به نام خدا

عنوان مقاله

طراحی معماری روتر مبتنی بر سوئیچینگ MPLS با استفاده از VHDL ساختاری بر روی FPGA

گردآوری

سدید سهامی

کلمات کلیدی

شبکه – روتر – پروتکل - MPLS - PAD

چکیده

در پایان نامۀ پیش رو طراحی یک روتر مبتنی بر MPLS مورد نظر است. MPLS خود نوع جدیدی از روشهای سوئیچینگ را ارائه میدهد. شبکه های مبتنی بر MPLS امروزه کاربردهای فراوانی پیدا کرده اند و به شدت در حال گسترش می باشند. از طرفی MPLS کاندیدای اول برای ابرشبکه های نسل بعدی یا به اصطلاح NGN است.

امروزه پیاده سازیهائی که از روترهای مبتنی بر MPLS انجام گردیده است تماما نرم افزاری است، بدین معنی که روش سوئیچنگ MPLS را با استفاده از نرم افزار – معمولا یک سیستم عامل ویژه – بر روی یک پلتفرم همه منظوره انجام میدهند. این روش انعطاف پذیری در تولید محصول و از طرفی صرفه جوئی اقتصادی را برای شرکتهای مطرح در این زمینه به بار می آورد. ازینرو طراحی سخت افزاری روترها، مبتنی بر ASIC در نسلهای اخیر، به فراموشی سپرده شده است.

اخیرا در محافل آکادمیک تلاشهائی برای طراحی روترها با استفاده از پیشرفتهائی که در تکنولوژیهائی مانند FPGA صورت گرفته است، شروع گردیده است. یکی از مفاهیم که میتواند مسئلۀ انعطاف پذیری را در کنار سرعت سخت افزاری به هم پیوند بزند مفهوم Reconfigurable Computing است که گرایشات در طراحی روترهای اینچنین را حداقل در سطح محافل آکادمیک تحت تأثیر قرار داده است.

پایان نامۀ پیشرو تلاشی برای طراحی ساختاری معماری یک روتر MPLS و سپس پیاده سازی آن با استفاده از کدهای VHDL برای به کار بردن بر روی چیپهای FPGA بر اساس یک طراحی مبتنی بر SoC است. در این پایان نامه ضمن معرفی MPLS به طراحی و پیاده سازی یک معماری برای روترهای MPLS با استفاده از مفاهیم Reconfigurable Computing پرداخته شده است. و سپس نتایج حاصل از کامپایل و شبیه سازی طرح ارائه گردیده است.

در این پایان نامه برای بخشهای مربوط به مهندسی ترافیک و پروتکلهای مرتبط که جزء متنوع ترین و متغیرترین بخشهای روتر هستند یک پلتفرم مبتنی بر Soft Core در نظر گرفته شده تا به اصل بازتنظیم پذیری لطمه ای وارد نشود. همچنین پیاده سازی و نوشتن برنامه ها و الگوریتمهای پروتکلهای مهندسی ترافیک، در این پایان نامه مد نظر نبوده است.

فهرست مطالب

عنوان **صفحه**

کوتاه نوشت .....

پیشگفتار **۲**

فصل اول: مروری بر سوئیچهای دیجیتال **۱۰**

سوئیچهای اولیه **۱۰**

X.25 ..... **۱۶**

Frame Relay **۲۴**

SMDS **۳۳**

SONET & SDH **۳۸**

ATM **۴۱**

فصل دوم: MPLS **۴۶**

معماری MPLS **۴۶**

LDP **۶۰**

CR-LDP **۷۰**

RSVP **۸۳**

RSVP-TE **۹۴**

فصل سوم: مقایسه **۱۰۱**

فصل چهارم: پروژه های مشابه **۱۰۸**

ضمیمهٔ اول- مقدمه ای بر انواع شبکه های مخابراتی **۱۱۳**

ضمیمهٔ دوم- روتر بالادستی و پائین دستی **۱۱۵**

منابع **۱۱۷**

Glossary

- **ANSI**
  American National Standard Institute
- **ASIC**
  Application Specific Integrated Circuit
- **ATM**
  Asynchronous Transfer Mode
- **BGP**
  Border Gateway Protocol
- **CoS**
  Class of Service
- **CR-LDP**
  Constrained-Based Routing Label Distribution Protocol
- **DLCI**
  Data Link Connection Identifier
- **ER-LSP**
  Explicitly Routed Label-Switched Path
- **FEC**
  Forward Equivalent Class
- **FIB**
  Forwarding Information Base
- **FPGA**
  Field Programming Gate Array
- **IEC**
  International Electronical Commission
- **IETF**
  Internet Engineering Task Force
- **IEEE**
  Institute of Electrical and Electronic Engineering
- **ITU**
  International Telecommunication Union
- **IGP**
  Internet Gateway Protocol
- **IP**
  Intellectual Property

- **IP**
  Internet Protocol
- **LAN**
  Local Area Network
- **LER**
  Label Edge Router
- **LFIB**
  Label Forwarding Information Base
- **LSP**
  Label-Switched Path
- **LSR**
  Label Switch Router
- **MPLS**
  Multiprotocol Label Switching
- **MTU**
  Maximum Transfer Unit
- **NHLFE**
  Next Hop Label Forwarding Entry
- **OSPF**
  Open Shortest Path First
- **OSI**
  Open System Interconnection Reference Model
- **PDH**
  Plesiochronous Digital Hierarchy
- **PIM**
  Protocol Independent Multicast
- **PSTN**
  Public Switched Telephone Network
- **QoS**
  Quality of Service
- **RFC**
  Request for Comments
- **RIP**
  Routing Information Protocol
- **RSVP**
  Resource Reservation Protocol

- **RSVP-TE**
  RSVP- Traffic Engineering
- **SDH**
  Synchronous Digital Hierarchy
- **SMDS**
  Switched Multigigabit Data Service
- **SOC**
  System On Chip
- **SONET**
  Synchronous Optical Network
- **TCP**
  Transmission Control Protocol
- **TLV**
  Type Length Value
- **TTL**
  Time To Live
- **UDP**
  User Datagram Protocol
- **Verilog-HDL**
  Verilog Hardware Description Language
- **VHDL**
  Very High Integrated Circuit Hardware Description Language
- **VPI/VCI**
  Virtual Path Identifier / Virtual Channel Identifier
- **VPN**
  Virtual Private Network

پیشگفتار

یکی از مهمترین تکنولوژی های آینده که بنا به اعتقاد بعضی از کارشناسان موج چهارم زندگی بشری بعد از انقلاب انفورماتیک است، ابر شبکه ای است که این توانائی را دارد که نه فقط انسانها و دستگاهای کامپیوتر شخصیشان، بلکه تمام وسائل را به یکدیگر وصل نماید، این ابرشبکه یکی از پایه های موج چهارم زندگی بشری به حساب می آید.

ادوات گوناگون پیرامونمان فیزیک و خصوصیات خاص خود را دارند و بنابراین شبکه های خاص خود را می طلبند به همین خاطر است که شبکهٔ تلفن همراه با شبکهٔ متشکل از کامپیوترهای PC و سرورها فرق میکند، وسائل خانگی نیز شبکه های خاص خود را می طلبند. یک چنین شبکه ناهمگونی که بتواند با ادوات مختلف کار کند یکی از ضروریات ابر شبکهٔ وعده داده شده یا NGN است.

همانطور که در پایان نامه توضیح داده خواهد شد، MPLS در حال حاضر بهترین گزینه برای این شبکه است. MPLS این قابلیت را دارد که با پاکتهای مختلف از شبکه های گوناگون بدون درگیر شدن با محتوای آنها کار کند بدین معنی که وقتی پاکتی از یک شبکه متفاوت می آید شبکهٔ MPLS با آن مانند یک جعبهٔ سیاه رفتار کرده و با استفاده از یک سیستم مشابه ایندکس، پاکت را به طرف مقصد هدایت میکند که معمولا تحویل یک شبکهٔ دیگر داده میشود بدین ترتیب شبکهٔ MPLS به عنوان هستهٔ پیوند دهندهٔ شبکه های مختلف به کار گرفته میشود.

کاربردهای شبکه های MPLS به اینجا ختم نمیشود بلکه این شبکه ها امروزه به سمت جایگزینی برای شبکه های قدیمتری مانند Frame Relay و ATM پیش میروند، امروزه بسیاری از شرکتها پس از اتمام قراردادهای خود به سمت به کارگیری یک شبکهٔ MPLS پیش میروند چرا که امکانات بسیاری را به ارمغان می آورد که در این پایان نامه بدان پرداخته میشود.

هدف از این پایان نامه طراحی یک روتر MPLS است که در شبکهٔ مبتنی بر MPLS به کار میرود. در این پایان نامه سعی شده است که در ابتدا یک معماری برای این نوع روترها طراحی گردد. طرح توسط زبان VHDL پیاده سازی و در نرم افزار Quartus شبیه سازی شده است. از آنجا که در این پایان نامه اقدام به طراحی یک معماری برای روتر شده است، کدهای VHDL نیز غالبا ساختاری نوشته شده اند و بدین جهت کاملا قابل سنتز هستنند.

در فصل اول این پایان نامه ابتدا مروری اجمالی بر انواع شبکه های قبل از MPLS پرداخته شده است تا راه برای توضیح شبکه های MPLS در فصل دوم باز شود. فصل اول که به معرفی شبکه های X.25 و Frame Relay و SMDS و SONET و ATM به همراه بحثی کوتاه در مورد تولد سوئیچنگ می پردازد، در واقع یک گردآوری از منابع مختلف به همراه تلخیص و تا حدی بازنویسی بوده است. این منابع به تفکیک ذکر گردیده اند. هدف از این فصل آماده کردن پایه ای برای بیان شبکه های MPLS در مقام مقایسه است و دیگر اینکه

فهم امکانات و مزیتهای MPLS بدون در نظر گرفتن روند تاریخی توسعه و مقایسه با کاستی های شبکه های قبلی ممکن نیست.

در فصل دوم شبکه های MPLS معرفی شده اند. روترهای MPLS باید قادر باشند که پروتکلهای این شبکه ها را اجرا کرده و بتوانند به عنوان یک گرهٔ MPLS به کار روند. در این فصل شبکهٔ MPLS توضیح داده شده و وظایفی که باید یک روتر MPLS انجام دهد در این فصل مشخص میشود. این فصل ترجمه ای از فصلهای ۶ و ۷ کتاب Connection Oriented Networks است و در آن دخل و تصرفی جز حذف چند بحث غیر ضرور انجام نگرفته است.

در فصل سوم که فصلی کوتاه است به مقایسه و امکانات شبکهٔ MPLS پرداخته شده است. علاوه بر یک مقایسه کوتاه، تلخیص و ترجمه ای از یک مقاله در مورد وضعیت اقتصادی و آینده مالی شبکه های MPLS آورده شده است.

فصل چهارم نیز، فصلی کوتاه در مورد طرحهای مشابه قبلی است، پروژه های معرفی شده در این فصل نتیجهٔ یک جست و جوی اینترنتی هستنند و شامل چند مقاله و یک پایان نامه است که در این فصل هر یک توضیح داده شده اند. هیچ یک ازین پروژه ها متاسفانه در این پایان نامه مورد استفاده قرار نگرفت چرا که در بین آنها تنها یک پایان نامهٔ کارشناسی ارشد کامل بوده و قابل استفاده، که اهداف و گرایشات آن نیز با این پروژه متفاوت بود. بقیه پروژه ها که تنها مقالاتی چند صفحه ای بودند قابل استفاده در این پایان نامه نبودند در این فصل هر یک ازین پروژه ها توضیح داده شده اند و اگر از ایده های آنها استفاده شده نیز در این فصل ذکر شده است.

در فصل پنجم که معماری طراحی شده به تفصیل توضیح داه شده است. برخلاف آنچه که در ابتدای شروع به کار پروژه تصور میشد، امکان طراحی سخت افزاری و ساختاری از بخشهائی از روتر که به routing component مشهورند به کلی ممکن نیست چرا این بخشها متشکل از پروتکلهای سطح بالا به لحاظ ساختار الگوریتمیک هستند و گاها از مفاهیم هوش مصنوعی نیز بهره میگیرند لذا تنها راه پیاده سازی آنها بر روی یک FPGA استفاده از یک یا چند پردازنده است که بتواند الگوریتمهای فوق را با استفاده از زبانهای سطح بالائی مانند C++ پیاده کند. این مسئله در خود فصل به تفصیل توضیح داده شده است. علیرغم طراحی بخش روتیگ با استفاده از پردازنده و نه بلوکهای ساختاری متداول در طراحی ASIC، بقیهٔ بخشها یعنی دو جزء Forwarding و Common Control به شکل ساختاری طراحی شده اند.

فصل آخر نیز نتیجهٔ کامپایل پروژه است که با استفاده از زبان VHDL ساختاری در نرم افزار Quartus II 7.2 طراحی گردیده است. در این فصل بحثی راجع به آنالیز زمانی برای اطمینان از صحت عملکرد و نیز منابع مورد نیاز برای پیاده سازی طرح بر روی FPGA و مسائل مشابه ذکر گردیده اند.

در ضمیمهٔ اول پایان نامه نیز کدهای VHDL نوشته شده آورده شده اند و در ضمیمهٔ دوم نیز یک بحث خیلی کوتاه راجع به دسته بندی شبکه های مخابراتی در حد یک صفحه آورده شده است که در واقع خلاصه و

بازنویسی از مقدمهٔ یکی از کتابها است که ذکر شده است. ضمیمهٔ سوم نیز مختصرا به تبین مفاهیم بالادست جریان و پائین دست جریان در حیطهٔ MPLS می پردازد. منابع نیز در بخش آخر ذکر گردیده اند.

سوئیچهای اولیه

مسیریابی دستی[۱]

در نخستین روزهای تکنولوژی تلفن یک جفت سیم برای هر مشترک نیاز بود تا بتوان سیگنالها را از تلفن به مرکز وصل کنند در آنجا گروهی از اپراتورها به اتصال تماسها از تماس گیرنده به مقصد مشغول بودند.

کاربر دسته ای را می چرخاند که یک زنگ را در Switchboard مرکز به صدا در می آورد. اپراتوری -معمولا یک زن- هدفون خود را به خط مربوطه وصل میکرد و معمولا عبارت "شماره تلفن، لطفا" را میگفت، سپس با توجه به شماره داده شده بوسیله جک های مخصوصی که در اختیار داشت یک اتصال بین دو مشترک برقرار میکرد و سپس تماس گیرنده یکبار دیگر می بایست دسته را میچرخاند تا این بار به وسیله یک سری سیگنالهای پالسی زنگ صدای دستگاه تلفن مقصد به صدا در آید.

این سیستم شدیدا پرزحمت بود و از طرفی بسیار مستعد برای سواستفاده که در طی تلاشی برای جلوگیری از همین سو استفاده ها بود که نسل بعدی سوئیچ ها به وجود آمد.

اختراع سوئیچینگ اتوماتیک

آلمون استراوجر[۲] یک مقاطعه کار در امور کفن و دفن در شهر کانزاس در ایالات متحده بود. داستان از آنجا شروع شد که همسر یکی از رقبایش به عنوان اپراتور در مرکز تلفن کار میکرد و هر وقت که مشترکی شماره استراوجر را درخواست میکرد آن زن آنرا به شرکت رقیب یعنی شرکت همسرش وصل میکرد. این مسئله سبب شد که استراوجر ناامید شده و به فکر درست کردن سیستمی بیافتد که بتوان نقش انسان را ازین معادله حذف کرد.

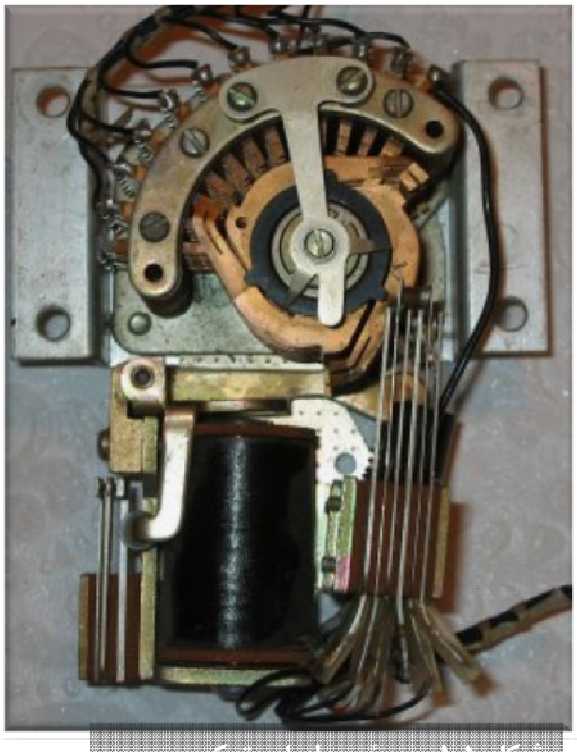
[۱] Manual Routing

[۲] Almon B.Strowger

استراوجر به کمک برادرزاده اش[۱] نوعی سیستم اتوماتیک بر پایه یک سوئیچ الکترومکانیکی که بر اساس الکترومغناطیس و چرخش یک یا چند چرخ دنده کار میکرد را توسعه داد. او مدلی عملی را در سال ۱۸۸۸ ارائه داد که بعدها هم ثبت گردید[۲]. در این سلکتور یک جاروب متحرک[۳] با داشتن یک کنتاکت در سر خود در بین بانکی از کنتاکتهای دیگر به حرکت میکرد (بالا یا طرفین) و یک اتصال با هریک به وجود می آورد.

استراوجر ایدهٔ سوئیچ اتوماتیک را ابداع نکرد؛ این ایده ابتدا در سال ۱۸۷۹ بوسیله Connolly & McTigthe ابداع شد ولی استراوجر اولین کسی بود که این مسئله را به یک کاربرد مؤثر رساند. وی به همراه Joseph B. Harris و Moses A. Meyer کمپانی خود را با نام در سال ۱۸۹۱ به نام "Strowger Automatic Telephone Exchange" بنا نهاد.

در اواخر ۱۸۹۰ استراوجر بازنشسته شد و سرانجام در سال ۱۹۰۲ فوت کرد. در سال ۱۹۰۱ Harris سلکتورهای استراوجر را به نام Automatic Electric Co. یا AE لایسنس کرد. دو شرکت در سال ۱۹۰۸ با یکدیگر ادغام شدند. کمپانی امروز هم تحت نام AG Communication Systems[۴] تحولات مختلفی را از سر گذرانده است.



شکل ۱.۱- سوئیچ رله ای تک محوره

سوئیچهای تک سلکتوری[۵]

در اینجا یک سوئیچ رله ای پله ای تک محوره را میبینید. این رله میتواند برای اجازه دادن به مشترک برای شماره گیری یک مشترک دیگر یکی از ده خط را بدین ترتیب انتخاب کند: وقتی مشترک شماره را میگیرد یک سری پالس الکتریکی بر روی خط تولید میشوند- در ماکزیمم نرخ ۱۰ پالس در ثانیه-. هر پالس موجب میشود روتر را که از مکان اولیه شروع میکند یک مرحله جلو ببرد و وقتی هر کنتاکت به یکی خط وصل باشند در این صورت این سلکتور به تنهائی به هر مشترک اجازه میدهد تا ۱۰ خط را در دسترس داشته باشد. در تئوری میتوان سیستم را با سری کردن چند تا ازین سلکتورهای توسعه داد به نحوی که وقتی یک زمان بین هر سری از پالسها مشاهده شده سری بعدی پالس به سلکتور بعدی میرود

---

[۱] Walter S. Strowger

[۲] US Patent No. 447918 10/6/1891

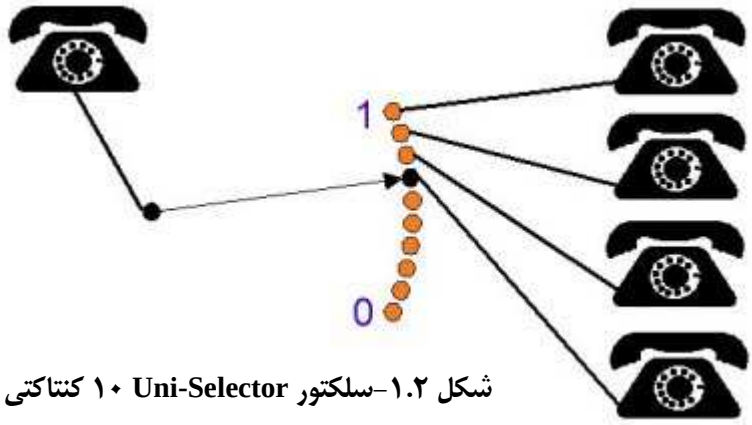
[۳] Moving Wiper

[۴] www.agcs.com

[۵] Uni-Selector Switches

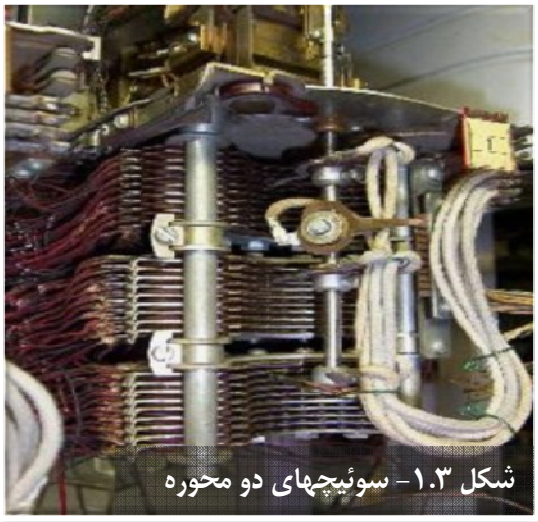
بدین ترتیب هد مشترک میتواند عوض ۱۰ تا به چندین برابر حالت یک روتر تماس بگیرید مثلا با ۳ روتر سری یک مشترک به ۱۰۰۰ مشترک دسترسی دارد. اما این روش در هنگام وجود مشترکین زیاد یا توسعه سیستم به شدت ناکارآمد است برای آنکه برای توسعه شبکه حتی به اندازه یک مشترک کلی مسئله پیش می آید. البته با Cascade کردن میتوان این روش را برای سیستم های ۵ رقمی توسعه داد ولی مسئله انعطاف پذیری و قابلیت توسعه و... با این عمل از بین نمی رود.

نوع بهتری از همین نوع Uni-Step به کار برده شد که این قابلیت را داشت که روتر ریست شده و به کنتاکت خانه برگردد. .



شکل ۱.۲–سلکتور Uni-Selector ۱۰ کنتاکتی

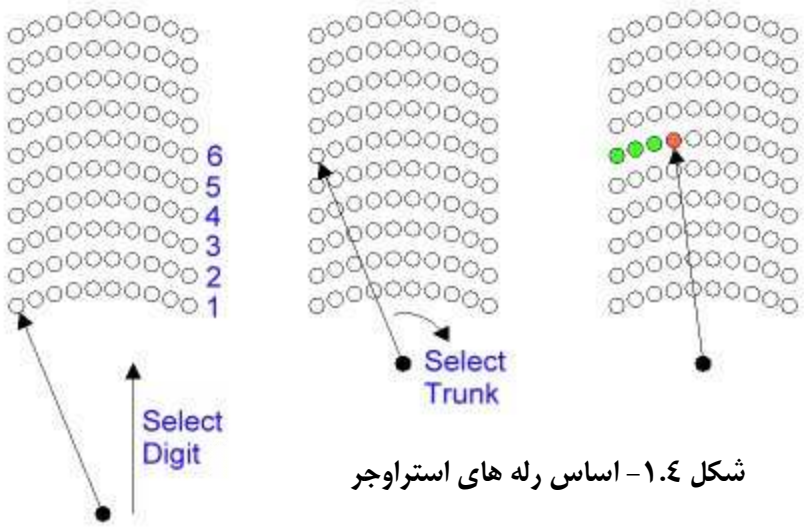
سوئیچهای دو محوره



شکل ۱.۳– سوئیچهای دو محوره

در عمل سوئیچها در رک ها و محفظها های مخصوص سوار میشوند. عمل اصلی یک روتر دو محور است یکی حرکت بالا/پائین است که حرکت ریست هم جزئی از همین نوع است و حرکت دوم مانند شکل بالا یک حرکت دورانی به اطراف است. یک رله واقعی ازین نوع سه هسته الکترومغناطیسی قرار دارد یکی برای حرکت بالا/پائین و دیگری برای حرکت به شکل گردشی و کار رله سوم نیز ریست کلی و بازگشت کنتاکت به محل اصلی و اولیه خود است. نمونه ای ازین نوع را در شکل ۱.۳ مشاهده میکنید:

Switching Mechanism (Trunking)

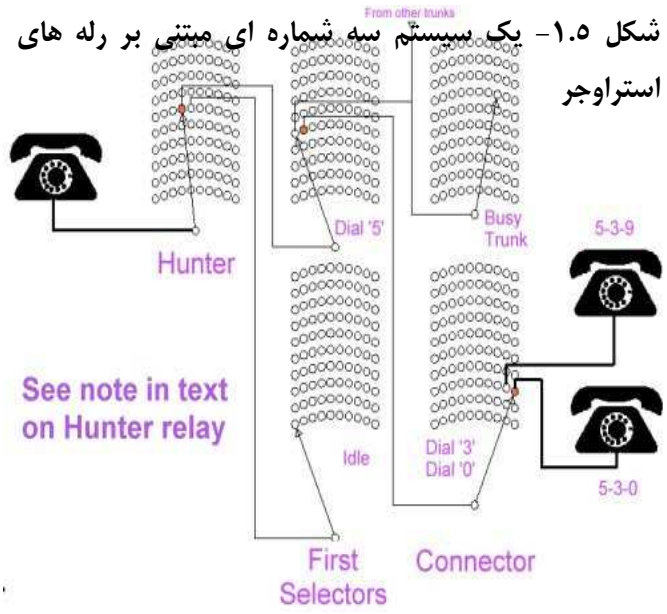


شکل ۱.٤- اساس رله های استراوجر

یک رله استراوجر میتواند جایگزین ۱۱ رله از نوع قبلی شود به نحوی که اولین مجموعه پالسهای شماره گیری رله ها متناسبا را در بانکی از کانتکتها چند قدم بالاتر میبرد و مجموعه بعدی پالسها رله را به گردش در می آورد تا به خط مقصد برسد. در این صورت سیستم رله مانند توده ای از ۱۰ رله Uniselector است که معرفی شد.

یک روش به کارگیری مفیدتر این رله ها شامل استفاده از Trunking که پالسهای تولید شده رله را بالا میبرد و بعد از آنکه یک مدار به شکل اتوماتیک به رله چسبید کانتکت را میچرخاند تا اولین trunk آزاد پیدا شود در مثال شکل ۱.۴ شمارهٔ ۶ شماره گیری شده و باعث میشود که رله ۶ ردیف بالا رود سپس به طور مداوم می چرخد تا یک trunk خالی پیدا کند و سپس آنرا به رله بعدی که شماره دوم را نمایندگی میکند وصل میکند. در شکل ۱.۴ سه trunk اول (کانتکتهای سبز) اشغال هستند و در دسترس نیستند اما trunk چهارم آزاد است و در نتیجه خط ورودی به آن وصل میشود.

شکل ۱.۵- یک سیستم سه شماره ای مبتنی بر رله های استراوجر



در شکل ۱.۵ یک سیستم سه شماره ای را نشان میدهد. اولین رله استراوجر در چپ را Hunter میخوانند، رله ای که به دنبال یک تلفن off-hook (گوشی برداشته شده) میگردد تا تماس را برقرار کند وقتی گوشی تلفن منزلی برداشته میشود ولتاژ خط که معمولا ۴۸ ولت است به ۱۲ ولت افت میکند. این رله خطهای

ورودی را جاروب میکند تا یک تلفن off-hook پیدا کند و بچرخد تا یک سلکتور آزاد را برای به اجرا درآوردن عمل شماره گیری پیدا کند. وقتی Hunter تلفن off-hook را پیدا کرد آن خط را به یک dial-tone geneator نیز وصل میکند تا مشترک از انجام شماره گیری خود و صحت سیستم مطمئن باشد. در این مثال هر دو سلکتور آزاد هستند و بنابراین اولین انتخاب میشود (بالائی). مشترک سپس اولین رقم یعنی ۵ را شماره گیری میکند در این مرحله سلکتور ۵ سطح بالا میرود. یک وقفه بین اعداد شماره گیری هست حالا سلکتور میچرخد تا اولین کانتکت آزاد را به رله بعدی پیدا کند در این مثال دومین سلکتور (که connector خوانده میشود) اشغال است پس رله بعدی (گوشه راست – پائین) انتخاب میشود. در هر زنجیر هر تعدادی ممکن است وجود داشته باشد و این بسته به امکانات سیستم هست هرچه تعداد سلکتورها در هر مرحله بیشتر امکان مواجهه شدن با اشغالی کمتر است. رله کانکتور دو شماره آخر را مدیریت میکند طبق این مثال کاربر شماره ۵۳۰ را شماره گیری کرده پس دو رقم آخر ۳ و ۰ است پس در سلکتور آخر شماره ۳ موجب رفتن کانتاکت به ردیف ۳ و شماره ۰ موجب چرخیدن کنتاکت ۱۰ قدم از چپ به راست است که در شکل مشخص شده است و این سبب میشود که صدای زنگ مشترک ۵۳۰ به صدا در آید به همین خاطر به سلکتور آخر کانکتور میگویند چرا که به هر یک از کانتکت های آن یک مشترک وصل شده است. برای شماره های بیشتر به سیستم بزرگتر و سلکتورهای بیشتری نیاز است.[1]

در سیستم بالا سه نوع رله معرفی شد-در سیستم های دیگر نیز به همین شکل است- رله hunter یا شکارچی که گوشی آماده شماره گیری را پیدا میکند. رله یا رله های میانی که به selector مشهورند و شماره های میانی را مسئول هستند و بیشترین تعداد را نیز دارند و رله طبقه آخر که به connector مشهور است و دو شماره آخر را مدیریت میکند و تماس را برقرار میکند. اما این سیستم که در اوایل قرن بیستم به کار برده شد برای شبکه های با مشترک زیاد مناسب نبود به این خاطر سیستم تقریبا مشابهی که عوض hunter از Line Finder استفاده میکرد به کار گرفته شد.این سیستم به وسیله Line Finder توسعه بیشتری یافت و به شکل مؤثرتری کار میکرد که مجال توضیح آن در اینجا نیست.[1]

شکل ۱.۶- یک سوئیچ قدیمی

[1] به عنوان نمونه یک سیستم ۷ شماره ای در اینجا آورده شده است:
http://technology.niagarac.on.ca/staff/mcsele/images/TelephoneRelayChain.jpg

شکل ۱.۷ – نمونه ای از یک سوئیچ استراوجر

اولین مرکز عمومی تبادل اتوماتیک

اولین مرکز عمومی در انگلستان در انگلستان در سال ۱۹۱۲ افتتاح شد. همانطور که گفته شد سوئچینگ دستی به یک اپراتور برای هر تماس نیاز داشت پس گران و وابسته به توانائی انسان بود با این وجود وقتی که اولین سیستم های سوئیچینگ اتوماتیک توسعه داده شد آنها نیز در مقام مقایسه گران بودند در سالهای بعد از جنگ جهانی اول (۱۹۱۴) کارگران زن ارزان بودند پس مزیت استفاده از سیستمهای اتوماتیک چندان زیاد نبود.

شکل ۱.۸ – سیستم تبادل تماس استراوجر

عکس ۱.۸ یک سیستم تبادل تماس استراوجر است که تا جولای سال ۱۹۹۵ در ساختمان عمومی Catford کار میکرد و سپس با یک سیستم مدرن تر عوض شد را نشان میدهد. این سیستم فضای بزرگی را اشغال میکرد سیستم جایگزین به اندازه یک کابینت بود! . سیستم قدیمتر به دقت توسط شرکت Telecomms Heritage Group برداشته شد و به موزه برده شد.

در پائین عکس یک سری باتریهای اسیدی می بینید که سیستم استراوجر از آنها به هنگام قطع برق استفاده میکرد.[2]

X.25

X.25 توسط گروه ITU[1] Study Group VII بر مبنای تعدادی از پروژهای شبکه داده پدیدار شده توسعه داده شد. مانند پروژه تحقیقاتی در آزمایشگاه فیزیک ملی بریتانیا زیر نظر Donald Davies که همان کسی بود که مفهوم شبکه های Packet Switch Networks را توسعه داد. در اواخر ۱۹۶۰ شبکه آزمایشی شروع به کار کرد و تا سال ۱۹۷۴ چند سایت به همدیگر لینک شده و SERCnet - یا همان Science and Engineering Research Council Networks – را تشکیل دادند. SERCnet بعدا رشد کرد و در سال ۱۹۸۴ تحت نام JANET دوباره سازماندهی شد که تا به امروز نیز ادامه دارد ولی به عنوان یک شبکهٔ TCP/IP. باقی شرکا در استاندارد کردن پروسه از شرکت ARPA آمده بودند. بهمراه افرادی از فرانسه، کانادا، ژاپن، و کشورهای اسکاندیناوی. در اوایل ۱۹۷۰ آپدیتهای متعددی در استاندارد به کار گرفته شد که درسری کتابهای تخصصی ITU گردآوری شده اند.[3]

X.25 یکی از اجزای پروتکل OSI است و یک مجموعه از پروتکلهائی است که بویژه در دهه ۸۰ بوسیله اپراتورهای مخابراتی و سیستمهای اقتصادی مانند دستگاههای خودپرداز به کار گرفته شدند. امروزه X.25 به طور وسیعی توسط پروتکلهای ارزانتر و ساده تر و ناامن تر جایگزین شده اند به ویژه پروتکل IP و با وجود اینکه هنوز اپراتورهای تلفنی هستند که ارتباطات مبتنی بر X.25 را با کانال سیگنالینگ خطوط ISDN ارائه میدهند X.25 قدیمیترین سرویس در دسترس Packet-Switch است. شبکه های X.25 گستردگی زیادی به ویژه در دهه ۸۰ تا ۹۰ میلادی در دنیا داشت.

X.25 هنوز برای کاربردهای مطمئن و ایمن مورد استفاده است مهمترین کاربرد آن در انتقال عملیات مربوط به کارتهای اعتباری و تشخیص هویت آنها و دستگاههای خودپرداز است.[4]

X.25 برای استفاده بر روی رسانه های غیر قابل اطمینان طراحی شد. X.25 بوسیله مکانیسم stack protocol خود مسئله تشخیص و تصحیح خطا را انجام میدهد. این سبب فشار مضاعفی بر ترافیک شبکه و توان در دسترس داده پردازی شبکه میشود..[5]

در دورهٔ بزرگی از تاریخ X.25 به عنوان PVC یا ارتباط مجازی دائم (Permanent Virtual Circuits) برای اتصال دو هاست کامپیوتری در یک لینک دائم مورد استفاده قرار میگرفت. یکی از این کاربردها بانک و نیاز آن

[1] International Telecommunication Union

به تکنولوژی مشابهی بود.X.25 به عنوان یک سیستم با هزینه ثابت ماهیانه و متناسب با سرعت یا پهنای باند ارائه شده توسط شرکت ارائه دهنده معرفی میشد. سرعتها بین 2.4Kbps تا 2Mbps تغییر میکردند.

مفهوم و هدف عام X.25 ایجاد بستری جهانی و Universal بر اساس مفهوم Packet Switch Network برای سیستمِ آنالوگِ مستعدِ خطایِ تلفن بود. بیشتر مستندات مربوط به X.25 شامل تدابیر سختگیرانه و دقیق برای دستیابی به این هدف است در حالیکه منابع قابل توجهی از منابع فیزیکیِ سرمایه برِ سیستم مصرف این منظور میگردد.

X.25 فقط اینترفیس بین مشترک (DTE) و یک شبکه X.25 (DCE) را تعریف میکند. X.75 یک پروتکل با مشابهت بسیار به X.25 است که اینترفیس بین دو شبکه X.25 را برای انتقال دو یا بیشتر کانکشن تعریف میکند. X.25 مشخص نمیکند که یک شبکه در داخل چگونه کار میکند، تعدادی از پیاده سازیهای X.25 از روشی بسیار شبیه خود X.25 یا X.75 استفاده میکنند اما بقیه از پروتکلهائی کاملا متفاوت در درون خود استفاده میکنند اما برای کاربر این مسئله بنا به خود X.25 و X.75 مهم نیست. ناهماهنگی فقط به این دلیل اتفاق می افتد که تمام شبکه ها از آخرین قوانین ارائه شده توسط CCITT یا ITU-T حمایت نمیکنند. پروتکل معادل با X.25 در سیستم ISO پروتکل ISO 8208 است که مشابه X.25 است با این تفاوت که علاوه بر آن شامل پاره از تدارکات برای دو X.25 DTE است که به شکل مستقیم به همدیگر متصل میشوند بدون وجود شبکه ای در بین این دو.[1]

مدل X.25 بر این اساس استوار شد که مفاهیم معمولی تلفن (تماس و...) را بر روی یک سیستم قابل اعتماد توسط منابع مشترک (Shared Resource) ولی به وسیله نرم افزاری که تماس مجازی را در شبکه ایجاد می کند تأسیس کند. این تماسها اتصال بین Data Terminal Equipment یا DTEها را که نقطه نهائی به کاربر هستند را به شکل یک تماس نقطه به نقطه برقرار میکند. هر endpoint که میتواند یک کاربر باشد میتوانند چندین تماس مجازی مجزا را به endpointهای متفاوت ایجاد کند.

تجهیزات انتخاب سریع[2] روشی بین برقراری تماس کامل و ارتباط بدون اتصال[3] است. Fast Select به طور وسیعی در کاربردهای Query-Response Transaction[4] مانند هویت سنجی کارتهای اعتباری و سیستمهای خودپرداز: درخواست اعتبار یک فیلد توسعه یافتهٔ درخواست تماس است و پذیرش درخواست یا عدم پذیرش یک فیلد توسعه یافتهٔ پاکت بستن تماس است. پروتکلهای X.29 & X.28 & X.3 که با X.25 ارتباط نزدیکی

---

[1] کاربر یا همان DTE را میتوان یک مودم در نظر گرفت در استاندارد X.25 تدارک خاصی برای اتصال مستقیم دو DTE وجود ندارد اما در استاندارد ISO8202 شرایطی برای اتصال مستقیم دو DTE که ممکن است کاربرد هم داشته باشد فراهم آماده است./س

[2] Fast Select Facility

[3] Connection-less

[4] تراکنش پرس و جو - پاسخ

دارند پروتکلهائی با هدف اتصال ادوات غیر سنکرون مانند PC و Dumb Terminals هستند. این عملکرد با استفاده از PAD[1] انجام میگیرد.[6]

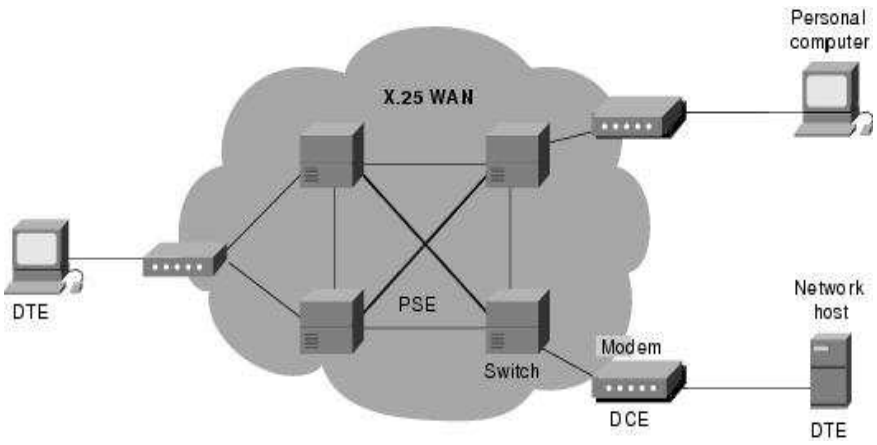
ادوات و عملیات پروتکلی

اجزاء یک شبکه X.25 به سه گروه کلی تقسیم میشوند:

1. Data Terminal Equipment (DTE)
2. Data Circuit-Termination Equipment (DCE)
3. Packet Switching Exchange (PSE)

DTE ها گره های پایانی هستند و در کناره های شبکه به کار گرفته میشوند. آنها معمولا ترمینالها، کامپیوترهای شخصی و کامپیوترهای میزبان شبکه هستند و بیشتر متعلق به مشترکین شبکه می باشند. ادوات DCE نوعی از ادوات ارتباطی مانند مودم ها و Packet Switch ها هستند که که یک اینترفیس بین DTE ها و PSE ها فراهم میکنند و معمولا در تأسیسات ارائه دهنده یا حامل دیده میشوند. PSE ها قطعاتی هستند که توده عمده شبکه را تشکیل میدهند آنها دیتا را از یک DTE به DTE دیگر بوسیله X.25 PSN در شبکه انتقال میدهند. شکل ۱.۹ این سه نوع وسیلهٔ مورد استفاده در شبکه X.25 را نشان میدهد.[2]

Fig1.9: DTEs, DCEs, and PSEs Make Up an X.25 Network Packet



Assembler/Disassembler

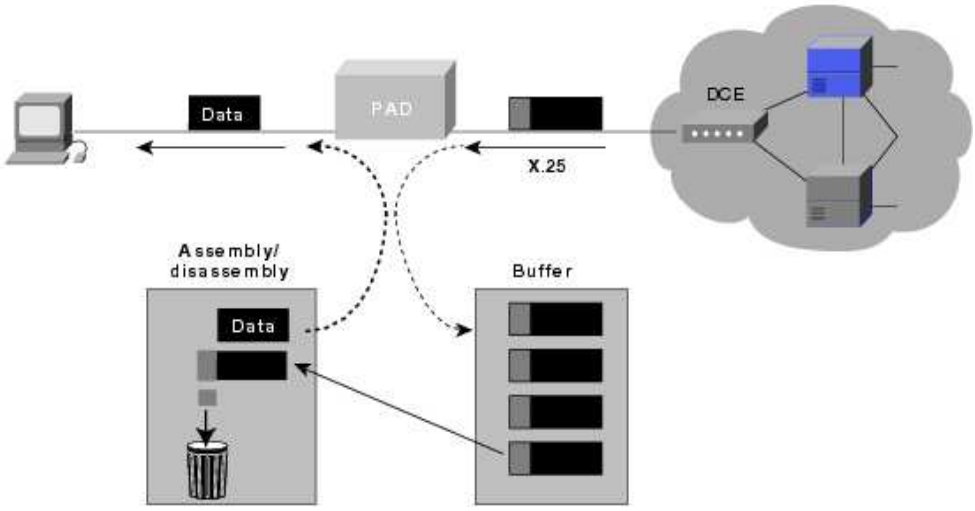
PAD وسیله ای است که به طور عام در شبکه های X.25 یافت میشود. PAD ها موقعی به کار برده میشوند که DTE به عنوان مثال یک ترمینال کاراکتری برای پیاده کردن کامل توابع X.25 بسیار ساده است

[1] Packet Assembler/Dis-assembler

[2] این مسئله حائز اهمیت است که بعضی منابع دیگر ادوات شبکه را تنها به دو گروه endpoint و سوئیچهای internetwork تقسیم کرده اند./س

دراین حالت PAD بین DTE و DCE قرار میگیرد و سه عملیات اصلی را انجام میدهد: بافرکردن (ذخیره داده تا وقتی وسیله آماده کار با آن شود.) سرهم کردن پاکت یا Packet Assembly و Packet Disassembly . که در واقع header یا سرآیند مخصوص X.25 را به پاکت اضافه و یا کم میکند.PAD داده های فرستاده شده یا رسیده از DTE را بافر میکند و همچنین دیتای خروجی را به شکل پاکت اسمبل میکند و به DCE می فرستد (این شامل سرآیند X.25 هم میشود.) و پاکتهای ورودی را سوا میکند تا به DTE بفرستد (که شامل برداشتن سرآیند X.25 است.) که این عملیات در نمودار ۱.۱۰ آورده شده است:

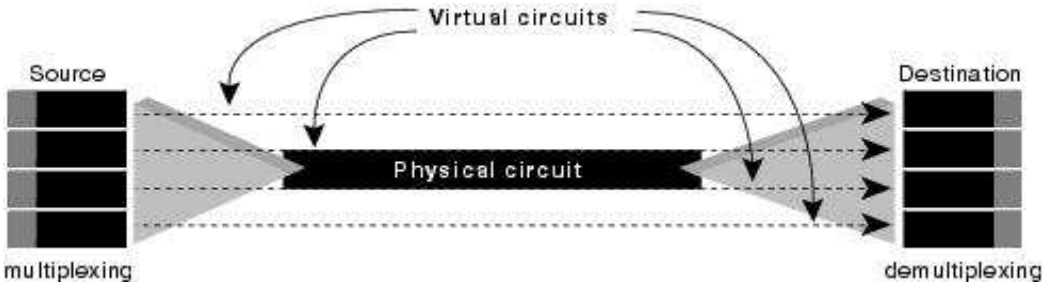
Fig1.10: The PAD Buffers, Assembles, and Disassembles Data Packets



تأسیس جلسه و مدار مجازی در X.25

در اینجا به خاطر دوری از اطناب به جزئیات کامل شبکه های X.25 نمی پردازیم. شبکه های X.25 هم مانند شبکه های جدیدتر قادر به ایجاد تماس مجازی به عنوان یک پروتکل اتصالگرا هستند و روشها و مراحلی را نیز برای ایجاد یک تماس دارند. که در اینجا نوعی از برقرای مفهومی یک اتصال مجزای را در این نوع شبکه میبینید.

