заштитна релеа диференцијалне заштите (C37.94), и POTT (*Permissive Overreaching Transfer Trip*) шемом заштите. На слици 8 приказани су резултати мерења кашњења између релеа повезаних директно наменским оптичким влакном (горња слика), и преко MPLS мреже (доња слика). Генерално, тестови су показали да је пренос сигнала телезаштите преко MPLS мреже задовољио све захтеве: кашњење < 5 ms, асиметрија кашњења < 2 ms, време пребацивања на резервни пут < 3 ms и расположивост > 99,95%.



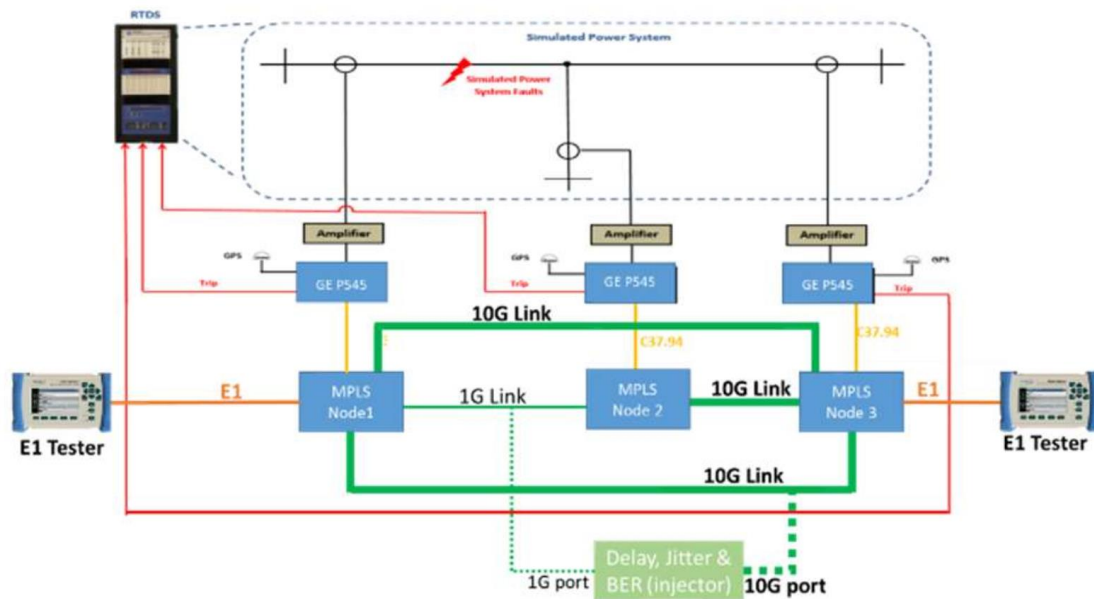
Слика 8: а) Лабораторијска тестна конфигурација. б) резултати мерења кашњења за директно наменским оптичким влакном повезана релеа (горња слика) и преко MPLS мреже (доња слика) у [33]

4.4.2 Тексас

Lower Colorado River Authority (LCRA) [41] је јавно комунално предузеће из Тексаса, које управља снабдевањем водом и производњом и испоруком електричне енергије. LCRA је у периоду од 2013-2018. мигрирала на MPLS мрежу за сервисе као што су SCADA, пренос говора и пословних података, видео надзор, и почела је тестирања размене података између заштитних релеа преко IP-MPLS мреже. Теоријска разматрања са резултатима тестирања за шеме заштите условним искључењем (*permissive tripping*) и диференцијалну заштиту, приказани су у [32]. При томе су тестирања вршена са IP-MPLS уређајима са гигабитним Етернет интерфејсом преко оптичког кабла и SONET мреже. Закључак је да са одговарајућим QoS и временском синхронизацијом IP-MPLS може да се користи за пренос сигнала телезаштите.

4.5 Велика Британија

Испитивања у Великој Британији углавном су спровођена у Глазгову, самостално или у сарадњи са колегама из Аустралије и Белгије. У овом поглављу ће бити представљени резултати самосталног истраживања на универзитету [5], када су вршена поређења параметара преноса сигнала телезаштите IP-MPLS и MPLS-TP технологија, који су обухватили BER (*Bit Error Rate*), пребацивање путања, кашњење и асиметрију кашњења, убацивање грешака и временску синхронизацију. Резултати истраживања су показали да је пренос сигнала телезаштите стабилан и да није било нерегуларности током тестова за обе тестиране телекомуникационе пакетске мреже. За демонстрацију неких од добијених резултата у табели Табела IV приказана су кашњења и асиметрија кашњења за обе мреже.



