INSO
19045

1st. Edition

2015

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization

استاندارد ملی ایران
۱۹۰۴۵

چاپ اول

۱۳۹۳

فناوری اطلاعات - مخابرات و تبادل اطلاعات بین سامانه‌ها – پیشکار(پروکسی) میزبان‌های در حالت خواب

Information technology — Telecommunications and information exchange between systems — proxZzzy for sleeping hosts

ICS: 35.110

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

موسسه استاندارد و تحقیقات صنعتی ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون فنی مرکب از کارشناسان سازمان، صاحب نظران مراکز و موسسات علمی، پژوهشی تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون‌های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیته ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که موسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند در کمیته ملی طرح و بررسی و در صورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شماره ۵ تدوین و در کمیته ملی استاندارد مربوط که موسسه استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

موسسه استاندارد و تحقیقات صنعتی ایران از اعضای اصلی سازمان بین‌المللی استاندارد ۳۴۰(ISO[1])، کمیسیون بین‌المللی الکترونیک (IEC[2]) و سازمان بین‌المللی اندازه شناسی قانونی (OIML[3]) است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC[5]) در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندیهای خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

موسسه استاندارد و تحقیقات صنعتی ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. موسسه می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و موسسات فعال در زمینه مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سامانه‌های مدیریت کیفیت و مدیریت زیست محیطی، آزمونگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، موسسه استاندارد این گونه سازمان‌ها و موسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامه تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

---

1 - International Organization for Standardization
2 - International Electrotechnical Commission
3 - International Organization for Legal Metrology (Organization International de Metrologie Legal)
4 - Contact Point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات - مخابرات و تبادل اطلاعات بین سامانه‌ها – پیشکار (پروکسی) میزبان‌های در حالت خواب»

رئیس	**سمت و/یا نمایندگی**
قسمتی، سیمین (فوق‌لیسانس مهندسی فناوری اطلاعات)	کارشناس استاندارد، سازمان فناوری اطلاعات
دبیر:	
معروف، سینا (لیسانس مهندسی کامپیوتر، سخت‌افزار)	کارشناس استاندارد، سازمان ملی استاندارد ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
اسدی پویا، سمیرا (فوق‌لیسانس، مهندسی فناوری اطلاعات)	مدیرعامل شرکت مهندسی پویا دانش و کیفیت آوا
سعیدی، عذرا (فوق‌لیسانس مهندسی مخابرات)	کارشناس استاندارد، سازمان فناوری اطلاعات
شیرازی میگون، مریم (لیسانس مهندسی فناوری اطلاعات)	کارشناس، پژوهشگاه استاندارد سازمان ملی استاندارد ایران
فرهاد شیخ احمد، لیلا (فوق‌لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس استاندارد، سازمان ملی استاندارد ایران
کماسی، مهدی (لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس، شرکت گسترش سرمایه‌گذاری ایران‌خودرو
مهدوی، مهدی (فوق‌لیسانس، مهندسی فناوری اطلاعات)	معاون طرح و توسعه بیمه سرمد
وحدت جعفری، محسن (فوق‌لیسانس، هوش مصنوعی)	رییس اداره فناوری اطلاعات، شرکت نفت پاسارگاد

یزدیان ورجانی، علی عضو هیات علمی دانشگاه تربیت مدرس

(دکتری، برق)

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات - مخابرات و تبادل اطلاعات بین سامانه‌ها – پیشکار (پروکسی) میزبان‌های در حالت خواب» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان ملی استاندارد ایران تهیه و تدوین شده و در سیصد و شصت و چهارمین اجلاس کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۳/۱۲/۱۱ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و مأخذی که برای تهیه این استاندارد مورداستفاده قرار گرفته به شرح زیر است:

ISO/IEC 16317:2011, Information technology — Telecommunications and information exchange between systems — proxZzzy for sleeping hosts

فناوری اطلاعات - مخابرات و تبادل اطلاعات بین سامانه‌ها – پیشکار (پروکسی) میزبان‌های در حالت خواب

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، تعیین روش‌های نگهداری و داشتن ارتباط شبکه توسط پیشکارها[1] (پروکسی‌ها) برای تمدید طول مدت حالت خواب[2] میزبان‌ها[3] است. این استاندارد ملی، موارد زیر را مشخص می‌کند:

- قابلیت‌هایی که پیشکار برای میزبان به نمایش می‌گذارد.
- اطلاعاتی که باید بین میزبان و پیشکار، مبادله شوند.
- رفتار پیشکار در قبال 802.3 (Ethernet) و 802.11 (WiFi)[4]
- رفتار اختیاری و الزامی پیشکار حین عملیات، شامل پاسخ به بسته‌ها، تولید بسته‌ها، نادیده گرفتن بسته‌ها و بیدار کردن میزبان.

این استاندارد ملی موارد زیر را انجام نمی‌دهد:

- مشخص کردن سازوکارهای ارتباط بین میزبان و پیشکارها؛
- توسعه یا تغییر مشخصات مرجع دار (برای هرگونه اختلافی که مشخصات آن معتبر است)؛

پروتکل‌های ارتباطی و امنیت، از قبیل IPsec، MACsec، SSL، TLS، Mobile IP و غیره را پشتیبانی نمی‌کند.

۲ انطباق

«M»، «S» یا «O» در ستون «M/S/O» در جدول‌های بند ۶، ۷ و ۸، الزامات را به ترتیب به‌صورت «M» برای الزامی، «S» برای باید و «O» برای اختیاری، مشخص می‌کند.

پیشکارهای منطبق، کمینه الزامات اجباری را در «پروتکل چارچوب پایه» بند ۶ و تعداد صفر گزینه یا بیشتر، از بند ۸ پیاده‌سازی می‌کنند. پیشکارها پیکربندی و رفتارهای مدیریتی مشخص‌شده در بند ۷ را رعایت می‌کنند.

جدول زیر، خلاصه‌ای از الزامات و وضعیت را نشان می‌دهد.

1 - Proxy
2 - Sleep
3 - Host
4 - Wireless Fidelity

الزامات پیاده‌سازی شده	الزامی/اختیاری
رسانه[a] (802.3, 802.11)	به پیاده‌سازی بند ۶-۱ یا ۶-۲ یا هر دو نیاز دارد
آدرس تفکیک پذیری پروتکل[b] برای پروتکل اینترنتی نسخه چهار[c] (IPv4 ARP)	اجباری
کشف همسایه[d] برای پروتکل اینترنتی نسخه شش (IPv6 Neighbor Discovery)	اجباری
سامانه نام دامنه (DNS)[e]	اختیاری
پروتکل پیکربندی پویای میزبان (DHCP)[f]	اختیاری
پروتکل مدیریت گروه اینترنت (IGMP)[g]	اختیاری
کشف شنونده چندپخشی (MLD)[h]	اختیاری
دسترسی از دور با استفاده از IPv4 و SIP	اختیاری
دسترسی از دور با استفاده از Teredo برای IPv6	اختیاری
پروتکل مدیریت شبکه ساده (SNMP)[i]	اختیاری
کشف خدمت با استفاده از mDNS	اختیاری
تفکیک‌پذیری نام توسط تفکیک‌پذیری نام چندپخشی محلی پیوند (LLMNR)[j]	اختیاری
بسته‌های بیدارباش	اجباری

[a] Media
[b] Address Resolution Protocol
[c] Internet Protocol
[d] Neighbor Discovery
[e] Domain Name System
[f] Dynamic Host Configuration Protocol
[g] Internet Group Management Protocol
[h] Multicast Listener Discovery
[i] Simple Network Management Protocol
[j] Link Local Multicast Name Resolution

۳ مراجع الزامی

مدارکی که به‌عنوان منبع به آن‌ها در ادامه ارجاع داده می‌شود در متن استاندارد ملی ایران مورداستفاده قرارگرفته است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود .

درصورتی‌که به مدارکی با ذکر تاریخ انتشار آن ارجاع داده‌شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن موردنظر این استاندارد ملی نیست و در غیر این صورت همواره تاریخ تجدیدنظر و اصلاحیه‌های بعدی آن‌ها موردنظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۳-۱ استاندارد ملی ایران شماره ۳-۸۸۰۲: سال ۱۳۸۸، فناوری اطلاعات- مخابرات و تبادل اطلاعات میان سامانه ها- شبکه‌های محلی و شهری- الزامات ویژه- قسمت۳- روش دسترسی و ویژگی‌های لایه فیزیکی دسترسی چندگانه دریافت حامل با تشخیص تلاقی(CSMA/CD)

3-2 ISO/IEC 8802-11:2005, Information technology — Telecommunications and information exchange betweensystems — Local and metropolitan area networks — Specific requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications

3-3 ISO/IEC TR 11802-2:2005, Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Technical reports and guidelines — Part 2: Standard Group MAC Addresses

3-4 RFC 826, An Ethernet Address Resolution Protocol; David C. Plummer (MIT); November 1982; http://tools.ietf.org/html/rfc826

3-5 RFC 1122, Requirements for Internet Hosts — Communication Layers; R. Braden; October 1989; http://tools.ietf.org/html/rfc1122

3-6 RFC 3261, SIP: Session Initiation Protocol; Many Authors; June 2002; http://tools.ietf.org/html/rfc3261

3-7 RFC 4380, Teredo: Tunneling IPv6 over UDP through Network Address Translations

3-8 (NATs); http://tools.ietf.org/html/rfc4380

3-9 RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, http://tools.ietf.org/html/rfc4443

3-10 RFC 2460, Internet Protocol, Version 6 (IPv6) Specification; http://tools.ietf.org/html/rfc2460

3-11 RFC 4861, Neighbor Discovery for IP Version 6 (IPv6); http://tools.ietf.org/html/rfc4861

3-12 IEEE Std 802.11r-2008, IEEE Standard for information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 2: Fast Basic Service Set (BSS) Transition

3-13 http://tools.ietf.org/html/draft-cheshire-dnsext-multicastdns-08 (Multicast DNS)

3-14 http://tools.ietf.org/html/draft-cheshire-dnsext-dns-sd-05 (DNS-Based Service Discovery)

3-15 [MS-LLMNRP] "Link Local Multicast Name Resolution (LLMNR) Profile", Microsoft Developer Network Open Specifications Developer Center Library, http://msdn.microsoft.com/en-us/library/dd240328%28PROT.10%29.aspx

۴ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود:

۴-۱

میزبان

هستاری که برای نگهداری داشتن شبکه، از پیشکار توان پایین‌تر استفاده می‌کند.

۲-۴

پیشکار (پروکسی)

پیشکار (پروکسی) شبکه

هستاری که از وجود شبکه برای میزبان توان بالاتر در حالت خواب، نگهداری می‌کند.

۳-۴

حالت خواب

حالتی که در آن میزبان نسبت به زمانی که به‌طور کامل در حال کار کردن است انرژی کمتری استفاده می‌کند.

