



دانشکده مهندسی کامپیوتر  
و فناوری اطلاعات

باسمه تعالی

## فرم تعریف پروژه فارغ التحصیلی دوره کارشناسی



دانشگاه صنعتی امیرکبیر  
(پلی تکنیک تهران)

تاریخ: .....

شماره: .....

عنوان پروژه:	
امضاء:	استاد راهنمای پروژه: دکتر سیاوش خرسندی
مشخصات دانشجو:	
نام و نام خانوادگی: الهه جلال پور <sup>۱</sup> شماره دانشجویی: ۹۱۳۱۰۳۶	گرایش: سخت افزار 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): 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: اردیبهشت 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:

MPLS یک فناوری در شبکه های سطح حمل<sup>۲</sup> است از ترکیب راه گزینی<sup>۳</sup> و مسیریابی<sup>۴</sup> بوجود آمده و گستره کاری مسیریابی لایه ۳ را در کنار سرعت و سادگی راه گزینی لایه ۲ فراهم می آورد. در شبکه های IP/MPLS، سرآیند اضافی کوچک shim، به بسته افزوده می شود. هر برچسب می تواند روی برجست قبلی قرار بگیرد و به این ترتیب برچسب ها می توانند یک پشته را ایجاد کنند. در شبکه های MPLS هر برچسب نماینده یک مسیر از پیش تعیین شده است. بنابراین، عمل تعیین مسیر یکبار در ورودی شبکه انجام می گیرد و درون شبکه LSRها بسته های برچسب خورده را بدون نیاز به مسیریابی سوئیچ می کنند. سرویس های VPN در زمره مهمترین سرویس های سرویس دهنده های سطح حمل قرار دارند. از آنجایی که قسمت بزرگی از هسته ی شبکه های حامل را IP/MPLS تشکیل می دهد، سرویس VPN نیز بر اساس MPLS محقق می شود. استفاده از MPLS برای فراهم آوردن سرویس VPN باعث سادگی پیاده سازی و گسترش پذیری گسترش می گردد. سرویس VPN بر روی MPLS را میتوان به صورت زیر دسته بندی کرد:

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

به طور کلی معماری های مختلفی برای ارائه سرویس VPN در لایه های مختلف وجود دارد ولی در اینجا تمرکز بر روی دو معماری VPLS، به عنوان یک VPN لایه ۲ که به صورت multipoint to multipoint عمل می کند و MPLS BGP VPN، به عنوان یک VPN لایه ۳ می باشد.

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

Provider Edge (PE): گره ای سمت سرویس دهنده که ارتباط با مشتری را فراهم می آورد. در این گره عموماً از LSR استفاده می شود. Customer Edge (CE): گره ای سمت مشتری که ارتباط با سرویس دهنده را فراهم می آورد. در این گره عموماً از Router استفاده می شود.

در معماری MPLS BGP VPN نیازه وجود جدول مسیر یابی مشتری در هر یک از PE ها است. برای این منظور هر CE این جدول را به PE متناظر از طریق E-BGP اطلاع داده و PE ها نیز این جداول را از طریق پروتکل I-BGP با یکدیگر به اشتراک می گذارند. در این معماری از LDP برای توزیع برچسب های مسیرهای PE ها استفاده می شود. LDP به این منظور از اطلاعات پروتکل های مسیریابی IGP که در شبکه هسته اجرا می شوند، استفاده می کند. در صورتی که مشتری بخواهد از static route استفاده کند میبایست این امر توسط مدیر شبکه service provider به صورت دستی تنظیم گردد.

در معماری VPLS، هر PE یک جدول MAC داشته و آدرس های MAC سیستم های مشتری را ذخیره می کند. در صورتی که مقصد بسته ورودی مشخص باشد، بسته به مقصد خود ارسال می گردد و در غیر این صورت به همه ی پورت های مشتری روی همه ی PE ها ارسال می گردد. در این مدل هر PE به صورت مستقل جدول MAC خود را آپدیت می کند. در این معماری بازهم از LDP و پروتکل های مسیریابی IGP برای توزیع برچسب ها استفاده می شود.

