Universitatea Națională de Știință și Tehnologie POLITEHNICA București

Facultatea de Electronică, Telecomunicații și Tehnologia Informației

Analiza şi implementarea VPN peste o reţea IP MPLS

Proiect de diplomă

Prezentat ca cerință parțială pentru obținerea titlului de *Inginer*

în domeniul *Inginerie electronică, telecomunicaţii şi tehnologii informaţionale*

programul de studii de licență *Rețele și software de telecomunicații*

Conducător științific

Prof. Dr. Ing. Roxana Zoican

Absolvent

Pop Ştefan

2024

Declarație de onestitate academică

Prin prezenta declar că lucrarea cu titlul *Analiza şi implementarea VPN peste o reţea IP MPLS*, prezentată în cadrul Facultății de Electronică, Telecomunicații și Tehnologia Informației a Universității Naționale de Știință și Tehnologie POLITEHNICA București ca cerință parțială pentru obținerea titlului de Inginer în domeniul *Inginerie electronică, telecomunicaţii şi tehnologii informaţionale* programul de studii *Rețele și software de telecomunicații* este scrisă de mine și nu a mai fost prezentată niciodată la o facultate sau instituție de învățământ superior din țară sau străinătate.

Declar că toate sursele utilizate, inclusiv cele de pe Internet, sunt indicate în lucrare, ca referințe bibliografice. Fragmentele de text din alte surse, reproduse exact, chiar și în traducere proprie din altă limbă, sunt scrise între ghilimele și fac referință la sursă. Reformularea în cuvinte proprii a textelor scrise de către alți autori face referințăla sursă. Înțeleg că plagiatul constituie infracțiune și se sancționează conform legilor în vigoare.

Declar că toate rezultatele simulărilor, experimentelor și măsurătorilor pe care le prezint ca fiind făcute de mine, precum și metodele prin care au fost obținute, sunt reale și provin din respectivele simulări, experimente și măsurători. Înțeleg că falsificarea datelor și rezultatelor constituie fraudă și se sancționează conform regulamentelor în vigoare.

București, 25.06.2024

Absolvent *POP Ştefan*

Universitatea "Politehnica" din Bucureşti **Anexa 1**
Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei
Program de studiu

TEMA PROIECTULUI DE DIPLOMĂ

a studentului **POP M.D. Ştefan, 444D**

1. Titlul temei: Analiza şi implementarea VPN peste o reţea IP MPLS

2. Descrierea temei și a contribuției personale a studentului (în afara părții de documentare):
Lucrarea are drept scop analiza modului de implementare MPLS VPN, tratând următoarele aspecte: analiza arhitecturii, a modului de operare şi a avantajelor utilizării protocolului MPLS; studiul tehnologiei VPN şi a modelelor Overlay VPN şi Peer-to-Peer VPN; analiza arhitecturii şi rutării MPLS VPN; implementarea în simulatorul de reţea GNS3 a unei reţele MPLS VPN, utilizând rutere Cisco; analiza, pe echipamente, a traficului de rutare, cu scopul de a studia principalele protocoale de comunicaţie implicate în funcţionarea reţelelor de tip MPLS VPN (OSPF, EIGRP, LDP, BGP). Sunt implementate următoarele studii de caz: analiza tabelelor de rutare pentru rutele de tip CE (Customer Edge) şi stabilirea convergenţei; analiza capabilităţii de scalare rapidă a reţelei prin adăugarea/ştergerea unor site-uri;determinarea lăţimii de bandă, întârzierii sau ratei de pierdere a pachetelor cu scopul de a stabili performanţele reţelei; capturarea, folosind analizorul Wireshark, a pachetelor ce se transmit in cadrul reţelei MPLS VPN şi analiza acestora; analiza, pe baza reţelei studiate, a principalelor avantaje/dezavantaje ale implementării tehnologiei MPLS VPN în cadrul reţelelor IP clasice.

3. Discipline necesare pt. proiect:
Reţele şi servicii, Arhitecturi şi protocoale de comunicaţii, Comunicaţii de date

4. Data înregistrării temei: 2023-12-10 12:09:00

Conducător(i) lucrare,
Prof. dr. ing. Roxana ZOICAN

Student,
POP M.D. Ştefan

Director departament,

Decan,
Prof. dr. ing. Mihnea UDREA

Cod Validare: **57e7ff8c42**

CUPRINS

LISTA FIGURILOR

LISTA ACRONIMELOR

MPLS - Multiprotocol Label Switching

LDP - Label Distribution Protocol

HDLC - High Data Level Communication (Cisco)

OSPF - Open Shortest Path Fast

BGP - Border Gateway Protocol

VPN - Virtual Private Network

L2VPN - Layer 2 VPN

L3VPN - Layer 3 VPN

MAC - Medium Access Control

MP-BGP - Multiprotocol Border Gateway Protocol

TE - Traffic Engineering

RSVP - Resource Reservation Protocol

QoS - Quality of Service

LER - Label Edge Router

LSP - Label Switching Path

LSR - Label Switching Router

PE - Provider Edge Router

P - Provider Router

CE - Customer Edge Router

VPLS - Virtual Private LAN Service

VPWS - Virtual Private Wire Service

AToM - Any Transport over MPLS

EoMPLS - Ethernet over MPLS

VC - Virtual Circuit

AC - Attachment Circuit

IP - Internet Protocol

VRF - Virtual Routing Forward

FEC - Forwarding Equivalence Class

LIFO - Last-In,First-Out

LIB - Label Information Base

RIB - Routing Information Base

LFIB - Label Forwarding Information Base

OSI - Open Systems Interconnection

WAN - Wide Area Network

LAN - Local Area Network

VLAN - Virtual LAN

ATM - Asynchronous Transfer Mode

L2TP - Layer 2 Tunneling Protocol

GRE - General Routing Encapsulation

IPSec - Internet Protocol Security

RD - Route Distinguisher

RT - Route Target

TLV - Type Length Value

MTU - Maximum Transmission Unit

SFD - Start Frame Delimiter

FCS - Frame Check Sum

TCP - Transmission Control Protocol

DUAL - Diffusing Update Algorithm

EIGRP - Ehnanced Interior Gateway Routing Protocol

RTT - Round-Trip Time

TTL - Time to Live

BoS - Bottom of Stack

ICMP - Internet Control Message Protocol

VPNv4 – Virtual Private Network version 4

IPv4 – Internet Protocol version

INTRODUCERE

Tehnologia Multiprotocol Label Switching (MPLS) reprezintă o tehnologie de comutare a etichetelor care oferă capacitatea de a configura cai orientate pe conexiune (“connection-oriented”) peste o rețea IP fără conexiune (“connectionless”).

În rețelele IP tradiționale, ce nu utilizează tehnologia MPLS, exista funcțiile principale: determinarea rutelor (“routing”), adică folosesc un algoritm de căutare a drumurilor cu costul minim si construirea tabelelor de rutare, dirijarea (“forwarding”) pachetelor, ce sosesc pe o interfață de intrare a ruterului, spre una sau mai multe interfețe de ieșire. În acest tip de rețele, fiecare router compară adresa destinație a pachetului din antetul de nivel trei al pachetului IP cu informațiile pe care le deține in tabelul de rutare propriu și determină pe cont propriu next-hop-ul pachetului. Această metodă reprezintă de fapt tipul de rețea “fără conexiune” (IP “connectionless”) adica fiecare router analizează în mod independent de routerele anterioare fiecare pachet. Acest tip de conexiune este foarte util deoarece prezintă aspectul de flexibilitate al protocolului Internet, dar consumă mult timp și resurse pentru procesarea fiecărui pachet.

In rețelele ce utilizează tehnologia MPLS, tehnologie ce folosește comutarea de etichete, doar primul router din rețea utilizează tehnica de IP lookup pentru a determina destinația finala a pachetului. Routerul inițial (“ingress router”) îi adaugă pachetului un antet MPLS bazat pe informațiile anterioare ale pachetului si stabileste calea spre destinația finala a pachetului denumita LSP (Label Switch Path). Cand pachetul ajunge la ultimul router din rețea (egress router) acesta elimină eticheta și o transmite mai departe catre destinația finală a pachetului.

MPLS este considerat un protocol independent de orice alt protocol de rutare, dar este denumit multiprotocol deoarece permite folosirea a multiple protocoale cum ar fi protocolul Internet (IP), modul de transport asincron (ATM) si protocoalele de rețea de tip relee de cadru (Frame Relay). Un alt avantaj adus de tehnologia MPLS este faptul că reduce congestia rețelei, deci prezintă performanțe si viteze ridicate. Prin intermediul acestei tehnologii este introdus și conceptul de Traffic Engineering, ce permite routerului de intrare intr-o rețea de tip MPLS să calculeze eficient calea către ultimul nod din rețeaua respectivă. De asemenea prin intermediul ingineriei traficului se evită suprasolicitarea sau subsolicitarea link-urilor deoarece cunoaște lățimea de bandă configurată static, atributele link-urilor (intarzieri, jittere) și se adaptează automat la modificarea lățimii de bandă.

Un serviciu foarte des utilizat in rețelele de tip MPLS este serviciul Virtual Private Network (VPN). Acest serviciu emulează o rețea privată peste o rețea publică de tip MPLS. Majoritar, companiile folosesc acest serviciu pentru a conecta mai multe site-uri prin intermediul unui furnizor de servicii. Serviciul VPN poate fi imparțit in doua categorii: Layer 2 VPN si Layer 3 VPN.

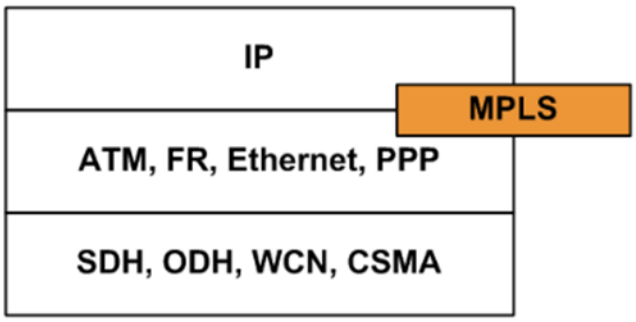
Scopul acestei lucrari este analiza și implementarea a tehnologiei MPLS VPN, prin intermediul simulatorului GNS3, unde vor fi configurate routere Cisco IOSv 15.6. De asemenea va fi prezentată o comparație intre performanțele serviciilor MPLS VPN Layer 2 și MPLS VPN Layer 3. Totodată vor fi efectuate defecțiuni asupra legăturilor din rețea pentru a se analiza capabilitatea de scalare și performanțele rețelei afectate.

CAPITOLUL 1. Multiprotocol Label Switching

1.1 MPLS – Prezentare general

Tehnologia MPLS este o tehnologie IP dezvoltată de către IETF în anul 1990 pentru a combate dezavantajele rețelelor IP clasice. [5] MPLS utilizează un tip de comutare similară cu cea din tehnologia ATM, dar simplificată pentru a implementa comutarea de date, atât la Layer-ul 2, cât și la Layer-ul 3. Fiecărui pachet IP îi este atribuită o etichetă pe bază căreia îi este stabilită ruta și prioritatea pachetului IP, ruterul nu mai preia informațiile din antetul pachetului, ci rutarea se execută pe baza etichetelor. [6] Datorită faptului că transmiterea pachetelor se face prin comutare de etichete, tehnologia MPLS este considerată o tehnologie de tip ”Layer 2.5”.

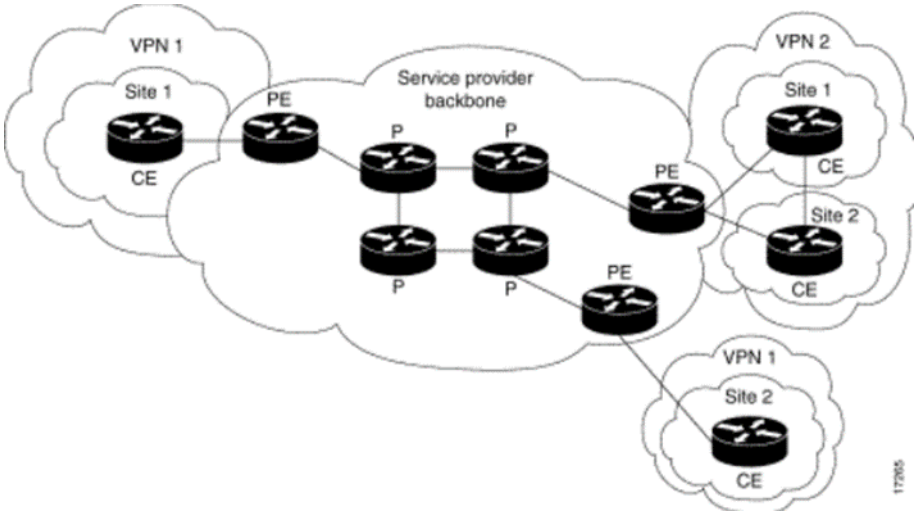
Termenul ”Multiprotocol” indică faptul că tehnologia suportă multiple protocoale de Layer 2 precum: Ethernet, ATM, FR, cât și de Layer 3 (IP). Din acest motiv, prin intermediul MPLS se poate crea o rețea de tip ”connection-oriented” peste o rețea de tip ”connectionless”.



Figură 1.1 Eticheta MPLS in stiva OSI [6]

Arhitectura unei rețele de tip MPLS VPN conține rutere specifice care au diferite roluri:

- Customer Edge Router (CE) – Este un ruter ce se află la marginea rețelei clientului și se conectează la rețeaua MPLS prin intermediul ruterului PE.
- Provider Egde Router (PE) – Se află la marginea rețelei provider-ului de servicii, face legătura între rețeaua provider și rețeaua client.
- Provider Router (P) – Se află în rețeaua provider-ului.

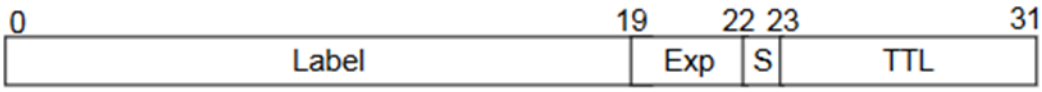


Figură 1.2 Rețea de tip MPLS [11]

Într-o rețea de tip MPLS, datorită conceptului de comutare de etichete, primul ruter din rețea (Ingress Label Edge Router) identifică destinațiile fluxurilor de pachete și le clasifică în clase de echivalență ("Forwarding Equivalence Class" - FEC). Fiecărui FEC îi corespunde o etichetă de lungime fixă de 32 biți, numită eticheta MPLS sau "label". [1].

O clasă de echivalență (FEC) reprezintă un grup sau un flux de pachete ce sunt trimise pe aceeași rută și sunt considerate echivalente din punct de vedere al dirijării. Toate pachetele care aparțin unei clase de echivalență conțin aceeași etichetă, dar există cazuri în care pachetele pot avea aceeași etichetă, dar să aparțină altei clase de echivalență. Acest lucru se datorează câmpului "EXP" din antetul pachetului MPLS. [2]

Antetul MPLS, întâlnit des sub numele de "eticheta" (Label) este un identificator de lungime fixă de 32 biți, amplasat între antetele nivelelor 2 și 3, local pentru o legătură între două rutere ce îndeplinesc funcțiile MPLS (Label Switch Router). Eticheta MPLS indentifică clasa de echivalență pentru fiecare pachet, astfel oferă o rută predeterminată într-o rețea de tip MPLS către destinația finală a fiecărui pachet. [9]



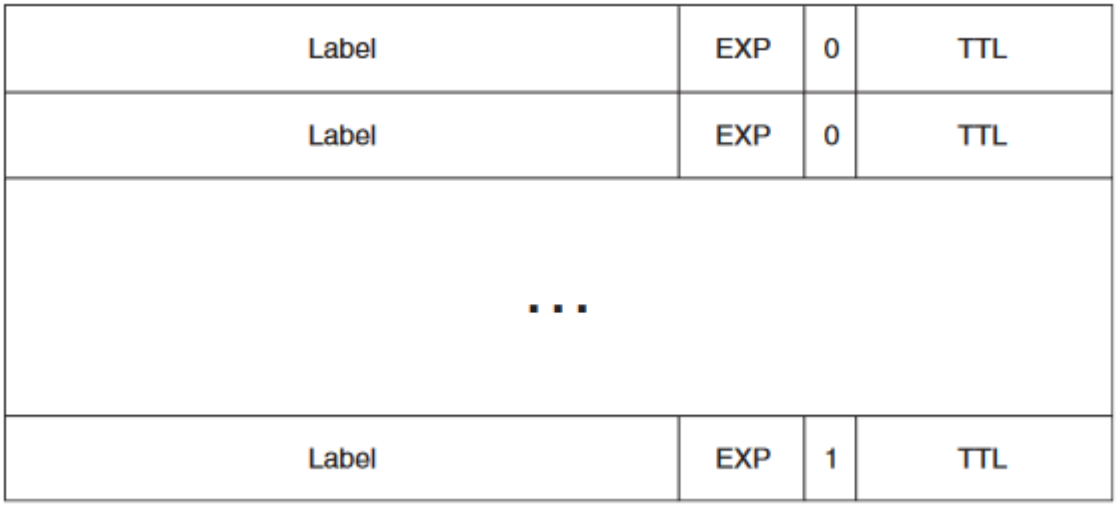
Figură 1.3 Formatul antetului MPLS [9]

Antentul este compus din 4 câmpuri:

- Label conține 20 de biți – indică valoarea numerică a etichetei,
- EXP (3 biți) – utilizat pentru Quality of Service (QoS),

- S (1 bit) – identifică care este ultima etichetă din stivă,
- TTL (8 biți) – este similar cu câmpul Time-To-Live din adresele IP tradiționale și indică timpul de viață al pachetului.

Stiva MPLS reprezintă un set de etichete ordonate. Un pachet de tip MPLS poate să conțină mai multe etichete, fără să existe un număr limită. Din acest motiv, câmpul de un bit S, din antetul pachetului identifică ultima etichetă din stivă. Dacă valoarea câmpului este 0, înseamnă că mai există etichete în partea inferioară a stivei, iar dacă valoarea este 1 este ultima etichetă din stivă. Eticheta de lângă câmpul de nivel de legătură al pachetul este numită etichetă din exterior (Outer Label), iar cea de lângă câmpul de nivel de rețea este denumită etichetă din interior sau etichetă de la bază (Inner/Bottom Label). Organizarea etichetelor în stivă se face după regula LIFO (Last-In, First -Out). [9]



Figură 1.4 Stiva de etichete [2]

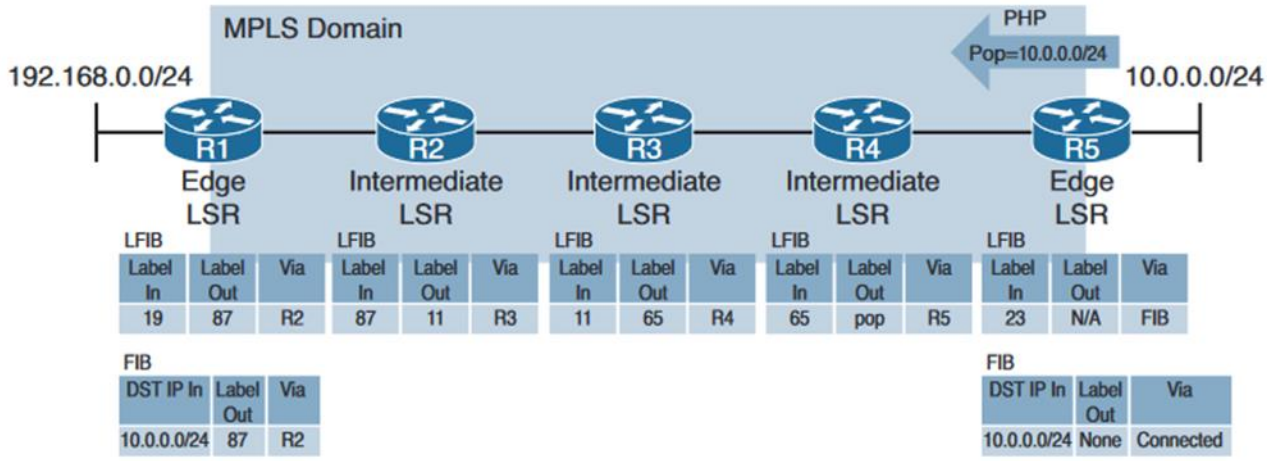
Unele aplicații de tip MPLS necesită mai multe etichete în stivă pentru a putea dirija pachetele, precum MPLS VPN sau AToM. [2]

Eticheta are o semnificație la nivel local, deoarece este modificată la fiecare pas din ruta pachetului și nu este asociată cu interfața specifică ruterului prin care intră pachetul. Fiecare pachet cu o anumită etichetă este tratat identic indiferent de interfața prin care trece.

Ruterele ce îndeplinesc funcțiile specifice rețelelor de tip MPLS sunt de două tipuri: Label Edge Router (LER), ruter de frontieră al domeniului MPLS și Label Switch Router (LSR), ruter intern al domeniului MPLS. LER interconectează un domeniu de tip non-MPLS de un domeniu de tip MPLS. Acesta este de clasificat astfel: de intrare (ingress) și de ieșire (egress).

Ruterul de intrare clasifică pachete ce intră în domeniul MPLS în clase de echivalență și prin operațiunea PUSH, care atribuie pachetelor o etichetă MPLS. De asemenea, ele determină rutele pachetelor în rețeaua MPLS, numite Label Switched Path (LSP).

Ruterul de ieșire are rolul de a face operațiunea de POP asupra stivei MPLS și elimină eticheta atribuită pachetului și dirijează pachetul către destinația acestuia. Ruterul de ieșire este capabil de o funcție numită Penultimate Hop Popping (PHP), prin care ruterul de frontieră își anunță vecinii că este ultimul din rețeaua MPLS printr-o etichetă specială numită eticheta implicit NULL (implicit NULL label) ce are valoarea 3. Prin această funcție penultimul ruter din rețea va elimina eticheta prin acțiunea POP, iar acest lucru va micșora dimensiunea pachetului. Ruterul de comutare (LSR) are ca funcție comutarea de etichete a pachetelor din rețea. Când acest ruter primește un pachet, analizează eticheta și determină next-hop-ul asociat LSP-ului respectivului pachet, realizează acțiunea de SWAP prin care elimină eticheta inițială și atribuie o altă etichetă, dirijând apoi pachetul către următorul ruter din rețea.



Figură 1.5Procesele de PUSH/SWAP/POP pentru etichetele MPLS și funcția de PHP [7]

Din punct de vedere arhitectural protocolul MPLS este divizat în două planuri:

- Control Plane – Sunt interschimbate informații de rutare specifice nivelului rețea, dar și etichete. Protocoalele specifice acestui plan sunt protocoalele de rutare compatibile cu tehnologia MPLS: OSPF, IS-IS, BGP, EIGRP, dar și protocoale prin care se realizează schimbul de etichete: LDP și RSVP.

- Data Plane – în planul de date are loc transmiterea pachetelor pe baza etichetelor print-un mecanism simplu de transmitere ale pachetelor.

1.2 Protocoale de distribuție ale etichetelor

Protocoalele de distribuție ale etichetelor sunt esențiale în rețelele de tip MPLS deoarece acestea au rol în distribuirea și gestionarea etichetelor între ruterele rețelei. De asemenea, prin determinarea etichetelor se stabilesc și LSP-urile care pot fi create în mod static și dinamic. Pe baza LSP-urile se crează o bază de date a etichetelor numită Label Information Base (LIB), în care sunt stocate informații referitoare la comutarea etichetelor de către fiecare router LSR de-a lungul rețelei. În contextul unor rețele de dimensiuni mari, crearea statică a LSP-urilor nu este eficientă.

1.2.1 Label Distribution Protocol (LDP)

Protocolul Label Distribution Protocol (LDP) a fost introdus în anul 2001 de către IETF nume complet pentru distribuirea etichetelor în rețelele de tip MPLS. [5] LDP este un protocol de control ce clasifică clasele de echivalență și se ocupă de distribuirea etichetelor, iar prin intermediul lui se stabilesc și mențin LSP-urile. Prin intermediul acestui protocol există două tipuri de distribuire ale pachetelor:

- Downstream on demand – Această metodă de distribuire permite ruterelor LER să trimită o cerere de tip LDP către un next-hop determinat pe bază tabelei de rutare, mesaj ce ajunge în final la ruterul de ieșire din rețeaua MPLS. Ruterul ce inițiază această cerere primește la final un mesaj de confirmare prin care anunță că LSP-ul a fost stabilit.
- Unsolicited Downstream – Ruterele de tip LSR trimit mesaje către toți vecinii cu informații despre etichete, iar acestea ajung din vecin în vecin la ruterele de tip LER. [3]

Pentru stabilirea sesiunii LDP sunt necesare mai multe tipuri de mesaje. Mesajele de tip “discovery”, prin intermediul cărora este anunțată și menținută prezența ruterelor de tip LSR, mesajele de tip “session” sunt utilizate pentru a stabili, menține sau închide sesiunile dintre ruterele LSR, mesajele de tip “advertisement” clasifică fiecare etichetă către un FEC, iar mesajele de tip “notification” semnalează erorile. Toate mesajele de tip LDP respectă formatul: tip, lungime, valoare (TLV). Protocolul LDP utilizează portul TCP 646, iar ruterul de tip LSR cu ruter ID-ul mai mare stabilește o conexiune de acest tip către alt LSR. Pentru menținerea sesiunilor LDP sunt trimise periodic mesaje de tip “Hello”. [3]

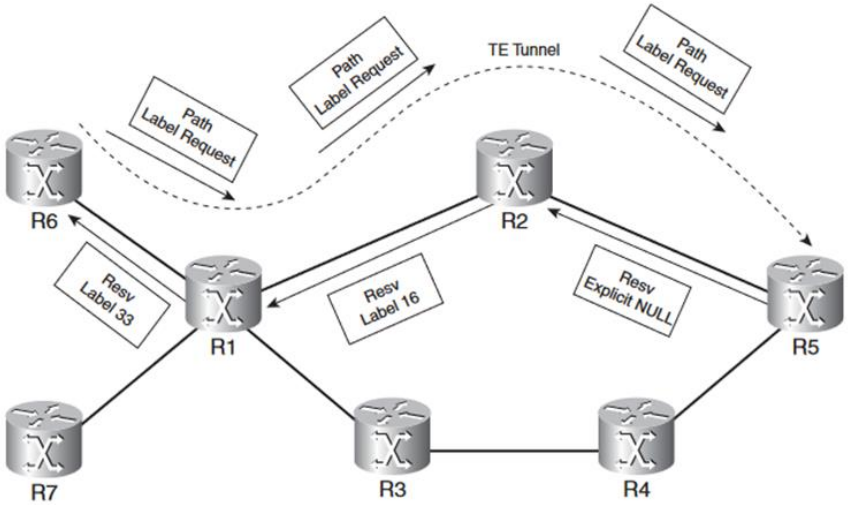
Prin protocolul LDP îi este alocată câte o etichetă fiecărei clase de echivalență, care are ca destinație același ruter de ieșire din domeniul MPLS. Pentru fiecare ruter de ieșire, LDP creează un arbore de LSP-uri de la fiecare ruter de intrare în rețeaua MPLS. Prin metoda ”unsolicited downstream” (un router ce e mai îndepărtat de sursa pachetului) etichetele sunt distribuite către fiecare ruter din rețea, informațiile fiind transmise hop-by-hop, iar fiecare LSR e considerat un ruter de intrare în rețea. Pentru a evita buclele din rețea, LDP utilizează rutele stabilite prin protocoalele de rutare de tip IGP (Internal Gateway Protocol), precum: OSPF, EIGRP, IS-IS. LDP este un protocol folosit doar în rețelele ce nu pot permite aplicarea ingineriei traficului.

