

فصل یازدهم

کیفیت سرویس

۱۱-۱- مقدمه

در حال حاضر شبکه جهانی اینترنت فقط سرویس بهترین تلاش را به کاربران خود ارائه می دهد. یکی از معایب اصلی سرویس فوق، این است که با وجود این که مسیریاب های شبکه به خوبی قادر به دریافت و پردازش بسته های ورودی می باشند، ولی هیچ گونه تضمینی در مورد سالم رسیدن بسته ها به مقصد وجود ندارد. با توجه به رشد روزافزون استفاده از اینترنت و به خصوص با توجه به اهمیت به اینترنت به عنوان ابزاری برای گسترش تجارت جهانی، تلاش های زیادی جهت حفظ کیفیت سرویس (QoS¹) در اینترنت در حال انجام می باشد. در این راستا در حال حاضر کلاس های سرویس متنوعی مورد بحث و توسعه می باشند. یکی از کلاس های سرویس فوق، به شرکت ها و مراکز ارائه سرویس وب که نیاز به ارائه سرویس سریع و مطمئن به کاربران خود دارند، اختصاص دارد. این نوع کلاس سرویس خود به زیر کلاس های دیگری که به ترتیب کیفیت با نام های سرویس طلایی، نقره ای و برنزی شناخته می شوند، تقسیم بندی می شود. یکی دیگر از کلاس های سرویس جدید در اینترنت، به سرویسی که نیاز به تأخیر و تغییرات تأخیر کمی دارند، اختصاص دارد. سرویسی مانند تلفن اینترنتی و کنفرانس های ویدئویی اینترنتی نمونه ای از این کلاس سرویس می باشند.

برای دست یافتن به سرویس جدید فوق، عده ای معتقدند که در آینده ای نزدیک فن آوری فیبرنوری و WDM آن قدر رشد خواهد کرد که اینترنت به طور کامل بر مبنای آن پیاده سازی خواهد شد و عملاً مشکل پهنای باند و همچنین تضمین کیفیت سرویس وجود نخواهد داشت. عقیده دوم که ظاهراً درست تر از عقیده اول می باشد، این است که با وجود گسترش فن آوری های انتقال و افزایش پهنای باند، هنوز به مکانیزم هایی برای تضمین کیفیت سرویس کاربران نیاز می باشد. در حال حاضر اکثر تولیدکنندگان مسیریاب و سوئیچ های شبکه اینترنت، در حال بررسی و افزودن مکانیزم هایی برای تضمین کیفیت سرویس در محصولات خود می باشند.

از سوی سازمان جهانی IETF مدل ها و مکانیزم های مختلفی برای تضمین کیفیت سرویس مورد تقاضای کاربران ارائه شده است. برخی از مهم ترین این مدل ها عبارتند از:

- پروتکل رزرو منابع در اینترنت (RSVP²)
- سرویس جدا شده³
- MPLS
- مهندسی ترافیک
- مسیریابی مبتنی بر قید⁴

در کاربردهای زمان حقیقی قبل از ارسال هرگونه داده ای، ابتدا باید با کمک پروتکل های سیگنالینگ یک مسیر اولیه برقرار شود و منابع لازم (در صورت وجود) در مسیر فوق رزرو گردد. از پروتکل RSVP برای رزرو منابع برای کاربردهای زمان حقیقی در اینترنت استفاده می شود.

در سرویس جداشده، جهت ارائه سرویس مختلف به کاربران، بسته‌های کاربران در لبه ورودی شبکه، علامت‌گذاری می‌شوند و بدین ترتیب کلاسهای سرویس متنوعی به کاربران ارائه می‌شود.

در پروتکل MPLS، به بسته‌های ورودی به شبکه، یک برچسب کوتاه متصل می‌شود و سپس با توجه به مقدار برچسب فوق، عملیات مسیریابی درون شبکه انجام می‌گردد.

به‌وسیله مهندسی ترافیک، می‌توان مسیرهای مختلفی از جریان‌های ترافیکی در شبکه به‌وجود آورد و هر یک را به‌طور جداگانه مدیریت نمود. در قسمت‌های بعدی به‌طور خلاصه با هر یک از مدل‌های فوق آشنا می‌شویم.

۱۱-۲- مفهوم کیفیت سرویس

مفهوم کیفیت سرویس همراه با توسعه شبکه‌های ارتباطی، تغییر زیادی نموده است. در روزهای آغازین ایجاد شبکه‌های کامپیوتری، ارسال بسته‌ها از مبدا به مقصد مهمترین و برجسته‌ترین هدف یک شبکه و دسترسی قابل اطمینان به شبکه مساله اصلی در زمینه کیفیت سرویس بود. امروزه با رشد سریع شبکه‌ها، مفاهیمی چون نیاز روزافزون به پهنای باند و پشتیبانی همزمان کلاسهای مختلف سرویس در درجه اول اهمیت قرار گرفته‌اند. در نتیجه کیفیت سرویس به فاکتوری کلیدی در بکارگیری شبکه‌ها و سرویسهای امروزه تبدیل شده است.

با وجود اینکه کیفیت سرویس اخیراً به مساله‌ای مهم در بین محققان شبکه تبدیل شده، هنوز هم ابهاماتی در شیوه فهم و تعریف آن وجود دارد. بطور کلی کیفیت سرویس به معنی ارائه سرویسی سازگار و قابل پیش‌بینی به منظور تأمین نیازهای کاربردهای مختلف است.

کیفیت سرویس را از دو دیدگاه می‌توان مشاهده نمود: کاربران شبکه و تأمین‌کنندگان سرویس شبکه^۱. هر یک از این دو دارای اهداف کیفیت سرویس متفاوتی هستند. آنچه که یک کاربر شبکه نیاز دارد، دسترسی به حداکثر پهنای باند با کمترین هزینه ممکن است. از طرف دیگر، هدف تأمین‌کننده شبکه به حداکثر رساندن کارایی شبکه همزمان با برطرف کردن نیازهای کیفیت سرویس همه کاربران به صورت همزمان است.

پارامترهای متداول کیفیت سرویس که برای توصیف کارایی شبکه بکار می‌روند عبارتند از:

- ۱- پهنای باند (گذردهی^۲): تعداد بایتهایی که در یک دوره تناوب خاص از طریق شبکه انتقال می‌یابند.
- ۲- تأخیر^۳: زمانی که طول می‌کشد تا یک بسته داده از مبدا خود به سمت مقصد حرکت کند. تأخیر شامل سه مؤلفه است: تأخیر انتشار، تأخیر انتقال و تأخیر صف‌بندی
- ۳- واریانس تأخیر^۴: واریانس تأخیری که یک بسته داده با آن مواجه است برابر با تفاوت بین حداکثر و حداقل تأخیر ممکن برای بسته، می‌باشد.
- ۴- درصد دور ریختن^۵: شانس دور ریخته شدن بسته در شبکه می‌باشد. حالتی وجود دارند که منجر به دور ریخته شدن بسته‌ها می‌شوند (مانند سرریز شدن بافر در نودهای سوئیچ شبکه).
- ۵- بهره‌وری^۶: نسبت زمان مشغول بودن اتصال، به کل زمان در یک دوره تناوب می‌باشد. میزان بهره‌وری را می‌توان در هر یک از عناصر شبکه مانند مسیریابها و اتصالات اندازه‌گیری نمود.

^۱ Internet Service Provider (ISP)

^۲ throughput

^۳ delay

^۴ jitter

^۵ packet loss

^۶ utilization

کیفیت سرویس، توانایی کاربردهای شبکه و عناصری چون میزبانها و مسیریابها بر تأمین نیازهای سرویس ترافیکهای مختلف و در نتیجه ارائه سطحی از اطمینان برای آنهاست. در ادامه به بررسی کاملتر پارامترهای کیفیت سرویس می پردازیم.

۱۱-۳- پارامترهای کیفیت سرویس

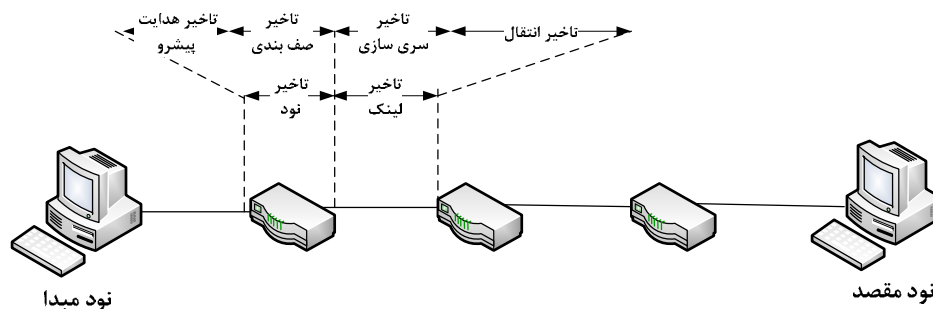
همانطور که در بالا به آن اشاره شد برای تعیین کیفیت سرویس در شبکه از پارامترهایی نظیر: گذرهی، تاخیر، تغییرات تاخیر و اتلاف استفاده می شود. در ادامه به بررسی هریک از پارامترهای کیفیت سرویس فوق می پردازیم:

۱۱-۳-۱- گذرهی

پارامتر گذرهی نشان دهنده ظرفیت سیستم برای ارسال داده ها می باشد. در یک سیستم TDM کلاسیک، گذرهی برابر با پهنای باند کانال انتقال می باشد که به آسانی قابل محاسبه می باشد. به عنوان مثال گذرهی یک کانال DS-3 برابر با ۴۵ مگابیت بر ثانیه است. در سیستم های TDM آماری محاسبه گذرهی به مراتب مشکلتر از TDM کلاسیک می باشد. در این سیستم ها میزان متوسط بسته های عبوری در واحد زمان به عنوان گذرهی محاسبه می شود.

۱۱-۳-۲- تاخیر

مقدار زمانی که به طور متوسط طول می کشد تا یک بسته از یک نقطه شبکه به نقطه دیگر آن برود، تاخیر بسته را مشخص می کند. تاخیر انتها به انتهای بسته توسط پارامترهایی نظیر: تاخیر هدایت پیشرو^۱، تاخیر صف بندی، تاخیر انتقال و تاخیر سری سازی، مشخص می شود. در شکل (۱۱-۱) مثالی از نحوه محاسبه تاخیر آورده شده است.



شکل (۱۱-۱): نحوه محاسبه تاخیر انتها به انتها

تاخیر هدایت پیشرو نشان دهنده مقدار زمانی است که طول می کشد تا مسیریاب بسته را دریافت نموده و برای هدایت آن از طریق یک درگاه مناسب تصمیم گیری نماید. به عبارت دیگر تاخیر هدایت پیشرو نشان دهنده حداقل زمان لازم برای پردازش و هدایت یک بسته در مسیریاب می باشد. مقدار زمان تاخیر فوق در محدوده ۱۰ تا ۱۰۰ میکروثانیه می باشد.

تاخیر صف بندی بیانگر میزان زمان انتظار یک بسته در صف، قبل از ارسال به درگاه خروجی مناسب می باشد. تاخیر انتقال نشان دهنده زمان لازم برای طی کردن کانال فیزیکی است. میزان تاخیر انتقال با طول کانال فیزیکی نسبت مستقیم دارد. به عنوان مثال برای یک کانال نقطه به نقطه به طول ۱۰۰ مایل (۱۶۰ کیلومتر) مقدار تاخیر انتقال رفت و برگشت حدود ۱ میلی

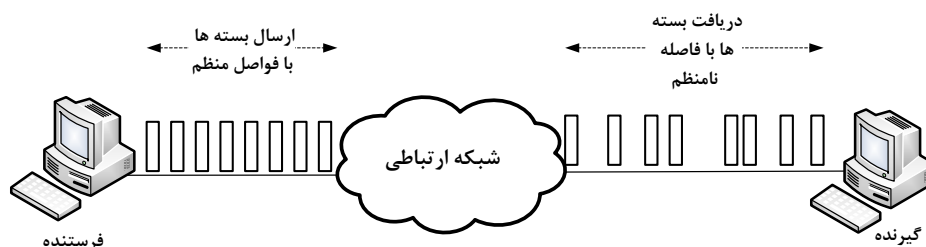
ثانیه می باشد. از طرف دیگر تاخیر انتقال با سرعت انتقال الکترون یا فوتون در محیط انتقال رابطه معکوس دارد. سرعت نور در فیبر نوری حدود 0.65 سرعت نور در خلاء و سرعت الکترون در یک هادی مسی حدود 0.75 سرعت نور در خلاء می باشد. هنگامی که یک مسیریاب آماده ارسال یک بسته می باشد، تاخیر سری سازی نشان دهنده زمان لازم برای قرارداد بیت های متعلق به یک بسته در کانال خروجی می باشد. تاخیر سری سازی با طول بسته رابطه مستقیم و با سرعت درگاه خروجی رابطه معکوس دارد. از آنجائیکه امکان کنترل و تغییر اندازه بسته وجود ندارد، تنها راه کاهش زمان سری سازی بسته افزایش سرعت درگاه های خروجی مسیریاب می باشد. در جدول (۱-۱۱) مقادیر زمان تاخیر سری سازی بسته ها بر حسب طول بسته و سرعت درگاه خروجی نشان داده شده است. تاخیر بسته ها با افزایش بهره وری کانال به صورت نمایی افزایش می یابد.

جدول (۱-۱۱) تاخیر سری سازی بر حسب طول بسته و سرعت درگاه خروجی

طول بسته	تأخیر کانال DS-1 (بر حسب میلی ثانیه)	تأخیر کانال DS-3 (بر حسب میلی ثانیه)	تأخیر کانال OC-3 (بر حسب میلی ثانیه)	تأخیر کانال OC-12 (بر حسب میلی ثانیه)	تأخیر کانال OC-48 (بر حسب میلی ثانیه)	تأخیر کانال OC-192 (بر حسب میلی ثانیه)
۴۰ بایت	0.2073	0.0072	0.0021	0.0005	0.0001	کمتر از 0.0001
۲۵۶ بایت	1.3264	0.0458	0.0132	0.0033	0.0008	0.002
۳۲۰ بایت	1.6580	0.0572	0.0165	0.0041	0.0010	0.003
۵۱۲ بایت	2.6528	0.0916	0.0264	0.0066	0.0016	0.004
۱۵۰۰ بایت	7.7720	0.2682	0.0774	0.0193	0.0048	0.0012
۴۴۷۰ بایت	23.1606	0.7994	0.2307	0.0575	0.0144	0.0036
۹۱۸۰ بایت	47.5648	1.6416	0.4738	0.1181	0.0295	0.0074

۱۱-۳-۳- تغییرات تاخیر

تغییرات تاخیر بسته های متعلق به یک جریان ترافیکی باعث کاهش کیفیت سرویس های زمان حقیقی می شود. در شکل (۱۱-۲) مثالی از اثر تغییرات تاخیر بر روی بسته های دریافتی در گیرنده نشان داده شده است.



