



جمهوری اسلامی ایران

وزارت ارتباطات و فناوری اطلاعات

شماره: ۱,۷۸,۴۹
تاریخ: ۹۴,۹,۲۲
پیوست:

وزیر

دبیرخانه
سازمان فناوری اطلاعات
۲۷۸۷۷
۱۳۹۴/۰۹/۲۲

«کلیه دستگاه‌های اجرایی»

در راستای عملیاتی نمودن مصوبه شماره ۲۰۰/۳۸۳ مورخ ۹۴/۴/۸ که در هشتمین جلسه شورای عالی فناوری اطلاعات کشور تصویب و از طرف ریاست محترم جمهور با عنوان "مهاجرت از پروتکل اینترنت نسخه ۴ به ۶ (IPv4 به IPv6)" ابلاغ گردید، بدینوسیله سند «نیازمندی‌های IPv6 در تجهیزات ICT» که منطبق بر استانداردهای به روز بین‌المللی تهیه و تدوین شده است، برابر اصل ۱۳۸ قانون اساسی جمهوری اسلامی ایران جهت اجرا و رعایت مفاد آن به پیوست ابلاغ می‌شود. ضمناً کلیه دستگاه‌های اجرایی موضوع ماده (۵) خدمات کشوری و مراجع زیر موظف به رعایت مفاد سند مذکور هستند.

- ۱- دستگاه‌های اجرایی برای برگزاری مناقصه جهت خرید تجهیزات (سخت افزاری و نرم افزاری) ICT
- ۲- شرکت‌های تولیدکننده سخت‌افزار و نرم‌افزار ICT جهت طراحی، تولید و ارائه انواع سخت‌افزارها و نرم‌افزارهای مورد نیاز شبکه
- ۳- شرکت‌های واردکننده تجهیزات سخت‌افزاری و نرم‌افزاری ICT در زمان خرید تجهیزات از شرکت‌های خارجی

- ۴- آزمایشگاه‌های تجهیزات ICT جهت ارزیابی تجهیزات از نظر پشتیبانی از پروتکل IPv6
- ۵- اپراتورهای دارنده پروانه‌های ارتباطی و فناوری اطلاعات جهت تجهیز، پشتیبانی، مدیریت و ارائه سرویس
- ۶- ارائه دهندگان خدمات میزبانی و محتوا جهت تجهیز، پشتیبانی، مدیریت و ارائه خدمات میزبانی و محتوا
- ۷- مراکز دانشگاهی و تحقیقاتی جهت آموزش به عنوان مرجع پشتیبانی‌کننده تجهیزات از IPv6

محمود واعظی

رونوشت:

- معاون محترم وزیر و رئیس سازمان فناوری اطلاعات ایران
- رئیس محترم مرکز روابط عمومی و اطلاع رسانی جهت اطلاع رسانی از طریق سایت وزارت
- دفتر وزارتی (۳۰۸۵۶-۷۳۴۰۵-۷۵۷۰۴)

شماره: ۲۴۳۸۳
تاریخ: ۱۴۹۴ ر ۴۸
پوست:
ارحیت:
طبقه بندی:

مصوبه هشتمین جلسه شورای عالی فناوری اطلاعات کشور

شورای عالی فناوری اطلاعات کشور در هشتمین جلسه مورخ ۱۳۹۳/۱۰/۲۲ در راستای سیاست‌های کلی توسعه فناوری اطلاعات، اقتصاد مقاومتی ابلاغی مقام معظم رهبری و برنامه پنجم توسعه جمهوری اسلامی ایران و باهدف هماهنگی و تعامل دستگاه‌های اجرایی جهت یکپارچگی و توسعه متوازن و نظام‌مند فناوری اطلاعات، موارد دستور العمل مهاجرت از پروتکل اینترنت نسخه ۴ به ۶ (IPv4 به IPv6) به شرح زیر (ممهور به مهر دبیرخانه شورای عالی فناوری اطلاعات کشور) را تصویب نمود.

مقدمه:

بهره‌گیری از خدمات شبکه ارتباطی و گسترش فناوری اطلاعات در کشور و کاهش شکاف دیجیتالی^۱ و هویت‌دار کردن فعالیت‌های دنیای مجازی، مستلزم استفاده از منابع اینترنتی معتبر و قابل‌ردیابی است. بر اساس اعلان سازمان‌های بین‌المللی از جمله سازمان منابع شبکه (NRO^۲)، منابع موجود در اینترنت نسخه ۴ رو به اتمام بوده و دست‌اندرکاران شبکه‌ها و سایر تأمین‌کنندگان سرویس، دیگر قادر به گسترش شبکه خود با منابع موجود نخواهند بود.

کشور ما در حال توسعه زیرساخت‌های ارتباطی فناوری اطلاعات بوده و برای این توسعه نیاز به منابع شبکه است و منابع عددی اینترنتی نسخه ۴ در حال اتمام است و با استفاده از این نسخه، توسعه فناوری اطلاعات در کشور مقدور نخواهد بود. از طرفی اکثر کشورهای جهان با شتاب به سمت استفاده از پروتکل اینترنت نسخه ۶ که دارای امنیت بیشتر، کیفیت بالاتر، تحرک پذیری بیشتر، پیکربندی خودکار و آسان‌تر است، 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، بیان‌کننده 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. نقشه راه حاضر در راستای مأموریت‌های کلان وزارت ارتباطات و فناوری اطلاعات به‌منظور توسعه فناوری اطلاعات در کشور و بهبود وضعیت شبکه IP کنونی کشور، رفع نواقص و مشکلات آن با به‌کارگیری پروتکل اینترنت نسخه ۶ باهدف ارتقاء بازده کاری و کاهش هزینه‌ها تهیه شده است. اجرای 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 بهره‌برداری از قابلیت‌ها، سرویس‌ها و توانایی‌های آن در کشور فراهم می‌شود.

ماده ۱- تعاریف:

در این مصوبه اصطلاحات زیر در معانی مشروح مربوطه به کار می‌روند.

- ۱-۱- وزارت: وزارت ارتباطات و فناوری اطلاعات
- ۲-۱- سازمان: سازمان فناوری اطلاعات ایران
- ۳-۱- دستگاه‌های اجرایی: دستگاه‌های مشمول ماده ۵ قانون مدیریت خدمات کشوری

^۱ Digital divide

^۲ Number Resource Organization



شماره: ۲۰۱۷/۳۸۳
تاریخ: ۱۳۹۴/۴/۸
پوست
ارحمت
طبقه بندی:

- ۳-۱- نشانی IP^۳: نشانی پروتکل اینترنت، برچسب عددی است که به تجهیزات در شبکه‌های رایانه‌ای اختصاص پیدا می‌کند و به منظور اتصال بین گره‌های شبکه^۴ استفاده می‌شود.
- ۵-۱- پروتکل اینترنت (IP) نسخه^۵: نسخه متداول پروتکل اینترنت است که با استفاده از مجموعه‌ای از پروتکل‌ها و توصیه‌نامه‌ها تحت عنوان TCP/IP شبکه فعلی اینترنت را راهبری می‌کند.
- ۶-۱- پروتکل اینترنت (IP) نسخه^۶: نسخه جدید و آتی پروتکل اینترنت است.
- ۷-۱- همزیستی^۷: به وجود همزمان یا استفاده همزمان از دو پروتکل اینترنت نسخه ۴ و ۶ در شبکه، همزیستی می‌گویند.
- ۸-۱- دوپشته پروتکلی^۸: پشتیبانی یک افزار شبکه به‌طور همزمان از پروتکل اینترنت نسخه ۴ و نسخه ۶ است.
- ۹-۱- گذر^۹: نشانیدن یا قرار دادن پروتکل اینترنت نسخه ۶ به جای و یا به همراه پروتکل اینترنت نسخه ۴ است.
- ۱۰-۱- مهاجرت^{۱۰}: در این حوزه، معادل گذراست.
- ۱۱-۱- گره^{۱۱}: هر تجهیزیزی که به شبکه کامپیوتری متصل شود مانند مسیریاب، میزبان، گوشی‌های تلفن همراه و غیره.
- ۱۲-۱- 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.
- ۱۳-۱- 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.
- ۱۴-۱- گره‌های دو پروتکلی: گره‌هایی هستند که به‌طور همزمان از هر دو نسخه پشتیبانی می‌کنند.

