**TEMA**

**REȚELE DE CALCULATOARE**

**Virtual Private LAN Service**

**(VPLS)**

**Studenți:**

Bardă Alexandru Mihai - Grupa 443A

Diaconescu Oana Ramona - Grupa 441A

**Cuprins:**

**Barda Alexandru Mihai**

1.   Introducere ce include VLAN si VPS………….……….…………………………….2

2.   Arhitectura……………………………….…….…………………………………...…3

      a.    H-VPLS……………………………….….…………………………………….....3

      b.   Exemple de configuratie………….…………………………………………….....4

      c.    Caracteristici………………………………………………………………….…..5

**Diaconescu Oana Ramona**

3.   Modelul topologic pentru VPLS……………………………………………………....6

     a.    Flooding si Forwarding ……………………………………………………….…...7

     b.   Address Learning……………………………………………………………….…..7

     c.    Tunnel Topology……………………………………………………………….…..8

     d.   Loop free VPLS………………………………………………………………….…9

4.   Ierarhia VPLS Model folosind Ethernet Access Network………………………….….9

5. Bibliografie……………………………………………………………………………..10

1. **Introducere - Ce includ VLAN si VPS**

**VPS (Virtual private server)[1]**

Un calculator end-user include un procesor care ruleaza un sistem de operare. O multitudine de servere virtuale private (VPS) sunt sprijinite in cadrul sistemului de operare. O multitudine de aplicatii sunt disponibile pentru un utilizator al calculatorului end-user. Aplicatiile sunt lansate in diferite VPS-uri. Cel putin unul din VPS-uri are multiple aplicatii lansate in cadrul acestuia. Cel putin doua dintre aplicatii sunt lansate in diferite VPS-uri, si comunica una cu celalalta, folosind mijloace de comunicare sigure, cum ar fi firewall-uri,proxy, clipboard-uri dedicate, Named Pipes, memorie partajata, de comunicatii inter-proces dedicate, apelurile de proceduri locale / Remote Procedure Calls, API, prize de retea, comunicatii TCP / IP, comunicatii de protocol de retea si fisiere mapate la memorie. VPS-urile pot fi create si incheiate dinamic. Mijloace de control VPS sunt la dispozitia utilizatorului si includ mijloace pentru crearea / terminarea a VPS-ului, un sistem de fisiere si registru de rezerva, informatii de control pentru backup / restore de date la nivel VPS, plasarea de reguli aplicatie / proces pentru crearea / sprijinirea corespunzatoare a VPS-ului, granulare de izolare pentru VPS / aplicatii / procese, controlul resurselor computerului, definirea operatiunilor admise pentru inter-VPS de comunicare, mijloace de definire a operatiunilor permise pentru comunicatii inter-proces.



**VLAN (Virtual Local Area Network)[2]**

Un sistem de control VLAN este prevazut cu: un server de acces de la distanta, conectat la o retea de domiciliu in VLAN cu o retea globala, pentru controlul comunicarii intre orice terminal mutat si reteaua de domiciliu, cu referire la un tabel de management ce indica locatia fiecarui terminal din conexiune; un client acces de la distanta, conectat la fiecare retea de la distanta, pentru controlul comunicarii intre reteaua de la distanta si reteaua globala, cu referire la un tabel de management ce indica o relatie de corespondenta intre fiecare terminal care este conectat la reteaua de la distanta si reteaua de domiciliu; si un server de gestionare a VLAN, conectat la reteaua globala, pentru gestionarea transmiterii de pachete, locatia fiecarui terminal cu referire la un tabel de management ce indica o relatie de corespondenta intre fiecare terminal si serverul de acces de la distanta si o locatie a fiecarui terminal din conexiune. In sistemul de control, deconectarea unui terminal care a fost mutat intr-o retea de la distanta este detectata, fara vreo functie speciala la partea terminala, bazat pe informatia de sincronizare a unui pachet transmis din informatiile terminalului sau conexiunii daca terminalul este mutat mai departe intr-o alta retea de la distanta. De asemenea, este asigurata o metoda de control a VLAN corespunzatoare sistemului de mai sus.

Figura 1 - VLAN

1. **Arhitectura**
2. **H-VPLS – Hierachical Virtual Private LAN Service[3]**

VPLS necesita un full mesh atat in planurile de control, cat si in cele de date; dar aceasta poate fi dificil de scalat.

Pentru BGP, problema scalarii planului de control a fost mult timp abordata prin utilizarea reflectoarelor de traseu (route reflectors - RR). RR-urile sunt utilizate pe scara larga in contextul rutarii de internet precum si pentru mai multe tipuri de VPN (Virtual Private Network).