Fig1.11: Virtual Circuits Can Be Multiplexed onto a Single Physical Circuit

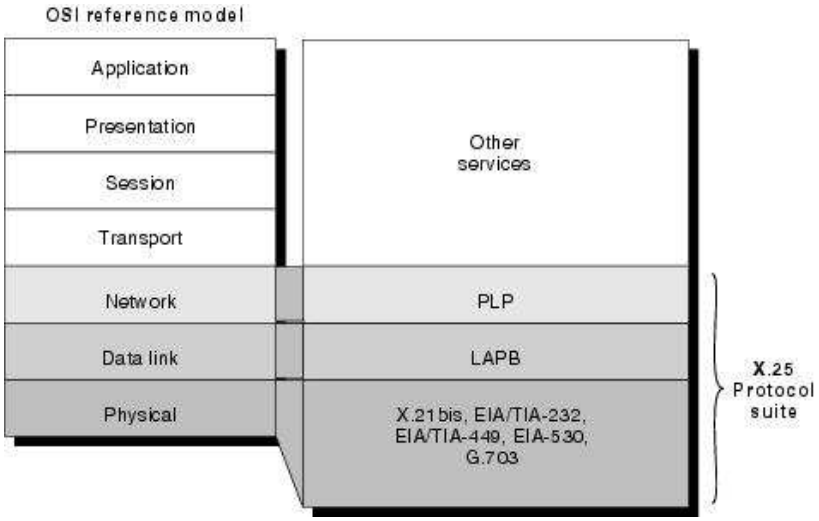


دو نوع اتصال مجزای در شبکه X.25 وجود دارد: Switched و Permanent . نوع اول که به SVC موسوم است یک تماس موقت است که ارسال داده های گاه به گاه استفاده میشود. آنها نیاز دارند که دو DTE هر موقع که نیاز بود یک اجلاس یا همان session را ایجاد، مدیریت و نگهداری، و سپس ببندند. PVC ها برای داده های پرکاربرد مورد استفاده قرار میگیرند. در PVC نیاز نیست که session ایجاد و بسته شود. پس DTE ها میتوانند هر وقت که لازم بود اقدام به تبادل داده کنند چرا که اتصال همواره برقرار است[1]. جزئیات چگونگی ایجاد و نگهداری و بستن این اتصالات در این بحث نمیگنجد.

بستهٔ پروتکلی X.25

این بسته سه لایه پائینی مدل OSI را شامل میشود. این پروتکلها نوعا در پیاده سازی X.25 مورد استفاده قرار میگیرند: Packet Layer Protocol (PLP) و Link Access Procedure Balanced (LAPB) و آن پروتکلهائی که به لایه های فیزیکی اینترفیس سریال مربوط هستند مثل – EIA/TIA-232 – EIA/TIA-449 EEA-530 & G.703 نمودار ۱.۱۲ این مطلب را نشان میدهد:

Fig1.12: Key X.25 Protocols Map to the Three Lower Layers of the OSI Model



[1] این مثل وجود یک خط ویژه یا Dedicated Line در سرویسهای مخابراتی است که به شکل مجازی پیاده شده است./س

پروتکل لایهٔ پاکت

PLP یک پروتکل لایه شبکه X.25 است. PLP تبادل پاکت بین DTE ها را از طریق اتصالات مجازی مدیریت میکند. PLP همچنین میتواند برد روی Logical Link Control 2 یا LLC2 یا یک ISDN که LADP را دارد پیاده شود. PLP در ۵ مود مشخص کار میکند:

Call setup, Data transfer, Idle, Call clearing, and restarting.

به خاطر تلخیص مطلب از توضیح هر یک با توجه به وضوح کاربرد این مودها با توجه به نام آنها خودداری میکنیم و دیگر اینکه یک پاکت PLP ۴ نوع فیلد دارد که در زیر به شکل استاندارد آن آورد میشود:

- **General Format Identifier (GFI)—**Identifies packet parameters, such as whether the packet carries user data or control information, what kind of windowing is being used, and whether delivery confirmation is required.
- **Logical Channel Identifier (LCI)—**Identifies the virtual circuit across the local DTE/DCE interface.
- **Packet Type Identifier (PTI)—**Identifies the packet as one of 17 different PLP packet types.
- **User Data**—Contains encapsulated upper-layer information. This field is present only in data packets. Otherwise, additional fields containing control information are added.

Link Access Procedure, Balanced

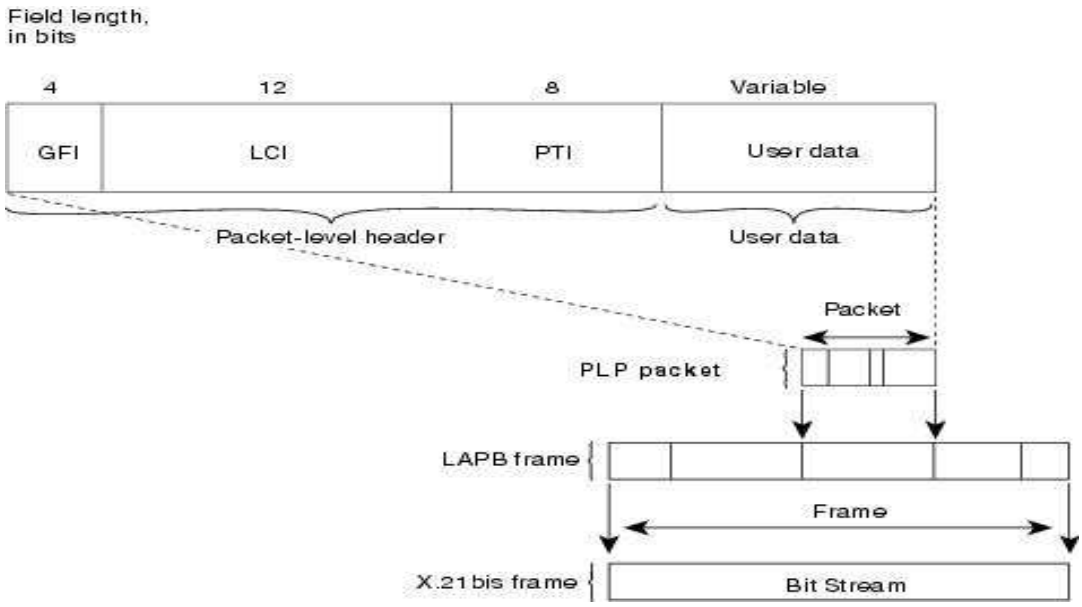
LAPB یک پروتکل لایه دیتا است که ارتباطات و packet frame های بین DTE و DCE را مدیریت میکند. LAPB یک پروتکل بیت-گرا[1] است که از ترتیب درست و صحیح بودن فریمها اطمینان حاصل میکند.جزئیات بیشتر LAPB در اینجا لحاظ نگردید است.

پروتکل *X.21bis*

X.21bis یک پروتکل سطح لایه فیزیک است که سیگنالینگ، نحوه تخصیص رقمها در سیستمهای تلفنی و حتی عملیات ارتباط مکانیکی را مدیریت میکند که در اینجا بدان پرداخته نمیشود. تنها در نمودار ۱.۱۳ پاکت PLP و نحوه ارتباط آن با داده های لایه های پائین تر یعنی LAPB و X21bis آورده شده است.

The PLP Packet Is Encapsulated Within the LAPB Frame and the X.21bis Frame **Fig1.13:**

[1] Bit-Oriented



از رواج افتادن

با گسترده شدن کلمه Perfect در کیفیت سرویسهای دیجیتال و قابلیت تصحیح خطای مودمها امروزه دیگر X.25 مانند قبل ارزشمند نیست. نتیجه به Frame Relay منتج گشته که به نحوی میتوان گفت که تدابیر سختگیرانهٔ X.25 را برداشته و در مقابل به کارائی بالاتری نسبت به سلف خود رسیده است. مفهوم اتصال مجازی کماکان بوسیلهٔ ATM استفاده میشود تا مدیریت ترافیک و مالتی پلکسینگ شبکه همچنان فراهم باشد.

X.25 today

شبکه های X.25 همچنان در همه جای جهان مورد استفاده قرار میگیرند. اگرچه در یک تنزل دراماتیک با جایگزین شدنش توسط تکنولوژیهای جدیدتر لایه ۲ مانند Frame Relay و ISDN و ATM و ADSL و POS و پروتکل همه جا موجود لایه ۳ : IP به نظر میرسد به پایان راه نزدیک شده باشد اما X.25 همچنان به عنوان تنها لینک قابل اعتماد موجود در بسیاری از بخشهای در حال توسعه دنیا باقی مانده است جائیکه دسترسی به یک PDN ممکن است که قابل اعتمادترین و کم هزینه ترین راه دسترسی به اینترنت باشد. از طرفی X.25 همچنین به طور وسیع بوسیلهٔ رادیوهای آماتوری packet-base مورد استفاده قرار میگیرد.

با وجود اینکه تلاشهائی مبنی بر جایگزین کردن X.25 با پروتکل کمتر قابل اعتماد ولی ارزانتر و کاراتر TCP/IP در میان هست، Racal Paknet که امروزه به Widanet مشهور است هنوز در بسیاری نقاط جهان از X.25 استفاده میکند. Widanet معمولا برای GPS Tracking و point-of-sale به کار میرود.

در بعضی کشورها مانند هلند یا آلمان امکان استفاده از نوعی از X.25 برروی D-Channel یک ISDN-2 برای کاربردهای کم حجم مانند یک ترمینال Point-of-Sale ممکن است اما در کل آینده این پروتکل چندان مشخص نیست.[7]

Frame Relay

Frame Relay یک تکنولوژی Packet-Switched است که نقاط انتهائی شبکه را قادر میکند تا به شکلی پویا منابع شبکه را به اشتراک بگذارند.

Frame Relay به عنوان نسخه مؤثرتر X.25 معرفی میگردد به خاطر اینکه به دو خاصیت Windowing و Retransmission که در X.25 یافت میشود نیاز ندارد. این در اصل به این واقعیت بر میگردد که سرویسهای Frame Relay نوعا روی شبکه ها و ادوات قابل اعتمادی به کار گرفته میشوند.

شبکه های Frame Relay نوعا به عنوان جایگزینی مؤثرتر به لحاظ هزینه برای خطوط خصوصی point-to-point یا leased line به خدمت گرفته میشود. در حالیکه مشتریان point-to-point متحمل هزینهٔ ماهیانه برای دسترسی محلی و هزینه برای یک اتصال دوربرد میشوند اما مشتریان Frame Relay تنها بخشی از هزینهٔ مربوط به دوربرد بودن خط را می پردازند. هزینهٔ دوربرد بودن خط نوعا بوسیله تکنولوژی Virtual Circuit بر حسب استفاده تقسیم میشود.

Frame Relay توسط دو مؤسسه استاندارد شده بوسیلهٔ ITU-T[1] و از طرف دیگر توسط ANSI این کار صورت گرفته است.[5]

Frame Relay & Cell Relay

Frame Relay اساسا با Packet Switching یکی است. F.R توسعه خود را در اثر سرعتهای بالای انتقال داده و کم خطای سیستمهای ارتباطی مدرن می بیند. در سیستمهای Packet-Switched قدیمی مقدار قابل توجهی سرآیند مربوط به تشخیص و بازیابی خطا وجود داشت که سبب افزایش افزونگی و اطلاعات مسیریابی میشد. بهمراه F.R پاکتها دارای طول متغیرند نه ثابت و این یعنی برای سرعتهای تا 2Mbps جواب میدهند و این برای VBR مناسب است. Cell Relay پاکتهای با طول ثابت را استفاده میکند و همچنین کانالهای چند نرخ ثابت را حمایت میکند. Cell Relay اجازه تعریف پویای کانالهای مجازی را میدهد. در مقایسه با F.R ، Cell Relay کنترل خطای بهتری را به کار میگیرد به طوری که قابلیت کار با سرعتهای بالاتر را فراهم میکند سلول با طول ثابت Overhead را در Packet-Switchig کاهش میدهد و به سرعتهای چند ده و چند صد مگابیت در ثانیه هم اجازه پیاده شدن میدهد.از طرفی Cell Relay از هردوی CBR وVBR به خوبی حمایت میکند. این طول پاکت ثابت برخلاف F.R زمینه ساز ATM است.[8]

[1] International Telecommunication Union Telecommunication-Standardization Sector

Frame Relay یک پروتکل WAN با عملکرد بالاست که در لایه های فیزیکی و پیوند داده در مدل OSI کار میکند. F.R در اصل برای استفاده در اینترفیس ISDN ساخته شد ولی امروزه در اینترفیسهای دیگر نیز به کار میرود.

F.R به عنوان یک تکنولوژی Packet-Swithed از دو تکنیک استفاده میکند:

- Variable Length Packet
- Statistical Multiplexing

پاکت طول متغیر به منظور انتقال دادهٔ مؤثرتر و انعطاف پذیرتر استفاده میشود. این پاکتها بین بخشهای مختلفی از شبکه سوئیچ میشوند تا به مقصد برسند.

تکنیک مالتی پلکس آماری دسترسی به شبکه در یک شبکه پاکت-سوئیچ را کنترل میکند. مزیت این تکنیک آماده کردن استفاده مؤثرتر و انعطاف پذیر تر از پنهای باند است. همانطور که گفته شد F.R نسبت به جد خود X.25 بسیاری از خواصی را که به خاطر قابلیت اعتماد پائین منابع در دهه ۷۰ و اوایل ۸۰ بود و X.25 برای آن منابع نه چندان قابل اعتماد ساخته شده بود را حذف کرد. F.R یک پروتکل است که کاملا در لایه ۲ قرار دارد در حالیکه X.25 در لایه ۳ هم سرویس میداد و خود این هم یکی از دلایل قدرت F.R در دادن امکانات بهتر نسبت به X.25 است.

Frame Relay origins

قبلا مقداری راجع به این امر گفته شد. در واقع F.R خود را از امر تصحیح خطا آزاد کرد. وقتی F.R یک خطا را پیدا میکند به سادگی آنرا ارسال نمیکند و به اصطلاح discard میکند. F.R از مفاهیم دسترسی مشترک استفاده میکند و بر تکنیکی که به عنوان best-effort استوار است که بوسیلهٔ آن تصحیح خطا عملا وجود ندارد و هیچ تضمینی برای انتقال صحیح داده نمیدهد و این را در واقع به عهده لایه های دیگر میگذارد. F.R یک استاندارد صنعتی کپسوله سازی را فراهم میکند که قدرت Packet-Switched را به سرعتهای بالا میبرد و به سرویسهای چند Virtual Circuit و چند پروتکلی اجازه برقرای بین دو روتر را میدهد.

Eric Scace یک مهندس در Sprint International تکنولوژی Frame Relay را اختراع کرد. او طراحی خود را بر پایه کارهای قبلی خود در توسعه AX.25 گذاشت. یک سیستم پاکت سوئیچ برای رادیوی آماتوری. Sprint International که بعدا در سال ۲۰۰۵ جزئی از Sprint Nextel شد با StrataCom برای اولین پیاده سازی قرارداد بست و سخت افزارهای StrataCom را در شبکه های دیتا عمومی به خدمت گرفت و اولین سرویس عمومی Frame Relay را ارائه داد.[9]

Frame Relay Standardization

طرح اولیه برای استاندارد کردن Frame Relay در سال ۱۹۸۴ به کمیته مشورتی در ITT [۱] به خاطر مشکل کمبود قابلیت سازگاری با سیستمهای دیگر و عدم وجود یک استاندارد کامل Frame Relay در دهه ۸۰ و حتی اواخر آن چندان به کار گرفته نشد.

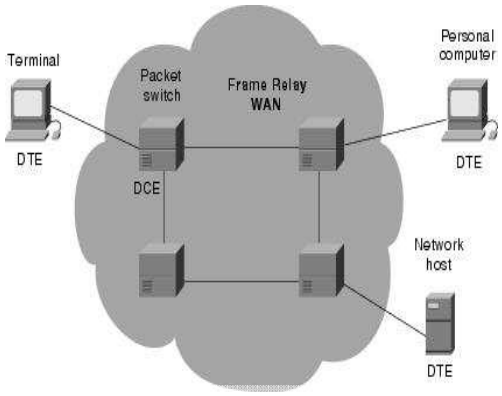
به خدمت گیری عمدهٔ F.R در سال ۱۹۹۰ رخ داد وقتی Cisco و DEC[۲] و Northern Telecom و StartaCom یک کنسرسیوم تشکیل دادند تا بر توسعه تکنولوژی Frame Relay تمرکز کنند. این کنسرسیوم یکسری مشخصات را توسعه داد که با استاندارد اولیه ای مطابق بود که در CCITT مورد بحث قرار گرفته بود بعلاوهٔ خاصیتهائی که قابلیت کار در محیطهای پیچیده و متنوع را میداد. این الحاقیه به Frame Relay عموما با نام Local Management Interface یا LMI خوانده میشود.

از هنگامی که کنسرسیوم specification خود را توسعه داد و سپس منتشر کرد بسیاری از فروشندگان ساپورت خود را ز Frame Relay اعلام کردند. و ANSI و CCITT بدنبال آن استاندارد خود را با LMI مطابقت دادند و این استاندارد از نمونه اولیه معمولتر شد.

F.R به طور کلی در آمریکا بیشتر تحت استاندارد ANSI و در بقیه دنیا تحت استاندارد ارائه شده توسط ITU-T به کار گرفته میشود که البته این دو بسیار به هم شبیه اند.

Frame Relay Devices

مانند X.25 میتوان اداوات شبکه را به دو بخش عمده DTE و DCE تقسیم کرد که در آنجا توضیح داده شد. اتصال بین DTE وDCE شامل اجزا هم لایه فیزیک و هم پیوند داده است.



شکل ۱.۱٤– ادوات مختلف شبکهٔ F.R

[۱] Consultative Committee on International Telephone and Telegraph (CCITT)

[۲] Digital Equipment Corporation

Frame Relay Virtual Circuits

Frame Relay یک ارتباط لایهٔ پیوند دادهٔ اتصال-گرا را فراهم میکند. این یعنی اینکه هر ارتباط بین هر جفت ادوات شبکه یک مشخص کننده یا identifier دارد. این سرویس بویسیلهٔ F.R Virtual Circuit پیاده میشود که یکجور اتصال منطقی (و نه فیزیکی) است که بین دو DTE در شبکه Packet Switch فریم رلی برقرار میگردد.

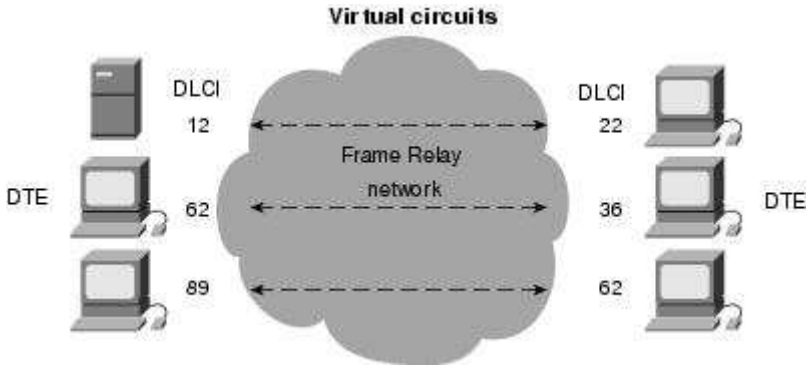
Virtual Circuit یک ارتباط دو طرفه بین دو DTE را فراهم میکند و به طور یگانه توسط یکه مشخص کننده سطح پیوند داده برچسب گذاری میشود که به DLCI[1] موسوم است. چندین VC میتوانند به یک اتصال فیزیکی مولتی پلکس شوند. و این باعث کم هزینه تر شدن و سهولت اتصال بین دو DTE میشود. در اینجا هم مانند X.25 دو نوع VC هست: سوئیچ و دائم : PVC و SVC .

به طور خلاصه SVC یک اتصال موقت مانند همانی است که در X.25 توضیح داده شد و دارای چهار حالت عملیاتی است: Call Setup & Data Transfer & Idle & Call Termination در مقابل نوع دائم که همان PVC تنها دو حالت Idle و Data Transfer را دارد.

Data-Link Connection Identifier

DLCI[2] یا Data-Link Connection Identifier توسط ارئه دهنده سرویس F.R فراهم میشود و این فیلد در واقع ارزش محلی دارد به معنی اینکه مقدار آن در LAN یکتاست ولی این یکتائی در مقیاس WAN لزومی ندارد. نمودار زیر نشان میدهد که چگونه دو DTE مختلف میتوانند به یک DLCI نگاشته شوند البته در یک شبکه WAN .

Fig1.15: A Single Frame Relay Virtual Circuit Can Be Assigned Different DLCIs on Each End of a VC



[1] Data Link Connection Identifier

[2] این فیلد در MPLS هم به کار برده میشود که در جای مقتضی به کار برده میشود.

Congestion-Control Mechanisms

F.R سرریز شبکه را با یک مکانیسم ساده اخطار ازدحام به جای کنترل صریح هر یک از VC ها پیاده میکند. F.R نوعا روی رسانه های قابل اعتماد پیاده میشود پس جامعیت داده قربانی کنترل جریان نمیشود و این کار به عهده پروتلکهای لایه های بالاتر گذاشته میشود. F.R دو مکانیسم اخطار ازدحام را به کار میگرد:

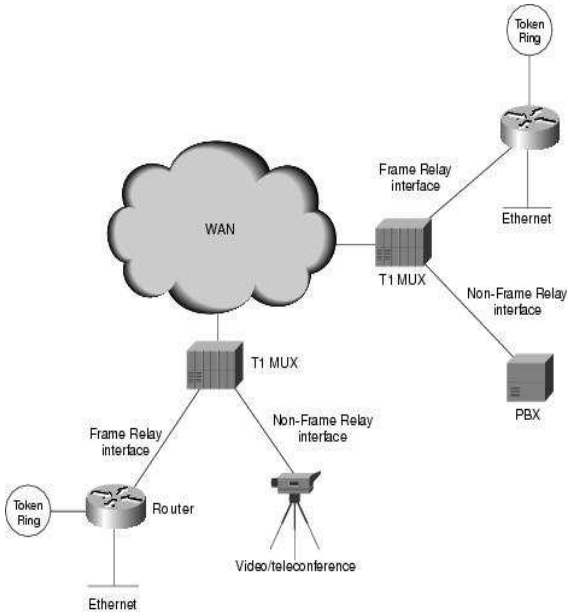
- Forward-explicit congestion notification (FECN)
- Backward-explicit congestion notification (BECN)

FECN و BECN هر یک با یک بیت که در سرآیند F.R هست کنترل میشوند علاوه بر آنها یک بیت موسوم به Discard Eligibility یا DE وجود دارد که نشان میدهد آن پاکت از ارزش ترافیکی پائینی برخوردار است و در صورت ازدحام و شلوغی میتواند discard گردد.

برای اطلاعات بیشتر میتوان به مراجع اصلی و یا گزارش قبلی که در لوح فشرده آمده است مراجعه کرد.

Frame Relay Network Implementation

یک پیاده سازی Private F.R network معمولا با تجهیز شدن به یک مالتی پلکسر T1 بهمراه هر دو اینترفیس F.R و غیر F.R انجام میشود. نوعی از این پیاده سازی در مقیاس WAN در شکل ۱.۱۶ مشاهده میشود در این شکل اینترفیسهای مختلف مشاهده میگردد. در ادامه دو نوع پیاده سازی عمومی و خصوصی F.R معرفی میگردد.



شکل ۱.۱۶- یک پیاده سازی نوعی F.R در مقیاس WAN

Public Carrier-Provided Networks

در پیاده سازی عمومی شبکه F.R تجهیزات در مرکز تلفن یا مخابرات قرار میگیرد و مشترک بر اساس استفاده از شبکه متحمل هزینه میشوند اما دیگر مسئولیت و هزینه ای در قبال نگهداری و مدیریت و مالکیت تجهیزات شبکه و سرویسها ندارند. معمولا تجهیزات DCE متعلق به شرکت ارائه دهنده است و در مالکیت وی می باشد از طرفی DTE هم معمولا توسط مشترک خریداری میشود و در مالکیت مشترک است البته ممکن است شرکت ارائه دهنده به عنوان بخشی از سرویس خود ادوات DTE را به شکل کامل یا دوره ای در اختیار مشترک بگذارد. اکثر شبکه های F.R به کار گرفته شدهٔ امروز از این نوع اند.

Private Enterprise Networks

این نوع شبکه ها بیشتر توسط سازمانها مورد استفاده قرار میگیرند. در این نوع شبکه مسئولیت تجهیزات و ادوات و مدیریت و نگهداری آنها به عهده سازمان سرویس گیرنده است . تمام تجهیزات در مالکیت مشتری است.

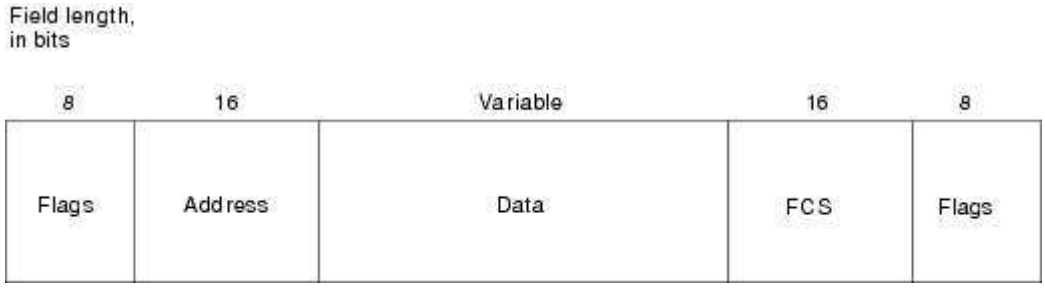
Frame Relay Frame Formats

برای فهمیدن خواص F.R مهمترین مسئلهٔ آشنائی با ساختار فریم است که در شکل نشان داده شده است. البته این شکل فریم پایه و basic را معرفی میکند. و در شکل بعدی ورژن LMI آن آمده است.

Flag ها ابتدا و پایان فریم را مشخص می کنند. اجزا ابتدائی یک فریم F.R را : سرآیند – آدرس – دیتای کاربر و FCS[1] تشکیل میدهند. بخش آدرس که ۱۶ بیت است شامل ۱۰ بیت مشخص کننده VC و ۶ بیت مربوط به مدیریت ترافیک است. آن ۱۰ بیت بیشتر به اسم DLCI مشهور است.

در شکل ۱.۱۷ ساختار همراه با توضیح متناسب آورده شده است بخشهای رسمی ترجمه نشده اند:

Fig1.17: Five Fields Comprise the Frame Relay Frame



- ✓ -- **Flags**—Delimits the beginning and end of the frame. The value of this field is always the same and is represented either as the hexadecimal number 7E or as the binary number 011111101.

[1] Frame Check Sequence

- ✓ **Address**—Contains the following information:
- ✓ – **DLCI**—The 10-bit DLCI is the essence of the Frame Relay header. This value represents the virtual connection between the DTE device and the switch. Each virtual connection that is multiplexed onto the physical channel will be represented by a unique DLCI. The DLCI values have local significance only, which means that they are unique only to the physical channel on which they reside. Therefore, devices at opposite ends of a connection can use different DLCI values to refer to the same virtual connection.
- ✓ – **Extended Address (EA)**—The EA is used to indicate whether the byte in which the EA value is 1 is the last addressing field. If the value is 1, then the current byte is determined to be the last DLCI octet. Although current Frame Relay implementations all use a two-octet DLCI, this capability does allow longer DLCIs to be used in the future. The eighth bit of each byte of the Address field is used to indicate the EA.
- ✓ – **C/R**—The C/R is the bit that follows the most significant DLCI byte in the Address field. The C/R bit is not currently defined.
- ✓ – **Congestion Control**—This consists of the 3 bits that control the Frame Relay congestion-notification mechanisms. These are the FECN, BECN, and DE bits, which are the last 3 bits in the Address field.

علاوه بر موارد بالا، بیت FECN یک فیلد تک بیتی است که میتواند توسط یک سوئیچ برای نشان دادن به DTE نهائی ست به ۱ شود. این سوئیچ یا روتر نشان میدهد که در مسیر مورد نظری که پاکت از آنجا آمده ازدحام وجود دارد. فایده این کار اینست که به پروتکلهای لایهٔ بالاتر اجازه میدهد که به شکل هوشمندانه ای با این شواهد و قرائن کار کنند. امروزه DECnet و OSI تنها پروتکلهای لایه بالاتری هستند که این قابلیت را پیاده میکنند. فیلد تک بیتی BECN بوسیلهٔ یک سوئیچ مثل روتر به ۱ ست میشود تا نشان دهد که در مسیر مورد تجربه پاکت از مقصد به مبدا (برعکس قبل) ترافیک بالا رفته است. بیت DE بوسیله DTE ست میشود تا نشان دهد که پاکت نشانه گذاری شده در مقایسه با بقیه پاکتها، پاکت ارزشمندی نیست و در صورت ازدحام میتوان آنرا Discard کرد.

- ✓ • **Data**—Contains encapsulated upper-layer data. Each frame in this variable-length field includes a user data or payload field that will vary in length up to 16,000 octets. This field serves to transport the higher-layer protocol packet (PDU) through a Frame Relay network.
- ✓ • **Frame Check Sequence**—Ensures the integrity of transmitted data. This value is computed by the source device and verified by the receiver to ensure integrity of transmission.

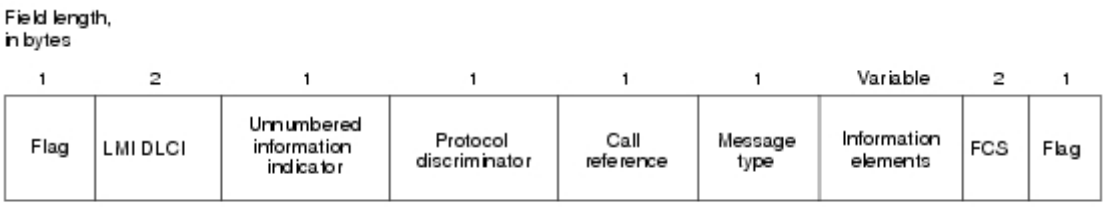
LMI Frame Format

در اینجا نیز ورژن LMI همانند بخش قبل معرفی میشود:

---

[1] Base upon the Wikipedia:

Flag Field. The flag is used to perform high-level data link synchronization which indicates the beginning and end of the frame with the unique pattern 01111110. To ensure that the 01111110 pattern does not appear somewhere inside the frame, bit stuffing and destuffing procedures are used See:
http://en.wikipedia.org/wiki/Bit_stuffing



- ✓ • **Flag**—Delimits the beginning and end of the frame.
- ✓ • **LMI DLCI**—Identifies the frame as an LMI frame instead of a basic Frame Relay frame. The LMI-specific DLCI value defined in the LMI consortium specification is DLCI = 1023.
- ✓ • **Unnumbered Information Indicator**—Sets the poll/final bit to zero.
- ✓ • **Protocol Discriminator**—Always contains a value indicating that the frame is an LMI frame.
- ✓ • **Call Reference**—Always contains zeros. This field currently is not used for any purpose.
- ✓ • **Message Type**—Labels the frame as one of the following message types:
- ✓ – **Status-inquiry message**—Allows a user device to inquire about the status of the network.
- ✓ – **Status message**—Responds to status-inquiry messages. Status messages include keepalives and PVC status messages.
- ✓ • **Information Elements**—Contains a variable number of individual information elements (IEs). IEs consist of the following fields:
- ✓ – **IE Identifier**—Uniquely identifies the IE.
- ✓ – **IE Length**—Indicates the length of the IE.
- ✓ – **Data**—Consists of 1 or more bytes containing encapsulated upper-layer data.
- ✓ • **Frame Check Sequence (FCS)**—Ensures the integrity of transmitted data.

[10].

با پیشرفت MPLS ، VPN و سرویسهای اختصاصی پهن باند مانند Cable Modem و DSL ممکن است پروتکل و کپسوله سازی F.R به انتهایش نزدیک شده باشد. اما هنوز مناطقی هستند – مثلا مناطق روستائی و کم جمعیت در آمریکا و کانادا و نقاط دیگر در دنیا – که با فقدان DSL و یا کابل مواجهه اند. در یک چنین مناطقی ممکن است کم هزینه ترین ارتباط دائم ۶۴ کیلوئی همین F.R باشد. همچنین فروشگاهای زنجیره ای که از تبادل اطلاعات پائینی برخوردارند گاها از F.R برای ارتباط بین شعبه های خود در مناطق دور افتاده استفاده میکنند.

F.R با این هدف ساخته شد که از منابع فیزیکی موجود به شکل مؤثرتری استفاده کند. F.R با هدف استفادهٔ موثرتر از منابع فیزیک طراحی شد و به شرکتهای مخابراتی این اجازه را میداد که یک سرویس دادهٔ دائمی به مشتریانش ارائه دهد. در سالهای اخیر F.R به یک سوء شهرت به خاطر رزواسیون افراطی پهنای باند توسط شرکتها در بازار رسیده است.

شرکتهای مخابراتی معمولا F.R را به مشتریانی میفروشند که دنبال جایگزینی ارزانتر برای خطوط اختصاصی هستند. استفاده و کاربرد F.R به شدت وابسته به سیاستهای دولتی و شرکتهاست.

AT&T امروزه یکی از بزرگترین ارائه دهندهٔ سرویسهای F.R در آمریکا است که ۲۲ شبکه محلی در ۲۲ ایالت را دارد به اضافه شبکه های ملی و بین المللی. این تعداد به نظر میرسد در بین سالهای ۲۰۰۷ تا ۲۰۰۹ همزمان با به پایان رسیدن قراردادهای F.R کاهش یابد بیشترین مشتریان در طول این دو سال بعد از اتمام این قراردادها به MPLS و یا اترنت مهاجرت خواهند کرد و بدنبال آن به هزینه کمتر و توان مؤثرتری در LAN های خود دست خواهند یافت.

Frame Relay versus X.25

طراحی X.25 باهدف یک ارتباط عاری از اشتباه در شبکه هائی با نرخ error بالا طراحی شد و بسیاری از خواص X.25 به این مسئله بر میگشت. برداشتن آن ملاحظات در F.R موجب افزایش سرعت تا ۲۰ برابر شد. از طرفی X.25 در هر سه لایهٔ ۱و ۲و ۳ کار میکرد در حالیکه F.R تنها در لایه های ۱و۲ کار میکرد و این یعنی پردازش کمتر در هر گره و در نتیجه توان و بهروری بیشتر.

X.25 پاکتها را آماده و می فرستد در حالیکه F.R اینکار را با فریم ها انجام میدهد[1]. X.25 در فیلد پاکتش چندین فیلد مربوط به کنترل خطا و جریان دارد که F.R هیچکدام را نیاز ندارد. در حالیکه F.R با کمترین پردازش در فیلد آدرس این کار را انجام میدهد. البته این خواص F.R با فرض به کار گرفته شدن در سیستمهای شبکه ای قابل اطمینان تر است و با تکیه بر این مسئله است که خود را از بسیاری از قابلیتهای مربوط به تصحیح خطای X.25 راحت کرده است.

[1] به پیغامهای لایه دسترسی را فریم یا قاب مینامند و به پیغام های لایه ۳ پاکت گفته میشود./س

X.25 یک پهنای باند ثابت را ارئه میدهد و به نحوی بخشی از منابع را تلف میکند در حالیکه F.R به شکلی پویا در حین Call Setup یا مواقع دیگر پهنای باند را هم در لایه ۱ و هم ۲ اختصاص میدهد.[9]

SMDS

SMDS بوسیلهٔ استاندارد IEEE 802.6 MAN که بویسلهٔ Bellcore پیاده شد. این پروتکل میتواند از تکنولوژی متفاوتی مانند B-ISDN و DQDB[1] استفاده کند. پیاده سازی فعلی در آمریکای شمالی از DQDB بهمراه خطوط DS1 – 1.5Mbps - یا DS3 – 45Mbps – است. پیاده سازیهای دیگر بر استفاده از خطوط E1 با سرعتی حدود 1.9Mpbs یا خطوط E3 است . SMDS های آینده با تزویج B-ISDN بهمراه SONET OC3 در سرعت 1555Mbps انجام خواهد شد.

توسعهٔ این سرویس با ATM همزمان بود. مانند ATM، SMDS هم از Cell Relay استفاده میکند. هر دو سرویس از سلولهای ۵۳ بایتی استفاده میکند که SMDS میتواند پاکتهائی با حداکثر طول ۹۱۸۸ و ATM پاکتهای باطول ۶۵۵۳۵ را ساپورت میکند.

SMDS یا Switched Multigigabit Data Service یک سرویس مخابراتی است که اتصالات پاکت-سوئیچینگ سرعت بالا را ساپورت میکند. در واقع SMDS نه یک پروتکل است نه یک تکنولوژی در عوض پروتکلهای استاندارد و اینترفیسهای مخابراتی را توسط تکنولوژیهای امروز و فردا حمایت میکند.

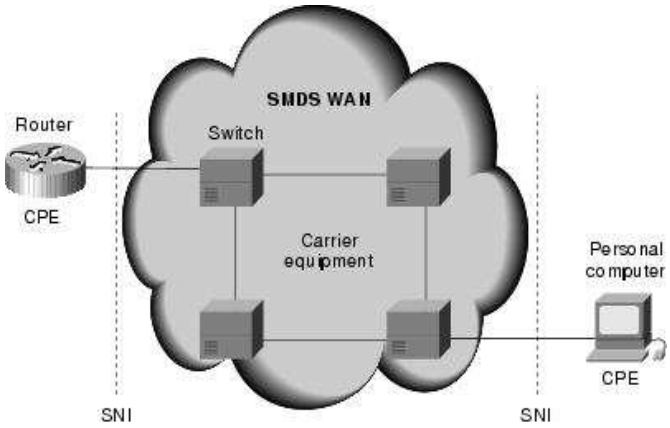
SMDS به کاربر اجازه میدهد که به طور شفاف قابلیتهای مخابراتی شبکه خود را در منطقهٔ جغرافیائی وسیعی با انعطاف پذیری مناسب توسعه دهد. از زمانیکه SMDS سرویسی بود که توسط شرکتهای تلفن پیشنهاد میشد، SMDS این توسعه را با استفاده از تجهیزات در اختیار مشتری با به اصطلاح CPE[2] و یک سری پروتکل با کمترین هزینه را اجازه میداد.

