به نام خدا

مهندسی اینترنت

حبیب اله خسروی

۱. مفهوم تأخیر در شبکه

قبلاً گفته شد که یک بسته در مسیر خود از سیستم انتهایی مبدأ به سیستم انتهایی مقصد، از مجموعه‌ای از مسیریاب‌ها عبور می‌نماید. به ازای جابه‌جایی یک بسته بین دو گره در شبکه (میزبان یا مسیریاب)، انواع مختلفی از تأخیر بر بسته‌ی عبوری تحمیل می‌گردد که بر مجموع زمان سپری شده بین مبدأ و مقصد بسته مؤثر است. مهمترین انواع تأخیر عبارتند از تأخیر پردازشی هر گره [۱]، تأخیر صف [۲]، تأخیر انتقال [۳] و تأخیر انتشار [۴].

- تأخیر پردازشی: این تأخیر شامل زمان صرف شده برای بررسی آدرس مقصد بسته و تعیین لینک خروجی بسته می‌باشد (ممکن است مسائل دیگری مانند بررسی خطا در بسته نیز مشمول این تأخیر شوند). این تأخیر معمولاً در حد چند میکروثانیه یا کمتر می‌باشند.

- تأخیر صف: قبل از هر لینک خروجی از یک مسیریاب یک صف (یک بافر) قرار داده شده است. پس از ورود یک بسته به مسیریاب و پس از تعیین لینک خروجی به سمت مقصد بسته، در صورتی که لینک خروجی مشغول به انتقال بسته‌ی دیگری باشد و یا اینکه از قبل تعدادی بسته در صف در انتظار انتقال باشند، بسته‌ی جدید باید در صف خروجی منتظر بماند که به آن تأخیر صف گفته می‌شود. مدت زمان مربوط به تأخیر صف به تعداد بسته‌هایی که از قبل در صف در حال انتظار هستند وابسته می‌باشد. در صورتی که صف خالی باشد و هیچ بسته‌ی دیگری در حال انتقال نباشد، تأخیر صف برابر با صفر خواهد بود. تأخیر صف می‌تواند در حد چند میکروثانیه تا چند میلی‌ثانیه باشد.

- تأخیر انتقال: این تأخیر به صورت مدت زمان مورد نیاز برای قرار دادن کل بیت‌های یک بسته بر روی لینک تعریف می‌گردد. در صورتی که طول یک بسته برابر با L بیت باشد و نرخ بیتی انتقال برای لینک مورد نظر نیز برابر با R بیت بر ثانیه (b/s) باشد، تأخیر انتقال برابر با L/R خواهد بود. لازم به ذکر است که تأخیر انتقال به دلیل خاصیت store-and-forward در تجهیزات شبکه‌ای به وقوع می‌پیوندد. در واقع، تجهیزات شبکه مانند مسیریاب‌ها به منظور فراهم‌سازی شرایط بررسی ویژگی‌های بسته‌ها، ابتدا آنها را به طور کامل از لینک ورودی دریافت می‌کنند و سپس اولین بیت آنها را بر روی لینک خروجی قرار می‌دهند و به این عمل store-and-forward گفته می‌شود. به تأخیر انتقال تاخیر store-and-forward نیز گفته می‌شود.

---

[1] Nodal Processing Delay
[2] Queuing Delay
[3] Transmission Delay
[4] Propagation Delay

- تأخیر انتشار: مدت زمان مورد نیاز برای **یک بیت** به منظور انتشار از ابتدا تا انتهای یک لینک (مدت زمان سفر کردن یک بیت در لینک فیزیکی) به عنوان تأخیر انتشار شناخته می‌شود. بیت مورد نظر با سرعت انتشار لینک مورد نظر جابه‌جا می‌شود که به ویژگی‌های فیزیکی و طراحی و ساخت لینک مورد نظر بستگی دارد (بین $2 * 10^8$ متر بر ثانیه تا $3 * 10^8$ متر بر ثانیه). تأخیر انتشار برابر با مسافت بین دو گره در شبکه تقسیم بر سرعت انتشار است. مثلاً در صورت که مسافت با d نمایش داده شود و v سرعت انتشار بر روی لینک باشد، تأخیر انتشار برابر با d/v خواهد بود. معمولاً در شبکه‌های WAN این تأخیر در حد چند میلی‌ثانیه است.

در مجموع می‌توان گفت که تأخیر وارد شده بر یک بسته به ازای هر گره موجود در شبکه برابر است با:

$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

که تأثیر هر کدام از آنها در کل تأخیر ایجاد شده متغیر است. به شکلی که ممکن است در یک شبکه تأخیر انتقال بیشترین تأثیر را در تأخیر کل ایجاد نماید و در یک شبکه‌ی دیگر، تأخیر انتشار بیشترین تأثیر را داشته باشد.

۲.افت بسته

در شرایط واقعی، صف قرار گرفته قبل از هر کدام از لینک‌های خروجی در یک مسیریاب از اندازه‌ی محدودی برخوردار است و ممکن است پُر شود. در نتیجه، یک بسته‌ی ورودی به شبکه ممکن است با وضعیت پر صف موجود قبل از لینک خروجی مواجه شود که باعث می‌شود مسیریاب بسته‌ی مورد نظر (یا یکی از بسته‌های حاضر در صف) را دور بیاندازد (drop) که در چنین شرایطی گفته می‌شود که افت بسته[5] رخ داده است. از دید سیستم‌های انتهایی، افت بسته بدین شکل مشاهده می‌شود که یک بسته به هسته‌ی شبکه انتقال یافته و هیچ‌گاه در مقصد خود مشاهده نشده است. هر چه ازدحام در شبکه افزایش یابد، میزان افت بسته‌ها نیز افزایش می‌یابد.

[5] Packet Loss

۳. گذردهی در شبکه‌های کامپیوتری

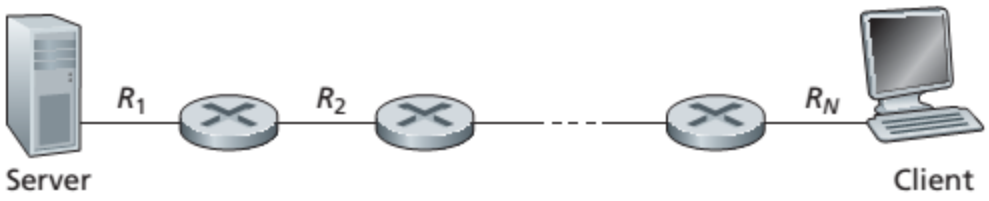
گذردهی[۶] لحظه‌ای در هر لحظه از زمان عبارت از نرخ بیتی دریافت اطلاعات در یک مقصد مشخص است. تشریح مفهوم گذردهی با استفاده از چند مثال و با بهره‌گیری از شکل ۱ و شکل ۲ و شکل ۳ انجام می‌شود.

شکل ۱ مثال اول مربوط به گذردهی در شبکه

شکل ۱ نمایش‌دهنده‌ی یک سیستم انتهایی کارخواه، یک سیستم انتهایی کارپذیر و یک مسیریاب است. ارتباط بین کارخواه و مسیریاب با یک لینک دارای نرخ بیتی برابر با R_c بیت بر ثانیه و ارتباط بین کارپذیر و مسیریاب با یک لینک دارای نرخ بیتی برابر با R_s بیت بر ثانیه برقرار شده است. حال شرایطی در نظر گرفته شود که کارخواه در حال دریافت (دانلود) یک فایل بزرگ از کارپذیر است. در صورتی که $R_s < R_c$ باشد، به دلیل اینکه امکان ارسال سریع‌تر داده‌ها برای کارپذیر وجود ندارد، داده‌ی مورد نظر با نرخ R_s بیت بر ثانیه وارد کارخواه می‌شود که برابر با گذردهی شبکه در شرایط فعلی است. اما در صورتی که $R_s > R_c$ باشد، مسیریاب نمی‌تواند داده‌ها را با همان نرخی که دریافت می‌کند (R_s) بر روی لینک خروجی ارسال کند و در نتیجه، داده‌ها با نرخ برابر با R_c بیت بر ثانیه به سمت مقصد ارسال می‌گردند. در چنین شرایطی، گذردهی شبکه برابر با R_c بیت بر ثانیه خواهد بود. به دلیل اینکه نرخ ورود داده‌ها به مسیریاب بیشتر از نرخ خروج آنها است، بیت‌های جمع‌شده در صف موجود پیش از لینک خروجی بیشتر و بیشتر شده که در نهایت باعث افت بسته‌ها می‌گردد.

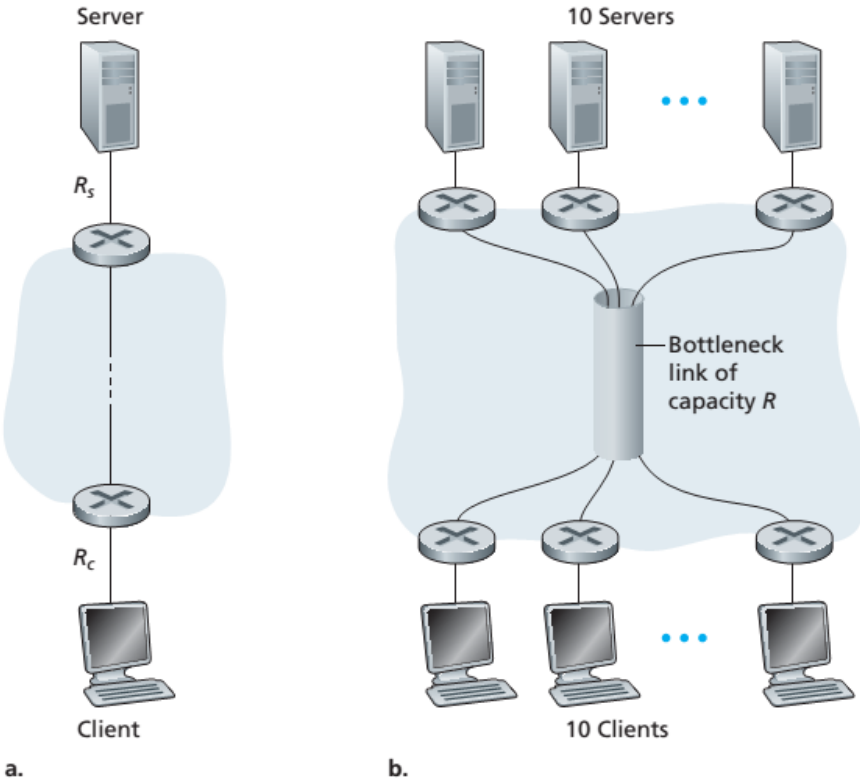
به عبارتی می‌توان گفت که گذردهی در شبکه‌ی مثال ذکر شده برابر با $\min\{R_c , R_s\}$ است که برابر با نرخ بیتی لینک گلوگاه یا لینک bottleneck است. در نتیجه، می‌توان زمان سپری شده برای انتقال یک فایل F بیتی به شبکه را به طور تقریبی با $F/\min\{R_s , R_c\}$ تخمین زد.

[6] Throughput



شکل ۲ مثال دوم مربوط به گذردهی در شبکه

شکل ۲ نمایش‌دهنده‌ی دو سیستم‌انتهایی کارخواه و کارپذیر است که با استفاده از یک شبکه‌ی حاوی چندین مسیریاب به هم متصل شده‌اند. گذردهی شبکه در چنین شرایطی برابر است با $\min\{R_1, R_2, \ldots, R_N\}$ که برابر با نرخ بیتی مربوط به لینک گلوگاه حاضر در مسیر بین کارپذیر و کارخواه است.



شکل ۳ مثال‌های سوم و چهارم مربوط به گذردهی در شبکه

بخش‌های (a) و (b) در شکل ۳ تأثیر شبکه‌های دسترسی و هسته‌ی شبکه را در بررسی گذردهی انتها به انتها دخیل می‌سازند. در بخش (a) نرخ بیتی لینک‌های دسترسی کارخواه و کارپذیر به هسته‌ی شبکه به ترتیب برابر با R_c و R_s هستند. نرخ بیتی هسته‌ی شبکه به قدری زیاد است که هیچ محدودیتی ایجاد نمی‌کند. در نتیجه، همچنان گذردهی در شبکه برابر با $\min\{R_s, R_c\}$ خواهد بود. بنابراین و با توجه به اینکه در اینترنت امروزی نرخ بیتی بکاررفته در هسته‌ی شبکه بسیار بیشتر از مقدار واقعی مورد نیاز است، می‌توان گفت که محدودیت اصلی و معمول، نرخ بیتی در شبکه‌های دسترسی می‌باشد.

در بخش (b) از شکل ۳ شرایطی نمایش داده شده است که در آن ۱۰ کارخواه به طور همزمان در حال دریافت اطلاعات از ۱۰ کارپذیر مجزا هستند. مشاهده می‌شود که ارتباط بین ۱۰ کارخواه و ۱۰ کارپذیر

از یک لینک مشترک در هسته‌ی اینترنت عبور می‌نماید. نرخ بیتی لینک دسترسی هر کدام از کارخواه‌ها به هسته‌ی شبکه برابر با R_c و نرخ بیتی لینک دسترسی هر کدام از کارپذیرها به هسته‌ی شبکه برابر با R_s بیت بر ثانیه است و نرخ بیتی لینک مشترک نیز برابر با R بیت بر ثانیه است. در صورتی که نرخ بیتی R برابر با، به طور مثال، چند صد برابر R_s و R_c باشد، مجدداً گذردهی شبکه برابر خواهد بود با $\min\{R_s, R_c\}$ اما، در صورتی که R مشخص کننده‌ی نرخ بیتی کمتری باشد، وضعیت متفاوت خواهد بود. به طور مثال فرض می‌شود که R_s برابر است با 2 Mbps و R_c نیز برابر است با 1 Mbps و نرخ بیتی لینک مشترک که برابر با 5 Mbps است به طور مساوی بین ۱۰ ارتباط دانلودی تقسیم می‌شود. در چنین شرایطی، لینک گلوگاه در هسته‌ی شبکه واقع است که باعث می‌شود گذردهی انتها به انتها برای هر کدام از ارتباط‌ها برابر با 512 kbps شود. بنابراین، مشاهده می‌شود که گذردهی شبکه علاوه بر نرخ بیتی لینک‌های حاضر در مسیر بین کارخواه و کارپذیر، به ترافیک مداخله‌کننده با ترافیک یک ارتباط نیز وابسته است.

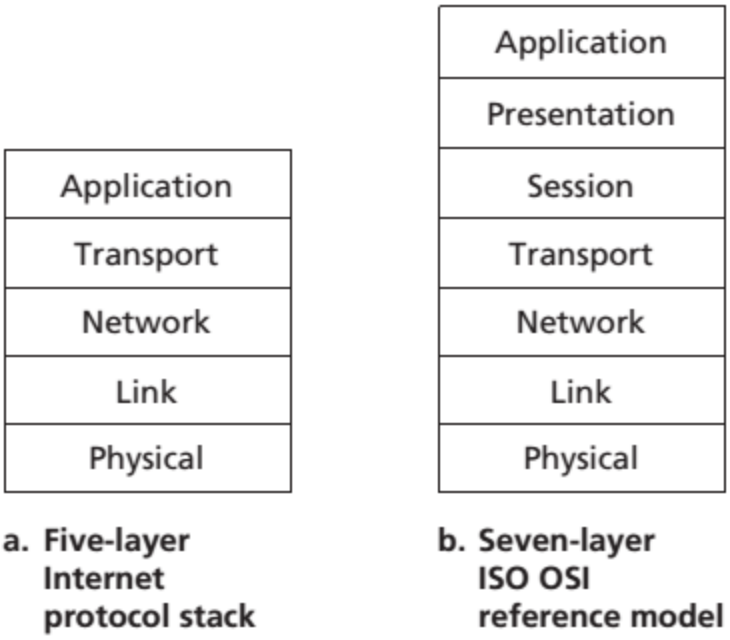
۴. پشته‌ی پروتکل استاندارد اینترنت: TCP/IP

کاملاً مشخص است که اینترنت یک سیستم بسیار پیچیده است و این پیچیدگی نیاز به مدیریت و سازمان‌دهی دارد. یکی از راه‌های مدیریت این پیچیدگی، تقسیم‌بندی پروتکل‌های بکاررفته در اینترنت در لایه‌های مختلف است.

در حقیقت، به منظور ساختاردهی به طراحی پروتکل‌های شبکه، طراحان شبکه پروتکل‌ها را در قالب لایه‌ها سازمان‌دهی می‌کنند. هر لایه مسئول فراهم‌سازی خدمت‌های مشخصی برای لایه‌ی بالاتر از خود است و از خدمت‌های ارائه شده توسط لایه‌ی پایین‌تر از خودش استفاده می‌نماید. در واقع، خدمت فراهم شده توسط هر لایه برای لایه بالاتر از آن، با اجرای مجموعه‌ای از اعمال مشخص در آن لایه و بهره‌گیری از خدمت‌های ارائه شده توسط لایه‌ی زیرین آن فراهم می‌شود. دستگاه‌های فیزیکی مختلفِ تشکیل‌دهنده‌ی یک شبکه باید مجموعه‌ای از لایه‌های مختلف شبکه را پیاده‌سازی نمایند.

از جمله مزایای تقسیم‌بندی پروتکل‌ها در قالب لایه‌های مختلف می‌توان به سازمان‌دهی مناسب پروتکل‌ها و در نتیجه، ایجاد شرایط مناسب برای بحث و تحلیل بخش‌های مختلف سیستم و همچنین، بروزرسانی ساده‌تر و مؤثرتر مجموعه پروتکل‌ها و اعمال اجرا شده در هر لایه به علت ساختار پیمانه‌ی ایجاد شده، اشاره نمود. از طرفی، تکرار یک عملکرد مشخص در چند لایه و نیاز به اطلاعات موجود در لایه‌های دیگر توسط یک لایه نیز از جمله ایرادات وارد شده بر تقسیم‌بندی پروتکل‌ها در لایه‌های مختلف هستند. شکل ۴

نمایش‌دهنده‌ی پشته‌پروتکل استاندارد اینترنت (TCP/IP) در کنار مدل مرجع لایه‌بندی پروتکل‌ها یا ISO OSI است. پشته‌ی پروتکل استاندارد اینترنت از پنج لایه‌ی کاربرد[۷]، انتقال[۸]، شبکه[۹]، پیوند[۱۰] و فیزیکی[۱۱] تشکیل شده است.



شکل ۴ مدل مرجع هفت لایه‌ی *OSI* در کنار پشته‌ی پروتکل پنج لایه‌ی اینترنت *TCP/IP*

- لایه‌ی کاربرد: برنامه‌های کاربردی شبکه‌ای و پروتکل‌های لایه‌ی کاربرد آنها در این لایه قرار داده می‌شوند. به بسته‌های تولید شده در این لایه message یا پیام گفته می‌شود.

- لایه‌ی انتقال: این لایه، پیام‌های تولید شده در لایه‌ی کاربرد را بین دو سیستم انتهایی حاضر در ارتباط انتقال می‌دهد (پروتکل‌های پیاده‌سازی شده در این لایه به صورت انتها به انتها[۱۲] عمل می‌کنند). دو پروتکل TCP و UDP در پشته‌ی پروتکل TCP/IP برای لایه‌ی انتقال مشخص شده‌اند که هر کدام خدمت‌های متمایزی را برای انتقال پیام‌های تولید شده در لایه‌ی کاربرد فراهم می‌سازد. از جمله خدمت‌های فراهم شده توسط TCP، کسب اطمینان از تحویل یک پیام به مقصد مورد نظر آن است. همچنین، این پروتکل راهکارهایی را برای کنترل میزان ازدحام و شلوغی در شبکه بکار می‌بندد. از طرفی، پروتکل UDP عملکرد ساده‌ای دارد و خدمت‌های اشاره شده را فراهم نمی‌سازد. بسته‌های لایه‌ی کاربرد به عنوان یک segment یا قطعه شناخته می‌شوند.

---

[7] Application
[8] Transport
[9] Network
[10] Link
[11] Physical
[12] End to End

- لایه‌ی شبکه: پروتکل بکاررفته در لایه‌ی انتقال (TCP یا UDP) یک segment را به همراه یک آدرس مقصد در اختیار لایه‌ی شبکه قرار می‌دهد. خدمت فراهم شده از طرف لایه‌ی شبکه برای لایه‌ی انتقال، تحویل segment مورد نظر به لایه‌ی انتقال در سیستم انتهایی حاضر در مقصد مشخص شده است. در واقع، وظیفه‌ی اصلی این لایه اجرای اعمال مربوط جابه‌جایی پیام‌های تولید شده در لایه‌ی کاربرد و گذر کرده از لایه‌ی انتقال (هر کدام از این لایه‌ها اعمال مشخصی را بر روی بسته‌ها اعمال می‌نمایند) به سمت مقصد آن، از طریق مجموعه‌ی گام‌ها و دستگاه‌های میانی است. بسته‌های تولید شده در این لایه با نام datagram یا دیتاگرام شناخته می‌شوند.

در پشته‌ی پروتکل TCP/IP از پروتکل IP برای لایه‌ی شبکه استفاده می‌شود که ساختار دیتاگرام‌های تولید شده و نحوه‌ی برخورد گره‌های شبکه (سیستم‌های انتهایی و مسیریاب‌ها) با آنها را مشخص می‌نماید. این لایه همچنین، شامل پروتکل‌های مسیریابی نیز هست که مسیر استفاده شده توسط یک دیتاگرام به سمت مقصد آن‌را تولید می‌نمایند.

به عبارتی می‌توان گفت که پروتکل IP مشابه یک چسب است که تمام اینترنت را به هم متصل می‌نماید.

- لایه‌ی پیوند: این لایه دیتاگرام‌های تولید شده در لایه‌ی شبکه را بین مجموعه‌ای از مسیریاب‌ها جابه‌جا می‌نماید. در واقع، لایه شبکه بر خدمت‌های ارائه شده توسط این لایه به منظور انتقال یک بسته از یک گره در مسیر (سیستم انتهایی یا مسیریاب) به گره بعدی تکیه می‌نماید. پس از انتقال دیتاگرام به گره بعدی در مسیر، لایه‌ی پیوند آن‌را مجدداً به لایه‌ی شبکه تحویل می‌دهد. از جمله پروتکل‌های لایه‌ی پیوند موجود، Ethernet، WiFi و PPP (پروتکل نقطه به نقطه) می‌باشند. این امکان وجود دارد که بین هر دو گره موجود در شبکه از پروتکل لایه‌ی پیوند متفاوتی استفاده شود. در نتیجه، لایه‌ی شبکه خدمت متفاوتی را از هر کدام از این پروتکل‌ها دریافت می‌نماید.

بسته‌های لایه‌ی پیوند با عنوان frame یا فریم شناخته می‌شوند.

- لایه‌ی فیزیکی: در حالی که لایه‌ی پیوند به جابه‌جایی کل یک فریم بین دو گره شبکه می‌پردازد، لایه‌ی فیزیکی مسئول انتقال تک‌تک بیت‌های موجود در فریم بین دو گره است. پروتکل‌های مختلف حاضر در این لایه بیت‌ها را به اشکال مختلفی بین دو گره شبکه منتقل می‌نمایند.