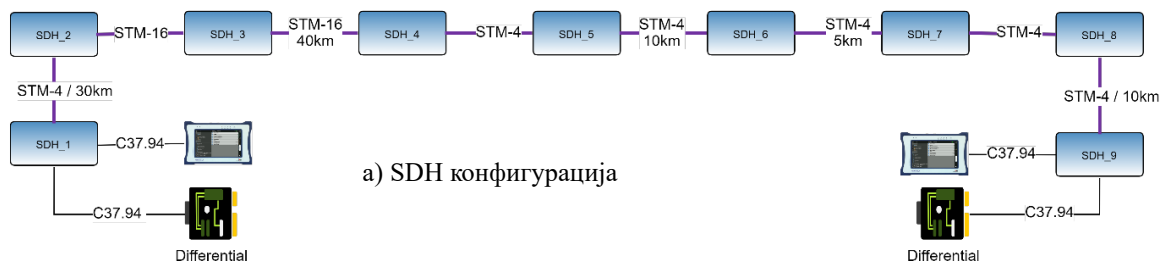
Слика 9: Тест систем у [5]

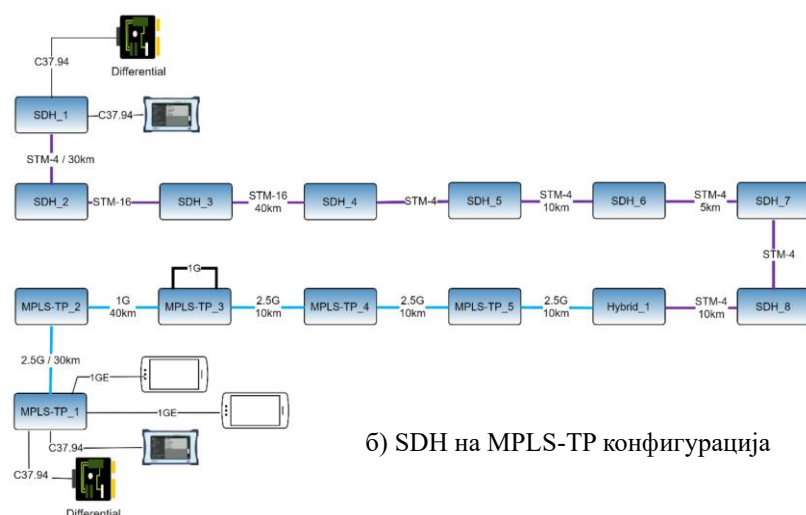
Табела IV: Резултати тестова кашњења и асиметрије кашњења из [5]

IP-MPLS				MPLS-TP			
X.21 [ms]		C37.94 [ms]		X.21 [ms]		C37.94 [ms]	
кашњење	асиметрија	кашњење	асиметрија	кашњење	асиметрија	кашњење	асиметрија
4.61	0.050	5.00	0.010	9.67	0.010	8.98	0.020
4.60	0.005	5.02	0.090	9.64	0.080	8.88	0.030
5.07	0.020	5.07	0.020	9.74	0.130	8.90	0.070

