فصل هشتم

پروتکل های لایه شبکه دراینترنت

لایه شبکه درمعماری TCP/IP شامل چند پروتکل مهم می باشد. دراین فصل به بررسی پروتکل های این لایه شامل : پروتکل ARP[1]، پروتکل RARP[2] و پروتکل IP می پردازیم.

۸-۱- پروتکل ARP

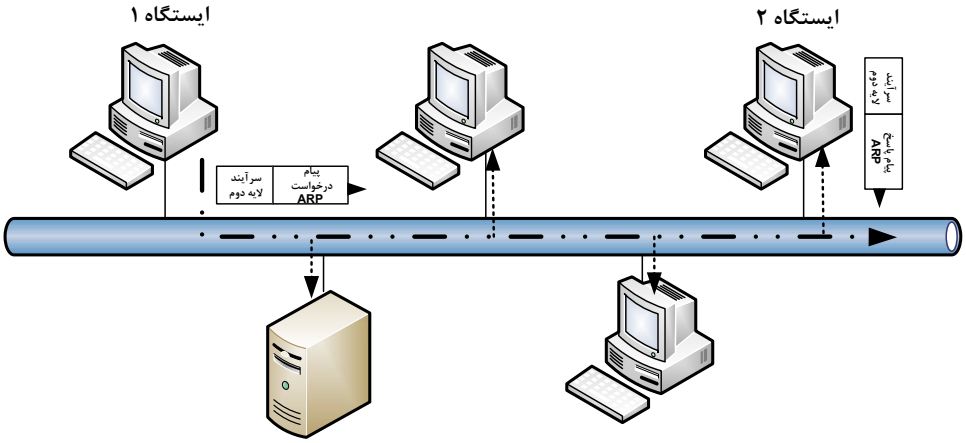
آدرس های IP به صورت منطقی تعریف شده و از آن برای ایجاد شبکه های مجازی استفاده می شود. همانطورکه درفصل قبل گفته شد، این آدرس ها دارای طول ۳۲ بیت می باشند. باید توجه داشت که انتقال بسته های IP مستلزم استفاده از لایه دوم می باشد. به عبارت دیگر ازآنجاییکه پروتکل IP درلایه سوم قراردارد، طبق روال ارسال داده درمعماری لایه ای شبکه، انتقال بسته های لایه سوم مستلزم استفاده از امکانات لایه دوم می باشد. بنابراین ازآنجاییکه بسته های IP دردل قابهای لایه دوم مثل اترنت و یا شبکه حلقه نشانه قرار می گیرند، برای ارسال آنها به مقصد نیاز به دانستن آدرس سخت افزاری کامپیوتر مقصد می باشد. به عبارت دیگر از آنجاییکه درکامپیوترمقصد، ابتدا لایه دوم قاب را از شبکه برداشته و بعد به لایه سوم که پروتکل IP است تحویل می دهد، لذا دانستن تنها آدرس IP مقصد کفایت نکرده و باید آدرس سخت افزاری مربوط به لایه دوم کامپیوتر مقصد نیز داشته باشیم. بدین منظور از پروتکل خاصی به نام پروتکل ARP استفاده می شود.
درمعماری TCP/IP از پروتکل DNS[3] برای نگاشت بین آدرس های اسمی که دربرنامه های کاربردی استفاده می شوند و آدرس های IP که درسطح لایه سوم استفاده می شود، بهره گرفته می شود. برخلاف پروتکل فوق، از پروتکل ARP برای استخراج آدرس لایه سخت افزاری (که به آن آدرس MAC[4] نیز گفته می شود) از آدرس IP استفاده می شود.سوالی که اینجامطرح می شوداین است که چگونه می توان با داشتن آدرس IP مقصد، آدرس سخت افزاری مربوط به لایه دوم آن را بدست آورد؟
یکی از ساده ترین راه حل ها این است که هرکامپیوتر شبکه، دارای جدولی باشد که درآن جدول آدرس IP و آدرس MAC همه کامپیوتر های شبکه نوشته شده است. هرگاه کامپیوتری نیاز به آدرس MAC کامپیوتردیگری داشته باشد، با فرض آنکه آدرس IP آن را می داند، به این جدول مراجعه کرده و آدرس MAC آن را بدست می آورد. این راه حل گرچه ساده به نظر می رسد، ولی مشکل اصلی آن این است که درصورت تغییر آدرس MAC یک ایستگاه (به عنوان مثال درهنگامی که کارت شبکه یک کامپیوتر عوض شود) باید رکورد مربوط به آن کامپیوتر جداول مربوط به سایر کامپیوتر ها نیز عوض شودکه این کار نیاز به صرف هزینه و وقت زیاد است.
این روش پیکره بندی دستی TCP/IP برای تعریف انطباق بین آدرس های IP و آدرس های MAC درگذشته استفاده می گردید. در سیستم های امروزه مدل انعطاف پذیر تری برای مشخص سازی پویای آدرس MAC با دانستن آدرس IP میزبان مورد نیاز است . این مکانیزم پویا به عنوان یک پروتکل جدا تحت عنوان پروتکل ARP پیاده سازی شده است.

---

[1] Address Resolution Protocol
[2] Reverse Address Resolution Protocol
[3] Domain Name System
[4] Medium Access Control

۸-۱-۱- نحوه عملکرد پروتکل ARP

شکل(۸-۱) یک نمای ساده از چگونگی عملکرد پروتکل ARP را نشان می دهد. دراین شکل فرض می شودکه ایستگاه ۱ می خواهد داده ای را برای ایستگاه ۲ ارسال دارد. بدین منظور باید ابتدا آدرس MAC ایستگاه ۲را بدست آورد.



شکل(۸-۱): عملکرد ARP

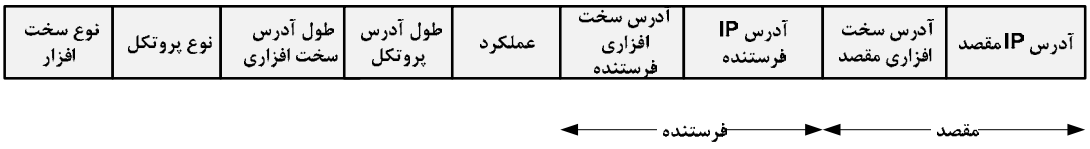
ایستگاه ۱ یک قاب همه پخشی MAC را که پیام درخواست ARP نامیده می شود، به شبکه می فرستد .پیام درخواست ARP شامل آدرس IP و آدرس MAC میزبان فرستنده یعنی ایستگاه ۱ و آدرس IP میزبان مقصد یعنی ایستگاه ۲ است . پیام درخواست ARP شامل یک فیلد خالی برای آدرس سخت افزاری مقصد یعنی ایستگاه ۱ است .همه نود ها در شبکه فیزیکی پیام در خواست همه پخشیARP را دریافت می کنند. سایر نود هاییکه قاب همه پخشی را دریافت می کنند ، آدرس IP خود را با آدرس IP موجود درقاب درخواست ARP مقایسه می نمایند. تنها میزبانی که همان آدرس IP خواسته شده در پیام در خواست ARP را دارد، به درخواست فوق پاسخ می دهد. اگر ایستگاه ۲ در شبکه موجود باشد، آدرس سخت افزاری خود را درفیلد خاصی درپیام فوق قرار داده و به آن پاسخ می دهد. به پیام ارسالی، پیام پاسخ ARP می گویند. بعد از آنکه ایستگاه۱ پاسخ ARP را دریافت کرد، دریک جدول خاص به نام جدول حافظه پنهان ARP که درحافظه اصلی خود نگهداری می کند، زوج آدرس IP و سخت افزاری ایستگاه ۲ را قرار می دهد. درصورتیکه درآینده نیاز به ارسال مجدد به ایستگاه ۲ باشد، ابتدا ایستگاه۱ محتوای این جدول را جستجوکرده و درصورت نیافتن آدرس سخت افزاری ایستگاه ۲ روال درخواست ARP را انجام می دهد. محتویات جدول فوق، یک زمان زندگی خاصی دارندکه دراکثر پیاده سازی های TCP/IP مقدار آن برابر با ۱۵ دقیقه می باشد.

بعد از اینکه مهلت زمانی فوق برای یک میزبان خاص تمام شد، قاب درخواست ARP مجدداً برای کشف آدرس سخت افزاری میزبان فرستاده می شود.

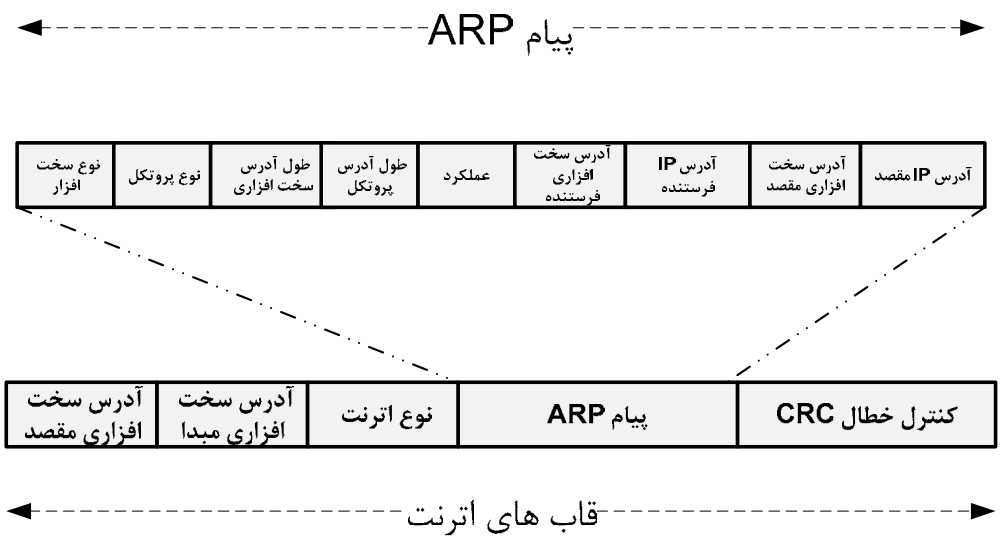
درهنگام ارسال پیام درخواست ARP ازآنجاییکه آدرس سخت افزاری مقصد هنوز معلوم نیست، بنابراین درخواست فوق درلایه دوم به صورت همه پخشی ارسال شده طوری که همه میزبان های شبکه بتوانند آنرا دریافت نمایند. پاسخ ARP که توسط نود مقصد فرستاده می شود یک قاب همه پخشی نیست، زیرا نود گیرنده درخواست ARP، آدرس سخت افزاری فرستنده پیام فوق را درفیلد خاصی درپیام فوق بدست آورده و درهنگام پاسخ دهی به درخواست فوق، قاب پاسخ را به صورت تک پخشی ارسال می دارد. فرض عملکرد پروتکلARP این است که شبکه فیزیکی زیرین توانایی همه پخشی را پشتیبانی می کند که در مورد شبکه های محلی مانند اترنت ، شبکه حلقوی ، FDDI، ARCnet صدق می کند.

۸-۱-۲- ساختاربسته های ARP

شکل (۸-۲) قالب بسته های درخواست ARP و پاسخ ARP را نشان می دهد. پروتکل ARP در آغاز برای اترنت DIX طراحی شده بود . بعدا" برای شبکه های محلی دیگر مانندشبکه های محلی IEEE802 توسعه داده شد . پیام هایARP در قالب قاب های لایه پیوند داده بسته بندی می شود . شکل(۸-۳) مثالی از یک بستهARP را نشان میدهد که در یک قاب اترنت جاسازی شده است.



شکل(۸-۲): قاب بسته ARP



شکل(۸-۳): بسته ARP بسته بندی شده در یک قاب اترنت

بانگاهی به شکل (۸-۲) درمی یابیم که فیلد نوع سخت افزار، اولین فیلد دربسته ARP است. این فیلد که دوبایت طول دارد (بایت ۸ بیتی) نشان دهنده نوع سخت افزار شبکه است. مقدار ۱در فیلد نوع سخت افزار نشان دهنده یک شبکه اترنت است. جدول (۸-۱) کدهای انتساب داده شده را برای مقادیر نوع سخت افزار در بسته ARP برای شبکه های مختلف نشان می دهد.

جدول(۸-۱): مقادیر نوع سخت افزار ARP

فیلد نوع سخت افزار ARP	توصیف
۰	اترنت ۱۰ مگابیت برثانیه
۲	اترنت آزمایشی ۳ مگابیت برثانیه
۴	حلقه نشانه
۵	Chaos Net
۶	شبکه های IEEE 802
۷	ARCNET

۱۴	SMDS
۱۵	Frame Relay
۱۶و۱۹و۲۱	ATM
۱۷	HDLC
۱۸	Fiber Channel

فیلد نوع پروتکل، نشان دهنده نوع پروتکل لایه بالاتر است. این فیلد ۲ بایت طول دارد. در مورد شبکه های TCP/IP آدرس پروتکل، آدرس IP است که برای این آدرس سخت افزاری مورد نیاز است. مقدار نوع پروتکل، نوع پروتکل لایه سوم را مشخص می کند. برای پروتکل IP مقدارعدد مبنای شانزده۸۰۰ برای فیلد نوع پروتکل استفاده می شود. فیلدطول آدرس سخت افزاری بر حسب بایت است. این فیلد ۱بایت طول دارد. مقدار فیلد فوق بوسیله مقدار فیلد نوع سخت افزار کنترل می شود. اگر نوع سخت افزار ۱ باشد، یک شبکه اترنت را نشان می دهدکه آدرس سخت افزاری آن ۸ بایت است. بنا براین مقدار فیلد طول آدرس سخت افزاری برای شبکه های اترنت ۸ است.

فیلد طول آدرس پروتکل، طول آدرس پروتکل مورد استفاده درلایه سوم را بر حسب بایت است. این فیلد ۱ بایت طول دارد . فیلد فوق بوسیله مقدار فیلد نوع پروتکل کنترل می شود. اگر نوع پروتکل ۸۰۰ (درمبنای شانزده) باشد ، پروتکل IP را مشخص می کند که آدرس IP آن ۴ بایت است. بنابراین مقدار فیلد طول آدرس پروتکل برای شبکه های IP ۴ است. فیلد عملکرد ۲ بایت طول دارد ونشان دهنده این است که آیا بسته فعلی یک بسته درخواست ARP و یا یک بسته پاسخ ARP است. البته به غیر از این دوبسته، این فیلد می تواند به عملکردهای دیگری اشاره داشته باشد. جدول(۸-۲) مقادیر ممکن در فیلد عملکرد را نشان می دهد، بعضی از مقادیر جدول(۸-۲) برای پروتکل های آزمایشی پیشنهادی هستند و ممکن است هرگز آنها را در شبکه های موجود نبینید.

جدول(۸-۲): مقادیر عملکرد برای بسته ARP

فیلد نوع عملکرد	توصیف
۱	پیام درخواست ARP
۲	پیام پاسخ ARP
۳	پیام درخواست RARP
۴	پیام پاسخ RARP
۵	پیام درخواست DRARP
۶	پیام پاسخ DRARP
۷	پیام خطای DRARP
۸	پیام درخواست InARP
۹	پیام پاسخ InARP
۱۰	پیام ARP NAK

فیلد آدرس سخت افزاری فرستنده، نشان دهنده آدرس سخت افزاری نود فرستندهٔ درخواست ARP است. فرستنده، آدرس سخت افزاری خود را با خواندن آن از کارت شبکه بدست آورده و این فیلد را پر می کند. آدرس IP فرستنده نشان دهنده آدرس IP نود فرستنده درخواست ARP است. فرستنده، آدرس IP خود را با خواندن از یک فایل پیکره بندی یا خواندن حافظه پنهان خود که شامل اطلاعات پیکره بندی شبکه است بدست می آورد و درفیلد متناظر قرار می دهد.

فیلد آدرس سخت افزاری مقصد، آدرس سخت افزاری نود مقصد را نشان می دهد. این مقدار برای فرستنده پیام درخواست ARP شناخته شده نیست. این مقدار، مقداری است که فرستنده درخواست ARP سعی به مشخص کردن آن می کند. این

فیلد معمولا بیتهای ۱ یا بیتهای صفر دارد. آدرس سخت افزاری مقصد می تواند آدرس همه پخشی سخت افزار باشد که آن را برای بعضی از جنبه های پیاده سازی مناسب می سازد.

فیلد آدرسIP مقصد در بسته درخواست ARP دربرگیرنده آدرسIP نودی است که قرار است آدرس سخت افزاری آن مشخص شود. این مقدار به وسیله فرستنده درخواست ARP فراهم می شود. ساختار بسته پاسخ ARP همانند قالب بسته درخواست ARP می باشد اما مقدار فیلد عملکرد آن۲ است که نشان دهنده یک پاسخ ARP است.

استفاده از قالب یکسان برای درخواست ها و پاسخ های ARP ،باعث می شود که از بافر بسته درخواست ARP دوباره برای پاسخ ARP استفاده شود. پاسخ ARP همان طول پیام درخواست ARP را دارد و چندین فیلد یکسان هستند. هنگامی که یک نود IP یک پاسخ ARP می فرستد، آدرس سخت افزاری خود را در فیلد آدرس سخت افزاری فرستنده قرار می دهد.

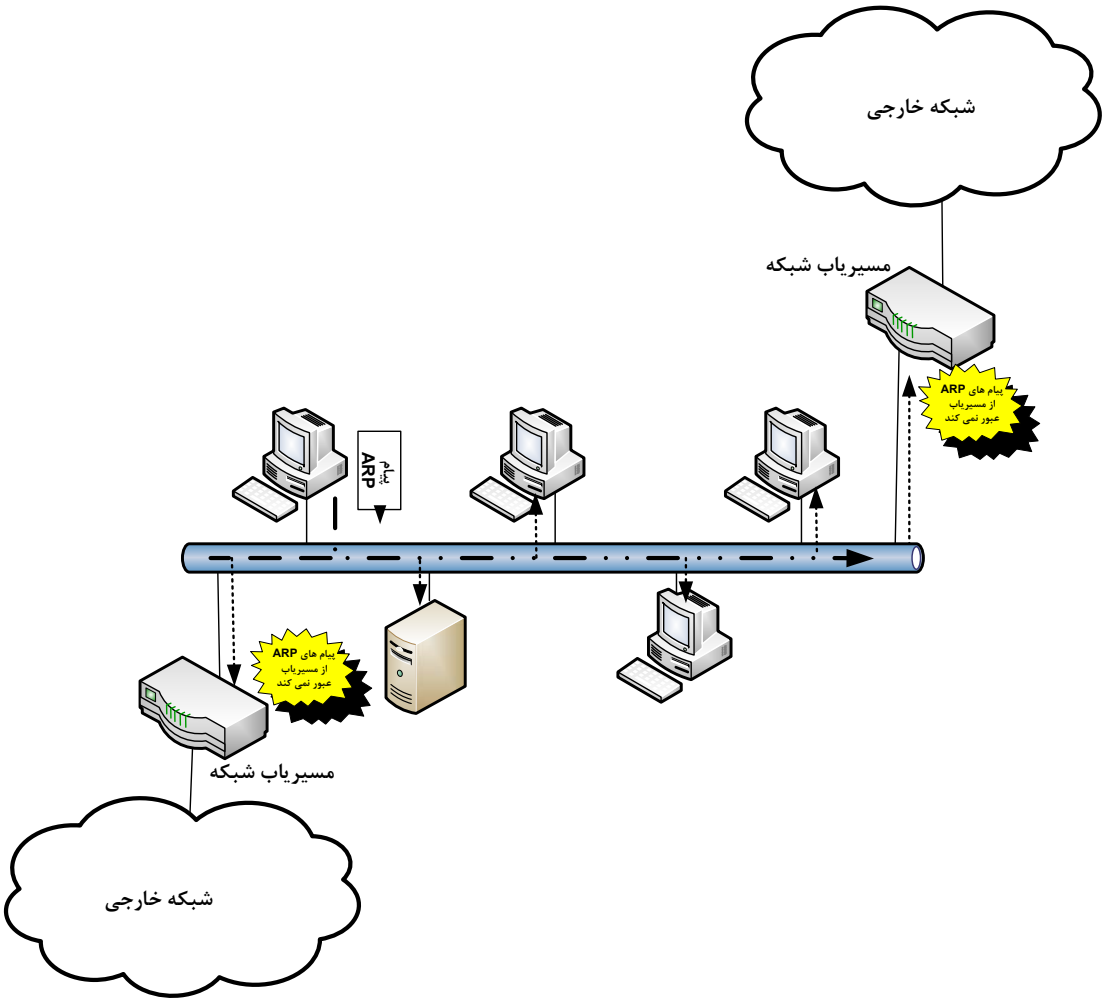
فیلد های بسته پاسخ ARP به شرح زیر می باشند :

- آدرس سخت افزاری فرستنده: شامل آدرس سخت افزاری نود مقصد (دلیل اصلی عملکرد ARP)
- آدرس IP فرستنده : شامل آدرس IP نود مقصد.
- آدرس سخت افزاری مقصد : شامل آدرس سخت افزاری فرستنده درخواست ARP است. نود مقصد آن را با بررسی فیلد آدرس سخت افزاری فرستنده در پیام درخواست ARP بدست می آورد.
- آدرس IP مقصد : شامل آدرس IP فرستنده درپیام درخواست ARP است. نود مقصد آن را با بررسی فیلد آدرس IP فرستنده در درخواست ARP بدست می آورد.

هنگامی که کامپیوتر مقصد دریک شبکه راه دور قرار داشته باشد، عملکرد پروتکل متفاوت می باشد. اگر مقصد در یک شبکه دور باشد (یک شبکه دیگر به جای شبکه محلی) ، فرستنده باید آدرس سخت افزاری درگاه مسیریابی را که بسته IP باید به آن ارسال شودرا پیدا کند.

در مورد شبکه های همه پخشی از پروتکلARP برای یافتن آدرس سخت افزاری نود مقصد استفاده می شود. پروتکلARP به عنوان بخشی از ماژول IP در شبکه هایی که نیاز به تجزیه آدرس دارند، مانند شبکه های محلی همه پخشی (اترنت ، شبکه حلقوی و غیره) پیاده سازی می شود. مطابق شکل (۸-۴)، پروتکل ARP توسط پروتکل IP بسته بندی نمی شود بلکه مستقیما توسط پروتکل لایه پیوند داده بسته بندی می گردد. این بدان معنی است که پیام های پروتکل ARP را نمی توان مسیریابی کرد، یعنی نمی تواند از مرز یک مسیر یاب عبور کند.

قبل از ارسال پیام درخواست ARP، پروتکل ARP سعی می کند تا آدرس مقصد را در حافظه پنهان محلی خود پیدا کند. جدول حافظه پنهان ARP که ساختار آن درشکل(۸-۵) نشان داده شده است، جفت ورودی های آدرس های IP و آدرس سخت افزاری متناظر را نگه می دارد. اگر آدرس IP مقصد در جدول حافظه پنهان ARP پیدا شود، آدرس سخت افزاری متناظر با آدرس IP مقصدرا جستجو نموده و آن را به ماژول ARP برمی گرداند.



شکل (۸-۴):محدودیت ARP در بخش شبکه محلی

درصورتیکه آدرس سخت افزاری کامپیوتر مقصد در جدول مربوطه پیدا نشود، ماژول ARP یک قاب لایه پیوند داده تولید می کند که شامل درخواست ARP برای کشف آدرس سخت افزاری نود مقصد است. درخواست ARP در لایه پیوند داده به همه نود ها در شبکه محلی پخش می شود. همانطور که قبلا ذکر شد، پاسخ ها و درخواست های ARP به بخش شبکه محلی محدود شده و از مرزمسیریاب عبور نمی کنند.

نوع پروتکل (IP)	آدرس پروتکل (آدرس های IP)	آدرس سخت افزاری	شماره واسط	برچسب زمانی

شکل(۸-۵): جدول حافظه پنهان ARP

هنگامی که یک درخواست ARP دریافت می شود، لایه پیوند داده در نود مقصد بسته را به ماژول مربوط به ARP می دهد. قاب درخواست ARP در سطح لایه پیوند داده همه پخشی می شود، بنابراین همه نود ها در شبکه محلی آن را دریافت می کنند با این وجود فقط نودی که آدرس IP آن مطابق با آدرس IP مقصد است با یک پاسخ ARP جواب می دهد. مراحل انجام شده توسط ماژول ARP در نود گیرنده به شرح زیر می باشد.