1.2.2 Resource Reservation Protocol (RSVP)

Resource Reservation Protocol este un protocol de control al rețelei și a fost definit prima oară în cadrul serviciilor IntServ IP QoS. Acest serviciu prezintă multiple diferențe față de serviciul tradițional "Best-effort", care nu garantează că datele sunt transmise eficient, ci este depus efortul maxim pentru acest lucru. Diferențele sunt reprezentate de IntServ, care asigură izolarea fluxului de date și calitatea serviciului fiecarui flux. Acest nou serviciu are o complexitate ridicată deoarece utilizează RSVP, iar acest serviciu nu este scalabil. [5]

RSVP are abilitatea de a crea un LSP pe o rută care nu este necesar să fie identică cu determinata de protocolul de rutare folosită în rețeaua respectivă, dar și de a rezerva lățimi de bandă de-a lungul acestei căi. De asemenea, se ocupă de distribuția informațiilor legate de etichete într-un mod eficient. Poate utiliza și protocoale de rutare existente în rețea și poate extinde funcțiile unui ruter tradițional ce functionează pe principiul best-effort, astfel încât să suporte funcțiile QoS.

RSVP folosește două tipuri de mesaje: PATH și RESV pentru a semnala o rută. Mesajele de tip PATH sunt trimise de ruterul de intrare în rețea, numit și sender, către ruterul de ieșire, numit și receiver, pentru a identifica clasele de echivilenta care conțin etichetele dorite. Ruterele aflate de-a lungul rețelei MPLS, care primesc acest mesaj se află într-o stare "path". După ce mesajul ajunge la ruterul final din rețea, un mesaj RESV, ce conține o etichetă specifică LSP-ului este trimisă către ruterul de intrare. Fiecare ruter LSR primește mesajul RESV, alocându-i o nouă etichetă și inserând informația în LIB. De asemenea, aceste mesaje sunt folosite pentru a menține un LSP activ. [4]



Figură 1.6 Funcționarea mesajelor PATH și RESV [2]

Alte tipuri de mesaje RSVP sunt:

- RESV Confirmation – confirmarea rezervării transmisă de sender to receiver,

- PATH Error – mesaj transmis upstream pentru a semnala erori în procesul mesajelor PATH,
- RESV Error – mesaj transmis downstream pentru a semnala erori în procesul mesajelor RESV,
- PATH Tear – mesaj transmis downstream pentru a renunța la o cale (path),
- RESV Tear – mesaj transmis upstream pentru a renunța la o "rezervare" (reservation).

1.3 Traffic Engineering (TE)

Conceptul de Traffic Engeineering se referă la controlul traficului, rutele pe care acesta le stabilește, capacitatea link-urilor unei rețele și alegerea priorităților anumitor servicii pentru a nu exista congestie în rețea. O altă funcție pe care o aduce ingineria traficului este distribuirea fluxului de pachete pe multiple link-uri. Unul dintre cei mai importanți factori în controlarea rutei traficului este reprezentat de schimbarea costului pe un anumit link.

Motivația apariției acestei tehnologii este reprezentată de limitările rutării IP tradiționale. Rețelele IP tradiționale dirijează traficul pe cele mai scurte rute fiind limitate din punct de vedere al distribuirii traficului pe multiple link-uri. De asemenea, în aceste rețele, protocoalele de rutare calculează rutele optime pe baza topologiei și a metricii, dar nu iau în considerare lărgimea de bandă disponibilă, iar convergența protocoalelor de rutare este lentă. În rețelele clasice, calitatea serviciilor este slabă, există congestii în rețele (pachete pierdute sau întârziate), utilizarea resurselor este una ineficientă și recuperarea lentă după o deficiență în rețea. [5]

În contextul rețelelor de tip MPLS TE este necesară utilizarea protocolului RSVP, mai exact RSVP-TE, o extensie pentru distribuirea de etichete și ingineria traficului. RSVP-TE a fost introdus pentru a fi utilizat de către ruterele de tip LSR pentru a stabili, menține tunelele LSP și pentru a rezerva resurse din punct de vedere al rețelei pentru acestea. [5]

Funcțiile pe care le poate îndeplini RSVP-TE sunt:

- Distribuire de etichete de tip downstream-on-demand,
- Stabilirea LSP-urile cu sau fără alocare de resurse (lățime de bandă),
- Setarea rutelor LSP explicite,
- Setarea prioritati ale LSP-urilor,
- Găsirea erorilor în tunelele LSP.

O rută stabilită prin intermediul RSVP-TE semnalizează LSP-ul către multiple rute din rețeaua respectivă, iar lărgimea de bandă rezervată acestei rute este scăzută din lărgimea de bandă alocată tuturor rutelor LSP din rețea. În acest caz, este posibil ca restul LSP-urilor să nu aibă destulă lățime de bandă valabilă, acestea fiind dirijate pe alte rute disponibile, ținându-se cont și de prioritatea fiecărei rute.

Există două tipuri de priorități în cazul LSP-urilor: SETUP, în care tunelul LSP este stabilit și HOLD când tunelul a fost stabilit. Prioritățile pot avea valoarea cuprinsă în intervalul 0 și 7, unde prioritatea cea mai mare este 0. Eliminarea unui LSP se poate face prin două moduri: SOFT, unde LSP-ul rămâne activ până când este determinată o altă rută valabilă, iar LSP-ul este șters și HARD, unde LSP-ul este șters direct.

1.4 Avantaje și dezavantaje ale rețelelor de tip IP/MPLS

Rețelele de tip MPLS au adus o multitudine de avantaje, în special pentru service provideri, dar și pentru rețele de tip core (centrale):

- Ruterele de tip LSR sunt mai rapide din punct de vedere al căutării în tabela LIB, decât ruterele clasice, care efectuează operația de look-up în tabela de rutare,
- Tehnologia MPLS este compatibilă atât cu nivelul de legătură de date, cât și cu nivelul de rețea (protocol de nivel 2.5),
- Oferă flexibilitate,
- Creșterea performanțelor prin intermediul ingineriei de trafic (TE),
- Asigură calitatea serviciului (QoS),
- Permite realizarea rețelelor virtuale private (VPN),
- Pot fi utilizate și în rețele optice,
- Arhitectura din punct de vedere al planelor de control și de date este mai clară.

Deși această tehnologie aduce un numar semnificativ de beneficii, are de asemenea și o serie de dezavantaje:

- Căile MPLS trebuie construite în avans,
- Rutarea nu mai este la fel de dinamica ca în cazul rețelelor tradiționale IP, deoarece rețelele de tip MPLS sunt connected-oriented,
- Deficiența unui link poate duce la întreruperea transferului de date. [1]

CAPITOLUL 2. Virtual Private Network

2.1 Virtual Private Network – Concepte de bază

Un Virtual Private Network (VPN) este o rețea privată care utilizează o rețea publică pentru a interconecta unul sau mai multe locuri/site-uri. Serviciul de VPN poate asigura comunicarea la nivelul de legatură de date (nivelul 2 din stiva OSI) sau la nivelul rețea (nivelul 3 din stiva OSI). Acest serviciu este, în general, deținut de o companie care dorește să interconecteze multiple site-uri prin intermediul unui furnizor de servicii (service provider). [2]

Acest serviciu a aparut pentru a reduce costul pe care companiile îl suportau când era necesară interconectarea mai multor locații, erau nevoiți să folosească un WAN (Wide Area Network) privat. Prin implementarea VPN-ului poate fi utilizată o infrastructură WAN comună, dezvoltată de un furnizor de servicii.

Acest serviciu aduce o multitudine de beneficii. În primul rand, din punct de vedere al conectivității si al calității serviciilor. În al doilea rând, există implementări ale VPN-ului pentru a securiza conexiunea. Se garantează confidențialitatea și integritatea datelor, controlul accesului asupra datelor și autenticitatea acestora. [5]

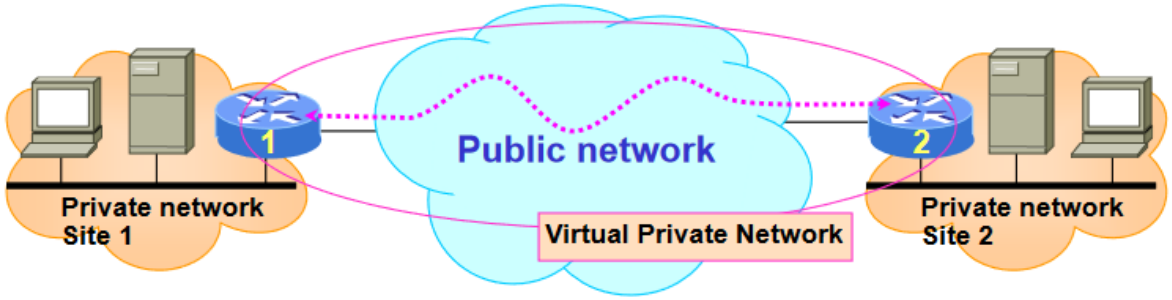


Figura 2.1 Rețea de tip Virtual Private Network [5]

2.2 Modele de rețele VPN

Cele mai des modele de rețele VPN oferite de furnizorii de servicii sunt: Overlay VPN Model și Peer-to-Peer VPN Model.

2.2.1 Overlay VPN Model

Inițial acest model a fost implementat de furnizorii de servicii prin conectivitate fie la nivelul fizic al stivei OSI (Layer 1), fie la nivelul legăturii de date al stivei OSI (Layer 2) sau prin un circuit de transport de Layer 2 între locațiile clienților. În cazul serviciilor la nivelul fizic, service providerul furniza conectivitate exclusiv la layer-ul 1, clientul fiind responsabil de gestionarea celorlalte nivele. În cee ce privește circuitul de transport de nivel 2, furnizorul de

servicii era responsabil pentru transportul cadrelor între locațiile clienților, care era făcut prin intermediul rețelelor de cadru (Frame Relay) sau prin intermediul comutatoarelor ATM. Astfel, service provider-ul nu avea cunoștințe despre protocoalele de rutare pe care clientul le utilizează sau informații despre nivelele superioare. Ultierior, modelele de Overlay VPN au fost implementate peste rețele IP, cu ajutorul unor protocoale de tunelare, precum L2TP (Layer 2 Tunneling Protocol), GRE (General Routing Encapsulation) și IPSec (Internet Protocol Security) pentru a interconecta site-urile clienților, iar protocoalele de rutare erau configurate pe ruterele din rețeaua clienților.

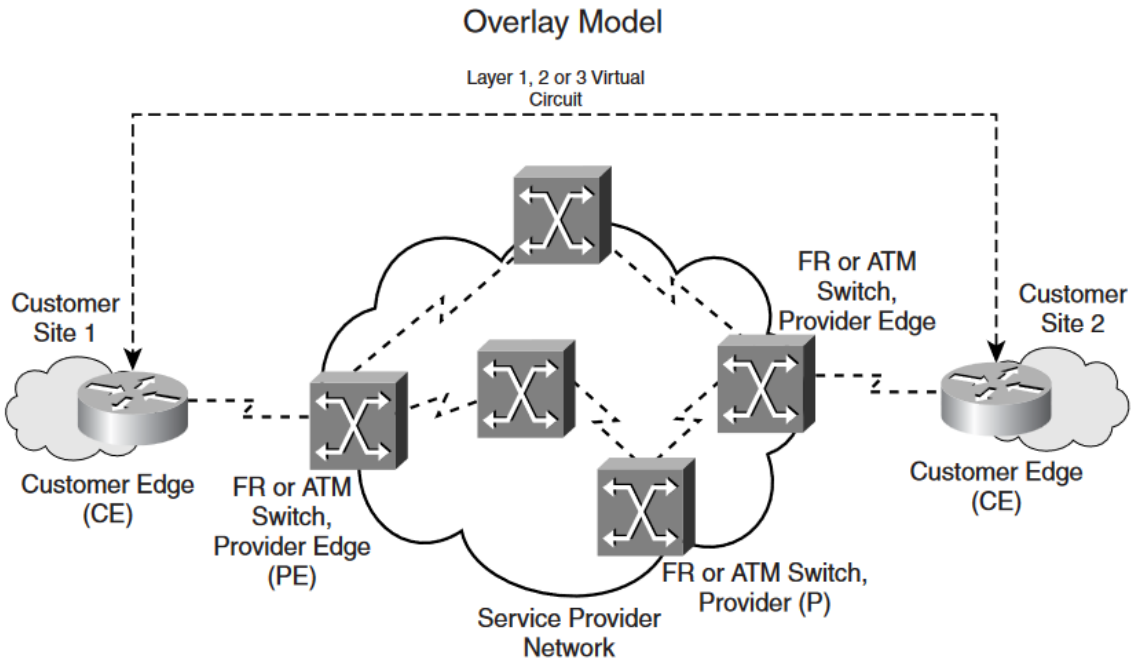


Figura 22 Modelul Overlay VPN [3]

2.2.2 Peer-to-Peer Model

Modelul Peer-to-Peer a fost dezvoltat pentru a reduce dezavantajele modelului Overlay. Acest model oferă clienților un transport optim de date prin intermediul rețelei "schelet" (backbone) al service provider-ului. Diferit față de modelul anterior, în modelul Peer-to-Peer, furnizorul de servicii are cunoștințe despre protocoalele de rutare pe care clienții le utilizează. Informațiile de rutare sunt distribuite între ruterele clienților și ruterele furnizorului de servicii, iar datele clienților sunt transportate prin core-ul rețelei service provider-ului. Ruterele de la marginea rețelei clienților sunt denumite Customer Edge Router (CE), cele de la marginea rețelei service provider-ului sunt numite Provider Edge Router (PE), iar cele din core-ul rețelei Provider Router (P). Acest model nu necesită crearea de circuite virtuale, iar informațiile de rutare primite de către

ruterele PE de la ruterele de tip CE sunt transmise mai departe la ruterele P care găsesc ruta optimă către destinație, în cazul de față un alt site al clientului.

Serviciul VPN trebuie să asigure confidențialitate și izolare între diferiții clienți ce au ca furnizor de servicii aceeași entitate. Acest lucru a fost realizat prin configurarea unor filtre de pachete (access list) pentru a controla traficul de la fiecare ruter al clienților. O altă metodă prin care se poate asigura confidențialitate este prin setarea unor filtre ce anunță rutele sau opresc anunțarea rutelor către ruterele clienților. Aceste două metode pot fi configurate și simultan. [3]

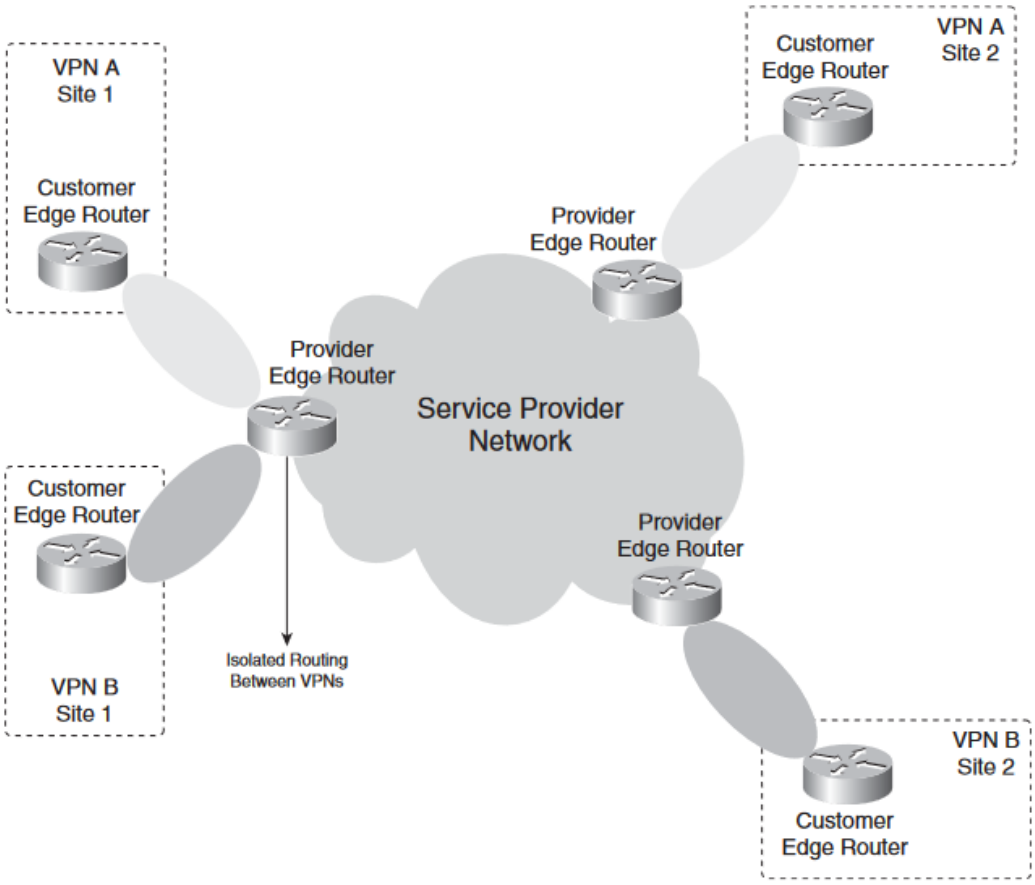


Figura 2.3 Modelul Peer-to-Peer VPN [2]

Înainte de apariția tehnologiei MPLS, modelul Overlay era mai des utilizat decât modelul Peer-to-Peer deoarece modelul din urmă necesită multiple schimbări de configurare la adăugarea unei noi locații. MPLS VPN este o aplicație MPLS ce a făcut ca modelul Peer-to-Peer să fie mult mai ușor de integrat și configurat.

2.3 Protocoale de tunelare utilizate în modelele VPN

Termenul de tunelare se referă la încapsularea pachetelor de date dintr-un protocol într-un alt protocol și la transportul datelor neafectate printr-o rețea străină. Spre deosebire de încapsulare, concept ce se referă la adăugarea unor headere pachetelor specifice fiecarui nivel din stiva OSI, prin tunelare pot fi transportate protocoale indiferent de nivel sau specific. [8]

În modelul VPN Overlay pot fi folosite următoarele protocoale de tunelare: IPSec, GRE sau L2TP.

2.3.1 Protocolul GRE (General Routing Encapsulation)

Un tunel GRE oferă conectivitate pentru o mare varietate de protocoale de nivel rețea prin încapsularea și expedierea pachetelor printr-o rețea IP, creându-se un link virtual între ruterele de la capetele tunelului. Inițial, tunelele GRE au fost utilizate pentru transportul protocoalelor ce nu pot fi rutate (DECnet, SNA, IPX).

Tunelurile GRE sunt clasificate ca fiind rețele suprapuse deoarece acest tip de tunel este stabilit peste o rețea de transport existentă numită și rețea underlay. Un header ce conține informații despre adresa IP a destinației este adăugat pachetului când ruterul încapsulează datele pentru tunelul GRE. Acest antet permite rutarea pachetului între cele două puncte terminale ale tunelului fără a inspecta datele efective ale pachetului. La finalul tunelului GRE, antetul este eliminat, iar pachetul este transmis la destinație. [7]

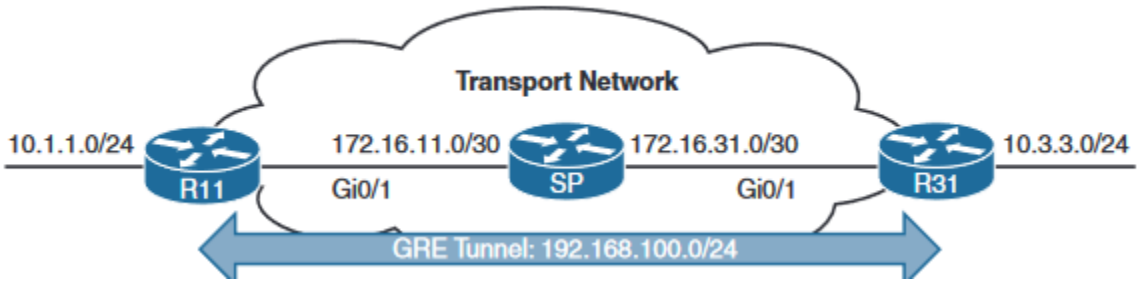


Figura 2.4 Tunel GRE [7]

2.3.2 Protocolul L2TP (Layer 2 Transport Protocol)

Protocol L2TP oferă o soluție scalabilă pentru implementarea VPN-urilor de layer 2 peste o rețea IP. Cadrele de layer 2 sunt încapsulate cu un header L2TP și sunt transportate de-a lungul rețelei IP sau o rețea de tip MPLS. Acest protocol suportă cadre ATM, Frame Relay, HDLC (High-level Data Link Control) și Ethernet.

Arhitectura folosită de protocolul L2TP se bazează pe conceptul de pseudowires (pseudofire). Pseudowire-le transportă traficul de layer 2 al clienților, de la un capăt la celălalt, prin rețeaua backbone care poate fi de tip IP sau MPLS, în acest context numindu-se PSN (Packet

Switched Network) care poate avea un pseudowire sau mai multe. Conexiunea de tip pseudowire este realizată între rutarele de tip PE ale unei rețele service provider și prin intermediul acestor pseudofire se pot conecta la ruterele de tip PE, cirucite atasate (Attachement Circuits). Aceste circuite atașate pot fi formate din ATM-uri, rețele cadru, iar cadrele care ajung la ruterul PE de intrare sunt încapsulate și trimise către ruterul PE de ieșire, unde vor fi decapsulate și trimise mai departe către destinație. Pentru ca acest proces să fie posibil, ruterele de tip PE trebuie să știe metoda încapsulării în contextul unei rețele ce nu este de tip MPLS, poate fi încapsularea 802.1q.

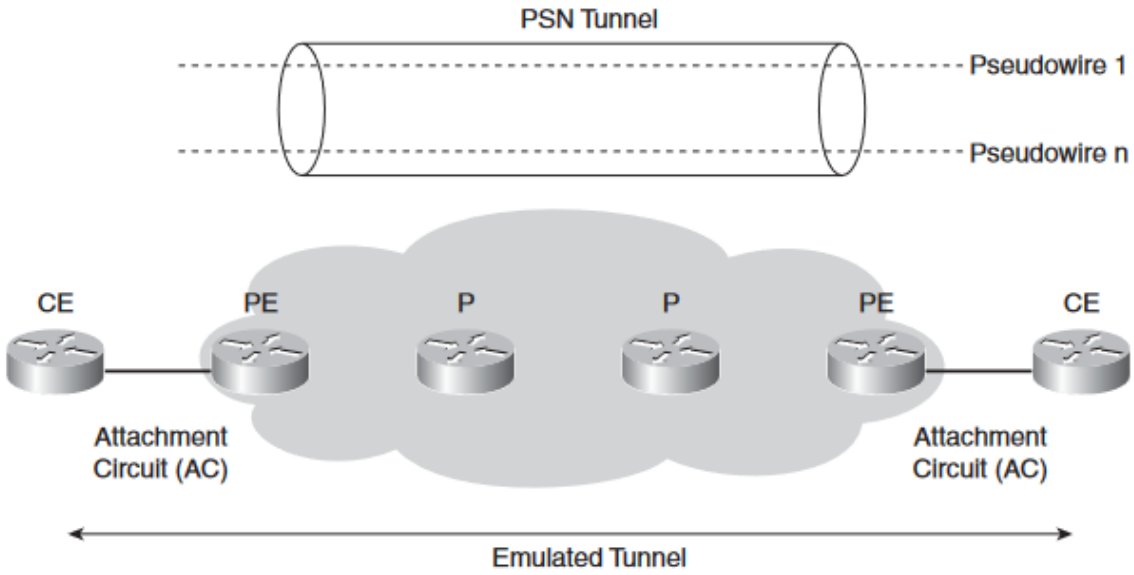


Figura 2.5 Tunelul L2TP si PSN-ul format din pseudowire-re [2]

Capitolul 3 – MPLS Layer 3 VPN

3.1 MPLS Layer 3 VPN – Concepte de bază

Modelul MPLS Layer 3 VPN este cea mai cunoscută și răspândită implementare ale tehnologiei MPLS. Acest model de VPN oferă scalabilitate și furnizorii de servicii ce folosesc această tehnologie trebuie să asigure izolarea între clienți. Acest lucru poate fi realizat cu ajutorul funcției VRF, prin care se pot crea multiple tabele de rutare pe un singur ruter.

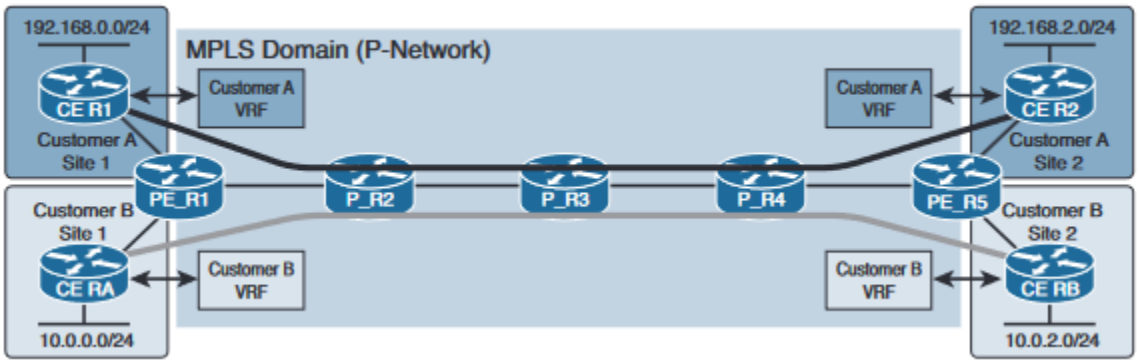


Figura 3.1 Rețea de tip MPLS VPN [7]

Această tehnologie folosește, în rețeaua core, tehnologia MPLS utilizând protocolul LDP sau RSVP pentru stabilirea unui LSP între ruterele marginale din rețea. Ruterele CE nu cunosc nicio informație despre ruterele de tip P, care sunt responsabile de comutarea etichetelor. Ruterele clienților necesită doar un protocol de rutare pentru a asigura interschimbarea de informații cu ruterele marginale ale rețelei MPLS. Rutarele de tip PE îndeplinesc multiple funcții precum izolarea traficului între clienți și stabilirea legăturii de tip VPN. Ruterele P nu au informații despre stabilirea VPN-ului în rețea. [3]

3.1.1 Virtual Routing Forwarding

Prin utilizarea conceptului de VRF (Virtual Routing Forwarding) pe rutarele de tip PE din rețeaua MPLS, traficul fiecărui client este izolat de restul, aspect foarte important din punct de vedere al securității informațiilor clienților. Acest concept aduce beneficii și furnizorilor de servicii deoarece este similar cu configurarea unui ruter fizic fiecărei locații ce se conectează la rețeaua de tip MPLS VPN. VRF permite existența simultană a mai multor tabele de rutare și forwarding (transmitere) pe un singur ruter.