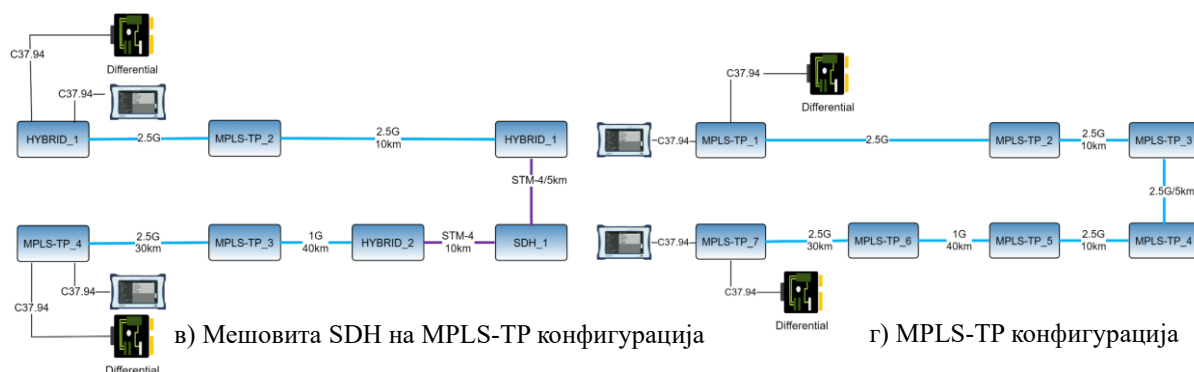
4.6 Финска

Иако је оператер преносног система Финске до тог тренутка користио искључиво C37.94 2Mbps везе преко SDH за пренос телезаштите и диференцијалне заштите, у оквиру техничког програма *Paris CIGRE 2024*. године представљена су два рада [27],[29], у којима су описани спроведени тестови и резултати поређења преноса сигнала заштите C37.94 протоколом преко различитих комбинација телекомуникационих мрежа, као што је приказано на слици 10. Резултати тестова су дати у табели Табела V.





б) SDH на MPLS-TP конфигурација



в) Мешовита SDH на MPLS-TP конфигурација

г) MPLS-TP конфигурација

Слика 10: Комбинације конфигурације телекомуникационе мреже приликом тестирања преноса сигнала заштите у [27]

Табела V: Резултати тестова из [27]

Параметар	SDH	SDH на MPLS-TP	SDH и MPLS-TP	MPLS-TP
Број скокова	8	13	6	6
Асиметрија	< 50 μ s	< 50 μ s	< 50 μ s	< 50 μ s
Диференцијална заштита мерено кашњење				
Rx	1,047 ms	1,881 ms	1,598 ms	1,010 ms
Tx	1,047 ms	1,881 ms	1,598 ms	1,010 ms
C37.94 мерени параметри				
Rx кашњење	0.950 ms	1.785 ms	1.507 ms	0.933 ms
Tx кашњење	0.963 ms	1.833 ms	1.509 ms	0.933 ms
асиметрија	13 μ s	48 μ s	0 – 2 μ s	0 – 2 μ s
варијација асиметрије	1 μ s	1 μ s	2 μ s	2 μ s
MPLS-TP (OAM DM) мерено кашњење	NA	NA	NA	0.52 ms
Rx				0.52 ms
Tx				

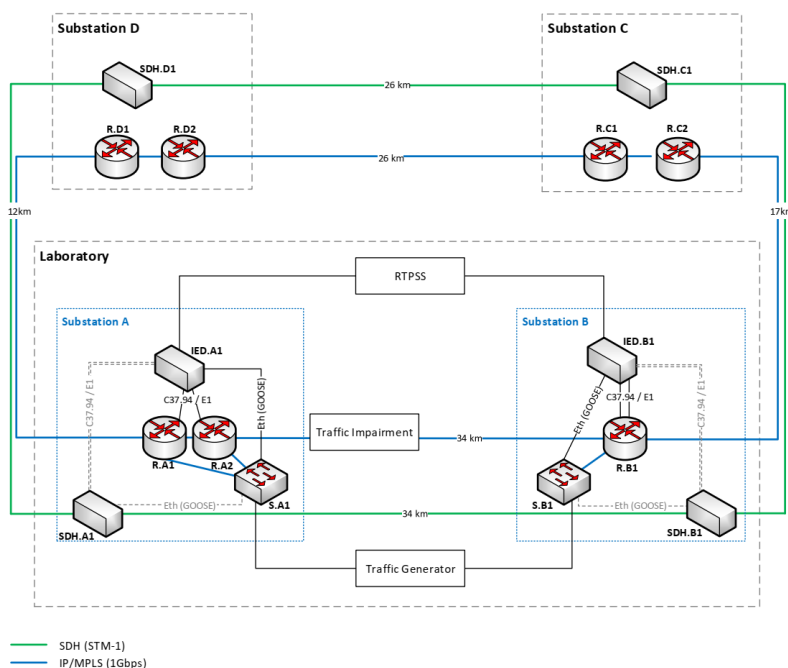
Закључци изнети у [27] махом се односе на компликоване процедуре подешавања, тумачења и тестирања уређаја у MPLS-TP мрежи, подложне људској грешци. Конкретни закључци изнети су у [29]. Резултати тестирања доказују да се пажљивим пројектовањем телекомуникационих сервиса на основу C37.94 стандарда и коришћењем већег броја C37.94 канала може смањити време преноса телезаштитног сигнала и време активирања диференцијалне заштите.