۱. آیا نوع سخت افزار را در فیلد نوع سخت افزار بسته درخواست ARP می شناسم ؟

۲. اگر جواب مرحله ۱ بلی است ، به طور اختیاری طول آدرس های سخت افزاری را در بسته درخواست ARP بررسی کن.
۳. آیا چگونگی پردازش پروتکل را در فیلد نوع پروتکل در بسته درخواست ARP می دانم؟
۴. اگر جواب مرحله ۳ بلی است، به طور اختیاری طول آدرس پروتکل را در بسته در خواست ARP بررسی کن .
۵. پرچم ادغام را برای کنترل پردازش ARP در مراحل بعدی به False مقدار دهی کن.
۶. اگر جفت "< نوع پروتکل ، آدرس پروتکل فرستنده >" هم اکنون در جدول ترجمه نود موجود است، فیلد آدرس سخت افزاری فرستنده را با ورودی اطلاعات جدید در بسته به روز برسان و پرچم ادغام را true کن.
۷. آیا آدرس پروتکلی مقصد هستم ؟ (به این معنی که آدرس IP من همان است که در فیلد آدرس IP مقصد آمده است؟)
۸ . اگر جواب مرحله ۷ بلی است سپس با تعیین کردن این که آیا پرچم ادغام false است ادامه بده . اگر پرچم ادغام false است، ۳ تایی (نوع پروتکل ، آدرس پروتکل فرستنده ، آدرس سخت افزاری فرستنده) را به جدول ترجمه اضافه کن .
۹ . آیا مقدار فیلد عملکرد، نشان دهنده یک درخواست است ؟
۱۰. اگر جواب مرحله ۹ بلی است، با عوض کردن فیلد های پروتکل و سخت افزار، قرار دادن آدرس های پروتکل و سخت افزار محلی در فیلد های فرستنده ادامه بده. فیلد عملکرد را به پاسخ ARP مقدار دهی کن. بسته را به آدرس سخت افزار مقصد (جدید) در همان سخت افزار که درخواست دریافت شده بفرست.

در الگوریتم فوق، قبل از این که فیلد عملکرد در مرحله ۶ بررسی شود ۳ تایی "< نوع پروتکل ، پروتکل فرستنده آدرس سخت افزاری فرستنده >" به جدول حافظه پنهان ARP ادغام می شود. این مرحله فقط زمانی رخ می دهد که یک نود یک ورودی برای آدرس IP فرستنده در جدول حافظه پنهان ARP دارد.

۸-۱-۳- نظارت برشبکه با کمک پروتکلARP

از پروتکل ARP می توان به عنوان یک وسیله نظارتی برای بدست آوردن اطلاعات لازم درباره فعالیت پروتکل های سطح بالا استفاده کرد. به عنوان مثال با بررسی فیلد نوع پروتکل موجود درقاب های ARP می توان اطلاعات مفیدی درمورد پروتکل های لایه سوم موجود درشبکه بدست آورد. هنگامی که سیستم نظارتی شبکه، یک پیامARP رادریافت می نماید، با بررسی آن می تواند به اطلاعات مفیدی نظیر: نوع پروتکل، آدرس IP فرستنده و گیرنده و آدرسهای سخت افزاری آنها دستیابی داشته باشد.
علاوه بر آن می تواند طول آدرس سخت افزاری و آدرس پروتکل را از فیلد های مربوطه موجود در بسته ARP مشخص کند. باید توجه نمودکه در خواست های ARP در سطح پیوند داده همه پخشی می شوند و یک سیستم ناظر همه در خواست های ARP را دریافت می کند. اگر فیلد عملکرد یک بستهARP نشان دهنده درخواستARP باشد وآدرس پروتکل مقصد با آدرس پروتکل ایستگاه ناظرمطابقت کند، ایستگاه ناظر نیزیک پاسخ ARP را مانند هر نود مقصد دیگر می فرستد.

۸-۱-۴- مهلت های زمانی[1] در جدول حافظه پنهان ARP

محتویات جداول حافظه پنهان ARP اغلب دارای یک مکانیزم مهلت زمانی می باشند. ورودی های جدول حافظه پنهان ARP ممکن است همراه با خود مقادیر برچسب زمانی داشته باشند. اگر یک نود درشبکه جابجا شود، معمولا قبل از نقل

[1] Timeout

مکان خاموش می شود . خاموش کردن یک نود، جدول حافظه پنهان ARP آن را پاک می کند. بنابراین ورودی های قدیمی باعث اشتباه نمی شوند، سایر نود های شبکه عموما آگاه نیستند که یک نود خاص نقل مکان کرده یا خاموش شده است.

اگر نود به مکانی در همان بخش شبکه نقل مکان کرده باشد، اطلاعات حافظه پنهان ARP درباره نود نقل مکان کرده هنوز معتبر هستند، زیرا دراین حالت آدرس IP و آدرس سخت افزاری نود نقل مکان کرده تغییر نمی کند. اگر نود خاموش شود سایر نود ها توانایی دسترسی به این نود را ندارند. سایر نود ها اطلاعات حافظه پنهان ARP خود را برای دستیابی به این نود استفاده می کنند اما قادر به ایجاد اتصال نیستند. اگر نود به مکانی در بخش متفاوتی از شبکه نقل مکان کرده باشد، دراین صورت پشت یک مرز مسیریاب است . دراین حالت آدرس IP نود نقل مکان کرده حتی اگر آدرس سخت افزاری همان باقی بماند، باید تغییر کند. ازآنجاییکه انتقال پیام های ARP از مرزیک مسیریاب امکان پذیرنمی باشد، بنابراین فرض می شود که نود جدید خاموش شده یا غیر قابل دسترس است.

همچنین برچسب های زمانی هنگامی که درخواست های ARP از نودی که ورودی آن در جدول حافظه پنهان ARP موجود است، دریافت می شود، به روز رسانی می شوند. چنانچه هیچ بسته ای از یک نود در یک مدت زمان معین دریافت نشود، دراین صورت ورودی مربوط به آن رکورد درجدول ARPپنهان حذف می شود. مدت زمان معین فوق برابر با مقدار مهلت زمانی ARP می باشد.

خیلی از پیاده سازی ها اجازه قراردادن ورودی های دستی را در جدول حافظه پنهان ARP می دهند. از آنجاییکه عملیات پویای ARP، آدرس IP و سخت افزاری مرتبط را مشخص می کند، معمولا نیازی به قرار دادن ورودی های دستی در جدول ARP نیست. ورودی های دستی ARP مهلت زمانی ندارند و می توانند برای رفع مشکلات با ورودی های نآدرست در جدول ARP به خاطر مشکلات آدرس IP تکراری یا عملکرد بد نرم افزار استفاده شوند.

۸-۱-۵- ARP در شبکه های پل بندی شده

اگر دریک شبکه TCP/IP مشکل فیزیکی ایجاد شود، ترمیم در لایه های پائین انجام می گردد. ماژول ARP سعی می کند در لایه های پائین تر به وسیله همه پخشی یک درخواست ARP اتصال را ترمیم کند. با این وجود هنگامی که چندین نود شروع به ارسال همه پخشی در خواست ARP کنند، ازدحام به وجود می آید. این امر هنگامی که میزبان مرکزی به خاطر نقص اتصال از کار افتاده است و اتصال فیزیکی آن به شبکه محلی قطع شده است، می تواند اتفاق بیافتد. به عنوان مثال، اگر ۱۵۰۰ ایستگاه به یک میزبان مرکزی در شبکه متصل باشند و اتصال شبکه به میزبان فوق از بین برود، همه ۱۵۰۰ ایستگاه فوق به طور همزمان شروع به ارسال قاب های همه پخشی ARP می کنند. در بعضی از سیستم ها، درخواست ARP در هر ثانیه فرستاده می شود. با ۵۰۰ ایستگاه فرستنده همه پخشی ARP ، در هر ثانیه ۵۰۰ بسته همه پخشی فرستاده می شود. این ترافیک همه پخشی مقدار مهمی ازترافیک شبکه ایجاد می کند که به قابلیت دسترسی به سایر نود های شبکه اثرمنفی می گذارد. ترافیک همه پخشی حتی نود هایی را که در حال حاضر به شبکه دستیابی ندارند، کند می کند. به این دلیل که کارت شبکه و نرم افزار مربوطه باید هر بسته همه پخشی را بررسی وپردازش نمایند.

ماژول ARP نیز برای هر درخواست همه پخشی اجرا می شود. پردازش حتی ۵۰ درخواست ARP در هر ثانیه مقدار زیادی از بار پردازشی را متحمل نود نموده وباعث کند کردن آن نود می شود. در نتیجه همه نود های شبکه به نظر کند میشوند.

همه پخشی های تکراری ARP ، درشبکه هایی که بوسیله پل از یکدیگر جدا شده اند، وضعیت را بدتر نیز می نماید. دراین حالت، درخواست ها و جواب های ARP باید از طریق این پل ها ارسال شوند. تکثیر ترافیک همه پخشی از وسط پل ها می تواند یک اثر افزایشی داشته باشد و ترافیک شبکه را بیشتر افزایش دهد.

۸-۱-۶- آدرس های تکراری و ARP

در یک شبکه باید آدرس های IP یکتا باشند. چون عنصر بشری در انتساب آدرس های IP وارد می شود، سهوا امکان انتساب نود های شبکه به آدرس های IP یکسان وجود دارد که باعث وقوع اشتباه و بی ثباتی درشبکه می شود. برای درک بهتر مشکل آدرس های IP تکراری، دو سناریوی مختلف زیر بررسی می شوند:

- آدرس های IP تکراری در سرویس گیرنده های TCP/IP
- آدرس های IP تکراری در سرویس دهنده های TCP/IP

ابتدا به بررسی مشکل آدرس های IP تکراری در سرویس گیرنده های TCP/IP می پردازیم. بدین منظور به ذکر یک مثال می پردازیم. به عنوان مثال شبکه ای را درنظر بگیرید که دو سرویس گیرنده TCP/IP به نامهای ایستگاه ۱ و ایستگاه ۲ درآن به یک سرویس دهنده مرکزی TCP/IP به آدرس IP 144.19.74.102 دسترسی دارند. آدرس سخت افزاری سرویس دهنده A است. فرض کنید که ایستگاههای ۱و۲ آدرس IP یکسان 144.19.74.1 را استفاده می کنند. آدرس های سخت افزاری آنها به ترتیب B و C است . ایستگاه ۱، یک جلسه FTP را با سرویس دهنده TCP/IP برقرار می کند. قبل از آغاز جلسه FTP ، ایستگاه ۱ باید برای بدست آوردن آدرس سخت افزاری سرویس دهنده، یک درخواست همه پخشی ARP برای آدرس سخت افزاری سرویس دهنده TCP/IP درشبکه منتشرکند. با دریافت درخواست ARP ، سرویس دهنده TCP/IP یک ورودی را برای فرستنده درخواست ARP (ایستگاه ۱) در جدول حافظه پنهان ARP خود اضافه می کند و یک پاسخ ARP را به فرستنده ارسال می نماید. با دریافت پاسخ ARP ، ایستگاه ۱ یک ورودی را برای سرویس دهنده TCP/IP در جدول حافظه پنهان محلی خود اضافه می کند. در این لحظه جدول حافظه پنهان ARP برای سرویس دهنده TCP/IP به شرح زیر است:

آدرس IP	آدرس سخت افزاری
144.19.74.1	B

همچنین جدول حافظه پنهان ARP برای ایستگاه ۱ به شرح زیر است :

آدرس IP	آدرس سخت افزاری
144.19.74.102	A

حال فرض کنید که ایستگاه ۲ تلاش به برقراری یک جلسه TCP/IP با همان سرویس دهنده TCP/IP می کند. قبل از ایجاد اتصال، ایستگاه ۲ باید آدرس سخت افزاری سرویس دهنده TCP/IP را بدست آورد. بدینمنظورایستگاه ۲ با ارسال یک درخواست ARP این امر را انجام دهد. با دریافت درخواست ARP، سرویس دهنده TCP/IP می خواهد یک ورودی برای فرستنده درخواست ARP (ایستگاه ۲) در جدول حافظه پنهان ARP خود اضافه کند و یک پاسخ ARP را به فرستنده ارسال کند. سرویس دهنده TCP/IP در می یابد که از قبل یک ورودی برای 144.19.74.1 در جدول حافظه پنهان ARP خود دارد. با توجه به توصیه نامه RFC826 درباره پروتکلARP، سرویس دهنده TCP/IP باید ورودی موجود را با ورودی جدید جایگزین کند.

بیشتر پیاده سازی های TCP/IP این جایگزینی را بی صدا و بدون ارسال پیام اخطار درباره امکان ایجاد مشکل آدرس IP تکراری، انجام می دهند. بعضی از پیاده سازی های TCP/IP یک پیام اخطار درباره امکان مشکل آدرس IP تکراری ارسال می دارند. سرویس دهنده TCP/IP به درخواست ARP از ایستگاه ۲ جواب می دهد. با دریافت پاسخ ARP، ایستگاه۲ یک ورودی را برای سرویس دهنده TCP/IP در جدول حافظه پنهان ARP محلی خود اضافه می کند. در این لحظه جدول حافظه پنهان ARP برای سرویس دهنده TCP/IP به شرح زیر است :

آدرس IP	آدرس سخت افزاری
144.19.74.1	C

جدول حافظه پنهان ARP برای ایستگاه ۲ به شرح زیر است :

آدرس IP	آدرس سخت افزاری
144.19.74.102	A

هنگامی که سرویس دهنده TCP/IP به ایستگاه ۱ داده ارسال می کند، آدرس سخت افزاری ایستگاه ۱ را که آدرس IP 144.19.74.1 است، در جدول حافظه پنهان ARP محلی خود جستجو می کند و داده را به این آدرس سخت افزاری می فرستد. متاسفانه این آدرس آدرس سخت افزاری ایستگاه ۲ است و داده به ایستگاه ۲ فرستاده میشود. ایستگاه ۱در انتظار برای یک پاسخ می ماند. در نهایت مهلت زمانی اتمام یافته و یا ممکن است ایستگاه برای ترمیم خطا دوباره راه اندازی شود. در هرصورت برنامه کاربردی فوق که تا مدتی پیش خوب کار می کرده است، ممکن است به طور ناگهانی از کاربیافتد.
البته ممکن است که ایستگاه ۲ با دریافت داده غیرمنتظره که در اصل برای ایستگاه ۱ در نظر گرفته شده بوده است، آن را رد کند و به طور اختیاری یک پیام خطا تولید کرده و جلسه خود را با سرویس دهنده TCP/IP ادامه دهد. همچنین ایستگاه ۲ نیز با داده های غیر منتظره گیج شده و آن نیز متوقف می شود.
حال با ذکر یک مثال به بررسی مشکل آدرس های IP تکراری درسرویس دهنده های TCP/IP می پردازیم. به عنوان مثال، یک شبکه محلی با دو سرویس دهنده به نام سرویس دهنده ۱ و سرویس دهنده ۲ رادرنظر بگیرید. فرض کنیدکه به طور اشتباه به هر دو ایستگاه آدرس IP تکراری 144.19.74.102 تخصیص داده شده است. آدرس های سخت افزاری سرویس دهنده ها به ترتیب A و B می باشند. فرض کنید یک ایستگاه با آدرس IP 144.19.74.1 سعی می کند تا به سرویس دهنده TCP/IP با آدرس IP 144.19.74.102 متصل شود. آدرس سخت افزاری ایستگاه C است. ایستگاه سعی می کند تا به سرویس دهنده ۲ متصل شود . قبل از ایجاد اتصال TCP/IP، ایستگاه فوق یک درخواست همه پخشی ARP را برای کشف آدرس سخت افزاری سرویس دهنده TCP/IP منتشر می کند. دو سرویس دهنده TCP/IP با همان آدرس IP مقصد 144.19.74.102 وجود دارند. با دریافت درخواست ARP فوق، هردو سرویس دهنده ۱ و سرویس دهنده ۲ یک ورودی را برای فرستنده درخواست ARP در جدول حافظه پنهان محلی ARP خود اضافه می کنند و یک پاسخ ARP را به فرستنده ارسال می نمایند. ایستگاه پاسخ ARP اول را می پذیرد و بی صدا پاسخ دوم را نادیده می گیرد. اگر پاسخ ARP سرویس دهنده۲ زودتر به ایستگاه برسد، ایستگاه یک ورودی برای سرویس دهنده ۲ در جدول حافظه پنهان ARP محلی خود اضافه می کند. در این لحظه جداول حافظه پنهان ARP برای سرویس دهنده ها و ایستگاه به شرح زیر است:

جدول حافظه پنهان ARP سرویس دهنده ۱:

آدرس IP	آدرس سخت افزاری
144.19.74.1	C

جدول حافظه پنهان ARP سرویس دهنده۲:

آدرس IP	آدرس سخت افزاری
144.19.74.1	C

جدول حافظه پنهان ARP ایستگاه:

آدرس IP	آدرس سخت افزاری
144.19.74.102	B

سپس ایستگاه محاوره را با سرویس دهنده ۲ به جای سرویس دهنده ۱ که در اصل قصد دارد، ادامه می دهد. اگر سرویس دهنده ۲ سرویس مورد نظر را نداشته باشد، اتصال قطع شده و کاربر یک پیام خطا راجع به پشتیبانی نشدن سرویس در سرویس دهنده دریافت می کند. اگر سرویس دهنده ۲ سرویس مورد انتظار ایستگاه را داشته باشد، کاربر سعی به برقراری ارتباط با آن سرویس می کند. اگر سرویس مورد نظر Telnet یا FTP باشد، نیاز به شناسه کاربر و رمز عبور می باشد. اگر کاربر یک حساب اتصال با همان شناسه و رمز عبور که در سرویس دهنده ۱ داشته است، درسرویس دهنده ۲ نداشته باشد، اتصال پذیرفته نمی شود. درصورتیکه شناسه کاربر و کلمه رمزعبوردر هر دو سرویس دهنده یکسان باشد، کاربر به سرویس دهنده اشتباه متصل می شود. دراین حالت این امکان وجود دارد که کاربربه دلیل آنکه به سرویس دهنده اشتباه متصل شده است، فایلها یا داده هایی را که انتظار آنها را داشته است، دریافت نکند.

۸-۱-۸- بررسی تکراری بودن آدرس های IP با کمک پروتکل ARP

دربسیاری از نسخه های معماری TCP/IP، هرکامپیوتر درهنگام راه اندازی یک درخواست ARP را درشبکه منتشر می نماید. دراین پیام، آدرس IP مقصد موجود درپیام درخواست ARP مساوی با آدرس IP نود ارسال کننده پیام می باشد. هدف از ارسال پیام درخواست ARPفوق، کشف این مطلب است که آیا نودی با آدرس IP تکراری وجود دارد یا خیر؟ درصورتیکه نودارسال کننده پیام، درپاسخ به درخواست فوق، پیام پاسخ ARP دریافت نماید، بدین معنی است که نوددیگری با آدرس IP نود فرستنده وجود دارد و این نشان دهنده وجود آدرس های IP تکراری درشبکه می باشد. درصورت وقوع این حالت، نودی که متوجه وجود آدرس تکراری درشبکه شده است، باید به نحوه مناسب تکراری بودن آدرس فوق را به اطلاع برساند.

با توجه به اینکه قاب های ARP از مسیریاب های موجود درمرزهای شبکه قابل عبور نمی باشند، بنابراین روال فوق وجود یا عدم وجود آدرس های IP تکراری درهمان شبکه محلی مقصد را بررسی نموده و نمی تواند مشکلات آدرس IP تکراری را که در بخش های دیگر شبکه که با مسیریاب به هم متصل شده اند را تشخیص دهد.

یکی دیگر از کاربردهای انتشار پیام درخواست ARP درابتدای راه اندازه همه نودهای شبکه این است که چنانچه کارت شبکه نود فرستنده پیام تعویض شده و آدرس سخت افزاری آن تغییر کرده باشد، دراین صورت با ارسال پیام فوق، تمام نودهای دیگر شبکه، آدرس جدید نود فرستنده را درجدول ARP پنهان خود قرار داده و آن را به روز رسانی می نمایند.

۸-۲- پروتکل RARP

هنگام توصیف عملکرد پروتکل ARP فرض براین بود که هر نود، آدرس IP خود را می داند. سوالی که مطرح می شود این است که چگونه یک نود آدرس IP خود را بدست می آورد؟ می توان آدرس IP نود رادرانباره محلی آن که معمولا یک فایل است، ذخیره نمود. اسم و محل آن فایل به پیاده سازی TCP/IP و سیستم عامل بستگی دارد. با این وجود بعضی از کامپیوترها انباره محلی ندارند. این کامپیوترها همه اطلاعات سیستم را در یک سرویس دهنده دور نگه می دارند. این کامپیوترها، ایستگاه های بدون دیسک خوانده می شوند. البته ممکن است که ایستگاه های بدون دیسک امروزی، دارای یک دیسک محلی باشند، اما این دیسک برای افزایش سرعت سیستم عامل استفاده می شود نه برای ذخیره سازی پارامتر های مربوط به معماری TCP/IP.

معمولا ایستگاه های بدون دیسک، یک کپی از تصویر سیستم عامل را در سرویس دهنده های دور نگهداری می کنند. هنگام راه اندازی، ایستگاه بدون دیسک یک کپی از تصویر سیستم عامل را از سرویس دهنده دور به حافظه خود بارگذاری می کند. قبل ازانجام این کار، نیاز به یک آدرس IP دارد. این آدرس IP نمی تواند یک مقدار تصادفی باشد، بلکه باید یکتا و دارای همان پیشوند آدرس های IP سایر نود های بخش شبکه باشد. معمولا ایستگاه بدون دیسک، آدرس IP خود را با ارسال یک

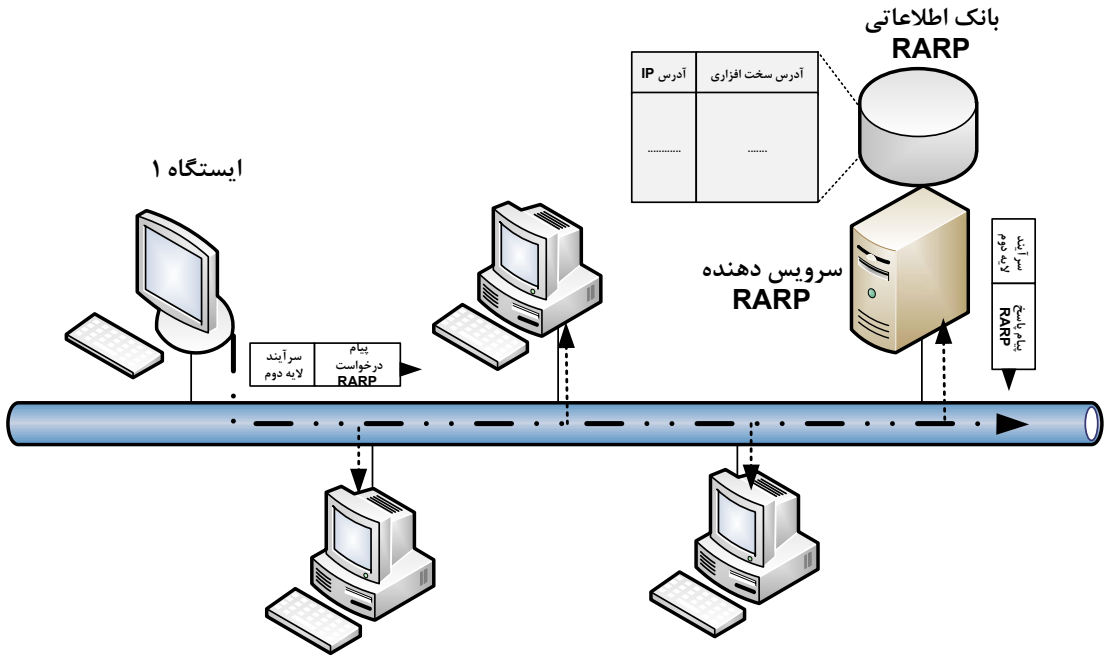
درخواست به سرویس دهنده های آن بخش شبکه بدست می آورد. چون ایستگاه فوق، اطلاعات آدرس سرویس دهنده دور را نمی داند، این درخواست به به صورت یک قاب همه پخشی لایه پیوند داده ارسال می شود. بدین منظور از پروتکل RARP استفاده می شود. اطلاعاتی که توسط پروتکلRARP جستجو می شود، برخلاف اطلاعات جستجو شده توسط پروتکل ARP است. سرویس گیرنده RARP ، آدرس سخت افزاری خود را می داند اما آدرس IP خود را ندارد، درصورتیکه سرویس گیرنده ARP ، آدرس سخت افزاری و آدرس IP خود را می داند اما آدرس سخت افزاری ایستگاه مقصد را نمی داند.

از ایستگاه های بدون دیسک برای کاهش هزینه های سخت افزاری ، ساده سازی پیکره بندی، امکان به روز رسانی توسط نگه داشتن اطلاعات بحرانی در یک جایگاه مرکزی و درامان ماندن از ویروس های نرم افزاری، استفاده می شوند.