ماده ۲- اهداف:

- ۱-۲- توسعه خدمات الکترونیکی
۲-۲- توسعه شبکه‌ی ملی اطلاعات
۳-۲- گذر به IPv6 در کشور
۴-۲- جلوگیری از هزینه‌های مضاعف دستگاه‌های اجرایی
۵-۲- ایجاد امکان مدیریت منابع اینترنتی کشور

ماده ۳- الزامات تجهیزات:

- ۱-۳- تولیدکنندگان داخلی تجهیزات سخت‌افزاری و نرم‌افزاری موظف‌اند کلیه تجهیزات تولیدی خود را با قابلیت پشتیبانی همزمان از IPv4 و IPv6 تولید و ارائه نمایند.

- ۲-۳- استفاده، ارائه، تولید و واردات کلیه تجهیزات سخت‌افزاری و نرم‌افزاری با قابلیت پشتیبانی همزمان از IPv4 و IPv6

ماده ۴- تکالیف و وظائف:

- ۱-۴- سازمان تنظیم مقررات و ارتباطات رادیویی موظف است برای اجازه ترخیص کالاها از گمرکات الزامات ماده ۳ را رعایت نماید.

³ Internet Protocol

⁴ Nodes

⁵ IPv4 (Internet Protocol version 4)

⁶ IPv6 (Internet Protocol version 6)

⁷ Coexistence

⁸ Dual stack

⁹ Transition

¹⁰ Migration

¹¹ Node

بسمتعالی
جمهوری اسلامی ایران
وزارت ارتباطات و فناوری اطلاعات


دبیرخانه شورای عالی فناوری اطلاعات

شماره: ۲۰۰/۱۳۸۳
تاریخ: ۱۳۹۴/۴/۸
پیوست:
ارجحیت:
طبقه بندی:

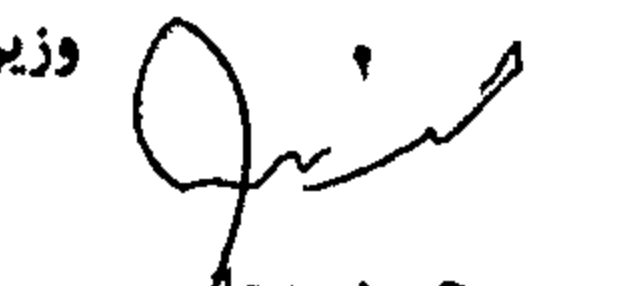
- ۲-۴- سازمان تنظیم مقررات و ارتباطات رادیویی موظف است حداکثر ظرف سه ماه نسبت به ایجاد سامانه‌ی اطلاع‌رسانی در خصوص تجهیزات (سخت‌افزاری و نرم‌افزاری) که الزامات موضوع این آیین‌نامه را رعایت می‌کنند اقدام نماید
- ۳-۴- گمرک جمهوری اسلامی موظف است نسبت به ترخیص تجهیزات (سخت‌افزاری و نرم‌افزاری) اقدام نماید که بنا به تأیید سازمان تنظیم مقررات و ارتباطات رادیویی الزامات این آیین‌نامه رعایت شده است.
- ۴-۴- وزارت صنعت، معدن و تجارت موظف است نسبت به بازنگری و تمدید پروانه‌ی بهره‌برداری تولیدکنندگان داخلی اقدام نماید که مطابق تأیید سازمان تنظیم مقررات و ارتباطات رادیویی الزامات موضوع این آیین‌نامه را رعایت نموده‌اند.
- ۵-۴- کلیه‌ی دستگاه‌های اجرایی موظف‌اند در خرید هرگونه تجهیزات سخت‌افزاری و نرم‌افزاری نسبت به رعایت الزامات فوق اقدام نمایند.
- ۶-۴- سازمان موظف است با ایجاد سامانه‌ای نسبت به مدیریت و توزیع آدرس‌های عددی اینترنتی در کشور اقدام نماید. کلیه‌ی فراهم‌کنندگان خدمات زیرساختی، ارتباطی و میزبانی داخلی اعم از دولتی و غیردولتی موظف‌اند ضمن رعایت الزامات موضوع این آیین‌نامه اطلاعات مربوط به آدرس‌های عددی خود را به صورت الکترونیکی و برخط در اختیار این سامانه قرار دهند.
- ۷-۴- سازمان موظف است ظرف سه ماه نسبت به ارائه‌ی برنامه‌ی زمان‌بندی و روش مهاجرت به IPv6 اقدام نماید و کلیه‌ی دستگاه‌ها و اپراتورها موظف‌اند مطابق برنامه‌ی اعلامی سازمان نسبت به مهاجرت به IPv6 اقدام نمایند.
- ۸-۴- سازمان تنظیم مقررات و ارتباطات رادیویی موظف است از طریق اختیارات قانونی و مقرراتی خود نسبت به ممانعت از ارائه خدمات به آدرس‌های عددی ثبت‌نشده در سامانه موضوع این دستورالعمل اقدام نماید.

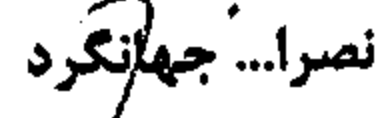
ماده ۵- نظارت:

- ۱-۵- نظارت بر حسن اجرای این آیین‌نامه بر عهده سازمان است. کلیه دستگاه‌های اجرایی و دارندگان پروانه فعالیت از سازمان تنظیم مقررات و ارتباطات رادیویی شرکت‌های ارائه‌دهنده خدمات میزبانی موظف به همکاری با سازمان در اجرای این دستورالعمل هستند.


محمود واعظی

وزیر ارتباطات و فناوری اطلاعات


حسن روحانی
رئیس‌جمهور و رئیس شورا


نصرا... جهانگرد
دبیر شورا



پوست

مصوبه مهاجرت از پروتکل اینترنت نسخه ۴ به ۶ (IPv4 به IPv6)

مقدمه

بهره‌گیری از خدمات شبکه ارتباطی و گسترش فناوری اطلاعات در کشور و کاهش شکاف دیجیتالی^۱ و هویت‌دار کردن فعالیت‌های دنیای مجازی، مستلزم استفاده از منابع اینترنتی معتبر و قابل‌ردیابی است. بر اساس اعلان سازمان‌های بین‌المللی از جمله سازمان منابع شبکه (NRO^۲)، منابع موجود در اینترنت نسخه ۴ رو به اتمام بوده و دست‌اندرکاران شبکه‌ها و سایر تأمین‌کنندگان سرویس، دیگر قادر به گسترش شبکه خود با منابع موجود نخواهند بود.