۵ کاربرد پیشکار پروتکل‌ها (اطلاعاتی)

۵-۱ معماری پایه

برای اینکه پیشکار درست کار کند و قادر باشد تا میزبان را به حالت خواب ببرد، کارکردهای پایه‌ای معینی باید در پیشکار، میزبان آن و ارتباطات بین پیشکار و میزبان وجود داشته باشد. این استاندارد ملی، پروفایلی از پروتکل‌های گسترش‌یافته متداول را ارائه می‌دهد که می‌توانند در پیشکار پیاده‌سازی شوند تا رفتار موردنظر سامانه را تولید کنند.

۵-۲ اترنت (IEEE 802.3)

استاندارد IEEE 802.3، لایه‌های واپایش دسترسی فیزیکی و رسانه‌ای پروتکل تعامل‌پذیری را که به اترنت معروف است مشخص می‌کند.

محیط IEEE 802.3، پروتکل‌هایی دارد که ممکن است عملیات پیشکار را از قبیل به‌روزرسانی‌های پارامترهای مدیریت شبکه در پاسخ به مبادلات پروتکل کشف لایه پیوند (LLDP)[1] که شامل بیدار کردن میزبان است تحت تأثیر قرار دهد. لایه‌های مشترک IEEE 802.3 قادر به پشتیبانی هم‌زمان چندین نشانی MAC هستند. این کارکرد، در پشتیبانی از ماشین‌های مجازی ـ هرکدام با یک یا چند نشانی MAC منحصربه‌فرد (هر نشانی MAC، با یک یا چند نشانی IPv4/IPv6) روی لایه فیزیکی منفردی به‌کاررفته است. ماهیت توسعه‌ی شبکه‌های سیمی متفاوت است (اتصالات شبکه‌ای خانگی، شرکتی و مهمان[2]) و حتی در هر پیکربندی توسعه و تعامل شبکه‌ای می‌تواند به‌طور قابل‌ملاحظه‌ای متفاوت باشد. اگر وضعیت اتصال، تغییر کند، ممکن است مدت‌زمان قابل ملاحظه‌ای قبل از اینکه پیشکار قادر به ارسال یا دریافت ترافیک روی درگاهی[3] سوده[4] باشد، سپری شود درحالی‌که پروتکل درخت پوشا[5]، اجراشده است.

۵-۳ شبکه محلی بی‌سیم (IEEE 802.11)

1 - Link Layer Discovery Protocol
2 - Guest
3 - Port
4 - Switch
5 - Spanning Tree Protocol

استاندارد IEEE 802.11، لایه‌های واپایش دسترسی فیزیکی و رسانه‌ای پروتکل تعامل‌پذیری را که به WiFi معروف است مشخص می‌کند.

ارتباط بی‌سیم که از استاندارد 802.11 استفاده می‌کند از عملیات شبکه محلی سیمی (IEEE 802.3) در روش‌های زیر متفاوت است:

- انتشار ارتباطات بی‌سیم 802.11 روی باند بدون مجوز آن را در معرض چند سطح از مسائل تداخل و هم‌پوشانی قرار می‌دهد بنابراین ارتباط WiFi نمی‌تواند تضمین شود.
- میزبان 802.11 و نقطه دسترسی(AP)[1] برای استفاده از رخ‌نمون (پروفایل) مشترک پیکربندی می‌شوند که مجموعه‌ای از پارامترهای ارتباطی از قبیل باند، کانال، امنیت و غیره هستند. این رخ‌نمون (پروفایل)، خارج از باند و قبل از اینکه میزبان به حالت خواب برود، شکل می‌گیرد.

در اینجا برخی ملاحظات توسعه‌ی خاص ارتباطات بی‌سیم، برای پیشکار ارائه‌شده‌اند:

- اغلب میزبان‌ها از AP جدا می‌شوند و ممکن است به همان AP یا AP دیگری با همان SSID، یا به یک AP با SSID دیگری دوباره مرتبط شوند. این امر بر اساس پیکربندی رخ‌نمون (پروفایل) ارتباطی است.
- ممکن است پیشکار، در نقاط عمومی WiFi که نیاز به مجوزسنجی صریح کاربر، از قبیل نیاز به توافق قانونی[2] (EULA)[3] هستند کار نکند.
- برخی توسعه‌های شبکه‌های محلی بی‌سیم (WLAN)[4] به DHCP Renew در زمان ارتباط، نیاز دارند.

۵-۴ پروتکل پیکربندی پویای میزبان (DHCP)[5]

DHCP، سازوکار اصلی تخصیص نشانی IP برای IPv4 و سازوکار مستقل تخصیص نشانی IP برای شبکه‌های IPv6 است. کارساز DHCP، نشانی‌های IP را برای سامانه‌های شبکه، تخصیص می‌دهد. ممکن است زمان اجاره نشانی IP در زمانی که سامانه در حالت خواب است منقضی شود. روش‌های زیر تضمین می‌کنند که پیشکار می‌تواند به استفاده از نشانی IP مشابهی که توسط کارساز DHCP به میزبان تخصیص داده‌شده است، ادامه دهد.

- میزبان، یک زمان‌سنج داخلی را تنظیم می‌کند و سر وقت به آن بیدارباش می‌دهد تا اجازه DHCP را تجدید کند. برای پیشکار، الزاماتی وجود ندارد.
- پیشکار، طبق زمان‌سنج پیشکار، به میزبان بیدارباش می‌دهد تا اجازه DHCP را تمدید کند.
- پیشکار، کارکرد نوسازی نشانی DHCP را بدون بیدار کردن میزبان، پیاده‌سازی می‌کند.

پیشکار، نشانی IP سامانه را در زمانی که میزبان، خواب است تغییر نمی‌دهد. انجام این کار، پیچیدگی اجرایی بی‌موردی را خصوصاً برای انتقال نشانی IP جدید به میزبان، معرفی می‌کند.

۵-۵ چارچوب پایه پروتکل اینترنتی نسخه ۴ (IPv4)

مجموعه پروتکل IPv4 که توسط IETF مشخص شد، مجموعه‌ای از پروتکل‌های همکاری است که تعامل‌پذیری لایه شبکه را برای شبکه‌های IP، فراهم می‌آورد.

۵-۱-۱ پروتکل تفکیک‌پذیری نشانی (ARP)[6]

پروتکل ARP (RFCs 826, FRC 1122)، نگاشت نشانی یک نشانی IPv4 را در MAC متناظر، ارائه می‌دهد.

---

1 - Access point
2 - legal agreement
3 - End-user licence agreement
4 - Wireless local area network
5 - Dynamic Host Configuration Protocol
6 - Address Resolution Protocol

ARP برای پیشکار مهم است زیرا برای اینکه هستارهای دیگر، قادر به ارسال بسته IPv4 به پیشکار باشند، باید قادر به انتقال نشانی IP به نشانی MAC متناظری، باشند. پیشکار به درخواست ARP برای نشانی MAC آن و حفظ ارتباط IPv4 به شبکه IPv4 پاسخ می‌دهد.

ARP، یک پروتکل شبکه‌ای غیرقابل‌اعتماد است و دیگر نقاط روی شبکه، فرض می‌کنند که هر درخواست ARP به مقصد نمی‌رسد؛ بنابراین، تأخیر کوتاه (۱۰-۲ ثانیه) در انتقال عملیات پیشکار نباید وضعیت دیگر نقاط شبکه را تحت تأثیر قرار دهد.

۵-۱-۲ تخصیص نشانی خودکار IP پیوند محلی

این نوع تخصیص نشانی از ARP برای تعیین نشانی IPv4 در نبود کارساز DHCP (دیگر روش‌های تخصیص) استفاده می‌کند. پیشکار، با استفاده از الگوریتم‌های فهرست شده در RFC5227 (جز درجایی که نشانی جدیدی موردنیاز است که در آن نقطه پیشکار باید پشتیبانی از سطح مشترک را متوقف کند و به‌طور اختیاری میزبان را بیدار کند) از نشانی خودکار IP پیوند، پشتیبانی می‌کند.

۵-۱-۳ تشخیص تداخل نشانی IPv4

شناسایی نشانی دوتایی (RFC5227) برای جلوگیری پیشکار از استفاده از نشانی که توسط بخش دیگری از شبکه مورداستفاده است، موردنیاز است.

۵-۱-٤ پروتکل مدیریت گروهی اینترنت (IGMP)[1]

این پروتکل (IGMP RFC 1112 نسخه ۱، IGMP RFC 2236 نسخه ۲، IGMP RFC 3376 نسخه ۳) به واسطهای مشترک شبکه اجازه می‌دهد تا در چندین گروه، مشارکت کنند (این کار توسط ره‌یاب، کنترل می‌شود).

۵-۱-۵ پروتکل بستک کاربر (UDP)[2]

پیشکار که از UDP پشتیبانی می‌کند ممکن است در دریافت داده‌های UDP خاص، میزبان را بیدار کند یا مستقیم به بستک، پاسخ دهد.

۵-۱-٦ پروتکل واپایش انتقال (TCP)[3]

این پروتکل (RFC 793)، ارتباط لایه انتقال قابل‌اعتماد و حالت‌داری[4] را بین نقاط نهایی شبکه، فراهم می‌آورد. پیشکار مجاز است پذیرش اتصال، ایجاد اتصال و بیدار کردن میزبان را در تلاش برای اتصال (TCP STN) یا داده‌های ورودی انجام دهد.

1 - Internet Group Management Protocol
2 - User Datagram Protocol
3 - Transmission Control Protocol
4 - Stateful

۵-۱-۷ سامانه نام دامنه (DNS)[1]

پیشکار اگر ارتباط TCP یا UDP را ارائه دهد مجاز است نیاز داشته باشد تا بررسی‌های DNS را مطرح کند و به میزبان اجازه می‌دهد تا نام‌های سازگار میزبان اترنت را برای نقاط پایانی دور و نشانی‌های IPv4 غیرمستقیم، مشخص کند. این استاندارد، فقط DNS کارخواه[2] را مد نظر قرار می‌دهد.

۵-۶ چارچوب پایه پروتکل اینترنتی نسخه ۶ (IPv6)

وجود شبکه برای IPv6، در زمانی که میزبان با پیاده‌سازی کارکرد تقاضای[3] همسایه‌ی کشف همسایه[4]، خواب است توسط پیشکار، حفظ می‌شود. پیشکار از نشانی‌های جهانی IPv6، نشانی‌های محلی پیوند و نشانی‌های موقتی استفاده می‌کند. پیکربندی خودکار نشانی، توسط میزبان ساماندهی می‌شود.

کشف همسایه مجموعه‌ای از پنج پیام است که در ICMPv6 (RFC 4861) پیاده‌سازی می‌شود و پیشکار از چهار نشانی شناسایی IPv6 برای نشانی MAC استفاده می‌کند: تقاضای ره‌یاب، اعلان ره‌یاب، تقاضای همسایه و اعلان همسایه. بهتر است پیشکار از چندین مجموعه نشانی، پشتیبانی کند. معمولاً سه مجموعه در شبکه IPv6 وجود دارند: نشانی جهانی[5]، نشانی محلی و احتمالاً نشانی موقتی.

