استاندارد ملی ایران

۱۷۶۰۶-۴

چاپ اول

۱۳۹۱

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization

INSO

17606-4

1st. Edition

2014

فن‌آوری اطلاعات – پروتکل کنترل شبکه
قسمت ۴: ارتباط IP

Information technology - Control network protocol - Part 4: IP communication

ICS: 35.200, 35.240.99

به‌نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و 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.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود . پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب ، به عنوان استاندارد ملی ایران چاپ و منتشر می شود . بدین ترتیب ، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

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

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون ، برای حمایت از مصرف کنندگان ، 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. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور ، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید . همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره ، آموزش ، بازرسی ، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی ، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم ، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند . ترویج دستگاه بین المللی 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 of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد
" فن‌آوری اطلاعات – پروتکل کنترل شبکه
قسمت ۴: ارتباط IP "

رئیس :	**سمت و/ یا نمایندگی**
بدلی افشرد، بابک (فوق لیسانس مهندسی کامپیوتر)	اداره کل استاندارد آذربایجان‌شرقی
دبیر :	
خاکپور، علی (لیسانس مهندسی کامپیوتر)	شرکت ایران دیتا
اعضاء : (اسامی به ترتیب حروف الفبا)	
بدلی افشرد، محمدرضا (فوق لیسانس مهندسی برق)	نیروگاه حرارتی تبریز
جباری خامنه، حسین (دکتری آمار)	دانشگاه سراسری تبریز
خوشقدم، سهیلا لیسانس مهندسی کامپیوتر	ریزفناوران آرکا پژوه
رحمانی، نعیم (فوق لیسانس مهندسی کامپیوتر)	
عظیمی حسینی، سارا (لیسانس مهندسی کامپیوتر)	ریزفناوران آرکا پژوه
علیوند، فاطمه (لیسانس مهندسی کامپیوتر)	ریزفناوران آرکا پژوه

فهرست مندرجات

پیش‌گفتار

استاندارد " فن‌آوری اطلاعات – پروتکل کنترل شبکه قسمت ۴: ارتباط IP " که پیش‌نویس آن در کمیسیون‌های مربوط توسط شرکت ریزفناوران آرکا پژوه تهیه و تدوین شده و در دویست و هفتاد و هفتمین اجلاس کمیته ملی استاندارد رایانه تاریخ ۹۱/۱۲/۰۵ مورد تصویب قرارگرفته‌است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوّب بهمن‌ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحوّلات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استاندارد های ملی ایران در موقع لزوم تجدید نظر خواهد شد و هرگونه پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه‌شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

منبع و مأخذی که برای تهیهٔ این استاندارد مورد استفاده قرارگرفته به شرح زیر است :

ISO/IEC 14908-4: 2012, Information technology– Control network protocol - Part 4: IP communication.

فن‌آوری اطلاعات پروتکل کنترل شبکه- قسمت ۴: ارتباط IP

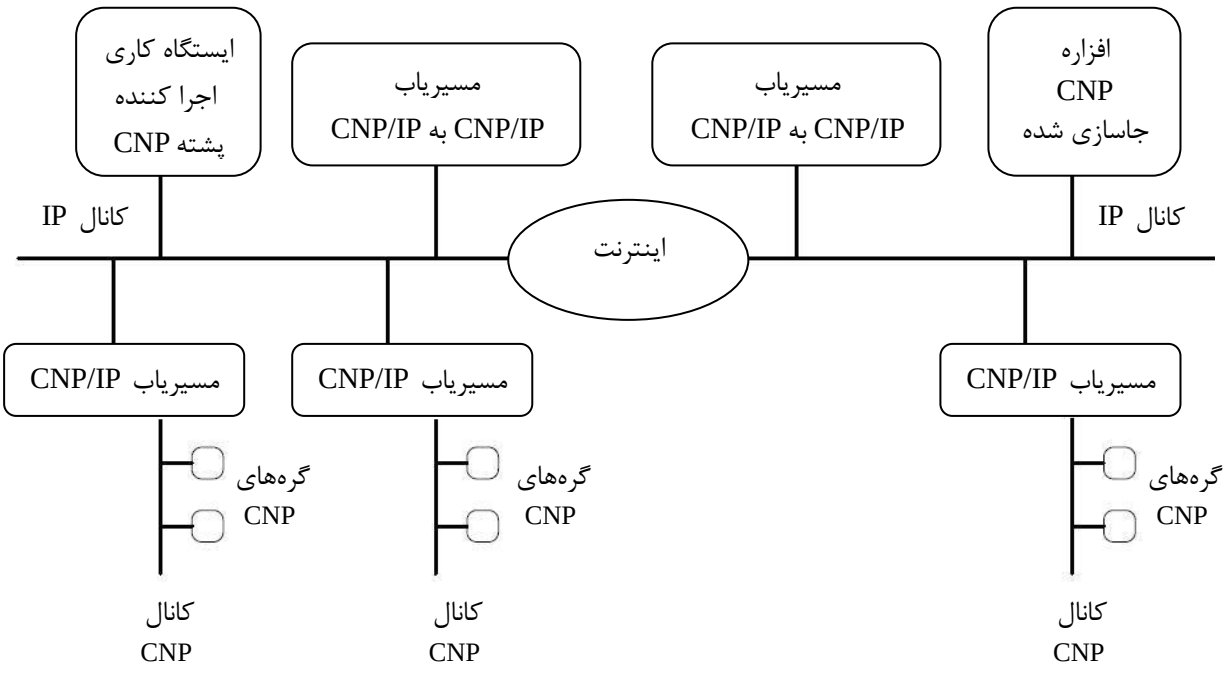
۱ هدف و دامنه کاربرد

هدف از این استاندارد ملی تضمین قابلیت تعامل مابین افزاره[1]های CNPای[2] است که تمایل دارند از شبکه‌های IP برای برقراری انتقال اطلاعات توسط پروتکل CNP استفاده کنند.

این استاندارد انتقال بسته‌های پروتکل کنترل شبکه (CNP) به مقصد شبکه‌های کنترل محلی تجاری را از طریق شبکه‌های پروتکل اینترنت (IP)[3] و با استفاده از مکانیزم تونل‌زنی تعیین می‌کند که در آن بسته‌های CNP در درون بسته‌های IP محصور می‌شوند. این فرآیند به گره‌های CNP و نیز به مسیریاب‌های CNP اعمال می‌شود.

تنه اصلی این استاندارد مستقل از پروتکل CNPای است که روی شبکه IP انتقال می‌یابد. کاربر برای جنبه‌های الزامی و اطلاعاتی این مشخصه که منحصر به این سری از استاندارد قسمت ۱ می‌باشند باید به ترتیب به پیوست الف و پیوست ب مراجعه کند.

شکل ۱ پیکربندی احتمالی افزاره‌ها و شبکه‌های CNP متصل به یک شبکه IP را نشان می‌دهد.



شکل ۱- نمونه کاربرد CNP/IP

شکل یک دو نوع افزاره CNP را نشان می‌دهد: گره‌های CNP و مسیریاب‌های CNP. باید توجه داشت که مسیریاب‌های نشان داده شده، می‌توانند بسته‌ها را مابین کانال‌های CNP خاص (مانند جفت به‌هم تابیده[4] یا خط جریان برق[5]) و کانال IP مسیریابی کنند یا می‌تواند بسته‌های CNP را مابین دو کانال IP مسیریابی

1- Device
2- Control Network Protocol
3- Internet Protocol
4- Twisted pair
5- Power line

کنند. در این استاندارد، کانال IP با چنین روشی تعیین خواهد شد تا بتواند مانند هر کانال CNP دیگری استفاده شود.

در شکل بالا می‌توان شبکه IP را یک یا چند کانال IP در نظر گرفت. این استاندارد، تنها این مورد که چگونه بسته‌های CNP روی کانال‌های IP، انتقال می‌یابند را پوشش می‌دهد. این استاندارد چگونگی مسیریابی بسته‌های CNP مابین کانال‌های CNP و کانال‌های IP استاندارد را پوشش نمی‌شود. این مشخصه برای پوشش لایه‌های پایین‌تر (لایه‌های فیزیکی، MAC و پیوند) از کانال‌های CNP یا IP استاندارد در نظر گرفته نشده است.

۲ مراجع الزامی

در این استاندارد مرجع الزامی وجود ندارد.

۳ تعاریف و اصطلاحات و اختصارات

در این استاندارد، تعاریف و اصطلاحات و اختصارات زیر به‌کار می‌رود.

۳-۱ تعاریف و اصطلاحات

۳-۱-۱

تونل‌زنی[1]

محصور سازی[2] یک بسته پروتکل در داخل بار[3] بسته‌های پروتکل دیگر است.

۳-۱-۲

کانال[4]

مکانیزم انتقال ارتباطات متداول که مجموعه‌ای خاصی از افزاره‌های CNP را به اشتراک می‌گذارد و بدون استفاده از یک مسیریاب اطلاعات را منتقل می‌کند.

یادآوری۱- کانال‌ها برای انتقال بسته‌های CNP که بخش پایین لایه پیوند پشته پروتکل CNP قرار دارند، استفاده می‌شوند.

یادآوری۲- معمولاً، به برخی از انواع رسانه فیزیکی مانند خط جریان برق، RF، جفت به‌هم تابیده اشاره دارد، اما در مورد شبکه‌های IP، این کانال فیزیکی نیست بلکه یک تونل پروتکل می‌باشد.

۳-۱-۳

افزاره CNP

افزاره‌ای که از پروتکل CNP برای برقراری ارتباط با دیگر افزاره‌های CNP استفاده می‌کند.

یادآوری- به‌طور خاص یک افزاره CNP/IP، افزاره CNPای است که با دیگر افزاره‌های CNP روی یک کانال IP، ارتباط برقرار می‌کند.

1- Tunneling
2- Encapsulaiton
3- Payload
4- Channel

۴-۱-۳

مسیریاب CNP

نوع خاصی از افزاره CNP است که مسیر بسته‌های پروتکل CNP را مابین دو یا چند کانال، مسیریابی می‌کند.

یادآوری- به طور خاص یک مسیریاب CNP/IP، مسیریاب CNPای است که در آن حداقل یکی از کانال‌هایی که این مسیریاب بر روی آن بسته‌ها را مسیریابی می‌کند، یک کانال IP است.

۵-۱-۳

گره[1] CNP

نوع خاصی از افزاره CNPای است که می‌تواند بسته‌های پروتکل CNP را ارسال یا دریافت کند. اما نمی‌تواند این بسته‌ها را مابین کانال‌ها، مسیریابی کند.

یادآوری۱- به‌طور خاص یک گره CNP/IP، گره CNPای است که در آن حداقل یکی از کانال‌هایی که آن بسته‌ها را روی آن‌ها ارسال و یا دریافت می‌کند، کانال IP است.

یادآوری۲- تمامی افزاره‌های CNP، یا مسیریاب یا گره و یا هر دو هستند.

۶-۱-۳

گروه CNP

مجموعه افزاره‌های CNPای است که یک آدرس چند پخشی عمومی را به اشتراک می‌گذارند.

۷-۱-۳

شناسه گره[2]

آدرس شبکه منطقی که گره‌های داخل زیرشبکه یا دامنه مشترکی را متمایز می‌کند.

۸-۱-۳

باید صفر باشد (MBZ)

فیلد رزرو شده‌ای که ممکن است در نسخه‌های دیگر پروتکل، استفاده شود.

یادآوری- در پیاده سازی مطابق با نسخه جاری مشخصه، مقدار چنین فیلدهایی باید صفر ارسال شود و توسط گیرنده نادیده گرفته شود.

۳-۲ اختصارات

CTP	Channel Timeout Period	دوره اتمام زمان درکانال
CNP	Control Network Protocol	پروتکل کنترل شبکه
LFS	Last Forwarded Sequence	آخرین ترتیب ارسال شده

1- Node
2- Node ID

MBZ	Must Be Zero	باید صفر باشد
NTP	Network Time Protocol	پروتکل زمان شبکه
PSN	Packet Sequence Number	شماره ترتیب بسته
SA/DA	Source Address / Destination Address	آدرس مقصد/آدرس مبدا
SID	Session Identifier	شناسه جلسه
SNTP	Simple Network Time Protocol	پروتکل زمانی شبکه ساده
UDP	User Datagram Protocol	پروتکل نمودار داده‌ای کاربر

۴ الزامات

موارد زیر مجموعه‌ای از الزامات عمومی برای انتقال بسته‌های CNP روی کانال‌های IP هستند:

الف- به اندازه ممکن کارا باشند تا عمل بلادرنگ را اجازه دهد؛

ب- مستقل از واسط سطح کاربرد استفاده شده برای دریافت بسته‌ها باشند. به‌عنوان مثال پروتکل تونل زنی نباید وابسته به وجود یک واسط سوکت یا چگونگی استفاده از واسط باشد؛

پ- حفظ ترتیب بسته CNP تضمین کنند؛

ت- تضمین کنند که بسته‌های CNPای که منقضی شده‌اند (خارج از ویژگی حداکثر مهلت کانال IP می‌باشد) ارسال نشوند.

ث- بسته‌هایی که در شبکه IP تکثیر می‌شوند را تشخیص دهند؛

ج- افزاره‌های مسیریابی IPای که بسته‌های IP را اولویت بندی می‌کنند، پشتیبانی کنند؛

چ- اقدامات امنیت اختیاری برای جلوگیری از دستکاری افزاره‌ها که توسط کاربران بدخواه صورت می‌گیرد.

ح- مقیاس پذیر باشند؛

خ- اجازه استخراج اطلاعات وضعیت از افزاره‌های CNP/IP داده شوند؛

د- مبادله اطلاعات پیکربندی مابین افزاره‌های CNP/IP و سرویس دهندگان پیکربندی را پشتیبانی کند.