Хибридна имплементација SDH – MPLS-TP технологије може донети уштеде и олакшати миграцију електропривредним компанијама, јер се потреба за заменом и редизајном телекомуникационе опреме и мреже може свести на минимум. Нове технологије и пакетске мреже пружају додатне могућности, као што је коришћење PTP (*Precision Time Protocol*) синхронизације за детекцију асиметрије, али је важно разумети да нове функционалности повећавају сложеност када је у питању конфигурација, рад и надзор телекомуникационе мреже, у поређењу са старијим SDH мрежама, где такве функционалности нису биле неопходне због поузданије комуникације. Надзор заснован на сервисима је обавезан у свим телекомуникационим мрежама које преносе временски критичне сервисе, као што је телезаштита.

4.7 Португал

Суочен са преласком са PDH/SDH на пакетске мреже, и чињеницом да произвођачи заштитних релеа још увек немају поуздано решење за пренос сигнала заштите пакетским мрежама, оператер преносног система у Португалу је у сарадњи са истраживачким центром покренуо пројекат са циљем да се испита могућност примене IP-MPLS мреже за пренос сигнала заштите [24]. За потребе пројекта је имплементирана тест платформа са симулатором енергетског система у реалном времену, генераторима саобраћаја и заштитним релеима три произвођача која су тренутно заступљена у преносној мрежи Португала. На слици 11 приказан је систем који је коришћен за тестирање. Тестиране су 3 категорије могућих сценарија:

- телекомуникациона мрежа: TEL1 – SDH мрежа, као референтни сценарио, и TEL2 – IP-MPLS мрежа;
- количина саобраћаја у мрежи, поред саобраћаја за пренос сигнала заштите: TRF1 – без додатног саобраћаја, TRF2 – око 50% капацитета линка, и TRF3 – загушен линк;
- заштитна релеа за диференцијалну заштиту: PRTO1 – E1, PROT2 и PROT3 – C.37.94.



Слика 11: Тест систем за испитивање преноса порука заштите преко IP-MPLS мреже [24]

Резултати тестова показали су да је могуће користити пакетске мреже за пренос сигнала телезаштите и диференцијалне заштите, конкретно IP-MPLS мрежу одређене архитектуре и конфигурације, чак и када се истовремено користи и за пренос пословних сервиса, као и да су резултати упоредиви са преносом ових критичних сервиса кроз SDH мрежу под истим условима.

