وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

سند راهبردی

گذر به IPv٦

جمهوری اسلامی ایران

مؤلفین:

کمیته راهبری مهاجرت به پروتکل اینترنت نسخه ٦

و

گروه ضربت مهاجرت به پروتکل اینترنت نسخه ٦ ایران

نسخه ۱.۲

مهرماه ۱۳۹۰

فهرست مطالب

عنوان **صفحه**

فهرست پیوست ها

عنوان **صفحه**

۱ مقدمه

توسعه فناوری اطلاعات در جهان عصر صنعتی را پشت سر نهاده و در حال گذر به عصر فرا صنعتی، جامعه اطلاعاتی، مدیریت دانش، جهانی شدن ارتباطات و انفجار اطلاعات می‌باشد. فناوری اطلاعات در همه سیستم‌های اجتماعی، اقتصادی، فرهنگی و مدیریتی جنبه کاربردی پیدا نموده و پیشران توسعه خدمات و سیستم‌های مبتنی بر فناوری در محیط‌های مجازی و غیرمجازی شده است، به‌گونه‌ای که آثار و پیامد کاربرد آن سبب تسریع در رشد اقتصادی و اجتماعی جوامع پیشرفته شده است. کشورهای در حال توسعه نیز رویکرد مثبتی نسبت به کاربرد این فناوری در ابعاد مختلف نشان داده‌اند، اما شکاف دیجیتالی که میان این جوامع با کشورهای توسعه یافته وجود دارد، روز به روز در حال افزایش می‌باشد. شبکه اینترنت نیز در حال رشد بوده و سرویس‌های آن بصورت چشم‌گیری در حال گسترش است. برای بهره‌گیری از سرویس‌های این شبکه و گسترش فناوری اطلاعات در کشور به منظور کاهش شکاف دیجیتالی[1] و هویت‌دار کردن فعالیتهای دنیای مجازی، نیاز به استفاده از منابع اینترنتی معتبر و قابل ردیابی می باشد. از طرفی بر اساس اعلان سازمان‌های بین‌المللی از جمله سازمان منابع شبکه (NRO[2])، منابع موجود در اینترنت نسخه ۴ رو به اتمام بوده و دست‌اندرکاران شبکه‌ها و سایر تأمین کنندگان سرویس، دیگر قادر به گسترش شبکه خود با منابع موجود نخواهند بود.

کشور ما در حال توسعه زیرساخت‌های ارتباطی فناوری اطلاعات است، این در حالی است که آدرس‌های عددی اینترنتی نسخه ۴ در حال اتمام است و با استفاده از نسخه موجود، توسعه فناوری اطلاعات در کشور مقدور نخواهد بود. از طرفی اکثر کشورهای جهان با شتاب به سمت استفاده از پروتکل اینترنت نسخه ۶ حرکت می‌کنند، بنابراین استفاده از امکانات پروتکل اینترنت نسخه ۶ و انجام راهکارهای مرتبط آن یک ضرورت اجتناب‌ناپذیر جهت توسعه فناوری اطلاعات در کشور است. نتیجه ارزیابی جایگاه جهانی کشورها از دیدگاه فناوری اطلاعات، بیان کننده آن است که مدیریت هماهنگ ملی، بسترسازی برای تهیه زیرساخت‌های نرم‌افزاری و سخت‌افزاری، تعیین اولویت‌های اساسی و سازماندهی مناسب برنامه‌های اجرایی در زمینه توسعه فناوری اطلاعات در قالب اسناد راهبردی که به تصویب مراجع ذیصلاح قانونی نیز رسیده باشد، عامل کلیدی در این توسعه خواهد بود. سند حاضر در راستای ماموریت‌های کلان وزارت ارتباطات و فناوری اطلاعات به منظور توسعه فناوری اطلاعات در کشور و بهبود وضعیت شبکه IP کنونی کشور، رفع نواقص و مشکلات آن با بکارگیری پروتکل

[1] Digital divide
[2] Number Resource Organization

اینترنت نسخه ۶ با هدف ارتقاء بازده‌کاری و کاهش هزینه‌ها تهیه شده است. با بهره‌گیری از این سند کلیه فعالیت‌های مختلف در بخش‌های اداری، اجرایی، آموزشی، فنی، صنعتی، قضایی، حقوقی اعم از دولتی و غیردولتی جهت گذر به پروتکل اینترنت نسخه ۶ همسو و همراستا خواهد شد و گذر از پروتکل اینترنت نسخه ۴ به ۶ و بهره‌بردای از قابلیت‌ها، سرویس‌ها و توانایی‌های آن در کشور فراهم می گردد.

۲ تعاریف

اصطلاحات مورد استفاده در این سند دارای معانی مندرج در این ماده می باشند. سایر اصطلاحات مورد استفاده در این سند در موارد مقتضی دارای معانی مقرر در قوانین و یا مقررات خواهند بود.

۲-۱ پروتکل اینترنت (IP) نسخه ۴[3] : نسخه متداول پروتکل اینترنت است که با استفاده از مجموعه‌ای از پروتکل‌ها و توصیه‌نامه‌ها تحت عنوان TCP/IP شبکه فعلی اینترنت را راهبری می‌کند.

