بررسی کیفیت سرویس در شبکه‌های BGP/MPLS VPN مبتنی‌بر سرویس خدمات متمایز

علی اسماعیلی[۱]، مهدی مهدوی[۲]، پژمان خدیوی[۳]
۱- کارشناس ارشد برق، دانشگاه آزاد اسلامی، واحد نجف آباد، a_es1357@yahoo.com
۲- استادیار، دانشگاه صنعتی اصفهان، m_mahdavi@cc.iut.ac.ir
۳- استادیار، دانشگاه صنعتی اصفهان، pkhadivi@ec.iut.ac.ir

چکیده

رشد نمایی اینترنت منجر به اهمیت گسترش روزافزون سرویس‌ها، کاربران و برنامه‌های کاربردی بیشتر شده است. در نتیجه سرعت بیشتر و کیفیت سرویس بهتر، مهمترین چالش‌های دنیای شبکه امروزی می‌باشند. با ترکیب تکنولوژی MPLS همراه با سرویس خدمات متمایز و مهندسی ترافیک می‌توان به ارتقاء پارامترهای کیفیت سرویس و استفاده بهینه از منابع و اجتناب از ازدحام در شبکه‌های نسل آتی کمک نمود. MPLS می‌تواند در یک توپولوژی شبکه BGP/MPLS VPN که توسعه‌یافته سایت‌های مختلف از کاربران برای انتقال‌داده می‌باشد پیاده‌سازی گردد. در این مقاله به ارائه ساختار BGP/MPLS VPN پرداخته شده و سپس با پیاده‌سازی شبکه MPLS مبتنی‌بر DiffServ بر روی VPN کیفیت سرویس در شبکه بررسی گردیده است و سپس با استفاده از نرم‌افزار OPNET مکانیزم‌های مختلف جهت ارتقاء کیفیت سرویس در شبکه، در قالب سناریوهای مختلف شبیه‌سازی شده است. در اکثر روش‌های ارائه شده قبلی، با افزایش منابع برای ترافیک‌های اولویت پایین‌تر مانند BE و AF ترافیک‌های اولویت بالاتر مانند EF (Voice، Video) خدشه‌دار شده است. با اعمال مکانیزم‌های مدیریت و اجتناب از ازدحام برای ترافیک‌های با اولویت پایین‌تر و همچنین مهندسی ترافیک، نتایج بهتری برای ارائه کیفیت سرویس به ترافیک‌هایی که فوق‌العاده حساس به تأخیر می‌باشند نسبت‌به روش‌های قبلی ارائه شده است.

واژه‌های کلیدی

سرویس خدمات متمایز (DiffServ)، مهندسی ترافیک، کیفیت سرویس، MPLS، BGP، VPN

۱– مقدمه

VPN (Virtual Private Network) یک شبکه اختصاصی مجازی بوده که از یک شبکه عمومی، عموماً اینترنت برای ارتباط با سایت‌های از راه دور و ارتباط کاربران با یکدیگر استفاده می‌نماید درخواست‌های تضمین سرویس در شبکه VPNمبتنی اینترنت با امنیت داده و مهندسی ترافیک برای سرویس‌های چندرسانه‌ای پرسرعت بلادرنگ افزایش یافته است [۱]، [۲]، [۳].

VPN باید بتواند چندصد سایت و کاربر را دریک ناحیه گسترده مقیاس‌بندی نماید. بنابراین شبکه VPN باید نیازهای محرمانه بودن داده‌ها و مقیاس‌پذیری داده‌ها و کیفیت سرویس را برآورده نماید. بنابراین لزوم یک پروتکل برای برآورده شدن این‌گونه نیازها در

هسته یک شبکه گسترده افزایش پیدا می‌نماید. MPLS (Multiprotocol Label Switching) به‌عنوان یک تکنیک جدید برای پشتیبانی از مهندسی ترافیک عرضه شده است. MPLS با ایجاد مسیر سوییچ برچسبی LSP مابین مسیریاب‌های IP ارسال بسته را از محاسبات مسیر تفکیک می‌نماید و مسیریابی مؤثرتری را در شبکه ایجاد می‌نماید. زیرا در IP هم محاسبات مسیر و هم ارسال مبتنی‌بر آدرس مقصد هستند [۴].

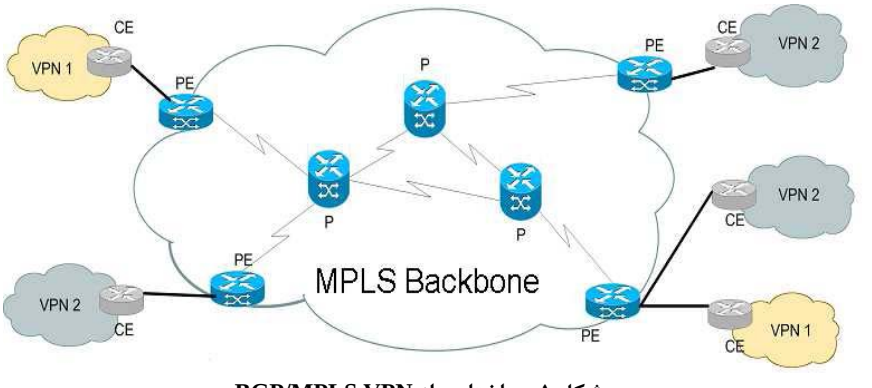
شبکه VPN می‌تواند به دوشبکه VPN مبتنی‌برIP و VPN مبتنی‌بر MPLS تقسیم‌بندی گردد. BGP/MPLS VPN یک نوع از شبکه VPN مبتنی‌بر IP می‌باشد که به‌طور صریح و آسان سایت‌های کاربران را گسترش می‌دهد [۵]. زیرا توسط لینک‌های نظیربه‌نظیر بین مسیریاب‌های لبه سرویس‌دهنده (PE[1]) و مسیریاب‌های سرویس‌گیرنده (CE[2]) پیکربندی شده‌اند. VPN مبتنی‌بر MPLS برای تضمین مقیاس‌پذیری و کیفیت سرویس در شبکه‌های VPN با مقیاس بزرگ مناسب می‌باشد. با ترکیب MPLS با سرویس خدمات متمایز می‌توان ترافیک‌های ورودی به هسته شبکه را کلاس‌بندی و QoS ترافیک‌ها را تضمین نمود [۵].

در این مقاله در قسمت اول ساختارBGP/MPLS VPN که در RFC2547 پایه‌گذاری شده است [۶] توضیح داده می‌شود. در این ساختار پروتکل دروازه مرزی (BGP) برای مبادله اطلاعات مسیریابی VPN و MPLS برای ارسال ترافیک VPN بکار می‌رود. ساختار پیشنهادی در یک زیرساخت فراهم‌کننده سرویس (SP[3]) با اجرای MPLS و DiffServ پیاده‌سازی شده است. در قسمت دوم پشتیبانی MPLS از سرویس خدمات متمایز برای تضمین کیفیت سرویس شرح داده می‌شود در قسمت سوم مکانیزم‌های مدیریت ترافیک و مدیریت ازدحام برای شبکه‌هایی که ترافیک‌های چند رسانه‌ای بلادرنگ مانند ترافیک‌های Video و Voice و ترافیک با گذردهی بالا مانند FTP را حمل می‌نمایند و نحوه پیاده‌سازی آنها اشاره می‌گردد و در قسمت چهارم به پیاده‌سازی مکانیزم‌های کیفیت سرویس و شبیه‌سازی و مقایسه سناریوهای مختلف پرداخته شده و در قسمت پایان نتیجه‌گیری شده است.