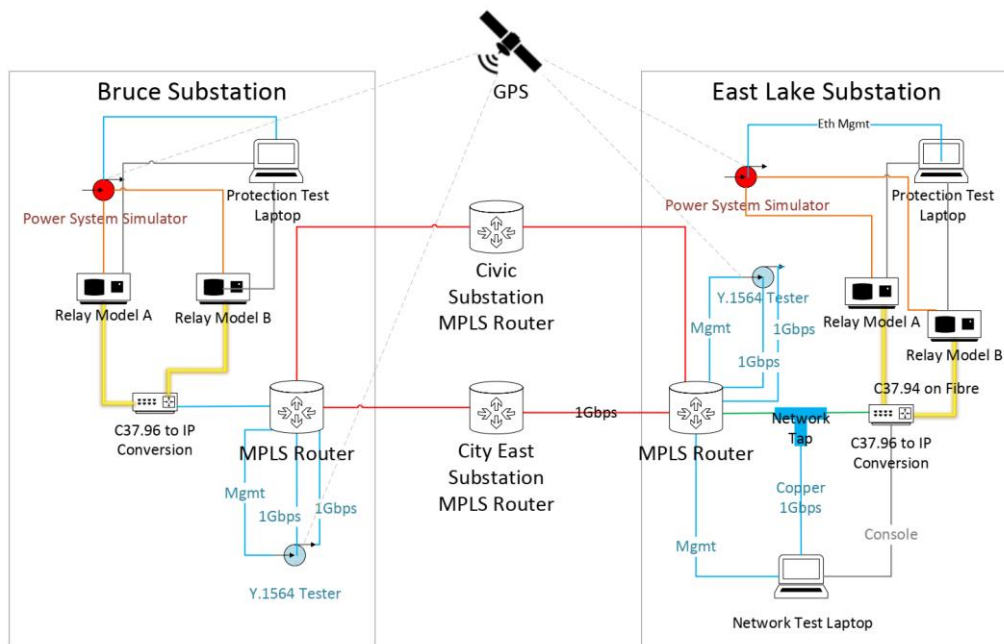
4.8 Аустралија

Највише је објављених истраживања примене MPLS технологије за пренос критичних сервиса у електропривреди у Аустралији, самостално [20],[26],[30], или у сарадњи са заинтересованим странама из других земаља [22],[23],[31]. Овде ће бити представљена два најинтересантнија резултата.

4.8.1 ACT (Australian Capital Territory) и Нови Јужни Велс

Интересантна чињеница истакнута у [20] и оно што чини ову имплементацију другачијом, је да аустралијске електропривредне компаније *Australian EPU (Electric Power Utilities)* нису имале имплементирану TDM мрежу, као ни сервис телезаштите, а за пренос података се користила корпоративна WAN (*Wide Area Network*) мрежа па у том смислу процес миграције није постојао, али свакако је требало превазићи проблеме преноса телезаштите протоколом C37.94 заснованог на TDM преносу кроз пакетску MPLS мрежу, која јесте предложена за имплементацију у оквиру корпоративне WAN мреже. У [20] је приказан процес развоја MPLS мреже у *ActewAGL* [45], једној од компанија у оквиру *Australian EPU* на територији ACT и југоисточног Новог Јужног Велса. Процес је обухватио период од 2013 – 2017. године, када је финализирана имплементација преноса сигнала телезаштите преко MPLS мреже. Закључено је да је најисплативије и најједноставније решење употреба C37.94-на-IP конвертора, без потребе конфигурисања MPLS рутера. C37.94-на-IP конвертор врши енкапсулацију C37.94 сигнала на UDP (*User Datagram Protocol*) пакете који се даље прослеђују ка MPLS рутеру. Телезаштита се преноси у оквиру посебне MPLS VPN мреже, као и остали сервиси (SCADA, пословни подаци, итд.). Да би се обезбедила симетрија линка за потребе преноса сервиса телезаштите имплементиран је MPLS-TE протокол, као и приоритети на основу QoS, док C37.94-на-IP конвертори садрже цитер бафере, да би се смањиле варијације кашњења при преносу.

У раду је приказан „доказ концепта“ (PoC – *Proof-of-Concept*) примене MPLS-TE протокола за пренос сигнала телезаштите на издвојеном сегменту постојеће MPLS мреже. Тест конфигурација је приказана на слици 12. Уведена је QoS шема са 5 класа сервиса, где највишем приоритету припадају телезаштита, пренос говора и TDMoIP. Закључено је да оваква имплементација задовољава захтеве за пренос сигнала телезаштите, а у том тренутку план *Australian EPU* био је да се имплементира више линкова са C37.94-на-IP конверторима.



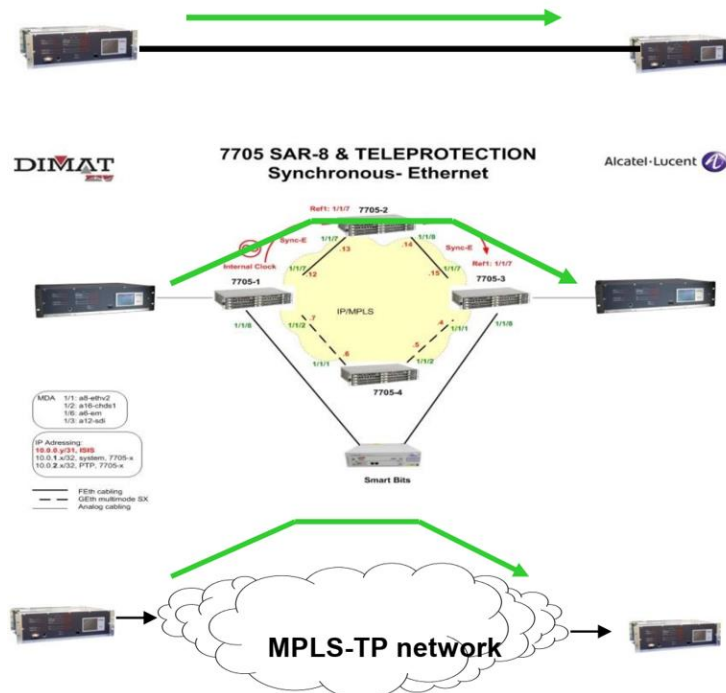
Слика 12: PoC тест систем за испитивање преноса порука телезаштите преко MPLS мреже [20]

