



## فرم تعریف پروژه فارغ التحصیلی دوره کارشناسی

تاریخ: .....

شماره: .....

عنوان پروژه: پیاده سازی VPLS در شبکه های نرم افزار بنیان	
امضاء:	استاد راهنمای پروژه: دکتر سیاوش خرسندی
مشخصات دانشجو:	
نام و نام خانوادگی: الهه جلال پور <sup>۱</sup>	گرایش: سخت افزار
شماره دانشجویی: ۹۱۳۱۰۳۶	ترم ثبت نام پروژه: اول ۹۴-۹۵
داوران پروژه:	
۱-	امضاء داور:
۲-	امضاء داور:
شرح پروژه (در صورت مشترک بودن بخشی از کار که بعهدہ دانشجو می باشد مشخص شود):	
هدف این پروژه پیاده سازی سرویس VPLS تحت شبکه های نرم افزار بنیان است. این سرویس تعدادی از مشکلات سرویس های VPLS سابق اعم از پیچیدگی و زمان بری کار با رابط های کاربری گوناگون موجود در شبکه های سنتی را به صورت چشمگیری بهبود می بخشد. در این پیاده سازی از کنترلر ONOS استفاده کرده و سرویس VPLS روی آن پیاده سازی شده و به این کنترلر اضافه می شود. شرح کامل پروژه به پیوست آمده است.	
وسائل مورد نیاز:	
- امکان دسترسی به مقالات مرتبط	
- یک دستگاه کامپیوتر دارای دسترسی به اینترنت	
محل انجام پروژه: دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر تاریخ شروع: آذر ۱۳۹۴	

این قسمت توسط دانشکده تکمیل می گردد:

تاریخ تصویب در گروه:	اسم و امضاء:
تاریخ تصویب در دانشکده:	اسم و امضاء:
اصلاحات لازم در تعریف پروژه:	

توجه: پروژه حداکثر یک ماه و نیم پس از شروع ترمی که در آن در درس پروژه ثبت نام به عمل آمده است باید به تصویب برسد.

نسخه ۱- دانشکده	نسخه ۲- استاد راهنما	نسخه ۳- دانشجو
-----------------	----------------------	----------------

## تعریف مسئله:

راه‌گزینی برچسب چندپروتکلی<sup>۴</sup> یا به اختصار MPLS، یک فناوری در شبکه‌های فراهم‌کننده سرویس سطح حمل<sup>۳</sup> است که از ترکیب راه‌گزینی<sup>۴</sup> و مسیریابی<sup>۵</sup> به وجود آمده و گستره کاری مسیریابی لایه شبکه را در کنار سرعت و سادگی راه‌گزینی لایه پیوند داده فراهم می‌آورد. در شبکه‌های IP/MPLS، سرآیندی مربوط به MPLS به بسته‌ها افزوده می‌شود. هر برچسب می‌تواند روی برچسب قبلی قرار بگیرد و به این ترتیب برچسب‌ها می‌توانند یک پشته را ایجاد کنند.

در شبکه‌های MPLS هر برچسب نماینده یک مسیر از پیش تعیین‌شده است. بنابراین، عمل تعیین مسیر یک‌بار در ورودی شبکه انجام می‌گیرد و در هسته شبکه مسیریاب‌های برچسب راه‌گزین<sup>۶</sup> یا به اختصار LSRها بسته‌های برچسب خورده را بدون نیاز به مسیریابی راه‌گزینی می‌کنند. از آنجایی که قسمت بزرگی از هسته‌ی شبکه‌های حامل را IP/MPLS تشکیل می‌دهد و سرویس‌های شبکه خصوصی مجازی<sup>۷</sup> یا به اختصار VPN، در زمره مهمترین سرویس‌های سرویس دهنده‌های سطح حمل قرار دارند، این سرویس‌ها نیز بر اساس MPLS محقق می‌شوند. استفاده از MPLS برای فراهم آوردن سرویس VPN باعث سادگی پیاده‌سازی و گسترش پذیری<sup>۸</sup> بیشتر آن‌ها می‌گردد. سرویس VPN بر روی MPLS را می‌توان به صورت زیر دسته‌بندی کرد:

- MPLS-based Layer 2 VPNs
- MPLS-based Layer 3 VPNs

به طور کلی معماری‌های مختلفی برای ارائه سرویس VPN در لایه‌های مختلف وجود دارد ولی در اینجا تمرکز بر روی دو معماری VPLS، به عنوان یک VPN لایه ۲ که به صورت چند به چند<sup>۹</sup> عمل می‌کند و MPLS BGP VPN، به عنوان یک VPN لایه ۳ می‌باشد.

