فصل ۲

Mahdi saghaei
Digitally signed by Mahdi saghaei
DN: CN = Mahdi saghaei, C = IR, O = Mojtama Fanni Tehran (ZANJAN branch)
Reason: I am the author of this document
Date: 2007.11.04 15:24:41 +03'30'

معرفی معماری *IPv6*

ترجمه و تالیف: مهدی سقایی (MCP, MCSE, CCNA, CCNP)
دانشجوی کارشناسی ارشد IT (گرایش امنیت اطلاعات) دانشگاه لیورپول انگلستان

راه حلهای موجود در این فصل :

- درک فواید IPv6
- مقایسه IPv6 با IPv4
- بررسی معماری شبکه IPv6
- انتشار پروتکل لایه بالاتر
- درک ICMPv6
- درک Neighbor Discovery

- ✓ پیگیری سریع راه حل ها
- ✓ سوال و جواب های متداول

معرفی

آدرس IPv6 بالاخره بشکل عملیاتی درآمد. اگرچه تاکنون تقریبا ده سال است که بر روی ویژگیها و استانداردهای این پروتکل کار شده ، اما اخیرا نهایی شده است. علاوه بر این برخی از جنبه های آن هنوز توسط گروههای کاری سازمان IETF در حال کار و بررسی است. آدرسهای صادر شده توسط IPv4 برای راهکارهای جامع ناکافی بود. این مسئله طراحان را مجبور کرد تا بر روی نسخه جدید این پروتکل کار کنند و این موضوع را بگونه ای انجام دهند که دوباره با مسائل مشابه رویارو نشوند. اعضای انجمن اینترنت که مسئولیت توسعه پروتکل را برعهده دارند ، هر پروتکل جدیدی را که تحت RFC توسعه یافته بدقت موشکافی و بررسی کردند. RFC ها پرونده هایی هستند که جزئیات و ویژگیهای پروتکلها را ارائه می دهند ، بنابراین سازندگان نرم افزار و سخت افزار از این طریق نحوه اِعمال پروتکل در استانداردها را خواهند دانست. این استانداردسازی باعث می شود که ارائه دهندگان نرم افزار و سخت افزار جدا از توسعه تخصصی یک پروتکل از یک طرح و برنامه یکسات تبعیت کنند. هدف این کتاب کمک به تضمین اجرای بدون اشکال این پروتکل جدید بوسیله تمرکز بر پیکربندی IP نسخه ۶ بر روی IOS سیسکو می باشد.

درک فواید IPv6

اجازه دهید در مورد برخی از فواید IPv6 ریزتر بحث کنیم تا ببینیم چگونه این پروتکل سعی می کند تا مشکلات امروزه اینترنت و شبکه های تجاری را حل کند. از مهمترین دلایل توسعه نسخه جدید IP می توان به محدودیت فضای آدرس کلاس B ، توسعه و گسترش جدولهای مسیریابی زیرساخت اینترنت ، موضوعات امنیتی ، محدودیت اندازه گزینه های IP و کارایی و بهره وری مسیریابی اشاره نمود. سپس دو مشکل مهمی را که بوسیله IPv6 حل شده اند ، مورد بررسی قرار خواهیم داد که عبارتند از: کاهش و محدودیت آدرسهای دارای نام و قابلیت توسعه مسیریابی.

فواید IPv6 عبارتند از:

- افزایش اندازه آدرس IP
- افزایش پشتیبانی از آدرس دهی سلسله مراتبی
- آدرس دهی ساده Host (آدرس دهی یکپارچه: Global , Site , Local)
- آدرس دهی اتوماتیک ساده (آدرس دهی دوباره ساده ، DHCPv6 ، Neighbor Discovery بجای آدرس فراگیر ARP)
- بهبودی و پیشرفت در توسعه مسیریابی گروهی (Multicast).
- آدرس Anycast
- سرایند موثر
- امنیت توسعه یافته (سرایندهای اضافی امنیت ، یکپارچه سازی درستی اطلاعات)
- تحرک و پویایی بهتر
- کارایی بهتر (یکپارچه سازی ، Neighbor Discovery بجای آدرسهای فراگیر ARP ، عدم قطعه قطعه شدن ، عدم آزمایش خطای سرایند ، جریان متناوب ، اولویت ، و سرویس کیفیت یکپارچه).

افزایش اندازه آدرس IP

در IPv6 ، ۱۲۸ بیت برای آدرس دهی در دسترس قرار دارد. ۱۲۸ بیت فضای آدرس به معنی اینست که شما بتوانید۲ بتوان ۱۲۸ عدد آدرس متفاوت در اختیار داشته باشید. ۳ بیت اول در این آدرس ، برای آدرسهای GRU (منحصربفرد قابل مسیریابی جهانی) رزرو شده است. این مسئله به این معنی خواهد بود که ما برای آدرس دهی فقط ۱۲۵ بیت در اختیار داریم (۱۲۵=۳-۱۲۸) و عملا ۲ بتوان ۱۲۵ آدرس در دسترس ما می باشد. این تقریبا معادل 4.25E+037 آدرس خواهد بود. برای درک بهتر مسئله ، اجازه دهید آن را با IPv4 مقایسه کنیم. در IPv4 ما تمام فضای آدرس بین 0.0.0.0 و 223.255.255.255 را برای آدرس دهی منحصربفرد (Unicast) استفاده می کنیم که در حدود 3.7E+09 آدرس می باشد. این به معنی آن خواهد بود که IPv6 به میزان ۱۰ بتوان ۲۸ عدد بیش از IPv4 دارای آدرس می باشد.

بصورت روشن و شفاف ، ۱۲۸ بیت فضای آدرس کافی برای تحت پوشش قرار دادن آینده اینترنت را در اختیار می گذارد. فضای آدرس IPv6 بسیار بزرگتر از IPv4 است. اولین نکته ای که در IPv6 مشخص است ، تعداد شبکه هایی است که IPv6 می تواند پشتیبانی کند. یک آدرس IPv6 ، ۶۴ بیت آخر را برای توضیح شناسه Host (کامپیوتر) بر روی یک شبکه استفاده می کند. علاوه بر این ، IPv6 از ۶۴ بیت آخر برای تمیز دادن و جدا کردن Hostها از یکدیگر بر روی یک زیرشبکه نیز بهره می برد. چه در صورت آدرس دهی به شکل Link-local ، چه Site-local و چه آدرس GRU ، ۶۴ بیت آخر بر روی یک کامپیوتر به همان میزان باقی خواهد ماند. این بدین دلیل است که IPv6 از آدرس MAC

لایه ۲ بعنوان شناسه Host برای یک کامپیوتر استفاده می کند (آدرس MAC لایه ۲ آدرسی است که در داخل سخت افزارهـای لایـه ۲ ماننـد کارت شبکه توسط کارخانه سازنده ایجاد شده است). از آنجائیکه آدرسهای MAC فقط ۴۸ بیت طول دارند ، در IPv6 یک پیشوند ۱۶ بیتی نیز به آنها اضافه می شود که این مورد را با جزئیات آن مورد بحث قرار خواهیم داد. بنابراین اگر شما ۶۴ بیت استفاده شده برای شناسه Host و سه بیت استفاده شده برای آدرس GRU را حذف کنید ، ۲ بتوان ۶۱ بیت آدرس بدست خواهید آورد (2.31E+018). بنابراین حتی بدون استفاده از تمام آدرسهایی که IPv6 در اختیار دارد ، ما می توانیم قابلیت توسعه بیشتری نسبت به آینده IPv4 در اختیار داشته باشیم. IPv6 ایـن اجـازه و توانایی را به ما می دهد که بدون نگرانی از محدودیت و اتمام آدرسها ، عمل آدرس دهی را انجـام دهـیم. جـدول ۱-۲ مقایسـه ای بـین انـدازه آدرسهای IPv4 و IPv6 ارائه می دهد.

جدول ۱-۲ مقایسه فضای آدرس

مشخصات	IPv4	IPv6
طول آدرس	۳۲ بیت	۱۲۸ بیت
طول شناسه Host	۲۴ - ۲ بیت	۶۴ بیت
طول شناسه شبکه	۳۰ - ۷ بیت	۶۱ بیت
حداکثر تعداد Host به ازای هر زیرشبکه	$۲^{۲}$ - $۲^{۲۴}$	$۲^{۶۴}$
حداکثر تعداد زیرشبکه	$۲^{۷} - ۲^{۳۰}$	$۲^{۶۱}$
حداکثر تعداد Host	3.7 E + 09	4.25 E + 037

افزایش پشتیبانی از آدرس دهی سلسله مراتبی

همانطور که می دانیم ،اختصاص IPv4 در ابتدا تحت قواعد Classful[۱] انجـام شـد و سـپس براسـاس اصـول Classless (CIDR)[۲] ادامـه یافـت. IPv6 مشکلات تراکم دوباره با هرکدام از این موارد را ، با استفاده از خرد کردن آدرس IPv6 در مجموعه ای از محدوده هـای معـین ، تصـحیح کرده است. قالب پیشوند برای این استفاده می شود که نشان دهـد آدرس از نـوع GRU اسـت و یـا از نـوعی دیگـر. ایـن اجـازه مـی دهـد کـه سیستمهای مسیریابی بسرعت تشخیص دهند که نوع پکت GRU است یا نوعی دیگر. با کسب سریع این اطلاعات ، دستگاه مسیریابی می تواند پکت را بصورت مناسب تر و بهتر به سمت سیستمهای زیرمجموعه مسیریابی جهت بررسی کامل ارسال کند.

شناسه TLA[۳] با دو هدف استفاده می شود:

اول؛ برای برگزیدن و تخصیص یک بلوک بزرگ از آدرسها از بین بلوکهای کوچکتر برای ارائه اتصال پایین دست جهـت دسترسـی بـه اینترنـت. دوم؛ برای تشخیص اینکه مبدا یک مسیر چه بوده و از کجا می آید. اگر بلوک های بزرگ آدرسها فقط به ISPها ارائه گردد و پـس از آن بنوبـت به مشتریها ، تشخیص اینکه مسیرهای طی شده مربوط به کدام شبکه بوده و آغاز و محل تولید هر مسیر کجـا بـوده اسـت ، بسـیار راحـت تـر خواهد بود. با IPv4 بسیاری از آدرسها قابل انتقال هستند. همچنین تعداد سازمانهایی که بلوک هـای آدرس را بـه سـازمانهای تجـاری و دیگـر مشتریان پایین دست ارائه می کنند ، بسیار زیاد است. بنابراین دانستن اینکه یک مسیر از کجا ناشی شده و شروع می شود ، بدون پیگیـری رو به عقب مبدا یک پکت (Trace) ، غیر ممکن است. اکنون بوسیله IPv6 ، تعیین مبدا یک مسیر ، بسیار عملی تر و امکـان پـذیرتر شـده اسـت. فرض کنید که اینترنت شامل ۵۰۰ تامین کننده ردیف اول باشد ، در این صورت توسط جستجو در یک مدت زمان بسیار کم ، بر مبنای شناسه TLA مربوط به طولانی ترین مسیر ، می توان فهمید که مسیر از کجا آغاز شده است. حتی می توان نرم افزاری را تولید کرد که ایـن وظیفـه را در داخل خود جای داده و انجام دهد (البته اگر آن نرم افزار توانایی بروزرسانی لیست آدرسهای اختصاص داده شده را داشـته باشـد). در بخـش پیشین گفتیم که آدرسها چگونه باید فقط به تامین کنندگان اختصاص داده شوند و آنها بر مبنای تشخیص خود IPv6 را به کسانی که احتیـاج دارند ، تخصیص دهند. با این راه ما می توانیم با متراکم کردن پیشوندها در بلوکهای بزرگ در زیرساخت اینترنت ، کارایی را بـالا بـرده و بـدین وسیله باعث شویم تا مسیرهای کمتری بین دامنه ها تبادل گردند.

بعنوان مثال ، اجازه دهید فرض کنیم ما نمایندگی آدرس IPv6 به آدرس 3D00::B234::/24 را در اختیار داریم. همچنین فرض کنیم که تمـام مشتریان ما احتیاج به دریافت نمایندگی برای یک آدرس 48/ (۴۸ بیتی) جهت ارائه به شـبکه هـای خودشـان را دارنـد. ایـن مسـئله ۲۴ بیـت مخصوص ارائه نمایندگی جهت آدرس دهی برای ما باقی می گذارد ، که فضـای آدرس بزرگـی اسـت. در حقیقـت تعـداد شـبکه هـایی کـه مـا می توانیم با این شکل پشتیبانی کنیم ، برابر با تعداد Host هایی است که می توانستیم بـا یـک بلـوک از کـلاس A در آدرس IPv4 پشـتیبانی

---

[۱] Classful به معنی عدم ارسال اطلاعات subnet mask بهمراه بسته های اطلاعاتی IP در هنگام مسیریابی می باشد.

[۲] Classless به معنی ارسال اطلاعات subnet mask با هر مسیر در جدولهای مسیریابی ارسال شده توسط پروتکلهای مسیریابی است.

[۳] متراکم کننده سطح بالا (Top Level Aggregator)

نماییم. در حال حاضر ، یک تامین کننده آدرس سطح بالا ، آدرسها را در مجموعه های ۱۶ بیتی (/16) یا کمتر دریافت می کند. حال اگر فرض کنیم یک تامین کننده آدرس ، آدرسهایی را با ساختار ۲۴ بیتی (/24) دریافت کند ، فقط ۸ بیت دیگر برای آدرس دهی باقی می ماند (۸=۲۴-۳۲) ، یعنی در عمل فقط می تواند ۲۵۴=۲-۲۵۶ (۲۵۴) عدد آدرس به زیرمجموعه خود اختصاص دهد. بسیاری از تامین کننده های امروزی آدرس (همان شرکتهای مخابراتی یا ISPها) احتیاج دارند تا آدرسهای خود را حداقل به میزان ۲۸ بیت (/28) برای زیرمجموعه های خود ، زیرشبکه سازی بکنند تا بتوانند آدرسهای بیشتری را تعریف و ارائه نمایند.

همانطور که در مثال قبل دیدیم ، یک تامین کننده سرویس سطح بالا ، با فضاهای آدرس بزرگی سر و کار دارد. این مسئله مشکل نیاز به مجموعه های بزرگ آدرس و محول کردن آدرسها را رفع نمی کند ، ولی انگیزه ای برای پشتیبانی بیشتر و اتوماتیک سازی توسعه زیرساخت یک سازمان ایجاد می کند. بسیاری از تامین کنندگان امروزی سرویس آدرس ، مشکلات زیادی برای بروزرسانی ساختار قدیمی خود جهت پشتیبانی از ساختارهای جدید دارند. IPv6 نه تنها فقط در محدوده معماری و مهندسی شبکه ، بلکه در چارچوب توسعه و یکسان سازی IT قابلیت ها و توانایی های بسیار خوبی را تامین می کند.

شناسه NLA[۴] شامل مجموعه ای از آدرسها است که بواسطه بلوک TLA و پس از آن به سیستمهای زیرمجموعه اختصاص داده می شود. ما می دانیم که این آدرسها (NLA) زمانی که بین تامین کننده های سرویس در ساختار اصلی اینترنت مبادله می شوند ، تا آنجائیکه ممکن باشد در داخل بلوک های TLA بصورت متراکم شده قرار می گیرند. اجازه دهید نگاهی به فایده های این نوع از ساختار آدرس دهی از دید NLA بیاندازیم.