شکل (۱۱-۲): مثالی از نحوه ایجاد تغییرات تاخیر در بسته های دریافتی در مقصد

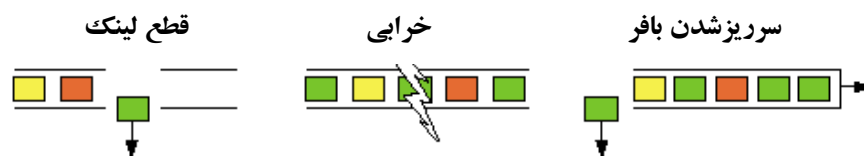
در سیستم های TDM^۱ کلاسیک تغییرات تاخیر بسیار کم بوجود می آید. در TDM آماری به خاطر پدیده صف بندی و تاخیر در بافر این احتمال وجود دارد که بسته های متوالی متعلق به یک جریان ترافیکی، با تاخیرهای متفاوتی مواجه شوند که این پدیده باعث ایجاد تغییرات تاخیر می گردد. یکی دیگر از دلایل وقوع تغییرات تاخیر این است که بسته های متعلق به یک جریان ترافیکی ممکن است بعد از انجام عملیات مسیریابی از مسیرهای فیزیکی متفاوتی به سمت مقصد ارسال شوند که این مسئله باعث ایجاد تغییرات تاخیر در بسته های دریافتی در مقصد می شود. با افزایش بهره وری کانال، مشابه تاخیر، تغییرات تاخیر نیز افزایش می یابد. در TDM آماری مقدار تغییرات تاخیر برای تمام بسته های متعلق به یک جریان ترافیکی ثابت نمی باشد. دلیل عمده این مسئله آن است که پدیده تراکم که عامل اصلی پیدایش تاخیر و تغییرات تاخیر است، یک پدیده دینامیک بوده و از نقطه ای به نقطه ای دیگر در شبکه متغیر است.

برخی از برنامه های کاربردی در مقابل تغییرات تاخیر مقاوم نمی باشند. به عنوان مثال در کاربردهایی نظیر ارسال صوت و تصویر زنده بر روی شبکه، پدیده تغییر تاخیر باعث کاهش کارایی سرویس می شود. البته برخی دیگر از برنامه های کاربردی TCP/IP وجود دارند که پدیده تغییرات تاخیر بر روی آنها چندان اثری ندارد.

۱۱-۳-۴- اتلاف

در شبکه های IP همانطور که در شکل (۱۱-۳) نشان داده شده است، سه عامل مهم باعث ایجاد اتلاف بسته ها می شوند که عبارتند از:

۱. قطع شدن کانال ارتباطی که باعث از بین رفتن بسته ها می شود.
 ۲. نویز کانال باعث خراب شدن برخی از فیلدهای بسته می شود. نودهای شبکه با بررسی مجموع مقابله ای بسته متوجه خراب بودن آن می شوند و اقدام به حذف بسته می نمایند.
 ۳. تراکم در شبکه باعث لبریز شدن بافر نودها و از بین رفتن بسته ها می شود.
- مشکل قطع شدن کانال ارتباطی به خاطر استفاده از کانال های ارتباطی ذخیره در شبکه و همچنین بهره گیری از شبکه های بی سیم، از اهمیت چندانی برخوردار نمی باشد. همچنین با توجه به گسترش کانال های ارتباطی مطمئن و بدون نویز نظیر فیبر نوری، احتمال خراب شدن بسته ها به خاطر وقوع نویز در کانال بسیار کم و قابل صرف نظر می باشد. بنابراین تنها عامل مهم خراب شدن بسته ها لبریز شدن بافر نودهای شبکه به خاطر وقوع تراکم در شبکه می باشد. از آنجائیکه اکثر ترافیک های امروزی از نوع انفجاری می باشند، شدت بار لینک های شبکه ثابت و از قبل قابل پیش بینی نمی باشد. چنانچه در نودهای شبکه تراکم بوجود آید، با حذف کردن بسته های ورودی از شدت تراکم کاسته می شود.



شکل (۱۱-۳): عوامل خراب شدن بسته در شبکه های کامپیوتری

۱۱-۴- مکانیزم های تضمین کیفیت سرویس در اینترنت

کیفیت سرویس در شبکه ها از طریق سه مکانیزم پیاده سازی می شود. این مکانیزمها عبارتند از:

۱۱-۴-۱- مکانیزمهای انتها به انتها

این مکانیزمها در هر دو انتهای یک ارتباط عمل می‌کنند و قادرند رفتار یک ارتباط مشخص را کنترل یا تطبیق نمایند. علاوه بر این مکانیزمها قادرند کیفیت یک ارتباط را کنترل کنند. نمونه‌ای از مکانیزمهای کنترلی، کنترل پذیرش ارتباط (CAC^1) است. احتمال بروز تراکم در شبکه‌ای که از CAC استفاده می‌کند پایین‌تر است. چرا که این مکانیزم، جامعیت ترافیک موجود در شبکه را با جلوگیری از پذیرش سایر ترافیکها حفظ می‌نماید. مکانیزمهای انطباقی رفتار یک جریان را بر اساس پارامترهای خاصی تطبیق می‌کنند. مثالی از این مکانیزمها، مکانیزمهای کنترل تراکم TCP هستند. این مکانیزمها نرخ ترافیک جریان را در واکنش به دور ریخته شدن بسته‌ها کاهش می‌دهند.

۱۱-۴-۲- مکانیزمهای لبه‌ای

این مکانیزمها بر روی واسط کاربر- شبکه عمل کرده و به دو دسته تقسیم می‌شوند. نظارت^۲ و شکل‌دهی^۳. این دو دسته مشابه هم هستند با این تفاوت که مکانیزمهای شکل‌دهی، در سمت شبکه و مکانیزمهای نظارت، در سمت کاربر عمل می‌کنند.

مکانیزمهای شکل‌دهی، نرخ تولید ترافیک کاربر را با نرخی که قبلاً بین کاربر و شبکه توافق شده بود منطبق می‌کنند. اگر منبعی، ترافیکی با نرخی بیش از آنچه در قراردادش مشخص شده ارسال نماید، شکل‌دهنده، ترافیک وارده را ذخیره کرده و آنرا بگونه‌ای به شبکه می‌فرستد که از مقادیر مشخص شده در قرارداد ترافیکی پیروی کند. در این مکانیزم، بسته‌های متخلف، دور ریخته نمی‌شوند. مکانیزمهای نظارت، که در سمت کاربر اجرا می‌شوند چک می‌کنند که آیا ترافیک تولید شده توسط کاربر با قرارداد آن با شبکه، تطابق دارد یا نه. در صورت عدم تطابق، مکانیزم به نحوی عمل می‌کند که ترافیک را با قرارداد منطبق سازد. در صورتیکه منبع ترافیک از نرخ ترافیک توافق شده تجاوز کند، دو کار توسط این مکانیزمها اجرا می‌شود:

- دور ریختن بسته، که در آن بسته‌های متخلف دور ریخته می‌شوند.
- علامت زدن بسته، که در آن بسته‌های متخلف توسط شبکه علامت^۴ زده می‌شوند تا در صورت بروز تراکم، اولین بسته‌هایی باشند که دور ریخته می‌شوند.

۱۱-۴-۳- مکانیزمهای میانی

این مکانیزمها در نودهای میانی شبکه، مانند مسیریابها و سوئیچها اجرا می‌شوند و به دسته‌های زیر طبقه‌بندی می‌گردند:

۱. بافر کردن: وقتی که ترافیک ورودی به یک مسیریاب، بیشتر از ظرفیت اتصال خروجی باشد، بسته‌ها بطور موقت، در محلی به نام بافر ذخیره می‌گردند. دو ساختار برای بافر کردن وجود دارد:

- بافر مشترک
- بافر به ازای هر جریان^۵.

در ساختار بافر مشترک، یک حافظه فیزیکی معمولی بین کلیه بسته‌های بافر شده به اشتراک گذاشته می‌شود. هر زمان که اتصال خروجی آزاد شود، بسته‌ها توسط زمانبند از بافر خارج می‌شوند.

Call Admission Control

^۱ policing

^۲ shaping

mark

per flow buffer

ساختار بافر به ازای هر جریان بخش مشخصی از حافظه را به بسته های ورودی از هر جریان اختصاص می دهد. این بخشهای حافظه در مسیریابها معمولاً صف نامیده می شوند.

مزیت ساختار بافر به ازای هر جریان این است که از تاثیر منبع حریص^۱ بر روی بقیه منابع شبکه جلوگیری می کند. از طرف دیگر، ساختار بافر مشترک از لحاظ پیاده سازی بسیار ساده است. یکی از مزایای بافر کردن این است که بهره وری شبکه بالا می رود؛ چرا که از لحاظ منطقی هر چه بافر بزرگتر باشد حجم داده انتقال یافته توسط شبکه بالاتر می رود.

۲. مدیریت صف^۲: مکانیزمهای مدیریت صف، مکانیزمهایی هستند که در صورت سرریز بافر، بسته ای را که باید دور ریخته شود انتخاب می کنند. هر صف، یک مکانیزم مدیریت صف مربوط به خود دارد. مکانیزمهای مدیریت صف در فصل چهارم بطور مفصل بیان خواهند شد.

۳. زمانبندی^۳: زمانبند، بسته بعدی را از میان بسته هایی که در بافرها قرار دارند انتخاب و به درگاه خروجی می فرستد. کار زمانبند در صورتی که ساختار بافر اشتراکی باشد، ساده است. چرا که زمانبند فقط باید بسته ای که بیشترین زمان انتظار را دارد انتخاب کند. عمل زمانبندی با وجود ساختار بافر به ازای هر جریان بسیار پیچیده تر می شود. مکانیزمهای زمانبندی بطور مفصل در فصل ششم بررسی می شوند.

برای پیاده سازی سرویس های جدید اینترنت، عده ای براین عقیده هستند که در آینده ای نزدیک تکنولوژی فیبرنوری و WDM^۴ آنقدر رشد خواهد کرد که اینترنت به طور کامل بر مبنای آن پیاده سازی خواهد شد و عملاً مشکل پهنای باند و همچنین تضمین کیفیت سرویس وجود نخواهد داشت. عقیده دوم که ظاهراً درست تر از عقیده اول می باشد، این است که با وجود گسترش فناوری های انتقال و افزایش پهنای باند، هنوز به مکانیزم هایی برای تضمین کیفیت سرویس کاربران نیاز می باشد. در حال حاضر اکثر تولیدکنندگان مسیریاب و سوئیچ های شبکه اینترنت، در حال بررسی و افزودن مکانیزم هایی برای تضمین کیفیت سرویس در محصولات خود می باشند.

همانطور که اشاره شد، کاربردهای جدید اینترنت دارای نیازمندی های متفاوت می باشند. سرویس های صوتی نیاز به تاخیر و تغییرات تاخیر کم دارند و در مقابل اتلاف بسته ها تاحدی تحمل دارند. سرویس های داده، تاخیر و تغییرات تاخیر بالایی را تحمل می کنند ولی نسبت به اتلاف بسته ها حساس می باشند. سرویس های ویدئو نسبت به سرویس های صوت تاخیر و تغییرات تاخیر بیشتری را تحمل می کنند ولی اتلاف بسته ها در آنها باعث کاهش محسوس کیفیت سرویس می شود. سرویس های ویدئویی interactive نیاز به تاخیر و اتلاف کم دارند ولی تغییرات تاخیر زیاد را تحمل می کنند. از سوی IETF مدل ها و مکانیزم های مختلفی برای تضمین کیفیت سرویس مورد تقاضای کاربران ارائه شده است. سه مدل عمده تضمین کیفیت سرویس در اینترنت عبارتند از:

۱. سرویس های مجتمع (Intserv^۵): در مدل سرویس های مجتمع برای کاربردهای زمان حقیقی قبل از ارسال هرگونه داده، ابتدا باید با کمک پروتکل سیگنالینگ یک مسیر اولیه بین مبدا و مقصد برقرار شود و منابع لازم (در صورت وجود) در مسیر فوق رزرو گردد. از پروتکل RSVP^۶ برای رزرو منابع برای کاربردهای زمان حقیقی در اینترنت استفاده می شود.

greedy

^۱queue management^۲scheduling

Wavelength Division Multiplexing

Integrated services

ReSource reserVation Protocol

۲. سرویس های جداشده ($Diffserv^1$): در مدل سرویس های جداشده، جهت ارائه سرویس های جداشده به کاربران، بسته های کاربران در لبه ورودی شبکه کلاس بندی^۲ می شود و بدین ترتیب کلاس های سرویس متنوعی به کاربران ارائه می گردد.
۳. $MPLS^3$: در پروتکل MPLS به بسته های ورودی به شبکه یک برچسب کوتاه الحاق می گردد و سپس با توجه به مقدار برچسب فوق، عملیات مسیریابی درون شبکه انجام می شود.
۴. مهندسی ترافیک

۱۱-۴-۴- سرویس مجتمع و RSVP

سرویس مجتمع علاوه بر سرویس "بهترین تلاش"، دو کلاس سرویس دیگر زیر را نیز پشتیبانی می نماید. این دو کلاس سرویس عبارتند از:

الف - سرویس تضمین شده^۴: این نوع سرویس برای کاربردهایی که نیاز به تأخیر اندک و محدودی دارند مناسب می باشد.

ب - سرویس بارکنترل شده^۵: در کاربردهایی که به اطمینان زیاد نیاز می باشد، از این نوع سرویس استفاده می شود.

پروتکل RSVP به عنوان یک پروتکل سیگنالینگ برای رزرو منابع در اینترنت استفاده می شود. در شکل (۱۱-۴) مثالی از عملیات سیگنالینگ RSVP نشان داده شده است. مطابق با شکل فوق، فرستنده ابتدا پیام PATH را ارسال می کند. در این پیام مشخصات و مشخصه های ترافیکی فرستنده موجود می باشند. هر مسیریاب شبکه با دریافت پیام PATH، با کمک جدول مسیریابی خود پیام را هدایت می نماید، تا این که پیام به مقصد نهایی برسد. گیرنده نهایی بعد از دریافت پیام PATH، پیام RESV را ارسال می دارد. از طریق این پیام درخواست رزرو منابع برای جریان ترافیکی بین فرستنده و گیرنده به اطلاع شبکه رسانده می شود. مسیریاب های میانی، پیام RESV را از خود عبور می دهند و منابع لازم شامل پهنای باند و فضای بافر را به ارتباط جدید اختصاص می دهند. چنانچه یکی از مسیریاب های موجود در مسیر، قادر به قبول پیام RESV نباشد، آن را رد می نماید و پیام خطایی به گیرنده ارسال می کند و سپس عملیات سیگنالینگ خاتمه می یابد. با قبول پیام RESV از جانب هر مسیریاب موجود در مسیر، اطلاعات وضعیت مربوط به جریان ترافیکی فوق ثبت می شود.