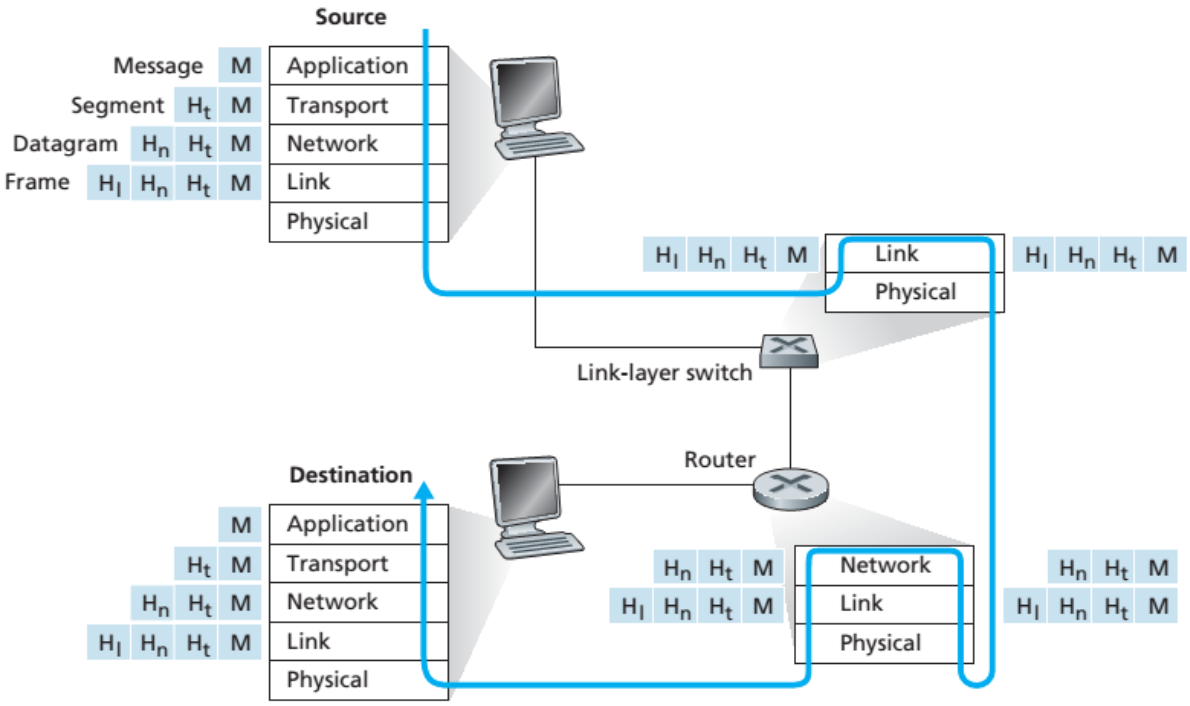
همان‌طور که در شکل ۴ مشخص است، پشته پروتکل مرجع OSI دو لایه‌ی نمایش[۱۳] و جلسه[۱۴] را بیشتر از پشته‌ی پروتکل TCP/IP دارد. لایه نمایش خدماتی را فراهم می‌سازد که به وسیله‌ی آنها برنامه‌های کاربردی می‌توانند مفهوم داده‌های جابه‌جا شده را درک نمایند. این خدمات شامل رمزنگاری داده‌ها،

[13] Presentation
[14] Session

فشرده‌سازی داده یا تشریح داده‌ها[15] است. لایه‌ی جلسه نیز به تعیین حدود و هماهنگ‌سازی اطلاعات جابه‌جا شده مربوط می‌شود که به اموری مانند ساخت الگوی بازیابی می‌پردازد.

همان‌طور که گفته شد، دو لایه‌ی نمایش و جلسه از پشته‌ی پروتکل TCP/IP حذف شده است. بکارگیری خدمت‌های مشخص شده توسط آنها و پیاده‌سازی اعمال مربوط به آنها بر عهده‌ی برنامه‌نویس یک برنامه‌ی کاربردی در اینترنت است. بدین معنی که این دو لایه در لایه‌ی کاربرد ترکیب شده‌اند.

شکل ۵ نمایش‌دهنده‌ی مسیری است که داده‌ها در یک شبکه‌ی مثال طی می‌نمایند. داده‌ها مسیری رو به پایین را در پشته‌ی پروتکل پیاده‌سازی شده در سیستم‌انتهایی مبدأ، مسیری رو به بالا و سپس رو به پایین را در سوئیچ‌های بسته‌ای (سوئیچ لایه‌ی پیوند یا مسیریاب) حاضر در بین مسیر و مسیری رو به بالا را در پشته‌ی پروتکل پیاده‌سازی شده در سیستم انتهایی مقصد طی می‌نمایند. همان‌طور که مشاهده می‌شود، لایه‌های انتقال و کاربرد توسط سوئیچ‌های بسته‌ای (مسیریاب‌ها و سوئیچ‌های لایه‌ی پیوند) پیاده‌سازی نمی‌گردند. در واقع، این دو لایه پروتکل‌های مربوط به خدمت‌های انتها به انتها را پیاده‌سازی می‌نمایند. مسیریاب‌های حاضر در مسیر تا لایه‌ی شبکه و سوئیچ‌های لایه‌ی پیوند (از این پس به این دستگاه‌ها فقط «سوئیچ» گفته می‌شود) فقط تا لایه‌ی پیوند را پیاده‌سازی می‌کنند. در نتیجه، می‌توان گفت که یک مسیریاب قابلیت پیاده‌سازی پرتکل IP را دارد ولی، یک سوئیچ این قابلیت را ندارد.



شکل ۵ مسیر طی شده توسط داده‌ها بین دو سیستم انتهایی مبدأ و مقصد و سوئیچ‌های بسته‌ای حاضر در مسیر

[15] Data Description

در شکل ۵ مشاهده می‌شود که پیام یا message تولید شده در لایه‌ی کاربرد (M) وارد لایه‌ی انتقال شده و توسط پروتکل بکاررفته در این لایه، اطلاعات اضافی (H_t که به آن سرآیند[۱۶] لایه‌ی انتقال نیز گفته می‌شود) به آن الصاق شده است. اطلاعات اضافی الصاق شده به بسته، توسط لایه‌ی انتقال در سیستم انتهایی مقصد مورد استفاده قرار می‌گیرد و ممکن است حاوی اطلاعات لازم برای تحویل پیام لایه‌ی کاربرد به برنامه‌ی کاربردی درست و مشخص در مقصد باشد. در واقع، سرآیند لایه‌ی انتقال راه‌حل بکاررفته برای مکاتبه بین دو لایه‌ی انتقال در مبدأ و مقصد است. مجموعه‌ی پیام لایه‌ی کاربرد و سرآیند اضافه شده در لایه‌ی انتقال با عنوان segment شناخته می‌شوند. می‌توان گفت که segment لایه‌ی انتقال پیام لایه‌ی کاربرد را کپسوله‌سازی[۱۷] کرده است.

در ادامه، لایه‌ی شبکه نیز سرآیند مخصوص به خود (H_n) را به segment لایه‌ی انتقال اضافه می‌کند و تشکیل یک دیتاگرام می‌دهد. دیتاگرام تولید شده وارد لایه‌ی پیوند شده و پس از دریافت سرآیند مخصوص لایه‌ی پیوند (H_l) یک فریم را تولید می‌نماید.

بدین ترتیب، در هر لایه از شبکه، یک بسته شامل دو بخش می‌باشد. یک بخش سرآیند اضافه شده توسط آن لایه است و بخش دیگر نیز، payload یا بار مفید بسته است که از لایه‌ی بالاتر وارد آن لایه شده است و به آن PDU[۱۸] نیز گفته می‌شود.

۵.مسیریاب

مسیریاب[۱۹] یک دستگاه شبکه‌ای است که بسته‌های داده را بین شبکه‌های مختلف هدایت می‌کند. یک مسیریاب به دو یا چند لینک ارتباطی متعلق به شبکه‌های مختلف متصل می‌باشد و زمانی که یک بسته‌ی جدید از یک لینک ارتباطی وارد مسیریاب می‌شود، مسیریاب آدرس ثبت شده در بسته را به منظور تعیین مقصد آن بررسی می‌کند. سپس، با استفاده از اطلاعات موجود در جدول پیش‌رانی[۲۰] و سیاست‌های مسیریابی، بسته را به شبکه‌ی بعدی هدایت می‌کند. استفاده از یک مسیریاب باعث جداسازی شبکه‌های محلی مختلف می‌شود به شکلی که هرکدام از واسطهای شبکه‌ی مسیریاب در یکی این شبکه‌های محلی متصل به آن واقع است.

16 Header
17 Encapsulation
18 Protocol Data Unit
19 Router
20 Forwarding Table

با توجه به اینکه وظیفه‌ی لایه‌ی شبکه جابجایی بسته‌ها از یک میزبان ارسال‌کننده به یک میزبان دریافت‌کننده است و با توجه به اینکه یک مسیریاب یک دستگاه متعلق به این لایه می‌باشد، مسیریاب‌ها دو نقش پایه را ایفا می‌نمایند. یکی از این دو عملکرد پایه، هدایت بسته‌های بین واسط‌های شبکه‌ایِ متصل به مسیریاب (سوئیچینگ لایه‌ی ۳ یا پیش‌رانی) است و دیگری، مبادله‌ی اطلاعات دسترسی‌پذیری بین مسیریاب‌ها (مسیریابی[۲۱]) است.

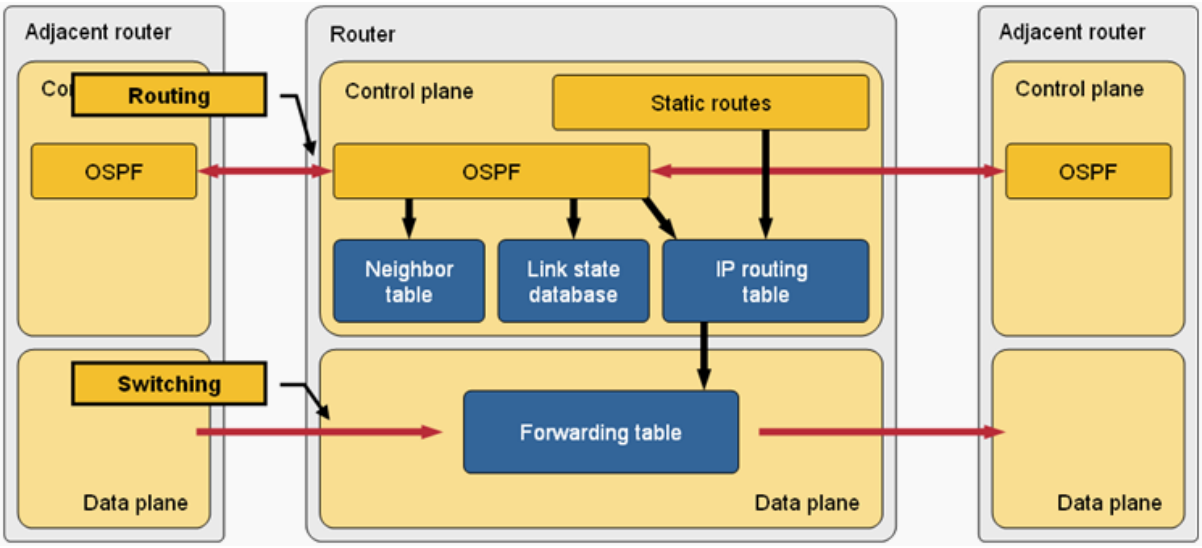
زمانی که یک بسته وارد یکی از لینک‌ّهای ورودی مسیریاب می‌شود، مسیریاب مورد نظر باید آن بسته را از طریق یک لینک خروجی به سمت مقصد ارسال نماید. به عمل انتقال یک بسته از یک لینک ورودی به لینک خروجی مناسب آن که یک عمل داخلی (local) برای مسیریاب محسوب می‌شود، پیش‌رانی (Forwarding) گفته می‌شود. از طرفی، مسیریابی (Routing) به فرایند تعین یک مسیر انتها به انتها در گستره‌ی شبکه اشاره می‌کند که توسط بسته‌ها به منظور رسیدن به مقصد مورد استفاده قرار می‌گیرد. به الگوریتم‌هایی که مسیرها را تولید می‌کنند، الگوریتم مسیریابی گفته می‌شود.

همان‌طور که پیش‌تر گفته شد، یک مسیریاب پس از بررسی یک مقدار مشخص در سرآیند بسته‌ی عبوری و سپس، استفاده از جدول هدایت موجود در مسیریاب، لینک خروجی مناسب برای بسته را انتخاب می‌نماید. در واقع، الگوریتم مسیریابی به منظور تعیین مقادیر موجود در جدول مسیریابی مورد استفاده قرار می‌گیرد. ممکن است در شبکه‌های مختلف، الگوریتم مسیریابی به صورت متمرکز[۲۲] (به صورت جدا از مسیریاب‌ها و در یک دستگاه دیگر) یا غیرمتمرکز[۲۳] (یک الگوریتم توزیع شده در دستگاه‌های مختلف) پیاده‌سازی شود. در هر حال، مسیریاب پیام‌هایی را دریافت می‌کند که می‌تواند از آنها برای پیکربندی جدول هدایت درون آن استفاده نماید.

سوئیچینگ یا پیش‌رانی[۲۴] در بخش داده[۲۵] از یک مسیریاب انجام می‌شود و مسیریابی نیز در بخش کنترل[۲۶] اجرا می‌شود. در واقع، تمام هوش یک مسیریاب شامل پروتکل‌های مسیریابی در بخش کنترل گردآوری شده است. در نتیجه‌ی مبادله‌ی اطلاعات مشخص بین بخش‌های کنترل موجود در مسیریاب‌های مختلف (اطلاعات مورد نظر بسته به نوع پروتکل مسیریابی متفاوت می‌باشند)، جداول پیش‌رانی موجود در مسیریاب‌ها تکمیل می‌گردند. در نهایت، با ورود بسته‌های شبکه به یک مسیریاب، بخش داده با بررسی جدول پیش‌رانی اقدام به پیش‌رانی بسته به سمت مقصد مشخص شده توسط آن از طریق مناسب‌ترین لینک خروجی

21 Routing
22 Centralized
23 Decentralized
24 Forwarding
25 Data Plane
26 Control Plane

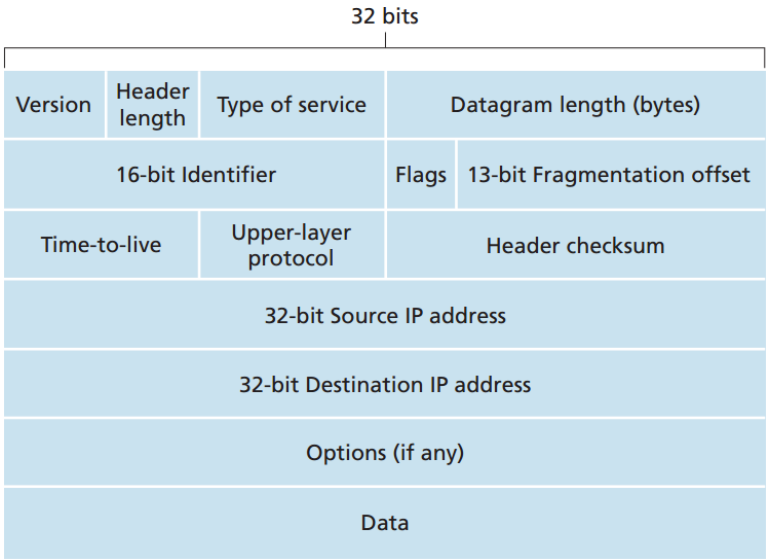
می‌نماید. شکل ۶ نمایش‌دهنده‌ی دو بخش داده و کنترل و همچنین، اجرای اعمال هدایت (Forwarding یا Switching) و مسیریابی (Routing) می‌باشد.



شکل ۶ ساختار مسیریاب و تقسیم‌بندی آن به دو بخش کنترل و داده

۶. قالب یک بسته‌ی IP

یک بسته‌ی IP از دو قسمت سرآیند (Header) و بار مفید (Payload) تشکیل شده است. اطلاعات موجود در سرآیند توسط هر مسیریاب حاضر در مسیر بسته مورد استفاده قرار می‌گیرد.



شکل ۷ قالب یک بسته‌ی *IP*

شکل ۷ نمایش‌دهنده‌ی قالب یک بسته‌ی IP است. در ادامه، بخش‌های مختلف یک بسته‌ی IP و کاربرد آنها معرفی می‌شوند.

- فیلد Version: یک فیلد چهار بیتی است که نسخه‌ی پروتکل IP را مشخص می‌کند. به طور مثال، پروتکل IP نسخه‌ی چهار با عدد 0100 و پروتکل IP نسخه‌ی شش با عدد 0110 مشخص می‌شوند.

- فیلد Header Length: این فیلد هم چهار بیتی است و طول کل سرآیند بسته را بر مبنای کلمات ۳۲ بیتی مشخص می‌نماید. به طور مثال، در صورتی که عدد ۱۰ در این فیلد قرار گرفته باشد، نشان‌دهنده‌ی ۳۲۰ بیت است که یک سرآیند ۴۰ بایتی را مشخص می‌نماید. لازم به ذکر است که طول قسمت اجباری سرآیند (بدون فیلد Options) برابر با ۲۰ بایت است. در نتیجه، حداقل مقداری که در این فیلد قرار می‌گیرد برابر با ۵ است. همچنین، با توجه به اینکه طول این فیلد برابر با ۴ بیت است، حداکثر می‌تواند شامل عدد ۱۵ (1111) باشد که در این صورت حداکثر طول کل قسمت سرآیند برابر با ۶۰ بایت خواهد بود که ۲۰ بایت آن اجباری و ۴۰ بایت آن اختیاری است.

- فیلد Type of Service: این فیلد ۸ بیتی است و توسط ماشین مبدأ بسته و به منظور درخواست یک خدمت ویژه از مسیریاب‌های حاضر در مسیر تا مقصد مورد استفاده قرار می‌گیرد. جدول 1 نمایش‌دهنده‌ی معنی و کاربرد مقادیر بکاررفته برای هر کدام از این ۸ بیت می‌باشد.

همانطور که مشاهده می‌شود، ۳ بیت سمت چپ تقدم و اولویت بسته را مشخص می‌کنند. هر چه این ۳ بیت مقدار بزرگ‌تری را شامل شود، بسته از اولویت بالاتری برخوردار خواهد بود و مسیریاب آن‌را پیش از سایر بسته‌ها ارسال می‌نماید. بیت D بدین معنی است که بسته‌ی مورد نظر تحمل پایینی نسبت به تأخیر دارد و مسیریاب بهتر است آن‌را از مسیرهای دارای تأخیر کمتر ارسال کند. بیت T نیاز بسته به گذردهی بالا را مشخص می‌کند و بیت R نیز، باعث می‌شود که مسیریاب از دور انداختن بسته‌ها اجتناب نماید. برای دو بیت آخر نیز هیچ کاربردی تعریف نشده است (ممکن است برای موارد خاص استفاده قرار گیرند؛ مثلاً بیت هفتم مربوط به هزینه است).

جدول *1* قالب فیلد ۸ بیتی *Type of Service*

P2	P1	P0	D	T	R	-	-
تقدم بسته			تأخیر	ظرفیت خروجی	قابلیت اطمینان	بی‌استفاده	

- فیلد Datagram Length: این فیلد ۱۶ بیتی طول کل بسته شامل بخش سرآیند و بار مفید را مشخص می‌نماید. مبنای طول بر حسب بایت است و در نتیجه، طول کل دیتاگرام حداکثر برابر با ۶۴ کیلوبایت خواهد بود (در واقع برابر با 2^{64}-1 خواهد بود که کمی کمتر از ۶۴ کیلوبایت است).

- فیلد 16-bit Identifier: ممکن است شرایطی پیش بیاید که یک مسیریاب مجبور شود که یک بسته را به تکه‌های کوچکتر بشکند. به طور مثال، ممکن است که پروتکل بکاررفته در لایه‌ی دوم اجازه‌ی ارسال بسته‌های بیش‌تر از ۱۵۰۰ بیت را ندهد. به هر کدام از تکه‌های ایجاد شده یک fragment گفته می‌شود و تمام این fragmentها دارای یک شناسه‌ی یکسان هستند که در این فیلد قرار داده می‌شود. در نتیجه، مقصد بسته‌ها می‌تواند تکه‌های مربوط به یک دیتاگرام واحد را تشخیص دهد و آنها را مجدداً به هم پیوند بزند. وظیفه‌ی بازسازی قطعات همیشه بر عهده‌ی مقصد است. در ادامه تکه‌تکه کردن بسته‌ها با جزئیات بیشتری مورد بررسی قرار می‌گیرد.

- فیلد Flags: از سه بیت تشکیل شده است که بیت اول برای اهداف خاص رزور شده است و استفاده نمی‌شود. دو بیت دیگر DF و MF نامیده می‌شوند. در صورتی که بیت DF در یک بسته برابر با ۱ باشد، مسیریاب‌ها حق شکستن آن به تکه‌های کوچکتر را ندارند زیرا، مقصد توانایی بازسازی آنها را ندارد. در صورتی که یک مسیریاب به دلیل اندازه‌ی بزرگ بسته قادر به ارسال آن نباشد و این بیت نیز شامل مقدار ۱ باشد، مسیریاب مجبور است که آنرا دور بیاندازد. بیت MF نیز برای تمام تکه‌های یک دیتاگرام واحد به جز آخرین تکه برابر با ۱ است.

- فیلد 13-bit Fragmentation Offset: این فیلد ۱۳ بیتی شماره‌ی ترتیب هر تکه در دیتاگرام شکسته شده را مشخص می‌نماید. اندازه‌ی هر تکه به استثنای تکه‌ی آخر باید مضربی از ۸ باشد.

- فیلد Time to Live یا TTL: این فیلد ۸ بیتی یک شمارنده است که طول عمر بسته را در مسیر آن به سمت مقصد مشخص می‌نماید. با توجه به این‌که این فیل شامل ۸ بیت است، حداکثر طور عمر بسته برابر با ۲۵۵ است که ممکن است به پیمودن ۲۵۵ گام[۲۷] در یک شبکه اشاره نماید. در واقع، به ازای عبور از هر مسیریاب در مسیر، یکی از مقدار مشخص شده در این فیلد کاسته می‌شود. همچنین، در صورتی که یک بسته در بافر یک مسیریاب برای خروج منتظر بماند، به ازای هر واحد زمان یکی از مقدار TTL آن کاسته خواهد شد. در نتیجه، زمانی که مقدار این بیت برابر با صفر شود، مسیریاب آن‌را دور می‌اندازد.

در واقع، علت استفاده از این فیلد این است که گاهاً ممکن است شرایطی در شبکه (در جداول پیش‌رانی مسیریاب‌ها) پیش بیاید که بسته‌ها در یک مسیر تکراری (دور) قرار بگیرند. در صورتی که از مقدار TTL استفاده نشود، ممکن است شبکه با بسته‌های بدردنخور اشباع گردد.