کشور ما در حال توسعه زیرساخت‌های ارتباطی فناوری اطلاعات بوده و برای این توسعه نیاز به منابع شبکه است و منابع عددی اینترنتی نسخه ۴ در حال اتمام است و با استفاده از این نسخه، توسعه فناوری اطلاعات در کشور مقدور نخواهد بود. از طرفی اکثر کشورهای جهان با شتاب به سمت استفاده از پروتکل اینترنت نسخه ۶ که دارای امنیت بیشتر، کیفیت بالاتر، تحرک پذیری بیشتر، پیکربندی خودکار و آسان‌تر است، 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، بیان‌کننده 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. نقشه راه حاضر در راستای مأموریت‌های 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 به‌کارگیری پروتکل اینترنت نسخه ۶ با هدف ارتقاء بازده کاری و کاهش هزینه‌ها تهیه شده است. اجرای 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 بهره‌برداری از قابلیت‌ها، سرویس‌ها و توانایی‌های آن در کشور فراهم می‌شود.

^۱ Digital divide

^۲ Number Resource Organization



توسعه فناوری اطلاعات

وزارت ارتباطات و فناوری اطلاعات

ماده ۱- تعاریف:

- در این مصوبه اصطلاحات زیر در معانی مشروح مربوطه به کار می‌روند.
- ۱-۱- وزارت: وزارت ارتباطات و فناوری اطلاعات
 - ۲-۱- سازمان: سازمان فناوری اطلاعات ایران
 - ۳-۱- دستگاه‌های اجرایی: دستگاه‌های مشمول ماده ۵ قانون مدیریت خدمات کشوری
 - ۴-۱- نشانی IP^۲: نشانی پروتکل اینترنت، برچسب عددی است که به تجهیزات در شبکه‌های رایانه‌ای اختصاص پیدا می‌کند و به منظور اتصال بین گره‌های شبکه^۳ استفاده می‌شود.
 - ۵-۱- پروتکل اینترنت (IP) نسخه^۴: نسخه متداول پروتکل اینترنت است که با استفاده از مجموعه‌ای از پروتکل‌ها و توصیه‌نامه‌ها تحت عنوان TCP/IP شبکه فعلی اینترنت را راهبری می‌کند.
 - ۶-۱- پروتکل اینترنت (IP) نسخه^۵: نسخه جدید و آتی پروتکل اینترنت است.
 - ۷-۱- همزیستی^۶: به وجود همزمان یا استفاده همزمان از دو پروتکل اینترنت نسخه ۴ و ۶ در شبکه، همزیستی می‌گویند.
 - ۸-۱- دوپشته پروتکلی^۷: پشتیبانی یک افزار شبکه به طور همزمان از پروتکل اینترنت نسخه ۴ و نسخه ۶ است.
 - ۹-۱- گذر^۸: نشانیدن یا قرار دادن پروتکل اینترنت نسخه ۶ به جای و یا به همراه پروتکل اینترنت نسخه ۴ است.
 - ۱۰-۱- مهاجرت^۹: در این حوزه، معادل گذراست.
 - ۱۱-۱- گره^{۱۰}: هر تجهیزیزی که به شبکه کامپیوتری متصل شود مانند مسیریاب، میزبان، گوشی‌های تلفن همراه و غیره.
 - ۱۲-۱- 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.

^۲ Internet Protocol

^۳ Nodes

^۴ IPv۴ (Internet Protocol version ۴)

^۵ IPv۶ (Internet Protocol version ۶)

^۶ Coexistence

^۷ Dual stack

^۸ Transition

^۹ Migration

^{۱۰} Node

وزارت ارتباطات و فناوری اطلاعات

- ۱-۱۳- 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.
- ۱-۱۴- گره‌های دو پروتکلی: گره‌هایی هستند که به‌طور همزمان از هر دو نسخه پشتیبانی می‌کنند.

ماده ۲- اهداف:

- ۱-۲- توسعه خدمات الکترونیکی
۲-۲- توسعه شبکه ملی اطلاعات
۳-۲- گذر به IPv۶ در کشور
۴-۲- جلوگیری از هزینه‌های مضاعف دستگاه‌های اجرایی
۵-۲- ایجاد امکان مدیریت منابع اینترنتی کشور

ماده ۳- الزامات تجهیزات:

- ۱-۳- تولیدکنندگان داخلی تجهیزات سخت‌افزاری و نرم‌افزاری موظف‌اند کلیه تجهیزات تولیدی خود را با قابلیت پشتیبانی همزمان از IPv۶ و IPv۴ تولید و ارائه نمایند.
- ۲-۳- واردکنندگان تجهیزات سخت‌افزاری و نرم‌افزاری موظف‌اند تنها تجهیزاتی را وارد کشور نمایند که قابلیت پشتیبانی همزمان از IPv۶ و IPv۴ را دارند.

ماده ۴- تکالیف و وظایف:

- ۱-۴- سازمان تنظیم مقررات و ارتباطات رادیویی موظف است برای اجازه ترخیص کالاها از گمرکات الزامات ماده ۳ را رعایت نماید.
- ۲-۴- سازمان تنظیم مقررات و ارتباطات رادیویی موظف است حداکثر ظرف سه ماه نسبت به ایجاد سامانه‌ی اطلاع‌رسانی در خصوص تجهیزات (سخت‌افزاری و نرم‌افزاری) که الزامات موضوع این آیین‌نامه را رعایت می‌کنند اقدام نماید.
- ۳-۴- گمرک جمهوری اسلامی موظف است نسبت به ترخیص تجهیزات (سخت‌افزاری و نرم‌افزاری) اقدام نماید که بنا به تأیید سازمان تنظیم مقررات و ارتباطات رادیویی الزامات این آیین‌نامه رعایت شده است.
- ۴-۴- وزارت صنعت، معدن و تجارت موظف است نسبت به بازنگری و تمدید پروانه‌ی بهره‌برداری تولیدکنندگان داخلی اقدام نماید که مطابق تأیید سازمان تنظیم مقررات و ارتباطات رادیویی الزامات موضوع این آیین‌نامه را رعایت نموده‌اند.

وزارت ارتباطات و فناوری اطلاعات

شماره:
تاریخ:
پست:

۴-۵- کلیدی دستگاه‌های اجرایی موظف‌اند در خرید هرگونه تجهیزات سخت‌افزاری و نرم‌افزاری نسبت به رعایت الزامات فوق اقدام نمایند.

۴-۶- سازمان موظف است با ایجاد سامانه‌ای نسبت به مدیریت و توزیع آدرس‌های عددی اینترنتی در کشور اقدام نماید. کلیدی فراهم‌کنندگان خدمات زیرساختی، ارتباطی و میزبانی داخلی اعم از دولتی و غیردولتی موظف‌اند ضمن رعایت الزامات موضوع این آیین‌نامه اطلاعات مربوط به آدرس‌های عددی خود را به صورت الکترونیکی و برخط در اختیار این سامانه قرار دهند.

۴-۷- سازمان موظف است ظرف سه ماه نسبت به ارائه برنامه‌ی زمان‌بندی و روش مهاجرت به IPv۶ اقدام نماید و کلیدی دستگاه‌ها و اپراتورها موظف‌اند مطابق برنامه‌ی اعلامی سازمان نسبت به مهاجرت به IPv۶ اقدام نمایند.

۴-۸- سازمان تنظیم مقررات و ارتباطات رادیویی موظف است از طریق اختیارات قانونی و مقرراتی خود نسبت به ممانعت از ارائه خدمات به آدرس‌های عددی ثبت‌نشده در سامانه موضوع این دستورالعمل اقدام نماید.