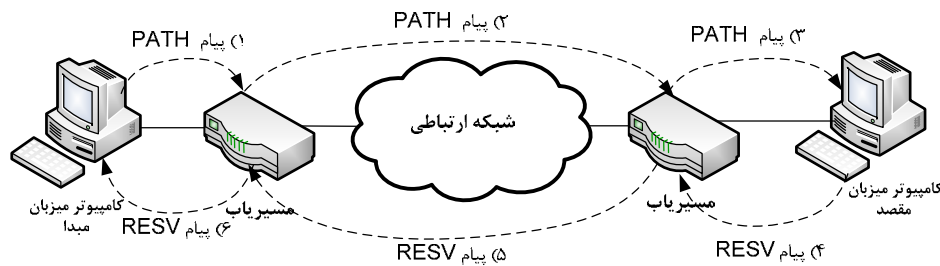
اخیراً پروتکل بهبود یافته RSVP ارائه شده است که امکان ایجاد مسیرهای صریح با کیفیت سرویس معین برای ترافیک های ترکیبی و همچنین امکان انجام سایر عملیات سیگنالینگ در آن وجود دارد. سرویس مجتمع دارای چهار قسمت بنیادی زیر می باشند:

الف) پروتکل سیگنالینگ مثل RSVP

ب) روتین کنترل دسترسی^۶

ج) کلاس بند^۷ جریان های ترافیکی

د) زمان بند بسته^۸



شکل (۱۱-۴): مثالی از عملیات سیگنالینگ RSVP

در سرویس تضمین شده و سرویس بار کنترل شده، قبل از ارسال هرگونه داده ای، باید یک مسیر اولیه بین مبدأ و مقصد برقرار شود و منابع مورد نیاز رزرو گردند. روتین کنترل دسترسی موظف به تصمیم گیری در مورد قبول یا رد درخواست رزرو منابع می باشد. با ورود هر بسته به مسیرهای شبکه، واحد کلاس بند بسته ورودی را به یک کلاس خاص طبقه بندی می نماید و سپس بسته ورودی را در یک صف خاص قرار می دهد. عملیات زمان بندی بسته ها در هر صف موجود در مسیر، توسط واحد زمان بند بسته، طوری انجام می گردد که کیفیت سرویس مورد نظر تأمین شود. سرویس مجتمع دارای مشکلات زیر می باشد:

- میزان اطلاعات وضعیت، متناسب با تعداد جریان های ترافیکی افزایش می یابد. بنابراین برای نگهداری اطلاعات وضعیت در مسیرهای شبکه نیاز به حافظه زیادی می باشد. همچنین بالاسری عملیات مسیرها به شدت افزایش می یابد. بنابراین قابلیت مقیاس پذیری در ساختار سرویس مجتمع به هیچ وجه مشاهده نمی گردد.
- هر مسیر نیاز به پروتکل RSVP، روتین کنترل کننده دسترسی، طبقه بندی کننده جریان ترافیکی و زمان بند بسته دارد. بنابراین می توان گفت که در سرویس مجتمع احتیاجات مسیرها به شدت زیاد می باشد.

۱۱-۴-۵- سرویس جداشده

به خاطر مشکلات پیاده سازی و توسعه سرویس مجتمع که در بالا به آنها اشاره شد، سرویس جداشده ارائه گردید. در سرآیند بسته های IPv4 فیلدیک بایتی به نام نوع سرویس (TOS¹) وجود دارد. در این فیلد سه بیت مختلف موجود هستند که برنامه های کاربردی با استفاده از این سه بیت قادر به تعیین نیازهای خود می باشند. سه بیت فوق عبارتند از :

- بیت D: نیاز به تأخیر کم
- بیت R: نیاز به نرخ اتلاف کم (اطمینان بالا)
- بیت T: نیاز به گذردهی بالا

در سرویس جداشده، فیلد نوع سرویس به فیلد DS² تغییر نام کرده است. با کدگذاری های مختلف فیلد DS و پردازش بسته ها بر اساس مقدار فیلد فوق، می توان کلاسهای سرویس متنوعی را ایجاد نمود.

برای دسترسی به سرویس جداشده، لازم است که کاربران شبکه به یک توافق سطح سرویس (SLA³) با سرویس دهنده های اینترنت برسند. کلاسهای مختلف سرویس و میزان ترافیک هر کلاس در SLA مشخص می شود. SLA

می تواند به یکی از دوصورت ثابت و پویا بیان شود. در نوع ثابت، توافق ترافیکی بین کاربر و ISP ثابت می باشد، در حالی که در نوع پویا، با استفاده از پروتکل سیگنالینگ (مثل RSVP) سرویس مورد نظر کاربر متناسب با تقاضای آن قابل تنظیم است. براساس سطح سرویس توافق شده بین کاربر و شبکه، در ورودی به شبکه، بسته های ورودی کاربران طبقه بندی، نظارت و در صورت لزوم شکل دهی می گردند. همچنین میزان بافر مورد نیاز جریان ترافیکی کاربر از اطلاعات موجود در SLA استخراج می شود. با کمک عملیات کلاس بندی، نظارت، شکل دهی و زمان بندی که در DS اجرا می شود، می توان به سرویس جداشده زیر دسترسی پیدا کرد.

- **سرویس ممتاز^۱**: برای کاربردهایی که به تأخیر و تغییرات تأخیر کم نیاز می باشد.
- **سرویس مطمئن^۲**: برای کاربردهایی که به اطمینان بالا نیاز می باشد.
- **سرویس المپیک**: این سرویس خود به سه دسته سرویس طلایی، نقره ای و برنزی تقسیم بندی می شوند که به ترتیب ذکر شده کیفیت سرویس در آنها کاهش می یابد.

بین سرویس مجتمع و سرویس جداشده، تفاوت های بنیادی زیر وجود دارد:

- با توجه به این که در سرویس جداشده تعداد کلاس های سرویس که توسط فیلد DS مشخص می شود، بسیار محدود است، بنابراین برخلاف سرویس مجتمع، میزان اطلاعات وضعیت متناسب با تعداد کلاس های سرویس می باشد، نه تعداد جریان های ترافیکی. این امر سبب قابلیت مقیاس پذیری بالاتر سرویس جداشده نسبت به سرویس مجتمع می شود.
 - عملیات کلاس بندی، نشانه گذاری، نظارت و شکل دهی فقط باید درمرز شبکه انجام شود. بنابراین پیاده سازی و اعمال سرویس جداشده ساده تر از سرویس مجتمع است.
- برای پیاده سازی سرویس مطمئن، ابتدا توسط مسیریاب ورودی شبکه عملیات کلاس بندی و نظارت صورت می گیرد. چنانچه ترافیک ورودی از آنچه که در SLA آمده است، بیشتر باشد در این صورت ترافیک ورودی متخلف است و درغیراین صورت نامتخلف می باشد. تمام بسته های ورودی و خروجی دریک صف قرار می گیرند و توسط مکانیزم های صف بندی مناسب، مدیریت می شوند.

سرویس ممتاز برای کاربرانی که ترافیک تولیدی آنها دارای حداکثر نرخ بیت ثابتی می باشند، تأخیر و تغییرات تأخیر کمی را تضمین می نماید. هر کاربر دارای یک توافق ترافیکی SLA با سرویس دهنده خود می باشد. در SLA حداکثر نرخ بیت مجاز کاربر قید شده است و کاربر موظف به رعایت آن می باشد. چنانچه نرخ بیت ارسال کاربر از حداکثر مجاز تجاوز نماید، در این صورت ترافیک های اضافی از بین می روند. شبکه نیز متعهد می شود که پهنای باند مورد نیاز کاربر را تامین نماید. در کاربردهایی مانند تلفن اینترنتی، کنفرانس ویدئویی، ایجاد خطوط استیجاری مجازی و شبکه های خصوصی مجازی (VPN) از سرویس ممتاز استفاده می شود.

در فصل ۱۱، سرویس جداشده به طور کامل بررسی می شوند.

۱۱-۴-۶- مهندسی ترافیک و مسیریابی مبتنی بر قید

عواملی مانند کمبود منابع کافی در شبکه و همچنین توزیع نادرست بار ترافیکی در شبکه، باعث ایجاد تراکم در شبکه می گردند. چنانچه منابع کافی در شبکه موجود نباشد در این صورت تمام مسیریاب های موجود در شبکه دچار تراکم و ازدحام باری شوند، که تنها راه حل مناسب آن، افزودن منابع دیگر به شبکه می باشد. اگر بار ترافیکی به طور مناسب و صحیح در شبکه توزیع نشود، در این صورت برخی از مناطق شبکه دچار تراکم می شوند، در حالی که در برخی نقاط دیگر هیچگونه

تراکمی مشاهده نمی شود. از آنجائی که اکثر پروتکل های مسیریابی دینامیکی از الگوریتم کوتاهترین فاصله استفاده می نمایند، بنابراین امکان ایجاد تراکم در برخی مسیرها و عدم وجود تراکم در مسیرهای دیگر شبکه وجود دارد. البته روش بهبود یافته $ECMP^1$ به شرط آن که بیش از یک مسیر به عنوان کوتاهترین مسیر موجود باشد، تاحدی مشکل فوق را در پروتکل مسیریابی دینامیکی OSPF حل می نماید. همچنین به عنوان یک راه حل دیگر می توان هزینه هر کانال شبکه را به صورت دستی تغییر داد تا عملیات تقسیم بار صورت گیرد؛ اما طبیعی است این راه حل برای شبکه های وسیع عملی نمی باشد.

با کمک روال هایی که در مهندسی ترافیک در نظر گرفته شده است، می توان تاحد زیادی از ایجاد تراکم در شبکه جلوگیری نمود. مسیریابی مبتنی بر قید یک روش برای مهندسی ترافیک و جلوگیری از تراکم در شبکه است. در مسیریابی مبتنی بر قید، با استفاده از چندین مشخصه مختلف، مسیرهای موجود بین مبدأ و مقصد محاسبه می شوند. درحقیقت مسیریابی مبتنی بر قید تکمیل یافته مسیریابی مبتنی بر کیفیت سرویس² می باشند. در مسیریابی مبتنی بر کیفیت سرویس، کلیه مسیرهایی که کیفیت سرویس مورد نظر کاربر را برآورده می نمایند، محاسبه می شوند. مسیریابی مبتنی بر قید، تکمیل یافته مسیریابی مبتنی بر سرویس می باشد که در آن سایر محدودیت های شبکه، مانند نظارت بر ترافیک نیز در نظر گرفته شده است. با استفاده از مسیریابی مبتنی بر قید، امکان انتخاب مسیرهایی با کیفیت سرویس مورد نظر و همچنین افزایش میزان بهره وری شبکه فراهم می آید. در مسیریابی مبتنی بر قید، در هنگام محاسبه مسیرهای موجود، نه تنها از توپولوژی شبکه بلکه از مشخصه های دیگری مانند نیازهای جریان های ترافیکی، میزان ظرفیت موجود در کانال های شبکه و سایر نظارت های لازم که توسط مدیر شبکه تعیین می شود، در نظر گرفته می شوند. بنابراین در مرحله اول ممکن است که مسیر محاسبه شده توسط الگوریتم مسیریابی مبتنی بر قید طولانی تر از مسیرهای دیگر باشد ولی مطمئناً مسیر محاسبه شده دارای سبکترین بار ترافیکی است و نیازهای کاربر را به خوبی برآورده می نماید.

همانند پروتکل های مسیریابی دینامیکی، برای محاسبه بهترین مسیر ممکن توسط الگوریتم مبتنی بر قید باید مسیریاب های شبکه به طور متناوب اطلاعات وضعیت کانال را بین یکدیگر مبادله نمایند.

در مسیریابی مبتنی بر قید، مشابه سایر روش های مسیریابی، اولین مسئله مهم، انتخاب معیار اندازه مورد نظر برای مسیرهای موجود در شبکه می باشد. معیارهای متداول اندازه در مسیریابی مبتنی بر قید عبارتند از: هزینه، تعداد پرشها، پهنای باند، اطمینان، تأخیر و تغییرات تأخیر. مسیریاب انتخاب شده الگوریتم های مسیریابی، یک یا چند معیار اندازه فوق را بهینه می نماید.

فرض کنید که $d(i,j)$ ، که در آن i و j شماره نودهای شبکه می باشند که توسط یک کانال به هم متصل شده اند، نشان دهنده معیار اندازه کانال (i,j) باشد. برای هر مسیر $p = (i,j,k,\dots,l,m)$ ، معیار اندازه d به یکی از سه صورت زیر محاسبه می شود:

$$d(p) = d(i,j) + d(j,k) + \dots + d(l,m) \quad \bullet \text{ جمع}$$

$$d(p) = d(i,j) * d(j,k) * \dots * d(l,m) \quad \bullet \text{ ضرب}$$

$$d(p) = \min \{ d(i,j), d(j,k), \dots, d(l,m) \} \quad \bullet \text{ مقعر}^3$$

چنانچه از چندین معیار اندازه فوق به صورت ترکیبی برای محاسبه مسیر بهینه استفاده شود، در این صورت پیچیدگی عملیات تولید جدول های مسیریابی به شدت زیاد می گردد. اگر از معیار اندازه های پهنای باند و یا تعداد پرش، در محاسبه

مسیر بهینه استفاده شود، در این صورت به خاطر وجود الگوریتم‌هایی مانند الگوریتم Bellman-Ford و Dijkstra محاسبات مسیریابی نسبتاً ساده می‌باشند.