۸-۲-۱- عملکردپروتکل RARP

در پروتکلRARP ، نودی که می خواهد آدرس IP خود را کشف کند (سرویس گیرنده RARP)، یک پیام درخواست را به نام پیام درخواست RARP درشبکه محلی همه پخشی می کند. چون سرویس گیرنده RARP ، آدرس سخت افزاری یا آدرس IP سرویس دهنده دور را نمی داند، بنابراین پیام درخواست RARP فوق درلایه پیوند داده همه پخشی می شود. همه نود های موجود درشبکه محلی، پیام درخواست RARP را دریافت می کنند اما تنها نود هایی که به عنوان سرویس دهنده های RARP عمل می کنند، به درخواست فوق پاسخ می دهند. چنانچه بیشتر از یک سرویس دهنده RARP وجود داشته باشد، همه سرویس دهنده های RARP تلاش می کنند تا درخواست RARP را پردازش نمایند. معمولا سرویس گیرنده RARP، اولین پاسخ دریافتی را پذیرفته و بقیه را نادیده می گیرد. سرویس دهنده RARP جدولی از آدرس های IP نود های شبکه را نگه داری می کند. این جدول توسط یک شناسه یکتا که برای هر ماشین خاص است، شاخص دار شده است. این شناسه یکتا به درخواست RARP فرستاده می شود. برای ایستگاه های بدون دیسک این شناسه یکتا، یک پارامتر سخت افزاری خاص می باشد که به آسانی قابل خواندن است.

به دلیل یکتا بودن آدرس های سخت افزاری، طراحان RARP از آدرس های سخت افزاری به عنوان شناسه های یکتای فوق استفاده می کنند. هنگامی که یک سرویس دهنده RARP یک درخواست RARP را دریافت می نماید، جدول خود را بررسی می کند. اگر یک ورودی در جدول RARP پیدا کرد که با آدرس سخت افزاری موجود در پیام درخواست RARPمطابقت دارد، آدرس IP متعلق به آن را در پیام پاسخ RARP بر می گرداند. از آنجاییکه سرویس دهنده RARP آدرس سخت افزاری سرویس گیرنده RARP را ازپیام درخواست RARP بدست می آورد، بنابراین نیازی به ارسال پیام پاسخ RARP به صورت همه پخشی نمی باشد. قالب بسته های دریافت و پاسخ RARP با قالب بسته های ARP یکسان می باشد. شکل (۸-۶) مثالی از عملکرد پروتکل RARP را نشان می دهد. دراین مثال فرض براین است که ایستگاه شماره ۱، آدرس IP ندارد. بدینمنظور پیام درخواست RARP به صورت همه پخشی درلایه ۲ ارسال می دارد. این پیام به سرویس دهنده RARP می رسد. سرویس دهنده با جستجو دربانک اطلاعاتی خود، آدرس IP متناظر با آدرس سخت افزاری ایستگاه فرستنده را پیدانموده و برای آن از طریق پیام پاسخ RARP ارسال می دارد.



شکل(۸-۶): مثالی از عملکرد RARP

توصیف فیلدهای موجود درپیام های درخواست و پاسخ RARP به شرح زیر می باشد:

پیام درخواست RARP

آدرس سخت افزاری مقصد درلایه دوم = همه پخشی

آدرس سخت افزاری مبدا درلایه دوم= آدرس سخت افزاری سرویس گیرنده RARP (ارسال کننده پیام)

فیلدEther Type موجود درقاب های پروتکل پیوند داده لایه دوم = 8035 hex

فیلد عملکرد موجود دربسته درخواست RARP = ۳ (نشان دهنده پیا م درخواستRARP)

آدرس سخت افزاری فرستنده موجوددربسته درخواستRARP = آدرس سخت افزاری سرویس گیرندهRARP (ارسال کننده پیام)

آدرسIP فرستنده موجود دربسته درخواستRARP = نامشخص است. معمولا از 0.0.0.0 استفاده می شود.

آدرس سخت افزاری مقصد موجود دربسته درخواستRARP = آدرس سخت افزاری سرویس گیرنده RARP

آدرسIP مقصد موجود دربسته درخواستRARP = نامشخص

پیام پاسخ RARP

آدرس سخت افزاری مقصد درلایه دوم= آدرس سخت افزاری سرویس گیرنده RARP

آدرس سخت افزاری مبدا درلایه دوم= آدرس سخت افزاری سرویس دهنده RARP

فیلدEther Type موجود درقاب های پروتکل پیوند داده لایه دوم = 8035 hex

فیلد عملکردموجود دربسته های RARP = ۴ (پاسخ RARP)

آدرس سخت افزاری فرستنده موجود دربسته پاسخ RARP= آدرس سخت افزاری سرویس دهنده RARP .

آدرس IP فرستنده موجود دربسته پاسخ RARP = آدرس IP سرویس دهنده RARP .

آدرس سخت افزاری مقصد موجود دربسته پاسخ RARP= آدرس سخت افزاری سرویس گیرنده RARP.

آدرسIP مقصد موجود دربسته پاسخ RARP = آدرس IP سرویس گیرنده RARP (این جواب است)

در خیلی از پیاده سازیهایTCP/IP، پروتکل RARP به طور اتوماتیک توسط ماژول ARP یا ماژول IP فراهم نشده بلکه باید به عنوان یک فرایند جداگانه درکامپیوتری که به عنوان سرویس دهنده RARP عمل می کند، اجرا گردد.

۸-۲-۲- مشکلات RARP

درصورتیکه بخاطر یک نقص اتصال سخت افزاری یا بخاطر از کار افتادن، سرویس دهنده RARP در دسترس نباشد، سرویس های گیرنده های RARP قادر به راه اندازی نیستند. دراین حالت سرویس گیرنده های RARP ، به منظور بدست آوردن آدرس IP خود، به طور پیوسته درخواست های همه پخشی RARP را می فرستند. اگر سرویس گیرنده های RARP زیادی به طور هم زمان درخواست RARP را منتشر کنند، این امر بار ترافیکی سنگینی را در شبکه ایجاد می کند. بنابراین مشکلات ایجاد شده به خاطر دریافت نکردن یک پاسخ RARP، به مراتب جدی تر از دریافت نکردن یک پاسخ ARP است. اگر پاسخ ARP دریافت نشود، به این معنی است که یک میزبان خاص و سرویس های آن دردسترس نبوده و سرویس گیرنده ARP هنوز می تواند برای دستیابی به سایر نود های شبکه تلاش کند. اما اگر پاسخ RARP دریافت نشود، سرویس گیرنده RARP نمی تواند راه اندازی شود. دراین حالت سرویس گیرنده های RARP زیادی به ارسال در خواست های همه پخشی RARP به طور نامحدود ادامه می دهند به امید اینکه سرویس دهنده RARP درنهایت به درخواست آنها پاسخ دهد. بنابراین این مسئله می تواند ترافیک زیادی را در شبکه ایجاد کند.

۸-۲-۳- سرویس دهنده های اصلی و پشتیبان RARP

رای دستیابی مطمئن تر به سرویس های RARP ، ازچندین سرویس دهنده RARP به طور همزمان استفاده می شود. با کمک سرویس دهنده های RARP چند گانه، همه سرویس دهنده ها به طور همزمان برای جواب دادن به درخواست همه پخشی RARP تلاش می کنند. فقط یکی از جواب های RARP توسط سرویس گیرنده RARP مورد استفاده قرارگرفته وسایرپاسخ های RARP دیگر حذف می شوند. برای جلو گیری از پاسخ های RARP چندتایی، یکی از سرویس دهنده ها به عنوان سرویس دهنده اصلی و سایر سرویس دهنده ها RARP به عنوان سرویس دهنده ثانویه درنظر گرفته می شوند.

با دریافت یک پیام درخواست RARP، سرویس دهنده اصلی RARP به درخواست پاسخ می دهد و سرویس دهنده های ثانویه پاسخی نمی دهند وفقط زمان ورود درخواست RARP را یادداشت می کنند. اگر سرویس دهنده اصلی در بازه زمانی معینی پاسخ نداد، سرویس دهنده ثانویه RARP فرض می کند که سرویس دهنده اصلی از کار افتاده و به درخواست RARP پاسخ می دهد.

۸-۳- پروتکل اینترنت (IP)

با استفاده ازپروتکل اینترنت (IP) می توان که پروتکل های لایه حمل مانند پروتکل های TCP و UDP، را فقط به عنوان یک شبکه IP دانست درحالیکه در واقعیت ممکن است که فقط یک شبکه IP نباشد و پروتکل های دیگری را در کنار TCP/IP پشتیبانی کنند. پروتکل IP سرویس های بدون اتصال را برای لایه بالاتر مهیا می سازد. این سرویس بدون اتصال با بسته هایی که شامل آدرس های IP مقصد و مبدا و سایر پارامتر های دیگر مورد نیاز برای عملکرد IP هستند، پیاده سازی می شوند.

لایه IP برای ارسال بسته های خود به سخت افزار زیرین شبکه تکیه دارد. به این معنی که بسته IP توسط قاب شبکه زیرین مانند اترنت، شبکه حلقوی ویا شبکه های سوئیچینگ بسته ای، بسته بندی می شود. پروتکل های لایه بالا مانند

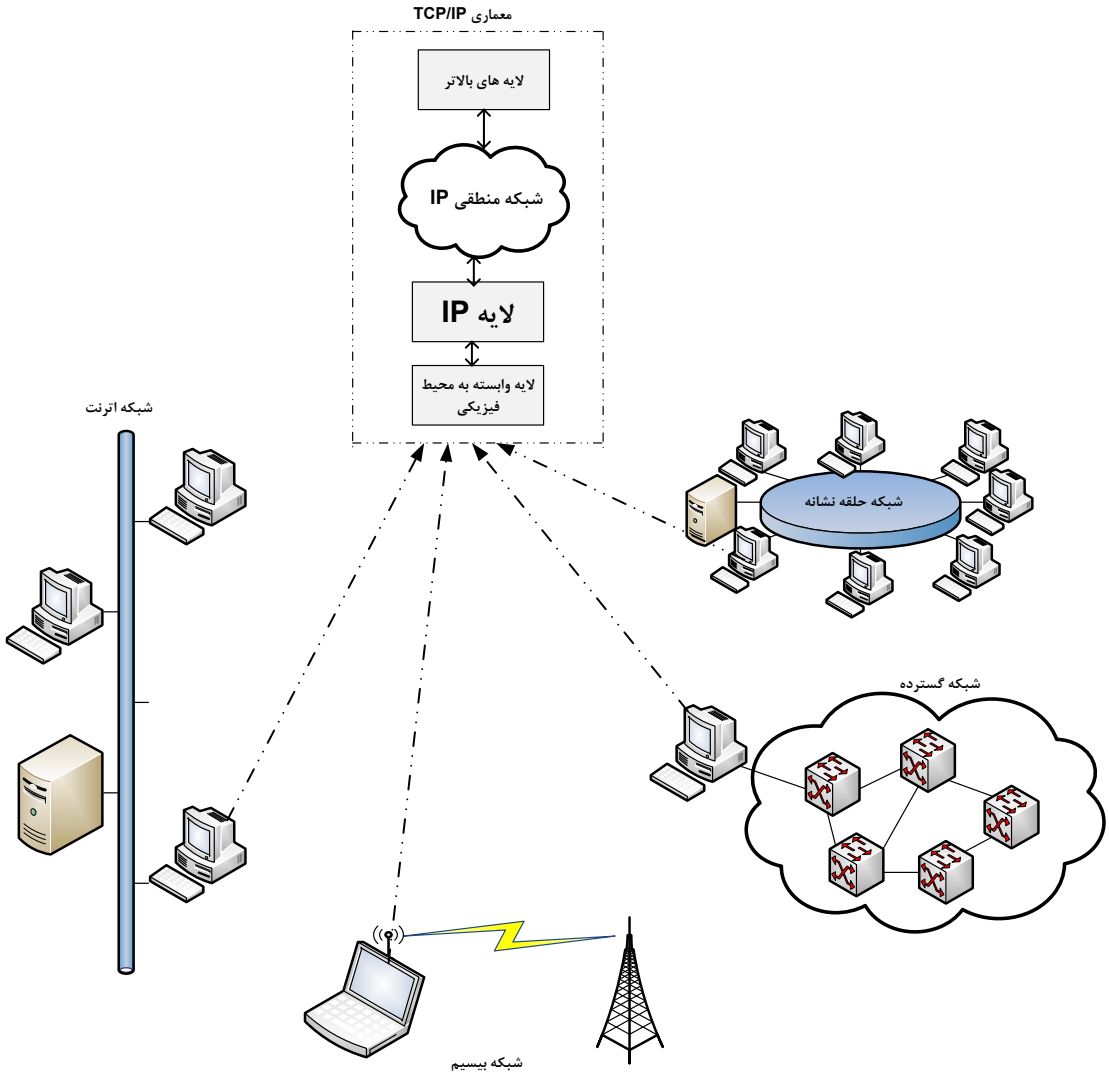
TCP و UDP نیازی به آگاهی از بسته بندی سخت افزار شبکه ندارند. پروتکل های لایه بالا ،کیفیت مطمئن سرویس مانند تاخیرکم و گذردهی مناسب را انتظاردارند. این عوامل پارامترهای کیفیت سرویس نامیده میشوند. لایه های بالاتر پارامترهای کیفیت سرویس را همراه با داده های خود به لایه IP پاس می دهند. لایهIP سعی براین دارد تا پارامتر های کیفیت سرویس را به سرویس های تهیه شده توسط سخت افزار زیرین شبکه نگاشت دهد. ممکن است که سخت افزار زیرین شبکه، قادر به فراهم سازی این سرویسها باشند.

شکل(۸-۷)، شبکه های ناهمگون مختلفی شامل : اترنت، شبکه حلقه نشانه، شبکه بیسیم و شبکه گسترده رانشان می دهد. درتمامی این شبکه ها میزبان هایی وجود دارند که از معماری TCP/IP استفاده می نمایند. دراین شبکه ها ، پروتکل IP در تمام شبکه ها اجرا می شود. میزبان های شبکه با کمک اتصال های IP به شبکه متصل می شوند. این اتصالات شبکه توسط یک شناسه ۳۲ بیتی یکتا به نام آدرس IP مشخص می شوند. لایه IP یک انتزاع را برای هر یک از سه شبکه به لایه های بالاتر معرفی می کند. این انتزاع به صفات فیزیکی شبکه ها مانند اندازه آدرس ، حداکثر واحد ارسال درلایه پیوند داده، پهنای باند شبکه، حداکثر سرعت ارسال داده و غیره بستگی دارد.

طبق تعریف، به حداکثر میزان نرخ قابل ارسال در یک شبکه فیزیکی، حداکثر واحد ارسال (MTU[1]) گفته می شود. به عنوان مثال در شبکه نشان داده شده در شکل (۸-۷) اندازه MTU شبکه اترنت ۱۵۰۰ بایت است. اندازه MTU برای شبکه حلقه نشانه IEEE802.5 ازنوع ۴ مگابیت برثانیه، ۴۴۴۰ بایت است. این اندازه برای شبکه حلقوی IEEE802.5 ۱۶مگابیت برثانیه، ۱۷۹۴۰ بایت می باشد. درشبکه هایX.25 اندازه MTU اختیاری بوده و در بازه ۶۴ بایت تا۴ کیلو بایت قابل تغییر است. باید توجه داشت که حداقل طول یک بسته IP نمی تواند از ۵۷۶ بایت کمتر باشد.

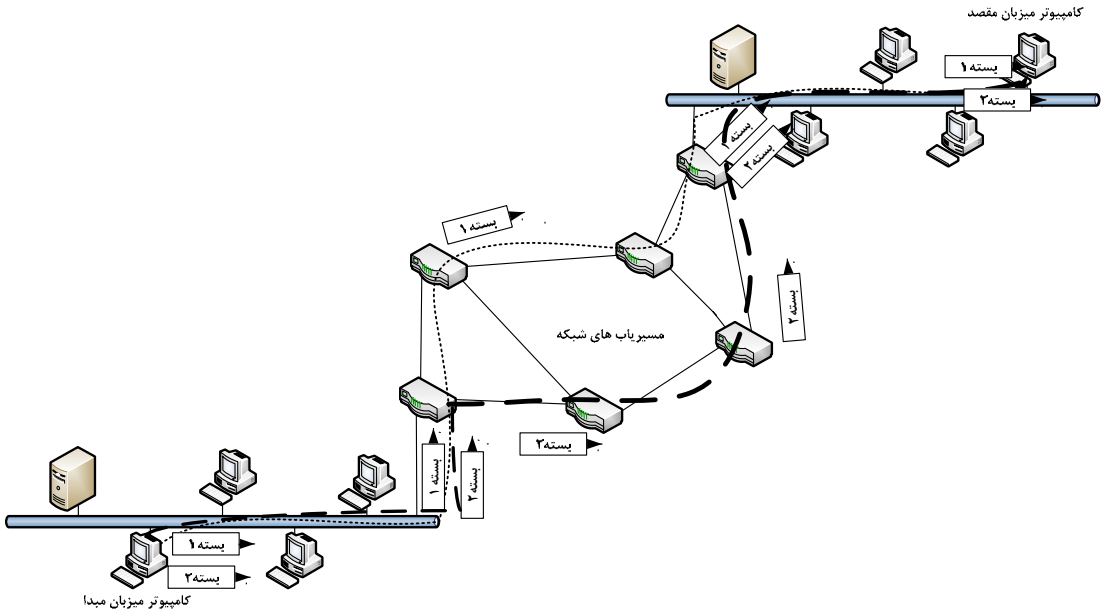
پروتکل IP بدون اتصال بوده که هر بسته درآن به طور مستقل مسیریابی می شود. بنابراین ممکن است بسته های متوالی در مسیر های متفاوت انتقال داده شوند.

[1] Maximum Transfer Unit



شکل(۸-۷): نمونه ای از استفاده از IP برروی شبکه های فیزیکی مختلف

درشکل(۸-۸) مثالی از مسیریابی بسته ها دریک شبکه IP نشان داده شده است.



شکل(۸-۸): مسیریابی مستقل بسته های IP

به خاطر اختلاف تاخیرهای زمینی در بین مسیر ها، این امکان وجود دارد که بسته ها با ترتیبی متفاوت با آن ترتیبی که فرستاده شده اند به مقصد برسند. لایه IP هیچ تلاشی برای تحویل مرتب بسته ها به لایه های بالاتر نمی کند. همچنین این پروتکل هیچ تلاشی برای تحویل مطمئن بسته ها به مقصد نمی نماید. مشکل ترتیب بسته ها و تحویل مطمئن داده ها توسط یک پروتکل لایه بالا مانند TCP حل می شود.

چون IP تلاشی بر ای حل ترتیب دهی و تحویل مطمئن داده ها نمی کند، به آسانی به هر نوع سخت افزار شبکه قابل نگاشت می باشد. پروتکل های لایه بالا، سطوح اطمینان اضافی را چنانکه مورد نیاز برنامه های کاربردی است فراهم می کنند. بنابراین شبکه IP بدون تضمین بوده و به صورت بهترین تلاش عمل می کند. این بدان معنی است که پروتکل IP سعی می کند که بهترین کار ممکن را برای تحویل بسته های IP انجام دهد ولی تحویل سالم و به ترتیب بسته ها را ضمانت نمی کند. درپروتکل IP هر بسته مستقل از بقیه بسته ها مسیر یابی می شود. هربسته شامل آدرسIP مقصد و آدرسIP فرستنده می باشد.

مسیریاب های میانی شبکه با استفاده از آدرس IP مقصد، بسته هایIP را به مقصد درست پیش می برند. مستقل بودن پروتکل IP از پروتکل های زیرین شبکه باعث می شود که بسته های IP بدون توجه به اندازه MTU لایه های پایین تر، ارسال شوند. نود های میانی شبکهIP در صورت نیاز می توانند یک بسته بزرگ را تکه سازی نمایند.

پروتکلIP برای تطبیق دادن با انواع مختلف سخت افزار شبکه طراحی شده است. همانطور که قبلا اشاره شد، شبکه های مختلف محدودیت های متفاوتی برای حداکثر اندازه داده قابل ارسال توسط قاب لایه پیوند داده دارند. جدول(۸-۳) اندازه MTU انواع سخت افزار های مختلف شبکه را فهرست کرده است.

جدول(۸-۳): اندازه های MTU شبکه های مختلف

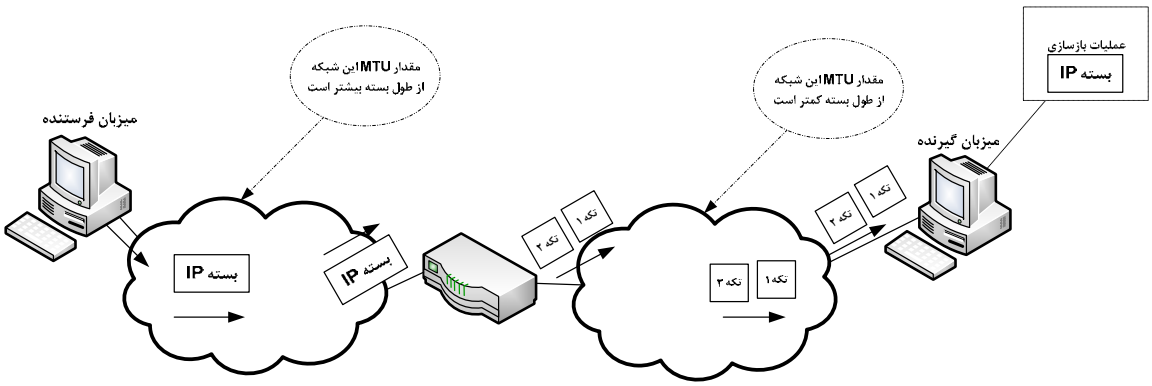
نوع شبکه	اندازه MTU
اترنت	۱۵۰۰بایت
IEEE 802.3	۱۴۹۲ بایت
شبکه حلقوی IEEE 802.5	۴۴۴۰ بایت تا ۱۷۹۴۰ بایت (بستگی به سرعت ارسال در شبکه دارد)
FDDI	۴۳۵۲ بایت

IEEE 802.4	۸۱۶۶ بایت
SMDS	۹۱۸۰ بایت

حداکثر طول یک بسته IP ۶۵۵۳۶ بایت است. مقدار MTU اغلب شبکه ها از مقدار حداکثر طول قابل ارسال بسته های IP به مراتب کمتر می باشد.هیچ مکانیزم کارامدی برای تعیین MTU شبکه های میانی توسط پروتکل IP وجود ندارد. اگر این امر انجام شود، فرستنده می تواند بسته های IP را به اندازه ای تنظیم کند که ازاندازه MTU شبکه های میانی تجاوز ننماید. ولی درعمل شبکه های IP با استفاده از مکانیزم تکه سازی قادر به تحویل بسته هایی با اندازه دلخواه به هر شبکه می باشند.

۸-۳-۱- تکه سازی IP

اگر یک بسته IP از اندازه MTU شبکه ای که باید از آن عبور کند، بیشترباشد دراین صورت نمی تواند در یک تکه کامل فرستاده شود. دراین حالت باید بسته IP به تکه های کوچکتری که از اندازه MTU شبکه تجاوز نمی کند، شکسته شود. این فرایند، عملیات تکه سازی نامیده می شود. هر تکه از بسته اصلی به عنوان یک بسته IP مستقل فرستاده می شود. در سرآیند IP اطلاعات کافی برای مشخص کردن تکه، حمل می شود. میزبان مقصد با استفاده از اطلاعات تکه سازی موجود در سرآیند بسته های IP قادربه سر هم کردن تکه ها می باشد. شکل(۸-۹) فرایند ارسال یک بسته IP را در شبکه هایی با اندازه های مختلف MTU نشان می دهد. در این مثال، اندازه MTU شبکه B کوچکتر از اندازه بسته ارسالی است. مسیریاب R1 این حقیقت را تشخیص داده و بسته های IP را به اندازه های کوچکتری تکه سازی می کند تا از اندازه MTU شبکه B تجاوز نکند. بسته های تکه شده به طور مستقل مسیریابی می شوند و به میزبان C می رسند. اگر چه اندازه MTU شبکه C از اندازه تکه های بسته IP بزرگتر بوده و حتی می تواند با بسته اصلی مطابقت کند، ولی مسیر یاب R2 موجود درمرز بین شبکه های B و C هیچ تلاشی برای دوباره سرهم کردن تکه ها برای تشکیل بسته اصلی نمی کند. عملیات بازسازی تکه های بسته IP توسط ماژول IP موجود درکامپیوتر میزبان درمقصد انجام می شود. هرگز مسیر یابهای میانی شبکه عملیات فوق را انجام نمی دهند.