Aceste tabele de rutare sunt similare cu tabela de rutare globală de pe un rutar obișnuit, dar conține informații despre rutele ce aparțin unui VPN. Funcția VRF suportă majoritatea protocoalelor de rutare: OSPF, BGP, EIGRP, RIP, IS-IS, dar și rutarea statică. [3]

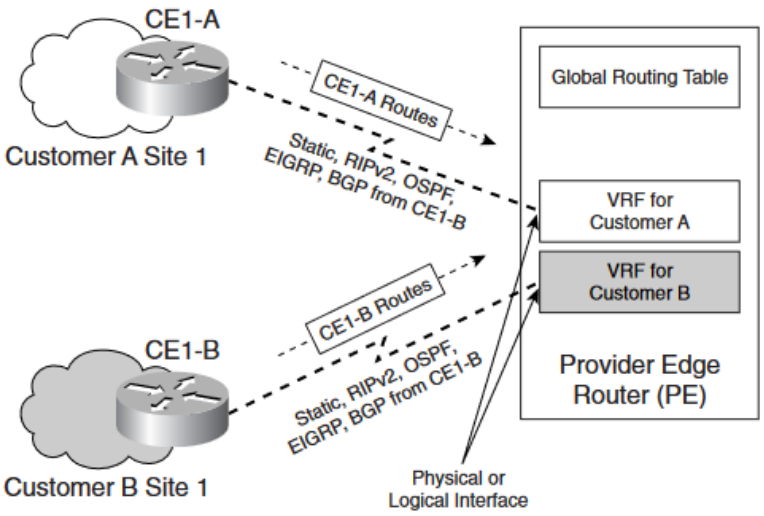


Figura 3.2 Conceptul de VRF [3]

3.1.2 Mutliprotocol iBGP

În modelul MPLS VPN, ruterele PE asigură izolarea informațiilor între fiecare client folosind conceptul de VRF, dar aceste informații trebuie transportate între ruterele marginale pentru a fi funcționale din punct de vedere al comunicației între locațiile clienților. Ruterele marginale trebuie să cunoască rutele primite de la ruterele clienților și să trimită aceste informații prin rețeaua de tip MPLS. Acest lucru este posibil folosind conceptul de route distinguisher (RD). [3]

RD este definit ca un identificator, ce are lungimea de 64 de biți, atribuit fiecărei rute dintr-un VRF, astfel încat ruterele de tip PE pot identifica VPN-ul aferent fiecărei rute. Acest identificator este concatenat cu lungimea unei adresei IP ce reprezintă o rută învățată de la ruterele CE, rezultând o adresă de tip VPN de 96 de biți. Identificatorul RD este alcătuit din două câmpuri: AS (Autonomous System) Number/IP Address și VPN Identifier.

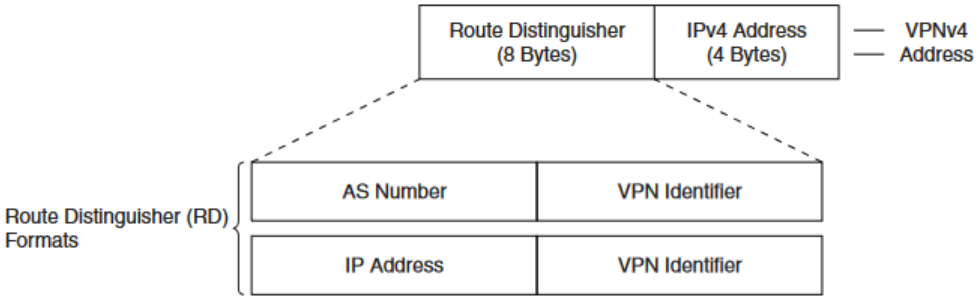


Figura 3.3 Adresa VPNv4 [3]

Route target-ul este un identificator ce este adăugat rutelor VPN pentru a specifica politicile de control, astfel încat rutele VPN să fie importate sau exportate în legătură cu VRF-ul respectiv. La exportul route target-ului, valoarea sa este adaugată ca o comunitate extinsă BGP-ului, atunci când ruta VPN este redistribuită de la VRF la BGP, iar la importul route target-ului, o rută VPN primită prin BGP este analizată, iar dacă valoarea atributului RT se potrivește, ruta va fi adaugată. În caz contrar, ruta nu va fi adaugată. [5]

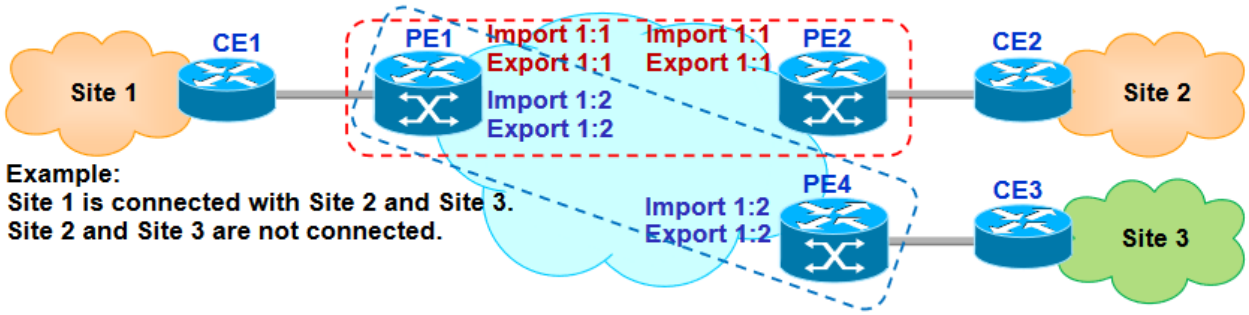


Figura 3.4 Conceptul de route target [5]

Protocolul care realizează interschimbarea acestor rute VPN între ruterele marginale ale rețelei MPLS, este numit MP-BGP (Multiprotocol Border Gateway Protocol). Legătura creată prin intermediul acestui protocol, între rutarele PE ce aparțin aceluiași AS, este numită o sesiune MP-iBGP (Multiprotocol internal Border Gateway Protocol). AS reprezintă un grup de rutere ce sunt gestionate de aceeași organizație.

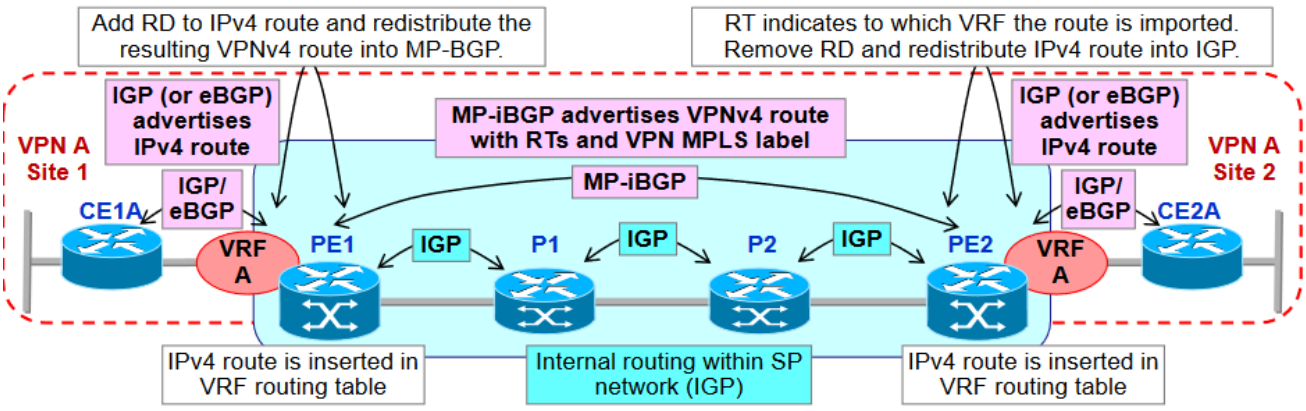


Figura 3.5 Propagarea rutei [5]

Etapele propagării unei rute sunt:

1. Ruterul PE primește rute de la CE prin intermediul unui protocol de rutare, fie el de tip intern sau extern, care vor fi introduse în tabela de rutare virtuală specifică. După ce le-au fost adăugate un RD, vor fi distribuite prin protocolul MP-iBGP,
2. Toate ruterele PE primesc rutele VPNv4 prin intermediul protocolului MP-BGP, împreuna cu RT-urile aferente,
3. Dupa ce RT-urile sunt verificate, ruterele marginale pentru care RT-urile se potrivesc, vor introduce în tabela de rutare virtuală aferentă rută IPv4. Pachetele vor fi apoi transmise la client printr-un protocol de rutare intern sau extern.

3.2 Moduri de operare

3.1.2 Planul de control (Control Plane)

În planul de control din modelul MPLS VPN, sunt regăsite informații despre protocoalele de rutare și procese de interschimbare a informațiilor specifice prefixelor IP, dar și de atribuire și distribuire ale etichetelor prin intermediul protocolului LDP sau RSVP. Operațiile regăsite în acest plan sunt următoarele:

- Un LSP este stabilit între ruterele marginale ale rețelei MPLS, prin utilizarea protocolului de distribuire de etichete LDP. Etichetele sunt distribuite pe rutele determinate de protocolul de rutare intern (IGP) în rețeaua furnizorului de servicii,
- Ruterele de tip PE atribuie VPN-urilor RD-uri și o etichetă specifică VPN,
- Ruterele de tip PE introduc în tabela de rutare, rutele primite de la CE,
- Prin intermediul protocolului MP-iBGP rutele de tip VPNv4 sunt anunțate către ruterele marginale. [5]

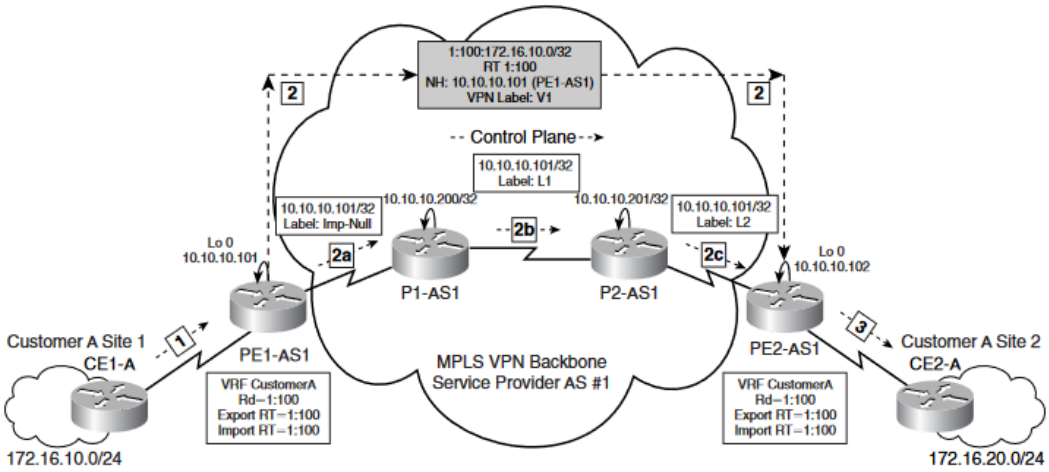


Figura 3.6 Operațiile din Control Plane [3]

3.2.2 Planul de date (Data Plane)

Planul de date realizează funcții referitoare la transmiterea (forwarding) pachetelor de tip MPLS ce au atribuite o etichetă, cât și la pachetele de tip IP către next-hop-ul din rețea. Operațiile ce au loc în planul de date sunt:

- Ruterul CE2 trimite pachete către rutarul PE2, având informații despre destinație,
- Ruterul PE2 analizează pachetele primite pe interfața și identifică VRF-ul asociat acesteia, Ruterul PE2 va adauga pachetelor atât eticheta de VPN, cât și eticheta MPLS și transmite pachetul către rutarul P2,
- Ruterul P2 va comuta etichetele pentru a trimite pachetul către rutarul P1,

- Ruterul P1 va elimina eticheta MPLS prin procedeul POP, deoarece respectă principiul Penultimate Hop-Popping,
- Ruterul PE1 elimină eticheta VPN și va transmite informația către ruterul CE1. [3]

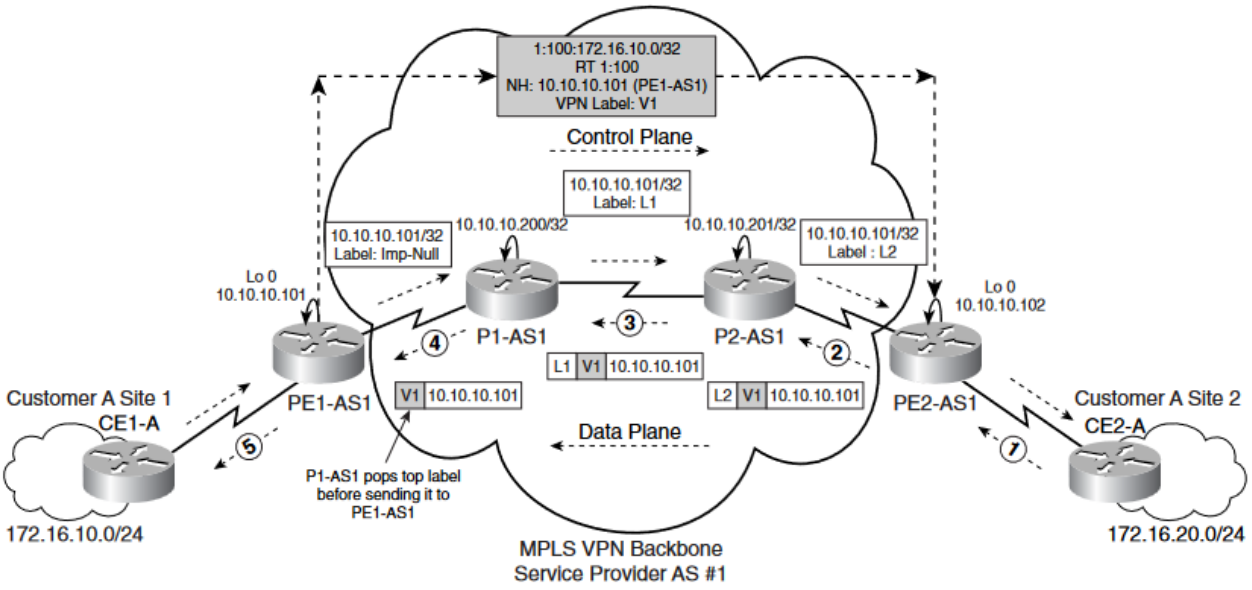


Figura 3.7 Operatiile din Data Plane [3]

Capitolul 4 – Any Transport over MPLS

4.1 AToM – Concepte de bază

Tehnologia Any Transport over MPLS (AToM) a fost dezvoltată după apariția modelului MPLS VPN, model ce reprezintă o soluție de rețea privată virtuală ce permite transportul traficului peste o rețea MPLS. Totuși, legăturile de tip ATM sau Frame Relay sunt încă utilizate pentru transmiterea informațiilor între locațiile clienților, obligându-i pe furnziorii de servicii să implementeze tipuri de rețele specifice pentru acest lucru. Prin intermediul tehnologiei AToM, furnizorii de servicii pot transmite informații specifice acestor legături ATM sau Frame Relay, dacă rețeaua lor de bază (backbone) este de tip MPLS, fară a mai implementa o rețea separată.

Any Transport over MPLS este denumirea dată de Cisco pentru serviciul de transport al nivelului de legătură de date peste o rețea de tip MPLS, denumit și Layer 2 VPN (L2VPN). Ruterele clienților se conectează cu cele ale furnizorului de servicii, conexiunea fiind una de layer 2 (Ehternet, HDLC, ATM, Frame Relay), fapt ce elimină necesitatea utilizării funcțiilor de layer 3 pentru transmiterea informațiilor. AToM este o tehnlogie specifică ruterelor marginale, ruterele din interiorul rețelei MPLS sunt de tip LSR și se ocupă doar de comutarea etichetelor. Tehnlogia AToM poate crea doar o conexiune de tip point-to-point, serviciu numit Virtual Private Wire Service (VPWS). Există un serviciu, numit Virtual Private LAN Service (VPLS), ce poate crea legături point-to-multipoint. [2]

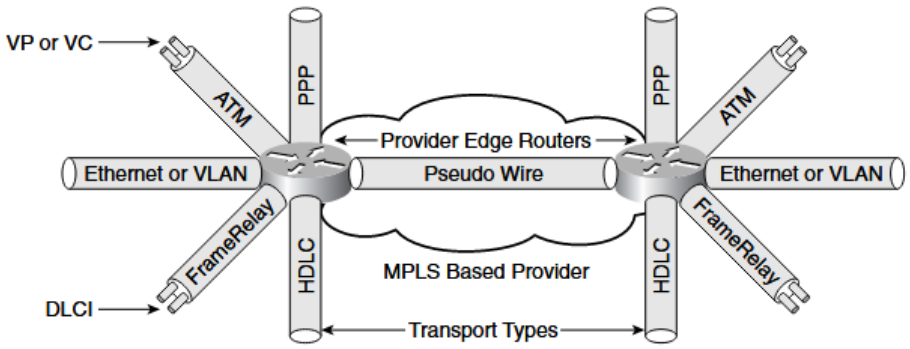


Figura 4.1 Exemplu rețea ce folosește tehnologia AToM [3]

4.2 Arhitectura modelului AToM

În rețele ce folosesc AToM, toate ruterele din rețeaua furnizorilor de servicii trebuie să fie configurate conform unei rețele de tip MPLS. Între ruterele PE și CE se formează un attachment circuit (AC), ruterul PE preluând cadrele de layer 2 pe acest circuit și le atașează o etichetă. Un attachment circuit reprezintă un circuit fizic sau unul virtual (VC) pentru ATM sau Frame Relay, dar poate fi reprezentat și de o interfață a unui port ethernet, un vlan sau un link HDLC. După ce ruterul PE adaugă eticheta la cadrul de layer 2 primit de la CE, acesta îl transmite mai departe către ruterul PE remote prin intermediul tunelului Packet Switched Network (PSN). O rețea cu comutare de pachete (PSN) ce folosește mecanismul IP sau MPLS pentru transmiterea (forwarding) pachetelor. Capetele acestui tunel PSN sunt rutere PE ce sunt conectate la circuite atașate. În cazul tehnologiei AToM, tunelul PSN este reprezentat de LSP-ul stabilit între cele două rutere marginale, eticheta asociată acestui tunel este denumită eticheta tunel (tunnel label). [3]

Ruterele LSR pot determina LSP-ul prin diferite metode: fie prin utilizarea protocolului LDP ce semnalează LSP hop-by-hop între ruterele PE sau dacă este utilizată tehnologia MPLS TE, tunelul poate fi stabilit prin intermediul protocolului RSVP-TE. Cu ajutorul etichetei tunelului, poate fi identificat cărui client îi aparțin respectivele cadre. Tunelul PSN poate fi multiplexat, pentru a permite utilizarea mai multor pseudofire (pseudowires), astfel un singur PSN ar putea fi folosit de mai mulți clienți. Pentru multiplexarea acestui tunel, ruterul PE folosește un alt tip de etichetă denumită VC sau PW pentru a identifica circuitul virtual sau pseudofirul pe care cadrul a fost multiplexat. Un LSP este unidirecțional, deci pentru crearea unui pseudofir sunt necesare două LSP-uri. [2]

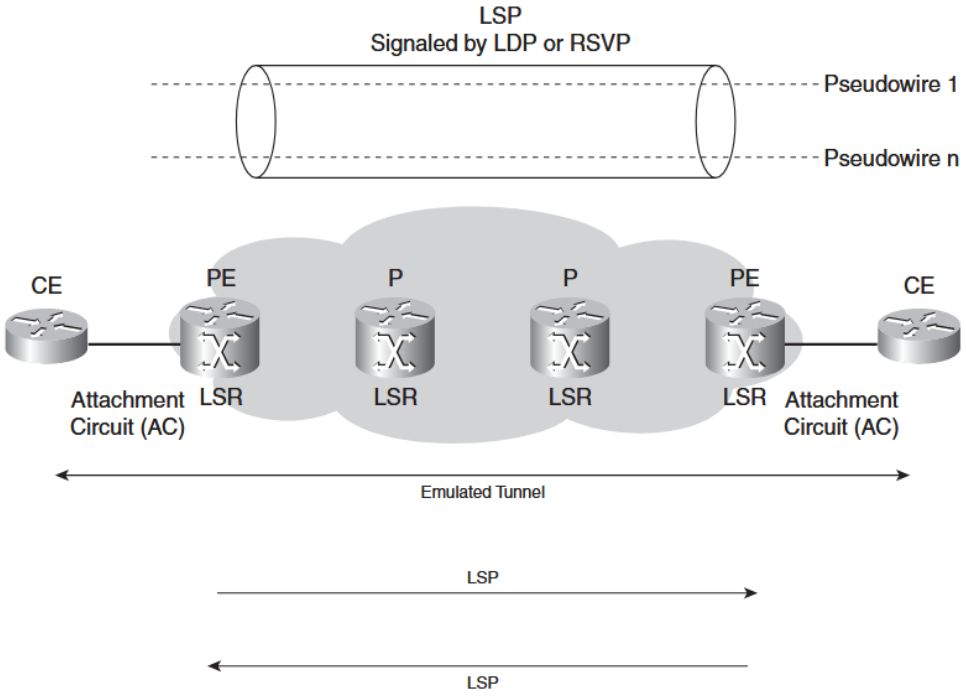


Figura 4.2 Creearea unui pseudowire [2]

În cazul AToM, schimbul de etichete VC este realizat prin stabilirea unei sesiuni LDP multihop direcționate între ruterele PE ale rețelei MPLS, iar ruterul de ieșire PE trimite un mesaj de tip LDP Label Mapping ce indică valoarea pentru clasa de echivalență a etichetei VC, denumită și VC-FEC. Schimbul de informații despre etichetele VC este distribuit prin modul downstream unsolicited label distribution, iar aceste valori sunt utilizate de ruterul PE de intrare pentru a atribui etichetele VC cadrelor primite de la ruterele CE. [3]

4.2.1 Semnalizarea pseudowire

Sesiunea LDP între ruterele marginale ale rețelei MPLS semnalizează pseudofirele, dar are și roulul de a menține aceste pseudofire. În cazul tehnologiei AToM, protocolul LDP a fost extins cu codări de tip Type Length Value, prescurtate TLV pentru a fi posibile aceste procedee, denumite VC/PW ID FEC TLV și VC/PW Label TLV. Scopul principal al acestei sesiuni de tip LDP este să anunțe eticheta VC asociată pseudofirului. VC ID FEC TLV identifică cărui pseudofir îi este atribuită eticheta, iar VC Label TLV este codarea de tip TLV folosită de LDP pentru a anunța eticheta MPLS.

Codarea VC ID FEC TLV conține următoarele elemente:

- C-bit – are lungimea de 1 bit și dacă are valoarea 1, indică prezența unui cuvânt de control,
- PW Type – are lungimea de 15 biți și indică tipul de pseudofir. Tipurile de pseudofir pot fi: Frame Relay, ATM, Ethernet, HDLC și fiecare fiind reprezentată în acest câmp printr-o valoare unică,
- Group ID – identifică un grup de pseudofire. Echipamentele Cisco atribuie același Group ID fiecărui pseudofir dacă acestea sunt conectate pe aceeași interfață,
- PW ID – reprezintă un identificator de 32 de biți, acesta împreuna cu PW Type identifică complet pseudofirul.
- Interface parameters – acesta descrie parametrii interfeței (MTU – Maximum Transmission Unit) [2]

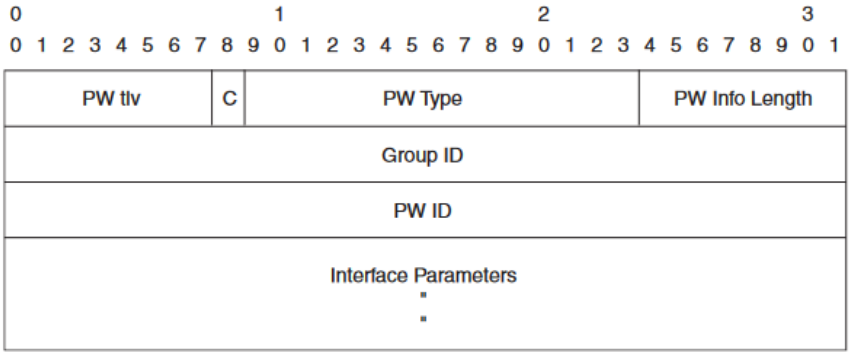


Figura 4.3 Formatul VC/PW ID FEC TLV [2]

Cuvântul de control reprezintă un câmp de 32 de biți inserat între eticheta VC și cadrele de layer 2 transportate în tehnologia AToM. Unele protocoale de nivel de legătură de date necesită un astfel de câmp. Cuvântul de control conține informații suplimentare precum informații despre controlul protocoalelor și un număr de secvențe într-un format compresat. Aceste informații sunt necesare pentru ca transportul informațiilor să fie realizat corect în cadrul rețelelor de tip MPLS. Funcțiile cuvântului de control sunt: completarea pachetelor mici din punct de vedere al dimensiunii, purtarea informațiilor despre biți de control al anetetelor de layer 2, păstrează secvența cadrelor transmise și facilitează un load balancing optim pachetelor transmise prin rețeaua MPLS. [2]

4.2.2 Procedura de LDP Label Mapping

Această procedură este independentă de transportul de informații de layer 2 și este descrisă de următorii pași:

1. Ruterul PE1 primește informații de tip layer 2 de la ruterul CE1,
2. PE1 stabilește o sesiune de tip LDP cu PE2,
3. PE1 recunoaște un VC configurat pe interfața pe care a primit cadrele de la CE1, le alocă o etichetă VC și le atribuie ID-ului VC respectiv interfeței de intrare,
4. PE1 codifică această legătură dintre eticheta VC și ID-ul VC ale interfeței cu VC-label TLV și VC FEC TLV și le trimite către PE2 într-un mesaj de mapare a etichetelor,
5. PE1 primește un mesaj de mapare a etichetelor de la PE2, iar în VC FEC TLV primit de la PE2, ID-ul VC se potrivește cu ID-ul VC configurat local pe PE1. Eticheta VC codificată cu VC-label TLV este eticheta atribuită de PE1 cadrelor primite de la CE1 în transmiterea lor către PE2.

PE2 trebuie să urmeze aceeași pași pentru a realiza o legătură bidirecțională, iar după ce ambele rutere marginale au realizat schimbul de informații despre etichetele VC pentru un ID particular, ID-ul VC este considerat stabilit. În cazul în care un circuit virtual este avariat sau este eliminat din rețea, ruterul PE trebuie să anunțe acest eveniment, trimițând o etichetă de tip retragere (withdraw) prin care anunță ruterul PE remote.

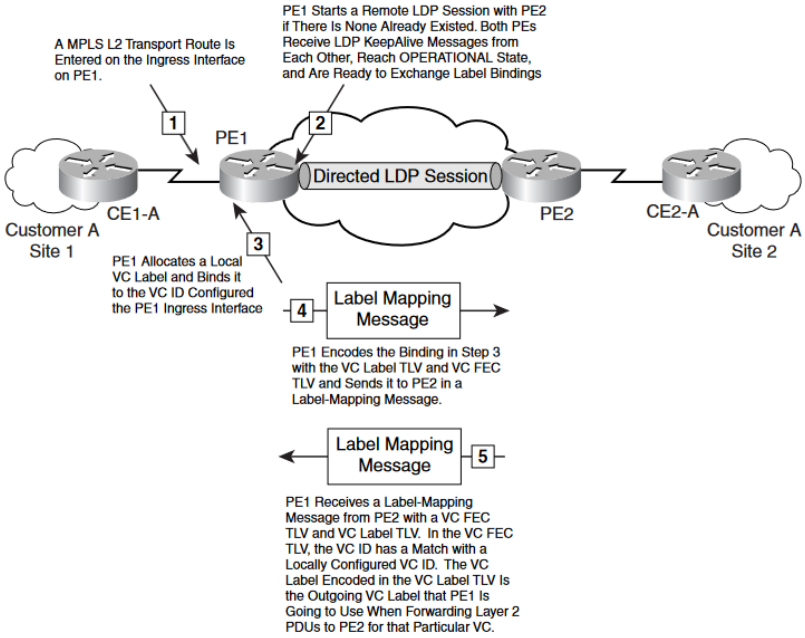


Figura 4.4 Procedeul de LDP Label Mapping [2]

4.3 Modurile de operare AToM

4.3.1 Planul de control (Control Plane)

În arhitectura AToM planul de control este reprezentat de protocoalele de rutare aflate în interiorul rețelei MPLS și protocolul LDP. Procesul începe cu ruterul PE1 ce anunță o etichetă implicit-null propria sa adresă de loopback, iar ruterul P anunță o etichetă cu o valoare L1 către

PE2, astfel creându-se un LSP între PE1 și PE2. O sesiune directă de tip LDP între PE1 și PE2 pentru a interschimba informații legate de etichetă VC. [3]

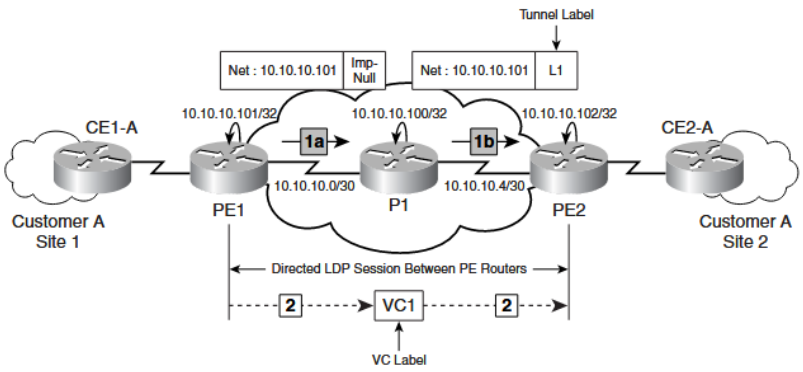


Figura 4.5 Planul de control în tehnologia AToM [3]

4.3.2 Planul de date (Data Plane)

În planul de date regăsim următoarele operații:

- CE2 trimite date la nivelul legăturii de date către PE2,
- PE2 atribuie o etichetă tunel și una specifică circuitului virtual și le trimite către PE2,
- P1 elimină eticheta tunel și trimite mai departe datele,
- PE1 verifică informațiile conținute în eticheta VC pentru a alege corect interfața către CE1 [3].

