|  |  |  |
| --- | --- | --- |
| دانشگاه صنعتي اميركبير **(پلي تكنيك تهران)** | **باسمه تعالي**  فرم تعريف **پروژه**  فارغ التحصيلي دوره كارشناسي | **دانشكده مهندسي كامپيوتر و فناوري اطلاعات** |

**تاريخ: ...........................**

**شماره: ..........................**

|  |
| --- |
| **عنوان پروژه:** |
| **استاد راهنماي پروژه: دکتر سیاوش خرسندی امضاء:** |
| **مشخصات دانشجو:**  **نام و نام خانوادگي: الهه جلال‌پور[[1]](#footnote-1) گرايش: سخت افزار**  **شماره دانشجویي: ۹۱۳۱۰۳۶ ترم ثبت نام پروژه: اول 9۴-9۵** |
| **داوران پروژه:**   1. **امضاء داور:** 2. **امضاء داور:** |
| **شرح پروژه** (در صورت مشترك بودن بخشي از كار كه بعهده دانشجو مي باشد مشخص شود)**:**  **به پیوست آمده است.** |
| **وسائل مورد نياز:**  **- امکان دسترسی به مقالات مرتبط**  **- یک دستگاه کامپیوتر دارای دسترسی به اینترنت** |
| **محل انجام پروژه: دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر تاريخ شروع: اردیبهشت 1394** |

اين قســمت توســط دانشــكده تكميــل مي‌گــردد:

|  |
| --- |
| **تاريخ تصويب در گروه: اسم و امضاء:**  **تاريخ تصويب در دانشكده: اسم و امضاء:**  **اصلاحات لازم در تعريف پروژه:** |

**توجه**: پروژه حداكثر يك‌ماه و نيم پس از شروع ترمي كه در آن در درس پروژه ثبت نام به عمل آمده است بايد به تصويب برسد.

|  |  |  |
| --- | --- | --- |
| نسخه1- دانشكده | نسخه 2- استاد راهنما | نسخه 3- دانشجو |

# تعریف مسئله:

MPLS یک فناوری در شبکه های سطح حمل[[2]](#footnote-2) است از ترکیب راه گزینی[[3]](#footnote-3) و مسیریابی[[4]](#footnote-4) بوجود آمده و گستره کاری مسیریابی لایه ۳ را در کنار سرعت و سادگی راه گزینی لایه ۲ فراهم می‌آورد.

در شبکه‌های IP/MPLS، سرآیند اضافی کوچک shim، به بسته افزوده می‌شود. هر برچسب می‌تواند روی برچست قبلی قرار بگیرد و به این ترتیب برچسب‌ها می‌توانند یک پشته را ایجاد کنند.

در شبکه‌های MPLS هر برچسب نماینده یک مسیر از پیش تعیین شده است. بنابراین، عمل تعیین مسیر یکبار در ورودی شبکه انجام می‌گیرد و درون شبکه LSR[[5]](#footnote-5)ها بسته‌های برچسب خورده را بدون نیاز به مسیریابی سوئیچ می‌کنند.

سرویس‌های VPN در زمره مهمترین سرویس‌های سرویس دهنده‌ها‌ی سطح حمل قرار دارند. از آنجایی که قسمت بزرگی از هسته‌ی شبکه‌های حامل را IP/MPLS تشکیل می‌دهد، سرویس VPN نیز بر اساس MPLS محقق می‌شود. استفاده از MPLS برای فراهم آوردن سرویس VPN باعث سادگی پیاده سازی و گسترش پذیری [[6]](#footnote-6)بیشتر می‌گردد.

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 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 multipoint to multipoint 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:

Provider Edge (PE): گره‌ای سمت سرویس دهنده که ارتباط با مشتری را فراهم می‌آورد. در این گره عموما از LSR استفاده می‌شود.

Customer Edge (CE): گره‌ای سمت مشتری که ارتباط با سرویس دهنده را فراهم می‌آورد. در این گره عموما از Router استفاده می‌شود.

