Univerza v Ljubljani
Fakulteta za Elektrotehniko

Miha Kukar

Storitev navideznih zasebnih LAN omrežij (VPLS)

Seminarska naloga pri predmetu

porazdeljeni informacijski sistemi in celovitost podatkov

Ljubljana 2006

VSEBINSKO KAZALO

KAZALO SLIK

Povzetek

Namen tega dela je predstaviti tehnologijo povezovanja lokalnih (Ethernet) omrežij preko širših mestnih omrežij, ki jo poznamo pod imenom storitev navideznih zasebnih LAN omrežij (VPLS). S tehnologijo VPLS lahko znotraj enega mestnega omrežja ali preko več mestnih omrežij povežemo večje število lokalnih (LAN) omrežij.

V sklopu tega dela spoznamo tehnologijo MPLS, na kateri temelji storitev navideznih zasebnih LAN omrežij, in tehnologije grajenja navideznih zasebnih omrežij (VPN) na tretjem in drugem sloju.

Na koncu je izpostavljen še varnostni vidik navideznih zasebnih omrežij, ki temeljijo na MPLS in VPLS tehnologijah. Navedenih je nekaj možnih vrst napadov in priporočil, kako se določenih napadov obvarujemo ali jih preprečimo.

Ključne besede: MPLS, VPLS, L2 VPN, L3 VPN, Storitev navideznega zasebnega LAN omrežja, Večprotokolna komutacija z izmenjavo label, Ethernet, enkapsulacija, labela, robna točka, robna naprava, ponudnik storitev, usmerjevalnik, stikalo, varnost

Abstract

The goal of this work is to present technology of connecting Local Area Networks (LANs) across Metropolitan Area Networks (MAN) known as Virtual Private LAN Service (VPLS). With VPLS technology it is possible to connect multiple Local Area Networks inside single MAN, or over multiple metro networks.

In this paper the concept of MPLS technology is described, as MPLS is the base for VPLS implementation. We also discuss MPLS-based Virtual Private Network (VPN) technologies like L2 MPLS VPN and L3 MPLS VPN.

At the end of the paper some security issues of MPLS and VPLS networks are pointed out along with some possible solutions for security problems.

Key words: MPLS, VPLS, L2 VPN, L3 VPN, Virtual private LAN Service, Multi protocol Label Switching, Ethernet, encapsulation, label, Provider Edge (PE), Service Provider, router, switch, security

1 Mestna Ethernet omrežja

V današnjem času je Ethernet najširše uporabljena tehnologija v lokalnih omrežjih (LAN – Local Area Network), z več kot 100 milijoni klientov po celem svetu. V preteklih nekaj letih se je na področju Ethernet tehnologije pojavilo kar nekaj inovacij, ki so pripomogle k večjemu pretoku podatkov skozi Ethernet omrežja (z 10 Mbit/s se je pretok povečal na do 10 Gbit/s). Pojavilo pa se je tudi nekaj izboljšav protokola, ki so omogočile večji fizični doseg Ethernet tehnologije, tako da je uporabna tudi za rešitve prostranih omrežij (WAN – Wide Area Network), ki jih večkrat imenujemo tudi mestno omrežje (Metro Ethernet) [4].

Mestna omrežja, ki jih nudijo ponudniki storitev so pogosto zgrajena le kot povezave od točke do točke. Večji izziv in cilj pa je ponuditi zveze več točk z več točkami v istem mestnem omrežju ali pa celo med več mestnimi omrežji in tako podjetjem ponuditi storitev, da so vse lokacije povezane v isto Ethernet lokalno omrežje, ne glede na to, kje se lokacije fizično nahajajo, in ne glede na to, ali so v istem mestnem omrežju ali razpršene po različnih omrežjih.

Ponudba storitev mestnega Ethernet omrežja je bila dodanes bolj ali manj omejena. Večina ponudnikov je podpirala le povezave od točke do točke (point-to-point), ki so zagotavljale povezanost v internet, ali pa zasebne povezave med različnimi lokacijami.

Le malo ponudnikov je nudilo strankam Ethernet LAN zveze več točk z več točkami. Več lokacij v istem mestnem omrežju je bilo v tem primeru povezanih tako, kot bi bili v istem lokalnem omrežju, za logično ločevanje prometa pa so uporabljali različne VLAN (Virtual LAN) oznake.

Ker pa je večina današnjih mestnih Ethernet omrežij zgrajenih z Ethernet stikali, je prihajalo pri storitvah mestnih Ethernet omrežij do določenih težav. Storitev je bilo težko upravljati, včasih pa je nedosegljiva predvsem zaradi problemov kot so nestabilnost protokola STP (Spanning Tree Protocol), problemov z poplavljanjem v primeru broadcast oddajanja in podobnih težav z velikimi Ethernet omrežji. Ta omrežja so bila tudi omejena glede na število uporabnikov, saj so podpirala le 4096 različnih VLAN identifikacij in posledično temu enako število uporabnikov. Težava je bila tudi v tem, da so VLAN oznake pomembne globalno, kar pomeni, da morajo biti vse VLAN oznake istega ponudnika storitev med seboj različne.

S tako arhitekturo nikakor ni prišlo v poštev, da bi LAN funkcionalnosti lahko zagotavljali preko več mestnih omrežij, saj bi ponudnik storitev potreboval še večje Ethernet omrežje, temu pa bi sledilo še več težav. Zato je bila storitev mestnih Ethernet omrežij s povezavami več točk z več točkami v bližnji preteklosti precej nerealna.

Eden izmed najbolj obetajočih pristopov k temu problemu je storitev virtualnih zasebnih LAN omrežij (VPLS), ki nudi prav Ethernet povezljivost več točk z več točkami (multipoint-to multipoint) preko razširljivega IP / MPLS omrežja ponudnika storitev.

2 MPLS

V preteklih nekaj letih se je s strani ponudnikov storitev pojavilo vedno večje zanimanje za tehnologijo MPLS. Sprva je bila zasnovana za potrebe prometnega inženiringa, v današnjem času pa se uporablja za vzpostavljanje navideznih zasebnih omrežij (VPN). Pojavlja se kot močna in uspešna alternativa uporabi VPN rešitev na izključno drugem sloju (layer 2), na izključno tretjem sloju (layer 3) ali katerikoli metodi tuneliranja, ki se navadno uporabljajo za implementacijo navideznih zasebnih omrežij.

Pri odločanju za implementacijo navideznega zasebnega omrežja na osnovi tehnologije IP/MPLS ima ponudnik storitev dve možnosti:

- rešitev na tretjem sloju, t.i. MPLS Layer-3 VPN
- rešitev na drugem sloju, t.i. MPLS Layer-2 VPN

Pri odločanju za posamezno rešitev moramo upoštevati naslednje parametre:

- podpiran tip prometa
- scenarije VPN povezavnosti, ki jih na ta način lahko ponudimo stranki
- razširljivost
- kompleksnost postavitve
- kompleksnost zagotavljanja storitve
- kompleksnost upravljanja in reševanja napak
- ceno postavitve
- ceno upravljanja in vzdrževanja

Ne moremo reči, da je ena izmed rešitev boljša, saj se vsaka loteva problema z druge strani, in rešitev, ki bolj odgovarja nekemu ponudniku storitev, ni nujno najugodneša za drugega ponudnika.

2.1 Kaj je MPLS

MPLS je tehnologija, ki skrbi za učinkovito posredovanje, usmerjanje in preklapljanje prometnih tokov skozi omrežje. Funkcije MPLS so:

- specifikacija mehanizmov za upravljanje različnih prometnih tokov (tudi med različnimi napravami, različno strojno opremo, in različnimi aplikacijami)
- neodvisnost od protokolov drugega in tretjega sloja
- označevanje IP naslovov s preprostimi labelami fiksne dolžine, ki jih uporabljajo različne tehnologije za preklapljanje in posredovanje paketov
- vmesnik obstoječim usmerjevalnim protokolom kot sta na primer OSPF in RSVP
- podpora protokolom IP, ATM, Frame Relay

V MPLS se podatki prenašajo prek labelno komutiranih poti (LSP – Label Switched Path). Labelno komutirane poti so pravzaprav sekvenca label v vsakem vozlišču med izvorom in ponorom podatkov. Labelno komutirana pot se vzpostavi ob oddaji podatkov ali ob detekciji toka podatkov. Labele so identifikatorji nižje ležečih protokolov. Prenašajo se z protokolom za distribucijo label (LDP – Label Distribution Protocol) ali RSVP (Resource Reservation Protocol), pa tudi z usmerjevalnimi protokoli kot sta BGP in OSPF. Vsak podatkovni paket v glavi vsebuje labelo, ki jo nosi na svoji poti od izvora do ponora. MPLS omogoča zelo hitro preklapljanje podatkov prav zaradi label fiksne dolžine, ki se nahajajo prav na začetku vsakega podatkovnega paketa. Na podlagi label nato strojna oprema hitro preklaplja pakete med povezavami.

Naprave, ki sodelujejo v MPLS mehanizmu lahko razvrstimo na labelne robne usmerjevalnike (LER – Label Edge Router) in labelno komutirane usmerjevalnike (LSR – Label Switching Router) [9].

LSR so zelo hitri usmerjevalniki v jedru MPLS omrežja, ki sodelujejo pri vzpostavljanju labelno komutiranih poti z uporabo ustreznega signalizacijskega protokola in pri hitri komutaciji podatkovnega prometa po vzpostavljenih poteh.

LER usmerjevalniki pa so naprave, ki delujejo na robu med dostopovnim omrežjem in MPLS omrežjem. LER usmerjevalniki so z več vrati povezani v dostopovna omrežja kot so Ethetnet, ATM, Frame Relay, in nato vhodni promet posredujejo v MPLS omrežje, izhodni promet iz MPLS omrežja pa v ustrezno dostopovno omrežje. Labelni robni usmerjevalniki imajo pomembno nalogo določanja in odstranjevanja label ob vstopu in izstopu prometa v ali iz MPLS omrežja.