۲–ساختار BGP/MPLS VPN

MPLS به‌عنوان یک تکنولوژی جدید برای کاهش گلوگاه‌های ارسال بسته‌ها در مسیریاب‌های زیرساخت بکار می‌رود [۷]. در این فن‌آوری به بسته‌ها در مسیرهای لبه‌ای برچسب تعلق می‌گیرد. MPLS با استفاده از برچسب به‌منظور ارسال بسته‌ها، ارسال را از محاسبات مسیر تفکیک می‌نماید. مسیرهای سوییچ برچسبی یا LSPها مابین مسیریاب‌های IP برای اجتناب از ارسال IP درمیان مسیریاب‌های IP هسته یا میانی بکار می‌روند. که MPLS با ایجاد این مسیرهای LSP مسیریابی مؤثرتری را نسبت‌به IP سنتی موجب می‌شوند. MPLS برای توزیع برچسب‌ها درون حوزه و درنتیجه ایجاد LSP از یک پروتکل توزیع برچسب یا LDP استفاده می‌نماید. دو پروتکل استانداردشده برای سیگنالینگ در شبکه MPLS برای مهندسی ترافیک معرفی شده است. یکی از آنها CR-LDP است [۸]. که برای پشتیبانی از مسیریابی مبتنی‌بر قید بکار گرفته می‌شود و دیگری RSVP-TE بوده که یک ست الحاقی روی RSVP است و برای پشتیبانی از مهندسی ترافیک و ایجاد برچسب MPLS بکارگرفته می‌شود [۹]. RSVP یک پروتکل ذخیره‌سازی منابع شبکه به‌صورت انتهابه‌انتها جهت ارائه کیفیت سرویس در اینترنت طراحی شد و در RFC 2205 به‌طور کامل شرح داده شده است.

یک BGP/MPLS VPN ساختاری از VPN است که مجموعه‌ای از مسیریاب‌های لبه مشتری (CE) که هرکدام به یک یا چند مسیریاب لبه تدارک‌دهنده متصل شده‌اند، سرویس (PE) را شامل می‌شود. شبکه شامل مسیریاب‌های هسته تدارک‌دهنده (P) نیز می‌باشند که در شکل زیر نشان داده شده است.



شکل ۱- ساختاری از BGP/MPLS VPN

BGP (Border Gateway Protocol) یا پروتکل دروازه مرزی یک پروتکل مسیریابی می‌باشد که برای برقراری مسیر جهت ارسال بسته‌های MPLS در میان شبکه‌های خودمختار[۴] مختلف بکار می‌رود. ازBGP بیرونی (Exterior BGP) برای مبادله مسیریابی بین PE و CE استفاده می‌شود و همچنین از BGP درونی (Interior BGP) برای مبادله اطلاعات مسیریابی بین PE و PE در شبکه MPLS VPN استفاده می‌شود [۱۰].

مسیریاب‌های PE پیشوند[۵] آدرس IP از CE را دریافت و ۸ بایت جداسازی مسیر (RD[۶]) را به پیشوند IP اضافه می‌نمایند. VPN با استفاده از جدول VRF[7] که شامل RD و RT[۸] (نشان مسیر) می‌باشد برقرار می‌شود. مسیریاب‌های PE و CE اطلاعات بین مشترکین VPN را به‌وسیله برقراری پروتکل دروازه مرزی (BGP) با دیگر عضوهای VPN یکسان تبادل می‌نمایند. LSPها بین همتاهای BGP برقرار می‌شوند و ترافیکی که وابسته به چندین VPN است را حمل می‌نمایند. مسیریاب‌های PE و CE اطلاعات مسیریاب‌های VPN را با استفاده از پروتکل اطلاعات مسیر مانند RIP و OSPF و BGP تغییر می‌دهند.

مسیرهای برقرار شده که وابسته‌به جدول VRF هستند مبتنی‌بر پردازش تصمیم‌گیری پروتکل مسیریابی‌شان می‌باشد، تجهیزات PE، باید این اطلاعات مسیرها را با دیگر مسیرهای تجهیزات PE مبادله نمایند، BGP چند پروتکلی یا (MP- BGP[۹]) برای توسعه مسیرهای VPN در میان شبکه فراهم‌کننده سرویس بکار می‌رود. درحالی که VPN می‌تواند از هم‌پوشانی فضای آدرس استفاده نمایند.

BGP می‌تواند مسیر مقصد را با پیوند آدرس یکسان مشخص نماید. با (MP-BGP) مسیریاب‌های درونی (Ingress) با اطلاعات برچسب درونی عمل می‌نمایند و دیتا برچسب بیرونی به‌وسیله پروتکل‌های سیگنالینگ MPLS مانند CR-LDP و RSVP-TE برداشته می‌شوند و مسیریاب‌های بیرونی هر دو برچسب را برداشت (Pop) می‌نمایند.

یکی از مزایای استفاده از BGP/MPLS در شبکه VPN این است که ستون فقرات فراهم‌کننده سرویس (SP) احتیاج به به‌روزکردن نرم‌افزارهای پروتکل را ندارند و دلیل آن این است که مسیریاب‌های P مبتنی‌بر VPN نیستند. مسیرهای VPN بین مسیر تجهیزات PE مبادله می‌شوند و مسیریاب‌های هسته P مبتنی‌بر این مسیرها نیستند و بنابراین ترافیک VPN باید در میان شبکه تونل زده شود که با برقراری تونل‌های MPLS بین تجهیزات PE قابل دسترس است.

۳– پشتیبانی MPLS از DiffServ در شبکه VPN

تکنولوژی MPLS به‌کمک مسیریابی مبتنی‌بر قید (Constraint-based) می‌تواند بسته‌ها را در مسیرهای معین هدایت نماید. حتی می‌تواند پهنای باند را برای FEC[۱۰]ها (مجموعه‌ای از بسته‌IP با کلاس هم‌ارزی ارسال) تنظیم نماید ولی MPLS توانایی رفتار مبتنی‌بر کلاس (Class-based) برای جریان بسته‌ها ندارد. بنابراین هیچ تضمینی برای تأخیر و افت و jitter ندارد. همچنین ساختار DiffServ به‌گونه‌ای است که نمی‌تواند یک کیفیت سرویس انتها به انتها را ارائه نماید به‌دلیل این‌که هیچ تأثیری بر روی مسیر بسته‌ها ندارد و فقط براساس اولویت کلاس بسته‌ها شروع به ارسال می‌نماید و هیچ‌گونه کنترل در برابر رخدادن ازدحام و خرابی شبکه (Failure) نمی‌تواند داشته باشد. بنابراین با ترکیب DiffServ با MPLS به توانایی کامل در تضمین کیفیت سرویس خواهیم رسید [۱۰].