۵-۱۱-۱ کشف شنونده چندپخشی (MLD)[6]

MLD (RFC 2710) به گره‌های نقاط پایانی اجازه می‌دهد تا عضویت خود را در گروه‌های چندپخشی گزارش دهند. MLD برای انتخاب نشانی منبع توسط RFC 3590 و برای چندپخشی خاص منبع، توسط RFC 3810، به‌روز می‌شود.

پیشکار جدولی از نشانی‌های چندپخشی را که در آن‌ها میزبان، متعهد شده است حفظ می‌کند و پیشکار، عضویت خود را در هر گروه چندپخشی با پاسخ به پیام‌های پرسمان[7] MLD به همراه پیام‌های گزارش MLD، حفظ می‌کند. پیشکار نیاز ندارد که گزارش غیر درخواستی MLD یا پیام‌های انجام کار MLD را ارسال کند. چون میزبان یک ره‌یاب چندبخشی نیست و پیشکار پیام‌های پرسمان MLD یا گزارش فرآیند MLD یا پیام‌های انجام MLD را ارسال نمی‌کند.

۵-۷ دسترسی از دور با استفاده از پروتکل آغاز نشست (SIP)[8] و IPv4

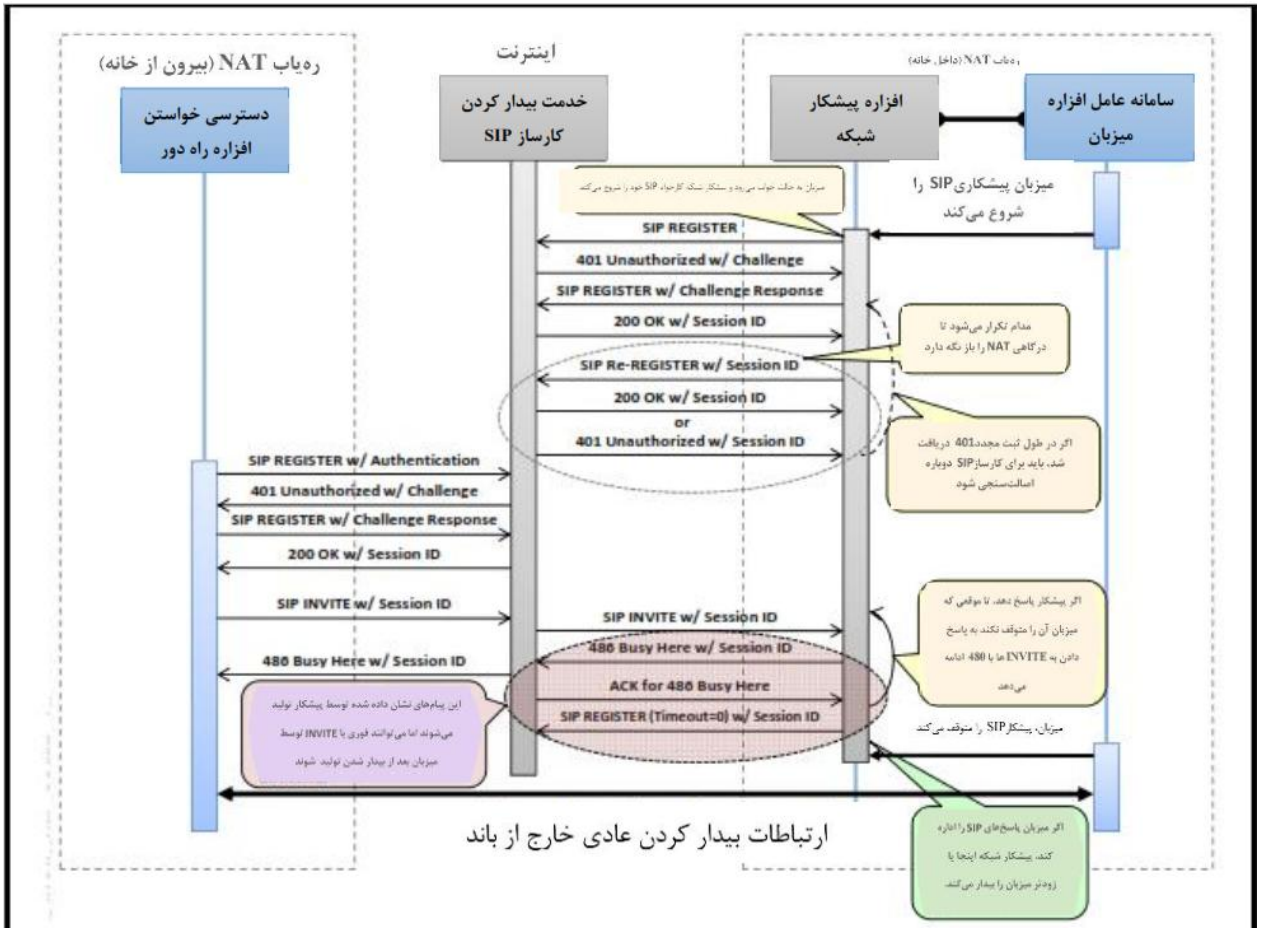
در این استاندارد ملی، پروتکل آغاز نشست، SIP (RFC 3261) توسط هستار دوری برای میزبان کار می‌کند. پیشکارهای (پروکسی‌های) SIP در امتداد مسیر می‌توانند پیمایش ترجمه نشانی شبکه (NAT)[9] و دیواره‌های آتش را تسهیل کنند. دلیل بیدار کردن میزبان (کاربرد خاص میزبان که برای استفاده،

---

1 - Domain Name System
2 - Client
3 - Solicitation
4 - Neighbor Discovery
5 - Global address
6 - Multicast Listener Discovery
7 - Query
8 - Session Initiation Protocol
9 - Network Address Translation

موردنیاز است) خارج از دامنه این استاندارد ملی است. روش‌های SIP و پاسخ‌های مورداستفاده در کارکرد بیدارباش از دور، کدهای وضعیت SIP، ACK، INVITE، REGISTER است.

شکل زیر پیاده‌سازی نمونه SIP را نشان می‌دهد که توسط پیشکار برای بیدار کردن میزبان، به کار می‌رود. فقط پیام‌های ورودی و خروجی افزاره پیشکار شبکه، در این مشخصات، دربر گرفته می‌شوند. بقیه پیام‌ها و هستارها، پیاده‌سازی احتمالی است و توسط این مشخصات پوشش داده نمی‌شود.



شکل ۱- بیداری از دور SIP

مثال بالا، پردازش بیداری میزبان را با استفاده از SIP به‌صورت « INVITE/486 Busy Here/...» نشان می‌دهد اما این یک الزام نیست.

الزامات در این استاندارد ملی به‌صورت کلی نوشته می‌شوند که شامل اجازه پاسخ «200 Ok» و برقراری SIP می‌شود.

۵-۸ دسترسی از دور با استفاده از Teredo برای IPv6

پروتکل Teredo (RFC 4380)، فناوری انتقال IPv6 است که اجازه ارتباط جفت به جفت بین همتاهای پشت NAT را می‌دهد. پروتکل Teredo، بسته‌های IPv6 را داخل بسته‌های UDP IPv4، پوشینه‌سازی می‌کند. یکی از تونل‌هایی که کارخواه Teredo حفظ می‌کند با کارساز Teredo در ابر است. پیشکار این تونل را با فرستادن پیام‌های تقاضای ره‌یاب (RS)[1] در بازه‌های منظم، حفظ می‌کند. پیشکار، هر پاسخی از کارساز به بسته RS را نادیده می‌گیرد.

۵-۹ پروتکل مدیریت شبکه ساده (SNMP)[2]

1 - Router Solicitation
2 - Simple network management protocol

پیشکار برای عامل SNMP نسخه ۱و نسخه ۲ (RFC 1156, 1157, 1141) است و از بیدارباش‌های غیرضروری برای برخی درخواست‌های SNMP اجتناب می‌کند. پیشکار SNMP به درخواست SNMP GET با مقادیر ارائه‌شده به آن از طرف میزبان، پاسخ می‌دهد. میزبان می‌تواند واکنش در دریافت SNMP SET را مشخص کند.

۵-۱۰ بررسی خدمت با استفاده از mDNS

هنگامی‌که مشتریان به دنبال خدماتی در اینترنت با استفاده از کشف خدمت مبتنی بر DNS یعنی (DNS-SD) بر روی DNS چندپخشی (mDNS) هستند، پیشکار، خدمات اعلان‌ها را اداره می‌کند و بهتر است فقط زمانی که مشتری، نشست کاربردی را با یک خدمت آغاز می‌کند، میزبان را بیدار کند.

پیشکار، خدمت‌ها را به‌عنوان پاسخ دهنده mDNS که با مجموعه ایستای ثبت‌نام‌های خدمت DNS-SD آغازشده‌اند اعلان می‌کند. پیشکار باید الزامات را برای پاسخ‌گوی چندپخشی DNS، تأمین کند. پیشکار به بررسی‌های چندپخشی با پاسخ‌های چندپخشی، پاسخ می‌دهد و به‌طور دوره‌ای، اعلان‌های غیر درخواستی می‌فرستد. هنگامی‌که مشتریان، نشست‌های برنامه‌های کاربردی را با نقاط پایانی انتقال اعلان‌شده به طور مثال درگاهی‌های TCP/UDP مشخص‌شده در ثبت‌های DNS SRV آغاز می‌کنند، پیشکار میزبان را بیدار می‌کند.

۵-۱۱ تفکیک نام با LLMNR

پیشکار به پرسمان‌های تفکیک نام چندپخشی لایه پیوند (LLMNR)[1]، در سمت میزبان، با گوش دادن به پرسمان‌های UDP LLMNR در درگاهی مرتبط و نشانی‌های چندپخشی، پاسخ می‌دهد به‌طوری‌که میزبان به این کار نیازی ندارد. اگر پیشکار، تداخل LLMNR را علاوه بر درخواست‌های ارتباطی، تشخیص دهد، میزبان را بیدار می‌کند. رفتار آن بر اساس RFC 4795 با تفاوت‌هایی است که در [MS-LLMNR] ذکرشده‌اند.

۵-۱۲ بسته‌های بیداری

درحالی‌که کارکرد پیشکار، افزایش زمانی است که میزبان با دخالت خود در سمت میزبان، طی دوره‌های جواب در خواب باقی می‌ماند، اما بیدار کردن برای عملیات صحیح میزبانی در شبکه، نیز مهم است. هر میزبانی که از پیشکار استفاده می‌کند باید یک یا چند سازوکار برای بیدار کردن در ترافیک شبکه داشته باشد درحالی‌که سازوکارهای زیادی می‌توانند درک شوند، چهار سازوکار احتمالی، به‌صورت زیر می‌باشند:

الف - Magic Packet™ (نشانی تجاری از Advanced Micro Devices).

ب - بیدارباش TCP STN

پ - بیدارباش UDP

ت - بیدارباش در TCP DATA

1 - Link-Layer Multicast Name Resolution

موارد ب تا ت، می‌توانند به عنوان درگاهی پالایش شده، نشانی پالایش شده، درگاه/نشانی پالایش شده و پالایش نشده، به‌طور اختیاری، محدودتر شوند. این لیست جامع نیست.