- فیلد Upper Layer Protocol: این فیلد در سیستم انتهایی مبدأ بسته و با مقدار متناظر با پروتکل لایه‌ی بالاتر (لایه‌ی انتقال) که بسته را به لایه‌ی شبکه تحویل داده پیکربندی می‌شود. در نتیجه، لایه‌ی شبکه در سیستم انتهایی مقصد با بررسی این فیلد، پروتکل لایه‌ی بالاتر را تشخیص می‌دهد و بسته را به آن تحویل می‌دهد. به طور مثال ممکن است بخش بار مفید بسته شامل یک بسته‌ی پروتکل TCP باشد که

[27] Hop

لایه‌ی شبکه در مقصد باید آن‌را به پروتکل TCP در مقصد تحویل دهد. این فیلد ۸ بیتی است و پروتکل‌های لایه‌ی بالاتر نیز دارای یک شناسه‌ی ۸ بیتی منحصر به فرد هستند.

- فیلد Header Checksum: این فیلد ۱۶ بیتی به منظور کشف خطاهای موجود در سرآیند هر بسته‌ی IP مورد استفاده قرار می‌گیرد. عمل محاسبه‌ی مقدار این فیلد بدین صورت انجام می‌شود که هر دو بایت در سرآیند به عنوان یک عدد در نظر گرفته می‌شود و جمع تمام این اعداد بر اساس محاسبات «مکمل یک» (one's complement) انجام می‌گردد. هر مسیریاب مقدار checksum را برای سرآیند هر دیتاگرام ورودی محاسبه می‌کند و وجود خطا را در صورت مغایرت مقدار محاسبه شده با مقدار موجود در فیلد Header Checksum تشخیص می‌دهد و دیتاگرام دارای خطا را دور می‌اندازد. به علت تغییر فیلد TTL در هر گره از مسیر یک دیتاگرام و تغییر احتمالی فیلد Options، هر مسیریاب حاضر در مسیر باید مقدار checksum را مجدداً محاسبه کند و در فیلد مربوطه قرار دهد. نحوه‌ی محاسبه‌ی مقدار checksum بعداً مورد بررسی قرار خواهد گرفت.
- فیلد 32-bit Source IP Address: آدرس IP میزبان مبدأ بسته در این فیلد قرار داده می‌شود.
- فیلد 32-bit Destination IP Address: آدرس IP میزبان مقصد بسته در این فیلد قرار داده می‌شود.
- فیلد Options: با توجه به این‌که بخش اجباری سرآیند بسته‌ی IP برابر با ۲۰ بایت است، در این فیلد می‌توان حداکثر ۴۰ بایت اطلاعات قرار داد. ممکن است این اطلاعات به مسیریاب‌ها در یافتن مسیر بهینه کمک کنند و یا اینکه، به منظور اشکال‌زدایی از شبکه پیکربندی شوند.

در این فیلد چند گزینه‌ی مختلف قابل استفاده هستند که هر کدام اطلاعات خاصی را مشخص می‌کنند و هر گزینه نیز با یک بایت خاص که معرفی کننده‌ی آن است آغاز می‌گردد. ۱ بیت سمت چپ از این بایت (Copy Flag) مشخص می‌کند که اگر مسیریابی مقدار آن‌را برابر با ۱ مشاهده کرد، این گزینه باید در تمام تکه‌های ایجاد شده از یک دیتاگرام واحد (در صورتی که مسیریاب مجبور به تکه‌تکه کردن دیتاگرام باشد) تکرار شود و اگر مقدار آن‌را برابر با ۰ مشاهده کرد، این گزینه فقط در تکه‌ی اول درج شود. دو بیت بعد (Option Class) نوع عملکرد (اطلاع رسانی یا تقاضا، اشکال‌زدایی و مدیریت شبکه) گزینه‌ی مورد نظر را مشخص می‌کنند. ۵ بیت بعد (Option Number) نیز نوع و معنای گزینه‌ی مورد نظر را با یک شماره‌ی خاص مشخص می‌کنند. جدول 2 نمایش‌دهنده‌ی انواع گزینه‌های قابل کاربرد در یک بسته‌ی IP است.

جدول *2* گزینه‌های قابل درج در فیلد *Option* از بسته‌ی *IP*

Option Class	Option Number	Name of Options	شرح
00	0	End of Options List	تعیین پایان لیست گزینه‌ها
00	1	Null Option	گزینه‌ی پوچ (فقط برای پر کردن فضا)

گزینه‌ی امنیت	Security	2	00
گزینه‌ی تعیین مسیر بصورت ناقص	Loose Source Routing	3	00
گزینه‌ی ثبت مسیر	Record Route	7	00
گزینه‌ی تعیین مسیر بصورت دقیق و صریح	Strict Source Routing	9	00
گزینه‌ی ثبت مسیر و زمان	Timestamp	4	10

- فیلد Data: این فیلد شامل بسته‌ی دریافت شده از لایه‌ی بالاتر می‌باشد. مثلاً segment دریافت شده از پروتکل TCP در این فیلد قرار داده می‌شود.

در این قسمت به بررسی بیشتر عمل تکه‌تکه کردن دیتاگرام‌ها یا IP Datagram Fragmentation پرداخته می‌شود. قبلاً گفته شد که یک دیتاگرام تولید شده در لایه‌ی شبکه در یک فریم لایه‌ی پیوند بسته‌بندی می‌شود و به سمت مسیریاب بعدی در شبکه ارسال می‌گردد. پروتکل‌های مختلف بکاررفته در لایه‌ی پیوند، ممکن است در اندازه‌ی بسته‌هایی که بر روی شبکه ارسال می‌کنند با محدودیت مواجه باشند (به حداکثر مقدار داده‌ای که یک فریم لایه‌ی پیوند می‌تواند حمل کند حداکثر واحد انتقال یا MTU[۲۸] گفته می‌شود). بنابراین، به علت تفاوت بین پروتکل‌های بکاررفته بر روی لینک‌های ورودی و خروجی متصل به مسیریاب، ممکن است لینک خروجی مشخص شده برای یک بسته، توانایی حمل بسته‌ی مورد نظر رابه خاطر اندازه‌ی بزرگ آن نداشته باشد (MTU لینک خروجی کمتر از MTU لینک ورودی است).

راه‌حل این مشکل تکه‌تکه کردن داده‌ی موجود در دیتاگرام IP به دو یا چند دیتاگرام کوچک‌تر و سپس، بسته‌بندی هر کدام از این دیتاگرام‌های کوچک‌تر در یک فریم لایه‌ی پیوند مجزا و ارسال آنها بر روی لینک خروجی است. هر کدام از این دیتاگرام‌های کوچک‌تر به عنوان یک تکه یا fragment شناخته می‌شود.

اما، یک دیتاگرام تکه‌تکه شده باید پیش از تحویل داده شدن به پروتکل لایه‌ی انتقال در مقصد مجدداً سرهم‌بندی شده و segment اولیه را تشکیل دهد (پروتکل‌های لایه‌ی انتقال منتظر دریافت یک segment کامل هستند). بنابراین، سیستم انتهایی مقصد وظیفه‌ی سرهم‌بندی مجدد دیتاگرام را بر عهده دارد. در واقع، با هدف ساده‌تر کردن پیاده‌سازی هسته‌ی شبکه، این کار فقط در ماشین مقصد امکان‌پذیر است.

استفاده از فیلدهای Identifier، Flags و Fragmentation Offset در سرآیند IP به منظور تشخیص یک fragment، تشخیص آخرین fragment و تعیین نحوه‌ی سرهم‌بندی مجدد تکه‌ها انجام می‌شود. سیستم انتهاییِ مبدأ هر دیتاگرام تولید شده را با یک شماره‌ی شناسه (Identifier) و آدرس‌های مبدأ و مقصد نشانه‌گذاری می‌کند. با تقسیم یک دیتاگرام به چند تکه، هر کدام از این تکه‌ها نیز با آدرس‌های مبدأ و مقصد و همچنین، شماره‌ی شناسه‌ی دیتاگرام اولیه نشانه‌گذاری می‌شوند. در نتیجه، با دریافت مجموعه‌ای از دیتاگرام‌ها از یک مبدأ یکسان توسط یک سیستم انتهایی، مقصد مورد نظر می‌تواند شماره‌ی شناسه‌ی بسته‌ها را به منظور

[28] Maximum Transmission Unit

تعیین تکه‌های مختلف یک دیتاگرام واحد بررسی نماید. با توجه به اینکه پروتکل IP هیچ تضمینی در رابطه با تحویل تکه‌ها به مقصد فراهم نمی‌کند، لازم است که در آخرین تکه‌ی دیتاگرام اصلی بیت MF از فیلد Flags دارای مقدار 0 و برای سایر تکه‌ها دارای مقدار ۱ باشد. همچنین، به منظور تعیین محل درست قرارگیری هر تکه در دیتاگرام اصلی و تشخیص تکه‌های مواجه شده با افت، از فیلد Fragmentation Offset استفاده می‌شود.

در ادامه با یک مثال به بررسی بیشتر مسأله‌ی مورد نظر پرداخته می‌شود. فرض شود که یک دیتاگرام با طول ۴۰۰۰ بایت (۲۰ بایت سرآیند بعلاوه‌ی ۳۹۸۰ بایت بار مفید یا payload) باید بر روی یک لینک خروجی با MTU برابر با ۱۵۰۰ بایت ارسال شود. در نتیجه بار مفید دیتاگرام باید به سه تکه‌ی مجزا (که هر کدام یک دیتاگرام جدید را تشکیل می‌دهد) تقسیم شود تا شرایط برای انتقال آن بر روی لینک خروجی فراهم گردد. نمایش‌دهنده‌ی مشخصات هر کدام از تکه‌های ایجاد شده است.

جدول ۳ تکه‌های *IP* یا *IP Fragments*

تکه	تعداد بایت‌ها	شناسه	Offset	پرچم
تکه‌ی شماره‌ی ۱	۱۴۸۰ بایت در فیلد داده در دیتاگرام	۷۷۷	0	MF = 1
تکه‌ی شماره‌ی ۲	۱۴۸۰ بایت در فیلد داده در دیتاگرام	۷۷۷	185	MF = 1
تکه‌ی شماره‌ی ۳	۱۰۲۰ بایت در فیلد داده در دیتاگرام	۷۷۷	370	MF = 0

بحث بعدی در رابطه با تولید مقدار بکاررفته برای فیلد checksum در سرآیند دیتاگرام IP است. همان‌طور که قبلاً گفته شد، مقدار checksum از مکمل یک جمع تمام کلمات ۱۶ بیتی در سرآیند حاصل می‌شود. هر مقدار سرریز شده نیز، با کم‌ارزش‌ترین بیت نتیجه جمع می‌شود. به عنوان یک مثال برای انجام محاسبات مشابه، سه کلمه‌ی ۱۶ بیتی 0110011001100000 و 0101010101010101 و 1000111100001100 در نظر گرفته می‌شود. جمع دو کلمه‌ی اول برابر با 1011101110110101 است و در نهایت حاصل جمع هر سه کلمه برابر با 0100101011000010 خواهد بود. توجه شود که در محاسبات انجام شده یک مقدار سرریز شده وجود داشت که با کم‌ارزش‌ترین بیت جمع شد. مکمل یک با تبدیل تمام 0ها به 1 و تبدیل تمام 1ها به 0 بدست می‌آید. در مثال مطرح شده مقدار نهایی پس از محاسبه‌ی مکمل یک برابر با 1011010100111101 است.

در هر مسیریاب و سیستم انتهایی مقصد، تمام کلمات ۱۶ بیتی (شامل checksum) سرآیند با هم جمع می‌شوند و در صورتی که تمام بیت‌های حاصل‌جمع برابر با 1 باشند (به صورت 1111111111111111)، دیتاگرام بدون خطا وارد مقصد شده و در صورتی که حتی یکی از این ۱۶ بیت برابر با 0 باشد، مشخص می‌شود که بسته به همراه خطا به گره مورد نظر رسیده است.

۷. آدرس‌های IP

تمام دستگاه‌های متصل به اینترنت اعم از کامپیوترهای رومیزی، تلویزیون‌ها، تلفن‌های هوشمند و حتی مسیریاب‌ها نیاز به یک آدرس IP به منظور برقراری ارتباط با دنیای اینترنت دارند. یک آدرس IP از چهار عدد دهدهی که با چهار نقطه از هم جدا شده‌اند تشکیل می‌شود. با توجه به اینکه هر کدام از چهار قسمت تشکیل‌دهنده‌ی یک آدرس IP یک بایت داده را در خود جای می‌دهد، نمایش آدرس به صورت دهدهی در محدوده‌ی 0.0.0.0 تا 255.255.255.255 قرار می‌گیرد. اما، امکان استفاده از تمام این آدرس‌ها در فضای اینترنت وجود ندارد و برخی از این آدرس‌ها برای اهداف خاصی رزرو شده‌اند. جدول ۴ نمایش‌دهنده‌ی برخی از آدرس‌های رزرو شده و کاربرد آنها است.

جدول ۴ برخی از آدرس‌های خاص و کاربرد آنها

کاربرد آدرس	آدرس خاص
این آدرس غیر معتبر می‌باشد.	0.0.0.0
از این آدرس به منظور ارسال همگانی یا همه‌پخشی استفاده می‌شود.	255.255.255.255
این آدرس loopback نامیده می‌شود و معادل آدرس خود ماشین محلی است.	127.0.0.1

قبلاً گفته شد که اینترنت از اتصال مجموعه‌ی شبکه‌های کامپیوتری تشکیل شده است و این شبکه‌های کامپیوتری دربرگیرنده‌ی سیستم‌های انتهایی متصل به اینترنت می‌باشند. در نتیجه، هر آدرس IP مشخص‌کننده‌ی یک سیستم انتهایی از دو بخش تشکیل شده است که یکی از آنها شماره‌ی شناسایی شبکه‌ی صاحب آن سیستم انتهایی است و بخش دیگر به شناسه‌ی سیستم انتهایی در آن شبکه اختصاص دارد. شکل ۸ نمایش‌دهنده‌ی قالب یک آدرس IP است. بدیهی است که شماره‌ی شناسه‌ی یک شبکه برای تمام سیستم‌های انتهایی حاضر در آن شبکه یکسان است. تعداد بیت‌های اختصاص یافته به بخش مشخص‌کننده‌ی شناسه‌ی سیستم انتهایی تعیین‌کننده‌ی حداکثر تعداد سیستم‌های انتهایی قابل استفاده در یک شبکه‌ی مشخص می‌باشد. طول بخش شناسه‌ی شبکه به کلاس آدرس آن شبکه بستگی دارد و در واقع، یک کلاس آدرس می‌تواند تعداد سیستم‌های انتهایی حاضر در یک شبکه را مشخص نماید.

شکل ۸ دو بخش تشکیل‌دهنده‌ی یک آدرس *IP*

لازم به ذکر است که الزاماً هر کامپیوتری که به اینترنت متصل است از یک آدرس IP قابل مشاهده توسط سایر سیستم‌های انتهایی حاضر در اینترنت برخوردار نمی‌باشد. در واقع، یک سیستم انتهایی متصل به

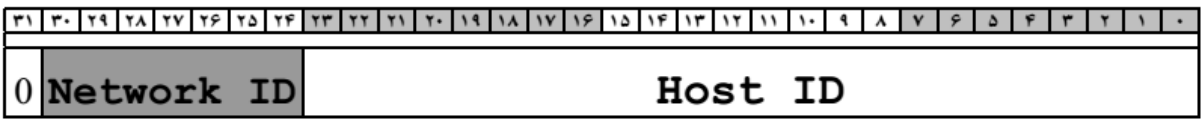
اینترنت ممکن است از یک آدرس معتبر (قابل مشاهده و ردیابی توسط سایر حاضرین در اینترنت) و یا یک آدرس غیر معتبر (غیرقابل مشاهده و ردیابی توسط سایر حاضرین در اینترنت) استفاده نماید. در بخش‌های بعد در رابطه با این مسأله صحبت خواهد شد. نکته‌ی حائز اهمیت دیگر در رابطه با آدرس‌های IP این است که این آدرس‌ها از یک ساختار سلسله مراتبی برخوردار بوده و هر کدام شامل اطلاعات ارزشمندی در مورد نقشه‌ی شبکه و محل یک سیستم انتهایی در شبکه‌ی اینترنت می‌باشد.

۸. کلاس‌های آدرس IP

آدرس‌های IP در پنج کلاس A، B، C، D و E تقسیم‌بندی می‌شوند. پر ارزشترین بایت (اولین بایت از سمت چپ) از آدرس IP کلاس آدرس آن‌را مشخص می‌نماید.

۱-۱ آدرس‌های کلاس A

در کلاس A پر ارزش‌ترین بیت آدرس دارای مقدار 0 است که این مقدار وجه مشخصه‌ی این کلاس از سایر کلاس‌ها می‌باشد. در نتیجه، بایت پر ارزش در کلاس A بین مقادیر 0 و 127 (یعنی از ۱ تا ۱۲۶) تغییر می‌کند. البته، دو مقدار 0 و 127 به دلیل اینکه رزرو شده هستند قابل استفاده نمی‌باشند. در نتیجه، حداکثر ۱۲۶ شبکه از کلاس A در دنیا وجود دارد. بدین ترتیب، در صورتی که عدد سمت چپ یک آدرس IP بین 0 و 127 (یعنی از مقدار ۱ تا مقدار ۱۲۶) باشد، آن شبکه به کلاس A تعلق دارد. به جز پر ارزش‌ترین بیت، ۷ بیت بعدی در بایت پر ارزش شامل شناسه‌ی شبکه و ۲۴ بیت دیگر مشخص‌کننده‌ی شناسه‌ی سیستم‌های انتهایی هستند. در نهایت ذکر این نکته نیز لازم است که مقادیر تماماً 0 و تماماً 255 (یعنی تمام بایت‌ها 0 باشند یا تمام آنها 255 باشند یا به عبارتی، تمام بیت‌ها 0 باشند یا تمام آنها 1 باشند) برای بایت‌های مشخص‌کننده‌ی شناسه‌ی سیستم‌های انتهایی مجاز نمی‌باشد.



شکل ۹ قالب ۳۲ بیتی آدرس در کلاس *A*

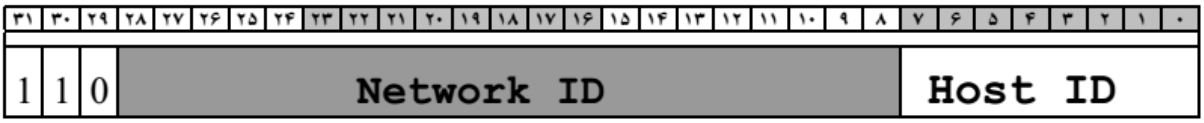
۱-۲ آدرس‌های کلاس B

شکل ۱۰ نمایش‌دهنده‌ی قالب آدرس‌های کلاس B است. همان‌طور که مشاهده می‌شود، دو بیت پر ارزش در این کلاس دارای مقدار 10 هستند. ۱۴ بیت باقی‌مانده از دو بایت سمت چپ به شناسه‌ی شبکه اختصاص دارند و ۱۶ بیت باقی‌مانده نیز مربوط به شناسه‌ی سیستم‌های انتهایی هستند. در نتیجه، با توجه به اینکه مقادیر تماماً 0 و تماماً 255 (در مجموع فقط شامل دو آدرس هستند) غیر مجاز هستند، در یک شبکه از کلاس B تعداد ۶۵۵۳۴ سیستم انتهایی قابل استفاده هستند که برابر با $2^{16} - 2$ است. تعداد شبکه‌های قابل استفاده در این کلاس برابر با 2^{14} یا ۱۶۳۸۴ است. در صورت نمایش یک آدرس IP در حالت ده‌دهی و در صورتی که عدد سمت چپ آن بین ۱۲۷ و ۱۹۲ باشد، آن آدرس متعلق به کلاس B است.

شکل ۱۰ قالب ۳۲ بیتی آدرس در کلاس *B*

۳–۱ آدرس‌های کلاس C

شکل ۱۱ نمایش‌دهنده‌ی قالب آدرس‌های کلاس C است. مشاهده می‌شود که سه بیت پر ارزش در این کلاس دارای مقدار 110 هستند. ۲۱ بیت از سه بایت سمت چپ از آدرس به شناسه‌ی شبکه‌های کلاس C (شامل 2^{21} یا ۲۰۹۷۱۵۲ شبکه) اختصاص دارد و ۸ بیت سمت راست نیز، مشخص‌کننده‌ی $2^{8} - 2$ یا ۲۵۴ سیستم انتهایی در هر شبکه است. اگر در شکل ده‌دهی نمایش آدرس IP عدد سمت چپ بین 191 و 224 بود، آن آدرس به کلاس C تعلق دارد.



شکل ۱۱ قالب ۳۲ بیتی آدرس در کلاس *C*

۴–۱ آدرس‌های کلاس D

چهار بیت پر ارزش در این کلاس حاوی مقدار 1110 هستند و ۱۲۸ بیت باقی‌مانده نیز برای تعیین آدرس چندپخشی[۲۹] مورد استفاده قرار می‌گیرند. این آدرس‌ها برای ارسال یک دیتاگرام واحد، به طور همزمان برای چندین سیستم انتهایی کاربرد دارند. شکل ۱۲ نمایش‌دهنده‌ی قالب آدرس‌های این کلاس است.

شکل ۱۲ قالب ۳۲ بیتی آدرس در کلاس *D*

[29] Multicast

۱–۵ آدرس‌های کلاس E

پنج بیت پر ارزش در آدرس‌های این کلاس دارای مقدار 11110 هستند. این آدرس‌ها فعلاً بدون استفاده هستند.

در انتها لازم است به ذکر چند نکته در رابطه با آدرس‌های IP پرداخته شود. به طور کلی تمام آدرس‌هایی که عدد دهدهی سمت چپ آنها برابر با 127 است به منظور اشاره به سیستم انتهایی محلی (خود ماشین درخواست دهنده) بکار می‌روند و بسته‌ی تولید شده توسط لایه‌ی شبکه‌ی آن ماشین مجدداً به لایه‌ی بالاتر باز می‌گردد (مشاهده می‌شود که تعداد بسیار زیادی از آدرس‌های IP بدین شکل هدر رفته است). در صورتی که در قسمت مشخص‌کننده‌ی شناسه‌ی سیستم انتهایی در آدرس متعلق به یکی از کلاس‌ها، به ازای همه‌ی بیت‌ها از مقدار 1 استفاده شود (مثلاً NetID.255)، بسته‌های مورد نظر به منظور تحویل به تمام سیستم‌های انتهایی حاضر در آن شبکه ارسال شده است و اصطلاحاً به آن بسته‌ی همه‌پخشی گفته می‌شود. بسته‌ای که کل آدرس آن از چهار عدد 255 ساخته شده است (255.255.255.255) به منظور ارسال بسته به تمام سیستم‌های انتهایی حاضر در شبکه‌ی محلی بکار می‌رود.

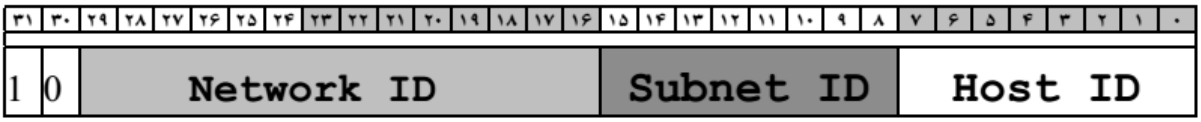
با ورود یک بسته به یک مسیریاب، مسیریاب مورد نظر می‌تواند به راحتی کلاس شبکه‌ی مورد نظر را تشخیص دهد و در جدول هدایت خود به دنبال مدخل مربوط به آن شبکه و لینک خروجی منتهی به آن بگردد.