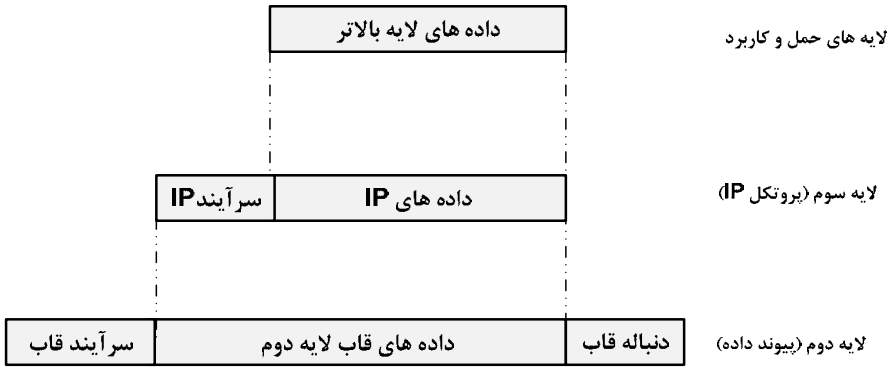
شکل(۸-۹): تکه سازی بسته IP

هنگامی که میزبان B نیاز به پاسخ به میزبان A داشته باشد دراین صورت اندازه بسته را طوری تنظیم می کند تا از اندازه MTU شبکه B تجاوز نکند. بسته هی ارسالی از میزبان C به میزبان A می تواند بدون هیچ تکه سازی تحویل داده شود. با این وجود، مسیریاب های میانی شبکه سعی نمی کنند که برای افزایش کارآیی انتقال، بسته های کوچکتر را با یکدیگر ترکیب نموده و یک بسته بزرگتر ایجاد نمایند. باید به این نکته توجه نمود که درشبکه های IP بسته های تکه شده فقط در مقصد سر هم می شوند.

۸-۳-۲- قالب بسته IP

همانطور که درشکل (۸-۱۰) نشان داده شده است، بسته های IP از دو قسمت تشکیل شده اند که عبارتند از: سرآیندIP و داده های IP . سرآیند IP برای مطابقت با خواص لایه IP طراحی شده است. سرآیند IP باید حداقل شامل اطلاعات زیر باشد:

- آدرس IP مبدا و مقصد: این اطلاعات لازم است چون IP یک پروتکل بدون اتصال است و اطلاعات کامل آدرس مقصد و مبدا باید در هر بسته موجود باشد.
- کیفیت سرویس: این فیلد برای مشخص کردن نوع سرویس مورد انتظار از شبکه زیرین لازم است.
- اطلاعات تکه سازی : چون بسته IP ممکن است که در داخل شبکه تکه سازی شود، باید فیلد هایی برای کمک به تشخیص تکه ها، درون بسته اصلی باشد.
- اندازه بسته: ازآنجاییکه اندازه بسته های IP می تواند متغیر باشد، بنابراین باید فیلدی برای مشخص کردن طول کلی بسته IP وجود داشته باشد.
- اندازه سرآیند IP : بسته های IP می تواند شامل فیلد های اختیاری برای مشخص کردن امکانات IP استفاده شده برای امنیت، مسیریابی مبدا و غیره باشد. این عامل اندازه طول سرآیند IP را متغیر می سازد. بنابراین اندازه واقعی بستهIP باید درسرآیند IP نشان داده شود.



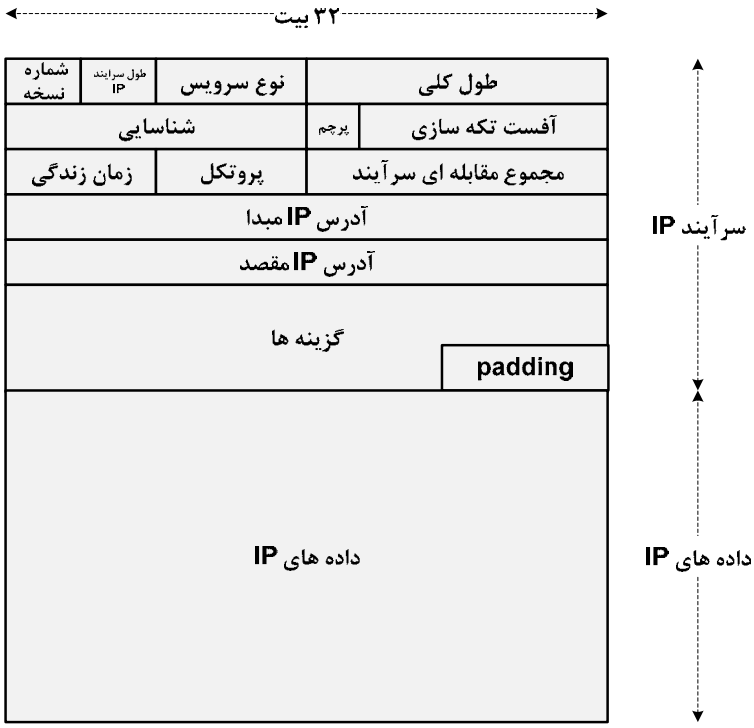
شکل(۸-۱۰): نحوه بسته سازی داده ها درمعماری TCP/IP

کمترین طول سرآیند IP ۲۰ بایت است. چون درسرآیندIP، فیلدی برای امکانات اضافی درنظر گرفته شده است، بنابراین طول سرآیند ممکن است بیشتراز۲۰ بایت باشد. شکل (۸-۱۱)، فیلدها و ساختار سرآیند IP را نشان می دهد. قالب سرآیند IP با جزئیات کامل در RFC 791 و RFC 1122 بحث شده است. همچنینRFC 1349 استفاده فیلد نوع سرویس را با جزئیات کامل در سرآیند IP توصیف می کند.

۸-۳-۲-۱- فیلد شماره نسخه

مطابق با شکل (۸-۱۱)، فیلد شماره نسخه درسرآیند بسته های IP دارای ۴ بیت طول می باشد و نشان دهنده شماره نسخه پروتکل IP است. این امرتوانایی معرفی ساختارهای آینده بسته IP را فراهم می سازد. شماره نسخه فعلی IP ۴ است و به این علت پروتکل فعلی اینترنت، پروتکل IPV4 نامیده می شود. نسل آتی پروتکل IP دارای مقدارفیلد شماره نسخه برابر با ۶ است. به این علت، پروتکل آتی IP، با عنوان IPV6 شناخته می شود. جدول (۸-۴) مقادیر مختلف فیلد شماره نسخه نشان داده شده است. باید توجه نمود که مقادیر شماره نسخه ۷ ، ۸ و ۹ پروتکل های IP پیشنهادی و تجربی برای حل

مشکل محدودیت آدرس های ۳۲ بیتی انتساب داده شده اند که این پروتکل ها با آمدن پروتکل IPV6 کنار گذاشته شده اند.



شکل (۸-۱۱): ساختار بسته های IP

فیلد شماره نسخه توسط فرستنده، گیرنده و مسیریاب های میانی برای مشخص کردن قالب سرآیند IP استفاده می شود. برای بررسی فیلد نسخه، نیاز به نرم افزارIP می باشد تا بدین وسیله اطمینان حاصل شود که قالب سرآیند همان قالب مورد انتظار است. بدین ترتیب اگر نرم افزار IP فقط بتواند بسته های نسخه ۴ را پردازش کند، بسته هایی را که مقدار شماره نسخه آنها غیر از ۴ می باشند، رد می گردند.

جدول(۸-۴): مقادیرمختلف شماره نسخه IP

شماره نسخه	توصیف
۰ و ۱۵	رزرو
۱-۳ و۱۰-۱۴	انتصاب داده نشده است
۴	پروتکل فعلی اینترنت (IPV4)
۵	پروتکل آزمایشی Stream IP
۶	پروتکل آتی اینترنت (IPV6)
۷	پروتکل اینترنت TP/IX
۸	پروتکل اینترنت P
۹	پروتکل TUBA

پروتکل Stream IP، یک پروتکل آزمایشی است که برای تضمین سرویس انتها به انتها دراینترنت استفاده می شود. این پروتکل در RFC 1819 توصیف شده است .پروتکلTP/IX ، پروتکل 'P" و TUBAهمه زمانی مدعی جدی جایگزینی IPV4 بودند، اما با آمدن پروتکل IPV6 این سه پروتکل اهمیت خود را از دست داده اند. پروتکل اینترنت "P"، یک پروتکل جدید با خواص پیشرفته و آدرس هایی با طول متغیر است. این پروتکل، بعد از مدتی که از پیدایش آن می گذشت

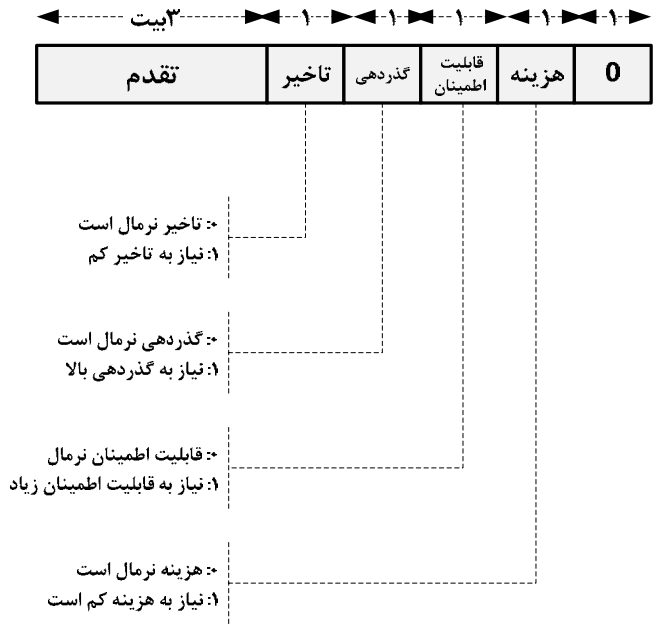
با پروتکل اینترنت ساده (SIP) ادغام گردید. پروتکلSIP از آدرس دهی ۶۴ بیتی استفاده می کند و نحوه گذر بین IPV4 و آدرس دهی طولانی تر را توصیف می کند. پروتکلSIP درRFC 1710 توصیف شده است. پروتکل TP/IX، یک پروتکل قدیمی بوده که پایه معماری مشترک برای اینترنت گردید. پروتکل TUBA در RFC 1347 ، RFC1526 ، RFC 1561 توصیف شده است

۸-۳-۲-۲- فیلد طول سرآیند اینترنت (IHL)

فیلد طول سرآیند اینترنت، طول سرآیند بسته های IP را برحسب کلمات ۳۲ بیتی نشان می دهد. این فیلد ۴ بیت طول دارد. از آنجاییکه سرآیند IP شامل فیلد امکانات با طول متغیر است، فیلد طول سرآیند اینترنت مورد نیاز می باشد. مقدار معمول این فیلد، ۵ کلمه ۳۲ بیتی است. دراین حالت امکانات اضافی دربسته IP وجود ندارد. حداکثرطول سرآیندبسته های IP با درنظر گرفتن فیلد امکانات، برابر با ۶۰ بایت است. در این حالت مقدار IHL ، ۱۵ کلمه ۳۲ بیتی خواهد بود.

۸-۳-۲-۳- فیلد نوع سرویس[1](TOS)

فیلد نوع سرویس ، نوع سرویس درخواستی را از نظر پارامترهایی نظیر: میزان تقدم ، تاخیر ، گذردهی و اطمینان را مشخص می کند. اجزای این فیلد ۸ بیتی در شکل (۸-۱۲) نشان داده شده است.



شکل(۸-۱۲): ساختار فیلد نوع سرویس برای بسته های IP

۳ بیت اول، مقدارترتیب تقدم همراه با بسته IP را نشان می دهد. فیلد ترتیب تقدم ۳ بیت طول دارد وکدینگ آن در جدول (۸-۵) نشان داده شده است.

[1] Type of Service

جدول(۸-۵): مقادیرزیرفیلد ترتیب تقدم درفیلد نوع سرویس

مقدارتقدم	توصیف
۰۰۰	تقدم عادی
۰۰۱	تقدم دارای اولویت
۰۱۰	تقدم فوری
۰۱۱	تقدم آنی
۱۰۰	تقدم برتر از آنی
۱۰۱	تقدم بحرانی
۱۱۰	تقدم کنترل بین شبکه ای
۱۱۱	تقدم کنترل شبکه

از۴ بیت بعدی که به دنبال فیلدترتیب تقدم درساختار فیلد نوع سرویس می آیند، برای نشان دادن نوع سرویس درخواستی استفاده می شود. این کدها همان طور که در جدول (۸-۶) نشان داده شده اند به صورت زیر تفسیر شده اند.

جدول(۸-۶): کدهای نوع سرویس

کد	توصیف
۱۰۰۰	نیاز به تاخیر کم
۰۱۰۰	نیاز به حداکثر گذردهی
۰۰۱۰	نیاز به حداکثر قابلیت اطمینان
۰۰۰۱	نیاز به کمترین هزینه
۰۰۰۰	سرویس معمولی

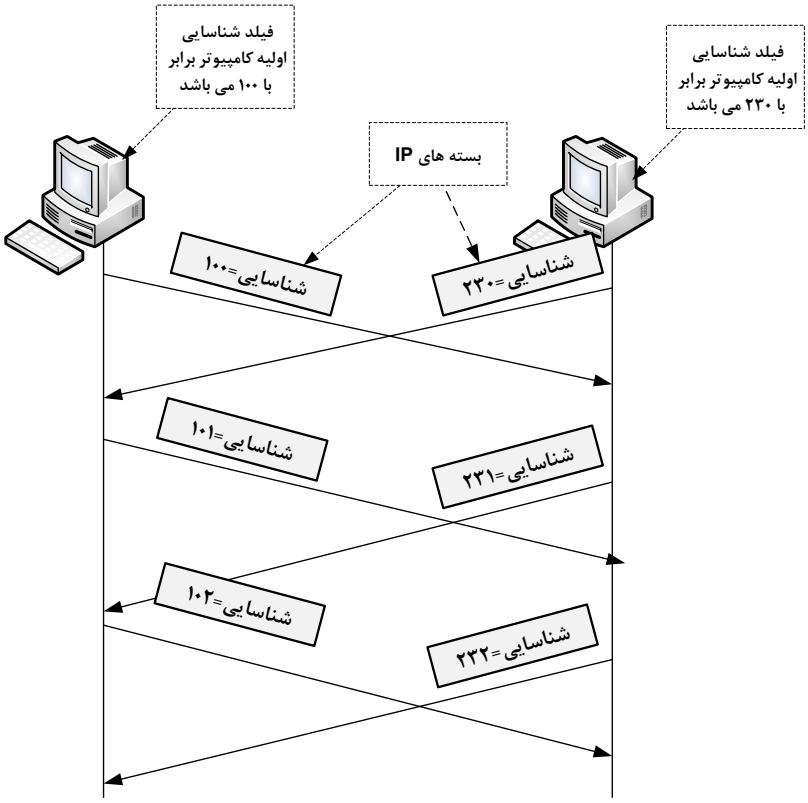
آخرین بیت فیلد نوع سرویس همواره برابر با ۰ می باشد و برای استفاده در آینده رزرو شده است.

۸-۳-۲-۴- فیلد طول کلی

فیلد طول کلی نشان دهنده طول بسته IP شامل سرآیند IP وداده بر حسب بایت می باشد. این فیلد ۱۶ بیت طول دارد و بسته را به حداکثر اندازه ۶۵۵۳۵ بایت محدود می کند. ازآنجائیکه معمولا اندازه MTU اغلب شبکه ها خیلی کمتر از ۶۵۵۳۵ بایت است، بنابراین بسته هایی که ۶۵۵۳۵ بایت طول دارند برای اغلب میزبانها و شبکه ها غیر قابل عبورمی باشند. همچنین چنانچه بسته های IP به بزرگی ۶۵۵۳۵ بایت باشند دراین صورت طراحی با فرهای ارسال درفرستنده وهمچنین بافرهای مسیریاب های میانی کارآمد نیست. معمولاً اندازه بسته برای اغلب شبکه ها و میزبانها بندرت از KB ۱۶ تجاوز میکند. همه نود های IP باید توانایی دریافت بسته هایی را با طول حداقل ۵۷۶ بایت داشته باشند. همانطور که قبلا اشاره شد، بسته هایی که دارای طول بیشتر از اندازه MTU شبکه زیرین باشند، باید تکه سازی شوند.

۸-۳-۲-۵- فیلد شناسایی

فیلد شناسایی برای هر بسته به طور یکتا مقدار دهی می شود و نشان دهنده شماره بسته است. هر طرف ارسال، درابتدای اتصال از یک مقدار اولیه به عنوان شماره بسته استفاده می کنند. همانطور که درشکل (۸-۱۳) نشان داده شده است، با ارسال هر بسته جدید، یکی به مقدار این فید اضافه می شود. اغلب پیاده سازیهای IP از یک شمارنده حافظه عمومی استفاده می کنند که با ارسال هر بسته IP ، یک واحد افزایش می یابد.



شکل (۸-۱۳): مثالی از کاربرد فیلد شناسایی

فیلد شناسایی۱۶ بیت طول دارد که این امر اجازه می دهد تا بسته ها از ۰ تا ۶۵۵۳۵ شماره گذاری شوند. فیلد شناسایی دراصل برای شناسایی تکه های بسته IP که متعلق به یک بسته IP اصلی خاص هستند، استفاده می شود. باید توجه نمود که درهنگام تکه سازی یک بسته IP به تکه های کوچکتر، مقدار این فیلد درتمام تکه های IP تغییرنکرده و یکسان می باشد.

۸-۳-۲-۶- فیلد های پرچم و افست تکه سازی

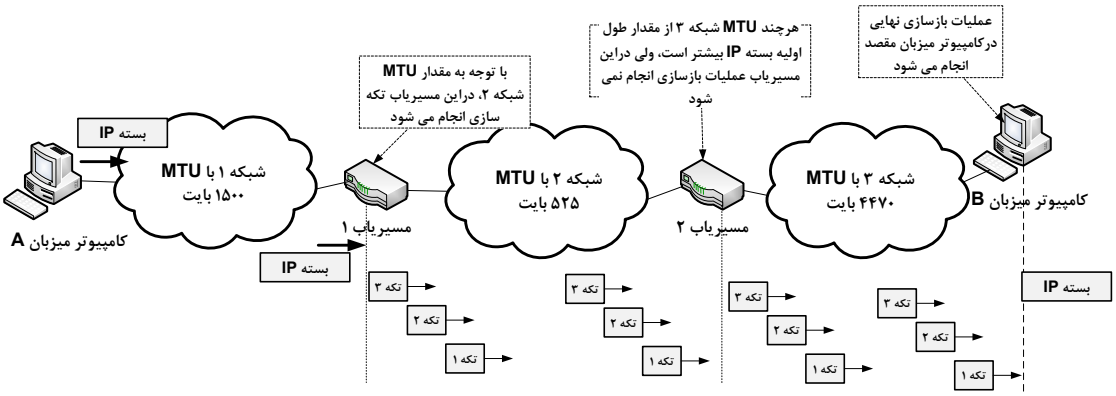
فیلد پرچم سه بیت طول دارد. اولین بیت این فیلد همواره صفر است. بیت های دوم و سوم به ترتیب بیت های DF[1] و MF[2] می باشند. اگر مقدار پرچم DF برابر با۱ باشد، به این معنی است که نباید بسته تکه سازی شود. چنانچه فرستنده بداند که گیرنده توانایی کافی برای بازسازی تکه های بسته اصلی را ندارد، آنگاه مقدار فیلد DF را برابر با ۱ قرار می دهد تا از تکه سازی احتمالی بستهIP درنودهای میانی جلوگیری شود. به عنوان مثال برنامه boot strap که در Rom کامپیوتراجرا می شود، داده ها را از یک ماشین سرویس دهنده بار گذاری می نماید. اگر کل داده برای جا شدن در یک بسته طراحی شده باشد، فرستنده می تواند پرچم DF را ۱ قرار دهد.

چنانچه پرچم MF برابر با۱باشد، گیرنده متوجه خواهد شد که تمام تکه های بسته اصلی هنوز نیامده اند وتکه های بیشتری درراه می باشند. مقدار ۰ درفیلد پرچم فوق، نشان دهنده این است که این تکه، آخرین تکه می باشد. برای بسته های IP کامل، پرچم MF همیشه ۰ خواهد بود که نشان می دهد تکه های بیشتری از این بسته وجود ندارد.

درادامه با ذکر یک مثال نحوه تکه سازی در پروتکل IP را توضیح می دهیم. شبکه نشان داده شده درشکل (۸-۱۴) را در نظر بگیرید که درآن یک میزبانA در شبکه۱ بسته های IP را به میزبانB در شبکه ۳ می فرستد. مقدار MTU درشبکه

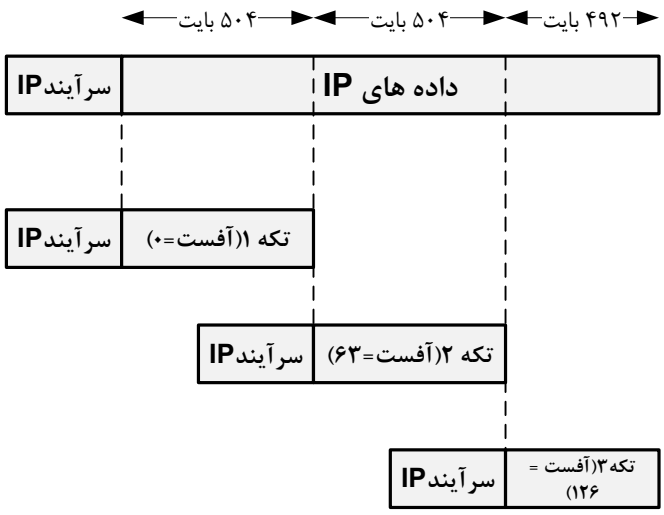
[1] Don’t Fragment
[2] More Fragment

های۱و۲و۳ به ترتیب ۱۵۰۰ ، ۵۲۵ ، ۴۴۷۰ بایت است. مسیریاب ۱ شبکه های۱ و ۲ را به هم پیوند می دهد و مسیر یاب ۲ شبکه های ۲ و ۳ را به هم متصل می کند. فرض کنید بسته ای با مقدار شناسایی ۵ به اندازه ۱۵۰۰ بایت به وسیله میزبان A فرستاده می شود. هنگامی که مسیریاب ۱ با این بسته مواجه می شود، قبل از این که بسته را به شبکه ۲ارسال نماید، باید آن راتکه سازی کند. دلیل این امرآن است که اندازهMTU شبکه ۲کوچکتر از اندازه بسته می باشد. اندازه تکه هاطوری انتخاب می شوند که بسته های تکه شده داخل MTU شبکه۲ که ۵۲۵ بایت است جا شوند.



شکل(۸-۱۴): مثالی ازنحوه تکه سازی درIP

فیلد افست تکه سازی ،مکان داده مربوط به آغاز بسته اصلی را نشان می دهد. این فیلد ۱۳ بیت طول دارد. با بررسی قالب سرآیندIP ، به این نتیجه می توان رسید که تنها ۱۳ بیت فضا برای این فیلد درنظر گرفته شده است. ازآنجاییکه حداکثر طول یک بسته IP می تواند تا ۶۵۵۳۵ بایت باشد، طول این فیلد برای توصیف مقادیر بزرگتر از ۸۱۹۲ بایت به اندازه کافی نیست. به این دلیل فیلد افست تکه سازی با ضمیمه کردن ۳ بیت صفر توسعه می یابد. در نتیجه مقدار افست تکه سازی همیشه ضریبی از۸ بایت است وهمواره تکه ها را در واحد های ۸ بایتی توصیف می کند. به عبارت دیگر، مقدار افست تکه سازی باید در ۸ ضرب شود تا افست حقیقی تکه بدست بیاید. بنابراین طول همه تکه ها غیر از آخرین تکه، باید مضرب ۸ باشند. به علاوه تکه ها باید داخل اندازه MTU شبکه جا شوند. با توجه به اندازه MTU ۵۲۵ بایت با تفریق اندازه معمول سر آیند IP که ۲۰ بایت است، ۵۰۵ بایت برای اندازه تکه حاصل می شود. ازآنجائیکه این عدد مضرب ۸ نمی باشد، کوچکترین اندازه بعدی تکه که قابل تقسیم بر ۸ است ۵۰۴ است. بنا براین می توان اندازه تکه های بسته IP را ۵۰۴ بایت انتخاب نمود. شکل (۸-۱۵) شکستن بسته IP اصلی را به تکه های کوچکتر نشان می دهد. طول تکه های اول و دوم برابر با ۵۰۴ بایت می باشد و آخرین تکه دارای طول ۴۹۲ بایت است.