در مسیریابی مبتنی بر قید، می‌توان در لحظه دریافت تقاضای کاربر و یا از قبل، مسیر لازم را تعیین نمود. در مسیریابی مبتنی بر قید بسامد محاسبه مسیرها به مراتب نسبت به سایر روش‌های دینامیکی بیشتر می‌باشد. دلیلی که می‌توان برای این مطلب آورد، این است که در مسیریابی دینامیکی تنها با تغییر توپولوژی شبکه، مسیرهای جدید محاسبه می‌شوند ولی در مسیریابی مبتنی بر قید، تغییرات پهنای باند نیز منجر به محاسبه مسیرهای جدید در جدول مسیریابی می‌گردند. بنابراین می‌توان نتیجه گرفت که پیچیدگی روش مسیریابی مبتنی بر قید به مراتب بیشتر از مسیریابی دینامیکی می‌باشد. برای محاسبه جدول‌های مسیریابی و کاهش پیچیدگی مسیریابی مبتنی بر قید، می‌توان از روش‌های پیشنهادی زیر استفاده نمود:

الف) استفاده از یک زمان سنج طولانی برای کاهش بسامد محاسبات

ب) استفاده از معیار اندازه پهنای باند و تعداد جهش

ج) استفاده از سیاست‌های مدیریت برای حذف برخی از کانال‌هایی که به هر دلیل مورد قبول نمی‌باشند. مثلاً اگر یک ارتباط نیاز به تأخیر کم داشته باشد، قبل از انجام مسیریابی، ابتدا تمام کانال‌هایی که تأخیر بالایی دارند، حذف می‌شوند و سپس مسیریابی انجام می‌شود.

ذکر این نکته ضروری می‌باشد که مسیریابی مبتنی بر قید دارای مشکلات زیادی است که عبارتند از:

- بالاسری زیاد در محاسبه مسیر
- افزایش اندازه جدول مسیریابی
- احتمال عدم پایداری
- بهینه نبودن مسیر انتخابی از نظر میزان مصرف منابع

۱۱-۵- مجتمع سازی IP و ATM

با گسترش سریع شبکه‌های مبتنی بر IP و همچنین با توجه به ویژگی‌های منحصر به فرد فن‌آوری ATM، تاکنون پیشنهاد‌های مختلف و فعالیت‌های زیادی در زمینه پیاده سازی IP بر روی ATM صورت گرفته است.

یکی از اولین و مهم‌ترین مشکلات پیاده سازی IP بر روی ATM، عملکرد متفاوت این دو فن‌آوری می‌باشد. IP یک پروتکل "بهترین تلاش" و بی‌اتصال است، در حالی که ATM از نوع اتصال گرا می‌باشد و کیفیت سرویس اتصال‌ها را به خوبی تضمین می‌نماید. در جدول (۱۱-۲) از جنبه‌های مختلف، IP و ATM با یکدیگر مقایسه شده‌اند.

با استفاده از فن‌آوری ATM، امکان استفاده از سرویس جداسده صوتی، تصویری و داده‌ای، فراهم می‌آید. از طرف دیگر، IP قدمت چندین ساله دارد و در این مدت فعالیت‌ها و نرم‌افزارهای زیادی بر پایه IP طراحی و پیاده سازی شده است. بنابراین اکثر شرکت‌های مخابراتی و متخصصان شبکه، یکی از راه‌حل‌های پیاده سازی نسل آینده اینترنت را ارسال ترافیک‌های IP بر روی شبکه فیزیکی ATM می‌دانند.

در شبکه‌های رایانه‌ای دو فن‌آوری مختلف سوئیچینگ بسته‌ای و سوئیچینگ مداری وجود دارند. میزان بهره‌وری از منابع شبکه در سوئیچینگ بسته‌ای، به خصوص در حالتیکه ترافیک‌های ارسالی کاربران از نوع انفجاری می‌باشد، به مراتب بالاتر از سوئیچینگ مداری است. اما مهم‌ترین برتری سوئیچینگ مداری آن است که امکان تضمین کیفیت سرویس در شبکه‌های سوئیچینگ مداری وجود دارد.

جدول (۱۱-۲): مقایسه ATM و IP

عنوان	IP	ATM
قالب داده های ارسالی	بسته	سلول
نحوه هدایت بسته ها	مسیریابی لایه سوم	سوئیچینگ لایه دوم
نوع عملکرد	"بهترین تلاش"	رزرو منابع
نحوه مسیریابی	پرش به پرش	مسیریابی مبدأ
نوع اتصالات	نقطه به نقطه، چندپراکنی/داده پراکن	نقطه به نقطه، نقطه به چند نقطه
نحوه عملکرد	بدون اتصال	اتصال گرا

با توجه به این که IP و ATM از دونوع سوئیچینگ مختلف که در بالا به آن اشاره شد، استفاده می نمایند، در ترکیب و مجتمع سازی این دو نوع فن آوری یکسری مشکلاتی وجود دارد. برای رفع مشکلات فوق و پیاده سازی IP بر روی ATM، تاکنون از سوی IETF، انجمن ATM و سایر شرکت های مخابراتی، روش های مختلفی ارائه شده است که عبارتند از: LANE¹، مدل کلاسیک پیاده سازی IP بر روی ATM²، MPOA²، NHRP³، I-PNNI⁴ و MPLS. هریک از روش های فوق، دارای ویژگی ها و مشخصات خاصی می باشند، ولی مطمئناً کاملترین روش پیاده سازی IP بر روی ATM، فن آوری MPLS است که به بررسی اجمالی آن می پردازیم.

MPLS ۱۱-۵-۱

MPLS در حقیقت ترکیبی از سوئیچینگ لایه دوم (لایه پیوند داده) با مسیریابی لایه سوم (لایه شبکه) می باشد، که هدف اصلی آن ایجاد یک فابریک انعطاف پذیر شبکه با کارایی و مقیاس پذیری بالا است. MPLS وابسته به پروتکل لایه دوم خاصی نمی باشد ولی پیاده سازی های اولیه آن بر روی ATM و Frame Relay صورت گرفته است. در اوایل سال ۱۹۹۷، گروه مطالعاتی MPLS که در آن مراکز ارائه دهنده سرویس زیادی عضویت دارند، شروع به فعالیت نمود که هدف اصلی آن پاسخ گویی و رفع نیاز مشکلات فراوان موجود در اینترنت فعلی می باشد. برخی از مهم ترین اهداف MPLS که در شبکه اینترنت فعلی وجود ندارد عبارتند از:

- ایجاد یک شبکه IP با قابلیت مقیاس پذیری بالا، برای رفع نیازهای رو به افزون ترافیک های اینترنت
 - فراهم سازی سرویس مبتنی بر IP
 - ترکیب ترافیک های مختلف بر روی یک شبکه IP واحد
 - بهبود سازی بازدهی عملیاتی شبکه در یک محیط رقابتی
- قبل از پیدایش MPLS از طرف برخی شرکت های مخابراتی راه حل های دیگری برای نیل به اهداف فوق ارائه گردید که عبارتند از:

- سوئیچینگ IP پیشنهادی شرکت (Nokia) Ipsilon
- سوئیچینگ نشانه^۵ پیشنهادی شرکت Cisco
- ARIS^۶ پیشنهادی شرکت Toshiba

• IP Navigator پیشنهادی Cascade Communication

در مقایسه با راه حل های فوق، MPLS کاملترین و بهترین راه حل می باشد که قادر به پشتیبانی از پروتکل های مختلف لایه شبکه و لایه پیوند داده است. با وجود این فعالیت های اولیه در زمینه پیاده سازی MPLS بر روی ترکیب IPv4 به عنوان پروتکل لایه شبکه و ATM یا Frame Relay به عنوان پروتکل لایه پیوند داده، صورت گرفته است.

در ابتدای پیدایش فن آوری ATM، تصور همگان بر این بود که با توجه به ویژگی های منحصر به فرد ATM در آینده شاهد یک شبکه کاملاً مبتنی بر ATM خواهیم بود. اما با گسترش IP و شبکه های مبتنی بر آن، این ایده به تدریج نادرست گردید. تصور فعلی بر این است که در نسل آینده شبکه ها از مزایای فن آوری های موجود مانند IP و ATM به نحو شایسته ای استفاده می شود.

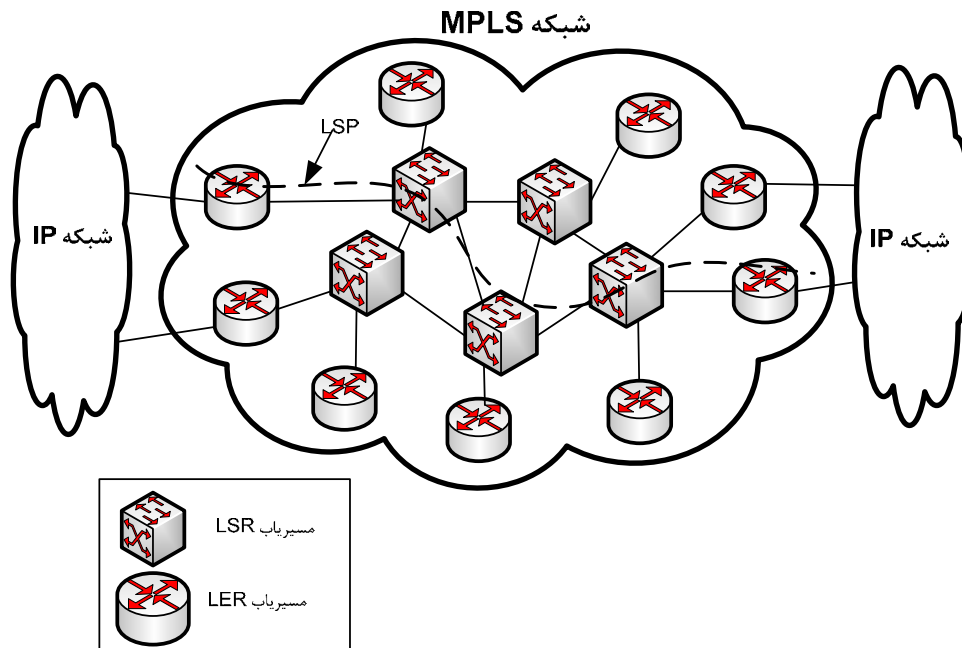
MPLS نتیجه ترکیب و استفاده توأم از مزایای فن آوری های سوئیچینگ لایه دوم و مسیریابی لایه سوم می باشد. طبیعی است که این نوع شبکه، به دلیل استفاده همزمان از فن آوری های سوئیچینگ و مسیریابی، بهترین راه حل برای استفاده همزمان از IP و ATM می باشد. در این زمینه، همان طور که قبلاً نیز اشاره گردید استانداردهای متعددی مانند IP over ATM پیشنهادی IETF و MPOA پیشنهادی انجمن ATM برای ترکیب IP و ATM ارائه شده اند.

در حالت کلی، فن آوری MPLS، فقط به IP و ATM محدود نمی شود، بلکه MPLS نحوه یکپارچه سازی فن آوری های لایه دوم و لایه سوم را توصیف می نماید. در MPLS یک سری روال ها برای استفاده از قابلیت های سوئیچینگ سریع ATM و Frame Relay در شبکه های IP توصیف شده است.

در شبکه های MPLS به هریک از بسته های IP ورودی توسط مسیریاب های موجود در لبه شبکه، یک برچسب متصل می شود. درون شبکه MPLS، هدایت بسته ها به مقصد به وسیله پردازش بر روی فیلد برچسب انجام می شود. در لبه خروجی شبکه MPLS، برچسب اضافه شده به بسته حذف می شود و بسته IP تحویل مقصد می گردد.

شکل (۱۱-۵)، مثالی از یک شبکه MPLS و تجهیزات آن را نشان می دهد. مطابق با شکل فوق، مسیریاب هایی که در لبه شبکه قرار گرفته اند و با استفاده از اطلاعات مسیریابی IP، به بسته های ورودی یک برچسب خاص اختصاص می دهند که با نام LER¹ شناخته می شوند. همچنین مسیریاب های داخل شبکه MPLS که تنها وظیفه آنها پردازش بسته های IP برچسب زده شده و هدایت آنها به سمت مقصد است، به نام LSR² مشهور می باشند. مطابق با شکل فوق، به مسیری که بسته های IP از طریق آن مسیر به سمت مقصد ارسال می شوند، LSP³ گفته می شود.

با گسترش اینترنت و سرویس آن به خصوص سرویس مبتنی بر وب اکثر ISP ها به سمت ایجاد شبکه های یکپارچه IP متمایل شده اند. برای نیل به سرویس جدید اینترنت، لزوم تحول و تغییرات در معماری TCP/IP به خصوص پروتکل IP حس می گردد.



شکل (۱۱-۵): مثالی از یک شبکه MPLS

۱۱-۵-۱-۱- مسیریابی در IP

قبل از بررسی پروتکل MPLS، به بررسی اجمالی مسیریابی در IP می پردازیم. در سرآیند بسته های IP، اطلاعات لازم برای مسیریابی وجود دارد. مسیریابی IP، براساس مسیریابی مبتنی بر مقصد انجام می گیرد. این بدان معنی است که برای هدایت هر بسته IP به مقصد، سرآیند آن پردازش می شود و با توجه به آدرس مقصد و محتوای جدول مسیریابی، پرش بعدی بسته تعیین می شود و بسته IP ارسال می گردد. با توجه به اینکه که هر بسته IP به طور مستقل مسیریابی می گردد و از یک مسیر از قبل تعیین شده عبور نمی کند، بنابراین می توان گفت که شبکه به صورت بی اتصال عمل می کند. بعد از برقراری ارتباط همسایگی بین مسیریاب های شبکه، جدول های مسیریابی بین مسیریاب ها مبادله می گردند. به عنوان مثال، با توجه به شکل (۱۱-۶)، مسیریاب A دارای سه همسایه B, C, D می باشد در حالی که مسیریاب های B و C هر کدام دارای دو همسایه مجاور می باشند.

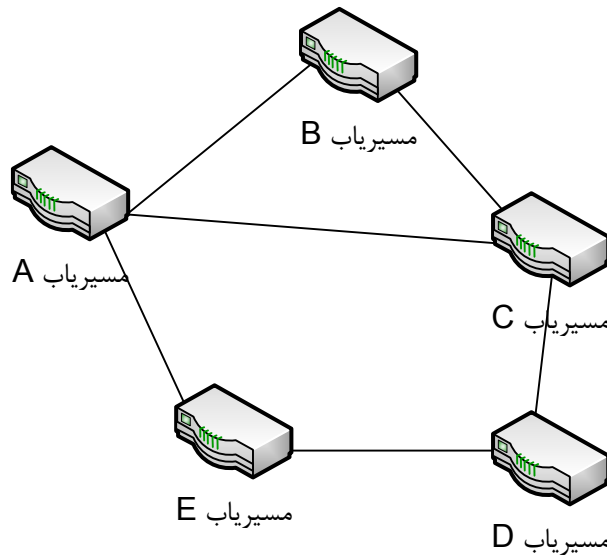
هر مسیریاب، بعد از دریافت بسته IP، باید پرش بعدی بسته را تعیین کند. با استفاده از پروتکل های مسیریابی دینامیکی مانند OSPF، هر مسیریاب قادر به فراگیری کل توپولوژی شبکه می باشد. با استفاده از اطلاعات به دست آمده از مسیریاب های مجاور، هر مسیریاب جدول های مسیریابی خود را کامل می نماید و بدین ترتیب قادر به تعیین پرش بعدی و هدایت بسته به سمت مقصد می باشد.