Ekvivalentni razred predajanja (FEC – Forwarding Equivalence Class) je reprezentacija skupine paketov, ki imajo enake pogoje za prenos preko omrežja. Vsi paketi v takšni skupini so enako obravnavani na njihovi poti do ponora. Za razliko od IP usmerjanja, se pri MPLS dodelitev paketa k določeni FEC skupini zgodi le enkrat, to je ob vstopu paketa v omrežje. FEC skupina temelji na potrebnih pogojih prenosa

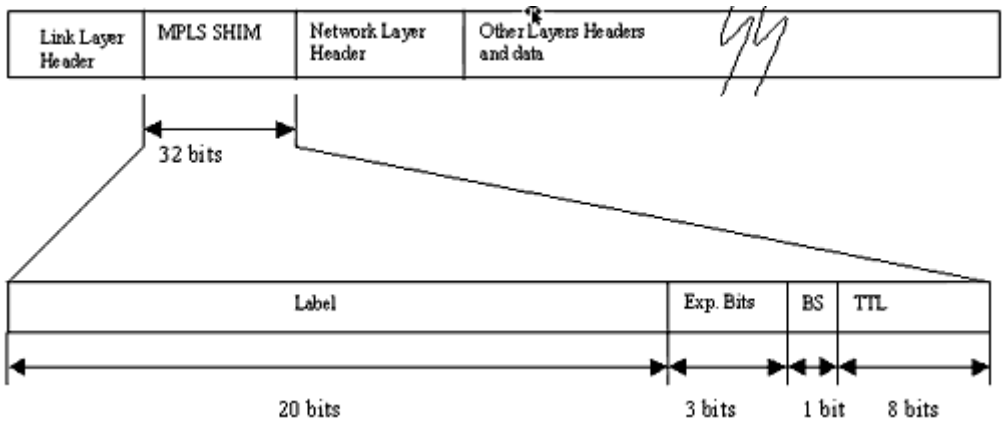
za določeno skupino paketov ali za določen naslov. Vsak labelno komutirani usmerjevalnik zgradi posebno tabelo imenovano labelna informacijska baza (LIB – Label Information Base), po kateri se paketi usmerjajo.

Labela identificira pot, po kateri mora paket potovati in je enkapsulirana oziroma vsebovana v glavi paketa. Usmerjevalnik, ki sprejme paket, v glavi poišče podatek, kam ga usmeriti naprej. Labele so lokalnega značaja, kar pomeni, da se ista vrednost labele ohrani le med enim skokom (med dvema LSR usmerjevalnikoma), ne pa skozi celotno MPLS omrežje.

Ko je paketu dodeljena nova ali obstoječa FEC skupina, se mu dodeli tudi labela. Vrednost labele lahko izvira iz nižje ležečega povezavnega sloja. Identifikatorje protokolov povezavnega sloja kot so na primer identifikatorji zveze v sloju podatkovne povezave (DLCI – Data Link Connection Identifier) pri Frame Relay omrežjih ali pa identifikatorji navidezne poti (VPI – Virtual Path Identifier) ali navideznega kanala (VCI – Virtual Channel Identifier) pri ATM omrežjih lahko direktno uporabimo kot labele. Paketi so nato posredovani glede na vrednost njihove labele.

Dodeljevanje label lahko temelji na različnih kriterijih [9]:

- končna destinacija usmerjanja oddaje enemu prejemniku (unicast)
- prometni inženiring
- oddajanje več prejemnikom hkrati (multicast)
- navidezna zasebna omrežja (VPN)
- kakovost storitev (QoS)



Slika 1 MPLS labela [9]

Distribucija label

V MPLS lahko uporabimo različne signalizacijske protokole za distribucijo label. Uporabi se lahko obstoječe usmerjevalne protokole kot sta BGP in RSVP, skupina IETF pa je definirala tudi nov protokol, namenjen prav izmenjavi label in upravljanju z labelnim prostorom, tako imenovani protokol za distribucijo label, LDP. Novejše razširitve protokola za distribucijo label z upoštevanjem omejitev (CR-LDP – Constraint-based Routing LDP) pa nudijo tudi podporo mehanizmom kakovosti storitev (QoS – Quality of Service) in razredov storitev (CoS – Class of Service).

Po [9] lahko povzamemo različne sheme izmenjave label:

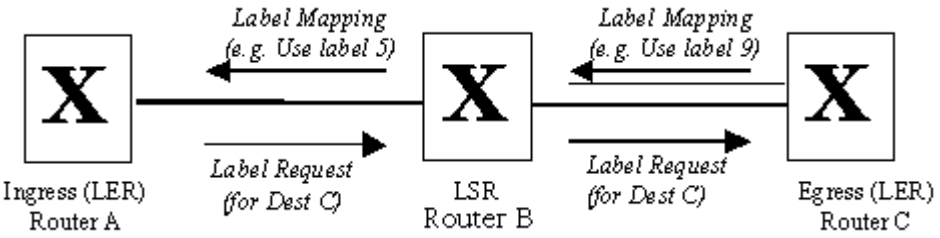
- **LDP** – gre za preslikavo ciljnega IP naslova v labelo
- **RSVP** in **CR-LDP** – se uporabljata za prometni inženiring ter rezervacijo virov
- **PIM** (Protocol-independent multicast) – se uporablja za preslikavo label v načinu oddajanja več prejemnikom hkrati
- **BGP** – zunanje labele (navidezna zasebna omrežja)

Znotraj MPLS domene se potujočemu paketu določi pot na osnovi FEC skupine. Uporabljata se dva načina vzpostavljanja labelno komutiranih poti, in sicer usmerjanje po skokih (hop-by-hop) in določeno usmerjanje. Pri usmerjanju po skokih vsak labelno komutirani usmerjevalnik samostojno določi naslednji skok za določen FEC. Ta metoda je podobna trenutno uporabljani metodi v IP omrežjih. Pri določenem usmerjanju pa vhodni usmerjevalnik določi listo vseh vozlišč, preko katerih bo tok potekal. Ni nujno, da je takšna pot optimalna. Vzdolž poti lahko tudi rezerviramo. Na ta način lahko olajšamo prometni inženiring, nudimo diferencirane storitve in zagotovimo kakovost storitev.

Če ima več podatkovnih tokov različnih vmesnikov isti cilj (ponor), jih lahko združimo in preklapljamo z uporabo skupne (enake) labele. Pozorni pa moramo biti v primeru, ko je na drugem sloju uporabljena tehnologija ATM, saj v tem primeru lahko pride do neželenega združevanja virtualnih poti ali virtualnih kanalov.

V MPLS se uporabljata dva signalizacijska mehanizma:

- **zahteva po labeli** - s tem mehanizmom labelno komutirani usmerjevalnik os naslednjega usmerjevalnika v smeri toka podatkov zahteva labelo. Ta mehanizem je vzpostavljen po celotni verigi usmerjevalnikov, preko celotne MPLS hrbtenice, do zadnjega robnega usmerjevalnika
- **preslikava labele** - je odgovor na zahtevo po labeli in vsebuje vrednost labele



Slika 2 Signalizacijski mehanizmi v MPLS

Protokol za distribucijo label je protocol, ki se uporablja za posredovanje informacije o povezavi med vrednostjo labele in FEC skupino labelno komutiranim usmerjevalnikom v MPLS omrežju. Uporablja se za preslikavo FEC oznak v labele, ki nato generirajo labelno komutirane poti. LDP seje se vzpostavljajo med soležnimi LDP entitetami, ki si izmenjujejo naslednje tipe LDP sporočil:

- sporočila o odkritju (discovery messages), ki napovedujejo prisotnost labelno komutiranih usmerjevalnikov v MPLS omrežju,
- sejna sporočila (session messages), s katerimi vzpostavljajo, vzdržujejo in rušijo LDP seje,
- oglasna sporočila (advertisement messages), s katerimi ustvarjajo, spreminjajo in brišejo labelne preslikave
- obvestila (notification messages), ki nudijo informacijo o nadzoru in napakah.

V MPLS domeni se uporablja tudi tako imenovani labelni sklad (label stack), to je mehanizem, ki omogoča hierarhično delovanje znotraj MPLS domene. V bistvu omogoča uporabo MPLS za hkratno usmerjanje na nivoju posameznih usmerjevalnikov znotraj omrežja ponudnika storitev (ISP) in na višjem, meddomenskem nivoju. Vsak nivo v labelnem skladu ne nanaša na nek hierarhični nivo. To omogoča tunelski način delovanja MPLS.

Prometni inženiring in kakovost storitev

Proces prometnega inženiringa izboljša celotni izkoristek omrežja s porazdelitvijo prometa po celotnem omrežju. Pomemben rezultat prometnega inženiringa je izogibanje zamašitvam v omrežju. V procesu prometnega inženiringa ni nujno, da vedno izberemo najkrajšo možno pot med dvema napravama. Paketi lahko potujejo prek popolnoma različnih poti, kljub temu, da sta izvor in ponor v isti napravi. Na ta način izkoristimo tudi manj uporabljene segmente omrežja in omogočimo boljšo kakovost storitev.

K prometnemu inženiringu lahko v MPLS pristopimo z uporabo določenega usmerjanja. Labelno komutirane poti se generirajo samostojno, vendar po politiki, ki jo vnaprej določimo. Ta način lahko zahteva veliko dela s strani operaterja. Uporaba

RSVP in CR-LDP sta dva možna načina zagotovitve dinamičnega prometnega inženiringa in kakovosti storitev v MPLS.

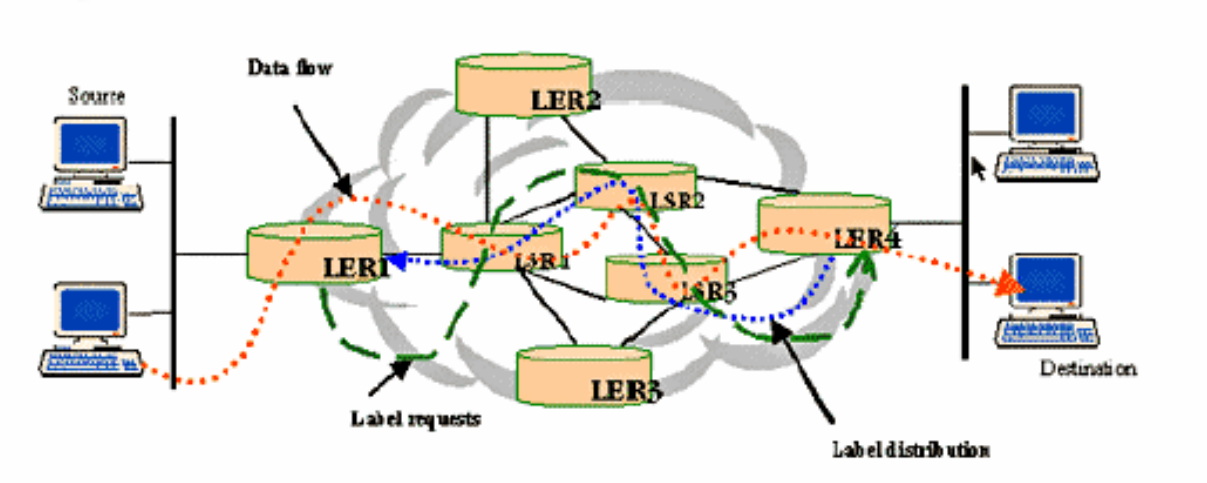
Usmerjanje z upoštevanjem omejitev (CR – Constraint-based Routing) upošteva parametre kot so karakteristika povezave, na primer pasovna širina, zakasnitve, število skokov, in kakovost storitev. Omejitve so lahko kakovost storitev, določeni skoki (vnaprej določena pot) ali kak drug parameter. Pogoji za kakovost storitev pa so največkrat implementacija mehanizmov razvrščanja in tudi uporaba vnaprej določenih poti za določen tok podatkov. Usmerjanje z upoštevanjem omejitev torej izboljša izkoristek omrežja, vendar pa poveča kompleksnost usmerjevalnih kalkulacij, saj mora izbrana labelno komutirana pot ustrezati pogojem za kakovost storitev.