۵ مشخصه افزاره CNP/IP

۵-۱ مشخصات مربوط به افزاره IP

یک افزاره CNP/IP باید مانند هر میزبان IP استانداردی عمل کند که قادر است بسته‌های IP با هر میزبان IP دیگری در زیرشبکه IP یکسان یا هر مکان دیگری در توده اینترنت مبادله کند. یک افزاره CNP/IP باید یک آدرس IP تک پخشی واحد داشته باشد و می‌تواند متعلق به حداکثر ۳۲ گروه چند پخشی باشد. پشتیبانی افزاره CNP/IP از چندپخشی، اختیاری است. این سند، مسیریابی بسته‌های IP مابین زیرشبکه‌ها یا به واسطه اینترنت را مدنظر قرار نمی‌دهد. افزاره‌های CNP/IP باید با هر آن‌چه که مکانیزم‌های استاندارد (مسیریاب‌های IP، سوئیچ‌ها و غیره) برای اجرای عملکرد مسیریابی IP نیاز دارند، سازگار باشند.

۵-۲ مشخصات مربوط به افزاره CNP

۵-۲-۱ قالب‌های بسته

قالب کلی بسته‌های CNPای که روی کانال IP بر روی آن‌ها فرایند تونل‌زنی انجام می‌شود، بسته‌هایی هستند که به لایه پیوند (لایه ۲) پشته پروتکل CNP، ارسال یا از آن دریافت می‌شوند.

برای مشخصه دقیق قالب‌های بسته مربوط به پروتکل CNP به پیوست الف رجوع شود.

۵-۲-۲ طرح‌های آدرس دهی

پروتکل‌های CNP متفاوت، برای مبادله بسته‌ها، معمولاً از طرح‌های آدرس دهی مختلفی استفاده می‌کنند. با وجود این‌که آگاهی از محتوای یک بسته CNP یا آدرس‌های آن به‌منظور تونل زنی بسته‌های CNP روی IP، ضروری نیست، برخی از جنبه‌های طرح آدرس دهی CNP در فرایند پیکربندی نمایان می‌شوند. این امر به‌خصوص زمانی درست است که پروتکل‌های CNP، کانال‌های IPای که برای تونل زنی استفاده می‌شوند را راه اندازی می‌کند. از آن‌جایی که پروتکل‌های CNP، طرح‌های آدرس‌دهی متفاوتی را به کار می‌برند، اصطلاحات مورد استفاده در تنه اصلی این مشخصه برای توصیف آدرس‌ها، به‌منظور توصیف مجموعه بزرگی از طرح‌های آدرس‌دهی به کار رفته در تمامی پروتکل‌های CNP، کلی و به اندازه کافی غنی هستند. در این مشخصه، اصطلاحات آدرس‌دهی زیر استفاده می‌شوند:

الف- شناسه منحصربه‌فرد[1]: این اصطلاح به شناسه‌ای اشاره دارد که به‌طور سراسری، در تمامی افزاره‌های درون یک پروتکل خاص، منحصربه‌فرد است. شناسه‌های منحصر به‌فرد معمولاً ماهیتی باثبات دارند، به‌طوری‌که هرگز در طول عمر یک افزاره تغییر نمی‌کنند.

ب- دامنه[2]: دامنه، بالاترین سطح از سه سطح طرح آدرس‌دهی سلسله مراتبی است. شناسه‌های دامنه باید در یک شبکه خاص منحصربه‌فرد باشد. بدین معنی که در شبکه ویژه‌ای که دامنه‌ها استفاده می‌شود، اگر دو افزاره، شناسه دامنه یکسانی داشته باشند، آن‌ها متعلق به دامنه مشابهی هستند. شناسه‌های دامنه معمولاً ماهیتی منطقی دارند و می‌توان آنها را تغییر داد و پیکربندی کرد.

پ- زیرشبکه[3]: زیرشبکه، سطح میانی از سه سطح طرح آدرس سلسله مراتبی است. شناسه‌های زیر شبکه باید در یک دامنه خاص، منحصر به‌فرد باشند. بدین معنی که در شبکه خاصی که شناسه‌های زیر شبکه استفاده می‌شوند، اگر دو افزاره، شناسه دامنه و شناسه زیرشبکه مشابهی داشته باشند، در آن‌صورت آن‌ها متعلق به زیرشبکه‌های یکسانی هستند. برخی از CNPها از دامنه‌ها استفاده نمی‌کنند که در این صورت، زیرشبکه می‌تواند بالاترین سطح آدرس برای یک افزاره باشد. شناسه‌های زیرشبکه معمولاً ماهیتی منطقی دارند و می‌توان آنها را تغییر داد و پیکربندی کرد.

ت-گره: گره، پایین‌ترین سطح از هر طرح آدرس دهی سلسله مراتبی است. در یک زیرشبکه خاص، شناسه‌های گره باید منحصربه‌فرد باشند. دو افزاره داخل زیرشبکه یکسان، نباید شناسه گره مشابهی داشته باشند. شناسه‌های گره، معمولاً ماهیتی منطقی دارند و می‌توان آنها را تغییر داد و پیکربندی کرد.

1- Unique ID
2- Domain
3- Subnet

ث- گروه: گروه‌ها یک طرح آدرس‌دهی متعامد به سلسله مراتب سه‌گانه دامنه/زیر شبکه/ گره هستند که پیشتر توصیف شد. گروه‌ها بدین منظور مورد استفاده قرار می‌گیرند که به پیام‌ها، امکان چندپخشی شدن دهند. برخی از CNPها ممکن است آدرس‌های گروه را پشتیبانی نکنند و حتی آن دسته از CNPهایی که پشتیبانی می‌کنند، قوانین متفاوتی برای چگونگی رابطه با طرح‌های آدرس‌دهی دیگر خواهند داشت. این ملاحظات مربوط به این مشخصه نمی‌باشد.

تعاریف بالا نسبتاً کلّی هستند و به‌عنوان راهنمایی برای چگونگی تطبیق پروتکل CNP با این اصطلاحات ارائه می‌شوند. به‌طور کلی، این‌که طرح‌های آدرس‌دهی متنوع چگونه در پروتکل CNP عمل می‌کنند، مربوط به این مشخصه نمی‌باشد. تنها لازم است بدانیم که اصطلاحات آدرس‌دهی مختلف، به چه چیزی اشاره دارند. توجه ویژه به این است که چگونه این آدرس‌ها برای مسیریابی در داخل پروتکل CNP استفاده می‌شوند.

۶ کانال IP

۶-۱ مشخصه

کانال‌های IP نظیر کانال‌های CNP متعارفی که در حال حاضر وجود دارند، نیستند. کانال‌های CNP متعارف، ذاتاً گذرگاه‌هایی فیزیکی هستند، یعنی که تمامی افزاره‌ها روی کانال، به‌طور پیش‌فرض همه بسته‌های انتقال یافته روی آن کانال را دریافت می‌کنند. علاوه بر این، زمانی‌که افزاره جدیدی به کانال اضافه می‌شود، لزومی ندارد که افزاره‌های دیگر روی کانال قبل از این‌که بتوانند بسته‌ها را مبادله کنند، از آن باخبر شوند. برای انتقال یک بسته روی کانال، تنها لازم است که افزاره قادر باشد به‌صورت فیزیکی بسته را انتقال دهد. اگر یک افزاره به سادگی و به‌صورت فیزیکی به یک کانال متصل شود، قادر به مبادله بسته‌ها با افزاره‌های دیگر روی کانال است.

در مقابل، یک کانال IP فیزیکی نیست، بلکه ذاتاً منطقی است. رسانه‌های فیزیکی مختلفی وجود دارند که می‌توانند ارتباطات IP را پشتیبانی کنند و هر کدام از آن‌ها باید قادر به پشتیبانی یک کانال CNP باشند. با توجه به این‌که با یک کانال منطقی سر و کار داریم، لازم است که با آگاه کردن هر افزاره روی کانال دربارهٔ وجود افزاره‌های دیگر روی آن کانال، کانال را ایجاد کنیم. به‌عبارت دیگر قبل از این‌که یک افزاره بتواند بسته‌ای را به افزاره‌های دیگر روی یک کانال IP ارسال کند، باید از این‌که چگونه به ویژه بسته به آن افزاره ارسال می‌شود (به‌عبارت دیگر از آدرس IP آن) آگاه شود.

تفاوت مهم دیگر مابین کانال‌های فیزیکی و منطقی آن است که در مورد کانال‌های فیزیکی متعارف، می‌توان به محض انتقال یک بسته بر روی کانال، مدت زمان حد بالای ثابت به هنگام حرکت یک بسته از افزاره‌ای به افزاره دیگر را محاسبه کرد. انحراف زمان‌های تحویل پیام مابین افزاره‌های CNP روی یک کانال IP، بیشتر از مقادیر تجربه شده با کانال‌های CNP است.

همان‌طور که در شکل ۱ مشاهده می‌کنید، کانال IP به عنوان یک مکانیزم انتقال رابط برای بسته‌های CNP توسط افزاره‌های CNP/IP مختلف به‌کار می‌رود. زمانی‌که یک بسته CNP روی کانال IP انتقال می‌یابد، یک بسته IP محصورکننده بسته‌های CNP به دیگر افزاره‌های CNP/IP روی آن کانال IP ارسال می‌شود. با

دریافت یکی از پیام‌های IP توسط یک افزاره CNP/IP، بسته‌های CNP استخراج و پردازش می‌شوند. یک پیام IP واحد می‌تواند شامل بیش از یک بسته CNP باشد. بنابراین در چنین روشی، بسته‌های IP باید قالب‌بندی شوند تا امکان استخراج بسته‌های CNP واحد را مهیا سازند. این فرایند به "دسته‌بندی" بسته اشاره دارد. افزاره‌های CNP/IP باید دریافت بسته‌های دسته‌بندی شده را پشتیبانی کنند. به‌علاوه دسته‌بندی بسته باید طوری انجام شود که هر بسته CNP موجود در یک پیام IP دسته‌بندی شده کامل باشد، به‌عبارت دیگر بسته‌های CNP نباید در نتیجه دسته‌بندی از مرزهای پیام IP عدول کنند. همچنین لازم است که افزاره‌های IP میانی بتوانند بسته‌های CNP دسته‌بندی شده را از حالت دسته‌بندی خارج سازند و آن‌ها را قبل از ارسال، به طور متفاوتی دسته‌بندی کنند.

مشخصه کانال IP، فهرستی از آدرس‌های IP تک‌پخشی[1] است که هر یک از این آدرس‌ها، منحصراً به یک افزاره CNP/IP اختصاص دارد. هیچ حدّی برای تعداد افزاره‌های CNP/IP موجود بر روی یک کانال IP واحد وجود ندارد.

برای میسر ساختن تونل‌زنی بسته‌های CNP، کافی است که هر افزاره CNP/IP روی کانال IP شامل فهرستی از آدرس‌های IP تک‌پخشی برای هر افزاره CNP/IP دیگر روی آن کانال باشد. در ناشیانه‌ترین حالت، برای هر بسته CNPای که روی کانال IP ارسال می‌شود، می‌توان یک پیام IP تک پخشی جداگانه به هر افزاره CNP/IP روی کانال ارسال کرد. این روش خیلی خوبی نیست، بنابراین به‌منظور کاهش ترافیک IP، روش‌های زیر به کار می‌روند:

-گروه‌های چندپخشی[2] IP؛

- ارسال انتخابی.

گروه‌های چندپخشی IP اجازه می‌دهند تا یک پیام IP واحد به بیش از یک افزاره CNP/IP ارسال شود. بنابراین تعریف کامل یک کانال نه تنها باید شامل آدرس‌های IP تک‌پخشی همه افزاره‌های CNP/IP روی کانال باشد، بلکه باید گروه‌های چندپخشی IP که به آنها تعلق دارد را نیز در بر بگیرد. هر افزاره CNP/IP می‌تواند حداکثر متعلق به ۳۲ آدرس چندپخشی باشد.

ارسال انتخابی اشاره به بررسی محتوای بسته CNP قبل از ارسال آن دارد تا تعیین شود که آیا این بسته باید به افزاره CNP/IP خاصی فرستاده شود. به‌منظور انجام این بررسی، باید در مورد هر مقصد اطلاعات اضافی ویژه CNP کسب گردد. اگر افزاره CNP/IP یک مسیریاب باشد، در آن صورت اطلاعات مورد نیاز به‌منظور اجرای ارسال انتخابی، جدول‌های مسیریابی از مسیریاب CNP/IP می‌باشند. اگر افزاره فقط یک گره هست، در آن صورت دامنه، زیرشبکه، شناسه گره، شناسه واحد و گروه‌های CNPای که گره متعلق به آن است، باید شناخته شوند. بنابراین تمامی این اطلاعات نیز بخشی از تعریف یک کانال IP کامل تلقی می‌شوند. به‌طور خلاصه تعریف کامل یک کانال IP شامل تمامی اطلاعات شناخته‌شده‌ای است که می‌تواند مربوط به ارسال بسته‌ها به افزاره‌های CNP/IP دیگر در کانال IP باشد. موارد مذکور، همهٔ دانش مربوط به کانال IP است.

صحیح بودن شرایط زیر برای هر طرح ارسالی که توسط یک افزاره CNP/IP استفاده می‌شود، اهمیت دارد:

1- Uni Cast

2- Multi Cast

الف- بسته‌های پروتکل CNP همیشه توسط تمامی افزاره‌های CNP/IP روی کانال IPای که نیاز به دریافت بسته‌ها دارند، علیرغم این‌که آن‌ها مسیریاب یا گره باشند، دریافت می‌شوند. اگر هرگونه ابهام یا عدم قطعیت در مورد افزاره‌های CNP/IPای که باید یک بسته CNP را دریافت کنند، وجود داشته باشد در آن صورت با توجه به ملاحظات خاص پیاده‌سازی افزاره، بسته می‌تواند حذف شود یا نشود. افزاره می‌تواند بسته را به همه افزاره‌های روی کانال ارسال کند و یا صرفاً آن را حذف کرده و به هیچ افزاره‌ای ارسال نکند.

ب- یک بسته CNP خاص هرگز نباید دو بار به افزاره CNP/IP یکسان ارسال شود مگر به دلیل برخی مکانیسم‌های امتحان مجدد بالای لایه پیوند پشته پروتکل CNP. به‌دلیل طبیعت شبکه‌های IP، امکان دارد که یک افزاره CNP/IP، پیام‌های IP تکراری دریافت کند اما این هرگز نباید نتیجه پیام‌هایی که بیش از یک بار از افزاره CNP/IP دیگر ارسال می‌شوند باشد.