## راه حل های فعلی و مشکلات آنها:

امروزه در شبکه های حامل برای فراهم آوردن سرویس VPN بر روی بستر MPLS از همان دو معماری VPLS و MPLS BGP VPN استفاده می شود. مشکل اصلی در این معماری ها این هست که مدیریت در این معماری بسیار پیچیده است و مدیر شبکه برای هر تغییری در تعداد سایت های مشتریان باید به صورت دستی تنظیمات دستگاه ها را تغییر دهد که این امر مستلزم کار با روابط کاربری مختلف آنهاست که هر کدام متعلق به یک سازنده خاص می باشد. یکی دیگر از مشکلات معماری کنونی موضوع مدیریت مشتری بر روی ترافیک خود می باشد، در این معماری مشتری برای اعمال یک سیاست روی ترافیک ارسال خود باید به سرویس دهنده تقاضا دهد و نمیتواند سیاست های ترافیک ارسال خود بین سایت هایش را مستقل از سرویس دهنده مدیریت کند.

<sup>۲</sup> Carrier-grade service providers

<sup>۳</sup> Switching

<sup>۴</sup> Routing

<sup>۵</sup> Label Switch Router

<sup>۶</sup> Scalability

## راه حل پیشنهادی:

در معماری SDVPN، CEها با سویچهای OpenFlow که قابلیت کنترل مرکزی از طریق یک کنترلر و پروتکل OpenFlow را دارند جایگزین شده‌اند. به این ترتیب سطح کنترل از سطح داده جدا شده و به صورت متمرکز در می‌آید. در این معماری مانند معماری سنتی برای توزیع برچسب‌ها از پروتکل LDP استفاده می‌کنیم که مبتنی بر پروتکل مسیریابی IGP که در هسته اجرا می‌شود عمل می‌کند. SDVPN از دو برچسب برای هر بسته استفاده می‌کند، یکی از آنها برای مسیریابی در هسته هست و دیگری برای مشخص کردن نوع سرویس که قرار هست برای آن بسته ارائه شود.

همانگونه که پیشتر اشاره شد، در سیستم سنتی VPNهای مبتنی بر MPLS، با ایجاد هرگونه تغییر در تعداد سایت‌های 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 مرکزی اعمال می‌شود. مساله دیگر پیش رو در این فناوری، عدم امکان اعمال سیاست توسط خود مشتریان روی شبکه VPN بود که در SDVPN مشتری با در اختیار داشتن برنامه‌ای منحصر به فرد، این قابلیت را پیدا می‌کند که بدون نیاز به مراجعه به سرویس دهنده ترافیک‌های شبکه خود را مدیریت کند.

## معماری SDVPN:

در این بخش معماری و پیاده سازی هر دو بخش صفحه کنترل و صفحه داده به صورت جداگانه تشریح می‌شود.

### بخش ۱ معماری صفحه کنترل

این بخش از ماژول‌هایی تشکیل می‌شود که وظیفه اصلی آنها به روز رسانی جداول جریان موجود در PEها است. این ماژول‌ها عبارتند از: (۱) سویچ مجازی:

در این ماژول شبکه هسته به صورت یک سویچ شبیه سازی شده که PEها هر کدام متناظر با یک اینترفیس این سویچ هستند. جدول آدرس‌های MAC که مشخص کننده ی هر آدرس‌های mac و درگاه‌های متناظر آنها برای خروج هستند و همچنین جدولی که تناظر VLANها و اینترفیس‌ها را مشخص می‌کند، در این ماژول پیاده سازی می‌شود.

(۲) مسیریاب مجازی:

در این ماژول مشابه ماژول پیشین، شبکه هسته به صورت یک مسیریاب شبیه سازی شده که PEها هر کدام متناظر با یک درگاه این سویچ هستند. در این ماژول مکانیزم‌های مسیر یابی بین شبکه‌های متصل به هر یک از این درگاه‌ها پیاده سازی خواهد شد.

(۳) اعمال سیاست :

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

### بخش ۲ معماری صفحه داده

در معماری صفحه داده SDVPN دو ویژگی اصلی وجود دارد:

۱. برای هر یک از مشتری‌ها یک جدول جداگانه در نظر گرفته می‌شود که این امر باعث مدیریت راحت‌تر می‌گردد و در ضمن 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 و از آن برای مسیریابی بسته در هسته استفاده می‌شود. شکل زیر شمایی کلی از پروسه را نشان می‌دهد.