۲-۲ پروتکل اینترنت (IP) نسخه ۶[4] : نسخه جدید و آتی پروتکل اینترنت است. برای آشنایی با ویژگی‌ها و مزایای این نسخه نسبت به نسخه فعلی به پیوست یک مراجعه شود.

۲-۳ همزیستی[5] : به وجود همزمان یا استفاده همزمان از دو پروتکل اینترنت نسخه ۴ و ۶ در شبکه، همزیستی می‌گویند.

۲-۴ دو پشته پروتکلی[6] : پشتیبانی یک افزار شبکه بطور همزمان از پروتکل اینترنت نسخه ۴ و نسخه ۶ است.

۲-۵ گذر[7] : نشاندن یا قرار دادن پروتکل اینترنت نسخه ۶ به جای و یا به همراه پروتکل اینترنت نسخه ۴ است.

۲-۶ مهاجرت[8] : در این حوزه، معادل گذر است.

۲-۷ گره[9] : هر تجهیزی که به شبکه کامپیوتری متصل شود مانند مسیریاب، میزبان، گوشی‌های تلفن همراه و غیره.

۲-۸ گره فقط IP نسخه ۴ : گره‌هایی هستند که تنها با پروتکل اینترنت نسخه ۴ کار می‌کنند و قابلیت پشتیبانی از پروتکل اینترنت نسخه ۶ را ندارند.

---

[3] IPv4 (Internet Protocol version 4)
[4] IPv6(Internet Protocol version 6)
[5] Coexistence
6 Dual stack
[7] Transition
8 Migration
[9] Node

۲-۹ گره فقط IP نسخه ۶ : گره‌هایی هستند که تنها از پروتکل اینترنت نسخه ۶ پشتیبانی می‌کنند و قابلیت پشتیبانی از پروتکل اینترنت نسخه ۴ را ندارند.

۲-۱۰ گره های دو پروتکلی : گره‌هایی هستند که بطور همزمان از هر دو نسخه پشتیبانی می‌کنند.

۳ لزوم گذر

سازمان IANA در بالاترین سطح اینترنت مسئولیت تخصیص آدرس‌های عددی اینترنت را به عهده دارد. بنابر اعلان این سازمان، فضای قابل تخصیص آدرس پروتکل اینترنت نسخه ۴ به اتمام رسیده است و این امر مانع بزرگی برای توسعه شبکه اینترنت نسخه ۴ می‌باشد. علاوه بر آن، پروتکل اینترنت نسخه ۴ دارای نواقص و کمبودهایی است که پروتکل اینترنت نسخه ۶ برای برطرف کردن آنها تدوین شده است. برخی از معایب پروتکل اینترنت نسخه ۴ و مزایای پروتکل اینترنت نسخه ۶ به شرح زیر است: (برای اطلاعات بیشتر به پیوست شماره یک مراجعه شود.)

۳-۱ معایب و محدودیت‌های پروتکل اینترنت نسخه ٤ :

۳-۱-۱ فضای آدرس‌دهی محدود

۳-۱-۲ کیفیت سرویس پایین

۳-۱-۳ امنیت پایین

۳-۱-۴ عدم مسیریابی بهینه (کارایی پایین به هنگام مسیریابی)

۳-۱-۵ پیکربندی پیچیده (سخت)

۳-۱-۶ تحرک پذیری[10] کم

۳-۲ مزایای پروتکل اینترنت نسخه ٦:

۳-۲-۱ افزایش فضای آدرس‌دهی

۳-۲-۲ پیکربندی خودکار

۳-۲-۳ امنیت بالاتر

۳-۲-۴ مسیریابی کاراتر

[10] Mobility

۳-۲-۵ آدرس‌دهی با امکان ZeroConf (پیکربندی اتوماتیک)

۳- ۲-۶ سهولت در تغییر فراهم‌کننده سرویس (ISP) توسط کاربر

۳-۲-۷ سهولت در ارتباط چندگانه[11]

۳-۲-۸ پشتیبانی قوی از امکانات چندپخشی[12]

٤ الزامات

٤-١ الزامات عمومی:

۴-۱-۱ با توجه به مزایای موجود در پروتکل اینترنت نسخه ۶ و اینکه امروزه اکثر کشورهای جهان برنامه گذر به این پروتکل را در صدر فعالیت‌های زیرساختی فناوری اطلاعات خود قرار داده اند، بنابراین لازم است همه وزارتخانه‌ها، سازمان‌ها و شرکت‌های دولتی و خصوصی طوری برنامه‌ریزی نمایند که زیرساخت شبکه‌ها و سامانه‌های تحت شبکه خود را در مدت ۲ سال به این پروتکل مجهز نمایند.

۴-۱-۲ در راستای تحقق اهداف این سند، به کلیه دستگاه‌ها شامل وزارتخانه‌ها، نهادها، سازمان‌ها و شرکت‌های دولتی و عمومی غیر دولتی توصیه می شود:

۴-۱-۲-۱ ضمن برآورد هزینه‌های لازم برای استفاده از پروتکل اینترنت نسخه ۶، نسبت به پیش‌بینی آن در بودجه‌های سال جاری و سال‌های آتی خود اقدام نمایند. (برنامه ریزی و پرداختن به فرآیند گذر)

۴-۱-۲-۲ منابع انسانی کارآمد را برای طراحی، اجرا، نگهداری و رفع عیب تجهیزات و سامانه‌هایی که با پروتکل اینترنت نسخه ۶ کار می‌کنند، تأمین نمایند.