2.2 Delovanje MPLS

Za potovanje podatkovnega paketa preko MPLS domene so potrebni naslednji koraki:

- tvorba in distribucija label,
- tvorba tabele v vsakem usmerjevalniku
- tvorba labelno komutiranih poti
- vstavljanje labele in vpogled v tabelo
- posredovanje paketov

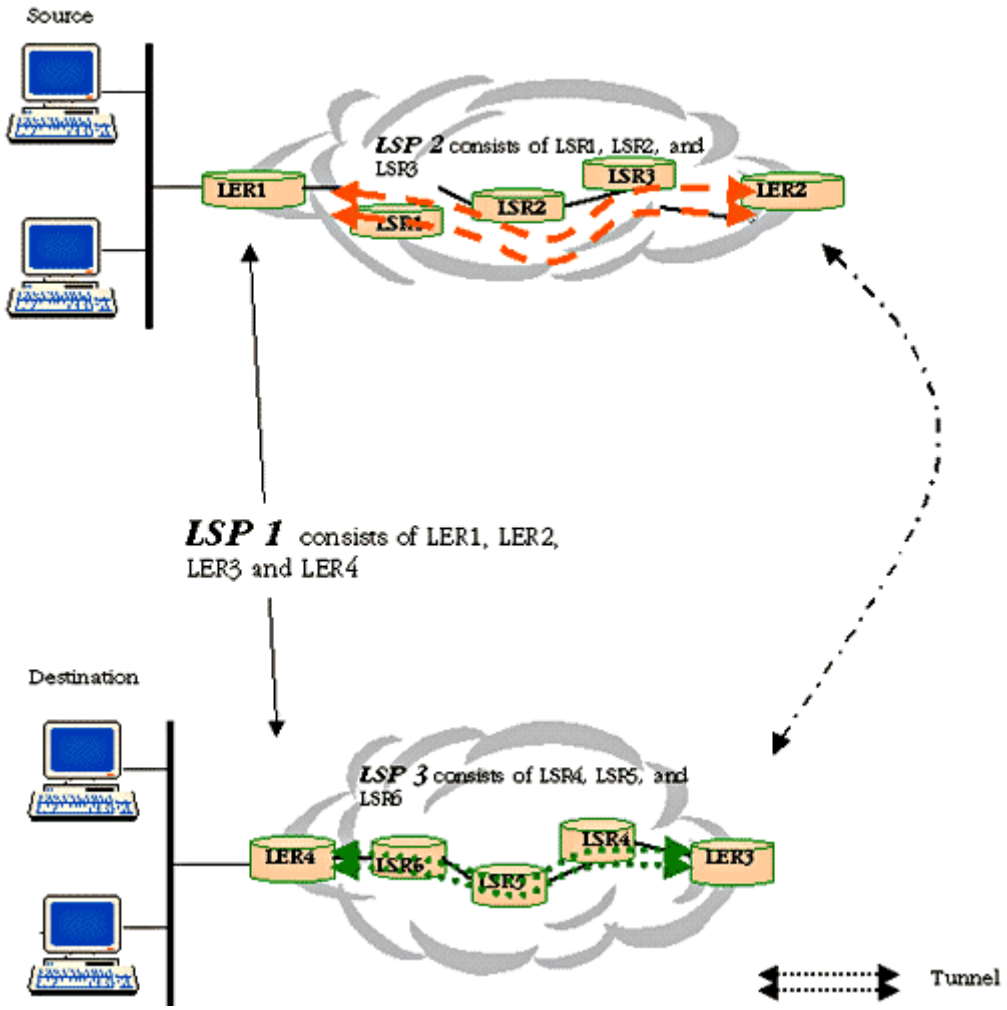
Izvor pošlje podatke proti ponoru. V MPLS domeni ni nujno, da ves promet, ki gre proti istemu ponoru, potuje po isti poti. Različne labelno komutirane poti se lahko tvorijo za pakete z različnimi pogoji razreda storitev, odvisno od prometne karakteristike.



Slika 3 Tvorba labelno komutirane poti in posredovanje paketa prek MPLS domene [9]

Tuneliranje v MPLS

Tuneliranje je posebna lastnost MPLS tehnologije. MPLS nadzoruje celotno pot paketa brez eksplicitne določitve vmesnih usmerjevalnikov. To doseže s tvorbo tunelov preko vmesnih usmerjevalnikov in se uporablja pri vzpostavljanju navideznih zasebnih omrežij na osnovi MPLS tehnologije (MPLS VPN).



Slika 4 MPLS tuneliranje [9]

Na zgornji sliki lahko vidimo kako tuneliranje poteka. Robni labelni usmerjevalniki (LER1, LER2, LER3 in LER4) uporabljajo BGP protokol in tvorijo labelno komutirane pot med njimi. To je LSP1. Robni usmerjevalnik LER1 se zaveda, da je naslednja destinacija usmerjevalnik LER2, saj podatke pošilja ponoru preko dveh segmentov omrežja. LER2 prepozna za naslednjo destinacijo LER3, in tako naprej. Vsi ti robni usmerjevalniki uporabijo LDP protokol za sprejem in shranitev label od izhoda iz MPLS omrežja (LER4) do vhoda (LER1).

Podatki, ki jih usmerjevalnik LER1 pošlje usmerjevalniku LER2 pa potujejo preko več labelno komutacijskih usmerjevalnikov. V našem primeru so ti označeni z LSR1, LSR2 in LSR3. Zato se med robnima usmerjevalnikoma LER1 in LER2 kreira nova labelno komutirana pot (LSP2), ki zajema vse tri labelno komutacijske usmerjevalnike. Ta pot je pravzaprav tunel med tema dvema robnima usmerjevalnikoma. Vrednosti label na tej poti so različne od vrednosti label, ki veljajo za pot LSP1. Prav takšen postopek velja tudi med usmerjevalnikoma LER3 in LER4 in za labelno komutirano pot med njima (LSP3).

Vidimo da imamo pri transportu preko omrežja z dvema segmentoma opravka z več vrednostmi label. V ta namen se uporablja koncept labelnega sklada. Ker paket istočasno potuje po dveh labelno komutiranih poteh, obenem prenaša vrednosti dveh različnih label hkrati. Ko paket potuje po prvem delu omrežja, bo imel hkrati vpisano vrednost labele za labelno komutirano pot LSP1 in LSP2. Ob izstopu iz prvega omrežja paket sprejme usmerjevalnik LER3, ki zamenja labelo za LSP2 z labelo za LSP3, za labelo naslednjega skoka pa bo v paketu nastavil labelo za pot LSP1. Usmerjevalnik LER4 pa bo pred posredovanjem paketa ponoru odstranil obe labeli.

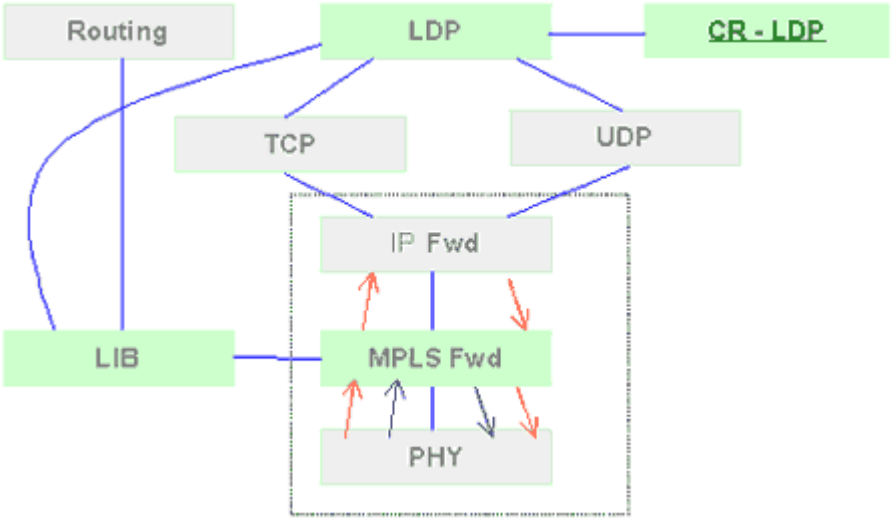
Delovanje v načinu oddajanja več prejemnikom hkrati (multicast)

Delovanje MPLS v načinu oddajanja več prejemnikom hkrati trenutno ni definirano, se pa pojavljajo priporočila za splošni pristop k temu problemu, kjer se vstopna labela preslika v nabor več izhodnih label, kar dosežemo z grajenjem multicast drevesa. V tem primeru se vhodna labela veže na multicast drevo, na izhodu pa se nabor več vrat uporabi za oddajo paketov.

Arhitektura MPLS protokolnega sklada

Komponente MPLS protokolnega sklada lahko razdelimo takole:

- usmerjevalni protokoli omrežnega sloja (IP)
- posredovanje na robu omrežnega sloja (edge of network layer forwarding)
- labelna komutacija v jedru omrežja
- shematika label
- signalizacijski protokol za distribucijo label
- prometni inženiring
- kompatibilnost s posredovalnimi protokoli povezavnega sloja (ATM, Frame Relay, PPP)



Slika 5 MPLS protokolni sklad [9]

Na zgornji sliki vidimo protokole, ki se uporabljajo v MPLS. Za usmerjevalni modul lahko uporabimo kateri koli od splošno razširjenih industrijskih protokolov, na primer OSPF, BGP in podobno. LDP modul uporablja TCP transportni protokol za zanesljiv prenos nadzornih podatkov med labelno komutacijskimi usmerjevalniki med LDP sejo. Prav tako LDP vzdržuje labelno informacijsko bazo (LIB). LDP uporablja tudi UDP protokol, in sicer med začetno fazo delovanja, ko labelno komutacijski usmerjevalniki identificirajo svoje sosede in signalizirajo omrežju svojo prisotnost preko t.i. pozdravnih sporočil (hello packets).