علاوه‌بر این در صورتی‌که گروه‌ها براساس برخی معیارها تشکیل شده باشند، ارسال انتخابی می‌تواند روی گروه‌های چندپخشی اجرا شود. برای مثال گروه چند پخشی 'A' می‌تواند شامل تمامی افزارهای متعلق به دامنه با شناسه 'W' باشد. در صورتی که یک بسته CNP روانه مقصد دامنه 'W' است، در آن صورت ارسال آن به گروه چندپخشی 'A' کافی خواهد بود. به‌منظوراجرای ارسال انتخابی روی آدرس‌های چند پخشی، لازم است بدانیم که آیا این گروه‌ها براساس برخی معیارها تشکیل شده‌اند.

با فهم این واقعیت که تعریف کامل کانال IP ممکن است برای استفاده و نگهداری، به آسانی قابل کاربرد نباشد، نیازی نیست که افزاره CNP/IP، از این تعریف برای ارسال بسته‌ها استفاده کند. ساختار داده دیگری به نام "فهرست ارسال" را می‌توان داخل هر افزاره CNP/IP نگهداری کرد. فهرست ارسال می‌تواند هم شامل آدرس‌های چندپخشی و هم شامل آدرس‌های تک‌پخشی باشد و منوط به شرایط داده شده در بالا می‌باشد. فهرست ارسال می‌تواند با ابزارهای پیکربندی شخص ثالث که برای ایجاد گروه‌های چندپخشی براساس برخی معیارها مناسب‌تر هستند، ایجاد شود و بر روی افزاره بارگذاری گردد. فهرست ارسال حداقل میزان اطلاعات لازم برای ارسال مناسب بسته‌های CNP را ارائه می‌کند و برای آسان‌سازی فرایند ارسال سازمان‌دهی می‌شود، طوری‌که افزاره CNP/IP نیاز دارد بسته‌ها را فقط به هر آدرس (چندپخشی یا تک‌پخشی) در فهرست ارسال بفرستد. برای این‌که افزاره CNP/IP اجازه داشته باشد به‌صورت کورکورانه‌ای بسته‌ها را به آدرس‌های موجود در فهرست ارسال کند، شرایط زیر باید برقرار باشد:

الف- بسته‌های پروتکل CNP باید توسط همه افزاره‌های CNP/IPای دریافت شوند که صرف نظر از مسیریاب یا گره بودنشان، نیاز به دریافت آن‌ها دارند. (مانند بالا)؛

ب- یک بسته CNP خاص هرگز دوبار به افزاره CNP یکسان، ارسال نمی‌شود. (مانند بالا)؛

پ- اگر افزاره A، یک مقصد در فهرست ارسال افزاره B باشد، در آن صورت افزاره B باید یک مقصد در فهرست ارسال افزاره A باشد. پشتیبانی از خدمت تأییدشده پروتکل CNP ضروری است.

اجرای انواع ساده ارسال انتخابی با استفاده از فهرست ارسال توسط ویژگی‌های مرتبط با مدخل‌های چندبخشی موجود در فهرست، باید امکان‌پذیر باشد.

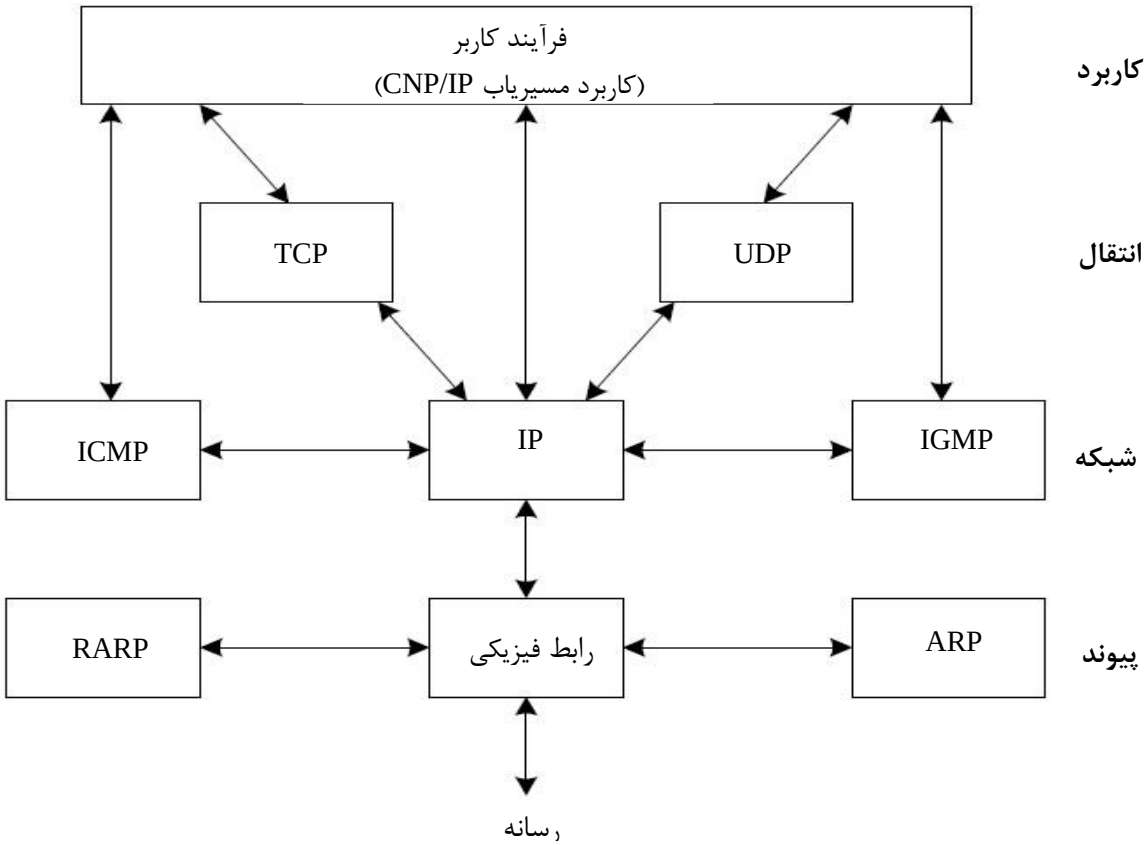
به طور کلی توجه به این امر ضروری است که وقتی فهرست ارسال احتمالاً از یک گروهبندی هوشمند افزاره‌ها مبتنی بر برخی ویژگی‌ها حاصل می‌شود،تعریف کانال IP، اطلاعات کلی و کاملی در مورد کانال IP ارائه می‌کند. هدف اصلی فهرست ارسال این است که به افزاره‌های CNP/IP اجازه دهد تا بدون نیاز به پردازش وسیع فهرست کامل تعریف کانال، فعالیت نسبتاً کارآمدی داشته باشند. همچنین توجه به این نکته اهمیت دارد که فهرست ارسال، یکی از ویژگی‌های پیکربندی افزاره CNP/IP است، بدین معنی که از طریق برخی فرآیندهای آشکار پیکربندی، کنترل و وارد یک افزاره می‌شود. با این‌که فهرست ارسال یکی از ویژگی‌های پیکربندی است، اما مانع یک افزاره CNP/IP برای پیکربندی خود و محاسبه فهرست ارسال خود نمی‌شود.

برای اعمال کنترلی دقیق بر رفتار افزاره‌های CNP/IP و چگونگی ارسال بسته‌ها توسط آن‌ها، باید پیکربندی یک افزاره CNP/IP امکان‌پذیر باشد تا از یک فهرست ارسال معین استفاده کند و هرگونه اطلاعات پیکربندی کانال IPای که ممکن است داشته باشد را نادیده بگیرد.

۶-۲ مکانیسم‌های انتقال IP

۶-۲-۱ کلیات

همان‌طور که در شکل ۲ ملاحظه می‌کنید، IP یک پروتکل سطح شبکه است که برای فعالیت کردن بر روی محدوده وسیعی از پروتکل‌های رسانه‌های فیزیکی و لایه پیوند طراحی شده است. به این ترتیب، این استاندارد هیچ چیزی در مورد لایه‌های فیزیکی و پیوند پشته IP، مشخص نمی‌کند.



شکل ۲- پشته پروتکل IP

همان‌طور که در شکل ۲ مشاهده می‌شود، سه مکانیزم متداولی که برای انتقال بسته‌های IP استفاده می‌شوند عبارتند از:

الف– raw IP؛

ب– TCP؛

پ- UDP .

TCP (به RFC 793 مراجعه شود) و UDP (به RFC 768 مراجعه شود)، پروتکل‌های انتقال بالای IP (به RFC 791 مراجعه شود) می‌باشند. با توجه به راندمان افزایشی UDP در مورد انتقال پیام‌های داده CNP و پشتیبانی آن از آدرس دهی چندپخشی، UDP باید برای برقراری ارتباط مابین افزاره‌های CNP/IP استفاده شود و تمامی افزاره‌های CNP/IP بایستی UDP را پشتیبانی کنند. TCP برخی مزایا برای استفاده در فرآیند پیکربندی دارد و می‌تواند برای انواع خاصی از پیام‌ها علاوه بر UDP، پشتیبانی شود. پشتیبانی از TCP در افزاره‌های CNP/IP، اختیاری است.

به منظور در نظر گرفتن مسئله ترتیب‌دهی، یک شماره ترتیب وجود خواهد داشت که به سرآیند بسته‌ها اضافه می‌شود تا به ترتیب دهی آن‌ها کمک کند. تمامی نمودارهای داده‌ای UDP باید مجموع‌های مقابله‌ای[1] معتبر ارسال شوند.

برای ارسال یک بسته از طریق TCP/UDP، علاوه برآدرس پورت، تعریف شماره پورت نیز ضروری است. به‌طور کلی شماره‌های پورت قابل تنظیم هستند و برای اهداف متفاوتی که در بخش‌های بعد تعریف شده‌اند، به کار می‌روند. برای سفارشات روی شماره پورت به‌منظور استفاده برای CNP، به پیوست ب مراجعه کنید.

با کاربرد UDP، نمودارهای داده‌ای می‌توانند با استفاده از آدرس‌دهی چندپخشی یا تک‌پخشی ارسال شوند. تک‌پخشی به صورت نقطه به نقطه است، یعنی یک نمودار داده از یک میزبان IP به یک میزبان IP دیگر ارسال می‌شود. زمانی‌که نمودار داده‌ای یکسانی به چندین میزبان IP ارسال می‌شود، استفاده از آدرس‌دهی چندپخشی، کارآمدتر است. در نتیجه توصیه می‌شود که افزاره‌های CNP/IP هر دو آدرس‌دهی چندپخشی و تک‌پخشی را پشتیبانی کنند. یادآور می‌شویم که یک کانال IP را فهرستی از آدرس‌های IP تعریف می‌کند. تعریف کانال یا فهرست ارسال می‌تواند شامل هر ترکیبی از آدرس‌های تک‌پخشی و چندپخشی باشد. نیازی نیست که یک افزاره CNP/IP، چندپخشی را پشتیبانی کند تا با افزاره CNP/IP که آن را پشتیبانی می‌کند، تعامل برقرار سازد.

برای این‌که یک مسیریاب CNP/IP، از آدرس‌دهی چندپخشی در میان مسیریاب‌های IP استفاده کند، لازم است که افزاره CNP/IP به مسیریاب IP اطلاع دهد که قصد دارد به گروه چندپخشی بپیوندد. روش‌های تثبیت‌شده‌ای برای انجام این کار وجود دارند که چگونگی انجام آن‌ها خارج از بحث این استاندارد می‌باشد. خواننده باید به RFC 1112 مراجعه کند.

1- Checksum

۶-۲-۲ ملاحظات اطلاعاتی

برخی از شبکه‌های IP شامل مسیریاب‌هایNAT هستند. این مسیریاب‌ها نمی‌توانند پروتکل‌هایی را که در بارشان، آدرس IP جاسازی شده دارند اداره کنند، مگر این‌که به‌طور خاص برای این منظور طراحی شده باشند. این موضوع در مورد پروتکل تونل‌زنی مشخص شده در این استاندارد صدق می‌کند.

به‌طور کلی این پروتکل در میان مسیریاب‌های NAT، کار نخواهد کرد. پروتکل می‌تواند در شبکه‌ای که از مسیریاب‌های NAT استفاده می‌کند به کار رود، البتّه تا زمانی‌که مسیریابی وجود داشته باشد که قادر به اداره این پروتکل باشد. آن مسیریاب می‌تواند یا خودش یک مسیریاب NAT باشد یا مسیریاب CNP/IP به CNP/IP دیگری باشد که در همان ناحیه از شبکه به‌عنوان مسیریاب NAT می‌نشیند.

۷ افزاره CNP/IP

۷-۱ پیکربندی افزاره CNP/IP

افزاره CNP/IP رفتاری دو گانه دارد. از منظر CNP، این افزاره یک گره CNP روی یک کانال CNP است و دارای تمامی ویژگی‌ها است. این پارامترها می‌توانند با استفاده از رویه‌های استاندارد مدیریت شبکه CNP و پیام‌ها، تنظیم و مدیریت شوند. از نقطه دید IP، افزاره CNP/IP، یک میزبان IP روی شبکه IP است و بنابراین باید مانند هر میزبان دیگر روی شبکه IP، پیکربندی شود.

علاوه بر این، اطلاعات پیکربندی‌ای وجود دارد که کانال IP منطقی مرتبط با آن افزاره CNP/IP را تعریف می‌کند.

این بند تنها عناصر مربوط به پیکربندی میزبان IP و پارامترهای کانال IP را شرح می‌دهد.

به‌طور کلی تمامی میزبان‌های IP و پارامترهای کانال با استفاده از تعدادی از روش‌ها و پروتکل‌ها، قابل پیکربندی خواهند بود. حداقل تمامی افزاره‌های CNP/IP باید پیکربندی دستی مکانیزم ارسال برای آن افزاره را پشتیبانی کنند تا حداقل سطح تعامل مابین افزاره‌هایی که ممکن است به روش‌های متفاوتی پیکربندی شده باشند را تضمین کنند. منظور ما از ارسال، عمل تونل‌زنی افزاره‌های دیگر روی کانال IP است که در بخش‌های قبل توصیف شد.