۴-۱-۲-۳ وظایف و مسؤلیت‌های ذینفعان را در پروسه گذر با دقت مشخص کنند.

۴-۱-۲-۴ برنامه‌ریزی دقیق و واقع‌گرایانه ای برای انجام فرآیند گذر تدوین نمایند.

۴-۱-۲-۵ برنامه زمانبندی مناسب و قابل سنجش برای تحقق طرح گذر تهیه و ارائه نمایند.

[11] Multi-Homing
[12] Multicasting

۴-۱-۲-۶ فرآیند گذر را مطابق با استانداردهای مصوبه مؤسسه استاندارد و تحقیقات صنعتی ایران و همچنین سازمان‌های جهانی متولی تدوین و توسعه پروتکل‌ها و استانداردهای شبکه (از جمله IETF[۱۳]، IANA[۱۴] و غیره) انجام دهند.

۴-۱-۲-۷ به نحو مقتضی از تجربیات موفق[۱۵] و پویای کشورها، سازمان‌ها و شرکت‌ها در سطح جهانی استفاده کنند.

تبصره ٤-۱: با توجه به تشکیل گروه ضربت IPv6 ایران با مرکزیت وزارت ارتباطات و فناوری اطلاعات و با مشارکت دانشگاه‌ها و سایر سازمان‌ها و ارگان‌های کشور، کلیه دستگاه‌ها می‌بایست مکانیزم‌های گذر پیشنهادی خود را با گروه مذکور نهایی نمایند.

تبصره ٤-۲: نقشه راه جامع‌گذر از طرف وزارت ارتباطات و فناوری اطلاعات در اختیار کلیه متقاضیان قرار خواهد گرفت.

٤-۲ الزامات فنی فرآیند گذر:

۴-۲-۱ عدم اختلال در کارکرد گره‌های موجود و عملکرد شبکه.

۴-۲-۲ توجه به اصل "عدم وقفه در ارائه خدمات".

۴-۲-۳ استفاده از راهکارهای سازگار با شبکه فعلی اینترنت جهت صرفه جویی در منابع شبکه.

۴-۲-۴ طراحی و پیاده‌سازی تدریجی راهکارهای گذر جهت جلوگیری از ایجاد اختلال در کارکرد شبکه.

تبصره ٤-۳: به منظور اطمینان از سازگاری مکانیزم گذر تدوین شده با شبکه موجود و در حال کار، به کلیه دستگاه‌ها توصیه می‌شود ابتدا سرویس‌های پروتکل اینترنت نسخه ۶ خود را بصورت گام به گام و در قالب طرح آزمایشی پیاده‌سازی نمایند و در صورت عدم بروز اختلال و وقفه، آن را به کل شبکه تعمیم دهند.

تبصره ٤-٤: شبکه پایلوت بایستی به گونه‌ای طراحی و پیاده‌سازی شود که ساختار تمامی لایه‌های شبکه اعم از هسته، لبه، توزیع و دسترسی و همچنین اتصالات کاربران را شامل شود.

[13] Internet Enginering Task Force
[14] Internet Assigned Numbers Authority
[15] Best practice

تبصره ٤-٥ : هر یک از مدیران فنی شبکهٔ دستگاه‌ها می‌بایست پس از مطالعه کامل و با توجه به ساختار شبکهٔ موجود نسبت به انتخاب فناوری‌ها و مکانیزم‌های گذر شبکه خود اقدام نمایند. (تعدادی از سرویس‌های مورد نظر در لایه های مختلف شبکه بعنوان نمونه در پیوست شماره دو آورده شده است).

۴-۲-۵ توجه به پروتکل‌ها و روش‌های امنیتی لازم در تمامی لایه‌های شبکه در طراحی مکانیزم‌های گذر توسط کلیه دستگاه‌ها

تبصره ٤-٦ : در این زمینه معیار "چارچوب پیوست امنیتی طرح‌های کلان فناوری اطلاعات و ارتباطات، تألیف کمیته تخصصی امنیت کار گروه مدیریت فاوا" خواهد بود.

۵ دامنه گذر

۵-۱ دامنه گذر شامل کلیه حوزه‌های شبکه‌های مبتنی بر پروتکل اینترنت در کشور است، از جمله: شبکه IP/MPLS شرکت ارتباطات زیرساخت، شبکه‌های اپراتورها، شبکه‌های تأمین کنندگان سرویس از قبیل شبکه‌های شهری[۱۶]، شبکه‌های دسترسی[۱۷] شبکه‌های بی‌سیم و سایر شبکه‌های مرتبط.

۵-۲ لازم است کلیه دستگاه‌ها نسبت به تهیه طرح گذر شبکه خود در سطح سرویس‌ها و پروتکل‌های مورد نیاز، مطابق راهبردهای ارائه شده در این سند اقدام نمایند. در ضمن همبندی‌ها و سناریوهای مندرج در طرح گذر بایستی از مدل کلی انتها به انتها[۱۸] پشتیبانی کند.