Pentru a scala planul de date pentru multicast si traficul broadcast, se studiaza implementarea utilizarii LPS-urilor unul-la-mai multi ca metoda de baza pentru transport.

Pentru LDP, s-a dezvoltat o metoda pentru a diviza un VLPS VPN in retele ierarhice de doua sau trei niveluri.

Asa numitele VPLS-uri ierarhice (H-VPLS), introduc un nou tip de dispozitiv MPLS: *multi-tenant unit* ***(MTU)*** *switch.*

Acest dispozitiv reuneste mai multi clienti intr-un singur PE, care are nevoie de o singura conexiune la planul control si de date in retea. Aceasta poate reduce semnificativ numarul de sesiuni LDP si de LPS-uri, si astfel elibereaza reteaua principala , concentrand utilizatorii pe dispozitivele marginale.

1. **Exemple de configuratie**

****

Figura 2 – Configuratie VPLS PE -> PE



Figura 3 – Configuratie VPLS PE -> CE

1. **Caracteristici: [4]**

**Flat VPLS**

***Caracteristici generale:***

* Recomandata pentru implementarile clientilor mici
* Provizionare (asigurare a accesului) simpla
* Full mesh de sesiuni LDP directionate necesare intre PE-urile participante

Figura 4 – Flat VPLS

* Nivel de support pentru VLAN si Port (fara QinQ)

***Dezavantaje:***

* Fara scalabilitate ierarhica
* Probleme de scalare: replicarea pachetelor PE full mesh cauzeaza clasica problema N\*(N-1)/2

****

**H-VPLS**

**Avantaje:**

* Recomandate pentru implementari la scala larga

Figura 5 – H-VPLS

* Reduce replicarea pachetelor si semnalizarea peste PE-uri
* Foloseste full mesh numai pentru nivelul nucleu (Hub)
* VC-uri de atasament „Virtual Switch Ports” afectate prin mecanisme de tunelare de Layer 2 (AToM, L2TPv3, QinQ)
* Expansiunea influenteaza numai noile noduri (fara reconfigurarea PE-urilor existente)

**Dezavantaje:**

* Asigurarea accesului este mult mai complicata
* MPLS Edge H-VPLS necesita:
* Design de retea complex
* Suport operational complex
* Echipament scump

**3. Modelul topologic pentru VPLS[3]**

O interfata participanta intr-un VPLS trebuie sa fie capabila sa flood-eze, forward-eze si sa filtreze frame-urile de Ethernet. Figura de mai jos reprezinta modelul topologic al unui VPLS. Setul de dispozitive PE interconectate prin PW apare pentru clientul X ca un singur LAN emulat. Fiecare PE va forma o adresa MAC la distanta pentru asocierile PW si asociaza direct adresele MAC atasate porturilor clientului local. Aceasta este modelata conform standardului IEEE802.1 MAC Adress Learning.



Figura 6 – Model Topologic VPLS

1. **Flooding si Forwarding**

Unul dintre atributele unui serviciu Ethernet este ca frame-urile trimiste catre adrese broadcast si adrese MAC necunoscute sunt flood-ate la toate porturile. Pentru a obtine flood-area in reteaua ce ofera serviciul, toate frame-urile unicast, broadcast si multicast necunoscute sunt flood-ate pe PW-urile corespunzatoare catre toate nodurile PE ce participa in VPLS, si deasemenea catre toate AC-urile.

Este de notat ca frame-urile multicast sunt un caz special si nu este necesar sa fie transmise catre toti mambrii VPN-ului. Pentru simplitate, este folosita abordarea standard a broadcast-ingului frame-urilor multicast.

Pentru a transmite un frame , PE trebuie sa poata asocia adresa MAC de destinatie cu un PW. Este nejustificat si probabil imposibil sa se ceara ca PE-urile sa configureze o asociere intre fiecare adresa MAC de destinatie posibila cu un PW. Asadar, PE-urile VPLS-capabile ar trebui sa aiba capabilitatea de a invata dinamic adrese MAC atat pe AC-uri cat si pe PW-uri si sa transmita si sa replice pachete ata peste AC-uri cat si peste PW-uri.

1. **Address Learning**

Spre deosebire de VPN-urile BGP, accesul la informatie nu este anuntat si distribuit via planului de control. Accesul este obtinut prin functii standard bridge de invatare in planul de date.