SMDS هر دو نوع رسانهٔ مسی و فیبرنوری را ساپورت میکند و سرعت آن از 1.544Mbps بر روی DS-1 یا 44.736Mbps برروی DS-3 تا سرعتهای بالاتر به کمک OC3 یا پیاده سازی های براساس FDDI را در بر میگیرد.

[1] Distributed Queue Dual Bus

[2] Customer Premises Equipment

شبکه SMDS شامل سه نوع تجهیزات است: Customer Premises Equipment یا CPE و Carrier Equipment و Subcriber Network Interface یا SNI ، CPE تجهیزات ترمینالی است که بیشتر توسط مشتری نگهداری میشود و در اختیار اوست. CPE ها گره های آخر شبکه هستند مانند کامپیوترهای شخصی و تجهیزات میانی مانند مودمها و مولتی پلکسها و روترها. البته گره های میانی گاه توسط ارائه دهنده تامین



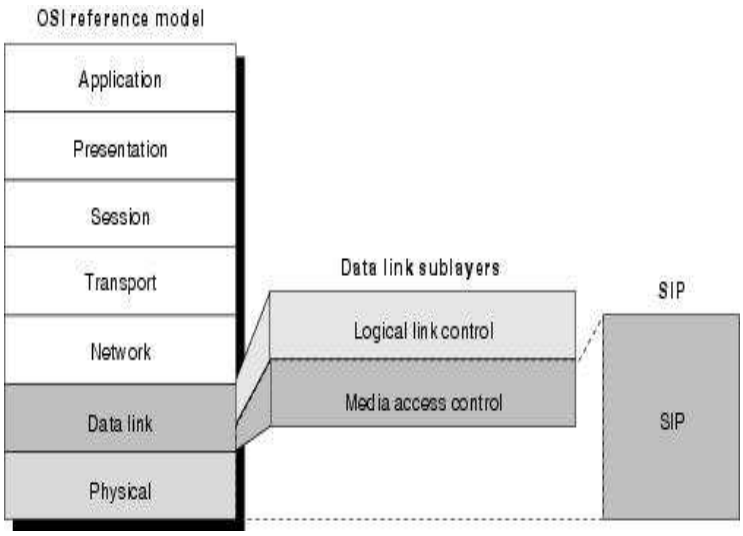
شکل ۱.۱۸- رابطهٔ بین تجهیزات مختلف شبکه

میشوند. و CE ها معمولا شامل سوئیچهای WAN پرسرعت هستند که باید با مشخصات معینی مطابق باشند مانند آنهائی که توسط Bell Communications Research یا BellCore معین شده اند. این مشخصات عملیات شبکه، اینترفیس بین Local Carrier Network و Long Distance Carrier Network و اینترفیس بین دو سوئیچ در یک شبکه را تعریف میکنند.

کاربرد SNI در رندرکردن تکنولوژی و عملیات حامل شبکه SMDS به نحوی شفاف برای مشتری است. شکل ۱.۱۸ این رابطه را بین سه نوع تجهیزات شبکه SMDS نشان میدهد:

SMDS Interface Protocol

SMDS Interface Protocol یا SIP برای ارتباط CPE و SMDS Carrier Equipment استفاده میشود. SIP سرویسی بدون اتصال را بر روی SNI فراهم میکند و به CPE اجازه دسترسی به شبکه را میدهد. SIP بر اساس استاندارد IEEE 802.6 DQDB برای انجام Cell Relay بر روی MAN ها به کار میرود. DQDB به عنوان پایهٔ SIP به کار میرود یکی از دلایل آن باز بودن این استاندارد است که همه سرویسها و خواص SMDS را حمایت میکند. بعلاوه



شکل ۱.۱۹- نحوهٔ ارتباط SIP با بقیهٔ لایه ها

DQDB برای سازگار شدن با استانداردهای انتقال حامل فعلی هم طراحی شده است و همچنین با استانندارهای پدیدار شده حول حوش B-ISDN نیز سازگار است و این قابلیت کار با سرویسهای انتقال video را میدهد. در شکل ۱.۱۹ نحوه ارتباط SIP با بقیه لایه و نقش آن نشان داده شده است.

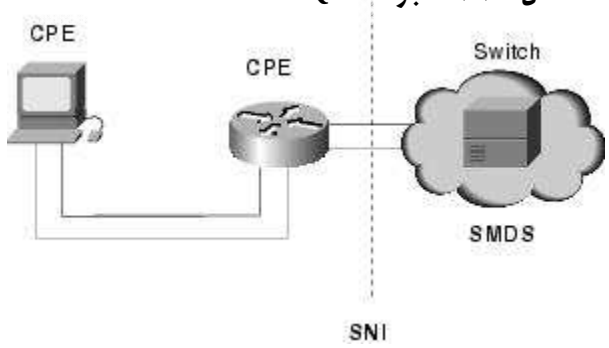
توضیح راجع به لایه های جزئی تر به عهده مراجع اصلی گذاشته میشود و در آخر با توضیح مختصری از DQDB و دو ورژن مختلف قالب SPI این بحث را به پایان میبریم.

Distributed Queue Dual Bus

DQDB یک پروتکل ارتباطی لایه پیوند داده است که برای استفاده در MAN ها طراحی شده است. DQDB توپولوژی شبکه ای را مشخص میکند که از دو باس منطقی دو طرفه تشکیل شده که چندین سیستم را به هم متصل میکند. این پروتکل در استاندارد IEEE 802.6 DQDB توضیح داده شده است.

Access DQDB از اجزا اصلی شبکه SMDS یعنی Carrier Equipment و CPE و SNI تشکیل شده است. که در شکل می بینید:

شکل ۱.۲۰- اجزاء Access DQDB



توضیحات بیشتر در این زمینه در اینجا نمگنجد در انتها نیز به ذکر ساختار و قالب کلی پاکتهای SMDS می پردازیم:

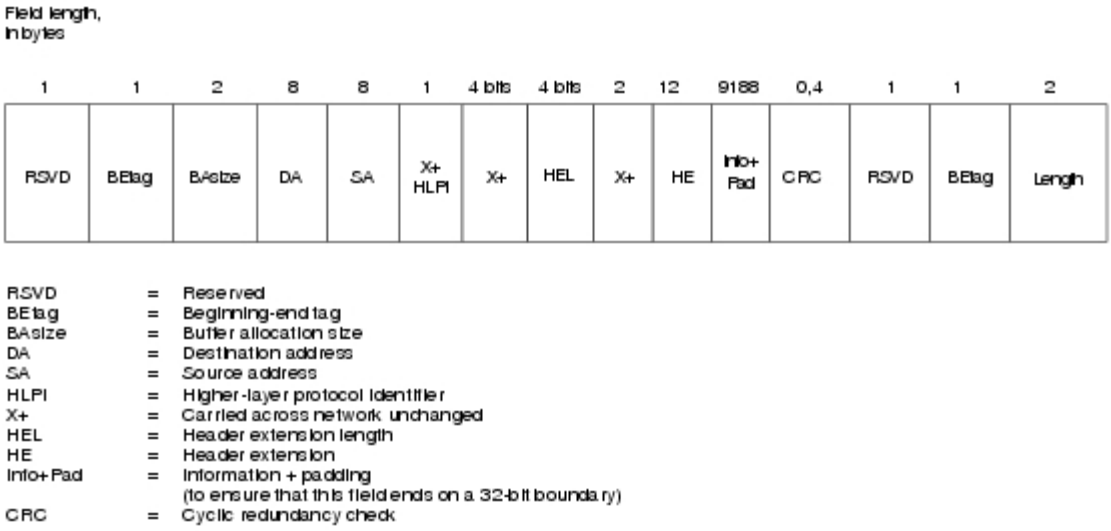
SMDS Addressing Overview

Protocol Data Unit یا PDU شبکه SMDS هر دو آدرس مبدا و مقصد را حمل میکند. آدرس SMDS ۱۰ رقم است و شبیه سیستم شماره تلفن معمولی است. پیاده سازی SMDS هم group addressing و هم ویژگیهای امنیتی را پیشنهاد میدهد.

SMDS group address اجازه میدهد که یک آدرس به چندین CPE رجوع کند. این قابلیت باعث میشود منابع کمتری در توزیع اطلاعات مسیریابی و مدیریت ترافیک و بقیه اطلاعات کنترلی مصرف شود. این قابلیت شبیه multicating در LAN هاست.

SMDS دو خاصیت امنیتی را پیاده میکند: Source address validation و address screening قابلیت source address validation قابلیت بسیار مهمی است و از address spoofing که درکارهای غیر قانونی و دزدی هویت مورد استفاده قرار میگیرد جلوگیری میکند بدین ترتیب که پاکتها نمیتوانند از آدرسی دیگر خود را با جریان اصلی قاطی کنند یا کنترل جریان را عوض کنند. قابلیت Address Screening به مشترک اجازه میدهد تا یک VPN ی را ایجاد کند که شامل ترافیکهای ناخواسته و نامربوط به نیاز کاربر نباشد. به عنوان سخن آخر در این بخش دو نوع از فرمت SIP را از مرجع می آوریم: [11]

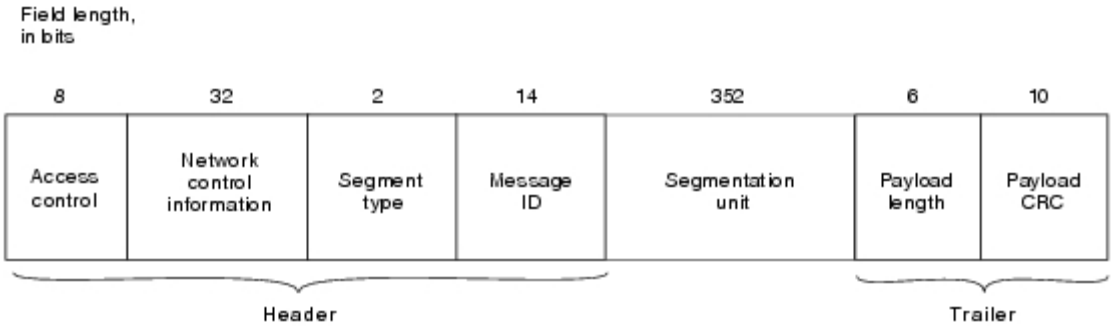
SMDS Reference: SIP Level 3 PDU Format



- ✓ • **X+**—Ensures that the SIP PDU format aligns with the DQDB protocol format. SMDS does not process or change the values in these fields, which may be used by systems connected to the SMDS network.
- ✓ • **RSVD**—Consists of zeros.
- ✓ • **BEtag**—Forms an association between the first and last segments of a segmented SIP Level 3 PDU. Both fields contain identical values and are used to detect a condition in which the last segment of one PDU and the first segment of the next PDU are both lost, which results in the receipt of an invalid Level 3 PDU.
- ✓ • **BAsize**—Contains the buffer allocation size.
- ✓ • **Destination address (DA)**—Consists of two parts:
- ✓ – **Address type**—Occupies the 4 most significant bits of the field. The Address Type can be either 1100 or 1110. The former indicates a 60-bit individual address, while the latter indicates a 60-bit group address.
- ✓ – **Address**—Gives the individual or group SMDS address for the destination. SMDS address formats are consistent with the North American Numbering Plan (NANP).
- ✓ The 4 most significant bits of the Destination Address subfield contain the value 0001 (the internationally defined country code for North America). The next 40 bits contain the binary-encoded value of the 10-digit SMDS address. The final 16 (least significant) bits are populated with ones for padding.
- ✓ • **Source address (SA)**—Consists of two parts:
- ✓ – **Address type**—Occupies the 4 most significant bits of the field. The Source Address Type field can indicate only an individual address.
- ✓ – **Address**—Occupies the individual SMDS address of the source. This field follows the same format as the Address subfield of the Destination Address field.
- ✓ • **Higher layer protocol identifier (HLPI)**—Indicates the type of protocol encapsulated in the Information field. The value is not important to SMDS, but it can be used by certain systems connected to the network.

- ✓ • **Header extension length (HEL)**—Indicates the number of 32-bit words in the Header Extension (HE) field. Currently, the field size for SMDS is fixed at 12 bytes. (Thus, the HEL value is always 0011.)
- ✓ • **Header extension (HE)**—Contains the SMDS version number. This field also conveys the carrier-selection value, which is used to select the particular interexchange carrier to carry SMDS traffic from one local carrier network to another.
- ✓ • **Information and Padding (Info + Pad)**—Contains an encapsulated SMDS service data unit (SDU) and padding that ensures that the field ends on a 32-bit boundary.
- ✓ • **Cyclic redundancy check (CRC)**—Contains a value used for error checking.
- ✓ • **Length**—Indicates the length of the PDU.

SMDS Reference: SIP Level 2 Cell Format



The following descriptions briefly summarize the functions of the SIP Level 2 PDU fields illustrated in Figure 2- 16:

- ✓ • **Access control**—Contains different values, depending on the direction of information flow. If the cell was sent from a switch to a CPE device, only the indication of whether the Level 3 protocol data unit (PDU) contains information is important. If the cell was sent from a CPE device to a switch, and if the CPE configuration is multi-CPE, this field can carry request bits that indicate bids for cells on the bus going from the switch to the CPE device.
- ✓ • **Network control information**—Contains a value indicating whether the PDU contains information.
- ✓ • **Segment type**—Indicates whether the cell is the first, the last, or a middle cell from a segmented Level 3 PDU. Four possible segment type values exist:
- ✓ – **00**—Continuation of message
- ✓ – **01**—End of message
- ✓ – **10**—Beginning of message
- ✓ – **11**—Single-segment message
- ✓ • **Message ID**—Associates Level 2 cells with a Level 3 PDU. The message ID is the same for all the segments of a given Level 3 PDU. In a multi-CPE configuration, Level 3 PDUs originating from different CPE devices must have a different message ID. This allows the SMDS network receiving interleaved cells from different Level 3 PDUs to associate each Level 2 cell with the correct Level 3 PDU.
- ✓ • **Segmentation unit**—Contains the data portion of the cell. If the Level 2 cell is empty, this field is populated with zeros.

- ✓ • **Payload length**—Indicates how many bytes of a Level 3 PDU actually are contained in the Segmentation Unit field. If the Level 2 cell is empty, this field is populated with zeros.
- ✓ • **Payload cyclic redundancy check (CRC)**—Contains a CRC value used to detect errors in the following fields: – Segment Type – Message ID – Segmentation Unit – Payload Length – Payload CRC

[11]

SONET & SDH

SONET یا Synchronous Optical Networking و SDH یا Synchronous Digital Hierachy دو پروتکل مولتی پلکسینگ شبیه هم هستند که برای ارسال دیتا با استفاده از لیزر و LED طراحی شده اند. این متدها برای جایگزینی PDH طراحی شدند[1]. بدین ترتیب امکان مقدار بیشتری از انتقال داده و تعداد تماس های بیشتر را دارد بدون اینکه مشکل سنکرون کردن پیش آید.

SONET و SDH بر اساس Circuit Mode Communication بنا شده است. این بدین معنی است که هر تماسی یک bitrate و تاخیر ثابت را میگیرد. بعنوان مثال SDH یا SONET ممکن است به نحوی به کار گرفته شوند تا به چندین ISP اجازه دهد تا فیبرنوری را به اشتراک بگذارند بدون اینکه تحت تأثیر ترافیک همدیگر قرار بگیرند و بهمین خاطر از طرف دیگر هم قادر نخواهند بود که به طور موقت از ترافیک شبکه دیگر استفاده کند. فقط مضارب معینی از 64Kbps به عنوان bit-rate های ممکن به طور ثابت اختصاص داده میشود.

از زمانی که SONET و SDH بعنوان یک سیستم پروتکلی کاملا TDM (که نباید با TDMA خلط گردد.) شناخته میشدند به عنوان اتصال دائم را پیشنهاد میکردند و شامل packet mode communication نمیشدند. این دو به عنوان پروتکلهای لایه فیزیکی در نظر گرفته میشوند.

هردوی SONET و SDH به طور وسیعی امروزه استفاده میشوند: SONET در ایالات متحده و کانادا و SDH در بقیه دنیا. اگرچه استاندارد SONET قبل از SDH توسعه داده شد نفوذ آن در بازار جهانی تغییرات و گونه گونی آنرا دیکته میکند.

استاندارد SDH بوسیله ITU در استاندارد G.707 و الحاقیه اش G.708 مستند شد. استاندارد SONET به عنوان GR-253-CORE از Telcordiaو T1.105 از انستیتو استاندارد ملی آمریکا تعریف شد.

Synchronous Networking متفاوت از PDH است که در آن سرعتهای دقیقی برای انتقال داده به کار برده میشود و به طور دقیقی در تمام شبکه سنکرون است و این به کمک ساعتهای اتمی ممکن است. این سیستم سنکرونیزاسیون به تمام شبکه داخل کشور اجازه میدهد که به شکل کاملا سنکرون با هم کار کنند و این سبب کاهش فوق العاده در نیاز به بافرینگ بین المانهای شبکه میشود.

هر دوی SONET و SDH میتوانند برای کپسوله سازی و کار با آخرین استانداردهای انتقال دیجیتال به کار برده شوند و یا مستقیما بوسیلهٔ ساپورت ATM یا به اصطلاح Packet Over SONET/SDH (POS) به

[1] سیستم PDH و به دنبال خطوط E1 و E3 و DS1 و.. به خاطر ارتباط کمتر در اینجا معرفی نشدند.

این هدف نا ئل گردند. همینطور درست نیست که SDH یا SONET بعنوان پروتکل ارتباطی در نظر گرفته شوند بلکه این دو یک بستر عمومی و همه منظوره برای انتقال هردوی داده و صوت اند. فرم اصلی سیگنال SDH به آن اجازه میدهد تا سرویسهای متفاوتی را در Virtual Container یا VC خود حمل کند چرا که یک پهنای باند منعطف دارد.

اطلاعات بیشتر راجع به جزئیات پروتکلهای SONET/SDH به خاطر ارتباط کمتر با MPLS و اینکه ایندو از کلاس و دستهٔ MPLS نیستند و اصولا سطح کاری آنها در لایه متفاوت تری است خودداری میکنیم اما در مراجع معرفی شده موجودند. در نهایت مختصری راجع به ارتباط SONET/SDH با اترنت 10G گفته میشود چرا که این اینترفیس در معماری پروژه مورد نظر بوده است. و در آخر هم جدول نرخ و سرعتهای SONET/SDH می آید.

SONET/SDH and relationship to 10 Gigabit Ethernet

نوع دیگری از شبکه های نوع سوئیچنگ مداری در بین تجهیزات دیتا اترنت 10G یا 10GbE است. که بسیار شبیه سرعت خطوط OC-192/STM-64 است که سرعت 9.953Bbps را دارد.[1] اتحاد موسوم به Gigabit Ethernet Alliance دو نوع 10GE ایجاد کرده است: اول (Local Area Varient) یا (LAN PHY) با سرعت خطوط ذکر شده یعنی (9,953,280 kbps) Oc-192/STM-64. و دیگر Ethernet WAN با سرعت دقیق 10,000,000 kbps که به (WAN PHY) موسوم است.

بااین وجود، 10GE هیچ برون-سازگاری روشن و صریحی در سطح جریان داده با بقیه سیستمهای SDH/SONET فراهم نمیکند. این با سیستم ترانسپوندرهای WDM فرق میکند و شامل هر دو نوع Ooarse and Dense WDM یا CWDM & DWDM که سیگنالهای OC-192 SONET را ساپورت میکند هست.

[1] خط STM-1 سرعت پایه 155Mbps را دارد پس STM-64 سرعت 64 X 155Mpbs یعنی 9,920 Mbps را دارد اما برخلاف STM سیستم OC از چنین روشی در شماره گذاری خود استفاده نمیکند.

SONET/SDH data rates

SONET Optical Carrier Level	SONET Frame Format	SDH level and Frame Format	Payload bandwidth (kbit/s)	Line Rate (kbit/s)
OC-1	STS-1	STM-0	48,960	51,840
OC-3	STS-3	STM-1	150,336	155,520
OC-12	STS-12	STM-4	601,344	622,080
OC-24	STS-24	STM-8	1,202,688	1,244,160
OC-48	STS-48	STM-16	2,405,376	2,488,320
OC-96	STS-96	STM-32	4,810,752	4,976,640
OC-192	STS-192	STM-64	9,621,504	9,953,280
OC-768	STS-768	STM-256	38,486,016	39,813,120
OC-1536	STS-1536	STM-512	76,972,032	79,626,120
OC-3072	STS-3072	STM-1024	153,944,064	159,252,240

ATM

ATM تکنولوژی است که ویژگی bandwidth-on-demand ی که packet-switching ارئه میدهد و سرعت بالای مورد نیاز شبکه های LAN و WAN امروزی[1] را باهم پیشنهاد میدهد. این تکنولوژی Cell-Relay مستقل از نوع انتقالی که در لایه های بالاتر تولید و در نظر گرفته میشود عمل میکند و روی هر رسانه ای با هر سرعتی (لایه های پائینتر) کار میکند و ازین لایه ها هم مستقل است. این باعث میشود تا بتوان به شکل مجازی هر نوع داده ای را فرستاد (صدا،دیتا،ویدئو و...) در یک جریان داده تجمیع شده تکی بر روی هر رسانه ای از خطوط T1/E1 گرفته تا سیگنالهای اپتیکی سرعت بالا مانند SONET بر روی OC-3 یا OC-12 یا OC-48 یا OC-192 و حتی OC-768 اجرا میشود. تکنولوژی ATM به هردو شبکه عمومی و خصوصی اجزا میدهد که یک اتصال شفاف و یکپارچه از یک کاربر نهائی به کاربر دیگر برقرار گردد چه ایندو نقطه پایانی در یک ساختمان باشند چه در دو شهر متفاوت.

ATM امروزه به عنوان یک تکنولوژی بالغ در نظر گرفته میشود. ATM یک پیاده سازی پایدار و به خوبی تست شده از مدیریت ترافیک و QoS را فراهم میکند که به شبکه های مجتمع سرویس میدهد. ATM به طور گسترده برای حمل بقیه سرویسهای داده به کار میرود ازین جمله میتوان به F.R اشاره کرد. و به خاطر قابلیت آن در انتقال داده های متفاوت شامل صدا، ویدئو، و داده و کار با سرعتهای متفاوت و گارانتی کیفیت سرویس در بسیاری از شبکه ها مورد استفاده قرار میگیرد.

ATM به کاربر اجازه میدهد تا از پهنای باند هر موقع که لازم شد استفاده کند. پهنای باند استفاده نشده توسط اپلیکیشنهای دیگر بوسیلهٔ به کار بردن قابلیت مالتی پلکس آماری مصرف میشود. ATM ناهمگام یا Asynchronous است چرا که cell میتواند به طور مستقل به یک اتصال مجازی تا اندازه ای که نیاز است پهنای باند به آن اختصاص دهد. ATM مدیریت ترافیک خود را بویسله سرآیندهای ۵۳ بایتی خود که به Cell مشهور هستند انجام میدهد. ATM از طول سرآیند ثابت استفاده میکند[2] و این باعث میشود که بتواند در سرعتهای بالاتری نسبت به سیستمهای طول متغیر کار کند. نکته مهم اینست که سلولهای کوتاه و طول ثابت مورد استفاده در ATM سبب پیش بینی دقیق تأخیر شبکه میشوند و این ATM را برای کار با صدا و ویدئو مناسب میکند.

[1] این کتاب در سال ۲۰۰۲ نوشته شده است. امروزه MPLS بسیاری ازین ویژگیها به شکل بهتری را ارائه میدهد./س

[2] که به همین خاطر عوض Frame به Cell موسوم است/س

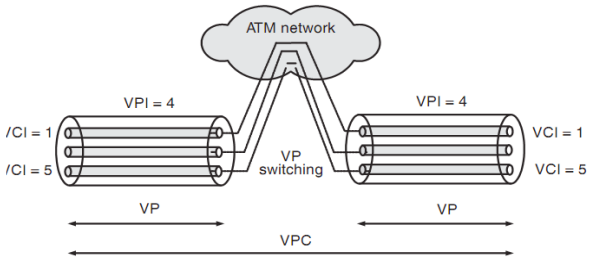
این بخش مفاهیم اولیه ATM را شرح میدهد و مقدار مختصری راجع به سیگنالینگ و آدرس دهی در آن توضیح داده میشود و بقیه مباحث در حد مقتضی پوشش داده میشوند.

یکی از مزایای ATM حمایتش از کیفیت سرویس QoS تضمین شده در اتصالها است که منجر به تضمین تاخیر و نیازها برای گارانتی و تضمین صحت داده است. گره ای که درخواست تشکیل یک اتصال را دارد میتواند درخواستی برای یک QoS مشخص هم داشته باشد و میتواند مطمئن باشد که شبکه آن QoS درخواستی را در طول زنده بودن اتصال فراهم خواهد کرد. این اتصالات به ۴ دسته سرویسهای ATM تقسیم میشوند:

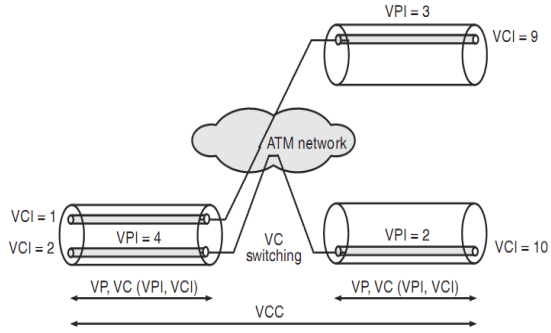
CBR, Real-Time & Non-Real-Time Variable Bit-rate (rt-VBR & nrt-VBR), Available Bit-rate (ABR), and unspecified Bit-Rate (UBR).

بر طبق طبیعت QoS درخواستی و مشخصات ترافیک مورد انتظار یکی ازین ۴ نوع درخواست داده میشود که برای جزئیات بیشتر راجع به آنها میتوان به منابع فراهم شده و معرفی شده مراجعه کرد.

ATM یک پروتکل اتصال-گرا[1] است که بدین معنی است که اتصال باید قبل از برقراری ارسال داده باید برقرار شود. یک اتصال توسط دو فیلد VPI و VCI مشخص میشوند. همانطور که در شکل ۱.۲۱ هم دیده میشود یک مسیر مجازی یا VP شامل یک دسته از کانالهای مجازی یا VC هاست که به شکل شفافی بر اساس VPI سوئیچ میشوند. VPI و VCI تنها در لایهٔ فیزیکی به کار برده میشوند و ارزش محلی دارند و در هر سوئیچ دوباره به شکلی که مناسب است نگاشت میشوند. سوئیچنگ سلولهای ATM در سخت افزار بر اساس فیلدهای VPI/VCI هر سلول انجام میشود. سوئیچینگی که فقط بر روی VPI اجرا میشود به نام Virtual Path Connection یا VPC نامیده میشود درحالیکه سوئیچینگی که بر روی هر دوی VPI/VCI انجام میشود به Virtual Channel Connection یا VCC معروف است. نمودارهای ۱.۲۱ و ۱.۲۲ را ببینید.



شکل ۱.۲۱- سوئیچینگ ATM VP



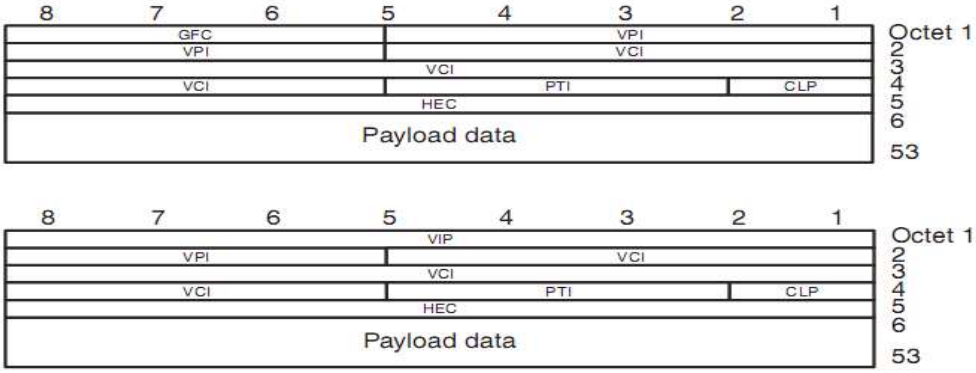
شکل ۱.۲۲- سوئیچینگ ATM VC

یک سوئیچ یا وسیلهٔ ATM هم میتواند یک گرهٔ پایانی و یا یک گره اتصالی در یک VP یا VC باشد. VPP و VCC بین گره های پایانی قرار میگیرند همانطور که در شکلهای ۱.۲۱ و ۱.۲۲ نیز نشان داده شده است. سوئیچنگ VP

[1] Connection-Oriented

بیشتر برای حالتی است که قرار است اطلاعات زیادی بین دو نقطه رد و بدل شود و VPI در VP در این حالت بلاتغییر می ماند و برای شبکه نیز به شکل شفاف در دسترس است و تمام VC ها یک عدد VCI بین نقاط ابتدائی و پایانی دارند. VC بیشتر هنگامی به کار میرود که اتصالات کوچکی بیشتر به هدف کنترلی و نگهداری QoS نیاز است.

در ATM دو نوع استاندارد اینترفیس وجود دارد که تنظیمات شبکه ATM را مشخص میکنند. UNI که بین دو وسیلهٔ دو کاربر قرار میگیرند (یا انتهای شبکه) و NNI که بین دو سوئیچ شبکه قرار دارد. نمودار پیش رو فرمت ۵۳ بایتی سلول ATM را در یک UNI نشان میدهد. سلول شامل یک آدرس است که تنها برای اینترفیس محلی معنادار است و از دو بخش تشکیل شده: یک VPI ۸ بیت و یک VCI ۱۶ بیت. این سرآیند سلول ۴ بیت هم برای کنترل جریان به اسم GFC دارد. ۳ بیت به عنوان Payload Type Identifier که و یک



شکل ۱.۲۳- فرمت سلولهای ۵۳ بایتی NNI و UNI در ATM

بیت CLP یا Cell Loss Priority و ۸ بیت چک کننده خطای سرآیند برخوردار است.فرمت مربوط به اینترفیس NNI هم به همین شکل در شکل ۱.۲۳ نشان داده شده است.

Why cells?

انگیزه برای استفاده از سلول به جای فریم و آنهم سلولهای کوچک کاهش jitter –در اینجا تاخیر متغیر- در مولتی پلکس کردن جریان داده بود. کاهش این (و همچنین کاهش تاخیر end-to-end round trip) در زمانیکه شبکه با صوت کار میکند بسیار مهم است.

این به این خاطر است که تبدیل صدای دیجیتال به آنالوگ یک پروسه ذاتا real-time است پس برای انجام یک کار خوب کدکی که این را انجام میدهد به یک جریان داده با فاصلهٔ ثابت[1] نیاز دارد. وقتی که داده بعدی در حالیکه مورد نیاز است در دسترس نیست، کدک راهی برای انتخاب ندارد جز تولید اصطلاحا silence or

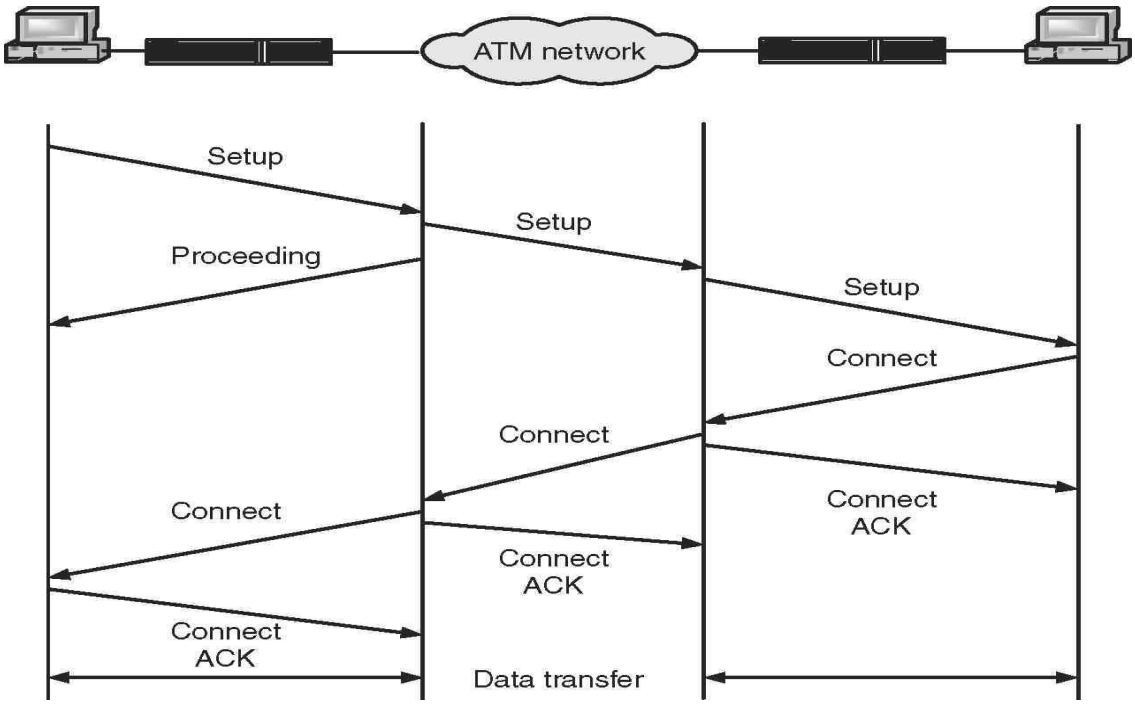
[1] تاخیر ثابت یکی از خواص ATM است که به خاطر طول ثابت سلول آن است/س

guess وقتی داده دیر کند این دیگر بیهوده است به خاطر اینکه دوره زمانی که باید به سیگنال تبدیل میشد گذشته است. حال یک سیگنال سخنرانی را که به پاکت تبدیل شده را در نظر بگیرید و آنرا در یک ترافیک با وجود داده های حجم بالا قرار دهید. این پاکت سخنرانی هر چقدر هم کوچک باشد همواره در پشت پاکتهای بزرگی قرار خواهند گرفت و این یعنی در صف به مدت طولانی منتظر شدن تبعات آن در پاراگراف قبل گفته شد پس ثابت بودن و کوچک بودن همه بسته ها در این امر مهم است.

در زمانیکه که ATM طرحی شد، 155Mbps SDH بعنوان خط نوری پرسرعت تلقی میشد و خط کم سرعت تر PDH مقداری بین 1.544 to 45 Mbps را در آمریکا (و دراروپا 2-34 Mbps) پیاده میکرد. در این سرعتها یک پاکت 1500 بایتی کامل 77.42 میکروثانیه برای انتقال نیاز داشت. در سرعتهای پائینتر مثل یک خط T1 که حدود 1.5Mbps سرعت دارد این پاکت 7.8 میلی ثانیه زمان نیاز داشت.

این زمان برای یک شبکه با قابلیت انتقال عملی صوت دیجیتال قابل قبول نبود، ATM طراحی شد تا اینترفیس شبکه ای low-jitter را پیاده کند. با این وجود برای فراهم کردن تأخیرهای کوتاه در عین حمل داده گرامهای بزرگ مجبور بود که از cell به جای frameای استفاده کند که طول متغیر داشت و در F.R توضیح داده شد. ATM همه انواع پاکتهای داده، صوت را به قطعات ۴۸ بایتی تقسیم میکند و ۵ بایت اطلاعات و سرآیندهای مسیریابی را به آن اضافه میکند. انتخاب ۴۸ بایت طبق معمول بیشتر سیاسی بود تا تکنیکی. وقتی CCITT سیستم ATM را استاندارد کرد شرکاء ایالات متحده سرآیند ۶۴ بایت را میخواستند چون هم مضربی از ۲ بود و هم کار با آن ساده تر بود و این سایز هم مصالحهٔ خوبی بین سرآیندهای بزرگ که مناسب انتقال داده بودند و سرآیندهای کوچکی که مناسب کاربردهای real-time مانند انتقال صدا بودند، برقرار میکرد. شرکاء و احزاب اروپائی سرآیند ۳۲ بایتی را میخواستند و این به خاطر سایز کوچکتر و در نتیجه تأخیر کمتر و ساده کردن[1] به کارگیری (عموما صوتی) آن با در نظر گرفتن مسئلهٔ echo cancellation در سیستمهای مخابراتی آنها بود. بیشتر شرکاء اروپائی سرانجام به نظر آمریکا متمایل گشتند بجز فرانسه و چند کشور دیگر که تا آخر کار بر روی نظر خود ایستادند. با ۳۲ بایت، فرانسه قادر بود که یک شبکه صوتی بر اساس ATM را در تمام فرانسه به گونه ای پیاده کند که با تماس از یک طرف آن به طرف دیگر نیازی به echo cancellation نباشد. 5+48 بایت سرانجام انتخاب شد تا مصالحه ای بین نظر دو طرف برقرار گردد اما این عدد برای هیچ یک از دو طرف ایده آل نبود و تا به امروز نیز چنین بوده است. ۵ بایت به این دلیل انتخاب شد چون ۱۰٪ سربار، حداکثر هزینه ای بود که میخواستند برای اطلاعات مسیریابی بپردازند. ATM این سلولهای ۵۳ بایت را عوض پاکتها مولتی پلکس میکند و بنابراین بدترین حالت یعنی Queuing Jitter را تا ۳۰ درصد کاهش میدهد بدون اینکه نیازی به echo canceller ها باشد.در شکل ۱.۲۴ زیر روند تشکیل یک اتصال نشان داده شده است برای پرهیز از اطناب از جزئیات زیاد این روند خودداری میکنیم در حالیکه خود شکل تا حد زیادی گویای کلیت ماجرا میباشد:

[1] و در نتیجه ارزان کردن/س



شکل ۱.۲٤- روند تشکیل یک اتصال ATM

ATM Adaptation Layer

این مسئله ازین جهت اهمیت دارد که در MPLS این مسئله به گونه ای کاملا هوشمندانه تر و کاراتر پیاده شده است که در جای خود توضیح داده خواهد شد.

AAL لایه های بالاتر را از خصوصیات ویژه لایه ATM ایزوله میکند. AAL ترافیک کاربر را در شبکه های cell-based تکنولوژی ATM همگرا یا سازگار میکند تا بتواند از کلاسهای ترافیکی مختلف مانند صدا، داده، و ویدئو حمایت کند. کار اصلی AAL تبدیل و جمع کردن ترافیک به فرمتهای استانداری است که توسط پروتکل AAL مشخص میشوند، است.

انواع مختلفی از AAL ها انواع مختلفی از کاربردهای ترافیک را ساپورت میکنند. انواع مختلف AAL در واقع طول واحد دادهٔ پروتکلی بسیار متفاوتی دارند. AAL1 و AAL2 دارای PDU کوتاهتری هستند تا از کاربردهای real-time حمایت کنند در عوض AAL3/4 و AAL5 از داده های معمولی حمایت میکنند در این سه از پاکتهای از طول یک بایت تا ۶۵۵۳۵ بایت حمایت میشود. AAL5 همینطور از چندین کانال منطقی بر روی یک ATM VPI/VCI حمایت میکند. برای جزئیات بیشتر در این مورد میتوان به منابع فراهم شده مراجعه کرد.[12]

MPLS

فصل زیر ترجمه ای نسبتا کامل از دو فصل مرتبط[۱] از مرجع [13] می باشد:

معماری سوئیچینگ برچسب چندپروتکلی (MPLS)

طرح ساختار سویچ چندپروتکلی(MPLS) بر اساس tag switching سیسکو(Cisco) می باشد که از IP Switching Scheme الهام گرفته شده است، روشی برای سوئیچ بستهٔ IP در ATM که توسط شبکه Ipsilon ارائه شده است. (این شرکت بعد ها توسط نوکیا خریداری شد). MPLS توسط IETF استاندارد شد و یک ساختار اتصال-گرا[۲] را به یک شبکه بدون اتصال IP معرفی میکند. MPLS عمل سنگینِ پردازش-بر جست و جو در جداول مسیردهی ارسال[۳] را که برای پیدا کردن روتر مجاور بعدی ضروری است را دور میزند. همچنین MPLS برای معرفیQoS در شبکه IP میتواند به کار برده شود. از زمان معرفی tag switching و بدنبال آن MPLS، چندین الگوریتم مؤثر به لحاظ پردازشی برای انجام دادن جست و جوی اطلاعات *جدول مسیردهی ارسال* معرفی شده اند. اهمیت MPLS از زمانی که به عنوان راه حل آوردن QoS به شبکهٔ IP مطرح شد به هیچ وجه کاهش نیافته است.

MPLS نیازمند به مجموعه ای از روشها برای توزیع قابل اطمینان متعلقات برچسبهاست. MPLS نیازمند پروتکل منفرد برای توزیع برچسب نمی باشد. با وجود این مسئله، طرح های مختلفی برای توزیع برچسب ها ارائه شده است که پروتکل توزیع برچسب (LDP) و پروتکل رزرواسیون منابع-مهندسی ترافیک (RSVP–TE) بیشتر بکار می روند.

در این فصل ویژگیهای اساسی ساختار MPLS را توضیح می دهیم . LDP و تعمیم یافته آن CR-LDP و RSVP و تعمیم آن RSVP-TE در فصل بعدی ارائه شده است.

MPLS یک استاندراد IETF مبتنی بر Cisco’s Tag Switching می باشد .قصد اصلی کار کردن با پروتکلهای مختلف سطح شبکه .مانند IPv4, IPv6, IPX و Appletalk بود. MPLS به طور اختصاصی برای شبکه های IP توسعه داده شده است که نام پروتکل را از آنچه در واقع هست عمومی تر میکند.

---

[۱] فصول ۶ و ۷

[۲] در مقدمهٔ کتاب که در لوح فشرده فراهم گردیده است، صفحات ۳ تا ۷ این مسئله و انواع شبکه ها شامل Switching و BroadCast و Packet Switching و Circuit Switching و دو مفهوم Connection-Oriented و Connection-less به طور خلاصه توضیح داده شده است. این مطلب در یک صفحه در ضمیمهٔ دوم آمده است.