IP FWD je klasični IP posredovalni modul, kjer se naslednji skok določi iz IP naslova. V MPLS se to dogaja le v robnih komutacijskih usmerjevalnikih. MPLS FWD je MPLS posredovalni modul, ki izvaja komutacijo na podlagi label in vpogleda v labelno informacijsko bazo. Moduli, ki slo na sliki prikazani v okviru, so ponavadi hardversko implementirani zaradi hitrega in učinkovitega delovanja.

Prednosti uporabe MPLS

MPLS se danes uporablja predvsem v hrbteničnih omrežjih ponudnikov storitev. Naj naštejem nekaj prednosti, ki jih nudi MPLS tehnologija:

- izboljšanje zmogljivosti posredovanja paketov v omrežju
- preprostost in enostavna implementacija
- izboljšanje zmogljivosti omrežja (preklapljanje pri večjih hitrostih)
- podpora mehanizmom kakovosti storitev in razredov storitev (QoS in CoS)
- podpora razširljivosti omrežja
- integracija IP in ATM omrežij, kjer MPLS lahko predstavlja most med tema dvema tehnologijama

2.3 Uporaba tehnologije MPLS za grajenje navideznih zasebnih omrežij

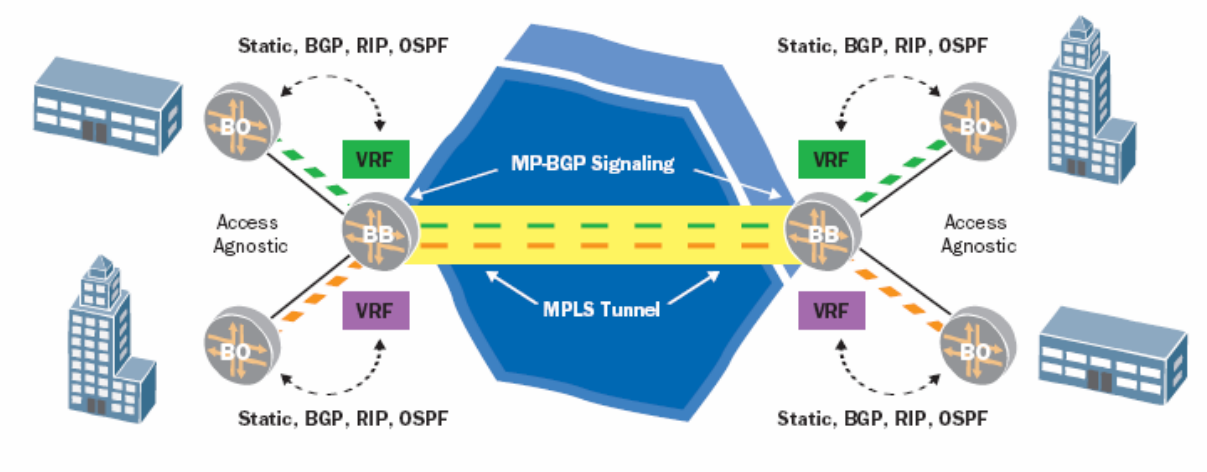
Navidezno zasebno omrežje (VPN) je omrežje, ki uporablja neko skupno omrežno infrastrukturo, a nudi varnost in zasebnost kot pri najetih vodih. Med starejše primere bi lahko uvrstili tehnologije kot sta ATM in Frame Relay, navidezna zasebna omrežja pa se pojavljajo tudi na omrežnem nivoju, kot na primer kriptirani IPSec tuneli preko interneta. Možni so tudi PPTP in L2TP klicni VPN dostopi preko skupnega omrežja. MPLS VPN je način uporabe tehnologije MPLS za graditev navideznih zasebnih omrežij. MPLS je zelo primerna tehnologija za ta namen, saj nudi izolacijo in razločevanje prometa praktično brez dodatne režije. MPLS VPN omrežja nudijo varne povezave in relativno preprosto konfiguracijo in so zato popularna tehnologija, ki se uporablja tako za intranet in ekstranet omrežja.

Cilj MPLS VPN tehnologije je zgraditi omrežje, ki naj deluje kot podaljšek zasebne korporativne omrežne infrastrukture preko omrežja nekega ponudnika storitev. Na ta način lahko povežemo geografsko razpršene lokacije, kot so na primer podružnice podjetja in domovi delavcev, v skupno, za uporabnika transparentno okolje.

Oba VPN pristopa, tako na omrežnem sloju kot tudi na povezavnem sloju, nakazujeta probleme z razširljivostjo in podporo več zasebnih omrežij na skupni deljeni omrežni infrastrukturi. V omrežjih tretjega nivoja bi moral vsak usmerjevalnik podpirati tisoče usmerjevalnih tabel (po eno za vsako virtualno zasebno omrežje, poleg tistih za javno omrežje). Pri omrežjih na drugem nivoju pa prihaja do težav z razširljivostjo, saj so omejena z omejitvami transportnega medija. Pri Ethernetu na primer, imamo omejitev števila VLAN omrežij na 4096. Pri vseh teh težavah lahko pomaga tehnologija MPLS.

2.4 MPLS navidezna zasebna omrežja na tretjem sloju (Layer 3)

Implementacija navideznih zasebnih omrežij na tretjem sloju temelji na IETF zahtevku za komentar RFC 2547bis. Pri tem razredu navideznih zasebnih omrežij poteka transport prometa skozi omrežje preko MPLS tunelov in s pomočjo MP-BGP (Multi Protocol BGP) signalizacije.



Slika 6 MPLS navidezno zasebno omrežje na tretjem sloju [10]

Na sliki 6 vidimo hrbtenični MPLS usmerjevalnik (BB – Backbone Router) in usmerjevalnik pri stranki (BO – Branch Office), ki pa ne deluje v MPLS načinu. To je najpogostejši način uporabe MPLS navideznih zasebnih omrežij, ki se široko uporablja po celem svetu, tudi v Sloveniji. Možno je tudi, da se MPLS razširi prav do strankine lokacije (BO), in se tako vzpostavi prav od ene končne točke do druge.

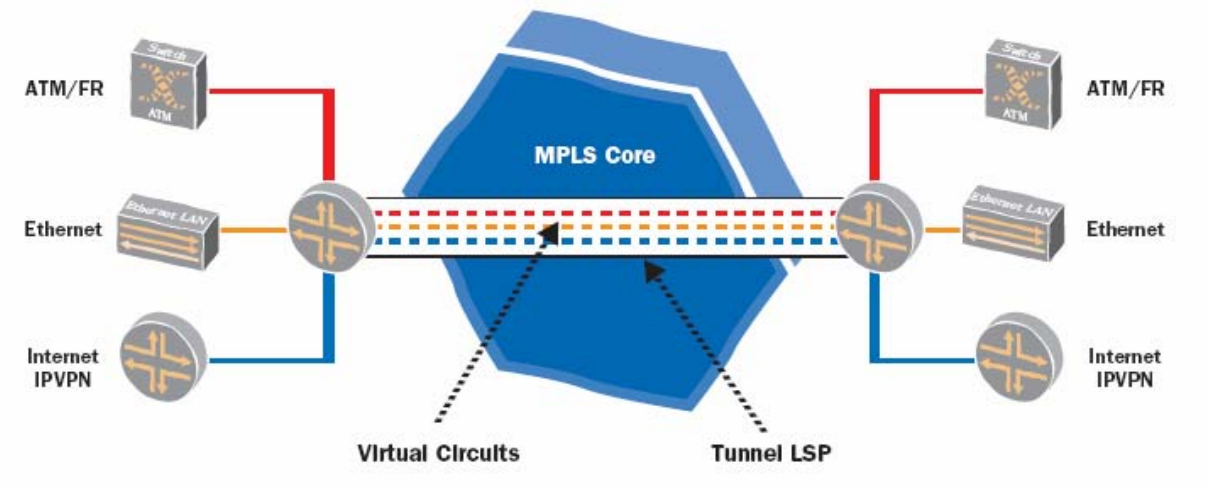
Vsak hrbtenični MPLS usmerjevalnik vsebuje usmerjevalno instanco, t.i. predajo navideznih smeri (VRF – Virtual Route Forwarding). Na ta način je hkrati v enem usmerjevalniku prisotnih več neodvisnih usmerjevalnih tabel. Ker so medsebojno neodvisne, s tem dosežemo, da lahko različni uporabniki MPLS omrežja uporabijo iste zasebne IP naslove za svoje navidezno zasebno omrežje, ne da bi s tem vplivali drug na drugega. S pomočjo predaje navideznih smeri in MPLS izolacije prometa tako kreiramo navidezna omrežje.

Prednost navideznih zasebnih omrežij na tretjem sloju je ta, da so standardizirana in dokaj enostavna. Ta tip navideznih zasebnih omrežij podpira širok nabor tipov dostopa in več topologij hrbteničnega omrežja. Taka rešitev je bolj razširljiva in cenejša od klasičnih ATM in Frame Relay omrežij ali navideznih zasebnih omrežij z uporabo IPsec-a. Prav tako pa ta pristop nudi tudi podporo mehanizmom kakovosti storitev.

2.5 MPLS navidezna zasebna omrežja na drugem sloju (Layer 2)

Navidezna zasebna omrežja na drugem sloju, ki temeljijo na ATM in Frame Relay, so tudi zelo razširjena. S strani delovne skupine IETF L2VPN so definirani mehanizmi enkapsulacije in distribucije label, ki omogočajo različnim protokolom prenos preko hrbteničnega MPLS omrežja.

Pri L2 MPLS navideznih zasebnih omrežjih je ključna vzpostavitev tunelov (oziroma labelno komutiranih poti), kot vidimo na sliki 7.



Slika 7 MPLS navidezno zasebno omrežje na drugem sloju [10]

Za nadzorni protokol se uporabljata protokola LDP ali BGP, s katerimi se vzpostavljajo navidezni vodi.

V splošnem lahko navidezna zasebna omrežja drugega sloja, ki delujejo na osnovi MPLS, razdelimo na dva tipa. To sta navidezno zasebno omrežje s signalizacijo BGP (BGP based VPN) in pa Layer 2 Circuit s signalizacijo LDP.

Layer 2 Circuit, imenovan tudi Martini VPN, temelji na internetnem osnutku avtorja Luca Martini. Tu so definirani postopki enkapsulacije in signalizacije na drugem sloju. Ta pristop imenujemo tudi emulacija navideznih vodov (Pseudo Wire Emulation), ker temelji na grajenju navideznih vodov od točke do točke (Point-to-point Pseudo Wires) preko MPLS jedra. Martini-VPN uporablja protokol LDP za vzpostavljanje tunelov in distribucijo label.