۶ پروتکل‌های چارچوب پایه

۶-۱ Ethernet 802.3 (اختیاری)

٦-١-١ داده پیکربندی

شناسه	داده‌های پیکربندی	مشاهده
C1	نشانی MAC	نشانی MAC لایه‌ای که باید پیشکار شود

٦-١-٢ الزامات رفتاری

پیشکار انتظار دارد که میزبان، ارتباط شبکه‌ای ایجاد کند. این امر مجاز است از طریق اختصاص نشانی-های ایستا یا پویا به درگاهی فیزیکی معینی باشد. اگر امنیت، فعال شده باشد، میزبان، اصالت‌سنجی درگاهی (802.1x) و پارامترهای رمزگذاری (802.1AE) را برقرار کرده است.

در طول انتقال‌های میزبان به پیشکار، میزبان باید از تغییر وضعیت پیوند واسط برای اقداماتی چون کاهش سرعت پیوند، برای کاهش مصرف توان، اجتناب کند. ممکن است نیاز باشد که میزبان، سرعت پیوند را برای تأمین الزامات توان در وضعیت خواب، کاهش دهد.

شناسه	الزامات	M/S/O	استدلال
R1	پیشکار باید قاب‌هایی را که شامل سرایندهای قاب غیر مشخص و سامان‌دهی نشده‌ی لایه ۲ هستند نادیده بگیرد	M	فرستادن بسته‌های برچسب زده QoS به پیشکار نباید باعث شود تا پیشکار برای پروتکل خاصی، شکست بخورد. این به آن معنا نیست که کاربرد خاصی، موردنیاز است. این ضمیمه‌ها می‌توانند نادیده گرفته شوند.
R2	اگر واسط اترنت 802.3، قطع شود و عملکرد روی واسطه‌های قطع‌شده، متوقف شود بهتر است پیشکار شناسایی شود	S	
R3	اگر میزبان، نشست 802.3a2LLDP را با جفت پیوند، ایجاد کرده است، بهتر است پیشکار LLDP را برای 802.3a2 پشتیبانی کند.	S	مجاز است پیشکار LLDP، پاسخ دهد که شامل تأیید هر اقدامی برای تغییر پارامتر EEE است.
R4	در پذیرش بسته هویت درخواست 802.1X EAPOL، پیشکار مجاز است میزبان را بیدار کند.	O	اعتبارنامه‌های اصلی امنیت، در میزبان هستند.

۶-۲ WiFi 802.11 (اختیاری)

۶-۲-۱ داده پیکربندی

شناسه	داده‌های پیکربندی	مشاهده
C2	نشانی MAC	نشانی MAC لایه واسطه‌ای که پیشکار شده است
C3	پروفایل کنونی	پروفایل مورداستفاده توسط میزبان برای ارتباط کنونی امن که ممکن است شامل پارامترهای ارتباطی از قبیل SSID، BSSIDT، باند/کانال باشد.
C4	کلید Pre_Master	کلید Pre-Master (802.11i PM, 802.11r PMK-R1) باید به‌طور ایمن به پیشکار منتقل شود

۶-۲-۲ الزامات رفتاری

پیشکار انتظار دارد که میزبان، ارتباط فعلی و معتبر 802.11 را با یک AP داشته باشد. اگر امنیت، فعال شده باشد، میزبان، حالت امنیت را با ساختارهای بی‌سیم ایجاد کرده است و میزبان قادر است تا قاب‌های اطلاعات 802.11 را به شبکه ارسال کند.

شناسه	الزامات	M/S/O	استدلال
R5	پیشکار باید به‌صورت غیر نقطه دسترسی الگوریتم درخت پوشا (STA) در حالت سامانه ایستگاه پایه (BSS) زیرساختی، عمل کند.	M	پیشکار فقط در حالت زیرساختی غیر نقطه دسترسی الگوریتم درخت پوشا (STA) کاربردپذیر است و حالت‌های دیگری چون IBSS، DLS، PAN و غیره را پشتیبانی نمی‌کند. (IEEE 802.11-IEEE 802.11-2007)
R6	پیشکار باید ارتباط 802.11 را با نقطه دسترسی که به SSID متعلق است حفظ کند یا دوباره ایجاد کند	M	در IEEE 802.11-2007
R7	اگر امنیت بی‌سیم در پروفایل فراهم باشد، پیشکار باید ارتباط امنی را با 4-way (802.11i, 802.11FT) به‌صورت درگاهی روش‌های ارتباطی، حفظ کند یا دوباره ایجاد کند.	M	در IEEE 802.11-2007

ادامه جدول

شناسه	الزامات	M/S/O	استدلال
R8	در نبـــود ترافیـــک دوره‌ای 802.11، پیشکار باید اتصال موجود (امن) با نقطه دسترسی را توسط فرستادن پیـام‌هـای زنده نگه‌داری حفظ کند.	M	زنده نگه‌داری مطلوب است چون برخی نقطه دسترسـی-ها، وضعیت خود را برای کارخواه‌های غیرفعال بـه‌عنـوان بخشی از روش‌های نگهداری پاک می‌کنند. سازوکارهای زنـده نگـه‌داری802.11 شـامل قـاب‌هـای اطلاعاتی NULL، 11w، روش‌هـای خـاص فروشـنده، ARP و SIP می‌باشند. بسامد مطرح‌شده، ۳ ثانیـه بـین ارسال پیام زنده نگه‌داری است
R9	پیشکار باید قطع ارتباط پیونـد مخـابره بی‌سیم با زیرساخت نقطـه دسترسـی را شناسایی کند	M	ممکن است قطع ارتباط توسط الگوریتم ویـژه فروشـنده، (مثلاً با استفاده از امواج رادیـویی ازدسـت‌رفتـه از نقطـه دسترسـی، RSSI پـایین‌تـر، سـطح آسـتانه و غیـره)، NULL، قـاب‌هـای داده یـا روش مشـخص‌شـده در 802.11w شناسایی شود.
R10		M	هر IEEE 802.11-2007
R11		M	هر IEEE 802.11-2007
R12	پیشکار(پروکسـی) اگـر توسـط AP پشتیبانی شود، از سازوکارهـای ذخیـره توان 802.11 استفاده می‌کند.	O	
R13	مجاز است پیشکار 802.11r (رومینگ سریع امن) را پیاده‌سازی کند	O	802.11r اجازه ارتباط امـن بـدون اعتبارسـنجی کامـل EAP 802.1x را می‌دهد و تأخیر رومینـگ را کـاهش می‌دهد. (IEEE 802.11r-2008)
R14	در پاسخ به AP که اعتبارسنجی را راه-انـدازی مـی‌کنـد یعنـی هویـت EAP، پیشکار، میزبان را بیدار می‌کند	M	با IEEE 802.11-2007
R15	پیشکار یـا روش‌هـای ارتبـاط مجـدد را پیاده‌سازی می‌کند یـا میزبـان را بیـدار می‌کند	M	اگر میزبان بیدار شود، انتظار مـی‌رود ارتبـاط 802.11 و روش‌های امنیتـی را پیـاده‌سـازی کنـد. توسـط IEEE 802.11.2007
R16	اگـر پیشـکار قـادر بـه ارتبـاط بـا AP نباشد، میزبان را بیدار خواهد کرد	O	
R17	ممکن اسـت پیشـکار در انقضـاء اصـلی عمر، میزبان را بیدار کند. (PMK,PMK-RO,PTK)	O	

ممکن است ارتباط بی‌سیم، در طول انتقال بیداری، متوقف شود. ممکن است پیشکار پارامترهای ارتباط بی‌سیم موجود را به میزبان تحویل دهد تا زمان انتقال بیداری را کاهش دهد.

۳-۶ ARP

۱-۳-٦ داده پیکربندی

شناسه	داده پیکربندی	مشاهده
C5	نشانی IP	نشانی IP لایه واسطهایی که پیشکار می‌شوند.

۲-۳-٦ الزامات رفتاری

شناسه	الزامات	M/S/O	استدلال
R18	پیشکار باید به‌طور صحیح به درخواست ARP که در نشانی منتشرشدهٔ لایه MAC دریافت شده‌اند پاسخ دهد	M	عملیات ARP مستلزم این است که پیشکار قادر به دریافت درخواست‌های ARP باشد (RFC 826, 1122)
R19	پیشکار باید به‌طور صحیح به درخواست ARP که در نشانی‌های یک پخشی MAC پیشکار شده دریافت می‌شوند پاسخ خواهد داد.	M	عملیات ARP مستلزم این است که پیشکار قادر به دریافت درخواست‌های ARP باشد (RFC 826, RFC, 1122)
R20	پیشکار باید به درخواست‌های ARP که در آن نشانی پروتکل هدف، نشانی IP پیشکار شده با پاسخ‌های ARP پاسخ دهد.	M	RFC 5227
R21	پیشکار باید به درخواست ARP که شامل نشانی پروتکل منبع به‌صورت صفر با پاسخ ARP است پاسخ دهد	M	این، پشتیبانی ردیاب‌های ARP برای شناسایی تناقض نشانی RFC 5227 است
R22	همه پاسخ‌های ARP ایجادشده توسط پیشکار، باید نشانی IPv4 و MAC مشابهی داشته‌باشند که در داده پیکربندی ارائه‌شده‌اند.	M	نشانی‌های فیزیکی و منطقی منبع، حوزه‌هایی در بسته پاسخ ARP هستند و پیشکار باید مقادیر مشابه آنچه میزبان اضافه کرده است را جانمایی کند.
R23	اگر پیشکار، QoS اختیاری را پشتیبانی کند، پیشکار، باید بسته‌های IPv4 را با مقدار پیش-فرض QoS یا هر مقدار QoS دیگری که توسط میزبان پیکربندی شده است نشان دهد	O	مجاز است مواردی وجود داشته باشد که در آن‌ها درخواستی بخواهد اولویت بسته‌ای را برای آن پروتکل، افزایش یا کاهش دهد (IEEE 802.1p, IEEE 802.1D)
R24	مجاز است پیشکار در هنگام شناسایی نشانی تکراری، میزبان را بیدار کند.	O	

۶-۴ کشف همسایه

۶-۴-۱ داده پیکربندی

شناسه	داده پیکربندی	مشاهده
C6	نشانی MAC	نشانی MAC واسطی که پیشکار شده است
C7	نشانی‌های تقاضای IPv6	نشانی‌های تقاضا برای نشانی‌های جهانی IPv6 و محلی پیوند واسطی که پیشکار شده است.
C8	نشانی‌های موقتی IPv6	نشانی‌های موقتی واسط‌هایی که پیشکار شده‌اند
C9	نشانی هدف IPv6	نشانی‌های هدف IPv6
C10	نشانی هدفMAC	

۶-۴-۲ الزامات رفتاری

پیشکار انتظار دارد که نشانی‌های جهانی و محلی پیوند، همان نشانی تقاضا را داشته باشند و نشانی‌های موقتی هم نشانی درخواست مشابه داشته باشند.