ماده ۵- نظارت:

۵-۱- نظارت بر حسن اجرای این آیین‌نامه بر عهده سازمان است. کلیدی دستگاه‌های اجرایی و دارندگان پروانه فعالیت از سازمان تنظیم مقررات و ارتباطات رادیویی شرکت‌های ارائه‌دهنده خدمات میزبانی موظف به همکاری با سازمان در اجرای این دستورالعمل هستند.





وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

نیازمندی های IPv6

در تجهیزات ICT

معاونت توسعه و مدیریت شبکه ملی اطلاعات
اداره کل مدیریت یکپارچه شبکه ملی اطلاعات

تهیه کنندگان:

بهروز عباس زاده - خدیجه فضائلی - محبوبه چنگیزی

مهرماه ۱۳۹۴



فهرست مطالب

صفحه	عنوان
۲	مقدمه
۳	موارد و نیازمندی‌های عمومی
۳	اطلاعات عمومی در خصوص نحوه استفاده از این سند
۳	تعیین نیازمندی‌ها
۳	پیشنهاد‌های لازم برای برگزارکننده مناقصه
۴	فهرست استانداردهای RFC/3GPP اجباری و اختیاری مورد نیاز برای سخت‌افزار و نرم‌افزارهای مختلف
۴	IPsec اجباری یا اختیاری؟
۵	تعریف تجهیزات شبکه و مراکز داده و شرح مختصر آن‌ها
۷	فهرست استانداردهای RFC/3GPP مورد نیاز برای انواع سخت‌افزارها
۷	نیازمندی‌های تجهیزات میزبان
۸	نیازمندی‌های تجهیزات لایه ۲ (سوئیچ‌های لایه ۲) در سمت مصرف‌کننده
۹	نیازمندی‌های تجهیزات لایه ۳ (مسیریاب‌ها و سوئیچ‌های لایه ۳) در سمت تأمین‌کنندگان سرویس (ISP)
۱۲	نیازمندی‌های تجهیزات امنیت شبکه
۱۴	نیازمندی‌های تجهیزات سمت مشتری (CPE)
۱۵	نیازمندی‌های تجهیزات متحرک (موبایل)
۱۶	استانداردهای 3GPP
۱۶	RFCهای IETF
۱۷	نیازمندی‌های تعدیل‌کننده‌های بار (Load Balancers)
۱۹	نیازمندی‌های پشتیبانی از IPv6 در نرم‌افزار
۱۹	مهارت‌های مورد نیاز برای یکپارچه‌سازی سامانه‌ها
۲۰	اظهارنامه صلاحیت IPv6



مقدمه

با توجه به روند جهانی مهاجرت به سمت IPv6 به منظور اطمینان از صحت کارکرد و مقرون به صرفه بودن پیاده‌سازی IPv6 در شبکه‌ها ضروری است. کلیه دستگاه‌های اجرایی (موضوع قانون برنامه‌ی پنجم توسعه، قانون مدیریت خدمات کشوری، قانون تنظیم بخشی از مقررات مالی دولت)، بخش عمومی و بخش غیردولتی و خصوصی و نهایتاً کلیه دارندگان شبکه IP در زمان برگزاری مناقصه و یا خرید تجهیزات ICT (اعم از سخت‌افزاری و نرم‌افزاری) نیازمندی‌های سازگاری آن‌ها با IPv6 را لحاظ نمایند. برای نیل به این منظور و در راستای تکمیل مصوبه شورای عالی فناوری اطلاعات کشور با عنوان «دستورالعمل مهاجرت از پروتکل اینترنت نسخه ۴ به ۶ (IPv4 به IPv6) ابلاغی طی نامه شماره ۳۸۳/۲۰۰ مورخ ۹۴/۴/۸»، سند نیازمندی‌های IPv6 در تجهیزات ICT به عنوان بهترین تجربه جاری^۱ (BCP) و به شرح مندرجات سند حاضر تهیه شده است.

این سند برای استفاده دستگاه‌های اجرایی و سازمان‌ها و نهادهای عمومی و غیردولتی، شرکت‌های تجاری بزرگ، متوسط و غیره بوده و مشخص می‌کند که چه ویژگی‌ها، پروتکل‌ها و استانداردهایی را در اسناد مناقصه‌ی خود لحاظ نمایند تا تجهیزاتی که خریداری می‌کنند، استانداردهای مورد نیاز برای پشتیبانی از IPv6 را داشته و شبکه‌ی آن‌ها را در زمان گذر دچار چالش نکند. همچنین این سند می‌تواند توسط پیمانکاران، تامین‌کنندگان کالا، مشاوران و کلیه کسانی که در مناقصات و استعلام‌های دستگاه‌های اجرایی و شرکت‌های غیردولتی شرکت می‌کنند نیز مورد استفاده قرار گیرد.

توجه:

- ۱- استانداردهایی که در این سند به آن‌ها اشاره شده توسط مراجع و نهادهای بین‌المللی مختلف ارایه شده است که اغلب آن‌ها فعالیت مستقل دارند و ما در این جا به جمع‌آوری آن‌ها اقدام کردیم.
- ۲- در زمان تهیه این سند سعی شده که آخرین نسخه استانداردها و RFCهای اشاره شده، آورده شود و در صورت تغییر در هر کدام از آنها، نسخه نهایی جایگزین نسخه جاری خواهد شد.
- ۳- این سند مطابق RFC6434 تهیه شده و کلیه نیازمندی‌های IPv6 در شبکه‌های IP را تحت پوشش قرار می‌دهد^۲. استانداردها و RFCهای به کار رفته در این سند به هشت قسمت کلی تقسیم شده است که در بخش‌های بعدی به آن‌ها اشاره می‌کنیم.
- ۴- برخی از توصیه‌نامه‌ها و استانداردهای آورده شده در این سند مبتنی بر مستندات ارایه شده از سوی NIST/USGv6 است.^۳

^۱Best Current Practice

^۲این RFC به عنوان یک راهنمای عمومی توسط IETF به منظور تعیین ویژگی‌هایی از IPv6 بر روی تجهیزات مختلف ارایه شده است.

^۳<http://www.antd.nist.gov/usgv6/>



موارد و نیازمندی‌های عمومی

اطلاعات عمومی در خصوص نحوه استفاده از این سند

گواهی‌نامه IPv6 Ready Logo می‌تواند به‌عنوان یک لوگوی تأیید برای هر تجهیزتی باشد. این ساده‌ترین راه برای فروشندگان تجهیزات است تا اثبات کنند که تجهیزات آن‌ها نیازمندی‌های اصلی IPv6 را پشتیبانی می‌کند. علاوه بر آن مناقصه‌گزار می‌تواند فهرستی از نیازمندی‌های اجباری مورد نیاز خود را که در این سند به آن‌ها اشاره نشده است شامل RFCها و استانداردهای مختلف، تهیه و به اسناد مناقصه خود ضمیمه نماید.

در زمان نوشتن فهرست RFCها و استانداردهای مورد نیاز باید همه نیازهای اجباری فهرست شود و اگر مورد یا مواردی به‌صورت شرطی مورد نیاز باشد، مناقصه‌گزار می‌تواند آن را هم به‌صورت مشروط و هم به‌صورت اجباری (بسته به نیاز خود) اضافه نماید. نکته قابل توجه آن است که تنها مناقصه‌گزار می‌تواند تشخیص دهد که کدام یک از RFCها و استانداردهای حاضر ضروری هستند و تشخیص این امر با خود اوست.