Navidezno zasebno omrežje z BGP protokolom je osnovano po internetnem osnutku avtorja Kireeti Kompella. Za komunikacijo med robnimi usmerjevalniki o povezavah uporabnikov uporablja kar protokol BGP in tako tu ni potrebe po vpeljavi protokola LDP.

Prednost navideznih zasebnih omrežij drugega sloja pred navideznimi zasebnimi omrežji tretjega sloja je ta, da podpirajo velik nabor različnih enkapsulacij. Le-te vključujejo tudi Ethernet, ATM, HDLC (High-Level Data Link Control) in PPP (Point-to-Point Protocol). Ena izmed slabosti pa je potreba po individualni konfiguraciji vsakega navideznega voda. Zaradi tega L2 VPN omrežja niso najbolj razširljiva oz. skalabilna.

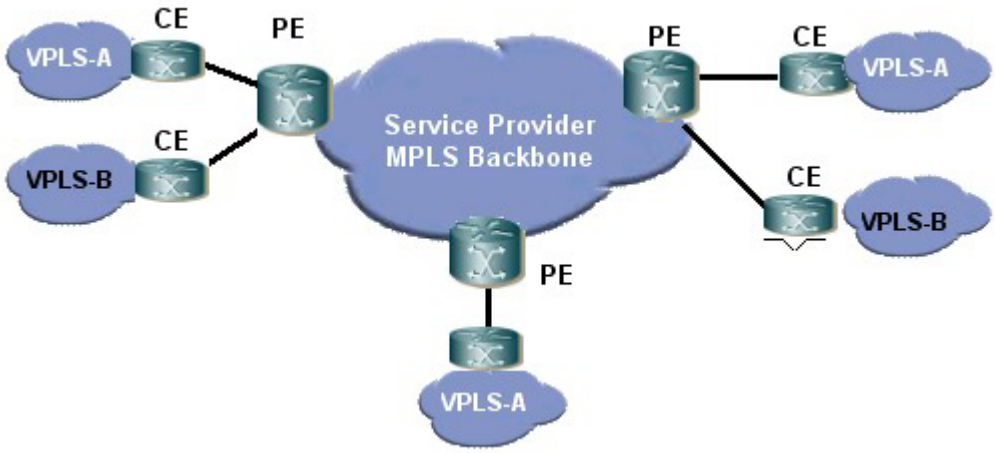
Večtočkovno navidezno zasebno omrežje drugega sloja (multipoint L2 VPN) za Ethernet lahko implementiramo z uporabo Storitve navideznih zasebnih LAN omrežij (VPLS) in MPLS navideznih vodov. Večtočkovno VPLS omrežje temelji na L2 navideznih zasebnih omrežjih od točke do točke, cilj pa je razširiti Ethernet domeno prek več geografsko oddaljenih lokacij. Celotno VPLS omrežje se za končnega uporabnika obnaša kot zasebno Ethernet stikalo.

3 Storitev navideznega zasebnega LAN omrežja (VPLS)

Storitev navideznih zasebnih LAN omrežij (VPLS) je tehnologija vzpostavljanja navideznih zasebnih omrežij (VPN) na drugem sloju (Layer 2), ki temelji predvsem na MPLS in Ethernet tehnologijah. Uporabnikom omogoča dostop do LAN omrežja z več geografsko razpršenih dostopovnih točk, kot da bi bile te povezane direktno v lokalno omrežje. Namen VPLS tehnologije je torej razširiti uporabnikovo lokalno omrežje preko MAN/WAN omrežij.

3.1 VPLS referenčni model

Celotno VPLS omrežje deluje kot ogromno stikalo. Med različnimi navideznimi zasebnimi omrežji se vzpostavljajo navidezni vodi in prek njih transparentno potujejo uporabniški datagrami.



Slika 8 VPLS referenčni model [5]

Osnovni referenčni model za storitev navideznih zasebnih omrežij je prikazan na zgornji sliki. Lokacije stranke (CE – Customer Edge) so povezane z omrežjem ponudnika telekomunikacijskih storitev v robnih točkah (Provider Edge). Vse robne točke v omrežju ponudnika pa so med seboj povezane v popolno zankasto (full mesh) topologijo tunelov, kjer vsak tunel vsebuje več navideznih vodov.

Navidezni vodi so zveze od točke do točke, vzpostavljene za vsako ponujeno storitev med dvema robnima točkama ponudnika storitev. Število navideznih vodov za stranko je odvisno od števila strankinih lokacij in lahko variira od enega samega voda (stranka z dvema lokacijama) do polne zankaste topologije za stranko, ki ima lokacije na vseh robnih točkah ponudnikovega omrežja.

Vsaka robna naprava ponudnika v omrežju je sposobna vzpostavljanja tunelov in signalizacijskih navideznih vodov z vsako robno napravo v omrežju ponudnika. Vsaka robna naprava ponudnika je tudi popolnoma sposobna zaznati MAC naslove vseh lokalno povezanih naprav in se z njimi povezovati z navideznimi vodi.

3.2 Komponente VPLS omrežij

Omrežja VPLS so sestavljena iz naslednjih osnovnih komponent [2]:

- **Priključitveno vezje** (Attachment Circuit – AC) je fizična ali virtualna povezava med robno napravo stranke in robno napravo ponudnika. V splošnem morajo biti vsi uporabniški paketi (vključno s paketi protokolov drugega in tretjega sloja) na priključitvenem vezju posredovani soležni lokaciji ponudnika.

- **Navidezni vod** (Pseudowire – PW) sestavljata virtualni kanal (VC) in tunel. Za vzpostavitev navideznega voda skozi VPLS omrežje potrebujemo signalizacijo (LDP ali BGP), s katero posredujemo informacijo o virtualnem kanalu. V VPLS omrežju je navidezni vod pravzaprav nek direkten kanal za transparenten transport uporabniških datagramov od lokalnega do soležnega priključitvenega vezja.

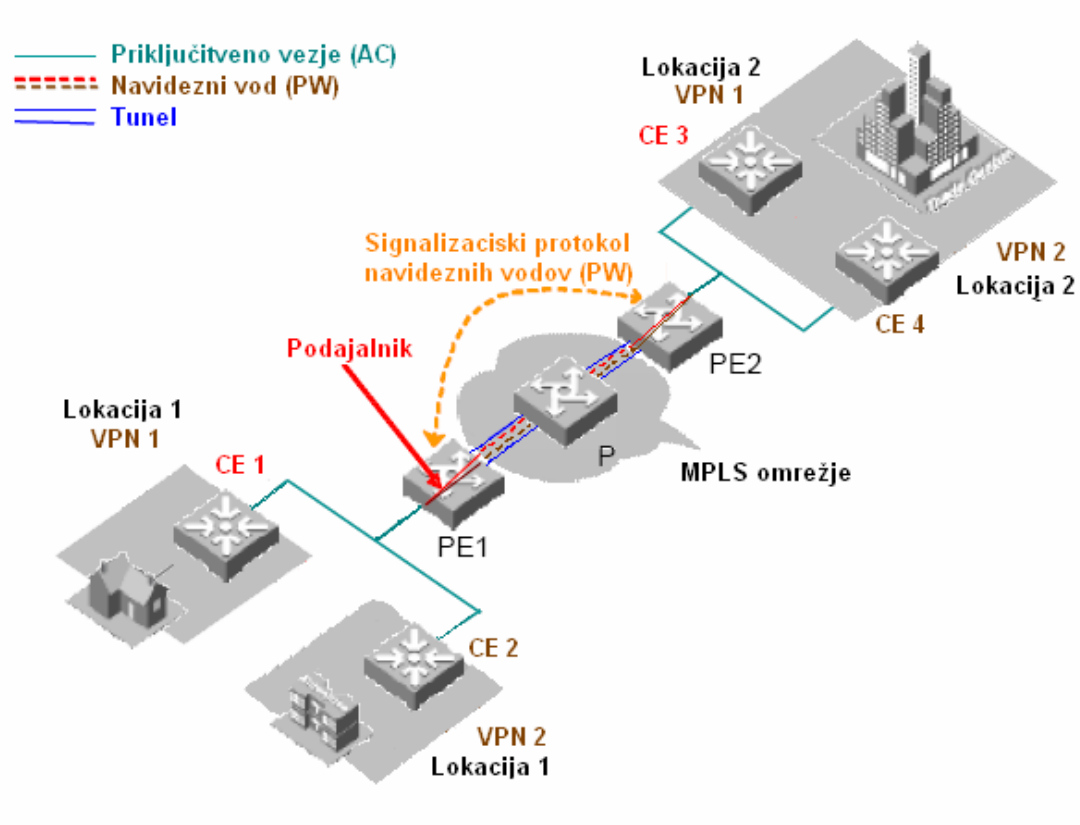
- **Podajalniki** (forwarders): Robna naprava ponudnika prejme datagrame, poslane prek priključitvenega vezja, podajalnik pa izbere navidezni vod za posredovanje paketov.

- **Tuneli**: uporabljajo se za prenos navideznih vodov. V enem tunelu je ponavadi več navideznih vodov, ponavadi so to MPLS tuneli. Tunel je direkten kanal med lokalno in soležno robno napravo ponudnika za transparenten prenos podatkov med njima.

Pomembna pojma pa sta tudi:

- **Enkapsulacija**: Paketi, posredovani preko navideznega voda, so zapakirani v standardni enkapsulacijski obliki in tehnologiji. Obstajata dva načina VPLS enkapsulacije paketov prek navideznih vodov: markirani način (Tagged mode) in osnovni način (Raw mode).

- **Signalizacija navideznih vodov**: Signalizacijski protokol za vzpostavljanje vzdrževanje navideznih vodov je osnova za implementacijo VPLS. Uporablja se lahko tudi za samodejno razpoznavanje soležnih robnih naprav. Trenutno se uporabljata dva signalizacijska protokola – LDP in BGP.