شکل(۸-۱۵): مثالی از تکه سازی بسته اصلی IP

هر تکه باید سرآیند IP خودش را داشته باشد. مقدار فیلد شناسایی در بسته های IP تکه شده، برابر با مقدار متعلق به بسته IP اصلی است. این امر مشخص می کند که تکه IP به یک بسته IP اصلی خاص تعلق دارد. مقادیر تنظیمات پرچم و افست تکه سازی بسته هایIP تکه سازی شده درجدول (۸-۶) نشان داده شده است:

شماره تکه	طول کلی	شناسایی	پرچم DF	پرچم MF	آفست تکه سازی
تکه اول	۵۰۴ بایت	۵	۰	۱	۰
تکه دوم	۵۰۴ بایت	۵	۰	۱	۶۳
تکه سوم	۴۹۲	۵	۰	۰	۱۲۶

برای این که گیرنده قادر به بازسای تکه های بسته IP باشد، باید همه آنها را دریافت نماید. به منظور انجام عملیات بازسازی، گیرنده ازفیلدهای : اندازه هر تکه (فیلد طول کلی سرآیند بسته IP)، مقدار افست تکه سازی و پرچم MF استفاده می کند. با استفاده از فیلدهای فوق، گیرنده قادر خواهد بود تا مشخص کندکه آیا همه تکه ها را دریافت کرده است یا خیر؟ باید توجه نمود که مقدار پرچم MF تکه آخر صفر می باشد. همچنین تکه اول با مقدار پرچم MF برابربا۱ و افست تکه سازی برابر با صفر شناسایی می شود. همچنین برای تکه های میانی، مقدار پرچم MF برابر با ۱ و مقدار افست تکه سازی غیر صفر است. بعد از تکه سازی بسته های IP، هرتکه در مسیر های جداگانه احتمالی به سمت مقصدحرکت می کند. تکه های IP در گیرنده مجدداً بازسازی می شوند. باید توجه داشت که هیچ گاه در یک مسیر یاب میانی عملیات بازسازی انجام نمی شود. علیرغم این که ممکن است شبکه های میانی دارای اندازه MTU بزرگتر از اندازه تکه باشند، تکه ها در بسته هایی با اندازه کوچک حمل می شوند که در نتیجه باعث کاهش بازدهی پروتکل می شود. همچنین باید توجه داشت که تکه سازی زیاد منجر به ترافیک زیاد شبکه می شود.

اگر یک تکه گم شود، امکان بازسازی بسته اصلی نبوده و علیرغم انتقال موفق تکه های باقیمانده، بسته اصلی باید حذف شود. درصورت از بین رفتن یک بسته، پروتکل های لایه بالا مانند TCP متوجه شده و درخواست ارسال مجدد بسته گم شده ازمقصد را می نمایند. گیرنده بسته هایIP بعد از دریافت اولین تکه، یک زمان سنج خاصی را که زمان سنج باز سازی نام دارد، راه اندازی می نماید. اگر این زمان سنج قبل از رسیدن سایرتکه ها تمام شود، گیرنده تکه های باقیمانده را حتی اگر به درستی دریافت شده اند، از بین می برد. با افزایش تعداد تکه ها، احتمال از دست دادن یک بسته IP نیز افزایش می

یابد. هنگامی که زمان سنج باز سازی به اتمام می رسد، یک پیام ICMP خاص به فرستنده ارسال می شود تا بدینوسیله به گیرنده اعلام شود که زمان سنج بازسازی تمام شده است.

انجام عملیات بازسازی بسته های IP درگیرنده، با وجود مشکلاتی که در قبل توضیح داده شد، این مزیت عمده را درپی دارد که باعث ساده سازی مسیریابهای میانی شبکه می شود. مسیریابهای IP هیچگونه نگرانی درمورد انجام عملیات باز سازی و ذخیره کردن مجدد تکه های IP ندارند. اگر چندین شبکه با اندازه MTU کوچک وجود داشته باشند، ازآنجاییکه بسته IP باز سازی شده قبل از عبور از یک شبکه با اندازه MTU کوچک باید مجدداً تکه سازی شود، بنابراین بازسازی مجدد تکه های IP در مسیریابهای میانی شبکه کاری بیهوده است.

۸-۳-۲-۷- فیلدزمان زندگی(TTL[1])

فیلد زمان زندگی که برحسب ثانیه اندازه گیری می شود، نشان دهنده حداکثر زمانی است که یک بسته IP می تواند در شبکه زنده بماند. درهر مسیریاب میانی، مقدار زمان لازم برای پردازش یک بسته از مقدار فیلد فوق کم می شود. هنگامی که فیلد فوق برابر با صفر می شود، زمان زندگی بسته به اتمام رسیده و بسته باید از بین برود. فیلد TTL دو وظیفه عمده زیر را انجام می دهد:

- زمان زندگی سگمنت های TCP را محدود می کند.
- به حلقه های مسیریابی داخل شبکه خاتمه می دهد.

هنگامی که مقدار فیلدTTL دریک بسته IP صفر می شود، یک پیام ICMP برای آگاهی از این حقیقت به مبدا فرستاده می شود. اگر چه TTL برحسب ثانیه اندازه گیری می شود، تخمین زدن دقیق زمان لازم برای عبور بسته های IP ازیک مسیریاب شبکه کار مشکلی است. بدینمنظور، مسیریاب های شبکه باید زمانی را که بسته IP داخل مسیریاب شده یاد داشت نموده و از زمان خروج بسته از مسیریاب، کم نمایند. حاصل تفریق فوق برابر با زمان لازم برای پردازش بسته درمسیریاب IP می باشد. چون پردازش فوق زمان بر می باشد، بنابراین بسیاری از مسیریاب ها برای سادگی مقدار TTL را از ۱کم می کنند. به خاطر این امر فیلد TTL نشان دهنده حداکثر تعداد پرش های مجاز یک بسته درشبکه می باشد. بعضی از پیاده سازی های قبلی پروتکل IP اشتباها مقدار TTL را ۱۶ می گرفتند. دلیل استفاده از عدد ۱۶ این است که عدد فوق برای پروتکل مسیریابی RIP نشاند دهنده فاصله بی نهایت می باشد. سایر نکات مهم برای فیلد TTL به صورت زیر است:

- یک میزبان نباید یک بستهIP را با مقدارفیلد TTL برابر با ۰ بفرستد. همچنین یک میزبان نباید یک بسته را فقط به خاطر این که با TTL کمتر از ۲ دریافت شده حذف کند.
- پروتکل های لایه بالا می توانند از TTL برای پیاده سازی یک حوزه وسیع جستجو برای یک منبع اینترنت استفاده کنند.
- مقدار TTL باید حداقل برابر با قطرشبکه باشد. منظور از قطر شبکه، طولانی ترین مسیر ممکن از مبدابه مقصد است. البته دراکثر موارد مقدار منطقی TTL برابر با دوبرابر قطر فوق تنظیم می شود.
- لایه IP باید ابزاری را برای لایه حمل فراهم کند تا بتوان فیلد TTL هر بسته ارسالی راتنظیم نمود. هنگامی که از یک مقدار TTL ثابت استفاده می شود، مقدارفوق باید قابل پیکره بندی باشد. متاسفانه خیلی از پیاده سازی ها، قادر به تعیین مقدار اولیه TTLنبوده واز مقدار پیش فرض ۳۲ یا ۶۴ استفاده می نمایند.

[1] Time to Live

۸-۳-۲-۸- فیلد پروتکل

فیلد پروتکل برای مشخص کردن پروتکل لایه بالایی که باید داده های موجود در بسته IP رادریافت کند، استفاده می شود. به عبارت دیگر از این فیلد برای تسهیم سازی و غیرتسهیم سازی داده به پروتکل های لایه بالا استفاده می شود. به عنوان مثال مقدار فیلد پروتکل برای پروتکل TCP برابر با۶ است. این مقدار برایUDP برابر با ۱۷ و برای ICMP برابر با۱ است. هنگامیکه پروتکلIP درسمت گیرنده متوجه شد که مقدار فیلد فوق دربسته دریافتی برابربا۶ است، می فهمد که داده های موجود دربسته IP متعلق به پروتکل TCP بوده و باید به ماژول TCP تحویل داده شود. به طور مشابه هنگامیکه IP می بیند مقدار فیلد پروتکل ۱ است، می فهمد که این بسته باید به ماژولICMP تحویل داده شود .

۸-۳-۲-۹- فیلد مجموع مقابله ای سرآیند[1]

این فیلد فقط برای بررسی خطای احتمالی در سرآیند IP استفاده می شود. مکمل۱تمام مقادیر۱۶ بیتی موجود درسرآیند IP با هم جمع می شود (بجز خود فیلد مجموع مقابله ای سرآیند)، سپس مکمل ۱مجموع حساب می شود. مقدار حاصل جمع فوق، برابر با مقدار مجموع مقابله ای سرایند بوده و درفیلد مناسب قرار می گیرد. از آنجاییکه فیلد TTL در هر مسیر یاب کاهش می یابد وباعث تغییرات درسرآیند IP می شود، بنابراین مقدار سرآیند درهر مسیریاب تغییر کرده و این باعث می شود که مقدار مجموع مقابله ای در هر مسیریاب دوباره حساب شود. شواهد نشان می دهد که این مکانیزم درتشخیص خطاهای انتقال بسته مناسب است.

۸-۳-۲-۱۰- آدرس های IP مبدا و مقصد

آدرسIP مبدا وآدرسIP مقصد، آدرس های IP ۳۲ بیتی نودهای مبدا و مقصد هستند. از آنجاییکه شبکه های IP از نوع بدون اتصال می باشند، هربسته به صورت مستقل پردازش و مسیریابی شده و بنابراین نیاز است که درهربسته IP مقادیر آدرس های IP مبدا و مقصد موجود باشند. مسیریاب ها از مقدار آدرس IP مقصد برای انجام مسیریابی هر بسته IP استفاده می کنند.

۸-۳-۳-۱۱- فیلد های گزینه و padding

ازفیلد گزینه برای فراهم سازی برخی امکانات اضافی درپروتکل IP استفاده می شود. فیلد گزینه دارای طول متغیر می باشد. با توجه به اینکه طول سرآیند بسته های IP حتما باید مضربی از ۳۲ بیت باشد، فیلد padding درانتهای گزینه قرار دارد. چنانچه طول فیلد گزینه مضربی از ۴ بایت نبود، به مقدار کافی درناحیه padding بیت صفر اضافه می شود تا فیلد گزینه مضربی از ۳۲ بیت باشد. درصورتیکه فیلد گزینه مضربی از ۳۲ بیت باشد، نیازی به فیلد padding وجود ندارد. درادامه به بررسی گزینه های مهم IP می پردازیم.

۸-۳-۳- گزینه های IP[2]

پروتکل IP دارای یکسری امکانات اضافی برای انجام برخی عملیات اختیاری می باشد. ازآنجاییکه این امکانات اختیاری بوده و الزامی دراستفاده آنها نمی باشد، با عنوان گزینه های IP شناخته می شوند. گزینه های IP به شرح زیر است :

- امنیت
- ثبت مسیر
- مسیریابی مبدا دقیق[3]

---

[1] Cheak sum
[2] IP Options
[3] Strict Source Routing

- مسیریابی مبدا ضعیف[1]
- برچسب زمانی اینترنت

همه نودهای شبکه IP باید قادر به پردازش و حمایت از گزینه های IP باشند. این گزینه هادرانتهای سرآیند IP ظاهر می شوند. برای مثال در محیط هایی که به امنیت بالا نیاز دارند، ممکن است گزینه امنیت در همه بسته های IP لازم باشد. طول فیلد گزینه متغیر است و باید مضربی از کلمات ۳۲ بیتی باشند. درصورت لزوم، می توان از مقادیر پرکننده صفر برای رساندن طول گزینه به مضرب ۳۲ بیت استفاده نمود. دو قالب برای مقادیر گزینه IP وجود دارند. قالب اول فقط شامل یک بایت منفرد از گزینه می باشد. قالب دوم گزینه، شامل یک بایت نوع گزینه، یک بایت طول گزینه و بایت های داده گزینه، می باشد. بایت طول گزینه دربرگیرنده اندازه همه اجزای گزینه شامل فیلد های نوع گزینه ، طول گزینه و داده گزینه می باشد.

بایت نوع گزینه ، اولین بایت موجود درگزینه است که از آن برای تعیین نوع گزینه استفاده می شود. فیلد نوع گزینه شامل سه فیلد زیر می شود:

- پرچم کپی شده (۱بیت)
- کلاس گزینه (۲ بیت)
- شماره گزینه (۵ بیت)

پرچم کپی شده، نحوه پردازش فیلد گزینه درهنگام عملیات تکه سازی درمسیریاب ها را کنترل می کند. چنانچه این پرچم ۱ باشد، بدان معنی است که گزینه ها باید در همه تکه های بسته IP کپی شود. هنگامی که پرچم فوق صفر باشد، بیانگز آن اشت که گزینه ها باید دراولین تکه IP و نه در همه تکه های بسته IP کپی شوند. فیلد کلاس گزینه دو بیت طول دارد و می تواند مقداری از صفر تا سه داشته باشد. کد۰ به منظور کنترل شبکه وکد۲ برای اشکال زدایی واندازه گیری به کار می رود. کد۱و۳ برای استفاده های آتی رزرو شده است. فیلد کلاس برای مشخص کردن نوع کلاس گزینه استفاده می شود. گزینه های مختلفی برای عملیات کنترل شبکه و اشکال زدایی استفاده می شوند. فیلد شماره گزینه ۵ بیت طول دارد وبه وسیله آن می توان حداکثر ۳۲ گزینه را برای کلاس گزینه داده شده تعیین نمود. جدول (۸-۷) گزینه های مختلف تعریف شده را فهرست کرده است.

جدول(۸-۷): گزینه های مختلف IP

طول گزینه	شماره گزینه	کلاس گزینه	پرچم کپی شده	مقدار	نام اختصاری گزینه	توصیف گزینه
–	۰	۰	۰	۰	EOOL	انتهای لیست گزینه: این گزینه فقط ۱ بایت رااشغال نموده وبایت طول ندارد. هنگامی که گزینه ها در انتهای سرآیند اتمام نیابند، از این گزینه استفاده می شود.
–	۱	۰	۰	۱	NOP	بدون عملکرد: این گزینه فقط ۱ بایت اشغال نموده و بایت طول ندارد. برای همتراز کردن بایتها در یک لیست گزینه ها استفاده می شود.
۱۱	۲	۰	۱	۱۳۰	SEC	امنیت اصلی: برای حمل اطلاعات مربوط به امنیت شبکه استفاده می شود.
متغیر	۳	۰	۱	۱۳۱	LSR	مسیریابی مبدا ضعیف: برای مسیریابی بسته IP براساس مسیرتهیه شده به وسیله مبدا استفاده می

[1] Loose Source Routing

						شود.
متغیر	۵	۰	۱	۱۳۳	E-SEC	امنیت توسعه یافته: برای مشخص کردن امنیت اضافی استفاده می شود
متغیر	۷	۰	۰	۷	RR	ثبت مسیر: برای ردیابی مسیری که بسته IP طی می کند، استفاده می شود
۴	۸	۰	۱	۱۳۶	SID	درپروتکل Stream IP استفاده شده و هم اکنون غیر مستعمل است.
متغیر	۹	۰	۱	۱۳۷	SSR	مسیر یابی مبدادقیق: برای مسیریابی بسته IP به کمک مسیرتعیین شده توسط مبدا استفاده می شود.
متغیر	۴	۲	۰	۶۸	TS	برچسب زمانی اینترنت: برای ثبت برچسب های زمانی در طی مسیر ارسال بسته استفاده می شود. این گزینه در کلاس اندازه گیری و اشکال زدایی تعریف شده است

بخش های بعدی انواع مختلف گزینه IP را با جزئیات بیشتر توضیح می دهد :

۸-۳-۳-۱- انتهای لیست گزینه و گزینه های بدون عملکرد

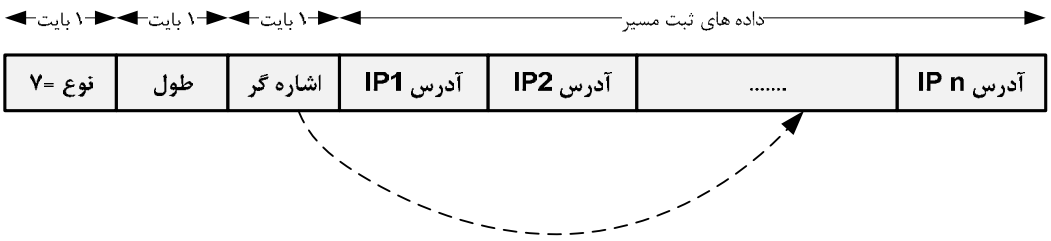
تنها گزینه های تک بایتی، گزینه های انتهای لیست گزینه و گزینه بدون عملکرد می باشند. انتهای لیست گزینه، یک گزینه تک بایتی حاوی بیتهای صفراست. این گزینه، انتهای لیست گزینه را نشان می دهد. این گزینه در انتهای لیست همه گزینه ها و نه درانتهای هر گزینه استفاده می شود. گزینه فوق، درصورتی که انتهای گزینه ها از جهات دیگر در مرز ۳۲ بیت نباشد، مورد نیاز است. گزینه بدون عملکرد بین گزینه ها استفاده شده و ابتدای یک گزینه بعدی را در یک مرز ۳۲ بیتی همتراز می کند.

۸-۳-۳-۲-گزینه امنیت

گزینه امنیت راهی را برای فراهم سازی امنیت برای میزبان ها مهیا می سازد. دو نوع گزینه امنیت وجود داردکه عبارتند از: امنیت پایه و امنیت توسعه داده شده. امنیت پایه برای مشخص کردن سطح امنیت، سمت های محرمانه ، غیر دسته بندی شده سری و غیره استفاده می شود. امنیت توسعه داده شده برای معین کردن امنیت اضافی در یک سازمان نظامی استفاده می گردد.

۸-۳-۳-۳-گزینه ثبت مسیر

گزینه ثبت مسیر توسط فرستنده استفاده می شود وبرای ثبت آدرس IP مسیر یاب هایی که بسته IP را به مقصد پیش می برند، استفاده می شود. دراین گزینه، لیست مسیریاب هایی که بسته ازآنهاعبورکرده است ، ثبت می شود. مطابق با شکل (۸-۱۶)، گزینه ثبت مسیر با مقدار کد نوع گزینه ۱۳۱ شروع می شود. بایت دوم، طول گزینه است. سومین بایت موجود درگزینه فوق، بایت اشاره گر می باشد. این فیلد اشاره کننده به محلی است که باید نود دریافت کننده این گزینه، آدرس IP خود را درآن محل قرار دهد. کوچکترین مقدار اشاره گر ۴ است . اگر مقدار اشاره گر بزرگتر از فیلد طول گزینه باشد، محل خالی در فیلد ثبت داده وجودندارد. به عبارت دیگرفیلد ثبت داده پر شده است. اگر لیست ثبت داده پر باشد، مسیریاب بدون این که آدرس IP خودش را در لیست درج کند بسته را پیش می برد.



شکل(۸-۱۶):ساختار گزینه ثبت مسیر

اگر اشاره گر بزرگتر ازطول گزینه نباشد، لیست ثبت داده پر نیست و محل های خالی دردسترس می باشد. مسیریاب، آدرس IP خود را در مکانی که توسط فیلد اشاره گر مشخص می شود، درج نموده و مقدار فیلد اشاره گر را ۴ واحد که اندازه آدرس IP است افزایش می دهد. آدرس ثبت شده، آدرس IP واسط شبکه مسیریابی است که از طریق آن باید این بسته پیش برده شود. هم فرستنده و هم گیرنده باید با استفاده و پردازش اطلاعات ثبت مسیرموافق باشند. فرستنده، گزینه ثبت مسیر و فضای کافی برای ثبت آدرس های IP مسیریاب های میانی را به بسته IP اضافه می کند. گیرنده با پردازش لیست آدرس های IP ثبت شده در فیلد ثبت داده، اطلاعات مفیدی از مسیریاب های موجود درشبکه بدست می آورد. اگر گیرنده با پردازش داده های ثبت مسیر موافق نباشد، این اطلاعات توسط گیرنده نادیده گرفته می شود.

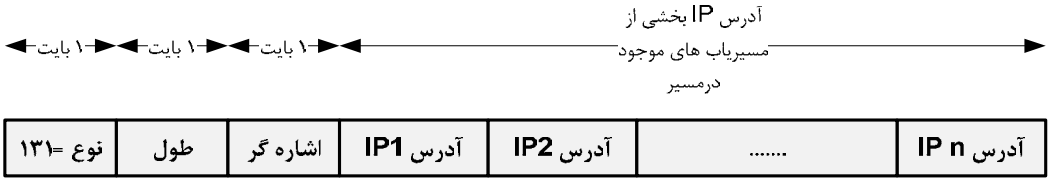
درشبکه های IP دونوع متفاوت از مسیریابی وجود دارد. مسیریابی پرش به پرش و مسیریابی مبداء. درمسیریابی پرش به پرش، درهر نود عملیات مسیریابی انجام شده و بهترین پرش بعدی برای تحویل بسته به مقصد تعیین می شود. سپس بسته برای رسیدن به مقصد نهایی، تحویل پرش بعدی می شود. این عملیات درهمه پرش های بعدی انجام می شود تانهایتا بسته به مقصد برسد. درمسیریابی مبدا، فرستنده کل مسیر یا بخشی از مسیری که باید بسته آن را طی نموده تا به مقصد برسد را تعیین می کند. به عبارت دیگردر مسیریابی مبدا ، فرستنده مسیری راکه بسته بایددر رسیدن به مقصد دنبال کند دیکته می کند.

برای آزمایش یک مسیر خاص هنگامی که میدانیم مسیریاب ها معمولا آن مسیر را انتخاب نمی کنند، استفاده از گزینه مسیریابی مبدا بسیارمفید می باشد. همچنین این گزینه این انعطاف پذیری را ارائه می کند که بسته ها را از طریق شبکه هایی با اطمینان بالا مسیریابی نماییم. توپولوژی و مسیر واقعی که یک بسته IP دریک شبکه پیچیده باید دنبال کند، ممکن است به سادگی مشخص نشود و این مسئله یکی از نقاط ضعف این روش می باشد. دو نوع مسیریابی مبدا وجود دارد که عبارتند از مسیریابی مبدا دقیق و مسیریابی مبدا ضعیف.