در حوزه DiffServ ارسال وضعیت یا سرویس که یک BA[11] (مجموعه‌های از بسته‌های DiffServ) دریک نود دریافت می‌نماید PHB[12] نامیده می‌شود. در نود ورودی از ناحیه DiffServ بسته‌ها کلاس‌بندی و شماره‌گذاری می‌شوند. ساختار DiffServ وضعیت ارسال یک PHB را مشخص می‌نماید. این ساختار توصیف کیفی از تأخیر و لرزش یا افت مشخصاتی که یک BA به‌سمت نود DiffServ انتقال داده شده است رانشان می‌دهد. نودهای DiffServ بسته را باتوجه به DSCP، به PHB مربوطه نگاشت می‌دهند. DSCP وضعیت مجموعه بسته‌های DS (PHB) را برحسب زمان‌بندی و اولویت هنگام حذف در نودهای شبکه تعیین می‌نماید [۱۱].

EF (هدایت پرشتاب)، AF (هدایت تضمین‌شده) [۱]2 و BE (هدایت بهترین تلاش) ازجمله PHBهای تعریف‌شده در نود DiffServ می‌باشد. ترافیک EF یک وضعیت PHB با کمترین تأخیر و لرزش و افت را که در یک نود DiffServ ممکن است پیاده‌سازی شود را مشخص می‌نماید؛ به‌این‌صورت‌که یک صف اختصاص یافته شده به ترافیک EF در نود DiffServ برای هر نرخ ورودی بسته کمتر از نرخ سرویس‌دهی آن می‌باشد. بنابراین با اجرای این وضعیت تأخیر و افت کمی در نود شبکه اتفاق می‌افتد. ترافیک‌هایی مانندvoic، video که به تأخیر و خطا و افت کم احتیاج دارند به ترافیکEF نگاشت می‌یابند. ترافیک AF (هدایت تضمین‌شده) PHBها برای تضمین ارسال مختلف ترافیک که یک نود DiffServ می‌تواند پشتیبانی نماید معین شده است. هدایت تضمین شده PHB چهار کلاس AFx را مشخص می‌نماید .که1AF، AF2، AF3 و AF4 نامیده می‌شوند. هر کلاس به یک

مقدار مشخص از فضای بافر و پهنای باند واسط برای تضمین کیفیت سرویس اختصاص می‌یابد. بسته‌های با کلاس‌های مشابه AFx تأخیر، لرزش وکیفیت سرویس مشابه دارند اما در نرخ افت بسته کیفیت سرویس آنها متفاوت است. برنامه‌های کاربردی که بلادرنگ نیستند مانند جریان‌های video، می‌توانند از سرویس AF استفاده نمایند [۱۲].

۲ مساله مهم برای پشتیبانی MPLS از DiffServ وجود دارد [۱۱]:

اول این‌که DSCP در سرآیند IP حمل می‌شود اما مسیریاب‌های سوییچ برچسبی(LSR) فقط سرآیند برچسب را بررسی می‌نمایند دوم اینکه DSCP ۶ بیت دارد اما فیلد EXP در MPLS فقط ۳ بیت دارد. دو راه حل ارائه شده برای حل این ۲ مشکل در IETF مطرح گردید:

- EXP مشتق‌شده از کلاس زمان‌بندی PHB (PSC) در مسیر سوییچ برچسبی (E- LSP)
- برچسب مشتق‌شده از کلاس زمان‌بندی PHB (PSC) در مسیر سوییچ برچسبی (L-LSP)

در مدل اول DSCP در سرآیند IP در درون فیلد EXP از سرآیند MPLS نگاشت پیدا می‌نماید. (E-LSP) و این نوع ترافیک تا ۸ PHB که چندین کلاس سرویس خدمات متمایز را شامل می‌شود را می‌تواند بر روی تنها یک LSP حمل نماید. و در مدل دوم پروتکل سیگنالینگ مانند LDP یا RSVP-TE برای ارسال بسته‌های IP در هرکلاس استفاده می‌شود. این نوع LSP برای ارسال فقط یک نوع ترافیک استفاده می‌شود.

برای پیاده‌سازی PHB در آزمایشات از مدل اول توصیف‌شده یعنی E-LSP استفاده شده است. نگاشت بین PHB و EXP در آزمایشات مربوط به شبیه‌سازی درجدول (۱) مشخص شده است.

جدول۱- نگاشت PHB به EXP با مقادیر وزنی

EXP	PHB	WFQ Weights
0	AF11	5
1	AF21	10
2	AF22	10
3	AF31	15
4	AF32	15
5	AF41	25
6	AF42	25
7	EF	55

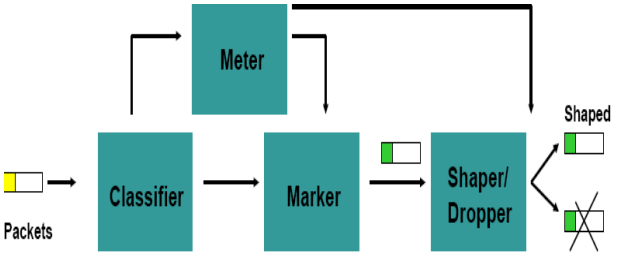
۴– مکانیزم‌های مدیریت ترافیک

از جمله پارامترهای مشخصات کیفیت سرویس شامل تضمین پهنای باند، تأخیر، تغییرات تأخیر (Jitter) و افت بسته می‌باشد. پیاده‌سازی کیفیت سرویس نهایتاً به مجموعه مکانیزم مدیریت ترافیک تکیه دارد. این مکانیزم‌ها به نودهای شبکه کمک می‌کند که از ازدحام جلوگیری نمایند. مکانیزم‌های کلی برای پیاده‌سازی QoS شامل کلاس‌بندی ترافیک، علامت‌گذاری ترافیک زمان‌بندی و شکل‌دهی ترافیک می‌باشد که این عملیات برای بسته ورودی در نود در شکل زیر مشخص گردیده است [۱۴].

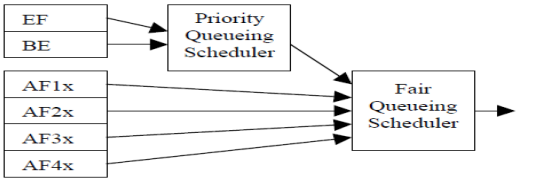
۴–۱– مدیریت ازدحام (Congestion Management)

مدیریت صف (Queuing Management) و مکانیزم زمان‌بندی بسته‌ها (Packet Scheduling) ۲ مکانیزم مهم برای مدیریت ازدحام می‌باشند [۱۴]. ازدحام ممکن است در چندین نقطه شبکه به‌وجود آید. هر نقطه ازدحام، منبع بالقوه‌ای از تأخیر و لرزش و افت را برای جریان ترافیک نشان می‌دهد. که مهمترین نقاط مشترک برای موضوع ازدحام در خروجی واسط‌های شبکه (مثلاً خروجی مسیریاب) است. از جمله مکانیزم‌های زمان‌بندی بسته‌ها می‌توان به‌روش FIFO، WFQ[13] (الگوریتم صف‌بندی منصفانه وزن‌دار)، CB-WFQ، PQ (اولویت صف) و WRR[14] (الگوریتم نوبت چرخشی وزن‌دار)و...اشاره کرد که هرکدام برای اولویت دادن به صف با روش‌های مختلف بکار می‌روند [۱۴]، [۱۵]. از مکانیزم‌های مدیریت صف برای اجتناب از ازدحام می‌توان به الگوریتم‌های RED[15] (تشخیص زودهنگام)، WRED و RIO اشاره نمود [۱۸].