Cand un pachet ajunge pe un PW, daca adresa MAC sursa nu este cunoscuta, trebuie sa fie asociata cu PW-ul, astfel incat pachetele outbound catre acea adresa MAC sa poata fi livrate prin PW-ul asociat. Analog, cand un pachet ajunge printr-un AC, daca adresa MAC sursa nu este cunoscuta, trebuie sa fie asociata AC-ului, astfel incat pachetele outbound trimise care acea adresa MAC sa poata fi livrate prin intermediul AC-ului asociat.

1. **Tunnel Topology**

Routerele PE se presupun ca avand capabilitatea de a stabili tunele de transport.

Tunelele sunt stabilite intre PE-uri pentru a concentra traficul. PW-urile sunt semnalizate frame-urilor de Ethernet encapsulate in demultiplexoare de catre multiple instante ale VPLS care traverseaza tunelele de transport.

 Intr-un Ethernet L2VPN, crearea unei topoligii loop-free devine responsabilitatea distribuitorului. De dragul simplitatii, putem spune ca topologia unui VPLS este un full mesh de PW-uri.



Figura 7 – Tunnel Topology (Non-Distributed PE)



Figura 8 – Tunnel Topology (Distributed PE)

1. **Loop Free VPLS**

Daca topologia VPLS-ului nu este restrictionata la un full mesh, atunci este posibil ca doua PE-uri sa nu fie conectate in mod direct prin PW-uri si ar fi nevoie sa foloseasca un PE intermediar pentru a schimba pachete. Aceasta topologie ar cere sa se foloseasca un protocol loop-breaking, ca un protocol spanning-tree.

In schimb, un full mesh este stabilit intre PE-uri. Din moment ce fiecare PE este conectat direct la toate celelalte PE-uri din VPLS prin PW, nu mai este nevoie sa se schimbe pachete, si putem instantia o regula simpla de intrerupere a buclelor: regula „split horizon”, in care un PE nu trebuie sa transmita trafic dintr-un PW prin celalalt in acelasi mesh VPLS.

**4. Ierarhia VPLS Model folosind Ethernet Access Network[3]**

In aceasta sectiune, modelul ierarhic este extins astfel incat sa includa o Ethernet Access Network. Acest model retine arhitectura ierarhica care sustine topologia full mesh intre dispozitivele PE; cu toate astea, nu este impusa nicio restrictie pentru topologia Ethernet Access Network.

Motivul pentru care se foloseste Ethernet Access Network este acela ca retelele bazate pe Ethernet sunt implementate in prezent de furnizorii de servicii pentru a oferi clientilor lor servicii VPLS. Asadar, este important sa fie oferit un mecanism care sa permita acestor retele sa se integreze cu un IP sau un nucleu MPLS pentru a oferi servicii VPLS scalabile.

O abordare pentru a tunela traficul Ethernet al unui client prin intermediul unei Ethernet Access Network este de a adauga o eticheta VLAN suplimentara la datele clientului. Eticheta suplimentara este denumita ca Provider’s VLAN (P-VLAN). In interiorul retelei furnizorului, fiecare P-VLAN desemneaza un client sau mai concret, o instanta VPLS pentru acel client.

Daca VLAN-urile clientului trebuie tratate ca delimitatoare de servicii, atunci MTU trebuie sa aiba capacitatea suplimentara de a traduce VLAN-ul unui client (C-VLAN) intr-un P-VLAN, sau sa mai adauge o eticheta P-VLAN aditionala pentru a rezolva suprapunerea etichetelor VLAN folosite de diferiti clienti.

**Bibliografie:**

[1] https://www.google.com/patents/US6075776

[2] <https://www.google.com/patents/US6111876>

[3] <http://www.rfc-editor.org/rfc/rfc4762.txt>

[4]<http://flylib.com/books/en/2.686.1.86/1/>

Figurile 1, 7, 8 - <https://www.google.ro/imgres?imgurl=http://alliedtelesis.com/manuals/AWPLUSV224CLIa1/Images/2252_Port-based_VLAN_Example_2.png&imgrefurl=http://alliedtelesis.com/manuals/AWPLUSV224CLIa1/port_based_VLANs_overview.html&h=1148&w=1208&tbnid=_DRLDnPzAQjEwM:&tbnh=160&tbnw=168&docid=663jHB4K60D8-M&itg=1&client=opera&usg=__EgnRBR_mbKOnYdEMjjrqAjhNSmo=&sa=X&ved=0ahUKEwja1tLosLTKAhXGvhQKHewZDaYQ9QEIJDAA>

Figurile 2,3, 4,5 - <https://www.cisco.com/application/pdf/en/us/guest/tech/tk891/c1482/ccmigration_09186a00801ed3ea.pdf>

Figura 6 - <https://www.rfc-editor.org/rfc/pdfrfc/rfc4762.txt.pdf>