دو ویژگی خوب برای دریافت آدرس از یک تامین کننده وجود دارد؛ اولین آنها پایداری مسیریابی در زیرساختهای ویژه و خاص است. اگر ما یک سازمان یا تامین کننده نوع NLA باشیم و بخواهیم به مشتریان زیرمجموعه خود سرویس بدهیم ، احتمالا بخاطر حفظ مشتریان و بازار خود نیازمند ارائه سرویسی کامل و قوی هستیم. ممکن است ما بخواهیم اجازه دهیم تا مشتریانمان بتوانند از مکانهای مختلف و بیرون از منطقه جغرافیایی که ما در آن قرار داریم ، به ما متصل شده و از طریق ما یک ارتباط قوی به سرویس دهنده های بالادست ما و از آنجا به سمت ساختار اصلی اینترنت داشته باشند. علاوه بر این ما می خواهیم به مشتریانمان اجازه دهیم تا جدول مسیریابی را که احتیاج دارند برای استفاده از مسیرهای خاص بمنظور تنظیم سیاستهای مسیریابی خود ، بصورت کامل را دریافت کنند. ممکن است آنها بخواهند بین دو ارتباط با استفاده از برقراری مسیر یک مقصد توسط یک ارتباط و استفاده از ارتباط دیگر برای برقراری ارتباطات باقیمانده ، تعادل بار ایجاد کنند. برای انجام اینکار ما مجبور هستیم تمام مسیرها را بر روی زیرساخت اصلی ارتباطی خود قرار داده و از این طریق بتوانیم آنها را به سمت مشتریان خود سوق دهیم. با وجود اینکه یک زیرساخت اینترنت ترکیبی از مدرنترین و قوی ترین ابزارهای مسیریابی است ، یک سرویس دهنده سطح دوم ، ممکن است نتواند از عهده بروزرسانی تکنولوژی های زیرساخت اینترنت و نیز افزایش اندازه جدول مسیریابی برآید. خوشبختانه توسط IPv6 قدرت پردازش آنقدر بزرگ نیست که ایجاد نگرانی کند. بدلیل اینکه هسته اینترنت بصورت ذاتی بسیار مناسب متمرکز شده است ، ما هم اکنون جدول های مسیریابی بسیار کوچکی برای نگهداری در اختیار داریم. ما می توانیم مسیرهای کاملی را برای یک مشتری تامین کنیم ، و آن مجموعه از مسیرها برای مدیریت و کنترل توسط ما بسیار بزرگ نیستند. بنابراین با بازی خوب هرکس و استفاده از استراتژی های مشروح ذیل ، می توانیم از فواید جدولهای مسیریابی کوچک هسته اینترنت در زیرساخت ارتباطی شبکه خود استفاده نماییم.

دومین فایده متراکم سازی NLA ، داشتن پایداری یک مسیر واقعی از میان مسیرهای موجود ما ، در بین هسته اینترنت جهانی است. در هنگام آغاز توسعه حجم اینترنت ، زمانهایی وجود داشت که اینترنت خیلی پایدار نبود. ارتباط برقرار کنندگان BGP تمایل دارند تا مسیرهای خراب ناشی از خرابی ارتباطات زیرساخت یا مسیرهای نارس نرم افزاری را بیرون اندازند. به این دلیل ، مسیرهایی که دائما انتشار داده شده و سپس کنار رفته اند (زمانی که مسیر غیر قابل دسترس می شود) ، باعث می شوند بطور قابل ملاحظه ای پردازش بیشتری بر روی مسیریابهای اصلی (هسته) قرار گیرد و بر این اساس باید بطور مداوم مجموعه ای از مسیرهای اینترنت در تمام مواقع بروز رسانی شوند. برای مبارزه با این ناپایداری و بی ثباتی BGP ، مفهومی بنام تعدیل مسیر[۵] ایجاد شده است. در اصل ، مکانیزم تعدیل مسیر به این شکل کار می کند: هر زمانی که یک مسیر کنار رفته و دوباره انتشار داده شد ، یک جریمه به آن اختصاص داده می شود و جریمه آن قرار داده شدن آن مسیر در لبه ناپایداری است (معمولا یک نشست eBGP). با دست و پا زدن بیشتر مسیر مذکور (یعنی تکرار عمل کنار رفتن و انتشار دوباره) ، جریمه بیشتری به مسیر اختصاص داده می شود. هنگامی که جریمه های اختصاص یافته به یک مسیر به سطح مشخصی برسد ، مسیر کنار گذاشته شده و تا مدت معینی برای انتشار مورد قبول واقع نخواهد شد. زمانی که این مسئله اتفاق بیافتد ، به مسیر مذکور ، مسیر تعدیل شده گفته می شود. مسیر تعدیل شده قبل از اینکه بتواند دوباره خود را به جدول مسیریاب[۶] BGP معرفی نماید ، باید یک دوره زمانی را بدون ایجاد ترافیک یا دریافت جریمه بیشتر تحمل کند. زمانی که مسیر مدت زیادی را بدون ایجاد ترافیک سپری کند (جریمه با گذشت زمان کاهش می یابد) ، دوباره اجازه می یابد تا به داخل جدول مسیریاب BGP بازگشته و دقیقا مانند مسیرهای دیگر رفتار کند. تعدیل مسیر راهی برای

---

[۴] متراکم کننده سطح بعدی (*Next Level Aggregator*)
[۵] *Route Dampening*
[۶] Router

هسته اینترنت در اختیار می گذارد تا بواسطه آن بتواند با ناپایداری ها تقابل کرده و باعث کاهش هزینه پردازش های سنگین و حجیم گردد. مسیریابی BGP نسخه ۶ (BGPv6) و IPv6 با جزئیات بیشتری در آخرین فصل بحث خواهد شد تا این مفهوم بهتر توضیح داده شود.

پیکربندی و اجرا

شماره گذاری مجدد سایت:

شماره گذاری مجدد سایت ، زمانی که نیاز به جایگزینی یا توزیع مجدد آدرسهای موجود باشد ، انجام می پذیرد. یک مثال گسترده در این مورد می تواند زمانی اتفاق بیافتد که یک تامین کننده جدید سرویس انتخاب می شود و بنابراین صدور آدرسهای جهانی جدید مورد نیاز خواهد بود. شماره گذاری مجدد سایت در IPv4 می تواند کابوس مدیریتی ایجاد کند ، اما IPv6 این مسئله را بطور بی اندازه ای ساده کرده است. در اینجا دو راه برای اجرای فرایند شماره گذاری مجدد سایت وجود دارد:

- اگر پیکربندی اتوماتیک نوع Stateful در حال استفاده باشد ، شماره های TLA و SLA می توانند در DHCPv6 قرار داده شده و در کل سایت توزیع شوند.
- اگر پیکربندی اتوماتیک نوع Stateless در حال استفاده باشد ، پیشوندهای شبکه جدید می تواند در مسیریابها قرار داده شده و در کل سایت توزیع شود.

ویژگی خوب معماری IPv6 اینست که شناسه رابط یا همان کارت شبکه بصورت یکسان و ثابت باقی می ماند و فقط پیشوندها تغییر می کنند. در حالت پیکربندی اتوماتیک IPv6 بصورت Stateful ، پیشوندها می توانند از یک نقطه مرکزی انتشار داده شوند.

حالا که ما تعدیل مسیر را درک کردیم ، می توانیم دومین فایده متراکم سازی را متوجه شویم. زمانی که سرویس دهنده بالادست ما ، این مسیر را برای ما متراکم کرده و این متراکم سازی را فقط به هم ردیف های خود اطلاع دهد ، این مجموعه تقریبا در تمام حالات بدون رابطه و نیاز به پایداری شبکه ما ، پایدار و فعال باقی می ماند. به این دلیل ، ما بصورت قطعی یقین پیدا می کنیم که سرویس دهنده های دیگر هرگز مسیرهای ما را در هرجایی از اینترنت ، تعدیل نخواهند کرد. همچنین هیچ مسیر مشخص بیشتری از آنچه ما استفاده می کنیم ، بیرون از سرویس دهنده بالادست ما نیاز به پخش شدن در بین هسته اصلی اینترنت ندارد. این نوع پایداری بهبود یافته در مسیریابی ، یک فایده اصلی و مهم برای متراکم سازی کامل در IPv4 و IPv6 است. بنابراین حالا تنها جایی که ما باید در مورد تعدیل شدن مسیر در آن نگران باشیم ، داخل شبکه سرویس دهنده بالادست خودمان است. خوشبختانه بدلیل اینکه ما در بسیاری از حالتها برای ارتباط با سرویس دهنده بالادست خود پول پرداخت می کنیم ، در واقع دریافت کمک برای رفع خطاها و حذف جریمه های ارائه شده به مسیرها برای ما راحت است. همینطور که می بینید ، انشعاب های زیادی برای متراکم سازی IPv6 نسبت به آنچه اول به چشم می خورد ، وجود دارد.

SLA (متراکم کننده سطح سایت) از بیشتر توانایی های NLA برخوردار است ، البته بجز اندازه آن: SLA معمولا به یک شبکه یا تامین کننده شبکه دارای شبکه کوچکتر گفته می شود. بهمین دلیل مجموعه های آدرس کمتری برای ارائه دادن مورد نیاز است. این مسئله باعث می شود که مقدار متراکم سازی ها در جدول مسیریابی مربوطه ، حتی در صورت دریافت جدول مسیریابی اینترنت بصورت کامل از تامین کننده بالادست ، در اندازه های کوچکتر نگهداری شود.

آدرس دهی ساده شده Host

همانطور که یاد گرفتیم ، IPv6 فضای آدرسی با حجم ۱۲۸ بیت را تعیین می کند. ۶۴ بیت اول برای شماره گذاری شبکه استفاده می شود ، و ۶۴ بیت آخر برای شماره گذاری سیستم یا همان Host. همچنین ۶۴ بیت آخر که مربوط به Host می شود ، از طریق آدرس سخت افزاری کارت شبکه سیستم (آدرس MAC) بدست می آید. ممکن است شما تعجب کنید که چگونه یک آدرس ۶۴ بیتی از آدرس MAC اخذ می شود ، در حالیکه خودِ آدرس MAC دارای طول ۴۸ بیت است؟ در این بخش ما نگاهی به چگونگی کسب آدرسها و پیشرفتهایی که در آینده در نتیجه طرح آدرس دهی IPv6 بدست خواهد آمد ، خواهیم انداخت.

طبق قرارداد و استانداردها ، هنگام اختصاص یک Host در IPv4 ، IPv4 به زیرشبکه های مشخص و آدرسهای Host براساس مقدار آدرسهای در دسترس ، تفکیک خواهد گردید. همچنین اولین آدرس بصورت معمول به مسیریاب برگزیده ، آدرسهای باقی مانده به Hostهای آن زیرشبکه ارائه شده و آخرین آدرس نیز برای آدرس فراگیر آن زیرشبکه رزرو می شود. در IPv6 وضعیت مقداری متفاوت است. با دارا بودن IPv6 می دانیم که طول آدرس Host ، ۶۴ بیت بوده و از طریق آدرس MAC اخذ می شود. با توجه به اینکه آدرسهای MAC امروزی معمولا ۴۸ بیتی هستند ، ما احتیاج به راهی داریم تا آدرس Host را بصورت ۶۴ بیتی بدست بیاوریم. راه حل این مشکل ، معبر آدرس MAC با مجموعه ای از بیتهای دارای تعاریف بهتر و درست تر است که بوسیله سیستمهای مسیریابی بر روی آن زیرشبکه (زیرشبکه مربوطه) شناسایی

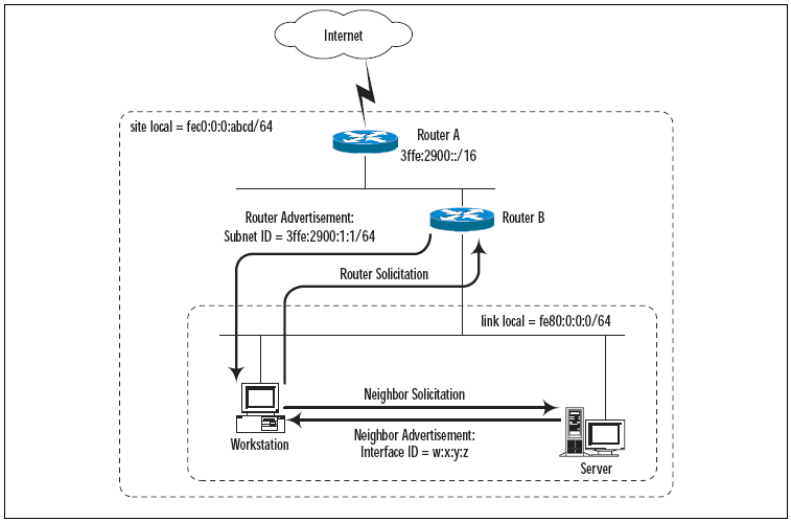
و آشکار می شود. ما از رشته 0XFF و 0xFE (در IPv6= :FF:FE) برای برقراری ارتباط در آدرس MAC بین شناسه کارخانه و شناسه فروشنده استفاده می کنیم. (آدرسهای MAC هم در بسیاری جهات مانند آدرسهای IP محول و ارائه شده اند ، بجز اینکه فضای آدرس MAC ارائه شده به کارخانه سازنده کارت رابط شبکه ، بیش از فضای آدرس IPv4 است که برای تامین کننده های ارتباط وجود دارد). با این راه (اضافه شدن رشته مذکور در بین دو قسمت) ، هر سیستم یک آدرس ۶۴ بیتی خواهد داشت که به آدرس MAC او وابسته است. علاوه بر این می دانیم بدلیل اینکه هر کارت رابط شبکه دارای آدرس MAC مخصوص بخود است ، آدرس ۶۴ بیتی MAC نیز ، باید در شبکه ارائه شده منحصر بفرد باشد.

یک بحث جالب توجه اینست که آیا نیازی به ۶۴ بیت شدن آدرسهای MAC برای توسعه گسترش IPv6 هست یا خیر؟ اگر احتیاج باشد تا آدرسهای MAC طولانی تر شوند (در صورتی که همه آدرسهای MAC استفاده شده باشند) ، به گزینه دیگری برای طولانی کردن آدرس نیاز می باشد که در این صورت بیش از 1.8E19 آدرس MAC بیشتر ، برای استفاده تامین خواهد شد ($2^{64} - 2^{48}$). بعلاوه ، اگر این مسئله بوقوع بپیوندد ، ممکن است ما دیگر نیازی به لایی گذاشتن و اضافه کردن رشته در بین آدرس MAC نداشته باشیم و این مورد متوقف گردد و آدرسهای MAC با طول ۶۴ بیت واقعی برای شناسه سیستم (Host) استفاده شود.

ساده سازی آدرس های پیکربندی خودکار

قبل از اینکه ما به سراغ جزئیات مربوط به پیکربندی خودکار برویم ، یک نوع آدرس بنام آدرس گروهی (Multicast) را مورد بررسی قرار می دهیم. یک آدرس گروهی آدرسی است که می تواند بصورت همزمان به بیش از یک سیستم اختصاص یابد. این آدرس با آدرس Anycast (که پکت ها را به نزدیکترین سیستم می رساند) متفاوت است. در حالیکه پکت های Multicast به سمت تمام سیستمهایی ارسال می شوند که یک آدرس یکسان به آنها اختصاص یافته است. این مسئله اساسی ترین تفاوت آدرس های گروهی با آدرسهای منحصر بفرد (Unicast یا بعبارت کاملتر GRU[۷]) است که در آن (آدرس های گروهی) امکان شماره گذاری بیش از یک سیستم (Host) با آدرسهای یکسان وجود دارد. بنابراین در آدرسهای نوع گروهی ، نیازی به منحصر بفرد بودن آن آدرس در محدوده عملکرد آن شبکه وجود ندارد. تمام سیستمهایی که یک آدرس Multicast به آنها اختصاص داده شده در داخل گروه Multicastای قرار می گیرند که در حال استفاده از آن آدرس هستند. در سیستمهایی که از مکانیزم صحبت گروهی استفاده می کنند ، ارسال و دریافت اطلاعات ، از بیش از یک سیستم انجام می پذیرد (هر کدام از اعضای گروه Multicast می تواند اطلاعات را ارسال یا دریافت کند). در این نوع آدرس دهی و مسیریابی نوع ارتباط و تراکنش ۱ به N و یا M به N استفاده می شود (زمانی که یک یا چند سیستم احتیاج دارند اطلاعات یکسانی را از بیش از یک مقصد بدست بیاورند).

اگر ما مفهوم Multicast را با مفهوم شناسه Host که از سخت افزار یک سیستم خاص بدست ما رسیده است ، یکی بکنیم ، می توانیم متوجه شویم که پیکربندی خودکار چگونه ممکن است. هنگامی که یک سیستم برای اولین بار روشن شده و وارد شبکه شد ، و متوجه گردید که با IPv6 ارتباط برقرار می کند ، یک پکت Multicast که مشخص و دارای استاندارد تعریف شده بر روی شبکه متصل به اوست ، ارسال می کند. این پکت به سمت یک آدرس Multicast محدوده محلی بنام آدرس SNM راهی می شود. هنگامی که مسیریاب ببیند این پکت وارد می شود ، با آدرس شبکه ای که بار ترافیک سیستم بر روی آن می افتد ، به آن پکت جواب می دهد. سیستم پکت را دریافت می کند و سپس شماره شبکه ای را که مسیریاب فرستاده است ، می خواند. سپس با استفاده از افزودن شناسه Host خود (که از آدرس MAC مربوط به رابط متصل به آن مسیریاب بدست آورده است) به آن شماره شبکه ، یک آدرس IPv6 به خود اختصاص می دهد. تصویر ۱-۲ مربوطه به پیکربندی خودکار را ببینید.