۵-۳ بدلیل تنوع زیاد فناوری‌ها در لایه‌های مختلف شبکه، برای ارائه یک طرح گذر کلان، کامل و دقیق لازم است دستگاه‌ها هریک از لایه‌های شبکه و ارتباط آن با لایه‌های دیگر را بررسی نمایند.

۵-۴ دستگاه‌های بایستی کلیه نیازمندی‌های گذر شامل نیازمندی‌های سمت مشترک (یا مشتری)، سمت تأمین کننده سرویس، اعم از نیازمندی‌های سخت‌افزاری، لخت‌افزاری و نرم‌افزاری را لحاظ نمایند.

٦ دست‌اندرکاران و ذینفعان گذر

۶-۱ دست‌اندرکاران و ذینفعان در امر گذر به چند دسته تقسیم می‌شوند:

[16] METRO
[17] ACCESS
[18] End to End

۶-۱-۱ سیاستگذاران و وضع‌کنندگان تدابیر امنیتی و مقرراتی

۶-۱-۲ سازمان‌ها، سرویس‌دهنده‌ها و اپراتورها بعنوان مالکان شبکه

۶-۱-۳ طراحان و مشاوران

۶-۱-۴ کاربران نهایی

تبصره ٦-۱: فهرست برخی از دست اندرکاران و ذینفعان در امر گذر و برخی از وظایف آنها در جدول پیوست شماره سه آمده است.

۶-۲ کلیه دست‌اندرکاران و ذینفعان می‌بایست تدابیر لازم برای مهاجرت به پروتکل اینترنت نسخه ۶ را به گونه‌ای اتخاذ نمایند که کمترین وقفه در سرویس، خدمات و امور جاری بوجود آید.

۶-۳ وزارت ارتباطات و فناوری اطلاعات بعنوان هماهنگ کننده بین دست‌اندرکاران و ذینفعان عمل خواهد کرد.

۶-۴ وزارت ارتباطات و فناوری اطلاعات، نقشه راه کامل گذر را به همراه جزئیات تهیه و در اختیار سایر دست‌اندرکاران قرار خواهد داد.

۶-۵ دست‌اندرکاران و ذینفعان به نحوی برنامه‌ریزی نمایند که تا پایان سال ۹۱ پروتکل اینترنت نسخه ۶ در کشور اجرایی شود.

۶-۶ توصیه می‌شود تمامی دست اندرکاران و ذینفعان به منظور کنترل و تسریع در انجام امور، اطمینان از کیفیت خروجی‌ها و افزایش اثربخشی فعالیت‌های خود در زمینه گذر را با وزارت ارتباطات و فناوری اطلاعات همسو نمایند.

۷ مراحل اجرایی گذر

۷-۱ مراحل اجرایی گذر با توجه به استانداردها و توصیه‌نامه‌های صادر شده از طرف سازمان‌های راهبری اینترنت[۱۹]، در چهار مرحله صورت می‌پذیرد که عبارتند از:

الف) آماده‌سازی[۲۰]

ب) بکارگیری اولیه[۲۱]

ج) بکارگیری وسیع[۲۲] پروتکل اینترنت نسخه ۶

[19] IETF, ISOC, WSIS, RIPE,ITU
[20] Preparation
[21] Initial Deployment

د) تفوق[۲۳] پروتکل اینترنت نسخه۶ به پروتکل اینترنت نسخه ۴

۷-۲ کلیه ذینفعان و دست‌اندرکاران لازم است برنامه گذر خود را مطابق مراحل اجرایی چهارگانه فوق تنظیم نمایند.

۷-۳ پیش بینی مدت زمان لازم برای مرحله آماده‌سازی ۳ ماه، بکارگیری اولیه که با اجرای پایلوت شروع می‌شود ۶ ماه، بکارگیری وسیع بین ۲ تا ۴ سال و برای تفوق بیش از ۴ سال می باشد. بدیهی است که این زمانها بسته به عوامل مختلف نظیر ابعاد شبکه، حجم و تنوع تجهیزات و ... متغیر است.

۸ تغییرات در سند راهبردی گذر

۸-۱ محتویات این سند بر اساس نیازهای جدید با تصویب کمیته راهبری گذر قابل تغییر و به روز شدن است.

۸-۲ کمیته راهبردی هر سال سند را بازبینی و در صورت لزوم بروز خواهد نمود.

۹ محدوده جغرافیایی

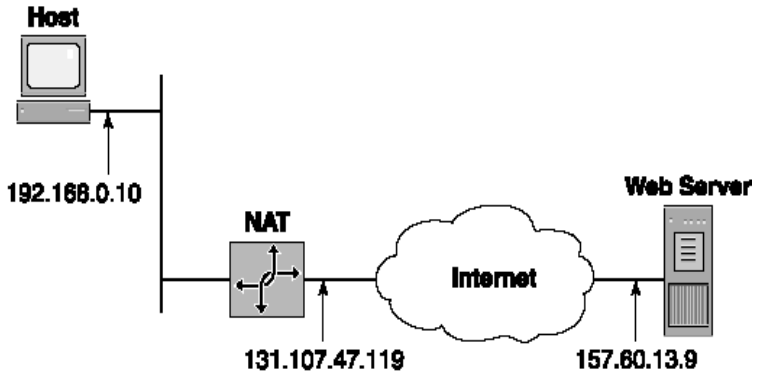
۹-۱ محدوده عمل سند، کشور جمهوری اسلامی ایران است.