در معماری MPLS BGP VPN نیازبه 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 PEها نیز این جداول را از طریق پروتکل I-BGP با یکدیگر به اشتراک می‌گذارند. در این معماری از LDP برای توزیع برچسب‌های مسیر‌های PEها استفاده می‌شود. LDP به این منظور از اطلاعات پروتکل‌های مسیریابی IGP که در شبکه هسته اجرا می‌شوند، استفاده می‌کند. 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 وآدرس های MAC سیستم های 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 مشتری روی همه‌ی PEها ارسال می‌گردد. در این مدل هر PE به صورت مستقل جدول MAC خود را آپدیت می‌کند. در این معماری بازهم از LDP و پروتکل‌های

مسیریابی IGP برای توزیع برچسب‌ها استفاده می‌شود.

# راه‌ حل‌های فعلی و مشکلات آن‌ها:

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

# راه ‌حل پیشنهادی:

در معماری SDVPN، CEها با سويیچ‌های 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 VPN های 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 کاریری‌ 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 ترافیک های 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 می شود.

## معماری صفحه کنترل

این بخش از ماژول هایی تشکیل میشود که وظیفه اصلی آنها به روز رسانی جداول جریان موجود در PEها است. این ماژول ها عبارتند از:

۱) سوییچ مجازی:

در این ماژول شبکه هسته به صورت یک سوییچ شبیه سازی شده که PE ها هر کدام متناظر با یک اینترفیس این سوییچ هستند. جدول آدرس های MAC که مشخص کننده ی هر آدرس های mac و درگاه های متناظر آنها برای خروج هستند و همچنین جدولی که تناظر VLAN ها و اینترفیس ها 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 PE ها هر کدام متناظر با یک درگاه این سوییچ هستند. در این ماژول مکانیزم های مسیر یابی بین شبکه های متصل به هر یک از این درگاه ها پیاده سازی خواهد شد.

۳) اعمال سیاست :

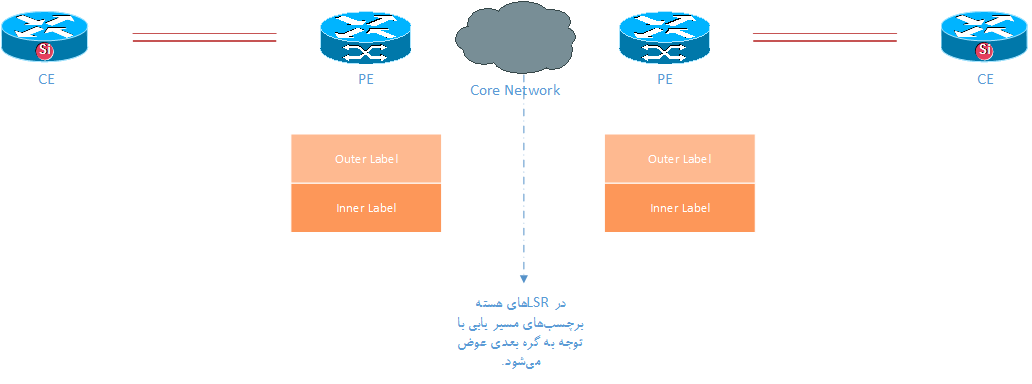
گاهی نیاز به لزوم اعمال سیاست برای جلوگیری از رسیدن بسته هایی از یک سایت مشخص مشتری به سایت دیکری از آن نیاز خواهد شد. امکان اعمال اینگونه دستورات توسط این ماژول به کاربر استفاده کننده از VPNداده می‌شود.

## 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 کاملا 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.



1. Email: [el.jalalpour@gmail.com](mailto:el.jalalpour@gmail.com) [↑](#footnote-ref-1)
2. Carrier-grade service providers [↑](#footnote-ref-2)
3. Switching [↑](#footnote-ref-3)
4. Routing [↑](#footnote-ref-4)
5. Label Switch Router [↑](#footnote-ref-5)
6. Scalability [↑](#footnote-ref-6)