در شکل (۱۱-۷)، جزئیات مربوط به استفاده و نحوه به روزآوری جدول های مسیریابی آورده شده است. همان طور که در این شکل دیده می شود، عملیات مسیریابی به صورت نرم افزاری و سخت افزاری قابل پیاده سازی است.

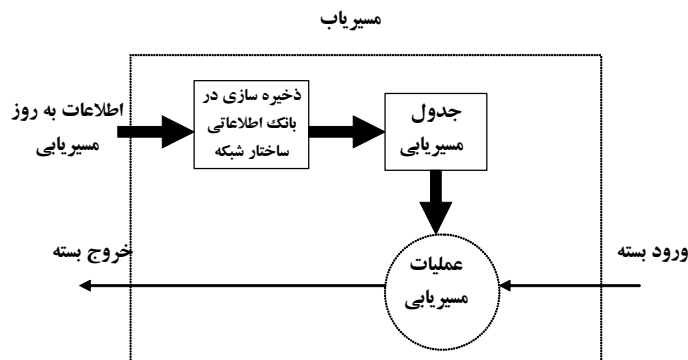
۱۱-۵-۱-۲- سوئیچینگ

با گسترش شبکه های مبتنی بر IP، سرویس دهنده های شبکه به این نتیجه رسیدند که چنانچه شبکه های آنها کاملاً مبتنی بر مسیریاب طراحی و توسعه یابد، مشکلات متعددی در شبکه به وجود خواهد آمد. برخی از این مشکلات عبارتند از:

- مشکلات موجود در قسمت نرم افزاری مسیریاب‌ها
- قیمت بالای مسیریاب‌های سریع IP
- مشکل بودن تخمین کارایی شبکه‌های وسیع مبتنی بر IP



شکل (۱۱-۶): یک شبکه مبتنی بر مسیریاب



شکل (۱۱-۷): نحوه استفاده و ایجاد جدول‌های مسیریابی

فن‌آوری‌های سوئیچینگ سریع در ATM و Frame Relay، از الگوریتم جابجایی برچسب^۱ استفاده می‌کنند. به خاطر سادگی الگوریتم فوق، امکان پیاده‌سازی سخت‌افزاری آن وجود دارد که باعث افزایش سرعت، کاهش قیمت و افزایش کارایی آن نسبت به مسیریاب‌های IP می‌گردد. فن‌آوری‌های ATM و Frame Relay هر دو به صورت اتصال‌گرا عمل می‌نمایند. بنابراین قبل از ارسال هرگونه داده، ابتدا یک اتصال اولیه بین مبدأ و مقصد به وجود می‌آید و داده‌های ارسالی

به طور کامل از یک مسیر مشخص ارسال می گردند. بنابراین در شبکه های اتصال گرا، امکان مدیریت و تخمین مشخصه ها فراهم می آید.

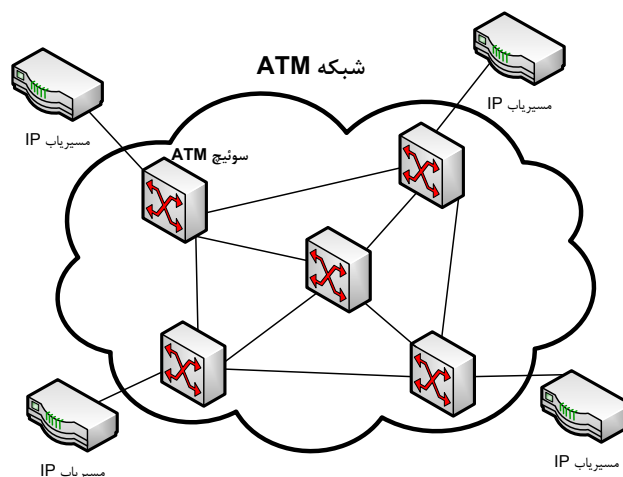
۱۱-۵-۱-۳- ترکیب مسیریابی و سوئیچینگ

برای استفاده از مزایای سوئیچینگ و رفع مشکلات مربوط به توسعه شبکه های مبتنی بر مسیریاب، از ترکیب مسیریاب و سوئیچ در توسعه شبکه های گسترده استفاده می شود. در این ساختار، مطابق با شکل (۸-۱۱)، مسیریابها در لبه های شبکه قرار می گیرند و اتصال بین آنها از طریق سوئیچ های شبکه صورت می گیرد. بنابراین امکان مدیریت و تخمین مشخصه ها فراهم می آید. به این نحوه مجتمع سازی IP و ATM، مدل پوشش^۱ گفته می شود.

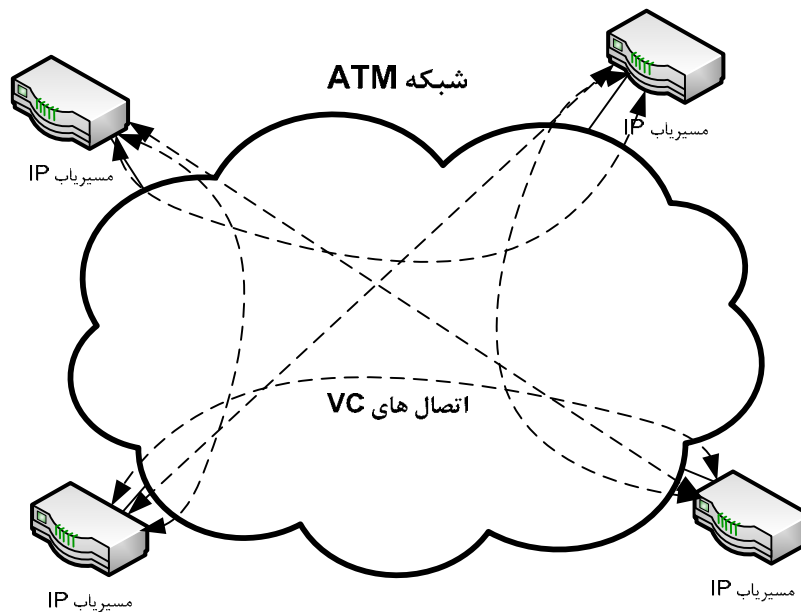
همان طور که قبلاً نیز اشاره شد، در شبکه های مبتنی بر مسیریاب، برای تبادل اطلاعات و جدول های مسیریابی، لازم است که مسیریاب های شبکه با یکدیگر ارتباط همسایگی برقرار نمایند. در ساختار شکل (۸-۱۱)، از طریق اتصال های بین سوئیچ ها (مثلاً VC در ATM)، ارتباط همسایگی برقرار می شود. در این حالت برای برقراری کامل اتصال بین مسیریابها، نیاز به ایجاد یک حلقه کامل VC می باشند. چنانچه تعداد مسیریابها در شبکه n تا باشد، به تعداد $n(n-1)/2$ اتصال VC برای برقراری ارتباط بین مسیریاب های شبکه نیاز است. طبیعی است که با افزایش n ، تعداد اتصال های لازم با توان دوم n افزایش می یابد، که این امر باعث پیچیدگی مدیریت شبکه می شود.

در شکل (۹-۱۱) یک شبکه با ۴ مسیریاب نشان داده شده است. در این شکل برای برقراری اتصال بین مسیریابها، به $4 \times (4-1) / 2 = 6$ اتصال VC نیاز است که این تعداد اتصال مورد نیاز، با افزایش تعداد مسیریابها به صورت توان ۲ افزایش می یابد.

با توجه به مطالب فوق، دیده می شود که مدل پوشش برای پیاده سازی IP بر روی ATM دارای ضعف زیادی در مقیاس پذیری می باشد که پروتکل MPLS تا حد زیادی این مشکل را رفع نموده است.



شکل (۸-۱۱): مدل پوشش برای مجتمع سازی IP و ATM



شکل (۹-۱۱): یک شبکه مجتمع شامل چهار مسیریاب IP

۱۱-۵-۲- تحول سوئیچینگ چند لایه در اینترنت

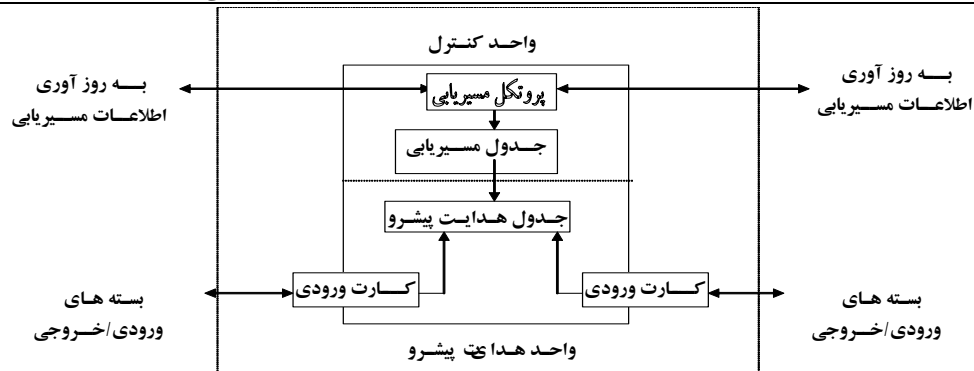
سوئیچینگ چند لایه، از ترکیب سوئیچینگ لایه دوم و مسیریابی لایه سوم به وجود می آید. مطابق با مدل پیشنهادی پوشش که در بالا آن را توضیح دادیم، برای گسترش اینترنت و برقراری ارتباط بین مسیریابها از سوئیچهای سریع ATM یا Frame Relay استفاده می شود. این سوئیچها عملیات سوئیچینگ سلول های ATM یا قابهای Frame Relay را در سطح لایه دوم انجام می دهند. یکی از مسائل اصلی مدل پوشش برای ترکیب فن آوری های IP و ATM، مشکل نگاهت بین دو معماری مختلف شبکه TCP/IP و ATM (یا Frame Relay) می باشد. این دو معماری از جنبه های مختلف مانند: مدیریت و نگه داری، فضای آدرس دهی، پروتکل های مسیریابی، پروتکل های سیگنالینگ و نحوه تخصیص منابع با یکدیگر متفاوت می باشند.

برای رفع مشکل فوق، سوئیچینگ چند لایه پیشنهاد شده است. در این راه حل که MPLS هم جزئی از آن می باشد، با ترکیب سوئیچینگ لایه دوم و مسیریابی لایه سوم، یک راه حل جامع برای ترکیب IP و ATM ارائه شده است. تکنیک سوئیچینگ چند لایه دارای دو ویژگی اصلی زیر می باشد:

- جداسازی واحد کنترل از واحد هدایت پیشرو^۱

- استفاده از الگوریتم جابجایی برچسب برای عملیات هدایت پیشرو

مطابق با شکل (۱۱-۱۰)، در سوئیچینگ چند لایه، دو واحد اصلی به نام واحد کنترل و واحد هدایت پیشرو به طور مجزا وجود دارند. وظیفه اصلی واحد کنترل، تبادل اطلاعات مسیریابی و به روز آوری جدول های مسیریابی با استفاده از پروتکل های استاندارد مسیریابی مانند OSPF، IS-IS و BGP-4 می باشد.



شکل (۱۱-۱۰): واحدهای تشکیل دهنده سوئیچینگ چند لایه

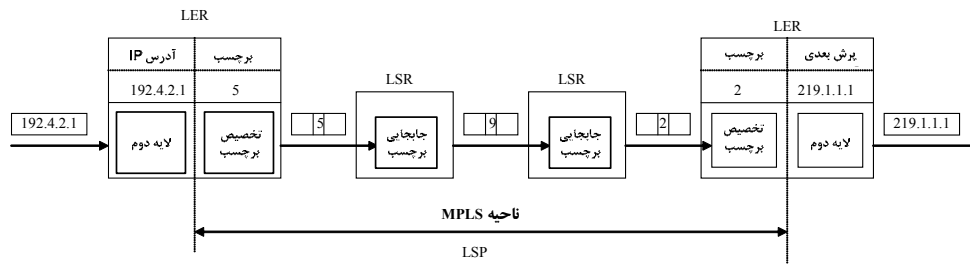
با ورود هر بسته به سوئیچهای چند لایه، واحد هدایت پیشرو با استفاده از جدول هدایت پیشرو و براساس اطلاعات موجود در سرآیند بسته ورودی، آن را مسیریابی و هدایت می نماید. جدول هدایت پیشرو توسط واحد کنترل، مدیریت و به روز آوری می گردد.

یکی از مزایای جداسازی واحد کنترل و واحد هدایت پیشرو، امکان توسعه و بهینه سازی هر یک از واحدهای فوق به طور مستقل و جداگانه می باشد. واحد هدایت پیشرو، برای هدایت بسته ها از الگوریتم جابجایی برچسب که مشابه الگوریتم مورد استفاده در ATM و Frame Relay است، استفاده می نماید. در این الگوریتم، سیگنالینگ و توزیع برچسبها از اهمیت بالایی برخوردار می باشد.

هر برچسب دارای طول ثابتی می باشد که در سرآیند بسته ها قرار می گیرد و از آن برای مشخص نمودن کلاس معادل هدایت پیشرو (FEC^1) استفاده می شود. فیلد برچسب، مشابه فیلدهای VPI/VCI در ATM و فیلد DLCI در Frame Relay می باشد. هر برچسب دارای اهمیت محلی می باشد و از آن برای نگاشت ترافیک های ورودی به یک کلاس FEC خاص استفاده می شود. هر FEC نشان دهنده مجموعه ای از بسته ها می باشد که از یک مسیر یکسان به سمت مقصد هدایت می شوند. این احتمال وجود دارد که بسته های متعلق به یک کلاس FEC خاص، دارای آدرس های مقصد یکسانی نباشند. به عنوان مثال در یک شبکه IP کلیه بسته هایی که بخش پیشوند آدرس IP مقصد آنها یکسان است، می توانند به یک کلاس FEC خاص تعلق داشته باشند.

در شبکه های سوئیچینگ چند لایه و MPLS، از مسیریاب های موجود در لبه ورودی به شبکه برای تعیین مقدار اولیه برچسب بسته های ورودی به شبکه استفاده می شود. در شکل (۱۱-۱۱)، مثالی از نحوه تخصیص برچسب به بسته های ورودی براساس آدرس مقصد آنها، آورده شده است.