در مقالات [۱۶]، [۱۷] نشان داده شده است که با پیاده‌سازی DiffServ در شبکه IP/MPLS مشکلات کمبود منابع مانند پهنای باند برای ترافیک‌های BE و AF را می‌توان ارتقاء داد ولی کارآیی ترافیک EF خدشه‌دار می‌شود. با اولویت دادن به ترافیک EF نیز، ترافیک BE دچار فقدان منابع می‌گردد. بنابراین در این مقالات الگوریتم صف‌بندی منصفانه وزن‌دار با اولویت (WFQ-P) برای فراهم‌نمودن تضمین کیفیت سرویس به هر سه ترافیک پیشنهاد شده است. در این دو مقاله نشان داده است WFQ-P کارآیی بهتری نسبت‌به ۱۶PQWRR (اولویت صف‌بندی با نوبت گردشی وزن‌دار) و ۱۷DDS (الگوریتم سرویس خدمات متمایز پویا) دارد.



شکل۲- عملیات شرطی‌سازی ترافیک

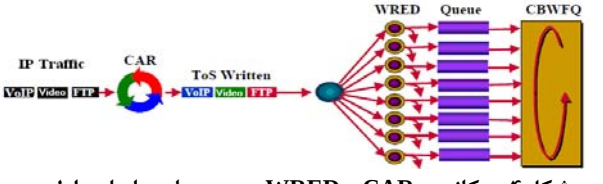


شکل ۳- مکانیزم WFQ-P

۴-۲- اجتناب از ازدحام (Congestion Avoidance)

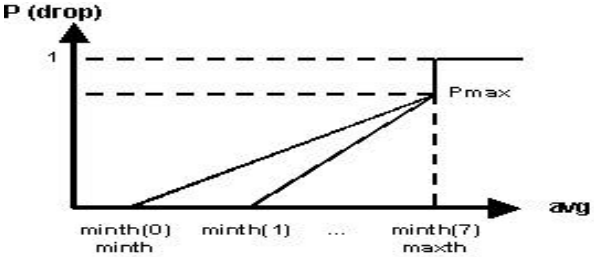
در مواردی که در أثر ورودی حجم بالای ترافیک به یک مسیریاب طول صف داخلی آن زیادمی‌شود. علاوه‌بر افزایش احتمال پرشدن کل فضای بافر، تأخیر بسته‌ها نیز بیشتر می‌شود. ازجمله روش‌ها برای این موضوع روش حذف از انتهای صف، WRED وRIO می‌باشد.که دراین گونه موارد با انتخاب حدود مشخص برای طول مجاز صف به‌طور هوشمندانه به حذف بسته‌های اضافی با اولویت پایین پرداخته می‌شود و از خدشه‌دارشدن ترافیک EF جلوگیری می‌گردد.

بنابراین روش پیشنهادی این است که از مکانیزم CAR[۱۸] در مسیریاب‌های لبه‌ای و از مکانیزم مدیریت ازدحام WRED در هسته شبکه استفاده نماییم. با توجه به شکل (۴) ما می‌توانیم از الگوریتم CAR برای مدیریت نرخ بسته‌ها و از مکانیزم WRED برای حذف بسته‌ها اولویت پایین برای کم‌کردن ازدحام استفاده نماییم.



شکل۴- مکانیزم CAR و WRED درمسیریاب‌براساس اولویت ترافیک

مکانیزم WRED (تشخیص زودهنگام وزن‌دار) به‌این صورت عمل می‌نماید. که هنگامی که یک بسته به نود می‌رسد بسته‌ها را بایک احتمال (P) که به‌صورت خطی از صفر تا ماکزیمم افزایش پیدا می‌کنند در بین رنجی از میانگین طول صف، حذف نماید این رنج بین یک کمینه آستانه (minth) و بیشینه آستانه (maxth) مشخص می‌شود. الگوریتم WRED در ابزار شبیه‌سازی OPNET چندین متوسط طول صف برای هر بسته با بایت‌های ToS (نوع سرویس) مختلف دارد. اما ماکزیمم متوسط اندازه بسته و احتمال حذف (Pmax) یکسان دارند که در شکل مشخص می‌باشد [۱۵].



شکل ۵-مکانیزم WREDدر OPNET

با توجه به شکل(۵) min th(0) و min th(1) وmin th(7) مینیمم طول متوسط صف برای بسته‌های با بایت ToS (نوع سرویس) ۰و۱و۲و....و ۷ به ترتیب می‌باشد. تابعی که minth را محاسبه می‌نماید طبق رابطه زیر می‌باشد [۱۴].

$$\text{minth (ToS)= minth+ (maxth-minth)*ToS/7} \qquad (۱)$$

اختلاف بین کمینه آستانه و بیشینه آستانه باید به حد کافی بزرگ باشد تا از هم‌زمانی عمومی جلوگیری نماید. اگر این اختلاف کم باشد خیلی از بسته‌ها در وهله اول حذف خواهند شد در نتیجه هم‌زمانی صورت می‌گیرد روش زیر برای انتخاب پارامترهای WRED با سرعت لینک R بکار می‌رود. هنگامی که B پهنای باند لینک خروجی در بسته‌های با سایز MTU است با روش زیر محاسبه می‌گردد.

$$B = \frac{R(Mbps)}{8(\frac{bit}{byte})\times 1/N(\frac{byte}{pac})} \qquad (۲)$$