[22] Co-existence
[23] Dominance

۱۰ پیوست شماره ۱

۱۰-۱ مقدمه‌ای بر IP نسخه ٦

رشد نمایی (سریع) شبکه اینترنت و اختصاص آدرس به میزبان‌ها و مسیریاب‌ها در شبکه‌هایIP نسخه ۴، سبب اتمام و در نتیجه کمبود سریع فضای آدرس شده است. این کمبود، بعضی از ارگان‌ها و سازمان‌ها را بر آن داشته است که از NAT[۲۴] استفـاده کرده و آدرس‌هـای خصوصی[۲۵] مختلف را به یک آدرس عمومی[۲۶] مربوط کنند. از آنجا که NATها استفاده از فضای آدرس‌های خصوصی را گسترش می‌دهند، نمی‌توانند تمامی جنبه‌های استانداردهای امنیتی موجود در لایه‌های مختلف شبکه را پشتیبانی کنند. همچنین نمی‌توانند عمل نگاشت آدرس‌های خصوصی را در پروتکل‌های لایه‌های بالاتر بخوبی انجام دهند و هنگام اتصال شبکه‌های دو سازمان مشکلات زیادی ایجاد می‌شود. بعلاوه گسـترش رو به رشد تجهیزات و افزارهایی که به شبکه اینترنت متصل می‌شوند و حتماً باید آدرس IP عمومی داشته باشند، اینترنت را با خطر جدی کمبود آدرس مواجه کرده است.



شکل ۱: استفاده از NAT در شبکه اینترنت

رشد سریع اینترنت، حجم جداول مسیریابی در مسیریاب‌های هسته مرکزی شبکه اینترنت را روز به روز افزایش داده و عمل مسیریابی و هدایت بسته‌ها را با کندی مواجه کرده است که در این صورت عمل مسیریابی در شبکه اینترنت، مسیریابی ساده و سلسله مراتبی خواهد بود و لذا بازدهی عمل میزبانی و کیفیت کاهش و تأخیر افزایش می یابد.

[24] Network Address Translator
[25] Not valid or private address
[26] Valid or public address

ایراد دیگری که در IP نسخه ۴ وجود دارد آن است که بسیاری از کارها و پیکربندی‌های آن بصورت دستی انجام می‌شود یا اینکه از پروتکل پیکربندی حالت کامل[۲۷] مانند DHCP [۲۸] استفاده می‌کند. با افزایش کامپیوترها و دیگر تجهیزاتی که از آدرس IP استفاده می‌کنند، به پیکربندی ساده و اتوماتیک آدرس‌ها و سایر روش‌های پیکربندی که نیاز به پیکربندی دستی و استفاده از ساختار DHCP وجود نداشته باشد، لازم است. مشکل دیگر، عدم وجود امنیت کافی و جلوگیری از مشاهده اطلاعات در طول انتقال در شبکه IP نسخه ۴ است، اگر چه در حال حاضر استاندارد IPSec امنیت بسته‌ها را تأمین می‌کند ولی این استاندارد در IP نسخه ۴ اختیاری بوده و بیشتر راه حل‌های اختصاصی شایع و متداول است.

نیاز به پشتیبانی از تحویل همزمان[۲۹] بسته‌ها که کیفیت سرویس نامیده می‌شود[۳۰]، در IP نسخه ۴ خیلی پایین است. هرچند استانداردهایی برای آن وجود دارد ولی پشتیبانی از ترافیک همزمان در IP نسخه ۴ در فیلد TOS[۳۱] و مشخصات payload قرار دارد که از پورت TCP یا UDP استفاده می‌کند که متاسفانه فیلد TOS در IP نسخه ۴ وظایف محدود داشته و بسیاری از اوقات تفسیر محلی از آن می‌شود همچنین تشخیص payload که از پورت UDP و TCP استفاده می‌کند در موقعیکه payload بسته رمز شده باشد، امکانپذیر نمی‌باشد.

گروه ضربت مهندسی اینترنت[۳۲] برای برطرف کردن نارسایی‌ها و عیب‌های اشاره شده، پروتکلIP نسخه ۶ را معرفی نمود، که بسیاری از روش‌ها و الگـوهایی که برای به روز کـردن پروتکل IP نسخه ۴ معرفی شده بود را شامل می‌شود و به گونه‌ای طراحی شده است که تاثیر زیادی بر کارکرد پروتکل‌های لایه‌های بالاتر و پایین‌تر نداشته باشد. پروتکل IP نسخه ۶ که در سال ۱۹۹۴ طراحی و به بازار آمد، چنان طراحی شده است که اولاً بتواند با IP نسخه ۴ کار کند و ثانیاً دارای فضای آدرس بیشتر، مسیریابی بهینه و امنیت بالا باشد. در اینجا به چند ویژگی IP نسخه ۶ به شرح زیر اشاره می‌کنیم:

۱. بهینه بودن سرآیندها[۳۳] در IP نسخه ۶
۲. فضای آدرس‌دهی ۱۲۸بیتی
۳. ساختار آدرس‌دهی و مسیریابی سلسله مراتبی و کارآمد
۴. پیکربندی آدرس Statefull و Stateless

[27] State full
[28] Dynamic Host Configuration Protocol
[29] Real time
[30] Quality of service
[31] Type of Service
[32] IETF (Internet Engineering Task Force)
[33] Header

۵. افزایش امنیت داخلی
۶. پشتیبانی بهتر از QOS
۷. پروتکل جدید برای پیدا کردن همسایه
۸. توسعه پذیری

در اینجا برخی از این ویژگی‌ها را بطور خلاصه بررسی می‌کنیم.