همان طور که قبلاً نیز اشاره گردید، در شبکه های سوئیچینگ چند لایه و MPLS، مسیر موجود بین مبدأ و مقصد با نام LSP شناخته می شود. در هر LSP، اولین و آخرین سوئیچ برچسب به ترتیب با نام های سوئیچ برچسب ورودی و سوئیچ برچسب خروجی شناخته می شوند. سوئیچ های برچسب موجود درون شبکه، بدون توجه به محتویات سرآیند بسته ها و فقط براساس مقدار برچسب هر بسته و با کمک الگوریتم جابجایی برچسب، اقدام به هدایت بسته ها به سمت مقصد می نمایند.



شکل (۱۱-۱۱): مثالی از نحوه تخصیص برچسب

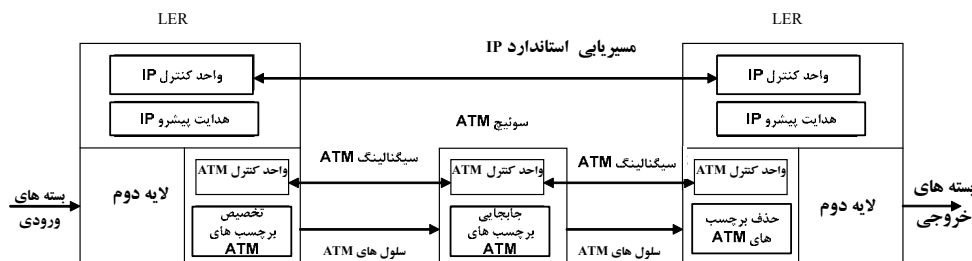
الگوریتم جابجایی برچسب نسبت به مسیریابی پرش به پرش لایه شبکه، دارای مزایای زیر می باشد:

- سوئیچ‌های برچسب در تخصیص بسته‌های ورودی به FEC ها، دارای انعطاف پذیری بالا می‌باشند.
- امکان اختصاص یافتن LSP مطابق با نیازهای لایه کاربرد وجود دارد. مثلاً می‌توان LSP را طوری تعیین کرد که تعداد پرش‌ها تا مقصد و یا میزان پهنای باند مورد استفاده حداقل گردد.
- مهم‌ترین برتری الگوریتم جابجایی برچسب، تخصیص ترافیک‌های مختلف به FEC و نگاشت FEC به LSP مناسب مطابق با نیازهای کاربران، می‌باشد.

در اواسط سال ۱۹۹۰، برخی از سرویس دهندگان اینترنت، شبکه‌های خود را از حالت کاملاً مبتنی بر مسیریاب خارج نمودند و از مدل پوشش برای اجرای IP بر روی ATM استفاده کردند. با گسترش ATM، ویژگی‌های منحصر به فرد آن مانند پهنای باند بالا، کارایی خوب و امکان استفاده از الگوریتم جابجایی برچسب، بسیار مورد توجه سرویس‌دهندگان اینترنت قرار گرفته است.

مطابق با شکل (۱۱-۱۲) در مدل پوشش برای پیاده سازی IP بر روی ATM، هر سوئیچ موجود در شبکه باید به نرم افزارهای کنترلی ATM (مانند سیگنالینگ و مسیریابی) و سخت افزار جابجایی برچسب مجهز باشد. در این مدل، تنها در مسیریاب‌های موجود در لایه شبکه، عملیات مسیریابی IP انجام می‌گیرد. همان‌طور که قبلاً نیز اشاره گردید این مدل دارای مشکلات متعددی می‌باشد که عبارتند از:

- عدم قابلیت مقیاس پذیری
- محدودیت پهنای باند ATM SAR
- بالاسری بالا
- نیاز به کانال‌های دائمی VC برای اتصال مسیریاب‌ها به یکدیگر
- عدم عملکرد بر روی مدل‌های غیر ATM

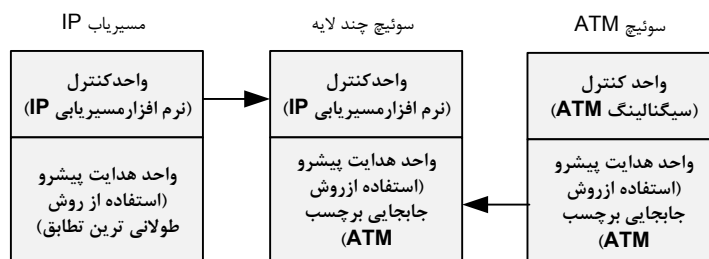


شکل (۱۱-۱۲): نحوه پیاده سازی IP بر روی ATM در مدل پوشش

با توجه به مشکلات زیاد مدل پوشش، از اواخر سال ۱۹۹۶ مدل های سوئیچینگ چند لایه که از ترکیب سوئیچینگ ATM و مسیریابی IP استفاده می کنند، ارائه شد. مهم ترین این مدل ها که قبلاً نیز به آنها ارائه شد، عبارتند از: مدل سوئیچینگ IP، مدل سوئیچینگ نشانه، مدل ARIS، مدل IP Navigator و مدل CSR¹.

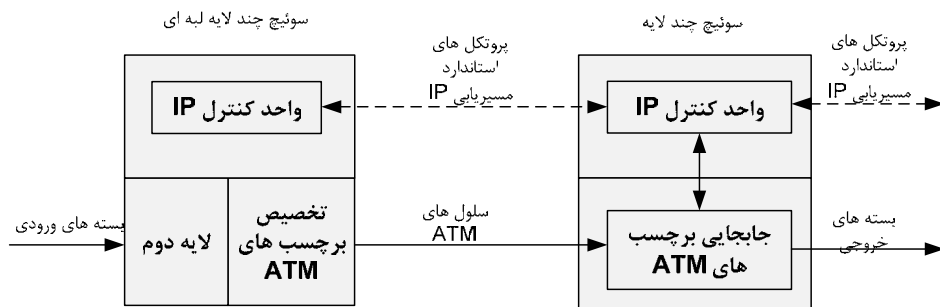
هرچند تمام مدل های پیشنهادی فوق از یک ایده اصلی استفاده می نمایند و از جنبه های مختلفی مشابه هم می باشند، اما عملاً قابلیت ارتباط بین آنها وجود ندارد. یکی از مهم ترین دلایل این امر آن است که مدل های فوق، از فن آوری های مختلف برای ترکیب مسیریابی IP با سوئیچینگ ATM استفاده می نمایند. ایده اصلی تمام روش های سوئیچینگ چند لایه، ترکیب بهترین ویژگی های مسیریابی IP و سوئیچینگ ATM می باشد. بدین منظور مطابق با شکل (۱۱-۱۳)، در سوئیچ های چند لایه از نرم افزارهای استاندارد مسیریابی IP مانند BGP-4، OSPF، IS-IS و سخت افزارهای جابجایی برچسب سوئیچ های ATM استفاده می شود.

با کمک نرم افزارهای مسیریابی IP، سوئیچ های چند لایه قادر به تبادل اطلاعات جدول های مسیریابی بین یکدیگر می باشند. با استفاده از مکانیزم نگاشت برچسب، کلید مسیره های لایه سوم به برچسب مناسب (مثل VPI/VCI در ATM) نگاشت می یابند و اطلاعات به دست آمده فوق، بین تمام سوئیچ های موجود در مسیر LSP مبادله می شوند. در سوئیچ های چند لایه، پروتکل مسیریابی در تمام سوئیچ های داخل شبکه اجرا می گردد، در حالی که در مدل پوشش، این عمل فقط در مسیریاب های موجود در لبه شبکه انجام می شود. بنابراین در سوئیچینگ چند لایه نسبت به مدل پوشش تعداد کانال های مورد نیاز برای اتصال مسیریاب های لبه شبکه به یکدیگر به شدت کاهش می یابد و همچنین پروتکل مسیریابی IGP ساده تر می شود.



شکل (۱۱-۱۳): مدل سوئیچ های چند لایه

مطابق با شکل (۱۱-۱۴)، سوئیچ های چند لایه برای انجام عملیات جابجایی برچسب، از سخت افزار سوئیچ های ATM استفاده می نمایند. استفاده از سخت افزارهای سوئیچ ATM برای انجام عملیات جابجایی برچسب، باعث بهینه سازی کارایی شبکه و امکان استفاده از مسیریابی صریح² می گردد. از پروتکل های IP جهت اختصاص یافتن برچسب به مسیره های LSP، توزیع برچسب بین سوئیچ های چند لایه و تولید و مدیریت جدول های هدایت پیشرو، استفاده می شود.



شکل (۱۱-۱۴): واحد های تشکیل دهنده سوئیچ های چند لایه

به طور کلی دو روش مختلف برای تخصیص و توزیع برچسب ها در سوئیچینگ چند لایه وجود دارد. در روش اول که داده رانده^۱ نام دارد، با ورود داده های ترافیکی کاربران، عملیات نگاشت برچسب انجام می گردد. تکنیکهای سوئیچینگ IP و CSR از این روش استفاده می نمایند. مزیت این روش در آن است که تنها در صورتیکه جریان ترافیکی کاربران برقرار شود، عملیات نگاشت برچسب انجام می گردد، اما این روش دارای معایب عمده زیر است:

- سوئیچ های شبکه باید قادر به تشخیص و جداسازی جریان های ترافیکی مختلف کاربران باشند.
 - میزان ترافیک های کنترلی برای توزیع برچسب ها به طور مستقیم به تعداد جریان های ترافیکی موجود بستگی دارد که این امر باعث نیاز به حجم حافظه بالاتر سوئیچ های شبکه می گردد.
 - این روش قابلیت مقیاس پذیری بالاندارد.
- در روش دوم که کنترل رانده^۲ نام دارد، با ورود اطلاعات کنترلی خاص، عملیات نگاشت برچسب انجام می شود. تکنیک های سوئیچینگ نشانه، ARIS، IP Navigator و MPLS از این روش استفاده می کنند. این روش نسبت به روش قبل دارای مزایای عمده زیر است:

- قبل از ورود داده های ترافیکی کاربران، عملیات تخصیص و توزیع برچسب صورت می گیرد. این مطلب به این معنی است که اگر در جدول مسیریابی IP، مسیری موجود باشد که قبلاً به آن مسیر، برچسب اختصاص یافته است، ترافیک های ورودی به سوئیچ به سرعت هدایت می شوند.
- در این روش تعداد LSP های لازم به تعداد مسیرهای موجود در جدول مسیریابی IP می باشد، نه به تعداد جریانهای ترافیکی موجود در شبکه. بنابراین در مقایسه با روش قبلی، این روش دارای قابلیت مقیاس پذیری بالاتری می باشد.
- در حالت پایدار، میزان بالاسری لازم برای تخصیص و توزیع برچسب ها نسبت به روش داده رانده کمتر می باشد. در فصل ۱۵ فن آوری MPLS و فن آوری های وابسته به آن به طور مفصل بررسی می شود.

۱۱-۶- کیفیت سرویس در شبکه های حسگر بی سیم

در این بخش به بررسی پشتیبانی کیفیت سرویس در شبکه های حسگر بیسیم خواهیم پرداخت. با توجه به افزایش کاربردهای شبکه های حسگر بیسیم، نیاز به پشتیبانی از کیفیت سرویس در این شبکه ها احساس می گردد. در واقع با افزایش کاربردها ترافیک هایی ایجاد گردیده اند که برای تضمین صحت عمل نیاز به پشتیبانی کیفیت سرویس دارند.

همانطور که با ظهور اینترنت انقلابی در صنعت کامپیوتر و ارتباطات ایجاد گردید در آینده ای نزدیک شبکه های حسگر نیز با فراهم آوردن بستری برای جمع آوری اطلاعات از پدیده های فیزیکی و امکان کنترل آنها انقلابی دیگر در زنگیمان ایجاد خواهند نمود. کاربردهای بالقوه ای برای شبکه های حسگر مانند نظارت محیط، کنترل صنعتی، بررسی مناطق جنگی، خودکار سازی فعالیت های خانگی، نظارت بر سلامت عمومی انسان و ... وجود دارند.

تحقیقات گسترده ای بر روی بخش های مهم تر شبکه های حسگر مانند طراحی معماری و پروتکلها، صرفه جویی انرژی و مکانیابی انجام شده است. اما پشتیبانی از کیفیت سرویس در شبکه های حسگر همچنان نا شناخته باقی مانده است. دلیل اصلی این امر تفاوت عمده میان شبکه های مرسوم و شبکه های حسگر بیسیم می باشد. بعنوان مثال هنوز سرویس هایی که شبکه های حسگر بیسیم می توانند ارائه دهند کاملا شناخته نشده اند و آنهایی هم که شناخته شده اند کاملا تکامل پیدا نکرده اند، در این شرایط طراحی مکانیزمی برای پشتیبانی از کیفیت سرویس برای این سرویسها مشکل می باشد.

کیفیت سرویس تعریفی کاملا استاندارد و مشخص ندارد و در واقع در مکانهای مختلف تعریفهای متفاوتی دارد. کاربردهای مختلف تعریف های متفاوتی برای کیفیت سرویس ارائه نموده اند. از دید کاربر، کیفیت سرویس بصورت کلی به کیفیت سرویس دریافت شده توسط کاربر یا دریافت کننده سرویس اطلاق می گردد. از دید شبکه؛ کیفیت سرویس، کیفیت سرویسی است که شبکه در اختیار کاربران و مشتریان خود قرار می دهد. بعنوان مثال در RFC 2386 پشتیبانی کیفیت سرویس بصورت مجموعه ای از پارامترهایی که باید در یک انتقال داده از مبدا به مقصد در شبکه رعایت گردد، بیان شده است. در این سناریوی کیفیت سرویس بعنوان تضمینی از جانب اینترنت برای فراهم نمودن مجموعه ای از پارامترهای سرویس به کاربران آنها به انتها مانند تاخیر، تغییرات تاخیر، پهنای باند موجود و اتلاف بسته می باشد. کاربر و کاربرد اهمیتی به اینکه شبکه چگونه منابع خود را برای پشتیبانی از کیفیت سرویس مدیریت می کند نمی دهند. آنها به سرویس دریافتی از جانب شبکه که در کیفیت عمل کاربرد موثر است توجه می کنند. از دید شبکه، هدف شبکه فراهم نمودن سرویسهای با کیفیت مورد نظر به همراه استفاده بهینه از منابع شبکه می باشد. برای رسیدن به این هدف شبکه باید نیازمندیهای کاربرد را تحلیل نموده و با توجه به آن مکانیزم پشتیبانی کیفیت سرویس را به کار بگیرد.