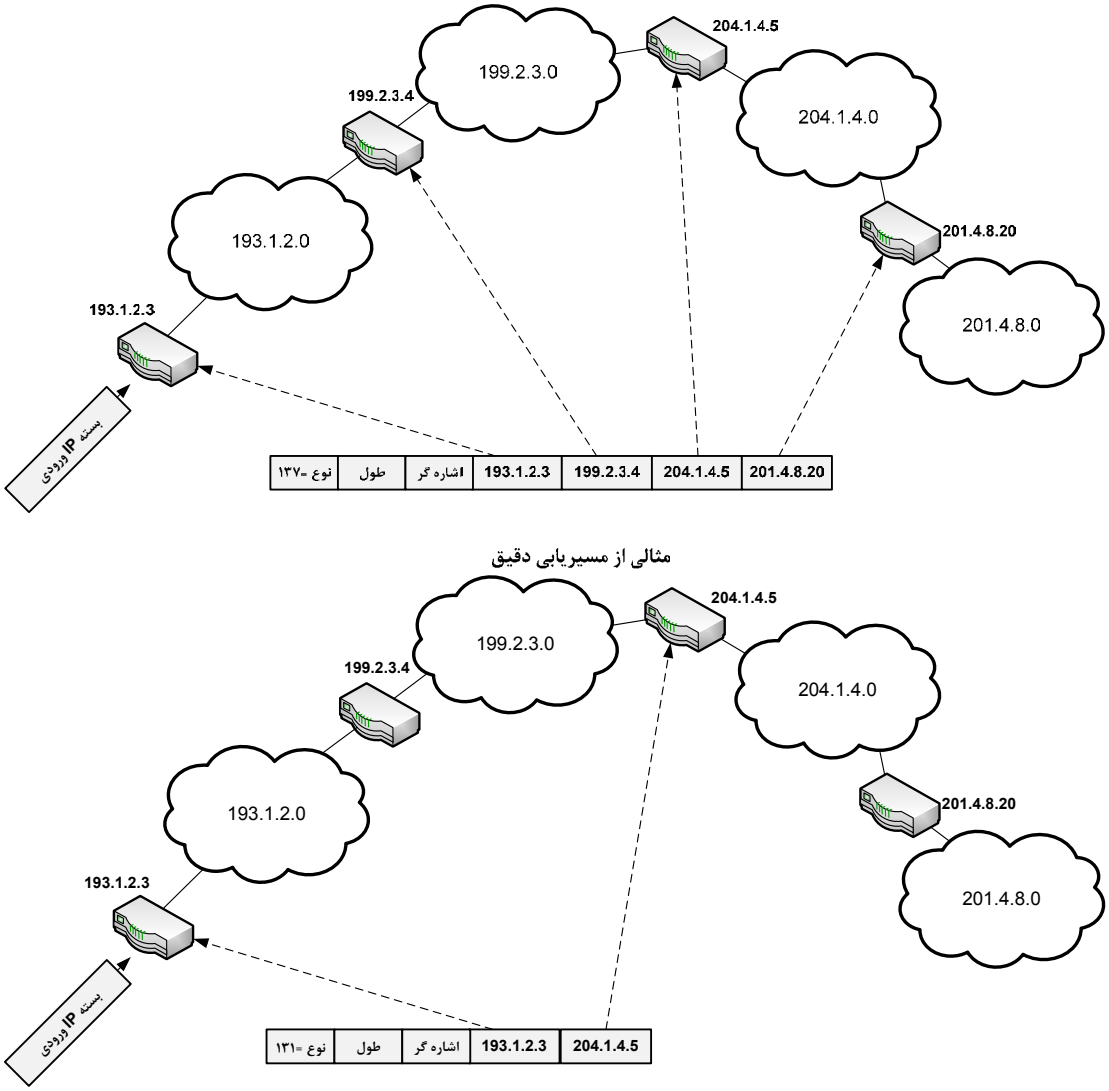
در گزینه مسیریابی مبدا دقیق که درشکل (۸-۱۷) نشان داده شده است، فرستنده رشته ای از آدرس های IP نودهایی را که باید دقیقا در پیش بردن بسته از آنها استفاده شود، را همراه بسته ارسال می نماید. مسیر بین دو آدرسIP متوالی موجود در لیست مسیریابی مبدا، فقط می تواندشامل یک شبکه فیزیکی خاص باشد و امکان وجود نودهای میانی بین آنها وجود ندارد. اگر مسیر یاب های میانی نتوانند مسیرتعیین شده توسط این گزینه را دقیقا دنبال کنند، بسته حذف می شود.

شکل(۸-۱۷): ساختارمسیریابی مبدا دقیق

مطابق با شکل (۸-۱۸)، در مسیریابی مبدا ضعیف، فرستنده رشته ای از آدرس های IP نودهایی را که باید در پیش بردن یک بسته دنبال شوند، درپیام ارسالی اضافه می نماید. برخلاف مسیریابی مبدا دقیق، درمسیریابی مبدا ضعیف، ممکن است مسیر بین دو آدرس IP متوالی شامل هر تعداد مسیریاب باشد. شکل (۸-۱۹) مقایسه بین مسیریابی مبدا دقیق و ضعیف را نشان می دهد.



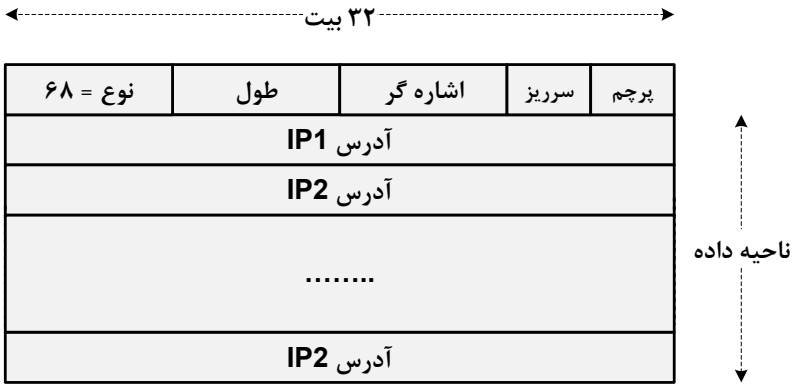
شکل (۸-۱۸): ساختار مسیریابی مبدا ضعیف



شکل (۸-۱۹): مقایسه مسیریابی مبدا دقیق ومسیریابی مبدا ضعیف

۸-۳-۳-۴- برچسب زمانی اینترنت

از این گزینه برای ثبت زمان دریافت هر بسته IP درمسیریاب های درون شبکه استفاده می شود. چنانچه بخواهیم که زمان دریافت هربسته و همچنین آدرس مسیریاب هایی که بسته IP را دریافت می کنندرا داشته باشیم، از این گزینه استفاده می کنیم. برچسب های زمانی برحسب تعداد میلی ثانیه های گذشته از نیمه شب طبق ساعت UTC اندازه گیری می شود. UTC سابقاً GMT نامیده می شد و زمان صفر درجه طولی است. شکل(۸-۲۰) قالب گزینه بر چسب زمانی اینترنت را نشان میدهد.



شکل (۸-۲۰): ساختارگزینه بر چسب زمانی اینترنت

درگزینه برچسب زمانی اینترنت، فیلد نوع گزینه ۶۸ است. فیلد طول گزینه، تعداد کل بایت های موجود درگزینه رانشان می دهد. هر ورودی در فیلد داده گزینه، شامل دو مقدار ۳۲ بیتی آدرسIP مسیریاب و بر چسب زمانی، می باشد. بایت طول، مقدار فضای رزرو شده برای آدرس های IP و برچسب های زمانی را در فیلد داده مشخص می کند. فیلد اشاره گر، محل خالی بعدی برای قراردادن مقدار آدرس IP و برچسب زمانی نود فعلی می باشد. کمترین مقدار فیلد اشاره گر ۵ است . هنگامی که مقدار اشاره گر بزرگتر از مقدار فیلد طول است، ناحیه برچسب زمانی پر شده است. فیلد سرریز۴ بیت طول دارد ونشان دهنده تعداد مسیریاب هایی است که به دلیل کوچکی زیاد فیلد داده، نمی توانند برچسب زمانی را درناحیه مربوطه قرار دهند. حداکثر مقدار فیلد سرریز ۱۵ است. اگر فضای کافی برای درج یک برچسب زمانی کامل در ناحیه داده وجود نداشته باشد ویا شماره سرریز از ۱۵ تجاوز کند، بسته IP اشتباه در نظر گرفته شده و حذف می شود. دراینصورت یک پیام ICMP از نوع خطا درپارامتر، به فرستنده ارسال می شود. فیلد پرچم، قالب اطلاعات در فیلد داده را کنترل می کند.

۸-۴- پروتکل ICMP[1]

همانطور که درقبل اشاره شد، پروتکل اینترت از نوع بدون اتصال و بدون گارانتی می باشد. بنابراین پروتکلIP سعی نمی کند تا تحویل مطمئن بسته ها را ضمانت کند بلکه این کاررا به پروتکل های لایه بالا مانند پروتکل TCP واگذار می نماید. بااین وجود، IP امکاناتی را برای ارسال پیام های هشدار و تشخیص عیب از طریق پروتکل ICMP فراهم می سازد. مدیر شبکه می تواند از این پیام ها در تشخیص مشکلات احتمالی شبکه استفاده کند. پروتکل ICMP توسط چندین RFC اینترنت توصیف شده است. این RFC ها عبارتند از: RFC 1256, RFC792, RFC950, RFC 1812, RFC 1122 و RFC 1191.

به دلیل بدون اتصال و بدون تضمین بودن پروتکل IP، احتمال اینکه بسته های IP با خطا مواجه شوند زیاداست.

[1] Internet Control Message Protocol

درشبکه های IP، فرستنده بسته های IP را ارسال نموده وآنها را به زیرلایه های شبکه زیرین تحویل می دهد. فرستنده راهی برای دانستن مشکلات احتمالی که ممکن است در ارسال بسته رخ بدهد ندارد. معمولا خطاها و مشکلات احتمالی موجود دربسته های IP درمسیریاب های میانی کشف و گزارش می شود. برخی از مشکلاتی که ممکن است درهنگام ارسال بسته های IP با آنها مواجه شویم عبارتند از:

- اتمام پارامتر زمان زندگی (TTL) در بسته به خاطر وجود حلقه مسیریابی درشبکه.
- عدم تحویل بسته به خاطر فقدان یک تکه از بسته .
- در دسترس نبودن یک پروتکل ، سرویس یا میزبان خاص درمقصد.
- عدم توانایی پیش بردن یک بسته به خاطر عدم اجازه تکه سازی.
- وقوع ازدحام در یک مسیریاب شبکه.

در هر یک از این موارد، ازپروتکل ICMP برای هشدار دادن به فرستنده درباره مشکلات بوجود آمده فوق استفاده می شود. خود پروتکل IP هیچ مکانیزمی برای هشدار دادن به شبکه درباره این مشکلات ندارد، بلکه این پروتکل کمکی ICMP است که این کاررا انجام می دهد. همه پیاده سازی های IP نیازمند به پشتیبانی ICMP هستند. بعضی از پیاده سازی های ICMP هنگام مواجهه با یک مشکل خاص پیامی ارسال نکرده درحالیکه برخی دیگر این کاررا انجام می دهند. بنابراین درسطوح مختلفی از پیاده سازی پروتکل ICMP درنودهای شبکه وجود دارد.

هم مسیریاب های میانی شبکه و هم میزبان های IP قادر به تولید وارسال پیام های ICMP می باشند. مسیریاب های شبکه درهنگام مواجه با مشکلاتی که باعث عدم توانایی آنها درپیش بردن بسته های دریافتی شود، اقدام به ارسال پیام های ICMP می نمایند. درحالیکه میزبان های شبکه، چنانچه با مشکلاتی نظیرعدم امکان تحویل بسته به پروتکل های لایه بالاتر مواجه شوند، بسته های ICMP ارسال می دارند. الزاما تمام بسته های ICMP برای گزارش مشکلات احتمالی درشبکه و یا میزبان های مقصد استفاده نمی شوند. برخی از پیام های ICMP برای عملیات خاص نظیر تست و جمع آوری اطلاعات از شبکه به کار می روند. بعضی از جنبه های مهم ICMP که باید از آن آگاه باشیم به شرح زیر است:

- همه پیاده سازی های IP نیز باید ICMP را پیاده سازی کنند.
- ICMP در بالای IP اجرا می شود، یعنی ICMP یک سرویس گیرنده IP است حتی با این که ICMP در ماژول IP پیاده سازی می شود.
- ICMP در هنگام تشخیص خطا به کاررفته و این بدین معنی نیست که قابلیت اطمینان پروتکل IP را افزایش داده است.
- ICMP فقط در مورد اولین تکه بسته IP گزارش خطا را صادر می نماید. این تکه، تکه ای از بسته IP است که آفست تکه سازی آن ۰است. مقصود از این کار پرهیز از ارسال پیام های ICMP برای هر یک از تکه های باقیمانده بسته است.
- ICMP یک مکانیزم گزارش خطا برای بسته های IP است. ICMP پیام های خطا در مورد مشکلات بسته های خودش تولید نمی کند. به عبارت دیگر پیام های ICMP برای اعلام وقوع خطا برای خودشان استفاده نمی شوند.

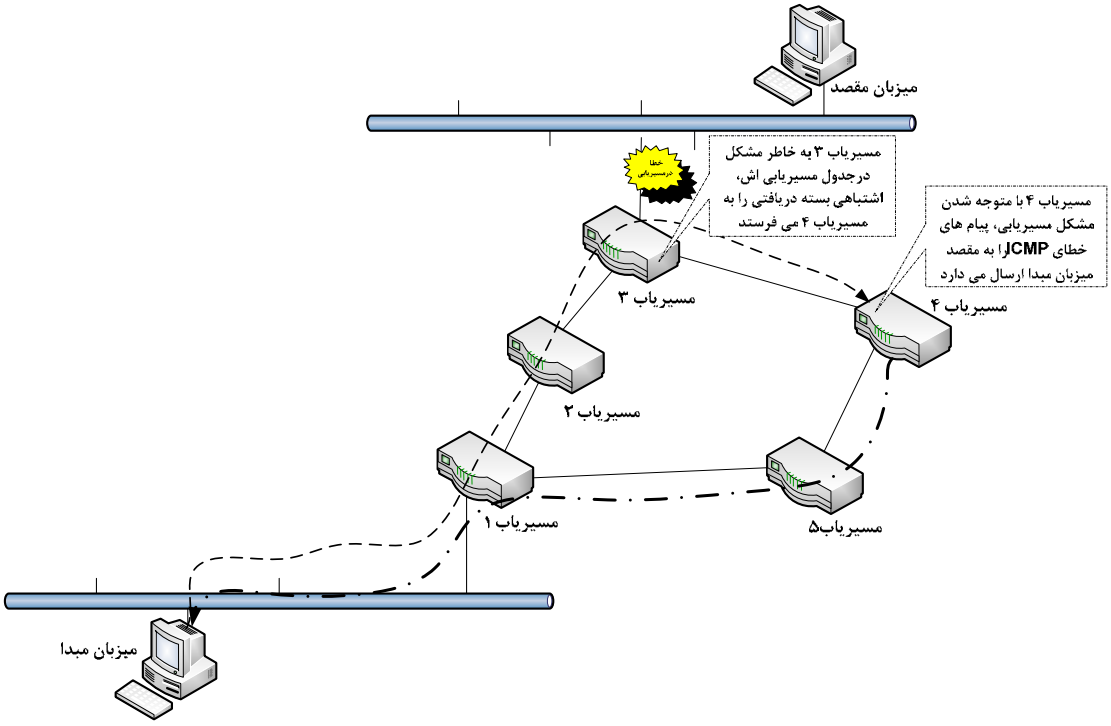
علاوه بر موارد فوق، پروتکلICMP نباید در مورد مشکلات ایجاد شده ذیل پیامی ارسال دارد:

- مسیریابی یا تحویل پیام های ICMP: اگر پیام های خطای ICMP در مورد پروتکلICMP تولید شوند، پیام ها به شدت زیاد شده و به ترافیک شبکه اضافه می شود.
- همه پخشی یا چند پخشی بسته های IP: اگر پیام های خطای ICMP برای بسته های همه پخشی یا چند پخشی IP تولید شوند، هر نود دریافت کننده بسته همه پخشی/ چند پخشی یک پیام ICMP را تولید می کندکه این مسئله باعث افزایش ناگهانی ترافیک شبکه می شود.

- همه پخشی یا چند پخشی لایه پیوند داده: اگر پیام های خطای ICMP برای بسته های همه پخشی یا چند پخشی لایه پیونداده تولید شوند، هر نود دریافت کننده پیام های همه پخشی/ چند پخشی یک پیام ICMP را تولید می کند و به ترافیک شبکه اضافه می شود.
- بسته هایی با آدرس مبدائی که یک نود IP یکتا را مشخص نمی کنند: برای بسته هایی که آدرس مبدا آنها آدرس های برگشت حلقه 127.x.x.x یا 0.0.0.0 یا آدرسی با پیشوند شبکه ۰ باشد، بسته های ICMP تولید نمی شود.

۸-۴-۱- تشخیص خطای ICMP

همان طور که در بخش پیش اشاره شد، ICMP یک مکانیزم گزارش خطا برای بسته های IP فراهم می آورد. پیام های خطای ICMP به مقصد فرستنده بستهIP ارسال می شوند.گیرنده بسته ICMP باید اقدام به عمل مقتضی برای رفع مشکل بوجود آمده نماید. به عنوان مثال شرایط شکل(۸-۲۱) را در نظر بگیرید که بسته ای ازمیزبان مبدا به میزبان مقصد فرستاده شده است و مسیری شامل مسیریاب های ۱،۲ و۳ را طی می کند.

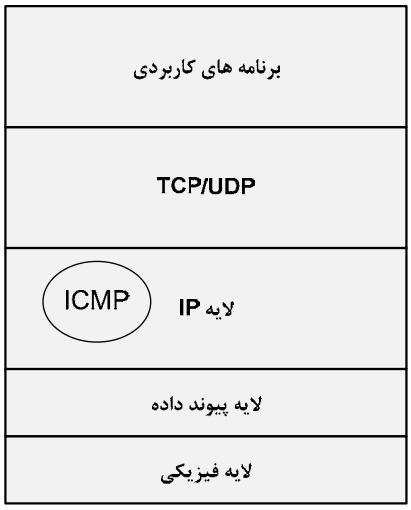


شکل (۸-۲۱): مثالی از کاربردپیام ICMP

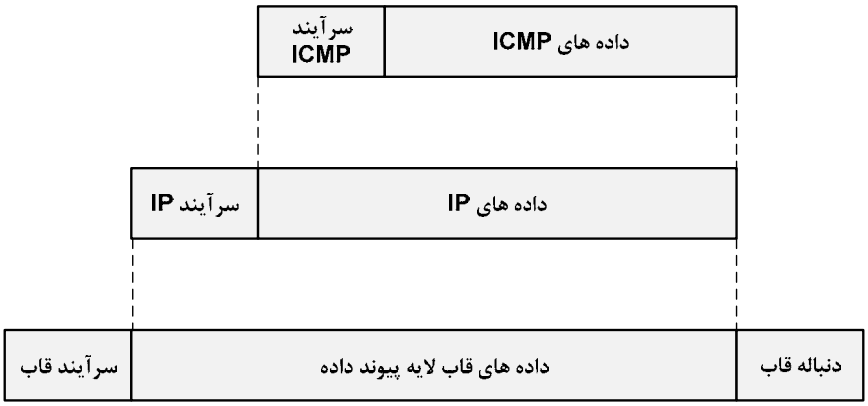
فرض کنید مسیریاب ۳ اطلاعات نادرستی درباره مقصد در جدول مسیریابی خود دارد و اشتباها به جای میزبان مقصد، بسته را به مسیر یاب ۴ ارسال می کند. مسیریاب ۴که متوجه وقوع خطا درشبکه شده است، یک پیام ICMP درباره مسیریابی نادرست به فرستنده پیام می فرستد. با توجه به اینکه پیام های ICMP فقط به مبدا تولید کننده بسته IP ارسال می شوند، بنابراین مسیریاب ۴ نمی تواند پیامی را به مسیریاب۳ درباره دلیل مشکل فوق ارسال دارد. دراین مثال، میزبان مبدا هیچ نقشی درخطای بوجود آمده نداشته است وبنابراین کاری برای رفع مشکل فوق نمی تواند انجام دهد. بنابراین سوالی که مطرح می شود این است که چرا ICMP محدود به ارسال پیام ها به مبدا اصلی است؟جواب این است که سرآیند بسته هایIP فقط دو فیلد آدرس شامل آدرسIP مبدا اصلی و آدرس IP مقصد نهایی را دارد. از آنجاییکه آدرس های IP مسیر یاب های میانی در فیلد سرآیند IP ثبت نمی شوند (مگر این که امکان ثبت مسیر IP توسط مبدا اصلی

فعال شده باشد) بنابراین بسته های ICMP فقط باید برای مبدااصلی ارسال می گردند. بنابراین درمثال فوق هنگامی که مسیریاب ۴ می خواهد پیام ICMP را ارسال کند، فقط از آدرس های IP مبدا آغازین و مقصد نهایی آگاهی دارد و از مسیریاب های میانی که بسته را پردازش نموده اند اطلاعی ندارد. بنابراین نمی تواند پیام ICMP را به آنها بفرستد. با توجه به شرایط پیش آمده دراین مثال، منطقی نیست که مسیریاب R4 بسته ICMP را به مقصد اصلی بفرستد چون به احتمال زیاد بسته اصلی مشکلی درون شبکه برای رسیدن به مقصد داشته است. همچنین مقصد اصلی درایجاد مشکل فوق نقشی نداشته است و دلیل مشکل اخیرنیست بلکه دلیل مشکل مبدأ یا یکی از مسیریاب های میانی است. بنابراین ارسال پیام ICMP به مبدا تنها انتخاب منطقی است. به هرحال ارسال پیام ICMP به مبدا از اصلا نفرستادن هیچ پیامی بهتر است.

ازآنجاییکه پیام های ICMP باید در اینترنت توسط مسیریاب ها حمل شوند، باید این پیام ها راتوسط پروتکلIP بسته بندی نمود. به این معنی که پیام ICMP در بخش داده بسته IP گنجانده می شود. ماژول IP دریافت کننده داده، بسته IP را براساس مقدار فیلد پروتکل غیرتسهیم سازی نموده وآن را به ماژول ICMP می فرستد. شکل (۸-۲۲) لایه بندی پروتکل ICMP و IP را نشان می دهد . همچنین نشان می دهد که ماژول ICMP به عنوان قسمتی از ماژول IP پیاده سازی شده است. شکل(۸-۲۳) بسته بندی ICMP را داخل یک سرآیند IP نشان می دهد.



شکل(۸-۲۲): ارتباط ICMP و IP



شکل (۸-۲۳): بسته بندی ICMP

باتوجه به شکل (۸-۲۲) می توان فهمید که حتی با اینکه پیام ICMP توسط IP بسته بندی شده است، ICMP به عنوان یک پروتکل لایه بالا در نظر گرفته نمی شود بلکه یک بخش مورد نیازپروتکل IP است. از پروتکل ICMP می توان برای ساخت کاربردهایی با مقصود خاص و ابزارهای تشخیصی استفاده نمود. این کاربرد های خاص را می توان به عنوان بخشی از لایه کاربرد در نظر گرفت . امکان PING، مثال خوبی از ابزارهای تشخیصی که ازپروتکل ICMP استفاده می کنند، می باشد. این قابلیت در بسیاری از سیستم های TCP/IP در دسترس می باشد. امکان PING برای ارسال یک پیام درخواست echo به یک مقصد خاص استفاده می شود. اگر پیام درخواست echo به یک ماژول IP برسد، آن ماژول مجبور به ارسال یک پیام پاسخ echo است. با دریافت پیام پاسخ echo ، فرستنده پیام متوجه می شود که نود IP دوردردسترس است.

سرآیند IP هیچ اولویت خاصی را برای تحویل پیام های ICMP مشخص نکرده است، بنابراین نود های IP با بسته های IP که دربرگیرنده پیام های ICMP هستند، با یک حالت عادی مانند هر بسته دیگری رفتار می کنند. چون IP تحویل پیام ها را ضمانت نمی کند، ممکن است پیام های ICMP گم شده ویا به خاطر ازدحام درمسیریاب های میانی حذف شوند. اگردرپردازش بسته های IP که شامل پیام های ICMP هستند با خطا مواجه شویم، هیچ پیام ICMP تولید نمی شود.

۸-۴-۲- سرویس های ICMP

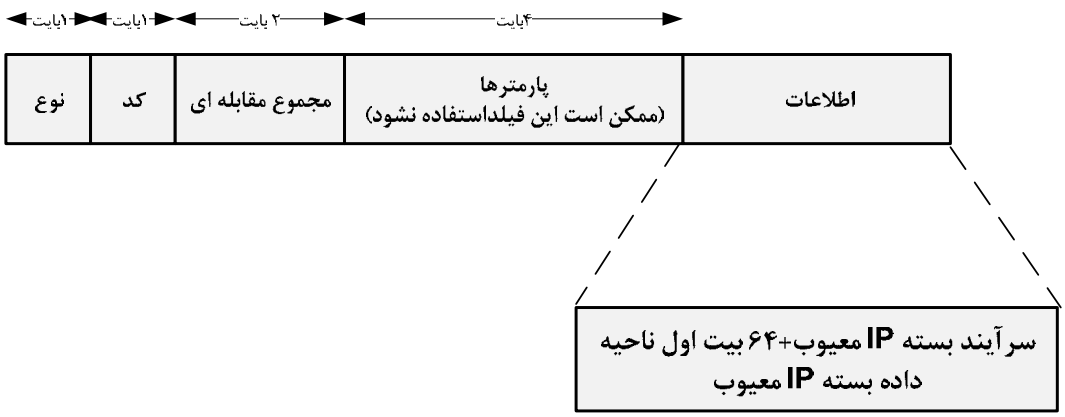
پروتکل ICMP سرویس های متنوع زیر را تامین می نماید:

- echo : به عنوان یک تشخیص برای تعیین کردن دسترس پذیری به یک نود IP بکار می رود.
- غیرقابل دسترس بودن مقصد : برای اعلام غیر قابل دسترس بودن نود IP مقصد به کار می رود.
- فرو نشاندن مبدا[1] : برای نشان دادن مشکل ازدحام درشبکه و درخواست از مبدا برای کاهش سرعت ارسال به کار می رود.
- تغییرمسیر[2]: بوسیله مسیر یاب های میانی شبکه برای آگاهی دادن از وجود یک مسیر جایگزین استفاده می شود.
- تخطی زمانی[3]: برای اعلام صفرشدن مقدار فیلد TTL سرآیند IP به کار می رود.
- مشکل پارامتر[4] : برای نشان دادن یک مشکل دریکی از پارامترهای بسته IP به کار می رود.
- برچسب زمانی[5]: برای اندازه گیری زمان در اینترنت استفاده میشود .
- پوشش آدرس[6] : برای به دست آوردن اطلاعات پوشش زیر شبکه استفاده می شود.