۷-۲ پارامترهای پیکربندی

۷-۲-۱ کلیات

این بند پارامترهایی را که یک CNP/IP برای کار کردن، استفاده می‌کند (یا ممکن است استفاده کند) را تعریف می‌کند. این بند به تعریف ساختارهای داده‌ای که برای ذخیره اطلاعات استفاده می‌شوند یا تعریف پیام‌هایی که برای مبادله آن‌ها استفاده می‌شوند، توجهی نمی‌کند. تنها هدف این بند داشتن بخش یکپارچه‌ای است که در آن، تمامی پارامترهای یک افزاره CNP/IP شناسایی و تعریف می‌شوند. این بند، مکانیزم‌هایی را برای انتقال این اطلاعات در بین افزاره‌ها مطرح می‌کند.

الف- تعریف کانال CNP/IP شرح داده شده در بند ۶؛

ب- فهرست ارسال شرح داده شده در بند ۶؛

پ- پارامترهای افزاره مربوط به وجود شیء روی یک کانال CNP/IP.

۷-۲-۲ پارامترهای تعریف کانال

تعریف کامل کانال به‌طور منطقی، فهرستی از هر افزاره CNP/IP روی کانال است. هر افزاره روی کانال می‌تواند با انواع اطلاعات زیر همراه شود:

الف- پشتیبانی چندپخشی (بله یا خیر). از آنجایی که این مورد اختیاری است، باید نشانه‌ای وجود داشته باشد مبنی بر اینکه آیا از چندپخشی پشتیبانی می‌شود؛

ب- نوع افزاره CNP/IP (مسیریاب، گره، پروکسی و غیره)؛

پ- نوع مسیریاب CNP (تکرارکننده، یادگیری، پیکربندی و غیره)؛

ت- پرچم " CNP "wants all Broadcasts

ث- نام، رشته متنی ساده استفاده شده برای شناسایی؛

ج- مهلت اتمام کانال. این پارامتر، در کانال سراسری است. هر افزاره‌ای این مقدار را دارد اما برای تمامی افزاره‌ها یکسان است.

چ- آدرس IP. این آدرس IP تک‌پخشی افزاره است.

ح- پورت تک‌پخشی برای گوش دادن به داده؛

خ- فهرستی از جفت آدرس چندپخشی/شماره پورتی که افزاره CNP/IP گوش می‌دهد؛

د- شناسه ۱ منحصر به‌فرد ویژه افزاره CNP (مسیریاب نزدیک کناره یا گره)؛

ذ- شناسه ۲ منحصربه‌فرد ویژه افزاره CNP (مسیریاب دور از کناره)؛

ر- شناسه ۳ منحصر به‌فرد ویژه افزاره CNP (کمکی برای پیکربندی)؛

ز-طول دامنه CNP و IP، زیرشبکه، آدرس گره برای هر دامنه؛

س- پارامترهایی که مخصوص گره‌ها هستند: اطلاعات عضویت گروه CNP؛

ش- پارامترهایی که مخصوص مسیریاب‌ها هستند. جدول مسیریابی CNP.

توجه کنید که این فهرست، صرفاً یک نمونه است. جزئیات کامل مورد نیاز، در بندهای بعدی این استاندارد آمده است.

پروتکل تونل‌زنی تعریف شده در این مشخصه، به هیچ طرح آدرس‌دهی خاص CNP نیاز ندارد. انواع آدرس‌های CNPای که در زیر آمده، پشتیبانی می‌شوند:

۱- شناسه منحصر به‌فرد افزاره؛

۲- شناسه دامنه؛

۳-شناسه زیر شبکه؛

۴-شناسه گره؛

۵-شناسه گروه.

برای قراردادهای آدرس‌دهی ویژه‌ای که مربوط به انواع آدرس‌های فهرست شده در بالا هستند، به پیوست الف مراجعه کنید.

۷-۳-۲ پارامترهای فهرست ارسال

پارامترهای زیر برای تعریف فهرست ارسال استفاده می‌شوند.

- فهرست آدرس‌های IP تک‌پخشی و پورت‌ها؛
- فهرست آدرس‌های IP چندپخشی و پورت‌ها.

۷-۲-۴ پارامترهای افزاره

- آدرس دروازه IP؛
- ماسک زیر شبکه IP؛
- پورت/ آدرس IP سرویس‌دهنده پیکربندی؛
- آدرس IP سرویس‌دهنده SNTP.

۷-۳ روش‌های پیکربندی

۷-۳-۱ کلیات

این بند، روش‌های مختلفی را که می‌توانند برای مقداردهی پارامترهای تعریف شده در بند قبلی به کار روند را شرح می‌دهد.

این پارامترها می‌توانند به چندین روش، مقداردهی شوند. لزومی ندارد که یک افزاره CNP/IP، تمامی این روش‌ها را پشتیبانی کند، اما در صورت پشتیبانی هر کدام از این روش‌ها، باید آن‌ها را با یک روش استاندارد پشتیبانی کند.

۷-۳-۲ پیکربندی

برای پیکربندی دستی، هیچ سرویس‌دهنده پیکربندی وجود ندارد. تمامی پارامترهای مورد نیاز تعریف کانال، پارامترهای فهرست را ارسال می‌کنند و پارامترهای افزاره باید به‌صورت دستی وارد شوند. هیچ روش استانداردی برای انجام این‌کار وجود ندارد. انجام این کار، مختص فروشنده است و آن را می‌توان توسط هر یک از روش‌های زیر انجام داد:

- فایل‌های پیکربندی؛
- واسط پایانه؛
- واسط شبکه راه دور؛
- انتقال فایل FTP؛
- واسط HTTP؛

۷-۳-۳ BOOTO و DHCP

۷-۳-۳-۱ پیش‌زمینه

افزاره‌ها برای به‌دست آوردن یک آدرس IP بدون پیکربندی قبلی، دو مکانیسم در اختیار دارند: DHCP(RFC 2131) و BOOTP(RFC 951).

DHCP در واقع شکل گسترش یافته‌ای از BOOTP است و سرویس‌دهنده‌های BOOTP که مطابق با RFC 951 هستند، می‌توانند پیام‌های ارسالی از سرویس گیرنده‌های DHCP را دریابند و به آن‌ها به‌طور صحیح پاسخ دهند.
اساساً، یک سامانه راه‌اندازی خواهد شد و از یک سرویس‌دهنده DHCP برای یک آدرس IP درخواست DHCP خواهدکرد. سرویس‌دهنده DHCP با آدرس IP معتبر استفاده دست‌نخورده‌ای پاسخ می‌دهد که سرویس گیرنده DHCP هم‌اکنون می‌تواند استفاده کند.

۷-۳-۳-۲ مطابقت

افزاره‌هایی که با این مشخصه مطابقت دارند و می‌خواهند یک آدرس IP را بدون پیکربندی قبلی به‌دست آورند، باید دست به پیاده‌سازی یک سرویس‌گیرنده DHCP بزنند و می‌توانند سرویس‌گیرنده BOOTP را پیاده‌سازی کنند.

۷-۳-۴ سرویس‌دهنده‌های پیکربندی

افزاره‌های روی یک کانال CNP/IP، بهتر است که تا حد امکان به‌صورت "استاندارد اتصال افزاره جانبی" باشند. با توجه به میزان زیاد اطلاعات پیکربندی که یک افزاره CNP/IP برای فعالیت به کار می‌برد، بهتر است مکانیسمی برای توزیع اطلاعات وجود داشته باشد تا مجبور نباشد به‌صورت جداگانه به هر افزاره‌ای وارد شود. افزاره‌ای که اجازه می‌دهد تا این مکانیسم کار کند، سرویس‌دهنده پیکربندی نام دارد.
افزاره‌هایی که از یک سرویس‌دهنده پیکربندی استفاده می‌کنند، باید با افزاره‌ای که از آن استفاده نمی‌کنند، تعامل برقرار کنند. لزومی ندارد که یک سرویس‌دهنده پیکربندی، تمامی تعاملات ارائه شده در این مشخصه را پشتیبانی کند. به‌ویژه بسته‌های مسیریابی نیازی به پشتیبانی ندارند.
یک سرویس‌دهنده پیکربندی به‌منظور پیکربندی سرویس‌گیرنده‌های CNP/IP در یک حالت خودکار، از پیام‌های IP استفاده می‌کنند. در حالت کلی یک سرویس‌دهنده پیکربندی قابلیت‌های زیر را پشتیبانی می‌کند:

الف- تنظیم پارامترهای متنوع CNP/IP گیرنده؛

ب- توزیع تعریف کانال IP و فهرست ارسال به افزاره‌های CNP/IP سرویس‌گیرنده. فهرست کانال، توصیف شبکه به‌عنوان یک کل است در صورتی‌که فهرست ارسال به‌صورت بالقوه منحصر به هر افزاره CNP/IP است.

پ- نگهداری اتوماتیک فهرست تعریف کانال توسط کشف زمانی‌که افزاره‌های CNP/IP روشن و خاموش می‌شوند.

علاوه بر پارامترهای شرح داده شده در بند ۷-۲، یک افزاره CNP/IP همچنین باید برای استفاده از یک سرویس‌دهنده پیکربندی، دارای آدرس IP یک سرویس‌دهنده پیکربندی و یک پورت برای برقراری ارتباط باشد.
افزاره‌های CNP/IP باید هنگام به کار افتادن سامانه، هنگام راه‌اندازی مجدد و هنگامی که پارامترهای فهرست تعریف کانال افزاره تغییر می‌یابند، یک پیام ثبت افزاره به سرویس‌دهنده پیکربندی ارسال کند.

این بند مشخص نمی‌کند که سرویس‌دهنده چگونه فهرست پارامترهایی را که به سرویس‌گیرنده‌ها توزیع می‌یابند مدیریت می‌کند. در واقع این پارامترها باید با استفاده از هر نوع روش مدیریتی مطلوبی، قابل نگهداری باشند. دریافته‌اند که بهتر است سرویس‌دهنده، به هنگام خاموش و روشن شدن سرویس‌گیرنده‌ها، قابلیت ایجاد و نگهداری خودکار پارامترها را داشته باشد. پروتکل و قالب‌های پیام تا حدی طراحی خواهند شد تا به سرویس‌دهنده‌ها امکان پشتیبانی از این قابلیت را بدهند.

۸ پیام‌های CNP/IP

۸-۱ تعریف پیام‌های CNP/IP و شیوه‌های عمل

هدف از این بند موارد زیر می‌باشد:

- شناسایی تمامی پیام‌هایی که می‌توانند مابین افزاره‌های CNP/IP روی یک کانال IP مبادله شوند؛
- تعریف محتواهای پیام؛
- مشخص کردن پروتکل و جنبه‌های رفتاری افزاره‌ها زمانی‌که این پیام‌ها را مبادله می‌کنند؛

بند ۹ قالب‌های دقیق بسته را برای پیام‌های تعریف شده در این بند مشخص می‌کند.

یک افزاره CNP/IP از کانال IP برای تنوع اهداف و شیوه‌های عمل استفاده می‌کند. بند جداگانه‌ای در این استاندارد هر یک از موارد را پوشش خواهد داد. شیوه‌های عمل شامل موارد زیر است:

الف- مبادله (تونل‌زنی) بسته‌های داده CNP؛

ب- مبادله اطلاعات پیکربندی با سرویس‌دهنده‌های پیکربندی؛

پ- پیام‌های وضعیت متفرقه؛

ت- پیام‌های ویژه فروشنده و پروتکل‌ها؛

برای هر یک از این شیوه‌های عمل، پیام‌هایی که مابین افزاره‌های CNP/IP مبادله می‌شوند، تعریف خواهند شد.

۸-۲ سرآیند عمومی پیام

هر پیام IP مبادله‌شده توسط افزاره‌های روی کانال IP، دارای یک سرآیند ثابت با قالبی که در همه پیام‌های CNP/IP مشترک است می‌باشد. این سرآیند شامل فیلدهای زیر هست:

- نسخه[1]؛
- پرچم‌های پروتکل؛
- کد فروشنده؛
- نوع بسته؛
- طول بسته داده؛
-اندازه سرآیند؛
- شناسه جلسه؛

1- Version

- ترتیب#؛
- نشان زمانی؛
- کلید امنیت.

قالب‌های خاص پیام، در بند ۹ پوشش داده شده است.

فرض می‌شود که تمامی بسته‌های دارای شماره نسخه یکسان، همیشه می‌توانند تجزیه شوند. اگر بسته‌ای با شماره نسخه نامشخص دریافت شود، این بسته باید بدون پردازش بیشتر حذف شود.

پرچم‌های پروتکل، اطلاعاتی را در مورد بسته مشخص می‌کنند مثلاً این‌که کدام بسته پروتکل CNP داخل پیام محصور می‌شود و آیا این پیام به صورت امن ارسال می‌شود.

کد فروشنده بسته‌های مختص فروشنده را امکان‌پذیر می‌سازد. طبق این مشخصه، این مقدار باید برای تمامی بسته‌های تعریف استاندارد، بر روی صفر تنظیم شود. بسته‌های مختص فروشنده تا حدودی توسط یک رمز منحصر به‌فرد فروشنده (غیر از صفر) شناسایی می‌شوند.

یک رمز منحصر به‌فرد نوع بسته، به هر تابعی اختصاص داده می‌شود که در بند ۹-۱ به‌صورت دقیق شرح داده شده است. رمزهای استاندارد نوع بسته که در این مشخصه تعریف شده‌اند، در بازه 0x00 تا 0x7F هستند. بسته‌های فروشنده خاصی که اطلاعات را مانند تابع استاندارد تعریف شده در این مشخصه ارسال می‌کنند، می‌توانند از رمز نوع بسته یکسان با تابع استاندارد استفاده کنند، اما رمز فروشنده باید یک شناسه منحصر به‌فرد برای آن فروشنده باشد. بسته‌های فروشنده خاصی که رابطه‌ای با توابع استاندارد موجود تعریف شده در این مشخصه ندارند، باید از رمز نوع بسته در بازه 0x80 تا 0xFF استفاده کنند.

طول بسته داده و اندازه سرآیند به ترتیب، اندازه بسته و اندازه سرآیند را مشخص می‌کند. شناسه جلسه همراه با شماره ترتیب کار می‌کند تا وقوع شماره‌های ترتیب تکراری را به حداقل برساند.