نیازمندیهای کیفیت سرویس در شبکه های مرسوم به جهت افزایش محبوبیت کاربردهای چند رسانه ای آنها به انتها که نیاز به پهنای باند بالا دارند بوجود آمده است. کاربردهای چند رسانه ای مختلف نیاز به نیازمندیهای کیفیت سرویس متفاوتی که بصورت پارامترهای کیفیت سرویس آنها به انتها بیان می گردند، دارند. در نتیجه شبکه ها نیاز به فراهم آوردن سرویسهایی مناسبتر از سرویسهای بهترین تلاش مانند سرویسهای تضمین شده و سرویسهای جدانشده برای کاربردهای آنها به انتها دارند. محققان مکانیزمها و پروتکل های بسیاری را در لایه های مختلف به منظور فراهم نمودن کیفیت سرویس به همراه حداکثر نمودن بهره وری از پهنای باند طراحی نموده اند. در همین دوره شبکه های مختلف با محدودیتهای مختلف در پشتیبانی از کیفیت سرویس به جهت خصوصیات منحصر بفردشان بوجود آمده اند. به عنوان مثال، پهنای باند محدود و توپولوژی پویا در شبکه های متحرک ad hoc موجب می شود که پشتیبانی از کیفیت سرویس در این شبکه ها دشوارتر از شبکه های مرسوم باشد.

در سالهای اخیر تلاشهای زیادی برای فراهم نمودن کیفیت سرویس در شبکه های کامپیوتری صورت گرفته است. اکثر تحقیقات در زمینه شبکه های تلفن سلولی موبایل، اینترنت سیمی و شبکه های MANET اجرا شده است.

شبکه های مرسوم دارای نیازمندیهای کیفیت سرویس مشابهی هستند که توسط کاربردهای چند رسانه ای که نیاز به پهنای باند بالا دارند ایجاد می گردد. در این شبکه ها پارامترهای کیفیت سرویس آنها به انتهای یکسانی برای بررسی مکانیزمهای پشتیبانی کیفیت سرویس وجود دارد. با توجه به خصوصیات مختلف شبکه ها نمی توان از پروتکل های یکسان استفاده نمود.

بصورت کلی به جهت افزایش تقاضا برای برقراری ارتباطی با کیفیت مناسب و مطمئن که بتواند در هر زمان و هر مکان ایجاد گردد، کیفیت سرویس بسیار اهمیت یافته است.

۱۱-۶-۱- بررسی مشکلات و خصوصیات شبکه های حسگر بیسیم

شناسایی مشکلات و کمبودهای شبکه های حسگر، برای شناسایی و بررسی پشتیبانی از کیفیت سرویس در این شبکه ها سودمند می باشد. در واقع مواردی که در ادامه بیان می گردند را باید در طراحی پروتکل های جدید در نظر گرفت. در ادامه این بخش به بررسی آنها خواهیم پرداخت.

- **خود پیکربندی^۱ و خود نگهداری^۲**: یکی از مهمترین اصولی که در بکارگیری از شبکه های حسگر مد نظر بوده است به کار بردن این شبکه ها در نقاط دور دست بدون مداخله انسان می باشد. بعلاوه شبکه های حسگر معمولا بصورت تصادفی در نقاطی نامناسب در مقیاسی وسیع توزیع می گردند. بدین لحاظ در اکثر موارد پیکربندی دستی تک تک نود ها غیر ممکن می باشد. در نتیجه نود ها باید توانایی خود پیکربندی و خود نگهداری را داشته باشند.

- **مقیاس پذیری**: به این دلیل که نود های حسگر اغلب در تعداد زیاد و در منطقه ای وسیع مورد استفاده قرار می گیرند، پروتکل هایی که برای این شبکه ها استفاده می گردد باید مقیاس پذیر باشند. کارایی این شبکه ها نباید با افزایش تعداد نود ها کاهش پیدا کند.

- **بهره وری انرژی**: نود های حسگر به جهت احساس پدیده ها و ارتباطات با دیگر نود ها انرژی مصرف می کنند. زمانیکه انرژی یک نود تمام شود، نود خواهد مرد و این موضوع ممکن است موجب قطعه قطعه شدن شبکه گردد. بطوریکه ارتباط میان گروهی از نود ها با دیگر نود ها قطع می شود. قطعه شدن شبکه ممکن است موجب از کار افتادن شبکه شود بطوریکه برخی از قطعه های شبکه دیگر در دسترس نباشند. بعضی از محققان، پایان عمر شبکه حسگر را زمانی می دانند که شبکه قطعه شده است. در نتیجه، شبکه حسگر باید مصرف بهینه انرژی را در نظر گیرد تا عمر شبکه مفیدتر باشد.

- **مقاومت در برابر خطا**: به سبب کمبود انرژی در نود ها و مناطق نامناسبی که شبکه ها معمولا در آن قرار می گیرند، نود های حسگر مستعد بروز خطا می باشند. با مقاومت در برابر خطا، شبکه باید بتواند با وجود خرابی تعدادی از نود های خود به عملیات خود ادامه دهد. این مورد موجب افزایش اطمینان شبکه حسگر شده و باعث افزایش ارائه کیفیت سرویس به کاربرد می گردد.

- **قابلیت انطباق**: توپولوژی شبکه و خصوصیات شبکه های حسگر به جهت بکارگیری آنها در محیط های خشن کاملا پویا می باشد. در نتیجه شبکه حسگر باید با انطباق خود با تغییر شرایط کارایی خود را حفظ نماید.

- **رسانه ارتباطی**: نود های حسگر معمولا از طریق یک کانال ارتباطی مشترک بیسیم ارتباط برقرار می کنند. زیرا محیط هایی که این شبکه ها در آن فعالیت می کنند اغلب اجازه ایجاد زیر ساخت های دیگر را نمی دهد. وابسته به شرایط محیطی که شبکه های حسگر در آن فعال است، از رسانه های متفاوت استفاده می گردد. مثلا شبکه های حسگر زمینی از لینک های رادیویی و شبکه های زیر آب از لینک های صوتی برای ارتباط استفاده می کنند. هر کدام از این رسانه ها خصوصیات مختص به خود مانند فرکانس عملیاتی بهینه و ... را دارد.

¹ self configuration

² self maintenance

- امنیت: باز بودن محیط فیزیکی و رسانه ارتباطی شبکه های حسگر، آنها را در برابر حملات امنیتی مانند DoS¹ و دسترسی های غیر مجاز به اطلاعات شبکه آسیب پذیر نموده است. در نتیجه، اطمینان از اینکه شبکه حسگر از مکانیزمهای امنیتی در پروتکل های خود به منظور حفظ یکپارچگی اطلاعات جمع آوری شده استفاده می کند ضروری است.

- پردازش داده: انتظار می رود نود های حسگر دارای توان پردازشی پایینی باشند و در نتیجه امکان اجرای پردازشهای پیچیده ای مانند تجمیع داده را ندارند. در MANET ها، پردازش اطلاعات در نود ها موجب بهبود زمان پاسخگویی شبکه به تغییرات محیطی می گردد.

- ذخیره سازی داده: در شبکه های حسگر با مقیاس بزرگ، محتوای داده های احساس شده، از نود ای که داده را جمع آوری نموده، مهمتر می باشد. در نتیجه، استفاده کارا از داده های جمع آوری شده نیاز به الگوریتمهای مقیاس پذیر، خود سازمان ده و آگاه به مصرف انرژی دارد. در این روش، داده باید نامگذاری شود و در ارتباطات از این نامگذاری بجای آدرس دهی شبکه استفاده می شود. با استفاده از الگوریتمهای ذخیره داده جدید مانند DCS² داده ها با استفاده نامشان در نود ذخیره می گردند. در این صورت، درخواستها برای داده با نامی مشخص به نود های که آن داده را ذخیره نموده اند ارسال می گردد، در این حالت دیگر نیاز به استفاده از الگوریتم flooding که در برخی پروتکل های مسیریابی استفاده می گردد نخواهد بود.

- محدودیت های سخت افزاری: یک نود حسگر شامل واحد احساس، واحد پردازش، واحد فرستنده/گیرنده و واحد انرژی می باشد. با توجه به اینکه تمام این قطعات باید در یک نود حسگر جا سازی شوند، واضح است که نود ها دارای محدودیت هایی از قبیل توان محاسباتی پایین، نرخ داده کم و منبع انرژی محدود خواهند بود. نود ها باید با وجود این کمبودهای سخت افزاری وظایف خود را اجرا نمایند و الگوریتمها نباید اجرای محاسبات پیچیده ریاضی را انتظار داشته باشند.

۱۱-۶-۲- نیازمندیهای کیفیت سرویس در شبکه های حسگر

شبکه های حسگر عضو جدیدی در شبکه های بیسیم با برخی خصوصیات منحصر بفرد می باشند، شبکه های حسگر بصورت عمومی از تعداد زیادی نود که در محدوده ای معین پخش می گردند، تشکیل شده اند. هر کدام از آنها توانایی جمع آوری اطلاعات در مورد شرایط محیطی مانند دما، فشار، رطوبت، نویز، نور و موارد دیگر را دارند و داده های جمع آوری کرده را برای نود چاهک ارسال می کنند. می دانیم که کاربردهای مختلفی برای شبکه های حسگر وجود دارد و هر کدام نیازمندیهای کیفیت سرویس خاص خود را دارند و امکان بررسی تمام آنها وجود ندارد. همچنین نمی توان یک شیوه کلی پشتیبانی کیفیت سرویس ارائه نمود که برای تمام کاربردها مناسب باشد.

در ادامه تاکید بر روی نیازمندیهای کیفیت سرویس کاربردها که بر شبکه تحمیل می گردند خواهد بود. البته همانطور که در بخشهای قبلی بررسی گردید نیازمندیهای کیفیت سرویس از دیگر دیدگاهها با دیدگاه شبکه متفاوت می باشد. در واقع انجمن های مختلف، تعاریف مختلفی با توجه به دیدگاهشان در مورد کیفیت سرویس ارائه نموده اند. برای مثال از دید کاربردهای تشخیص رویداد و پیگیری هدف، خطا در تشخیص و یا استخراج داده های نادرست و غلط در مورد پدیده فیزیکی و از دید مدیریت شبکه، پوشش محل روی دادن پدیده با حسگرهای فعال از این جمله می باشند. در واقع پوشش و یا تعداد نود های فعال را می توان بعنوان پارامتر کیفیت سرویس در نظر گرفت. از جهتی دیگر، فعالیت نامناسب نود ها مانند دقت پایین در بررسی پدیده و یا نرخ گزارش نا کافی نیز می تواند مشکل ساز باشد. در نتیجه می توان دقت بررسی پدیده و یا خطاهای اندازه گیری را بعنوان پارامتر کیفیت سرویس در نظر گرفت. گم شدن اطلاعات نیز مورد دیگری در

¹ Denial of Service

² data centric storage

ناکارآمدی شبکه می باشد. در نتیجه می توان پارامترهای انتقال داده را بعنوان پارامتر کیفیت سرویس در نظر گرفت. البته تقسیم دیدگاهها نسبت به کیفیت سرویس موضوعی استاندارد نمی باشد. بعنوان مثال نیاز کیفیت سرویس یک کاربرد مانند میزان کارایی، تمام پارامترهای مذکور را شامل می گردد. در ادامه بررسی می نماییم که چگونه لایه های زیرین کیفیت سرویس را بر حسب اینکه با کمک کدام پارامترها می توان نیازمندیهای کاربرد را بر شبکه نگاشت نمود و کیفیت سرویس را متناسب با آن اندازه گیری کنیم، برای کاربرد مهیا می کنند. بر این اساس دو نوع دیدگاه برای پشتیبانی کیفیت سرویس در شبکه های حسگر بیان می کنیم.

- کیفیت سرویس از دیدگاه کاربرد: از این دیدگاه، پارامترهایی مانند پوشش، وسعت دید، خطاهای اندازه گیری شده و تعداد بهینه نود های حسگر بررسی می گردند. بطور خلاصه، کاربردها نیازمندیهای خاصی را در استفاده از حسگرها ایجاد می کنند؛ تعداد نود های فعال، دقت اندازه گیری حسگرها و مواردی اینچنین از این جمله اند که وابسته به کیفیت کاربرد می باشند.

- کیفیت سرویس از دید شبکه : از این دیدگاه، اینکه چگونه شبکه داده های حس شده را با توجه به نیازمندیهای کیفیت سرویس آنها و در کنار استفاده بهینه از منابع شبکه منتقل می نماید بررسی می گردد. بدلیل گستردگی کاربردها نمی توان تمام آنها را بررسی نمود، اما می توان هر کلاس کاربرد را از نظر مدل ارائه داده¹ بررسی نمود. می دانیم کاربردهایی که در یک کلاس عضو هستند تقریباً دارای خصوصیات مشابهی می باشند. از دید شبکه در توجهی به اینکه کاربرد واقعا به خواسته های خود می رسد نداریم و تنها به اینکه داده چگونه به چاهک منتقل شده و نیازمندیهای مشابه آن توجه می نماییم. ۴ مدل ارائه داده وجود دارد که عبارتند از: مدل رخداد گرا، مدل درخواست گرا، مدل پیوسته و مدل ترکیبی. قبل از نمایش نیازمندیهای کاربردها، به بررسی ملاکهایی که در زیر ارائه می گردند می پردازیم:

- انتها به انتها: کاربرد ممکن است نیاز به کارایی انتها به انتها داشته باشد و یا نداشته باشد.

- فعل و انفعالی: کاربرد می تواند بصورت فعل و انفعالی باشد و یا نباشد.

- تحمل پذیری تاخیر: کاربرد می تواند در قبال تاخیر مقاوم باشد و یا نباشد.

- بحرانی: کاربرد می تواند دارای ماموریتی بحرانی باشد و یا نباشد.