[۷] Globally Routable Unicast

اینگونه نیست که هیچ مداخله دستی توسط مدیر برای پیکربندی سیستم مورد نیاز نباشد (بهر حال ممکن است نیاز به پیکربندی دستی مسیریاب بر روی آن شبکه وجود داشته باشد) ، در عین حال این مسئله تضمین می کند که آدرس منحصر بفرد بوده و تکراری نباشد. سیستم برای دریافت و دراختیار داشتن یک آدرس منحصر بفرد گارانتی می شود ، بدلیل اینکه شماره شبکه بشکل منحصر بفرد توسط مسیریاب موجود در آن شبکه اختصاص داده می شود و شناسه Host (سیستم) نیز بدلیل استفاده از آدرس MAC منحصر بفرد ، منحصربفرد بوده و تکراری نخواهد بود. از این گذشته ، سیستم هم اکنون یک آدرس قابل مسیریابی در اختیار دارد که از طریق آن می تواند مسیر پیش فرضی را که برای خروج از آن شبکه نیاز دارد ، فرا گیرد. ما در بخش آخر به سراغ جزئیات بیشتری در مورد مفاهیم آدرس Multicast خواهیم رفت.

بهبود مقیاس پذیری در مسیریابی Multicast

حالا که در مورد آدرس دهی منحصر بفرد ، مزیت های اصلی آدرس دهی گروهی مطالعه کرده و بررسی مقیاس پذیری اندازه جدولهای مسیریابی در اینترنت با IPv6 ، اجازه دهید یک مقدار با جزئیات بیشتری در مورد آدرس Multicast بحث کنیم. ما این بحث را با بررسی مفهوم عمومی Multicast آغاز می کنیم. در ابتدا ، اینترنت یک شبکه پژوهشی بود که اطلاعات آن بین یک دانشگاه و دانشگاه دیگر جریان داشت. این مسئله تجارت بزرگی نبود ، و مشکلات تراکم باید تحمیل می شد و تاریخ اطلاعاتی که مردم ارسال می کردند مهم نبود ، بدلیل اینکه اطلاعات بصورت لحظه ای دریافتی نمی گردید. امروزه تولیدکنندگان ، بازرگانان و مصرف کنندگان در گستره وسیعی از اینترنت استفاده می کنند. ما هر روزه بیشتر و بیشتر ، رسانه های مختلفی را مانند تماسهای تلفنی ، کانالهای تلویزیونی و ... می بینیم که بر روی اینترنت فعالیت می کنند. همچنین همانگونه که می بینید ، ما احتیاج به رسانه ای داریم که با اطلاعات ارسالی را سریعتر به مقصد برساند ، بعنوان مثال مانند گروههای خبری که اطلاعات را به میلیونها نفر در روز می رسانند. این روند انتقال ۱ به N ، موجب نیاز برای نوع جدیدی از ارسال ترافیک گردیده است که در آن یک نفر بتواند یک بخش از اطلاعات را به چندین نفر ارسال نماید. در گذشته هنگامی که ما می خواستیم اطلاعاتی را به ده نفر از دوستانمان بفرستیم ، می بایست ده کپی از اطلاعات تهیه کرده و آنها را به هر نفر بصورت یک به یک و بنوبت ارسال می کردیم. بهرحال این نوع انتقال اطلاعات دارای منافع قابل قبولی است. بعنوان مثال فرض کنید ما یک برنامه رادیویی یا تلویزیونی داریم که می خواهیم آن را بر روی اینترنت ارسال نماییم. اگر بخواهیم این برنامه را برای ۱۰.۰۰۰ نفر پخش کنیم ، و همه آنها در یک زمان بخواهند آن را بصورت لحظه ای ببینند یا بشنوند ، ما باید اطمینان حاصل کنیم که پهنای باند بالادست ما برای پشتیبانی از ۱۰.۰۰۰ بار تبادل اطلاعات مذکور بصورت جداگانه توانایی لازم را داشته باشد. این مسئله ما را مجبور خواهد کرد تا هزینه مالی زیادی را برای تامین پهنای باند بالادست مورد نیاز صرف نماییم تا رضایت مشتریان خود را حفظ کنیم.

دروضعیت Multicast ما یک ارتباط ۱ به N بین مبدا و مقصد داریم. در IPv4 یک آدرس Multicast معمولا بعنوان یک آدرس گروه ارجاع داده می شود. این آدرس گروه ، هنگامی که بر روی یک سیستم و یا برنامه کاربردی موجود بر روی آن سیستم اِعمال گردید ، دلالت بر این دارد که ما علاقه داریم تا هر اطلاعاتی را که به آن آدرس ارسال می گردد ، دریافت کنیم. در IPv4 ، محدوده آدرس ۲۲۴.۰.۰.۰ تا ۲۳۹.۲۵۵.۲۵۵.۲۵۵ برای طراحی آدرسهای گروه Multicast استفاده می شود. هنگامی که کسی بخواهد خوراک Multicast را دریافت کند ، آن آدرس را به خود اختصاص داده (موقت یا دائمی ، بسته به موقعیت او) و بطور موثر به پکت هایی که به مقصد آن آدرس وارد می شوند ، گوش فرا می دهد.

مسیریابی برای Multicast پیچیده تر بوده و فراتر از محدوده این کتاب است ، اما شما می توانید اطلاعات خوبی در این زمینه در صفحه اصلی تالار گفتگوی Multicast به آدرس: www.ipmulticast.com و یا در گروههای کاری www.ietf.org بدست آورید.

با توجه به اهداف این کتاب ، فرض کنیم که Multicast هم اکنون در حال کار است. در این هنگام Multicast به ما کمک خواهد کرد تا پهنای باند خود را تا حد ممکن حفظ کنیم (بنابراین به ما اجازه خواهد داد تا فقط یک جریان داده را به سمت بیرون ارتباط اینترنت خود ارسال کنیم. زیرساخت اینترنت ، آن را تا اطمینان از ارسال به تمام مقصدهای مورد نظر ، تکثیر خواهد کرد). یک مثال خوب ، بویژه در مورد برنامه های کاربردی Multicast می تواند شبکه یک شرکت باشد. ممکن است ارسال یک سری اطلاعات به تمام کامپیوترهای کاربران و یا برگزاری یک ویدئو کنفرانس از طرف مدیر شرکت با کارکنان مورد نیاز باشد. در شبکه شرکت ، ما می خواهیم تا آنجا که ممکن است در هزینه برای تامین پهنای باند ، صرفه جویی کنیم ، البته بهمراه حفظ کیفیت و کارایی ساختار مسیریابی. Multicast دقیقا این مورد را برای ما تامین می کند. در عین حال در بسیاری از حالت ها ، ما فقط می خواهیم که جریان اطلاعات Multicast فقط به جاهایی برسد که نیاز می باشد. ما نمی خواهیم تمام اینترنت قادر به شنیدن صحبت مدیر با کارکنان شرکت باشند و باعث لو رفتن اطلاعات حساس شرکت گردد. برای تامین این مورد ، IPv6 در داخل خود مفهومی بنام محدوده Multicast[۸] دارد. بوسیله IPv6 ما می توانیم یک جریان مشخص Multicast را برگزینیم تا فقط در یک محیط معین و مشخص مسیریابی شده و هرگز اجازه خروج از آن محدوده را نداشته باشد. این گروه بندی بخوبی توسط تمام مسیریابی های موجود تشخیص داده خواهد شد و با استفاده از یک پیکربندی جزئی ، تضمین خواهد کرد که اطلاعات به بیرون از محدوده مسیریابی مذکور ارسال نشود. تصویر ۲-۲ قالب آدرس دهی Multicast را با جزئیات بیشتری نمایش داده است.

---

[۸] Multicast Scope

```
|   8    |  4 |  4 |                 112 bits                 |
+------ -+----+----+------------------------------------------+
|11111111|flgs|scop|                 group ID                 |
+--------+----+----+------------------------------------------+
```

همانطور که می بینید ، معماری و ساختار آدرس دهی Multicast تفاوت کمی با ساختار و قالب آدرس دهی منحصر بفرد (Unicast) دارد. توجه کنید که ۸ بیت اول بصورت یک مجموعه واحد هستند و این مسئله به دستگاه مسیریابی (مسیریاب) اجازه می دهد بلافاصله متوجه شود که طبیعت پکت Multicast است. چهار بیت بعدی برای flag (پرچم) استفاده می شود. در اینجا ، سه بیت اول در داخل flag رزرو بوده و تعریف نشده هستند ، بنابراین آنها باید صفر باشند (برخی از پروتکلهای عملیاتی در آینده از این سه بیت برای مرتب سازی ویژه برقراری ارتباط یا همان مکانیزم سیگنالینگ استفاده خواهند کرد). چهارمین بیت ، بنام بیت T (تحت RFC 2373) شناخته شده و برای تعیین اینکه آیا این آدرس Multicast بصورت دائمی (well-known) اختصاص یافته و یا بصورت موقت (transient) ، استفاده می گردد. بنابراین این فیلد به ما خوهد گفت که آیا آدرس Multicast مورد نظر بصورت دائمی (بعنوان مثال برای ایجاد یک ارتباط بین تمام سیستمهای موجود در یک دامنه) و یا بصورت موقت (بعنوان نمونه برای پخش یک مسابقه فوتبال در دوشنبه شب بر روی اینترنت) استفاده خواهد شد؟! فیلد بعدی ، فیلدی است که ما در اینجا دنبالش بودیم. فیلد scope (محدوده) تعیین خواهد کرد که پکت های Multicast چقدر می توانند دور شوند ، در چه محیطها و محدوده های مسیریابی می توانند حرکت کنند و آدرس چه گروهی را می توانند انتشار دهند. ارزش های داخل فیلد scope در جدول ۲-۲ نشان داده شده اند.

جدول ۲-۲ تعاریف scope

ارزش فیلد Scope	تعریف
0	رزرو شده
1	محدوده سیستم محلی
2	محدوده ارتباط محلی
3	اختصاص داده نشده
4	اختصاص داده نشده
5	محدوده سایت محلی
6	اختصاص داده نشده
7	اختصاص داده نشده
8	محدوده سازمان محلی
9	اختصاص داده نشده
A	اختصاص داده نشده
B	اختصاص داده نشده
C	اختصاص داده نشده
D	اختصاص داده نشده
E	محدوده جهانی
F	رزرو شده

بسته به اینکه ما چگونه آدرس Multicast خود را اختصاص می دهیم ، می توانیم کنترل کنیم که پکت های Multicast تا کجا می توانند دور شوند و اعلانیه های مربوط به مسیریابی آن گروه Multicast تا چه حجمی می توانند انتشار یابند. بعنوان مثال اگر شما دوست دارید منبعی از اطلاعات مانند یک تصویر را از شرکت خود انتشار دهید ، به شکلی که در تمام دنیا قابل دیدن باشد ، شما باید محدوده E (در حالت مبنای دو: 1110) را اختصاص دهید. همچنین ، اگر شما می خواهید یک گروه Multicast راه اندازی کنید تا شما و دیگر کارکنان شرکت بتوانید در یک ویدئو کنفرانس با هم ارتباط برقرار کنید ، شما باید scope ۵ (0101) یا ۲ (0010) را به آدرس خود اختصاص دهید تا همه کسانی که در آن شبکه محلی درگیر هستند ، با شما در ارتباط باشند. هم اکنون بجای اعتماد به مدیر شبکه برای اِعمال کردن فیلترهایی جهت محدود کردن و

مرزبندی محدوده ، ما می توانیم به ساختار نرم افزاری اعتماد کنیم تا ترافیک ما را در محدوده ای که می خواهیم نگه دارد. این یکی دیگر از فایده های IPv6 است؛ نه فقط برای مرزبندی خوب و مفید است ، بلکه نگهداری آن هم ساده و راحت می باشد.

آدرس Anycast

IPv6 یک نوع جدیدی از آدرس را با عنوان آدرس anycast تعیین می کند. اگرچه این نوع از آدرس در سبک محدودی در IPv4 مطرح شده ، اما IPv6 این نوع آدرس را بشکل عملیاتی کامل کرده و این باعث بالارفتن راندمان مسیریابی شده است. در این بخش ما نگاهی به جزئیات بخشی از ویژگیهای آدرس anycast خواهیم انداخت و در مورد برخی از برنامه های کاربردی اینترنت IPv6 در آینده بحث خواهیم کرد.

آدرس anycast یک آدرس IPv6 است که به گروهی متشکل از یک سیستم یا تعدادی سیستم که همه دارای یک هدف یا عملکرد مشترک هستند ، اختصاص داده می شود. هنگامی که پکتها به سمت یک آدرس IPv6 از نوع anycast فرستاده شدند ، مکانیزم مسیریابی تعیین خواهد کرد که کدامیک از اعضای گروه ، پکت را از طریق نزدیک ترین سیستم به مبدا (که بوسیله IGP شبکه طی سوالی مشخص می گردد) دریافت خواهد کرد. IGP یا پروتکل گذرگاه داخلی[۹] (شبکه)؛ یک پروتکل مسیریابی است که شما می توانید از آن در محدوده مسیریابی داخلی خود استفاده کنید. اگرچه آدرس مقصد هردو پکت Multicast و anycast بیش از یک سیستم است ، اما آدرس anycast برای انتقال اطلاعات بصورت ۱ به ۱ بکار می رود ، در حالیکه آدرس دهی Multicast هنگامی استفاده می شود که انتقال اطلاعات به سمت چندین مقصد مورد نیاز باشد. اجازه دهید به دو فایده اصلی ساختار آدرس دهی anycast بپردازیم:

اول؛ اگر شما بخواهید به نزدیکترین سیستم در گروه بروید ، و مهم نباشد که با کدامیک از اعضای گروه اطلاعات خود را تبادل کنید ، شما می توانید با استفاده از برقراری ارتباط با نزدیکترین سیستم به خود (IGP-wise) که عضو گروه است ، در استفاده از زمان صرفه جویی نمایید.