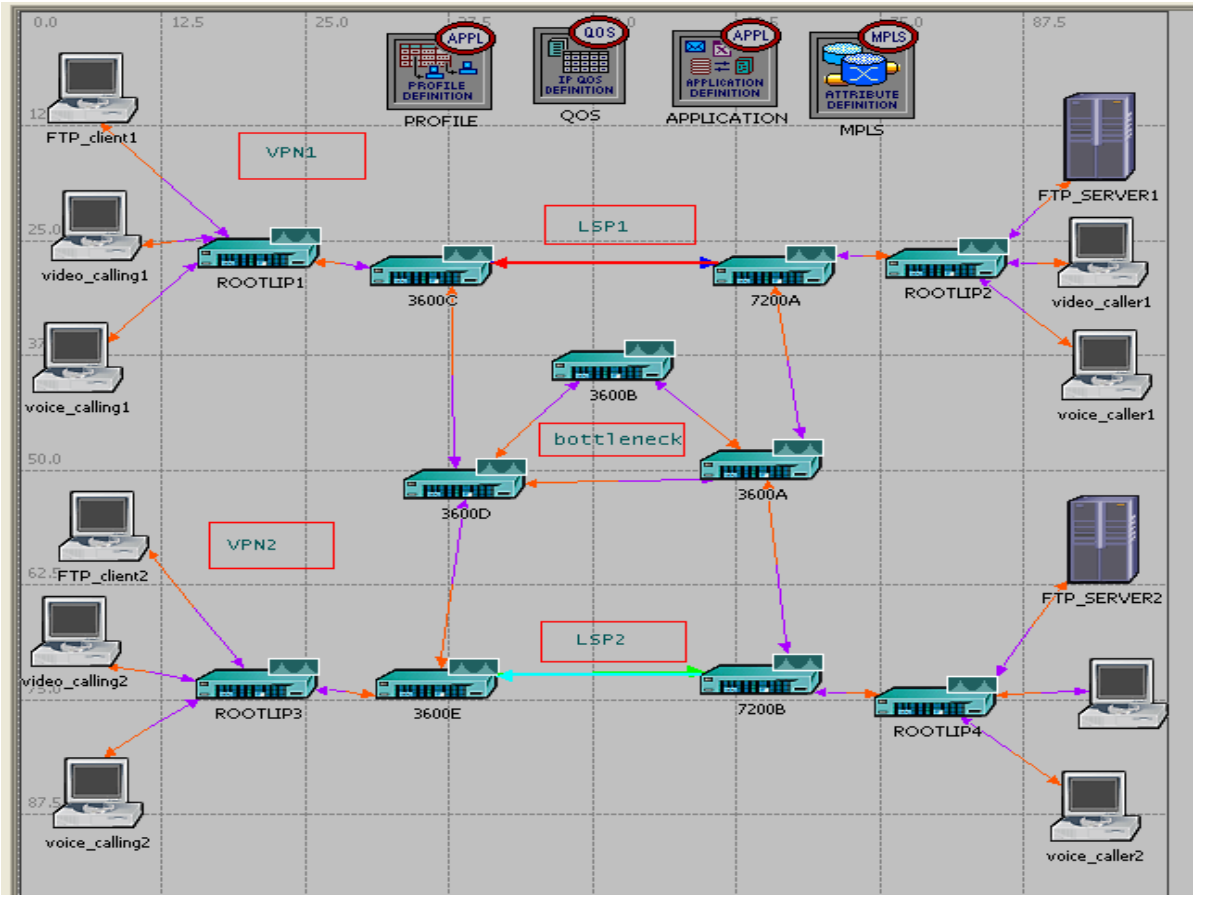
B پهنای باند لینک خروجی و N تعداد بایت در هر بسته است.

۵- توپولوژی شبکه و شبیه‌سازی

در این قسمت توپولوژی شبکه VPN BGP/MPLS طراحی و پیکربندی شده که در شکل (۶) نشان داده شده است .برای شبیه‌سازی از نرم‌افزار شبیه‌ساز OPNET (11.5) استفاده شده است. ساختار به‌این‌گونه است که توپولوژی شبکه فراهم‌کننده سرویس از دو سرویس‌گیرنده VPN با دو سایت تشکیل شده است.

تمامی لینک ها دوطرفه می باشند و با توجه به شکل (۶) برای تشریح کیفیت سرویس بین مسیریاب‌های هسته تنگ راه یا (Bottleneck) درنظرگرفته شده است.

پهنای باند لینک‌های بین مسیریاب‌ها 3600C و 3600D و 3600A ، 6.5 Mb/S می‌باشد و لینک‌های بین سرورها و ایستگاه‌های کاری (Workstations) و مسیریاب‌ها 10 Mb/S می‌باشند.



شکل۶- توپولوژی شبکه BGP/MPLS VPN

۵-۱- سناریو اول: توپولوژی BGP/MPLSVPN (Baseline)

در این سناریو برنامه‌های کاربردی VoIP، Video و FTP را مطابق با پروفایل نشان داده شده در جداول (۲)، (۳) و (۴) به‌طور یکسان در هر دو VPN تعریف می‌نماییم. در سناریو Baseline پروتکل MPLS بدون پارامترهای کیفیت سرویس در مسیریاب‌ها فعال می‌باشند.

جدول۲- پارامترهای برنامه کاربردی FTP

FTP Table	
Command Mix (Get/Total)	100%
Inter-Request Time	exponential (1)
File Size (byte)	Pareto (83333.33,1.5)
Type of Service	Best Effort (0)

جدول ۳- پارامترهای برنامه کاربردی VoIP

VoIP Table	
Silence Length (sec)	exponential (0.65)
Talk Spurt Length (sec)	Exponential (0.352)
Encoder Scheme	GSM (silence)
Voice F rams per Packet	1
Type of Service	Best Effort (0)

جدول ۴- پارامترهای برنامه کاربردی Video Conferencing

Video Conferencing Table	
exponential (0.65)	exponential (0.65)
exponential (15625)	exponential (15625)
Best Effort (0)	Best Effort (0)

این مشخصات پیکربندی برنامه کاربردی، یک بار ترافیک FTP 2Mb/s تولید می‌نماید. وهمچنین بار ترافیکیVideo 1.5Mb/s و بار ترافیکی Voice 20 Kb/p در هر VPN تولید می‌نماید.

مسیریاب‌ها مکانیزم صف‌بندی FIFO را با استفاده از بافر 1Mb/s پیاده‌سازی می‌نمایند. تمامی ترافیک VPN 1 در شروع شبیه‌سازی آغاز به کار می‌کنند و برنامه کاربردی ترافیک VPN 2 بعد از ۳۰ دقیقه آغاز به کار می‌کنند. شبیه‌سازی در ۶۰ دقیقه و با ۵۰۰۰۰۰ event (رویداد) در تمام سناریوها اجرا می‌شود.

۵–۲– سناریو دوم: ترکیب MPLS با DiffServ

هدف از این سناریو این است که چگونه با ترکیب MPLS با DiffServ، کیفیت سرویس در شبکه را می‌توان ارتقاء داد.

مراحل زیرنحوه اختصاصQoS به سناریو BGP/MPLS VPN می‌باشد.

۱- برای ترافیک‌های مختلف براساس نیاز سرویس باید نوع سرویس مشخص گردد و سپس با نگاشت PHB و EXP (سرآیند فیلد MPLS) باتوجه به جدول (۱) در اینترفیس‌های LSR تنظیم می‌گردد.

۲- نوع سرویس (ToS) برای بسته‌ها در برنامه کاربردی برای FTP و Video و Voice با توجه به جدول (۵) برای VPNهای هر سایت تنظیم می‌شود.

با توجه به جدول (۵) برای VPN 1 ما سه نوع PHB تنظیم می‌نماییم و برای VPN 2 یک نوع PHB تنظیم می‌گردد.

۳- مکانیزم صف‌بندی منصفانه وزن‌دار (WFQ) با توجه به جدول شماره (۱) بر روی مسیریاب‌های واسط پیاده‌سازی می‌شود. درحقیقت به کلاس‌های ترافیکی وزن اختصاص داده می‌شود.

جدول ۵-پیکربندی PHB برای هر VPN

	Application	PHB
VPN Client 1	FTP_1	AF21
	Video_1	AF41
	Voice_1	EF
VPN Client 2	FTP_2	AF11
	Video_2	AF11
	Voice_2	AF11

۵–۳– سناریو سوم: اعمال مدیریت ازدحام

باتوجه به این‌که شبکه MPLS از روش مسیریابی کوتاهترین مسیر(IGP) برای مسیردهی استفاده می‌نماید و این‌که تمام ترافیک از میان مسیریاب‌های 3600 D و 3600 A که تنگ‌راه است، عبور می‌نماید. بنابراین در این لینک ازدحام صورت می‌گیرد.