[۳] Forwarding Routing Table

برای درک مفاهیم اصلی در MPLS نیاز به دانستن نحوه کارکرد مسیریاب IP می باشد.که شامل دو مولفه مسیریابی و ارسال می باشد. مولفه مسیریابی شامل پروتکلهای مسیریابی مانند اولین مسیر کوتاه باز (OSPF)، پروتکل اتصال دو شبکه مرزی (BGP)، پروتکل مستقل چند طرحی (PIM) است که برای ساختن مسیرها بکار می رود و اطلاعات بین مسیرها را در IP های مختلف جابجا می کند. این اطلاعات توسط مسیریاب IP برای ساختن جدول مسیریابی ارسال که بعنوان پایگاه اطلاعات ارسال FIB[1] از آن یاد میشود به کار میرود.

جزء forwarding شامل رویه هائی است که روتر استفاده میکند تا تصمیم ارسال را بر روی بستهٔ IP بگیرد. به عنوان مثال در تک پراکنی[2] ، مسیریاب از آدرس مقصد IP استفاده میکند تا یک مدخل را در جدول FIB به کمک الگوریتم طولانی ترین تطبیق پیدا کند. نتیجهٔ این جست و جو یک شمارهٔ اینترفیس است که شمارهٔ پورتِ خروجی ای است که روتر را به روتر بعدی ای وصل میکند، این روتر بعدی همان روتری است که بستهٔ IP باید بدانجا ارسال شود.

یک مسیریاب، بسته IP را باتوجه به پیشوند آن ارسال می کند. در مسیریاب مجموعهٔ تمام آدرسهائی که دارای پیشوند یکسانی می باشند به "کلاس ارسال معادل" یا FEC[3] معروفند. پاکتهای IP یی که به یک FEC یکسان تعلق دارند اینترفیس خروجی یکسانی نیز دارند. در MPLS هر FEC با برچسب متفاوتی همراه می باشد. این برچسب برای مشخص کردن رابط خروجی بستهٔ IP بدون جست و جوی آدرس آن در FIB می باشد. یک برچسب، یک مشخص کنندهٔ کوتاه با طول ثابت میباشد که ارزش محلی دارد. یک برچسب در عملکرد شبیه مقادیر VPI/VCI سلولهای متعلق به ATM است.

در IPv6 برچسب میتواند در فیلد flow label حمل شود. با این وجود در IPv4 فضایی برای یک چنین برچسبی در سرآیند IP وجود ندارد. اگر شبکهٔ IP در در بالای شبکهٔ ATM کار کند برچسب در فیلد VPI/VCI سلول ATM انتقال می یابد .اگر آن در Frame Relay بکار رود برچسب در رشتهٔ DLCI انتقال می یابد. در اترنت، Token Ring واتصال نقطه به نقطه که از پروتکل لایه پیوندی استفاده می کنند (برای مثال PPP) برچسب در میان سرآیند LLC و سرآیند IP با یکدیگر تلفیق و جایگذاری میشود. (شکل روبرو را مشاهده کنید.) (توجه داشته باشید که در tag switching،برچسب تلفیق داده شده به sheam-header معروف است.)

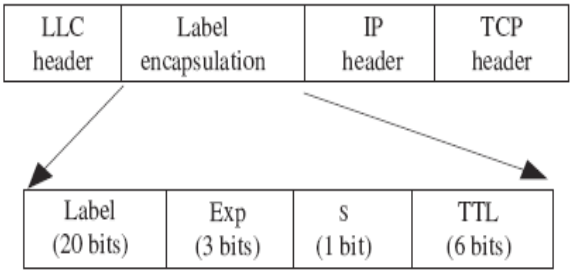


Fig 2.1 Lable Encapsulation

[1] Forwarding Information Base

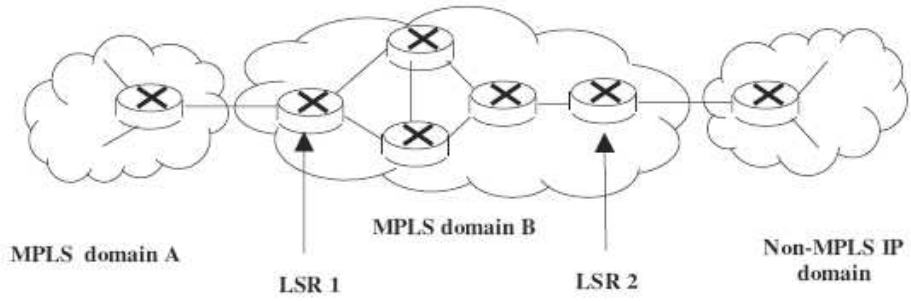
[2] یا همان Unicast

[3] Forwarding Equvalent Class –pronounce as /fek/

اولین فیلد برچسب کپسوله شده یک فیلد یا میدان ۲۰ بیتی است که برای حمل برچسب مورد استفاده قرار میگیرد. میدان دوم ۳ بیتی می باشد که برای اهداف آزمایشی بکار می رود. برای مثال برای انتقال CoS که اولویت پاکتها را درانتقال از اینترفیس خروجی معلوم میکند، بکار می رود. فیلد S در ارتباط با برچسب پشته که در این فصل با جزئیات کامل بحث خواهد شد قرار دارد. سرانجام حوزۀ TTL است که مشابه با حوزۀ TTL در سرآیند IP می باشد.

شبکۀ MPLS شامل مسیریابهای سوئیچینگ برچسب یا LSR و گره های MPLS است. یک LSR یک روتر IP می باشد که پروتکل MPLS را اجرا میکند و می تواند برچسب را به FEC متناسب مقید کند، بستۀ IP را براساس برچسب آن ارسال کند، و تصمیم ارسال IP را با انجام یک جست و جو در جدول FIBی که حامل پیشوند است انجام دهد. گره MPLS یک LSR می باشد بجز آنکه لزوما دارای قابلیت ارسال بستۀ IP بر اساس پیشوند نیست.

Fig 2.2 MPLS domain, LSRs and MPLS



مجموعه بهم پیوسته از گره های MPLS که در مسیر یا محدوده مدیریت یکسانی هستند، یک محدودۀ MPLS را تشکیل می دهند. در محدوده MPLS بسته های IP با استفاده از برچسبهایشان سوئیچ می شوند. یک محدودۀ MPLS می تواند به گره ای خارج از محدوده متصل شود که به محدوده MPLS یا یک محدودۀ غیر MPLS در IP تعلق دارد. همانطوری که در شکل بالا ملاحظه می کنید محدودۀ B در MPLS شامل ۵ مسیریاب می باشدکه دو تا از آنها LSRیعنی LSR 1و2 می باشند و سه تای دیگر ممکن استLSR ها یا گره های MPLS باشند. در محدودۀ MPLS دامنۀ B به محدودۀ A از طریق LSR 1 متصل می باشد و به محدودۀ غیر MPLS نوع IP با نام C از طریق LSR 2 متصل می باشد. LSR 1 و LSR 2 به گره های لبۀ MPLS مشهورند. به صورت ساده تر ما فرض می کنیم که تمامی گره ها در محدوۀ MPLS همان LSR ها می باشند.[1]

برای فهمیدن نحوه کار MPLS به بررسی محدوده ای که شامل پنج LSR (LSRs A, B, C, D, and E)می باشد،می پردازیم. تمامی آنها با اتصال نقطه به نقطه همانطوری که در شکل زیر مشاهده می کنید متصل می باشند .LSR AوLSR C به به محدوده ها غیر MPLS نوع IP ۱و۲ متصل می باشند مجموعۀ

[1] در این پایان نامه از روش دیگری از تقسیم بندی که کاراتر نیز هست و به هدف طراحی هم نزدیکتر است استفاده شده است و آن تقسیم روترها به دو نوع روتر LSR و LER است که در فصل معماری توضیح داده شده است.

جدیدی از میزبانان با پیشوند <X.0.0.0 , Y.0.0.0> که x.0.0.0 آدرس شبکهٔ پایه ای و y.0.0.0 ماسکی می باشد که مستقیما به E متصل است را در نظر بگیرید. جریان بسته های IP با این پیشوند از A تا E از طریق B و D می باشد. یعنی مسیریاب بعدی A برای این پیشوند B و برای B ، D و برای D، E می باشد. به همچنین جریان بسته IP از همان پیشوند از C تا E از طریق D می باشد. یعنی روتر مجاور C برای این پیشوند D و برای D، E است. اینترفیسهای نشان داده شده در شکل نحوهٔ اتصال این مسیریاب هارا به هم نشان می دهد. برای مثال A به از B طریق if0 متصل شده و B به A، C و D از طریقif1 ، if2 و if0 متصل شده است.

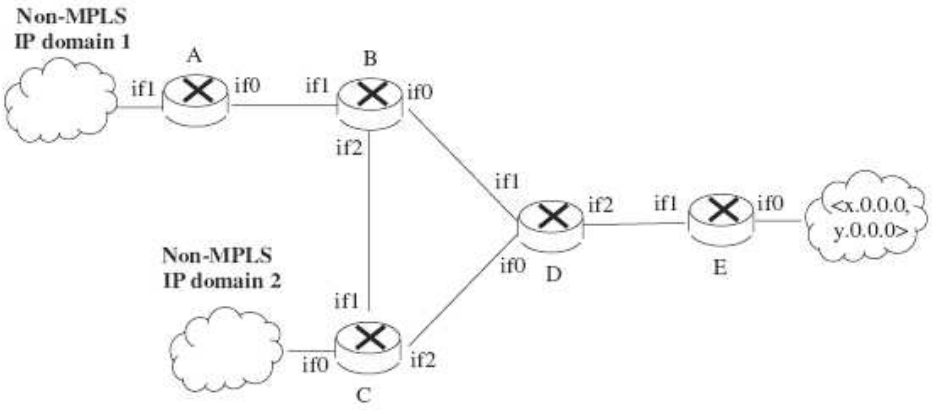


Fig 2.3 An example of Multi-Protocol Label Switching

هنگامی که LSR مقدار FEC را با پیشوند جدید ,_x.0.0.0 y.0.0.0_ مشخص می کند برچسبی را از انبوه برچسبهای آزاد انتخاب کرده و یک ورودی در لیستی که به عنوان پایگاه اطلاعاتی ارسال برچسب[1] مشخص می کند.این لیست شامل اطلاعاتی درباره برچسب های ورودی و خروجی که با FEC معین و اینترفیس خروجی آن FEC مرتبط است. پس برای این FEC روتر مجاور بعدی برای A، B است که از طریق اینترفیس if() انجام میگیرد.

ورودی در LFIB همراه با مقادیر ویژه برای هر LSR در جدول ۲.۱ نشان داده شده است[2]. به خاطر داشته باشید که B به سرآیند برچسب ورودی برابر ۶۲ را انتخاب کرده است و D دارای مقدار ۱۵ می باشد و E مقدار ۶۰ را انتخاب کرده است. از آنجایی که A و C روترهای کناری هستند و انتظار دریافت برچسبی را از شبکه هائی که بدان متصلند ندارند، برچسبی را برای آن FEC انتخاب نکرده اند. اطلا عات باقیمانده در هر ورودی LSR بعدی رابط خروجی برای FEC می باشد. بنابراین برای این FEC، مسیر داده مسیریاب بعدی برای A، B از طریق if0 می باشد.

[1] Label Forwarding Information Base (LFIB)

[2] در اینجا بنا به هدف ارائه و آموزش همگی در یک جدول نشان داده شده اند.

برچسب ورودی در حقیقت برچسبی می باشد که LSR برای یافتن تمامی ورودی های بسته های IP که به FEC تعلق دارد بکار می برد. به عنوان نمونه در مثال بالا LSR B تمامی ورودی های بستهIP که به FEC تعلق داردو با پیشوند _x.0.0.0, y.0.0.0_ شروع می شود با ۶۲ مقدار دهی می شود. برچسب گذاری این پاکتها بوسیلهٔ LSR هائی که نسبت به B اصطلاحا Upstream یا بالادستی هستند انجام میشود. یعنی آنها بالادستی هستند در جریان پاکتهای IP همراه این FEC . در این مثال تنها LSP که نسبت به B بالادستی است، A است. در مورد D هر دوی B و C روترهای بالادستی هستند.[1]

برای دریافت تمامی ورودی های بسته IP با مقدار انتخابی، LSR باید از برچسب انتخابی مسیریاب همسایه برای FEC ویژه آگاه باشد. در مثال بالا LSR B اطلا عات خود را به A، D و C ارسال می کند. A تشخیص میدهد که نسبت به B بالادستی است و بنابراین از اطلاعات برای آپدیت FEC مربوطه در LFIB استفاده میکند. تا زمانی که این FEC مد نظر است D و C نسبت به B بالادستی محسوب نمیشوند و آنها ازین اطلاعات در LFIB خود استفاده نمیکنند با این وجود آنها میتوانند این اطلاعات را برای کاربردهای بعدی ذخیره کنند. بعنوان مثال شکستن لینک C-D میتواند سبب شود که B به عنوان مسیریاب بعدی برای این FEC تبدیل شود. در این حالت C از اطلاعاتی که B اعلام کرده استفاده میکند تا LFIB خود را آپدیت کند.

D اطلاعات خود را به C ,B و E ارسال می کند در صورتی که B و C هردو بالادستی D باشند. از اطلاعات برای به روز کردن ورودی LFIB هایشان استفاده می کنند. سرانجام E اطلا عات خود را به D ارسال می کند که از آن برای به روز کردن LFIB خود استفاده می کند. به عنوان نتیجه هر ورودی در LFIB هر LSR اصلاح خواهد شد (جدول۲.۲ را مشاهده کنید)

Table 2.1 FEC entry in each LFIB

LSR	Incoming label	Outgoing label	Next hop	Outgoing interface
A	–	–	LSR B	if0
B	62	–	LSR D	if0
C	–	–	LSR D	if2
D	15	–	LSR E	if2
			LSR E	if0

Table 2.2 FEC entry in each LFIB with

LFIB	Incoming label	Outgoing label	Next hop	Outgoing interface
A	–	62	LSR B	if0
B	62	15	LSR D	if0
C	–	15	LSR D	if2
D	15	60	LSR E	if2
E	60		LSR E	if0

[1] برای آشنائی با تعریف روترهای بالادستی و پائین دستی مراجعه به ضمیمهٔ ۳ مراجعه کرد.

برای LSR E ، مسیریاب بعدی همان E می باشد که این بیانگر این است که بسته IP با پیشوند x.0.0.0, _ y.0.0.0_ به مقصد محلی از طریق if 0 با استفاده از پیشوند آنها ارسال خواهد شد.

هنگامی که برچسب ها توزیع می شود و ورودی در LFIB به روز می شود ارسال بسته IP که به FECی تعلق دارد که با پیشوندx.0.0.0_ _y.0.0.0 همراه می باشد به تنهایی با برچسب ها انجام می شود. با فرض اینکه A بستهٔ IP را از محدوده۱ در IP غیر MPLS با پیشوند <X.0.0.0 , Y.0.0.0> دریافت کند، A مشخص میکند که آدرس بسته به FEC معینی تعلق دارد و برای پیدا کردن مقدار برچسب و اینترفیس خروجی متناظر به LFIB خود مراجعه میکند. مقدار برچسب را در ۶۲ تنظیم می کند و داده ها را با استفاده از طرح شکل 2.1 با یکدیگر تلفیق می کند و به رابط خروجی if0 ارسال می کند. هنگامی که بسته IP به مقدار LSR B رسید،برچسب آن استخراج شده و در LFIB خود به دنبال آن میگردد. برچسب قبلی توسط برچسب جدید جایگزین می شود که برابر ۱۵ می باشد و بسته IP به رابط if0 ارسال میشود. LSR D دقیقا همان رویه را دنبال می کند. هنگامی که بسته IP از B دریافت شد، برچسب خروجی به جای برچسب ورودی جایگزین می شود که برابر ۶۰ می باشد و بسته IP را به رابط if2 ارسال می کند. سرانجام E بسته IP را به مقصد محلی آن ارسال می کند. رویه یکسان برای بسته IP با پیشوند x.0.0.0, y.0.0.0_ که به C از محدوده غیر MPLS ۲ رسیده است، انجام میشود.

در شکل 2.4 تخصیص برچسب ها توسط LSR ها نشان داده شده است. این برچسب ها مشابه مقادیر VPI/VCI در ATM می باشد که دارای مفهوم محلی می باشد بدین معنی که هر برچسب برای یک پیوند معتبر می باشد.

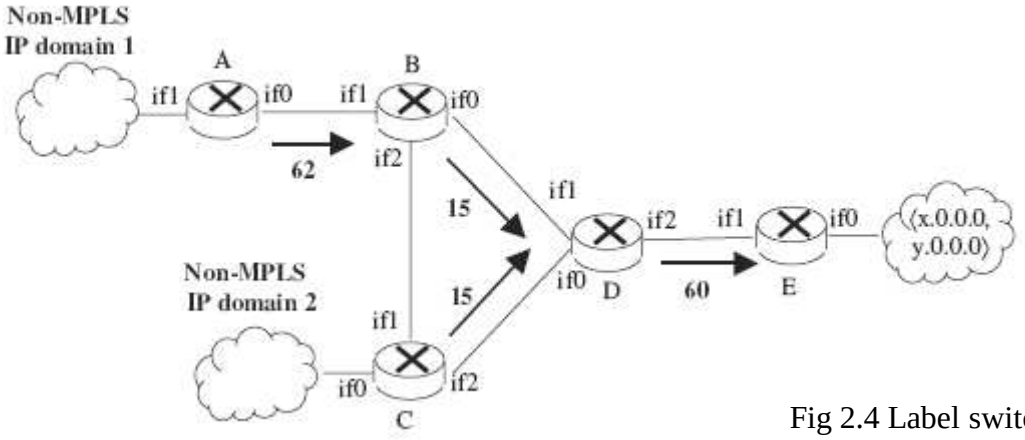


Fig 2.4 Label switched paths.

ترتیب برچسب 62؛ 15؛ 60 به عنوان مسیر سوئیچ برچسب (LSP) شناخته می شود. این مسیر مشابه با ارتباط ATM نقطه به نقطه می باشد که توسط دنباله ای از مقادیر VPI/VCI تعریف می شود. یک اتصال ATM با دو وسیلهٔ پایانی همراه است، از آنجائیکه یک LSP با یک FEC همراه است، چندین LSP که نوعا با

FEC ی یکسان همراه اند تشکیل یک درخت میدهند که در شکل 2.4 نشان داده شده است. هر LSP دارای یک LSR ورودی[1] و یک LSR خروجی[2] میباشد. بعنوان نمونه در شکل 2.4 روترهای A و E بترتیب روترهای ورودی و خروجی برای مسیر سوئیچنگ برچسب از روتر A تا E هستند. به طور مشابه برای مسیر C تا E روترهای C و E بترتیب LSR ورودی و LSR خروجی هستند.

Label switching جست وجو در جدول FIB که عملی پردازش بر است را حذف میکند عملی که برای تشخیص روتر بعدی مربوط به بستهٔ IP به کار میرود. یک جست و جو در LFIB است که به اندازهٔ جست و جو در FIB زمان-بر نیست چرا که LFIB به طور قابل توجهی کوچکتر از FIB است. از زمان معرفی Label Switching چندین الگوریتم مؤثر به لحاظ پردازشی برای انجام دادن جست و جو در FIB توسه داده شده اند .اهمیت MPLS از زمانی که به عنوان راه حل آوردن QoS به شبکهٔ IP مطرح شد به هیچ وجه کاهش نیافته است.

یکی از راههای ممکن معرفی QoS در شبکه اختصاص دادن یک اولویت به هر بستهٔ IP است. این اولویت میتواند در ۳ بیت فیلد آزمایشی برچسب قرار بگیرد.(شکل 2.1 را ببینید). اولویت ها میتوانند توسط گره های کناری شبکهٔ MPLS اختصاص داده شوند. بسته های IP برچسب گذاری شده بر اساس اولویتهایشان همانگونه که در ATM است خدمت دهی میشوند. به یاد آورید یک سوئیچ ATM نوع QoS سلول ورودی را با استفاده از مقادیر VPI/VCI تشخیص میدهد و مطابق با آن قادر به مرتب کردن سلولها برای صف متناسب با QoS می باشد. سوئیچ ATM برای هر رابط خروجی صفوف مختلف QoS را نگهداری میکند. این صفوف با استفاده از الگوریتم زمانبندی خدمات دهی میشوند. بنابراین اتصال VC با توجه به QoS مورد نیاز بکار گرفته میشود. ساختار صفوف مشابهی در یک مسیریاب IP به کار برده میشود. بسته IP در اینترفیس خروجی مطابق با اولویت مرتب می شود و در زمانبندی معین ارسال می گردد.

طرح های تخصیص برچسب

در مثال های سویچ برچسب که در بالا شرح داده شد LSR یک برچسبی برای FEC بدست آورده و این اطلاعات را در LFIB به عنوان برچسب ورودی ذخیره می کند. سپس انقیادهای بین برچسب ورودی و FEC را به روترهای مجاور اعلام میکند. یک LSR بالادستی برچسب را در بخش برچسب خروجی LFIB خود میگذارد. یک LSR غیر بالادستی میتواند از این اطلاعات صرفنظر کرده یا آنرا برای کاربردهای آینده ذخیره کند. به خاطر اینکه LSR ی که بر طبق جریان داده پائین دستی است، برچسب را میسازد و در واقع به این خاطر که برچسب را به شکلی ناخواسته و بدون اطلاع به روترهای مجاور اعلام میکند، این شکل تخصیص و اعلام برچسب به Unsolicited Downstream Scheme یا طرح پائین دستی ناخواسته مشهور است.

---

[1] Ingress LSR

[2] Egress LSR

به عنوان مثال LSR B در شکل 2.4 را بررسی می کنیم .LSR B برچسب ورودیش، ۶۲ را برای FEC مشخص شده با _x.0.0.0,y.0.0.0_ به LSR های مجاورش یعنی A, C, D اعلام می کند.از بین اینها، تنها LSR A بالادست LSR B است تا هنگامی که جریان بسته IP به طرف مقصد_x.0.0.0,y.0.0.0_ می باشد. در این زمینه LSR A از این برچسب برای به روز رسانی LFIB خود استفاده می کند. LSR C وLSR D میتوانند ذخیرهٔ این برچسب را انتخاب کنند. در این حالت تا وقتی که جهت جریان IP مد نظر است آنها میتوانند نسبت به A بالادست شوند در صورتی است که یک لینک یا روتر از شبکه خارج شوند مثلا وقتی که لینک بین C و D بریده میشود در این صورت LSR C ممکن است مجبور شود که دوباره اقدام به مسیردهی ترافیک از طریق B کند. در این مورد C بالادست B خواهد شد.(با توجه به توپولوژی داده شده در شکل 2.4 امکان بالادست شدن D نسبت به B وجود نخواهد داشت.) از طرفی C و D میتوانند اصطلاحا تبلیغات تعلقات برچسب های B را در نظر نگیرند.

یک LSR غیر بالادستی بر حسب اینکه Conservative Retention Mode یا Liberal Retention Mode استفاده شود، اطلاعات مربوط به برچسب را ذخیره میکند یا در نظر نمیگیرد. در حالت نگهداری محافظه کارانه یک برچسب در صورتی نگهداشته میشود که از روتر بالادست روتری باشد که آن اطلاعات را تبلیغ میکند. در حالت نگهداری آزادانه تمامی برچسب ها چه از طرف یک روتر بالادست اعلام شده باشند و چه پائین دست نگهداشته میشوند.

MPLS همچنین میتواند از تخصیص بر حسب تقاضای پائین دستی یا Downstream on Demmand Allocation استفاده کند. در این مورد هر LSR یک برچسب ورودی را به FEC مقید میکند و یک مدخل در LFIB ایجاد میکند با این وجود در این حالت روتر این اطلاعات را به روترهای همسایه آنگونه که در طرح تخصیص پائین دستی ناخواسته انجام میشد، اعلام نمیکند در عوض روتر بالادستی اطلاعات موردنیاز خود را درخواست میکند.

The Next Hop Label Forwarding Entry (NHLFE)

تاکنون بنا به اهداف ارائه فرض کرده ایم که LSR برای هر برچسب یک مدخل را نگهداری میکند. در این مدخل، روتر برچسب ورودی را به یک برچسب خروجی پیوند میدهد و اطلاعاتی مربوط به روتر بعدی و اینترفیس خروجی را فراهم میکند.

معماری MPLS این اجازه را به LSR میدهد تا مدخلهای متعددی برای هر برچسب ورودی نگهداری کند. هر مدخل به عنوان یک NHLFE شناخته میشود و اطلاعات زیر را فراهم میکند: روتر بعدی بسته، عملیاتی که قرار است بر روی برچسب بسته انجام شود و همچنین هر مدخل NHLFE میتواند اطلاعات بیشتری که برای معزول کردن بسته ضروری است فراهم کند.

MPLS به هر بسته امکان حمل چندین برچسب را میدهد که به شکل پشته تنظیم می شوند.یک مثال برای برچسب پشته در شکل 2.5 داده شده است. هر ردیف شامل تلفیق برچسب های مختلفی می باشد. بیت S بیانگر این می باشد که برچسب کنونی آخرین است (S = 1) یا خیر (S = 0). سه عملیات زیر میتواند در بسته برچسب می تواند اجرا شود:

Replace کردن برچسب بالائی با برچسب جدید

POP

Replace then Push

شکل 2.4 تنها نشان دهنده ی اولین عملیات می باشد.هنگامی که LSR B بسته ای از LSR A در یافت می کند برچسب ورودی ۶۲ را با برچسب ۱۵ جایگزین می کند.

Fig 2.5 the Label Stack

Label (20 bits)	Exp (3 bits)	S = 0	TTL (8 bits)
Label (20 bits)	Exp (3 bits)	S = 0	TTL (8 bits)
	• • •		
Label (20 bits)	Exp (3 bits)	S = 1	TTL (8 bits)

همان وقایع در مورد LSR D نیز اتفاق می افتد. دو عملیات بعدی در زیر شرح داده خواهد شد.که استفاده از پشته برچسب را بحث می کنیم.

در موردی که روتر بعدی یک LSR، خود همان روتر است، LSR برچسب بالائی را POP کرده و بستهٔ حاصل بر اساس برچسب به جامانده فوروارد میشود چه بعد از POP برچسبی بر جای مانده باشد چه آن

برچسب تنها برچسب بوده و با خود IP طرف باشیم که باید بر حسب پیشوندش با آن رفتار شود. در مثال 2.4 روتر E برچسب پاکت را POP کرده و بر حسب پیشوند آن در لایهٔ IP به ارسال آن به شبکهٔ غیر MPLS اقدام میکند.

نگاشت برچسب ورودی یا ILM، یک برچسب ورودی را به مجموعه ای از NHLFE هائی که با آن برچسب مرتبط هستند، می نگارد. داشتن چندین مدخل برای هر برچسب ورودی میتواند مفید باشد برای آنکه اجازه ارسال چند-مسیری برای متعادل کردن و محافظت ترافیک یا بار را میدهد. رویهٔ انتخاب یکی از مدخلهای NHLFE فراتر از بحث معماری MPLS است.

در نهایت یک نگاشت FEC-NLFE یا FTN وجود دارد که برای نگاشت یک FEC به مجموعه ای از NHLFEها به کار می رود. این وقتی به کار میرود که بسته ای می رسد که فاقد برچسب است و لازم است قبل از ارسال, برچسبی به آن اختصاص داده شود. در مورد ILM اگر یک FTN نگاشتی را از یک FEC به چندین NHLFE ایجاد کرده بود به رویکردی نیازمندیم که یکی از آنها را انتخاب کند. در مثال شکل 2.4 A و C با استفاده از FTN برای مشخص کردن مدخل مناسب که برچسب خروجی و رابط خروجی بدست می آیند.

Explicit Routing

یک مسیریاب IP تصمیم ارسال خود را با استفاده از آدرس IP مقصدِ پاکت در FIB خود برای تشخیص روتر IP مجاور بعدی انجام میدهد. در هنگام استفاده از یک پروتکل link-state مانند OSPF هر روتر IP بوسیلهٔ تبادل اطلاعات با روترهای دیگر از توپولوژی حوزه اش آگاه میشود. سپس روتر مجاور بعدی را برای هر مقصد با استفاده از الگوریتم OSPF محاسبه میکند. این hop[1] در FIB ش ذخیره میشود. MPLS از اطلاعات هاپ بعدی مشابه برای ایجاد یک LSP[2] استفاده میکند. ازین منظر، این روش مسیریابی به عنوان مسیریابی hop-by-hop مشهور است. به عنوان نمونه در مثال 2.4 ، LSP بین LSR های A و E بوسیلهٔ اطلاعات هاپ بعدی در هر LSR انتخاب شد.

بعلاوه LSP های hop-by-hop در معماری MPLS این اجازه را برای ایجاد یک LSP میدهد که یک مسیر صریح را در شبکه دنبال میکند که لزوما متعلق به مسیر hop-by-hop نیست. این نوع از روتینگ به عنوان explicit routing مشهور است. یک LSP صریحا مسیردهی شده در MPLS معادل اتصال نقطه-به-نقطه در ATM است. یک مسیر صریح ممکن است با هدف ارضای ظوابط QoS مانند حداقل کردن تاخیر end-to-end و بیشینه کردن توان بنا شود. یک همچین ظوابط QoS ممکن است لزوما توسط روتیگ hop-by-hop که معمولا تنها میکوشد که تعداد hop ها را کاهش دهد، ارضا نشود. همچنین explicit routing میتوند به عنوان

[1] در لغت به معنی لی لی و یا پرش کوتاه است و در اصطلاح به معنی روتر نزدیک به روتر فعلی است. به شکل یک شبکه و روترهایش توجه شود هر روتر یک هاپ میتواند باشد. در فارسی شاید بتوان از کلمهٔ خوان مثلا به شکل خوان بعدی استفاده کرد.

[2] Label Switch Path

فراهم کنندۀ تعادل بار به کار رود که بویسلۀ مجبور کردن بخشی از ترافیک برای دنبال کردن مسیری متفاوت در شبکه انجام میشود بنابراین به کار گیری لینکهای شبکه تا حد نهایت ممکن، امکان پذیر است. سرانجام، explicit routing میتواند برای برپاسازی تونلهای مبتنی بر MPLS و شبکه های خصوص مجازی به کار روند.

یک مسیریابی صریح یا explicit route میتواند یکی از دو نوع سختگیر و آسانگیر یا strictly explicity routed یاloosely explicity routed باشد. در مورد نوع strictly explicity routed مسیر بین روتر ورودی و خروجی با دقت معین میشود. یعنی تمام روترها در مسیر به طور کامل ذکر میشوند. در نوع loosely explicity routed تمام روترهای موجود در مسیر لزوما ذکر نمیشوند. بعنوان مثال اگر مسیری مجبور است از چندین دامنه عبور کند، مسیر واقعی ممکن است با دقت ذکر نشود. در این مورد LSR کناری MPLS مسیر را در دامنه اش محاسبه میکند[1] .

طرحهای Strictly explicity routed و Loosely explicity routed در PNNI هم به کار میروند. به عنوان نمونه اگر یک سوئیچ ورودی ATM بخواهد که یک اتصال ATM به سوئیچ خروجی ATMی ایجاد کند که به یک گروه یکسان تعلق دارد، تمام سوئیچهای ATM موجود در مسیر را ذکر میکند، این شبیه روش strictly در MPLS است. از طرف دیگر، اگر سوئیچ خروجی ATM به گروه دیگری تعلق داشته باشد سوئیچ ورودی ATM تمام سوئیچهای موجود در مسیر و متعلق به گروه خود را ذکر میکند و بعد دنباله ای از گره های گروهی منطقی[2] که باید طی شوند را خواهد داد. وقتی که پیغام برپاسازی به گره های گروهی منطقی میرسد آن گره منطقی خود موظف است که مسیر را در گروه خود محاسبه کند.[3] این شبیه طرح loosely explicity routed است.

مثالی از کاربرد پشته برچسب

مثالی از کاربرد پشته برچسب در شکل ۲.۶ نشان داده شده است.در آنجا سه حوزه MPLS (A, B, C) و مسیر صریح میان LSR 1 در حوزه A و LSR 6 درحوزۀ C ایجاد شده است.

پشته برچسب در هر hop و انجام عملیات برچسب در هر LSR در طول مسیر در شکل ۲.۶ نشان داده شده است. برچسب خروجی از LSR 1 تا LSR 2 برابر ۶۰ می باشد.(در اینجا برای سادگی راجع به اینکه LSR 1 چگونه این برچسب را انتخاب کرد و این بسته از کجا آمده کاری نداریم.) عملکرد برچسب در LSR 2 به صورت زیر می باشد: جایگزین کردن برچسب جدید در بالای پشتۀ برچسب و سپس push کردن یک برچسب جدید دیگر در بالای پشته. در نتیجۀ این عملیات، برچسب ۶۰ با ۷۰ جایگزین شده و یک برچسب

---

[1] پس نیازی به ذکر روترهای میانی هر دامین نیست./س

[2] میتوان گفت ابر گره یا گره ای که در واقع متشکل از چندین گره است و در واقع این گره مجازی یک دامنه یا گروه متفاوت است که جزئیات آن توسط روتر مورد بحث ذکر نمیشود/س

[3] در واقع در این حالت روتر تمام روترهای گروه خود را ذکر میکند اما مسئولیت روترهای گروه های دیگر را به روتر ورودی آن گروه محول میکند و بنابراین برای گروههای دیگر تنها به ذکر نام گره های ورودی گروههای دیگر می پردازد /س

جدید با مقدار ۴۰ در بالای پشته قرار میگیرد. از LSR 3 به LSR 4 پاکت بوسیلهٔ این عملیات ارسال میگردد که در شکل به وضوح می بینید. مسئلهٔ مهم در LSR 4 اتفاق می افتد که عملیات pop در بالای پشته انجام میشود و در نتیجهٔ آن برچسب بالائی ۶۶ از پشته حذف میشود و اکنون پاکت به سمت LSR 5 بوسیلهٔ برچسب ۷۰ فرستاده میشود. LSR 5 هم پاکت را با این عملیات روی برچسب به LSR 6 می فرستد: جایگزین کردن برچسب بالای پشته با یک برچسب جدید. در نتیجه با برچسب ۳۰ به LSR 6 میرسد.

همانطور که دیده شد، وقتی که پاکت در دامین B MPLS فرستاده شد شامل دو برچسب بود. برچسب بالائی برای سوئیچنگ در داخل حوزهٔ B مورد استفاده قرار گرفت و برچسب پائینی برای اتصال گره های کناری دامینهای B و C به کار رفت.

این استفاده از پشتهٔ برچسب ایجاد تونل LSP یا LSP Tunnel را اجازه میدهد. بعنوان نمونه میتوان اینگونه فرض کرد که مسیر بین LSR 3 و 4 در دامین B بوسیلهٔ برچسبهای ۲۲ و ۵۴ و ۶۶ یک تونل است که LSR 2 را به LSR 5 وصل میکند. برای LSR 2 به منظور فروارد کردن پاکتها به داخل تونل مجبور است از

برچسب ۴۰ استفاه کند. در طرف دیگر تونل، برای فرستادن پاکت به LSR 6 ، برچسب ورودی به LSR 5 باید برچسب ۷۰ را داشته باشد، بنابراین LSR 5 میتواند آنرا به LSR 6 سوئیچ کند. این برچسب در پائین پشتهٔ برچسب حمل شد.

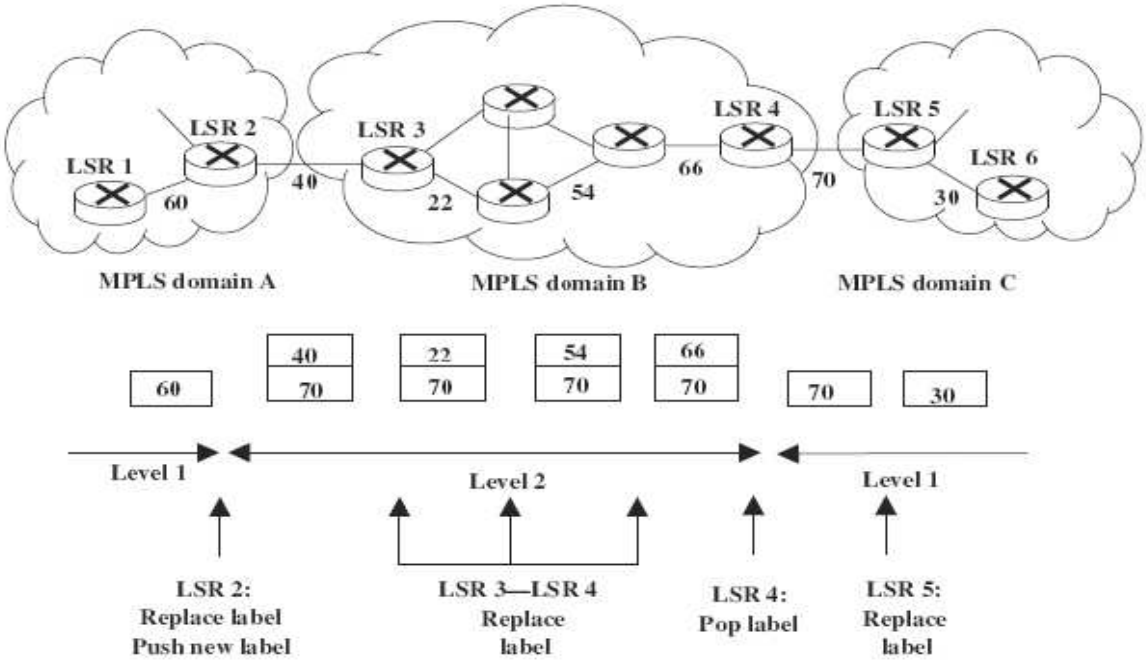


Fig 2.6: an Label Stack application as MPLS

در معماری MPLS این امکان وجود دارد که یک LSP را مجبور ساخت که از طریق LSR ها در ترتیب ویژه ای ایجاد شوند. به طور مشخص این دو سبک میتوانند مورد استفاده قرار گیرند:

Independt LSP Control

Ordered LSP Control

در independent LSP control هر LSR یک برچسب را به هر FEC وابسته میکند و این انقیاد ها را به روترهای همسایه به محض مواجه شدن با یک FEC جدید اطلاع میدهد. در ordered LSP control اختصاص برچسب ها از LSR خروجی به عقب می آید. این قونین به کار میرود: یک LSR فقط وقتی یک برچسب را به یک FEC مقید میکند که آن، یک LSR خروجی برای آن FEC باشد؛ یا در حال حاضر یک انقیاد برچسب را برای آن FEC از طریق هاپ بعدی آن دریافت کرده باشد.

در مثالی که در شکل ۲.۴ مطرح شد، ما میتوانیم فرض کنیم که Independent LSP control استفاه شده بود. یعنی هر LSR مستقل از بقیه LSR ها یک برچسب را به FEC < X.0.0.0 , Y.0.0.0 > مقید میکند و آنرا به بقیه اعلام میکند بدون اینکه منتظر باشد که تا LSR کناری اعلانی را برای آن FEC بدهد. Ordered LSP control برای ایجاد یک explicit route به کار میرود.

در MPLS این امکان وجود دارد که پاکتهای IP متعلق به دو یا چند FEC مختلف یک مسیر را طی کنند. این ممکن است وقتی رخ دهد این FEC ها یک گره خروجی را دارند. در این مورد، این امکان وجود دارد تا این FEC ها در یک یا چند FEC متراکم کرد یا اینکه اصلا آنها را تجمیع نکرد و جداگانه گذاشت.[1]

پروتکل های توزیع برچسبی[1]

[1] MPLS برای اجرا بر روی شبکه های مختلف طراحی شده است که شامل ATM و Frame Relay هم میشود. در این مورد دیگر MPLS بر روی IP اجرا نمیشود بلکه از پروتکلهای مخصوص هر یک ازین شبکه های استفاده میکند برای بحث مفصلتر میتوان به خود کتاب مراجعه کرد بحث MPLS over ATM به خاطر ارتباط کمتر با هدف در اینجا ذکر نمیشود ./س

MPLS برای توزیع معتبر انقیادهای برچسبی بین LSR ها ، به مجموعه ای از رویه ها نیاز دارد. MPLS به استفاده از یک پروتکل توزیع برچسبی واحد نیازی ندارد. از این نظر، رویه های متعددی برای توزیع برچسب ها پیشنهاد شده اند، که پروتکل توزیع برچسبی (LDP) و پروتکل رزرواسیون منابع – مدیریت ترافیک (RSVP-TE) متداول ترین پروتکل ها می باشند.

LDP یک پروتکل سیگنالینگ جدید می باشد، که برای توزیع انقیادهای برچسبی برای LSP مرتبط با یک FEC استفاده می شود، که به پروتکل توزیع برچسبی مسیریابی مبتنی بر محدودیت (CR-LDP) توسعه یافته است که برای برقرار کردن یک مسیر صریح استفاده می شود (یعنی، یک LSP بین دو LSR) . LDP و CR-LDP در بخش های ۷.۱ و ۷.۲ توضیح داده می شوند.

یک روش پیشنهادی برای توزیع انقیادهای برچسبی ، بسط یک پروتکل کنترل IP موجود مانند BGP ، PIM و RSVP می باشد ، بنابراین می تواند انقیادهای برچسبی را حمل کند. نسخه ی توسعه یافته ی RSVP به صورت RSVP-TE معرفی می شود و متداول ترین پروتکل در بین سه پروتکل دیگر توزیع انقیادهای برچسبی می باشد. RSVP-TE برای نصب LSP ها با استفاده از اطلاعاتhop بعدی در مسیریابی لیستی از LSR و LSP هایی با مسیریابی صریح قابل استفاده می باشد. RSVP و RSVP-TE در بخش های بعدی توضیح داده خواهد به طور نمونه، یک LSR هر دوی LDP و RSVP-TE را راه اندازی خواهد کرد. دو پروتکل توزیع برچسبی سازگار نمی باشند. با این حال، برای ایجاد یک LSP از LDP و یا RSVP-TE استفاده می شود.

کل چارچوب این بخشهای پیش رو با توضیح LDP و سپس CR-LDP شروع شده و با پروتکلهای RSVP و RSVP-TE به پایان میرسد.