۱–۶ آدرس‌های زیرشبکه

در جلسات قبل گفته شد که ممکن است یک شبکه (به عنوان مثال، یک شبکه از کلاس C) از چند بخش مختلف تشکیل شده باشد که با استفاده از یک یا چند مسیریاب از هم جدا شده‌اند. هر کدام از این شبکه‌ها به عنوان یک زیرشبکه شناخته می‌شوند.

از دید یک مسیریاب خارجی کل شبکه (مجموعه‌ی شبکه‌های محلی) با استفاده از یک آدرس واحد (مثلاً 211.11.121.0 برای کلاس C) شناخته می‌شود. اما، لازم است که روشی وجود داشته باشد تا مسیریاب‌های داخلی نیز قادر به شناسایی و تفکیک زیرشبکه‌های داخلی باشند. همچنین، لازم است که هر سیستم انتهایی قادر به تشخیص سیستم‌های انتهایی حاضر در شبکه‌ی محلی مشترک با خود و سایر شبکه‌های محلی باشند. در واقع، یک سیستم انتهایی با استفاده این اطلاعات تصمیم می‌گیرد که آیا ارسال اطلاعات باید مستقیماً بر روی شبکه‌ی محلی انجام شود یا آنکه باید از طریق یک مسیریاب برای یک شبکه‌ی دیگر ارسال شود. با توجه به تعداد بسیار زیاد میزبان‌ها در شبکه‌های کلاس A و B، مسأله‌ی ذکر شده بسیار حائز اهمیت است. برای این منظور از مفهومی به نام «الگوی زیرشبکه» (Subnet Mask) استفاده می‌شود و به گونه‌ای در بخش شناسه‌ی سیستم‌های انتهایی، زیرشبکه‌ها را مشخص می‌نماید.

همان‌طور که گفته شد، به منظور تقسیم یک شبکه به چند زیرشبکه‌ی مختلف، با استفاده از تغییر مقادیر بکاررفته در بخش سیستم‌های انتهایی در کلاس آدرس مورد نظر انجام می‌شود. به طور مثال، می‌توان در یک شبکه‌ی کلاس B با استفاده از قالب آدرس‌دهی مشخص شده در شکل ۱۳ اقدام به بکارگیری ۲۵۴ زیرشبکه نمود. همان‌طور که مشاهده می‌شود، ۸ بیت سمت چپ از مجموعه‌ی بیت‌های موجود در بخش شناسه‌ی میزبان در آدرس کلاس B به منظور تعیین ۲۵۴ زیرشبکه مورد استفاده قرار گرفته‌اند. بنابراین، به منظور اینکه یک سیستم انتهایی تشخیص دهد که یک سیستم انتهایی دیگر در زیرشبکه‌ی خودش (شبکه‌ی محلی مشترک با خودش) قرار دارد یا در یک زیرشبکه‌ی دیگر قرار دارد، باید قسمت‌های شناسه‌ی شبکه و شناسه‌ی زیرشبکه از آدرس IP آن سیستم انتهایی را با آدرس IP خود مقایسه کند. این کار با استفاده از یک الگوی زیرشبکه انجام می‌شود. به طور مثال، الگوی زیرشبکه برای آدرس‌های مشخص شده با قالب شکل ۱۳ به صورت 255.255.255.0 مشخص می‌گردد.



شکل ۱۳ تقسیم فضای ۳۲ بیتی آدرس به سه بخش شناسه‌ی شبکه، شناسه‌ی زیرشبکه و شناسه‌ی میزبان یا سیستم انتهایی

تعیین محل یک سیستم انتهایی دیگر بدین صورت انجام می‌شود که هر سیستم انتهایی آدرس IP خود و آدرس IP سیستم انتهایی دیگر را با الگوی زیرشبکه AND می‌کند (با این کار بخش شناسه‌ی سیستم‌های انتهایی را صفر می‌نماید) و هر دو آدرس بدست آمده را با هم مقایسه می‌نماید. اگر دو آدرس بدست آمده با هم برابر باشند، دو سیستم انتهایی در یک زیرشبکه‌ی یکسان قرار دارند و در صورت مغایرت، سیستم انتهایی مبدأ باید بسته‌های تولید شده به مقصد سیستم انتهایی حاضر در یک زیرشبکه‌ی دیگر را به یکی از مسیریاب‌های حاضر در شبکه‌ی محلی خود ارسال نماید.

به عنوان یک مثال دیگر، الگوی زیرشبکه‌ی 255.255.240.0 در نظر گرفته می‌شود. شکل دودویی این الگو به صورت 11111111.11111111.11110000.00000000 قابل نمایش می‌باشد. در صورتی که فرض شود الگوی مورد نظر برای یک شبکه از کلاس B تعریف شده است، مشاهده می‌شود که چهار بیت سمت چپ از بخش مربوط به شناسه‌ی سیستم‌های انتهایی به منظور تعیین ۱۴ ($2^4 - 2$) زیرشبکه مورد استفاده قرار گرفته است. با توجه به اینکه ۱۲ بیت در این بخش باقی مانده است، می‌توان 4094 ($2^{12} - 2$) سیستم انتهایی در هر زیرشبکه بکار گرفت.

لازم به تذکر است که همیشه تعداد زیرشبکه‌ها و تعداد سیستم‌های انتهایی حاضر در آن ۲تا کمتر از کل تعداد قابل تعریف است. زیرا زیرشبکه یا ماشینی که تمام بیت‌های آن صفر یا یک باشد قابل تعریف نیست. نکته‌ی دیگر اینکه، گاهی اوقات الگوی زیرشبکه یا Subnet Mask [به عنوان مثال] به صورت 133.189.0.0/21 در جلو آدرس شبکه نوشته می‌شود که معادل 133.189.0.0/255.255.248.0 است.

۹. CIDR (Classless Inter Domain Routing): آدرس‌دهی بدون کلاس

همان‌طور که قبلاً گفته شد، در شرایطی که از کلاس‌های آدرس برای تعیین آدرس شبکه‌های کامپیوتری مختلف در اینترنت استفاده می‌شد، در یک مسیریاب به ازای هر آدرس شبکه، یک مدخل در جدول پیش‌رانی مسیریاب وجود دارد که به مناسب‌ترین لینک خروجی منتهی به آن شبکه اشاره می‌نماید. با گذر زمان و رشد شبکه‌ی اینترنت، وضعیت کلاس‌های آدرس به شکلی شد که تمام آدرس‌های کلاس‌های A و B فروخته شد و فقط آدرس‌های کلاس C قابل خریداری بودند. اما، ممکن است که تعداد سیستم‌های انتهایی موجود در یک شبکه بیشتر از تعداد سیستم‌های انتهایی قابل تعریف با استفاده از آدرس یک شبکه‌ی کلاس C باشد که در این صورت، شبکه‌ی مورد نظر با چند آدرس شبکه‌ی C مشخص می‌گردد. به طور مثال، اگر سازمانی نیاز به راه‌اندازی شبکه‌ای با حدود ۴۰۰۰ سیستم انتهایی داشته باشد، مجبور است ۱۶ آدرس شبکه‌ی کلاس C خریداری نماید. در این حالت، در جداول هدایت مسیریاب‌های حاضر در ستون فقرات اینترنت به ازای یک شبکه‌ی واحد ۱۶ مدخل درج می‌شود که به مسیر منتهی به آن اشاره می‌کنند.

بدین ترتیب، ساختار آدرس‌های «بدون کلاس یا Classless» معرفی شدند که باعث کاهش چشمگیر حجم جداول هدایت در مسیریاب‌ها، به دلیل یکی شدن تمام مداخل مربوط به یک شبکه‌ی واحد متشکل از چند شبکه‌ی کلاس C می‌شود. به عنوان مثال، یک شبکه با ۴۰۰۰ سیستم انتهایی باعث ایجاد ۱۶ مدخل در جدول پیش‌رانی نمی‌شود و تمام این ۱۶ مدخل در یک مدخل «تجمیع» (Aggregate) می‌شوند.

آدرس‌های بدون کلاس که در محدوده‌ی فضای آدرس‌های کلاس C تعریف می‌شوند (یعنی عدد سمت چپ آنها بین 191 و 224 است)، اگرچه که مثل قبل از دو بخش شناسه‌ی شبکه و شناسه‌ی سیستم‌های انتهایی تشکیل شده‌اند، برخلاف کلاس‌های آدرس A، B و C این دو بخش دارای طول متغیری هستند. از آنجائیکه در آدرس‌های بدون کلاس اندازه‌ی دقیق بخش شناسه‌ی شبکه مشخص نیست، لذا استفاده از یک الگوی شبکه برای مشخص کردن آن ضروری می‌باشد که بیت‌های ۱ در این الگو مشخص‌کننده‌ی شماره‌ی شناسایی شبکه هستند.

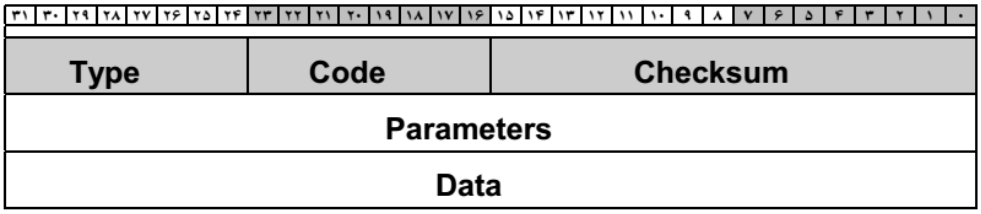
در نتیجه، جدول موجود در مسیریاب‌ها شامل مداخلی می‌شود که به صورت مجموعه‌ی گام بعدی، شناسه‌ی شبکه، الگوی شبکه مشخص می‌گردند. این مدخل‌ها مشخص می‌کنند که دستیابی به یک شبکه‌ی راه دور از طریق کدام‌یک از لینک‌های خروجی مسیریاب ممکن است. با ورود یک بسته‌ی جدید به هر مسیریاب، آدرس مقصد آن با الگوهای شبکه‌ی موجود در هر مدخل AND می‌شود و در صورتی که یک انطباق مشاهده شد (نتیجه‌ی AND با شناسه‌ی شبکه‌ی صاحب الگوی شبکه برابر بود)، بسته به گام بعدی مشخص

شده توسط آن مدخل ارسال می‌شود. ممکن است که بیش از یک الگوی شبکه در بیش از یک مدخل با بسته‌ی مورد نظر منطبق باشند که در این صورت، الگوی طولانی‌تر به منظور تعیین گام بعدی مورد استفاده قرار می‌گیرد. در صورتی که هیچ‌کدام از الگوهای زیرشبکه با آدرس مقصد بسته منطبق نباشند، بسته به یک لینک خروجی پیش‌فرض ارسال می‌شود.

۱۰. پروتکل ICMP

پروتکل IP یک پروتکل بدون ارتباط [۳۰] و غیر قابل اعتماد است. بدون ارتباط بدین معنا که مسیریاب هر بسته را بدون هیچ‌گونه هماهنگی با مقصد بسته یا مسیریاب بعدی ارسال می‌نماید و پس از ارسال بسته نیز آنرا فراموش می‌کند و منتظر دریافت رسید بسته از طرف گیرنده نمی‌شود. در واقع، ممکن است بسته‌ی مورد نظر به دلایل متعددی همچون منقضی شدن TTL یا ارسال به مسیر اشتباه، به مقصد مورد نظر خود دست پیدا نکند. در نتیجه، عدم اطلاع‌رسانی به فرستنده باعث ارسال مجدد آن بسته یا بسته‌های دیگر توسط آن سیستم انتهایی شده، بدون اینکه نتیجه‌ای در پی داشته باشد.

پروتکل ICMP در کنار پروتکل IP به منظور بررسی انواع خطا و ارسال پیام برای مبدأ بسته در هنگام بروز اشکالات ناخواسته استفاده می‌شود. ICMP یک پروتکل گزارش خطا است که بر روی پروتکل IP عمل می‌کند و در صورت بروز هرگونه خطا، به فرستنده پیام مناسب متناظر با آن رخداد را ارسال می‌نماید. بدین صورت که بسته‌ی ICMP تولید شده خود توسط یک دیتاگرام کپسوله می‌شود و به سمت مقصد خود ارسال می‌شود. بنابراین، فیلد Protocol در سرآیند بسته‌ی IP باید با شماره‌ی مشخصه‌ی پروتکل ICMP پیکربندی شود. لازم به ذکر است که در صورت بروز خطا و حذف بسته‌های ICMP هیچ پیام خطایی ارسال نخواهد شد. شکل ۱۴ نمایش‌دهنده‌ی قالب بسته‌های IP است.



شکل ۱۴ قالب بسته‌های *ICMP*

- فیلد Type: نوع پیام را مشخص می‌کند.

[30] Connectionless

- فیلد Code: ممکن است نوع خاصی از پیام به چند نوع فرعی دیگر تقسیم شود که کد نوع فرعی در این فیلد قرار داده می‌شود.
- فیلد Checksum: به منظور تعیین درستی یک پیام استفاده می‌شود و با استفاده از محاسبات مکمل یک بدست می‌آید.
- فیلد Data: در تمام بسته‌های ICMP که به عنوان گزارش خطا به سمت سیستم انتهایی مبدأ بسته ارسال می‌شود، سرآیند دیتاگرام حذف شده به همراه ۶۴ بیت از اول داده (۸ بایت اول از سرآیند segment موجود در بسته) برای آن ارسال می‌شود.

انواع پیام‌های ICMP (که با استفاده از مقادیر مختلف برای فیلدهای Type و Code حاصل می‌شوند، در ادامه معرفی می‌گردند:

- Destination Unreachable: این پیام شامل چند نوع فرعی دیگر می‌باشد که به دلیل غیرقابل دسترس بودن مقصد، چه در اثر امکان‌ناپذیر بودن دسترسی به شبکه‌ی مقصد، دسترسی ناپذیر بودن میزبان مقصد، چه در صورت پشتیبانی نشدن از پروتکل لایه‌ی انتقال در مقصد، چه در صورت در دسترس نبودن برنامه‌ی کاربردی در مقصد و چه در صورت عدم توانایی مسیریاب در شکستن پیام به چند پیام کوچکتر ارسال می‌شود. فیلد Type در بسته‌ی تولید شده برای این نوع پیام دارای مقدار برابر با ۳ است.
- Time Exceeded: این پیام زمانی که مهلت قانونی بسته (فیلد TTL در سرآیند IP) پایان یافته باشد به سمت مبدأ ارسال می‌گردد و فیلد Type برای آن برابر با مقدار ۱۱ است.

سایر پیام‌های ICMP نیز شامل موارد زیر است:

- Parameter Problem
- Source Quench
- Redirect
- Echo Request و Echo Reply
- Timestamp Request و Timestamp Reply

۱۱. پروتکل ARP

یک شبکه‌ی محلی در نظر گرفته شود که از چندین سیستم انتهایی تشکیل شده است و هر کدام از این سیستم‌های انتهایی از یک آدرس IP برخوردار می‌باشد و امکان ارتباط با سیستم‌های انتهایی حاضر در اینترنت برای آنها فراهم است. فرض می‌شود که بخشی از یک برنامه‌ی کاربردی در یکی از این سیستم‌های انتهایی نیاز به ارتباط با بخش دیگری از آن برنامه‌ی کاربردی در یک سیستم انتهایی حاضر در شبکه‌ی مشترک با آن دارد. سیستم انتهایی مبدأ (در واقع لایه‌ی شبکه‌ی سیستم انتهایی مبدأ) با بررسی آدرس سیستم انتهایی مقصد تشخیص می‌دهد که این سیستم انتهایی در شبکه‌ی مشترک با آن قرار دارد. قبلاً گفته شد که ارسال بسته‌ها به یک گام بعد در هر شبکه توسط پروتکل‌های لایه‌ی پیوند اجرا می‌شود و این امر نیاز به دانستن آدرس فیزیکی (آدرس MAC) سیستم انتهایی مقصد دارد. این درحالی است که با وجود فراهم شدن آدرس IP توسط لایه‌ی کاربرد، ممکن است آدرس فیزیکی سیستم انتهایی مقصد برای لایه‌ی دوم شبکه در مبدأ مشخص نباشد. از طرفی، در صورتی که سیستم انتهایی مقصد در یک شبکه‌ی راه دور در اینترنت باشد، لازم است که بسته‌ها به یک مسیریاب دروازه ارسال شوند که مجدداً نیاز به آدرس فیزیکی آن وجود دارد.

بدین ترتیب، هر سیستم انتهایی حاضر در اینترنت علاوه بر اینکه نیاز به دانستن آدرس IP سایر سیستم‌های انتهایی دارد، لازم است که آدرس فیزیکی سیستم‌های انتهایی یا مسیریاب‌هایی که به طور مستقیم با آنها در ارتباط است را نیز بداند (به طور مثال، آدرس شش بایتی بکاررفته توسط پروتکل لایه‌ی پیوند اترنت[۳۱]). پروتکل ARP[۳۲] به عنوان راه‌حلی برای این مشکل مورد استفاده قرار می‌گیرد و امکان کسب اطلاع از آدرس فیزیکی سیستم‌های انتهایی که از آدرس IP خود باخبر هستند را فراهم می‌نماید.

عمل دریافت آدرس فیزیکی یک مقصد مشخص با ارسال یک بسته‌ی همه‌پخشی[۳۳] (منظور در لایه‌ی دوم است که با آدرس فیزیکی مقصد برابر با ff:ff:ff:ff:ff:ff انجام می‌شود) بر روی شبکه‌ی محلی آغاز می‌شود که حاوی پرسش زیر است (به طور مثال آدرس IP سیستم انتهایی مقصد برابر با 192.31.65.5 است):

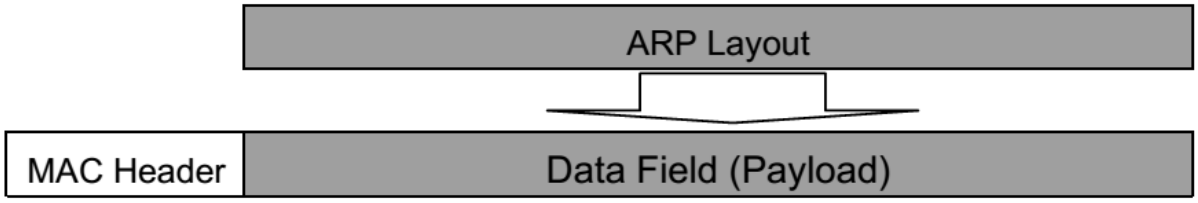
«کسی که آدرس IP او 192.31.65.5 است، آدرس فیزیکی او چیست؟»

در نتیجه، این پیام فراگیر توسط تمام سیستم‌های انتهایی حاضر در شبکه‌ی محلی دریافت می‌شود و آن سیستم انتهایی که آدرس IP خود را در این بسته مشاهده می‌کند، فوراً به آن پاسخ می‌دهد و آدرس فیزیکی خود را برای درخواست کننده ارسال می‌کند (ممکن است پاسخ به صورت همه‌پخشی یا تک‌پخشی[۳۴] ارسال گردد). پس از حصول آدرس فیزیکی گام بعدی در مسیر یک دیتاگرام لایه‌ی شبکه، دیتاگرام به لایه‌ی

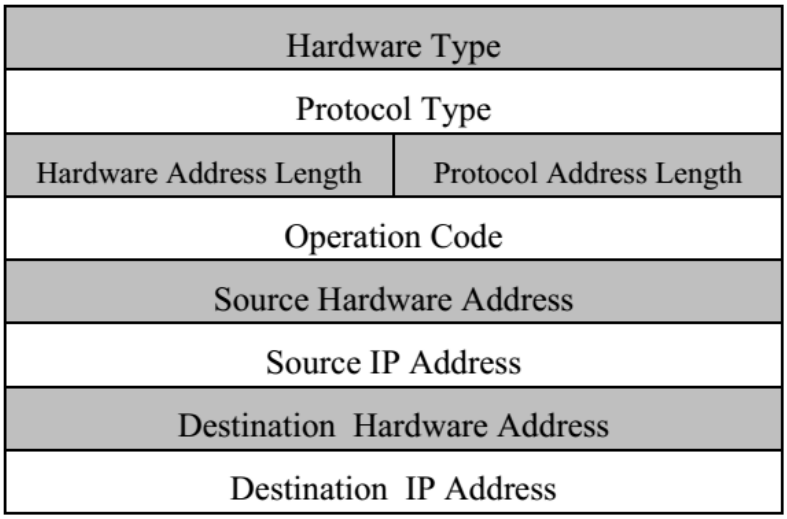
31 Ethernet
32 Address Resolution Protocol
33 Broadcast
34 unicast

پیوند تحویل داده می‌شود و در قالب یک فریم به سمت سیستم انتهایی گام بعدی ارسال می‌شود. کاملاً واضح است که تمام سیستم‌های انتهایی حاضر در یک شبکه‌ی محلی باید از پروتکل ARP پشتیبانی نمایند.

بسته‌های تولید شده توسط پروتکل ARP در یک فریم کپسوله شده (برخلاف بسته‌های پروتکل ICMP) و در شبکه‌ی محلی ارسال می‌شوند. شکل ۱۵ نمایش‌دهنده‌ی نحوه‌ی کپسوله‌سازی بسته‌ی ARP در یک فریم لایه‌ی پیوند است و شکل ۱۶ نیز قالب یک بسته‌ی ARP نشان داده شده است.



شکل ۱۵ نحوه‌ی قرار گیری یک بسته‌ی *ARP* در یک فریم لایه‌ی پیوند



شکل ۱۶ قالب یک بسته‌ی *ARP* کپسوله‌شده در یک فریم لایه‌ی پیوند

- Hardware Type: در فیلد مشخصه‌ی نوع سخت‌افزار واسط خروجی شبکه[۳۵] که وظیفه‌ی انتقال اطلاعات روی کانال فیزیکی را برعهده دارد، ثبت می‌شود.
- Protocol Type: این فیلد نوع پروتکل بکاررفته در لایه‌ی شبکه که درخواست ARP برای آن تولید شده است را مشخص می‌نماید.
- Hardware Address Length: با توجه با اینکه طول آدرس‌های فیزیکی بکاررفته توسط پروتکل‌های لایه‌ی پیوند مختلف با هم متفاوت است، در این فیلد طول آدرس (بر حسب بایت) مشخص می‌شود.
- Protocol Address Length: طول آدرس‌های لایه‌ی شبکه را بر حسب بایت مشخص می‌نماید.

[35] Output Network Interface

- Operation Code (Opcode): مقدار ۱ در این فیلد مشخص‌کننده‌ی یک درخواست ARP (ARP Request) و مقدار ۲ در این فیلد مشخص‌کننده‌ی یک پاسخ ARP (ARP Reply) است.
- Source Hardware Address: آدرس فیزیکی مبدأ
- Source IP Address: آدرس IP سیستم انتهایی مبدأ
- Destination Hardware Address: آدرس فیزیکی سیستم انتهایی مقصد
- Destination IP Address: آدرس IP ماشین مقصد

وقتی یک درخواست و پاسخ از نوع ARP در شبکه اتفاق می‌افتد و در صورتی که پاسخ به صورت همه‌پخشی ارسال شود، تمام سیستم‌های انتهایی حاضر در آن شبکه‌ی محلی بسته‌ی پاسخ را مشاهده می‌کنند. لذا تمام سیستم‌های انتهایی پاسخ تولید شده را مشاهده می‌کنند و آدرس IP و آدرس فیزیکی موجود در آن‌را در حافظه‌ی خود نگهداری می‌کنند تا شاید در آینده مورد استفاده قرار بگیرد.