شناسه	الزامات	M/S/O	استدلال
R25	پیشکار باید به تقاضای همسایه ND توسط پاسخ با اعلان همسایه ND، جواب دهد.	M	به RFC 8461 رجوع شود
R26	پیشکار باید به درخواست‌های تقاضای همسایه نشانی جهانی، پاسخ دهد.	M	
R27	پیشکار باید به درخواست‌های تقاضای همسایه پیوند محلی پاسخ دهد	M	
R28	پیشکار باید به درخواست‌های تقاضای نشانی موقت جواب دهد.	M	
R29	پیشکار باید به پیام‌های تقاضای همسایه ND که شامل سرایندهای بسط‌یافته تشخیص داده شده هستند پاسخ دهد	M	سرایندهای IPv6 برای پیام‌های تقاضای همسایه می‌تواند شامل سرایندهای بسط‌یافته (REC 2460) باشد

۶-۵ بسته‌های بیدارباش

۶-۵-۱ داده پیکربندی

داده پیکربندی وجود ندارد

۲-۵-۶ الزامات رفتاری

شناسه	الزامات	M/S/O	استدلال
R30	پیشکار باید موقع تلاش اتصال ورودی TCP (TCP STN) میزبان را بیدار کند	M	پیشکار باید روش استانداردشده‌ای را برای بیدار کردن میزبان دسترسی‌های دور، پشتیبانی کند. ممکن است پیشکار معیارهای پالایش اضافی را پیاده‌سازی کند، مثلاً روی نشانی‌ها و درگاهی‌های پروتکل تا از رویدادهای بیدارباش ساختگی جلوگیری کند.
R31	پیشکار باید با ورود بسته جادویی، میزبان را بیدار کند	M	

۷ مدیریت و پیکربندی پیشکار

میزبان، پیشکار را برای عملیاتی شدن هدایت می‌کند. مجاز است تا پیشکار(پروکسی) آغاز به کار کند و میزبان بیدار شود زمانی صرف شود بنابراین، مجاز است بارها زمانی که نه میزبان فعال است و نه پیشکار، برسد. تغییر واپایش عملیاتی بین پیشکار و میزبان بهتر است به شیوه‌ای به‌موقع انجام شود تا از افت کارکردی اجتناب شود.

مجاز است چندین واسط به یک شبکه یکسان مرتبط شوند. مجاز است پیشکار بیش از یک واسط را پشتیبانی کند.

۷-۱ داده‌های پیکربندی

شناسه	داده‌های پیکربندی	مشاهده
C11	قابلیت‌های پیشکار	مجموعه قابلیت‌هایی که پیشکار نشان می‌دهد
C12	پیکربندی پیشکار	میزبان، قابلیت‌های خاصی را امکان‌پذیر می‌سازد و برای آن قابلیت‌ها داده فراهم می‌کند

۷-۲ الزامات رفتاری

پیشکار قابلیت‌های خود را به میزبان نشان می‌دهد. میزبان، عملیات پیشکار را پیکربندی، آغاز می‌کند و پایان می‌دهد.

شناسه	الزامات	M/S/O	استدلال
R32	پیشکار باید برای شروع و پایان عملیات از دستورالعمل‌های میزبان پیروی کند	M	هر توانایی پیشکار مجاز است غیرفعال شود. انتظار نمی‌شود که پیشکار آن توانایی‌ها را فعال کند میزبان مجاز است خودش بیدار شود بنابراین مجاز است قبل از اینکه پیشکار، خودش با شرایط بیداری مواجه شود عملیات پیشکار را خاتمه دهد

ادامه جدول

شناسه	الزامات	M/S/O	استدلال
R33	با پیگیری توقف یک قابلیت، مجاز است پیشکار عملیات قابلیت‌های فعال دیگر را ادامه دهد.	O	
R34	توصیه نمی‌شود هنگامی‌که اتصال رسانه قطع می‌شود پیشکار میزبان را بیدار کند.	S	در غیر این صورت، هنگامی‌که سوده دوباره راه‌اندازی می‌شود، همه میزبان‌ها بیدار می‌شوند. برای بیدار کردن میزبان، دلایل معتبری وجود دارد.
R35	پیشکار باید قادر به بیدار کردن میزبان باشد	M	
R36	پیشکار باید بسته‌های بدشکل را نادیده بگیرد	M	پردازش بسته‌های IPv4، باید با RFC791 مطابقت کند
R37	پیشکار باید بسته‌های IPv4 تکه‌شده را نادیده بگیرد	M	بسته‌های تکه‌شده قابلیت بهره‌جویی امنیتی را مقدور می‌سازد.
R38	پیشکار باید بسته‌های IPv4 با منبع خاص فرستنده را نادیده بگیرد	M	با استفاده از مسیریابی نشانی منبع، دیواره‌های آتش پیشگیری‌کننده مانع بسته می‌شوند

۷-۲-۱ داده برگشتی (اختیاری)

شناسه	داده پیکربندی	مشاهده
C13	نشان وضعیت، شامل هر اطلاعات خطا (اختیاری)	
C14	بسته‌ای که بیداری میزبان را راه‌اندازی می‌کند	

۸ اختیاری‌ها

۸-۱ IGMP چندپخشی (اختیاری)

۸-۱-۱ داده‌های پیکربندی

شناسه	داده پیکربندی	مشاهده
C14	نشانی‌های چندپخشی مشترک شده	نشانی‌های IP چندپخشی که پیشکار می‌شوند.

۸-۱-۲ الزامات رفتاری

شناسه	الزامات	M/S/O	استدلال
R39	در انتقالات میزبان به پیشکار، پیشکار باید همه نشانی‌های چندپخشی پیکربندی شده را ثبت کند.	M	این امر، احتمال پرسمان گزارش ازدست‌رفته را در طول انتقال به عملیات پیشکار، کاهش می‌دهد.
R40	پیشکار باید نسخه دو IGMP را پیاده‌سازی کند	M	نسخه ۳ با در برگرفتن/مستثنی کردن میزبان‌های دیگر نسخه ۲ را بسط می‌دهد و این برای پیشکار، ضروری نیست. (RFC 2236)

۸-۲ اختصاص نشانی DHCP (اختیاری)

۸-۲-۱ داده پیکربندی

شناسه	داده پیکربندی	مشاهده
C16	نشانی IP میزبان	
C17	پوشش زیرشبکه برای نشانی IP تک‌پخشی	
C18	نشانی IP دروازه	
C19	زمان باقی‌مانده اجاره DHCP	
C20	نشانی IP کارساز DHCP	مجاز است همان نشانی دروازه در بالا باشد.

۸-۲-۲ الزامات رفتاری

شناسه	الزامات	M/S/O	استدلال
R41	مجاز است پیشکار، میزبان را قبل از انقضا اجاره نشانی، بیدار کند.	O	در بیداری، انتظار می‌رود، میزبان، اجاره را تمدید کند.
R42	مجاز است پیشکار،DHCP RENEW را انجام دهد.	O	پیشکار ممکن است عملیات نشانی را از قبیل تجدید اجاره، انجام دهد. این امر، پیاده‌سازی DHCP در پیشکار تعریف می‌شود.
R43	اگر DHCP RENEW در پیشکار پیاده‌سازی شود، پیشکار مجاز است اگر اجاره نشانی، از دست برود یا پارامترهای بحرانی DHCP تغییر کرده باشند میزبان را بیدار کند.	O	اگر حالت نشانی IP از دست برود یا به چیزی غیر از آنچه میزبان، قبل از شروع پیشکار داشته است تغییر کند، پیشکار بیش از این برای میزبان، کار پیشکاری (پروکسی) انجام نمی‌دهد.

۸-۳ دسترسی از دور با استفاده از SIP و IPv4 (اختیاری)

شناسه	داده پیکربندی	مشاهده
C21	کارساز SIP(نشانی IP یا نام دامنه)	
C22	روش اصالت‌سنجی SIP و اعتبارنامه‌های SIP	
C23	نشانی IP کارساز DNS	

۸-۳-۱ الزامات رفتاری

شناسه	الزامات	M/S/O	استدلال
	الزامات چارچوب پایه IP		
R44	SIP باید رروی UDP پیاده‌سازی شود	M	همان‌طور که در RFC های SIP موردنیاز است
R45	مجاز است SIP روی TCP پیاده‌سازی شود	O	از RFC 3261 مشخص می‌شود که به TCP نیاز دارد.
R46	اگر پیشکار کارسازی را با اسم بپذیرد، باید تفکیک نام را پیاده‌سازی کند.	O	کارساز DNS ممکن است متعادل کردن بار را پیاده‌سازی کند و یک نشانی IP تکی بهتر است استفاده نشود.
	پروتکل آغاز نشست SIP برای بیداری از دور		
R47	پیشکار باید ثبت‌نام SIP را در کارساز SIP همان طورکه در RFC 3261 آمده است، حفظ کند	M	برای کاربرد بیداری برای کار کردن، موردنیاز است.
R48	پیشکار باید تضمین کند که پیام INVITE می‌تواند از کارساز SIP دریافت شود حتی از طریق چندین لایهNAT	M	کارساز باید قادر باشد تا پیام بیداری را به پیشکار بفرستد. بخش خارج از محدوده RFC SIP، روش-هایی را برای باز نگه‌داشتن NAT، شرح می‌دهد. یک روش متداول، فرستادن پیام ثبت مجدد SIP هر ۲۹ ثانیه است.
R49	هنگامی‌که چالش احراز هویت SIP، توسط کارساز و با دریافت پیام ثبت‌نام مجدد از پیشکار دریافت می‌شود باید با کارساز SIP دوباره اصالت‌سنجی شود.	M	شکست در اصالت‌سنجی مجدد، باعث می‌شود تا پیشکار، در کارساز «در دسترس» نباشد یا «بیرون» رود.
R50	هنگامی‌که یک پیام معتبر SIP INVITE توسط پیشکار دریافت می‌شود و انتقال SIP، از نوع TCPاست، پیشکار باید پردازش حالت در هر RFC 3261 را با فرستادن پیام پاسخ SIP و دریافت پیام ACK SIP، کامل کند.	M	اگر پیشکار بتواند در طول پردازش حالت زود بیدار شود و به عملکردش ادامه دهد، بیداری می‌تواند در هرزمانی روی دهد. اگر پیشکار نتواند عملکرد را پس از سیگنال بیداری، انجام دهد، پیشکار نیاز دارد تا برای پایان پردازش، قبل از اینکه بتواند سیگنال بیداری ارسال کند، صبر کند.

ادامه جدول

شناسه	الزامات	M/S/O	استدلال
R51	هنگامی‌که یک پیام معتبر SIP INVITE توسط	M	انتظار می‌رود که میزبان، ثبت SIP را پس از بیداری،

	پیشکار دریافت می‌شود و انتقال SIP، از نوع UDPاست، پیشکار باید پیام پاسخ SIP پردازش حالت را آن‌طور که در RFC 3261 است ارسال و میزبان را بیدار کند.		خاتمه دهد.