با اعمال مکانیزم پیشنهادی از ازدحام و همچنین از خدشه‌دار شدن ترافیک EF جلوگیری می‌نماییم. بنابراین از مکانیزم CAR در مسیریاب‌های لبه‌ای و از مکانیزم مدیریت ازدحام WRED در هسته شبکه استفاده می‌کنیم. الگوریتم CAR در ابزار QoS در ویژگی خروجی Interface مسیریاب تنظیم می‌گردد که‌در جدول زیر به‌این‌صورت در مسیریاب لبه‌ای تنظیم می‌شود.

جدول ۶-پیاده‌سازی مکانیزم CAR بر روی مسیریاب‌های لبه‌ای

CoS	Rate Limit	Conforming Traffic Policy	Exceeding Traffic Policy
FTP	2 Mb/s	Best Effort(0)	None
Video Conferencing	1.5 Mb/s	Streaming Multimedia(	Best Effort
VoIP	20 kb/s	Interactive voice(6)	Best Effort

روش زیر برای انتخاب پارامترهای WRED با سرعت لینک بین دو مسیر یاب R=6.5 Mbps بکار می‌رود. B، پهنای باند لینک، طبق رابطه (۲) محاسبه می‌گردد.

مقدار N= 1250 Byte/Packet برای لینک 6.5 Mbps اندازه‌گیری شده است و طبق رابطه (۲) مقدار B=650Packet/s بدست می‌آید. مقدار کمینه آستانه (minTH) 05. B و بیشینه آستانه (maxTH) 0.1B درنظرگرفته شده و ضریب نمایی وزن‌دار ۹ قرار داده می‌شود.

باتوجه به مطالب پارامترهای WRED طبق جدول زیربر روی مسیریاب‌های هسته تنظیم می‌شود.

جدول ۷-پیاده‌سازی مکانیزم WRED بر روی مسیریاب‌های هسته

Match property	Min TH (packets)	Max TH (packets)	Mark Probability denomin	exponential weights constant
DSCP	32	65	100	9

برای ترافیک EF در پروفایل WFQ مکانیزم LLQ[19] (صف‌بندی با تأخیر کم) را تنظیم می‌نماییم.

۵–۴– سناریو چهارم: اعمال مهندسی ترافیک

در این سناریو با ترکیب مهندسی ترافیک و MPLS/DiffServ

نتایج بهتری برای ارتقاء کیفیت سرویس بدست می‌آید.

دراین سناریو از روش E-LSP داینامیکی استفاده شده است و ترانک‌های ترافیکی برای هر FEC در هر LSP بین سایت‌های VPN1 و VPN2 تنظیم می‌شود. برای مسیریابی پروتکل OSPF درهر LSRها اجرا شده است و در آخر با اعمال مینیمم قید پهنای باند LSPها مقید به پهنای باند می‌گردند.

VPN Client1→4.0 Mbps
VPN Client 2→4.0 Mbps

۵–۵– بررسی نتایج

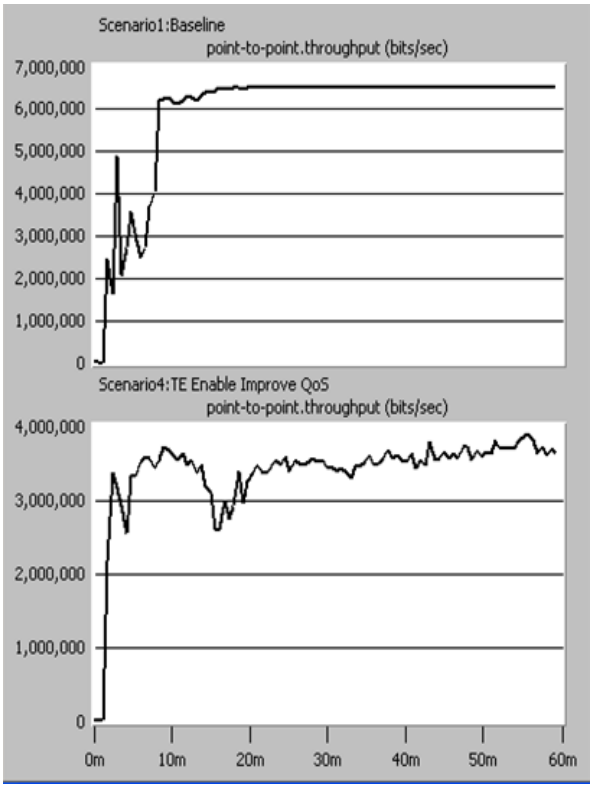
نتایج شبیه‌سازی در این قسمت از خروجی نرم‌افزار OPNET گرفته شده است و رفتار پارامترهای پاسخ زمانی دانلود FTP، تأخیر و تغییرات تأخیر VoIP و Video و افت بسته‌های ترافیکی به‌عنوان پارامترهای کیفیت سرویس، در هر VPN مقایسه شده است.

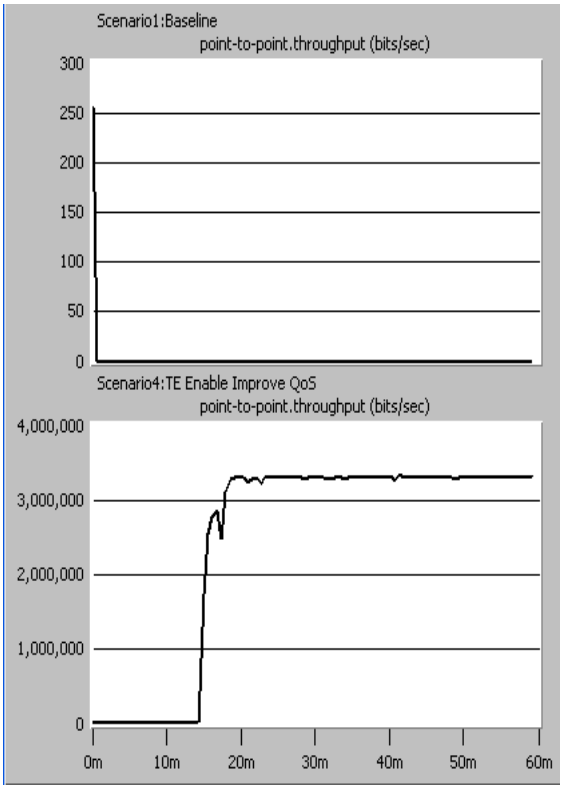
در سه سناریو اول تمام ترافیک‌های VPN از مسیر یکسان، مسیر مستقیم ارتباطی بین مسیریاب 3600D و مسیریاب 3600 A، عبور پیدا می‌نمایند.

در سناریو ۴ بعد از اعمال مهندسی ترافیک، قید مینیمم پهنای باند در هر LSP تمام ترافیک VPN2 را از مسیر یاب 3600D به 3600A از طریق 3600B به‌صورت اجباری عبور می‌دهد.