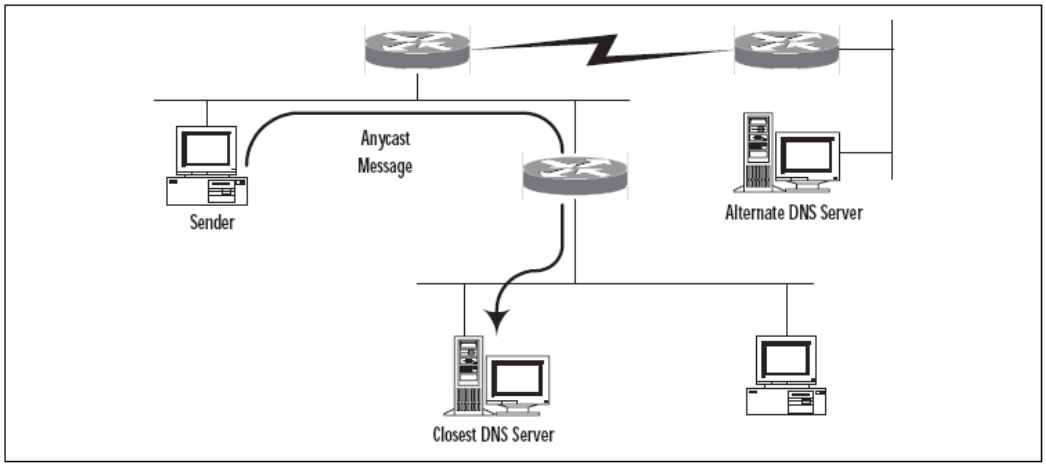
دوم؛ برقراری ارتباط با نزدیکترین آدرس anycast که عضو گروه باشد ، باعث صرفه جویی در پهنای باند می شود. بدلیل اینکه فاصله ای که پکت طی می کند در بسیاری از حالت ها کوتاه می شود. بنابراین نه فقط anycast می تواند در زمان شما صرفه جویی کند ، علاوه بر این در هزینه مربوط به پهنای باند شما نیز ، باعث صرفه جویی خواهد شد. آدرس anycast مجموعه بیتهای خود را برای تعریف کردن آنها در اختیار ندارد ، بجای آن ، آدرس دهی anycast از طریق آدرس های scope شده و یا آدرس های منحصربفرد انجام می شود. از نظر سیستمی که با استفاده از IPv6 صحبت می کند ، تفاوتی بین آدرس anycast و آدرس منحصربفرد (Unicast) وجود ندارد. تنها تفاوت اینکه ممکن است سیستمهای دیگری نیز با همان محدوده (scope) آدرس منحصربفرد و در همان ناحیه ای که آن scope تعریف شده است ، شماره گذاری شده باشند (برای مثال ، شما ممکن است بیش از یک کامپیوتر که دارای آدرس anycast از نوع سایت محلی است ، در یک ناحیه مشخص داشته باشید). حالا که تفاوتهای موجود بین آدرسهای anycast و multicast را درک کردیم ، اجازه دهید نگاهی به برخی استفاده های ممکن از آدرسهای anycast بیاندازیم. یک برنامه کاربردی که از ارتباط anycast بهره می برد ، می تواند به سیستم تامین نام دامنه (DNS) کمک کند. اگر ما بخواهیم خدمات DNS به مردم یا مشتریانمان ارائه کنیم ، بعنوان ارائه دهنده خدمات سطح بالا احتیاج خواهیم داشت DNS خود را به شکلی تنظیم کنیم که بتواند تعداد زیادی از تقاضاها را از بخشهایی که ما به آنها سرویس می دهیم ، مدیریت کند. به این دلیل ، بسیار موثرتر خواهد بود اگر چندین سرور DNS ایجاد کنیم و آنها را در مناطق مختلف جغرافیایی پراکنده سازیم. این نوع راه اندازی DNS ، علاوه بر ایجاد تعادل و بالانس بین سرویس دهی این سرورها ، اجازه اصلاح خرابی را هنگامی که یک سرور DNS بدلیل خرابی شبکه غیرقابل دسترس می شود ، فراهم می سازد. علاوه بر این ما نمی خواهیم که مشتریانمان آدرسهای IP متفاوت و مختلفی برای اشاره به DNS سرورها ، به سیستم خود اختصاص دهند. همچنین راهی نیاز داریم تا یک یا دو آدرس IP برای کلیه سرویسهای DNS در تمام مناطق مختلف جغرافیایی استفاده شود. یک راه انجام اینکار اینست که به هر سرور DNS که دارای پیکربندی و اطلاعات یکسان است ، آدرس IP یکسان اختصاص دهیم. سپس اگر ما مسیرهای هرکدام از این سرورهای DNS را به جدول مسیریابی زیرساخت شبکه تزریق کنیم ، در صورت ارسال پیغامهای تقاضا و پرس و جو توسط یک کاربر به سمت سرور DNS ما ، تقاضای مورد نظر به سمت DNSسرورهایی ارسال خواهد شد که از جهت جغرافیایی نزدیکترین گزینه به ما باشند. این مسئله به ما اجازه خواهد داد که بارگذاری سرویس تامین نام را بین چندین سرور DNS تقسیم کرده و از حمل شدن و بارگذاری تعداد زیادی از تقاضاهای پرس و جو بر روی زیرساخت شبکه مان جلوگیری کنیم. بنابراین با استفاده از این نوع گسترش ، ما هم می توانیم در زمان مورد نظر برای مشتریانمان (سرورهای DNS نزدیک هستند ، بنابراین ارسال اطلاعات زمان کمتری می گیرد) و هم در هزینه خود (هزینه پهنای باند اضافی) صرفه جویی کنیم. بدلیل اینکه DNS یک پروتکل نوع UDP (یک سویه) است ، تراکنش های بین سرویسهای DNS و ایستگاههای کاری ، سریع و کوتاه هستند و نیازی به پیگیری و کنترل تشخیص خطا و ... نداریم. هنگامی که ما می خواهیم یک نام سیستم (Host) را از طریق سرویس DNS بدست آوریم ، یک پکت به سمت سرور DNS فرستاده شده وآدرس مربوطه را بهمراه نام دامنه اینترنتی آن تقاضا می کند و در مقابل یک واکنش بهمراه جواب ، بر می گردد. این مسئله آدرس دهی

---

[۹] Interior Gateway Protocol

anycast را برای این نوع برنامه کابردی ، قابل دوام می سازد. یک مثال از anycast در تصویر ۳-۲ نمایش داده شده است. برای مطالعه بیشتر می توانید آدرس www.globecom.net/ietf/draft/draft-catalone-rockell-hadns.00.txt را ببینید.

تصویر ۳-۲ پیغام Anycast



طراحی و اجرا

چه برنامه های کاربردی بهترین کاندیدا برای استفاده از Anycast هستند؟

برخی از برنامه های کاربردی ممکن است خیلی برای گسترش و توسعه anycast مناسب نباشند. برای مثال ، برنامه های کاربردی با مبنای TCP که از آدرس دهی anycast استفاده می کنند ، قابلیت اصلاح خرابی را تامین نمی کند ، گزینه ای که در مثال قبلی تامین می شد. هنگامی که ما برنامه های با مبنای UDP را استفاده می کنیم ، هیچ اطلاعات ترتیبی برای پیگیری وجود ندارد. اما با TCP به یک مشکل بر می خوریم: هنگامی که یک مشکل شبکه اتفاق می افتد و کاربران در میانه یک نشست و ارتباط TCP با یک سیستم anycast هستند ، تمام مرتب سازی TCP هنگامی که ترافیک برای رسیدن به نزدیکترین سرور بعدی ، مسیریابی دوباره می شود ، بهم خورده و خراب خواهد شد. در ترافیک وب که تا حد زیادی بر مبنای TCP است ، کاربر نیاز خواهد داشت زمانی که خرابی در شبکه اتفاق بیافتد ، حداقل یک بار صفحه را دوباره بارگذاری کند.

سرایند موثر

سرایند جدید IPv6 نسبت به سرایند IPv4 ساده تر و موثرتر شده است. سرایند جدید فقط دارای شش فیلد و دو آدرس است ، در حالیکه IPv4 دارای ده فیلد ، دو آدرس و فیلد گزینه های طول متغیر بود. تصویر ۴-۲ قالب بندی سرایند IPv6 را نمایش می دهد.

تصویر ۴-۲ سرایند IPv6

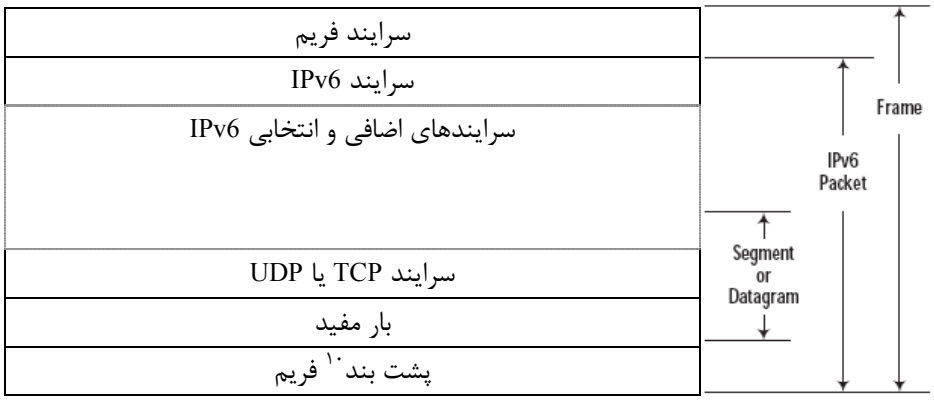
برچسب جریان		کلاس ترافیک	نسخه
محدوده پرش	سرایند بعدی	طول بار مفید	
آدرس مبدا			
آدرس مقصد			

سرایند IPv6 تسهیلات زیر را تامین می کند:

- **قالب ساده شده:** سرایند IPv6 دارای یک قالب ثابت و با تعداد فیلدهای کمتر است. فیلد گزینه های طول متغیر محدود شده است. فیلدهای دیگر IPv4 محدود شده و یا به سرایندهای اضافی انتخابی تغییر پیدا کرده اند. نیازی نیست تا تمام سرایندهای اضافی انتخابی بوسیله هر سیستم پردازش شوند. این قالب ساده شده بار کاری پروتکل IPv6 را کاهش داده و اجازه انعطاف پذیری بهتری را می دهد.

- **عدم آزمایش خطای سرایند:** فیلد تشخیص خطای IPv4 محدود شده است. این فیلد بدلیل اینکه شبکه های اولیه دارای سرعت کم و ارتباطات نامطمئن بودند و جهت تضمین درستی اطلاعات نیاز بود که در هر پرش از یک مسیریاب ، مکانیزم تشخیص خطا محاسبه می گردید ، در IPv4 وجود داشت. ارتباطات شبکه های امروزی سریع و بصورت فزاینده ای قابل اطمینان هستند و فقط سیستم ها احتیاج به چک کردن و تشخیص خطای اطلاعات را دارند ، نه مسیریابها.
- **عدم وجود فرایند قطعه قطعه کردن اطلاعات از یک پرش به پرش دیگر:** در IPv4 ، مسیریابها پکت هایی را که برای تبادل از رابطهای خروجی خود بزرگ هستند ، تکه تکه می کردند تا به قطعات کوچکتر تقسیم شوند. این مسئله بصورت قابل توجهی باعث افزایش بارِ کاری جهت پردازش IPv4 می شد. در IPv6 فقط ممکن است یک سیستم یک پکت را خرد کند. برای کمک کردن به سیستم ، IPv6 شامل عملکردی می شود که باعث می گردد حداکثر اندازه واحد انتقال اطلاعات (MTU) از مبدا به مقصد ، تشخیص داده شود. تصویر ۵-۲ یک فریم انتقالی نوع TCP را که از IPv6 استفاده می کند ، نشان می دهد.

تصویر ۵-۲ فریم انتقالی با استفاده از IPv6



امنیت

یکی از اهداف طراحان IPv6 ، پشتیبانی از تامین امنیت بر مبنای رمزنگاری بود. IPv6 امنیت را در داخل ساختار خود با استفاده از ارائه دو سرایند اضافی و انتخابی جدید ، کامل کرده است؛ سرایند تصدیق هویت (AH[۱۱]) و سرایند بار مفید امنیتی رمزنگاری شده (ESP[۱۲]). این دو سرایند می توانند با یکدیگر یا بصورت جداگانه جهت پشتیبانی از انواع وظایف امنیتی استفاده شوند.

- **سرایند تصدیق هویت:** قلب و مرکز سرایند تصدیق هویت فیلدی بنام ICV[۱۳] (ارزش سنجش درستی) می باشد. ICV بوسیله مبدا محاسبه گردیده و دوباره برای تایید ، توسط مقصد نیز محاسبه می گردد. این فرایند هر دو هدف تصدیق هویت مبدا اطلاعات و درستی اطلاعات را (بصورت یکسویه) تامین می کند. درستی اطلاعات یکسویه ایجاد تغییرات بر روی بار مفید را تشخیص می دهد. تصدیق هویت مبدا اطلاعات ، یگانگی مبدا اطلاعات را بررسی می کند. AH یا همان تصدیق هویت ، شامل فیلد دیگری نیز بنام شماره ردیف[۱۴] می شود که برای تشخیص حملات پکت های پاسخ (Replay Packet) استفاده می شود که باعث انسداد یا پایین آمدن شدید میزان دریافت اطلاعات توسط منابع سیستم می گردد. بوسیله بررسی شماره ردیف ما می توانیم دریافت پکت های IP تکراری را که دارای شماره ردیف یکسان هستند ، تشخیص دهیم.
- سرایند ESP (بار امنیتی رمزنگاری شده): IPv6 می تواند محرمانه بودن اطلاعات را با استفاده از رمزنگاری بار اطلاعات ، تامین نماید. سرایند ESP مربوط به IPv6 ، شامل یک فیلد بنام SPI[۱۵] (شاخص پارامتر امنیتی) می گردد که به یک رابط و پیوند امنیتی اشاره می کند و از طریق آن به مقصد می گوید که بار مفید و پکت ، چگونه رمزنگاری شده است. سرایندهای ESP ممکن است برای ارتباطات دو سره (End-to-End) و یا برای تونل گذاری استفاده شوند. در هنگام تونل گذاری ، سرایند اصلی IPv6 و بار مفید اطلاعات یا همان Data ، هر دو رمزنگاری شده و توسط سرایندهای بیرونی IPv6 و ESP ، پوشانده می شوند. نزدیک مقصد ، یک دروازه امنیتی سرایندهای بیرونی را دور انداخته و سپس اطلاعات و سرایند اصلی IPv6 را از حالت رمزنگاری خارج می کند. این نوع

---

[۱۰] Trailer
[۱۱] Authentication Header
[۱۲] Encrypted Security Payload
[۱۳] Integrity Check Value
[۱۴] Sequence Number
[۱۵] Security Parameter Index

پوشش گذاری باعث ایجاد جریان ترافیک محرمانگی محدودتر و کمتری می شود ، بدلیل اینکه یک بررسی کننده ترافیک فقط سرایندهای بیرونی را می بیند و کاری با اطلاعات و سرایند اصلی IPv6 که رمزنگاری شده اند ، ندارد.

تحرک و پویایی

تعداد کاربران اینترنت که بصورت سیار از اینترنت استفاده می کنند در حال رشد است. این مسئله باعث ایجاد یک توانایی مهم در IPv6 جهت پشتیبانی از سیستمهای متحرک مانند لپ تاپ ها شده است. IPv6 چهار مفهوم کلیدی را برای پشتیبانی از محاسبات و ارتباطات متحرک معرفی کرده است:

- آدرس Home
- آدرس Care of (واسطه)
- Binding[۱۶]
- Home agent[۱۷]

در IPv6 ، سیستمهای متحرک بوسیله آدرس home ، صرف نظر از اینکه آنها در آن لحظه کجا هستند ، شناخته می شوند. هنگامی که یک سیستم متحرک از یک زیرشبکه به زیرشبکه دیگر تغییر مکان دهد ، باید از طریق فرایند پیکربندی خودکار ، یک آدرس Care of کسب کند. پیوند بین آدرس home و آدرس care of ، با عنوان binding شناخته می شود. زمانی که یک سیستم متحرک یک آدرس care of کسب می کند ، به home agent خود (دلال یا واسطه خانه) توسط پیغام بهنگام سازی اتصال[۱۸] اطلاع می دهد. Home agent نقشه ارتباطی بین آدرس های home و آدرسهای care of را تحت عنوانی بنام Binding Cache نگهداری می کند. توسط ارسال پکت به آدرس home یک سیستم متحرک ، می توان به آن دسترسی یافت یا وضعیت دسترسی به آن را تست نمود. اگر یک سیستم متحرک به شبکه خانگی خود متصل نباشد ، home agent پکت را به سمت سیستم متحرک از طریق آدرس care of آن ارسال خواهد کرد. سپس سیستم متحرک یک پیغام بهنگام سازی اتصال به سیستم مبدا خود بر می گرداند. سیستم مبدا ، اطلاعات binding cache خود را بهنگام سازی کرده و پکت های بعدی را بصورت مستقیم به سمت سیستم متحرک ، از طریق آدرس care of او ، ارسال می نماید. فقط اولین پکت بین مبدا و سیستم متحرک از طریق home agent تبادل می شود ، و تمام پکت های بعدی بصورت مستقیم و بدون واسطه بین آن دو مبادله خواهند گردید. این مکانیزم راهنمایی توسط IPv6 ، قابلیت توسعه و مقیاس پذیری را برای پشتیبانی از تحرک و پویایی سیستم ها ، تضمین می کند. پیشنهاد ارائه شده برای استفاده IPv6 در موبایل ها را می توان بعنوان مثالی برای عملکرد سیستم های متحرک معرفی نمود. هنگامی که یک دستگاه تلفن همراه مجهز به IPv6 ، برای دریافت تماس ها فعال گردید ، یک آدرس Care of از گوشی که داخل آن است ، دریافت می کند. سپس تلفن همراه ، خود را به home agent خود (که توسط مرکز مخابراتی نگهداری می شود) معرفی می کند. تماس های دریافتی بوسیله home agent به سمت تلفن همراه مذکور از راه آدرس Care of او ارسال می شوند و تلفن همراه نیز پیغام بهنگام سازی اتصال را به تلفن مبدا ارسال می کند. تلفن مبدا یا مرکز مخابراتی مبدا ، اطلاعات binding cache خود را بهنگام سازی کرده و سپس پکت های بعدی را از طریق آدرس Care of کسب شده ، بشکل مستقیم به تلفن همراه ارسال می کنند. اگر سیم کارت به گوشی دیگری منتقل شود ، یک آدرس Care of دیگر کسب خواهد شد. پس از آن پیغامهای بهنگام سازی اتصال به home agent و تلفن یا مرکز مخابراتی مبدا فرستاده خواهند شد. پکت های بعدی مستقیم و از طریق آدرس جدید Care of به تلفن همراه ارائه خواهند گردید. احتمالا آدرس های Care of قبلی در داخل binding cache نگهداری خواهند شد تا اجازه دهد تلفن همراه پکت ها را از گوشی قبلی (در صورت وجود مجوز) بوسیله ایجاد تغییرات در شدت سیگنال دریافت کند.