پس از بدست آمدن آدرس فیزیکی متناظر با یک آدرس IP، پروتکل ARP این دو آدرس را در جدولی درون حافظه‌ی اصلی که ARP Cache نامیده می‌شود ذخیره می‌کند تا اگر در آینده‌ی این آدرس مورد نیاز بود به سرعت مورد استفاده قرار بگیرد. قالب هر مدخل در جدول ARP به صورت مشخص شده در شکل ۱۷ است.

IF Index	Physical Address	IP Address	Type

شکل ۱۷ قالب هر مدخل در جدول *ARP*

۱۲. پروتکل DHCP[۳۶]

این پروتکل به منظور پیکربندی پویای آدرس‌های IP در سیستم‌های انتهایی مورد استفاده قرار می‌گیرد. در صورتی که از این کارکرد در شبکه‌های کامپیوتری استفاده نشود، لازم است که آدرس IP هر سیستم انتهایی به صورت دستی توسط مدیر شبکه تنظیم شود که امری زمان‌بر و دارای خطا می‌باشد و در محیط‌هایی که سیستم‌های انتهایی به صورت بی‌سیم هستند و امکان تعویض نقطه‌ی دسترسی[۳۷] برای آنها وجود دارد امری حیاطی به شمار می‌رود.

[36] Dynamic Host Configuration Protocol
[37] Access Point

بدین منظور، نیاز به وجود یک سیستم انتهایی کارپذیر[۳۸] در شبکه وجود دارد که به تقاضای دریافت آدرس توسط سیستم‌های انتهایی پاسخ می‌دهد. البته، لازم نیست که یک کارپذیر DHCP[۳۹] بر روی همان شبکه‌ای باشد که یک سیستم انتهایی درخواست دهنده قرار دارد. با وجود اینکه امکان استفاده از کارپذیر DHCP در یک شبکه‌ی مجزا از سیستم‌های انتهایی موجود است، در این قسمت فقط یک کارپذیر DHCP در یک شبکه‌ی مشترک با سیستم‌های انتهایی درخواست دهنده‌ی آدرس IP در نظر گرفته می‌شود.

آن سیستم انتهایی که تازه روشن شده است به منظور بدست آوردن یک آدرس IP بسته‌ای تحت عنوان DHCP DISCOVER را به صورت همه‌پخشی بر روی شبکه‌ی محلی (LAN) ارسال می‌نماید. با توجه به اینکه سیستم انتهایی تولیدکننده‌ی درخواست دارای هیچ آدرس IP نیست، از آدرس برابر با 0.0.0.0 به عنوان آدرس مبدأ استفاده می‌کند و با توجه به اینکه آدرس IP کارپذیر را نمی‌داند، بسته را به صورت همه‌پخشی ارسال می‌کند. استفاده از یک مقدار شناسه‌ی تراکنش[۴۰] باعث متمایز شدن این پیام و پاسخ آن از سایر پیام‌های DHCP در شبکه می‌گردد و امکان تشخیص پاسخ را برای سیستم انتهایی تازه وارد فراهم می‌نماید.

در پاسخ به پیام DHCP DISCOVER، کارپذیر با استفاده از یک پیام DHCP OFFER خود را معرفی کرده و پارامترهای مورد نیاز را پیشنهاد می‌کند. آدرس IP مبدأ برای این پیام برابر با آدرس IP کارپذیر DHCP است و به دلیل اینکه مقصد هنوز دارای آدرس IP نیست، بسته به صورت همه پخشی ارسال می‌شود. فیلد yiaddrr مشخص‌کننده‌ی آدرس IP پیشنهاد شده توسط کارپذیر DHCP است. همچنین، در یا بسته آدرس IP کارپذیر DHCP به عنوان شناسه‌ی آن ثبت شده است و یک مقدار طول عمر نیز مشخص شده است. مقدار طول عمر، مدت زمان مشخص شده تا منقضی شدن رزرو آدرس IP در کارپذیر DHCP را معین می‌کند.

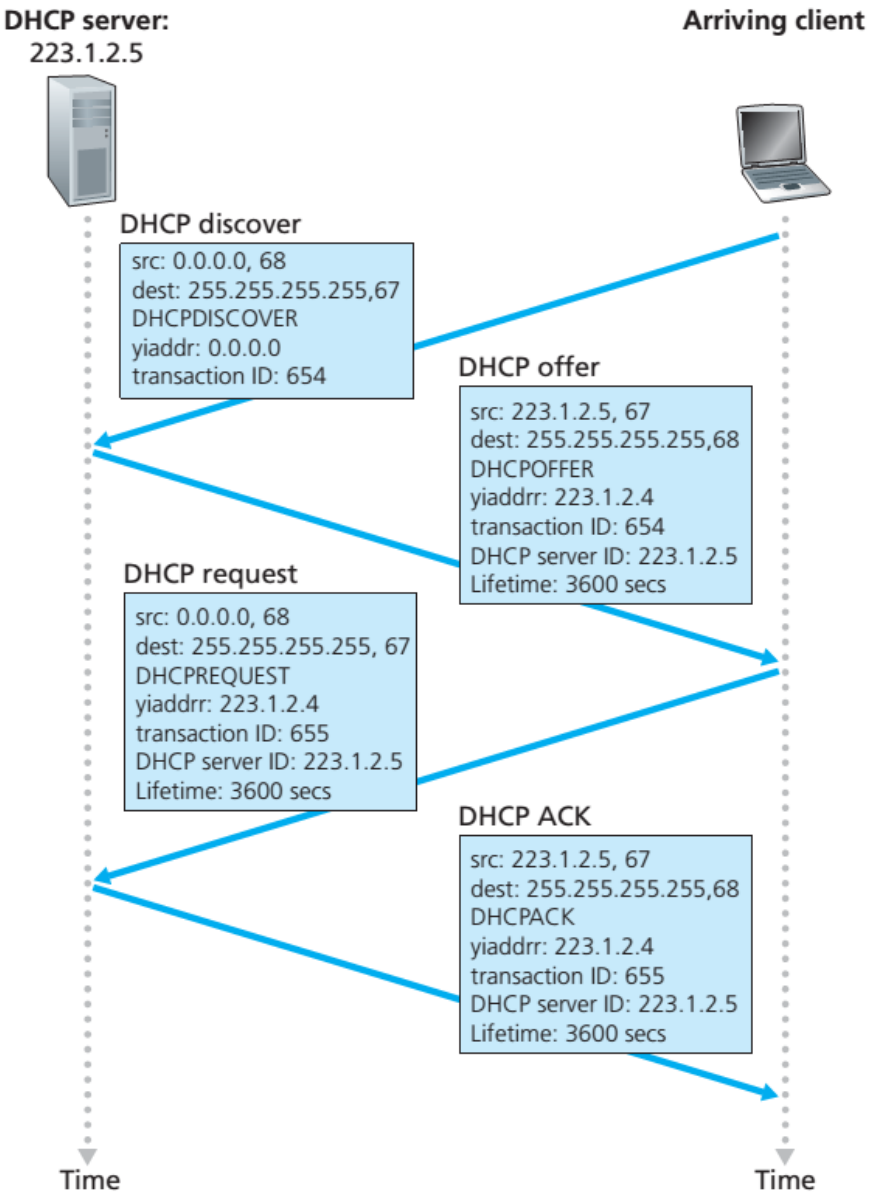
از بین پیشنهادهای دریافت شده، کارخواه فقط یکی از آنها را انتخاب می‌کند و یک پیام DHCP REQUEST را به طور مستقیم (تک‌پخشی[۴۱]) برای آن ارسال می‌کند تا پارامترهای پیشنهاد شده برای کارخواه قطعی و ثبت شوند. هنوز این سیستم انتهایی دارای آدرس IP نمی‌باشد و از آدرس IP برابر با 0.0.0.0 به عنوان آدرس مبدأ استفاده می‌کند. این بسته به صورت همه‌پخشی ارسال می‌شود تا سایر کارپذیرهای موجود در شبکه از انتخاب این سیستم انتهایی مطلع شوند. شناسه‌ی تراکنش در این بسته به روزرسانی شده است.

سیستم انتهایی کارپذیر در قالب یک پیام DHCP ACK پارامترها را مجدد ارسال می‌کند و آدرس IP آن‌را ثبت می‌نماید. سپس، سیستم انتهایی کارخواه نیز می‌تواند با این پارامترها خود را پیکربندی کرده و کارش را آغاز کند.

---

[38] Server
[39] DHCP Server
[40] Transaction ID
[41] Unicast

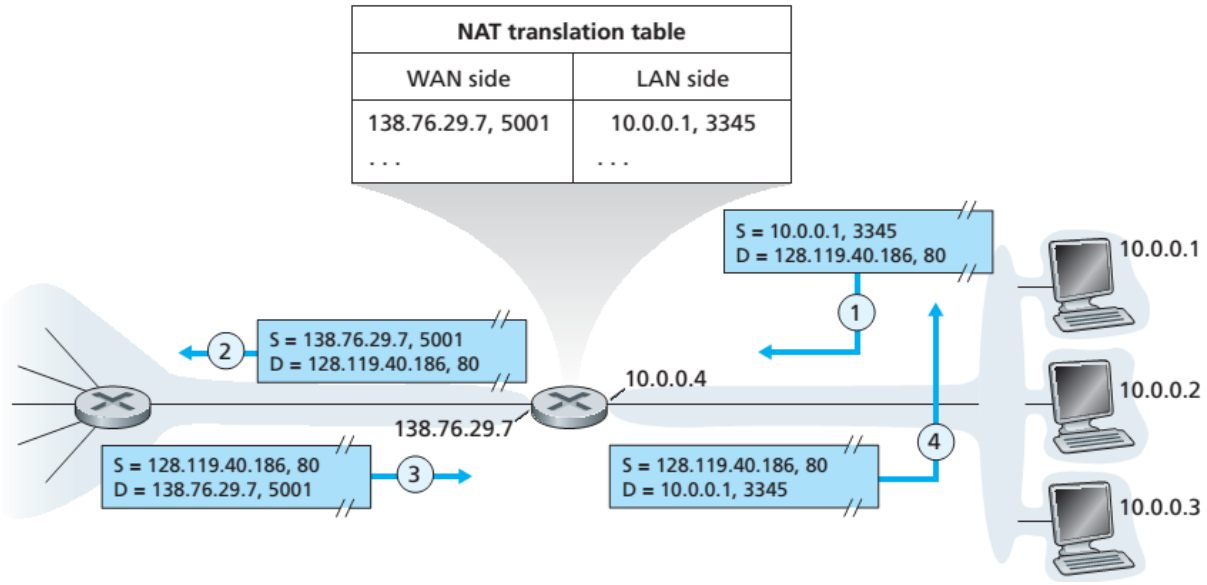
سیستم انتهایی کارخواه می‌تواند با ارسال یک پیام DHCP RELEASE آدرس IP خود را آزاد کند (مثلاً پیش از ترک یک شبکه). در نتیجه، با توجه به اینکه برای یک آدرس IP طول عمر یا زمان انقضا مشخص می‌شود و ممکن است که مدت حضور سیستم انتهایی در شبکه بیش از این مدت مشخص شده باشد، لازم است که در این مدت چند پیام DHCP REQUEST توسط کارخواه به سمت کارپذیر ارسال گردند وگرنه پس از زمان انقضا آدرس نامعتبر خواهد بود. شکل ۱۸ نمایش‌دهنده روند ذکر شده در یک شبکه‌ی محلی می‌باشد.



شکل ۱۸ تعامل کارخواه و کارپذیر *DHCP*

۱۳. Network Address Translation یا NAT

همان‌طور که قبلاً گفته شد، فیلد آدرس IP در سرآیند بسته‌های IP قادر به حمل ۳۲ بیت داده می‌باشد و به عبارتی، آدرس IP سیستم‌های انتهایی در اینترنت ۳۲ بیتی است. بنابراین، حداکثر 2^{32} یا ۴۲۹۴۹۶۷۲۹۶ آدرس IP قابل تعریف می‌باشند که با توجه به تعداد قابل توجه سیستم‌های انتهایی متصل به اینترنت و روند رو به رشد آنها، به نظر می‌رسد که ممکن است برای پاسخ‌گویی به نیاز اینترنت کافی نباشد. یکی از راه‌هایی که برای رفع این مشکل مطرح شده است و به شکل گسترده‌ای مورد استفاده قرار گرفته است، ترجمه‌ی آدرس شبکه[۴۲] یا NAT است. شکل ۱۹ نمایش‌دهنده‌ی مثالی از عملکرد NAT است.



شکل ۱۹ یک نمونه از عملکرد *NAT*

مسیریاب نمایش داده شده در وسط شکل ۱۹ دارای یک واسط متصل به شبکه‌ی خانگی و محلی و همچنین، دارای یک واسط دیگر متصل به اینترنت می‌باشد. تمام آدرس‌های IP منتسب شده به واسط‌های شبکه در شبکه‌ی خانگی در یک زیرشبکه‌ی مشترک با آدرس زیرشبکه‌ی 10.0.0.0/24 قرار دارند (هم‌خانواده هستند). این محدوده‌ی آدرس، یکی از سه محدوده‌ی رزرو شده (محدوده‌های آدرس 10.0.0.0/8، 172.16.0.0/12 و 192.168.0.0/16) برای آدرس‌دهی به شبکه‌های محلی خصوصی می‌باشد (یک شبکه‌ی خصوصی شبکه‌ای است که آدرس‌های آن فقط برای سیستم‌های انتهایی داخل آن شبکه معنادار می‌باشند). در واقع، هیچ بسته‌ای در اینترنت (ورای شبکه‌ی محلی) نمی‌تواند از آدرس‌های موجود در این محدوده‌ها به عنوان آدرس مبدأ یا مقصد استفاده نماید زیرا، چند صد یا چند هزار شبکه‌ی دیگر وجود دارند که از همین محدوده برای آدرس‌دهی به سیستم‌های انتهایی خود استفاده می‌نمایند.

مسیریاب مجهز به NAT، توسط اینترنت به عنوان یک مسیریاب مشاهده نمی‌شود و به جای آن، مانند یک سیستم انتهایی مستقل با یک آدرس IP مستقل مشاهده می‌شود. در شکل ۱۹ مشاهده می‌شود که تمام بسته‌های خروجی از مسیریاب به سمت اینترنت دارای آدرس مبدأ 138.76.29.7 هستند و بسته‌های ورودی

[42] Network Address Translation

به مسیریاب از طرف اینترنت دارای آدرس مقصد برابر با 138.76.29.7 هستند. به نوعی مشاهده می‌شود که مسیریاب مجهز به NAT جزئیات شبکه‌ی خانگی را از اینترنت مخفی نگه می‌دارد. ذکر این نکته نیز خالی از لطف نمی‌باشد که یکی از روش‌های اخصاص آدرس‌های IP به سیستم‌های انتهایی مشاهده شده در شکل ۱۹، استفاده از یک کارپذیر DHCP[۴۳] است. آدرس IP واسط سمت اینترنت مسیریاب توسط کارپذیر DHCP در ISP به آن اختصاص یافته است و آدرس‌های IP سیستم‌های انتهایی توسط کارپذیر DHCP اجرا شده در مسیریاب به آنها اختصاص یافته است.

بنابراین، عملکرد NAT بدین صورت است که هر کدام از سیستم‌های انتهایی ترافیک خود را با ثبت آدرس IP خود در آن تولید می‌کنند و در حین عبور بسته‌های مربوط به این ترافیک از مسیریاب مجهز به NAT، بخشی از مشخصات آنها دچار تغییر می‌شود (مثلاً آدرس IP مبدأ آنها با آدرس IP سمت اینترنت مسیریاب جایگزین می‌شود) و به سمت اینترنت ارسال می‌شوند. اما، سؤالی که مطرح می‌شود این است که مسیریاب چگونه بسته‌های ورودی از سمت اینترنت را به سیستم انتهایی درست ارسال می‌کند. در واقع این کار با استفاده از یک جدول ترجمه‌ی NAT و ثبت آدرس‌های IP و شماره‌های پورت در آن انجام می‌شود.

به عنوان مثال فرض شود که کاربر استفاده کننده از سیستم انتهایی 10.0.0.1 یک صفحه‌ی وب بر روی یک کارپذیر وب (پورت 80) با آدرس IP برابر با 128.119.40.186 را درخواست می‌دهد. این سیستم انتهایی شماره‌ی پورت 3345 را به صورت دلخواه بر روی بسته ثبت می‌کند و آن‌را با آدرس IP خودش به عنوان آدرس مبدأ برای مسیریاب ارسال می‌کند (این مسیریاب از دید سیستم‌های انتهایی درون شبکه‌ی خانگی یک مسیریاب واقعی است). مسیریاب بسته را دریافت می‌کند، یک شماره‌ی پورت جدید (5001) برای آن تولید می‌کند، آدرس IP سمت اینترنت خود را با آدرس IP مبدأ آن را جایگزین می‌کند و شماره‌ی پورت قدیمی را با شماره‌ی پورت جدید جایگزین می‌کند. در واقع فقط هر کدام از شماره پورت‌هایی که در جدول ترجمه‌ی NAT موجود نباشند می‌توانند به عنوان شماره‌ی پورت جدید انتخاب شوند (شماره‌ی پورت یک عدد ۱۶ بیتی است که بیش از ۶۰۰۰۰ شماره‌ی پورت همزمان را ممکن می‌سازد). این نگاشت در جدول ترجمه‌ی NAT ثبت می‌گردد.

حال، آن دسته از بسته‌های ورودی به مسیریاب از طرف اینترنت که آدرس مقصد آنها برابر با آدرس مقصد ثبت شده در جدول است و شماره‌ی پورت مقصد آنها نیز برابر با 5001 است دچار تغییر می‌شوند و آدرس سیستم انتهایی تولید کننده‌ی درخواست و شماره‌ی پورت استفاده شده برای تولید درخواست در آنها ثبت می‌گردد. بدین ترتیب، بسته‌ها توسط سیستم انتهایی درست و برنامه‌ی کاربردی درست دریافت می‌شوند.

[43] DHCP Server

۱۴. الگوریتم‌های مسیریابی

به نوعی می‌توان الگوریتم‌های مسیریابی را به دو دسته‌ی ایستا[۴۴] و پویا[۴۵] تقسیم نمود. در روش ایستا، جدول پیش‌رانی/مسیریابی به صورت دستی و در زمان پیکربندی مسیریاب تنظیم می‌شود و درطول زمان ثابت می‌ماند. هر گونه تغییر در این جدول نیز توسط مدیر شبکه اعمال می‌گردد. در روش پویا، جدول مسیریابی هر T ثانیه و بر اساس عواملی همچون آخرین وضعیت توپولوژی (شکل اتصال دستگاه‌های شبکه و لینک‌های آن) یا میزان ترافیک شبکه به‌روزرسانی می‌شوند.

از یک دیدگاه دیگر می‌توان این الگوریتم‌ها را به دو دسته‌ی «سراسری متمرکز[۴۶]» و «غیرمتمرکز توزیع شده[۴۷]» تقسیم نمود. در روش متمرکز هر مسیریاب لازم است اطلاعات تمام مسیریاب‌های موجود در شبکه و ارتباط بین آنها را جمع‌آوری نماید و پس از تشکیل گراف شبکه، به منظور یافتن بهترین مسیر بین دو مسیریاب از یک الگوریتم یافتن کوتاهترین مسیر مناسب (مثل الگوریتم دایجسترا[۴۸]) استفاده کند. به این الگوریتم‌ها اصطلاحاً الگوریتم‌های LS (Link State Algorithm) نیز گفته می‌شود.

در روش غیرمتمرکز، مسیریاب اطلاعات کاملی از زیرساخت شبکه ندارد و فقط قادر است هزینه‌ی ارتباط با مسیریاب‌هایی که به طور مستقیم با آنها در ارتباط است (**مسیریاب‌های همسایه**) را محاسبه نماید. سپس، در فواصل زمانی منظم هر مسیریاب جداول مسیریابی خود را فقط برای مسیریاب‌های همسایه ارسال می‌نماید و در نتیجه این مسیریاب‌ها می‌توانند با توجه به مقادیری که خود محاسبه کرده بودند، جدول خود را کامل کرده و مسیر بین مسیریاب‌های مختلف را تعیین کنند. این الگوریتم‌ها پیچیدگی زمانی بسیار کمی دارند. به این الگوریتم‌ها اصطلاحاً DV (Distance Vector Algorithm) گفته می‌شود.

۱۵. روش ارسال سیل آسا یا Flooding

این روش برای ارسال بسته‌های همگانی (مثل اعلام جداول مسیریابی در پروتکل‌های LS) کاربرد دارد. در این روش، هر مسیریاب موظف است که با دریافت یک بسته آن‌را بر روی تمام واسطهای خروجی خود به

[44] Static
[45] Dynamic
[46] Global Routing Algorithm
[47] Decentralized Routing Algorithm
[48] Dijkstra Shortest Path Algorithm

جز واسطی که بسته را از آن دریافت کرده ارسال نماید. در نتیجه، تمام مسیریاب‌های موجود بسته‌ی مورد نظر را دریافت خواهند کرد و بسته در سریع‌ترین زمان ممکن به مقصد می‌رسد.

لازم به ذکر است که ممکن است پس از ارسال یک بسته توسط مسیریاب، آن بسته پس از طی چند گام مجدداً وارد مسیریاب مورد نظر (که قبلاً یک‌بار بسته را ارسال کرده بود) شود که اگر با آن مقابله نشود به بروز مشکل دور بی‌نهایت منجر می‌شود. این مشکل با درج یک شماره‌ی شناسایی منحصر به فرد بر روی بسته و ذخیره‌ی این اطلاعات توسط مسیریاب‌ها (در صورت مشاهده‌ی مجدد بسته، مسیریاب آنرا شناسایی می‌کند) یا با استفاده از فیلد طول عمر بسته برطرف می‌شود.

۱۶. الگوریتم‌های LS

به طور کلی در یک الگوریتم مسیریابی LS باید پنج عمل زیر توسط هر مسیریاب اجرا شوند:

۱. مسیریاب‌های همسایه‌ی خود را شناسایی کرده و آدرس IP آنها را بدست آورد. این کار با ارسال یک بسته‌ی خاص به نام Hello Packet بر روی تمام واسط‌های خروجی مسیریاب انجام می‌شود. مسیریاب‌هایی که به صورت مستقیم با فرستنده‌ی پیام در ارتباط هستند، به آن پاسخ می‌دهند و پس از دریافت اطلاعات توسط فرستنده‌ی Hello Packet، اطلاعات مورد نظر در یک جدول ذخیره می‌شوند.

۲. هزینه‌ی مسیر تا مسیریاب‌های مجاور خود را اندازه‌گیری نماید. این کار ممکن است با روش خاصی و به صورت خودکار محاسبه شود (مثلاً با ارسال بسته‌های Echo و دریافت پاسخ آن و محاسبه‌ی زمان رفت و برگشت آن).