پروتکل توزیع برچسبی[۲] (LDP)

LDP برای ایجاد و نگهداری انقیادهای برچسبی برای یک LSP مرتبط با یک FEC استفاده می شود. دو LSR ی که از LDP برای تعویض انقیادهای برچسبی استفاده می کند، به صورت همتاهایLDP (LDP Peers) معرفی می شوند. LDP پیام های متعدد LDP را فراهم می سازد که به صورت زیر طبقه بندی می شوند :

- پیام های کشف: این پیام ها برای اعلان و نگهداری از حضور یک LSR در شبکه مورد استفاده قرار می گیرند.

---

[۱] بخشهای پیش رو ترجمهٔ فصل ۷ کتاب فوق الذکر است. که بر پروتکلهای روتینگ و مهندسی ترافیک تاکید دارد.

[۲] Label Distribiution Protocol

- پیام های جلسه ای : به منظور مبادله ی اطلاعات توسط دو همتای LDP ، آنها باید ابتدا یک جلسهٔ LDP ایجاد کنند. پیام های جلسه ای برای ایجاد، نگهداری و به پایان رساندن جلسه های LDP بین peerهای LDP استفاده می شوند.
- پیام های تبلیغاتی : این پیام ها برای ایجاد، تغییر و حذف انقیادهای برچسبی به FECها مورد استفاده قرار می گیرند.
- پیام های اعلان : این پیام ها برای فراهم سازی اطلاعات مشورتی و اطلاعات خطای سیگنالی استفاده می شوند.

LDP برای افزایش قابلیت اطمینان به استثنای پیام های کشف LDP که روی UDP اجرا می شود، روی TCP راه اندازی می شود.

قبل از اینکه به توصیف پیام های LDP و فرمت آنها بپردازیم ، در بخش بعدی مفاهیم متعدد LDP مانند فضای برچسب به ازای هر پلتفرم و هر واسط ، جلسهٔ LDP و همجواری های hello را مورد بحث و بررسی قرار می دهیم.

فضاهای برچسب، جلسه های LDP و همجواری های Hello

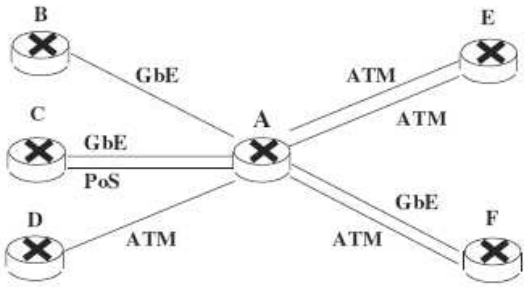
LDP استفاده از مفهوم فضای برچسب را ایجاد می کند که مجموعه ای از تمام برچسب ها می باشد. دو نوع از فضای برچسب ارائه شده اند : فضای برچسب به ازای هر واسط[۱] و فضای برچسب به ازای هر پلتفرم[۲]. فضای برچسب به ازای واسط، مجموعه ای از برچسب ها می باشد که به یک واسط خاصی تخصیص می یابند .به عنوان مثال، یک واسط ATM از شماره های VPI/VCI که مختص واسط می باشند، استفاده می کند. همچنین، یک واسط Frame Relay از مقادیر DLCI استفاده می کند که به واسط خاصی اختصاص می یابد. فضای برچسب به ازای هر پلتفرم ، مجموعه ای از برچسب های به اشتراک گذاشته شده توسط تمام واسط ها به غیر از ATM و واسط های Frame Relay مانند packet-over-SONET(Pos) و اترنت گیگابایت (GbE) می باشد. هنگام انتقال این بسته ها بر روی این لینک ها ، برچسب های MPLS در تلفیق های داده ای برچسب خاص حمل می شوند. (شکل ۲.۱). این برچسب ها توسط نرم افزار یکسانی پردازش می شوند و همه ی آنها به فضای برچسب پلتفرم یکسان تعلق دارند.

یک فضای برچسب LSR توسط یک مقدار ۶ بایتی مشخص می شود. ۴ بایت اول یک مقدار واحد مشخص کننده ی LSR را حمل می کند، مانند یک ID مسیریاب ۳۲ بیتی که توسط مدیر سیستم خودکار به LSR تخصیص یافته است. دو بایت آخر فضای برچسب را مشخص می سازد. اگر فضای برچسب به ازای هر پلتفرم باشد، بنابراین، دو بایت آخر به id فضای برچسب 0.A تنظیم می شود ، که اصولا به عنوان یک LDP id به آن

[۱] Per Interface Label Space

[۲] Per Platform Label Space

اشاره می شود که به شکل و فرم زیر <LSRDid, Label Space Number> بیان می شود. مثالی از id های فضای برچسب در شکل ۲.۷ نشان داده می شود. شماره ی LSR id برای LSR A ، lsr170 می باشد. LSR A به LSR های B,C,D,E و F متصل می شود. از طریق واسط A GbE به B وصل می شود. از طریق یک واسط GbE و همچنین از طریق واسط مجزای PoS به C وصل می شود. از طریق واسط ATM به D وصل می شود و از طریق دو واسط ATM مجزا به E وصل می شود و از طریق یک واسط GbE و یک واسط مجزای ATM به F متصل می شود. LSR A ، id _lsr170,0_ فضای برچسب به ازای هر پلتفرم را به B و C اعلان می کند . فضای برچسب غیرصفر _lsr170,1_ را به D اعلان می کند و id فضای برچسب غیرصفر _lsr170,2_ روی اولین لینک ATM و _lsr170,3_ روی دومین لینک ATM را به E اعلان می کند و فضای برچسب غیرصفر _lsr170,4_ روی لینک ATM و id فضای برچسب به ازای هر پلتفرم _lsr170,0_روی واسط GbE را به F اعلان می کند.



شکل ۲.۷ .نمونه ای از Id فضای برچسب

به صورت خلاصه،Id فضای برچسب که به همسایه های خود انتشار می دهد اینها هستند:

- _lsr170,0_ برای LSR B, LSR C (هردو واسط) وLSR F (واسط GbE).
- _lsr170,1_ برای LSR D (برای اینترفیس ATM).
- _lsr170,2_ برای LSR E (برای اولین اینترفیس ATM).
- _lsr170,3_ برای LSR E (برای اینترفیس دوم ATM).
- _lsr170,4_ برای LSR F (برای اینترفیس ATM).

یک اجلاس LDP بین دو LSR ی که مستقیما به هم وصل شده اند برای ایجاد امکان تبادل پیامهای LDP بین خود ایجاد میشود. یک اجلاس LDP بین دو LSR با یک Label Space همراه است. برای مثال بالا اجلاس های زیر بنا میشوند:

- A-B: یک اجلاس LDP برای <lsr170,0>
- A-C: یک اجلاس LDP برای <lsr170,0>
- A-D : یک اجلاس LDP برای <lsr170,1>
- A-E:2 LDP اجلاس یکی برای <lsr170,2> و یکی برای <lsr170,3>

- A-F:LDP 2 اجلاس یکی برای <lsr170,0> و یکی برای <lsr170,4>

همچنین نصب یک جلسهٔ LDP بین دو LSR که بصورت غیر مستقیم متصل شده اند، امکان پذیر می باشد که زمانیکه دو LSR دور از هم بخواهند از طریق یک LSP ارتباط برقرارکنند ، قابل استفاده می باشد. دو LSR می توانند جلسه ای (یا اجلاسی یا همان session) را به منظور برقراری ارتباط یک انقیاد برچسبی ایجاد کنند. این برچسب می تواند پشته ی برچسب را همانند مثال بیان شده در بخشهای قبلی به کار گیرد.

مکانیزم کشف LDP ، LSR را به منظور کشف همتاهای LDP بالقوه اش فعال می سازد. (یعنی، سایر LSRهایی که به طور مستقیم به آن وصل می شوند). یک LSR به صورت پریودیک hello های لینک LDP خارج از هر واسط را ارسال می کند. بسته های Hello از طریق UDP آدرس دهی شده به یک پورت کشف LDP برای تمام مسیریاب های موجود روی آدرس چندگانه ی گروه زیرشبکه ارسال می شوند. Hello لینک LDP ارسال شده توسط یک LSR ، id فضای برچسبی را که LSR می خواهد برای واسط و احتمالا اطلاعات اضافی استفاده کند، را حمل می کند. دریافت یک Hello لینک LDP یک مجاورت hello را مشخص می سازد. برای هر واسط ، یک مجاورت hello وجود دارد.

مبادله ی hello های لینک LDP بین دو LSR ، ایجاد یک جلسهٔ LDP را مورد هدف قرار می دهد. اگر یک لینک مجزا بین دو LSR وجود داشته باشد، بنابراین یک مجاورت hello مجزا و یک جلسهٔ LDP مجزا تنظیم می شوند. اگر لینک های موازی به همراه فضای برچسب به ازای هر پلتفرم وجود داشته باشند، در اینصورت به تعداد لینک های مجاورت های hello وجود خواهد داشت ولی تنها یک جلسهٔ LDP وجود خواهد داشت. اگر لینک های موازی وجود داشته باشند، یکی به همراه فضای برچسب به ازای هر پلتفرم خواهد بودو بقیه به همراه فضای برچسب به ازای هر واسط خواهند بود که یک جلسهٔا جلسه به ازای هر واسط و یک مجاورت به ازای هر جلسه تنظیم می شود. برای مثال موجود در شکل ۲.۷ ، جلسه های بعدی و مجاورت های hello تنظیم می شوند:

- A-B:یک جلسهٔ LDP با یک همجواری Hello
- A-D یک جلسهٔ LDP با یک همجواری Hello
- A-C: یک جلسهٔ LDP با دو همجواری Hello
- A-E: دو جلسهٔ LDP هرکدام با یک همجواری Hello
- A-F دو جلسهٔ LDP هرکدام با یک همجواری Hello

برقراری یک جلسهٔ LDP از دو مرحله تشکیل می یابد. سپس یک جلسه LDP مقداردهی اولیه می شود زمانیکه دو LSR پارامترهای جلسهٔ را منتقل می کنند (مانند نسخه ی پروتکل، روش توزیع برچسبی ، مقادیر تایمر ، دامنه ی تغییرات مقادیر VPI/VCI برای ATM و دامنه ی تغییرات مقادیر DLCI برای Frame Relay).

LSR از تایمر برای هر مجاورت hello حفاظت می کند که هر بار که یک پیام hello دریافت می کند مجددا راه اندازی می شود. اگرتایمر بدون دریافت یک پیام hello از LSR خاتمه یابد، مجاورت Hello حذف می شود. جلسهٔ LDP در صورتی خاتمه می یابد که تمام همجواری های hello مرتبط با یک جلسهٔ LDP حذف شوند.

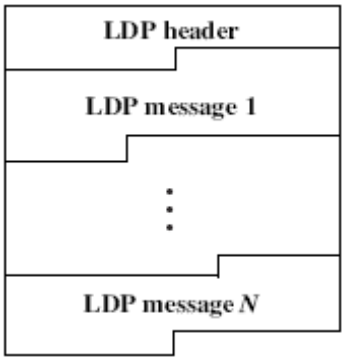
LSR از تایمر keepAlive برای هر جلسه حفاظت می کند. تایمر هر بار که هر LSP PDU را از LDP peer دریافت می کند ، مجددا راه اندازی می شود. اگر LDP peer چیزی برای ارسال نداشته باشد، پیام keepAlive را ارسال می کند.

فرمت *LDP PDU*

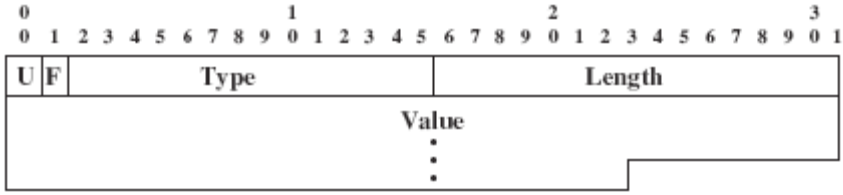
LDP PDU از یک LDP header به همراه یک یا چند پیام LDP که ممکن است به یکدیگر مرتبط نباشند ، تشکیل می یابد. فرمت LDP PDU در شکل ۲.۸ نشان داده شده است. LDP header از موارد زیر تشکیل می یابد :

- ✓ نسخه (version) : یک فیلد ۱۶ بیتی که شامل نسخه ی پروتکل می باشد.
- ✓ طول PDU : یک فیلد ۱۶ بیتی که کل طول LDP PDU را در بایت ها می دهد ، شامل فیلد های نسخه و طول PDU از LDP PDU header .
- ✓ LDP id : یک فیلد ۴۸ بیتی که شامل LDP id می باشد (یعنی id فضای برچسب) که دارای فرم id ۳۲ بیتی مسیریاب و شماره فضای برچسب می باشد.

فرمت پیام LDP از یک header به همراه پارامترهای اجباری و اختیاری تشکیل می یابد . header و پارامترها با استفاده از طرح نوع-طول-مقدار (TLV) که در شکل ۲.۹ نشان داده شده است کدگذاری می شوند. موارد زیر تعریف شده اند :



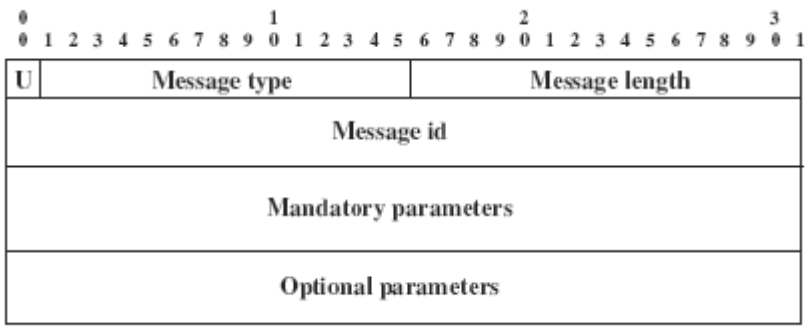
شکل۲.۸. فرمت LDP PDU



شکل ۲.۹. فرمتTLV

- ✓ U (بیت نامعلوم TLV) : زمانی مورد استفاده قرار می گیرد که TLV نامعلوم دریافت شود. اگر U=0 باشد ، در اینصورت یک اعلان به تولید کننده ی پیام برگردانده می شود و کل پیام حذف می شود. اگر U=1 باشد، بنابراین TLV حذف می شود و بقیه ی پیام طوری پردازش می شود که گویی TLV وجود نداشته است.
- ✓ F (بیت نامعلوم ارسالی TLV) : این بیت تنها زمانی مورد استفاده قرار می گیرد که U=1 باشد، و پیام LDP دربرگیرنده ی TLV نامعلوم باید ارسال شود . اگر F=0 باشد ، TLV نامعلوم به همراه بقیه ی پیام ارسال نمی شود، اگر F=1 باشد ، TLV نامعلوم به همراه بقیه ی پیام ارسال می شود.
- ✓ نوع : یک فیلد ۱۴ بیتی که مشخص می سازد که چگونه فیلد مقدار تفسیر می شود.
- ✓ طول : یک فیلد ۱۶ بیتی که فیلد مقدار را در بایت ها نشان می دهد.
- ✓ مقدار : شامل اطلاعاتی می باشد که به صورتی تفسیر می شود که در فیلد نوع مشخص شده است. ممکن است شامل کدگذاری TLV توسط خود TLV باشد.

فرمت پیام LDP



شکل ۲.۱۰. فرمت پیامLDP

فرمت پیام LDP در شکل ۲.۱۰ نشان داده شده است. موارد زیر تعریف شده اند :

- ✓ U (بیت پیام نامعلوم) : در طول دریافت یک پیام نامعلوم ، اگر U=0 باشد ، در اینصورت یک اعلان به تولید کننده ی پیام برگردانده می شود. اگر U=1 باشد ، در اینصورت پیام نامعلوم به آرامی حذف می شود.
- ✓ نوع پیام : یک فیلد ۱۵ بیتی که برای شناسایی نوع پیام مورد استفاده قرار می گیرد.
- ✓ طول پیام : یک فیلد ۱۶ بیتی که کل طول فیلد ID پیام را در بایت ها و فیلد های پارامترهای اختیاری و اجباری را برمی گرداند .
- ✓ ID پیام : یک مقدار ۳۲ بیتی استفاده شده برای شناسایی این پیام . پیام های بعدی مربوط به این مقدار باید ID پیام یکسانی را حمل کند.

فیلد های اجباری به صورت مجزا برای هر پیام اختصاصی LDP مورد بررسی قرار خواهند گرفت.

پیام های LDP

پیام های LDP زیر تعریف شده اند : اخطار، hello ، مقداردهی اولیه، keepAlive ، آدرس ، بازپس گیری آدرس ، نگاشت برچسب ، درخواست برچسب، درخواست توقف برچسب، بازپس گیری برچسب و انتشار برچسب.

- ✓ پیام اخطار (notification) :

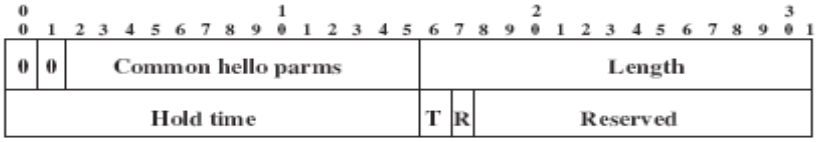
این پیام برای مطلع ساختن یک LDP peer از یک خطای مهلک یا برای فراهم سازی اطلاعات مشورتی با درنظرگرفتن خروجی پردازش یک پیام LDP یا وضعیت یک جلسهٔ LDP مورد استفاده قرار می گیرد. برخی از پیام های notification به صورت زیر می باشند :

- PDU ناقص یا پیام
- TLV نامعلوم یا ناقص
- انقضای مدت keepAlive جلسه
- بستن جلسهٔ یک طرفه
- رویدادهای مقداردهی اولیه ی پیام
- رویدادهای حاصل از خطاهای دیگر

- ✓ پیام Hello

پیام های LDP hello به عنوان بخشی از مکانیزم کشف LDP مبادله می شوند. فرمت پیام Hello در شکل ۲.۱۰ با تنظیم بیت U به صفر و تنظیم نوع پیام به hello(0x0100) نشان داده شده است. فیلد پارامترهای اجباری ، اشاره شده به صورت پارامترهای TLV متداول hello در شکل ۲.۱۱ نشان داده شده است. موارد زیر برای پارامترهای TLV متداول hello تعریف شده اند:

- زمان نگهداری : زمان نگهداری hello در چند ثانیه مشخص می شود. این زمانی است که LSR فرستنده رکوردی از helloهای دریافتی از LSR گیرنده را بدون دریافت hello دیگر نگهداری خواهد کرد. اگر hold time=0 باشد، در اینصورت مقدار پیش فرض ۱۵ ثانیه برای hello های لینک یا ۴۵ ثانیه برای hello های مورد نظر استفاده می شود.مقدار 0xffff به معنی بینهایت می باشد. تایمر hold هر بار که پیام hello دریافت می شود ، مجددا راه اندازی می شود. درصورتیکه قبل از دریافت پیام hello خاتمه یابد ، همجواری hello حذف می شود.
- T : نوع hello را مشخص می سازد : یک hello هدف (T=1) یا hello لینک (T=0) .
- R : این فیلد به request send targeted hellos یا سلامهای مورد هدف درخواست ارسال مشهورند. مقدار ۱ نشان می دهد که گیرنده hello های مورد نظر پریودیکی را به مبدا این hello می فرستد. مقدار ۰ چنین درخواستی نمی کند.

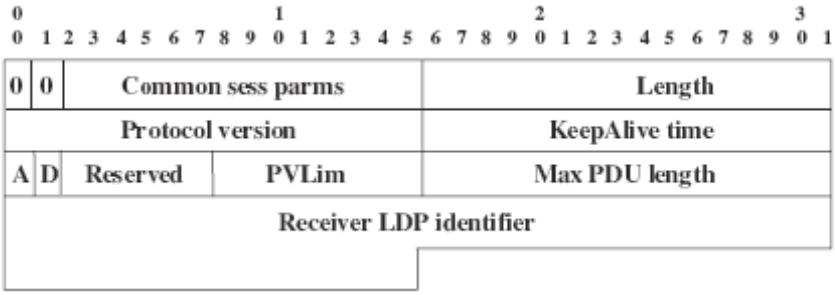


شکل ۲.۱۱. پارامترهای TLV عمومیhello

✓ پیام مقداردهی اولیه (Initialization) :

این پیام برای درخواست ایجاد یک جلسهٔ LDP مورد استفاده قرار می گیرد. فرمت پیام مقداردهی اولیه در شکل ۲.۱۰ به همراه تنظیم بیت U به صفر و تنظیم نوع پیام به مقداردهی اولیه (0X0200) نشان داده شده است. فرمت برای فیلد پارامترهای اجباری ، اشاره شده به صورت "پارامترهای TLV جلسه های عمومی" که در شکل ۲.۱۲ نشان داده شده است. موارد زیر تعریف شده اند :

- زمان KeepAlive : ماکزیمم تعداد ثانیه هایی را مشخص می سازد که می تواند بین دریافت دو LDP PDU متوالی سپری شود. تایمر keepAlive هر بار که LDP PDU دریافت می شود، مجددا راه اندازی می شود.
- A : نوع اعلان برچسب را مشخص می سازد: جریان پائین دستی بدون درخواست (A=0) یا جریان پایین دستی همراه با درخواست (A=1) .جریان پایین دستی همراه با درخواست تنها برای یک ATM یا یک لینک Frame Relay استفاده می شود. جریان پایین دستی بدون درخواست نیز باید مورد استفاده قرار گیرد.



شکل۲.۱۲.پارامترهای جلسه عمومی TLV

- D : تشخیص حلقه را فعال می سازد.
- PVLim[1] (محدوده ی بردار مسیر) : ماکزیمم تعداد LSR های ثبت شده در بردار مسیر را برمی گرداند که در تشخیص حقله به کار میرود.
- ماکزیمم طول PDU : مقدار پیش فرض ماکزیمم طول مجاز ، ۴۰۹۶ بایت می باشد.
- تعیین کننده ی گیرنده ی LDP : فضای برچسب گیرنده را مشخص می سازد.

فیلد پارامترهای جلسهٔ اختیاری می تواند برای فراهم سازی پارامترهای مربوط به جلسات ATM و Frame Relay به کار رود.

✓ پیام KeepAlive :

LSR پیام های KeepAlive را به صورت بخشی از مکانیزمی که یکپارچگی یک جلسهٔ LDP را بازبینی می کند، ارسال می کند. فرمت پیام KeepAlive در شکل ۲.۱۰ به همراه تنظیم بیت U به صفر و تنظیم نوع پیام به KeepAlive(0X0201) نشان داده شده است. هیچ پارامتر اختیاری یا اجباری در نظر گرفته نشده است.

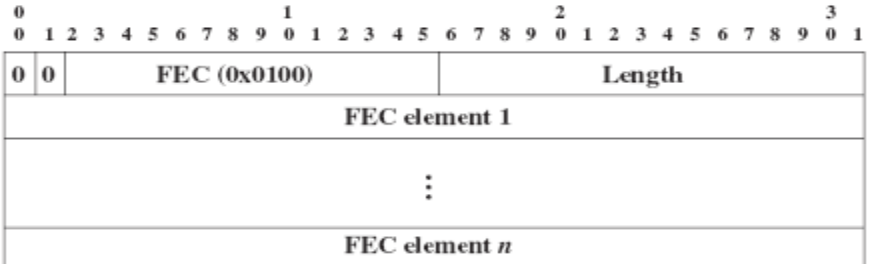
✓ پیام های آدرس و پس گرفتن آدرس (Address and address withdraw) :

قبل از ارسال یک نگاشت برچسب و پیام های درخواست برچسب ، LSR آدرس های واسطش را با استفاده از پیام های آدرس اعلان می کند. آدرس های از قبل اعلان شده می تواند با استفاده از پیام پس گیری آدرس پس گرفته شود.

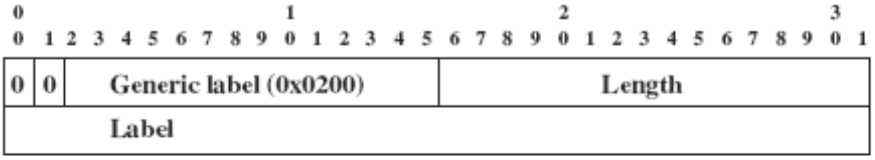
✓ پیام نگاشت برچسب (Label Mapping):

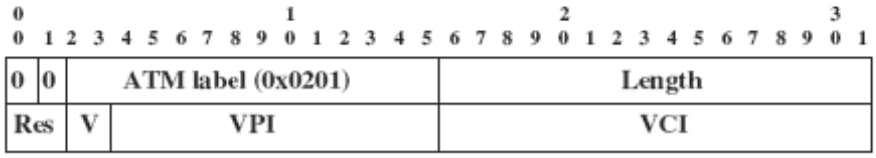
LSR از این پیام برای اعلان یک نگاشت برچسب برای یک FEC به LDP peer هایش استفاده می کند. فرمت پیام نگاشت برچسب دارای ساختاری مشابه با ساختار نشان داده شده در شکل ۲.۱۰ به همراه تنظیم بیت U به صفر و تنظیم نوع پیام به نگاشت برچسب (0x0400) می باشد. فیلد پارامترهای اجباری از یک FEC TLV و یک برچسب TLV تشکیل می یابد.

[1] Pathe vector limit



شکل۲.۱۳.FEC TLV





شکل۲.۱۴.برچسب عمومی و TLVبرچسب ATM

در LDP ، عنصر FEC می تواند یک پیشوند آدرس IP باشد یا آدرس IP کامل یک میزبان مقصد باشد. FEC TLV در شکل ۲.۱۳ نشان داده شده است. LDP به FEC اجازه می دهد که توسط مجموعه ای از عناصر FEC مشخص شود، که هر عنصر FEC مشخص کننده ی مجموعه ای از بسته هایی است که می توانند به LSP مورد نظر نگاشت یابند. (به عنوان مثال زمانی می تواند مورد استفاده قرار گیرد که یک LSP توسط چندین مقصد FEC که همگی از یک مسیر استفاده میکنند، به اشتراک گذاشته شود). برچسب TLV ، برچسب مرتبط با FEC درنظرگرفته شده در FEC TLV را برمی گرداند. این برچسب می تواند یک مقدار برچسب ۲۰ بیتی یا یک مقدار VPI/VCI در حالت ATM یا یک مقدار DLCI در حالت Frame Relay باشد .برچسب کلی و برچسب ATM TLV ها در شکل ۲.۱۴ نشان داده شده است. فیلد دو بیتی V موجود در برچسب ATM TLV ، معروف به v bit ، به صورت زیر مورد استفاده قرار می گیرد. اگر V بیت به صورت 00 باشد ، در اینصورت هر دوی فیلد های VPI و VCI مهم می باشند ،اگر V بیت به صورت 10 باشد در اینصورت فقط VCI مهم می باشد.

- ✓ پیام درخواست برچسب :

LSR یک پیام درخواست برچسب به یک LDP Peer برای درخواست یک نگاشت برای FEC خاص ارسال می کند. پیام درخواست برچسب دارای فرمت نشان داده شده در شکل ۷.۴ به همراه تنظیم بیت U به صفر و

تنظیم نوع پیام به درخواست برچسب (0x0401) می باشد. فیلد پارامترهای اجباری شامل FEC TLV نشان داده شده در شکل ۲.۱۳ می باشد.

LSR می تواند پیام درخواست برچسب را تحت شرایط زیر ارسال کند :

- LSR یک FEC جدیدی را از طریق ارسال جدول مسیریابی تشخیص می دهد، hop بعدی یک LDP peer می باشد، و LSR فعلا دارای یک نگاشت از hop بعدی برای FEC مورد نظر نمی باشد.
- hop بعدی برای FEC تغییر می یابد ، و LSR فعلا دارای یک نگاشت از hop بعدی برای FEC مورد نظر نمی باشد.
- LSR یک درخواست برچسب برای یک FEC از یک LDP peer بالادستی دریافت می کند ، hop بعدی FEC یک LDP peer می باشد و LSR فعلا دارای یک نگاشت از hop بعدی نمی باشد.

✓ پیام های توقف برچسب، بازیابی برچسب و آزادسازی برچسب[۱] :

LSR A می تواند یک پیام توقف برچسب به یک LDP peer در اینجا LSR B برای متوقف سازی یک پیام درخواست برچسب معوقه، ارسال کند. به عنوان مثال این مسئله ممکن است زمانی رخ دهد که hop بعدی LSR برای FEC از LSR B به یک LSR متفاوت تغییر یابد.

LSR A از پیام بازیابی برچسب برای برچسب دهی به یک LDP peer در اینجا LSR B استفاده می کند که نمی تواند با استفاده از یک نگاشت برچسب FEC خاص که LSR A قبلا اعلان کرده بود، ادامه یابد. LSR A یک پیام آزادسازی برچسب به یک LDP peer در اینجا LSR B برای برچسب دهی به LSR B ارسال می کند که LSR A دیگر نیازی به نگاشت برچسب FEC خاصی که قبلا درخواست شده بود ، ندارد.

پروتکل توزیع برچسب–مسیریابی مبتنی برتحمیل[۲] (CR-LDP)

CR-LDP یک پروتکل توزیع برچسب مبتنی بر LDP می باشد. همانطور که در بالا اشاره شد، LDP می تواند برای نصب یک LSP مرتبط با یک FEC خاص مورد استفاده قرار گیرد. CR-LDP برای نصب یک LSP نقطه به نقطه ی یک جهته ای که به صورت صریح مسیریابی شده است مورد استفاده قرار می گیرد که به مسیر سوییچ شده ی برچسب- مسیریابی مبتنی بر تحمیل[۳] . (CR-LSP)

LSP به عنوان نتیجه ای از اطلاعات مسیریابی در یک شبکه ی IP با استفاده از الگوریتم کوتاه ترین مسیر نصب می شود. CR-LSP در مبدا LSR بر اساس شرایط که تنها به اطلاعات مسیریابی محدود نمیباشد مانند

---

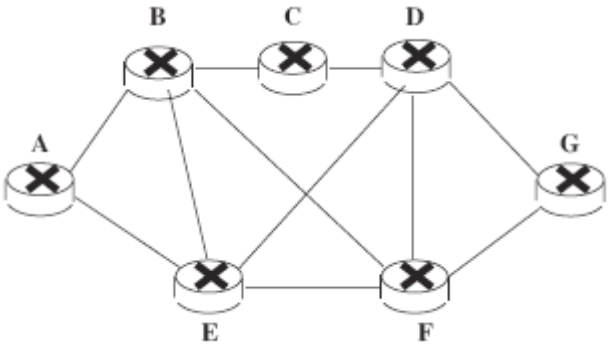
[۱] Label abort, label withdraw, and label release messages

[۲] Contrained-Based Label Distribiution Protocol

[۳] Constrained-Based routed label switched path

مسیریابی صریح و مسیریابی QoS محاسبه می شود. سپس مسیر به سایر گره های موجود در طول مسیر که دستورات مسیریابی مبدا را رعایت می کند ، فرستاده می شود. این تکنیک مسیریابی ، در اصطلاح source routing همچنین در ATM مورد استفاده قرار می گیرد. CR-LSP موجود در MPLS شبیه یک اتصال در ATM می باشد ، البته یک جهته می باشد. رویه های ارسال ATM به صورت اتوماتیک یک اتصال دوجهته بین دو میزبان ATM تنظیم خواهد کرد ، جاییکه هر جهت اتصال می تواند با پارامترهای ترافیکی مختلف و QoS در ارتباط باشد. CR-LSP دو جهته بین LSR های ۱ و ۲ تنها می تواند با نصب یک CR-LSP از LSR1 به LSR2 و یک CR-LSP مجزا از LSR2 به LSR1 ایجاد شود.

در حالت LSP، یک CR-LSP دارای یک LSR ورودی و یک LSR خروجی می باشد. CR-LSP ها می توانند به روش های مختلفی مورد استفاده قرار گیرند. به عنوان مثال، می توانند در یک شبکه ی IP برای توازن بار مورد استفاده قرار گیرند. ترافیک موجود بین لینک هایش می تواند با استفاده از فشردن برخی از ترافیک بر روی CR-LSP ها توزیع شود که از طریق لینک هایی که کمتر به کاربرده می شوند عبور می کنند. CR-LSP ها همچنین می توانند برای ایجاد تونل ها در MPLS و معرفی مسیرها بر اساس یک ضابطه ی QoS مانند کمینه سازی کل تاخیر end-to-end و بیشینه سازی توان عملیاتی مورد استفاده قرار گیرند.



شکل ۲.۱۵ .نمونه ای از CR-LSP

به عنوان مثال، شبکه ی MPLS موجود در شکل ۲.۱۵ را درنظر بگیرید و فرض کنید که مسیر بین LSR A ورودی و LSR G خروجی که با استفاده از OSPF محاسبه می شود، از E و F عبور می کند. با استفاده از CR-LDP می توانیم یک CR-LSP نصب کنیم که شرایط QoS را ارضا میکند. مانند کمینه سازی تاخیر end-to-end . به عنوان مثال، اگر LSR های B,C,D زیاد به کاربرده نمی شوند ، مسیریابی CR-LSP از طریق این LSRها تاخیر end-to-end را کاهش خواهد داد ، حتی در صورتیکه تعداد hop ها بیشتر از مسیر E به F باشد.

این ویژگی های برخی از ویژگی های CR-LDP می باشند :

- CR-LDP مبتنی بر LDP می باشد و بر روی TCP برای قابلیت اطمینان اجرا می شود.
- ماشین حالتِ CR-LDP نیاز به نوسازی پریودیک (دوره ای) ندارد.

- CR-LDP مسیرهای صریح سختگیر و آسانگیر[1] را اجازه می دهد. این به LSR ورودی ، تا حدی امکان داشتن اطلاعات ناقص در مورد توپولوژی شبکه را اجازه می دهد . (رجوع شود به بخش ۶.۲.۳) . LSR مبدا ممکن است همچنین پین کردن مسیر، route pinning را درخواست کند، که مسیر را از طریق یک مسیر آسانگیر ثابت می سازد ، بنابراین تا زمانیکه hop بهتری دردسترس نباشد ، تغییر نمی یابد.
- CR-LDP پیشدستی مسیر را با تخصیص اولویت های نصب/ نگهداری به CR-LSP ها اجازه می دهد. اگر یک مسیر برای یک CR-LSP با اولویت بالا یافت نشود، دراینصورت CR-LSP های با اولویتِ پایین ترِ موجود می توانند برای ایجاد CR-LSP با اولویت بالاتر مجددا مسیریابی شود.
- اپراتور شبکه می تواند منابع شبکه را به روش های مختلفی طبقه بندی کند. CR-LDP تخصیص کلاسهای منابع را که هنگام ایجاد یک CR-LSP می تواند استفاده شود را اجازه می دهد.
- مانند ATM، CR-LDP مشخص کردن پارامترهای ترافیکی روی یک CR-LSP و نحوه ی سیاستگذاری این پارامترها را اجازه می دهد.

CR-LDP به حداقل عملکردهای LDP زیر وابسته است:

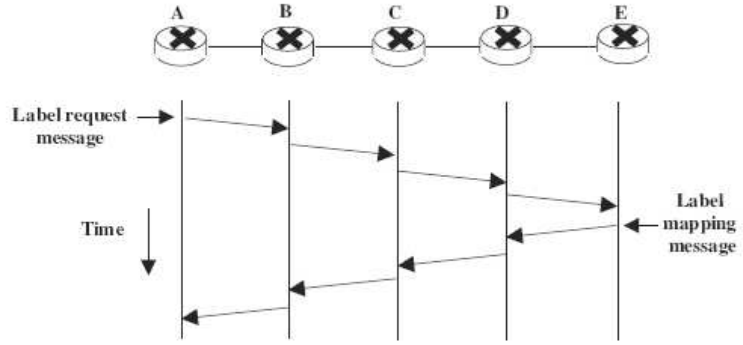
- مکانیزم کشفِ پایه و/ یا، توسعه یافته
- پیام درخواست برچسب برای درخواست پائین دستی به همراه کنترل سفارش شده
- پیام نگاشت برچسب برای درخواست پائین دستی به همراه کنترل سفارش شده
- پیام های اعلان
- پیام های بازیابی و آزادسازی برچسب
- تشخیص حلقه برای بخش هایی که به صورت آسانگیر مسیریابی شده اند.

رویه ی نصب CR-LSP:

CR-LSP با درخواست تخصیص به همراه کنترل سفارش شده نصب می شود. این نکته را به یادآورید که هر LSR یک برچسب ورودی را به یک FEC متصل می سازد و یک ورودی مناسبی در LFIB اش ایجاد می کند. با این حال، نگاشت برچسبش را به همسایه هایش به صورت "طرح تخصیص دریافت شده بدون درخواست" اعلان نمی کند. در عوض، یک LSR بالادستی، با صدور یک درخواست، نگاشت برچسب را به دست می آورد. در طرح کنترل سفارش شده ، تخصیص برچسب ها به عقبگردهایی از LSR خروجی در نزدیکی LSR ورودی می پردازد. مخصوصا، LSR تنها یک برچسب به FEC مقید میکند که یا LSR خروجی برای آن FEC باشد یا در یک انقیاد برچسب برای آن FEC از LSR بعدی اش دریافت کند. مثالی از نحوه ی نصب CR-LSP در شکل ۷.۱۰ نشان داده شده است. فرض کنید که LSR A برای ایجاد یک CR-LSP به LSR E درخواست داده باشد. درخواست برای نصب یک CR-LSP به LSR E ممکن است از یک سیستم

[1] Strict explicit routing & loosly explicit routing

مدیریتی یا یک کاربرد ناشی شود . LSR A مسیر صریح را با استفاده از اطلاعات تهیه شده توسط سیستم مدیریتی یا کاربرد یا از یک جدول مسیریابی محاسبه می کند و پیام درخواست برچسب را ایجاد می کند. مسیر صریح در این حالت با مجموعه ای از LSR های B,C,D درنظر گرفته می شود که در یک TLV خاص موجود در پیام درخواست برچسب حمل می شود که TLV مسیر صریح (ER-TLV) نامیده می شود.



شکل ۲.۱۶ .نمونه ای از ایجاد CR-LSP

LSR ورودی A پیام درخواست برچسب را به LSR B ارسال می کند، و این همان اولین LSRای است که در ER-TLV مشخص شده، که یک نگاشت برچسب برای FECمرتبط با CR-LSP درخواست می کند. به علت طرح کنترل سفارش شده ، LSR B نمی تواند نگاشت برچسبی برای FEC ایجاد کند تازمانیکه یک نگاشت برچسب از hop بعدی LSR C دریافت کند. همچنین به علت طرح تخصیص دریافت مبتنی بر درخواستِ پائین دستی ، LSR C نگاشت های برچسبش را به همسایه هایش اعلان نمی کند. از این نظر ، LSR B پیام درخواست برچسب را به LSR C برای درخواستِ یک نگاشت برچسب برای آن FEC ارسال می کند. LSR C درخواست نگاشت برچسب را به LSR D به همان دلیل ها ارسال می کند که نهایتا پیام درخواست برچسب به LSR خروجی E می رسد. LSR خروجی E اکنون می تواند یک نگاشت برچسب برای FEC ایجاد کند. و به پیام درخواست برچسب LSR D به همراه یک پیام نگاشت برچسب که شامل برچسب تخصیص داده شده می باشد پاسخ می دهد. زمانیکه LSR D پیام نگاشت برچسب را از LSR E دریافت می کند به پیام درخواست برچسب LSR C به همراه یک پیام نگاشت برچسب که شامل برچسب ورودی اش می باشد پاسخ می دهد، تا زمانیکه LSR A یک پیام نگاشت برچسب از LSR B دریافت کند. در همین زمان ، CR-LSP نصب می شود. در مرحله ی بعد پیام درخواست برچسب و پیام نگاشت برچسب شرح داده می شوند.

پیام درخواست برچسب[1]

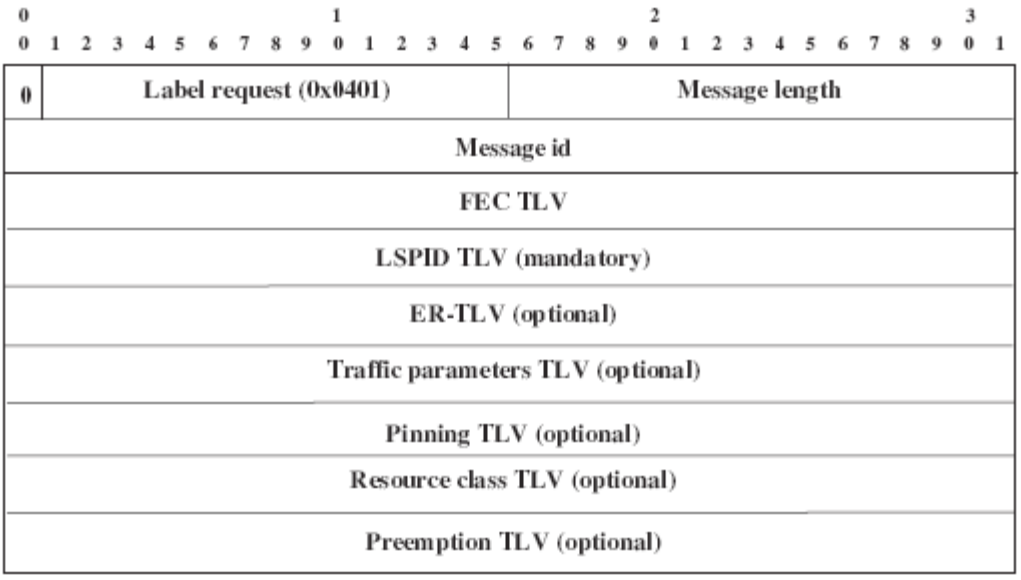
پیام درخواست برچسب در شکل ۲.۱۷ نشان داده شده است. بیت U به صفر تنظیم شده و نوع پیام به "درخواست برچسب" (0x0401) تنظیم گردیده است. FEC TLV باید در پیام درخواست برچسب قرار گیرد و

[1] Label Request Message

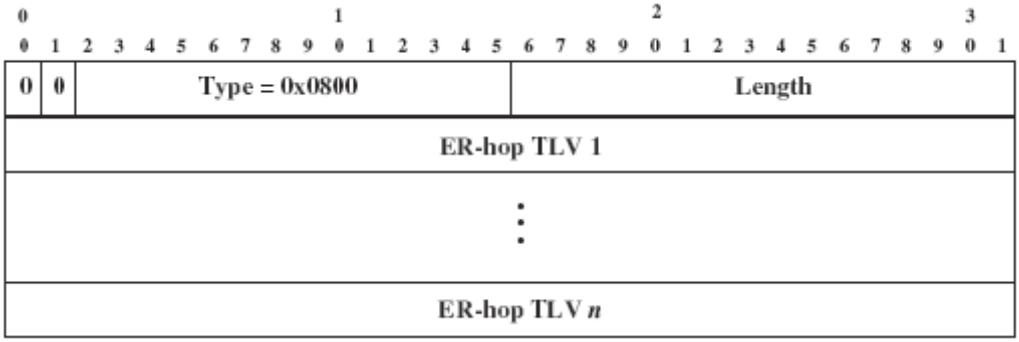
شامل یک عنصر FEC جدید با نام CR-LSP می باشد. LSPID TLV مورد نیاز می باشد و برای نشان دادن یک تعیین کننده ی یگانه برای CR-LSP مورد استفاده قرار می گیرد. که از id مسیریاب LSR ورودی و یک CR-LSP id تشکیل می یابد که به صورت محلی برای آن LSR یگانه می باشد.