Slika 9 Osnovne komponente VPLS [2]

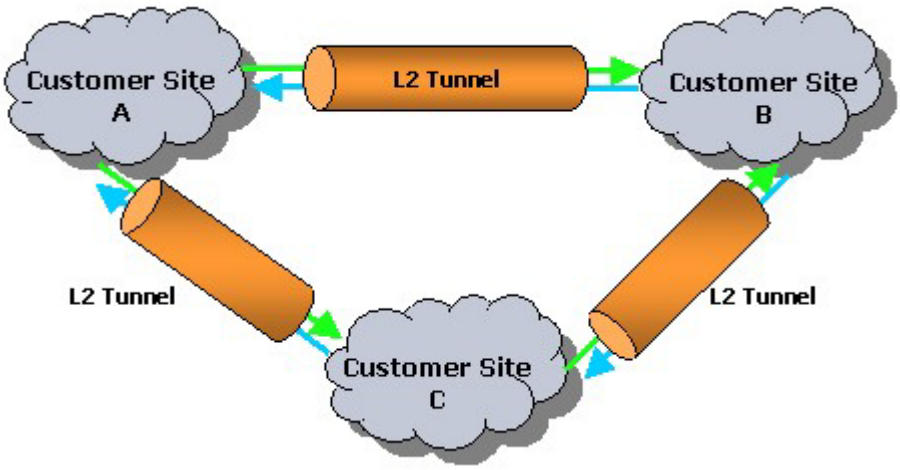
Na zgornji sliki so prikazane osnovne komponente VPLS v omrežju. Pretok podatkov preko VPLS omrežja si poglejmo na primeru navideznega zasebnega omrežja VPN 1 od lokacije stranke CE 1 do lokacije CE 3. CE 1 pošlje datagram preko priključitvenega vezja robni napravi ponudnika storitev PE 1. Ko robna naprava PE 1 prejme paket, podajalnik izbere navidezni vod, po katerem bo ta paket posredovan, sistem pa generira labelo navideznega voda na podlagi FDB vnosa navideznega voda in jo doda paketu, ki ga preko tunela pošlje robni napravi PE 2. Ko dospe do naprave PE 2, ta naprava na podlagi labele posreduje paket na ustrezno priključitveno vezje. Paket dospe na končno destinacijo CE 3.

Vsaka robna naprava ponudnika je tudi popolnoma sposobna zaznati MAC naslove vseh lokalno povezanih naprav in se z njimi povezovati z navideznimi vodi.

3.2.1 Preprečevanje pojava posredovalnih zank v omrežju

Pri protokolu Ethernet se za preprečevanje posredovalnih zank (forwarding loops) v omrežju uporablja t.i. protokol razširitve drevesa (STP - Spanning Tree Protocol).

V VPLS omrežnem modelu je predvideno, da so vse robne naprave ponudnika povezane v popolno zankasto topologijo navideznih vodov, kjer je zelo pomembno, da ne prihaja do pojavljanja posredovalnih zank v omrežju. Za preprečevanje pojava zank pri posredovanju paketov v VPLS se uporablja mehanizem deljenega horizonta (split horizon mechanism). Pri tem mehanizmu velja, da ne sme nobena robna naprava (PE) paketov, ki jih dobi od neke druge robne naprave, posredovati tretji robni napravi. V povezavi tega mehanizma s »full mesh« topologijo robnih naprav ponudnika tako zagotovimo dosegljivost in okolje brez posredovalnih zank za posredovanje VPLS paketov.



Slika 10 Popolna zankasta topologija (Full Mesh)[5]

Posredovalnim zankam v VPLS omrežju pa se ni mogoče izogniti v primeru, ko ima stranka (CE) več povezav z robno točko ponudnika (PE) ali pa imajo strankine naprave, povezane v VPLS VPN dodatne povezave med seboj. V teh primerih uporabimo druge metode, na primer STP protokol [2].

3.3 VPLS - koncept navideznih vodov

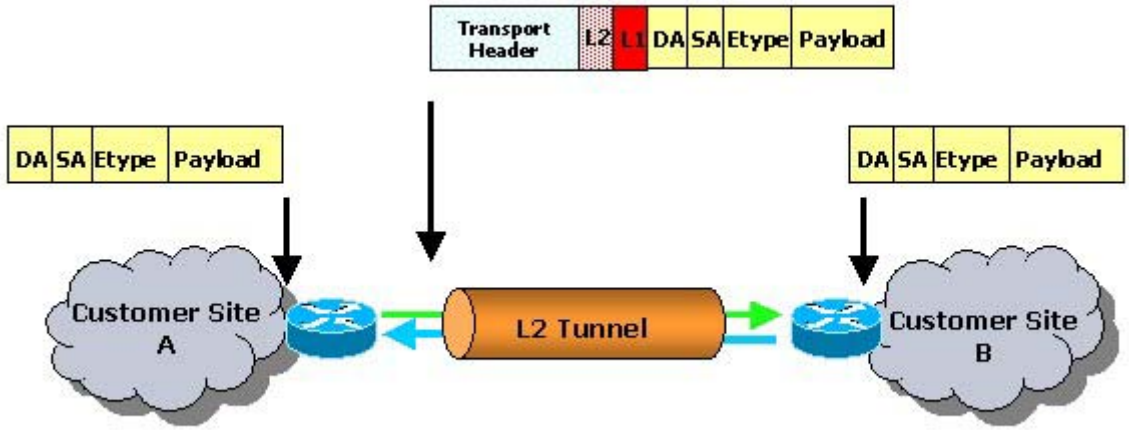
Navidezni vodi (Pseudowires – PW) so zveze od točke do točke med pari robnih usmerjevalnikov (PE) v omrežju. Njihova funkcija je emulacija storitev kot so ATM, Frame Relay, Ethernet in TDM preko ponudnikovega MPLS omrežja. Emulacijo teh storitev dosežemo z enkapsulacijo v MPLS format (po t.i. »martini draft« standardu).

Slika 11 Splošni Pseudowire koncept [5]

V splošnem imamo dva signalizacijska modela vzpostavljanja navideznih vodov:

- Model na osnovi LDP protokola
- Model na osnovi BGP protokola

Gradniki VPLS storitve so torej navidezni vodi, ki enkapsulirajo Ethernet pakete ali pakete katerega drugega protokola na drugem sloju.



Slika 12 MPLS Ethernet enkapsulacija [5]

Protokol za izmenjavanje label (LDP – Label Distribution Protocol) se uporablja za grajenje, vzdrževanje in podiranje navideznih vodov v omrežju ponudnika storitev po internetnem osnutku avtorja Martini. Popolna zankasta topologija LDP sej se vzpostavi med robnimi napravami ponudnika in preko teh sej se gradijo posamezni navidezni vodi. Graditev navideznega voda se začne tako, da neka robna naprava pošlje sporočilo za preslikavo labele (label mapping) drugi robni napravi. To sporočilo signalizira, da prihaja labelno komutirana pot (LSP – Label Switched Path) v robno napravo. Če končna robna naprava sprejme sporočilo, sproži enak proces v obratni smeri. Vsaka labelno komutirana pot je enosmerna, navidezni vod pa zahteva dve labelno komutirani poti, vsako v svojo smer.

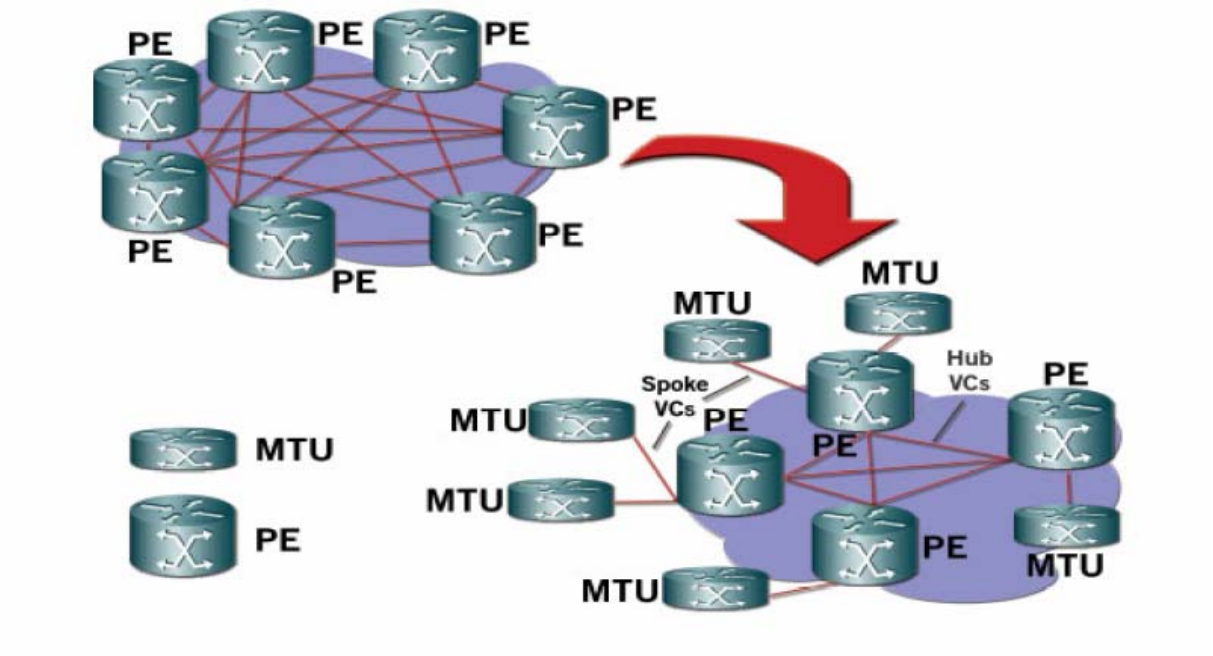
Namesto LDP protokola se lahko uporablja tudi MP-BGP protokol.

3.4 Hierarhični VPLS

Storitev VPLS omogoča ponudnikom storitev dostavo VPN storitev, ki temeljijo na Ethernet tehnologiji, z enakim nivojem podpore in zanesljivosti kot obstoječe storitve ATM ali Frame Relay. S kombinacijo ugodne cene in učinkovitosti Ethernet tehnologije in razširljivosti, zanesljivosti in prometnega inženiringa MPLS tehnologije, je VPLS postala tako učinkovita rešitev za večtočkovne Ethernet storitve na drugem sloju za poslovne uporabnike kot tudi infrastruktura za rezidenčne glasovne, video in podatkovne storitve (na primer Triple Play).