تعیین نیازمندی‌ها

برخی از تولیدکنندگان تجهیزات ادعا می‌کنند که تجهیزات آن‌ها دارای گواهی‌نامه IPv6 Ready Logo است، برای اطمینان از نحوه‌ی پشتیبانی تجهیزات اشاره شده در مناقصات، مناقصه‌گران می‌توانند تجهیزات انتخابی خود را در سایت با آدرس <http://www.IPv6ready.org/> بررسی نموده و با استانداردها و RFCهای مورد نظر خود تطابق دهند. علاوه بر IPv6 Ready Logo سایت دیگری با آدرس <http://www.boundv6.org/> وجود دارد که می‌توان قابلیت پشتیبانی از IPv6 توسط تجهیزات شبکه و برنامه‌های کاربردی را در آن جست‌وجو کرد.

پیشنادهای لازم برای برگزارکننده مناقصه

اگر برخی از ویژگی‌ها، استانداردها و RFCهای مورد نیاز مناقصه‌گزار در این سند آورده نشده است، وی می‌تواند خود آن را اضافه نماید. مناقصه‌گزاران کافی است متن زیر را به‌عنوان یک جمله عمومی در اسناد مناقصه‌ی خود اضافه نمایند:



نیازمندی‌های IPv6 در تجهیزات ICT

صفحه ۴ از ۲۱

"تمامی سخت‌افزارهای ICT موضوع این مناقصه باید از هر دو پروتکل IPv4 و IPv6 پشتیبانی نمایند. این پشتیبانی شامل مواردی همچون ورودی، خروجی، توان عملیاتی، کارایی جریان داده‌ها، انتقال و پردازش بسته‌ها است. هر نرم‌افزاری که از طریق پروتکل IP ارتباط برقرار می‌کند باید هر دو نسخه از پروتکل (IPv4, IPv6) را پشتیبانی کرده و تفاوت آن‌ها برای کاربران انتهایی شبکه قابل توجه نباشد. پشتیبانی از IPv6 می‌تواند توسط گواهینامه IPv6 Ready Logo تایید شود."

تجهیزاتی که دارای گواهینامه IPv6 Ready Logo نباشند، باید RFC‌های فهرست شده در زیر را پشتیبانی نمایند. فهرست RFC‌های اجباری و اختیاری به شرح زیر است:

فهرست استانداردهای RFC/3GPP اجباری و اختیاری مورد نیاز برای سخت‌افزار و نرم‌افزارهای مختلف

این نیازمندی‌ها براساس تجهیزات سخت‌افزاری و پشتیبانی یکپارچه‌کننده^۴ تقسیم می‌شوند. با توجه به این که تمام ترافیک مبتنی بر IPv4 در آینده به IPv6 مهاجرت خواهد کرد، لذا تمام نیازمندی‌هایی که بر اساس قابلیت‌های ترافیک IPv4 استوار است مانند تأخیر، پهنای باند، توان عملیاتی^۵ و غیره باید در ترافیک‌های IPv6 هم ضروری باشند.

IPsec اجباری یا اختیاری؟

در برخی از استانداردها و RFC‌ها، پشتیبانی از پروتکل امنیت در IPsec (IPsec) با عبارت "must" آورده شده است، مانند RFC4294. در حالی که در برخی دیگر از آن‌ها مانند RFC6434 پشتیبانی از IPsec با عنوان "should" آورده شده است. دلیل این کار آن است که وجود IPsec در برخی از موارد ضروری و اجباری است، لکن ممکن است در برخی از شرایط بتوان از آن چشم‌پوشی کرد. بنابراین در این موارد با در نظر گرفتن پیامدهای مربوطه و عواقب جانبی می‌توان آن را نادیده گرفت. سازمان‌هایی که در کارها و ارتباطات خود از IPsec استفاده

^۴Integrator

^۵Latency, Bandwidth, throughput



می‌کنند و یا انتظار دارند در آینده آن را مورد استفاده قرار دهند، در زمان برگزاری مناقصه باید عبارت زیر را در بخش اجباری مناقصه‌ی خود قرار دهند:

- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *

تعریف تجهیزات شبکه و مراکز داده و شرح مختصر آنها

تعاریف زیر برای تجهیزات سخت‌افزاری مختلف مورد استفاده قرار می‌گیرد. با توجه به این‌که برخی از سخت‌افزارها ممکن است از نظر عملیاتی همپوشانی داشته باشند (مانند سویچ لایه ۲ که گاهی اوقات می‌تواند به عنوان مسیریاب لایه ۳ هم عمل نماید و یا مسیریاب لایه ۳ که قابلیت دیواره آتش را هم دارد) انتظار می‌رود در این‌گونه موارد، نیازمندی‌ها به صورت ترکیبی از وظایف دو یا چند لایه آورده شود. در حالت کلی در این سند تجهیزات شبکه را با توجه به کارکرد آنها به هفت گروه اصلی به شرح زیر دسته‌بندی می‌کنیم:

۱- میزبان^۶:

میزبان‌ها تجهیزاتی هستند که بسته‌ها را فقط ارسال یا دریافت می‌کنند و آنها را به تجهیزات دیگر هدایت^۷ نمی‌کنند.

۲- سویچ یا سویچ لایه ۲:

یک سویچ لایه ۲ دستگاهی است که برای ارسال قاب‌های^۸ اترنت بر اساس ویژگی‌های خود استفاده می‌شود. تبادل اطلاعات اترنت با دیگر سویچ‌های اترنت معمولاً بخشی از وظایف آن است.

۳- مسیریاب:

یک مسیریاب^۹ یا سویچ لایه ۳ تجهیزاتی است که در درجه اول برای هدایت بسته‌های IP بر اساس ویژگی‌های آن استفاده می‌شود. تبادل اطلاعات مسیریابی با سایر مسیریاب‌ها معمولاً بخشی از عملکرد آن است.

^۶ Host

^۷ Forward

^۸ Frames



۴- تجهیزات امنیت شبکه:

تجهیزات امنیت شبکه، تجهیزاتی هستند که به ترافیک بین رابط‌های شبکه اجازه عبور می‌دهند، از عبور آن جلوگیری می‌کنند یا آن‌ها را پایش می‌کنند تا فعالیت کدهای مخرب را تشخیص داده و از آن جلوگیری کنند. این رابط‌ها می‌توانند شامل انواع VPNها (مانند SSL یا IPsec) باشند. تجهیزات امنیت شبکه اغلب یک سویچ لایه ۲، لایه ۳، مسیریاب، دیوار آتش و غیره است.

۵- تجهیزات سمت مشتری (CPE):

یک تجهیز CPE معمولاً یک مسیریاب موجود در دفاتر کوچک یا منازل است که برای اتصال کاربران خانگی یا دفاتر کوچک به شبکه اینترنت با پیکربندی‌های متنوع مورد استفاده قرار می‌گیرد. اگر چه یک CPE معمولاً یک مسیریاب است، ولی مسیریاب‌ها و سویچ‌های لایه ۳ استفاده شده در ISPها و شبکه‌های تجاری متفاوت است.

۶- دستگاه‌های متحرک (موبایل):

در این سند منظور از تجهیزات موبایل تنها تجهیزاتی نیستند که به سامانه‌های 3GPP متصل شده و از فناوری‌هایی مانند 2G, 3G, LTE استفاده می‌کنند، بلکه شامل تمام تجهیزاتی است که قابلیت جابجایی در شبکه‌ی اینترنت را دارند، مانند کامپیوترهای سیار و یا کامپیوترهایی که با استفاده از پروتکل TCP/IP از جاهای مختلف برای کنترل سامانه‌های مختلف استفاده می‌شوند.