LSPID در مدیریت شبکه ، در تعمیر CR-LSP و در استفاده از CR-LSP ایجاد شده به عنوان یک hop در یک ER-TLV قابل استفاده می باشد. مسیر صریح TLV یا (ER-TLV) نشان داده شده در شکل ۲.۱۸ برای تعیین مسیر برای ایجاد LSP مورد استفاده قرار می گیرد که از یک یا چند explicite route hop TLVs یا (ER-hop TLV) تشکیل می یابد که دارای فرمتی می باشد که در شکل ۲.۱۹ نشان داده شده است. فیلد نوع ، نوع محتویات ER-hop را مشخص می کند و می تواند یکی از مقادیر زیر را بگیرد : پیشوند IPv4 ، پیشوند IPv6 ، شماره سیستم خودکار ، LSPID . اگر یک LSR یک پیام درخواست برچسب دربرگیرنده ی یک ER-hop TLV را دریافت کند که پشتیبانی نمی کند ، LSR پیام برچسب را به LSR پائین دستی بعدی نخواهد کشاند، و یک پیام اعلان "مسیری وجود ندارد" یا no route notification message را ارسال خواهد کرد. بیت L برای تشخیص اینکه ER-hop سختگیر یا آسانگیر می باشد مورد استفاده قرار می گیرد(رجوع شود به بخش explicite routing). فیلد محتویات شامل یک گره یا یک گره انتزاعی نمایش دهنده ی گروهی از گره ها می باشد.

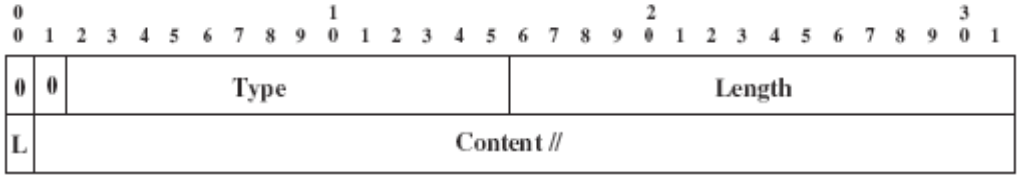
پین کردن مسیر یا route pinning برای بخشهائی از یک CR-LSP که به شکل آسانگیر مسیردهی شده اند به کار میرود که با استفاده از route pining TLV سیگنالدهی می شود . کلاس های منابعی که می تواند برای برپاسازی یک CR-LSP مورد استفاده قرار گیرد در resource class TLV مشخص میگردند.



شکل۲.۱۷ .پیام درخواست برچسب CR-LDP



شکل۲.۱۸ .ER-TLV



شکل۲.۱۹.ER-hop TLV

Preemption TLV برای تخصیص یک اولویت نصب و اولویت نگهداری CR-LSP مورد استفاده قرار می گیرد. این اولویت ها برای تعیین اینکه آیا CR-LSP جدید می تواند بر CR-LSP موجود مقدم باشد مورد استفاده قرار می گیرد. تخصیص یک اولویت بالاتر نگهداری به این مفهوم است که CR-LSP یکبار که نصب می شود ، دارای شانس پایینتری از مقدم بودن می باشد. تخصیص یک اولویت بالای نصب به این مفهوم است که درحالتی که منابع دردسترس نمی باشند، CR-LSP دارای شانس بالایی از اولویت دهی در مقابل CR-LSP های موجود می باشد.

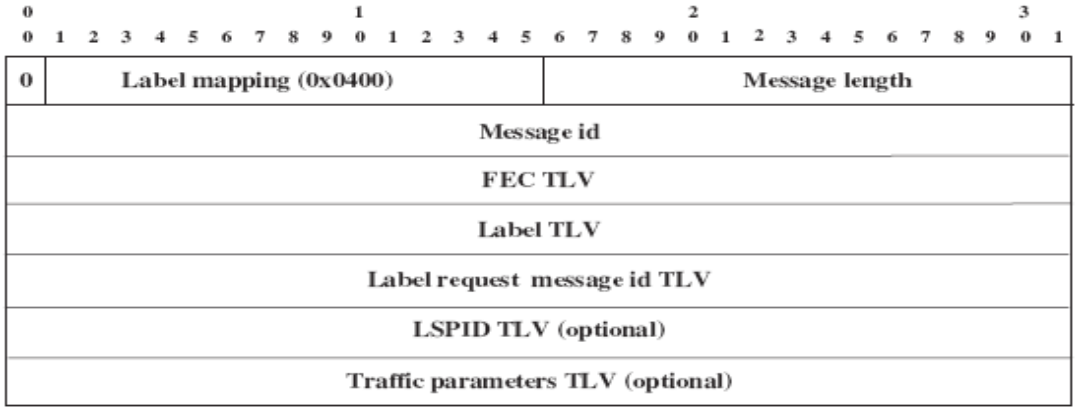
پارامترهای ترافیک TLV برای سیگنالدهی مقدارهای پارامترهای ترافیکی که CR-LSP را تشخیص می دهد مورد استفاده قرار می گیرد. این TLV به طور اجمالی در بخشهای بعد مورد بررسی قرار خواهد گرفت.

پیام نگاشت برچسب :

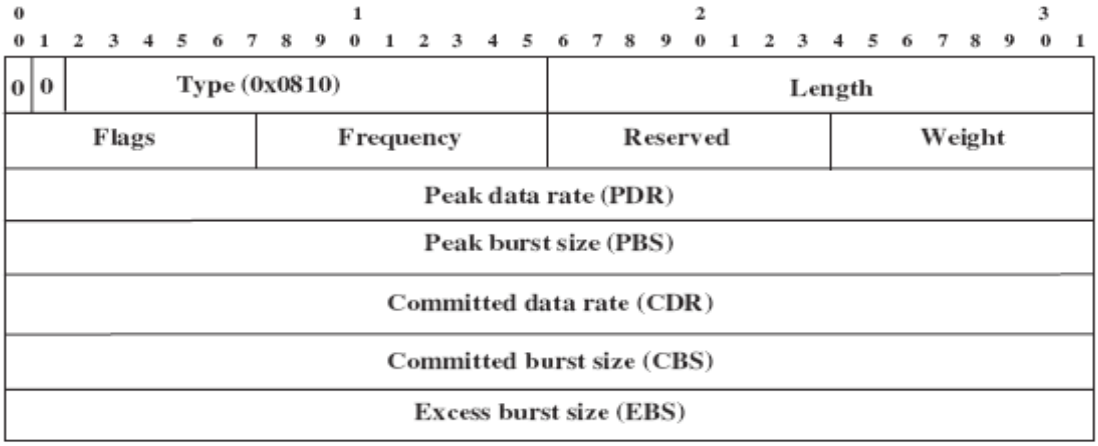
پیام نگاشت برچسب در شکل ۲.۲۰ نشان داده شده است. بیت U به صفر تنظیم شده و نوع پیام به نگاشت برچسب (0x0400) تنظیم گردیده است. FEC و LSPID TLV ها مشابه پیام درخواست برچسب CR-LDP می باشند . برچسب TLV مشابه برچسب موجود در LDP می باشد (رجوع شود به شکل ۲.۱۴) . پیام درخواست برچسب id TLV به صورت زیر مورد استفاده قرار می گیرد. اگر این پیام نگاشت برچسب پاسخی برای یک پیام درخواست برچسب باشد، بنابراین باید پارامتر id پیام درخواست برچسب را دربرگیرد. این پارامتر در id TLV پیام درخواست برچسب حمل می شود پارامترهای ترافیک TLV در بخش بعدی توضیح داده می شوند.

پارامترهای ترافیک TLV:

پارامترهای ترافیک TLV در پیام های درخواست برچسب و نگاشت برچسب مورد استفاده قرار می گیرند. برای توصیف پارامترهای ترافیک CR-LSP ای که ایجاد شده است، مورد استفاده قرار می گیرد. پارامترهای ترافیک TLV در شکل ۲.۲۱ نشان داده شده است. نوع پارامترهای ترافیک TLV ، 0x0810 می باشد و طول فیلد مقدار ۲۴ بایت می باشد. موارد زیر تعریف شده اند :



شکل ۲.۲۰ .پیام ترسیم برچسب



شکل ۲.۲۱ .پارامترهای ترافیک TLV

پرچم ها ، فرکانس ، وزن ، نرخ داده ی پیک[۱] (PDR) ، ماکزیمم سایز داده های پشت سرهم[۲] (PBS) ، نرخ داده ی تعهد شده[۳] (CDR) ، سایز داده های پشت سرهم تعهد شده[۴] (CBS) و سایز انتقال داده های پشت

[۱] Peak Data Rate
[۲] Peak Burst Size
[۳] Committed Data Rate
[۴] Committed Burst Size

سرهم (قطاری) اضافی[1] (EBS) . پارامترهای PDR و PBS برای تعیین ترافیک ارسال شده به CR-LSP مورد استفاده قرار می گیرند. پارامترهای CDR,CBS,EBS برای تعیین اینکه شبکه چگونه ترافیک ثبت شده در CR-LSP را کنترل خواهد کرد مورد استفاده قرار می گیرند. درنهایت، فیلد های پرچم ها ، فرکانس و وزن برای فراهم سازی اطلاعات اضافی مورد استفاده قرار می گیرند.

- ✓ نرخ داده ی پیک (PDR) و و سایز انتقال بدون تاخیر داده های پیک (PBS) :

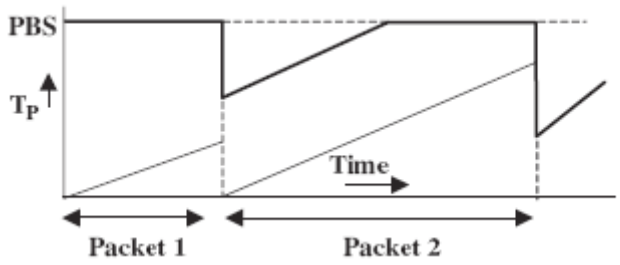
نرخ پیک ، ماکزیمم نرخی می باشد که در آن ترافیک به CR-LSP ارسال می شود و به صورت byte/s نشان داده می شود. پارامتر معادل آن در ATM نرخ پیک سلول (PCR) می باشد . برخلاف PCR ، که توسط یک مقدار مجزا تعیین می شود ، نرخ پیک در CR-LDP برحسب ظرف نشانهٔ P یا token bucket P تعیین می شود. ماکزیمم سایز P برابر با PBS در نظر گرفته می شود که به صورت byte/s نشان داده می شود. PBS ماکزیمم سایزِ پاکتهای ارسالی را مشخص می سازد که می توان به یک CR-LSP ارسال شود و PDR ماکزیمم نرخی را که در آن ترافیک توسط کاربر انتقال می یابد، برمی گرداند. نرخ پیک، خروجی ای از مشخصه ی P می باشد که به CR-LSP ارسال شده است.

مشخصه ی P به صورت زیر اجرا می شود:

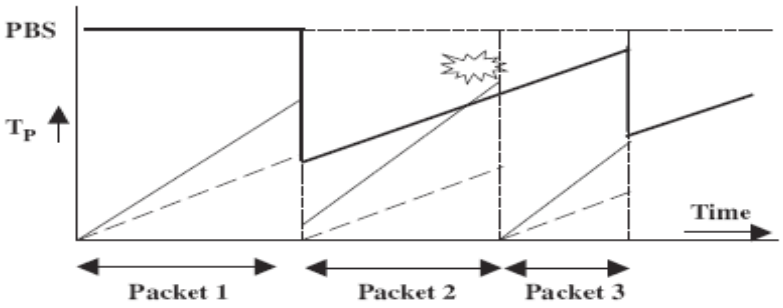
- در ابتدا، تعداد نشانه ها (یعنی تعداد نشانه ها در ظرف یا سطل نشانه، token bucket) برابر Tp=PBS می باشد.
- byte/s PDR=N را در نظر بگیرید، سپس اگر $Tp \leq PBS$ باشد، شمارهٔ نشانه ها یعنی Tp، هر ثانیه به اندازهٔ N تا افزایش می یابد. (نباید بیشتر از PBS شود)
- زمانیکه بسته ای با سایز B بایت دریافت می شود، اگر $Tp\text{-}B \geq 0$ باشد، بسته بزرگتر از نرخ پیک نمی باشد و $Tp=Tp-B$ می باشد.
- درغیر اینصورت، بزرگتر از نرخ پیک می باشد و Tp کاهش نمی یابد. بسته یک بستهٔ مختل کننده می باشد و می تواند برچسب گذاری یا حذف شود.

توجه کنید که یک مقدار مثبت بینهایت از PBS یا MBS به معنی این است که بسته های دریافتی هرگز بزرگتر از نرخ پیک نمی باشند.

[1] Excess Burst Size



شکل۲.۲۲ .نمونه ای از عملکرد



شکل ۲.۲۳ . نسبت انتقال که از PDRعبور می کند.

مثالی از عملیات ظرف نشانهٔ نرخ پیک در شکل ۲.۲۲ نشان داده شده است. خط ضخیم در بالا مقدار Tp را نشان می دهد و خط باریک در قسمت زیرین زمان ورود یک باکت را مشخص می سازد. شیب تمام خطوط برابر با PDR می باشد. در زمان t=0 ، ظرف نشانه ، PBS تا نشانه را دربرمی گیرد . بسته ی ۱ در نرخ PDR byte/s شروع به دریافت شدن می کند. زمانیکه به صورت کامل دریافت شد، سایز بسته نشان داده شده به صورت بایت از مقدار نشانه ی فعلی کم می شود و آن پاکت به قسمتهای بعدی میرود و دوباره پر کردن باکت نشانه در نرخ byte/s PDR شروع می شود. بسته ی ۲ شروع به رسیدن بلافاصله بعد از بسته ی ۱ می کند. تا زمانیکه سایز بسته ی ۲ کمتر از تعداد نشانه فعلی باشد، می تواند عبور کند. درکل، تمام بسته ها عبور داده خواهند شد به شرطیکه کاربر در نرخی کمتر یا برابر PDR ارسال کند.

حالتی را در نظر بگیرید که در آن نرخ انتقال کاربر به صورت موقت از PDR بیشتر میشود(رجوع شود به شکل ۲.۲۳). خطوط خط چین نرخ انتقال یک بسته را در حالتیکه منبع در نرخ PDR داده را میفرستد، مشخص میکند. خطوط پیوسته ی باریک بالای خط چین نرخ انتقال بسته فرستاده شده را مشخص می سازد و خط ضخیم در بالای دیاگرام تعداد نشانهٔ فعلی را نشان می دهد. توجه کنید که بسته ی ۱ ، گرچه سریعتر از آنچه که باید باشد دریافت می شود، مرور می شود. تعداد نشانه به طور مناسبی کاهش می یابد و دوباره پرکردن باکت نشانه در نرخ PDR شروع می شود. بسته ی ۲ خوش شانس نمی باشد و یا برچسب گذاری خواهد شد یا با در نظر گرفتن در یک شبکه حذف خواهد شد. بسته ی ۳ مرور می شود.

بنابراین، اگر نرخ انتقال به صورت موقت متجاوز از PDR گردد، امکان پذیر است که برخی از بسته ها مانند آنچه در طرح GCRA در ATM هست، مرور (پردازش و عبور) گردند . از طرف دیگر، اگر کاربر بخواهد بسته

ای را با سایز بزرگتر از MBS ارسال کند، این بسته فورا به صورت بستهٔ مختل کننده طبقه بندی خواهد شد به خاطر اینکه باکت نشانه هرگز بیشتر از عدد PBS را دربرنخواهد گرفت.

- ✓ نرخ داده ی تعهد شده (CDR) ، سایز داده های پشت سرهم تعهد شده (CBS) و سایز انتقال داده های پشت سرهم (قطاری) اضافی (EBS)

ترافیکی که به شبکه ارسال می شود، که خروجی باکت (سطل) نشانهٔ P می باشد، با استفاده از باکت نشانهٔ C کنترل می شود ، که باکت نشانهٔ تعهد شده نامیده می شود. ماکزیمم سایز باکت نشانهٔ C برابر با (CBS) تنظیم می شود که به صورت بایت نشان داده می شود و ظرف نشانه با نرخ (CDR) مجددا پر می شود، که به صورت byte/s نشان داده می شود. خروجی این باکت نشانه، نرخ تعهد شده نامیده می شود که مقدار پهنای باند شبکه است که باید برای CR-LSP تخصیص داده شود.

علاوه بر C ، استفاده از یک باکت نشانه کنترل کننده ی ثانویه، E، امکان پذیر می باشد که باکت نشانهٔ فراوانی نامیده می شود. ماکزیمم سایز این باکت نشانه برابر با (EBS) می باشد که به صورت بایت نشان داده می شود و باکت نشانه با نرخ (CDR) که به صورت بایت بر ثانیه نشان داده می شود، مجددا پر می گردد. همانطور که در سطور پائین خواهیم دید، این باکت نشانه می تواند برای تصمیم گیری در مورد اینکه آیا یک پاکت مختل باید برچسب گذاری شده و در شبکه قرار گیرد یا باید حذف شود ، مورد استفاده قرار می گیرد.

عملیات باکت های نشانه اضافی و تعهد شده به صورت زیر می باشد :

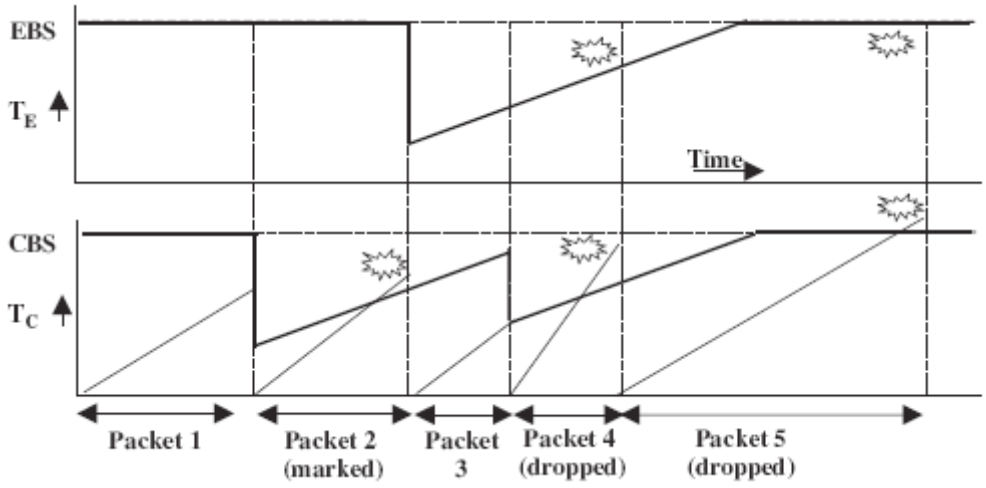
- ابتدا، تعداد نشانه در ظرف نشانهٔ تعهد شده به مقدار Tc=CBS، و تعداد نشانه در ظرف نشانهٔ افزونی به صورت TE=EBS مقداردهی میشود.
- سپس، Tc و Te هر ثانیه به صورت زیر آپدیت می شوند :
  - o اگر Tc< CBS باشد در اینصورت Tc با M بایت افزایش می یابد(نباید بیشتر از CBS باشد).
  - o اگر TE<EBS باشد در اینصورت TE با Mبایت افزایش می یابد. (نباید بیشتر از EBS باشد) جائیکه CDR=M byte/s
- گزینه های بعدی زمانی مورد استفاده قرار می گیرند که یک باکت با سایز B برسد :
  - o اگر Tc-B ≥ 0 باشد در اینصورت نشانه های کافی در باکت نشانهٔ تعهد شده برای بسته وجود دارد و Tc=Tc-B می باشد.
  - o اگر Tc-B < 0 و TE-B≥0 باشد در اینصورت نشانهٔ کافی در باکت نشانهٔ تعهد شده وجود ندارد ولی نشانهٔ کافی در باکت نشانهٔ افزونی وجود دارد و TE=TE-B می باشد.

- اگر Tc-B < 0 و TE-B < 0 باشد در اینصورت نشانهٔ کافی در باکت نشانهٔ تعهد شده یا در باکت نشانهٔ افزونی وجود ندارد و Tc و TE کاهش نمی یابند.

توجه کنید که اکر CDR یک مقدار بینهایت مثبت باشد، در اینصورت یک بسته ی دریافتی هرگز متجاوز از مقدارهای سطل نشانه نخواهد بود.

گزینه ی انتخابی هنگامیکه سایز بسته بیشتر از تعداد نشانهٔ مشخص شده در باکت نشانه باشد ، (چه تعهد شده و چه افزونی) وابسته به پیاده سازی می باشد. به عنوان مثال، اگر سایز بسته، بزرگتر از شمارهٔ نشانه در باکت نشانهٔ تعهد شده باشد اما کمتر از شمارهٔ نشانه در باکت نشانهٔ افزونی باشد، ممکن است که آنرا مارک کرده و به آن اجازه دهیم که به شبکه وارد شود، اگر سایز پاکت از هردو عدد بالاتر بود، آنگاه ممکن است پاکت اصطلاحا انداخته شود (کاری روی آن صورت نگیرد). مثالی از نحوه ی استفاده ی این دو طرح کنترل کننده در شکل ۲.۲۴ نشان داده شده است. بالاترین نمودار به باکت نشانهٔ افزونی اشاره می کند و پایین ترین به باکت نشانهٔ تعهد شده اشاره می کند .

قوانین بیان شده در پاراگراف بالا برای ایجاد و حذف به کار برده می شود. همه ی چهار بسته در نرخ هایی بزرگتر از CDR دریافت می شوند . همانطور که می توان مشاهده کرد ، بسته های ۱ و ۳ مرور می شوند . بسته ی ۲ هنگامیکه باکت نشانهٔ تعهد شده ، نشانهٔ کافی نداشته باشد ، وارد می شود ولی نشانه های کافی در باکت نشانهٔ افزونی وجود دارد. در نتیجه ، مقدار نشانهٔ Tc بدون تغییر باقی می ماند ، مقدار نشانهٔ TE با توجه به سایز بسته ی ۲ کاهش می یابد. و بسته ی ۲ برچسب گذاری شده و در شبکه قرار می گیرد. زمانیکه هیچکدام از باکت های نشانه تعهد شده و افزونی ، نشانهٔ کافی نداشته باشند بسته های ۴ و ۵ حذف می شوند و در هر دو مورد مقادیر نشانهٔ Tc,TE تغییر نمی یابند.



شکل ۲.۲۴ .نمونه ای از رویه دو طرح

پنج پارامتر ترافیک – PDR,PBS,CDR,CBS,EBS – می توانند به مقادیر مختلفی تنظیم شوند ، بنابراین برای ایجاد کلاس های مختلفی از سرویس مانند یک سرویس حساس به تاخیر و یک سرویس با بهترین

فعالیت استفاده می شود. همچنین می توانند برای فراهم سازی دسته های مختلف سرویس ATM تنظیم شوند. مثالی از نحوه ی تنظیم این ۵ پارامتر ،برای فراهم سازی کلاس های مختلفی از سرویس ها می باشد که در بخش بعد بیان می شوند.

همانطور که در بالا اشاره شد، خروجی باکت نشانهٔ تعهد شده ، ترافیکی می باشد که وارد شبکه خواهد شد. الگوریتم تخصیص پهنای باند می تواند در هر LSR برای تصمیم گیری در مورد اینکه آیا CR-LSP جدید پذیرش خواهد شد یا نه ، مورد استفاده قرار گیرد. همانند ATM، طرح های مختلفی می توانند برای محاسبه ی میزان پهنای باندی که باید به CR-LSP تخصیص می یابد مورد استفاده قرار گیرند. ساده ترین طرح ، تخصیص پهنای باندی برابر با CDR می باشد. که برابر با طرح تخصیص نرخ پیک در ATM می باشد.

- ✓ فیلد های پرچم ها، فرکانس و وزن :

پارامترهای ترافیک TLV می توانند در پیام نگاشت برچسب قرار گیرند. که به LSR اجازه می دهد مقدار پیشنهادی را با یک مقدار کمتر برای یک یا چند پارامتر ترافیک جایگزین کند. فیلد پرچم ها مشخص می کند که کدامیک از پارامترهای ترافیک قابل اغماض می باشند. یعنی ، می توانند با یک مقدار کمتر جایگزین شوند. که از یک زیرفیلد رزرو شده ی ۲ بیتی و ۶ پرچم ۱ بیتی تشکیل می یابد. ۵ تا از این پرچم ها با ۵ پارامتر ترافیک در ارتباط می باشند و ششمین پرچم به فیلد وزن مربوط می شود. به طور ویژه، پرچم F1 به PDR ، پرچم F2 به PBS ، پرچم F3 به CDR ، پرچم F4 به CBS و پرچم F6 به فیلد وزن مربوط می شوند. هر پرچم نشان می دهد که آیا پارامتر ترافیک مربوطه اش کم اهمیت می باشد یا نه . پرچم F6 نشان می دهد که آیا وزن قابل اغماض می باشد یا نه . اگر پرچمی به صفر تنظیم شود در اینصورت پارامتر ترافیک مربوطه اش در مدیریت ترافیک شبکه قابل اغماض نمی باشد. در غیر اینصورت قابل اغماض می باشد.

همانطور که در بالا اشاره شد، CDR می تواند برای تخصیص پهنای باند به یک CR-LSP استفاده شود. پهنای باند تخصیص یافتهٔ دقیق می تواند هر بار متفاوت باشد ولی پهنای باند میانگین محاسبه شده در طول این مدت باید حداقل برابر با CDR باشد. فیلد فرکانس ۸ بیتی برای تعیین این دوره استفاده می شود. کدهای فرکانس زیر تعریف شده اند :

- مشخص نشده (مقدار ۰)
- تکرار شونده (مقدار ۱) : یعنی نرخ قابل دستیابی باید میانه باشد، حداقل برابر CDR هنگامی که با استفاده از دوره های زمانی که برابر یا طولانی تر از تعداد کمی از کوتاهترین پاکتهای ارسالی در نرخ CDR هستند.
- خیلی تکرارشونده (مقدار ۲) : یعنی ، نرخ قابل دستیابی باید حداقل برابر با CDR باشد زمانیکه در هر بازه ی زمانی مساوی یا طولانی تر از تعداد کوچکی از کوتاهترین مدت های ارسال بسته در CDR اندازه گیری می شود.

- رزرو شده (مقادیر ۳ تا ۲۵۵) :

در نهایت فیلد ۸ بیتی وزن برای تشخیص سهم نسبی CR-LSP از پهنای باند افزونی استفاده می شود. دامنه ی تغییرات مقادیر وزن از ۱ تا ۲۵۵ می باشد. مقدار ۰ به این معنی است که وزن قابل استفاده نمی باشد.

کلاس های سرویس:

کلاسهای سرویس می توانند با دستکاری مناسب پارامترهای ترافیک و قوانین مربوط به عبور ، برچسب گذاری و حذف یک بسته ایجاد شوند. در جدول ۲.۳ ، پارامترهای ترافیک داده شده است و قوانین برای برچسب گذاری و حذف بسته ها برای سه گروه از سرویس به صورت زیر می باشند: سرویس حساس به تاخیر[۱] (DS)، سرویس حساس به بازدهی[۲] (TS) ، و سرویس بهترین کوشش[۳] (BE) . در سرویس حساس به تاخیر ، شبکه با احتمال بالایی به تحویل بسته ها در نرخ PDR با حداقل تاخیر تعهد شده می پردازد. بسته های با افزونی بیشتر از PDR حذف خواهند شد. در سرویس حساس به بازده ، شبکه ارسال پاکتها را با نرخ حداقل CDR و با احتمال بالا تعهد میکند.

جدول ۲.۳. پارامتر های ترافیک،کلا سهای سرویسDS, TS, BE

Traffic Parameters	Delay sensitive	Throughput sensitive	Best effort
PDR	User-specific	User-specific	Infinite
PBS	User-specific	User-specific	Infinite
CDR	PDR	User-specific	Infinite
CBS	PBS	User-specific	Infinite
EBS	0	0	0
Frequency	Frequent	Unspecified	Unspecified
Dropping action	Drop > PDR	Drop > PDR, BPS, Mark > CDR, CBS	None

[۱] Delay Sensitive Service

[۲] Throughput Sensitive Service

[۳] Best effort Service

جدول ۲.۴. پارامتر های ترافیک،دسته سرویسATM

Traffic parameters	CBR	RT-VBR	NRT-VBR	UBR
PDR	PCR	PCR	PCR	PCR
PBS	CDVT	CDVT	CDVT	CDVT
CDR	PCR	SCR	SCR	–
CBS	CDVT	MBS	MBS	–
EBS	0	0	0	0
Frequency	VeryFrequent	Frequent	Unspecified	Unspecified
Dropping action	Drop > PCR	Drop > PCR, Mark > SCR, MBS	Drop > PCR	Drop > PCR

کاربر می تواند در نرخی بزرگتر از CDR پاکتها را منتقل کند ولی بسته ها دارای افزونی بر CDR دارای احتمال کمتری برای ارسال شدن می باشند . در سرویس بهترین فعالیت هیچ ضمانت سرویسی وجود ندارد.

در جدول ۲.۴ پارامترهای ترافیک داده شده و قوانین برای برچسب گذاری و حذف بسته ها برای دسته های سرویس ATM به صورت زیر می باشند: نرخ بیت ثابت (CBR) ، نرخ بیت متغیر بلادرنگ (RT-VBR) ، نرخ بیت متغیر غیر بلادرنگ (NRT-VBR) و نرخ بیت مشخص نشده (UBR) .

پروتکل رزرو کردن منبع (RSVP)

پروتکل جایگزین برای LDP و CR-LDP، پروتکل رزرواسیون منبع – مهندسی ترافیک یا RSVP-TE می باشد. RSVP-TE پروتکلی الحاقی بر پروتکل رزرو منبع RSVP می باشد که برای پشتیبانی معماری سرویس های مجتمع یا intserv طراحی شده است. برای درک RSVP-TE ، ابتدا باید نحوه های کارهای RSVP را درک کنیم. از این نظر، در این بخش، ویژگی های عمده ی RSVP و در بخش بعدی RSVP-TE را مورد بحث بررسی قرار می دهیم.

معماری سرویس مجتمع در اواسط دهه ی ۱۹۹۰ توسط IETF با دیدگاه معرفی QoS در شبکه ی IP توسعه یافته است. دو دسته ی سرویس زیر در intserv تعریف شده اند :

۱. سرویس ضمانت شده : این سرویس یک حاشیهٔ ثابت بر روی تأخیر صفهای end-to-end بدون از دست دادن حتی یک پاکت برای تمامی پاکتهای نامنطبق فراهم میکند.
۲. سرویس بار کنترل شده : این سرویس یک QoS که تقریب نزدیکی از QoS سرویس بهترین تلاش یا best effort service است و کاربر ممکن است آنرا از یک شبکهٔ بی بار دریافت کند را برای کاربر فراهم میکند. مخصوصا کاربرممکن است این موارد را در نظر بگیرد:

(a) درصد خیلی بالایی از بسته های ارسال شده توسط شبکه به گیرنده با موفقیت تحویل داده خواهد شد. درصد بسته هایی که با موفقیت تحویل گرفته نشده اند باید به طور نزدیکی، نرخ اصلی خطای پاکتِ لینکهای انتقال را تقریب بزند.
(b) تاخیر end-to-end تجربه شده توسط درصد خیلی بالایی از بسته های ارسال شده به طور فاحشی متجاوز از حداقل تاخیر end-to-end تجربه شده توسط هر بستهٔ ارسال شده بطور موفقیت آمیز، نخواهد بود.

در intserv ، فرستنده مشخص می کند چه مقدار ترافیک را به گیرنده (ها) انتقال خواهد داد و گیرنده مشخص می کند که چه مقدار ترافیک می تواند دریافت کند و QoS مورد نیاز برحسب اتلاف بسته و تاخیر end-to-end نشان داده می شود. این اطلاعات هر مسیریاب IP را در طول مسیر دنبال شده توسط بسته های فرستنده را برای اجرای عملیات زیر مجاز می سازد :

۱. policing : برای تعیین اینکه ترافیک انتقال داده شده توسط فرستنده با Tspec فرستنده سازگاری دارد مورد استفاده قرار می گیرد، Tspec مجموعه ای از توصیف گرهای ترافیکی است که ترافیک منتقل شده توسط فرستنده را مشخص می سازد.
۲. کنترل پذیرش : برای تعیین اینکه آیا یک مسیریاب IP دارای منابع کافی برای بازبینی QoS درخواست شده می باشد یا نه مورد استفاده قرار می گیرد.
۳. طبقه بندی : برای تصمیم گیری در مورد اینکه کدام یک از بسته های IP باید به عنوان بخشی از ترافیک فرستنده درنظر گرفته شود مورد استفاه قرار می گیرد.
۴. صف بندی و زمان بندی : برای اینکه یک مسیریاب IP ، QoS های مختلفی برای گیرنده های مختلفی فراهم سازد، باید قادر به صف بندی بسته ها در صف های مختلف و انتقال بسته ها خارج از این صف ها با توجه به یک زمانبندی باشد.

معماریintserv به یک پروتکل سیگنالینگ برای برپاسازی و نگهداری قبل اطمینان از رزرواسیون منابع نیاز دارد. همانند MPLS ، intserv نیازی به استفاده از یک پروتکل سیگنالینگ خاص ندارد و می تواند تعداد زیادی از پروتکل های سیگنالینگی را که RSVP متداول ترین آنها می باشد را مطابقت دهد. RSVP برای پشتیبانی معماری intserv توسعه یافته است ، ولی می تواند انواع دیگری از اطلاعات کنترل را حمل کند. این به این دلیل است که RSVP از محتوای فیلدهای پروتکل RSVPی که شامل اطلاعات کنترل ترافیک و ضوابط استفاده شده توسط مسیریاب ها برای رزرو منابع است،

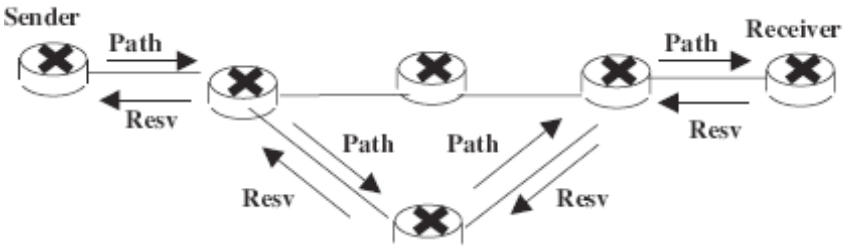
مطلع نمیباشد. RSVP می تواند برای ایجاد رزروهای منبع برای هر دو کاربردهای تک پراکنی و چند به چند چند-پراکنی مورد استفاده قرار گیرد.

RSVP با ایده ی پشتیبانی از کنفرانسهای چندگانه یعنی ارتباطات چند به چند به همراه گیرنده های ناهمگن طراحی شده بود. در RSVP ، رزرواسیون منابع توسط یک گیرنده تصمیم گیری و مقداردهی اولیه می شود ، زمانیکه فقط گیرنده واقعا می داند چه مقدار پهنای باند مورد نیاز می باشد. این رویه همچنین یک گیرنده را به اتصال یا ترک چند پراکنش، هر زمانی که بخواهد ، قادر می سازد.

یک مشکل در رویه ی مقداردهی اولیه ی گیرنده این است که گیرنده مسیرموجود از فرستنده به خودش را نمی شناسد. بنابراین قادر به تخصیص پهنای باند به هر روتر متصل به خود تا زمانی که آن روتر و مسیر آنرا نشناسد، نیست. این مسئله با استفاده از پیام Path (مسیر) حل می شود که از فرستنده شروع می شود و پس از طی یک مسیر واحد یا چندگانه به گیرنده میرسد. هدف عمده ی این پیام مسیر ، ذخیره ی اطلاعات وضعیت مسیر در هر گره در طول مسیر و حمل اطلاعات با توجه به ویژگی های ترافیک فرستنده و ویژگی های مسیر end-to-end می باشد. در زیر به برخی از اطلاعات شامل شده در پیام مسیر اشاره شده است :

- Phop : آدرس hop قبلی مسیر یاب سازگار با RSVP می باشد که پیام را ارسال می کند. این آدرس در اطلاعات وضعیت مسیر در هر گره ذخیره می شود و برای ارسال پیام رزرو در جهت بالادستی فرستنده استفاده می شود.
- Sender template : این فیلد ، آدرس IP فرستنده و اختیارا پورت UDP/TCP فرستنده را حمل می کند.
- sender TSpec : ویژگی های ترافیک جریان داده ای را که فرستنده تولید خواهد کرد، مشخص می سازد . فرمت TSpec فرستنده که برای معماری intserv مورد استفاده قرار می گیرد در ادامه توضیح داده خواهد شد.
- Adspec : اطلاعات One-Pass with advertising یا OPWA را حمل می کند. این اطلاعاتی است که در هر گره در طول مسیرِ دنبال شده توسط پیام مسیر، جمع آوری شده است. این اطلاعات به گیرنده ارسال می شوند، گیرنده ای که میتواند بعدا از آن برای ایجاد یک درخواست رزرو جدید یا اصلاح رزرو موجود استفاده کند.

در طول دریافت پیام مسیر یا Path message ، گیرنده یک پیام Resv به فرستنده در طول مسیر برگشتی ای که پیام مسیر، دنبال کرده است، ارسال می کند.(رجوع شود به شکل ۲.۲۵) . موارد زیر برخی از اطلاعات موجود در پیام Resv می باشند :



شکل ۲.۲۵ .نمونه ای از مسیر و پیام Resv

- Flowspec : QoS مورد نظر را مشخص می سازد. از TSpec و RSpec گیرنده و کلاس سرویس تشکیل می یابد. TSpec گیرنده مجموعه ای از توصیف گرهای ترافیک می باشد که در طول مسیرِ رزرو منابع، توسط گره ها مورد استفاده قرار می گیرد. RSpec پهنای باند مورد نظر و ضمانت های تاخیر را بیان می کند. هنگامی که RSVP در intserv بکار می رود طبقه خدمات هم قابلیت ارائه خدمت و هم کنترل بار را دارا می باشد. فرمت دریافت TSpecوRSpec که در ساختار intserv بکار می رود در زیر شرح داده شده است:
- Filter Spec : پاکتهائی را که QoS درخواست شده را طلب میکنند، تعریف میکند. خود QoS نیز در flowspec تعریف شده است.یک filter spec ساده میتواند فقط آدرس IP فرستنده باشد و پورتهای UDP و TCP آن نیز میتوانند شامل گردند.

هنگامی که یک مسیریاب پیام Resv را دریافت می کند، "منابع در هر دستور العملِ گیرنده" را رزرو میکند و سپس پیام Resv را به hop قبلی که از اطلا عات حالت مسیر بدست آمده را ارسال می کند. پیامهای RSVP در داده گرامهای IP خالص بدون کپسوله سازیهای TCP وUDP فرستاده میشوند.

RSVP با استفاده از مفهوم جریان اطلاعات و جلسه به وجود می آید. یک جلسه توسط عوامل زیر مشخص می شود.آدرس مقصد IP ، پروتکل تعیین هویت و تعداد پورت مقصد انتخابی . جریان اطلاعات در حقیقت بسته هایی هستند که توسط فرستنده در یک جلسهٔ خاص فرستاده می شوند.

RSVP بصورت ساده عمل رزرواسیون را برای جریان های اطلاعات به صورت تک جهته انجام می دهد. بنابراین به منظور اینکه دو کاربر A , B ارتباطی برقرار کنند در دو روش، دو جلسهٔ جدا باید ایجاد شودکه یکی از A تا B و دیگری از B تا A می باشد.

شیوه های رزرو کردن

سه شیوهٔ مختلف رزرواسیون می تواند با RSVP بکار رود وبه منظور درک این طرح فرض کنید تعدادی فرستنده عمل انتقال را بین خود انجام می دهند. هر فرستنده اطلاعات بسته خود را در یک جلسه انتقال می دهد که توسط آدرس گیرنده و پروتکل id مشخص می شود . یک انتخاب برای رزرواسیون در ارتباط با رزو کردن منبع این جلسات انجام می گیرد. حال فرض کنیم که چندین جریان اطلا عات از همان مسیریاب عبور

می کند. مسیریاب دارای انتخاب بین برقراری رزواسیون جداگانه برای هر جریان داده یا رزواسیون منفرد برای تمامی جریان داده ها می باشد.

انتخاب رزرواسیون دوم، گزینش فرستنده ها را کنترل میکند و میتواند صریح یا به شکل کاراکتر عام (explicit & wildcard) باشد. در گزینش فرستنده صریح، گیرندۀ یک لیست از فرستنده ها و اینکه متمایل به دریافت داده از کجا هستند را فراهم میکند.