نشان زمانی برای تشخیص بسته‌های داده‌های منقضی استفاده می‌شود و مبتنی بر مرجع زمان است که مابین تمامی افزاره‌ها در کانال CNP/IP (تعریف‌شده در بند ۸-۴-۴) همگام می‌شود. همان‌طور که در بند ۸-۸ شرح داده شده، کلید امنیت برای امنیت بسته‌ها به کار می‌رود. تمامی بسته‌های CNP/IP می‌توانند با استفاده از نمودار داده‌های UDP ارسال شوند. هر نمودار داده UDP می‌تواند شامل یک یا چند پیام CNP/IP باشد. اگر بیش از یک پیام CNP/IP داخل یک نمودار داده UDP واحد (دسته بندی شده) وجود داشته باشد، در آن صورت هر پیام سرآیند خود را خواهد داشت. چون هر سرآیند دارای اطلاعات اندازه پیام است، امکان استخراج هر پیام به‌صورت جداگانه وجود دارد.

همه افزاره‌های CNP/IP باید از دسته‌بندی بسته‌ها پشتیبانی کنند. شکل ۳ بیش از یک پیام CNP/IP را داخل یک نمودار داده UDP واحد نشان می‌دهد (دسته‌بندی کردن بسته)

سرآیند عمومی بسته پیام 1-n	بخش داده پیام 1-n	سرآیند عمومی بسته پیام n	بخش داده پیام n

شکل۳-دسته‌بندی بسته

برخی از پیام‌های CNP/IP می‌توانند از مرز یک نمودار داده UDP عبور کنند. در چنین مواردی یک پروتکل قطعه‌بندی خاص تعریف می‌شود که می‌توان برای تسهیل این کار مورد استفاده قرار داد. پیام‌هایی که از مرز

یک نمودار داده UDP عبور می‌کنند و طرح قطعه‌بندی را به کار می‌برند، نیازی ندارند که با بسته‌های دیگر دسته‌بندی شوند.

۸-۳ قطعه‌بندی بسته

۸-۳-۱ بررسی

پاسخ‌ها به درخواست‌های پیکربندی برای ساختارهای داده‌ای CNP/IP، به علّت حداکثر ۵۴۸ بایت بار در هر بسته UDP، داده‌های بیشتری بیش از آن چه که بتوان در یک بسته UDP واحد حمل کرد دارند. این بند یک روش عمومی را توصیف می‌کند که از طریق آن، ساختارهای داده می‌توانند انتقال یابند. توجه داشته باشید که این روش به طور ذاتی از تحریف داده‌ها، در جاهایی که بخش‌های ساختار داده‌ای کل بین انتقال بخش‌های واحد تغییر می‌کنند جلوگیری نمی‌کند. در تمامی تعریف‌های بسته پاسخ پیکربندی در این پروتکل، یا الف) قالب بسته پاسخ به طور خاص برای حذف حساسیت به داده تحریف‌شده سازگار می‌شود، یا ب) روش ساده‌تری ارائه می‌شود که از طریق آن، تحریف داده‌های بالقوه را می‌توان تشخیص داد.

این پروتکل شامل نوع بسته قطعه می‌باشد. هر نوع بسته پیکربندی دیگری می‌تواند همانند بار در مجموعه‌ای از بسته‌های قطعه حمل شود. دنباله بایت‌ها از بسته بار انتخاب می‌شوند، طوری‌که بسته قطعه حاصل در یک قاب UDP جا خواهد شد و این قطعه‌ها به‌عنوان پاسخ ارائه می‌شوند. اگر بسته درخواست شده در یک قاب UDP جا شود، در آن صورت بدون محصور کردن ارسال می‌گردد. بسته‌های ارسال شده و بسته‌های قطعه به‌صورت تمام و کمال ارسال می‌شوند. بسته بار یک سرآیند عمومی بسته با طول بسته بار دارد. تمامی بسته‌های قطعه، نوع بسته‌های یکسانی دارند.

به‌منظور تسهیل این روش، هر بسته درخواست پیکربندی که یک پاسخ پیکربندی را فراخوانی می‌کند، شامل یک فیلد شناسه قطعه است و هر بسته قطعه شامل یک بیت معتبر و یک بیت نهایی در فیلد پرچم‌ها، همچنین یک نمایشگر زمان تاریخ است.

- فیلد ***"شناسه درخواست"***به وسیله سرویس‌دهنده پاسخ، از درخواست به بسته قطعه کپی می‌شود. این فیلد نمایانگر مقدار نشانه‌داری است که توسط مبدأ این درخواست به‌کار گرفته می‌شود تا بتواند به‌طور منحصربه‌فردی، پاسخ این درخواست را مشخص کند. بنابراین چندین درخواست می‌توانند به‌طور همزمان به یک مقصد یکسان ارسال شوند. فیلد شناسه درخواست، ۱۶ بیت است تا علاوه بر یک شماره درخواست، هرگونه اطلاعات افزاره‌ای دیگر نیز بتوانند در یک روش مستقل پیاده‌سازی در این فیلد گنجانده شوند.

- ***"شناسه قطعه"***، ارجاع به یک بلوک جزئی داده در درون یک ساختار کامل داده است. ارجاع شناسه قطعه به اولین بلوک جزئی داده، 0x0 است.

- بیت ***"اعتبار"*** در یک بسته قطعه، نشان دهنده صحت داده در این بسته مربوط به شناسه قطعه ظاهری است. مقداردهی بیت اعتبار (valid set) به معنای اعتبار داده است و مقدار نداشتن بیت اعتبار (valid clear) بدین معنی است که داده معتبری برای شناسه قطعه ظاهری وجود ندارد.

- بیت ***"نهایی"*** در بسته قطعه، وجود داده اضافی در ساختار برای مقادیر شناسه قطعه بزرگتر از مقدار برگشتی در این بسته را نشان می‌دهد. مقداردهی بیت نهایی نشان می‌دهد که هیچ داده اضافی‌ای وجود ندارد.

- شاخص ***"زمان‌تاریخ"***، برای تشخیص تحریف داده اکتسابی به کار می‌رود. این فیلد نشان می‌دهد که یک ساختار داده در چه زمانی معتبر شده است. این شاخص زمانی را به منظور انتقال از داده درخواست شده است را نشان نمی‌دهد. در مورد داده‌های پیکربندی‌ای که به تحریف داده حساس هستند، تحریف داده را می‌توان از طریق مقایسه فیلد زمان تاریخ برگردانده شده در هر یک از بسته‌های پاسخ که ساختار کل داده را نشان می‌دهند، تشخیص داد. اگر فیلد تاریخ زمان در تمامی بسته‌ها یکسان نباشد، در آن صورت برخی از بخش‌های داده به‌دست آمده تحریف شده است. قالب فیلد تاریخ زمان در بند ۹-۵ مشخص شده است.

۸-۳-۲ مبادله قطعه

۸-۳-۲-۱ کلیات

روش متداولی که از طریق آن، داده پیکربندی حاصل می‌شود به‌صورت زیر است:

گام الف) گره درخواست‌کننده، یک بسته درخواست را با شناسه قطعه برابر با صفر ارسال می‌کند. آن می‌تواند به طور اختیاری پرچم REQUEST-ALL را مقداردهی کند تا نشان دهد که تمامی بسته‌های قطعه بدون منتظر شدن برای بسته‌های درخواست اضافی، ارسال می‌شوند.

گام ب) اگر پیام پاسخ در یک قاب جا شود، در آن صورت قاب ارسال می‌گردد. زمانی‌که گیرنده یک بسته از نوع درخواست‌شده دریافت می‌کند، شناسه درخواست را به کار نمی‌برد و بر روی پاسخ فعالیت می‌کند.

گام پ) اگر بسته پاسخ در یک قاب واحد جا نشود، گره پاسخ‌دهنده یک بسته قطعه ارسال می‌کند که شناسه قطعه‌ای برابر با شناسه قطعه بسته درخواست دارد. به‌علاوه اگر داده‌ای برای آن قطعه وجود نداشته باشد، بسته پاسخ با "*flags:final*" تنظیم و فرستاده می‌شود. اگر داده‌ای برای آن قطعه وجود داشته باشد، "*flags:valid* " پاک شده و مدنظر قرار می‌گیرند. علاوه بر آن، در صورتی که داده‌های بیشتری ورای شناسه قطعه ظاهری وجود داشته باشد، بخش داده بسته جاری تا گنجایش خودش پر می‌شود و *flags:final* پاک می‌شوند.

گام ت) اگر گره درخواست‌کننده، پاسخی دریافت نکند، پیام درخواست تا زمانی‌که پاسخی دریافت شود تکرار می‌شود. افزایش در نرخ نمایی[1] برای بازه تکرار، تا بازه حداکثری ۳۰ ثانیه وجود دارد.

گام ث) گره درخواست‌کننده، فیلد پرچم‌های پیام پاسخ را بررسی می‌کند. اگر *flags:valid* پاک شوند، باقیمانده بسته پاسخ نادیده گرفته می‌شود به گام ج بروید.

گام د) اگر *flags:valid* برقرار باشند، داده پردازش می‌شود. در صورتی‌که تحریف داده تشخیص داده شود، فیلد تاریخ زمان بررسی می‌شود.

گام ج) اگر *flags:final* برقرار باشند، ترتیب درخواست برای این ساختار داده خاتمه می‌یابد و ساختار به‌دست آمده به‌عنوان معتبر علامتگذاری می‌شود.

1- exponential rate

چ) اگر *flags:final* پاک شده باشند، بسته درخواست دیگری که شناسه قطعه‌ای برابر با یک واحد بزرگتر از درخواست قبلی دارد ارسال می‌شود (فرآیند با گام پ ادامه می‌یابد. اگر زمان تاریخ برای هر بسته دریافت شده متفاوت از دیگری باشد، در آن صورت فرآیند با گام الف آغاز می‌شود.

آغاز اکتساب یک ساختار داده‌ای با هر مقدار شناسه قطعه، همان‌قدر اعتبار دارد، با این حال درخواست برای قطعه صفر، معمولاً در پاسخ با داده معتبر به‌دست خواهد آمد. حتی اگر درخواست با قطعه غیرصفر شروع شود، در صورتی‌که پاسخ در یک قاب UDP واحد جا شود، از بسته قطعه استفاده نمی‌کند بلکه تنها با بسته پاسخ، پاسخ می‌دهد.

در صورتی‌که گره درخواست‌کننده، جریانی از بسته‌های قطعه با مجموعه‌ای کامل از شناسه‌های قطعه و تاریخ زمان یکسان در همه بسته‌ها را دریافت کند، آن بسته بار را گرد هم می‌آورد و آن را پردازش می‌کند. در صورتی‌که هر بخش، تاریخ زمان متفاوتی داشته باشد، کل مجموعه حذف می‌شود و پردازش دوباره از گام الف شروع می‌شود. چون پاسخ ممکن است شامل قطعه‌های دارای یک تاریخ زمان کاملاً جدید باشد، هیچ قطعه‌ای نگهداری نمی‌شود.

۸-۳-۲-۲ مقادیر شناسه درخواست

بسته‌های قطعه‌بندی شده، هرگز به طور ناخواسته‌ای توسط سرویس‌دهنده ارسال نمی‌شوند.

مقدار شناسه درخواست در بسته درخواست، از افزاره به سرویس‌دهنده ارسال می‌شود و مقدار آن کاملاً تحت کنترل افزاره درخواست‌کننده است. شناسه درخواست می‌تواند شامل هر مقداری از جمله صفر باشد و این امر در بسته‌های قطعه ارسال شده توسط سرویس‌دهنده تکرار خواهد شد. مقدار شناسه درخواست باید برای هر درخواست همزمان فعال، منحصر به‌فرد باشد. در صورتی‌که این امر صادق نباشد، درخواست برای قطعه دیگر در سرویس‌دهنده مبهم خواهد بود. رفتار سرویس‌دهنده در این حالت تعریف نشده است.

۸-۳-۳ بررسی

۸-۳-۳-۱ کلیات

این بند، فرایند قطعه‌بندی را با جزئیات بیشتری شرح می‌دهد. مفاهیم معماری این طراحی و نیازهای پیاده‌سازی افزاره و سرویس‌دهنده شرح داده می‌شوند.

۸-۳-۳-۲ هدف دامنه

این طرح قطعه‌بندی اجازه می‌دهد تا بسته‌هایی با فرمت دلخواه به‌طور قابل اطمینان بر روی یک پیوند با اندازه قاب محدود، مبادله شوند. بعد از این‌که دنباله‌ای از قطعه‌ها دریافت شدند، بار هر قطعه‌ای به شکل جریانی از بایت‌ها به‌صورت پیوسته در می‌آید و این جریان بایتی به‌عنوان یک بسته تفسیر می‌شود. این بسته شامل سرآیند عمومی بسته دیگری با رمز نوع بسته و طول بسته می‌باشد.

هر بسته بعدی می‌تواند در همین روش، محصور شده و قطعه بندی شود. هیچ فیلد اضافی در سرآیند عمومی بسته مورد نیاز نیست و هیچ فیلد دیگری در هر یک از قالب‌های فعلی یا بعدی بسته مورد نیاز نیست.

قطعه‌بندی بسته برای اعمال در مورد بسته‌های داده، در نظر گرفته نشده است.

قطعه‌های بسته می‌توانند در هر ترتیبی و بارها درخواست شوند و در صورتی‌که سرویس‌دهنده به بسته‌های دارای تاریخ زمان یکسان پاسخ دهد، هر پاسخ دارای تاریخ زمان و شناسه قطعه یکسان، باید شامل بایت‌های یکسان با دیگر پاسخ‌های این چنینی باشد.

۸-۳-۳-۳ پیاده‌سازی‌های سرویس‌دهنده

تنوع پیاده‌سازی‌ها در یک سرویس‌دهنده می‌تواند اطمینان دهد که فیلد تاریخ زمان نشان‌دهنده سازگاری ترتیب بسته‌ها برای یک شناسه درخواست است. از جمله:

- قفل کردن پایگاه داده در طی هر در خواست نامناسب و اعمال بروزرسانی‌ها در پایان آخرین درخواست؛
- نمایش لحظه‌ای داده برای یک درخواست و کنار گذاشتن آن، زمانی‌که بسته نهایی ارسال می‌شود یا در زمان‌هایی که ترتیب درخواست/ پاسخ هرگز کامل نمی‌شود.