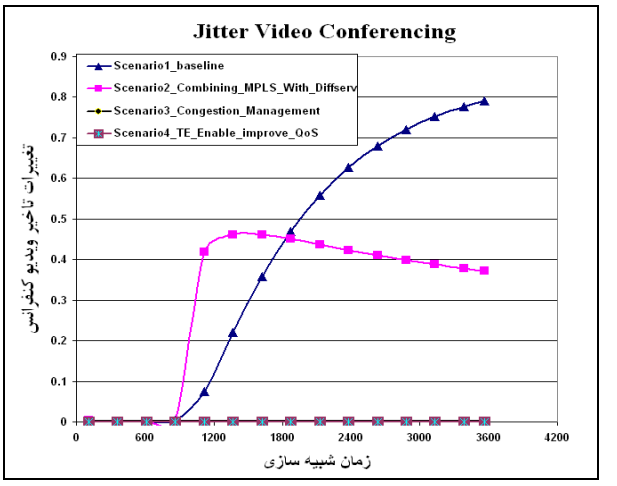
با توجه به شکل(۷) مشاهده می‌شود در سناریو اول در نمودارهای بالا تمام ترافیک شبکه از یک مسیر یکسان بین LSR D وLSR A عبورنموده است و چون محدودیت پهنای باند 6.5 Mbps داشته است تمامی ترافیک عبور داده نشده است ولی در سناریو ۴ نمودار پایین مشاهده می‌شود با اعمال TE و قید پهنای باند تمام ترافیک VPN2 از کوتاهترین مسیر بعدی عبور یافته است و بار ترافیکی در هسته شبکه به تعادل رسیده است.

شکل‌های(۸)، (۹)، (۱۰) و (۱۱) مقایسه تأخیر و شکل‌های (۱۲) و (۱۳)پاسخ زمانی دانلود FTP و میزان Loss کلی در شبکه باتوجه به سناریوهای مختلف را نشان می‌دهد. خروجی تمامی شکل‌ها از نرم‌افزار OPNET ،باتوجه به تفکیک‌پذیری بهتر در نمودار Excel آورده شده است.

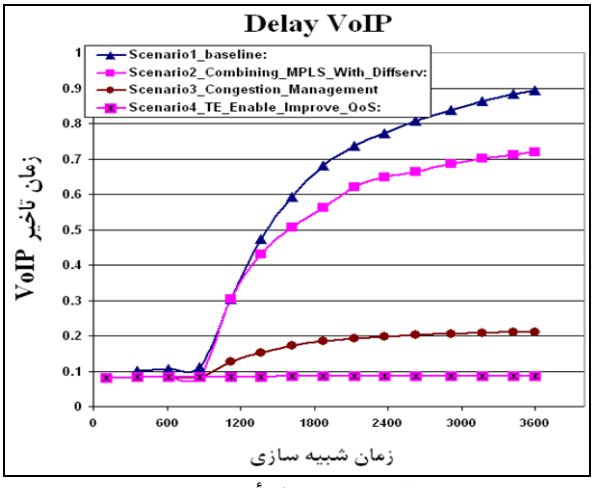




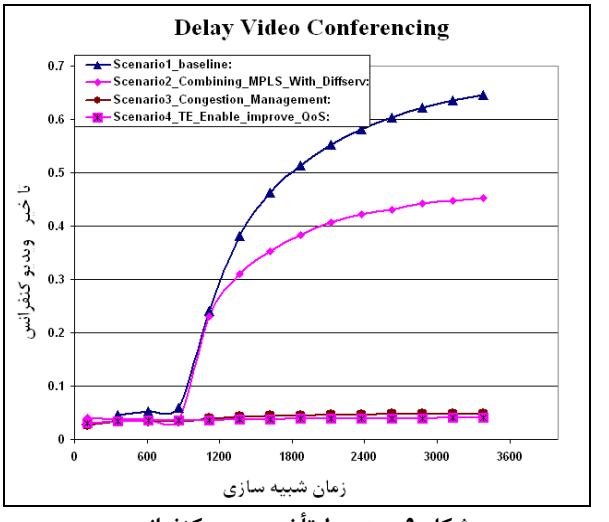
شکل ۷- مقایسه میزان گذردهی ترافیک بسته‌ها از هسته شبکه



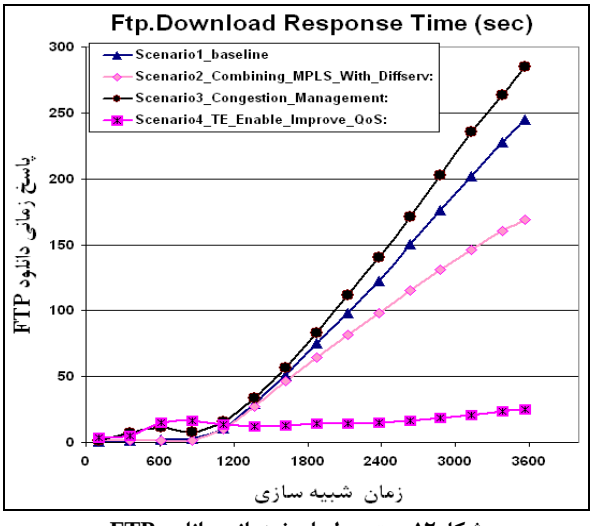
شکل ۸– متوسط تغییرات تاخیر ویدیو کنفرانس



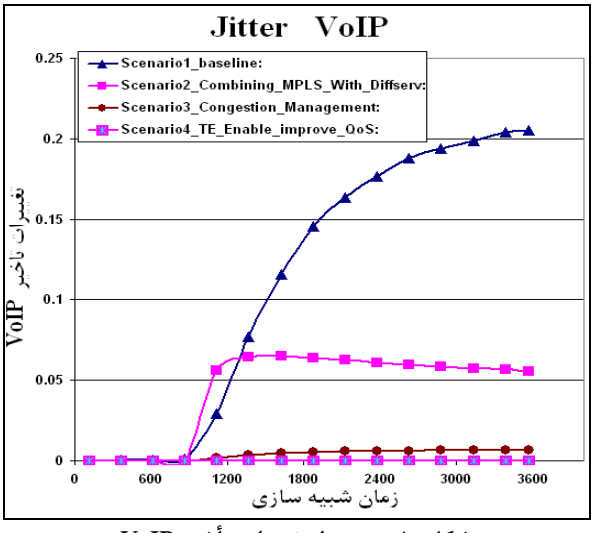
شکل ۱۱– متوسط تأخیر VoIP



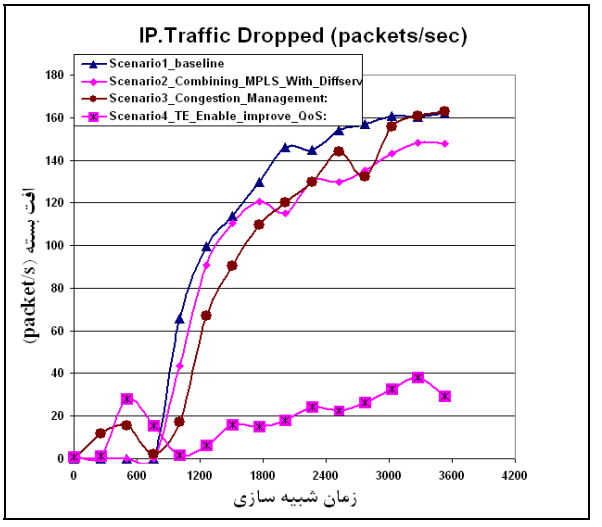
شکل ۹– متوسط تأخیر ویدیو کنفرانس



شکل۱۲– متوسط پاسخ زمانی دانلود FTP



شکل ۱۰– متوسط تغییرات تأخیر VoIP



شکل۱۳– میزان افت کلی بسته‌های ترافیکی

با توجه به شکل‌های (۱۲) و (۱۳) در سناریو سوم مشاهده می‌شود با اعمال مدیریت و اجتناب ازدحام اگر چه زمان میزان دانلود FTP بیشتر شده است و افت کلی بسته‌های ترافیک با اولویت پایین زیاد می‌باشد، کیفیت سرویس را برای ترافیک‌های حساس به تأخیر افزایش داده است و با توجه به نمودارها مشاهده می‌شود که در سناریو۳ با اجرای مکانیزم مدیریت ازدحام نتایج تأخیر بهتری برای ترافیک‌های با اولویت بالاتر بدست آمده است، در سناریو ۴ با اعمال مهندسی ترافیک میزان گذردهی شبکه و نتایج تأخیر و میزان افت بسته بهتر از سناریوهای قبلی می‌باشد و کیفیت سرویس برای هر سه ترافیک AF، EF، BE افزایش یافته است.