کارایی

معماری IPv6 مزایایی را در مورد کارایی شبکه و مقیاس پذیری آن ارائه می کند. این مزایا عبارتند از:

- **کاهش بار ترجمه آدرس:** برای چیره شدن بر محدودیت فضای آدرس ، IPv6 اجازه استفاده می دهد از آدرسهای خصوصی که فقط برای استفاده در داخل شبکه های خصوصی ایجاد شده اند را می دهد. ترجه آدرس های شبکه (NAT) باید جهت مسیریابی آدرسهای خصوصی به سمت مجموعه محدودی از آدرسهای معتبر و عمومی استفاده گردد. این ترجمه آدرس باعث افزایش بار کاری مربوط به کارایی شبکه می شود. در IPv6 ترجمه آدرس برای غلبه بر محدودیت فضای آدرس ، لازم نیستو

---

[۱۶] اتصال
[۱۷] واسط یا دلال خانه
[۱۸] Binding Update Message

- **کاهش بار مسیریابی:** بسیاری از مجموعه های آدرس IPv4 (مانند مجموعه های آدرس کلاس C) بدون توجه به تراکم ، به کاربران اختصاص داده شده اند. نتیجه این مسئله وجود زیرشبکه های جداگانه است که هرکدام به جدول مسیریابی داخلی جداگانه ای نیاز دارند. آنها نمی توانند متراکم شده و بعنوان یک شبکه واحد عمل کنند. این مسئله به شدت باعث افزایش حجم جدول مسیریابی و در نتیجه منجر به بالا رفتن بار کاری شبکه می شود. در مقابل ، آدرسهای IPv6 از طریق تامین کننده های سرویس اختصاص داده می شوند تا باعث تشویق جهت آدرس دهی سلسله مراتبی شوند و در نهایت ، کاهش بار مسیریابی را موجب گردند.
- **افزایش ثبات و پایداری مسیر:** در IPv4 آویختگی مسیر رخ می دهد. این مورد زمانی اتفاق می افتد که یک ارتباط نامطمئن بصورت مرتب قطع و وصل شده و باعث انتشار مکرر خود شود. انتشار و پردازش این تغییرات مسیریابی ، باعث قرارگیری بار اضافی بر روی زیرساخت اینترنت می شود. در IPv6 ، یک تامین کننده سرویس ، به تنهایی می تواند مسیرهای بسیاری از شبکه ها را متراکم کرده و باعث گردد که آویختگی مسیر بصورت جداگانه و فقط در آن شبکه اجرا گردد. تغییرات مسیریابی فقط احتیاج دارند بین مسیریابهای هم ردیف در آن شبکه انتشار یابند.
- **کاهش فریم های فراگیر[۱۹]:** پروتکل استخراج آدرس (ARP) در IPv4 ، از پیغامهای فراگیر برای ارتباط دادن آدرسهای لایه Data Link (لایه انتقال داده) با آدرسهای لایه Network (لایه شبکه) استفاده می کند. IPv6 از مکانیزم اکتشاف همسایه (Neighbor Discovery) برای اجرای همان کار در طی فرایند پیکربندی خودکار و البته بدون استفاده از پیغامهای فراگیر ARP ، استفاده می کند.
- **Multicast های محدود شده:** در IPv6 ، یک آدرس Multicast شامل فیلدی بنام Scope است که می تواند پکت ها را به یک سیستم ، یک ارتباط و یا یک سازمان محدود کند. در IPv4 اجرا کردن این محدودیت ، نیاز به اجرای فیلترها و فضای آدرس خصوصی دارد.
- **سرایند موثر:** درمقابل ۱۲ فیلد طول ثابت و یک فیلد طول متغیر در سرایند IPv4 ، سرایند موثر و بهینه شده IPv6 ، فقط دارای هشت فیلد طول ثابت است. برای اجرای عملکردهای اضافی ، سرایندهای اضافی می توانند استفاده شوند ، آن هم به شکلی که نیازی به چک شدن آنها توسط مسیریابهای میان راه نیست. این نوع ساختار سرایند بهینه شده ، باعث کاهش بار شبکه خواهد شد.
- **خرد نشدن داده توسط سیستمهای میانی:** در IPv4 هنگامی که یک سیستم میانی یا یک مسیریاب ، پکت هایی را دریافت می کرد که برای ارسال و عبور دادن از خود دارای حجم خیلی بزرگی بود ، ممکن بود آنها را خرد کرده و به قطعات کوچکتر تقسیم کند. این عملکرد پرهزینه در IPv6 انجام نمی پذیرد. بجای آن ، فقط سیستم مبدا عمل خرد کردن پکت ها را انجام خواهد داد. برای کمک به سیستم مبدا ، IPv6 عملکردی را بنام اکتشاف مسیر MTU را اجرا می کند تا از طریق آن بتواند اندازه MTU برای مسیر مبدا تا مقصد را تعیین نماید.
- **عدم آزمایش خطای سرایند:** سرایند IPv4 شامل فیلدی بنام Checksum (تشخیص خطا) می شود که اجازه تشخیص خطا در هر پرش در شبکه را می دهد. برای محدود کردن بارِ کاری مربوط به پردازش تشخیص خطا در هر پرش ، IPv6 فیلد Checksum را محدود کرده است. رسیدگی و بررسی Checksum در مبدا و مقصد بوسیله پردازش لایه بالاتر مانند TCP یا UDP اجرا می شود. در حقیقت در IPv6 ، وظیفه Checksum فقط در مبدا و مقصد انجام می پذیرد و باعث کاهش ترافیک شبکه می شود.

مقایسه IPv6 با IPv4

IPv6 در بسیاری جهات با IPv4 متفاوت است. اجازه دهید در اینجا بیشترین تفاوت های مهم بین دو نسخه این پروتکل را بررسی نماییم. این کار اجازه خواهد داد تا کسانیکه با IPv4 کار می کنند بتوانند بسادگی تفاوت های اصلی نسخه جدید پروتکل اینترنت را تشخیص دهند. مهمترین تفاوت ها اینها هستند:

- ساختار سرایند بهینه شده
- برچسب جریان
- آدرس شبکه ۱۲۸ بیتی
- محدودیت تشخیص خطای سرایند
- خرد شدن داده فقط توسط سیستم مبدا
- سرایندهای اضافی

---

[۱۹] Broadcasts

- امنیت داخلی

ساختار آدرس دهی

آدرس منحصر بفرد IPv6 ۱۲۸ بیت طول دارد و شامل پیشوند زیرشبکه (Subnet) و یک شناسه کارت شبکه می شود. به جهت متراکم سازی آدرسهای منحصربفرد جهانی (GRU) ، هر دو پیشوند زیرشبکه و شناسه کارت شبکه ، بصورت مجموع ، ۶۴ بیت طول دارند که در تصویر ۶-۲ نمایش داده شده است. پیشوند زیرشبکه شماره شبکه ای است که به ارتباط اختصاص داده شده است. شناسه کارت شبکه از آدرس MAC سیستم مشتق می شود. در جریان پیکربندی خودکار آدرس IPv6 ، سیستم ، شناسه کارت شبکه خودش را از حافظه ROM خود و همچنین ارسال تقاضا به مسیریاب محلی یا سرویس دهنده DHCPv6 برای یک پیشوند زیرشبکه ، تامین می کند.

تصویر ۶-۲ قالب بندی و ساختار آدرس دهی IPv6

64 bits	64 bits
Subnet Identifier	Interface Identifier

آدرسهای MAC امروزه ، فقط ۴۸ بیت طول دارند ، بنابراین ۱۶ بیت در شناسه کارت شبکه رزرو شده است. سازمان IEEE یک آدرس MAC جدید را با طول ۶۴ بیت ارائه کرده که با عنوان EUI-64 نامگذاری شده است.

در مقابل ، آدرسهای IPv4 ، فقط ۳۲ بیت طول دارند. همچنین این آدرسها دارای یک شماره زیرشبکه و یک شماره سیستم می شوند.

آدرسهای IPv4 از طریق آدرس MAC کسب نمی شوند و مدیران شبکه هر دو آدرس زیرشبکه و سیستم را به هر سیستم اختصاص می دهند.

مدیریت آدرس

پیشوند ۶۴ بیتی زیرشبکه در یک آدرس منحصربفرد IPv6 ، به پنج فیلد تقسیم شده است. این پنج فیلد در تصویر ۷-۲ نمایش داده شده است.

3	13	8	24	16
FP	TLA ID	RES	NLA ID	SLA ID

اولین فیلد ، فیلد FP یا فیلد قالب پیشوند است ، که یک آدرس منحصربفرد (GRU) را با ارزش مبنای دو 001 شناسایی می کند. سومین فیلد برای استفاده در آینده ذخیره شده است. دو فیلد دیگر بنامهای TLA ID و NLA ID وجود دارند که کلید درک پشتیبانی IPv6 از سلسله مراتب آدرس دهی قابل تراکم هستند. TLA ID شناسه متراکم سازی سطح بالا است. آدرسهای جهانی IPv6 به ارائه دهندگان سرویس یا همان سازمان های TLA اختصاص داده خواهد شد. سازمانهای TLA فضای آدرس دهی را به سازمانهای زیر مجموعه خود بنام NLA اختصاص خواهند داد. این نوع ساختار سلسله مراتبی برای اختصاص فضای آدرس ، باعث متراکم سازی آدرسها شده و حجم جدول های مسیریابی اصلی را کاهش خواهد داد.

در طرف مقابل ، آدرسهای IPv4 معمولا با استفاده از مجموعه های CIDR[۲۰] اختصاص داده می شوند. هر مجموعه CIDR شامل چندین آدرس کلاس C می شود. هر مجموعه کلاس C می تواند تقریبا ۲۵۴ سیستم را آدرس دهی نماید. متاسفانه ، مجموعه های CIDR اختصاص داده شده به سازمانهای مختلف ، نمی توانند بسادگی متراکم شوند. علاوه بر این هر مجموعه CIDR ممکن است به یک جدول مسیریابی جداگانه ای در داخل مسیریاب اصلی نیاز داشته باشد. بهمین دلیل ، انتشار مجموعه های CIDR باعث رشد انفجاری حجم جدولهای مسیریابی اصلی می شود.

برای مدیران شبکه محلی ، یک فیلد بسیار مهم بنام شناسه متراکم سازی سطح سایت (SLA[۲۱]) وجود دارد. برخلاف TLA و NLA ، شناسه SLA معمولا به سازمانهای زیرمجموعه با یک ارزش از پیش تعریف شده ، محول نمی شود. با توجه به اطلاعات ثبت شده در RFC شماره ۲۳۷۴ ، شناسه SLA اجازه می دهد یک سازمان بتواند با استفاده از آن ساختار آدرس دهی و زیرشبکه های داخلی خود را تعیین کند.

[۲۰] Classless InterDomain Routing
[۲۱] Site-Level Aggregation

بیت متعلق به SLA که برای شناسه زیرشبکه استفاده می شود ، می تواند تا ۶۵۵۳۵ زیرشبکه را پشتیبانی کند که برای بزرگترین سازمانها نیز کافی است. برای سازمانهای بزرگتر که محدوده آدرس بیشتری نیاز باشد ، می توان یک بخش کوچکتری از NLA را نیز درخواست نمود.
یک مدیر شبکه نیازی ندارد تا در مورد اختصاص شناسه های زیرشبکه و سیستم در IPv6 نگرانی داشته باشد ، در صورتی که در IPv4 این نگرانی وجود دارد. در IPv4 هر دو شناسه سیستم و زیرشبکه ، معمولا از یک مجموعه محدود شده از آدرسهای قابل دسترس بدست می آیند. یک مدیر شبکه IPv4 برای تامین تعداد زیرشبکه مورد نیاز ، معمولا بیتهای سیستم (Host) را به زیرشبکه ها قرض می دهد. در IPv6 ، نیمه بالایی (نیمه اول) ساختار آدرس دهی IPv6 ، فضای آدرس دهی کافی را برای شناسه های زیرشبکه تامین می کند. در یک فیلد مجازی پایدار و البته جداگانه ، شناسه Host (سیستم) IPv6 بصورت کاملا منحصربفرد برای هر سیستم و بوسیله یک فرایند جداگانه پیکربندی خودکار ، ایجاد می شود.
IPv6 از یک طریق دیگر هم به سبک شدن مسئولیت مدیر شبکه کمک می کند؛ آدرسهای قابل تراکم منحصربفرد (GRU) یا همان آدرسهای Unicast ، هنگامی که برای دسترسی به شبکه های بیرونی مانند اینترنت استفاده می شوند ، نیازی به ترجمه ندارند. در IPv4 هنگامی که آدرسهای عمومی (آدرسهای Valid) در دسترس نباشد ، از فضای آدرس خصوصی استفاده خواهد شد. این آدرسهای خصوصی باید به یک مجموعه از آدرسهای جهانی ترجمه شوند تا بتوان با شبکه های بیرونی مانند اینترنت ارتباط برقرار نمود. ساختار ترجمه آدرس IPv4 ، شامل دو تکنولوژی بنامهای NAT[۲۲] و PAT[۲۳] می باشد. IPv6 بصورت مجازی نیاز به ترجمه آدرس را جهت دسترسی به شبکه های بیرونی ، محدود می کند. جدول ۳-۲ کاهش بار و مسئولیت مدیریتی آدرس را برای مدیران شبکه IPv6 نشان می دهد.

جدول ۳-۲ مقایسه مدیریت آدرس

موضوع مدیریت آدرس	مجموعه آدرس خصوصی کلاس A در IPv4	آدرس منحصربفرد قابل تراکم در IPv6 (Unicast)
طول آدرس	۳۲ بیت	۱۲۸ بیت
طول فیلد از پیش تعریف شده توسط بالادست (طول شناسه شبکه)	۸ بیت	۴۸ بیت
طول فیلد آدرس دهی محول شده (شناسه زیرشبکه + شناسه سیستم)	۲۴ بیت	۸۰ بیت
طول شناسه سیستم (Host)	۲۴ – بیتهای زیرشبکه	۶۴ بیت
طول شناسه زیرشبکه (Subnet)	۲۴ – بیتهای سیستم	۱۶ بیت (شناسه SLA)
اختصاص آدرس سیستم برای شناسه زیرشبکه	بله	خیر
تعیین شناسه زیرشبکه	بله	بله
تعیین شناسه سیستم	بله	خیر
نیاز به ترجمه آدرس (NAT/PAT)	بله	خیر

مقایسه سرایند

IPv6 یک سرایند بهینه شده تر و موثرتری را نسبت به IPv4 ارائه می نماید. پنج فیلد محدود شده اند ، از جمله آنها فیلد گزینه طول متغیر IPv4 است. حذف فیلد طول متغیر و فیلدهای دیگر ، اجازه می دهد که سرایند IPn6 دارای یک قالب ثابت با طول ۴۰ بایت باشد. مقایسه بین دو سرایند در جدول ۴-۲ ارائه گردیده است.

جدول ۴-۲ مقایسه سرایند

سرایند	IPv4	IPv6
قالب سرایند	متغیر	ثابت
فیلدهای سرایند	۱۳	۸
طول سرایند	۲۰ تا ۶۰ بایت	۴۰ بایت
طول آدرس	۳۲ بیت	۱۲۸ بیت
سرایند تشخیص خطا	بله	خیر

[۲۲] Network Address Translation
[۲۳] Port Address Translation

فیلدهای خرد کردن داده	بله	خیر
سرایندهای اضافی	خیر	بله

برای تامین گزینه های اضافی ، IPv6 سرایندهای اضافی زیر را تعریف کرده ، که بصورت جزئی تر در فصل بعدی در مورد آنها بحث خواهد شد:

- سرایند گزینه های Hop-by-Hop
- سرایند گزینه های مقصد
- سرایند مسیریابی
- سرایند قطعه
- سرایند تصدیق هویت
- سرایند پوشش گذاری بار امنیتی

مقایسه ویژگی

معماری IPv6 شامل گزینه های متراکمی می شود که در IPv4 وجود ندارد. جدول ۵-۲ وضعیت ویژگیهای IPv4 و IPv6 را نشان می دهد.