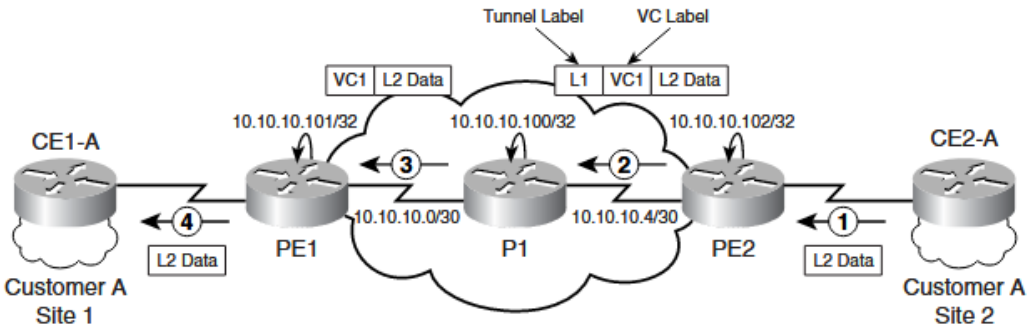


Figura 4.6 Planul de date în tehnologia AToM [3]

4.4 Ethernet over MPLS

Transportul cadrelor de tip Ethernet peste MPLS în cadrul tehnologiei AToM este strict punct-la-punct. Toate cadrele Ethernet sunt transportate între ruterele marginale ale rețelei MPLS, asemănător unei punți LAN-to-LAN (bridge) peste o rețea de tip WAN.

Circuitul atașat poate fi un port Ethernet sau un VLAN. Pentru fiecare tip de AC, protocolul LDP semnalează un VC/PW Type diferit prin sesiunea dintre ruterele marginale, deoarece formatele celor două cadre sunt diferite. Pentru porturile Ethernet este folosit VC/PW Type 5, iar pentru VLAN este folosit VC/PW Type 4. Formatul cadrului VLAN este denumit Ethernet II With 802.1Q și conține 4 octeți suplimentari față de formatul cadrului Ethernet II. Acești 4 octeți sunt împărțiți în două câmpuri:

- TPID – are lungimea de 16 biți și are valoarea 0x8100 pentru a identifica protocolul etichetat ca fiind de tip 802.1Q,
- TCI – are lungimea de 16 biți și este format din 3 câmpuri: Priority ce are lungimea de 3 biți și este folosit pentru QoS cu scopul de a prioritiza cadrele Ethernet, CFI de lungimea 1 bit și indică dacă adresa MAC e de formă canonică și VID cu lungimea de 12 biți pentru a identifica ID-ul VLAN-ului.

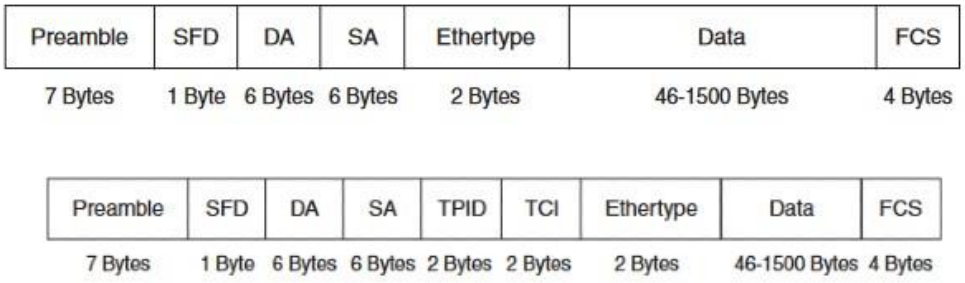


Figura 4.7 Formatele cadrelor de tip Ethernet II și Ethernet II With 802.1Q [2]

4.4.1 Transmiterea EoMPLS

Ruterul de intrare PE primește cadrele Ethernet, elimină preambulul și câmpurile SFD și FCS, adaugă un cuvânt de control și atribuie o etichetă VC și îl transmite mai departe în rețeaua MPLS. Dacă acest cadru are și un identificator 802.1Q, acest identificator va fi păstrat. La ruterul de ieșire PE, eticheta VC va fi eliminată, precum și cuvântul de control, iar campul FCS este adăugat și cadrul este transmis mai departe către ruterul CE.

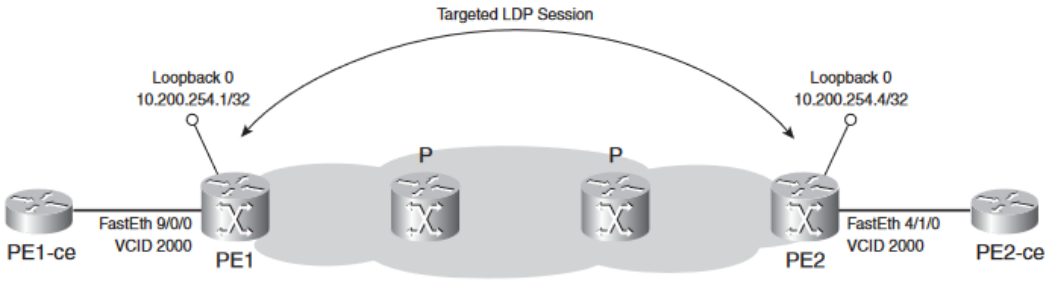


Figura 4.8 Transmiterea cadrelor Ethernet II [2]

Capitolul 5 – Implementarea tehnologiilor de tip VPN

Emulatorul GNS3 (Graphical Network Simulator 3) reprezintă un program software ce permite simularea rețelelor, putând fi conectate atât sisteme reale, cât și sisteme virtuale.

Pentru implementarea tehnologiilor MPLS și AToM, au fost utilizate imagini Cisco IOSv 15.6. Imaginea sistemului de operare IOSv (Internetwork Operating System virtual) reprezintă versiunea virtuală a Cisco IOS 15.6, având aceleași funcții de gestionare și transmitere a traficului.

Sistemul de operare Cisco IOS este utilizat pentru multiple functionalități cum ar fi: rutare, fie ea statică sau dinamică, comutare, securitate, QoS, gestionare și monitorizare și virtualizare. Pentru implementarea tehnologiilor prezentate anterior, cele mai importante funcții pe care le deține acest sistem de operare sunt cele de rutare dinamică, suportarea rețelelor de tip VPN, permiterea creării VRF-urilor și configurarea de tip MPLS a ruterelor.

5.1 Topologie

Pentru implementarea noțiunilor teoretice prezentate anterior, am realizat următoarea topolgie de rețea:

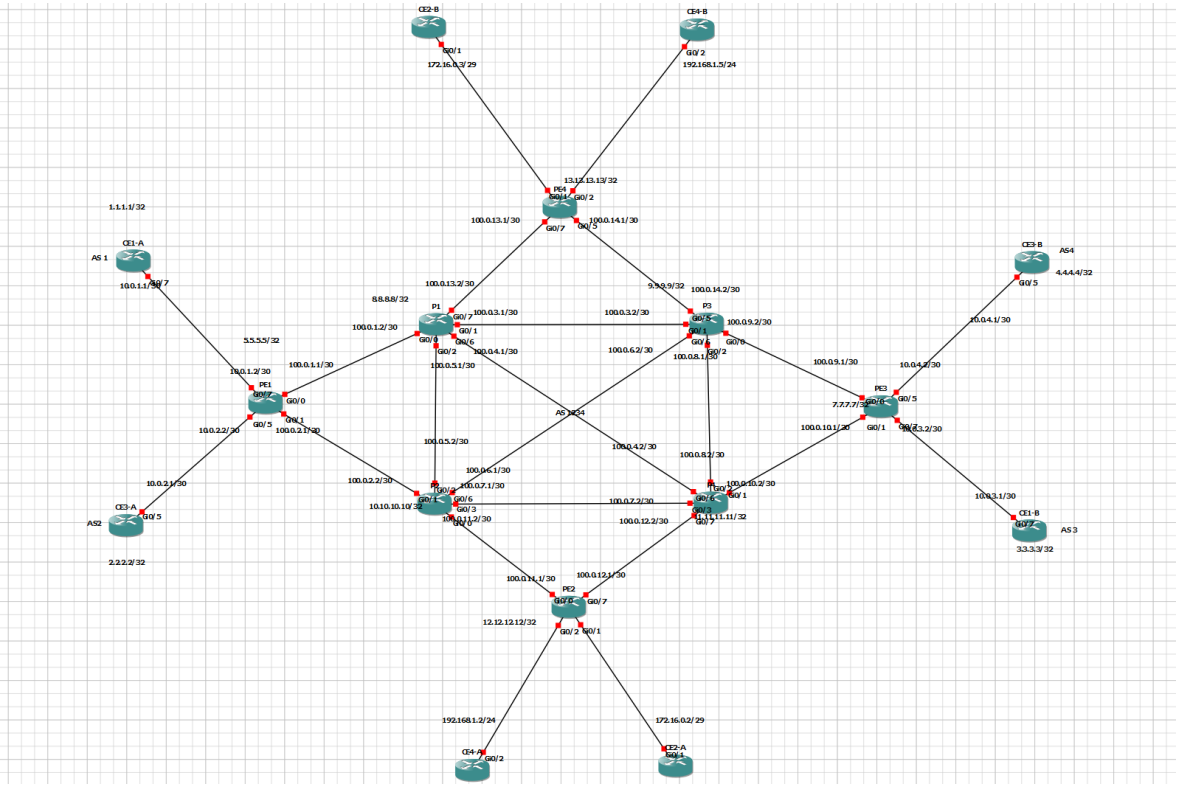


Figura 5.1 Topolgia rețelei MPLS VPN și AToM

În cadrul acestei rețelei am utilizat 16 rutere Cisco IOSv, 8 dintre ele pentru formarea rețelei de tip MPLS, restul fiind destinate clienților. Au fost considerați 4 clienți, fiecare având două locații diferite: Customer 1 cu site-urile A și B, Customer 2 cu site-urile A și B, Customer 3 cu site-urile A și B și Customer 4 cu site-urile A și B. În acest caz, furnizorul de servicii oferă servicii de VPN celor 4 clienți prin interconectarea locațiilor prin intermediul rețelei de bază MPLS, astfel Customer 1 Site A și Customer 1 Site B, cât și Customer 3 Site A și Customer 3 Site B vor beneficia de serviciul MPLS Layer 3 VPN, iar Customer 2 Site A și Customer 2 Site B și Customer 4 Site A și Customer 4 Site B sunt interconectați prin MPLS Layer 2 VPN, cunoscut și sub numele de AToM. Deoarece în cazul de față ambele tipuri de rețele VPN sunt realizate prin intermediul aceluiași service provider, putem realiza o comparație între aceste tehnologii.

Ruterele PE1 și PE3 sunt ruterele marginale ale rețelei MPLS ce permit utilizarea VPN-ului de layer 3 de către ruterele CE1-A, CE1-B, CE3-A și CE3-B. Pe de altă parte, ruterele PE2 și PE4 reprezintă ruterele marginale permit utilizarea VPN-ului de layer 2 între site-urile Customer 2 site A și site B și Customer 4 site A și site B. Ruterele de tip P (P1, P2, P3, P4) sunt conectate full-mesh, fapt ce aduce multiple beneficii din punct de vedere al redundanței și fiabilității și de asemenea în cazul în care unul din link-urile ce leagă cele 4 rutere, este defect sau avariat, traficul poate fi transmis în continuare prin intermediul acestor rutere. Ruterele marginale sunt legate de câte 2 rutere de tip P, fapt ce duce la minimizarea redundanței. Ruterele ce fac parte din rețeaua MPLS fac parte din sistemul autonom 1234, iar ruterele clienților fac parte din sisteme autonome diferite. Un sistem autonom reprezintă un grup de rețele ce țin de o singură administrație tehnică.

5.2 Protocoale de rutare utilizate

5.2.1 OSPF (Open Shortest Path Fast)

Protocolul OSPF reprezintă un protocol de rutare de tip IGP (interior gateway protocol) utilizat des în rețelele de mărimi ridicate. Acest protocol utilizează un algoritm de rutare a stării de legătură (Link State Routing) și funcționează într-un singur sistem autonom.

Fiecare ruter ce funcționează pe baza protocolului OSPF, distribuie starea link-urilor proprii către toate ruterele din domeniu, prin hop-by-hop flooding. Mesajul prin care sunt distribuite stările legăturilor este denumit Link State Advertisement (LSA). Toate ruterele colectează starea link-urilor anunțate și realizează o bază de date identică, conținând informații despre topologia domeniului. Prin intermediul acestei baze de date, fiecare ruter își construiește propriul său tabel de rutare utilizând un algoritm Shortest Path First sau Dijkstra. Tabelul de rutare conține informații despre toate destinațiile pe care ruterul le cunoaște prin intermediul protocolului de rutare asociate cu adresa IP next hop și interfața de ieșire.

Protocolul OSPF recalculează rutele atunci când topologia este modificată și minimizează traficul de protocol de rutare pe care îl generează. De asemenea, acest protocol oferă suport pentru căi cu costuri egale.

Fiecare ruter din rețeaua configurată cu protocolul OSPF, comunică cu alte rutere vecine pe fiecare interfață pentru a stabili stările tuturor adiacentelor. Stările prin care un ruter poate trece sunt: down, attempt, init, two-way, exstart, exchange, loading și full. Starea down reprezintă starea inițială a unei conversații. Starea attempt, similară cu starea down, doar că unul dintre ruterele ce sunt configurate cu protocolul OSPF inițiază o conversație. Starea init indică faptul că un pachet de tip „hello" a fost transmis, dar încă nu a fost stabilită o conversație bidirecțională. Starea two-way indică stabilirea conversației bidirecționale. Starea exstart reprezintă primul pas al adiacentei dinre rutere, iar starea exchange reprezintă furnizarea de informații a unui ruter despre baza de date creată pe baza stărilor legăturilor. Starea loading, ruterul solicită cele mai recente LSA-uri de la vecinii descoperiți. Starea full, ruterele au încheiat conversația și au bazele de date ale LSR-urilor sincronizate.

In topologia considerata, protocolul de rutare OSPF a fost implementat pe ruterele din reteaua MPLS in aria 0: PE1, PE2, PE3, PE4, P1, P2, P3 si P4. Acest protocol este potrivit pentru o asemenea retea de tip full-mesh deoarece determina ruta cu costul minim.

5.2.2 BGP (Border Gateway Protocol)

Protocolul de rutare BGP menține o tabelă cu prefixe IP, prin intermediul cărora găsește ruta către rețeaua respectivă prin diferite sisteme autonome. Este considerat un protocol vector-cale, fiind similar cu protocoalele vector-distanță, diferența fiind că deciziile sunt luate pe baza politicilor de rutare ale sistemului autonom.

BGP stabilește și menține conexiuni între ruterele vecine folosind protocolul TCP. În cazul ruterelor aflate în sisteme autonome diferite, conexiunea de tip BGP poate fi realizată doar dacă ruterele sunt direct conectate. Legătura este stabilită pe portul 179 și este menținută prin mesaje periodice de 19 bytes, intervalul între aceste mesaje fiind de 60 de secunde.

Tipurile de mesaje ale protocolului BGP sunt următoarele: Open, prin care se stabilesc conexiuni între rutere, Keepalive, sunt mesaje cu lungimea de 19 bytes trimise periodic pentru a menține conexiunea, Update, conțin rute către diverse rețele dacă există actualizări în tabela de rutare a unui ruter din conexiune și Notification, mesaje ce raportează erori în comunicație.

În topologia prezentată, protocolul de rutare eBGP a fost implementat în ruterele CE1-A și CE1-B pentru a se conecta la rețaua MPLS, la ruterele PE1 și PE3. De asemenea a fost utilizat și protocolul de tip iBGP, MP-BGP pentru stabilirea VPN-ului de layer 3 între PE1 și PE3.

5.2.3 EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP este un protocol de rutare intern vector-distanță îmbunătățit. Inițial acest protocol de rutare a fost conceput de Cisco, dar ulterior a fost lansat de către IETF.

EIGRP combate deficiențele protocoalelor de rutare vector distanță, prin funcționalități precum load balancing pe rute cu costuri inegale, posibilitatea de identificare a rețelelor aflate la

255 de hop-uri și caracteristici de convergență rapidă. Acest protocol utilizează un algoritm de actualizare difuză, prescurtat DUAL, pentru a identifica rute ale rețelelor și pentru a furniza convergența rapidă folosind rute predefinite fără bucle. Majoritatea protocoalelor de rutare bazate pe vector de distanță utilizează număr de salturi de metrică pentru deciziile de rutare, neluându-se în calcul întârzierea totală și viteza link-ului. EIGRP ține cont de acești factori pentru luarea deciziilor de rutare.

În topologia considerată, protocolul de rutare EIGRP a fost implementat în ruterele CE3-A, CE3-B, PE1 și PE3, pentru a conecta ruterele client la rețeaua MPLS.

5.3 Configurarea echipamantelor

Înainte de a configura echipamentele, am alocat adrese IP dispozitivelor:

1. Pentru Customer 1:
    - Adresa loopback CE1-A: 1.1.1.1/32
    - Adresa loopback CE1-B: 3.3.3.3/32
    - CE1-A către PE1: 10.0.1.0/30
    - CE1-B către PE3: 10.0.3.0/30
2. Pentru Customer 3:
    - Adresa loopback CE3-A: 2.2.2.2/32
    - Adresa loopback CE3-B: 4.4.4.4/32
    - CE3-A către PE1: 10.0.2.1/30
    - CE3-B către PE2: 10.0.4.1/30
3. Pentru Customer 2:
    - CE2-A către PE2: 172.16.0.2/29
    - CE2-B către PE4: 172.16.0.3/29

4. Pentru Customer 4:
    - CE4-A către PE2: 192.168.1.2/24
    - CE4-B către PE4: 192.168.1.5/24

5. Pentru rețeaua furnizorului de servicii (rețeaua MPLS):
    - Adresa loopback PE1: 5.5.5.5/32
    - Adresa loopback PE2: 12.12.12.12/32
    - Adresa loopback PE3: 7.7.7.7/32
    - Adresa loopback PE4: 13.13.13.13/32
    - Adresa loopback P1: 8.8.8.8/32
    - Adresa loopback P2: 10.10.10.10/32

- Adresa loopback P3: 9.9.9.9/32
- Adresa loopback P4: 11.11.11.11/32
- PE1 către CE1-A: 10.0.1.2/30
- PE1 către CE3-A: 10.0.2.2/30
- PE1 către P1: 100.0.1.0/30
- PE1 către P2: 100.0.1.0/30
- PE2 către P2: 100.0.11.0/30
- PE2 către P4: 100.0.12.0/30
- PE3 către CE1-B: 10.0.3.2/30
- PE3 către CE3-B: 10.0.4.2/30
- PE3 către P3: 100.0.9.0/30
- PE3 către P4: 100.0.10.0/30
- PE4 către P1: 100.0.13.0/30
- PE4 către P3: 100.0.14.0/30
- P1 către P2: 100.0.5.0/30
- P1 către P3: 100.0.3.0/30
- P1 către P4: 100.0.4.0/30
- P2 către P3: 100.0.6.0/30
- P2 către P4: 100.0.7.0/30
- P3 către P4: 100.0.8.0/30

Rețeaua furnizorului de servicii este încadrată în sistemul autonom cu numărul 1234, rețeaua clientului 1 site A este în sistemul autonom 1, clientul 1 site B este în sistemul autonom 3, clientul 3 site A se află în sistemul autonom 2, iar client 3 site B în sistemul autonom 4.

Protocolul de rutare IGP din interiorul rețelei furnizorului de servicii este OSPF. Întrucât rețeaua este una de tip full mesh, prin utilizarea protocolului OSPF există multiple beneficii precum: calculul eficient al rutelor, convergența rapidă, load balancing, fiabilitate ridicată, redundanță scăzută și selectarea rutei optime. Ruterele ce fac parte din rețeaua MPLS au fost adăugate în aria 0, iar ID-ul ruterelor a fost setat ca fiind adresa de loopback. Pe baza acestui protocol de rutare, protocolul LDP poate stabili foarte rapid LSP-urile din rețeaua MPLS.

```
router ospf 1
 router-id 5.5.5.5
 network 5.5.5.5 0.0.0.0 area 0
 network 100.0.1.0 0.0.0.3 area 0
 network 100.0.2.0 0.0.0.3 area 0
```

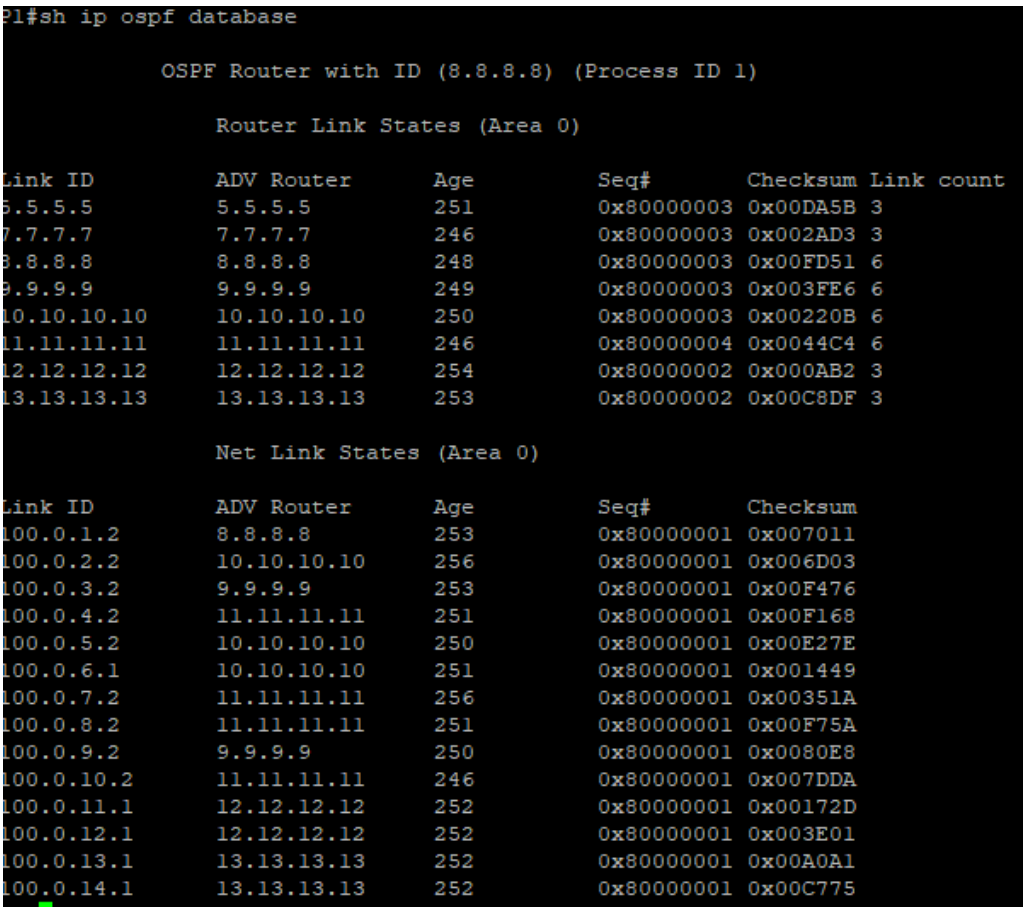
Figura 5.2 Configurarea protocolului OSPF a ruterului PE1

```
router ospf 1
 router-id 8.8.8.8
 network 8.8.8.8 0.0.0.0 area 0
 network 100.0.1.0 0.0.0.3 area 0
 network 100.0.3.0 0.0.0.3 area 0
 network 100.0.4.0 0.0.0.3 area 0
 network 100.0.5.0 0.0.0.3 area 0
 network 100.0.13.0 0.0.0.3 area 0
```

Figura 5.3 Configurarea protocolului OSPF a ruterului P1

```
PE1#sh ip ospf database

            OSPF Router with ID (5.5.5.5) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
5.5.5.5         5.5.5.5         166         0x80000003 0x00DA5B 3
7.7.7.7         7.7.7.7         163         0x80000003 0x002AD3 3
8.8.8.8         8.8.8.8         164         0x80000003 0x00FD51 6
9.9.9.9         9.9.9.9         166         0x80000003 0x003FE6 6
10.10.10.10     10.10.10.10     166         0x80000003 0x00220B 6
11.11.11.11     11.11.11.11     163         0x80000004 0x0044C4 6
12.12.12.12     12.12.12.12     170         0x80000002 0x000AB2 3
13.13.13.13     13.13.13.13     170         0x80000002 0x00C8DF 3

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
100.0.1.2       8.8.8.8         171         0x80000001 0x007011
100.0.2.2       10.10.10.10     172         0x80000001 0x006D03
100.0.3.2       9.9.9.9         171         0x80000001 0x00F476
100.0.4.2       11.11.11.11     168         0x80000001 0x00F168
100.0.5.2       10.10.10.10     166         0x80000001 0x00E27E
100.0.6.1       10.10.10.10     166         0x80000001 0x001449
100.0.7.2       11.11.11.11     172         0x80000001 0x00351A
100.0.8.2       11.11.11.11     168         0x80000001 0x00F75A
100.0.9.2       9.9.9.9         166         0x80000001 0x0080E8
100.0.10.2      11.11.11.11     163         0x80000001 0x007DDA
100.0.11.1      12.12.12.12     168         0x80000001 0x00172D
100.0.12.1      12.12.12.12     168         0x80000001 0x003E01
100.0.13.1      13.13.13.13     169         0x80000001 0x00A0A1
100.0.14.1      13.13.13.13     169         0x80000001 0x00C775
```