۱۰-۲ سرآیندهای بهینه

سرآیندهای IP نسخه ۶ دارای شکل جدید بوده و طوری طراحی شده است که پارامترهای اضافی آن را به حداقل برساند. این کار بوسیله حذف فیلدهای غیر ضروری و اضافه کردن سرآیندهای گسترش یافته[۳۴] که بعد از سرآیندهایIP نسخه ۶ اضافه می‌گردد، انجام می‌شود. سرآیندهای موثر IP نسخه ۶ در مسیریاب‌های مرکزی شبکه اینترنت دارای بازدهی و بهره وری بالایی از نظر پردازش هستند.

سرآیندهای IP نسخه ۶ و IP نسخه ۴ با همدیگر کار نمی‌کنند.IP نسخه ۶ دارای کارائی مناسب برای اینکه بتواند با IP نسخه ۴ سازگار باشد، نیست. برای اینکه یک میزبان یا مسیریاب سرآیندهای IP نسخه‌های ۶ و ۴ را تشخیص دهد و پردازش مربوط به هر دو را انجام دهد، بایستی هر دو نسخه همزمان بر روی آن اجرا شده باشد. اگرچه اندازه آدرس‌های IP نسخه ۶ چهار برابر اندازه آدرس‌هایIP نسخه ۴ است، سرآیندهای IP نسخه ۶ تنها دو برابر سرآیندهای IP نسخه ۴ هستند.

۱۰-۳ فضای آدرس دهی بالا

IP نسخه ۶ دارای آدرس IP مبدأ و مقصد ۱۲۸ بیتی (۱۶ بایتی) می‌باشد. با ۱۲۸ بیت می‌توان[۳۸]۱۰*۳.۴ ترکیب آدرس ایجاد کرد. این فضای آدرس‌دهی بالا طوری طراحی شده است که بتوان به سطوح مختلفی از زیرشبکه‌سازی[۳۵] و اختصاص فضای آدرس مختلف دسترسی داشت.

اگرچه در حال حاضر تنها تعداد کمتری از آدرس‌های ممکن IP نسخه ۶ توسط میزبان‌ها استفاده می‌شود ولی بسیاری از آدرس‌ها برای کاربردهای آینده رزرو شده است. با توجه به فضای آدرس بالای IP نسخه ۶، استفاده از مکانیزم‌های صرفه جویی در مصرف آدرس که در IP نسخه ۴ وجود دارد مانند روش‌های NAT و CIDR در IP نسخه ۶ مورد نیاز نمی‌باشد.

[34] Extension header
[35] Subnetting

۱۰-٤ ساختار مسیریابی و آدرس‌دهی مؤثر و سلسله مراتبی

آدرس‌های جهانیIP نسخه۶ [۳۶] که در شبکه جهانی اینترنت قابل استفاده بوده و مسیردهی می‌شوند، طوری طراحی شده است که ساختار مسیریابی سلسله مراتبی و قابلیت خلاصه‌سازی داشته باشد. این عمل، درخواست مشترک خیلی از تأمین‌کنندگان سرویس اینترنت می‌باشد. در اینترنت مبتنی بر IP نسخه ۶ مسیریاب‌های موجود در زیرساخت شبکه اینترنت و مسیریاب‌های تأمین‌کنندگان بزرگ سرویس اینترنت، دارای جداول مسیریابی با حجم کمتری نسبت به IP نسخه ۴ هستند.

۱۰-۵ پیکربندی آدرس حالت کامل و بدون حالت[۳۷]

برای ساده‌کردن پیکربندی میزبان‌ها، IP نسخه ۶ هم پیکربندی آدرس حالت کامل مانند پیکربندی با استفاده از سرویس‌دهنده DHCP و هم پیکربندی آدرس بدون حالت (پیکربندی بدون حضور سرویس‌دهندهDHCP) را پشتیبانی می‌کند. در حالت پیکربندی آدرس حالت کامل، میزبان‌ها بصورت اتوماتیک خود را با استفاده از آدرس لینک محلی IP نسخه ۶[۳۸] و همچنین با استفاده از پیشوندهایی[۳۹] که از مسیریاب‌های محلی اعلان شده است پیکربندی می‌کنند. حتی بدون وجود مسیریاب‌های محلی هم، میزبان‌های موجود در یک لینک با استفاده از آدرس لینک محلی خود را پیکربندی نموده و می‌توانند بدون نیاز به پیکربندی دستی با همدیگر ارتباط داشته باشند.

۱۰-٦ امنیت داخلی بالا

یکی از ویژگی‌های خوب IP نسخه ۶، پشتیبانی از IPSec است. این ویژگی یک راه حل استاندارد و منطقی برای ارتقاء و بهینه نمودن امنیت شبکه جهت ایجاد ارتباط بین دو شبکه IP نسخه ۶ می‌باشد. IP نسخه ۶ ترکیبی از توانایی‌های امنیتی تولید می‌کند، بویژه در IP نسخه ۶ توانایی پشتیبانی از احراز هویت و اختفاء[۴۰] را داریم.