۸-۴ دسترسی از دور با استفاده از TEREDO برای IPv6

پیشکار انتظار دارد که میزبان از قبل یک ارتباط TEREDO با کارساز TEREDO ایجاد کرده باشد. پیشکار فقط مسئول فرستادن پیام زنده نگه‌داری دوره‌ای است. ممکن است یک یا چند نمونه از این توانایی، وجود داشته باشد.

۸-۴-۱ داده پیکربندی

شناسه	داده پیکربندی	استدلال
C24	بازه زمان بیشینه و کمینه	کمینه و بیشینه می‌توانند در مقدار مشابهی تنظیم شوند. بازه زمان دوره‌ای (بر حسب ثانیه) زمان بیشینه بین بسته‌هایی را که به بیرون فرستاده می‌شوند مشخص می‌کند.
C25	بسته کامل	بسته‌های تقاضای ره‌یاب، توسط میزبان در RFC 4380، تشکیل می‌شوند. پیشکار با تکیه بر میزبان سعی می‌کند بسته خوش فرم وارسی شده‌ی یکپارچه‌ای را فراهم آورد.

۸-۴-۲ الزامات رفتاری

شناسه	الزامات	M/S/O	استدلال
R52	پیشکار باید به‌طور دوره‌ای، بسته را در دامنه بازه‌های بیشینه و کمینه ارسال کند.	M	پیام تقاضای مسیر (RS) به کارساز TEREDO فرستاده می‌شود. پیام‌های RS، نگاشت‌های NAT را نوسازی می‌کنند.(RFC 4380 بخش ۵-۲). پیشکار همه پاسخ‌ها به RS را نادیده می‌گیرد.
R53	پیشکار باید برای دریافت بسته حبابی[1] غیرمستقیم، میزبان را بیدار کند.	M	برای بسته حبابی غیرمستقیم به RFC 4380 رجوع شود.

۸-۵ پروتکل مدیریت شبکه ساده (SNMP)

این گزینه، عملیات پیشکار را برای SNMPv1 و SNMPv2 مشخص می‌کند.

۸-۵-۱ داده پیکربندی

شناسه	داده پیکربندی	مشاهده
C26	درگاهی‌های UDP مورداستفاده، نام‌های ارتباطی SNMP (با خاصیت دسترسی) getall_flag(در مجموعه OID، در GET/SET با	

1 - Bubble packet

	OID ناشناخته)	
C27	فهرست جفت مقادیر OID	جفت مقادیر OID واجد تمام شرایط و هر خاصیت دسترسی OID ذخیره شوند.

۸-۵-۲ الزامات رفتاری

شناسه	الزامات	M/S/O	استدلال
R54	پیشکار باید SNMPv1,v2 را پشتیبانی کند.	M	به RFC 1156,RFC 1157,RFC 1441 رجوع شود.
R55	پیشکار باید به مقدار مشخص‌شده در جدول جفت مقادیر OID به SNMP GET REQUEST به OID ذخیره‌شده، پاسخ دهد.	M	مقدار برگشتی، از جدول مقادیر OID تأمین می‌شود.
R56	پیشکار باید از درخواست SNMP GET NEXT پشتیبانی کند.	M	برای جابجایی‌های SNMP موردنیاز است. جدول جفت مقادیر OID، توالی‌های دیگری را نسبت به MIB اصلی و دیگر NEXT ها دارد.
R57	اگر getall_flag، فعال نیست، پیشکار باید به SNMP GET REQUEST برای یک OID ذخیره نشده همان‌طور که در RFC 1157(RETURN NO SUCH NAME) مشخص‌شده پاسخ دهد.	M	پیشکار نمی‌تواند بین OID که میزبان آن را پشتیبانی نمی‌کند یا OID که از MIB از دست رفته است، تمایز قائل شود.
R58	اگر getall_flag، فعال باشد، پیشکار باید میزبان را با یک SNMP GET REQUEST به OID ذخیره نشده، بیدار کند.	M	
R59	اگر هر ارتباط قابل تغییری، توسط میزبان تعریف شود، پیشکار باید با یک SNMP SET REQUEST میزبان را بیدار کند.	M	بهتر است اگر ارتباط قابل تغییری وجود ندارد تنظیمات دلخواه برای OID های ذخیره شده یا ذخیره نشده میزبان را بیدار نکنند.

۸-۶ کشف خدمت با استفاده از mDNS

۸-۶-۱ داده پیکربندی

شناسه	داده پیکربندی	مشاهده
C28	نشانی‌های واسط	نشانی‌های واسط میزبان همان‌گونه که به‌صورت رکوردهای A و AAAA اعلان شده‌اند.
C29	دامنه نام میزبان	نام میزبان در «local.» همان‌گونه که در رکوردهای PRT اعلام شده است (DNS معکوس)
C30	رکوردهای خدمت	همان‌طور که در رکوردهای SRV اعلام شده است.
C31	مجموعه‌های رکورد منابع اشتراکی	اگر پیشکار قادر به شرکت در مجموعه‌های رکورد منابع اشتراکی باشد، پس میزبان، این داده‌ها را برای پیشکار فراهم می‌آورد.

C32	نام‌های خدمت	همان‌طور که در رکوردهای PTR با رجوع به رکوردهای SRV اعلام شده است.
C33	داده‌های کمکی	همان‌طور که در رکوردهای TXT مرتبط با رکوردهای SRV در مجموعه‌های رکورد منابع اشتراکی ، اعلام شده است.
C34	نشانی‌های چندپخشی	اگر پیشکار عضویت در گروه‌های چندپخشی mDNS را با گستره بیشتری نسبت به پیوند محلی، حفظ کند.

۸-۶-۲ الزامات رفتاری

پیشکار انتظار دارد مشابه هر چارچوب پایه با دست‌کم یک نام دامنه تمام واجد شرایط متناظر در دامنه سطح بالای<.local>، یک یا چند نشانی IP معتبر (IPV6 و/یا IPV4) حمایت شود. میزبان همه عملیات اعلام و جستجوی mDNS را قبل از شروع خواب، کامل می‌کند (به بخش ۹ پیش‌نویس mDNS رجوع شود)

شناسه	الزامات	M/S/O	استدلال
R60	پیشکار باید عضویت در گروه mDNS محلی مرتبط با چارچوب‌های اصلی پروتکل اینترنتی خودش را حفظ کند. 224.0.0.251 برای IPV4 ff02::fb برای IPV6	M	این امر شامل فرستادن بسته‌های IGMP وMLD است و پیشکار نیاز به دریافت و پردازش پیام‌های mDNS پیوند محلی دارد.

ادامه جدول

شناسه	الزامات	M/S/O	استدلال
R61	پیشکار مجاز است عضویت در گروه‌های mDNS را با محدوده‌ای گسترده‌تر از دامنه پیوند محلی حفظ کند.	O	در آینده mDNS محدود به دامنه پیوند محلی نخواهد بود.
R62	پیشکار باید همه پیام‌های دریافت شده در درگاهی 5353 UDP با مقصد چندبخشی IP پیوند محلی را برای گروه‌های mDNS که در آن‌ها میزبان یک عضو است پردازش کند.	M	
R63	پیشکار باید برای هر شناسه mDNS، پرسمان‌های mDNS دریافت شده در درگاهی5353 UDP را در همه واسط نشانی‌های IP پردازش کند.	M	
R64	پیشکار باید نشانی منبع پیام‌های دریافت شده mDNS را وارسی کند و پیام‌های انتقال‌یافته از نشانی‌های خارج از دامنه گروه چندبخشی mDNS را نادیده بگیرد.	M	شکست در برآورده کردن این الزام ممکن است پیامدهای منفی امنیتی داشته باشد.
R65	هنگام انتقال در IPV4، پیشکار باید پاسخ‌های mDNS را با TTL در سرایند IP با تنظیم مقدار ۲۵۵ بفرستد.	M	این الزامی برای پاسخ‌دهنده‌های mDNS با استفاده از IPV4 به خاطر وجود کارخواه‌های قدیمی‌تر mDNS است.
R66	پیشکار بهتر است بیت پاسخ تک‌پخشی در فیلد رسته DNS چندپخشی را قبول کند و طبق آن پاسخ‌های تک‌پخشی بفرستد.	S	یعنی اگر پاسخ‌دهنده، چندپخشی دارد که اخیراً ثبت می‌کند (در یک‌چهارم TTL برای ثبت) این توصیه هم برای پیشکار همچون میزبان اعمال می-شود.
R 67	پیشکار باید پاسخ‌های جواب معلوم را موقوف کند و نباید به سؤالی که شامل پاسخی با TTL حداقل نصف مقدار صحیح است پاسخ دهد.	M	بخش ۷-۱ از پیش‌نویس نسخه mDNS 07

ادامه جدول

شناسه	الزامات	M/S/O	استدلال
R68	پیشکار باید پاسخ‌های جواب معلوم چند بسته‌ای را موقوف کند و باید در یک فاصله زمانی تصادفی بین 400ms و 500ms پس از دریافت پرسمانی با مجموعه بیت بریده (TC)[a] قبل از فرستادن پاسخ منتظر بماند و نباید درحال انتظار، به پاسخی که در پرسمان‌های بعدی دریافت شده، می‌آید جواب دهد.	M	بخش ۷-۲ و ۷-۴ از پیش‌نویس نسخه 07 mDNS
R69	جز زمان موقوف کردن پاسخ‌های معلوم، پیشکار باید زمانی که جواب‌های منفی یا غیر پوچ مثبت معتبر را پردازش می‌کند، پاسخ دهد.	M	بخش ۸ از پیش‌نویس mDNS
R70	پیشکار باید فوری به پرسمان برای رکوردهای A و AAAA برای یکی از نام-های دامنه تمام واجد شرایط میزبان، پاسخ دهد.	M	بخش ۸ از پیش‌نویس mDNS
R71	پیشکار باید فوری پاسخ مثبتی به پرسمان برای رکوردهای PTR دامنه 254.169.in-addr.arpa که متناظر با هر نشانی واسط پیوند محلی IPV4 است پاسخ دهد.	M	بخش‌های ۵ و ۸ از پیش‌نویس mDNS
R72	پیشکار بهتر است به پرسمان برای رکوردهای A و AAAA با قرار دادن همه نشانی‌های دیگر واسط که توسط میزبان در بخش جواب‌های اضافی، پیکربندی‌شده‌اند پاسخ دهد.	S	بخش ۸-۲ از پیش‌نویس mDNS
R73	پیشکار نباید با پاسخ پوچ جواب دهد	M	
R74	پیشکار باید قبل از پاسخ به پرسمان برای رکوردهای PTR با نام‌های دامنه تمام واجد شرایط که به «local.» ختم می-شوند منتظر فاصله زمانی اتفاقی که بیش از 500ms نیست، بماند.	M	