Figura 5.4 Baza de date OSPF a ruterelui PE1



```
P1#sh ip ospf database

            OSPF Router with ID (8.8.8.8) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
5.5.5.5         5.5.5.5         251         0x80000003 0x00DA5B 3
7.7.7.7         7.7.7.7         246         0x80000003 0x002AD3 3
8.8.8.8         8.8.8.8         248         0x80000003 0x00FD51 6
9.9.9.9         9.9.9.9         249         0x80000003 0x003FE6 6
10.10.10.10     10.10.10.10     250         0x80000003 0x00220B 6
11.11.11.11     11.11.11.11     246         0x80000004 0x0044C4 6
12.12.12.12     12.12.12.12     254         0x80000002 0x000AB2 3
13.13.13.13     13.13.13.13     253         0x80000002 0x00C8DF 3

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
100.0.1.2       8.8.8.8         253         0x80000001 0x007011
100.0.2.2       10.10.10.10     256         0x80000001 0x006D03
100.0.3.2       9.9.9.9         253         0x80000001 0x00F476
100.0.4.2       11.11.11.11     251         0x80000001 0x00F168
100.0.5.2       10.10.10.10     250         0x80000001 0x00E27E
100.0.6.1       10.10.10.10     251         0x80000001 0x001449
100.0.7.2       11.11.11.11     256         0x80000001 0x00351A
100.0.8.2       11.11.11.11     251         0x80000001 0x00F75A
100.0.9.2       9.9.9.9         250         0x80000001 0x0080E8
100.0.10.2      11.11.11.11     246         0x80000001 0x007DDA
100.0.11.1      12.12.12.12     252         0x80000001 0x00172D
100.0.12.1      12.12.12.12     252         0x80000001 0x003E01
100.0.13.1      13.13.13.13     252         0x80000001 0x00A0A1
100.0.14.1      13.13.13.13     252         0x80000001 0x00C775
```

Figura 5.5 Baza de date OSPF a ruterelui P1

Pe baza figurilor 5.2 si 5.3 se observă faptul că bazele de date OSPF ale ruterelor PE1 și P1 sunt identice, implicit toate ruterele ce fac parte din aria 0 trebuie să aibă baze de date identice.

```
PE1#sh ip ro ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      7.0.0.0/32 is subnetted, 1 subnets
O        7.7.7.7 [110/4] via 100.0.2.2, 00:08:19, GigabitEthernet0/1
                 [110/4] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
      8.0.0.0/32 is subnetted, 1 subnets
O        8.8.8.8 [110/2] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
      9.0.0.0/32 is subnetted, 1 subnets
O        9.9.9.9 [110/3] via 100.0.2.2, 00:08:19, GigabitEthernet0/1
                 [110/3] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
      10.0.0.0/32 is subnetted, 1 subnets
O        10.10.10.10 [110/2] via 100.0.2.2, 00:08:29, GigabitEthernet0/1
      11.0.0.0/32 is subnetted, 1 subnets
O        11.11.11.11 [110/3] via 100.0.2.2, 00:08:29, GigabitEthernet0/1
                     [110/3] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
      12.0.0.0/32 is subnetted, 1 subnets
O        12.12.12.12 [110/3] via 100.0.2.2, 00:08:19, GigabitEthernet0/1
      13.0.0.0/32 is subnetted, 1 subnets
O        13.13.13.13 [110/3] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
      100.0.0.0/8 is variably subnetted, 16 subnets, 2 masks
O        100.0.3.0/30 [110/2] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
O        100.0.4.0/30 [110/2] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
O        100.0.5.0/30 [110/2] via 100.0.2.2, 00:08:29, GigabitEthernet0/1
                      [110/2] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
O        100.0.6.0/30 [110/2] via 100.0.2.2, 00:08:29, GigabitEthernet0/1
O        100.0.7.0/30 [110/2] via 100.0.2.2, 00:08:29, GigabitEthernet0/1
O        100.0.8.0/30 [110/3] via 100.0.2.2, 00:08:29, GigabitEthernet0/1
                      [110/3] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
O        100.0.9.0/30 [110/3] via 100.0.2.2, 00:08:19, GigabitEthernet0/1
                      [110/3] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
O        100.0.10.0/30 [110/3] via 100.0.2.2, 00:08:29, GigabitEthernet0/1
                       [110/3] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
O        100.0.11.0/30 [110/2] via 100.0.2.2, 00:08:19, GigabitEthernet0/1
O        100.0.12.0/30 [110/3] via 100.0.2.2, 00:08:19, GigabitEthernet0/1
                       [110/3] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
O        100.0.13.0/30 [110/2] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
O        100.0.14.0/30 [110/3] via 100.0.2.2, 00:08:19, GigabitEthernet0/1
                       [110/3] via 100.0.1.2, 00:08:19, GigabitEthernet0/0
```

Figura 5.6 Tabela de rutare determinată prin OSPF a ruterelui PE1

```
PE1#ping 7.7.7.7 repeat 10 size 1024
Type escape sequence to abort.
Sending 10, 1024-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 5/8/12 ms
```

Figura 5.7 Testarea conectivității între ruterele PE1 și PE3

Pentru distribuirea etichetelor în rețeaua MPLS a furnizorului de servicii am utilizat protocolul LDP. Pentru fiecare ruter ce face parte din rețea am activat acest protocol, atribuindu-i fiecărui ruter un range unic de valori ale etichetelor, pentru a putea realiza o analiză cât mai exactă. Intervalul de valori alocat fiecărui ruter este:

- PE1 – 100-199
- P1 – 200-299

- P2 – 300-399
- P3 – 400-499
- P4 – 500-599
- PE3 – 600-699
- PE2 – 700-799
- PE4 – 800-899

```
PE1#sh mpls label range
Downstream Generic label region: Min/Max label: 100/199
```

Figura 5.8 Intervalul de valori ale etichetelor pentru ruterul PE1

În contextul atribuirii intervalelor de valori pentru fiecare LSR în parte, am ales această configurație deoarece primele 16 valori ale etichetelor reprezintă funcții speciale, cum ar fi: eticheta cu valoarea 0 este eticheta explicit NULL și eticheta cu valoarea 3 este eticheta implicit NULL.

Pentru a verifica comunicația dintre ruterele din rețeaua MPLS și de asemenea comutarea de etichete putem utiliza două comenzi pe care sistemul de operare IOS le conține: ping mpls și traceroute mpls.

```
E1#traceroute 7.7.7.7
ype escape sequence to abort.
racing the route to 7.7.7.7
RF info: (vrf in name/id, vrf out name/id)
 1 100.0.1.2 [MPLS: Label 218 Exp 0] 12 msec
   100.0.2.2 [MPLS: Label 316 Exp 0] 7 msec
   100.0.1.2 [MPLS: Label 218 Exp 0] 7 msec
 2 100.0.6.2 [MPLS: Label 405 Exp 0] 22 msec
   100.0.4.2 [MPLS: Label 516 Exp 0] 8 msec
   100.0.6.2 [MPLS: Label 405 Exp 0] 16 msec
 3 100.0.10.1 8 msec
   100.0.9.1 5 msec
   100.0.10.1 15 msec
```

Figura 5.9 Verificarea comutării etichetelor în rețeaua MPLS

```
PE1#traceroute mpls ipv4 7.7.7.7/32
Tracing MPLS Label Switched Path to 7.7.7.7/32, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
  0 100.0.1.1 MRU 1500 [Labels: 220 Exp: 0]
L 1 100.0.1.2 MRU 1500 [Labels: 520 Exp: 0] 21 ms
L 2 100.0.4.2 MRU 1504 [Labels: implicit-null Exp: 0] 22 ms
! 3 100.0.10.1 12 ms
```

Figura 5.10 Verificarea comutării etichetelor în rețeaua MPLS

Din figura 5.10 se observă faptul că la penultimul ruter din LSP, se execută funcția de Penultimate Hop-Popping, fapt ce duce la creșterea vitezei transferului de pachete.

```
PE1#sh mpls ldp bindings 7.7.7.7 32
  lib entry: 7.7.7.7/32, rev 40
        local binding:  label: 116
        remote binding: lsr: 10.10.10.10:0, label: 318
        remote binding: lsr: 8.8.8.8:0, label: 220
```

Figura 5.11 LSP-ul dintre PE1 către PE3

```
PE2#sh mpls ldp bindings 13.13.13.13 32
  lib entry: 13.13.13.13/32, rev 8
        local binding:  label: 702
        remote binding: lsr: 10.10.10.10:0, label: 315
        remote binding: lsr: 11.11.11.11:0, label: 505
        remote binding: lsr: 13.13.13.13:0, label: imp-null
```

Figura 5.12 LSP-ul dintre PE2 către PE4

```
▸ Ethernet II, Src: 0c:ee:46:64:00:01 (0c:ee:46:64:00:01), Dst: 0c:13:b5:6d:00:01
▾ MultiProtocol Label Switching Header, Label: 122, Exp: 0, S: 1, TTL: 252
    0000 0000 0000 0111 1010 .... .... .... = MPLS Label: 122 (0x0007a)
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 1111 1100 = MPLS TTL: 252
▸ Internet Protocol Version 4, Src: 3.3.3.3, Dst: 10.0.1.1
```

Figura 5.13 Header-ul MPLS în comunicația dintre ruterele PE1 și P2 în analizatorul de rețea Wireshark

Din figura 5.13 putem observa că header-ul MPLS este situată între header-ele de layer 2 și layer 3, valoarea etichetei este 122, câmpul S are valoarea 1, indicând faptul că este ultima etichetă din stivă, iar câmpul TTL arată durata de viață a pachetului.

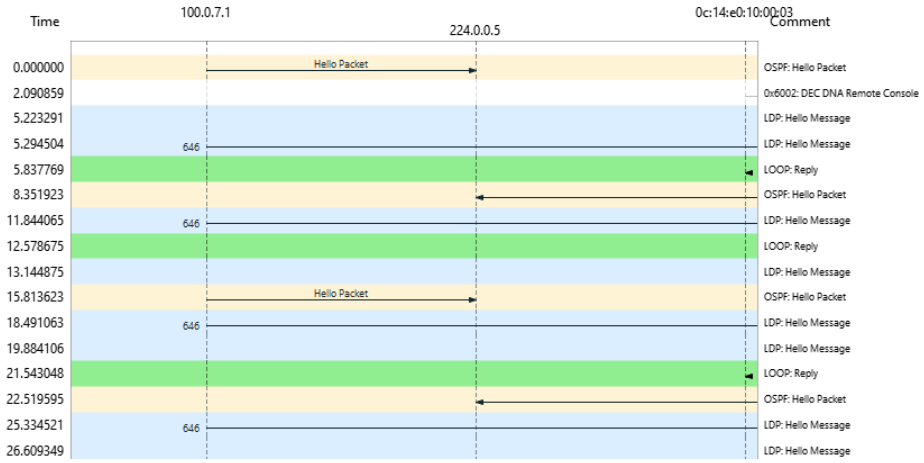


Figura 5.14 Menținerea sesiunilor OSPF și LDP

5.3.1 MPLS Layer 3 VPN

Pentru stabilirea VPN-ului de layer 3, este necesară configurarea protocolului MP-BGP pe ruterele marginale PE1 și PE3 pentru transportarea tipurilor de pachete vpnv4. Acest protocol este unul de tip iBGP, deci ruterele ce fac parte din aceaste sesiuni trebuie să se afle în același sistem autonom. În cazul de față atât PE1, cât și PE3 fac parte din AS-ul 1234.

```
For address family: VPNv4 Unicast
 Session: 7.7.7.7
 BGP table version 21, neighbor version 21/0
 Output queue size : 0
 Index 2, Advertise bit 1
 2 update-group member
 NEXT_HOP is always this router for eBGP paths
 Extended-community attribute sent to this neighbor
 Slow-peer detection is disabled
 Slow-peer split-update-group dynamic is disabled
                         Sent       Rcvd
 Prefix activity:        ----       ----
   Prefixes Current:        4          4 (Consumes 640 bytes)
   Prefixes Total:          4          4
   Implicit Withdraw:       0          0
   Explicit Withdraw:       0          0
   Used as bestpath:      n/a          8
   Used as multipath:     n/a          0
```

Figura 5.15 Sesiunea MP-BGP dintre ruterele PE1 și PE3

```
!
router bgp 1234
 bgp log-neighbor-changes
 neighbor 7.7.7.7 remote-as 1234
 neighbor 7.7.7.7 update-source Loopback0
 !
 address-family vpnv4
  neighbor 7.7.7.7 activate
  neighbor 7.7.7.7 send-community extended
  neighbor 7.7.7.7 next-hop-self
 exit-address-family
```

Figura 5.16 Configurarea protocolului MP-BGP pentru ruterul PE1

Politica de export "next-hop-self" este configurată pentru ruterele marginale pentru a seta adresa de next-hop ca fiind adresă de loopback pentru rute primite prin eBGP înainte ca acestea să fie transmise către alte rutere din grupul MP-BGP. De asemenea, actualizările vor avea ca sursă adresele de loopback ale ruterelor PE.

Pentru serviciul de layer 3 VPN dedicat clienților Customer 1 și Customer 3, au fost configurate două instanțe de rutare pe ambele rutere marginale PE1 și PE3, denumite Customer1, respectiv Customer3. Fiecare VRF a fost atribuit interfeței ce conectează ruterele de tip PE cu cele CE și de asemenea a fost asignat un route distinguisher de forma Router-ID: Customer-ID, unde Customer-ID este 1 pentru Customer 1 și 3 pentru Customer 3. Totodată este atribuit și un route target.

```
PE1#sh vrf
  Name                             Default RD          Protocols   Interfaces
  Customer1                        5.5.5.5:1           ipv4        Gi0/7
  Customer3                        5.5.5.5:3           ipv4        Gi0/5
```

Figura 5.17 Instanțele VRF

Ruterele clienților Customer 1 au fost configurate cu eBGP, pentru a stabili o sesiune cu ruterele marginale ale rețelei MPLS. Prin intermediul instanțelor de rutare VRF, am putut separa tabela de rutare globală în două tabele de rutare, specifică fiecărui client de MPLS Layer 3 VPN. Astfel ruterele CE1-A și CE1-B se conectează la VRF-ul denumit Customer1.

```
PE1#sh ip ro vrf Customer1

Routing Table: Customer1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
B        1.1.1.1 [20/0] via 10.0.1.1, 00:34:05
      3.0.0.0/32 is subnetted, 1 subnets
B        3.3.3.3 [200/0] via 7.7.7.7, 00:33:30
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.0.1.0/30 is directly connected, GigabitEthernet0/7
L        10.0.1.2/32 is directly connected, GigabitEthernet0/7
B        10.0.3.0/30 [200/0] via 7.7.7.7, 00:33:30
```

Figura 5.18 Tabela de rutare a VRF-ului Customer1 pentru PE1

Se poate observa din figura 5.16 că prin intermediul protocolului MP-BGP, tabela de rutare a instanței de rutare Customer1 a ruterului PE1 conține adresa clientului CE1-B. Aceasta conține și adresa ruterului CE1-A, prin intermediul protocolului eBGP. VRF-ul adaugă RD-ul atribuit VPN-ului și distribuie ruta de tip vpnv4 prin MP-BGP, împreună cu RT-ul de export către PE3.

```
PE1#sh vrf detail
VRF Customer1 (VRF Id = 1); default RD 5.5.5.5:1; default VPNID <not set>
  New CLI format, supports multiple address-families
  Flags: 0x180C
  Interfaces:
    Gi0/7
Address family ipv4 unicast (Table ID = 0x1):
  Flags: 0x0
  Export VPN route-target communities
    RT:5.5.5.5:1
  Import VPN route-target communities
    RT:7.7.7.7:3
```

Figura 5.19 Detaliile despre VRF Customer1

Ruterul PE3 primește această rută de tip vpnv4, compară RT-ul local cu cel primit, iar pe baza acestei comparații adaugă ruta în tabela de rutare a protocolului iBGP, va fi înlăturat RD-ul,

ruta IPv4 fiind adaugată în tabela de rutare VRF, specifică Customerului 1. Prin protocolul eBGP această rută va fi trimisă către CE1-B.

```
CE1-B#
CE1-B#sh ip ro bgp
CE1-B#sh ip ro bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
B        1.1.1.1 [20/0] via 10.0.3.2, 00:52:27
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
B        10.0.1.0/30 [20/0] via 10.0.3.2, 00:52:27
```

Figura 5.20 Tabela de rutare a protocolului BGP a ruterului CE1-B

Prin urmare, vom testa conectivitatea și hop-urile prin care pachetele trec pentru comunicația dintre CE1-A și CE3-B:

```
CE1-A#ping 3.3.3.3 repeat 10 size 1024
Type escape sequence to abort.
Sending 10, 1024-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 10/13/16 ms
CE1-A#traceroute 3.3.3.3
Type escape sequence to abort.
Tracing the route to 3.3.3.3
VRF info: (vrf in name/id, vrf out name/id)
  1 10.0.1.2 7 msec 4 msec 4 msec
  2 100.0.1.2 [MPLS: Labels 212/619 Exp 0] 18 msec 12 msec 11 msec
  3 100.0.3.2 [MPLS: Labels 410/619 Exp 0] 15 msec 24 msec 25 msec
  4 10.0.3.2 [AS 3] [MPLS: Label 619 Exp 0] 34 msec 21 msec 12 msec
  5 10.0.3.1 [AS 3] 21 msec 16 msec 19 msec
```

Figura 5.21 Testarea conectivității dintre CE1-A și CE1-B

Pentru clienții Customer 3, conexiunile dintre ruterele CE3-A și PE1, respectiv CE3-B și PE3 au fost realizate prin intermediul protocolului EIGRP. Față de Customer 1 este necesară

redistribuirea protocolului iBGP. VRF-ul Customer3 are o configurație asemănătoare, diferind doar RD-ul, importul și exportul RT-urilor.

```
VRF Customer3 (VRF Id = 2); default RD 5.5.5.5:3; default VPNID <not set>
  New CLI format, supports multiple address-families
  Flags: 0x180C
  Interfaces:
    Gi0/5
Address family ipv4 unicast (Table ID = 0x2):
  Flags: 0x0
  Export VPN route-target communities
    RT:5.5.5.5:2
  Import VPN route-target communities
    RT:7.7.7.7:4
```

Figura 5.22 Detaliile despre VRF Customer3

```
router eigrp 1
 !
 address-family ipv4 vrf Customer3 autonomous-system 2
  redistribute bgp 1234 metric 1000000 1 255 1 1500
  network 10.0.2.0 0.0.0.3
 exit-address-family
router bgp 1234
 bgp log-neighbor-changes
 neighbor 7.7.7.7 remote-as 1234
 neighbor 7.7.7.7 update-source Loopback0
 !
 address-family vpnv4
  neighbor 7.7.7.7 activate
  neighbor 7.7.7.7 send-community extended
  neighbor 7.7.7.7 next-hop-self
 exit-address-family
 !
 address-family ipv4 vrf Customer1
  neighbor 10.0.1.1 remote-as 1
  neighbor 10.0.1.1 activate
 exit-address-family
 !
 address-family ipv4 vrf Customer3
  redistribute eigrp 2
 exit-address-family
```

Figura 5.23 Redistribuirile protocoalelor EIGRP si BGP pentru ruterele marginale

Învățarea rutelor de către ruterele CE3-A și CE3-B este asemănătoare cu cea a ruterelor CE1-A și CE1-B, diferența este că aceste rute IPv4 vor fi primite prin intermediul protocolului EIGRP de tip extern.

```
CE3-A#sh ip ro eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      4.0.0.0/32 is subnetted, 1 subnets
D EX     4.4.4.4 [170/3072] via 10.0.2.2, 01:02:31, GigabitEthernet0/5
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D EX     10.0.4.0/30 [170/3072] via 10.0.2.2, 01:02:31, GigabitEthernet0/5
```

Figura 5.24 Tabela de rutare a protocolului EIGRP a ruterului CE3-A

Am testat conectivitatea dintre CE3-A și CE3-B:

```
CE3-A#ping 4.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/15/29 ms
CE3-A#tr
CE3-A#traceroute 4.4.4.4
Type escape sequence to abort.
Tracing the route to 4.4.4.4
VRF info: (vrf in name/id, vrf out name/id)
  1 10.0.2.2 5 msec 3 msec 2 msec
  2 100.0.1.2 [MPLS: Labels 212/621 Exp 0] 10 msec 13 msec 11 msec
  3 100.0.4.2 [MPLS: Labels 505/621 Exp 0] 15 msec 10 msec 20 msec
  4 10.0.4.2 [MPLS: Label 621 Exp 0] 16 msec 10 msec 9 msec
  5 10.0.4.1 17 msec 11 msec 11 msec
```

Figura 5.25 Testarea conectivitatii dintre rutrele CE3-A și CE3-B

Pentru a analiza performanțele rețelei MPLS am folosit analizatorul de rețea Wireshark pentru a genera un grafic al lățimii de bandă. Formula lățimii de bandă este:

$$Lățimea\ de\ bandă = Numărul\ total\ de\ octeți * \frac{8}{Timpul\ de\ transmitere}$$

Voi considera transmisiunea între clienții Customer 1 și clienții Customer 3, întrucât sunt utilizate protocoale de rutare diferite în configurarea acestora. Astfel vom transmite inițial 1000 de pachete ICMP de lungime 1024 octeți din CE1-A către CE1-B și din CE3-A către CE3-B. Pentru a realiza o analiză cât mai bună voi ține cont de timpul round-trip maxim al pachetelor.

Timpul round-trip reprezintă durata pe care un pachet de date o are în drumul sau de la sursă la destinație și de la destinație înapoi la sursă. Cu cât timpul este mai mare, cu atât întârzierile sunt mai mari.

Aceste transmisiuni vor fi analizate folosind funcția “I/O Graphs” din cadrul aplicației Wireshark, o aplicație destinată analiziei comunicațiilor în cadrul rețelelor de calculatoare si nu numai. Pe axa Y este reprezentat numărul de pachete în unitatea de timp, iar pe axa X este reprezentat timpul.

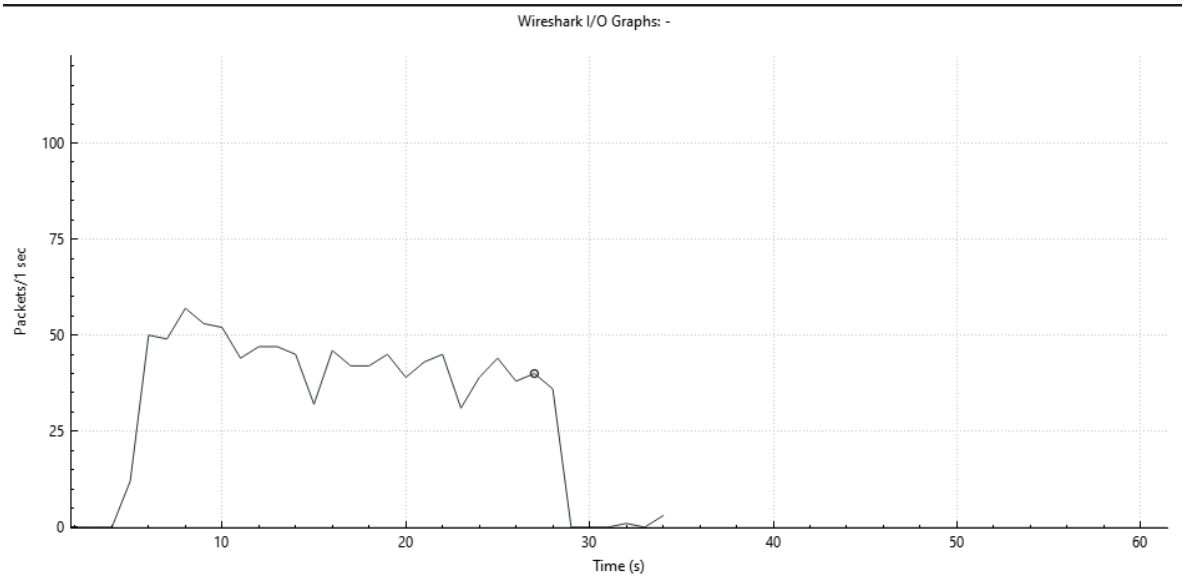


Figura 5.26 Graficul lățimii de bandă în cazul clientului Customer 1 pentru 1000 de pachete

Timpul RT maxim a fost de 73 milisecunde. Se poate observa faptul că în primele 10 secunde există o creștere exponențială, cauzată de începerea transmisiunii de pachete, apoi o stabilizare a graficului. Numărul de pachete transmise în unitatea de timp fluctuează intre 25, respectiv 50, scăderile graficului arătand faptul că există întarzieri in transmiterea de informații. În final se observă o scădere bruscă, fapt ce arată terminarea comunicării. Durata transmiterii infromațiilor a fost de aproximativ 26 de secunde.

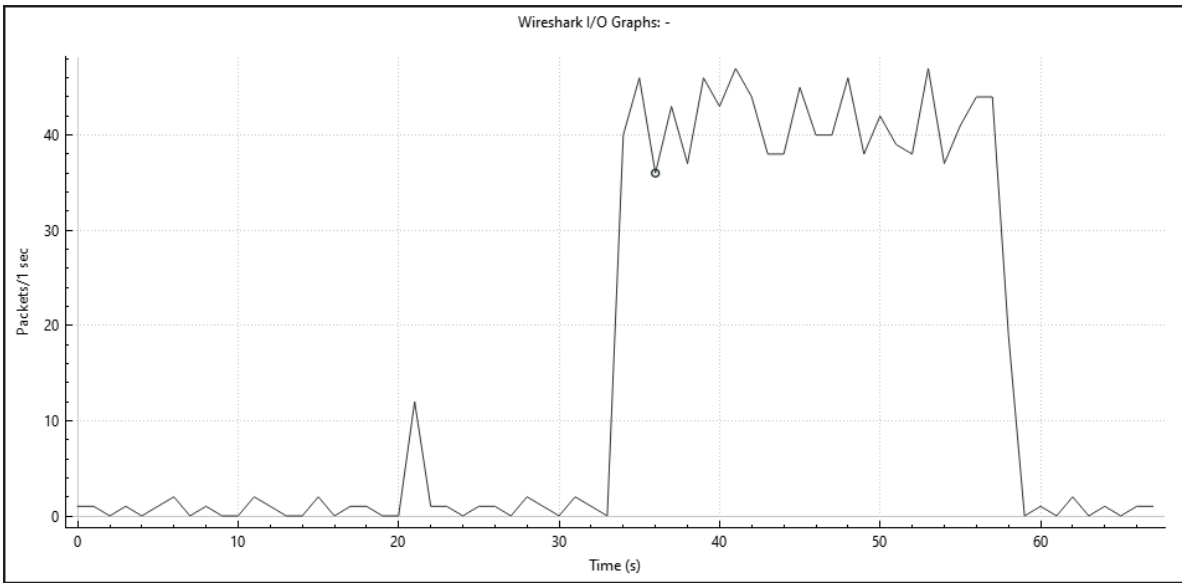


Figura 5.27 Graficul lățimii de bandă în cazul clientului Customer 3 pentru 1000 de pachete

Timpul RT maxim a fost de 82 milisecunde. În acest caz, transmiterea de informații începe în secunda 33, cresterea exponențială semnalând începerea transmisiei de pachete, urmată de o stabilizare a fluxului. Scăderile din partea superioară sunt datorate întarzierilor sau congestiilor ce apar în rețea. Rata de transmisie a pachetelor este în medie 40 de pachete pe secundă. Oprirea transmisiei este dată de scăderea bruscă a graficului, durata acestei transmisii fiind de 25 de secunde.