۷- تعدیل کننده بار^۹:

یک تعدیل کننده بار افزار شبکه‌ای است که بار کاری را بین چند کامپیوتر، سرویس‌دهنده یا سایر منابع شبکه توزیع می‌کند تا بتوان منابع شبکه را به صورت بهینه و طرح‌ریزی شده استفاده کرد، از حداکثر توان عملیاتی بهره برد، زمان پاسخ‌دهی را به حداقل رساند و از بار اضافی هم اجتناب کرد.

^۹ Router

^{۱۰} Customer Premise Equipment

^{۱۱} Load Balancer



فهرست استانداردهای RFC/3GPP مورد نیاز برای انواع سخت‌افزارها

نیازمندی‌ها به دو دسته کلی تقسیم می‌شوند "اجباری" و "اختیاری". تجهیزات خریداری شده در مناقصات حتماً باید استانداردهای اجباری را پشتیبانی کنند. پشتیبانی از نیازمندی‌های اختیاری را در صورتی که مورد درخواست مناقصه‌گزار باشد، می‌توان با در نظر گرفتن امتیاز مثبت لحاظ نمود. سخت‌افزارهایی که تمامی استانداردهای اجباری را پشتیبانی نکنند، باید در زمان ارزیابی مناقصه توسط مناقصه‌گزار به‌عنوان سخت‌افزارهای نامناسب ارزیابی شوند. لازم به ذکر است استانداردهایی که مراحل آزمایشی IPv6 Ready Logo را گذرانده باشند، معمولاً توسط آزمایشگاه‌های معتبر ارزیابی شده‌اند و در این متن آن‌ها را با علامت ستاره * مشخص نموده‌ایم.

نیازمندی‌های تجهیزات میزبان

استانداردهایی که در تجهیزات میزبان باید به‌صورت اجباری پشتیبانی شوند، شامل موارد زیر است:

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] *
- DHCPv6 client [RFC3315] *
- SLAAC [RFC4862] *
- Path MTU Discovery [RFC1981] *
- Neighbor Discovery [RFC4861] *
- If support for tunneling and dual stack is required, the device must support Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213]
- If support for mobile IPv6 is required, the device must support "MIPv6" [RFC6275, RFC5555] and "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture" [RFC4877]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]



نیازمندی‌های IPv6 در تجهیزات ICT

صفحه ۸ از ۲۱

- DNS message size requirements [RFC3226]
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *

استانداردهایی که در صورت نیاز به صورت اختیاری پشتیبانی شوند، شامل موارد زیر است:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736] *
- DS (Traffic class) [RFC2474, RFC3140]
- Cryptographically Generated Addresses [RFC3972]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- Multicast Listener Discovery version 2 [RFC3810] *
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

نیازمندی‌های تجهیزات لایه ۲ (سوئیچ‌های لایه ۲) در سمت مصرف‌کننده

استانداردهایی که در سوئیچ‌های لایه ۲ به صورت انتخابی (مدیریتی) پشتیبانی می‌شوند، شامل موارد زیر است:

- MLDv2 snooping [RFC4541]
- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]



نیازمندی‌های IPv6 در تجهیزات ICT

صفحه ۹ از ۲۱

- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]

نیازمندی‌های تجهیزات لایه ۳ (مسیریاب‌ها و سوئیچ‌های لایه ۳) در سمت تأمین‌کنندگان سرویس (ISP)

استانداردهایی که باید به صورت اجباری پشتیبانی شوند، شامل موارد زیر است:

- MLDv2 snooping [RFC4541]
- DHCPv6 filtering [RFC3315]
- Router Advertisement (RA) filtering [RFC4862]
- Dynamic "IPv6 Neighbor solicitation/advertisement" inspection [RFC4861]
- Neighbor Unreachability Detection [NUD, RFC4861] filtering
- Duplicate Address Detection [DAD, RFC4429] snooping and filtering.

استانداردهای مدیریتی که باید به صورت اجباری پشتیبانی شوند، شامل موارد زیر است:

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- IPv6 Routing Header [RFC2460, Next Header value 43] filtering *
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *
- UPnP filtering

استانداردهای اجباری عمومی شامل موارد زیر است:

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] *



- SLAAC [RFC4862] *
- MLDv2 snooping [RFC4541]
- Multicast Listener Discovery version 2 [RFC3810] *
- Router-Alert option [RFC2711]
- Path MTU Discovery [RFC1981] *
- Neighbor Discovery [RFC4861] *
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *
- If a dynamic interior gateway protocol (IGP) is requested, then RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol.
- If OSPF-v3 is requested, the equipment must comply with "Authentication/Confidentiality for OSPF-v3" [RFC4552]
- If BGP4 protocol is requested, the equipment must comply with RFC4271, RFC1772, RFC4760, RFC1997, RFC3392 and RFC2545
- Support for QoS [RFC2474, RFC3140]
- If support for tunneling and dual stack is required, the device must support Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213]
- If support for tunneling and dual stack is required, the device must support Generic Packet Tunneling and IPv6 [RFC2473]
- If 6PE is requested, the equipment must support "Connecting IPv6 Island over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)" [RFC4798]
- If mobile IPv6 is requested, the equipment must support MIPv6 [RFC6275, RFC5555] and "Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture" [RFC4877]
- If the IS-IS routing protocol is requested the equipment must support "M-ISIS: Multi-Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC5120]
- If MPLS functionality (for example, BGP-free core, MPLS TE, MPLS FRR) is requested, the PE-routers and route reflectors must support "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)" [RFC4798]
- If Layer 3 VPN functionality is requested, the PE-routers and route reflectors must support "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN" [RFC4659]



- If MPLS Traffic Engineering is used in combination with IS-IS routing protocol. The equipment must support "M-ISIS: Multi-Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC5120]

استانداردهای اختیاری شامل موارد زیر است:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- DHCPv6 client/server/relay [RFC3315] *
- Extended ICMP for multi-part messages [RFC4884]
- SeND (Secure Neighbor Discovery) [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736] *
- DHCPv6 PD [RFC3633] *
- Route Refresh for BGP-4 Capabilities [RFC2918]
- BGP Extended Communities Attribute [RFC4360]
- (QOS) Assured Forwarding [RFC2597]
- (QOS) Expedited Forwarding [RFC3246]
- Generic Routing Encapsulation [RFC2784]
- Cryptographically Generated Addresses [RFC3972]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- Using IPsec to Secure IPv6-in-IPv4 tunnels [RFC4891]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size Requirements [RFC3226]
- 127-bit IPv6 Prefixes on Inter-Router Links [RFC6164]
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]



نیازمندی‌های تجهیزات امنیت شبکه

تجهیزات در این بخش به ۳ زیرگروه تقسیم شده است:

- Firewall (FW)
- Intrusion prevention device (IPS)
- Application firewall (APFW)

برای هر استاندارد اجباری، زیرگروه‌های مناسب در انتهای هر خط و در داخل پرانتز مشخص شده است.