پیش از معرفی این دو معماری به معرفی چند اصطلاح در این حوزه می‌پردازیم:

لبه سرویس دهنده<sup>۱۰</sup> یا به اختصار PE: گره‌ای سمت سرویس دهنده که ارتباط با سایت‌های کاربر را فراهم می‌آورد. در عمل عموماً این گره‌ها LSRها هستند.

لبه سرویس دهنده<sup>۱۱</sup> یا به اختصار CE: گره‌ای سمت سایت کاربر که ارتباط با سرویس دهنده را فراهم می‌آورد. در عمل عموماً این گره‌ها Routerها هستند.

در معماری MPLS BGP VPN نیاز به وجود جدول مسیریابی سایت‌های کاربر در هر یک از PEها است؛ برای این منظور هر CE این جدول را به PE متناظرش از طریق پروتکل دروازه‌ای مرزی خارجی<sup>۱۲</sup> یا به اختصار E-BGP، اطلاع داده و PEها نیز این جداول را از طریق پروتکل دروازه‌ای مرزی داخلی<sup>۱۳</sup> یا به اختصار I-BGP، با یکدیگر به اشتراک می‌گذارند و سپس در صورت لزوم مسیری را برای ارتباط بین خودشان در نظر می‌گیرند. در این معماری از پروتکل توزیع برچسب<sup>۱۴</sup> یا به اختصار LDP، برای توزیع برچسب‌های مسیریابی بین PEها استفاده می‌شود. LDP به این منظور از اطلاعات پروتکل‌های مسیریابی IGP که در شبکه هسته اجرا می‌شوند، استفاده می‌کند. در صورت تقاضای مشتری به مسیریابی مسیر ثابت<sup>۱۵</sup>؛ مدیر شبکه سرویس دهنده باید این تنظیمات را روی LSRها به صورت دستی اعمال کند.

در معماری VPLS، هر PE یک جدول مک داشته و آدرس‌های مک سیستم‌های مشتری را ذخیره می‌کند. در صورتی که مقصد بسته ورودی مشخص باشد، بسته به مقصد خود ارسال می‌گردد و در غیر این صورت به همه‌ی پورت‌های کاربر در PEها ارسال می‌گردد. ایجاد یک شبکه

<sup>۴</sup>Multiprotocol Label Switching

<sup>۵</sup>Carrier-grade service providers

<sup>۶</sup>Switching

<sup>۷</sup>Routing

<sup>۸</sup>Label Switch Router

<sup>۹</sup>Virtual Private Network

<sup>۱۰</sup>Scalability

<sup>۱۱</sup>Multipoint to multipoint

<sup>۱۲</sup>Provider Edge

<sup>۱۳</sup>Customer Edge

<sup>۱۴</sup>Exterior Border Gateway Protocol

<sup>۱۵</sup>Interior Border Gateway Protocol

<sup>۱۶</sup>Label Distribution Protocol

<sup>۱۷</sup>Static Route

تمام مش بین PE ها در ابتدای پیکر بندی شبکه این امکان این ارسال را فراهم می آورد. در این مدل هر PE به صورت مستقل جدول مک<sup>۱۶</sup> خود را آپدیت می کند. در این معماری همانند معماری پیشین، از LDP و پروتکل های مسیریابی IGP برای توزیع برچسب ها استفاده می شود.

## راه حل های فعلی و مشکلات آن ها:

امروزه در شبکه های حامل برای فراهم آوردن سرویس VPN بر روی بستر MPLS از دو معماری VPLS و MPLS BGP VPN که پیشتر گفته شد، استفاده می شود. مشکل اصلی این معماری ها مدیریت پیچیده آن ها است که مدیر شبکه را ملزم به تنظیم دستی تنظیمات دستگاه ها و کار با روابط کاربری مختلف آن ها را به هنگام ایجاد هر گونه تغییر در تعداد سایت های مشتریان می کند. از دیگر مشکلات معماری کنونی پیچیدگی مدیریت مشتری بر روی ترافیک داده خود می باشد. در این معماری لازم است که کاربر برای اعمال سیاست روی ترافیک ارسال خود به سرویس دهنده تقاضا داده و نمی تواند سیاست های ترافیک ارسال خود بین سایت هایش را مستقل از سرویس دهنده مدیریت کند.