جدول ۵-۲ نمودار ویژگی ها

ویژگی	IPv4	IPv6
آدرس Anycast	خیر	بله
محدود سازی Multicast	خیر	بله
پشتیبانی از امنیت	خیر	بله
پشتیبانی از تحرک و پویایی	خیر	بله
پیکربندی خودکار	خیر	بله
کشف مسیریاب	خیر	کشف همسایه
عضویت Multicast	IGMP	کشف از طریق شنونده Multicast
خرد کردن داده توسط مسیریاب	بله	فقط توسط مبدا

آدرسهای Anycast و محدود سازی Multicast در IPv4 وجود ندارد. در حالیکه امنیت یک عملکرد در پروتکلهای لایه بالاتر در IPv4 است ، IPv6 یک امنیت متراکم و مجتمع را تامین می کند که برای پشتیبانی از عمل تصدیق هویت و رمزنگاری در سرایند ها از آن استفاده می شود. برای پشتیبانی از تحرک و پویایی ، IPv6 مکانیزم هایی را بنامهای home agent ، آدرسهای care-of و binding-cache ارائه می کند.

IPv6 از قابلیت Plug and Play پشتیبانی می کند. یک آدرس سیستم و طول پیشوند - جدا از امکان ورود آنها بصورت دستی – می توانند بصورت خودکار پیکربندی شده و مسیریاب ها و همسایه ها نیز می توانند کشف شوند. IPv4 در خودش هیچگونه قابلیت کشف نداشته و نیاز دارد که عناصر اصلی IP بصورت دستی پیکربندی شده و یا از منابع دیگر مانند سرویس دهنده های DNS کسب شوند.

برای پشتیبانی از عضویت Multicast ، IPv4 به گزینه های اضافه ای مانند پروتکل IGMP تکیه می کند. در مقابل ، IPv6 یک قابلیت داخلی بنام پروتکل MLD[۲۴] (کاشف شنونده Multicast) درون خود دارد که اجازه می دهد یک مسیریاب مشخص نماید کدامیک از درگاههای آن شامل شنونده های Multicast بوده تا بتواند بصورت مناسب تبادل اطلاعات Multicast را اضافه کرده یا از آن جلوگیری نماید.

IPv4 اجازه می دهد تا مسیریاب ها بتوانند پکت ها را خرد کنند که همین مسئله باعث افزایش بار ترافیکی شبکه می گردد. اما در نقطه مقابل ، IPv6 فقط اجازه می دهد که سیستم مبدا اقدام به خرد کردن پکت ها کند. IPv6 از مکانیزمی بنام کشف مسیر MTU پشتیبانی می کند که اجازه خرد کردن پکت ها بصورت موثر توسط مبدا را می دهد. این قابلیت نیاز به وجود دستگاهی جهت خرد کردن پکت را در مسیر شبکه تا مقصد آن ، رفع می کند.

[۲۴] Multicast Listener Discovery

بررسی معماری شبکه IPv6

در سال ۱۹۹۰ ، سازمان IETF طراحی IPv6 با موضوع توسعه IPv4 جهت پوشش دادن نیازهای جدید مانند توسعه روزافزون کاربران اینترنت و برنامه های کاربردی که بصورت زنده از اینترنت استفاده می کنند ، را شروع کرد. این گزینه های مورد نیاز برای توسعه شامل موارد زیر می شوند:

- **محدودیت فضای آدرس:** کمبود آدرس IP از سالها قبل ، پیش بینی شده بود و بهمین دلیل انواع وصله ها و گزینه های اضافی به IPv4 اضافه گردیده بود تا بحران را به حداقل برساند. از جمله این گزینه ها. اقدامات اضافی می توان به Maskهای زیرشبکه متغیر (VLSM) ، مسیریابی بدون کلاس داخل محدوده (CIDR) ، ترجمه آدرسهای شبکه (NAT) ، ترجمه آدرس درگاه (PAT) و فضای آدرس های خصوصی اشاره نمود. IPv6 یک ساختار آدرس دهی بزرگ و یکپارچه شده را ارائه می کند که بسیاری از این گزینه های اضافی و گاهی منسوخ شده را بصورت کامل تحت پوشش قرار می دهد.
- **کارایی شبکه:** بزرگتر شدن اینترنت که دارای گزینه های بسیاری نیز در IPv4 است ، از کارایی خوب شبکه جلوگیری می کند. از جمله این گزینه ها که از کارایی بهتر شبکه جلوگیری می کنند ، می توان از سرایندهای تشخیص خطا ، اندازه MTU و خرد کردن پکت ها نام برد. IPv6 برای کاهش بار ترافیکی پروتکلها ، بهینه سازی شده است.
- **امنیت:** IPv4 برای اهداف امنیتی طراحی نشد – بدلیل اینکه بحث امنیت جزو وظایف لایه های بالایی در مدل OSI محسوب می گردید- . IPv6 امنیت را با هدف رمزنگاری و تصدیق هویت ، پشتیبانی می کند.
- تشخیص و اجرای خودکار: پیکربندی سیستمهای شبکه در IPv4 همیشه آسان نبوده و گاهی پیچیده و مشکل می نمود. بسیاری از وظایف پیکربندی ، نیاز به تمرکز و عملکرد دستی داشته و در شبکه های بزرگ عملی نبود. یک نمونه از این مشکل ، شماره گذاری مجدد شبکه در هنگام انتخاب یک تامین کننده سرویس جدید بود. رشد ارتباطات متحرک و محاسبه آنها نیز بر بار کاری مدیران شبکه می افزود. مکانیزم پیکربندی خودکار IPv6 ، قدمهای کوتاه تری برای محاسبات ارتباط های متحرک و تشخیص و اجرای خودکار آنها در اختیار ما می گذارد.

مفاهیم بنیادی ارتباطات IPv6

در این بخش ما بصورت جزئی تر بررسی خواهیم کرد که چگونه ارتباط ها بین دستگاههای موجود بر روی یک شبکه برقرار می شوند و IPv6 چگونه این ارتباط ها را ساده می کند. علاوه بر این ما ارتباط بین سیستم های یک زیرشبکه و همچنین ارتباط سیستم و مسیریاب را در بین زیرشبکه ها بررسی خواهیم کرد.

ارتباط های داخل زیرشبکه[۲۵]

یک کامپیوتر برای اینکه بتواند به یک شبکه متصل گردد ، باید پیکربندی شود. علاوه بر این مدیر شبکه نیز باید دستگاههای شبکه را پیکربندی کند تا ارتباط بین سیستمها ساده و راحت گردد. سیستمها در هر دو سر ارتباط شبکه نیز ، باید پیکربندی سازگار با هم داشته باشند. گزینه های مختلفی به IPv4 اضافه شده اند تا نیاز به فرایند پیکربندی دستی را کاهش دهند. IPv6 برای تشخیص و اجرای خودکار طراحی شده است. پشتیبانی از پیکربندی خودکار نیز در داخل IPv6 گنجانده شده است. ما در ابتدا پیکربندی خودکار نوع Stateless و نقش آن در ارتباطات داخل زیرشبکه را بررسی خواهیم کرد. سپس به سراغ پیکربندی نوع Stateful خواهیم رفت و عملکرد آن را در ارتباطات بین زیرشبکه مورد بررسی قرار خواهیم داد. مفاهیم کلیدی درک ارتباطات داخل زیرشبکه عبارتند از:

- پیکربندی خودکار نوع stateless
- آدرس ارتباط محلی (Link-Local)
- پیشوند ارتباط محلی
- شناسه رابط (کارت شبکه)
- پیغام تقاضای همسایه
- پیغام آگهی همسایه

---

[۲۵] Intra-Subnet Communications

- ذخیره گاه (Cache[26]) همسایه

اجازه بدهید تصور کنیم که یک زیرشبکه در یک اداره وجود دارد. این زیرشبکه شامل تعداد کمی از ایستگاههای کاری و چاپگرها می شود. شبکه مذکور دارای هیچگونه مسیریاب ، ارتباط به اینترنت و سرویس دهنده ای که نیاز به پیکربندی داشته باشد ، نیست. یک سیستم بر روی چنین زیرشبکه ای ، باید آدرس IPv6 خود را توسط فرایندی بنام پیکربندی خودکار stateless ، پیکربندی نماید. هنگامی که یک ایستگاه کاری به یک درگاه بر روی زیرشبکه متصل شد ، بصورت خودکار یک آدرس آزمایشی پیکربندی می کند که به این آدرس ، آدرس ارتباط محلی ، گفته می شود. این آدرس با استفاده از آدرس فیزیکی کارت شبکه سیستم (MAC) تشکیل شده است. آدرس ارتباط محلی پیکربندی شده توسط سیستم ، ۱۲۸ بیت طول داشته و شامل یک پیشوند ارتباط محلی بهمراه شناسه کارت شبکه سیستم می شود. پیشوند آدرس محلی ، یک شناسه شبکه کاملا –صفر- است که با سرآغاز اعداد مبنای ۱۶ ((FE8)) شروع می شود. شناسه کارت شبکه یا همان آدرس MAC ، بر روی حافظه ROM در سخت افزار شبکه مقیم شده است. آدرسهای MAC امروزی ۴۸ بیت طول دارند ، اما مشخصات و ویژگیهای جدید ، آدرسهای MAC با طول ۶۴ بیت را پشتیبانی خواهند کرد. یک آدرس ارتباط محلی معمولی ، به شکل زیر خواهد بود و حروف X محل قرارگیری شناسه ۶۴ بیتی کارت شبکه را نشان می دهند.

```
FE80:0:0:0:xxxx:xxxx:xxxx:xxxx.
```

برای تضمین منحصربفرد بودن آدرس ، ایستگاه کاری یک پیغام ویژه تقاضای همسایه را به آدرس جدید پیکربندی شده می فرستد و به مدت یک ثانیه منتظر جواب می ماند. اگر در جواب ، هیچ پیغام انتشار همسایه برگردانده نشده و دریافت نشود ، این آدرسِ ارتباط محلی ، منحصربفرد فرض می شود (در ادامه ، خواهیم دید که پیغامهای تقاضای همسایه و انتشار همسایه برای عملکردهای دیگری که بخشی از پروتکل اکتشاف همسایه IPv6 هستند ، نیز استفاده می شود).

پس از شناسایی و بررسی آدرس ارتباط محلی ، انجام پرس و جو برای مسیریاب های همسایه موجود بر روی شبکه است. در مثال ما (زیرشبکه موجود در اداره) ، هیچ مسیریابی وجود ندارد. بنابراین سیستم ایستگاه کاری ما ، برای برقراری ارتباط با همسایه های خود آماده است.

برای برقراری ارتباط با یک سیستم مقصد بر روی زیرشبکه یکسان ، ایستگاه کاری باید شناسه کارت شبکه مقصد را کشف کند. برای انجام اینکار ، ایستگاه کاری از قابلیت پروتکل کشف همسایه IPv6 استفاده می کند. در این هنگام ، ایستگاه کاری یک پیغام تقاضای همسایه به مقصد ارسال کرده و در جواب ، شناسه کارت شبکه را در داخل یک پیغام انتشار همسایه ، دریافت می کند. این شناسه کارت شبکه در داخل یک سرایند قبل از سرایند IPv6 قرار داده شده و بر روی زیرشبکه انتقال داده می شود. سپس ایستگاه کاری یک داده را در بخش حافظه Cache همسایه خود ، ذخیره می کند. این داده شامل آدرس IPv6 مقصد ، شناسه کارت شبکه آن ، یک اشاره گر به پکت هایی که منتظر انتقال هستند ، و یک نشانه که مشخص می کند آیا مقصد یک مسیریاب است یا خیر. اطلاعات این حافظه Cache برای تبادل اطلاعات در آینده بجای ارسال پیغام تقاضای (همسایه) مجدد استفاده می شود.

آدرسهای ارتباط محلی نمی توانند برای برقراری ارتباط با بیرون از زیرشبکه مورد استفاده قرار گیرند. برای ایجاد ارتباط بین زیرشبکه ها ، باید از آدرسهای سایت محلی یا آدرسهای جهانی و با اتصال مسیریاب ها استفاده شود.

ارتباط های بین زیرشبکه

فرض کنید در مثال قبلی ، ایستگاه کاری ما متوجه شود که یک مسیریاب بر روی زیرشبکه وجود دارد. فرایند پیکربندی خودکار چه تفاوتی خواهد کرد و ایستگاه کاری ما چطور با سیستمهای موجود در زیرشبکه های دیگر ، ارتباط برقرار خواهد کرد؟ برای بحث در مورد ارتباطهای بین زیرشبکه ، ما به تفصیل در مورد فرایند پیکربندی خودکار از نوع stateless و مفاهیم مربوط به آن که در ذیل معرفی می شوند ، بحث خواهیم نمود؛

- کشف همسایه
- آدرس سایت محلی
- شناسه زیرشبکه
- پیغام تقاضای مسیریاب

---

[26] **نهانگاه بازنویسی :**
نوعی منبع ذخیره موقتی است که داده ها قبل از نوشته شدن در منبع ذخیره دائمی ، در آن نگهداری می شوند. این روند با کاهش تعداد روندهای خواندن و نوشتن و یا ایجاد ارتباط که نسبتاً کند انجام می شود، سرعت عملیاتی کامپیوتر را نیز افزایش می دهد.

- پیغام انتشار همسایه
- ذخیره گاه (Cache) لیست مسیریاب پیش فرض
- ذخیره گاه مقصد
- ذخیره گاه لیست پیش فرض
- پیغام راهنمایی مجدد
- کشف مسیر MTU

در طی مرحله پیکربندی خودکار و پس از آن ، ایستگاه کاری بر قابلیت پروتکل کشف همسایه IPv6 تکیه می کند. این پروتکل اجازه می دهد که سیستم های موجود بر روی یک زیرشبکه همدیگر را کشف کرده و همچنین مسیریاب ها را برای استفاده بعنوان واسط پرش بعدی خود به سمت یک مقصد در زیرشبکه دیگر ، پیدا کنند. پروتکل کشف همسایه ، جای پروتکل تحلیل آدرس IPv4 ، فرایند دروازه پیش فرض IPv4 و فرایند راهنمایی IPv4 را می گیرد و بجای آنها عمل می کند.

در طی فرایند پیکربندی خودکار ، پس از اینکه ایستگاه کاری یک آدرس ارتباط محلی منحصربفرد ایجاد کرد ، یک تقاضا به سمت مسیریاب ارسال می کند. ایستگاه کاری ، یک پیغام تقاضای مسیریاب ارسال کرده و در مقابل ، مسیریاب توسط پیغام انتشار مسیریاب به تقاضای ارسال شده جواب می دهد. وجود مسیریاب نشان می دهد احتمالا زیرشبکه های دیگری نیز وجود دارند که به مسیریاب متصل هستند. هر زیرشبکه باید شناسه زیرشبکه خود را داشته باشد ، بدلیل اینکه مسیریابی ، به شماره های زیرشبکه منحصربفرد وابسته است. شناسه های سیستم برای تصمیمات مسیریابی استفاده نمی شوند. آدرس ایستگاه کاری هم اکنون باید یک شناسه زیرشبکه منحصربفرد و تک داشته باشد. آدرس ارتباط محلی بهمراه زیرشبکه صفر خود ، برای ارتباط بین زیرشبکه ها مفید نبوده و کارایی ندارد.

برای پشتیبانی از پیکربندی خودکار نوع stateless ، آگهی و انتشار مسیریاب شامل یک شناسه زیرشبکه می شود. انتشارهای مسیریاب برای هر رابط و کارت شبکه آن ، یک شناسه زیرشبکه جداگانه را ارائه می کند. این شناسه به شناسه کارت شبکه متصل شده و با هم آدرس IPv6 ایستگاه کاری را تشکیل خواهند داد.