۸-۳-۳-۴ پیاده‌سازی‌های افزاره

تنوع پیاده‌سازی‌ها در یک افزاره می‌تواند تضمین کند که درخواستی که پاسخ کاملی دریافت نکرده است، برای جلوگیری از هدر دادن منابع، دیگر ادامه نمی‌یابد. از جمله، در موارد زیر:

۱- مجزا کردن قطعه‌هایی که دریافت می‌شوند و کنار گذاشتن این قطعه‌ها و داده‌های کنترل هنگامی که:

۲- اتمام مهلت زمان اتفاق می‌افتد و نشان می‌دهد که سرویس دهنده به درخواست‌ها پاسخ نمی‌دهد (بعد از یک ترفند ارسال مجدد)

۳- پاسخ بسته قطعه‌بندی نشده مناسب، نشان می‌دهد که در خواست برآورده شده است. (هیچ فیلد شناسه درخواست صریحی به سرآیند بسته اضافه نمی‌شود، اما این وضعیت مبهم نیست چون افزاره تنها با یک سرویس‌دهنده پیکربندی واحد ارتباط برقرار می‌کند، در نتیجه نیازی به پشتیبانی چندین درخواست از نوع یکسان با آن سرویس‌دهنده نیست.)

۴- دنباله‌ای از بسته‌های قطعه با شناسه درخواست صحیح و همه با تاریخ زمان یکسان، دریافت شوند. بار این قطعه‌ها به‌عنوان بسته‌ای که پاسخ به این درخواست است، رمزگشایی می‌شود.

۸-۴ مبادله بسته داده

۸-۴-۱ کلیات

این بند، چگونگی مبادله بسته‌های داده CNP روی کانال‌های IP را تعریف می‌کند. این بند به ویژه تعریف می‌کند که بسته‌های CNP به افزاره CNP/IP دیگر چگونه ارسال می‌شود. با این حال چگونگی تعیین این که چه افزاره‌های CNP/IPای، بسته‌های داده CNP را ارسال می‌کنند، در این بند گنجانده نشده است. فرض می‌شود که تعیین افزاره‌ها با استفاده از تعریف کانال IP یا فهرست ارسال انجام می‌گیرد. بنابراین به دلیل بحث، اجازه دهید که فهرست "ارسال رو به جلو" را به عنوان فهرستی از آدرس‌های IPای تعریف کنیم که بسته داده خاص CNP را دریافت خواهد کرد. توجه داشته باشید که فهرست ارسال رو به جلو می‌تواند هم شامل آدرس‌های IP تک‌پخشی و هم شامل آدرس‌های IP چندپخشی باشد. چگونگی تعیین این فهرست ارسال رو به جلو، ربطی به بحث مورد نظر ندارد.

چون CNP از سرویس تصدیق انتها به انتها استفاده می‌کند، فرض‌های زیر اعمال می‌شوند:
- نیازی به اضافه کردن تصدیق‌ها به بسته‌های داده CNP/IP ارسال شده نمی‌باشد.
- نیازی به ارسال مجدد بسته‌های IP حذف شده نمی‌باشد.
از طرف دیگر برای درست کارکردن CNP، شرایط زیر باید برقرار باشد:
- ترتیب بسته مربوط به بسته‌های CNP باید حفظ شود.
-فرستنده بسته‌های CNP، نیازی به ارسال بیش از یک کپی از بسته CNP به هر یک از اعضای دیگر کانال CNP/IP ندارد.
- گیرنده باید بسته‌های CNP/IP تکراری را تشخیص دهد و نیازی به ارسال آنها نیست.
- بسته‌هایی که مهلت زمانی آن‌ها برای کانال به پایان رسیده، لازم نیست ارسال شوند. این بسته‌ها، بسته‌های منقضی‌شده نام دارند.
بسته‌های داده CNP با استفاده از تونل‌زنی روی UDP، مابین افزاره‌ها CNP/IP مبادله می‌شوند. هر بسته CNP با یک سرآیند داخل نمودار داده UDP محصور می‌شود. ترکیب سرآیند و بار بسته داده CNP اشاره به "پیام داده CNP/IP" دارد. بخش سرآیند،"سرآیند پیام داده CNP/IP" و بسته داده CNP، "بار داده CNP" نام دارد. توجه داشته باشید که یک نمودار داده UDP واحد می‌تواند شامل بیش از یک پیام داده CNP/IP باشد.
با توجه به فهرست ارسال رو به جلوی خاص، یک افزاره CNP/IP صرفاً پیام‌های داده CNP/IP یکسان را به هر یک از آدرس‌های موجود در فهرست با استفاده از UDP ارسال می‌کند. به دلیل ویژگی‌های شبکه‌های IP و UDP، ارسال پیام‌ها تضمین نمی‌کند که میزبان مقصد، بسته‌های تکراری، خارج از ترتیب و منقضی را دریافت نکند. بنابراین لازم است که فرستنده پیام‌های داده CNP/IP، شامل اطلاعاتی اضافی باشد تا تضمین کند که گیرنده می‌تواند با هر یک از شرایط، به‌طور مناسبی برخورد کند. بندهای زیر این موضوع را توصیف می‌کنند.

۸-۴-۲ بسته‌های خارج از ترتیب

بسته‌هایی که توسط گیرنده، خارج از ترتیب تشخیص داده می‌شوند، نیازی به ارسال ندارند. افزاره CNP/IP باید سعی کند بسته‌هایی که دریافت می‌شوند را دوباره ترتیب‌گذاری کند تا مشکل ترتیب حل شود، اما در صورتی‌که آن‌ها خارج از ترتیب باشند در هیچ حالتی نباید ارسال شوند. اگر ترتیب‌گذاری مجدد پشتیبانی نشود یا ممکن نباشد، در آن صورت بسته‌ها باید حذف شوند.
برای حصول اطمینان از عدم ارسال خارج از ترتیب بسته‌ها توسط گیرنده، باید الگوریتم زیر را به کار برد.
- هر منبع داده CNP/IP، برای هر آدرس IP مقصد بسته داده، یک شناسه جلسه (SID) و یک شماره ترتیب بسته ۳۲ بیت بدون علامت (PSN)، نگهداری می‌کنند.
- هر پیام داده CNP/IP، به‌وسیله یک منبع داده، به آدرس IP خاص مقصد شامل این جفت SID/PSN فرستاده می‌شود. بعد از هر پیامی که ارسال می‌شود، هر PSN یک واحد افزایش می‌یابد، برعکس SID مابین

پیام‌های داده CNP/IP متوالی تغییر نمی‌کند، SIP می‌تواند در بین تمامی آدرس‌های IP مقصد متنوعی که آدرس CNP/IP پیام‌ها را به آن ارسال می‌کند، مشترک باشد.

- اگر یک افزاره CNP/IP، "جلسه" جدیدی را به یک آدرس مقصد خاص آغاز کند (به عبارت دیگر، بعد از یک چرخه راه‌اندازی یا راه اندازی مجدد)، این افزاره باید از یک SID که از SID به کار رفته قبلی متفاوت است استفاده کند. در حالت کلی، SID برای پیام‌های متوالی ثابت می‌ماند در حالی‌که PSN افزایش می‌یابد.

-PSN، از 0xFFFFFFFF تا 0x00000000 را شامل می‌شود. به علاوه X و Y باید جزو PSN باشند. رابطه $X<Y \text{ if } (X-Y)<0\times80000000$ برقرار است با فرض این که مقدار ۳۲بیت بدون علامت استفاده می‌شود.

- هر افزاره سینک[1] داده CNP/IP برای هرجفت آدرس مبدا/آدرس مقصد IP (SA/DA) که از آن، یک بسته داده دریافت شده است، شماره " آخرین ترتیب ارسال " را نگهداری می‌کند.

- مقدار اولیه LFS برای هر SA/DA برابر با مقدار PSN پیام داده CNP/IP دریافت شده از SA/DA است، در صورتی‌که هر یک از شرایط زیر برقرار باشند:

الف - بعد از راه‌اندازی افزاره سینک داده؛

ب- اگر SID متفاوت از پیام داده CNP/IP قبلی دریافت شده از آن SA/DA باشد.

- پذیرش توسط یک سینک داده از یک پیام داده CNP/IP با PSN=LFS+1، موجب می‌شود بسته داده ارسال شود. LFS یک واحد افزایش می‌یابد.

- دریافت توسط سینک داده یک پیام داده CNP/IP با PSN>(LFS+1)، ممکن است موجب شود که بسته در اسکرو[2] نگه داشته شده و منتظر ورود و ارسال پی در پی تمامی بسته‌های دیگر با (PSN اولین بسته اسکرو)> PSN >(LFS+1) باشد.

- اگر (بسته‌های اسکرو موجود باشند) و (زمان بعد از پذیرش اولین بسته در اسکرو، بیشتر از دوره مهلت زمانی کانال و کمتر از حداکثر ۱/۵ ثانیه باشد) در آن صورت انتظار برای تمامی بسته‌های در فاصله PSNهای مابین (LFS+1) و (PSN اولین بسته در اسکرو) متوقف می‌شود.

- پذیرش توسط یک سینک داده بسته داده CNP/IP با PSN<(LFS+1) به‌عنوان یک بسته تکراری، حذف می‌شود.

- اسکرو کردن بسته‌های داده CNP/IP از یک SA/DA، بر ارسال و یا اسکرو کردن بسته‌های داده CNP/IP از SA/DAهای دیگر، تاثیری نمی‌گذارد.

۸-۴-۳ شناسایی بسته تکراری

بسته‌هایی که تکراری تشخیص داده می‌شوند، باید از طرف دریافت‌کننده کنار گذاشته شوند. این کار را می‌توان با استفاده از الگوریتم مشابهی که برای حصول اطمینان از ترتیب‌دهی در بند قبل توصیف شد تکمیل کرد.

1- Sink

2- Scrow

۸-۴-۴ تشخیص بسته منقضی‌شده

افزاره‌های CNP/IP باید قادر به تشخیص بسته‌های منقضی شده باشند. یک افزاره CNP/IP باید قابلیت غیرفعال کردن تشخیص بسته‌های منقضی شده برای شرایطی که نیازی به آن‌ها نیست را پشتیبانی کند. مثالی از این می‌تواند شبکه‌های محلی اترنت بخش واحدی باشند که در آن‌ها، مسیریاب‌های IP مداخله‌کننده وجود ندارد که موجب تأخیرهای نامعلوم در ترافیک شبکه شود. با فرض توانایی سامانه برای شناسایی بسته منقضی، بسته‌هایی که منقضی تشخیص داده می‌شوند، باید از طرف دریافت‌کننده کنار گذاشته شوند. اگر مدت زمان انتقال یک بسته از فرستنده به یک گیرنده روی کانال، بیشتر از دوره مهلت زمانی کانال (CTP) باشد، این بسته به‌عنوان بسته منقضی شده در نظر گرفته می‌شود. CTP دوره زمانی است که حد بالای منطقی زمانی که طول می‌کشد تا یک بسته از یک فرستنده به یک گیرنده روی کانال IP برود را نشان می‌دهد. این استاندارد، چگونگی تعیین دوره مهلت زمانی کانال را پوشش نمی‌دهد. کافی است گفته شود که مهلت زمانی کانال برحسب میلی‌ثانیه است و برای همه افزاره‌های CNP/IP روی کانال IP شناخته شده می‌باشد. دوره مهلت زمانی واحدی وجود دارد که به تمامی افزاره‌های CNP/IP روی کانال اعمال می‌شود.

برای این‌که افزاره‌ها قادر به تشخیص مدت زمان انقضای یک بسته شوند، باید تعیین شود که از زمان ارسال بسته روی کانال IP چه مدت سپری شده است. روش مذکور در این بخش مختص فرستنده است و وی باید قبل از ارسال هر بسته داده روی کانال IP، نشان زمان هر کدام را مشخص کند. در مورد مسیریاب‌های CNP/IP به CNP/IP، بسته‌ها قبل از ارسال روی کانال IP بعدی، با جدیدترین زمان، مجدداً نشانه‌گذاری می‌شوند. در وضعیت گره‌های پروکسی که بسته‌ها را روی کانال IP یکسانی ارسال می‌کنند، بسته‌ها مجدداً نشانه‌گذاری نمی‌شوند. همچنین توجه داشته باشید که تمامی آدرس‌های CNP/IPای که بسته خاصی را دریافت می‌کنند، باید نشان زمانی یکسانی داشته باشند.

برای مؤثر واقع شدن نشان زمان، ساعت موجود در همه افزاره‌های روی کانال IP باید هماهنگ شوند. دقت دقیق این هماهنگی مشخص نشده است. با توجه به نوع شبکه IP استفاده شده، محدوده وسیعی از دقت‌ها امکان پذیر است. باید در نظر داشت که عدم دقت در هماهنگی زمان، خود را به شکل تأخیر در انتقال نشان می‌دهد که برای پروتکل تونل‌زنی زیان‌بار است. بخش‌هایی که به این امر ارتباط دارند و برای یک پروتکل خاص مهم تلقی می‌شوند، در پیوست ویژه در این استاندارد گنجانده شده است.

ابزار هماهنگی ساعت‌های تمامی افزاره‌های CNP/IP، SNTP می‌باشد که در RFC2030 مشخص شده است. این بدین معنی است که یک سرویس‌دهنده زمانی SNTP، در بخشی از شبکه IP وجود دارد و این‌که افزاره‌های CNP/IP برای دسترسی به آدرس IP آن تنظیم شده‌اند. قالب نشان زمانی که در RFC 1305 مشخص شده است، یک مقدار صحیح ۳۲ بیتی برحسب ثانیه و یک مقدار صحیح ۳۲ بیتی بر حسب پیکوثانیه می‌باشد. دامنه پیوسته‌ای از بیت‌ها به شکل این قالب وجود ندارد که خواص محاسباتی و دقت موردنیاز را داشته باشد. بنابراین قالب نشان زمانی در این مشخصه، ۳۲ بیت برحسب میلی‌ثانیه می‌باشد. این قالب با زمان فعلی SNTP تراز می‌شود. این نشان زمانی، تقریبا هر ۴۹/۷ روز به پایان می‌رسد.