۳. یک بسته تولید کند و تمام اطلاعاتی که از مسیریاب‌های همسایه خود بدست آورده را در آن قرار دهد. به این بسته، بسته‌ی «LS» گفته می‌شود و شامل آدرس جهانی مسیریاب تولیدکننده‌ی بسته، یک شماره‌ی ترتیب (برای تشخیص بسته‌ها جدید از بسته‌های تکراری)، طول عمر بسته (اطلاعات بسته زمان انقضا دارند) و آدرس جهانی مسیریاب‌های همسایه‌ی تولیدکننده‌ی بسته به همراه هزینه‌ی تخمینی مسیر رسیدن به آنها می‌باشد. تولید و توزیع هماهنگ این بسته‌ها به عنوان یک مسأله‌ی مهم به شمار می‌رود (ممکن است این بسته‌ها به صورت دوره‌ی برای سایر مسیریاب‌ها ارسال شوند یا اینکه در صورت ایجاد یک تغییر اساسی در زیرساخت شبکه جدول مورد نظر ارسال گردد).

۴. بسته‌ی تولید شده را به صورت سیل‌آسا برای تمام مسیریاب‌های موجود در شبکه ارسال کند و بسته‌های ارسالی توسط آنها را دریافت و ذخیره کند و مجدداً آنرا ارسال نماید. با ورود یک بسته‌ی جدید، مسیریاب شماره‌ی ترتیب آنرا بررسی می‌کند و در صورتی که قبلاً آنرا مشاهده نکرده باشد (این بررسی به منظور پیش‌گیری از مشکل دور بی‌نهایت در ارسال سیل‌آسا انجام می‌شود)، اطلاعات آنرا در یک جدول موقت ذخیره کرده و بسته را بر روی تمام واسط‌های خروجی خود (به غیر از واسط ورودی آن) ارسال می‌کند. پس از دریافت یک بسته با یک شماره‌ی خاص، بسته‌های دارای شماره‌ی کوچکتر از آن دریافت نخواهند شد.

۵. گراف شبکه را تشکیل داده و با استفاده از یک الگوریتم مناسب مسیر بهینه را بین هر دو مسیریاب در شبکه تعیین نماید. یکی از نمونه‌های مسیر بهینه بین دو مسیریاب کوتاه‌ترین مسیر بین آنها است که می‌توان برای یافتن آن از الگوریتم دایجسترا استفاده نمود. جدول حاصل شده پس از اجرای محاسبات تا دفته‌ی بعد که فرایند به‌روزرسانی انجام می‌شود در اختیار پروتکل IP قرار خواهد داشت. لازم به ذکر است که اگر یک مسیریاب اطلاعات غلطی را برای سایر مسیریاب‌ها فراهم کند، کل مسیریابی شبکه با مشکل مواجه می‌شود و تمام جداول مسیریابی با اطلاعات آلوده تنظیم خواهند شد.

در ادامه با یک مثال استفاده از الگوریتم دایجسترا شرح داده می‌شود. شکل ۲۰ نمایش‌دهنده‌ی مراحل مختلف انجام این مثال است. در این مثال با توجه به گراف شبکه‌ی موجود و با توجه به هزینه‌ی ثبت شده برای مسیرهای بین هر جفت مسیریاب، کم‌هزینه‌ترین مسیر بین گره A (مسیریاب A) و گره D یافت می‌شود. لازم است که در طول اجرای مثال به ازای هر کدام از گره‌ها اطلاعات مشخصی شامل هزینه‌ی فعلی از مبدأ تا این گره، گره قبلی در مسیر حاصل شده و یک مشخصه‌ی خاص برای تعیین وضعیت گره (دائمی یا موقت) نگهداری می‌شوند. مقدار اولیه برای هزینه برابر با مقدار بی‌نهایت است. گره قبلی در مسیر در ابتدای کار بدون مقدار است و وضعیت اولیه‌ی تمام گره‌ها در ابتدای کار به صورت موقت می‌باشد. مراحل مختلف اجرای مثال در ادامه ذکر می‌گردند.

- مرحله‌ی ۱: وضعیت گره مبدأ که همان گره A است به صورت دائمی تغییر می‌کند. بدین معنی که کار این گره در فرایند یافتن کوتاه‌ترین مسیر پایان یافته است. در شکل ۲۰ گره‌های دائمی با یک دایره‌ی توپر نمایش داده شده‌اند. در این مرحله که نشان‌گر (➔) به گره A اشاره می‌کند، هزینه از مبدأ تا گره‌های همسایه‌ی این گره (گره‌های B و G که دارای وضعیت موقت هستند) محاسبه شده و به همراه گره پیشین در مسیر (گره A)، برای گره‌های همسایه ثبت می‌گردد.
- مرحله‌ی ۲: سپس از بین تمام گره‌های دارای وضعیت موقت، گره با کمترین مقدار هزینه تا مبدأ (گره B) انتخاب می‌شود، نشان‌گر به آن انتقال یافته و وضعیت آن به دائمی تغیر می‌یابد.

- مرحله‌ی ۳: مقدار هزینه از گره A تا گره‌های همسایه‌ی B که دارای وضعیت موقت هستند (گره‌های C و E) محاسبه شده و به همراه گره پیشین در مسیر (گره B) برای آنها ثبت می‌شود. در این مرحله از بین تمام گره‌های دارای وضعیت موقت، گره E دارای کمترین هزینه تا مبدأ است و نشان‌گر به آن انتقال می‌یابد. وضعیت گره E نیز به صورت دائمی ثبت می‌گردد.

- مرحله‌ی ۴: هزینه‌ی گره‌های همسایه‌ی E که دارای وضعیت موقت هستند محاسبه یا اصلاح می‌شود و گره پیشین در مسیر برای آنها ثبت می‌گردد. توجه شود که با وجود اینکه مقدار هزینه تا مبدأ، قبلاً برای گره G محاسبه شده بود، به دلیل اینکه مقدار هزینه‌ی جدید از مقدار قبلی ثبت شده کمتر است، مقدار جدید مورد استفاده قرار می‌گیرد و گره قبلی در مسیر نیز برای آن اصلاح می‌شود و شامل گره E می‌گردد. از بین تمام گره‌های دارای وضعیت موقت، گره G دارای کمترین مقدار هزینه است و نشان‌گر به آنجا انتقال می‌یابد و وضعیت آن به صورت دائمی می‌گردد.

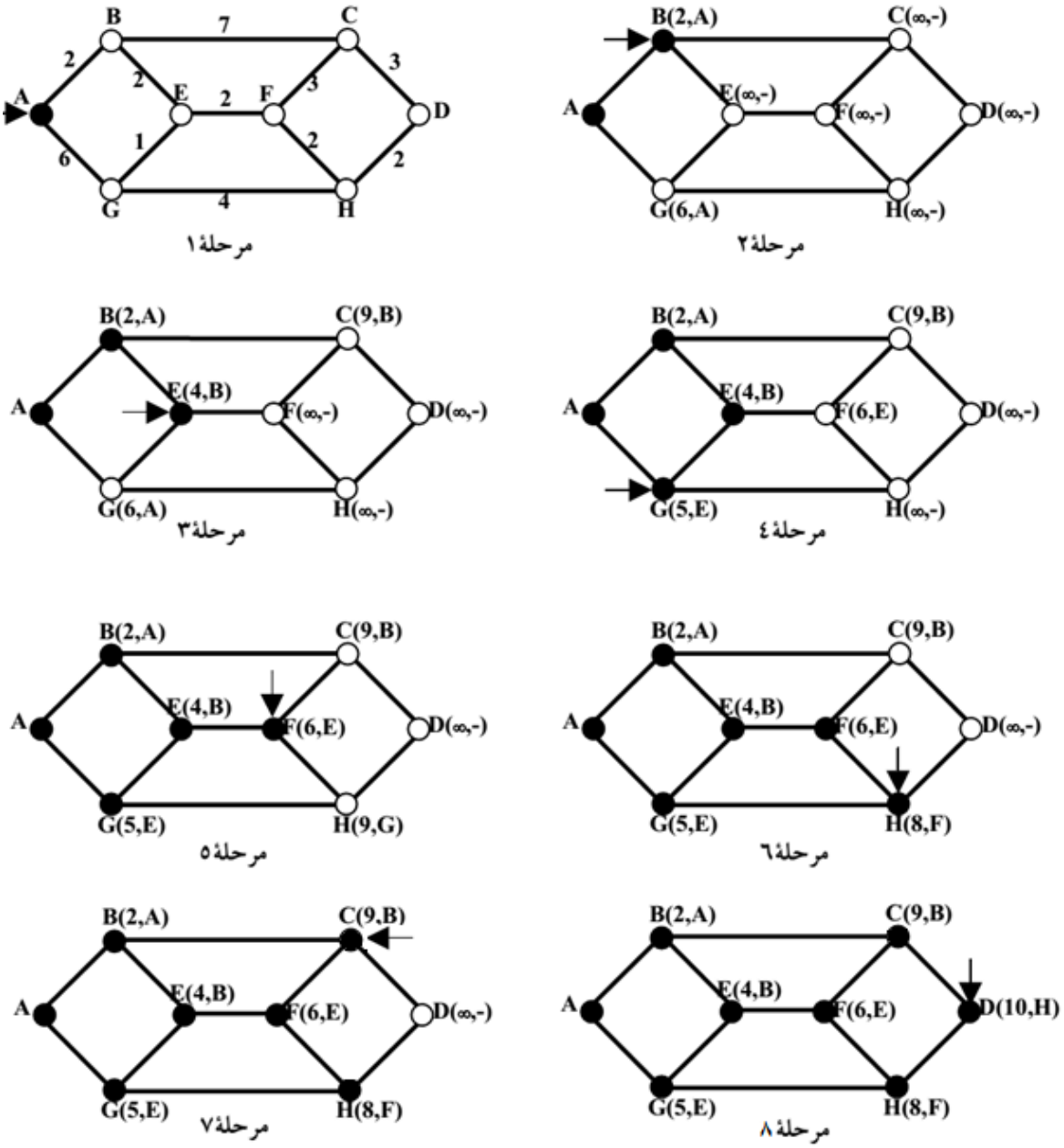
- مرحله‌ی ۵: پس از اصلاح هزینه‌ی گره‌های موقت همسایه‌ی G و ثبت گره قبلی در مسیر برای آنها، از بین تمام گره‌های موقت موجود در گراف، گره F به عنوان گره جاری انتخاب شده و نشان‌گر به آنجا انتقال می‌یابد. وضعیت این گره به صورت دائمی می‌شود.

- مرحله‌ی ۶: هزینه‌ی گره‌های C و H به عنوان همسایه‌های موقت گره F محاسبه شده و گره قبلی در مسیر برای آنها ثبت می‌گردد. هزینه از مبدأ تا گره H اصلاح شده و از مقدار ۹ به ۸ کاهش می‌یابد. از بین تمام گره‌های موقت موجود (گره‌های C، H و D) گره H دارای کمتری ن هزینه تا مبدأ است و نشان‌گر به آنجا انتقال می‌یابد که باعث دائمی شدن وضعیت آن می‌گردد.

- مرحله‌ی ۷: هزینه‌ی گره‌های همسایه‌ی H که وضعیت موقت دارند (گره D) تا مبدأ (گره A) محاسبه شده و به همراه گره قبلی در مسیر برای آن ثبت می‌شود. در این قسمت مشاهده می‌شود که از بین گره‌های موقت موجود در گراف (گره‌های C و D)، گره C از هزینه‌ی کمتری برخوردار است. پس نشانگر به آنجا انتقال یافته و وضعیت آن دائمی می‌شود.

- مرحله‌ی ۸: با محاسبه‌ی مقدار هزینه‌ی جدید برای گره D (تنها گره موقت موجود) مشاهده می‌شود که هزینه‌ی قبلی آن از وضعیت بهتری برخوردار است (مقدار کمتری دارد) و در نتیجه، مقدار جدید محاسبه شده برای آن ثبت نمی‌شود. تنها گره موقت موجود (یعنی گره D که همان مقصد است) در این مرحله به وضعیت دائمی انتقال می‌یابد در شرایطی که هزینه‌ی رسیدن به آن از گره مبدأ برابر با 10 است و گره قبلی آن در مسیر برابر با گره H است.

در نهایت و برای بدست آوردن مسیر کامل، از گره D شروع کرده و گره قبلی آن پیدا می‌شود. این کار به صورت بازگشتی انجام می‌شود تا به نقطه‌ی شروع (گره A) برسد.

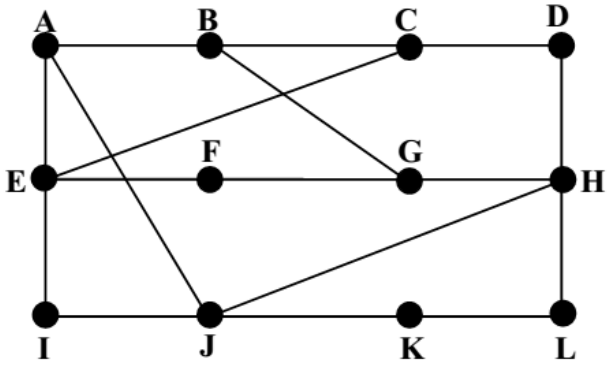


شکل ۲۰ مراحل مختلف اجرای یک نمونه مثال از الگوریتم دایجسترا

۱۷. الگوریتم‌های DV

در جدول مسیریابی مربوط به این روش پویای در مسیریابی دو فیلد وجود دارد. یکی **فیلد مسیر** که واسط خروجی مناسب برای رسیدن به یک مسیریاب خاص در شبکه را مشخص می‌کند و **فیلد مقدار تقریبی هزینه** که هزینه‌ی تقریبی رسیدن یک بسته تا مسیریاب مقصد را تعیین می‌کند. در این روش بر

خلاف الگوریتم‌های LS، جدول مسیریابی بدون اطلاع از هزینه‌ی مربوط به کل لینک‌های ارتباطی در شبکه تکمیل می‌گردد. شکل ۲۱ نمایش‌دهنده‌ی یک شبکه‌ی فرضی و جدول مسیریابی الگوریتم DV برای یکی از گره‌های آن (گره J) است. منظور از خط در شکل همان واسط خروجی است. واحد هزینه می‌تواند تأخیر یا تعداد گام (Hop) در نظر گرفته شود.



	هزینهٔ تقریبی	خط
A	8	A
B	20	A
C	28	I
D	20	H
E	17	I
F	30	I
G	18	H
H	12	H
I	10	I
J	0	—
K	6	K
L	15	K

شکل ۲۱ یک شبکه‌ی فرضی و جدول مسیریابی الگوریتم *DV* برای گره *J*

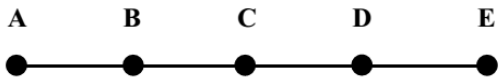
روش تکمیل جداول مسیریابی در یک الگوریتم DV بدین صورت است که ابتدا هر مسیریاب هزینه تا هر کدام از مسیریاب‌های همسایه‌ی خود را یافته و در جدول درج می‌نماید. گام بعدی به این مسیریاب‌ها برابر با شناسه‌ی خود آنها است. مسیریاب‌ها موظفند در بازه‌های زمانی مشخص (هر T ثانیه)، ستون هزینه (Distance Vector) از جدول مسیریابی خود را برای مسیریاب‌های همسایه‌ی خود ارسال نمایند (فقط مسیریاب‌های همسایه و نه تمام مسیریاب‌های حاضر در شبکه). هر مسیریاب بر اساس اطلاعات دریافت شده جدول مسیریابی خود را به‌روزرسانی می‌کند.

به‌روزرسانی جدول هر مسیریاب بدین صورت است که با مشاهده‌ی مقادیر جدید در ستون‌های هزینه‌ی دریافت شده از طرف همسایه‌ها، هزینه تا این گره جدید به صورت محاسبه‌ی مجموع هزینه تا هر کدام از همسایه‌ها که گره مورد نظر را در اطلاعات ارسالی ذکر کرده‌اند و هزینه از آن همسایه تا گره جدید و سپس، انتخاب حداقل هزینه‌ی حاصل شده محاسبه می‌شود. به طور مثال، ستون‌های هزینه‌ی نمایش‌داده شده در شکل ۲۲ برای تکمیل جدول مسیریابی نشان داده شده در شکل ۲۱ مورد استفاده قرار می‌گیرند. به عنوان نمونه مشاهده می‌شود که هزینه‌ی گره J تا گره گره G برابر است با 18 که از مجموع هزینه‌های 12 (هزینه تا گره H) و 6 (هزینه از گره H تا گره G) بدست می‌آید. مشاهده می‌شود در صورتی که برای رسیدن به یک گره مشخص چند هزینه‌ی مختلف از چند مسیریاب مختلف (به عنوان گام بعد) فراهم بود، مقدار هزینه‌ی حداقل انتخاب می‌شود. جدول حاصل شده تا به‌روزرسانی بعدی مورد استفاده قرار می‌گیرد. حجم جدول مورد نظر در این روش بسیار کمتر از جدول نگهداری شده در روش LS است.

	A	I	H	K
A	0	24	20	21
B	12	36	31	28
C	25	18	19	36
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	6	31
H	17	20	0	19
I	21	0	14	22
J	9	11	7	10
K	24	22	22	0
L	29	33	9	9

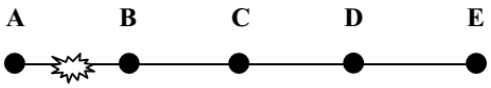
شکل ۲۲ ستون هزینه‌ی دریافت شده توسط مسیریاب *J* از طرف مسیریاب‌های *A*، *I*، *H* و *K*

یک مشکل موجود در این روش مسیریابی، «عدم همگرایی سریع جداول مسیریابی» پس از خروج یک مسیریاب یا یک لینک از شبکه است (مثلاً در اثر خرابی) که به آن شمارش تا بی‌نهایت هم گفته می‌شود. به عنوان مثال، شکل ۲۳ نمایش‌دهنده‌ی یک شبکه‌ی فرضی و جدول مسیریابی هر کدام از مسیریاب‌ها پیش از ایجاد خرابی در شبکه است و شکل ۲۴ نمایش‌دهنده‌ی خروج لینک بین مسیریاب‌های A و B و روند ایجاد تغییرات در جدول مسیریابی هر کدام از مسیریاب‌ها است. یکی از راه‌حل‌ها برای این مشکل بدین صورت است که مسیریاب‌ها در ستون هزینه‌ی ارسال شده به هر مسیریاب، مدخل‌هایی که مسیر رسیدن به آنها از مسیریاب دریافت‌کننده‌ی پیام است را حذف می‌کند و یا آن را برابر با مقدار بی‌نهایت ∞ قرار می‌دهد.



A	0,-	1,A	2,B	3,C	4,D
B	1,B	0,-	1,B	2,C	3,D
C	2,B	1,C	0,-	1,C	2,D
D	3,B	2,C	1,D	0,-	1,D
E	4,B	3,C	2,D	1,E	0,-

شکل ۲۳ جدول مسیریابی مسیریاب‌ها پیش از خرابی لینک بین مسیریاب‌های *A* و *B*



هزینهٔ رسیدن به A در هنگام بروز خرابی	A	∞,A	2,B	3,C	4,D
هزینهٔ رسیدن به A پس از اولین به‌هنگام‌سازی	A	3,C	2,B	3,C	4,D
هزینهٔ رسیدن به A پس از دومین به‌هنگام‌سازی	A	3,C	4,B	3,C	4,D
هزینهٔ رسیدن به A پس از سومین به‌هنگام‌سازی	A	5,C	4,B	5,C	4,D
هزینهٔ رسیدن به A پس از چهارمین	A	5,C	6,B	5,C	6,D
هزینهٔ رسیدن به A پس از پنجمین به‌هنگام‌سازی	A	7,C	6,B	7,C	6,D
هزینهٔ رسیدن به A پس از ششمین به‌هنگام‌سازی	A	7,C	8,B	7,C	8,D
هزینهٔ رسیدن به A پس از به‌هنگام‌سازی n ام	A	….	….	….	….
∞	A	∞	∞	∞	∞

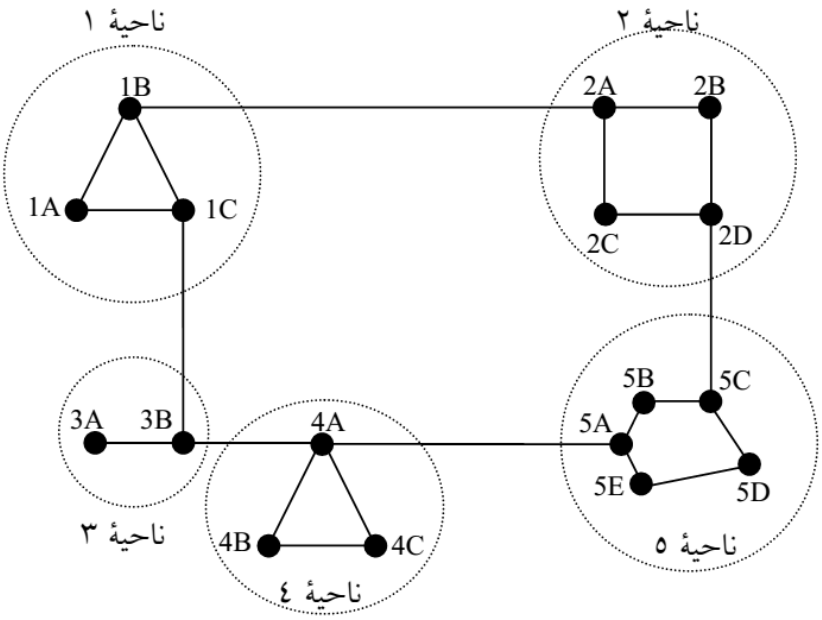
شکل ۲۴ جدول مسیریابی مسیریاب‌ها پس از خرابی لینک بین مسیریاب‌های A و B

۱۸. مسیریابی سلسله‌مراتبی

زمانی که یک شبکه رشد می‌کند و بزرگ می‌شود، شبکه‌های محلی و مسیریاب‌ها اضافه می‌شوند و حجم جداول مسیریابی و زمان لازم برای تعیین گام بعدی برای یک بسته افزایش می‌یابد. به طور مثال، یک جدول مسیریابی برای یک الگوریتم LS یا DV ممکن است شامل صدها یا هزاران مسیریاب باشد که ذخیره، پردازش و ارسال جداول مسیریابی را تحت تأثیر قرار می‌دهد.

در مسیریابی سلسله‌مراتبی، مسیریاب‌ها در گروه‌هایی به نام «ناحیه» (Area) دسته‌بندی می‌شوند و هر مسیریاب فقط «نواحی» و مسیریاب‌های درون ناحیه‌ی خود را می‌شناسد و هیچ اطلاعی از مسیریاب‌های درون نواحی دیگر ندارد. به طور مثال، شکل ۲۵ تقسیم‌بندی یک شبکه به پنج ناحیه‌ی کوچکتر را نمایش می‌دهد. در جدول مسیریابی هر مسیریاب به ازای هر ناحیه‌ی به غیر از ناحیه‌ی خودش یک مدخل و به ازای هر کدام از مسیریاب‌های حاضر در ناحیه‌ی خودش نیز یک مدخل ثبت می‌شود. شکل ۲۶ نمایش‌دهنده‌ی جدول مسیریابی برای مسیریاب 1A در مثال شکل ۲۵ است. اگر از مسیریابی سلسله مراتبی استفاده نمی‌شد، تعداد مدخل‌های جدول به جای ۷ برابر با ۱۷ بود.