سپس ایستگاه کاری آدرس ارتباط محلی خود را که از نوع آزمایشی بود ، نابود کرده و یک آدرس جدید بنام آدرس سایت محلی پیکربندی می کند. آدرس سایت محلی ، شامل یک شناسه زیرشبکه بطول ۱۶ بیت به شکل زیر خواهد بود و حروف X محل قرارگیری شناسه ۶۴ بیتی کارت شبکه را نشان می دهند؛

```
FEC0:0:0:<subnet ID>:xxxx:xxxx:xxxx:xxxx.
```

ایستگاه کاری اطلاعات دریافتی از انتشار مسیریاب را برای بهنگام سازی اطلاعات cache (ذخیره گاه) خود استفاده کرده و شناسه زیرشبکه را به حافظه cache در لیست پیشوند ایستگاه کاری اضافه می کند. اطلاعات cache برای تعیین و تشخیص اینکه آیا یک آدرس بر روی زیرشبکه ایستگاه کاری قرار دارد (on-link) یا زیرشبکه دیگر (off-link) استفاده می شود. اطلاعات مسیریاب به حافظه cache همسایه و cache مقصد اضافه خواهد شد. اگر مسیریاب بتواند بعنوان مسیریاب پیش فرض استفاده شود ، یک داده به حافظه cache لیست مسیریاب پیش فرض اضافه می شود. هنگامی که سیستم برای ارسال یک پکت به سمت سیستم مقصد آماده شد ، یک پرس و جو و تقاضایی به سوی لیست پیشوند ارسال می کند تا تشخیص دهد که آدرس IPv6 مقصد از نوع on-link است یا off-link ؟. اگر سیستم مقصد off-link باشد ، پکت به سمت واسط پرش بعدی انتقال داده خواهد شد که یک مسیریاب در لیست مسیریاب پیش فرض می باشد. سپس ایستگاه کاری ما ، اطلاعات cache مقصد خودش را با وارد کردن یک داده مربوط به سیستم مقصد و آدرس واسط پرش آن ، بهنگام سازی می کند. اگر مسیریاب پیش فرض انتخاب شده ، واسط پرش مناسب و بهینه ای برای مقصد نباشد ، مسیریاب یک پیغام راهنمایی مجدد حاوی اطلاعات واسط پرش جدید بعنوان مقصد ، به سمت ایستگاه کاری مبدا ارسال خواهد کرد. سپس ایستگاه کاری ، اطلاعات cache مقصد خود با آدرس واسط پرش جدید بعنوان مقصد ، بهنگام سازی می کند.

اطلاعات cache بوسیله هر سیستم IPv6 نگهداری شده و قبل از ارسال پیغام های تقاضای همسایه ، بررسی می شوند. اطلاعات cache باعث کاهش تعداد پیغامهای تقاضای همسایه و انتشار همسایه می شوند که باید بصورت مداوم ارسال گردند. این اطلاعات در دوره های زمانی معین خالی و پاک شده و بصورت همیشگی و مداوم بهنگام سازی می شوند.

برای ساده کردن ارتباط های بین زیرشبکه ها ، IPv6 یک سرویس مفید دیگر هم ارائه می کند که نام آن کشف مسیر MTU است. IPv6 اجازه نمی دهد که مسیریاب ها پکت های با حجم زیاد را جهت عبور دادن آنها از طریق ارتباط واسط پرش یا کارت شبکه خود ، خرد کنند ؛ فقط سیستم مبدا می تواند یک پکت را خرد کند. با استفاده از سرویس کشف مسیر MTU ، سیستم مبدا می تواند پکت های بزرگی را که ممکن است به سوی مقصد فرستاده شوند ، تشخیص دهد. با داشتن این اطلاعات ، سیستم مبدا می تواند بصورت مناسب اندازه پکت ها را قبل از ارسال ، دوباره تنظیم نماید.

آدرس سایت محلی ، فقط می تواند برای ارتباطات بین سایت استفاده گردد. برای ایجاد ارتباط بیرون از سایت ، باید آدرس های جهانی تحت یک فرایند توسعه پذیر پیکربندی خودکار اختصاص داده شوند.

ارتباط های داخل شبکه

در پیکربندی خودکار نوع stateless ، هر سیستم وظیفه دارد تا آدرس و اطلاعات cache خودش را با استفاده از شناسه کارت شبکه و اطلاعات تامین شده توسط پروتکل کشف همسایه انتشار یافته ، پیکربندی کند. در شبکه های کوچک ، پیکربندی خودکار نوع stateless ، دارای مزایایی از جمله سادگی و راحت بودن استفاده از آن است. البته عیب هایی هم مانند متکی بودن بر مکانیزم کشف multicast ، استفاده از فضای آدرس کم بازده ، فقدان امنیت و کنترل از طریق سیساستهای دسترسی را در خود جای داده است.
برای ساده تر کردن ارتباط ها در شبکه های داخلی کاملتر و بزرگتر ، مطلوب تر این است که از فرایندی بنام پیکربندی خودکار نوع statful استفاده شود. در طی بحث ما در مورد این فرایند ، با مفاهیم زیر آشنا خواهیم شد؛

- پیکربندی خودکار نوع statful
- پروتکل پیکربندی اتوماتیک سیستم ، نسخه ۶ (DHCPv6)
- سرویس گیرنده DHCPv6 ، مامور بازپخش (Relay Agent) ، سرویس دهنده

پیکربندی خودکار نوع statful متکی بر سرویس دهنده ای است که مجموعه ای از اطلاعات پیکربندی از جمله اطلاعات شبکه که برای بدست آوردن آدرسهای منحصر بفرد جهانی لازم است ، را تامین می کند. به این سرویس دهنده ، DHCPv6 گفته می شوند. از دیدگاه یک مدیر شبکه پیکربندی خودکار نوع statful ، نسبت به پیکربندی خودکار نوع stateless کاملتر است. بدلیل اینکه در این حالت فقط نیاز به وارد کردن اطلاعات پیکربندی در بانک اطلاعاتی DHCPv6 می باشد. از طرف دیگر پیکربندی خودکار نوع statful ، قابلیت توسعه و مقیاس پذیری بیشتری را در شبکه های بزرگ فراهم می کند.
پیکربندی خودکار نوع statful می تواند با پیکربندی خودکار نوع stateless بصورت همزمان استفاده شود. بعنوان مثال ، یک سیستم ممکن است از فرایند stateless در هنگام شروع بکار ، برای بدست آوردن یک آدرس ارتباط محلی پیروی کند. پس از بدست آوردن این آدرس ، سیستم ممکن است از پیکربندی خودکار نوع statful برای بدست آوردن اطلاعات اضافی از DHCPv6 استفاده کند.
برای کسب کردن اطلاعات پیکربندی ، یک ایستگاه کاری در ابتدا با استفاده از صادر کردن پیغام تقاضای DHCP [۲۷] ، دنبال DHCPv6 گشته و یا به پیغامهای انتشار شده DHCPv6 گوش می دهد. سپس ایستگاه کاری ، یک پیغام تقاضای DHCPv6 صادر می کند. اگر سرویس دهنده DHCPv6 در شبکه محلی قرار نداشته باشد ، مامور بازپخش DHCPv6 –که معمولا یک مسیریاب است- تقاضای ایستگاه کاری را به سوی سرویس دهنده مذکور که در بیرون شبکه محلی است ، از خود عبور داده و ارسال می کند. سرویس دهنده با یک پیغام جواب DHCPv6 که حاوی اطلاعات پیکربندی مورد نیاز برای ایستگاه کاری است ، به پیغام مذکور جواب می دهد.

استفاده از سرویس DHCPv6 دارای مزایای زیادی است؛

- **کنترل؛** سرویس DHCPv6 توزیع و اختصاص آدرسها را از یک نقطه مرکزی کنترل می کند.
- **تراکم؛** از طریق توزیع متفکرانه و با دقت آدرسها ، می توان با ایجاد یک ساختار سلسله مراتبی آدرس دهی از متراکم سازی و مجتمع شدن آدرسها اطمینان حاصل نمود.
- **شماره گذاری مجدد؛** هنگامی که یک ISP (تامین کننده سرویس اینترنت) جدید برای جایگزینی با یک ISP قدیمی انتخاب می شود ، آدرسهای جدید می توانند براحتی توسط سرویس DHCPv6 توزیع گردند.
- **امنیت؛** سیستم ثبت نام کامپیوتر (Host) می تواند توسط سرویس DHCPv6 اجرا شود. این سیستم ثبت نام ، می تواند باعث دسترسی سیستمهای ثبت شده به سرویس های شبکه گردیده و جلوی دسترسی سیستم های ثبت نشده را به آنها بگیرد.

---
[۲۷] DHCP Solicit Message

طراحی و اجرا

پیکربندی خودکار

پیکربندی های خودکار نوع stateless و stateful ، هر دو می توانند با هم IPv6 وجود داشته باشند و استفاده شوند. هنگام طراحی و اجرای شماره گذاری IPv6 مربوط به یک سایت ، معمولا بهتر است که برای اجرای هر دو نوع پیکربندی خودکار برنامه ریزی شود. ما این کار را با طبقه بندی انواع سیستم ها بر مبنای نیاز آنها جهت دسترسی به سایت و اینترنت شروع می کنیم:

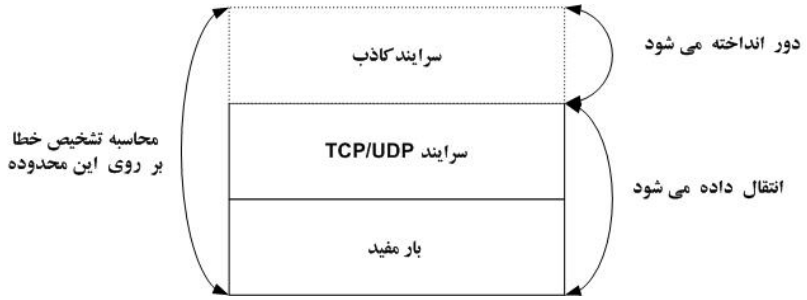
- ایستگاههای کاری که نیازی به برقراری ارتباط با بیرون از زیرشبکه محلی خود ندارند ، ممکن است برای بدست آوردن آدرسهای ارتباط محلی از فرایند پیکربندی خودکار stateless استفاده کنند.
- ایستگاههای کاری که علاوه بر زیرشبکه داخلی ، نیاز به برقراری ارتباط بین سایتها نیز دارند ، اما احتیاجی به دسترسی به اینترنت ندارند می توانند از پیکربندی خودکار stateless برای بدست آوردن آدرسهای سایت محلی از مسیریابهای محلی خود ، استفاده نمایند.
- ایستگاههای کاری که احتیاج به دسترسی به اینترنت دارند ، می توانند آدرسهای منحصر بفرد جهانی را از سرویس دهنده DHCPv6 بدست آورند. DHCPv6 اجازه توزیع آدرسها و کنترل آنها را از یک نقطه مرکزی در اختیار ما می گذارد.

انتشار پروتکل لایه بالاتر

پروتکل های لایه بالاتر که تشخیص خطاها را بر روی پکت محاسبه می کنند ، باید برای تغییرات در IPv6 مانند استفاده از آدرسهای با طول ۱۲۸ بیت ، داشتن مقصد نهایی بجای سیستمهای میانی در هنگام استفاده از سرایندهای مسیریابی و ... محاسبه شوند.

همانطور که قبلا بحث کردیم ، فیلد TTL (زمان زنده بودن) به محدوده پرش[۲۸] تغییر نام یافت. هر پروتکل لایه بالاتر که بر روی معنی اصلی TTL تکیه می کند ، ممکن است نیاز به تنظیم لازم داشته باشد. حداکثر اندازه بار مفید در لایه بالاتر نیاز به تنظیم شدن جهت منعکس کردن طول سرایند IPv6 دارد (۴۰ بایت).

- **تشخیص خطاهای لایه بالاتر:** در حال حاضر پروتکل انتقال (Transport) لایه بالاتر مانند TCP و UDP به یک سرایند کاذب قبل از بار مفید آن و در هنگام محاسبه تشخیص خطای لایه انتقال ، الحاق می شود. این سرایند کاذب آدرسهای IPv4 مبدا و مقصد ، طول پکت لایه بالاتر و فیلد سرایند بعدی را در داخل خود جای داده است. تشخیص خطا بر روی سرایند کاذب IPv6 ، سرایند TCP یا UDP و بار مفید TCP یا UDP محاسبه شده است. تصویر ۸-۲ نشان می دهد که تشخیص خطا بر روی یک سرایند کاذب IPv6 محاسبه شده است.



- **حداکثر زمان زنده بودن پکت:** سرایند IPv4 یک فیلد بنام TTL دارد که برای تعیین زمان دور انداخته شدن پکت در صورت نرسیدن به مقصد استفاده می شود. آن همچنین شامل یک شمارش پرش یا یک زمان در واحد ثانیه نیز می گردد. در IPv6 این فیلد

[۲۸] Hop Limit

بنام محدوده پرش تغییر نام یافته و اندازه گیری زمان در واحد ثانیه دیگر پشتیبانی نمی شود و وجود ندارد. برنامه های کاربردی که از این فیلد برای زمان بندی داده استفاده می کنند باید ارتقا یافته و تجدید گردند.

- **حداکثر اندازه بار مفید لایه بالاتر:** سرایند ظاهری IPv6 ، ۴۰ بایت طول دارد. سرایند ظاهری IPv4 دارای طول ۲۰ بایتی است. جایگزینی سرایند IPv4 با سرایند IPv6 باعث حاصل شدن پکت های بزرگتری می گردد
- **سرایندهای مسیریابی و امنیت:** اضافه سرایند IPv6 شامل سیستم های میانی است که پکت باید در طول مسیر به سمت مقصد از آنها عبور کند. هنگامی که یک پکت با سرایند مسیریابی بوسیله مقصد دریافت شد ، نباید فرض کند که مسیر معکوس (همان مسیری که پکت از طریق آن به مقصد رسیده بود) ، مسیر مناسبی به سمت مبدا نیز می باشد. در حقیقت ، جواب دادن از طریق مسیر معکوس (همان مسیر) ممکن است باعث تسهیل در انواع رخنه های امنیتی گردد.
- **سیستم نام دامنه (DNS):** سرویس DNS یک سیستم بانک اطلاعاتی توزیع شده است که قرارداد نام گذاری سلسله مراتبی را برای سیستمها تعیین کرده و این نام سیستم ها را به آدرس های IP مسیردهی می نماید. برای مثال ، آدرس www.syngress.com به آدرس IPv4 : 216.238.176.55 مسیردهی می شود. افزوده شده های IPv6 به DNS شامل یک نوع نگاشت[۲۹] جدید برای آدرس IPv6 با طول ۱۲۸ بیت (Host Record) و یک سرویس جدید می شود که می تواند نام سیستم را در هنگام ارائه آدرس IPv6 آن ، برگرداند.
- **رابط برنامه نویسی کاربردی (API):** برنامه های کاربردی که برای IPv4 نوشته شده اند باید برای استفاده از API های IPv6 تبدیل شوند. همچنین برنامه های کاربردی باید شامل ساختمان داده جدیدی برای پشتیبانی از آدرسهای طولانی تر IPv6 شوند. توابعی که آدرسهای IPv4 را اداره می کنند باید با توابع اداره کننده آدرسهای IPv6 ، جایگزین گردند.

درک ICMPv6

پروتکل پیغام کنترل اینترنت نسخه ۶ (Internet Control Message Protocol, Version 6) ، یک بخش کلیدی از معماری IPv6 می باشد. ICMPv6 وظایف اجرای و کنترل پیغام های برگشتی لازم را برای تضمین درست و هموار عمل کردن فرایند IPv6 را بر عهده دارد. این وظایف شامل گزینه های زیر می شود:

- گزارش خطای پردازش پکت
- تشخیص و عیب یابی
- کشف همسایه
- گزارش عضویت Multicast

ICMPv6 آن دسته از وظایف مربوط به IPv4 را که دیگر استفاده نمی شوند ، حذف کرده و برخی دیگر از وظایف آن مانند؛ ICMPv4 ، IGMP و ARP را در خود ترکیب کرده است. پیغامهای ICMPv6 به دو بخش پیغامهای خطا و پیغامهای اطلاع رسانی تقسیم می شوند.