تا زمانی‌که ارتباطات با سرویس‌دهنده زمان ادامه دارد، افزاره‌ها باید با یکدیگر هماهنگ باشند و تشخیص بسته منقضی‌شده می‌تواند به‌صورت متعارف انجام پذیرد. در صورتی‌که به هر دلیلی ارتباط با سرویس‌دهنده زمان از بین برود، ممکن است مشکلاتی بروز دهد. تحت این شرایط تنها تا وقتی‌که افزاره بتواند به‌طور منطقی مطمئن باشد که ساعتش از محدوده دیگر افزاره‌های موجود در شبکه خارج نشده است، می‌تواند به ارسال بسته‌ها ادامه دهد. از آنجایی که سرویس‌دهنده زمان، مبنای مشترک برای زمان در شبکه است، یک افزاره تنها تا زمانی‌که می‌تواند به ارسال بسته‌ها ادامه دهد که قبل از خروج از حد خطای سرویس‌دهنده، به‌طور منطقی مطمئن شود که در درون این حد قرار دارد. این امر در صورتی می‌تواند اتفاق بیفتد که افزاره میزان انحراف ساعتش را بداند. اگر افزاره روشی برای تخمین حد خطا بین ساعت خود و ساعت افزاره‌های دیگر موجود در شبکه نداشته باشد، در آن صورت نباید بسته‌ها را به کانال IP ارسال کند.

هنگامی‌که دقت زمان NTP برحسب پیکوثانیه است، دقت عملی یک زمان به‌دست آمده در یک سامانه در مورد وقفه‌های زمان‌سنج، معمولاً ۱۰ میلی‌ثانیه یا ۱۶ میلی‌ثانیه می‌باشد. دقت نشان زمانی بر حسب میلی‌ثانیه است، اما بیت‌های کم (۳ یا ۴) مقداری ندارند. این بدین معنی است که گرد کردن یا برش، مشکلی ندارد. همچنین مشاهده می‌شود که کوچکترین مقدار دریافتی زمان‌سنج برای CNP، ۱۲۸ میلی‌ثانیه است، طوری‌که مقادیر کوچک اختلاف مابین دو نشان زمانی، با یکدیگر مرتبط نیستند.

۸-۵ تعامل‌های سرویس‌دهنده پیکربندی

۸-۵-۱ تعامل عمومی افزاره

۸-۵-۱-۱ کلیات

ارتباط مابین یک افزاره CNP/IP (سرویس‌گیرنده) و یک سرویس‌دهنده پیکربندی به‌صورت زیر است:

الف- افزاره، یک پیام ثبت به سرویس‌دهنده پیکربندی ارسال می‌کند. در این پیام برخی از پارامترهای پیکربندی قرار گرفته‌اند. برای بازه تکرار با بازه حداکثر ۳۰ ثانیه، افزایشی در نرخ نمایی وجود دارد. اگر افزاره، پیکربندی درستی داشته باشد، می‌تواند هنگامی‌که منتظر پاسخی از سرویس‌دهنده است، از آن برای مسیریابی پیام‌ها استفاده کند.

ب- سرویس‌دهنده باید با یکی از دو پیام ممکن پاسخ دهد. اگر سرویس‌دهنده نمی‌خواهد سرویس‌گیرنده را به کانال اضافه کند، یک پیام تصدیق با مقدار ACK-DEVICE-REFUSED، یا یک پیام پیکربندی افزاره که شامل برخی از پارامترهای پیکربندی است را ارسال می‌کند. سرویس‌دهنده بسته تصدیق را دوباره ارسال نمی‌کند. اگر افزاره آن پیام را دریافت نکند، درخواست اولیه را دوباره ارسال خواهد کرد.

پ- افزاره باید تصدیق کند که پیام پیکربندی افزاره که در بند (ب) به آن ارسال شده را دریافت کرده است. پیام تصدیق می‌تواند مقادیر مختلفی به خود بگیرد؛ مقدار ACK-OK بیان می‌کند که افزاره، پیکربندی را پذیرفته است؛ مقدار ACK-FIXED بیان می‌کند که افزاره، پیکربندی ثابتی دارد؛ مقدار ACK-BAD-MESSAGE بیان می‌کند که پیام دریافت شده، دارای خطا است؛ و مقدار ACK-CANT-COMPLY بیان می‌کند که افزاره به هر دلیلی نمی‌تواند از پارامترهای پیکربندی استفاده کند.

ت- بعد از فرایند ثبت، افزاره می‌تواند مجموعه‌ای از پیام‌های درخواست را به سرویس‌دهنده ارسال کند.

ث- سرویس‌دهنده باید با پیام‌های پاسخ مناسب به این درخواست‌ها پاسخ دهد. چگونگی پاسخ دادن سرویس‌دهنده به تصدیق‌های مختلف، در اینجا تعریف نشده است، اما سرویس‌دهنده باید برای امکان‌پذیر ساختن اشکال‌زدایی، پیام‌ها را ثبت کند.

۸-۵-۱-۲ بسته‌های ناخواسته از سرویس‌دهنده

سرویس‌دهنده ممکن است یک پیام ناخواسته پیکربندی افزاره را به یک افزاره ارسال کند. افزاره به همان روشی که در بالا شرح داده شد، آن را تصدیق می‌کند. بهترین روش برای سرویس‌دهنده این است که مانع بالا آمدن افزاره‌ای شود که با بسته‌های ناخواسته روی خط می‌آید، تا زمانی‌که این افزاره به درخواست بسته‌ها خاتمه نداده باشد. جزئیات پیاده سازی، یک موضوع انتخابی است. سایر بسته‌های پیکربندی هرگز به‌طور ناخواسته‌ای ارسال نمی‌شوند. پیام پیکربندی افزاره‌ای که به‌طور ناخواسته ارسال می‌شود، هرگز قطعه‌بندی نخواهد شد.

پیام ناخواسته پیکربندی افزاره که از سرویس‌دهنده ارسال می‌گردد، مورد استفاده قرار می‌گیرد تا به افزاره نشان دهد که برخی از بخش‌های دیگر پیکربندی کانال تغییر یافته است. فیلدهای تاریخ زمان در پیام پیکربندی افزاره، در این پیام‌ها معتبر هستند و تاریخ زمان‌های آخرین بسته‌های فهرست ارسال و فهرست عضویت کانال را نشان می‌دهند. پس از مقایسه این تاریخ زمان‌ها با تاریخ زمان‌های بسته‌هایی که در حال حاضر توسط یک افزاره ذخیره شده‌اند، افزاره باید برای به‌دست آوردن آخرین نسخه‌ها، بسته‌های مسیریابی کانال، فهرست ارسال و عضویت کانال را از سرویس‌دهنده در خواست کند.

اگر چه یک سرویس‌دهنده پیکربندی به کار گرفته می‌شود، پیکربندی یک کانال CNP/IP می‌تواند ایستا باشد. این شرایط در صورتی صدق می‌کند که پیکربندی بدون بررسی تأیید شده و در سرویس‌دهنده پیکربندی ثابت باشد. این یکی از دلایلی است که یک سرویس‌دهنده ممکن است به پیام ثبت یک سرویس‌گیرنده، با یک پیام رد افزاره CNP/IP پاسخ دهد. ثبت افزاره با سرویس‌دهنده ممکن است بخشی از پیکربندی ثابت نباشد. روشی که از طریق آن، سرویس‌دهنده تعیین می‌کند که چگونه به پیام ثبت سرویس‌گیرنده پاسخ دهد، مختص فروشنده است.

۸-۵-۱-۳ درخواست از افزاره‌ها یا گره‌های دیگر

افزاره‌ها باید درخواست‌های گره‌های دیگر و احتمالاً افزاره‌ها را پاسخ دهند. غیر از پیام‌هایی که قطعه‌بندی می‌شوند، هیچ تضمینی در مورد داده‌هایی وجود ندارد که توسط سایر افزاره‌ها یا گره‌هایی که افزاره یا سرویس‌دهنده نیستند درخواست می‌شود. تضمین قطعه‌بندی به این معنی است که مجموعه بسته‌ها، تاریخ زمان یکسان و مجموعه سازگاری از بایت‌ها را خواهند داشت. یک افزاره باید با توجه به ارتباط خود با سرویس‌دهنده، یکپارچگی کلّی خود را حفظ کند.

به‌عنوان مثال، اگر افزاره الف برای بسته مسیریابی کانال به افزاره ب پاسخ دهد و در طول این مبادله، اطلاعات مسیریابی افزاره الف تغییر کند، افزاره الف مسئولیتی برای اطلاع دادن به افزاره برای رد کردن پاسخ‌ها به افزاره ب یا اطلاع دادن به افزاره ب از طریق تغییر تاریخ زمانی که نشاندهنده می‌دهد تغییر داده

یافته ندارد. (مگر اینکه باقیمانده داده‌ها در طول این مبادله از مجموعه داده تغییر یافته، باشد.) تنها مسئولیت کاملی که افزاره الف دارد، اطلاع دادن به سرویس‌دهنده درباره اطلاعات به‌روزرسانی شده است.
افزاره‌ها مسئولیتی برای پاسخ یا پردازش پیام‌های ناخواسته پیکربندی از افزاره‌هایی غیر از سرویس‌دهنده ندارند. آن‌ها باید به پیام‌های ناخواسته درخواست از افزاره‌هایی غیر از سرویس‌دهنده پاسخ دهند. این بدین معنی است که اگر یک افزاره یک پیام ناخواسته پیکربندی افزاره، مسیریابی کانال، فهرست ارسال یا عضویت کانال را از گره‌ای که سرویس‌دهنده نیست دریافت کند، می‌تواند آن را حذف کند.

۸-۵-۱-۴ زمان تاریخ

همه بسته‌های پیکربندی شامل زمان تاریخ هستند. این تاریخ زمان برای داده معتبر است. نسخه‌های قدیمی‌تر یا جدیدتر این داده را می‌توان از طریق جستجو در این فیلد، با دقت ۱ ثانیه مشخص کرد. این فیلد محدود است، طوری‌که اگر در یک لحظه، بیش از یک نسخه از داده ایجاد شود، هر کدام از آن‌ها مقادیر منحصربه‌فرد و فزاینده‌ای برای این فیلد خواهند داشت.
اگر شبکه، از SNTP یا NTP را پشتیبانی کند، مقدار زمان تاریخ، بخش ثانیه تاریخ زمان NTP از RFC 1305 خواهد بود. این بخش، تعداد ثانیه‌ها از اول ژانویه سال ۱۹۰۰ میلادی می‌باشد. این زمان در سال ۲۰۳۶ منقضی خواهد شد. برای جزئیات بیشتر، بند ۳ از RFC 2030 را ملاحظه نمایید.
اگر یک شبکه، از پروتکل SNTP یا NTP را پشتیبانی نمی‌کند، زمان تاریخ می‌تواند عدد کوچک صحیحی باشد که شامل صفر نمی‌شود. آشکار است که این تاریخ‌ها در اوایل دهه ۱۹۰۰، منطبق با ساعت معمول نیستند، اما همان‌طور که پیشتر ذکر شد، ملزم به پیروی از شرایط یگانگی برای هر نوع زمان هستند. به‌عبارت دیگر این مقادیر که توسط چنین افزاره‌ای منتشر می‌شوند، هرگز داده‌های متفاوت را شامل نشده یا در مورد آن‌ها تکرار نمی‌شوند.
تاریخ/زمان در UTC (زمان جهانی هماهنگ)، یا در معادل آن یعنی GMT به نمایش درمی‌آید، طوری‌که منطقه زمانی، مقدار را تحت تأثیر قرار نمی‌دهد. همچنین ساعت در فصل تابستان به جلو کشیده نمی‌شود. از آنجایی‌که UTC به کار می‌رود، اگر افزاره‌ای بین مناطق زمانی جابجا شود، یا اگر جلو کشیدن ساعت در فصل تابستان تأثیرگذار باشد، زمان‌های گزارش‌شده برای بسته‌های پیکربندی، همواره به طور یکنواختی افزایش خواهد یافت.
با توجه به این‌که ساعت‌ها به صورت جزئی تغییر می‌کنند و به‌صورت دستی یا خودکار مجدداً تنظیم می‌شوند، تنظیم زمان در افزاره می‌تواند ارسال رو به جلو یا رو به عقب را تغییر دهد. یک افزاره هرگز نباید بسته پیکربندی با تاریخ زمان زودتر از زمانی که هر بسته خارج می‌شود را منتشر کند. این عمل می‌تواند با چندین روش انجام گیرد. یک روش این است که افزاره، تاریخ/زمان آخرین بسته پیکربندی منتشرشده را در حافظه بلندمدت ذخیره کند. هر لحظه‌ای که یک بسته پیکربندی منتشر می‌شود، افزاره آخرین تاریخ/زمان جاری را انتخاب می‌کند و به آخرین تاریخ زمان ذخیره شده، یک واحد اضافه می‌کند. اگر افزاره، بسته‌های پیکربندی جدیدی در نرخ میانگین کمتر از یک ثانیه منتشر کند، زمان/تاریخ پیکربندی و زمان/تاریخ سامانه سرانجام با یکدیگر تلاقی خواهند کرد که در این حالت، زمان تاریخ سامانه دیرتر خواهد بود.

۸-۵-۲ تعامل عمومی پروتکل

به‌طور کلّی، هر بسته ارسال شده، یک پاسخ مورد انتظار دارد. در یک پروتکل مبادله، پاسخ ممکن است یک ACK باشد یا یک پیام دیگر. رسید پیام دیگر باید به‌عنوان یک ACK_OK برای پیام قبلی تفسیر شود.

الف- برای جلوگیری از تراکم، بسته‌ها با استفاده از الگوریتم رو به عقب[1]، چندین بار ارسال می‌شوند. برای مثال می‌توان زمان‌سنج ارسال مجدّد را بر روی ۱ ثانیه تنظیم کرد و هر لحظه‌ای را می‌توان دو برابر کرد تا به ۳۰ ثانیه رسید.

ب- ACKها مجدداً ارسال نمی‌شوند، اما تغییر وضعیت در یک افزاره همیشه چنین است که دریافت پیام تکراری قبلی در پروتکل، موجب هیچ تغییر وضعیتی نشده و موجب ارسال مجدّد ACK مناسب می‌شود.