---

[36] Aggregately Global Unicast Addresses
[37] Stateless
[38] Link-Local
[39] Prefix
[40] privacy

۱۰-۷ پشتیبانی بهینه از QoS

فیلدهای جدیدی در سرآیندهای IP نسخه ۶ طراحی شده است که مشخص می‌کند ترافیک شبکه چگونه مشخص شده و هدایت شود. جریان‌های ترافیکی که از فیلد Flow Label در سرآیندهایIP نسخه ۶ استفاده می‌کنند، به مسیریاب‌ها اجازه می‌دهند که روش‌های ارسال و دریافت متفاوت و خاصی برای هر کدام از بسته‌هایی[۴۱] که به مسیریاب وارد می‌شوند و از مبدای به مقصدی ارسال می‌شوند، مشخص کرده و آنها را به مقصد هدایت نماید. به دلیل اینکه نوع ترافیک با توجه به سرآیندIP نسخه ۶ مشخص می‌شود، بنابراین پشتیبانی از QoS را می توان بدست آورد، حتی اگر Payload بسته بوسیله IPsec رمز[۴۲] شده باشد.

۱۰-۸ پروتکل جدید برای ارتباط گره‌های همسایه[۴۳]

پروتکل پیدا کردن همسایه[۴۴] در IP نسخه ۶ یکی از پروتکل های سری ICMPv6[۴۵] است که ارتباط بین گره های همسایه‌ها را در IP نسخه ۶ مدیریت می‌کند. این پروتکل جایگزین پروتکل‌های ARP[۴۶]، ICMP4 RD و ICMPv4 RM که براساس خاصیت پخشی کار می‌کنند، می باشد و برای پیدا کردن همسایه از پیغامهای مبتنی بر چندپخشی و تک‌پخشی استفاده می‌کند و از خاصیت پخشی[۴۷] استفاده نمی‌کند.

۱۰-۹ قابلیت توسعه پذیری[۴۸]

IP نسخه ۶ را به‌راحتی می‌توان توسعه داده و ویژگی‌های جدیدی به آن اضافه نمود. این کار با اضافه کردن سرآیندهای گسترش‌دهنده بعد از سرآیندهای IP نسخه ۶ امکان‌پذیر می باشد. برخلاف سرآیند اختیاری IP نسخه ۴ که تنها از۴۰ بایت پشتیبانی‌می‌کند، اندازه سرآیندهای‌گسترش‌دهنده درIP نسخه ۶، تنها بوسیله اندازه بسته IP نسخه ۶ تعیین می‌شود.

---

[41] Packet
[42] Encrypt
[43] Neighboring Node Interaction
[44] Neighbor Discovery
[45] Internet Control Message protocol
[46] Address Resolution Protocol, Router Discovery, Redirect Message
[47] Broadcast
[48] Extensibility

۱۰-۱۱ اهم تفاوت‌های بین IP نسخه ٦ و IP نسخه ٤

در جدول شماره ۱ اهم تفاوت‌های بین IP نسخه ۶ و IP نسخه ۴ فهرست شده است.

IPv6	IPv4
آدرس‌های مبدا و مقصد ۱۲۸ بیتی (۱۶بایتی) هستند.	آدرس های مبدا و مقصد ۳۲ بیتی (۴ بایتی) هستند.
IPSec توسط IPv6 پشتیبانی می‌شود.	پشتیبانی از IPSec اختیاری است.
تشخیص جریان بسته‌ها برای بررسی QoS بوسیله مسیریاب در سرآیندهای IPv6 که از فیلد "flow label" استفاده می‌کند، وجود دارد.	تشخیص جریان بسته‌ها برای بررسی QoS بوسیله مسیریاب در حال حاضر با استفاده از سرآیندهای IPv4 انجام نمی‌شود.
عمل Fragmentation توسط مسیریاب‌ها انجام نمی‌شود و فقط توسط میزبان فرستنده انجام می‌شود.	عمل Fragmentation هم بوسیله مسیریاب‌هاو هم بوسیله میزبان فرستنده انجام می‌شود.
سرآیندها شامل checksum نیستند.	سرآیند ها شامل checksum هستند.
تمامی داده‌های اختیاری به سرآیندهای گسترش یافته (extended header) منتقل شده است.	سرآیندهای IPv4 دارای فیلد اختیاری (option) است.
ARP Request frameها با پیغام‌های Multicast Neighbor Solicitation جایگزین شده است.	پروتکل ARP از خاصیت پخشی خود استفاده می‌کند و ARP Request frame هایی را برای بدست آوردن آدرس‌های لایه دیتا لینک (MAC) می‌فرستد.
IGMP با پیغام های Multicast Listener Discovery (MLD) جایگزین شده است.	IGMP (Protocol Internet Group Management) جهت مدیریت اعضاء گروه زیر شبکه محلی مورد استفاده قرار می‌گیرد.
ICMP Router Discovery با پیغامهای ICMPv6 Router Solicitation و Router Advertisement جایگزین شده و اجباری است.	ICMP Router Discovery جهت مشخص کردن آدرس IPv4 بهترین دروازه (gateway) مورد استفاده قرار می گیرد و اختیاری است.
آدرس پخشی در IPv6 وجود ندارد بجای آن از آدرس‌های Link-local و آدرس های چندپخشی تمامی گره‌ها استفاده می‌کند.	آدرس‌های پخشی جهت ارسال ترافیک به همه گره‌های زیرشبکه مورد استفاده قرار می گیرد.
به پیکربندی دستی یا استفاده از DHCP نیازی نیست	عمل پیکربندی بصورت دستی یا با استفاده از DHCP است.
از رکوردهای منبع آدرس میزبان (AAAA) که در Domain Name System (DNS) وجود دارد برای مربوط کردن نام میزبان‌ها به آدرس آنها استفاده می‌شود.	از رکوردهای منبع آدرس میزبان (A) که در Domain Name System (DNS) وجود دارد استفاده می‌کند و نام میزبان‌ها را به آدرس های آنها مربوط می‌کند.
از رکوردهای منبع اشاره‌گر (PTR) که در دامنه IPv6.ARPA DNS قرار دارد استفاده می‌کند تا آدرس‌های IPv6 را به نام میزبان مربوط کند.	از رکوردهای منبع اشاره‌گر (PTR) که در دامنه ADDR.ARPA DNS قرار دارد استفاده می‌کند تا آدرس های IPv4 را به نام میزبان مربوط کند.