پیغامهای خطا

ICMPv6 پیغامهای خطایی را که مربوط به پردازش پکت هستند ، صادر می کند. این پیغامهای خطا عبارتند از؛

- Destination Unreachable : یک سیستم مبدا یا یک مسیریاب این پیغام را هنگامی که یک پکت به هر دلیلی غیر از تراکم ، نتواند توسط مقصد دریافت شود ، صادر می نماید.
- Packet Too Big : مسیریاب این پیغام را هنگامی که یک پکت بدلیل حجم و اندازه زیاد آن نسبت به MTU واسط بعدی ارتباط ، نتواند از مسیریاب به سمت مقصد عبور داده شود ، صادر می کند. MTU واسط بعدی ارتباط در داخل پیغام مذکور برگردانده می شود. این پیغام توسط تابع کشف مسیر MTU استفاده می گردد.
- Time Exceeded : سرایند IPv6 شامل یک محدوده پرش می گردد که توسط هر مسیریابی که پکت را از خود عبور می دهد ، کاهش می یابد. هنگامی که این محدوده پرش به صفر برسد ، مسیریاب پکت را از بین برده و یک پیغام Time Exceeded به سیستم مبدا بر می گرداند. این عملکرد ، پایه عملکرد Traceroute می باشد ؛ که یک مسیر را تا مقصد توسط فرستادن پکت هایی با محدوده

---

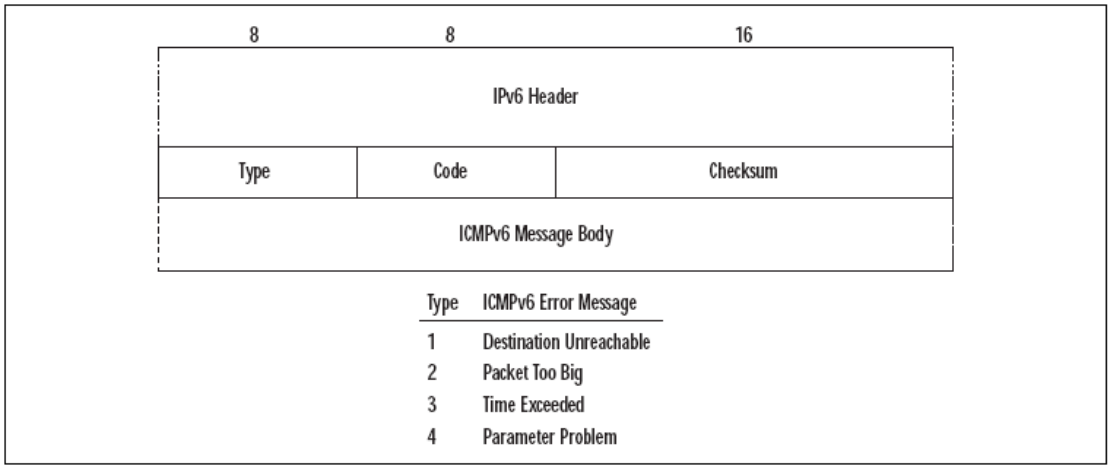
[۲۹] Record

پرش افزایشی ، پیگیری می کند. پیغام Time Exceeded برگردانده شده برای شناسایی مسیریابهای واقع شده در مسیر استفاده می گردد.

- Parameter Problem : هنگامی که یک مشکل موجود در بخشی از سرایند IPv6 ، از پردازش موفقیت آمیز پکت توسط مسیریاب جلوگیری می کند ، پکت از بین رفته و مسیریاب یک پیغام Parameter Problem را به سیستم مبدا بر می گرداند.

هر پیغام خطای ICMPv6 شامل سه فیلد طول ثابت بعلاوه بدنه پیغام طول متغیر می گردد. تصویر ۹-۲ قالب این پیغام خطا را نمایش می دهد.

تصویر ۹-۲ پیغام خطای ICMPv6



پیغامهای اطلاع رسانی

ICMPv6 همچنین پیغامهای اطلاع رسانی را استفاده می نماید که شامل موارد زیر می گردند:

- پیغامهای تشخیص و عیب یابی: پیغامهای تشخیص و عیب یابی شامل دو پیغام تقاضای Echo (Echo Request) و جواب Echo (Echo Reply) می شوند. هنگامی که یک مقصد پیغام تقاضای Echo را دریافت کرد ، یک جواب بر می گرداند. این تقاضا و جواب Echo برای اجرای عملکرد تشخیص و عیب یابی توسط دستور Ping استفاده می شوند. عملکرد Ping یک گزینه مهم برای تعیین اینکه آیا سیستم مقصد به همان شبکه ای که سیستم مبدا در آن قرار دارد ، متصل است یا خیر ، استفاده می شود.
- پیغامهای کشف شنونده Multicast: مسیریاب این پیغام را هنگامی که یک پکت بدلیل حجم و اندازه زیاد آن نسبت به MTU واسط بعدی ارتباط ، نتواند از مسیریاب به سمت مقصد عبور داده شود ، صادر می کند. MTU واسط بعدی ارتباط در داخل پیغام مذکور برگردانده می شود. این پیغام توسط تابع کشف مسیر MTU استفاده می گردد.
- پیغامهای کشف همسایه: ICMPv6 پیغامهای مورد نیاز برای پروتکل اکتشاف همسایه را تامین می کند. این پیغامها شامل ؛ تقاضای مسیریاب[۳۰] و انتشار مسیریاب[۳۱] ، تقاضای همسایه[۳۲] و انتشار همسایه[۳۳] و پیغام راهنمایی مجدد[۳۴] می شوند. این پیغامها شامل اطلاعاتی مانند آدرس لایه ارتباط مبدا ، آدرس لایه ارتباط مقصد ، اطلاعات پیشوند ، سرایند راهنمایی شده و اندازه MTU می شوند.

پیغامهای اطلاع رسانی ICMPv6 دارای قالب یکسانی مانند پیغامهای خطای ICMPv6 هستند که در تصویر ۹-۲ نمایش داده شد. ارزشهای داخلی فیلد *Type* برای پیغامهای اطلاعاتی ، دارای محدوده ۱۲۸ تا ۲۵۵ می باشد. جدول ۶-۲ برخی از مهمترین ارزشهای داخلی فیلد *Type* را برای پیغامهای اطلاع رسانی ICMPv6 نشان می دهد.

جدول ۶-۲ پیغامهای اطلاع رسانی ICMPv6

ارزش داخلی فیلد *Type*	پیغام اطلاع رسانی ICMPv6
۱۲۸	تقاضای Echo

[۳۰] Router Solicitation
[۳۱] Router Advertisement
[۳۲] Neighbor Solicitation
[۳۳] Neighbor Advertisement
[۳۴] Redirect

۱۲۹	جواب Echo
۱۳۰	پرس و جوی شنونده Multicast
۱۳۱	گزارش شنونده Multicast
۱۳۲	انجام شدن شنونده Multicast
۱۳۳	تقاضای مسیریاب
۱۳۴	انتشار مسیریاب
۱۳۵	تقاضای همسایه
۱۳۶	انتشار همسایه
۱۳۷	راهنمایی مجدد

درک اکتشاف همسایه

پروتکل اکتشاف همسایه ICMPv6 برای بدست آوردن اطلاعاتی بکار می رود که فرایند عبور دادن پکت ها را تسهیل می نماید. این اطلاعات توسط پروتکل اکتشاف همسایه گردآوری می شود و می تواند برای اهداف زیر استفاده شود؛

- تعیین واسط پرش بعدی
- استخراج آدرس
- کشف پیشوند
- کشف پارامتر
- راهنمایی مجدد

ما در ادامه موضوع ، در مورد پنج پیغام ICMPv6 که در پروتکل اکتشاف همسایه استفاده می شوند و پیشتر آنها را نام بردیم ، بحث خواهیم کرد.

تقاضای مسیریاب و انتشار مسیریاب

در طی فرایند پیکربندی خودکار ، پس از اینکه ایستگاه کاری یک آدرس ارتباط محلی منحصربفرد را ایجاد کرد ، اقدام به فرستادن تقاضا به یک مسیریاب می کند. ایستگاه کاری ، یک پیغام تقاضای همسایه ارسال نموده و منتظر شنیدن و دریافت پیغام انتشار مسیریاب می گردد.

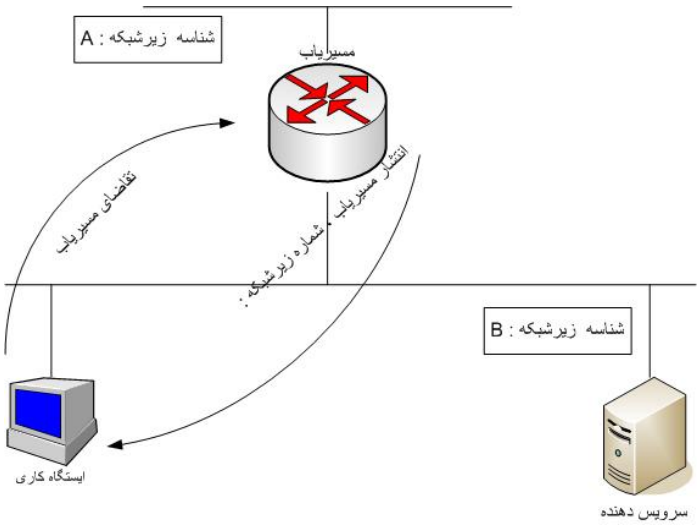
وجود یک مسیریاب نشان می دهد که احتمالا زیرشبکه های دیگری نیز به مسیریاب متصل هستند. هر زیرشبکه باید دارای شناسه منحصربفرد زیرشبکه خودش باشد ، زیرا مکانیزم مسیریابی برمبنای شماره های منحصربفرد زیرشبکه ها عمل می کند. شناسه های سیستم برای تصمیمات مسیریابی استفاده نمی شوند. آدرس ایستگاه کاری هم اکنون باید دارای یک شناسه زیرشبکه منحصر بفرد باشد. آدرس ارتباط محلی با شناسه زیرشبکه –صفر- ، برای برقراری ارتباط بین زیرشبکه ها کارایی ندارد.

پیغام انتشار مسیریاب ، شامل یک شماره شبکه یا پیشوند می شود. پیشوند ممکن است شامل یک پیشوند آدرس منحصربفرد جهانی یا یک شناسه زیرشبکه باشد. پیغام مذکور ، برای هر رابط و کارت شبکه مسیریاب ، دارای پیشوندهای متفاوتی خواهد بود. این پیشوند به شناسه کارت شبکه الحاق خواهد شد تا آدرس IPv6 ایستگاه کاری را ، تشکیل دهد.

ایستگاه کاری از اطلاعات انتشار مسیریاب برای بهنگام سازی حافظه Cache خود استفاده می کند. در عین حال ، شناسه زیرشبکه نیز به حافظه Cache مربوط به لیست پیشوندهای ایستگاه کاری اضافه شده است. این Cache برای تعیین اینکه آیا یک آدرس در داخل زیرشبکه ایستگاه کاری قرار دارد (On-Link) و یا در خارج از آن (Off-Link) استفاده می شود. اطلاعات مسیریاب به حافظه Cache همسایه و حلفظه Cache مقصد اضافه خواهد شد. اگر یک مسیریاب بتواند بعنوان مسیریاب پیش فرض استفاده شود ، یک داده به حافظه Cache لیست مسیریاب پیش فرض اضافه خواهد شد.

تصویر ۱۰-۲ یک ایستگاه کاری را در طی فرایند پیکربندی خودکار نمایش می دهد. ایستگاه کاری مسیریاب محلی را تقاضا می کند و در مقابل شناسه زیرشبکه ای را که برای کامل کردن آدرس IPv6 سیستم نیاز دارد ، دریافت می نماید.

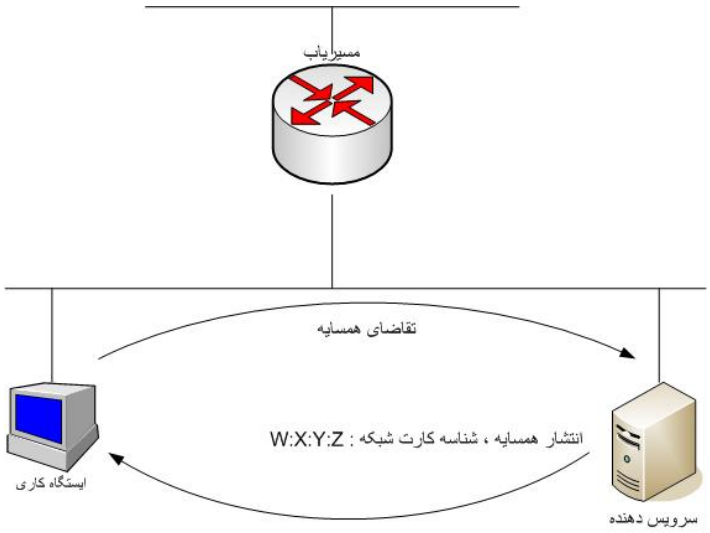
تصویر ۱۰-۲ اکتشاف مسیریاب



تقاضای همسایه و انتشار همسایه

برای برقراری ارتباط با یک سیستم مقصد در داخل یک زیرشبکه یکسان ، ایستگاه کاری باید شناسه کارت شبکه مقصد خودش را پیدا کند. برای انجام این کار ، ایستگاه کاری از توابعی استفاده می کند که توسط پروتکل اکتشاف همسایه IPv6 تامین می شوند. ایستگاه کاری یک پیغام تقاضای همسایه به سوی مقصد ارسال می کند و در جواب ، شناسه رابط کارت شبکه مقصد در داخل پیغامی بنام انتشار همسایه ، برگردانده می شود. این شناسه رابط ، در داخل سرایندی قبل از سرایند IPv6 قرار داده شده و بر روی زیرشبکه انتقال داده می شود. سپس ایستگاه کاری یک داده به حافظه Cache همسایه خود اضافه می کند که این داده شامل آدرس IPv6 مقصد و شناسه کارت شبکه آن ، یک اشاره گر برای پکت هایی که منتظر انتقال هستند و نیز پرچمی برای نشان دادن اینکه آیا مقصد یک مسیریاب است یا خیر ، می شود. اطلاعات این Cache برای انتقال داده ها در آینده استفاده می شود (بجای ارسال مجدد پیغام تقاضا). تصویر ۱۱-۲ نشان می دهد که چگونه پیغامهای تقاضا و انتشار همسایه یک نقش کلیدی را در فرایند اکتشاف همسایه بازی می کنند.

تصویر ۱۱-۲ اکتشاف همسایه



پیغام راهنمایی مجدد

مسیریاب ها پیغام راهنمایی مجدد را برای آگاه ساختن سیستمهای دیگر از یک مسیر اولیه بهتری به سمت مقصد ، صادر می کنند. یک سیستم می تواند بر روی یک ارتباط یکسان ، به سمت یک مسیریاب دیگر ، بصورت مجدد مسیردهی گردد.

حالا ببینیم مسیردهی مجدد در فرایند پردازش پکت ، چگونه کار می کند؛

هنگامی که یک ایستگاه کاری برای ارسال یک پکت به سمت یک سیستم مقصد آماده می شود ، یک تقاضای لیست پیشوند ارسال می کند تا متوجه گردد که آدرس IPv6 مقصد در داخل زیرشبکه خودش قرار دارد (On-Link) یا بیرون از آن (Off-Link). اگر سیستم مقصد Off-Link باشد ، پکت به سوی واسط پرش بعدی فرستاده خواهد شد ، که یک مسیریاب در لیست مسیریاب های پیش فرض است. ایستگاه کاری سپس ، Cache مقصد خودش را با اضافه کردن یک داده برای سیستم مقصد و آدرس واسط پرش بعدی آن ، بهنگام سازی می کند. اگر مسیریاب پیش فرض انتخاب شده ، واسط پرش مناسبی برای مقصد نباشد ، مسیریاب یک پیغام راهنمایی مجدد را به ایستگاه ماری مبدا ارسال می کند که در داخل آن ، آدرس مسیریاب واسط پرش جدید برای مقصد را توصیه کرده است. ایستگاه کاری سپس ، Cache مقصد خودش را با آدرس واسط پرش جدید برای مقصد ، بهنگام سازی می نماید.

گزینه های پیغام

پیغامهای اکتشاف همسایه ممکن است شامل گزینه های اطلاع رسانی اضافه تری هم باشد. این گزینه ها عبارتند از؛

- آدرس لایه ارتباط مبدا: این گزینه شامل آدرس لایه ارتباط مبدا در پیغام می باشد و در پیغام تقاضای مسیریاب ، انتشار مسیریاب و پیغامهای تقاضای همسایه استفاده می گردد.
- آدرس لایه ارتباط مقصد: : این گزینه شامل آدرس لایه ارتباط مقصد در پیغام می باشد و در پیغام انتشار همسایه و پیغامهای راهنمایی مجدد استفاده می گردد.
- اطلاعات پیشوند: این گزینه شامل پیشوند هایی برای پیکربندی خودکار آدرس شده و در پیغام انتشار مسیریاب مرد استفاده قرار می گیرد.
- سرایند راهنمایی شده: این گزینه شامل تمام یا بخشی از پکتی است که راهنمایی مجدد شده است و در پیغامهای راهنمایی مجدد استفاده می شود.
- MTU: این گزینه شامل اندازه MTU مربوط به ارتباط می شود و در پیغامهای انتشار مسیریاب استفاده می گردد.