Voi mări numărul de pachete la 2500:

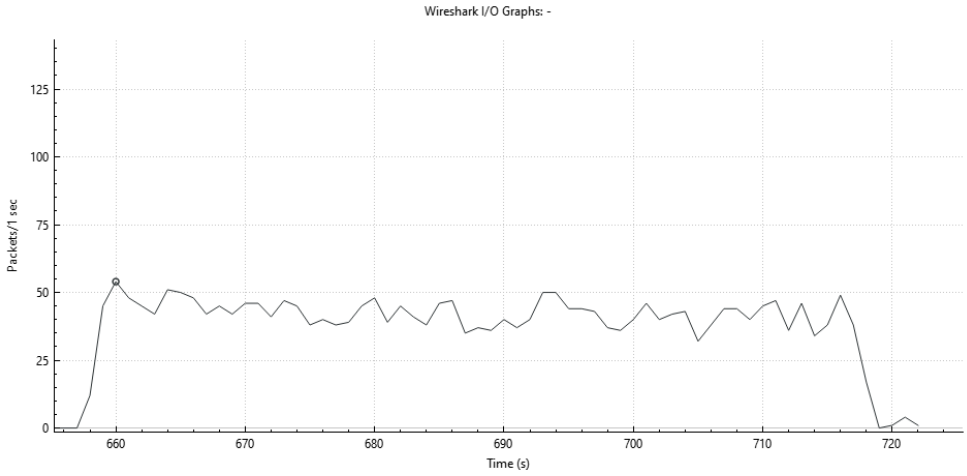


Figura 5.28 Graficul lățimii de bandă în cazul clientului Customer 1 pentru 2500 de pachete

Timpul RT maxim a fost de 95 de milisecunde. Se observă că atunci când dimensiunea fluxului de pachete este crescut, timpul de transmitere al acestor pachete este mai mare, în cazul de față fiind de 61 de secunde. Rata de transmisie al pachetelor fluctuează intre 30 si 50 de pachete pe secundă, dar scăderile nefiind exponențiale nu au existat pierderi de pachete.

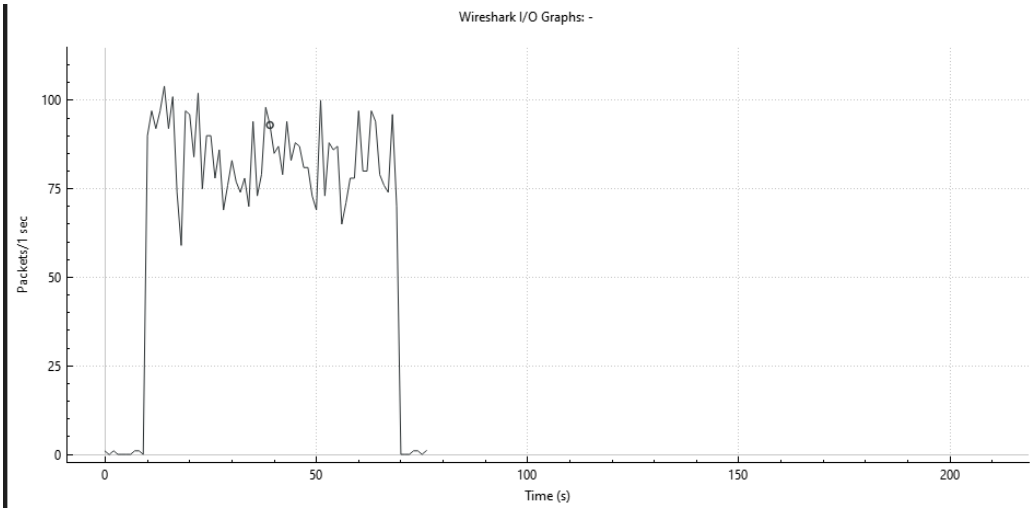


Figura 5.29 Graficul lățimii de bandă în cazul clientului Customer 3 pentru 2500 de pachete

Timpul RT maxim a fost de 100 de milisecunde. Durata transmiterii pachetelor a fost de 60 de secunde, rata de transfer a pachetelor fiind între 60 si 105 pachete pe secundă. Scăderile bruște din acest grafic indică pierderi de pachete sau congestii severe in rețea.

Voi mări din nou numărul de pachete la 5000:

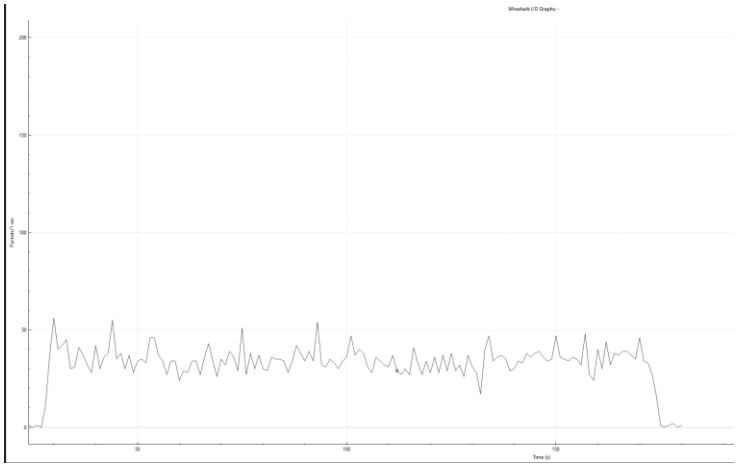


Figura 5. 30 Graficul lățimii de bandă în cazul clientului Customer 1 pentru 5000 de pachete

Timpul RT maxim a fost de 120 milisecunde. Se poate observa faptul că durata transmisiei pachetelor a crescut la 120 de secunde, existând și scăderi bruște. Fluxul de pachete a fost transmis cu o rată de transmsiei intre 30 și 50 pachete pe secundă.

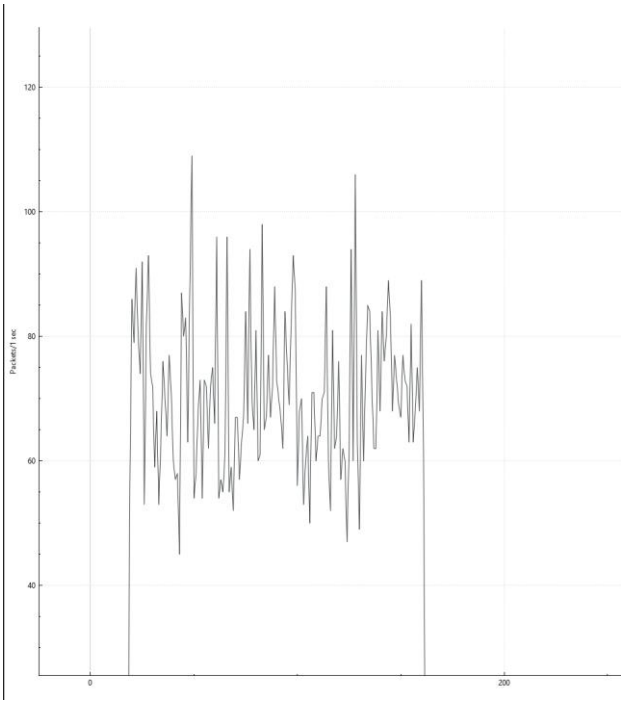


Figura 5.31 Graficul lățimii de bandă în cazul clientului Customer 3 pentru 5000 de pachete

Timpul RT maxim a fost de 115 milisecunde. Pe baza acestui grafic ce prezintă fluctuații continue, se observă faptul că rata de transmisie a datelor este intre 40 și 130 pachete pe secundă, într-un interval de 120 de secunde. Aceste fluctuații sunt datorate congestiilor și întârzierilor din rețea.

Voi mări numărul de pachete la 7500.

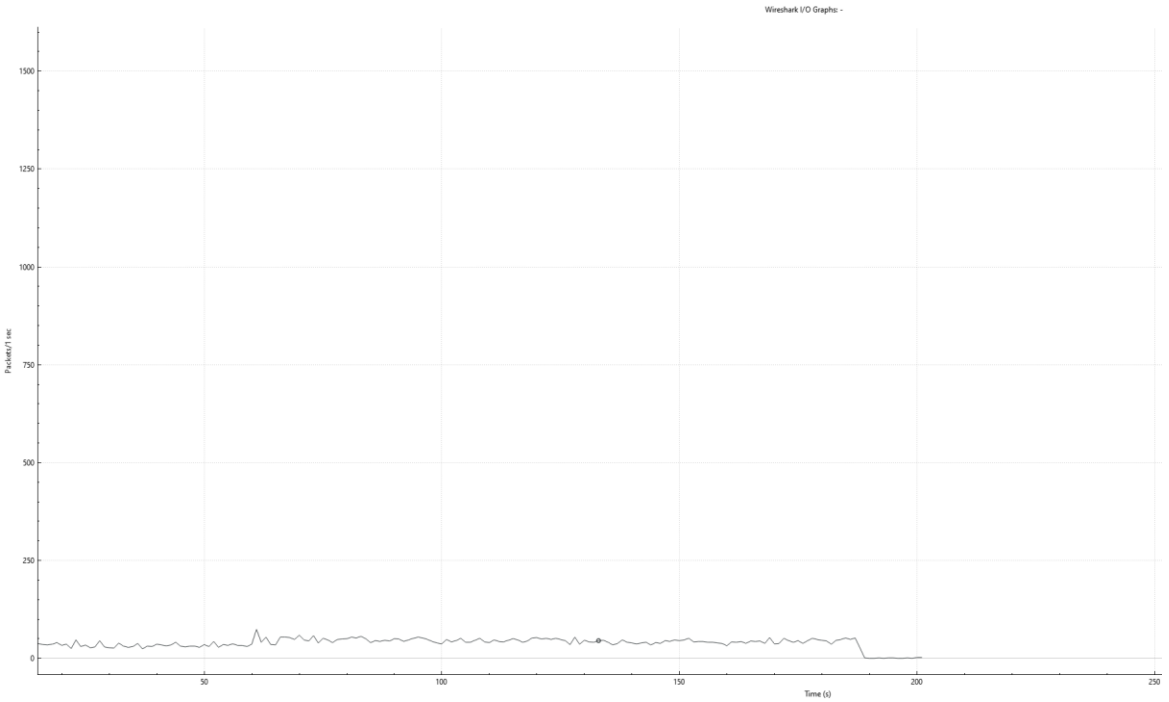


Figura 5.32 Graficul lățimii de bandă în cazul clientului Customer 1 pentru 7500 de pachete

Timpul RT maxim a fost de 101 milisecunde. Durata transmisiei a fost de 190 de secunde cu rate de transfer ce variaza între 50 și 100 de pachete pe secundă. Graficul nu prezintă scăderi bruște, transmisia datelor fiind una stabilă prezentând doar întârzieri nu și pierderi de pachete.

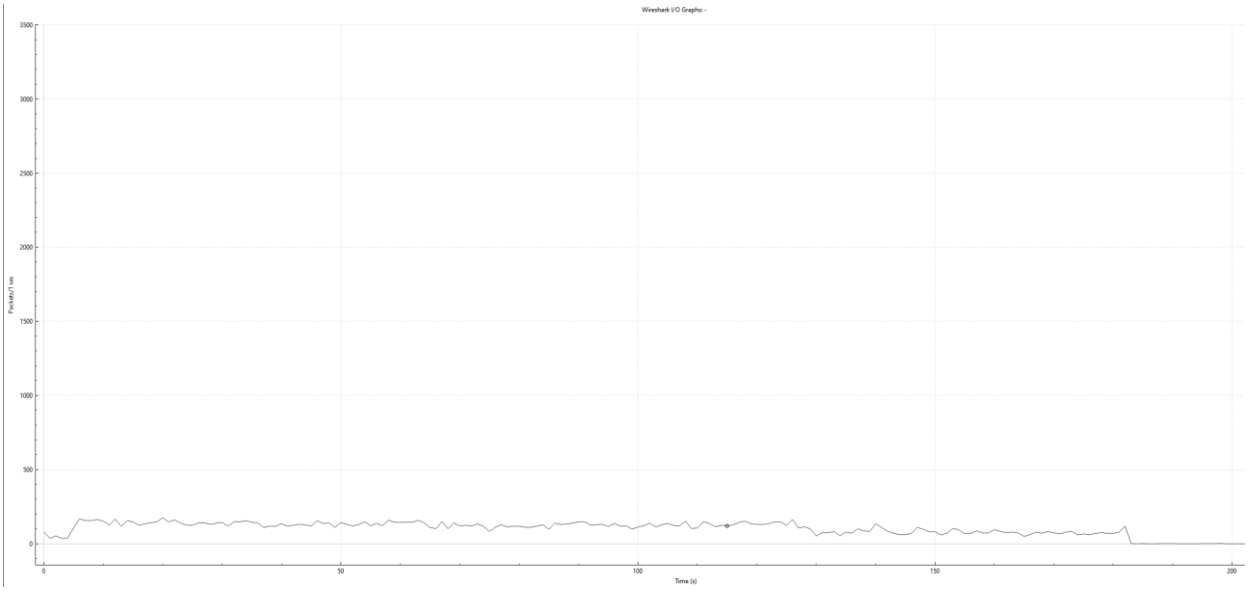


Figura 5.33 Graficul lățimii de bandă în cazul clientului Customer 3 pentru 7500 de pachete

Timpul RT maxim a fost de 97 milisecunde. Timpul de transmisie al datelor a fost de 180 de secunde cu rate de transfer între 100 și 200 de pachete pe secundă. Graficul nu prezintă scăderi bruște, transmisia datelor fiind una stabilă prezentând doar întârzieri nu și pierderi de pachete.

În final voi mări numărul de pachete la 10000.

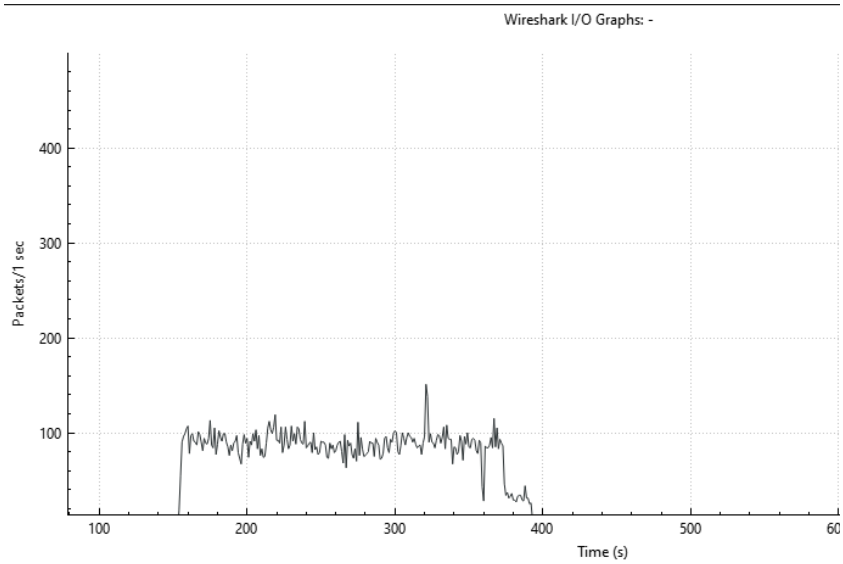


Figura 5.34 Graficul lățimii de bandă în cazul clientului Customer 1 pentru 10000 de pachete

Timpul RT maxim a fost de 119 milisecunde. Durata de transmisie a datelor a fost de 240 de secunde cu rate de transfer cuprinse între 100 si 140 de pachete pe secundă. Graficul prezintă scăderi bruște, mai ales la finalul transmisiei de date atingând un minim al ratei de transfer de 10 pachete pe secundă, fapt ce indică o pierdere de pachete.

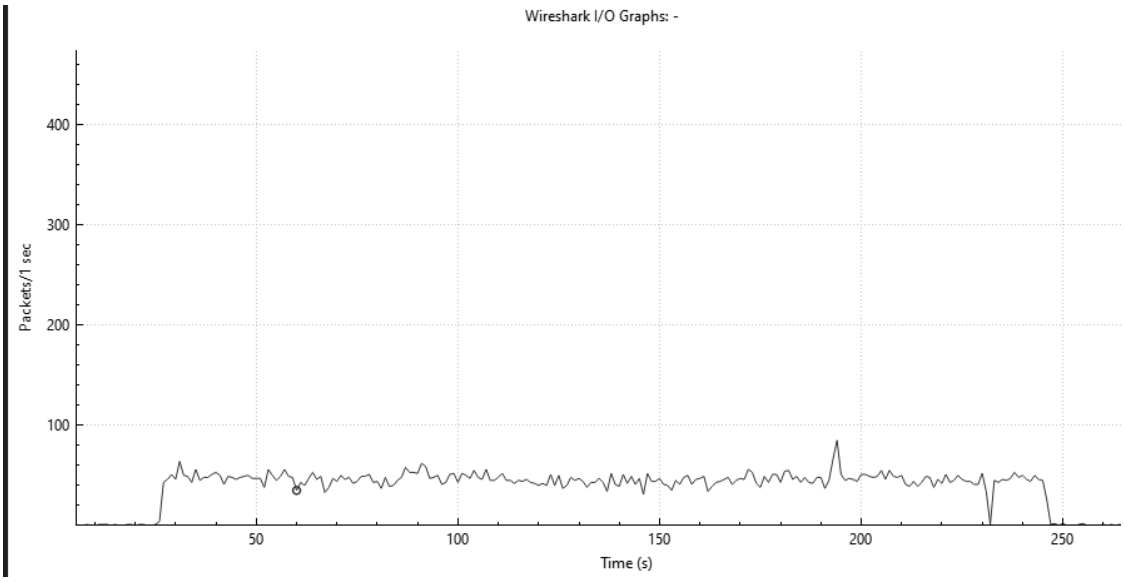


Figura 5.35 Graficul lățimii de bandă în cazul clientului Customer 3 pentru 10000 de pachete

Timpul RT maxim a fost de 91 de milisecunde. Durata de transmisie a datelor a fost de 215 secunde cu rate de transfer cuprinse între 40 si 80 de pachete pe secundă. Graficul prezintă scăderi bruște, mai ales la finalul transmisiei de date atingând un minim al ratei de transfer de 0 pachete pe secundă, fapt ce indică o pierdere de pachete sau o congestie a traficului severă.

Pe baza analizei, se poate observa faptul că pentru un număr de pachete cuprins între 1000 și 7500, comunicația dintre clienții Customer 3, este mai avantajoasă, fapt ce poate fi datorat utilizării protocolului EIGRP. În schimb, pentru o transmisie de 10000 de pachete, se observă faptul că lățimea de bandă în cazul clienților Customer 1 este mai bună.

De asemenea, scăderea graficelor arată faptul că există deficiențe în comunicație. Aceste deficiențe pot fi jittere, întârzieri, pierderi de pachete, congestii în rețea sau chiar performanțe slabe ale echipamentelor. În funcție de numărul de pachete transmise, fiecare client are mai multe sau mai puține scăderi în grafice, panta acestor grafice arătând de fapt modificarea lățimii de bandă în timp.

5.3.2 MPLS Layer 2 VPN

Pentru a stabili un VPN de layer 2 prin intermediul tehnologiei AToM este nevoie de crearea unei clase denumite pseudowire-class. Am implementat două astfel de clase pentru ruterele PE2 și PE4, denumite Customer2 atribuit clienților Customer 2 și Customer4 atribuită clienților Customer 4. În cazul ambelor clase încapsularea cadrelor este de tip mpls.

```
pseudowire-class Customer2
 encapsulation mpls
!
pseudowire-class Customer4
 encapsulation mpls
```

Figura 5.36 Clasele de tip pseudowire atribuite clienților Customer 2 și Customer 4

Interfețele ruterelor PE2 și PE4 ce se conectează la ruterele clienților CE2-A, CE4-A, CE2-B și CE4-B nu sunt configurate cu adrese IP deoarece VPN-ul de layer 2 nu necesită funcția de rutare, iar interfețele ruterelor conectate se află în aceeași subrețea.

```
CE2-A#sh run int g0/1
Building configuration...

Current configuration : 132 bytes
!
interface GigabitEthernet0/1
 ip address 172.16.0.2 255.255.255.248
CE2-B#sh run int g0/1
Building configuration...

Current configuration : 132 bytes
!
interface GigabitEthernet0/1
 ip address 172.16.0.3 255.255.255.248
```

Figura 5.37 Interfețele ruterelor CE2-A și CE2-B conectate la ruterele PE

Pe interfețele ruterelor marginale trebuie implementată comanda “xconnect”, comanda specifică tehnologiei AToM, urmată de Router-ID-ul routerului marginal remote și un VC ID specific clientului.

```
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no cdp enable
 xconnect 13.13.13.13 200 encapsulation mpls pw-class Customer2
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no cdp enable
 xconnect 13.13.13.13 400 encapsulation mpls pw-class Customer4
```

Figura 5.38 Configurarea interfețelor conectate la ruterele clienților ale ruterului PE1

Voi testa conectivitatea între ruterele clientului Customer 4:

```
CE4-B#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/12/19 ms
```

Figura 5.39 Testarea conectivității dintre CE4-B și CE4-A

Prin utilizarea comenzii “traceroute” se vor afla hop-urile prin care trec cadrele, dar fiind un protocol specific nivelului de legătură de date va exista un singur hop, neexistând un protocol de rutare.

```
CE4-B#traceroute 192.168.1.2
Type escape sequence to abort.
Tracing the route to 192.168.1.2
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.2 10 msec 10 msec 11 msec
```

Figura 5. 40 Vizualizarea hop-urilor în comunicația dintre CE4-B și CE4-A

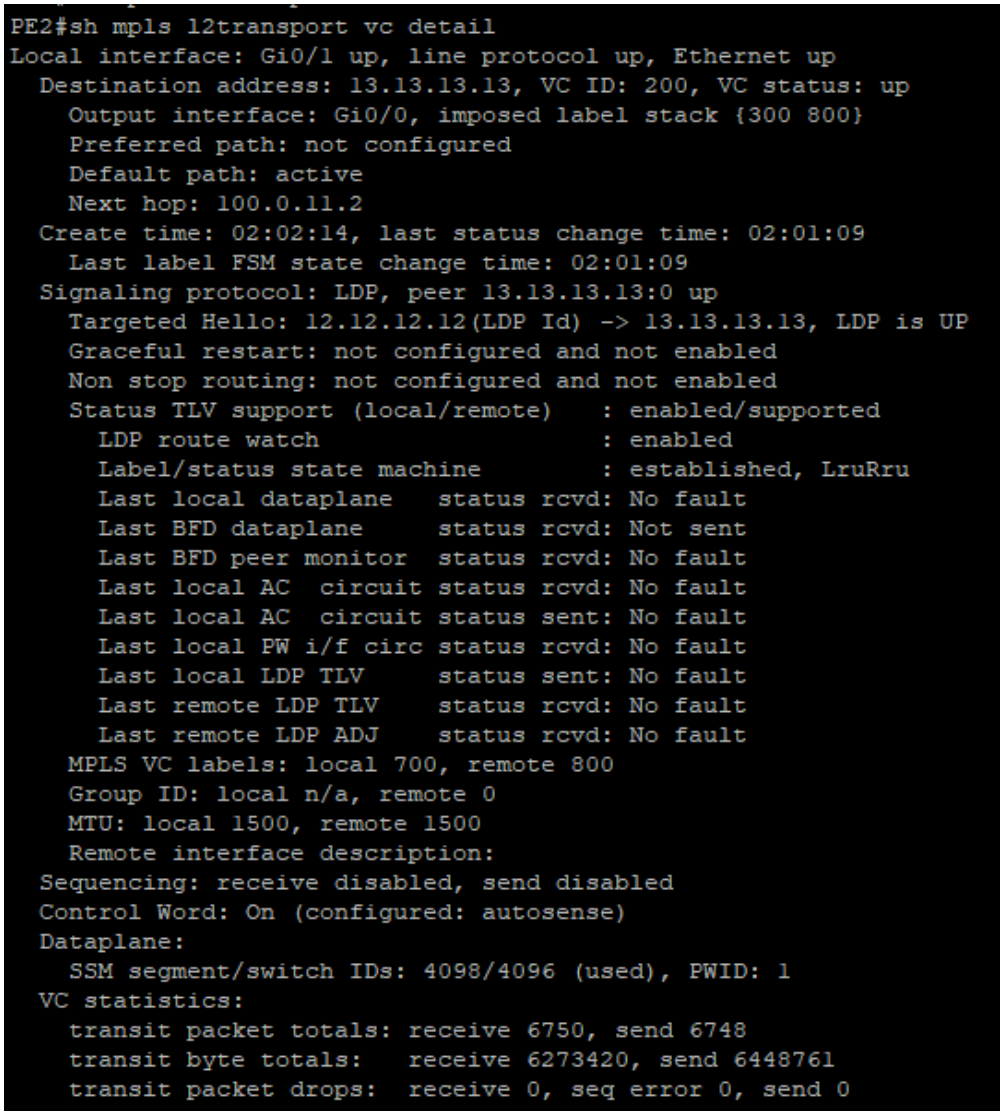


Figura 5.41 Informatii despre LSP-urile dintre PE2 si PE4

Cu ajutorul comenzii "show mpls l2transport binding" putem observa VC ID-urile specifice circuitelor virtuale transportate prin intermediul pseudofirelor și eticheta VC. Se observă și eticheta locală atribuită cadrelor și cea remote pentru fiecare VC ID.

Cadrelor le este atribuită o etichetă de tip VC pentru a identifica cărui pseudofir aparțin, apoi le sunt asignate o etichetă MPLS specifică LSP-ului. Acest pachet de date este transportat peste rețeaua MPLS, iar la ieșirea din rețea aceste etichete sunt eliminate cadrelele fiind trimise mai departe către destinație. Un avantaj al acestei tehnologii este reprezentat de faptul că ruterele clienților au o conectivitate directă și pot fi configurate protocoale de rutare între acestea.

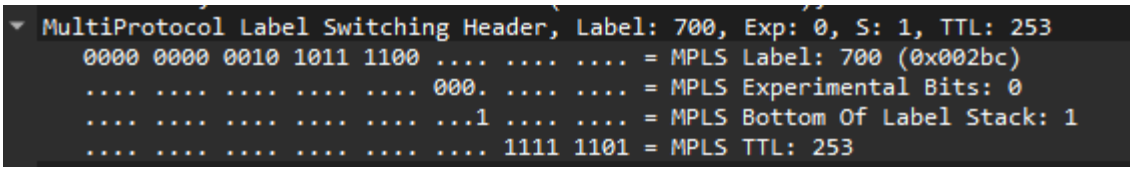


Figura 5.42 Antetul MPLS atribuit cadrelor

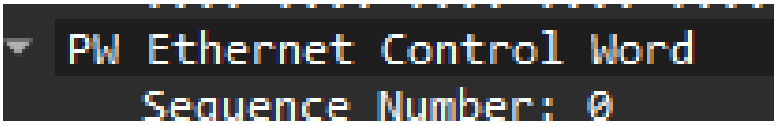


Figura 5.43 Câmpul Control Word

La fel ca în cazul serviciului de VPN layer 3 voi realiza o analiză a transmisiei dintre clienții Customer 2. Deoarece atât clientul Customer 2, cât și Customer 4 utilizează tehnologia AToM, voi analiza doar comunicația dintre CE2-A și CE2-B. Se vor transmite inițial pachete de lungime 1024 de octeți în număr de 1000. De asemenea, voi ține cont de timpul round-trip maxim al pachetelor.

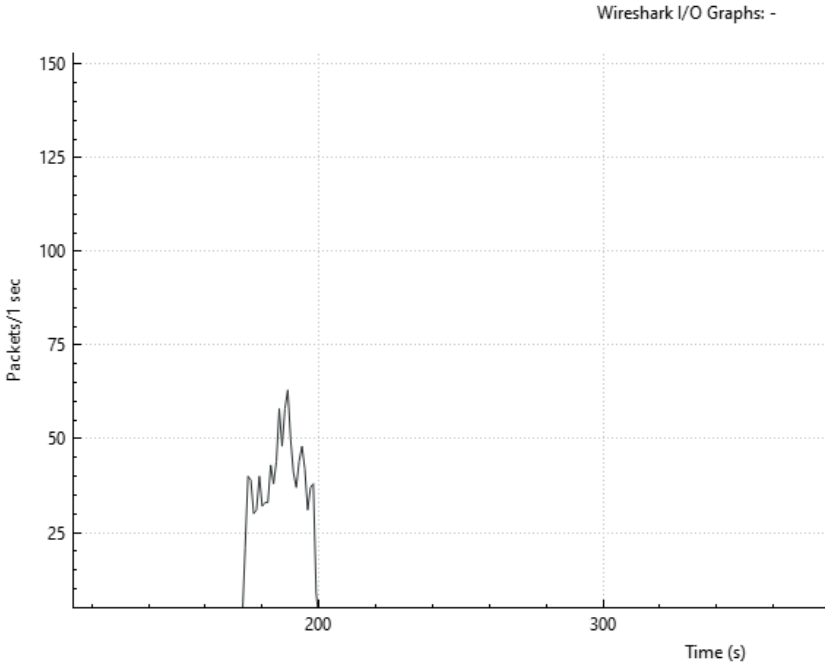


Figura 5.44 Graficul lățimii de bandă în cazul clientului Customer 2 pentru 1000 de pachete

Timpul round-trip (RT) în acest caz este maxim 49 de milisecunde. Durata transmisiei de informații a fost de 25 de secunde cu rate ce variază între 30 și 65 de pachete pe secundă. Se observă scăderi ale graficului ce pot fi interpretate ca fiind pierderi de pachete și întârzieri.