بر اساس این دو انتخاب سه سبک مختلف تعریف شده است:

- Wild-Card Filter Style (WF):هر فرستنده می توان عمل انتقال را انجام دهد .در آنجا یک رزواسیون منبع منفرد برای تمامیی جریان داده ها از فرستنده های بالا دستی می باشد. رزرو منابع بزرگترین درخواست رزرواسیون می باشد
- Fixed Filter Style : رزرو جداگانه برای هر فرستنده ویژه که در لیست فرتنده ها مشخص شده است انجام می گیرد.فرستنده های دیگر که در در لیست صریح مشخص نشده اند همان جلسه را انتقال می دهند که در این رزواسیون تقسیم نشده است.
- Shared Explicit Style (SE): لیستی از فرستنده ها بصورت واضح و تقسیم منفرد رزرواسیون برای هریک جریان ها صورت می گیرد.

حالت Soft

RSVP از روش حالت Soft برای نگهداری حالت رزواسیون در مسیریابها و میزبان ها استفاده می کند.حالت اطلاعات در هر مسیریاب و میزبان باید در فواصل معین توسط پیام مسیر و پیام های Resv refresh شود. اگر پیامهای تازه کردن، refresh در دورۀ زمانی معینی موسوم به cleanup timout نرسند، حالت رزرواسیون پاک خواهد شد. این حالت همچنین بوسیلۀ یک پیام پاره سازی یا tear down به شکل صریح میتواند پاک شود.

وقتی مسیر تغییر میکند، پیام مسیر بعدی حالت مسیر را بر روی روترهائی که در مسیر جدید قرار دارند، مقداردهی خواهد کرد و پیام Resv یک رزرواسیون بر روی هر یک ازین روترها بنا میکند. حالت مسیر استفاده نشده به خاطر time out به پایان میرسد.

RSVP پیام خود را به شکل داده گرام IP بدون هیچ تضمینی مبنی بر تحویل آن ارسال می کند. ممکن است پیام RSVP به علت بروز خطا ها یا سرریز بافر به مقصد نرسد. چک کردن این وضعیت توسط پیامهای متناوب دوباره سازی صورت می گیرد. ارسال پیام دوباره سازی باعث افزایش بار در شبکه می شود در عوض نیازی به استفاده از پروتکل های قابل اطمینان مانند TCP که تحویل پیام RSVP را تضمین می کنند نمی باشد.

فرمت پیام RSVP:

پیام RSVP شامل سرآیند های عمومی می باشد که به دنبال تعداد متغیری از اشیاء (برنامه نویسی) می آیند. هر شئ شامل گروهی از پارامترهای مرتبط است و دارای طول متغیر می باشد. سرآیند عمومی در شکل ۲.۲۶ نشان داده شده است. فیلدها به صورت زیر تعریف شده اند:

- Vers:فیلد ۴ بیتی برای نمایش تعداد نسخه پروتکل بکار می رود.
- Flags: فیلد ۴ بیتی برای پرچم ها بکار می رود. هیچ پرچمی مشخص نشده است.
- MsgType توسط ارقامی که در یک فیلد ۸ بیتی بکار می رود مشخص می شود. نوع پیام وارقام در زیر مشخص شده است:
    - Path
    - Resv
    - PathErr
    - ResvErr
    - PathTear
    - ResvTear
    - ResvConf
- RSVP checksum : مجموع مقابله ای ۱۶بیتی که کل پیام را چک میکند.
- Send_TTL: یک فیلد ۸ بیتی مبین زمان زندگی پاکت IP که به Time To Live مشهور است.
- RSVP Length : طول کلی بر حسب بایت در این فیلد ۸ بیتی ذخیره می شود. این طول شامل سرآیند عمومی و تمامی فیلدهای بعدی پاکت می باشد.

فرمت بخشهای بعد از سرآیند در شکل ۲.۲۷ نشان داده شده است. این فیلدها تعریف شده اند:

- Length : فیلد ۱۶بیتی برای نمایش کلی بر حسب بایت می باشد.که باید ضریبی از ۴ باشد و حداقل مقدار آن ۴ باشد.
- Class-num: یک فیلد ۸ بیتی برای مشخص کردن کلاس مورد نظر.
- C-Type : فیلد ۸ بیتی برای مشخص کردن نوع شیء بکار میرود.

4 Bits	4 Bits	8 Bits	16 Bits
Vers	Flags	MsgType	RSVP checksum
Send_TTL		Reserved	RSVP length

شکل ۲.۲۶ : فرمت سرآیند عمومی

2 Bytes	1 Byte	1 Byte
Length (bytes)	Class-num	C-Type
Object contents		

شکل ۲.۲۷ : فرمت داده

کلاسهای اشیاء[۱] زیر تعریف شده اند:

- NULL : :محتوی داده نوع NULL توسط گیرنده در نظر گرفته نمی شود.
- SESSION : شامل آدرس مقصد IP، id پروتکل IP و به شکل اختیاری پورت مقصد می باشد. این داده در هر پیام RSVP مورد نیاز می باشد.
- RSVP hop :آدرس IP روتری را که با RSVP سازگار است و این پیام را فرستاده حمل میکند. برای پیامهایی که از فرستنده به گیرنده ارسال می شود RSVP hop Object به Previous RSVP hop Object موسوم به Phop ارجاع داده میشود. وبرای پیامهایی که از گیرنده به فرستنده ارسال می شود به Next hop Object یا NHOP موسوم هستند.
- TIME VALUES : شامل زمان refresh است که توسط سازندهٔ پیام به کار میرود.
- STYLE : سبک رزرواسیون و اطلاعات سبک ویژه را مشخص می کند. در هر پیام Resv مورد نیاز می باشد.
- FLOWSPEC : اطلا عات ضروری پیام Resv را برای ایجاد رزواسیون در مسیریاب حمل می کند.
- FILTER SPEC: نشان میدهد که کدام پاکت به QoS ذکر شده در بخش قبل نیاز دارد. این بخش در پیام Resv ضروری است.
- SENDER_TEMPLATE : آدرس IP فرستنده را مشخص می کند و گاها بعضی از اطلاعات دمالتی پلکس را مانند شماره پورت مشخص می کند و در Path message ضروری است.
- SENDER_TSPEC : شامل ویژگیهای ترافیکی جریان اطلا عاتِ فرستنده می باشد و در پیام مسیر مورد نیاز می باشد.
- ADSPEC : اطلاعاتِ OPWA[۲] را حمل می کند. همانطوری که در بالا بحث شد اطلاعات از هر گره در طول مسیری که توسط پیام مسیر طی شده است، جمع آوری میشود. این اطلاعات به گیرنده تحویل داده می شود که سپس از آن برای درخواست رزرواسیون یا تنظیم رزرو موجود به صورت مناسب استفاده می شود.
- ERROR_SPEC : یک خطا را در پیامهای PathErr, ResvErr یا پیام تأئید Resv مشخص می کند.

---

[۱] بنا به اهداف الگوریتمیک با اسم Object در منبع آمده است که در اینجا بر طبق کاربرد آن در برنامه نویسی به اشیاء ترجمه شده اند.

[۲] One Path With Advertising

- POLICY_DATA : اطلاعاتی را که مسیریاب برای مشخص کردن مجاز بودن عمل رزرو استفاده می کند را دارا می باشد.در مسیر،Resv, PathErr یا پیام ResvErr مشاهده می شود. یک یا چند POLICY DATA می تواند مورد استفاده قرار گیرد.
- INTEGRITY : داده های مخفی را برای تصدیق گره اصلی برای رسیدگی به محتوی پیام RSVP بکار می برد.
- SCOPE : لیستی از میزبان فرستنده ها که در اطلاعات پیامی که باید ارسال شود دارا می باشد. در Resv, ResvErr, یا ResvTear ظاهر می شود.
- RESV CONFIRM : آدرس گیرنده ای را که درخواست تصدیق دارد را حمل میکند و در پیام Resv یاResvConf ظاهر می شود.

در زیر به تشریح پیام مسیر و Resv می پردازیم:

پیام مسیر

پیام مسیرشامل عناوین عمومی که در شکل ۲.۲۶ نشان داده می شود که بدنبال این Object ها می آید:

- INTEGRITY (Optional)
- SESSION
- RSVP_HOP
- TIME_VALUES
- POLICY_DATA objects (Optional)
- شرح دهندهٔ فرستنده شامل SENDER_TEMPLATE و SENDER_TSPEC
- ADSPC (Optional)

هر میزبان فرستنده یک پیام مسیر برای هر جریان داده ای که بخواهد ارسال می کند . پیام مسیر از مسیریاب به مسیریاب دیگر با استفاده از اطلاعات hop بعدی در جدول مسیریابی هر روتر ارسال می شود تا به گیرنده برسد. هر مسیریاب در طول مسیر پیام مسیر را گرفته و آنرا پردازش می کند. مسیریاب یک حالت مسیر برای هردو گیرنده و فرستنده ایجاد می کند. که در SENDER_TEMPLATE و SESSION پیام مسیر مشخص می شود. تمامی اطلاعات POLICY_DATA و SENDER_TSPEC و ADSPEC هم در متغیر حالت مسیر ذخیره می شوند. اگر خطایی صورت گیرد پیام PathErr به مسیرباب مبدأ بازگردانده می شود.

پیام Resv:

هنگامی که گیرنده پیام مسیر را دریافت می کند، پیام Resv را به فرستنده در مسیر معکوسی که پیام مسیر ارسال شده است، منتشر میکند. به یاد آورید که بستهٔ اطلاعات همان مسیری که توسط پیام مسیر طی شده را دنبال می کند. پیام Resv در واقع به تمام گره ها در آن مسیر درخواست رزرو منابع برای آن جریان

داده را میدهد که شامل سرآیند عمومی است که در شکل ۲.۲۶ نشان داده شد و بدنبال Object های زیر می آید:

- INTEGRITY
- SESSION
- RSVP_HOP
- TIME_VALUES
- RESV_CONFIRM (OPTIONAL)
- SCOPE (OPTIONAL)
- POLICY DATA objects (OPTIONAL)
- STYLE
- یک لیست شرح دهندهٔ جریان

RSVP_HOP شامل NHOP است (یعنی آدرس روتری که پیام Resv را فرستاده است). وجود RESV Confirmation در پیام Resv برای ارسال پیام تصدیق ResvConf به گیرنده برای تایید رزرواسیون می باشد. پیام تصدیق ResvConf آدرس گیرنده را دارا می باشد.

لیست واصف جریان وابسته به سبک می باشد. برای سبک WF یا همان Wild-Card لیست واصف جریان شامل داده های FLOWSPEC می باشد. برای سبک های FF یا Fixed Filter و SE یا Shared explicit شامل FlOWSPEC و FILTER_SPEC می باشد.

همانطوری که در بالا اشاره شد RSVP از محتویات اشیاء RSVP که شامل اطلاعات ترافیکی می باشند و این اطلاعات وسط مسیریاب برای استفاده از منابع به کار میروند، باخبر نمی باشد. قابلیت اجرای RSVP تنها محدود به ساختار intserv نمی باشد. در زیر ما اشیاء یا Object های SENDER_SPEC & FLOW_SPEC که در ساختار intserv بکار می رود را توضیح می دهیم:

: SENDER_TSPEC and FLOWSPEC contents in intserv

SENDER_TSPEC شامل پارامترهای ترافیکی می باشد:

Token Bucket Rate[1], Token Bucket Size[2], Peak Data Rate[3], Minimum Policed Unit[4], Maximum policed Unit[1]

[۱] نرخ پرشدن ظرف نشانه

[۲] سایز ظرف نشانه

[۳] نرخ ماکزیمم داده

[۴] اندازهٔ کوچکترین پاکت مجاز

خصوصیات جریان بستگی به سرویس بار کنترلی یا سرویس ضمانت که مورد درخواست می باشد دارد. هنگام درخواست سرویس بار کنترلی، خصوصیات جریان که شامل TSPec گیرنده است دارای مقادیر پارامترهای فوق الذکر می باشد و این پارامترها هستند که برای محاسبه رزو منابع در مسیریاب بکار می رود.

هنگامی که از "سرویس ضمانتی" استفاده می شود FLOWSPEC شامل خصوصیات TSPEC و RSPEC گیرنده می باشد که زمان سکون و نسبت پارامترها را مشخص می کند این دو پارامتر برای مشخص کردن تاخیر و پهنای باند مطلوب بکار می روند.

RSVP-TE

پروتکل رزرو منابع - مهندسی ترافیک (RSVP–TE) بسط پروتکل رزرو منابع (RSVP) است که در بالا شرح داده شد. RSVP-TE را میتوان در MPLS برای ایجادLSP با استفاده از اطلاعات hop در جدول مسیرها و یا یک مسیر واضح بکار برد.

با مجموعه اصطلاحات که در RSVP بکار رفت ما از شرایط گره، فرستنده و گیرنده برای نمایش LSR، LSR ورودی و خروجی استفاده می کنیم. تا به نحوی معادل سازی نیز بین اصطلاحات موجود پروتلکهای مبتنی بر LDP کرده باشیم. به خاطر آورید که یک جلسه یا session در RSVP یک جریان داده با آدرس مقصد IP ویژه و id پروتکل می باشد. درRSVP-TE یک جلسه یک LSP می باشد.

RSVP-TE از downstream-on-demand برای ایجاد LSP استفاده می کند. این تکمیل کردن با استفاده از پیام مسیر و پیام Resv که با اشیاء جدید تقویت شده است اجرا می شود. یک LSP با استفاده از اطلاعات hop بعدی در جدول مسیر یابی بکار می رود. RSVP-TE همچنین قادر به ایجاد مسیر واضح برایLSP ها می باشد.که با استفاده از شیء جدید EXPLICIT_ROUTE برای کپسوله سای hop هائی که مسیر صریح ایجاد می کنند بکار می رود. هر hop می تواند به عنوان گره منفرد یا گره انتزاعی باشد. یک گرۀ انتزاعی مجموعه ای از گره ها می باشد که توپولوژی داخلی آن نسبت به فرستنده شفاف نمی باشد.مسیر strictly یا loosly از طریق گره انتزاعی امکانپذیر می باشد.

برای تنظیم یک LSP، گره ورودی یک پیام مسیر را با استفاده از شیء LABEL REQUEST ارسال می کند . که این شئ جدیدی می باشد و بیانگر درخواست انقیاد برچسب برای مسیر می باشد. اگر یک مسیر واضح درخواست شود شئ EXPLICIT ROUTE در پیام مسیر قرار داده می شود. اگر LSP با استفاده از اطلاعات hop در جدول مسیریابی ایجاد شود در آن صورت شئ EXPLICIT ROUTE بکار نمی رود.

---

[1] اندازۀ بزرگترین پاکت مجاز

"پیام مسیر" به hop بعدی که مذکور در جدول مسیریابی گیرنده است و متناسب با آدرس مقصد IP ویژه ای می باشد، یا hop بعدی که در شئ EXPLICIT_ROUTE ذکر شده، ارسال میشود. گره ای که قادر به پذیرش LSP جدید نیست یک پیام PathErr را برگشت میدهد.

گیرنده، LSR ورودیِ LSP، با پیام Resv پاسخ می دهد. شئ جدید که Label خوانده میشود در پیام قرار داده میشود و به فرستنده در جهت بالادستی برگشت داده میشود، به این معنی که در جهت عکس همان مسیرِ طی شده توسط پیام مسیر، عودت داده میشود. هر گره که پیام Resv دریافت می کند از شئِ برچسبِ موجود در پیام به عنوان برچسبی برای ترافیک خروجی مرتبط با آن LSP استفاده میکند. یک برچسب جدید را اختصاص میدهد و آنرا در شئ LABEL جاگذاری میکند و سپس آنرا در جهت بالادست به hop بعدی میفرستد. .همانطوری که میتوان مشاهده کرد، در RSVP-TE یک LSP با استفاده از طرح Ordered LSP Control ایجاد می شود.

RSVP-TE عمل رزرواسیون منابع را در طول LSP را فعال می کند. برای مثال پهنای باند را میتوان به یک LSP با استفاده از استاندارد رزرواسیون RSVP و کلاسهای سرویس intserv تخصیص داد.تخصیص منابع اختیاری می باشد و LSP ها میتوانند بدون رزرو هیچ منبعی بوجود آیند. این LSP ها میتوانند برای نمونه برای حمل ترافیک Best Effort و پیاده سازی مسیرهای پشتیبانی به کار برده شوند.

از ویژگیهای دیگر RSVP-TE، ایجاد و نگهداری همراه با اولویت بندی برای LSP و مسیردهی مجدد یک LSP به شکل پویا را میتوان نام برد. همچنین با استفاده از اضافه کردن شئ RECORD_ROUTE به پیام مسیر، فرستنده قادر به دریافت اطلاعات واقعی دربارهٔ مسیری که LSP طی می کند، می باشد.

سبکهای رزرواسیون و کلاسهای سرویس

محدودیتی در RSVP-TE در مورد اینکه کلاسهای سرویس intserv چگونه حمایت شوند وجود ندارد. RSVP-TE همچنین باید از سرویسهای تهی و سرویسهای بار کنترل شده حمایت کند. کلاس بار سرویس کنترل شده در بخش قبلی توضیح داده شد. Null service سرویس جدیدی است که در RSVP معرفی شده تا از سیگنالیگ RSVP در معماری diffserv حمایت کند. در null service یا سرویس تهی درخواست رزرواسیون منابع در هر گره موجود در طول مسیر فرستنده تا گیرنده انجام نمیشود. در عوض آن، عامل سیاستگذاری QoS در هر گره پارامترهای مناسب QoS را برای درخواست، آنگونه که توسط مدیر شبکه تنظیم شده، فراهم میکند.

در قسمت قبلی ۳ سبک رزرو RSVP را شرح دادیم که عبارت بودن از :WF، FF، SE از این سه سبک، WF در RSVP-TE بکار نمی رود گره ورودی می تواند از سبکSE، FF برای هر LSP استفاده کند و می تواند سبکهای مختلف را برای LSP های مختلف انتخاب کند.

هنگام استفاده از سبک FF، هر LSP در هر گره، در طول مسیر، رزرواسیون مخصوص به خود را دارد. و هر گره برچسب منحصر بفردی را برای هر فرستنده اختصاص می دهد. برای نمونه اگر یک مسیر صریح توسط سبک FF ایجاد شود بنابراین هر گره منابع را برای LSP و یک برچسب منحصر به فرد که hop قبلی مجبور به استفاده از آن در آن LSP شده، رزرو میکند. LSPی را که با استفاده از اطلاعات hop بعدی از جدول مسیریابی بنا شده است را در نظر میگیریم. در این مورد اگر چندین فرستنده وجود داشته باشد آنگاه درخت معکوس چند نقطه به نقطه شکل می گیرد. هر فرستنده دارای مسیر خاص خود به گیرنده می باشد که مستقل از مسیرهای دیگر گیرنده هاست. گره ای که در این درخت معکوس که چندین مسیر را نگهداری میکند برای هر مسیر رزواسیون منابع را جداگانه انجام میدهد و برچسبهای مختلفی را بر هر مسیر بر اساس hop قبلی اختصاص میدهد. در نتیجهٔ این عمل این درخت معکوس شامل چندین LSP نقطه به نقطهٔ مستقل میشود. این بدین معنا نیز هست که یک hop قبلی مشابه میتواند برچسبهای مختلفی را برای انتقال ترافیک به گیرندهٔ مشابه از طرف فرستنده های مختلف استفاده کند.

سبک SE به گیرنده اجازه میدهد تا به طور صریح فرستنده را برای شامل شدن رزرواسیون مشخص کند. یک رزواسیون در هر گره برای همهٔ فرستنده هائی که مسیر گیرنده شان از این گره میگذرد وجود دارد. برچسب های مختلف به فرستنده های مختلف نسبت داده میشوند بنابراین LSP های جداگانه ای ایجاد میشود.

اشیاء جدید RSVP-TE

۵ شئ جدید زیر برای حمایت از عملکرد RSVP-TE معرفی شده اند:

- LABEL
- LABEL_REQUEST
- EXPLICIT_ROUTE
- RECORD_ROUTE
- SESSION_ATTRIBUTE

یک C-Type جدید هم برای اشیاء SESSION و SENDER_TEMPLATE و FILTER_SPEC تعریف شده است. حال به بررسی این ۵ شئ میپردازیم:

The Label Object

شئ برچسب در پیام Resv به جهت اعلان یک برچسب به کار میرود. برای سبکهای FF و SE، یک گره یک برچسب جداگانه برای هر فرستنده که بوسیلهٔ hop قبلی استفاده میشد اختصاص داده میشود. فرمت شئ برچسب در شکل ۲.۲۸ نشان داده شده است. کلاس شئ برچسب (در فیلد شمارهٔ کلاس class num داده شده). ۱۶ است. نوع شئ (در فیلد C-Type داده شده است)، C-Type یک است.و محتوای object با یک انکد برچسب منفرد در ۴ بایت است. یک برچسب معمولی MPLS و frame relay در چهار بایت انکد میشود. یک برچسب ATM با فیلد VPI از ۰ تا ۱۵ و فیلد VCI از ۱۶ تا ۳۱ (در مجموع ۳۲ بیت یا ۴ بایت) انکد میشود.

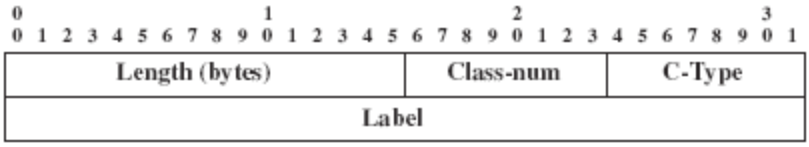
یک گره میتواند از چندین فضای برچسب حمایت کند. به عنوان نمونه میتواند یک فضای برچسب یگانه را به هر اینترفیس ورودی نسبت دهد، اینترفیسهائی که اغلب متفاوت درنظر گرفته میشوند حتی به یک برچسب متعلق باشند.

The LABEL_REQUEST Object

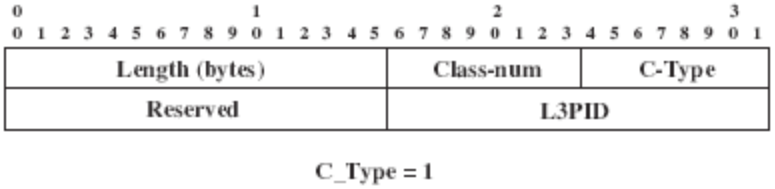
کلاس درخواست برچسب ۱۹ می باشد و سه نوع مختلف ازفیلد نوع C وجو دارد (C-Type 1, C-Type 2 , C-Type 3)

C-Type 1 برای برچسبهای عمومی ، C-Type 2 برای برچسب های ATM و C-Type 3 برای برچسب های frame relay می باشد.این سه نوع در شکل ۲.۲۹ نشان داده شده اند.C-Type 1 شامل ۱۶بیت فیلد معکوس و ۱۶بیت فیلد L3PID که با پروتکل لایه ۳ در مسیر مشخص می شود، شامل فیلد های زیر می باشد.(فیلد های ذخیره ذکر نشده است.)

- LP3ID : یک فیلد ۱۶ بیتی که شناسهٔ پروتکل لایهٔ ۳ که ازین مسیر استفاده میکند را حمل میکند.
- M : یک فیلد ۱ بیتی است که برای مشخص کردن اینکه آیا گره مناسب ادغام طرح داده است یا نه.
- Minimum VPI : یک فیلد ۱۲ بیتی است که مرز پائینی بلوک مقدار مورد حمایت VPI را نشان میدهد.
- Minimum VCI : یک فیلد ۱۶ بیتی است که مرز پائینی بلوک مقدار مورد حمایت VCI را نشان میدهد.
- Maximum VPI : یک فیلد ۱۲ بیتی که مرز بالائی بلوک مقدار مورد حمایت VPI را میدهد.
- Maximum VCI : یک فیلد ۱۶ بیتی که مرز بالائی بلوک مقدار مورد حمایت VCI را میدهد.



شکل ۲.۲۸ فرمت شئ برچسب



شکل ۲.۲۹ فرمت درخواست برچسب

C-type 3 شامل فیلد های زیر می باشد. (فیلد های ذخیره ذکر نشده است.)

- L3PID : یک فیلد ۱۶ بیتی که شناسهٔ پروتکل لایهٔ ۳ که ازین مسیر استفاده میکند را حمل میکند.
- DLCI Length Indicator (DLI) : یک فیلد ۲ بیتی که طول DLCI را مشخص میکند. این مقادیر ساپورت میشود: DLI=0 یعنی طول DLCI ۱۰ بیت است. DLI=2 یعنی طول DLCI ۲۳ بیت است.
- Minimum DLCI : این فیلد ۲۳ بیتی مرز پایئن بلوک مورد حمایت DLCI را مشخص میکند.
- Maximum DLCI : این فیلد ۲۳ بیتی مرز بالائی بلوک مورد حمایت DLCI را مشخص میکند.

به منظور ایجاد یک LSP، فرستنده یک پیام مسیر به همراه LABEL_REQUEST درست میکند. این شئ مشخص میکند که انقیاد برچسب برای این مسیر درخواست شده است و آن یک شاخص لایهٔ پروتکل شبکه ای است که بر روی مسیر حمل میشود. این به پاکتها اجازه میدهد تا از یک پروتکل لایهٔ شبکهٔ غیر IP در یک LSP به کار گرفته شود. این اطلاعات همچنین در اختصاص برچسب نیز مفید است زیرا بعضی از برچسبهای رزرو شده مخصوص پروتکلهای خاصی هستند. یک گیرنده که از پروتکل مشخص شده در فیلد L3PID حمایت نمیکند، یک پیام PathErr به فرستند برمیگرداند.

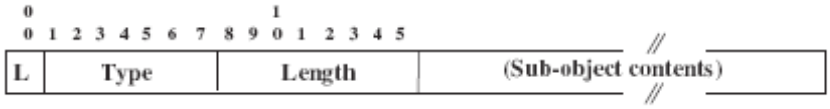
The EXPLICIT_ROUTE Object

این شئ برای مشخص کردن hop ها در مسیر صریح درخواست شده به کار میرود. هر hop میتواند یک گره یا گروهی از گره ها باشد که به گرهٔ انتزاعی موسوم است. برای سادگی، RSVP-TE با همهٔ گره ها به شکل گرهٔ انتزاعی برخورد میکند با در نظر گرفتن این مطلب که یک یک گرهٔ انتزاعی میتواند فقط شامل یک گره باشد.

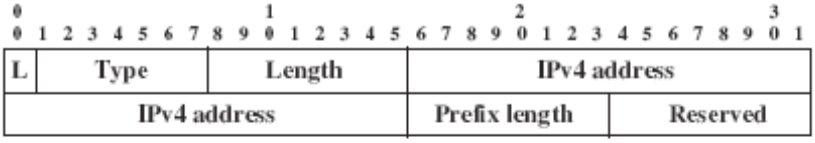
کلاس شئ EXPLICIT_ROUTE ۲۰ است، و تنها یک نوع شئ تعریف شده است (C-Type 1). محتوای شئ شامل یک سری از زیر اشیاء طول متغیر است که هر یک از یک گرهٔ انتزاعی متشکل اند. فرمت زیر اشیاء در نمودار ۳.۳۰ نشان داده شده است. فیلدهای پیش رو تعریف شده اند:

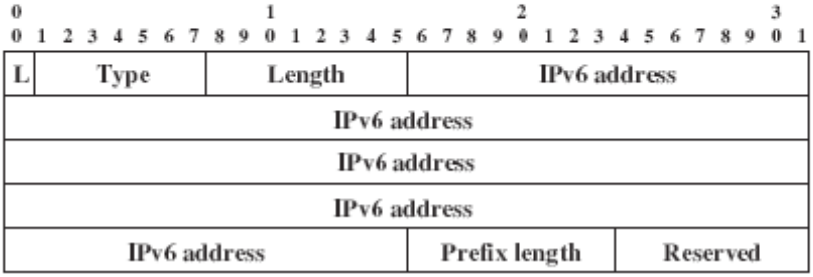
- L : یک فیلد ۱ بیتی که برای مشخص کردن اینکه مسیر گذرنده از یک گرهٔ انتزاعی سخت گیرانه است یا آسانگیر.
- Type : این فیلد ۷ بیتی با یک مقدار که نشان دهندهٔ نوع محتوای زیر شئ است همراه است. این دو مقدار تعریف شده اند مقدار ۰ بدین معنی است که زیر-شئ حاوی یک پیشوند IPv4 است. و ۱ بدین معنی است که حاوی پیشوند IPv6 است، و ۳۲ اگر شمال یک شمارهٔ سیستم خودکار باشد.
- Length : این فیلد ۸ بیتی با طول (بر حسب بایت) زیر-شئ شامل فیلدهای L و Type و Length همراه است.

فرمت sub-objects برای IPv4 وIPv6 در شکل ۲.۳۱ نشان داده شده است. فیلد آدرس IPv4 و بهمین شکل IPv6 در زیر شئ IPv4 (و بهمین ترتیب IPv6) حاوی یک پیشوند IPv4 (IPv6) است که طول آن در فیلد طول داده شده است. گرهٔ انتزاعی که با این زیر شئ نمایندگی میشود شامل مجموعهٔ تمام گره هائی است که آدرس IPv4 (IPv6) آنها آن پیشوندی است که در فیلد آدرس IPv4 (IPv6) است. توجه کنید که یک پیشوند با طول ۱۲۸ نشانگر یک گرهٔ منفرد است.



شکل ۳.۳۰ فرمت sub-object





شکل ۲.۳۱ فرمت sub-objectبرای پیشوند های IPv4 , IPv6

فرمت زیر-شئ برای سیستم خودکار مانند همانی است که در شکل ۲.۳۰ نشان داده شد. با محتوای زیر-شیئی که شامل فیلد ۲ بایتی است که با سیستم شمارهٔ خودکار کار گذاشته است. گرهٔ انتزاعییٔ که با این یزر شئ نمایندگی میشود مجموعه ای از گره هاست که به این شمارهٔ خودکار تعلق دارد.

The RECORD_ROUTE Object (RRO)

وجود مسیرهای loose route در یک گرهٔ انتزاعی بدین معنی است که این امکان وجود دارد که حلقه ها در طول یک جلسه به طور ویژه هنگامی که پروتکل زیری در حالت گذار است ایجاد شوند. حلقه های میتوانند توسط شئ RECORD_ROUTE کشف شوند. در این شئ آدرس IP هر گره در مسیر میتواند ثبت شود. و به همچنین برچسبهای استفاده شده در مسیر نیز میتوانند ثبت شوند. RECORD_ROUTE object میتواند در هردو پیام path و resv پیدا شوند.

کلاس شئ RECORD_ROUTE ۲۱ است و یک نوع شئ C-Type وجود دارد، C-Type 1. محتوای شئ شامل مجموعه ای از زیر-شئ های طول متغیر سازماندهی شده در یک پشتهٔ LIFO است. دو زیر-شئ اول مانند حالت EXPLICIT_ROUTE هستند که در شکل ۲.۲۸ نشان داده شده اند. (با این تفاوت که فیلد reserved با فیلد پرچم یا flag جایگزین شده است). زیر-شئ برچسب ساختاری که در شکل ۲.۳۰ است را دارد و شامل تمامی محتوای شئ LABEL است.

The SESSION_ATTRIBUTE Object

این شئ شامل اولویتهای نگهداری برای یک LSP است به اضافهٔ پرچمهای مختلف. برپاسازی اولویت یا setup priority اولویتی است که برای تخصیص منابع به کار میرود. Holding priority اولویتی است که برای نگهداشتن منابع به کار میرود.

پیام Resv و مسیر RSVP-TE:

پیامهای Path و Resv در RSVP-TE مشابه همان پیامها در RSVP است. پیام مسیر RSVP-TE متشکل است همان سرآیند معمول در شکل ۲.۲۶ است که با این اشیاء همراه است:

- INTEGRITY (Optional)
- SESSION
- RSVP_HOP
- TIME_VALUES
- EXPLICIT_ROUTE (Optional)
- LABEL_REQUEST
- SESSION_ATTRIBUTE (Optional)
- POLICY_DATA objects (Optional)
- یک شارح فرستنده که شامل SENDER_TEMPLATE و SENDER_TSPEC است.
- ADSPEC (Optional)
- RECORD_ROUTE (Optional)

و پیام Resv نیز در RSVP-TE همانطور که در شکل ۲.۲۶ آمده با اشیاء زیر همراه است:

- INTEGRITY (optional)
- SESSION
- RSVP_HOP
- TIME_VALUES
- RESV_CONFIRM (optional)
- SCOPE (optional)
- POLICY_DATA objects (optional)
- STYLE

یک لیست شرح دهندهٔ جریان وابسته به سبک برای سبک Fixed Filter یا FF شامل اشیاء FLOWSPEC و FILTER_SPEC و LABEL و RECORD_ROUTE (optional) است. برای سبک shared explicit یا SE شامل اشیاء FILTER_SPEC و LABEL و RECORD_ROUTE (optional) است.

RSVP-TE Extensions

RSVP برای حمایت از رزواسیون منابع در جریان دادهٔ تعریف شده بین فرستنده و گیرنده تعریف شد.با افزایش تعداد جریانهای داده، سربار (Overhead) مربوط به RSVP بر روی شبکه نیز افزایش یافت و این بعلت

پیامهای مداوم refresh ی بود که باید مبادله میشد. همچنین حافظهٔ مورد نیاز برای ذخیرهٔ اطلاعات حالت مسیر در هر روتر و بهمین شکل میزان پردازش مورد نیاز افزایش یافت. ازین منظر، بعنوان پروتکلی که به خوبی انعطاف یابد در نظر گرفته نمیشد. و مشکلاتی مشابهی نیز در RSVP-TE هست چرا که این هم بر اساس RSVP کار میکند.

چندین راه حل برای کاستن این مشکلات ارائه شده است. به عنوان مثال یک مکانیسم برای انتقال مطمئن ارائه شده است که نیاز به پیامهای refresh را مرتفع میکند. این مکانیسم به کمک دو شئ جدید ساخته میشود: MESSAGE_ID و MESSAGE_ID_ACK . همچنین میزان داده ای که بر اثر پیامهای رفرش منتقل میشود میتواند با پیام Srefresh که یک پیام خلاصهٔ رفرش جدید است، کاهش یابد.

مقایسه

در زمانهای قدیم شبکه ها در یک پایه per-service به کار گرفته میشدند. اگر یک F.R می خواستند، خوب یک F.R میخریدند، امروزه شبکه چند سرویسی طغیان کرده و در این وادی داغتر از MPLS وجود ندارد. امروزه اکثر سازمانهای بزرگ به سمت multiprotocol label switching یا همان MPLS رفته اند و بنابراین کاربران میتوانند منتظر باشند تا سرویسی مانند Frame Relay روی یک پلتفرم ناآشنا و با قیمتی جذاب ببینند. اما نباید انتظار داشته باشند که سرویس F.R مانند روزهای قدیمیش کار کند.[14]

با توجه به مفهوم شبکهٔ کامپیوتری، frame relay شامل روش مؤثری برای انتقال داده با تکنیکی ارزان قیمت است. ارائه دهندگان شبکه عموما F.R را به عنوان یک تکنیک کپسوله سازی برای انتقال داده و صوت بین LAN ها روی یک WAN به کار میگرفتند. هر کاربر یک خط اختصاصی یا leased line به گره F.R میگیرد و F.R این خط انتقال را با عمل سوئیچنگ بین کاربرها نگه میدارد. اما با پیشرفت MPLS و VPN و سرویسهای پهن باند اختصاصی مانند مودم کابلی و DSL، ممکن است پایان پروتکل F.R به سر آمده باشد. هدف اولیه label based switching آوردن سرعت لایهٔ ۲ و سوئیچنگ لایهٔ ۳ با هم بود. سوئیچنگ بر اساس مفهوم label به روتر اجازه میدهد تا تصمیم forwarding خود را بر اساس محتوای سادهٔ یک برچسب به جای انجام عملیات پیچیده روی IP انجام دهد. این هدف اولیه امروزه تنها دلیل استفاده از MPLS نیست و دیگر به عنوان مزیت اصلی آن تلقی نمیشود چرا که سوئیچهای ASIC لایهٔ ۳ وجود دارند که قادرند عملیات لازم را در سرعت قابل قبولی ارائه دهند. با این وجود MPLS مزیت های دیگری را به شبکه IP-based میدهد که عبارتند از:

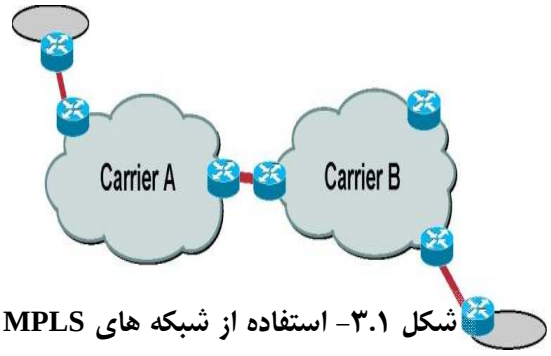
- Traffic Engineering : توانائی برای تنظیم مسیر ترافیک و قابلیت کلاس بندی ترافیک و مشخصات عملکردی
- VPNs : با استفاده از MPLS ارائه دهندگان سرویسها قاردند که یک تونل IP را در شبکه برقرار کنند بدون اینکه به رمزنگاری یا اپلیکیشنهای کاربر نیاز باشد.
- Layer 3 Transport : استاندارد جدیدی که بویسلهٔ گروههای کاری IETF's PWE3 و PPVPN تعریف شده است به ارائه دهندگان سرویس اجازه میدهد که سرویسهای لایهٔ ۲ را حمل کنند که شامل Ethernet و F.R و ATM over an IP/MPLS میشود.
- Elimination of Multiple Layers : نوعا بیشتر حاملهای شبکه هنگامی که از یک مدل رویهم قرار گرفته مانند SONET/SDH در لایهٔ ۱ و ATM در لایهٔ ۲ و IP در لایهٔ ۳ استفاده میکنند. استفاده از MPLS میتواند سبب مهاجرت بسیاری از کاربردهای SONET/SDH & ATM به لایهٔ ۳ شود. پس این خود سبب مدیریت بهتر شبکه و ساده سازی در این کاراتر کردن آن شود.[15]

MPLS به کاربران شبکه عملکرد بهتری را برای اپلیکیشنها، برای انعطاف پذیری در divert کردن مسیر ترافیک در اطراف یک لینک خراب یا پرترافیک میدهد و عملکرد شبکه در گلوگاهها را بین ۱۰ تا ۴۰ درصد نسبت به F.R بهتر میکند.[[16]]

MPLS برای حل مشکل پل و اتصال بین چند پروتکل مختلف مانند F.R و ATM و Ethernet اختراع شد. در واقع MPLS حمل داده را برای هم سوئیچنگ Circuit-base و هم Packet-base یکنواخت میکند. MPLS میتواند برای حمل انواع مختلف ترافیک از F.R تا Sonet و Ehternet به کار برده شود.

MPLS مزایای چندی دارد مانند امکان کلاس بندی خدمات که به Class of Service یا CoS مشهور است. با سرویس MPLS میتوان جریان داده را اولویت بندی کرد و مطمئن بود که بیشتر داده های مهم با ضریب اطمینان بالا در شرایط ازدحام و ترافیک سنگین منتقل میشوند. کاندایدای اول برای یک چنین شبکهٔ MPLS میتواند VOIP باشد چرا که صدا در شبکه با ترافیک سنگین به شدت به مسئله jitter و تأخیر حساس است و این مورد معمولا در شبکه های Frame Relay پیش می آید که به خصوص در دنیای تجارت قابل تحمل نیست. پس کاربردهائی مانند VoIP, CRM, ERP, Videoconferencing, etc بر روی MPLS نسبت به تکنولوژی ۲۰ سال قدیمتر F.R بسیار بیشتر است. [17]

شرکتهای ارائه دهندهٔ سرویس، مدیریت ساده تر و شبکه ای کم هزینه تر میخواهند. اینست که پوشش دادن چند شبکه و سرویس به یک هستهٔ پرسرعتِ Low-Latency و کارای IP-MPLS که نیاز به QoS های مختلف برای این شبکه ها را برطرف میکند، به این هدف کمک میکند. از طرف دیگر پدیدهٔ جهانی سازی مؤسسات را به این سمت کشانده که شبکه هایشان را در تمام نقاط جهان به همدیگر وصل کنند و بدین ترتیب مشتریها و فراهم کننده هایشان را، و این درحالیست که تا کنون مؤسسه یا ارگانی این درجه از جهانی شدن را تجربه نکرده است. علاوه بر این یک مؤسسه ممکن است که چند فراهم کنندهٔ سرویس متفاوت برای شعب مختلف خود به کار گیرد بنابراین این مؤسسه نیاز دارد تا این شبکه ها را به هم وصل کند تا به اهدافش برسد و بتواند یکه شبکه سراسری و کارا بین شعبات خود برقرار کند.