4.8.2 Држава Викторија

Лабораторијска тестирања, описана у [23], настала су на иницијативу оператора преносног система у аустралијској држави Викторији, где су испитиване могућности MPLS-TP мреже да успешно преноси сигнале телезаштите. Пренос сигнала телезаштите је поређен коришћењем два протокола SAToP (*Structure Agnostic TDM over Packet*) [42] и CESoPSN (*Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network*) [42] за енкапсулацију TDM пакета преко асинхроне мреже каква је MPLS-TP. MPLS-TP мрежа је конфигурисана тако да постоје редундантни путеви. Добијени су резултати упоредљиви са TDM системима при брзинама од 1GB. Закључено је да MPLS-TP чвор може лако да замени одговарајуће PDH/SDH чворове.

4.9 Индија

На слици 13 приказан је систем за лабораторијско тестирање преноса команди телезаштите за *Avantha Group* [44], компаније за производњу и дистрибуцију електричне енергије, између осталог, у Индији. Добијени резултати су сумирани у табели Табела VI [18]. Додатно, пребацивање на резервни пут се одвијало без аларма и губитака података. У одговорима стручним известиоцима истакнуто је да се MPLS показао као могућа варијанта за критичне сервисе, али је неопходна добра инжењерска пракса приликом коришћења. Предлог је да се због редундантности система за пренос података користи комбинација наменских линкова са пакетским мрежама.



Слика 13: Комбинације конфигурације телекомуникационе мреже приликом тестирања преноса сигнала заштите у [18]

Табела VI: Резултати тестова из [18]; цитер бафер је величине 5 ms за пакетски пренос

Конекција	<i>blocking</i>	<i>direct tripping</i>
директна веза оптичким каблом	2,48 – 3,29 ms	13,4 – 14,2 ms
IP-MPLS без додатног саобраћаја	4,64 – 5,92 ms	15,2 – 16,8 ms
IP-MPLS са додатним саобраћајем	-	15,2 – 16,8 ms
MPLS-TP без додатног саобраћаја	7,44 -8,44 ms	20 – 20,6 ms
MPLS-TP са додатним саобраћајем	7,82 -8,72 ms	20,8 – 21,2 ms

5 ЗАКЉУЧАК

У овом раду приказане су основе IP/MPLS технологије, укључујући њене варијанте MPLS-TE и MPLS-TP, у контексту очекиваног преласка са мрежа комутације кола SDH/SONET, које се традиционално користе у електропривредним компанијама, на савремене пакетске мреже. Представљени имплементирани системи у оквиру оператера преносних система више земаља, као и примењени тестови у лабораторијским и реалним условима и њихови резултати, могу бити добра смерница за испитивање и потенцијалну имплементацију резервног пута за пренос сигнала телезаштите коришћењем MPLS протокола у оквиру EMC АД. На основу анализираних референци, уочава се да се као препорука за пренос сигнала заштите често истиче комбинација примарног пута, реализованог преко наменских (директних) оптичких веза, и резервног пута, реализованог преко MPLS мреже. Ово решење омогућава задржавање високог нивоа поузданости, али уз флексибилност коју MPLS инфраструктура пружа. Иако су представљена тестирања дала обећавајуће резултате, важно је напоменути да су она углавном извођена у лабораторијским условима, где је често занемариван утицај других мрежних токова. Стога су даља истраживања и тестирања у оперативним условима неопходна како би се донела коначна оцена о поузданости и перформансама оваквог решења у реалним ситуацијама.