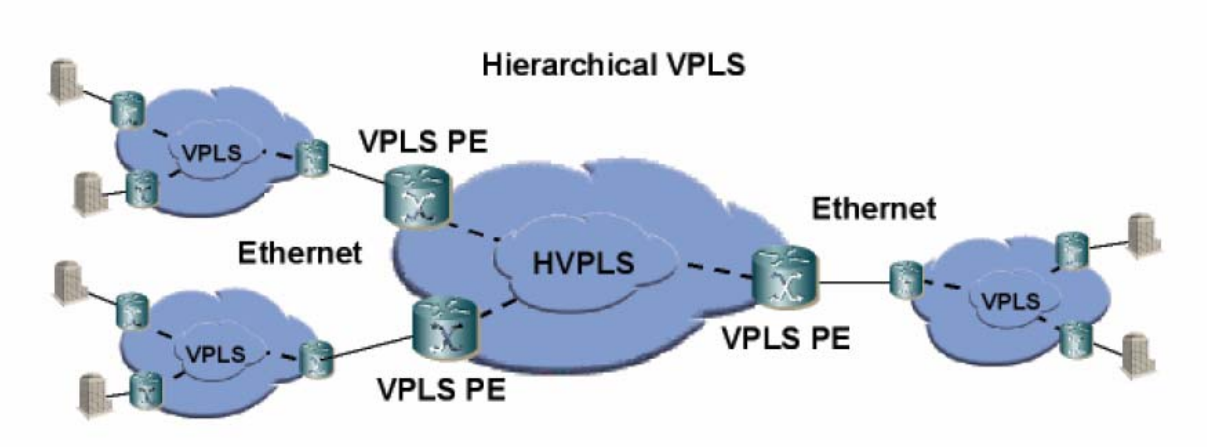
Do problemov pa pride, ko želimo VPLS storitev razširiti na zelo velika omrežja, kjer se popolna zankasta topologija povezav med posameznimi robnimi napravami zaradi kompleksnosti ne obnese najbolje. Izkušnje ponudnikov storitev [7] so pokazale da se popolna zankasta arhitektura VPLS najbolje obnese v omrežjih z največ 60 vozlišči, pri večjih pa pride do prevelike kompleksnosti zaradi povezav vsakega vozlišča z vsakim.

Za rešitev tega problema v velikih omrežjih so definirali novo metodo, tako imenovani hierarhični VPLS (HVPLS). HVPLS je pravzaprav način grajenja dvo ali večnivojskih hierarhičnih omrežij z vpeljavo novega MTU stikala (Multi Tenant Unit Switch), ki nam nudi MPLS funkcionalnosti, je cenovno ugodno in lahko upravljivo. MTU stikalo je povezano na robno točko ponudnika storitev (PE). S kreiranjem takšnih dvonivojskih omrežij, HVPLS omogoča razširitev omrežja na precej več kot 60 vozlišč.



Slika 13 Popolna zankasta topologija VPLS omrežja je nadgrajena z MTU stikali, ki so povezani v robne naprave ponudnika storitev [7]

Hierarhični VPLS zmanjšuje omejitve v zvezi z razširljivostjo z zmanjšanjem števila usmerjevalnikov v jedru omrežja in z zamenjavo robnih naprav ponudnika (povezanih v popolno zankasto topologijo) z MTU stikali, niso povezana v popolno zankasto topologijo, so pa velikokrat dvodomska (dual-homed). Vsako MTU stikalo lahko nudi storitve večjemu številu uporabnikov. Uporaba MTU stikal zmanjšuje signalizacijsko režijo in porabo pasovne širine, poenostavlja omrežno arhitekturo kar posredno izboljšuje zmogljivost in olajša upravljanje omrežja [7].



Slika 14 Hierarhična VPLS storitev [7]

Prednosti HVPLS

Ena izmed največjih prednosti HVPLS je premik replikacije prometa na rob omrežja, kjer za to poskrbijo MTU stikala. To zmanjšuje porabo pasovne širine v jedru omrežja in signalizacijsko režijo, kar zniža celotne stroške lastništva (TCO – Total Cost of Ownership). Zmanjšajo se tudi zakasnitve in trepetanje (jitter), kar izboljša kakovost in čistost storitev kot so prenos govora in videa preko IP protokola.

Še ena pomembna prednost uporabe MTU se izkaže pri omrežjih, ki se razprostirajo preko več držav in so podvržena različnim družbenim standardom, zakonom in regulacijam. Z implementacijo storitvenih pravil na lokalnem MTU stikalu se lahko prilagodimo določenim zahtevam regulatorja, kar bi bilo ob popolni zankasti topologiji težje izvedljivo.

4 Varnost v MPLS in VPLS

Najpogostejša možnost napada je sleparjenje (spoofing) ali spreminjanje paketov oz label. Toda labele so lokalnega značaja, in imajo enako vrednost le za en hop. Soležna usmerjevalnika se s pomočjo protokola za distribucijo label dogovorita o vrednostih label. Tako z spreminjanjem ali vstavljanjem drugih label ne bi dosegli prav dosti.

Če po [11] povzamem sklep testiranja IP-VPN omrežij na osnovi MPLS podjetja Cisco, lahko navedem ugotovitev, da so Ciscova MPLS VPN omrežja povsem varna zaradi naslednjih razlogov:

- Uporabnikova topologija omrežja ni razkrita zunanjemu svetu
- Uporabniki obdržijo svoj naslovni prostor in poljubno razpolagajo s svojimi zasebnimi ali javnimi IP naslovi
- Napadalci ne morejo dobiti dostopa v VPN ali omrežje ponudnika storitev
- Napadalec ne more vstaviti sleparske (spoofed) labele v Ciscovo MPLS omrežje

Ker pa so to le podatki z uradnega vidika podjetja, se moramo vseeno zavedati, da pri MPLS tehnologiji ni nobene enkripcije in da si uporabniki ponavadi robno (PE) napravo delijo z drugimi uporabniki. Zaradi tega imamo lahko določene pomisleke glede same varnosti. V nadaljevanju

4.1 Primeri napadov v MPLS omrežjih

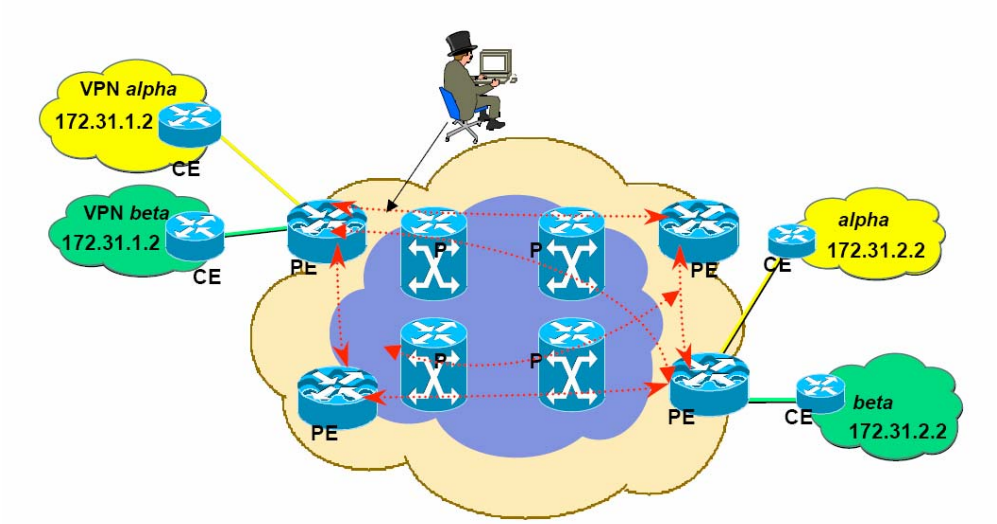
Zaradi same »zasebnosti« navideznega zasebnega omrežja, so zanimivi predvsem napadi, ki vključujejo prisluškovanje in nepooblaščen dostop. Možni napadi na MPLS VPN omrežje so torej naslednji:

Vstavitev labeliranega prometa na strani uporabnika (CE)
V tem primeru gre za to, da uporabnik A poskuša vstaviti pakete v navidezno zasebno omrežje uporabnika B. RFC 2547 nam pove, da labeliranih paketov, ki izhajajo iz nezaupnih (untrusted) virov, hrbtenični usmerjevalniki ne sprejmejo in jih torej zavržejo. Po [11] takšnega napada na Ciscovih usmerjevalnikih niso mogli izvesti.

Vstavitev labeliranega prometa prek interneta
V tem primeru poskuša internetni napadalec vstaviti pakete v navidezno zasebno omrežje nekega uporabnika. Za ta namen mora poznati IP naslove in vrednosti label in imeti mora dostop prek interneta do ponudnikovega usmerjevalnika. Po RFC 2547 pa bodo hrbtenični usmerjevalniki take pakete zavrgli zaradi nezaupnega vira. Tudi takšnega napada niso uspeli izvesti na Ciscovih usmerjevalnikih [11].

Spreminjanje MP-BGP sej, da se vzpostavijo »napačna VPN omrežja«
Za tak napad bi moral napadalec imeti dostop do hrbtenice omrežja in imeti prava orodja za napad na usmerjevalnik. Napadalec bi moral ali prestreči osnovno (inicializacijsko) BGP sejo ali pa odstraniti VPN poti (routes) in vstaviti nove. Obe možnosti sta težko uresničljivi, če pa bi se napad posrečil, bi utegnil imeti resnejše posledice.

Spreminjanje in vstavljanje label v hrbtenici omrežja
Tudi za ta napad potrebuje napadalec dostop do hrbtenice in pravo orodje za napad na usmerjevalnik. Če to ima, lahko zamenja vrednosti label in vstavi spremenjene pakete v hrbtenično omrežje [11].



Slika 15 Napad na MPLS omrežje s spreminjanjem label v hrbteničnem omrežju [11]

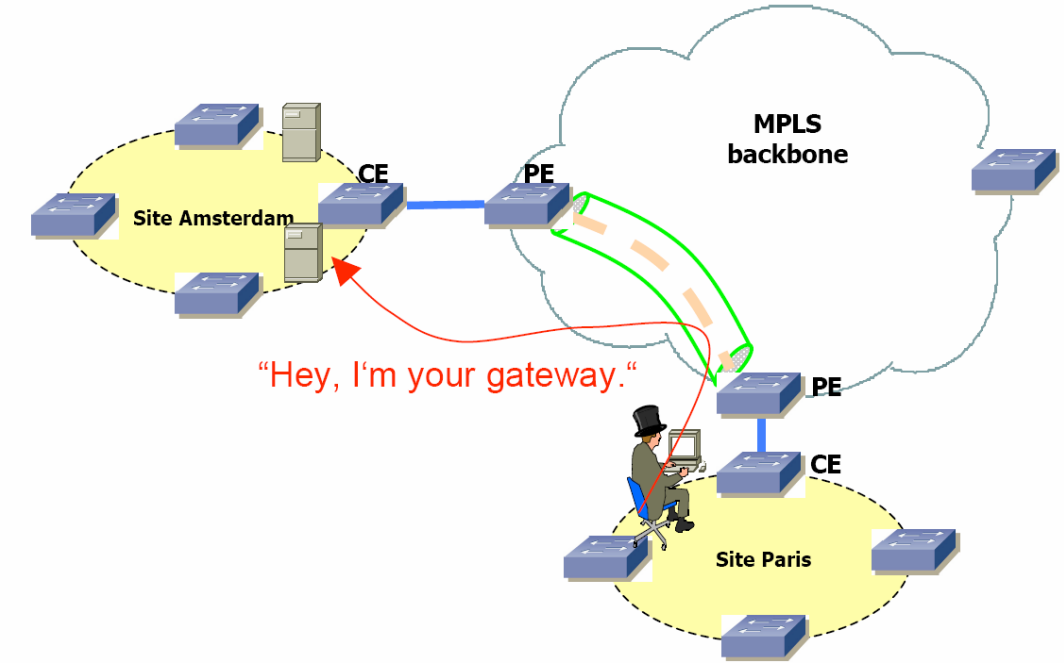
Zaključek
Spreminjanje label in posledično prehajanje med VPN omrežji je en izmed možnih napadov. Je pa samo enosmeren, in ga ne bomo uspeli detektirati. Tudi napadalec si z njim ne bo veliko pomagal. Spreminjanje MP-BGP paketov predstavlja resnejšo nevarnost, a je težje izvedljivo. Oba tipa napadov potrebujeta dostop do hrbtenice omrežja ponudnika MPLS storitev. Večinoma pa je hrbtenica omrežja ponudnika storitev varna in »zaupna« (trusted). Ponudnik lahko do neke mere tudi jamči za varnost v svojem MPLS omrežju.