شکل ۳.۱- استفاده از شبکه های MPLS در هستهٔ شبکه ها

اتصال بین حاملهای شبکه (شرکتهای ارائه دهنده) محدود به انتقال پاکتهای IP بر روی یک اتصال IP است و یا انتقال به کمک انتقال سرویس لایهٔ ۲ . فراهم کنندگان سرویسها تنها قادرند که QoS را برروی اتصالات IP با وجود یک توافق اختصاصی دوطرفه انجام دهند و اینها از وجود یک استاندار کامل و سراسری رنج میبرند. تا به امروز که این مقاله نوشته شده (۲۰۰۵) هیچ مشخصات و استانداری برای یک MPLS Inter-Carrier Interconnection یا MPLS-ICI طراحی نشده است. با این وجود خدمات میتوانند از لبهٔ یک شبکه MPLS به لبهٔ MPLS دیگر به شکل شفاف انجام گیرد. بعلاوه به خاطر اینکه MPLS یک تکنولوژی انتقال چند سرویسه است یک MPLS-ICI میتواند نیاز به داشتن چندین تکنولوژی تماس بینابینی در محل اتصال را

حذف کند وسبب کاهش هزینه و سادگی مدیریت شود. اینا فاکتورهائی هستند که carrier ها را تشویق میکند تا MPLS را برای شبکه های متمایل به همگرائ زیربنائی packet-base خود به خدمت گیرند.[1] [18]

در ظرف چند سال، MPLS از یک تکنولوژی نامتعارف به یک ابزار اصلی که توسط فراهم کننده سرویسها SPs نمو کرده است تا یک سرویس منفعت-زا تولید کند. امروزه رشد سریعی در به کار گیری سرویسهای دارای امکان MPLS وجود دارد و در استانداردها نیز یک روند توسعهٔ فعال در توسعه تکنولوژیهای و کاربردهای جدید وجود دارد. [19] اولین جلسهٔ گروه کاری IETF-MPLS در آوریل ۱۹۹۷ شکل گرفت که تا به امروز نیز وجود دارد و MPLS رشد یافته تا به مرحلهٔ ای برسد که بیشتر فعالیتهای گروههای دیگر IETF را تحت تأثیر گذاشته است مانند Layer 3 VPN & Layer 2 VPN, Pseudo Wire Emulation Edge to Edge و Common Control و Measurement Plane (ccamp) و... که ازین مسئله تأثیر پذیرفته اند. [20]

به عنوان مقدمه ای توسط نگارنده برای تلخیص مطلب این نکته مهم را یادآور میشوم که یک از مزایای مهم تکنولوژی MPLS امید برای بحث همگرا شدن شبکه ها در آینده است که منجر به یکی از مهمترین دستاوردهای قرن ۲۱ در تمام حوزه های زندگی بشری خواهد شد.[2] این شبکهٔ نسل آینده را NGN یا Next Generation Network می نامند و کاندیدای اول برای پیاده کردن و رسیدن به شبکه ای است که بتواند با سرویسهای مختلف و شبکه های اختصاصی مختلف از شبکه های موبایل، شبکه های کامپیوتری و شبکه های تلویزیونی تا شبکه ای از سیستم های خدمات عمومی و حتی لوازم خانگی متصل به شبکه کار کند همین Multi-Protocol Label Switching است. نوع ساختار این شبکه نه تنها این اجازه را میدهد بلکه با پروتکلهای لایه های دیگر نیز به خوبی سازگار میشود. این MPLS است که میتواند بدون نیاز به درگیر شدن در جزئیات پروتکلهای مختلف با سرویسهای متفاوتی کار کند در چند سطر بعد دلایلی از کتاب *MPLS Enabled Applications: Emerging Developments & New* Technologies که توسط Ina Minei و Julian Lucek نوشته شده است را می آوریم این کتاب در فصل ۱۳ خود به خصوص در بخش ۱۳-۲ به معرفی دلایلی که MPLS میتواند به زیرساختی برای شبکه ها و سرویسهای مختلف تبدیل شود پرداخته است و راجع به آن به طور مبسوط تر توضیح داده شده است و در اینجا تنها به خلاصه ای از توضیحات هر سرآیند اکتفا میشود در این تلخیص سعی شده است تا حد امکان مفهوم مورد نظر کتاب رسانده شود. کتاب فوق الذکر با سایر منابع در لوح فشرده همراه پایان نامه فراهم گردیده است. در ادامه برای پرهیز از پیش آمدن ابهام و نامأنوس شدن ترجمه اصطلاحات تا حد ضرورت عناوین ترجمه نشدند:

Flexibility with respect to connectivity:

[1] برای اطلاعات بیشتر راجع به MPLS-ICI و GMPLS به منبع معرفی شده رجوع شود.

[2] ابر شبکه نسل آینده در کنار واقعیت مجازی به عنوان موج چهارم پس از موج سوم یعنی انقلاب اطلاعات تلقی میشود که توسط برخی نظریه پردازان معرفی شده است.

انعطاف پذیری در عین قابلیت اتصال به این خاطر است که در شبکهٔ IP رسیدن به تضمین پهنای باند end-to-end ممکن نیست. اما MPLS به عنوان یک شبکهٔ اتصال-گرا یا Connection-Oriented و با استفاده از امکانات مدیریت ترافیک و کنترل پذیریش یا admission control این قابلیت را دارا میباشد.

Aggregation Properties:

یک LSP[1] میتواند تمام ترافیک بین دو PE را در یک یا چند کلاس را حمل کند. در حالت کلی ممکن است تعداد زیادی از جریانهای کوچک[2] در این مسیر تجمع یابند، در نتیجه هستهٔ MPLS اظهار یا پاسخی مربوط به این جریانهای کوچک[3] شخصی ندارد پس اگر تعداد LSP ها در شبکه به حدی زیاد شد که به یک مشکل به خاطر مسئله کنترل و نگهداری و افزایش حجم این microflows ها بدل شد ساختار سلسله مراتبی MPLS این اجازه را میدهد تا این microflow ها در بین تعدادی از LSP ها متناسب بپیچند و ترافیک اضافی به سایر LSP ها تحمیل نکنند و بدین ترتیب گسترش شبکه را به هر تعداد بیشتری مختل نکنند.

Single forwarding mechanism

مسئلهٔ مهم در این امر اینست که با استفاده از Label Swapping روترها نیازی به دانستن اینکه چه نوع ترافیکی را حمل میکنند ندارند و تنها یک برچسب به عنوان اندیس به آن میچسپانند/س

Failover mechanisms

IP همواره این خاصیت را داشته که به مسئله شکست یا خرابی پاکت پاسخ کندی داشته و در مقابل MPLS در این زمینه با تکنولوژیهائی مثل SONET/SDH مقایسه میشود.

Ability to support multiple services on common equipment

MPLS جزئیات را از دید روتر پنهان میکند و کار را با اندیسها انجام میدهد بدین تریب به شبکه های مختلفی از ATM تا اترنت کار میکند و میتواند به اشکال مختلفی مانند اترنت و DSL و SONET و ... به مشتریان دسترسی بدهد.

علاوه بر این MPLS مزایای دیگری در بعد طراحی روتر و مدیریت شبکه دارد که برای اطلاع از آنها به منبع [21] ارجاع داده میشود.

---

[1] Label Switch Path

[2] بیشتر جریانهای ناشی از تبادل اطلاعات روتینگ مدنظر است که در متن اصلی به نام microflows آورده شده اند./س

[3] بیشتر محلی/س

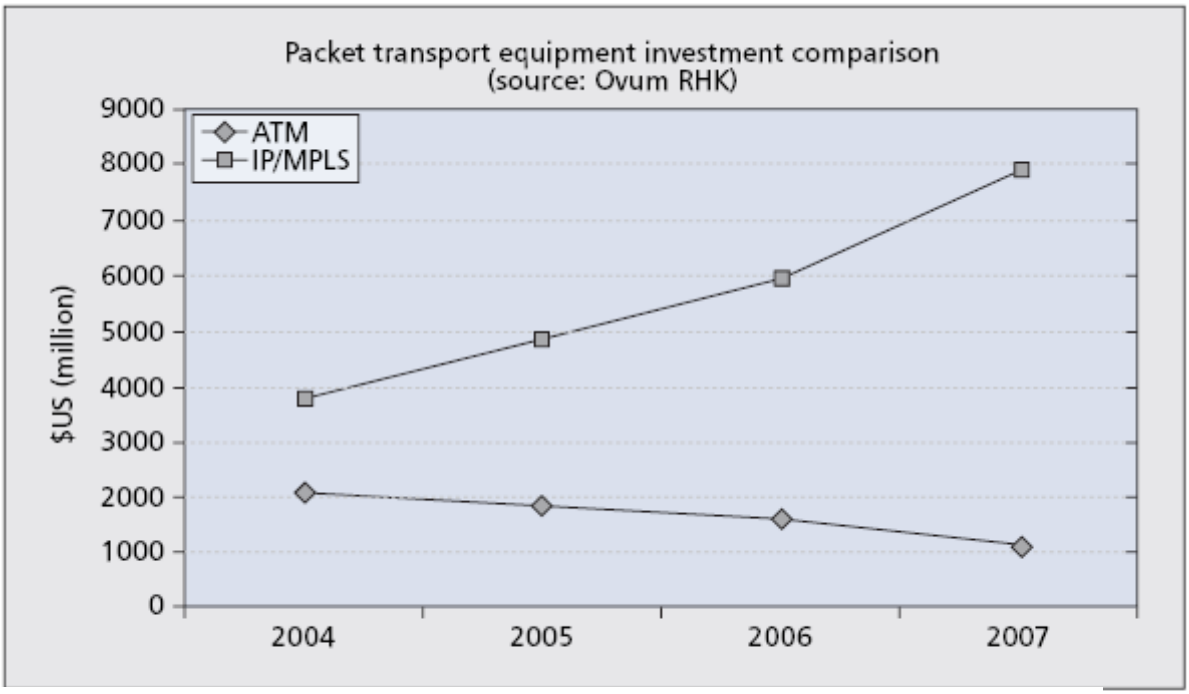
گرایشات در بازار MPLS

در زمان نوشتن این کتاب ([21]) بیشترین سرویس Customer-Visible MPLS که به طور وسیعی به کار برده شده Layer 3 VPN که به اسامی IP VPN یا 2547bis VPN بعد از استاندارد ارائه شده هستند که توسط IETF نیز شناخته میشوند. MPLS همچنین در بعضی از شبکه ها به عنوان یک ابزار ساختاری برای فراهم کردن مدیریت ترافیک و قابلیت مسیریابی سریع به کار میرود. یک کاربرد به سرعت در حال رشد دیگر Point-to-Point Layer2 Transport به عنوان هم وسیلهٔ حامل ترافیک اترنت بر روی یک WAN یا به عنوان جزئی از یک ایمولاتور ATM یا Frame Relay.

بسیاری از فراهم آورندگان سرویسها بر روی استفاده از یک شبکهٔ مبتنی بر MPLS برای فراهم کردن یک پلتفرم مشترک برای رنج وسیع سرویسهای مختلف سرمایه گذاری کنند. سرویسهائی که در حال حاضر بر روی شبکه های متمایزی اجرا میشوند. یک چنین شبکه ای بایدقادر باشد تا ترافیک شبکه هائی مثل Public Switched Telephone Network (PSTN) و Public Internet and Private IP data Service و Layer 2 ATM و Frame Relay و سرویسهای Broadcast TV و TDM و... باشد. این صرفه جوئی قابل ملاحظه ای را در هزینه مالی و مدیریت و نگهداری شبکه به بار می آورد چرا که عوض مدیریت و ساخت یک شبکه برای هر سرویس از یک بستر عمومی استفاده میشود. یکی از مهمترین قابلیت های مربوط در شبکهٔ MPLS خاصیت و پروتکلهای DiffServ Aware TE است که نقش اساسی در این قابلیت شبکه MPLS بهمراه خود مفهوم Label Switching ایفا میکند.[21]

وضعیت اقتصادی پیش رو

این بخش از مقالهٔ [22] گرفته شده و برای جلوگیری از اطناب در اینجا ذکر نمیشود این مقاله نیز به عنوان یکی از منابع فراهم است ولی به طور خلاصه بحث این مقاله بر نشان دادن افزایش سرمایه گذاریها در زمینه MPLS و روند رو به رشد آن و از طرفی چالشهای پیش رو در راه این امر از دیدی اقتصادی است



شکل ۳.۲- سرمایه گذاری های انجام شده بر روی MPLS و ATM

موفقیتها و شکستهای تکنولوژی ATM

ATM در سناریوی WAN موفق بود و تعداد زیادی از شرکتهای مخابراتی آنرا در هسته شبکه های WAN خود پیاده کردند. تعداد زیادی از پیاده سازیهای ADSL هم از ATM استفاده میکنند. اما ATM در جلب نظرات برای استفاده در تکنولوژیهای LAN ناموفق مانده است. پیچیدگی مدیریتی آن باعث شده که آنرا از به کار گیری کامل به عنوان تنها تکنولوژی کاندید برای این موضوع همانطور که طراحان آن تصور میکردند باز دارد. از زمانی که هم تکنولوژیهای جدید و هم کهنه به خصوص در LAN وجود دارد، تمام آنها در قالب SONET که ATM برای آن درست شده قرار نمیگیرند. بنابراین یک پروتکل نیاز است تا یک لایهٔ یکنواخت بر روی هم لایه های پیوند ATM و غیر ATM فراهم کند و از آنجائیکه ATM نمیتواند آن نقش را خودش ایفا کند، IP در حال حاضر آنرا انجام میدهد. بنابراین اغلب ویژگی در پیاده کردن ATM در سطح لایهٔ شبکه وجود ندارد. بعلاوه به خاطر بهینه سازیها و پیشرفتهای اخیر در سرعتهای انتقال در VoIP که تجمیع صوت با لایه ای بالاتر در سطح لایهٔ داده مانند IP را موجب شده است، سبب گردیده تا نیاز به سلولها برای کاهش jitter[۱] کم گردد. از طرف دیگر از بین رفتن انگیزه برای به کار بردن یک سیستم ATM فراگیر موجب شده است تا بیشتر شرکتهای مخابراتی به سمت تجمیع فعالیتهای صوتی خود در لایهٔ IP به جای به کار بردن شبکهٔ IP خود در ساختارهای صوتی خود بروند[۲].ATM هنوز به طور وسیعی به عنوان سرویس multiplexing در شبکه های DSL به کار میرود چرا که توقعات نرخ داده پائین DSL را به خوبی ساپورت میکند. در عوض

[۱] به بخش تحت نام Why Cells? در همین پایان نامه در بخش مربوط به ATM مراجعه کنید.

[۲] کنسرسیوم حمایت کنندهٔ ATM انجام اینکار را توسط MPOA (IP over ATM) پیشنهاد داده که یارای رقابت با MPLS را ندارد چرا که هر چند مزایای IP را به ATM می آورد ولی تمام مضرات ATM را حفظ میکند /سهامی

شبکه های DSL از IP و سرویسهائی مبتنی بر IP مانند VoIP از طریق PPP بر روی ATM و Ethernet over ATM که در RFC شمارهٔ ۲۶۸۴ توضیح داده شده است حمایت میکنند.[23]

پروژه های مشابه

در این فصل به مروری اجمالی از کارهای قبلی می پردازیم این کارها نتیجه جست و جوئی در اینترنت برای پروژه های مشابه است و کارهائی که در این زمینه یافت شدند در اینجا به اختصار معرفی میگردد. همهٔ این پروژه ها به شکل جداگانه در لوح فشرده همراه پایان نامه موجود است. متاسفانه هیچ یک ازین پروژه ها در این طرح مورد استفاده قرار نگرفت چون از ۵ منبعی که ذکر میشود تنها ۳ منبع به واقع اقدام به طراحی روتر سخت افزاری کرده بودند و از ۳ منبع نیز ۲ تای آن تنها یک مقالهٔ ۵-۶ صفحه ای بود که چندان قابل استفاده نبود و تنها یک منبع یک پروژه کامل کارشناسی ارشد بود که بیشتر به بحثهای مخابراتی شبکه پرداخته بود و طراحی نیز تا حدی با استفاده از Verilog HDL انجام داده بود که این ۵ تا برای مقایسه فراهم گردیده اند:

طبق تحقیقاتی که به عمل آمده است امروزه تمام شرکتهای مطرح در زمینه طراحی روتر و مسائل مربوطه مانند Cisco, Nortel, Alcatel, Juniper, Nokia,… از پیاده سازی نرم افزاری سوئیچهای مبتنی بر MPLS بر روی یک پلتفرم عمومی[۱] استفاده میکند. به عنوان مثال شرکت سیسکو به عنوان شرکت پیشرو و اصلی بازار در این زمینه از MPLS به شکل یک پکیج افزودنی به سیستم عامل اختصاصی خود به نام IOS[۲] استفاده میکند.البته تمامی سوئیچهای این شرکت قابلیت استفاده ازین پکیج را ندارند و پشتیبانی از MPLS مختص سریهای خاصی است که توسط شرکت سیسکو نام برده شده اند.

دلیل رویکرد شرکتها به این مسئله بحث هزینهٔ طراحی و تولید با انعطاف پذیری بالاست. هرچند سیستم های مبتنی بر ASIC از سرعت بالاتری برخوردارند ولی بدلیل هزینه بالای تولید یک پلتفرم ویژه و وجود پروتکلهای متنوع و متغیر در این زمینه و نگهداری، توسعه و رقابت این محصول مطابق نیاز بازار عملا موجب شده است که شرکتها به سراغ ASIC نروند. از این گذشته خود بحث MPLS و مطرح شدن آن به سالهای آخر دهه نود و اوایل قرن ۲۱ [۳] برمیگردد بسیاری از استانداردهای این مبحث هنوز در مرحله پیش نویس قرار دارند و تنها RFC های اصلی آن چند سالی است که به شکل نهائی خود رسیده اند. لذا نیاز به یک پلتفرم انعطاف پذیر با هزینه کم بسیار مورد نیاز است.

در چند سال اخیر- شاید بتوان گفت بعد از ۲۰۰۵ – در محافل آکادمیک و نه تجاری، پیشنهاد یا طرحهائی مبنی بر استفاده از پلتفرمهای مبتنی بر FPGA/CPLD و تحت مفهومی مانند Reconfigurable Computing

---

[۱] Genral Purpose Platform

[۲] Internetworking OS

[۳] بین سالهای ۱۹۹۷ تا ۲۰۰۱ بحثهای اولیه و پایه ای آن شکل گرفت

ارائه شده است. با توجه به جست و جوئهائی که در اینترنت انجام شد این طرحها بر طبق نتایج جست و جو شامل ۴یا ۵ طرح است که در ادامه معرفی میگردند:[1]

مقالهٔ اول [24]:

A Hierarchical Approach for Modeling an MPLS Network Using VHDL

M. Minero-Muñoz, V. Alarcon-Aquino ,*Departamento de Ingeniería Electrónica, Universidad de las Américas, Puebla Sta. Catarina Mártir, Cholula, Puebla 72820 MEXICO*

در این مقاله اقدام به شبیه سازی یک شبکه MPLS با ۲۵۶ روتر و ۸ مسیر توسط VHDL گردیده است. در این مقالهٔ ۶ صفحه ای ارائه شده در IEEE نتایج شبیه سازی به طور مختصری توضیح داده شده است اما مرجعی برای دسترسی به کدها ارائه نگردیده است. بخش عمدهٔ مقاله شامل توضیحات کلی قضیه است و شبیه سازی در ۱-۲ صفحه آورده شده است.

مقالهٔ دوم [25]:

A HARDWARE/SOFTWARE CO-DESIGN FOR RSVP-TE MPLS

Raymond Peterkin
School of Information Technology and Engineering (SITE)
University of Ottawa
email: peterkin@site.uottawa.ca

Dan Ionescu
School of Information Technology and Engineering (SITE)
University of Ottawa
email: ionescu@site.uottawa.ca

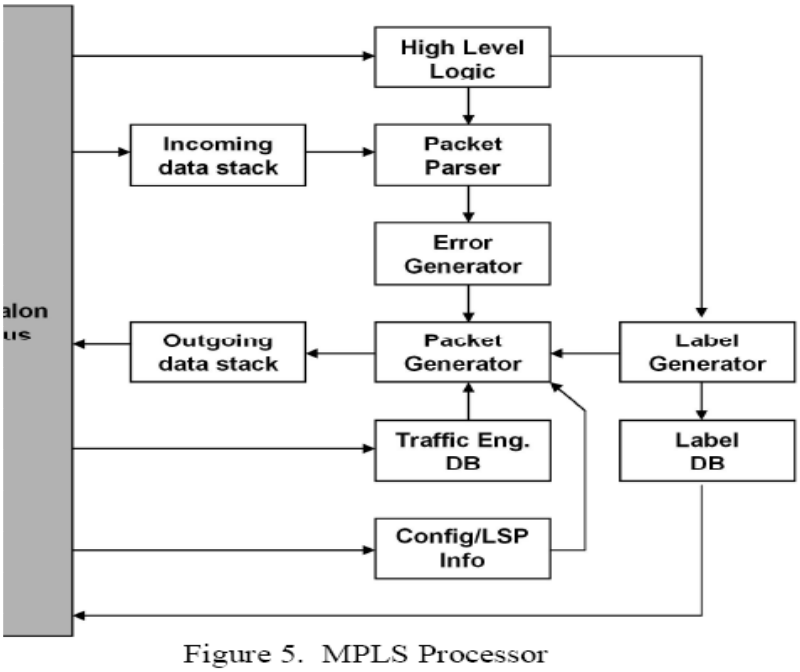


Figure 5. MPLS Processor

در این مقاله یک روتر MPLS با استفاده از در نظر گرفتن RSVP-TE به عنوان پروتکل سیگنالینگ آن طراحی شده است در این مقالهٔ ۴ صفحه ای ارائه شده در IEEE تنها نمائی کلی از معماری و نتیجهٔ شبیه سازی ارسال یک پاکت آورده شده است:

[1] پاسخ زیر جواب یکی از مهندسان شرکت سیسکو است که در جواب سؤالی برای امکان پیاده کردن پروتکلهای سطح بالائی مانند OSP روی یک چیپ FPGA یا ASIC است که نشاندهندهٔ غیرعملی بودن این مسئله در شرایط حاضر است:

"If you figure out to do a OSPF on a FPGA don't forget to sell it for big bucks to Cisco and Juniper!"

مقالهٔ سوم [26]:

شرکت Altera نیز اقدام به ارائه یک راهنما یا مقاله ۱۲ صفحه ای کرده است هدف این راهنما نه طراحی روتر بلکه معرفی امکانات شرکت برای یک چنین کاری است در این راهنما باسهای Avalon شرکت و مگافانکشنهای شرکت مانند CAM معرفی شده است ایدهٔ استفاده از CAM/RAM برای Label Swapper ازین مقاله گرفته شده است. در این راهنما چیپهای سری APEX نیز معرفی گردیده اند.

مقالهٔ چهارم [27]:

MPLS Forwarding Service APIs with Diffserv and TE Extensions Implementation Agreement

این در واقع یک توافق نامه برای طراحی است و در آن یکسری انواع داده و فانکشن تعریف شده تا مبنای کارهای مشترک قرار بگیرد این موافقت نامه یا توصیه نامه در این پروژه مورد استفاده و ملاک طراحی قرار نگرفت چون تمرکز این توافق نامه بر بخشهای دیگر مانند یکپارچگی در طراحی بخش طراحی پروتکلها و نوع و مشخصات کلاسهای برنامه نویسی است که در این پروژه مد نظر نیستند.

منبع پنجم[28]

تز کارشناسی ارشد:

SYSTEM ARCHITECTURE AND HARDWARE IMPLEMENTATIONS FOR A RECONFIGURABLE MPLS ROUTER

A Thesis Submitted to the College of Graduate Studies and Research in Partial Fulfillment of the Requirements for the Degree of Master of Science in the Department of Electrical Engineering University of Saskatchewan, Canada

By **Li Sha**

بخشهای مختلف این تز بدین شرح است:

Ch1. Introduction

Ch2. MPLS

Ch3. Reconfigurable MPLS Router Design Issues

Ch4. Reconfigurable MPLS Hardware Implementation

Ch5. Test Development and Procedures

Ch6. Test Result and Analysis

معماری ارائه شده در تز فوق با معماری ارائه شده در این پایان نامه به کلی متفاوت است ضمن آنکه این تز

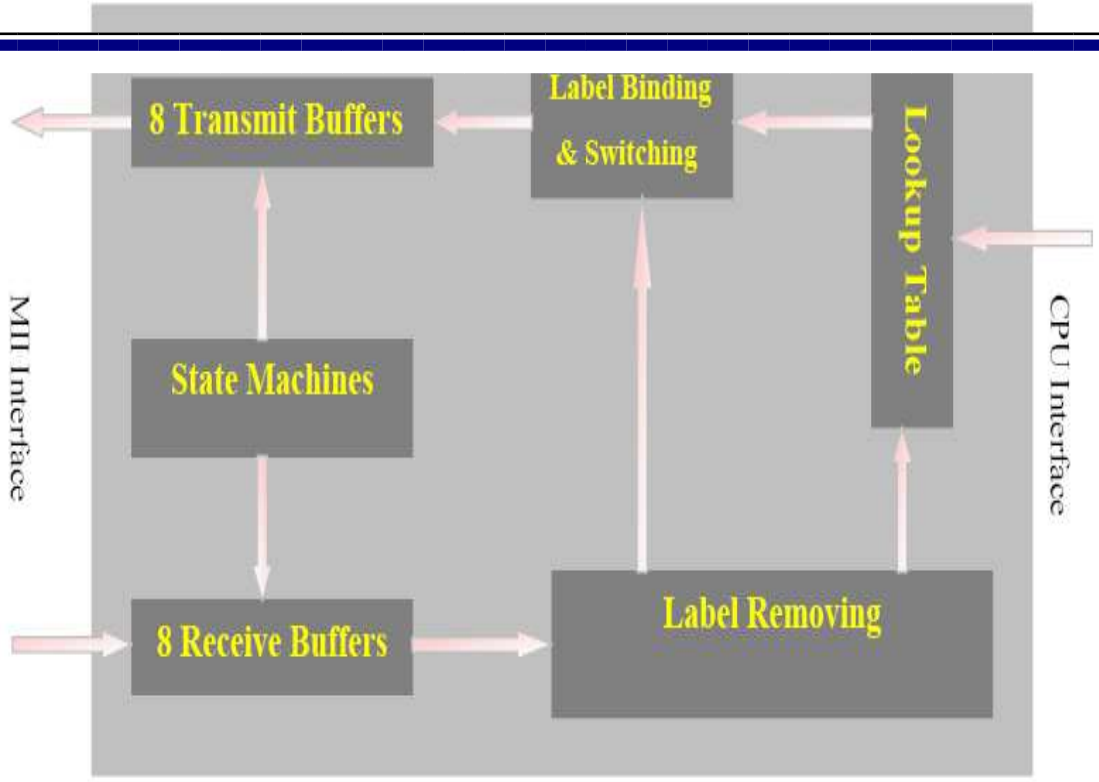


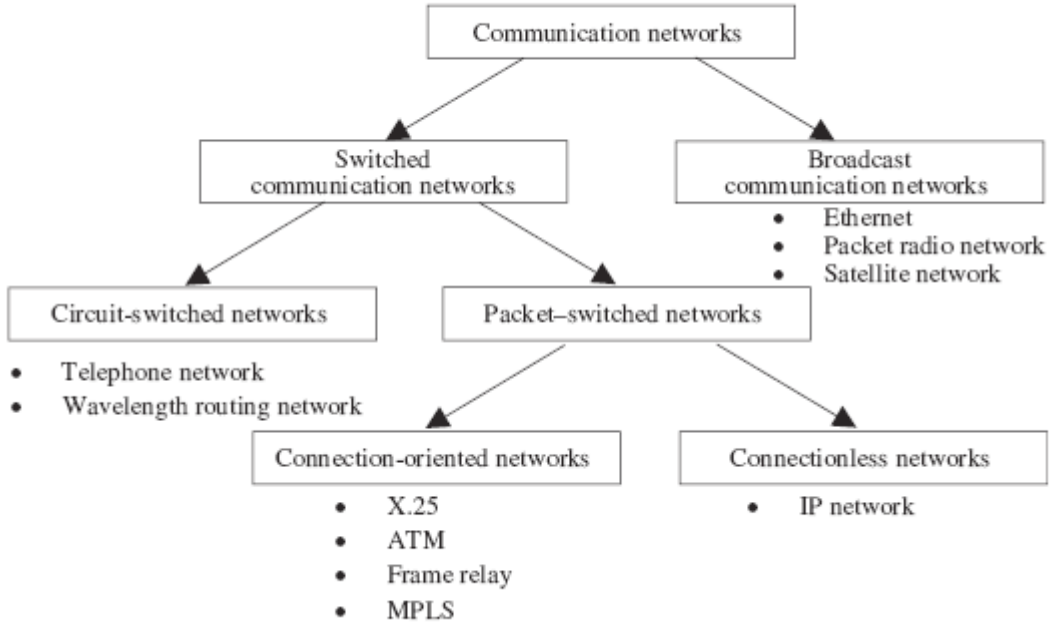
Figure 4-2 MPLS Functional Block Diagram

طراحی بر اساس Verilog انجام داده و بیشتر به بحثهای شبیه سازی عملکرد کلی شبکه و نه شبیه سازی خود روتر پرداخته است. ایدهٔ گرفته شده از این تز استفاده کردن از اترنت به عنوان تنها اینترفیس و تمرکز بر روی روند اصلی پروژه بود که در صفحهٔ ۵۶ تز علت استفاده کردن از تنها یک اینترفیس برخلاف روترهای تجاری توضیح داده شده است. این تز نیز برای مقایسه در لوح فشرده موجود است. در زیر معماری ارائه شده در تز آورده شده است. در این طرح نیز مانند پایان نامهٔ حاضر عملیات روتینگ نرم افزرای و به کمک یک پردازنده انجام گردیده است. در این طرح نیز از روش CAM/RAM استفاده شده است. متاسفانه در این تز کدهای Verilog HDL مورد استفاده برای بلوکها ضمیمه نشده اند. بهرحال این منبع مرتبط ترین منبع با پایان نامهٔ فعلی است که متاسفانه به خاطر نوع ارئه و فراهم آوردن سورس چندان مورد استفاده قرار نگرفت. در فصل بعدی به معماری ارائه شده توسط اینجانب با جزئیات کافی می پردازیم و در نهایت کدهای VHDL نیز ضمیمه خواهند شد:

شکل ٤.٢- بلوک دیاگرام تابعی MPLS

ضمیمهٔ ۱- مقدمه ای بر انواع شبکه های مخابراتی[۱]

شبکه های مخابراتی به دو گروه میتوانند تقسیم شوند: شبکه های switching و broadcasting ، خود شبکه های سوئیچینگ هم دو نوع اند Circuit Switching و Packet Switching . شبکهٔ تلفن یک نمونه از شبکه های Circuit Switching است، و از شبکه های Packet Switching میتوان به IP و ATM و Frame Relay و MPLS یاد کرد. از شبکه های broadcast هم میتوان به ماهواره و اترنت (از دیدگاهی) یاد کرد. Packet Switching خود به دو نوع Connection-less و Connection-Oriented تقسیم میشود از نوع بدون اتصال میتوان به شبکهٔ IP اشاره کرد و از انواع اتصال-گرا میتوان به ATM و X.25 و F.R و MPLS اشاره کرد.



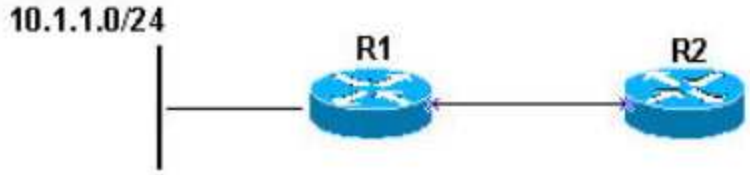
به طور خلاصه و از جهت آشنائی برای این انواع مختلف میتوان اینگونه گفت که: در شبکه های Circuit Switching ابتدا شبکه بین دو گره نهائی باید یک کانال اختصاص دهد و این کار معمولا سه بخش دارد: ایجاد مدار، انتقال دیتا، قطع مدار، که به خوبی بدون توضیحی اضافی در مثال تلفن کردن به یک شماره و صحبت کردن و سپس قطع کردن کاملا مشخص است آنچه که ویژگی این دسته از شبکه هاست اختصاص دادن کانال به طور اختصاصی به دو مشترک است حتی اگر دیتائی رد و بدل نشود در کل میتوان گفت در این شبکه های از مفهوم channel sharing خبری نیست. بهمین جهت سوئیچنگ مداری گزینهٔ مناسبی برای انتقال صوت است که در مقابل تاخیر حساس است و کیفیت را پائین می آورد ازینرو معمولا شبکه هائی که درگیر با انتقال

[۱] این بخش بخشی خلاصه است که بر اساس مقدمهٔ کتاب Connection Oriented Networks نوشته شده است با مراجعه به آن کتاب میتوان به شکل مفصل تری از مباحث مرتبط آگاهی یافت در اینجا تنها سعی شد نکات مهم و مورد نظر بر اساس مقدمهٔ کتاب بازنویسی و خلاصه شوند.

صوت بوده اند ازین نوع اند مانند شبکه تلفن و همچنین GSM در تلفن همراه. این درحالیست که در شبکه های Packet switching اطلاعات به شکل بسته هائی بین گره ها حرکت کرده تا به گره مقصد برسند در این شبکه ها معمولا مفاهیم کنترل خطا و Virtual Circuit و در کل ایدهٔ به اشتراک گذاشتن یک کانال فیزیکی به چند مشترک به چشم میخورد. در بحث مدار مجازی نیز مانند مدار واقعی سه بخش ایجاد، انتقال و قطع تماس وجود دارد. شبکه های مبتنی بر سوئیچینگ پاکتی که امکان Virtual Circuit را فراهم میکنند شبکه های اتصال گرا می گویند و شبکه ای مثل IP که بسته ها بدون ایجاد یک مدار مشخص در شبکه پخش میشوند و توسط سوئیچنگ روترها به مقصد میرسند شبکه های بدون اتصال میگویند. در این شبکه هر گره هر وقت که بخواهد بسته را میفرستد و با توجه به سرآیندهای موجود در بسته به مقصد هدایت میشود همچنین مکانیسمهائی نیز برای خطا تعبیه میشود. شبکه های broadcast نیز همانطور که از اسم آن مشخص است یک کانال بین همهٔ ایستگاهها مشترک شده و فرستنده اطلاعات را روی آن کانال میفرستد و مشترکین مجاز (در صورت آبونمانی بودن) نیز آن را دریافت میکنند.

ضمیمهٔ ۲- روتر بالادستی و پائین دستی

کلمات Upstream که به بالادست جریان یا مختصرا بالادست ترجمه شده است و همچنین Downstream که به پائین دست جریان یا به طور خلاصه پائین دست ترجمه شده اند کلماتی مهم و پرکاربرد در حیطهٔ MPLS هستند و معمولا با FEC در ارتباط هستند. مثال زیر را در نظر بگیرید:

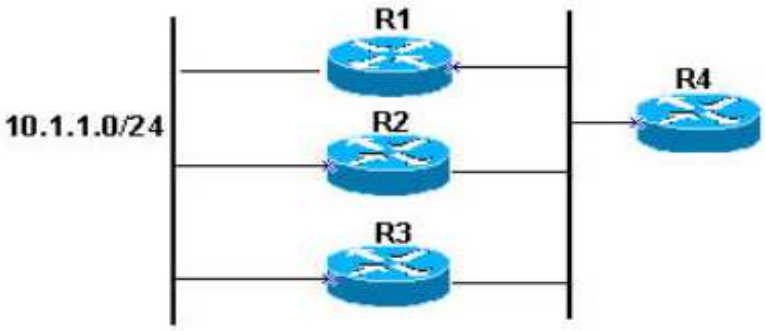


برای FEC مشخص شده یعنی 10.1.1.0/24 روتر R1، روتر پائین دست جریان برای R2 است.

برای FEC مشخص شده، روتر R2 بالادست جریان برای R1 است.

به همچنین R1 روتر پائین دست R2 و R2 روتر پائین دست R3 برای FEC مشخص شده است.

در اینجا نیز R1، روتر پائین دستِ R2 برای FEC مشخص شده با 10.1.1.0/24 است و به عکس، R2، روتر پائین دستِ R1 برای FEC مشخص شده با آدرس 10.2.2.0/24 می باشد.



جدول مسیریابیِ روتر R4 روترهای R1 و R2 را برای دسترسی به FEC محتوی 10.1.1.0/24 به عنوان next-hop دارد.[29]

در کل میتوان گفت جریان دادهٔ کاربر از روتر بالادست به پائین دست جریان حرکت میکند. وظیفهٔ عملیات تخصیص برچسب در MPLS به عهده مسریاب پائین دستی است. به عبارت دیگر میتوان گفت که در MPLS عملیات تخصیص برچسب در جهت معکوس و از سمت مسیریاب پائین دستی به سمت مسیریاب بالادستی انجام میشود.

منابع

[1]. (Online), Telephone Switches, http://technology.niagarac.on.ca/staff/mcsele/TelephoneSwitch.html Accessed: May 2008

[2]. (Online), SEG Communications, The Strowger Telecomms Page, http://www.seg.co.uk/telecomm/index.htm
Accessed: May 2008

[3]. (Online), The Spiritus Temporis Web Ring Community, http://www.spiritus-temporis.com/x.25/history.html Accessed: May 2008

[4]. (Book), "**Internetworking Technologies Handbook",** Cisco Systems , X.25, Ch17

[5]. (Online), Enterprise Network Planet, http://www.enterprisenetworkingplanet.com/netsp/article.php/951371 Accessed: May 2008

[6]. (Online), Wikipedia, http://en.wikipedia.org/wiki/X.25

[7]. (Book), **"X.25 and related protocols",** IEEE, 1991

[8]. (Online), A History of ATM, http://ntrg.cs.tcd.ie/undergrad/4ba2/atm/ATMhist.html Accessed: May 2008

[9]. (Online), Wikipedia, http://en.wikipedia.org/wiki/Frame_Relay Accessed: May 2008

[10]. (Book), "**Internetworking Technologies Handbook",** Cisco Systems , Frame Relay

[11]. (Book), "**Internetworking Technologies Handbook",** Cisco Systems , SMDS, Ch14

[12]. (Book), "**ATM Interworking; In Broadband Wireless Application"**; *auth. Sreetharan M. and S. Subramaniam:* ARTECH House, 2002.

[13]. (Book), "**Connection Oriented Networks, SONET/SDH, ATM, MPLS and Optical Networks"**; *Harry G.Perros*: John Wiley & Sons, ltd; 2005

[14]. (Online), Network Computing Web Site, http://www.networkcomputing.com/showArticle.jhtml?articleID=17601103 Accessed: May 2008

[15]. (Online), http://www.mplsrc.com/faq1.shtml

[16]. (Online), Alain Nguyen at ShopforBandwidth.com Accessed: May 2008

[17]. (Online), Shop for bandwidth, http://www.send2press.com/newswire/2007-05-0503-002.shtml Accessed: May 2008

[18]. (Report), MPLS Inter-Carrier Interconnection (MPLS-ICI) Backgrounder , MPFA Forum

[19]. (Book), **"The history of MPLS and its precursors"**, *Davie Rekhter and Doyle Kolon, 2001*
[20]. RFC3945

[21]. (Book), **"MPLS-Enabled Applications, Emerging Development and New Technologies";** *Ina Minei & Julian Lucek:* Wiley, 2005

[22]. (Article), **"Packet Transport Trends: IP/MPLS Success Challenged as Deployment Footprint Expand";** *Mark Seery, Ovum*: Industry Analyst Forum, July 2008

[23]. (Online), Wikipedia, http://en.wikipedia.org/wiki/Asynchronous_Transfer_Mode Accessed: May 2008

[24]. (Article), **"A Hierarchical Approach for Modeling an MPLS Network Using VHDL";** *M. Minero-Muñoz, V. Alarcon-Aquino ,Departamento de Ingeniería Electrónica:* Universidad de las Américas, Puebla Sta. Catarina Mártir, Cholula, Puebla 72820 MEXICO

[25]. (Article), **"A HARDWARE/SOFTWARE CO-DESIGN FOR RSVP-TE MPLS";**
Raymond Peterkin, email: peterkin@site.uottawa.ca
Dan Ionescu, email: ionescu@site.uottawa.ca
School of Information Technology and Engineering (SITE), University of Ottawa

[26]. (Article)**," Implementing Multiprotocol Label Switching with Altera PLDs",** Application Note 132, Altera Corporation.

[27]. (Book), **“MPLS Forwarding Service APIs with Diffserv and TE Extensions Implementation Agreement”,** Network Processing Forum, *Manikantan Srinivasan,* manis@futsoft.com
Reda Haddad, reda.haddad@ericsson.com
Copyright 2003 revision 1.0

[28]. (Proposal), **“SYSTEM ARCHITECTURE AND HARDWARE IMPLEMENTATIONS FOR A RECONFIGURABLE MPLS ROUTER”**
A Thesis Submitted to the College of Graduate Studies and Research in Partial Fulfillment of the Requirements for the Degree of Master of Science in the Department of Electrical Engineering University of Saskatchewan, Canada
By Li Sha

[29]. (Article**),” Cisco − MPLS FAQ For Beginners”,** DocID:4649, Cisco

[30]. (Article), **“Content-Addressable Memory (CAM) Circuits and Architectures: A Tutorial and Survey”** *Kostas Pagiamtzis, Student Member, IEEE, and Ali Sheikholeslami, Senior Member, IEEE*

Abstract
This proposal is a study to design an architecture for a Label Switch Router, LSR, which considered as the building block of Multi-Protocol Label Switching or MPLS. MPLS itself has many applications today and intensively under developing. In addition, MPLS is the first candidate for Next Generation Networks or NGN.
In flexible-oriented demands of routers' market, flexibility is a key factor in addition to economical production cost. Currently routers and their variant, and changing protocols and also functionalities have been implemented on a General Purpose Platform by companies to satisfy flexibility and economical characteristics of a demanded commercial router.
Designed LSR in this proposal as it will be seen, belongs to new generation of Reconfigurable routers that have been developing inside academic circles during these days with the advent of PLD's and FPGA's technologies to new horizons in recent years.
This Proposal aimed to design an MPLS Router and then Implementing that with the help of VHDL codes to providing SoC-Oriented design for being used on a FPGA chip. In this design, in addition to providing MPLS' concepts in relevant chapter, an structural architecture has been proposed with the spirit of Reconfigurable Computing in it's Router Component and then simulation and analyzing results has been demonstrated. Using FPGA and if possible -due to the size and practical limitation- SoC design, brings flexibility and speed to the router.
Routers mainly have two components: Forwarding Components, and Routing Components. In addition, a third component as Common Control Component has been added to the design. All these components has been described in a relevant chapter.
In this proposal Routing Component has been implemented on a soft-core, because of its variant, and developing nature to maintain the Reconfigurablity of the router. In designed router, deploying desired, variant, and always developing routing protocols have been supposed with the help of provided platform that designed to satisfy this task. Writing or designing the High-Level algorithm of routing protocols has not been considered in this proposal.