Voi mări numărul de pachete la 2500.

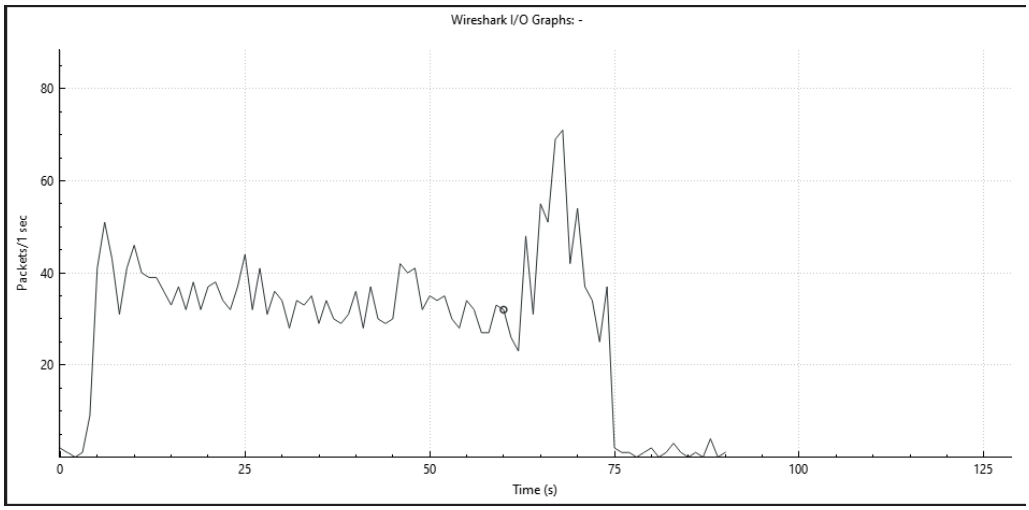


Figura 5.45 Graficul lățimii de bandă în cazul clientului Customer 2 pentru 2500 de pachete

Timpul RT maxim a fost de 116 milisecunde. Durata transmisiei de informații a fost de 73 de secunde cu rate ce variază între 25 și 75 de pachete pe secundă. Se observă scăderi ale graficului ce pot fi interpretate ca fiind întârzieri sau pachete pierdute, iar în finalul transmisunii, creșterea ratei de transmisie a pachetelor este data de retrimiterea pachetelor pierdute.

Voi mări numărul de pachete la 5000.

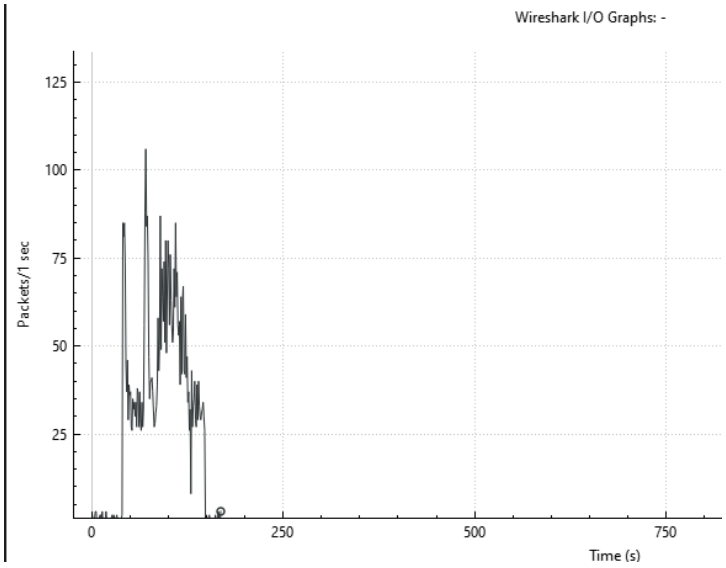


Figura 5.46 Graficul lățimii de bandă în cazul clientului Customer 2 pentru 5000 de pachete

Timpul RT maxim a fost de 96 milisecunde. Durata transmisiei de pachete a fost de 120 de secunde, cu rate de transmisie a pachetelor între 10 și 110 pachete pe secundă. Există multiple scăderi bruște ale ratei de transmisie, fapt ce îndică pierderi severe de pachete și întârzieri.

Voi mări numărul de pachete la 7500.

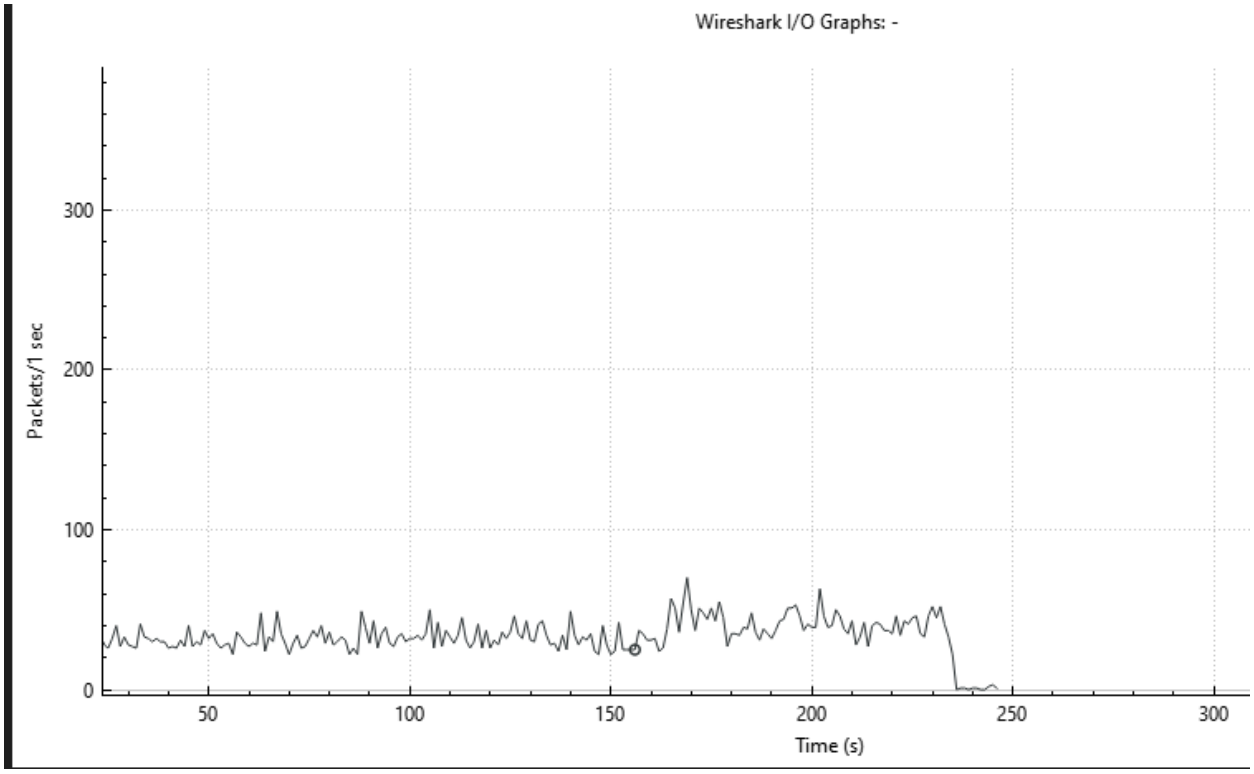


Figura 5.47 Graficul lățimii de bandă în cazul clientului Customer 2 pentru 7500 de pachete

Timpul RT maxim a fost 96 de milisecunde. Durata transmisiei de pachete a fost de 190 de secunde, cu rate de transmisie a pachetelor între 20 și 70 pachete pe secundă. Există multiple scăderi bruște ale ratei de transmisie, fapt ce îndică pierderi severe de pachete și întârzieri.

În final voi mări numărul de pachete la 10000.

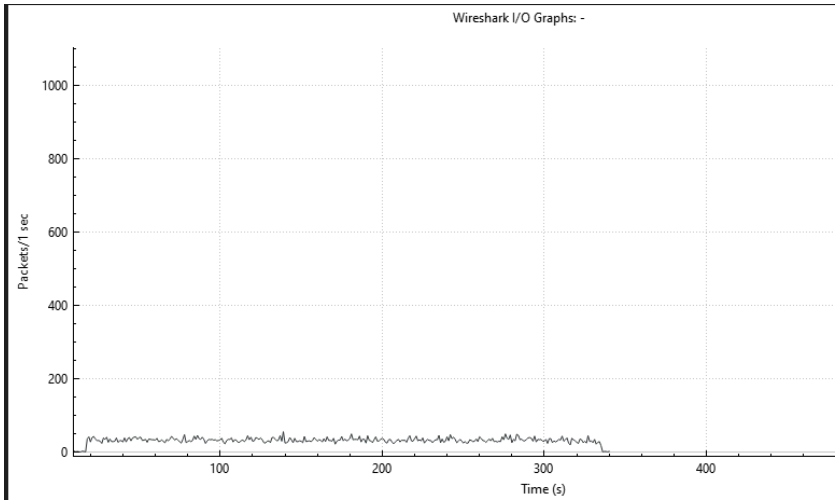


Figura 5.48 Graficul lățimii de bandă în cazul clientului Customer 2 pentru 10000 de pachete

Timpul RT maxim a fost de 110 milisecunde. Durata transmisiei de pachete a fost de 240 de secunde, cu rate de transmisie a pachetelor între 50 și 90 pachete pe secundă. Conform graficului nu există scăderi bruște, fapt ce indică o transmitere cu întârzieri, nu și pierderi de pachete.

5.3.3 Comparație Layer 3 VPN și Layer 2 VPN

Pe baza graficelor și a timpului round trip putem crea un tabel pentru a vizualiza timpul total al transmiterii pachetelor ICMP și RT-ul maxim pentru fiecare flux de pachete trimis în ambele tipuri de VPN. Vom compara comunicația dintre CE1-A și CE1-B și comunicația dintre CE2-A și CE2-B.

RT pentru fiecare flux de pachete (milisecunde)	Layer 3 VPN	Layer 2 VPN
1000 de pachete	73	49
2500 de pachete	95	116
5000 de pachete	120	96
7500 de pachete	101	96
10000 de pachete	119	110

Figura 5.49 Comparație timp maxim RT

Timp total de transmisie a fluxurilor de pachete (secunde)	Layer 3 VPN	Layer 2 VPN
1000 de pachete	26	25
2500 de pachete	64	73
5000 de pachete	150	120
7500 de pachete	190	240
10000 de pachete	240	340

Figura 5.50 Comparație timpul total de transmisie a datelor

Comparând rezultatele trecute în cele două tabele se poate observa faptul că prin intermediul VPN-ului de layer 2 întârzierile sunt mai mici, cât și timpul de transmisie al fluxurilor de pachete ICMP. Acest lucru era de așteptat deoarece nu sunt necesare operații de rutare sau redistribuire ale ruterelor. Totodată, ambele tipuri de VPN prezintă avantaje cât și dezavantaje din punct de vedere al configurării echipamentelor clienților. Un avantaj foarte important al VPN-ului de layer 2 este faptul că echipamentele clienților nu necesită un protocol de rutare pentru a putea comunica, acest serviciu necesită doar o conexiune de nivel de legătură de date către ruterele marginale ale rețelei. Un avantaj al serviciului VPN de layer 3 este faptul că prin intermediul protocoalelor RSVP-TE poate fi integrată tehnologia Traffic Engineering ce aduce o multitudine de funcții, un exemplu fiind serviciul QoS.

5.4 Simularea unor defecțiuni în topologia prezentată

Pentru a putea verifica scalarea rapidă a rețelei MPLS, vom elimina mai multe link-uri din rețeaua service provider-ului.

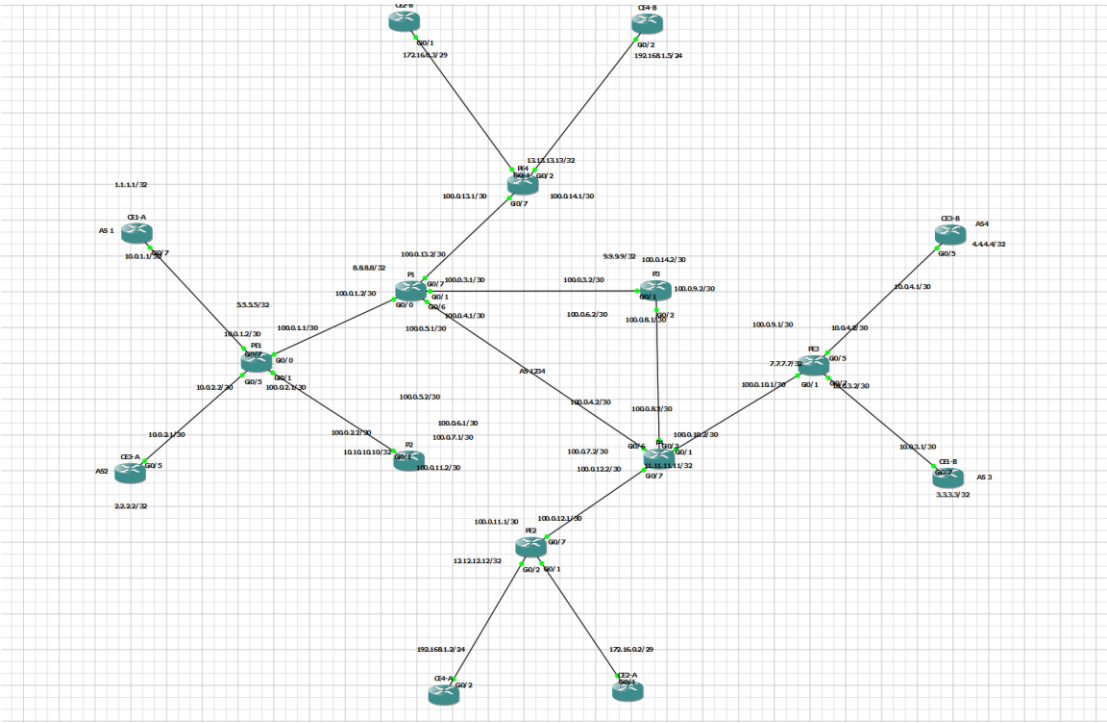


Figura 5.51 Topologia rețelei după eliminarea unor link-uri

Am eliminat legăturile dintre ruterele P1-P2, PE4-P3, PE2-P2, PE3-P3. Eliminarea link-uri dintre ruterele marginale și ruterele clienților nu ar avea sens deoarece, fiind o singură legătură pentru fiecare ruter client, nu ar mai exista deloc conectivitate între rețeaua MPLS și rețeaua clienților.

După eliminarea acestor legături, se observă că ruterele ce au implementate protocolul OSPF din aria 0, vor trimite mesaje de tip LSA, pentru a crea o bază de date ce conține noi informații din aria respectivă pentru a putea crea tabela de rutare.

```
    Number of LSAs: 1
  ▼ LSA-type 1 (Router-LSA), len 84
      .000 0000 0000 0001 = LS Age (seconds): 1
      0... .... .... .... = Do Not Age Flag: 0
    ▶ Options: 0x22, (DC) Demand Circuits, (E) External Routing
      LS Type: Router-LSA (1)
      Link State ID: 8.8.8.8
      Advertising Router: 8.8.8.8
      Sequence Number: 0x80000006
      Checksum: 0xd35e
      Length: 84
    ▶ Flags: 0x00
      Number of Links: 5
    ▶ Type: Stub     ID: 8.8.8.8         Data: 255.255.255.255 Metric: 1
    ▶ Type: Transit  ID: 100.0.13.1      Data: 100.0.13.2      Metric: 1
```

Figura 5.52 Mesaje de tip LSA între ruterele OSPF

```
PE1#sh ip ospf database

            OSPF Router with ID (5.5.5.5) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
5.5.5.5         5.5.5.5         1251        0x80000004 0x00D85C 3
7.7.7.7         7.7.7.7         80          0x80000005 0x00CA1F 2
8.8.8.8         8.8.8.8         103         0x80000006 0x00D35E 5
9.9.9.9         9.9.9.9         54          0x80000008 0x00EFFF 3
10.10.10.10     10.10.10.10     81          0x80000008 0x00EEE2 2
11.11.11.11     11.11.11.11     101         0x80000005 0x006290 5
12.12.12.12     12.12.12.12     83          0x80000004 0x00406B 2
13.13.13.13     13.13.13.13     55          0x80000004 0x004459 2

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
100.0.1.2       8.8.8.8         1270        0x80000002 0x006E12
100.0.2.2       10.10.10.10     1253        0x80000002 0x006B04
100.0.3.2       9.9.9.9         1239        0x80000002 0x00F277
100.0.4.2       11.11.11.11     1244        0x80000002 0x00EF69
100.0.8.2       11.11.11.11     1244        0x80000002 0x00F55B
100.0.10.2      11.11.11.11     1244        0x80000002 0x007BDB
100.0.12.1      12.12.12.12     1246        0x80000002 0x003C02
100.0.13.1      13.13.13.13     1267        0x80000002 0x009EA2
```

Figura 5.53 Noua bază de date OSPF a ruterelui PE1

```
PE1#sh ip ro ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      7.0.0.0/32 is subnetted, 1 subnets
O        7.7.7.7 [110/4] via 100.0.1.2, 00:54:17, GigabitEthernet0/0
      8.0.0.0/32 is subnetted, 1 subnets
O        8.8.8.8 [110/2] via 100.0.1.2, 00:54:27, GigabitEthernet0/0
      9.0.0.0/32 is subnetted, 1 subnets
O        9.9.9.9 [110/3] via 100.0.1.2, 00:54:27, GigabitEthernet0/0
      10.0.0.0/32 is subnetted, 1 subnets
O        10.10.10.10 [110/2] via 100.0.2.2, 00:54:17, GigabitEthernet0/1
      11.0.0.0/32 is subnetted, 1 subnets
O        11.11.11.11 [110/3] via 100.0.1.2, 00:54:06, GigabitEthernet0/0
      12.0.0.0/32 is subnetted, 1 subnets
O        12.12.12.12 [110/4] via 100.0.1.2, 00:01:54, GigabitEthernet0/0
      13.0.0.0/32 is subnetted, 1 subnets
O        13.13.13.13 [110/3] via 100.0.1.2, 00:54:27, GigabitEthernet0/0
      100.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
O        100.0.3.0/30 [110/2] via 100.0.1.2, 00:54:27, GigabitEthernet0/0
O        100.0.4.0/30 [110/2] via 100.0.1.2, 00:54:17, GigabitEthernet0/0
O        100.0.8.0/30 [110/3] via 100.0.1.2, 00:54:17, GigabitEthernet0/0
O        100.0.10.0/30 [110/3] via 100.0.1.2, 00:54:06, GigabitEthernet0/0
O        100.0.12.0/30 [110/3] via 100.0.1.2, 00:54:06, GigabitEthernet0/0
O        100.0.13.0/30 [110/2] via 100.0.1.2, 00:54:27, GigabitEthernet0/0
```

Figura 5.54 Noua tabelă de rutare OSPF a ruterelui PE1

Deoarece prin intermediul link-urile rămase, încă există conectivitate între toate ruterele OSPF din aria 0, adresele vecinilor au rămas în tabela de rutare, dar este diferit next-hop-ul pentru fiecare rută.

Vom testa conectivitatea între ruterele marginale ale rețelei, urmând să verificăm dacă comunicația între clienți este în continuare posibilă.

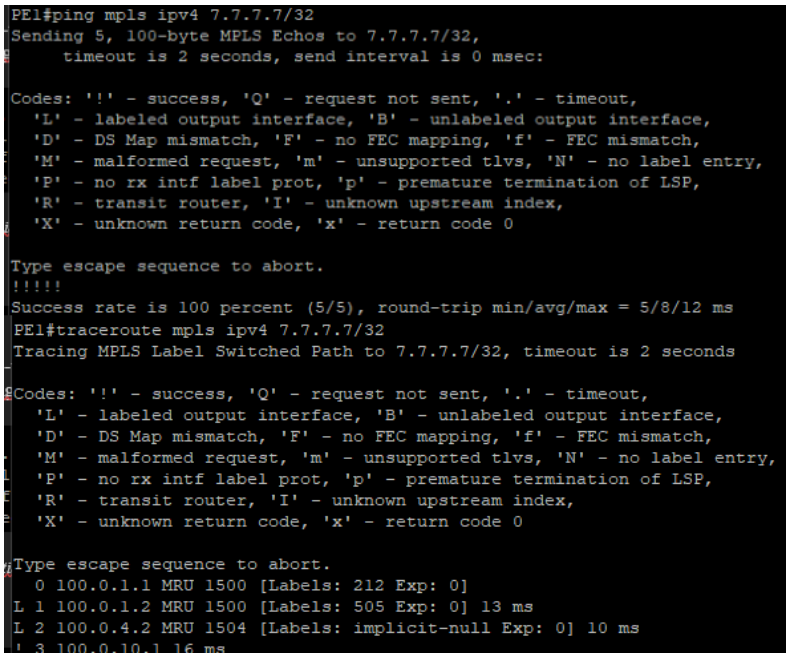


Figura 5.55 Verificarea conectivității între ruterele PE1 și PE3

Datorită rețelei de tip full mesh și faptului că protocolul de rutare IGP folosit este OSPF se poate observa faptul că există în continuare rute pe care pachetele le pot urma pentru a ajunge la destinație, chiar dacă numărul de hop-uri a scăzut.

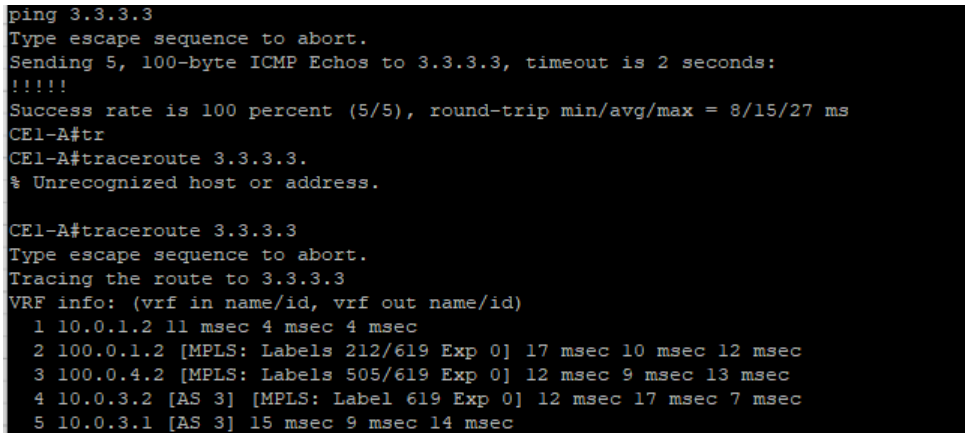


Figura 5.56 Verificarea conectivității între site-urile clienților Customer 1

```
CE3-A#ping 4.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/11/16 ms
CE3-A#tr
CE3-A#traceroute 4.4.4.4
Type escape sequence to abort.
Tracing the route to 4.4.4.4
VRF info: (vrf in name/id, vrf out name/id)
  1 10.0.2.2 5 msec 2 msec 8 msec
  2 100.0.1.2 [MPLS: Labels 214/619 Exp 0] 15 msec 14 msec 12 msec
  3 100.0.4.2 [MPLS: Labels 510/619 Exp 0] 12 msec 14 msec 11 msec
  4 10.0.4.2 [MPLS: Label 619 Exp 0] 10 msec 6 msec 13 msec
```

Figura 5.57 Verificarea conectivității între site-urile clienților Customer 3

De asemenea, putem observa faptul că între site-urile clienților ce utilizează serviciul VPN layer 3 funcționează în continuare optim. Similar cazului anterior numărul de hop-uri a scăzut.

```
CE2-A#ping 172.16.0.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/19/36 ms
CE2-A#tr
CE2-A#traceroute 172.16.0.3
Type escape sequence to abort.
Tracing the route to 172.16.0.3
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.0.3 22 msec 7 msec 12 msec
```

Figura 5.58 Verificarea conectivității între site-urile clienților Customer 2

La fel și în cazul clienților ce utilizează serviciul de VPN layer 2, conectivitatea înca este stabilită, diferă doar faptul că numărul de hop-uri este identic cu cel din topologia inițială deoarece comunicația rămâne una de nivel de legatură de date.

În continuare, voi analiza performanțele rețelei, în condițiile defecțiunii unor legături. Se vor efectua transmiteri de fluxuri de pachete între ruterele CE1-A și CE1-B, cât și între CE2-A și CE2-B pentru a se observa dacă vor fi schimbări majore din punct de vedere al performanțelor rețelei MPLS.

Inițial voi trimite 1000 pachete de 1024 de octeți, crescând ulterior numărul.

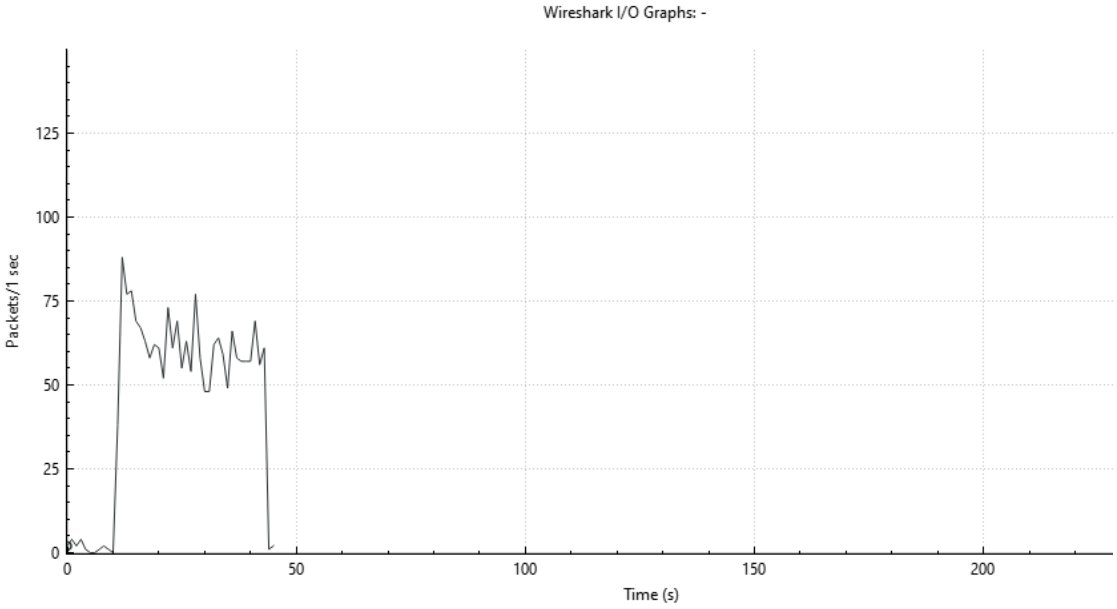


Figura 5.59 Graficul lățimii de bandă în cazul clientului Customer 1 pentru 1000 de pachete

Timpul RT maxim a fost de 72 milisecunde. Se poate observa faptul că în primele 10 secunde există o creștere exponențială, cauzată de începerea transmisiunii de pachete, apoi o stabilizare a graficului. Numărul de pachete transmise în unitatea de timp fluctuează intre 50, respectiv 85, scăderile graficului arătand faptul că există întarzieri in transmiterea de informații, dar si pierderi de pachete. În final se observă o scădere bruscă, fapt ce arată terminarea comunicării. Durata transmiterii infromațiilor a fost de aproximativ 35 de secunde.