4.2 Primeri napadov na VPLS omrežje

Glede na to, da za storitev navideznih zasebnih LAN omrežij uporabljamo MPLS hrbtenico, so seveda možni tudi napadi na MPLS omrežje, ki sem jih naštel v prejšnjem poglavju. Poleg tega lahko dodamo še naslednja napada [11]:

- Napadi preko VPLS oblaka (over-the-cloud attacks)
- Napadi na naprave, na katerih deluje VPLS
- Splošni napadi na drugem sloju (L2)

Napadi preko oblaka
Ta vrsta napadov je odvisna od stopnje transparentnosti VPLS oblaka. V primeru popolne transparentnosti je možno izvesti vse klasične napade na drugem sloju preko VPLS oblaka, kot so vohljanje (sniffing), sleparjenje (spoofing), ARP-napadi, sleparjenje MAC naslovov, manipulacija STP protokola in podobno.



Slika 16 Napad preko VPLS oblaka [11]

Napadi na naprave, na katerih deluje VPLS

Napadi na naprave so odvisni od tega, kakšno funkcijo opravlja sama naprava. Po [11] je najlažje izvedljiv napad s poplavljanjem MAC naslovov (MAC address flooding), kar procesorsko obremeni napravo (stikalo).

Ker celoten se celoten VPLS oblak obnaša kot veliko stikalo, si moramo za lažje razumevanje problematike varnosti v VPLS pogledati možne napade na stikalo.

Naj naštejem nekaj najpogostejših primerov napadov na drugem sloju:

- Preskakovanje VLAN-ov (VLAN hopping) – je napad, kjer gre za pošiljanje paketov na vrata (port) naprave, ki normalno ni dostopen končnemu uporabniku. VLAN hopping napad se lahko uporabi za krajo občutljivih uporabniških podatkov kot so na primer gesla, za spreminjanje in uničevanje podatkov, ali za razpečevanje virusov in trojanskih konjev prek omrežja.
- MAC napadi (na primer poplavljanje MAC naslovov, preobremenitev naprav v omrežju)
- DHCP napadi (Dynamic Host Configuration Protocol) – možni so razni DoS (Denial of Service) napadi na strežnik
- ARP napadi - ARP (Address Resolution Protocol) je protokol s katerim stikala iščejo napravo z določenim MAC naslovom v omrežju. V primeru napada gre ponavadi za ponarejene odgovore o identiteti naprave (ARP spoofing).
- Sleparjenje (spoofing) – nepooblaščen vdor v sistem s prevzemom lažne identitete
- Vohljanje (sniffing) – gre za spremljanje vsega odhodnega prometa nekega uporabnika. Na ta način se lahko napadalec dokoplje do nezaščitenih (clear text) gesel in podobnih podatkov.
- Drugi napadi…

Zaključek:

Ker je za vse naštete napade potrebno imeti dostop do omrežja, se je potrebno potruditi, da nepooblaščenim osebam ne dovolimo dostopa. To dosežemo na primer s filtrirnimi mehanizmi kot so seznami za nadzor dostopa (ACL – Access Control Lists). Promet uporabniških naprav je dobro tudi podrobneje spremljati. Prav tako je potrebno podrobno definirati odgovornosti ponudnika MPLS in VPLS storitev proti uporabniku oziroma stranki.

Preventivni ukrepi, s katerimi lahko preprečimo napade:

- Potrebno je omejiti dostop do upravljanja stikal, tako da osebe iz nezaupnih (non-trusted) omrežij ne morejo zlorabljati vmesnikov in protokolov za upravljanje
- Potrebno je izklopiti (shut down) vrata (ports), ki niso v uporabi

- Potrebno je uporabiti varnostne mehanizme vrat (port security) stikala za omejitev števila dovoljenih MAC naslovov, ter tako zagotoviti varnost pred napadi s poplavljanjem MAC naslovov
- Na »sovražnem« omrežju se je dobro se je izogibati uporabi upravljalskih protokolov, ki delujejo v načinu clear text
- Uporaba filtrirnih mehanizmov in seznamov za nadzor dostopa
- Uporaba varnostnih mehanizmov vrat z določanjem MAC naslova (MAC-based port security) prepreči neavtoriziranim postajam dostop do stikala
- DHCP filtriranje
- Večnivojska zaščita pri konzolnem dostopu do stikala
- Nadzor nad oddaljenim dostopom do stikala (na primer Telnet)

5 Sklep

VPLS tehnologijo lahko uporabimo ne le za mestne Ethernet storitve, ampak tudi za povezovanje velemestnih (MAN) omrežij, ki temeljijo na različnih tehnologijah, kot so sinhrona digitalna hierarhija (SDH) ali elastični paketni obroč (RPR - Resilient Packet Ring). Storitev navideznih zasebnih LAN omrežij je idealna za povezavo več lokacij v istem velemestnem omrežju.

VPLS je cenovno ugodna metoda, saj temelji na tehnologiji Ethernet, ki je preprosta in poceni. Je večprotokolna, kar pomeni, da podpira prenos različnih komunikacijskih protokolov preko MPLS hrbtenice – AtoM (Any Transport over MPLS).

Uporabnikom omogoča uporabo lokalne usmerjevalne domene, tako da uporabnik ne razkrije informacije o topologiji svojega omrežja in naslovnega prostora ponudniku storitev. Uporabniške naprave (CE) so lahko preproste, na primer Ethernet stikalo, most ali spojnik.

Uporaba dinamične signalizacije v MPLS za vzpostavljanje novih labelno komutiranih poti omogoča hiter preklop prometa na rezervno pot. Uporaba prometnega inženiringa za doseganje kakovosti storitev od konca do konca (end-to-end QoS) VPLS omrežja podpira uporabo storitev, ki potrebujejo zagotovljeno pasovno širino ter minimalne zakasnitve (na primer prenos govora in videa preko protokola IP).

Kar se varnosti tiče, je ob uporabi priporočenih varnostnih mehanizmov VPLS tehnologija povsem varna, in jo v praksi uporabljajo velika podjetja in mednarodne korporacije (na primer banke). V splošnem je dandanes tako, da uporabniki morajo zaupati ponudnikom storitev, da je njihovo omrežje varno. Če pa gre za zelo zaupne posle, pa lahko seveda tudi v VPLS ali MPLS omrežju uporabimo enkripcijo za dodatno zaščito prenašanih podatkov.

6 Seznam uporabljenih kratic

Kratica	Angleški pomen	Slovenski pomen
AC	Attachment Circuit	Priključitveno vezje
BGP	Border Gateway Protocol	Protokol mejnih usmerjevalnikov
CE	Customer Edge device	Robna naprava uporabnika
DLCI	Data Link Connection Identifier	Identifikator zveze v sloju podatkovne povezave
FEC	Forward Equivalence Class	Ekvivalentni razred predajanja
FIB	Forwarding Information Base	Posredovalna informacijska baza
LAN	Local Area Network	Lokalno omrežje
LDP	Label Distribution Protocol	Protokol za distribucijo label
LER	Label Edge Router	Robni labelni usmerjevalnik
LSP	Label Switched Path	Labelno komutirana pot
MTU-s	Multi Tenant Unit switch	Večuporabniško stikalo
PE	Provider Edge	Robna točka ponudnika storitev
PW	Pseudo wire	Navidezni vod
RSVP	Resource Reservation Protocol	Protokol z rezervacijo virov
STP	Spanning Tree Protocol	Protokol razširjajočega drevesa
VLAN	Virtual LAN	Navidezni LAN
VPLS	Virtual Private LAN Service	Storitev navideznega zasebnega LAN omrežja

7 Seznam uporabljenih virov

[1] Virtual private LAN Service and Virtual Private Wire Service – a market and technology overwiew – Cisco Systems White Paper http://www.cisco.com/application/pdf/en/us/guest/tech/tk891/c1550/cdccont_0900aecd80162178.pdf

[2] VPLS Technical White Paper, Huawei Technologies, www.huawei.com

[3] MPLS VPNs: Layer 2 or Layer 3? Technology white paper #128, Tim Wu, Riverstone Networks, http://www.riverstonenet.com/pdf/mpls_vpns_layer2_or_layer3.pdf

[4] White paper: VPLS: Scalable Transparent LAN Services, Mike Capuano, Juniper Networks, http://www.juniper.net/solutions/literature/white_papers/200045.pdf

[5] VPLS standards, http://vpls.org

[6] Tutorial on VLANs - Part 2, Manikantan Srinivasa, http://www.commsdesign.com/showArticle.jhtml?articleID=26806955

[7] Riverstone Networks Whitepaper: HVPLS – Scaling VPLS to the next level http://www.riverstonenet.com/pdf/hvpls.pdf

[8] Marc Lasserre, Vach Kompella, Virtual Private LAN Services over MPLS, Internet Draft, http://bgp.potaroo.net/ietf/ids/draft-ietf-l2vpn-vpls-ldp-08.txt

[9] IEC tutorial: MPLS, http://www.iec.org/online/tutorials/mpls/

[10] MPLS in Private Networks: Is it a good idea?, Jim Metzler, Juniper Networks, http://www.juniper.net/solutions/literature/white_papers/mpls_private.pdf

[11] Enno Rey, MPLS and VPLS security, http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Rey-up.pdf