مدل رخدادگرا :

اکثر کاربردهای رخداد گرا در شبکه های حسگر فعل و انفعالی، حساس در برابر تاخیر (بلادرنگ)، بحرانی و غیر انتها به انتها می باشند. در واقع حسگرهای رخداد گرا، پدیده های احساس شده در موفقیت کاربردها بسیار مهم می باشند. کاربرد باید پدیده ها را احساس نموده و پس از آن عکس العمل خاصی را در اولین فرصت و با بالاترین اطمینان ممکن اجرا نماید. در مورد این کاربردها نکات مهمی وجود دارد. اول اینکه این کاربردها به خودی خود انتها به انتها نمی باشند، به عبارت دیگر یک طرف ارتباط چاهک می باشد اما در طرف دیگر یک نود واحد وجود ندارد بلکه گروهی از نود ها که در محدوده مورد نظر پدیده را احساس نموده اند وجود دارند. دوم، جریانهای داده مربوط به این کاربردها بسیار همبسته بوده و داده تکراری زیادی وجود دارد. سوم، ترافیک ایجاد شده توسط یک نود شدت کمی دارد اما توسط مجموعه ای از نود ها که پدیده را احساس نموده اند ترافیک قابل توجهی ایجاد می گردد. و نهایتاً، در صورت نیاز به عکس العمل در قبال پدیده احساس شده، باید در اولین فرصت و با بالاترین اطمینان ممکن اجرا گردد. عاملانی که عکس العمل تصمیم گرفته شده را اجرا می کنند

¹ data delivery model

می توانند با نود هایی که پدیده را احساس نموده اند، متفاوت باشند. این مدل ارائه داده در کاربردهایی که نیاز به تشخیص پدیده ها و پی جویی/تخمین نشانه ها دارند مانند احساس و پاسخ به انتشار یک ماده شیمیایی در فضای ساختمان، استفاده می گردد.

مدل درخواست گرا :

اکثر کاربردهای درخواست گرا، در شبکه های حسگر فعل و انفعالی، بسته به نوع درخواست مقاوم در برابر تاخیر، بحرانی و غیر انتها به انتها می باشند. به منظور حفظ انرژی، درخواستها بر اساس نیاز و در مواقع لزوم ارسال می گردند. این مدل مشابه با مدل رخداد گرا می باشد با این تفاوت که در این مدل داده توسط چاهک کشیده می شود ولی در مدل رخداد گرا داده به سمت چاهک ارسال می شود. در این مدل نیز داده ها باید در اولین فرصت و با بالاترین اطمینان ممکن در اختیار چاهک قرار گیرد. نکات مهم بحث شده در مورد مدل رخدادگرا ، برای این مدل نیز قابل توجه می باشند. امکان دارد که از درخواست به جهت مدیریت و پیکربندی نود های حسگر نیز استفاده گردد. برای مثال، اگر یک نود چاهک بخواهد نرم افزار نود را بروز رسانی کند، یا پیکربندی نرخ ارسال را دوباره اجرا کند و یا وظایف نود ها را تغییر دهد باید درخواستی را به آن دلیل ارسال نماید. فرمانهای چاهک یک طرفه بوده و باید با بالاترین اطمینان ممکن به مقصد ارسال گردد.

مدل پیوسته :

در مدل پیوسته، حسگرها داده های خود را با نرخ مشخص بطور پیوسته برای چاهک ارسال می کنند. داده های ارسالی در این مدل، به یکی از صورت های زیر می باشد:

- صدا، تصویر و عکس بلادرنگ: داده های بلادرنگ نسبت به تاخیر حساس می باشند و به پهنای باند مشخصی نیاز دارند. اتلاف بسته تا حد معینی در این حالت قابل تحمل می باشد.
- داده های غیر بلادرنگ: چاهک امکان دارد داده ها را بصورت دوره ای از شبکه حسگرها جمع آوری نماید. در این حالت، تاخیر و اتلاف بسته تا حد معینی قابل تحمل می باشد.

مدل ترکیبی:

در برخی کاربردها، مدل‌های ارائه داده متفاوتی بصورت یکجا در شبکه استفاده می گردد. در این میان نیاز به مکانیزمی برای هماهنگی انواع مختلف ترافیک با نیازهای متفاوت کیفیت سرویس وجود دارد. این نیازمندیها در جدول (۱۱-۳) خلاصه شده است.

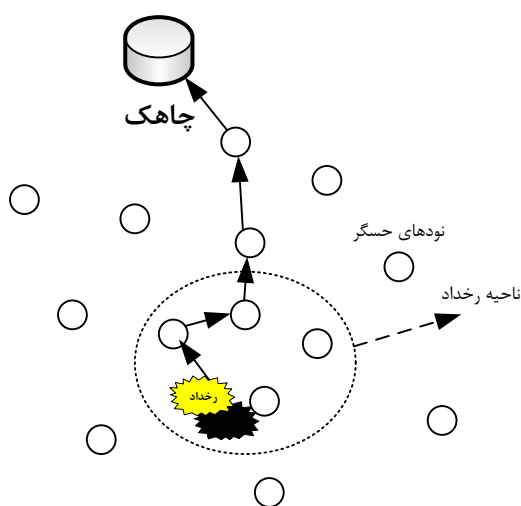
جدول (۱۱-۳): خصوصیات مدل های مختلف ارائه داده

کلاس	مدل رخدادگرا	مدل درخواست گرا	مدل پیوسته
انتها به انتها	خیر	خیر	خیر
فعل و انفعالی	بله	بله	خیر
تحمل تاخیر	خیر	توسط درخواست مشخص می شود	بله
بحرانی	بله	بله	بله

تفاوت‌های قابل توجهی در نیازمندی‌های شبکه‌های حسگر بیسیم و شبکه‌های مرسوم وجود دارد. اول، کاربردهای شبکه‌های حسگر انتها به انتها نمی‌باشند. دوم، پهنای باند اصلی‌ترین مسئله نودهای حسگر نمی‌باشد. اما توسط گروهی از نودهای حسگر در دوره‌های مختلف ترافیک شدید ایجاد می‌گردد و مسئله پهنای باند اهمیت می‌یابد. سوم، ائتلاف بسته مربوط به یک نود تا حدی قابل قبول می‌باشد. با این وجود که افزونگی داده در شبکه‌های حسگر وجود دارد. نهایتاً، اکثر کاربردهای شبکه‌های حسگر بحرانی می‌باشند و این موضوع نشان‌دهنده اهمیت این کاربردها می‌باشد. با توجه به موارد ذکر شده، برای پشتیبانی از کیفیت سرویس در شبکه‌های حسگر نمی‌توان از پارامترهای کیفیت سرویس انتها به انتها استفاده نمود. در نتیجه نیاز به استفاده از پارامترهای جدید کیفیت سرویس برای شبکه‌های حسگر داریم که عبارتند از:

- تاخیر جمعی
- ائتلاف بسته جمعی
- پهنای باند جمعی
- گذردهی اطلاعات

قصد نداریم که تعاریف دقیقی در مورد موارد ذکر شده بیان کنیم. با طرح مثال آنها را بررسی می‌نماییم. در شکل (۱۱-۱۵)، حسگرها در اطراف یک پدیده قرار داشته و اطلاعاتی را در مورد آن برای چاهک ارسال می‌کنند. در این حالت تاخیر جمعی، مدت زمان میان ایجاد اولین بسته گزارشی توسط مبدا تا دریافت آخرین بسته توسط چاهک به طول می‌انجامد می‌باشد. تعداد بسته‌های مربوط به این پدیده که در طول انتقال اطلاعات تلف می‌گردند را ائتلاف بسته جمعی می‌گویند. پهنای باندی که برای گزارش رویداد مورد نیاز می‌باشد را پهنای باند جمعی می‌گوییم. بطور خلاصه، توجه چاهک بجای اینکه بر روی بسته‌های مربوط به نود خاصی باشد باید بر روی پدیده بصورت انتها به انتها باشد. بعلاوه، پهنای باند اطلاعات را باید با توجه به حجم داده وارد شده از مجموعه نودهای مرتبط بدست آورد؛ در واقع نباید به داده‌های تنها یک نود بسنده نمود.



شکل (۱۱-۱۵): یک شبکه حسگر بیسیم رخدادگرا

۱۱-۶-۳- مشکلات موجود برای پشتیبانی کیفیت سرویس در شبکه های حسگر

نظر به اینکه شبکه های حسگر با محیط تعامل دارند، خصوصیات آنها با شبکه های مرسوم متفاوت می باشد. در نتیجه علاوه بر اینکه شبکه های حسگر مشکلات پشتیبانی کیفیت سرویس شبکه های مرسوم را به ارث می برند، خود نیز مشکلات مخصوص خود را دارند. این مشکلات عبارتند از:

- **کمبود شدید منابع:** کمبود منابع شامل انرژی، پهنای باند، حافظه، اندازه بافر، قدرت پردازش و توان ارتباط محدود، می باشد. در میان آنها، انرژی اولین مورد می باشد؛ زیرا انرژی بشدت در نود های حسگر محدود بوده و به این دلیل که نود ها اغلب در مکانهای دور از دسترس و نا مناسب جایگذاری می گردند شارژ دوباره و جایگزینی منبع انرژی در آنها مرقوم بصره نمی باشد. در نتیجه کمبودهای ارائه شده، نیازمندیهای ضروری اضافه ای برای پشتیبانی از کیفیت سرویس در شبکه های حسگر بوجود می آید که عبارتند از: سادگی، الگوریتم متمرکز محاسباتی، پروتکل های سیگنالینگ گران و یا اینکه نگهداری حالت شبکه بدلیل سربار قابل توجهی نمی باشد.

- **ترافیک نا متعادل:** در اکثر کاربردهای شبکه های حسگر ترافیک از تعداد زیادی از نود های شبکه به سمت تعداد محدودی از نود های چاهک جریان دارند. مکانیزم کیفیت سرویس باید برای ترافیک محدود از نظر کیفیت سرویس و نا متعادل طراحی گردد.

- **افزونگی داده:** یکی از خصوصیات شبکه های حسگر افزونگی داده می باشد. با وجود اینکه افزونگی داده نیازمندیهای اطمینان و صحت در انتقالات شبکه را کاهش می دهد، اما انرژی ارزشمند قابل توجهی را بی دلیل مصرف می نماید. تجمیع^۱ و آمیزش داده^۲ با حفظ اطمینان شبکه، افزونگی داده را کاهش می دهند؛ اما موجب افزایش تاخیر و پیچیدگی مکانیزم پشتیبانی کیفیت سرویس می گردند.

- **پویایی شبکه:** خرابی نود ها، خرابی لینک های بیسیم، تحرک نود ها و انتقال حالت نود ها به جهت مدیریت انرژی و استفاده بهینه از انرژی عامل پویایی شبکه می باشند. پویایی شبکه موجب افزایش پیچیدگی پشتیبانی از کیفیت سرویس می شود.

- **تعادل انرژی:** به منظور افزایش طول عمر شبکه، بار انرژی باید در تمام شبکه توزیع گردد، طوریکه انرژی در نود ای خاص یا در گروهی از نود ها خیلی زودتر از آنچه انتظار می رود پایان یابد. در پشتیبانی از کیفیت سرویس باید این پارامتر را در نظر گرفت.

- **مقیاس پذیری:** یک شبکه حسگر عادی دارای بیش از صدها یا هزارها نود می باشد که بصورت گسترده ای در منطقه جغرافیایی خاص توزیع شده اند. بنابراین، مکانیزم پشتیبانی از کیفیت سرویس باید کار در محیطی با مقیاس های بزرگ را داشته باشد به عبارت دیگر پشتیبانی از کیفیت سرویس نباید با افزایش تعداد نود ها کارایی خود را از دست بدهد.

- **وجود چندین چاهک:** امکان دارد در شبکه حسگر چندین چاهک موجود باشد که هر کدام دارای نیازمندیهای مخصوص خود باشد. برای مثال، یک چاهک قصد دارد گزارشهای مربوط به دما را از نود های شمالی شبکه دریافت نماید و چاهکی دیگر قصد دارد گزارشی از نود های جنوبی که دمای بالایی را احساس می نمایند دریافت کند. مکانیزم پشتیبانی از کیفیت سرویس باید قادر باشد سطوح مختلف کیفیت سرویس را برای چاهک های مختلف ارائه کند.

¹ aggregation

² fusion

- چندین نوع ترافیک: وجود چندین نوع نود مختلف در شبکه برای پشتیبانی از کیفیت سرویس مشکل زا می باشد. برای مثال، برخی کاربردها نیاز به چندین نوع نود برای بررسی دما، فشار و رطوبت دارند و در نتیجه نرخ ارسال اطلاعات در نود های مختلف متفاوت خواهد بود. در چنین محیطی پشتیبانی از کیفیت سرویس مشکل تر خواهد بود.

- بسته های بحرانی: محتوای داده ها یا اطلاعات سطح بالا، وضعیت پدیده فیزیکی واقعی را از نظر بحرانی بودن یا نبودن مشخص نموده و بر این اساس اولویتهای متفاوتی برای کاربرد در نظر گرفته می شود. ممکن است مکانیزم پشتیبانی از کیفیت سرویس نیاز داشته باشد ساختاری برای رعایت اولویت میان بسته های مختلف ایجاد نماید.

بصورت خلاصه، مکانیزم پشتیبانی از کیفیت سرویس برای شبکه امکان دارد تنها تعداد محدودی از پارامترهای مذکور را برای کاربردی خاص در نظر گیرد.

پرسش های فصل

۱. مکانیزمها و روشهایی که ازسوی سازمان جهانی IETF برای حمایت از کیفیت سرویس دراینترنت ارائه شده است را توصیف نمایید.
۲. ویژگیهای سرویس تضمین شده و سرویس کنترل بار را توضیح دهید.
۳. چهارقسمت اصلی تشکیل دهنده سرویس مجتمع را توضیح دهید.
۴. معایب ومزایای عمده سرویس مجتمع را شرح دهید.
۵. سرویس جدانشده را توضیح داده و تفاوت اصلی آن را با سرویس مجتمع شرح دهید.
۶. مفهوم SLA و کاربرد آن را توضیح دهید.
۷. مزایای مهندسی ترافیک را شرح دهید.
۸. مسیریابی مبتنی برقید را توضیح داده و برتری آن را نسبت به روشهای متداول مسیریابی بنویسید.
۹. مشکلات اساسی مسیریابی مبتنی برقید را شرح دهید.
۱۰. پروتکل های IP و ATM را ازجانبه های مختلف مقایسه نموده و مشکلاتی که درمجتمع سازی IP و ATM وجود دارد شرح دهید.
۱۱. مهم ترین اهداف طراحی شبکه های MPLS را شرح دهید.
۱۲. ویژگیهای اصلی MPLS را توصیف نمایید.
۱۳. مسیریابی IP را با سوئیچینگ ATM مقایسه نموده و مزایا و مشکلات هر یک را توضیح دهید.
۱۴. روشهای مختلف ترکیب مسیریابی IP و سوئیچینگ ATM را توصیف نمایید.
۱۵. تکنیک سوئیچینگ چند لایه را توضیح دهید.
۱۶. مفهوم LSP و FEC و ادرشکبه های MPLS بنویسید.
۱۷. مشکلات شبکه های حسگر بیسیم ازجانبه تامین کیفیت سرویس را تشریح نمایید.
۱۸. نیازمندی های کیفیت سرویس ازدید کاربر را درشکبه های حسگر بیسیم تشریح کنید.