۸-۴-۳- ساختار پیام های ICMP

ساختار پیام های ICMP درشکل (۸-۲۴) نشان داده شده اند. اولین بایت در سرآیند ICMP فیلد نوع می باشدکه نشان دهنده نوع سرویس ICMP است. بایت بعدی فیلد کد است که بیشتر طبیعت نوع پیام را توصیف می کند. هم مقدار فیلد نوع و هم مقدار فیلد کد باید برای تعیین نوع پیام ICMP ارسالی در نظر گرفته می شوند.

[1] source quench
[2] redirect
[3] time exceeded
[4] parameter problem
[5] time stamp
[6] address mask



شکل (۸-۲۴): ساختار کلی پیام ICMP

جدول(۸-۸) مقادیر مختلف فیلد نوع ICMP را نشان می دهد. همچنین جدول(۸-۱۰) مقدار کد انتساب داده شده متعلق به نوع را نشان می دهد . بعضی از مقادیر نوع به پروتکل های آزمایشی انتساب داده شده اند و مقدار کد آنها لیست نشده است.

جدول(۸-۸): مقادیر نوع ICMP

مقدارفیلد نوع	توصیف
۰	پاسخ Echo
۱،۲،۷و۳۷-۲۵۵	انتساب داده نشده است
۲	انتساب داده نشده
۳	مقصد غیر قابل دسترس است
۴	فرو نشاندن مبدا
۵	تغییر مسیر
۶	آدرس میزبان جایگزین
۸	درخواست Echo
۹	اعلان مسیریاب
۱۰	انتخاب مسیریاب
۱۱	تخطی از زمان
۱۲	مشکل پارامتر
۱۳	درخواست برچسب زمانی
۱۴	پاسخ برچسب زمانی
۱۵	درخواست اطلاعات
۱۶	پاسخ اطلاعات
۱۷	درخواست پوشش آدرس
۱۸	پاسخ پوشش آدرس
۱۹	رزرو شده برای کاربردهای امنیتی
۲۰-۲۹	رزرو شده برای کاربردهای آزمایشی
۳۰	ردیابی مسیر
۳۱	خطای ازدحام بسته
۳۲	تغییر مسیرمیزبان قابل حمل
۳۳	IPV6 Where- Are- You
۳۴	IPV6 I- Am – Here
۳۵	درخواست ثبت قابل حمل
۳۶	پاسخ ثبت قابل حمل

جدول (۸-۱۰): فیلدهای کد ICMP

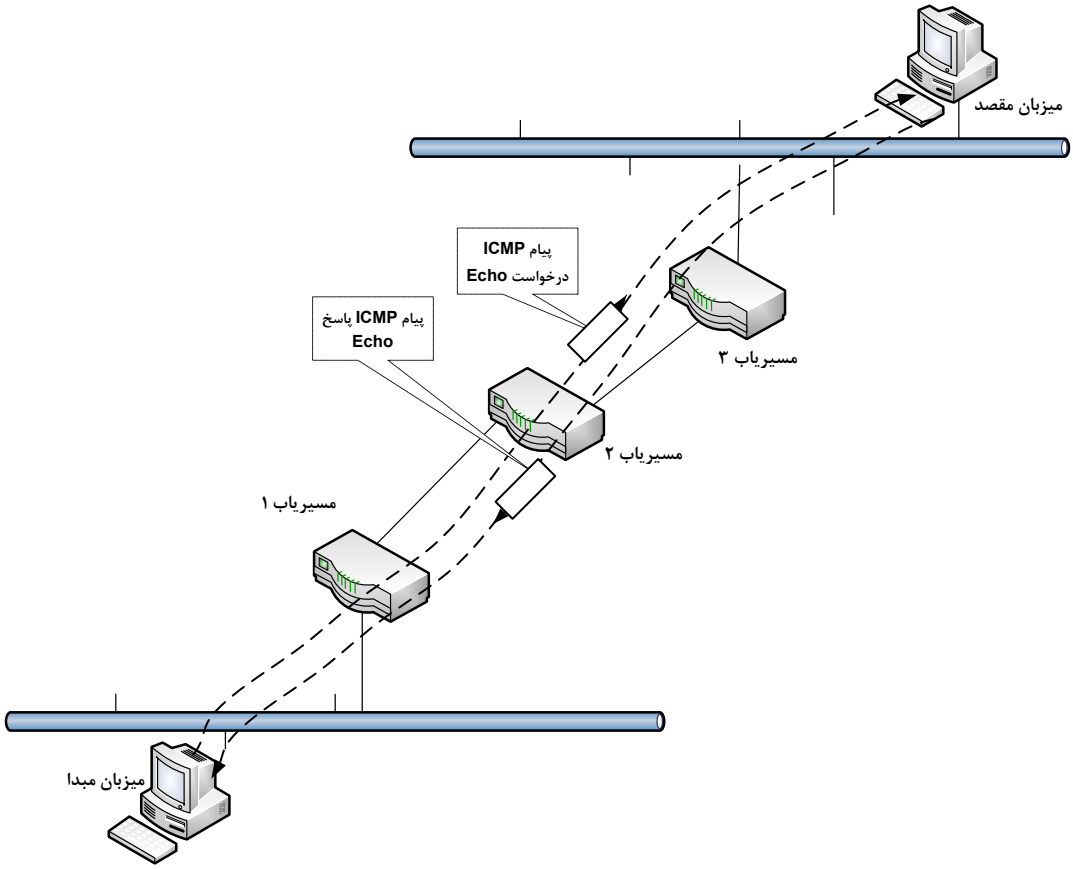
نوع	کدها	توصیف
۰(پاسخ echo)	-	کد ندارد
۲۵۵-۱،۲،۷،۳۷	-	انتساب داده نشده است
۳ (غیرقابل دسترس بودن مقصد)	۰	شبکه غیر قابل دسترس است
	۱	میزبان غیر قابل دسترس است
	۲	پروتکل غیر قابل دسترس است
	۳	درگاه غیر قابل دسترس است
	۴	تکه سازی مورد نیاز است ولی پرچم DF ۱ است
	۵	مسیریابی مبدا ناموفق
	۶	شبکه مقصد ناشناخته است
	۷	میزبان مقصد ناشناخته است
	۸	میزبان مبدا جدا شده است
	۹	ارتباط با شبکه مقصد از جانب مدیریت ممنوع شده است
	۱۰	ارتباط با میزبان مقصد از جانب مدیریت ممنوع شده است
	۱۱	شبکه مقصد برای نوع سرویس درخواستی غیر قابل دسترس است
	۱۲	میزبان مقصد برای نوع سرویس درخواستی غیر قابل دسترس است
۴ (فرو نشاندن مبدا)	-	کد ندارد
۵ (تغییر مسیر)	۰	تغییر مسیر بسته به خاطر شبکه (یا زیر شبکه)
	۱	تغییرمسیر بسته به خاطر میزبان
	۲	تغییر مسیر بسته به خاطر نوع سرویس و شبکه
	۳	تغییر مسیر بسته به خاطر نوع سرویس و میزبان
۶ (آدرس جایگزین میزبان)	۰	آدرس جایگزین برای میزبان
۸ (پاسخ Echo)	-	کد ندارد
۹(اعلان مسیریابی)	-	کد ندارد
۱۰(انتخاب مسیریاب)	-	کد ندارد
۱۱(تخطی از زمان)	۰	زمان زندگی بسته برای عبور از شبکه اتمام یافته است
	۱	زمان بازسازی تکه های بسته IP درمقصد اتمام یافته است
۱۲(مشکل پارامتر)	۰	اشاره گر خطا را نشان می دهد
	۱	گم شدن یک امکان مورد نیاز
	۲	طول بد
۱۳(برچسب زمانی)	-	کد ندارد
۱۴(پاسخ برچسب زمانی)	-	کد ندارد
۱۵(درخواست اطلاعا ت)	-	کد ندارد
۱۶(پاسخ اطلاعات)	-	کد ندارد
۱۷(درخواست پوشش آدرس)	-	کد ندارد
۱۸(پاسخ پوشش آدرس)	-	کد ندارد

دو بایت بعدی فیلد مجموع مقابله است که برای بررسی خطا دربسته ICMP به کار می رود. فیلد بررسی خطای فوق فقط شامل پیام ICMP بوده و سرآیند بستهIP را دربرنمی گیرد. الگوریتم بررسی خطا همان الگوریتم بررسی خطا یی است که برای پروتکل IP استفاده می شود. ۴ بایت بعدی شامل پارامتر های اختیاری است. پارامترهای واقعی مورد استفاده به پیام

ICMP بستگی دارد. این فیلد اختیاری است و ممکن است بعضی از انواع پیام های ICMP آن را در برنداشته باشند. فیلد اطلاعات، شامل سرآیند IP بسته معیوب به علاوه ۶۴ بیت از داده پروتکل لایه بالا موجود در بخش داده بسته IP معیوب می باشد. اطلاعات فوق برای مبدا ارسال کننده پیام بسیار مفید است و به کمک آن می تواند دلیل و نوع مشکل بوجود آمده را بفهمد. دلیل گنجاندن سرآیند بسته IP معیوب درپیام های ICMP این است که بتوان آدرسIP مقصد ومبدا فرستنده بسته را تعیین کرد. این آدرس ها بیان می کنند که بسته را کی و به کجا فرستاده است ؟۶۴ بیت داده لایه بالا شامل قسمتی از سرآیند TCP یا همه سرآیند UDP می باشد. ۸ بایت اول سرآیند TCP شامل شماره درگاه های مقصد و مبدا و فیلد شماره ترتیب هستند. همانطور که درفصل های بعدی اشاره خواهد شد، شماره های درگاه نوع برنامه های کاربردی لایه بالا را مشخص می نمایند. از طرف دیگر اگر UDP به عنوان پروتکل لایه انتقال استفاده شود چون اندازه سرآیند UDP فقط ۸ بایت است، همه سرآیند UDP گزارش می شود. درادامه به توصیف برخی از مهمترین پیام های ICMP می پردازیم.

۸-۴-۳-۱- پیام ICMP Echo

یکی از پراستفاده ترین پیام های ICMP، پیام فوق echo می باشد. ابزار PING که در اغلب سیستم های TCP/IP در دسترس است برای مقاصد تشخیصی خود از پیام فوق استفاده می کند. با استفاده از امکان PING قابل دسترس بودن یک نود IP خاص بررسی می شود؟ با کمک امکان PING یک پیام درخواست ICMP Echo با مقدار فیلد نوع برابر با ۸ به یک نود IP خاص ارسال می شود. نود IP با دریافت این پیام، یک پیام پاسخ ICMP Echo با فیلد نوع برابر با ۰ را به فرستنده ارسال می دارد. درپیام پاسخ Echo، یک کپی از داده های فرستاده شده در پیام درخواست Echo موجود می باشد. با دریافت موفق پیام پاسخ Echo مشخص می شود که لایه IP ولایه های پائین ترآن در سیستم انتقال بین مبدا و مقصد درست کار می کنند. اگر بین مبدا و مقصد هر تعداد مسیریاب میانی وجود داشته باشد، با دریافت پیام پاسخ Echo مشخص می شود که مسیریاب های فوق قادر به مسیریابی بین مبدا و مقصد هستند. نود IP ای با کمک امکان PING دردسترس بودن آن بررسی می شود، یک میزبان یا یک مسیریاب می باشد. شکل (۸-۲۵) مثالی از چگونگی عملکرد PING را نشان می دهد.



شکل(۸-۲۵): استفاده از پیام های درخواست / پاسخ ICMP Echo

۸-۴-۳-۲-پیام ICMP در دسترس نبودن مقصد

همانطور که قبلا گفته شد، شبکه IP یک سرویس بهترین تلاش را فراهم می کند. این امکان وجود دارد که پروتکل IP قادر به تحویل بسته IP به مقصد نباشد. عدم تحویل بسته ها، معمولا به وسیله مسیریاب های شبکه شناسایی می شود. هنگامی که یک مسیریاب قادر به تحویل بسته به مقصد نباشد، یک پیام ICMP دردسترس نبودن مقصد را به فرستنده ارسال می دارد. پیام ICMP ارسالی فوق، فرستنده را از دلیل تحویل ناموفق آگاه کند. دراین پیام، مقدار فیلد نوع ۳ است که نشان می دهد این یک پیام ICMP ازنوع در دسترس نبودن مقصد است. فیلد کد، اطلاعات بیشتری را در مورد این که چرا مقصد در دسترس نیست می دهد. مقادیر فیلد کد در جدول (۸-۱۰) لیست شده بودند. درادامه به بررسی مفهوم هریک از مقادیر فیلد کد آورده شده درجدول فوق می پردازیم.

هنگامی که شبکه مشخص شده در آدرس مقصد IP قابل دسترس نباشد، مقدار کد۰ (شبکه در دسترس نیست) استفاده می شود. این پیام خطا فقط توسط مسیریاب ها تولید می شود. دلیل وقوع خطای فوق، ناشی از یک اشتباه در مشخص کردن آدرس IP مقصد و یا یک اشتباه در جدول مسیریابی مسیریاب تولید کننده پیام ICMP می باشد. آدرس مبدا موجود در سرآیند IP حمل کننده این پیام ICMP، مسیریابی راکه این خطا را تولید کرده است مشخص می کند.

مقدار کد ۱ (میزبان در دسترس نیست) به وسیله مسیریابی تولید می شود که مستقیما به شبکه مقصد متصل است. این کد نشان دهنده این است که بسته با موفقیت توسط مسیریاب ها تحویل داده شده است اما مسیریاب آخر قادر به ارتباط با میزبان مشخص شده نمی باشد. این امر به این دلیل می تواند باشد که تلاش پروتکلARP انجام شده توسط مسیریاب برای پیدا کردن آدرس سخت افزاری مقصد موفقیت آمیز نبوده است. همچنین این احتمال وجود دارد که میزبان مقصد به دلیل از کار افتادگی، پیکره بندی اشتباه یا تعیین آدرس IP نادرست در دسترس نباشد. باید توجه نمود که پیام خطای

ICMP در دسترس نبودن مقصد بر نقص تحویل دلالت می کند حال آن که پیام خطای ICMP در دسترس نبودن شبکه نشان دهنده نقص مسیریابی است.

مقدار کد ۲ (در دسترس نبودن پروتکل) به وسیله میزبان مقصد تولید می شود . این پیام دلالت براین دارد که بسته به میزبان مقصد رسیده است اما پروتکل بالایی نظیر TCP ، UDP و OSPF که IP باید محتویات بسته خود را به آن تحویل دهد، در دسترس نیست.

مقدار کد ۳ (در دسترس نبودن درگاه) هنگامی تولید می شود که پروتکل لایه حمل (UDP یا TCP) قادر به غیرتسهیم سازی بسته و تشخیص برنامه کاربردی لایه بالاتر نباشد. درمواردی ممکن است پروتکل لایه حمل به خاطر عدم حضور یک سرویس کاربردی خاص در میزبان مقصد قادر به غیرتسهیم سازی بسته نباشد. سرویس های کاربردی به وسیله شماره های درگاه UDP و TCP مشخص می شوند.

مقدار کد ۴ (تکه سازی نیاز است ولی پرچم DF ۱ است) توسط مسیریاب های میانی شبکه تولید می شود. هنگامی که به خاطر اندازه MTU شبکه، نیاز به تکه سازی بسته IP باشد ولی پرچم DF موجود درسرآیند بسته IP مقدار ۱ داشته باشد، مسیریاب نمی تواند بسته را تکه سازی کند واز طرفی نمی تواند بسته را پیش ببرد و بنابراین باید آن را حذف نموده ویک پیام ICMP ارسال دارد.

مقدار کد ۵ (مسیریابی مبدا ناموفق) توسط یک مسیریاب تولید می شود. این پیام برای بسته های IP که از امکان مسیریابی مبدا IP استفاده می کنند، تولید میشود. با کمک امکان مسیریابی مبدا IP ، می توان مسیر کامل وآدرس های مسیریاب هایی را که باید برای پیش بردن بسته استفاده شوند ، مشخص نمود. اگر یک مسیریاب، نتواند بسته را براساس مسیر تعیین شده پیش ببرد، باید بسته را حذف کند. دراین حالت مسیریاب یک پیام نوع ۳ ICMP با کد ۵ به فرستنده می فرستد و بدین وسیله ناموفق بودن مسیریابی را به مبدا اطلاع می دهد.

هنگامی که یکی از مسیریاب های میانی شبکه از طریق جدول مسیریابی خود تشخیص دهد که شبکه مقصد ناشناخته می باشد، بسته ICMP با مقدار کد ۶ (شبکه مقصد ناشناخته است)به مبدا ارسال می دارد. این پیام در شبکه های فعال حقیقی تولید نمیشود، چون مسیریاب دراین حالت ازیک پیام ICMP با نوع ۳ و با کد ۰ (در دسترس نبودن شبکه) استفاده می نماید.

درصورتیکه مسیریاب میانی شبکه با کمک لایه پیوند خود متوجه عدم وجود میزبان مقصد شود، از پیام ICMP با مقدارکد ۷ (میزبان مقصد ناشناخته است) استفاده می نماید. به عنوان مثال چنانچه لایه پیوند مسیریاب ازطریق یک اتصال نقطه به نقطه به میزبان مقصد وصل باشد، دراین صورت قادر به تشخیص عدم وجود یک میزبان خاص می باشد.

هنگامی که مسیریاب شبکه تشخیص دهد که یک میزبان خاص از بقیه شبکه جدا شده است، از پیام های ICMP بامقدار کد ۸(میزبان مبدا جدا شده است) استفاده می نماید. البته RFC ۱۸۱۲ توصیه می کندکه مسیریاب های شبکه از کد خطای فوق استفاده ننمایند و در عوض ازیکی از پیام های در دسترس نبودن شبکه (کد صفر) یا در دسترس نبودن میزبان (کد ۱) استفاده نمایند. بنابراین پیام های ICMP با کد ۸ فقط جنبه تاریخی داشته و استفاده ای نمی شود.

مدیرشبکه می تواند به دلایل مختلف از ارسال بسته ها توسط مسیریاب های شبکه و ازطریق یک مسیر خاص جلوگیری نماید. حتی ممکن است که مسیریاب های شبکه مسیری به سمت مقصد یا شبکه تعیین شده داشته باشند و از نظر فنی مشکلی برای مسیریابی موجود نباشد ولی به عنوان بخشی از سیاست شبکه یک سازمان وبه خاطر عوامل مختلفی مانند دلایل مدیریتی، هزینه شبکه و امنیت، مدیر شبکه نخواهد بسته ها توسط مسیریاب ازطریق مسیرخاصی پردازش شود. دراین حالت از بسته های ICMP نوع ۳ و کد ۹ و ۱۰ (ارتباط با شبکه/ میزبان مقصداز طرف مدیریت ممنوع شده است)، استفاده می گردد. مقدار فیلد کد ۹ نشان می دهد که ارتباط با شبکه مقصد از طرف مدیریت ممنوع شده است، در صورتی که مقدار کد ۱۰ نشان دهنده این است که ارتباط با میزبان مقصد از طرف مدیریت ممنوع شده است.

چنانچه مسیریاب های میانی شبکه قادر به تامین نوع سرویس درخواست شده درفیلد نوع سرویس موجود درسرآیند IP بسته ها باشد، نمی تواند بسته را به شبکه یا میزبان مقصد پیش ببرد. دراین حالت یک بسته ICMP با نوع۳ وکد های۱۱،۱۲ (شبکه/ میزبان مقصد برای نوع سرویس دردسترس نیست) ارسال می شود. کد۱۱ نشان دهنده این است که شبکه مقصد برای مقدارکیفیت سرویس درخواستی در دسترس نیست درحالیکه کد ۱۲ نشان می دهد که میزبان مقصد برای کیفیت سرویس درخواستی دردسترس نمی باشد.

بسیاری از مسیر یاب های امروزه دارای نرم افزار فیلتر کردن بسته هستند که با کمک آن می توانند قوانین فیلتر کردن را اعمال نموده و از ارسال بسته ها به آدرس های IP خاص، نوع های پروتکل خاص و شماره های درگاه خاص جلوگیری کنند. این کار به خاطردلایل امنیتی انجام شده و اولین خط دفاع در برابر کاربران متخاصم است. دراین حالت از پیام های ICMP نوع ۳ و کد ۱۳(ارتباط به خاطر دیواره های آتش از جانب مدیریت ممنوع شده است) استفاده می شود.

پیام های ICMP با کد ۱۴(تخلف تقدم میزبان)، توسط مسیریاب اولین پرش به میزبان فرستنده ارسال می شوند. مسیریاب اولین پرش، اولین مسیریابی است که بسته برای رسیدن به مقصد خود باید از آن عبور کند. این پیام ICMP نشان دهنده این است که تقدم خواسته شده برای آدرس مبدا / مقصد و شماره های درگاه مبدا/ مقصد، مجاز نمی باشند.

پیام ICMP با کد ۱۵(تقدم در اثر عمل نمی کند) توسط مسیریاب های میانی شبکه تولید میشود. مدیر شبکه این امکان را دارد که درجدول مسیریابی نودهای میانی شبکه، حداقل تقدم مورد نیاز برای عبوربسته ها از یک مسیرخاص را تعیین کند. اگر بسته ارسالی با مقدار تقدم پائین تر از آنچه درجدول مسیریابی مشخص شده است، ارسال گردد دراین صورت بسته ها قادر به عبور از این مسیر نبوده و ناگزیر باید حذف شوند. دراین حالت یک پیام ICMP با کد ۱۵(تقدم در اثر عمل نمی کند) به سمت مبدا ارسال می شود.

۸-۴-۳-۳-پیام ICMP فرونشاندن مبدا

ازآنجاییکه شبکه های IP بدون اتصال می باشند، درهنگام مسیریابی و پیش بردن بسته ها به سمت مقصد، اطلاعات مربوط به آنها را درحافظه های خود ذخیره نمی نمایند. بنابراین ممکن است که مسیریاب های میانی شبکه به طور موقت دچار ازدحام شوند. درشرایطی که حافظه یا ظرفیت بافر بیشتری در مسیریاب های میانی شبکه برای ذخیره بسته های ورودی وجود ندارد، ازدحام بوجود می آید. بسته های ارسالی، قبل از پردازش و هدایت به سمت مقصددر بافر مسیریاب های میانی ذخیره می شوند. معمولا مسیریاب ها تلاش دارند که اتصالاتی را که تحت تاثیر ازدحام شبکه قرار گرفته اند، آهسته نمایند. هنگامی که یک مسیریاب متوجه وقوع ازدحام در بافرهای خود گردید، باید بسته های ورودی اضافی را حذف کند. یکی از بهترین روش های کاهش ازدحام شبکه، درخواست از میزبان های مبدا برای کاهش سرعت ارسال می باشد. بدینمنظور مسیر یاب از پیام ICMP فرونشاندن مبدا استفاده می کندوبدین ترتیب از فرستنده ها درخواست می کند که سرعت ارسال خود را کاهش دهند.

اگرقرارباشد برای هر بسته ای که مسیریاب به خاطر پر بودن بافر های حافظه خود آن را حذف می کند یک پیام فرو نشاندن مبدا ارسال شود، دراین صورت، پیام های ICMP فرونشاندن مبدا ارسالی، ازدحام را در شبکه افزایش می دهند و به سایر مسیر یاب ها اثر منفی می گذارند. برای رفع این مشکل، درپیاده سازی های پیشرفته پروتکل ICMP، پیام های فرو نشاندن مبدا، فقط به مبداء هایی ارسال می شودکه بیشترین بسته ها را تولید می کنند. همچنین دربرخی از پیاده سازی ها، مسیریاب ها به جای این که صبر کنند تا بعد ازپرشدن بافر،پیام ICMP فرونشاندن مبدا ICMP ارسال نمایند، هنگامی که بافر در حال پر شدن است، ارسال پیام های فوق را شروع کرده تا بدینوسیله از سرریزشدن بافر های خود جلو گیری نمایند. سوالی که اینجا مطرح می شود این است که چگونه یک مبدا می فهمد که مشکل ازدحام رفع شده است؟ و چه هنگامی می تواند سرعت ارسال خود را افزایش دهد؟ متاسفانه هیچ پیام ICMP برای لغو یا معکوس کردن پیام فرو نشاندن مبدا و نشان دادن این که مشکل ازدحام بر طرف شده است، وجود ندارد. بنابراین در سطح IP فرستنده نسبت به

اینکه چه زمانی نرخ ارسال را افزایش دهد آگاه نمی باشد. برخلاف IP، پروتکلTCP نسبت به زمانی که باید نرخ ارسال را افزایش دهد، آگاهی دارد. این قابلیت دربخش کنترل جریان TCP پیاده سازی شده است که درفصل های بعدی آن را توصیف خواهیم نمود.