(جدول شماره ۱)

۱۱- پیوست ۲

در جدول شماره ۲ اهم فناوریها و سرویس‌های پایه نمونه فهرست شده است.

مکانیزم‌ها		میزبانها	فراهم‌کنندگان سرویس			
			شبکه دسترسی	شبکه مترو	شبکه‌های بیسیم	شبکه زیرساخت
ساختار شبکه	انواع سرویس‌ها و کاربردها	.v6 OS support .v6 applications (DHCP ،FTP ، HTTP،SMTP)	VoIP (H323v6 ،SIPv6) Video conferencing IP-TV	VoIP (H323v6 ،SIPv6) IPTV Multicast(IGMP)	VoIP (H323v6، SIPv6)	
	سرورها و درگاه‌های طرف شبکه	APP Servers DHCP AAA DNS SIP Proxy	DNS Firewalls IDS Appl. Servers (DHCP, FTP, HTTP، SMTP)	DNS BRAS Filtering	xGSNs	Automatic tunn. Manual tunn. DPI/LI
	سرویس‌های پایه شبکه	VRRP	NAT Security services	L2 Tunneling L3 Tunneling	.v6 IP mobility .v6 GPRS	.v6 L2/L3 VPN
	زیرساخت سوییچینگ و روتینگ		.v6 Addressing	.v6 Routing (OSPFv3، RIPv3 ،ISIS , BGP) Dual stack support .v6 Multicast	3G/4G .v6 support	.v6 ASN .v6 Routing (OSPFv3، RIPv3 ،ISIS , BGP) Dual stack support .v6 IP-MPLS .v6 Multicast

(جدول شماره ۲)

۱۲- پیوست ۳

در جدول شماره ۳، فهرست برخی از دست اندرکاران و ذینفعان در امر گذر و سرفصل بخشی از وظایف آنها آمده است.

نام ذینفع یا دست‌اندرکار	بخشی از وظایف گذر به IPv6
وزارت ارتباطات و فناوری اطلاعات	• مرجع سیاست گذاری عالی • وضع تدابیر امنیتی • ایجاد هماهنگی بین دست‌اندرکاران و ذینفعان • تصویب و ابلاغ نقشه راه گذر
سازمان فناوری اطلاعات ایران	• تهیه نقشه راه گذر • بومی‌سازی استانداردهای مربوطه • ساماندهی آدرس‌های عددی اینترنتی • فرهنگ‌سازی و آموزش
مؤسسه آموزش و تحقیقات ارتباطات و فناوری اطلاعات	• مطالعه، تحقیق و پژوهش
سازمان تنظیم مقررات و ارتباطات رادیویی	• تنظیم ضوابط و مقررات • نظارت و اعمال مقررات
شرکت ارتباطات زیرساخت	• ایجاد، توسعه، مدیریت و نگهداری زیرساخت شبکه ملی ارتباطات • تامین و توزیع پهنای باند بین‌الملل در شبکه ملی
دارندگان پروانه‌های ارتباطی و فناوری اطلاعات: (شرکت مخابرات ایران، شبکه علمی کشور، اپراتورهای تلفن همراه، ISP، ISDP، PAP، SAP، GMPCS و WiMAX)	• تجهیز، پشتیبانی و مدیریت شبکه‌های موضوع پروانه • ارائه انواع سرویس‌های موضوع پروانه
ارائه‌دهندگان خدمات میزبانی و محتوا	• تجهیز، پشتیبانی و مدیریت شبکه‌های ارائه خدمات میزبانی و محتوا • ارائه انواع سرویس‌های میزبانی و محتوا
تولیدکنندگان سخت‌افزار و نرم‌افزار	• طراحی، تولید و ارائه انواع سخت‌افزار و نرم‌افزار مورد نیاز در شبکه
سایر دستگاه‌های دولتی و غیر دولتی	• تجهیز، پشتیبانی و مدیریت شبکه‌های خود

(جدول شماره ۳)