Voi mări numărul de pachete la 2500.

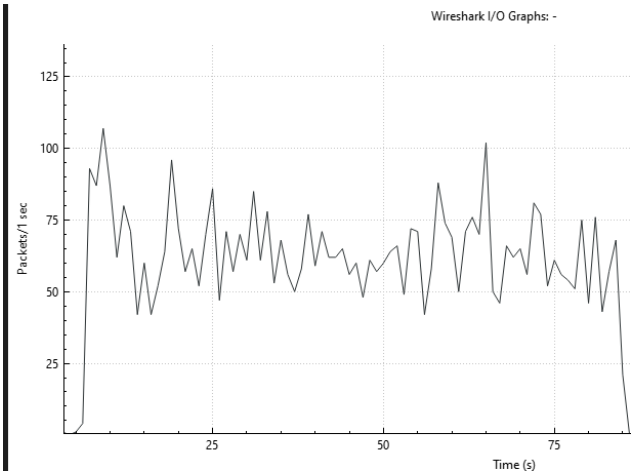


Figura 5.60 Graficul lățimii de bandă în cazul clientului Customer 1 pentru 2500 de pachete

Timpul RT maxim a fost de 77 de milisecunde. Se observă că atunci când dimensiunea fluxului de pachete este crescut, timpul de transmitere al acestor pachete este mai mare, în cazul de față fiind de 80 de secunde. Rata de transmisie al pachetelor fluctuează intre 40 și 105 de pachete pe secundă, dar scăderile fiind exponențiale au existat pierderi de pachete.

Voi mări numărul de pachete la 5000.

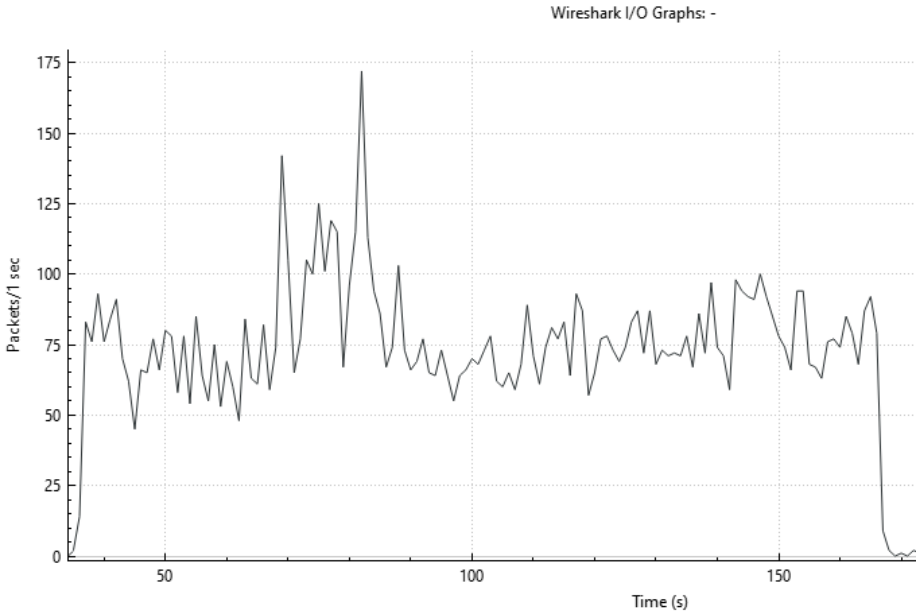


Figura 5.61 Graficul lățimii de bandă în cazul clientului Customer 1 pentru 5000 de pachete

Timpul RT maxim a fost de 126 milisecunde. Se poate observa faptul că durata transmisiei pachetelor a crescut la 120 de secunde, existând și scăderi bruște. Fluxul de pachete a fost transmis cu o rată de transmsiei intre 40 și 170 pachete pe secundă. Creșterile exponențiale ale graficului arată faptul că a existat o pierdere de pachete semnificativă, urmată de o transmitere cu o rată marită de pachete pe secundă.

Aceeași analiză va fi făcută asupra comunicației dintre CE2-A și CE2-B, inițial transmițându-se 1000 de pachete ICMP.

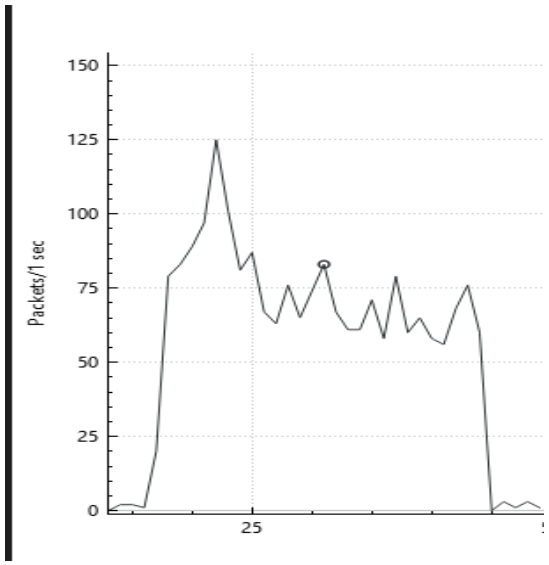


Figura 5.62 Graficul lățimii de bandă în cazul clientului Customer 2 pentru 1000 de pachete

Timpul round-trip în acest caz este maxim 67 de milisecunde. Durata transmisiei de informații a fost de 24 de secunde cu rate ce variază între 60 și 125 de pachete pe secundă. Se observă scăderi ale graficului ce pot fi interpretate ca fiind pierderi de pachete și întârzieri.

Voi mări numărul la 2500 de pachete.

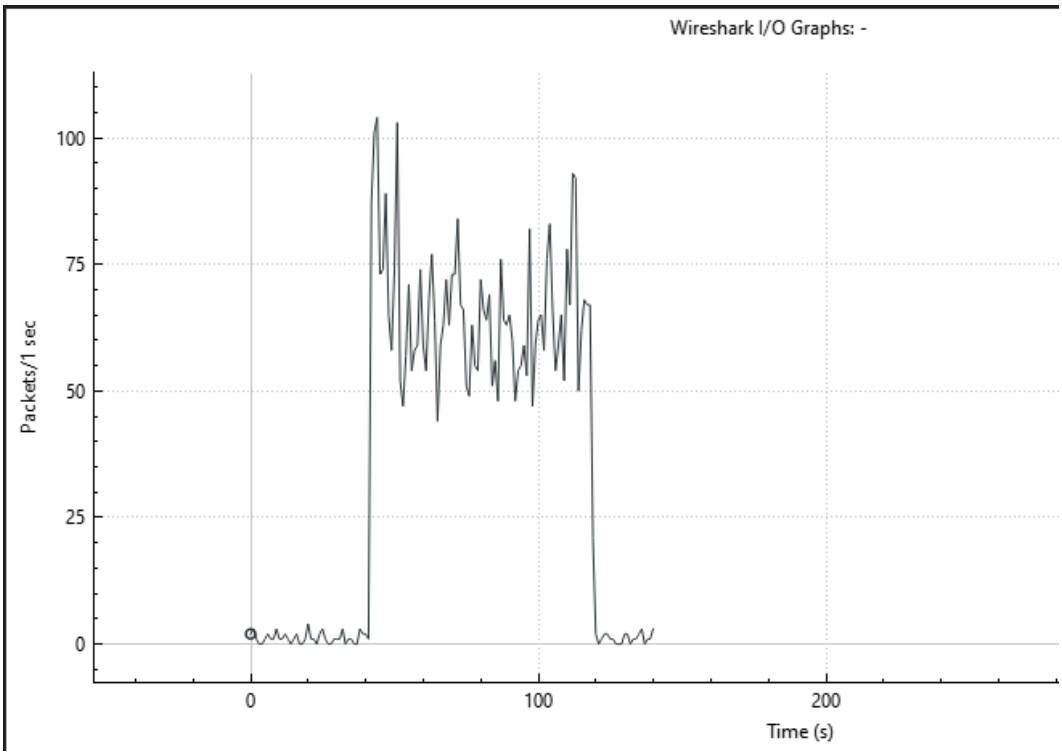


Figura 5.63 Graficul lățimii de bandă în cazul clientului Customer 2 pentru 2500 de pachete

Timpul RT maxim a fost de 102 milisecunde. Durata transmisiei de informații a fost de 80 de secunde cu rate ce variază între 45 și 105 de pachete pe secundă. Se observă scăderi ale graficului ce pot fi interpretate ca fiind întârzieri sau pachete pierdute, iar în finalul transmisunii, creșterea ratei de transmisie a pachetelor este data de retrimiterea pachetelor pierdute.

Voi mări numărul la 5000 de pachete.

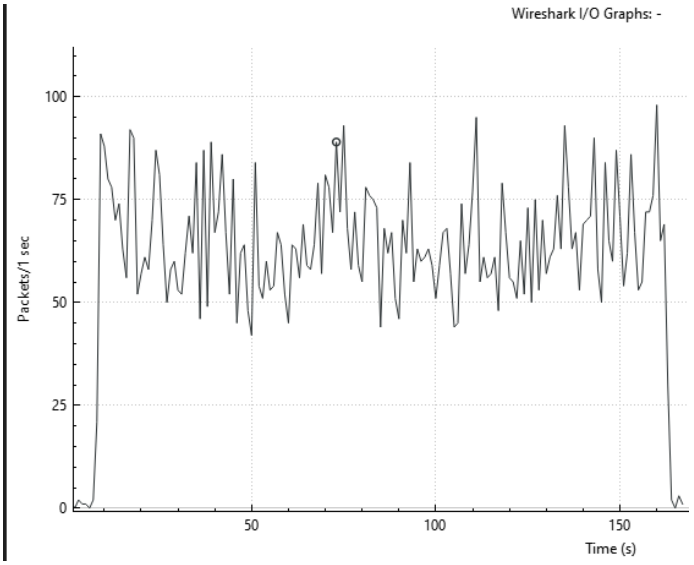


Figura 5.64 Graficul lățimii de bandă în cazul clientului Customer 2 pentru 5000 de pachete

Timpul RT maxim a fost de 123 milisecunde. Durata transmisiei de pachete a fost de 152 de secunde, cu rate de transmisie a pachetelor între 40 și 95 pachete pe secundă. Există multiple scăderi bruște ale ratei de transmisie, fapt ce îndică pierderi severe de pachete și întârzieri.

Pe baza graficelor și a timpului round-trip maxim putem observa faptul că eficiența transmisiilor este ușor mai scăzută față de cea inițială. Totuși, prin intermediul protocolului OSPF, ruterele au găsit rapid alte căi de transmitere ale pachetelor, fapt ce arată capabilitatea de scalare rapidă a rețelelor ce utilizează acest protocol de rutare intern.

Concluzii

Avantajele folosirii unei astfel de tehnologii sunt multiple, cele mai importante dintre acestea fiind: capabilitatea de scalare rapidă, flexibilitatea, fiabilitatea și securitatea din punct de vedere al izolării traficului diferiților clienți. Totuși, există și dezavantaje ale acestei tehnologii: costuri ridicate pentru implementarea și menținerea unei astfel de tehnologii, dar și securitatea din punct de vedere al criptării informațiilor.

Adăugarea clienților la o astfel de rețea este o operație ușor de realizat deoarece necesită configurația unui singur ruter din rețeaua MPLS. Ruterele de tip PE au configurate o tabelă de rutare, numită VRF, pentru fiecare client în parte, ceea ce asigură izolarea datelor, iar prin folosirea protocolului MP-BGP și a conceptelor Route Distinguisher și Route Target, se asigură transportul datelor între locații diferite ale clienților.

Un alt avantaj pe care tehnologia MPLS VPN îl oferă este posibilitatea de a implementa conceptul de Traffic Engineering, concept ce poate reduce întârzierile rețelei, congestiile, jitterele prin îndrumarea traficului de pe o rută deja utilizată pe una cu mai puțin trafic sau chiar deloc. De asemenea, prin utilizarea conceptului TE, traficul unui anumit client poate fi prioritizat prin utilizarea serciviului Quality of Service.

În urma implmentării tehnologiilor MPLS VPN layer 3 și AToM, am observat faptul că principiul acestora de funcționare este unul asemănător, deoarece ambele necesită o rețea de bază MPLS a furnizorului de servicii. Ambele folosesc principii prin care traficul clienților este izolat unul față de celălalt, dar complexitatea tehnologiei specifice nivelului de rețea este mai ridicat față de cel de nivel inferior.

Prin analizarea celor două tehnologii, se poate concluziona faptul că pentru un trafic de dimensiuni reduse utilizarea tehnologiei AToM, asigură un timp mai scăzut de transmitere al informațiilor, dar în contextul fluxurilor de dimensiuni mai mari, tehnologia MPLS VPN Layer 3 are performanțe mai bune.

BIBLIOGRAFIE

[1] E. Borcoci, "Network and Services V0.8: *Arhitectura MPLS* "

[2] Cisco Systems, Inc., "MPLS Fundamentals" 2007

[3] L. Lobo, U. Lakshman, "MPLS Configuration on Cisco IOS Software" 2006

[4] Alcatel-Lucent, "7750 SR OS MPLS Guide" 2008

[5] O. Catrina, "Architectures for Networks and Services: Multi-Protocol Label Switching"

[6] ZTE CORPORATION, "Feature Guide (Command Mode) (MPLS)" 2017

[7] R. Lacoste, B. Edgeworth, "CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide" 2020

[8] J. H. Carmouche, "IPsec Virtual Private Network Fundamentals" 2007

[9] Huawei Technologies Co., "Feature Description – MPLS" 2012

[10] E. Osborne, A. Simha "Traffic Engineering with MPLS" 2002

[11] Cisco , "Configure a Basic MPLS VPN Network" [Online] Available: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html

[12] Cisco Systems, Inc., "MPLS: Layer 2 VPNs, Configuration Guide, Cisco IOS Release 12.4T" 2011

[13] Juniper Networks, "Layer 2 VPNs and VPLS User Guide for Routing Devices" [Online] Available:

https://www.juniper.net/documentation/us/en/software/junos/vpn-l2/topics/concept/vpn-types.html

[14] Cisco, "Implementing Tunnels" [Online] Available: https://www.cisco.com/c/en/us/td/docs/ios/12_4/interface/configuration/guide/inb_tun.html

[15] N. Kocharians, P. Palúch, "CCIE Routing and Switching v5.0 Official Cert Guide, Volume 1" 2015

[16] N. Kocharians, T. Vinson, "CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2" 2015

[17] Y. Rekhter, E.C. Rosen, "BGP/MPLS IP Virtual Private Networks (VPNs) RFC 4364" [Online] Available: https://datatracker.ietf.org/doc/rfc4364/

[18] Juniper Networks, “MPLS Overview” [Online] Available: https://www.juniper.net/documentation/us/en/software/junos/mpls/topics/topic-map/mpls-overview.html

[19] Juniper Networks, “IPv4 Traffic Over Layer 3 VPNs” [Online] Available: https://www.juniper.net/documentation/us/en/software/junos/vpn-l3/topics/topic-map/l3-vpns-ipv4-traffic.html

[20] Juniper Networks, “LDP Overview” [Online] Available: https://www.juniper.net/documentation/us/en/software/junos/mpls/topics/topic-map/ldp-overview.html

[21] I. Pepelnjak, J. Guichard, “MPLS and VPN Architectures, CCIP Edition” 2002

[22] J. Guichard, I. Pepelnjak, J. Apcar, “MPLS and VPN Architectures, Volume II” 2003

[23] Cisco Press, “Advanced MPLS Design and Implementation” 2002

[24] Cisco Systems, Inc., “Implementing Cisco MPLS Student Guide” 2003

[25] M. Morrow, A. Sayeed, “MPLS and Next-Generation Networks: Foundation for NGN and Enterprise Virtualization” 2006

Anexa 1

CE1-A

configure terminal

hostname CE1-A

interface Gi0/7

ip address 10.0.1.1 255.255.255.252

no shutdown

interface loopback 0

ip address 1.1.1.1 255.255.255.255

router bgp 1

neighbor 10.0.1.2 remote-as 1234

redistribute connected

CE3-A

configure terminal

hostname CE3-A

interface Gi0/5

ip address 10.0.2.1 255.255.255.252

no shutdown

interface loopback 0

ip address 2.2.2.2 255.255.255.255

router eigrp 2

network 2.2.2.2 0.0.0.0

network 10.0.2.0 0.0.0.3

CE1-B

configure terminal

hostname CE1-B

interface Gi0/7

ip address 10.0.3.1 255.255.255.252

no shutdown

interface loopback 0

ip address 3.3.3.3 255.255.255.255

router bgp 3

neighbor 10.0.3.2 remote-as 1234

redistribute connected

CE3-B

configure terminal

hostname CE3-B

interface Gi0/5

ip address 10.0.4.1 255.255.255.252

no shutdown

interface loopback 0

ip address 4.4.4.4 255.255.255.255

router eigrp 4

network 4.4.4.4 0.0.0.0

network 10.0.4.0 0.0.0.3

CE2-A

configure terminal

interface Gi0/1

ip address 172.16.0.2 255.255.255.248

no shutdown

CE4-A

configure terminal

interface Gi0/2

ip address 192.168.1.2 255.255.255.0

no shutdown

CE2-B

configure terminal

interface Gi0/1

ip address 172.16.0.3 255.255.255.248

no shutdown

CE4-B

configure terminal

interface Gi0/2

ip address 192.168.1.5 255.255.255.0

no shutdown

P1

configure terminal

interface Gi0/0

ip address 100.0.1.2 255.255.255.252

no shutdown

interface Gi0/1

ip address 100.0.3.1 255.255.255.252

no shutdown

interface Gi0/7

```
ip address 100.0.13.2 255.255.255.252
no shutdown
interface Gi0/6
ip address 100.0.4.1 255.255.255.252
no shutdown
interface Gi0/2
ip address 100.0.5.1 255.255.255.252
no shutdown
interface loopback 0
ip address 8.8.8.8 255.255.255.255
router ospf 1
router-id 8.8.8.8
network 100.0.1.0 0.0.0.3 area 0
network 100.0.3.0 0.0.0.3 area 0
network 100.0.13.0 0.0.0.3 area 0
network 100.0.4.0 0.0.0.3 area 0
network 100.0.5.0 0.0.0.3 area 0
network 8.8.8.8 0.0.0.0 area 0
end
mpls label range 200 299
mpls ip
interface range Gi0/0 - 2
mpls ip
interface range Gi0/6 - 7
mpls ip
```

P2

```
configure terminal
interface Gi0/0
ip address 100.0.11.2 255.255.255.252
no shutdown
interface Gi0/1
ip address 100.0.2.2 255.255.255.252
no shutdown
interface Gi0/3
ip address 100.0.7.1 255.255.255.252
no shutdown
interface Gi0/6
ip address 100.0.6.1 255.255.255.252
no shutdown
interface Gi0/2
ip address 100.0.5.2 255.255.255.252
no shutdown
interface loopback 0
ip address 10.10.10.10 255.255.255.255
router ospf 1
router-id 10.10.10.10
network 100.0.11.0 0.0.0.3 area 0
network 100.0.2.0 0.0.0.3 area 0
network 100.0.6.0 0.0.0.3 area 0
network 100.0.7.0 0.0.0.3 area 0
network 100.0.5.0 0.0.0.3 area 0
network 10.10.10.10 0.0.0.0 area 0
end
mpls label range 300 399
```

mpls ip

interface range Gi0/0 - 3

mpls ip

interface Gi0/6

mpls ip

P3

configure terminal

interface Gi0/0

ip address 100.0.9.2 255.255.255.252

no shutdown

interface Gi0/1

ip address 100.0.3.2 255.255.255.252

no shutdown

interface Gi0/5

ip address 100.0.14.1 255.255.255.252

no shutdown

interface Gi0/6

ip address 100.0.6.2 255.255.255.252

no shutdown

interface Gi0/2

ip address 100.0.8.1 255.255.255.252

no shutdown

interface loopback 0

ip address 9.9.9.9 255.255.255.255

router ospf 1

router-id 9.9.9.9

network 100.0.14.0 0.0.0.3 area 0

network 100.0.3.0 0.0.0.3 area 0

network 100.0.9.0 0.0.0.3 area 0

network 100.0.8.0 0.0.0.3 area 0

network 100.0.6.0 0.0.0.3 area 0

network 9.9.9.9 0.0.0.0 area 0

end

mpls label range 400 499

mpls ip

interface range Gi0/0 - 2

mpls ip

interface range Gi0/5 - 6

mpls ip

P4

configure terminal

interface Gi0/7

ip address 100.0.12.2 255.255.255.252

no shutdown

interface Gi0/1

ip address 100.0.10.2 255.255.255.252

no shutdown

interface Gi0/3

ip address 100.0.7.2 255.255.255.252

no shutdown

interface Gi0/6

ip address 100.0.4.2 255.255.255.252

no shutdown

interface Gi0/2

ip address 100.0.8.2 255.255.255.252

no shutdown

interface loopback 0

ip address 11.11.11.11 255.255.255.255

router ospf 1

router-id 11.11.11.11

network 100.0.12.0 0.0.0.3 area 0

network 100.0.10.0 0.0.0.3 area 0

network 100.0.4.0 0.0.0.3 area 0

network 100.0.7.0 0.0.0.3 area 0

network 100.0.8.0 0.0.0.3 area 0

network 11.11.11.11 0.0.0.0 area 0

end

mpls label range 500 599

mpls ip

interface range Gi0/1 - 3

mpls ip

interface range Gi0/6 - 7

mpls ip

PE1

configure terminal

interface Gi0/0

ip address 100.0.1.1 255.255.255.252

no shutdown

interface Gi0/1

ip address 100.0.2.1 255.255.255.252

no shutdown

```
interface Gi0/7
ip address 10.0.1.2 255.255.255.252
no shutdown
interface loopback 0
ip address 5.5.5.5 255.255.255.255
router ospf 1
router-id 5.5.5.5
network 100.0.1.0 0.0.0.3 area 0
network 100.0.2.0 0.0.0.3 area 0
network 5.5.5.5 0.0.0.0 area 0
end
mpls label range 100 199
mpls ip
interface Gi0/0
mpls ip
interface Gi0/1
mpls ip
router bgp 1234
neighbor 7.7.7.7 remote-as 1234
neighbor 7.7.7.7 update-source loopback 0
address-family vpnv4
neighbor 7.7.7.7 activate
end
vrf definition Customer1
rd 5.5.5.5:1
address-family ipv4
route-target export 5.5.5.5:1
route-target import 7.7.7.7:3
```

```
exit
vrf definition Customer3
rd 5.5.5.5:2
address-family ipv4
route-target export 5.5.5.5:2
route-target import 7.7.7.7:4
exit
interface Gi0/7
vrf forwarding L3VPN
ip address 10.0.1.2 255.255.255.252
no shutdown
exit
interface Gi0/5
vrf forwarding Customer3
ip address 10.0.2.2 255.255.255.252
no shutdown
exit
router bgp 1234
address-family ipv4 vrf Customer1
neighbor 10.0.1.1 remote-as 1
exit
address-family vpnv4
neighbor 7.7.7.7 next-hop-self
end
router eigrp 1
address-family ipv4 vrf Customer3 autonomous-system 2
network 10.0.2.0 remote-as 2
end
```

router bgp 1234

address-family ipv4 vrf Customer3

redistribute eigrp 2

exit

router eigrp 1

address-family ipv4 vrf Customer3 autonomous-system 2

redistribute bgp 1234 metric 1000000 1 255 1 1500

end

PE2

configure terminal

interface Gi0/0

ip address 100.0.11.1 255.255.255.252

no shutdown

interface Gi0/7

ip address 100.0.12.1 255.255.255.252

no shutdown

interface loopback 0

ip address 12.12.12.12 255.255.255.255

router ospf 1

router-id 12.12.12.12

network 100.0.11.0 0.0.0.3 area 0

network 100.0.12.0 0.0.0.3 area 0

network 12.12.12.12 0.0.0.0 area 0

end

mpls label range 700 799

mpls ip

interface Gi0/0

```
mpls ip
interface Gi0/7
mpls ip
pseudowire-class Customer2
encapsulation mpls
exit
pseudowire-class Customer4
encapsulation mpls
exit
interface Gi0/1
xconnect 13.13.13.13 200 pw-class Customer2
end
interface Gi0/2
xconnect 13.13.13.13 400 pw-class Customer4
```

PE3

```
configure terminal
interface Gi0/0
ip address 100.0.9.1 255.255.255.252
no shutdown
interface Gi0/1
ip address 100.0.10.1 255.255.255.252
no shutdown
interface Gi0/7
ip address 10.0.3.2 255.255.255.252
no shutdown

interface loopback 0
```

```
ip address 7.7.7.7 255.255.255.255
router ospf 1
router-id 7.7.7.7
network 100.0.9.0 0.0.0.3 area 0
network 100.0.10.0 0.0.0.3 area 0
network 7.7.7.7 0.0.0.0 area 0
end
mpls label range 600 699
mpls ip
interface Gi0/0
mpls ip
interface Gi0/1
mpls ip
router bgp 1234
neighbor 5.5.5.5 remote-as 1234
neighbor 5.5.5.5 update-source loopback 0
address-family vpnv4
neighbor 5.5.5.5 activate
end
vrf definition Customer1
rd 7.7.7.7:1
address-family ipv4
route-target export 7.7.7.7:3
route-target import 5.5.5.5:1
exit
vrf definition Customer3
rd 7.7.7.7:2
address-family ipv4
```

```
route-target export 7.7.7.7:4
route-target import 5.5.5.5:2
exit
interface Gi0/7
vrf forwarding Customer1
ip address 10.0.3.2 255.255.255.252
no shutdown
exit
interface Gi0/5
vrf forwarding Customer3
ip address 10.0.4.2 255.255.255.252
no shutdown
exit
router bgp 1234
address-family ipv4 vrf Customer1
neighbor 10.0.3.1 remote-as 3
exit
address-family vpnv4
neighbor 7.7.7.7 next-hop-self
end
router eigrp 1
address-family ipv4 vrf Customer3 autonomous-system 4
network 10.0.4.0 remote-as 2
end
router bgp 1234
address-family ipv4 vrf Customer3
redistribute eigrp 4
exit
```

router eigrp 1

address-family ipv4 vrf Customer3 autonomous-system 4

redistribute bgp 1234 metric 1000000 1 255 1 1500

end

PE4

configure terminal

interface Gi0/5

ip address 100.0.14.1 255.255.255.252

no shutdown

interface Gi0/7

ip address 100.0.13.1 255.255.255.252

no shutdown

interface loopback 0

ip address 13.13.13.13 255.255.255.255

router ospf 1

router-id 13.13.13.13

network 100.0.13.0 0.0.0.3 area 0

network 100.0.14.0 0.0.0.3 area 0

network 13.13.13.13 0.0.0.0 area 0

end

mpls label range 800 899

mpls ip

interface Gi0/5

mpls ip

interface Gi0/7

mpls ip

```
pseudowire-class Customer2
encapsulation mpls
exit
pseudowire-class Customer4
encapsulation mpls
exit
interface Gi0/1
xconnect 12.12.12.12 200 pw-class Customer2
end
interface Gi0/2
xconnect 12.12.12.12 400 pw-class Customer4
```