ادامه جدول

شناسه	الزامات	M/S/O	استدلال
R75	پیشکار باید فوری به پرسمان برای رکوردهای TXT و SRV با نام‌های دامنه تمام واجد شرایط که به «local.» ختم می‌شوند و برای آن‌ها پاسخ‌دهنده منحصربه‌فردی است، پاسخ دهد	M	بخش ۸ از پیش‌نویس mDNS
R76	اگر پیشکار در رکوردهای منابع اشتراکی شرکت کند باید قبل از پاسخ به پرسمان برای رکوردهای TXT و SRV با نام‌های دامنه تمام واجد شرایط که به «local.» ختم می‌شوند منتظر فاصله زمانی اتفاقی که بیش از 500ms نیست، بماند.	M	بخش ۸ از پیش‌نویس mDNS
R77	پیشکار باید پیام‌های پرسمان mDNS تشکیل‌شده از بیش از یک سؤال را پردازش کند.	M	بخش ۸-۳ از پیش‌نویس mDNS
R78	پیشکار بهتر است هر زمان مقدور است، پاسخ‌ها را جمع‌آوری کند.	S	بخش ۸-۴ از پیش‌نویس mDNS
R79	پیشکار باید پاسخ درستی به پرسمان‌های DNS چندپخشی (بخش ۸-۵ از mDNS) DNS با پاسخ‌های تک‌بخشی مستقیم با قالب DNS تک‌بخشی متداول، بدهد.	M	بخش ۸-۵ از پیش‌نویس mDNS
R80	هنگامی‌که تفکیک تداخل نیاز است پیشکار باید میزبان را بیدار کند.	M	تشخیص تفکیک تداخل، در بخش ۱۰ پیش‌نویس mDNS شرح داده‌شده است.
R81	اگر پیشکار دانش پیشرفته‌ای دارد که الزامات مصرف انرژی میزبان، هنگامی‌که رویدادی ایجاد می‌شود که مستلزم بیداری آن است برآورده نمی‌شود، مجاز است بسته خداحافظی بفرستد تا نشان دهد که دیگر این خدمت در دسترس نیست	O	بخش ۱۱-۲ از پیش‌نویس mDNS

[a] Truncated

۸-۷ تفکیک اسم با LLMNR

۸-۷-۱ داده‌های پیکربندی

شناسه	داده‌های پیکربندی	الزامات
C35	نشانی‌های واسط	نشانی‌های واسط میزبان آن‌طور که در رکوردهای A و AAAA اعلام شده است.
C36	نام میزبان	نام میزبان، آن‌طور که در رکوردهای PTR (DNS معکوس) اعلام شده است.

۸-۷-۲ الزامات رفتاری

این الزامات، فرض می‌کنند مشابه هر چارچوب پایه با دست‌کم یک نام تک برچسبی[1]، یک یا چند نشانی IP معتبر (IPV6 و/یا IPV4) حمایت شود.

شناسه	الزامات	M/S/O	استدلال
R82	پیشکار باید دریافت و فرستادن پرسمان‌ها روی UDP را پشتیبانی کند.	M	بخش ۲-۱ از [MS-LLMNRP]
R83	پیشکار باید پاسخ‌هایی به بزرگی بیشینه مقدار پایه‌بار UDP را که می‌تواند در IPv4 یا IPv6 حمل شود، بپذیرد و بفرستد.	M	این الزامی از پروفایل LLMNR شرح داده شده در بخش‌های ۵-۱-۳ و ۵-۲-۳ [MS-LLMNRP] است.
R84	پیشکار باید عضویت در گروه‌های پیوند محلی LLMNR مرتبط با چارچوب‌های اصلی پروتکل اینترنتی آن را یعنی 224.0.0.252 برای IPv4 و ffo2::1::3 برای IPv6 حفظ کند.	M	این امر، شامل فرستادن بسته‌های IGMP و MLD است و نیاز است که پیشکار اجازه دریافت و پردازش پیام‌های پیوند محلی LLMNR را بدهد.
R85	پیشکار باید پرسمان‌های LLMNR معتبر دریافت شده در درگاهی UDP 5355 را با نشانی چندپخشی IP پیوند محلی به‌عنوان مقصد، پردازش کند.	M	این، الزام اصلی هر پاسخ‌دهنده LLMNR است.
R86	پیشکار باید پرسمان‌های UDP LLMNR فرستاده‌شده به نشانی تک‌پخشی را نادیده بگیرد.	M	این، الزام اصلی هر پاسخ‌دهنده LLMNR است. شکست در برآورده کردن این الزام مجاز است پیامدهای امنیتی منفی داشته باشد.
R87	پیشکار باید به پرسمان برای AAAA، A، PTR و ANY پاسخ دهد.	M	این امر الزام اصلی برای پیاده‌سازی‌های LLMNR مطابق با پروفایل LLMNR شرح داده‌شده در بخش ۵-۲- ۳ از [MS-LLMNRP] است.

1 - Single-label

ادامه جدول

شناسه	الزامات	M/S/O	استدلال
R88	هنگام انتقال در IPV4، پیشکار باید همه پاسخ‌های LLMNR را با TTL در سرایند IP تنظیم شده با مقدار ۲۵۵ بفرستد.	M	این امر الزامی برای پاسخ‌دهنده‌های LLMNR، با استفاده از IPV4 است که در کنار کارخواه-های قدیمی‌تر LLNR وجود دارند.
R89	هنگامی‌که تفکیک تداخل نیاز است پیشکار باید میزبان را بیدار کند.	M	تشخیص تفکیک تداخل، در بخش ۴ از RFC4795 شرح داده‌شده است.
R90	پیشکار باید به پرسمان LLMNR با استفاده از کدگذاری UTF-8 (برچسب‌های U) پاسخ خواهد داد.	M	پشتیبانی بین‌المللی کردن، در [LLMNRP] بخش ۵-۲-۳ شرح داده‌شده است.

پیوست الف

(اطلاعاتی)

ملاحظات سامانه

الف-۱ حالت توان DC و AC

اگر پیشکار بتواند وضعیت عملیاتی میزبان (به‌طور مثال درپوش رایانه کیفی[1]) یا منبع توان فعلی را تشخیص دهد و برای آن اقدامی کند، خط‌مشی‌های مدیریت توان و پیشکارهای شبکه، سودمند هستند.
در بخش زیر برخی موارد ارتقایی برای سامانه ارائه‌شده‌اند که عمر باطری را طولانی می‌کنند و تجربه سیار بودن بهتری را به کاربران می‌دهند. توصیه می‌شود که OEM[2] به حل این مسائل سخت‌افزاری کمک کند. موارد زیر توسط کاربر، پیکربندی می‌شوند تا سناریوهای زیر پیاده‌سازی شوند:
- پیشکار خواب می‌تواند اگر منبع توان از AC به حالت استفاده از باطری تغییر کند درحالی‌که خواب بوده است WoL[3]/پیشکار را خاموش/روشن کند. برای مثال، هنگامی‌که کاربری، رایانه کیفی در حالت خوابی را جدا می‌کند تا ببرد.
- یک پیشکار خواب اگر بتواند تشخیص دهد که کاربر، پوشش رایانه کیفی را بسته است می‌تواند WoL/پیشکار را غیرفعال کند. این کارکرد بهتر است توسط کاربر به‌عنوان بخشی از خط‌مشی یا گزینه-های مدیریت توان قابل پیکربندی باشد. برای مثال کاربر درحالی‌که پوشش رایانه کیفی باز است WoL/پیشکار را فعال می‌سازد اما زمانی که رایانه کیفی بسته است و در کیف قرار می‌گیرد خاموش است.
- پیشکار خواب می‌تواند تغییر در منبع توان (DC به AC) را شناسایی کند و پیشکار را در شبکه‌ی از پیش پیکربندی‌شده، فعال کند.
- پیشکار می‌تواند زمانی که سامانه از حالت AC به DC تغییر کند به عملیات ادامه دهد.
توانایی تشخیص این رویدادها زمانی که در حالت توان پایین (D3) است با این سخت‌افزارهای امروزی، امکان‌پذیر نیست. پیاده‌سازی یک راه‌حل برای این رویدادها به ذخیره انرژی و تقویت تجربه کاربر، کمک می‌کند.

الف-۲ موارد امنیتی

این استاندارد ملی، نگرانی‌های امنیتی ایجادشده از طراحی پروتکل پیشکار ارائه‌شده را نشان نمی‌دهد. اما تعدادی از سناریوهای تعریف‌شده تهدید بالقوه و کاهش بالقوه آن‌ها در بخش زیر، ارائه‌شده است.

1 - Laptop Lid
2 - Other Equipment Manufacturer
3 - Wake on LAN

– بندآوری[1] حمله خواب: این امکان هست که رقیب، بسته‌های نقطه به نقطه اصالت‌سنجی نشده‌ای را به صورت دوره‌ای به پیشکار بفرستد و سامانه را از وارد شدن یا ماندن در وضعیت خواب، بازدارد. این امر می‌تواند به‌طور جزیی و با استفاده از سازوکارهای دفاعی (دیواره‌های آتش، سامانه‌های تشخیص و پیشگیری ازنفوذ) به‌صورت بیرونی یا به‌صورت بخشی از سامانه، کاهش یابد.

– پیشکار در معرض خطر: این امکان هست که رقیب، واپایش پیشکار را به دست گیرد و از پیشکار برای شروع حملات به سامانه، شبکه یا دیگر ماشین‌های مرتبط به اینترنت استفاده کند. این امر می‌تواند به‌طور جزیی با استفاده از فنون سنجش سامانه برای تضمین یکپارچگی و استحکام سخت‌افزار/میان‌افزار/ نرم‌افزاری که در داخل پیشکار اجرا می‌شود کاهش یابد.

– حملات انهدامی: امکان دارد که رقیب، واپایش پیشکار را به دست گیرد و از آن برای ایجاد بسته‌های IP با سرایند اختیاری استفاده کند که سازوکارهای بیرونی دفاعی را گیر بیندازد. از این کار می‌توان به‌طور جزیی با غیرمجاز کردن پیشکار برای ایجاد بسته‌های IP با گزینه‌هایی در سرایند آن، پیشگیری کرد.

–IPSec: IPSec می‌تواند در یک یا دو حالت باز شود- حالت‌های تونل و انتقال. حالت تونل، برای پوشینه‌دارسازی[2] IPSec ترافیک VPN در جایی که یک کارخواه دور به یک یا چند گره شبکه از طریق دروازه VPN دسترسی می‌یابد، استفاده می‌شود. ترافیک در مسیرها در شبکه‌ی مورداطمینان، معمولاً معلوم است.

حالت انتقال IPSec برای پشتیبانی از روابط منفرد بین نقاط پایانی IP درون شبکه استفاده می‌شود. در این مورد، هر اتصال نظیر به نظیر بین گره‌ها می‌تواند توسط مجمع امنیت IPSec (SA) پشتیبانی شود. تصمیم برای پشتیبانی کردن یا نکردن، توسط خط‌مشی IPSec است و خط‌مشی توصیه‌شده‌ی سازمان، نیاز به IPSec داخلی است نه IPSec خارج از محدوده. در صورت نیاز، دریافت‌کننده، آغازکننده را برای برقراری IPSec به چالش می‌کشد. اثر جانبی قابل مشاهده، اتصالات TCP آغازین (TCP SYN) است که معلوم(Clear) فرستاده می‌شود. علاوه بر این خط‌مشی‌ها، مذاکرات IPSec به‌موازات درخواست اتصال، روی می‌دهد. ترافیک پس از آغاز TCP SYN، شامل استراحت‌های اضافی TCP SYN است و هم‌چنان که ترافیک بیشتر می‌شود احتمالاً در IPSec خواهد بود.