6 ЛИТЕРАТУРА

- [1] Carlos Samitier “Utility Communication Networks and Services Specification, Deployment and Operation,” CIGRE Green Book, Springer 2017, DOI 10.1007/978-3-319-40283-3
- [2] IEC 61850:2021 SER Communication networks and systems for power utility automation
- [3] “Teleprotection over MPLS Wide-Area Networks,” CISCO & Siemens White Paper, 2017
- [4] “Application of MPLS-TP for Transporting Power System Protection Data,” UTC Journal, Strategies for the Future, 1st Quarter 2017
- [5] K. Ghanem, S. Ugwuany, J. Irvine (UK) “IP/MPLS and MPLS/TP Teleprotection Latencies over High Voltage Power Lines,” 2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Montreal, QC, Canada, 2023, pp. 381-386, DOI: 10.1109/WiMob58348.2023.10187795
- [6] Н. Чукић, М. Ристић, М. Медин, Ж. Васиљевић „Анализа савремених телекомуникационих технологија за потребе замене постојеће SDH транспортне телекомуникационе мреже код система са преносом критичних сервиса“, Д2 04, 35. саветовање CIGRE Србија, 3 – 7.10.2021., Златибор, Србија
- [7] E. Rosen, A. Viswanathan, R. Callon “Multiprotocol Label Switching Architecture,” RFC 3031, Jan. 2001
- [8] E. Rosen, D. Tappan, G. Fedorkow, Y. Rekhter, D. Farinacci, T. Li, A. Conta, “MPLS Label Stack Encoding,” RFC 3032, Jan. 2001
- [9] M.A. Ridwan, N.A. Mohamed Radzi, W.S.H.M. Wan Ahmad, F. Abdullah, Md.Z. Jamaludin, M.N. Zakaria “Recent trends in MPLS networks: technologies, applications and challenges,” IET Communications, Vol. 14 Iss. 2, pp.177-185, 2020, DOI: 10.1049/iet-com.2018.6129
- [10] James F. Kurose, Amherst Keith W. Ross “Computer Networking: A Top-Down Approach”, 7th Edition, PEARSON 2017
- [11] I. Minei, J. Lucek “MPLS-enabled applications: emerging development and new technologies,” John Wiley & Sons Ltd, UK, 2011
- [12] Luc De Ghein: “MPLS Fundamentals”, Cisco Press, 2007
- [13] NetEngine AR6700V-L “Basic MPLS Configuration”, Huawei, <https://support.huawei.com/enterprise/en/doc/EDOC1100412538/b53f337/overview-of-mpls>
- [14] Стратегија развоја система електронских комуникација у Републици Србији до 2027. године, „Службени гласник РС“, број 70 од 14. августа 2024.
- [15] Д. Богојевић „Електропривредне телекомуникационе мреже: развој, одржавање и људски фактор“, Д2 10, 21. симпозијум CIGRE Србија, 30.10 – 2.11.2024., Врњачка Бања, Србија