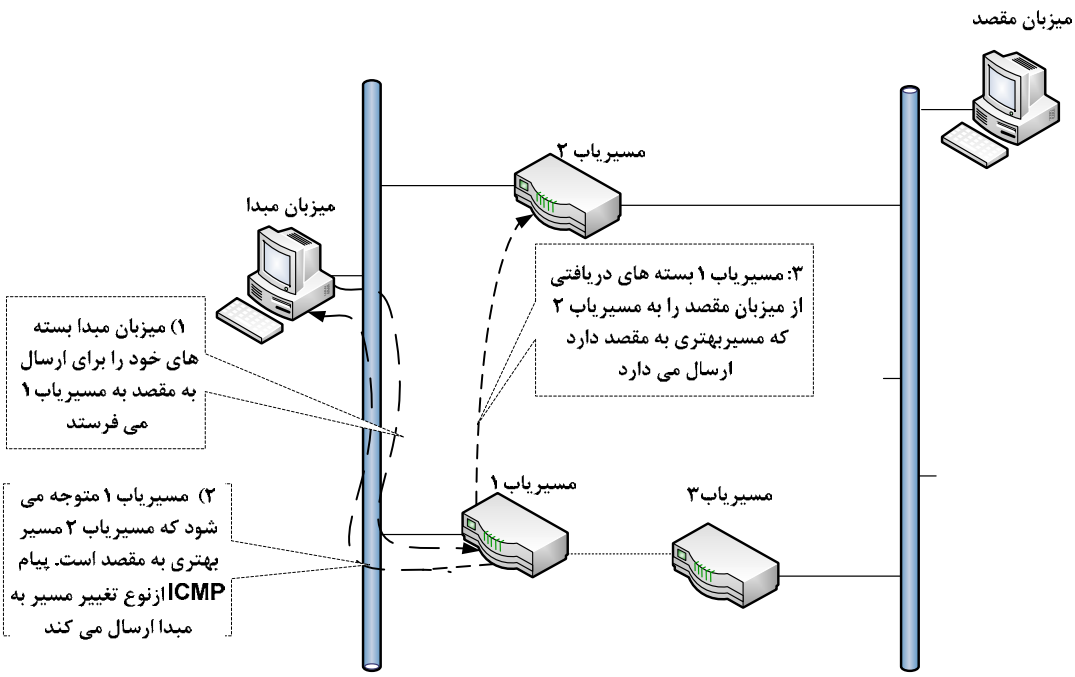
درساختار پیام های فرو نشاندن مبداء، مقدار فیلد نوع برابر با ۴ است. فیلدکد برابر با صفربوده و از فیلد۴ بایتی پارامتر استفاده نشده و همواره صفر است.

۸-۴-۳-۴-پیام ICMP تغییر مسیر

هنگامی که یک مسیریاب شبکه بسته ای را برای ارسال دریافت نماید ولی تشخیص دهد که مسیریاب دیگری مسیر بهینه تری برای ارسال بسته به سمت مقصد دارد، اقدام به ارسال پیام ICMP تغییر مسیر می نماید. مسیریاب ها اطلاعات مسیریابی را در شبکه با استفاده از پروتکلهای مسیریابی با یکدیگر رد و بدل می کنند. بنابراین مسیریاب های شبکه، همواره اطلاعات بهینه یا اطلاعات نزدیک به بهینه را درباره مسیرهای شبکه دارند. از طرف دیگراطلاعات مسیریابی میزبان ها بسیار کم بوده و قابل مقایسه با مسیریاب ها نمی باشد. معمولا یک میزبان شبکه آگاهی کمی نسبت به شبکه داشته و فقط مسیریاب های پرش بعدی خود را می شناسد. مسیریاب های پرش بعدی، مسیر یابهایی هستند که یک پرش از میزبان مبدا فاصله دارند. بنابراین میزبان مبدا و مسیریاب های پرش بعد مستقیما به یک شبکه متصل شده اند.

میزبان های شبکه معمولا دارای مسیریاب پیش فرض می باشندکه از آن برای پیش بردن بسته های ارسالی به مقصد هایی که صریحا در جدول مسیریابی میزبان لیست نشده است، استفاده می شود. جدول مسیریابی، در ناحیه داده پیکره بندی مانند یک فایل در میزبان نگه داشته می شود. با توجه به اینکه مسیریاب های شبکه مجهز به پروتکل های مسیریابی می باشند، درصورت وقوع تغییر درتوپولوژی شبکه، قادر به شناسایی مسیرهای جدید هستند. معمولا میزبان های شبکه در مبادلات پروتکل مسیریابی به طور مستقیم شرکت نمی کنند. در نتیجه میزبان ها از تغییرات توپولوژی آگاه نبوده و ممکن است جداول مسیریابی آنها شامل اطلاعات بهینه برای دستیابی به یک مقصد نباشد.

به عنوان مثال، شبکه نشان داده شده درشکل (۸-۲۶) را درنظر بگیرید. دراین شکل، مسیریاب جدید R2 به شبکه اضافه شده است. این مسیریاب جدید دارای یک مسیر بهینه تری برای دستیابی به میزبان مقصد B است. از آنجاییکه میزبان A هنوز متوجه اضافه شدن مسیریاب جدید R2 به شبکه نشده است، بنابراین برای پیش بردن بسته هایش به مقصد B همچنان از مسیریاب R1 استفاده می نماید. اگر مسیریاب R1 تشخیص دهدکه مسیریاب R2 مسیر بهینه تری به مقصد دارد ، یک پیام ICMP تغییر مسیر به فرستنده ارسال می کند. همچنین بسته را به مسیریاب بهینه تر یعنی R2 ارسال می دارد.



شکل (۸-۲۶): مثالی از کاربرد پیام های ICMP تغییر مسیر

میزبان های شبکه با دریافت یک پیام ICMP تغییرمسیر، جدول مسیریابی خود را با اطلاعاتی درباره مسیریاب جدید برای دستیابی به مقصد به روزرسانی می نمایند. بنابراین بسته های بعدی که به همان مقصد فرستاده می شوند باید از مسیر بهینه تر که از پیامICMP تغییرمسیر بدست می آید، استفاده نمایند. برخی از پیاده سازی های TCP/IP فاقد قابلیت فوق بوده و بسته های ICMP تغییر مسیر را نادیده می گیرند. از آنجاییکه با هر بسته ای که به مسیریاب غیر بهینه فرستاده می شود، یک پیام ICMP تغییر مسیر به مبدا ارسال می شود، این امر منتج به تولید ترافیک اضافی در شبکه می شود. درساختار پیام های ICMP تغییر مسیر، مقدار فیلد نوع برابر با۵ است. همچنین مقادیر فیلد کد دراین پیام ها، قبلا در جدول (۸-۱۰) نشان داده شده بود. دربسته های ICMP تغییر مسیر، فیلدی برای نمایش آدرسIP مسیریاب بهینه درنظر گرفته شده است.

۸-۴-۳-۵-پیام هایICMP اعلان و انتخاب مسیریاب

از این پیام ها برای پیاده سازی مکانیزم کشف مسیریاب استفاده می شود. با کمک این مکانیزم، میزبان ها قادر خواهند بود تا به طور پویا همه مسیریاب های موجود که مستقیم به شبکه آنها متصل شده اند را کشف نمایند. با استفاده از قابلیت کشف مسیریاب ICMP ، میزبان های شبکه مجبور به وابستگی به پیکره بندی ایستا یا دستی جداول مسیریابی خود نخواهند بود، بلکه می توانند همه مسیر یاب هایی را که برای آنها در دسترس است به روشی که مستقل از پروتکل مسیریابی استفاده شده توسط مسیریاب ها است پیدا کنند.

قابلیت کشف مسیریاب ICMP ، برای کشف مسیریاب های محلی که در شبکه به طور مستقیم به هم متصل هستند، استفاده می شود و پروتکل عمومی مسیریابی نمی باشد. پیام های ICMP اعلان مسیریاب، دربازه های متناوب ۷ تا ۱۰ دقیقه توسط مسیریاب ها فرستاده می شوند. همچنین از این پیام ها می توان درپاسخ به پیامICMP انتخاب مسیریاب استفاده نمود.

۸-۴-۳-۶-پیام ICMP تخطی زمانی

پیام ICMP تخطی زمانی در شرایط زیر تولید می شود :

- هرگاه مقدار فیلد TTLموجود دربسته های IP به صفر رسید، مسیریاب های شبکه یک پیام ICMP تخطی زمانی به سمت مبدا ارسال نموده و به آنها درمورد اتفاق فوق اطلاع رسانی می نمایند. مقدار کد برای این پیام صفر می باشد. اگر بسته ای دریک حلقه مسیریابی قرارگرفت، هر بار که مسیریاب بسته را دریافت می نماید حداقل ۱ واحد فیلد TTL را کاهش می دهد. درنهایت فیلد TTL به صفر می رسد که در این زمان بسته باید دور انداخته شود و یک پیام ICMP تخطی زمانی تولید می گردد.
- هرگاه یک تکه از بسته های IP تکه شده به میزبان مقصد نرسد، میزبان مقصد یک پیام ICMP تخطی زمانی با مقدار کد برابر با ۱ ارسال می دارد. میزبان های شبکه معمولا مجهز به یک زمان سنج بازسازی می باشندکه با دریافت اولین تکه بسته شروع به کار می کند. چنانچه تا زمانیکه این زمان سنج فعال است، همه تکه های مربوط به یک بسته IP به میزبان مقصد نرسد، تکه های دریافتی حذف شده و یک پیام ICMP تخطی زمانی به مبداء ارسال می گردد.

مقدار فیلد نوع درساختارپیام های ICMP تخطی زمانی، برابر با ۱۱ می باشد. همچنین مقدار کد این پیام ها ۰ یا ۱ است. کد ۰ بیانگر این مطلب است که پیام توسط مسیریاب های میانی شبکه تولید شده است درحالیکه کد۱ نشان دهنده اتمام زمان سنج بازسازی بسته ها درمیزبان مقصد می باشد. پیام های ICMP تخطی زمانی توسط میزبان های شبکه تولید می شوند.

۸-۴-۳-۷-پیام ICMP مشکل پارامتر

چنانچه مسیریاب و یا میزبان شبکه متوجه مشکلی درپارامترهای سرآیندIP بسته های دریافتی شوند، از پردازش بسته جلوگیری کرده و یک پیام ICMP مشکل پارامتر، با مقدار فیلد نوع برابر با ۱۲ ارسال می دارند. با کمک فیلد اشاره گرموجود دراین پیام، محل و نوع پارامتری که دارای مشکل است، درسرآیند IP مشخص می شود. مقدار فیلد کد برابر با ۰ ،۱ ویا ۲ می باشد. کد ۰ بیانگر این است که اشاره گر موجود درپیام ICMP مشکل پارامتر محل خطا را نشان می دهد. کد ۱ نشان دهنده نادرست بودن یکی از امکانات موجود درسرآیند IP است و نهایتا کد ۲ نشان دهنده این است که طول بسته IP نادرست است. بنابراین درصورتیکه پیام فوق با کد ۱ ارسال شود، ازفیلد اشاره گراستفاده ای نمی شود.

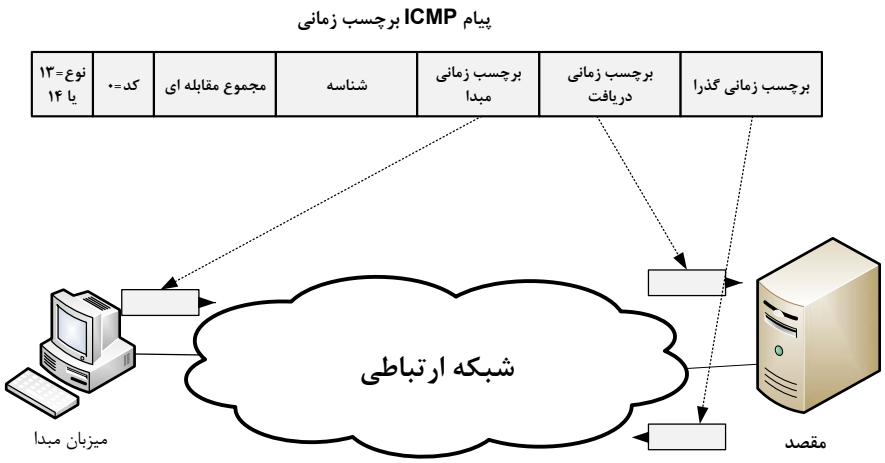
۸-۴-۳-۸-پیام ICMPدرخواست برچسب زمانی/پاسخ برچسب زمانی

هر نود شبکه های IP دارای یک ساعت داخلی می باشد. برای همزمان سازی ساعت های نودهای شبکه، از پیام های ICMP درخواست برچسب زمانی/پاسخ برچسب زمانی استفاده می شود. البته می توان از پروتکل NTP[1] نیز برای همزمان سازی ساعت نودهای شبکه نیز استفاده نمود، اما استفاده از پیام هایICMP درخواست برچسب زمانی/پاسخ برچسب زمانی به مراتب ساده تر است.

درساختار پیام های فوق، مقدار فیلد نوع برای پیام های درخواست برابر با ۱۳ و برای پیام های پاسخ برابر با ۱۴ می باشد. همچنین مقدار فیلد کد برابر با ۰ است. مقدار برچسب زمانی، برحسب تعداد میلی ثانیه های گذشته از نیمه شب طبق ساعت جهانی اندازه گیری می شود. درساختار پیام های فوق، سه فیلد برای درج برچسب زمانی درنظر گرفته شده است که عبارتند از: برچسب زمانی مبداء، برچسب زمانی دریافت و برچسب زمانی گذرا. برچسب زمانی مبدا، توسط مبداء فرستنده پیام مقداردهی می شود. گیرنده ، به محض دریافت پیام فوق مقدار زمان جاری خود را درفیلد برچسب زمانی دریافت قرارمی دهد. بعد از پردازش بسته دریافتی، درپاسخ به آن، پیام پاسخ ارسال می شود. دراین حالت، گیرنده مقدار برچسب

[1] Network Time Protocol

زمانی جاری را درفیلد برچسب زمانی گذرا قرار داده و ارسال می دارد. شکل (۸-۲۷) مثالی از نحوه مقدار دهی برچسب زمانی دراین پیام ها نشان داده شده است.



شکل (۸-۲۷): مثالی از نحوه پرنمودن فیلدهای برچسب زمانی

۸-۴-۳-۹-پیام های ICMP درخواست اطلاعات/پاسخ اطلاعات

از این پیام ها برای بدست آوردن آدرس IP میزبان هایی که آدرس IP خود را نمی دانند استفاده می شود. البته با وجود پروتکل هایی مثل RARP ، BOOTP و DHCP که مکانیزم های عالی تری را برای کشف آدرس IP فراهم می کنند، استفاده از پیام های فوق مرسوم نبوده و به هیچ وجه توصیه نمی شود. برای پیام ICMP درخواست اطلاعات مقدار فیلد نوع برابر با ۱۵ بوده و برای پیام پاسخ آن این فیلد برابر را ۱۶ است. فیلد کد همواره ۰ است.

۸-۴-۳-۱۰-پیام های ICMP درخواست پوشش آدرس/پاسخ پوشش آدرس

درفصل قبلی، مفهوم زیر شبکه سازی و آدرس های پوشش زیرشبکه توصیف شدند. میزبان های شبکه برای بدست آوردن پوشش زیر شبکه، از پیام ICMP درخواست پوشش آدرس استفاده می کنند. دراین پیام ها مقدار فیلد نوع برابر با ۱۷ می باشد. همچنین درپاسخ به پیام درخواست فوق، پیام ICMP پوشش آدرس با مقدار فیلد نوع برابر با ۱۸ ارسال می شود.
میزبان درخواست کننده آدرس پوشش زیرشبکه، درخواست خود را مستقیما به آدرس مسیریاب شبکه ارسال می دارد. درحالتیکه میزبان فوق، آدرس مسیریاب را نداند، درخواست را به صورت همه پخشی درشبکه پخش می کند. فقط مسیریاب های شبکه مجاز به پاسخ دهی به پیام های درخواستی فوق می باشند.

پرسش های فصل

۱. کاربرد و دلیل عمده استفاده از پروتکل ARP را توضیح دهید.
۲. ساختار بسته های ARP را رسم نموده و کاربرد هرفیلد آن را بنویسید.
۳. محدودیت های پروتکل ARP را ذکر کنید.
۴. به چه علت پیام درخواست ARP به صورت همه پخشی ارسال می شود؟
۵. آیا پیام پاسخ ARP نیز به صورت همه پخشی ارسال می شود یا خیر؟ توضیح دهید.
۶. با ذکر یک مثال و رسم شکل، حداقل دو کاربرد اصلی پروتکل ARP را توضیح دهید.

۷. اگر یک میزبان شبکه به طور ایستا با اطلاعاتی درباره آدرس های MAC و آدرس های IP مطابق پیکره بندی شود، با چه مشکلاتی مواجه می شود ؟
۸. چگونه آزمون آدرس IP تکراری ARP انجام می شود ؟
۹. مشکلات ناشی از پروتکل ARP/RARP را درشکه های پل بندی شده توضیح دهید.
۱۰. فرض کنید که دریک شبکه دو ایستگاه کاری وجود دارند که هر دو آدرس197.12.35.67 دارند. آدرس های MAC دو ایستگاه فوق به ترتیب A وB می باشد. این دو ایستگاه همزمان اقدام به برقراری همزمان یک جلسه Telnet با یک سرویسگر به آدرس IP 197.12.35.99 وآدرس سخت افزاری C می نمایند. به طور کامل توضیح دهید که دراین حالت چه اتفاقی می افتد و مشکل ایجاد شده به چه صورت قابل رفع می باشد؟
۱۱. کاربرد پروتکل RARP را توضیح داده و ساختار بسته های آن را رسم کنید.
۱۲. نقش سرویس دهنده های اصلی و ثانویه RARP چیست ؟ توصیف کنید چگونه یک سرویس دهنده ثانویه می تواند به یک درخواست RARP پاسخ دهد ؟
۱۳. ویژگی های اصلی شبکه های IP را توضیح دهید.
۱۴. با توجه عدم اطمینان پروتکل IP، توضیح دهیدکه مشکل ناشی از گم شدن بسته ها درمعماری TCP/IP به چه صورت قابل رفع می باشد؟
۱۵. ساختار بسته های IPV4 را رسم کرده و به طور خلاصه کاربرد هر فیلد را توضیح دهید.
۱۶. کمترین و بیشترین طول بسته های IP چقدر می باشد؟
۱۷. فرض کنیدکه نرم افزار IP موجود دریک مسیریاب فقط بتواند بسته های نسخه ۴ را پردازش کند. اگر بسته هایی را با مقدار فیلد نسخه متفاوت دریافت کند چه اتفاقی می افتد ؟
۱۸. کاربرد فیلد نوع سرویس و اجزای آن را بنویسید.
۱۹. مفهوم MTU را نوشته و مقدار آن را برای شبکه های مختلف بنویسید.
۲۰. مفهوم تکه سازی و بازسازی بسته های IP را نوشته و فیلدهایی را که به این منظور به کارمی روند، ذکر کنید.
۲۱. کاربرد فیلد TTL را دربسته های IP بنویسید؟
۲۲. مزایا و معایب بازسازی بسته های درمسیریاب های میانی شبکه را توضیح دهید.
۲۳. یک بسته IP با اندازه ۱۵۰۰ بایت با پرچم DF برابر با ۱ در یک شبکه با اندازه MTU ۱۵۰۰ بایت فرستاده شده است مسیر به نود مقصد از شبکه هایی با اندازه MTU ۲۰۰۰ و ۴۴۷۰ بایت میگذرد آیا تکه سازی اتفاق می افتد ؟ آیا IP قادر به تحویل بسته به مقصد می باشد ؟
۲۴. یک بسته IP با اندازه ۱۵۰۰ بایت و مقدار فیلد شناسایی ۱۰۰ با پرچم DF برابر با صفر در یک شبکه با اندازه MTU ۵۰۰ بایت می گذرد . اندازه MTU شبکه مقصد ۱۵۰۰ بایت است آیا تکه سازی اتفاق می افتد ؟ اگر چنین است تکه ها را با مقادیر فیلد های شناسایی MF و DF و افست تکه سازی مشخص کنید .
۲۵. یک بسته IP با اندازه ۱۵۰۰ بایت و مقدار فیلد شناسایی ۱۰۰ با پرچم DF برابر با صفر در شبکه با اندازه MTU ۱۵۰۰ بایت فرستاده شده است . مسیر به نود مقصد از شبکه با اندازه MTU ۶۲۵ می گذرد . اندازه MTU شبکه مقصد ۵۲۵ بایت است آیا تکه سازی اتفاق می افتد؟ اگر چنین است تکه ها را در مسیریاب بین شبکه ها مشخص کنید . برای هر تکه مقادیر فیلد های شناسایی ، MF و DF و افست تکه سازی را نشان دهید
۲۶. کاربرد گزینه های IP را نوشته و انواع آن را ذکر کنید.
۲۷. با ذکر یک مثال کاربرد امکان مسیریابی مبدادقیق را ذکر کنید.
۲۸. با ذکر یک مثال تفاوت مسیریابی مبداء ضعیف با مسیریابی مبداءدقیق را بنویسید.
۲۹. گزینه برچسب زمانی اینترنت در چه موردی استفاده می شود ؟

۳۰. حداقل ۵ مشکل را نام ببرید که از ICMP می توان برای گزارش دادن آنها استفاده کرد ؟
۳۱. چه نوع وسایلی در یک شبکه می توانند پیام های ICMP را تولید کنند ؟
۳۲. آیا استفاده از ICMP ، IP را مطمئن تر می سازد ؟ دلایل جواب خود را بیان کنید .
۳۳. اگر یک بسته IP تکه سازی شود آیا پیام های ICMP برای هر تکه تولید می شود؟جواب خود را توجیه کنید.
۳۴. آیا ICMP در مورد بسته هایی که شامل پیام ICMP هستنداستفاده می شود یا خیر؟ جواب خود را توجیه کنید .
۳۵. درچه حالت هایی از پیام های ICMP استفاده نمی شود؟
۳۶. چرا پیام های ICMP به تولید کننده اصلی بسته که گزارش شده فرستاده می شود ؟ اگر یک خطا در جدول مسیریابی مسیریاب مسئول تولید پیام ICMPباشد. چرا نمی توان پیام ICMP را به خود مسیریاب فرستاد ؟
۳۷. آیا ضمانتی وجود دارد که پیام های ICMP تحویل داده شده اند ؟ جواب خود را توضیح دهید.
۳۸. ساختار بسته های ICMP را رسم کرده و عملکرد هرفیلد را توضیح دهید.
۳۹. مقصود از فیلد های نوع و کد در یک پیام ICMP چیست ؟
۴۰. فیلد اطلاعات یک پیام ICMP شامل چه نوع اطلاعاتی می شود ؟
۴۱. کاربرد امکان PING را بارسم یک شکل توضیح دهید.
۴۲. چه هنگامی پیام های ICMP نوع ۳، باید فرستاده شود ؟
۴۳. توضیح دهید چگونه پیام ICMP نوع ۳ می توان برای تخمین کمترین اندازه MTU مسیر به مقصد استفاده کرد ؟
۴۴. چه هنگامی پیام فرونشاندن مبدا فرستاده می شود ؟ چرا این پیام نباید توسط مسیریاب ها فرستاده شود ؟ چه لایه ای از OSI مناسب ترین لایه برای اداره کردن مشکلی است که توسط پیام فرو نشاندن مبدا مشخص شده است ؟
۴۵. دلایل ایجاد ازدحام در یک مسیریاب شبکه را توضیح دهید.
۴۶. با ذکر یک مثال کاربرد پیام تغییر مسیر ICMP را توضیح دهید.
۴۷. تحت کدام شرایط مسیریاب ها باید پیام های ICMP را تولید کنند ؟
۴۸. در مورد پیا مهای ICMP که برای کشف مسیریاب استفاده می شود بحث کنید. مزایای این روش بر سایر تکنیک ها چیست ؟
۴۹. درچه حالت هایی پیام ICMP تخطی اززمان فرستاده می شود ؟
۵۰. چه هنگامی پیام ICMP مشکل پارامتر ارسال می شود ؟
۵۱. کاربرد پیام های ICMP درخواست / پاسخ پوشش آدرس چیست ؟ سایر پروتکل های دیگر که می توانند برای این مقصود استفاده شوند چیست ؟