استانداردهایی که باید برای تجهیزات امنیتی به صورت اجباری پشتیبانی شوند، شامل موارد زیر است:

- IPv6 Basic specification [RFC2460] (FW, IPS, APFW) *
- IPv6 Addressing Architecture [RFC4291] (FW, IPS, APFW)
- Default Address Selection [RFC3484] (FW, IPS, APFW)
- ICMPv6 [RFC4443] (FW, IPS, APFW) *
- SLAAC [RFC4862] (FW, IPS) *
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *
- Inspecting IPv6-in-IPv4 protocol-41 traffic, which is specified in: Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (IPS)
- Router-Alert option [RFC2711] (FW, IPS)
- Path MTU Discovery [RFC1981] (FW, IPS, APFW) *
- Neighbor Discovery [RFC4861] (FW, IPS, APFW) *
- If the request is for the BGP4 protocol, the equipment must comply with RFC4271, RFC1772, RFC4760 and RFC2545 (FW, IPS, APFW)
- If the request is for a dynamic internal gateway protocol (IGP), then the required RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol. (FW, IPS, APFW)
- If OSPF-v3 is requested, the device must support "Authentication/Confidentiality for OSPFv3" [RFC4552] (FW, IPS, APFW)
- Support for QoS [RFC2474, RFC3140] (FW, APFW)
- If tunneling is required, the device must support Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (FW)



نیازمندی‌های IPv6 در تجهیزات ICT

صفحه ۱۳ از ۲۱

جایگاه دستگاه‌های امنیتی در شبکه همانند سوئیچ لایه ۲ یا مسیریاب/سوئیچ لایه ۳ است. بنابراین نیازمندی‌های لازم برای این جایگزینی باید گنجانده شوند. قابلیت‌ها و ویژگی‌هایی که بر روی IPv4 پشتیبانی می‌شود باید در IPv6 هم پشتیبانی شوند. برای مثال، اگر یک سامانه پیشگیری از نفوذ قادر به عملیات بر روی IPv4 در لایه‌های ۲ و ۳ باشد، باید این قابلیت را در IPv6 هم ارائه دهد یا اگر یک دیواره آتش که توانایی کار با شبکه‌های خوشه‌ای (Cluster) برای همزمان نمودن جلسات IPv4 بین اعضای مختلف خوشه را دارد، برای جلسات IPv6 هم امکان‌پذیر باشد.

استانداردهایی که در صورت نیاز به صورت اختیاری پشتیبانی شوند، شامل موارد زیر است:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- DHCPv6 client/server/relay [RFC3315] *
- Extended ICMP for Multipart Messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736] *
- DHCPv6 PD [RFC3633] *
- BGP Communities Attribute [RFC1997]
- BGP Capabilities Advertisement WITH-4 [RFC3392]
- (QOS) Assured Forwarding [RFC2597]
- (QOS) Expedited Forwarding [RFC3246]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- Cryptographically Generated Addresses [RFC3972]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891] (FW)
- OSPF-v3 [RFC5340]
- Authentication/Confidentiality for OSPF-v3 [RFC4552]
- Generic Packet Tunneling and IPv6 [RFC2473]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]



نیازمندی‌های IPv6 در تجهیزات ICT

صفحه ۱۴ از ۲۱

- DNS extensions to support IPv6 [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size requirements [RFC3226]
- Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891]
- Multicast Listener Discovery version 2 [RFC3810] *
- MLDv2 snooping [RFC4541] (when in L2 or passthrough mode) *
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)[RFC5739]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

نیازمندی‌های تجهیزات سمت مشتری (CPE)

استانداردهایی که باید به صورت اجباری در تجهیزات CPE پشتیبانی شوند، شامل موارد زیر است:

- RFC6204 (Basic Requirements for IPv6 Customer Edge Routers) *
استانداردهایی که در صورت نیاز به صورت اختیاری پشتیبانی شوند، شامل موارد زیر است:
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- If support for mobile IPv6 is required, the device needs to comply to “MIPv6”[RFC6275, RFC5555] and “Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture” [RFC4877]
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- DS (Traffic class) [RFC2474, RFC3140]
- Cryptographically Generated Addresses [RFC3972]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- Multicast Listener Discovery version 2 [RFC3810] *
- Packetisation Layer Path MTU Discovery [RFC4821]



نیازمندی‌های IPv6 در تجهیزات ICT

صفحه ۱۵ از ۲۱

- IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) [RFC5969]
- Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion
- [RFC6333] If support this then also must support Dynamic Host Configuration protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite [RFC6334]
- The A+P Approach to the IPv4 Address Shortage [RFC6346]
- IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)[RFC5739]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

نیازمندی‌های تجهیزات متحرک (موبایل)

استانداردهایی که باید در تجهیزات متحرک به صورت اجباری پشتیبانی شوند، شامل موارد زیر است:

- IPv6 basic specification [RFC2460] *
- Neighbor Discovery for IPv6 [RFC4861] *
- IPv6 Stateless Address Auto configuration [RFC4862] *
- IPv6 Addressing Architecture [RFC4291] *
- ICMPv6 [RFC4443] *
- IPv6 over PPP [RFC2472]
- Multicast Listener Discovery version 2 [RFC3810] *
- IPv6 Router Alert Option [RFC2711]
- DNS protocol extensions for incorporating IPv6 DNS resource records[RFC3596]

استانداردهایی که در صورت نیاز به صورت اختیاری پشتیبانی شوند، شامل موارد زیر است:

- Privacy Extensions for Stateless Address Auto configuration in IPv6[RFC4941]
- Path MTU Discovery for IPv6 [RFC1981] *
- Generic Packet Tunneling for IPv6 [RFC2473]
- DHCPv6 [RFC3315] *
- Stateless DHCPv6 [RFC3736]
- DHCPv6 option for SIP servers [RFC3319]



نیازمندی‌های IPv6 در تجهیزات ICT

صفحه ۱۶ از ۲۱

- IPv6 Prefix Options for DHCPv6 [RFC3633]
- Prefix Exclude Option for DHCPv6-based Prefix Delegation [draft-ietf-dhc-pdexclude]
- Default Address Selection [RFC3484]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- IKEv2 Mobility and Multi-homing Protocol MOBIKE [RFC 4555]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

استانداردهای 3GPP

- Internetworking Between Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) [3GPP TS29.061]
- GPRS Service Description [3GPP TS 23.060]
- General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access [3GPP TS 23.401]
- Signaling flows for IP multimedia Call control based on SIP and SDP [3GPP TS 24.228]
- IP multimedia call control protocol based on SIP and SDP [3GPP TS24.229]
- IP Based Multimedia Framework [3GPP TS 22.941]
- Architectural Requirements [3GPP TS 23.221]
- Packet domain; Mobile Stations (MS) Supporting Packet Switching Service [3GPP TS 27.060]
- IPv6 migration guidelines [3GPP TR 23.975]

IETF های RFC

- IPv6 for Some Second and Third Generation Cellular Hosts [RFC3316]
- Recommendations for IPv6 in 3GPP Standards [RFC3314]
- IPv6 in 3rd Generation Partnership Project (3GPP) [RFC6459]



نیازمندی‌های تعدیل‌کننده‌های بار (Load Balancers)

یک تعدیل‌کننده بار، درخواست‌های ورودی و یا اتصالات مشتریان را بین سرورهای متعدد توزیع می‌نماید. تعدیل‌کننده بار باید از ترکیبات مختلف اتصالات IPv6 و IPv4 پشتیبانی نماید:

- Load balancing IPv6 clients to IPv6 servers (6-to-6) must be supported
- Load balancing IPv6 clients to IPv4 servers (6-to-4) must be supported
- Load balancing IPv4 clients to IPv4 servers (4-to-4) should be supported
- Load balancing IPv4 clients to IPv6 servers (4-to-6) should be supported
- Load balancing a single external/virtual IPv4 address to a mixed set of IPv4 and IPv6 servers should be supported
- Load balancing a single external/virtual IPv6 address to a mixed set of IPv4 and IPv6 servers should be supported