همچنین، به منظور ساده‌تر شدن جداول می‌توان از روش «سلسله‌مراتبی سه‌سطحی» استفاده کرد تا حجم جداول باز هم کاهش یابد به طوری که هر شبکه به چند «دسته» یا Cluster، هر «دسته» به چند «ناحیه» یا Region تقسیم می‌شود و هر ناحیه دربرگیرنده‌ی چند مسیریاب است. حتی می‌توان تعداد سلسله‌مراتب را از عدد سه نیز بالاتر برد که به بزرگی شبکه بستگی دارد.



شکل ۲۵ نمونه‌ای از تقسیم یک شبکه به چند ناحیه‌ی کوچکتر

مقصد	خطّ	هزینه
1A	–	–
1B	1B	1
1C	1C	1
Region	1B	2
Region	1C	2
Region	1C	3
Region	1C	4

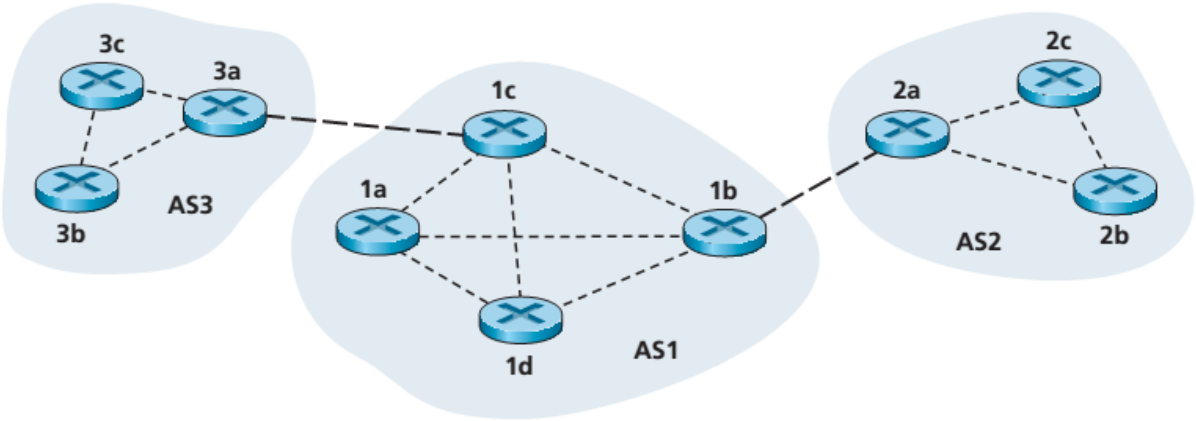
شکل ۲۶ جدول مسیریابی مسیریاب *1A* در شبکه‌ی نمایش داده شده در شکل ۲۵

۱۹. مسیریابی در اینترنت

اینترنت شامل مجموعه‌ای از شبکه‌های خودمختار (Autonomous System یا AS) و مستقل است که به یکدیگر متصل شده‌اند و شبکه‌ی اینترنت را تشکیل داده‌اند. یک شبکه‌ی خودمختار شبکه‌ای تحت نظارت و سرپرستی یک مجموعه یا سازمان خاص است که تمام اعمال درون آن از جمله اضافه یا حذف شدن یک شبکه‌ی محلی، اضافه یا حذف شدن سیستم‌های انتهایی و ... با توجه به صلاحدید مسئول شبکه و بر اساس سیاست‌های سازمان انجام می‌شود. علاوه بر موارد ذکر شده، موارد دیگری مانند توپولوژی کل شبکه، سیستم‌های عامل نصب شده بر روی سیستم‌های انتهایی، طراحی زیرساخت ارتباطی، طریقه‌ی اتصال شبکه‌های محلی و حتی نوع پروتکل‌های مسیریابی تحت تأثیر سیاست‌های خاص سازمان مورد نظر انتخاب و بکارگیری می‌شوند که ممکن است با سایر شبکه‌های خودمختار موجود در اینترنت متفاوت باشد.

در حالی که هر کدام از شبکه‌ّهای خودمختار از یک روش مستقل برای مسیریابی درونی خود (بین مسیریاب‌های درونی) استفاده می‌کنند، مسیریابی بسته‌ها بین این شبکه‌های خودمختار به شکل کاملاً متفاوتی انجام می‌شود. در مسیریابی بین ASها مسائلی متفاوتی نسبت به مسیریابی درونی هر کدام از این ASها دخیل می‌باشد. هر کدام از این ASها از دید مسیریابی بین AS به عنوان یک گره در شبکه تلقی می‌شود.

بدین ترتیب، در صورتی که یک سیستم انتهایی حاضر در یک شبکه‌ی خودمختار قصد ارتباط با دنیای خارج از شبکه‌ی خودمختار خود را داشته باشد، لازم است که بسته‌های تولید شده توسط آن از طریق مسیریابی درونی به یکی از مسیریاب‌هایی که ارتباط AS مورد نظر با دنیای خارج را فراهم ساخته است ارسال شود. سپس مسیریاب مورد نظر بسته‌ها را روی زیرساخت خارجی شبکه به جریان می‌اندازند. مسیریاب‌هایی که در درون شبکه‌ی AS نقش برقراری ارتباط‌های داخلی (بین سیستم‌های انتهایی حاضر در AS یکسان که شامل واسط داخلی مسیریاب متصل به دنیای خارج نیز می‌شود) را بر عهده دارند به نام «دروازه‌های درونی[۴۹]» مشهورند و مسیریاب‌هایی که ارتباط شبکه‌های خودمختار متفاوت را برقرار می‌کنند به نام «مسیریاب‌های مرزی» یا «دروازه‌های مرزی[۵۰]» یا «یا مسیریاب‌های BGP» شناخته می‌شوند. مسیریاب‌های مرزی و ساختار ارتباطی آنها تابع قواعد «مسیریابی برونی» و مسیریاب‌های داخلی تابع الگوریتم‌های «مسیریابی درونی» هستند که می‌تواند کاملاً با هم متفاوت باشد. لازم به ذکر است که هر شبکه‌ی خودمختار دارای یک شماره‌ی منحصر به فرد و جهانی با عنوان ASN است. شکل ۲۷ نمایش‌دهنده‌ی سه شبکه‌ی خودمختار AS1، AS2 و AS3 است که به از طریق مسیریاب‌های 1b، 1c، 2a و 3a به هم متصل شده‌اند.



شکل ۲۷ مثالی از سه شبکه‌ی خودمختار متصل به هم

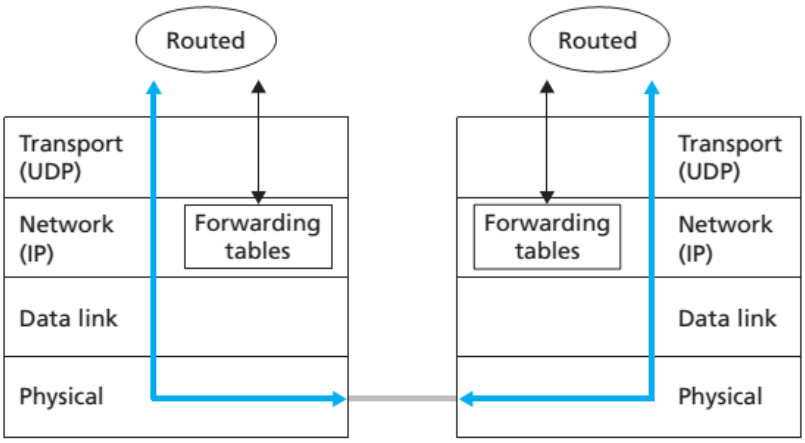
[49] Interior Gateway
[50] Border Gateway

۲۰. پروتکل RIP در مسیریابی درونی

پروتکل RIP[۵۱] ذاتاً مبتنی بر الگوریتم بردار فاصله (DV) است و معیار هزینه برای آن «تعداد گام» می‌باشد (به این معنی که هزینه‌ی ارسال یک بسته بین دو مسیریاب همسایه برابر با ۱ است). این پروتکل یکی از پروتکل‌های قابل استفاده در بخش مسیریابی درونی (درون یک AS مستقل) در شبکه‌ی اینترنت است.

در پروتکل RIP مسیریاب‌ها هر ۳۰ ثانیه جداول مسیریابی خود را برای مسیریاب‌های همسایه ارسال می‌کنند و اگر جدول مسیریابی یک همسایه‌ی شناخته شده پس از ۱۸۰ ثانیه دریافت نشود (به مدت ۱۸۰ ثانیه از همسایه هیچ خبری نباشد)، ضمن درج مقدار ∞ برای هزینه‌ی رسیدن به آن همسایه، این مسأله را با ارسال جدول مسیریابی خود به همسایه‌ها اطلاع می‌دهد. اصطلاحاً به ارسال جداول مسیریابی در پروتکل RIP «اعلان[۵۲]» گفته می‌شود. در این پروتکل هر مسیریاب می‌تواند با ارسال یک «پیام تقاضا[۵۳]» از همسایه‌ی خود در مورد هزینه‌ی رسیدن به یک مسیریاب خاص در شبکه سؤال کند. لازم به ذکر است که در این پروتکل حداکثر طول مسیر به ۱۵ گام محدود شده است. به این معنی که با هر تعداد مسیریاب موجود در یک شبکه، طول بزرگترین مسیر نباید از ۱۵ بیشتر باشد.

پروتکل RIP به صورت یک برنامه‌ی کاربردی در هر مسیریاب پیاده‌سازی می‌شود و از پورت شماره‌ی 520 پروتکل لایه‌ی انتقال UDP استفاده می‌کند. در شکل ۲۸ نحوه‌ی ارتباط برنامه‌ی کاربردی پروتکل RIP (این برنامه‌ی کاربردی در سیستم عامل یونیکس با نام routed اجرا می‌شود) در دو مسیریاب مختلف و نحوه‌ی تنظیم جداول مسیریابی در دو مسیریاب نمایش داده شده است.

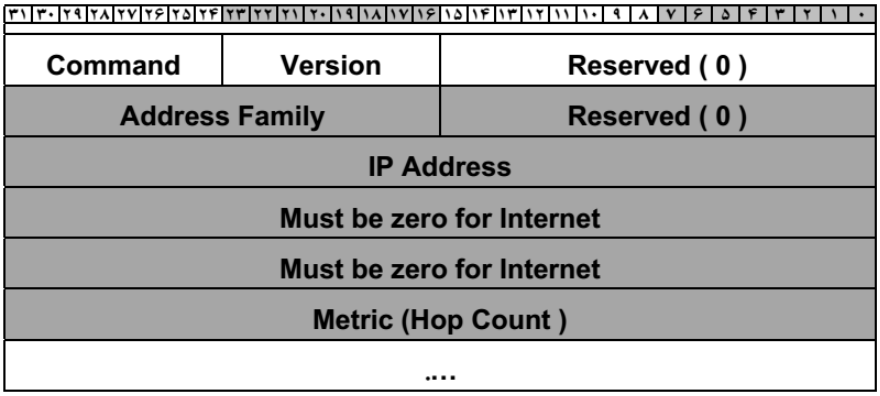


شکل ۲۸ نحوه‌ی ارتباط برنامه‌ی کاربردی پروتکل *RIP* در دو مسیریاب و تنظیم جداول مسیریابی/پیش‌رانی

[51] Routing Information Protocol
[52] Advertisement
[53] Request Message

در شکل ۲۹ قالب پیام‌ها در پروتکل RIP نمایش داده شده است. مفهوم هر کدام از این فیلدها عبارت است از (لازم به ذکر است که قسمت خاکستری رنگ در بدنه‌ی پیام RIP می‌تواند به ازای هر مدخل در جدول مسیریابی تکرار شود):

- Command: این فیلد پیام تقاضا یا پیام پاسخ را مشخص می‌کند. اگر در بدنه‌ی پیام درخواست آدرس IP درج شده باشد، بدین معنا است که هزینه‌ی رسیدن به یک مسیریاب خاص درخواست شده است ولی اگر هیچ آدرسی درج نشده باشد، یعنی کل جدول مسیریابی برای تقاضادهنده ارسال شود. در بدنه‌ی پیام پاسخ کل یا قسمتی از جدول مسیریابی قرار داده شده است.
- Version: نسخه‌ی پروتکل RIP را مشخص می‌کند.
- Reserved: این فیلد بدون استفاده است و با مقدار صفر پر می‌شود.
- Address Family: خانواده‌ی آدرس‌ها و نوع آدرس‌دهی را مشخص می‌کند. برای شبکه‌ای که از پروتکل IPv4 استفاده می‌کند در این فیلد مقدار ۲ ثبت می‌شود.
- IP Address: آدرس IP یک مسیریاب در شبکه را معین می‌کند.
- Metric: مقدار این فیلد هزینه‌ی رسیدن به مسیریاب مشخص شده در فیلد قبلی را بر حسب تعداد گام تعیین می‌کند که حداکثر مقدار آن برابر با ۱۵ است. مقدار ۱۶ نماینده‌ی مقدار بی‌نهایت یا غیرقابل دسترس بودن یک مسیریاب (یا یک شبکه) است. شکل ۳۰ نمایش‌دهنده‌ی یک جدول مسیریابی واقعی در حافظه‌ی یک مسیریاب است. هر مدخل ممکن است شامل آدرس یک سیستم انتهایی یا یک شبکه‌ی کامپیوتری باشد.



شکل ۲۹ قالب پیام‌ها در پروتکل *RIP*

```
Destination Gateway         Flags    Ref   Use    Interface
----------- --------------- -----    ---   ---    ----------
127.0.0.1   127.0.0.1       UH       0     26492  lo0
192.168.2.  192.168.2.5     U        2     13     fa0
193.55.114. 193.55.114.6    U        3     58503  le0
192.168.3.  192.168.3.5     U        2     25     qaa0
224.0.0.0   193.55.114.6    U        3     0      le0
default     193.55.114.129  UG       0     143454
```

شکل ۳۰ یک نمونه از جدول مسیریابی نگهداری شده در حافظه‌ی مسیریاب

در نهایت، لازم به ذکر است حداکثر زمانی که در صورت عدم به‌روزرسانی یک مسیر، هزینه‌ی آن به همسایه‌ها بی‌نهایت (۱۶) اعلام می‌شود برابر با ۱۸۰ ثانیه است. این در حالی است که در فاصله‌ی زمانی ۹۰ تا ۱۸۰ ثانیه هیچ اطلاعاتی از مسیر مورد نظر برای همسایه‌ها اعمال نخواهد شد. پس از ۱۲۰ ثانیه از زمان ذکر شده (پایان ۱۸۰ ثانیه)، مسیر مورد نظر برای همیشه از جدول حذف می‌شود.

۲۱. پروتکل OSPF در مسیریابی درونی

در ابتدا ذکر این نکته لازم است که در این فرصت کوتاه مجال بررسی تمام بخش‌های و ویژگی‌های پروتکل OSPF[۵۴] وجود ندارد و مطالب گردآوری شده با هدف آشنایی کلی با این پروتکل تهیه شده‌اند.

پروتکل OSPF برخلاف پروتکل RIP از الگوریتم LS برای محاسبه‌ی بهترین مسیر استفاده می‌کند. همچنین، این پروتکل علاوه بر تعداد گام به عنوان معیار هزینه، چندین معیار دیگر برای انتخاب بهترین مسیر در نظر گرفته می‌شوند. در واقع حجم بار و ترافیک موجود بر روی یک مسیریاب در محاسبه‌ی بهترین مسیر دخالت داده می‌شوند. همچنین، بر خلاف پروتکل RIP، همگرایی جداول مسیریابی (سازگار شدن مقادر آنها و دریافت مقادیر درست منطبق با همه‌ی جداول مسیریابی در مسیریاب‌های دیگر) در پروتکل OSPF سریع انجام می‌شود (به علت استفاده از الگوریتم LS). یکی از ویژگی‌های پروتکل OSPF تعیین مسیر بر اساس نوع سرویس درخواستی در سرآیند بسته‌ی IP است (بر اساس فیلد ToS در سرآیند IP) که در پروتکل RIP موجود نیست. در پروتکل OSPF تمام بسته‌های ارسالی برای یک مقصد خاص، بر روی بهترین مسیر هدایت نمی‌شوند بلکه درصدی از آنها روی مسیرهایی که در رتبه‌های ۲، ۳ و ... قرار دارند ارسال می‌شوند تا پدیده‌ی «نوسان

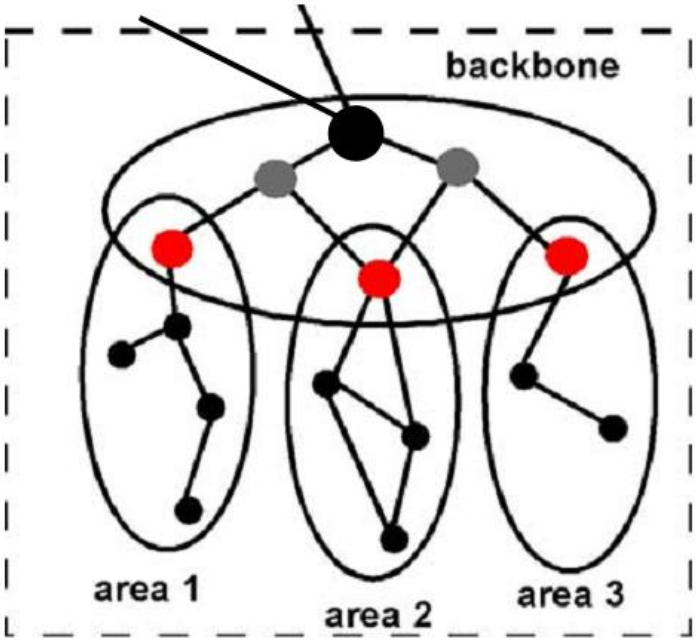
54 Open Shortest Path First

مسیر[۵۵]» رخ ندهد. به این کار «موازنه‌ی بار[۵۶]» گفته می‌شود. در نهایت اینکه، در این پروتکل از مسیریابی سلسله مراتبی پشتیبانی می‌شود مسیریاب‌ها جداول مسیریابی همسایه‌های خود را فقط در صورت احراز اصالت آنها (با استفاده از یک کلمه‌ی عبور) قبول می‌کنند (که این دو ویژگی در پروتکل RIP موجود نمی‌باشند). در ادامه به بررسی مفاهیم مختلف در فرهنگ اصطلاحات پروتکل OSPF پرداخته می‌شود.

یک شبکه‌ی خودمختار (AS) به تعدادی ناحیه (Area) تقسیم می‌شود و تمام مسیریاب‌های درون یک ناحیه باید مسیریاب‌های هم‌ناحیه‌ی خود را بشناسند و هزینه‌ی ارتباط با آنها را بدانند و در جدولی ذخیره نمایند. در زمان به‌روزرسانی این جداول به صورت سیل‌آسا برای تمام مسیریاب‌های هم‌ناحیه ارسال می‌گردد. مسیریاب هیچ اطلاعی از وضعیت مسیریاب‌های درون نواحی دیگر ندارد. تمام مسیریاب‌های درون یک ناحیه اطلاعات کاملی از توپولوژی ناحیه‌ی خود دارند. به جدول مسیریابی آنها که این اطلاعات درون آن سازماندهی و نگهداری می‌شود اصطلاحاً «پایگاه اطلاعات توپولوژیکی» یا Topological Database گفته می‌شود. تمام مسیریاب‌های هم‌ناحیه باید نسخه‌ی مشابهی از این پایگاه اطلاعاتی را داشته باشند. مسیریاب‌های موجود در یک ناحیه هیچ اطلاعی از توپولوژی سایر نواحی ندارند و فقط اطلاعات کلی در مورد نواحی همسایه را در اختیار دارند.

درون هر ناحیه یک یا چند مسیریاب وجود دارند که ارتباط بین نواحی را برقرار می‌سازند و به آنها «مسیریاب‌های مرزی» (یا مسیریاب مرزی ناحیه[۵۷]) گفته می‌شود. مجموعه‌ی مسیریاب‌های مرزی و مسیریاب‌هایی که در خارج از نواحی نقش توزیع ترافیک بین نواحی مختلف یک AS را بر عهده دارند (به‌همراه ساختار ارتباطی بین آنها)، «ستون فقرات» شبکه‌ی AS را تشکیل می‌دهند. شکل ۳۱ نمایش‌دهنده‌ی نواحی مختلف موجود در یک AS و ستون فقرات آن است. مسیریاب‌هایی که با رنگ قرمز مشخص شده‌اند مسیریاب‌های مرزی در هر ناحیه می‌باشند.

55 Route Oscillation
56 Load Balancing
57 Area Border Router



شکل ۳۱ نمایش از نواحی موجود در یک *AS*، ستون فقرات آن و مسیریاب‌های موجود در آنها

در هر شبکه‌ی AS ممکن است یک یا چند «دروازه‌ی مرزی» وجود داشته باشد که در فرهنگ اصطلاحات پروتکل OSPF به آن «Border Gateway» گفته می‌شود. یک دروازه‌ی مروزی مسیریابی است که از یک طرف با مسیریاب‌های درون AS و بر اساس پروتکل OSPF در تعامل است و از طرف دیگر، با دروازه‌های مرزی شبکه‌های AS دیگر و مبتنی بر یک پروتکل مسیریابی بیرونی (همانند پروتکل BGP) در ارتباط است. لازم است که این مسیریاب‌ها تنظیمات لازم برای تعامل با مسیریاب‌های درون شبکه با استفاده از پروتکل OSPF و تنظمیات لازم برای تعامل با دروازه‌های مرزی سایر ASها بر اساس پروتکل مسیریابی بیرونی را دریافت نماید. هر دروازه‌ی مرزی با استفاده از OSPF اطلاعات مسیرهای درونی شبکه را گردآوری و تجمیع می‌کند و سپس بخش‌های مفید این اطلاعات را از طریق یک پروتکل مسیریابی بیرونی در اختیار شبکه‌های AS دیگر (که با آنها در تماس است) قرار می‌دهد. یک شبکه‌ی AS می‌تواند چندین دروازه‌ی مرزی داشته باشد. در شکل ۳۱، دایره‌ی مشکی بزرگ نشان‌دهنده‌ی یک دروازه‌ی مرزی است.

در پروتکل OSPF جداول زیر به طور متناوب توسط مسیریاب‌ها «اعلان» (Advertise) می‌شوند:

جدول مسیریابی درون یک ناحیه: شامل اطلاعات گراف هزینه‌ی ناحیه‌ای است که یک مسیریاب به آن تعلق دارد و توسط هر مسیریاب درون آن ناحیه، به تمام مسیریاب‌ها اعلان می‌شود.

جدول خلاصه‌ی مسیریابی مسیریاب‌های مرزی: محتوی اطلاعات خلاصه و تجمیعی، در مورد مسیرهای موجود در خارج از نواحی است و توسط مسیریاب‌های مرزی به تمام مسیریاب‌های نواحی اعلان می‌شود.

جدول مسیریابی شبکه: محتوی اطلاعاتی در مورد مسیریاب‌ها و کانال‌های بین آنها در خارج از شبکه‌ی AS است و توسط مسیریاب‌های واقع بر ستون فقرات شبکه‌ی AS به تمامی مسیریاب‌های مرزی نواحی (ABR یا Area Border Router) مختلف اعلان می‌شود ولی فقط در مسیریاب‌های مرزی مورد استفاده قرار می‌گیرد.