۶–نتیجه‌گیری

با ترکیب MPLS با سرویس خدمات متمایز، نتایج بهتری برای پیاده‌سازی کیفیت سرویس در شبکه بدست می‌آید. ترافیک سرویس‌گیرنده‌های VPN می‌تواند درمیان مسیرهای سایت‌های مربوطه با ذخیره‌سازی منابع ارسال شود. با اعمال سرویس خدمات متمایز می‌توان برنامه‌های کاربردی را براساس نیازهای کیفیت سرویس اولویت‌بندی کرد. در این مقاله با اعمال مدیریت و اجتناب از ازدحام از جمله مکانیزم‌های WFQ و WRED می‌توان از خدشه‌دار شدن ترافیک EF هنگام ورود بار سنگین به شبکه جلوگیری نمود. نتایج شبیه‌سازی نشان می‌دهد با حذف هوشمندانه بسته‌های ترافیکی با اولویت کلاس پایین‌تر نتایج بهتری برای ترافیک‌های بلادرنگ که نیازهای کیفیت سرویس بالاتری دارند بدست می‌آید.

در سناریو آخر با اجرای مهندسی ترافیک و استفاده از ترانک‌های ترافیکی با اولویت کلاس بر روی LSPها می‌توان به تعادل بار ترافیکی در شبکه کمک نمود. قید پهنای باند به‌اجبار ترافیک VPN2 را از میان مسیر کوتاهتر دیگر عبور می‌دهد و از ازدحام در هسته شبکه جلوگیری می‌کند.

در مجموع در شبکه‌های نسل آتی (NGN) نیازهای ذخیره‌سازی منابع همراه با ارتقاء پارامترهای QoS برای برنامه‌های کاربردی مختلف امری بدیهی به‌نظر می‌رسد. طراحان شبکه باید درنظر داشته باشند که کاربردهای مورد نظر شبکه چیست و یا کاربران برای برآوردن چه نیازهایی از شبکه استفاده می‌کنند. MPLS همراه با تکنولوژی که روی آن قابل پیاده‌سازی هستند (مانند مهندسی ترافیک، QoS و VPN) یک انتخاب مناسب برای برآوردن این نیازها است و می‌تواند به‌خوبی در هسته شبکه‌های NGN بکار گرفته شود.

۷–مراجع

[1] J. Zeng, N. Ansari; **"Toward IP Virtual Private Network Quality of Service: A Service Provider Perspective"**, IEEE Communication Magazine, IEEE, Vol. 41, Issue 4, pp. 113-119, April 2003

[2] P. Zhang, R. Kantola; "**Building MPLS VPNs with QoS Routing Capability**", Interworking, pp. 292-301, 2000.

[3] H. Lee, J. Hwang, B. Kang, K. Jun; "**End-To-End QoS Architecture for VPNs: MPLS VPN Deployment in a Backbone Network**", International Workshop on Parallel Processing, Toronto, Canada, 2000.

[4] E. Rosen, A. Viswanathan, R. Callon; "**Multi protocol Label Switching Architecture**", RFC 3031, January 2001.

[5] E. Rosen, Y. Rekhter; "**BGP/MPLS VPNs**", RFC 2547, October, 2002.

[6] E. C. Rosen, Y. Rekhter; "**BGP/MPLS IP VPNs**", draft-ietf-l3vpnrfc2547bis-01. txt, September 2003.

[7] B. Davie, Y. Rekhter; "**MPLS Technology and Applications**", Morgan Kaufmann, San Francisco, CA 2000.

[8] B. Jamoussi, Ed. L. Andersson, R. Callon, R. Dantu; "**Constraint-Based LSP Setup using LDP**" IETF 3212, January 2002.

[9] F. L. Faucheur, T. D. Nadeau, A. Chiu,W. Townsend, et al; "**Extensions to RSVP-TE and CR-LDP for support of DiffServ-aware MPLS traffic engineering**", IETF Internet drafts ,November 2000.

[10] Y. Rekhter, T. Li; "**A Border Gateway Protocol 4 (BGP-4)",** RFC 1771**,** March 1995.

[11] F. L. Faucheur, B. Davie, S. Davari, P. Vaananen; "**MPLS Support of Differentiated Services**", RFC 3270, May 2002.

[12] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski; "**Assured Forwarding PHB Group**" IETF RFC 2597.

[13] M. C. Castro, N. A. Nassif, W. C. Borelli; "**QoS Performance Evaluation in BGP/MPLS VPN**", I2TS', 2003.

[14] S. Álvarez; "**QoS for IP/MPLS Networks**", Cisco Systems Inc,2006.

[15] E. Tsolakou, I. S. Venieris; **"Implementation of Traffic Conditioning and PHB Mechanisms in OPNET",** 1 Sep 2000.

[16] I. Sh. Hwang, 1B. J. Hwang, Ch. Sh. Ding; "**Adaptive Weighted Fair Queuing with Priority (AWFQP) Scheduler for Diffserv Networks**" Journal of Informatics & Electronics, Vol. 2, No. 2, pp. 15-19, March 2008.

[17] X. Zeng, C. H. Lung, C. Huang; "**A Bandwidth-efficient Scheduler for MPLS DiffServ Networks**", The IEEE Computer Society's 12th Annual International Symposium, pp. 251-258, 4-8 Oct. 2004.
[18] S. Cnodder, O. Elloumi; "**RED behavior with different packet sizes**", Proceedings of the Fifth IEEE Symposium on Computers and Communications, Vol. 3, p.p. 793- 805, July 2000.
[19] Jing-bo XIA, Ming-hui LI, Lu-jun WAN; **"Research on MPLS VPN Networking Application Based on OPNET",** International Symposium on Information Science and Engieering, 2008.
[20] http://www.opnet.com/support/des_model_library /MPLS.html

۸–پی‌نوشت‌ها

1- Provider Edge
2- Customer Edge
3- Service Provider
4 - Autonomous
5 - Prefix
6 - Route Distinguisher
7 - VPN Routing & Forwarding
8 - Route Target
9 - Multiprotocol
10- Forward Equivalence Forward
11- Behavior Aggregate
12- Per Hop Behavior
13- Weighted Fair Queuing
14- Weighted Round Robin
15- Random Early Detection
16- Priority Queuing Weighted Round Robin
17- Dynamic Differential Service
18- Committed Access Ratio
19- Low Latency Queuing