## راه حل پیشنهادی:

در معماری SDVPN، CE ها با سویچ های OpenFlow که قابلیت کنترل متمرکز از طریق یک کنترلر و پروتکل OpenFlow را دارند، جایگزین شده اند. به این ترتیب سطح کنترل از سطح داده جدا شده و به صورت متمرکز در می آید. در این معماری همانند معماری سنتی برای توزیع برچسب ها از پروتکل LDP که مبتنی بر یک پروتکل مسیریابی IGP عمل می کند، استفاده می شود. SDVPN از دو برچسب برای ارسال هر بسته استفاده می کند که یکی از آنها برای مسیریابی در هسته بوده و دیگری برای مشخص کردن نوع سرویسی که قرار است برای آن بسته ارائه شود، اعمال می شود.

همانگونه که پیشتر اشاره شد، در سیستم سنتی VPN های مبتنی بر MPLS، با ایجاد هرگونه تغییر در تعداد سایت های کاربران نیاز به پیکربندی هر کدام از این تجهیزات به صورت جداگانه و با رابط کاربری مخصوص به آن تجهیز بود. در SDVPN تمامی این تغییرات به صورت متمرکز اعمال می شوند.

مساله دیگر پیش رو در این فناوری، عدم امکان اعمال سیاست توسط خود مشتریان روی شبکه VPN بود. در SDVPN کاربر با در اختیار داشتن برنامه ای منحصر به فرد، قابلیت مدیریت ترافیک های شبکه را بدون نیاز به مراجعه به سرویس دهنده پیدا می کند.

## معماری SDVPN:

در این بخش معماری و پیاده سازی هر دو بخش صفحه کنترل<sup>۱۷</sup> صفحه داده<sup>۱۸</sup> به صورت جداگانه تشریح می شوند.

### بخش ۱ معماری صفحه کنترل

این بخش از ماژول هایی تشکیل می شود که وظیفه اصلی آنها به روز رسانی جداول جریان موجود در PE ها است. این ماژول ها عبارتند از: (۱) سویچ مجازی:

در این ماژول شبکه هسته به صورت یک سویچ شبیه سازی می شود که PE ها هر کدام متناظر با یک اینترفیس این سویچ هستند. جدول آدرس های مک که مشخص کننده ی هر آدرس مک و درگاه خروج برای آن و همچنین جدولی که تناظر VLAN ها و اینترفیس ها را مشخص می کند، در این ماژول پیاده سازی می شوند.

(۲) اعمال سیاست :

گاهی نیاز به اعمال سیاست برای جلوگیری از رسیدن بسته هایی از یک سایت مشخص مشتری به سایت دیگری از آن خواهد شد. امکان اعمال اینگونه دستورات توسط این ماژول به کاربر استفاده کننده از VPN داده می شود.

### بخش ۲ معماری صفحه داده

در معماری صفحه داده SDVPN دو ویژگی اصلی وجود دارد:

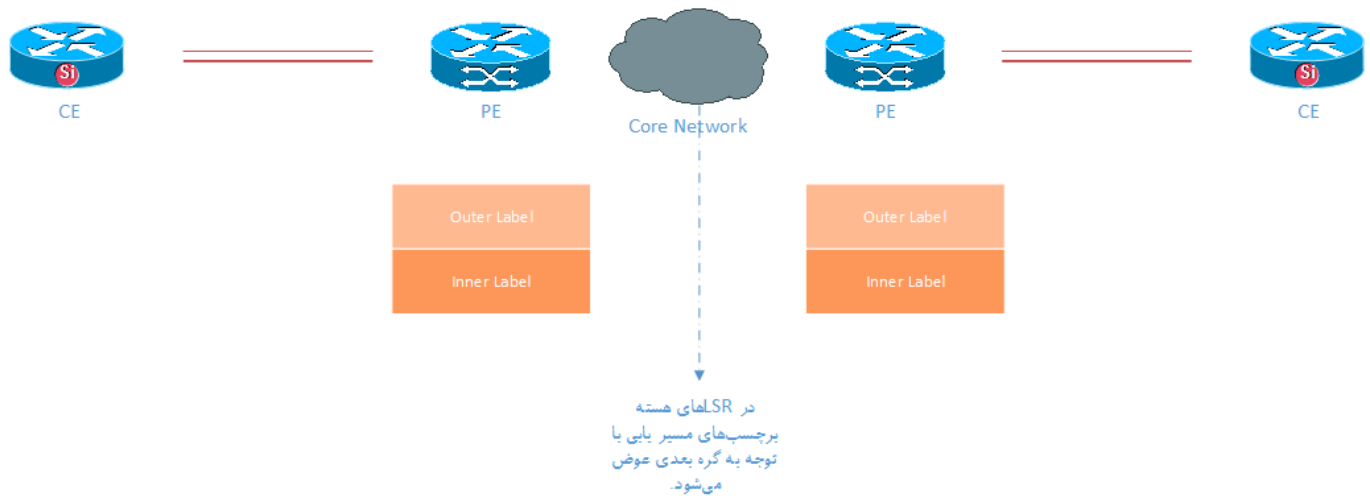
<sup>۱۶</sup>Mac table

<sup>۱۷</sup>Control plane

<sup>۱۸</sup>Data plane

۱. برای هر یک از مشتری‌ها یک جدول جداگانه در نظر گرفته می‌شود که این امر ضمن مدیریت راحت‌تر جلوی بروز اشکال در صورت محدودیت اندازه‌ی جدول جریان را می‌گیرد.

۲. روش انتساب برچسب‌های MPLS کاملاً مشابه با معماری سنتی می‌باشد، به این ترتیب که یک برچسب برای مشخص کردن سرویس مورد نیاز بسته و دیگری مشخص کننده مقصد بسته است که از آن برای مسیریابی بسته در هسته استفاده می‌شود. شکل زیر شمایی کلی از پروسه را نشان می‌دهد. سرویس مورد نیاز هر بسته در این پروژه همان VLAN مربوط به کاربر است که باعث محدود کردن فضای Broadcast و مدیریت بهینه تر در طرف دیگر شبکه‌ها در PE طرف دیگر می‌شود.



## پیاده سازی:

اجزای پیاده‌سازی این پروژه از قرار زیر می‌باشند:

۱: کنترلر ONOS<sup>۱</sup>: این پلتفرم یک کنترلر برای معماری SDN است که قابلیت گسترش پذیری در سطح بالا و کارایی بهینه را به کاربران می‌دهد. در این پروژه، نرم افزار SDVPN با استفاده از رابط برنامه نویسی نرم‌افزار یا به اختصار API<sup>۲</sup> مربوط به ONOS نوشته و در نهایت روی بستر آن اجرا خواهد شد.

۲: Mininet: ابزاری برای شبیه سازی شبکه‌های نرم افزار بنیان است که در آن سوئیچ‌ها و میزبان‌ها شبیه سازی می‌شوند. در این پروژه کنترلر ONOS به عنوان کنترلر این شبکه شبیه سازی شده عمل می‌کند.

لازم به ذکر است که در صورت فراهم بودن امکانات لازم، امکان قرار دادن این کنترلر و اجرای نرم‌افزار SDVPN بر روی بستر فیزیکی شبکه نیز وجود دارد که در این صورت نیازی به Mininet نخواهد بود. برای پیاده سازی این پروژه به ترتیب مراحل زیر را انجام می‌دهیم:

- مرحله اول:

در این مرحله برنامه ای روی بستر ONOS نوشته و پیاده سازی می شود که مدیریت اتصال و قطع CEها را انجام داده و تناظر بین PEها و CEها را مدیریت می‌کند.

- مرحله دوم:

در این مرحله جدول مک پیدا سازی می‌شود: در این جدول، آدرس‌های مک مربوط به PEهای مختلف و درگاه خروجی برای آن‌ها نوشته می‌شود. برای این کار از یکی از پروتکل‌های یادگیری آدرس مک استفاده می‌شود.

- مرحله سوم:

هدف در این مرحله برآورده ساختن قصدها<sup>۳</sup> با استفاده از بستر ONOS است. در این قسمت ماژول مربوط به ایجاد یک مسیر بین هر دو PE نوشته می‌شود. پس از پایان این مرحله، امکان ایجاد سرویس VPLS برای هر توپولوژی از PEها و CEها وجود دارد.

- مرحله چهارم:

<sup>۱</sup>Open Network Operating System

<sup>۲</sup>Application Programming Interface

<sup>۳</sup>Intents

در این مرحله یک GUI پیاده‌سازی می‌شود. تنظیمات ایستای موجود روی سوئیچ‌ها به صورت دینامیک و از طریق رابط کاربری توسط کاربران قابل تنظیم می‌باشد.

• مرحله پنجم:

در این مرحله سعی در پیاده‌سازی برنامه‌ی نوشته شده روی بستر ONOS به صورت توزیع شده است. این ویژگی امکان پراکندگی بستر شبکه را در سطح جغرافیایی گسترده ایجاد می‌کند.