لازم به ذکر است که پروتکل OSPF مستقیماً بر روی پروتکل IP کار می‌کند و یک برنامه‌ی لایه‌ی انتقال تلقی می‌شود (پروتکل RIP به عنوان یک برنامه‌ی کاربردی پیاده‌سازی شده است). شماره‌ی پروتکل 89 در سرآیند پروتکل IP مشخص‌کننده‌ی پروتکل OSPF است.

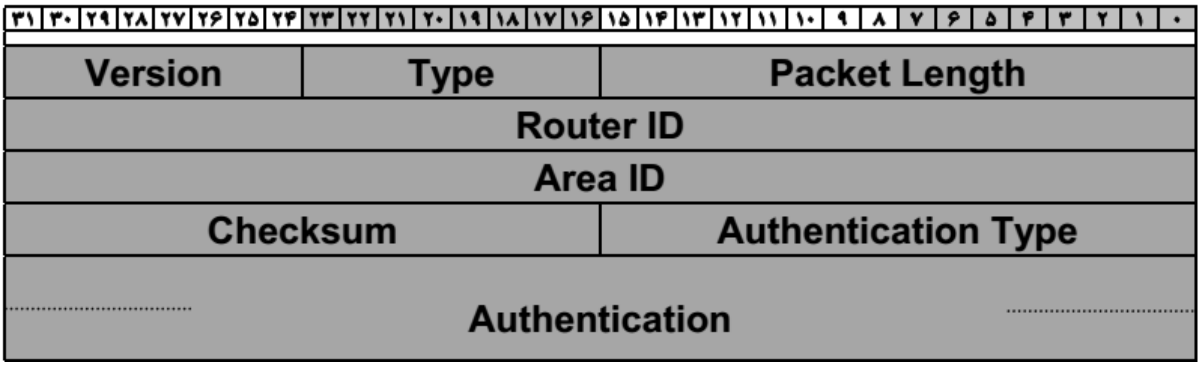
انواع پیام‌های رد و بدل شده در پروتکل OSPF:

- پیام «سلام»: وقتی یک مسیریاب روشن می‌شود موظف است به تمام مسیریاب‌های همسایه‌ی خود یک پیام «سلام» ارسال کند تا آنها را از حضور خود مطلع سازد.
- پیام Link State Update: هر مسیریاب موظف است که در بازه‌های زمانی مشخص، بسته‌ی وضعیت لینک یا بسته‌ی LS خودش را به روش سیل‌آسا به اطلاع دیگر مسیریاب‌های هم‌ناحیه‌ی خود برساند. این کار با ارسال پیام Link State Update انجام می‌شود. در ضمن، وقتی هزینه‌ی یکی از لینک‌های متصل به مسیریاب تغییر کرد یا مسیریاب همسایه‌اش از شبکه بیرون رفت (یا وارد شبکه شد) باید این پیام رخداد را سریعاً به اطلاع دیگران برساند.
- پیام Database Description: این پیام برای ارسال اطلاعات کامل جدول مسیریابی مورد استفاده قرار می‌گیرد. ارسال این پیام زمانی انجام می‌شود که یک مسیریاب همسایه روشن شده است و توسط آن همسایه مورد استفاده قرار می‌گیرد. این پیام شامل محتویات پایگاه داده‌ی اطلاعات توپولوژیکی مسیریاب فرستنده است.
- پیام Link State Request: با این پیام هر مسیریاب می‌تواند اطلاعات جدول مسیریابی را از یک مسیریاب خاص تقاضا نماید. مسیریاب می‌تواند با بررسی شماره‌ی ترتیب مدخل‌های جداول همسایه‌های خود اقدام به به‌روزرسانی جدول خود نماید.
- پیام Link State Ack: این پیام در پاسخ به دریافت پیام Link State Update برای ارسال‌کننده‌ی آن فرستاده می‌شود تا فرستنده از دریافت صحیح جدول مسیریابی مطمئن شود.

تمام پیام‌های تعریف شده در پروتکل OSPF دارای سرآیند مشترک ۲۴ بایتی هستند که در شکل ۳۲ نمایش داده شده است. در ادامه معنی و مفهوم هر کدام از فیلدهای سرآیند معریف می‌گردد:

- فیلد Version: نسخه‌ی پروتکل OSPF را تعیین می‌کند.

- فیلد Type: یکی از انواع پنج‌گانه‌ی پیام OSPF را مشخص می‌کند.
- فیلد Packet Length: طول کل پیام (شامل سرآیند) را بر حسب بایت مشخص می‌کند.
- فیلد Router ID: شناسه‌ی مسیریاب ارسال‌کننده‌ی پیام را تعیین می‌کند. این مقدار برای مسیریاب توسط مدیر شبکه تنظیم می‌شود.
- فیلد Area ID: شناسه‌ی ناحیه‌ای است که مسیریاب ارسال‌کننده‌ی پیام به آن تعلق دارد. این مقدار نیز توسط مدیر شبکه تنظیم می‌گردد.
- فیلد Checksum: یک کد کشف خطای ۱۶ بیتی از کل پیام (شامل سرآیند و بدنه‌ی پیام) است که بر اساس محاسبات مکمل ۱ بدست می‌آید.
- Authentication Type: مشخص می‌کند که آیا برای این پیام احراز اصالت انجام شود یا خیر. مقدار 0برای آن عدم احراز اصالت را مشخص می‌کند (فیلد بعدی بی‌اهمیت می‌شود) و مقدار 1 برای آن وجود احراز اصالت را مشخص می‌کند.
- فیلد Authentication: کلمه‌ی عبور مسیریاب را مشخص می‌کند و در هنگام نصب و تنظیم شبکه توسط مسئول آن تعیین می‌گردد. مسیریاب‌های دریافت‌کننده‌ی هر بسته به شرطی آن را می‌پذیرند که کلمه‌ی عبور آن مسیریاب معتبر و تعریف شده باشد.



شکل ۳۲ سرآیند مشترک در تمام پیام‌های *OSPF*

در نهایت، معیار هزینه در پروتکل OSPF در نظر گرفته می‌شود. مقدار پیش‌فرض در OSPF پهنای باند هر لینک است. هرچه پهنای باند یک لینک کمتر باشد هزینه‌ی آن بالاتر خواهد بود. در این پروتکل پس از آنکه یک مسیریاب پهنای باند لینک متصل به هر یک از واسط‌های شبکه‌ی خود را کشف کرد، هزینه‌ی لینک متصل به آن‌را مطابق با رابطه‌ی زیر محاسبه و اعلام می‌کند:

$$\text{هزینه‌ی لینک در OSPF} = \text{هزینه}/10^8$$

هزینه به عدد صحیح گرد می‌شود. هزینه‌ی یک مسیر که از چندین گام و لینک متوالی تشکیل شده، مجموع هزینه‌های آنها است.

۲۲. پروتکل BGP: پروتکل مسیریابی برونی

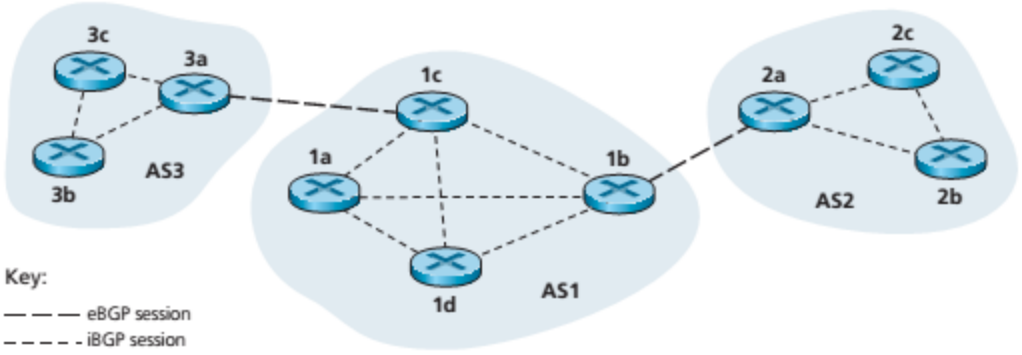
در این قسمت پروتکل BGP به طور مختصر مورد بررسی قرار می‌گیرد. در همین ابتدا ذکر می‌شود که اطلاعات جزئی‌تر درباره‌ی این پروتکل در مستندات RFC-1263 و RFC-1654 موجود می‌باشند.

نکته‌ی جالب درباره‌ی پروتکل مسیریابی BGP این است که مسیریاب‌های BGP علاوه بر تأثیرپذیری از شرایط مربوط به تأخیر یا سرعت بیشتر در فرایند تصمیم‌گیری برای یافتن بهترین مسیرها، مسائل سیاسی، اقتصادی و امنیتی را نیز در این تصمیم‌گیری دخیل می‌نمایند. تمام شبکه‌های خودمختار موجود در اینترنت از طریق یک ستون فقرات به هم متصل شده‌اند که مسیریاب‌های BGP بر روی آن واقع هستند.

فرایندی که یک بسته‌ی تولید شده در یک شبکه‌ی محلی در یک AS برای رسیدن به یک شبکه‌ی محلی دیگر در یک AS راه دور طی می‌کند عبارت است از (در این فرایند پروتکل OSPF به عنوان پروتکل مسیریابی درونی در نظر گرفته شده است):

- بر اساس اطلاعات جدول مسیریابیِ مسیریاب‌های موجود در ناحیه‌ای که به آن متعلق است، به سمت دروازه‌ی مرزی ناحیه (ABR) هدایت می‌شود.
- پس از آن بر روی شبکه‌ی ستون فقرات AS (ناحیه‌ی 0 در پروتکل OSPF) هدایت شده و به یک دروازه‌ی مرزی تحویل داده می‌شود.
- سپس، مبتنی بر پروتکل BGP بر روی ستون فقرات کل شبکه‌ی اینترنت (متصل‌کننده‌ی ASهای مختلف) هدایت شده و توسط دروازه‌ی مرزی AS مقصد دریافت می‌شود.
- در این مرحله بر اساس اطلاعات حاصل شده از مسیریابی درونی در AS مقصد به سمت ناحیه‌ی صاحب شبکه‌ی محلی مقصد هدایت می‌شود.
- در نهایت بر اساس اطلاعات مخصوص ناحیه‌ی مقصد در جداول مسیریابی مسیریاب‌های موجود در آن به سمت شبکه‌ی محلی مقصد و سپس، سیستم انتهایی مقصد ارسال می‌گردد.

بین دروازه‌های مرزی موجود در دو AS مختلف یک ارتباط TCP با استفاده از شماره‌ی پورت 179 (پروتکل BGP به صورت یک برنامه‌ی کاربردی پیاده‌سازی می‌شود) شبه‌دائمی وجود دارد که اطلاعات مسیرها بر روی آن مبادله می‌گردد. به ارتباط TCP بین دو دروازه‌ی مرزی در دو AS مختلف به همراه پیام‌های BGP مبادله شده بر روی آن یک جلسه‌ی BGP خارجی (eBGP session یا external BGP session) گفته می‌شود. به دو مسیریاب حاضر در دو طرف ارتباط همتاهای BGP (BGP Peers) گفته می‌شود. علاوه بر جلسه‌ی eBGP، یک ارتباط شبه‌دائمی دیگر بین مسیریاب‌های درون یک AS (شامل دروازه‌ی مرزی) وجود دارد که به آن جلسه‌ی BGP داخلی (iBGP session یا internal BGP session) گفته می‌شود. شکل ۳۳ نمایش‌دهنده‌ی مثالی از چند شبکه‌ی خودمختار و ارتباط‌های eBGP و iBGP موجود در آنها است.



شکل ۳۳ مثالی از چند شبکه‌ی خودمختار و ارتباط‌های *eBGP* و *iBGP* موجود در آنها

مسیریاب‌های BGP باید شناسه‌ی (پیش‌شماره یا prefix) شبکه‌های درون AS خود را به مسیریاب‌های همتای خود در سایر ASها اعلام کنند. شناسه‌ی این شبکه‌ها به شکلی که در روش CIDR معرفی شد اعلام می‌گردند به صورتی که هر پیش‌شماره نمایش‌دهنده‌ی یک یا مجموعه‌ای از زیرشبکه‌ها است. لازم به ذکر است که پروتکل BGP به روش الگوریتم مسیریابی DV عمل می‌کند. به منظور پیش‌گیری از مشکلات حلقه و شمارش تا بی‌نهایت (این دو مشکل در الگوریتم DV رخ می‌دهد)، مسیرها به طور کامل اعلان می‌شوند (این کار در انتخاب مسیرها بر اساس معیارهای امنیتی، اقتصادی، سیاسی و ملی کمک می‌کند). به این معنی که تمام مسیر از مسیریاب فرستنده‌ی بسته‌ی شامل مسیرها تا مقصد مورد نظر (دنباله‌ی شماره ASها تا AS مقصد) به عنوان یکی از خاصیت‌های[۵۸] مسیر ارسال می‌شود (اصطلاحاً به این پارامتر مسیر، AS-PATH گفته می‌شود). لازم به ذکر است که اعلام هزینه‌ی یک مسیر به سایر مسیریاب‌ها لازم نیست و انتخاب مسیر می‌تواند بر اساس معیارهای دیگری انجام شود.

به طور مثال، روش مورد نظر با استفاده از مسیریاب‌ها به جای ASها و استفاده از شناسه‌ی مسیریاب‌ها به جای ASNها (شناسه‌ی AS) و با بهره‌گیری از شکل ۳۴ ارائه می‌شود. فرض می‌شود که مسیریاب F از

[58] Attributes

مسیریاب‌های همسایه‌ی خود یعنی B، I، G، و E اطلاعاتی را در مورد D دریافت می‌کند. این مسیرها می‌توانند به صورت زیر باشند:

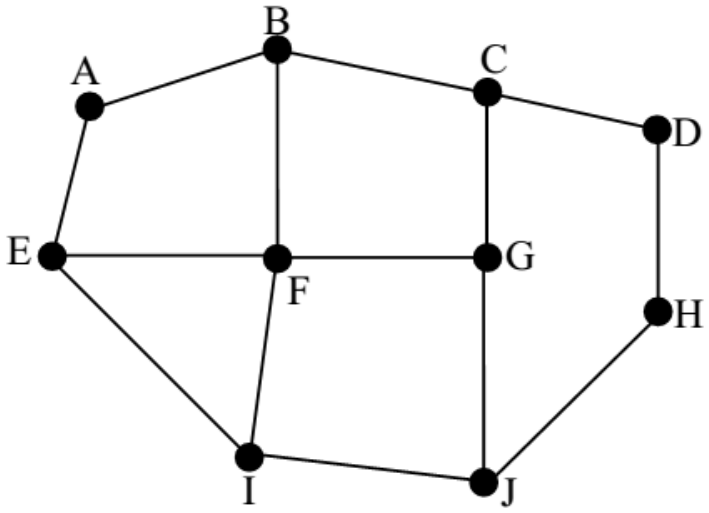
از B به D: I use BCD

از G به D: I use GCD

از I به D: I use IFGCD

از E به D: I use EFGCD

در همان ابتدا مسیرهای دریافت شده از I و E دور انداخته می‌شوند. زیرا این مسیرها از F می‌گذرند و مسیر مستقلی محسوب نمی‌شوند. برای انتخاب از بین دو مسیر باقی‌مانده، لازم است که پارامترهای ترافیکی، توپولوژیکی، اقتصادی، سیاسی و امنیتی در نظر گرفته شوند.



شکل ۳۴ شکل استفاده شده در مثال ارسال مسیر کامل در *BGP*

همان‌طور که قبلاً گفته شد، هر شبکه‌ی خودمختار دارای یک شناسه‌ی منحصر به فرد به نام ASN است که به پیش‌شماره‌ی تمام شبکه‌ای محلی موجود در آن منسوب می‌شود (یک شبکه‌ی خودمختار ممکن است از صدها یا هزاران شبکه‌ی محلی تشکیل شده باشد). در اینجا ذکر این نکته لازم است که یک شبکه‌ی خودمختار فقط زمانی شرایط دریافت یک ASN را دارا می‌باشد که یک شبکه‌ی «چند اتصالی» باشد. بدین معنی که به بیش از یک شبکه‌ی خودمختار دیگر متصل باشد. در غیر این صورت (در صورتی که شبکه‌ی خودمختار یک «شبکه‌ی پایانی» محسوب شود)، می‌توان آنرا به عنوان عضوی از یک شبکه‌ی خودمختار بزرگتر در نظر گرفت. هر مسیریاب BGP اطلاعات مسیریابی را با شماره‌ی ASN مربوط به خود به مسیریاب‌های دیگر اعلام می‌کند.

به عنوان مثالی از انتساب یک شناسه‌ی شبکه‌ی خودمختار (ASN) به چند آدرس زیرشبکه، ASی با شناسه‌ی 1000 (ASN = 1000) در نظر گرفته می‌شود. ممکن است که این شناسه به پیش‌شماره‌های (آدرس‌های زیرشبکه) 10.34.0.0/16 و 10.40.0.0/18 و 10.60.0.0/16 منسوب شود. توجه شود که هرکدام از این پیش‌شماره‌ها ممکن است مجتمع شده از تعداد زیادی آدرس زیرشبکه‌ی دیگر باشند (به روش CIDR). به این معنی که تمام شبکه‌های موجود در این AS در محدوده‌ی آدرس‌های ذکر شده قرار دارند.

انواع پیام‌های مبادله شده بین مسیریاب‌های BGP عبارت هستند از:

- پیام OPEN: وقتی یک مسیریاب وارد شبکه می‌شود، با ارسال این پیام خود را به مسیریاب‌های همتای خود معرفی می‌کند. مسیریاب‌های همتا در پاسخ پیام KEEPALIVE را ارسال می‌کنند.
- پیام KEEPALIVE: علاوه بر کاربرد ذکر شده برای این پیام، اگر در موعد اعلان مسیرها یک مسیریاب هیچ چیز جدیدی برای ارسال نداشته باشد، با ارسال این پیام اعلام می‌کند که در شبکه حضور دارد و فعال است. اگر یک مسیریاب در بازه‌ی زمانی مشخص هیچ پیامی از همتای خود دریافت نکند فرض خواهد کرد که آن مسیریاب به هر دلیلی از شبکه خارج شده است.
- پیام NOTIFICATION: با این پیام مسیریاب به همتای خود اعلام می‌کند که در دریافت پیام قبلی خطایی رخ داده است.
- پیام UPDATE: با این پیام یک مسیریاب اطلاعات مسیریابی مورد نظر را به اطلاع همتای خود می‌رساند. این اطلاعات پس از برقراری جلسه‌ی مورد نظر مبادله می‌شود. در دو صورت امکان دارد که یک مسیریاب مجبور به دریافت کامل جدول مسیریابی همتای خود شود (حجم این جدول بسیار زیاد است و ممکن است زمان‌گیر باشد): وقتی که مسیریاب مورد نظر برای اولین بار پیکربندی می‌شود و زمانی که مسیریاب به هر دلیل از راه‌اندازی مجدد (reset) می‌شود. اطلاعات دریافت شده توسط هر همتا مجدداً برای مسیریاب‌های جدید ارسال می‌شود و به همین ترتیب و به صورت گام به گام اطلاعات دسترسی به شبکه‌ها در سراسر اینترنت منتشر می‌گردند.

همان‌طور که قبلاً گفته شد، زمانی که یک مسیریاب یک پیش‌شماره‌ی شبکه را بر روی یک جلسه‌ی BGP به اطلاع همتای خود می‌رساند، همراه با پیش‌شماره‌ی مورد نظر چند خصیصه نیز ارسال می‌گردند. یک پیش‌شماره به همراه خواص آن به عنوان یک مسیر یا یک route شناخته می‌شود. دو مورد از مهم‌ترین خواص ارسال شده به همراه یک پیش‌شماره عبارت هستند از AS-PATH و NEXT-HOP.

- AS-PATH: این خصیصه شامل ASهایی است که اعلان پیش‌شماره‌ی مورد نظر از آنها گذشته است (به صورت دنباله‌ای از ASNها مشخص می‌شود). زمانی که یک پیش‌شماره از یک AS عبور می‌کند، AS مورد نظر ASN خود را به خصیصه‌ی AS-PATH اضافه می‌کند. قبلاً گفته شد که این خصیصه برای پیش‌گیری

از وقوع دور و پیش‌گیری از مشکل شمارش تا بی‌نهایت مورد استفاده قرار می‌گیرد. این خصیصه می‌تواند به منظور انتخاب یک مسیر از بین مسیرهای متعدد به یک مقصد مشخص مورد استفاده قرار بگیرد.

- NEXT-HOP: این خصیصه واسط شبکه‌ی مسیریابی را مشخص می‌کند که آغازکننده‌ی AS-PATH است. به طور مثال فرض شود که یک مسیر به یه مقصد مشخص در شکل ۳۳ توسط مسیریاب 3a در AS3 به مسیریاب 1c در AS1 و از طریق یک ارتباط eBGP ارسال شده است. خصیصه‌ی NEXT-HOP واسط شبکه‌ی مسیریاب 3a است که در شبکه‌ی بین این مسیریاب با 1c قرار دارد. لازم به ذکر است که راهکار مسیریابی داخلی AS شرایط دسترسی به تمام شبکه‌های متصل به مسیریاب‌های داخلی AS (از جمله‌ی شبکه‌ی متصل به واسطی از مسیریاب 1c که به مسیریاب 3a منتهی می‌شود) را فراهم می‌سازد و در نتیجه، پس از دریافت این مسیر توسط مسیریاب 1d در AS1 (از طریق یک ارتباط iBGP)، این مسیریاب می‌تواند با توجه به اطلاعات مسیریابی درونی بهترین مسیر تا واسط شبکه‌ی مشخص شده با استفاده از خصیصه‌ی NEXT-HOP را پیدا نماید.

نکته‌ی دیگر مربوط به زمانی است که بیش از یک مسیر به یک پیش‌شماره‌ی مشخص توسط یک مسیریاب دریافت شوند. در چنین شرایطی، با توجه به قوانین زیر یکی از این مسیرها برای هدایت بسته‌ها انتخاب می‌شود:

- یکی از خصیصه‌های مسیرها یک مقدار ارجحیت است. مسیرهای دارای بالاترین مقدار ارجحیت انتخاب می‌شوند.
- از بین مسیرهای باقی‌مانده، مسیرهای دارای کوتاه‌ترین AS-PATH انتخاب می‌گردند.
- از بین مسیرهای باقی‌مانده، مسیرهای دارای نزدیک‌ترین مسیریاب NEXT-HOP انتخاب می‌شوند. پروتکل مسیریابی درونی در این قسمت تأثیرگذار است.
- در نهایت از بین مسیرهای باقی‌مانده (مسیرهای دارای بالاترین مقدار ارجحیت، دارای کوتاه‌ترین AS-PATH و مسیرهای دارای نزدیک‌ترین مسیریاب NEXT-HOP) بر اساس شناسه‌ی BGP مسیریاب‌ها یکی از این مسیرها انتخاب می‌شوند (مثلاً انتخاب مسیر با کمترین مقدار ID برای یکی از مسیریاب‌ها).

در نهایت به عنوان مثالی از مسیریابی مبتنی بر سیاست می‌توان به این مسأله اشاره کرد که فقط ترافیک ورودی از طرف ASهایی که مشتری یک AS مشخص هستند اجازه‌ی ورود به آن AS را دارند. بنابراین، لازم است که سیاست‌های مناسب برای برقراری این شرایط تنظیم گردند.