اگرچه یک خط‌مشی متداول نیست اما ممکن است خط‌مشی آغازین به IPSec خارج از محدوده نیز نیاز داشته باشد. اگر این‌گونه باشد، راه‌اندازی اتصال با بسته کاوند[3] در درگاهی AUTHIP UDP یا IKE مقدم خواهد بود.

در استفاده IPSec به همراه یک پیشکار، بسته آغازین IPV6 TCP SYN که برای بیدار کردن میزبان استفاده می‌شد، مجاز است توسط IPSec ، رمزگذاری شود (اگر خط‌مشی هماهنگی SA ی موجود، قبلاً

1 - Denial
2 - Encapsulation
3 - Probe

بین نقاط نظیر مذاکره شده باشد)؛ اما مورد متداول مورد انتظار، بـرای بسـته آغـازینIPV6 TCP SYN که فرستاده می‌شود در حالت معلوم است. (با خط‌مشی‌های توصیه‌شده IPSec که در بالا ذکر شد). بـرای ساده‌سازی این دو مورد، میزبان بهتر است به‌طور مشخص، IPSec های مجمع امنیتی موجـود را قبـل از رفتن به حالت خواب و گذار به حالت پیشکار، حذف یا غیرفعال کند.

اگر IPSec ، برای «راز اشتراکی» یا نیاز به IPSec خارج از محدوده، پیکربندی شـود، IPV6 TCP SYN در ابتدا معتبرسازی و رمزگذاری می‌شود. در هرکدام از این توالی‌ها، بیداری می‌تواند از آغاز انتقـال IKE باشد. پیشکار باید قادر به بیدار کردن الگوی IKEV1/AUTHIP باشد تا این پیکربندی را انجام دهد.

پیوست ب

(اطلاعاتی)

پروتکل‌های در نظر گرفته‌شده‌ی ضمیمه نشده

ب-۱ SNMPv3

گروه وظایف، پروتکل SNMPv3 را برای پیشکار تحلیل کرده است اما اتفاق‌نظر بر این شد تا ویژگی‌های SNMPv3 تا حد زیادی به خاطر ملاحظات امنیتی که در معماری امنیت SNMPv3 از RFC 3411، RFC 3414 و RFC 3415 تعریف شده است، از این استاندارد مستثنی شود.

ب-۲ UPnP

گروه وظایف، UPnP را برای پیشکار تحلیل کرده است و تعیین کرده است که UPnP DA 1.1 مانع هر پیشکار قابل‌اعمال ساده‌ای می‌شود. هزینه و پیچیدگی طراحی، پیاده‌سازی و اعتبارسنجی پیشکار بسیار زیاد خواهد بود. پیشکار UPnP به کارکردهای متعدد پیوند UPnP به درگاه‌های مختلفی که در حال حاضر توسط استاندارد UPnP پشتیبانی نمی‌شود، نیاز دارد. اگر UPnP از درگاه‌های مختلف پشتیبانی کند، پیشکار مجاز است طوری طراحی شود که کارکردهای خاص را ساماندهی کند و میزبان-های دیگر را بیدار کند.

در صورت علاقه‌مندی برای پیاده‌سازی، به استانداردهای زیر رجوع شود:

- ISO/IEC 29341-16-1:2011, Information technology -- UPnP Device Architecture -- Part 16-1: Low Power Device Control Protocol -- Low Power Architecture

- استاندارد ملی ایران قسمت ۱۶-۱۰- شماره ۲۹۳۴۱: سال ۱۳۹۳، فناوری اطلاعات - معماری افزاره جامع اتصال و اجرا (UPnP) - قسمت ۱۶-۱۰: پروتکل واپایش افزاره توان پایین – خدمت پیشکار(پروکسی) توان پایین

- - استاندارد ملی ایران قسمت ۱۶-۱۱- شماره ۲۹۳۴۱: سال ۱۳۹۳، فناوری اطلاعات - معماری افزاره جامع اتصال و اجرا (UPnP) - قسمت ۱۶-۱۱: پروتکل واپایش افزاره توان پایین – خدمت توان پایین

کتاب‌نامه

[1] RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[2] RFC 3736, Stateless Dynamic Host Configuration Protocol
[3] RFC 4862, IPv6 Stateless Address Autoconfiguration
[4] RFC 4941, Privacy Extensions for Stateless Address Autoconfiguration in IPv6
[5] RFC 4795, Link-Local Multicast Name Resolution (LLMNR)
[6] RFC 4214, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
[7] RFC 4380, Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)
[8] RFC 2710, Multicast Listener Discover (MLD)
[9] RFC 3810, Multicast Listener Discover (MLD)
[10] RFC 826, An Ethernet Address Resolution Protocol; David C. Plummer (MIT); November 1982; http://tools.ietf.org/html/rfc826
[11] RFC 3927, Dynamic Configuration of IPv4 Link-Local Addresses; S. Cheshire (Apple Computer), B. Aboba (Microsoft), E. Guttman (Sun Microsystems); May 2005; http://tools.ietf.org/html/rfc3927
[12] RFC 2131, Dynamic Host Configuration Protocol; R. Droms (Bucknell University); March 1997; http://tools.ietf.org/html/rfc2131
[13] RFC 1112, Host Extensions for IP Multicasting; S. Deering (Stanford University); August 1989; http://tools.ietf.org/html/rfc1112
[14] RFC 2236, Internet Group Management Protocol, version 2; W. Fenner (Xerox PARC); November 1997; http://tools.ietf.org/html/rfc2236
[15] RFC 3376, Internet Group Management Protocol, version 3; Multiple Authors and Multiple Organizations; October 2002; http://tools.ietf.org/html/rfc3376
[16] RFC 675, Specification of Internet Transmission Control Program; Vinton Cerf, Yogen Dalal, Carl Sunshine; December 1974; http://tools.ietf.org/html/rfc675
[17] RFC 793, Transmission Control Protocol; Multiple Authors; September 1981; http://tools.ietf.org/html/rfc793
[18] RFC 2988, Computing TCP's Retransmission Timer; V. Paxson (ACIRI), M. Allman (NASA);November 2000; http://tools.ietf.org/html/rfc2988
[19] RFC 1034, Domain Names – Concepts and Facilities; P. Mockapetris (ISI); November 1987; http://tools.ietf.org/html/rfc1034
[20] RFC 1035, Domain Names – Implementation and Specification; P. Mockapetris (ISI); November 1987; http://tools.ietf.org/html/rfc1035
[21] RFC 768, User Datagram Protocol; J. Postel; August 1980; http://tools.ietf.org/html/rfc768
[22] RFC 791, Darpa Internet Program Protocol Specification; Information Sciences Institute University of Southern California; September 1981; http://tools.ietf.org/html/rfc791
[23] IEEE, "Draft supplement to Standard for Telecommunications and Information Exchange between systems – LAN/MAN Specific requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specification: Amendment 4: Protected Management Frames", IEEE Standard 802.11w D9.0
[24] IEEE, "Draft supplement to Standard for Telecommunications and Information Exchange between systems – LAN/MAN Specific requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specification: Amendment v: Wireless Network Management", IEEE Standard 802.11v draft D5.0, March 2009
[25] IEEE, "Draft supplement to Standard for Telecommunications and Information Exchange between systems – LAN/MAN Specific requirements – Part 11: Wireless

Medium Access Control (MAC) and Physical Layer (PHY) Specification: Amendment n: Enhancements for Higher Throughput", IEEE Standard 802.11n draft D9.0, May 2009
[26] WiFi Alliance, www.wi-fi.org
[27] RFC 2460, Internet protocol, version 6 (IPv6)
[28] RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[29] RFC 3736, Stateless Dynamic Host Configuration Protocol
[30] RFC 4862, IPv6 Stateless Address Autoconfiguration
[31] RFC 4941, Privacy Extensions for Stateless Address Autoconfiguration in IPv6
[32] RFC 4861, Neighbor Discovery for IP version 6 (IPv6)
[33] RFC 4294, IPv6 Node Requirements
[34] RFC 4795, Link-Local Multicast Name Resolution (LLMNR)
[35] RFC 4443, Internet Control Message Protocol (ICMPv6) for IPv6 Specification
[36] RFC 4214, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
[37] RFC 2710, Multicast Listener Discover (MLD) for IPv6
[38] RFC 3810, Multicast Listener Discover version 2 (MLDv2) for IPv6
[39] RFC 2617, HTTP Authentication: Basic and Digest Access Authentication; Multiple Authors; June 1999; http://tools.ietf.org/html/rfc2988
[40] RFC 3261, SIP: Session Initiation Protocol; Many Authors; June 2002; http://tools.ietf.org/html/rfc3261
[41] RFC 4380, Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)
[42] M. Jimeno, K. Christensen, and B. Nordman, "A Network Connection Proxy to Enable Hosts to Sleep and Save Energy," *Proceedings of the IEEE International Performance Computing and*
Communications Conference, pp. 101-110, December 2008. http://www.csee.usf.edu/~christen/energy/ipccc08.pdf
[43] RFC 1156, Management Information Base for Network Management of TCP/IP-based Internets
[44] RFC 1157, A Simple Network Management Protocol (SNMP)
[45] RFC 1141, Introduction to version 2 of the Internet-standard Network Management Framework
[46] RFC 1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II
[47] RFC 3410 (Informational), Introduction and Applicability Statements for Internet Standard
Management Framework
[48] 3411 (Standard 62), An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
[49] RFC 3412 (Standard 62), Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
[50] RFC 3413 ((Standard 62), Simple Network Management Protocol (SNMP) Application
[51] RFC 3414 (Standard 62), User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
[52] RFC 3415 (Standard 62), View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
[53] RFC 3416 (Standard 62), Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
[54] RFC 3417 (Standard 62), Transport Mappings for the Simple Network Management Protocol (SNMP)

[55] RFC 3418 (Standard 62), Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
[56] RFC 3584 (Best Current Practice), Coexistence between version 1, version 2, and version 3 of the Internet-standard Network Management Framework
[57] UPnP™ Standards http://upnp.org/sdcps-and-certification/standards
[58] Internet Gateway Device CPS http://upnp.org/sdcps-and-certification/standards/sdcps
[59] DLNA http://www.dlna.org/home
[60] HTTP 1.1 http://www.w3.org/Protocols/rfc2616/rfc2616.html
[61] UDP http://www.faqs.org/rfcs/rfc768.html
[62] TCP http://www.faqs.org/rfcs/rfc793.html
[63] Magic Packet Technology, AMD White Paper
[64] [RFC4795] Aboba, B., Thaler, D. and L. Esibov, "Link-Local Multicast Name Resolution (LLMNR)",RFC 4795, January 2007.