- [16] IEC 60834-1: Teleprotection Equipment of Power System – Performance and Testing – Part 1: Command Systems, Ed. 2, 1999
- [17] В. Челебић, М. Кабовић, А. Кабовић, Ј. Гајица, И. Салом, Б. Планић, С. Митровић, Д. Максић „Реализација резервног пута за пренос сигнала телезаштите у мрежи ЕМС АД БЕОГРАД“, Д2 6, 33. саветовање CIGRE Србија, 5 – 8.06.2017., Златибор, Србија
- [18] F. Castro (India) “A New Teleprotection System over IP Networks,” D2 01, CIGRE Comite Andino, Lima, Peru, 15 – 16th October 2015
- [19] J. Ramirez, H. Cabrera, O. Bautista (Venezuela) “MPLS-TP as packet platform for critical services in power transmission,” D2-309, CIGRE Paris Session 2016
- [20] V. Tan, J. Cole (Australia) “Teleprotection over Multiprotocol Label Switching (MPLS): Experiences from an Australian Electric Power Utility,” D2-305, CIGRE Paris Session 2018
- [21] L.H.M. Leite, R.A. Fernandes, L.F.F. Almeida, A.M. Alberti, S.H. Suoza. R.S.J. Santos (Brazil) “Challenges in the Migration to Packet Switched Networks for Teleprotection Service of Power Transmission Lines,” D2-301, CIGRE Paris Session 2020
- [22] N. Joshi (Australia), S.M. Blair, C.D. Booth (UK), J. Michielsen (Belgium) “Application of MPLS-TP for Transporting Power System Protection Data,” D2-307, CIGRE Paris Session 2020
- [23] K. Kulbuhsan, N. Zeinert (Australia), R. Liebert (Belgium), D. Perera, J. Dortmans (Australia) “Verification and Validation of MPLS-TP for Tele-protection (Current Differential) services with existing TDM (SDH & PDH), Radio & WDM technologies through Proof of Concept,” D2-309, CIGRE Paris Session 2020
- [24] J. Caseiro, R. Cartaxo, J. Saragoca, N. Marins, N. Amaro (Portugal) “Testing line differential protection and teleprotection over an IP/MPLS communication network,” B5-222, CIGRE Paris Session 2020
- [25] A. Louh (Netherlands), S. Zhang (France), A. Goerbing (Germany), J. Godefrooi (Netherlands), A. Jahr (Germany), R. Troost (Netherlands) “Seamless extension of fibre optical IP/MPLS network with 5G technology Releases allowing Business service segregation, Precision time synchronization and Critical teleprotection services in Utility distribution networks,” D2-10547, CIGRE Paris Session 2022
- [26] M. Shahi, P. Tuazon, M. Sainclair, S. Gharti Chhetri (Australia) “Teleprotection signal testing over IP/MPLS network,” D2-10589, CIGRE Paris Session 2022
- [27] K. Karkulehto, A. Virro (Finland) “Migration from time division multiplexing networks to MPLS-TP, field test experiences,” D2-10110, CIGRE Paris Session 2024
- [28] J. Ramirez (Panama), J. Borda (Peru) “Optical Systems Performance for Line Protection Schemes,” D2-10376, CIGRE Paris Session 2024
- [29] S. Sjörgen, T. Viinikainen, M. Holmgren (Finland) “Field testing, Experiences and Results with Line Differential and Teleprotection Applications in TDM/MPLS-TP Hybrid Networks,” B5-10103, CIGRE Paris Session 2024
- [30] N.A.J. McDowell (Australia) “Teleprotection Signaling over an IP/MPLS Network,” BScEE Thesis, University of Southern Queensland, 2014

- [31] S.M. Blair, C.D. Booth (UK), B. De Valck, D. Verhulst, C. Kirasack. K.Y. Wang, K. Lakshminarayanan (Belgium/Canada) “Validating Secure and Reliable IP/MPLS Communications for Current Differential Protection,” 13th International Conference on Development in Power System Protection 2016 (DPSP), Edinburgh, UK, 2016, pp. 1-6, DOI: 10.1049/cp.2016.0070.
- [32] M.A. Nunez, J. Denman, J.B. Melton Jr, G.T. Coruy, H. Chan, I. Schonwald (USA) “Case Study Protective Relaying over IP MPLS: Myth to Facts,” 70th Annual Conference for Protective Relay Engineers (CPRE), College Station, Texas, USA, 2017, DOI: 10.1109/CPRE.2017.8090014
- [33] T. Rahman, J. Morales, S. Ward, E.A. Udren, M. Bryson, K. Garg (USA) “Teleprotection with MPLS Ethernet Communications – Development and Testing of Practical Installations,” 2018
- [34] “IP/MPLS Performance and Path Analytics for Teleprotection in Power Utilities “Solution Brief, BluePlanet – a division of Ciena, 2020
- [35] NetEngine AR6700V-L “Basic MPLS Configuration”, Huawei, <https://support.huawei.com/enterprise/en/doc/EDOC1100412538/b53f337/overview-of-mpls>
- [36] N. Brownlee “Traffic Flow Measurement: Meter MIB,” RFC 2720, Oct. 1999
- [37] B. Niven-Jenkins, D. Brungard, M. Betts, N. Sprecher, S. Ueno, “Requirements of an MPLS Transport Profile,” RFC 5654, Sep. 2009
- [38] Grid Resources Inc, <https://gridres.com/>
- [39] NAKAMA SOLUTIONS SAC, <https://nakama.com.pe/>
- [40] San Diego Gas & Electric (SDG&E), <https://www.sdge.com/>
- [41] Lower Colorado River Authority (LCRA), <https://www.lcra.org/>
- [42] A. Vainshtein, YJ. Stein “Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP),” RFC 4553, Jun. 2006
- [43] A. Vainshtein, E. Metz, T. Frost, P. Pate “Structure-Agnostic Time Division Multiplexing (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN),” RFC 5086, Dec. 2007
- [44] Avantha Group, <https://ahlaprsacks.com/>
- [45] ActewAGL, <https://www.actewagl.com.au/>