اگر تعدیل‌کننده بار، در لایه ۷ عمل می‌کند (لایه کاربرد/پروکسی معکوس، که در بخش ۲-۲ از RFC3040 به‌عنوان "جانشین"^{۱۲} معرفی شده‌است) در این‌صورت در زمان هدایت بسته‌های HTTP باید بتواند آدرس IP آن را استخراج و آن را به سمت سرویس‌دهنده‌ی مورد نظر هدایت نماید. استانداردهایی که باید به‌صورت اجباری پشتیبانی شوند، شامل موارد زیر است:

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] *
- Path MTU Discovery [RFC1981] *
- Neighbor Discovery [RFC4861] *
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size requirements [RFC3226]
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *

^{۱۲}Surrogate



نیازمندی‌های IPv6 در تجهیزات ICT

استانداردهایی که در صورت نیاز به صورت اختیاری پشتیبانی شوند، شامل موارد زیر است:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- DS (Traffic class) [RFC2474, RFC3140]
- Cryptographically Generated Addresses [RFC3972]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- Multicast Listener Discovery version 2 [RFC3810] *
- Packetisation Layer Path MTU Discovery [RFC4821]
- NAT64/DNS64 [RFC6146, RFC6147]
- If support for IPsec is required, the device must support IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] * and Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2) [RFC5685]
- If support for BGP4 is required, the equipment must comply with RFC4271, RFC1772, RFC4760 and RFC2545
- If support for a dynamic internal gateway protocol (IGP) is required, the RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol.
- If OSPF-v3 is requested, the device must support "Authentication/Confidentiality for OSPFv3" [RFC4552] (FW, IPS, APFW)
- IPv6 Host-to-Router Load Sharing [RFC4311] (FW)
- Default Router Preferences and More-Specific Routes [RFC4191] (FW)



نیازمندی‌های پشتیبانی از IPv6 در نرم‌افزار

تمامی نرم‌افزارهای شبکه خریداری شده در مناقصه باید بتوانند از هر دو پروتکل IPv4 و IPv6 پشتیبانی نمایند و قادر باشند با شبکه‌های فقط IPv4، فقط IPv6 و دو پشته‌ای ارتباط برقرار نمایند.

اگر در تنظیمات یک نرم‌افزار چه در طرف مشتری و چه در طرف سرویس‌دهنده نیاز به IPv6 باشد باید امکان پیکربندی آن هم به صورت محلی و هم از راه دور امکان‌پذیر باشد، یعنی نرم‌افزار بتواند از پیکربندی پارامترهای IPv6 نیز پشتیبانی نماید.

تمامی تنظیمات و ویژگی‌هایی که در IPv4 انجام می‌شود باید برای IPv6 نیز ارایه شود و هنگام برقراری ارتباط کاربر نباید تفاوت قابل توجهی بین این دو پروتکل احساس نماید، مگر این که فایده‌ای برای کاربر داشته باشد. اکیداً توصیه می‌شود که از لیترال‌های^{۱۳} آدرس در کد نرم‌افزار استفاده نکنید، همان‌گونه که در "Default Address Selection for Internet Protocol version 6" (RFC 3484) توضیح داده شد.

مهارت‌های مورد نیاز برای یکپارچه‌سازی سامانه‌ها

فروشنده‌گان و نمایندگی‌های فروش که سامانه‌های یکپارچه خدمات ارایه می‌دهند، باید حداقل دارای سه نفر کارمند حائز صلاحیت برای دریافت گواهی‌نامه معتبر از تولیدکنندگان تجهیزات که در مناقصه فروخته می‌شود، داشته باشند. این کارمندان همچنین باید دانش عمومی در مورد پروتکل IPv6، طراحی شبکه‌ی مبتنی بر IPv6 و امنیت آن را داشته باشند. (گواهی‌نامه‌ها باید نشانگر این موضوع باشند).

اگر در طول نصب تجهیزات و یکپارچگی مشخص شود که کارمندان دارای دانش، صلاحیت و تجارب کافی برای نصب و پیکربندی تجهیزات به منظور برقراری ارتباطات توسط پروتکل‌های IPv4 و IPv6 در شبکه نمی‌باشند، این قرارداد باید لغو شود.

^{۱۳}Literals



نیازمندی‌های IPv6 در تجهیزات ICT

صفحه ۲۰ از ۲۱

تعریف یکپارچگی مناسب، تنظیم سرعت و میزان اختلال در شبکه در زمان راه اندازی، باید در قرارداد بین مشتری و یکپارچه کننده سامانه مورد توجه قرار گیرد. همچنین پیشنهاد می شود یکپارچه کننده سامانه‌ها و کارمندان وی علاوه بر گواهی‌نامه‌های فوق دارای تخصص گسترده و گواهینامه‌های معتبر در زمینه IPv6 به غیر از آنچه که سازندگان تجهیزات ارائه کرده‌اند باشند. این گواهی‌نامه‌ها را می‌توان از مؤسسات آموزشی مستقل اخذ نمود. شاید چنین دانشی در فرآیند مناقصه امتیاز اضافی محسوب شود.

همه پیشنهاددهندگان در فرآیند مناقصه باید اظهارنامه‌ای را امضا نمایند که نشان می‌دهد شرکت و همه کارکنان مربوطه آموزش‌های فنی را برای طراحی، اجرا و یکپارچگی تجهیزات فناوری اطلاعات و ارتباطات (ICT) در شبکه‌های مبتنی بر پروتکل‌های IPv4 و IPv6 گذرانده‌اند. نمونه ای از چنین اظهارنامه‌ها را می‌توانید در زیر مشاهده فرمایید.

اظهارنامه صلاحیت IPv6

برگزارکنندگان مناقصه باید اظهارنامه صلاحیت فنی IPv6 را از شرکت‌های یکپارچه کننده سامانه‌ها و تأمین کنندگان تجهیزات، درخواست نمایند. به منظور اطمینان از نصب، راه‌اندازی و یکپارچه سازی دانش و تجربه لازم در مورد IPv6 و کارایی آن در محیط ICT اجتناب ناپذیر است. این اظهارنامه اعلام می‌دارد که تأمین کننده تجهیزات یا شرکت‌های یکپارچه کننده سامانه‌ها، با قبول هرگونه مسئولیت مادی و کیفی، اعلام می‌دارند که:

- افراد کافی برای ارائه خدمات تعهد شده را دارند
- این افراد در خصوص طراحی، ساخت و یکپارچه نمودن تجهیزات ICT در شبکه‌های مبتنی بر IPv4 و IPv6 آموزش‌های حرفه لازم را دیده‌اند.
- کیفیت خدمات ارائه شده، نیازمندی‌های بیان شده در اسناد مناقصه را برآورده می‌سازد. و این نیازمندی‌ها برای هر دو پروتکل IPv4 و IPv6 اعمال می‌شوند.



نیازمندی‌های IPv6 در تجهیزات ICT

صفحه ۲۱ از ۲۱

توجه داشته باشید که چنین اظهارنامه‌هایی ممکن است بسته به قوانین محلی هر کشور و بسته به انتظارات دارنده شبکه، متفاوت باشد. بنابراین برگزارکنندگان مناقصه به منظور اظهار دقیق این موارد بهتر است با مشاوران حقوقی خود مشورت نمایند.