یک سرویس‌دهنده پیکربندی ممکن است چندین کانال را پشتیبانی کند. در این حالت سرویس‌دهنده پیکربندی با فهرستی از آدرس‌های IP افزاره برای هر کانال پیکربندی می‌شود. پیام‌های ثبت افزاره شامل آدرس IP افزاره می‌باشند، طوری‌که عضویت کانال افزاره می‌تواند تعیین شود. برای همه پیام‌های دیگر، آدرس IP ارسالی می‌تواند به‌عنوان آدرس منبع قاب UDP یا آدرس منبع ارتباط TCP تعیین شود.

۸-۵-۳ قطعه‌بندی بسته

۸-۵-۳-۱- UDP

طول تقریبی ۵۴۸ بایت بار UDP، موجب محدودیت‌هایی در عضویت کانال‌ها می‌شود و اگر گره‌ها نیز در نظر گرفته شوند، مشکلات دیگری را به بار می‌آورند. برخورد با بسته‌های بزرگ می‌تواند به این پروتکل‌های پیکربندی محدود شود و نگرانی اصلی برای این نوع بسته‌ها موارد زیر هستند:

الف- بسته‌های عضویت کانال برای تعداد تقریباً بیشتر از ۱۲۸ افزاره؛

ب- بسته‌های فهرست ارسال برای تعداد تقریباً بیشتر از ۶۴ افزاره؛

پ- اطلاعات مسیریابی کانال برای گره‌هایی با حدوداً بیشتر از ۴ دامنه.

زمانی‌که این مجموعه‌های داده‌ای از محدودیت ۵۴۸ بایت اندازه بسته UDP فراتر رفت، طرح قطعه‌بندی توصیف‌شده در بند ۸-۳ به کار می‌رود.

۸-۵-۳-۲ TCP

TCP یک ابزار اختیاری برقراری ارتباط با یک سرویس‌دهنده است. زمانی‌که فیلد IP-PROTOCOL از بسته ثبت افزاره، TCP یا BOTH TCP AND UDP را نشان می‌دهد، در آن‌صورت سرویس‌دهنده می‌تواند برای مبادله داده با افزاره، از یک پیوند TCP استفاده کند.

در این حالت:

الف- بسته‌های قطعه هرگز استفاده نمی‌شوند. بسته‌ها صرف نظر از اندازه، به‌صورت تمام و کمال فرستاده می‌شوند.

ب- پیام‌های ACK روی ارتباطات TCP ارسال نمی‌شوند.

ت- پیام‌های ارسال‌شده مجدد بر روی ارتباطات TCP عمل نمی‌کنند.

1- Back-off

ث- درخواست‌ها می‌توانند با استفاده از TCP یا UDP از یک افزاره به سرویس‌دهنده ارسال شوند. چنین درخواست‌هایی می‌توانند توسط سرویس‌دهنده با استفاده از TCP یا UDP سرویس‌دهی شوند. اگر افزاره با استفاده از TCP با سرویس‌دهنده ارتباط برقرار کند و سرویس‌دهنده، TCP را پشتیبانی کند، در آن‌صورت سرویس‌دهنده باید با استفاده از TCP پاسخ دهد.

ج- زمانی‌که سرویس‌دهنده پیکربندی، تغییری را در پیکربندی تشخیص می‌دهد، ممکن است داده پیکربندی ناخواسته‌ای را بر روی پیوند TCP به افزاره ارسال کند. بسته عضویت کانال همواره ابتدا ارسال می‌شود و بعد از آن، بسته‌های به‌روز رسانی شده مربوطه ارسال می‌شوند. بسته‌های بعدی می‌توانند به این صورت ارسال شوند: بسته‌های فهرست ارسال، پیکربندی افزاره یا مسیریابی کانال.

ح- هنگامی‌که اتصال TCP به طور ناموزونی قطع می‌شود، افزاره و نه سرویس دهنده، مسئول برقراری مجدد اتصال است. فرض می‌شود که افزاره دچار خطا شده یا از شبکه جدا شده است. زمانی‌که به‌روزرسانی جدیدی اتفاق می‌افتد، سرویس‌دهنده پیکربندی دوباره سعی می‌کند که ارتباطی را با افزاره برای ارسال به‌روزرسانی برقرار کند. افزاره همواره باید سعی کند با استفاده از دوره زمانی پیاده‌سازی وابسته و مطمئن، ارتباطی با سرویس‌دهنده برقرار کند و به مسیریابی پیام‌ها براساس هر داده پیکربندی موجود ادامه دهد. هنگامی‌که TCP استفاده می‌شود، افزاره یا سرویس‌دهنده می‌تواند ارتباط را آغاز کند. ارتباط برای یک دوره زمانی پیاده‌سازی وابسته و مطمئن برقرار می‌ماند و منتظر استفاده شدن توسط ترافیک بعدی است. هر طرف ممکن است بعد از مهلت زمانی خود، ارتباط را خاتمه دهد. بستن ارتباط موزون TCP بهتر است، اما لازم نیست.

وقتی افزاره‌ای که از TCP پشتیبانی می‌کند، اولین ارتباط خود را با سرویس‌دهنده آغاز می‌کند، نمی‌داند که آیا سرویس‌دهنده TCP را پشتیبانی می‌کند یا نه. افزاره می‌تواند از مکانیزم زیر تعیین کند که آیا از TCP استفاده می‌شود:

۱- افزاره سعی می‌کند که یک ارتباط TCP با سرویس‌دهنده پیکربندی ایجاد کند.

۲- لازم نیست افزاره قبل از ارسال درخواست‌ها از طریق UDP به سرویس‌دهنده، منتظر برقراری موفق ارتباط یا اتمام مهلت زمانی باشد. برای مثال افزاره می‌تواند ارتباط TCP را آغاز کند و سپس فوراً بسته ثبت افزاره را به سرویس‌دهنده ارسال کند. توجه داشته باشید که بسته ثبت افزاره شامل فیلد پروتکل IP است که بیان‌کننده این است که افزاره، TCP را پشتیبانی می‌کند.

تنها راه برای این‌که افزاره تعیین کند که آیا سرویس‌دهنده پیکربندی از TCP پشتیبانی می‌کند، داشتن ارتباط موفق است. این مکانیزم فرض می‌کند، گره‌ای که از TCP پشتیبانی نمی‌کند، نمی‌تواند با ارتباط رد شده پاسخ دهد.

اگر تعداد ارتباطات همزمان پشتیبانی شده توسط سرویس‌دهنده از تعداد افزاره‌های روی کانال کمتر باشد، امکان دارد افزاره‌ها هنگامی‌که سعی می‌کنند تا ارتباط را برقرار کنند، پیام‌های رد شدن ارتباط از سرویس‌دهنده را دریافت کنند. چنین پاسخ‌هایی باید نشان دهند که منابع ناکافی روی سرویس‌دهنده وجود

دارد. در این حالت آن‌ها بعد از مدت زمان مناسبی، مجدداً سعی می‌کنند یا ترجیح می‌دهند که از UDP استفاده کنند.

سرویس‌دهنده‌ها باید مهلت‌های زمانی ارتباطات TCP ذخیره شده را تسریع کنند، طوری‌که یک یا چند ارتباط باز برای مکالمات افزاره جدید فراهم آورند.

۸-۵-۴ ثبت افزاره

این تعامل بدین منظور طراحی می‌شود که به افزاره اجازه دهد تا هویت خود را به سرویس‌دهنده پیکربندی اطلاع دهد و پارامترهای عملیاتی IP را از سرویس‌دهنده به‌دست آورد.

افزاره برای شروع تعامل با سرویس‌دهنده، به اطلاعات زیر نیاز دارد. تمامی اطلاعات دیگر را می‌توان براساس منحصربه‌فرد بودن این داده‌ها، از سرویس‌دهنده کسب کرد.

الف- آدرس IP/پورت افزاره؛

ب- آدرس IP/پورت سرویس‌دهنده پیکربندی.

چندین حالت وجود دارد که با این تعامل رفع می‌شود:

۱- افزاره دارای برخی از اطلاعات هویتی است و نیاز دارد تا باقیمانده را از سرویس‌دهنده کسب کند. سرویس‌دهنده از افزاره اطلاع دارد.

۲- افزاره دارای یک پیکربندی ثابت بوده و احتمالاً به‌صورت محلی وارد شده است و باید از طریق سرویس‌دهنده ثبت شود و فهرست ارسال و فهرست عضویت کانال را به‌دست آورد.

۳- افزاره ممکن است قادر به پیروی از اطلاعات پیکربندی پیشنهادی سرویس‌دهنده باشد یا نباشد. پروتکل، گفتگو درباره پیکربندی را میسر نمی‌سازد. اگر افزاره قادر به پیروی از پیکربندی پیشنهادی سرویس‌دهنده نباشد، این مورد را گزارش می‌کند و عملیات را متوقف می‌سازد.

۴- هنگامی‌که افزاره عملیات را متوقف می‌کند، به پردازش پیام‌ها از سرویس‌دهنده پیکربندی ادامه می‌دهد، اما پیام‌ها را مسیریابی نمی‌کند. افزاره فعالیت بیشتر با سرویس‌دهنده را دامن نمی‌زند، اما پیام‌های پاسخ افزاره را پردازش می‌کند. این پروتکل در جدول ۱ نشان داده شده است.

جدول۱- ثبت افزاره با پروتکل سرویس‌دهنده پیکربندی

سرویس دهنده	→ ←	افزاره
به پیکربندی اضافه می‌کند یا رد می‌کند.	→	پیام ثبت افزاره را ارسال می‌کند
رد کردن روی ACK-DEVICE_REFUSED یا	←	تا راه‌اندازی دوباره، عملیات را متوقف می‌کند و
بسته پیکربندی افزاره	←	با پارامترهای جدید، عملیات را آغاز می‌کند، و
ارسال مجدد پیکربندی افزاره را متوقف می‌کند، در پایگاه داده نشان می‌دهد که افزاره یک عضو است.	→	ACK-OK عملیات را آغاز می‌کند.
عدم فعالیت بیشتر، عدم تغییر در پایگاه داده‌ای را به دنبال دارد.	→	ACK-CANT-COMPLY تا راه اندازی مجدد، عملیات را متوقف می‌کند.

ادامه جدول ۱

بسته ناخواسته پیکربندی افزاره را ارسال می‌کند.	←	یا گام بعدی را اجرا می‌کند.
در صورت لزوم بر اساس تاریخ/زمان‌های پاسخ افزاره، اطلاعات بیشتری را درخواست می‌کند.	→	ACK-OK یا ACK-CANT-COMPLY ارسال می‌کند.

در حالت خواسته‌شده، سرویس‌دهنده بسته پیکربندی را دوباره ارسال نمی‌کند. در صورتی‌که سرویس‌گیرنده بسته پیکربندی افزاره را به موقع دریافت نکند، مجدداً بسته ثبت افزاره را به سرویس‌دهنده ارسال خواهد کرد.

در حالت ناخواسته، در صورتی‌که سرویس‌دهنده یک ACK-OK یا ACK-CANT-COMPLY از سرویس گیرنده دریافت نکند، باید بسته پیکربندی افزاره را مجدداً ارسال کند.

سرویس‌دهنده پیکربندی، همچنین می‌تواند با استفاده از این پیام‌ها، اعضای یک کانال را از تغییر سرویس‌دهنده پیکربندی آگاه کند. اگر آدرس IP یا پورت سرویس‌دهنده پیکربندی تغییر کند، این امر ضروری نیست. این پروتکل در جدول ۲ نشان داده شده است. در حال حاضر این یک عمل مورد اطمینان نیست. امکان دارد افزاره‌ها این درخواست را رد کنند، بنابراین باید پیکربندی در برخی از روش‌های وابسته پیاده سازی، برای شناسایی مدیر پیکربندی انجام گیرد. این پروتکل به خودی خود، مصالحه امنیتی قابل توجهی را میسر نمی‌سازد؛ چون تقلید از IP امکان‌پذیر است، لذا هرگاه که مدیر پیکربندی در شبکه خاموش است، گره دیگری می‌تواند هویت IP و نقش مدیر پیکربندی را غصب کند.

جدول ۲- پروتکل پیام ناخواسته پیکربندی سرویس دهنده به افزاره

سرویس‌دهنده	←→	**افزاره**
تقاضای بسته درخواست پیکربندی	←	پاسخ را می‌سازد
ایجادبسته پیکربندی افزاره	→	بسته پیکربندی افزاره را ارسال می‌کند
ارسال بسته پیکربندی افزاره	←	
پیش‌روی معمولی همانند سرویس دهنده پیکربندی	→	پذیرش آدرس IP/پورت جدید برای سرویس دهنده پیکربندی و سرویس دهنده زمان و ارسال ACK-OK
علامت‌گذاری افزاره‌ای که دیگر عضور کانال نیست	→	ارسال ACK-CANT-COMPLY. توقف عملیات طوری‌که مانع عملیات دیگر کانال نشود.

اگر افزاره تدبیری را اتخاذ می‌کند که مانع عملیات نمی‌شود، هنگامی‌که تغییری در رابطه با سرویس‌دهنده دریافت می‌کند که نمی‌تواند از آن پیروی کند یا پیروی از آن را رد می‌کند، در آن صورت افزاره تنها قابلیت کار با افزاره‌های مشابه را خواهد داشت. این بدین دلیل است که مدیر پیکربندی جدید یا باید متکی به همه افزاره‌هایی باشد که از دستورات و اطلاعاتش پیروی می‌کنند و یا متکی به آن‌هایی باشد که دچار شکست می‌شوند تا با برخی روش‌های دیگر ، به صورت دستی به‌روزرسانی شوند.

سرویس‌دهنده باید قبل از ارسال یک بسته جدید پیکربندی افزاره، پیکربندی سرویس‌گیرنده را درخواست کند. نیازی نیست که سرویس گیرنده قبل از پردازش یک بسته جدید پیکربندی افزاره، چنین در خواستی را از سرویس گیرنده دریافت کند.

۸-۵-۵ عضویت کانال

هدف از این تعامل این است که به افزاره اجازه داده شود تا فهرست کاملی از افزاره‌های دیگر روی کانال را به‌دست آورد. این پروتکل در جدول ۳ نشان داده شده است.

اگر فهرست عضویت کانال بعد از این‌که برخی از افزاره‌ها فعال شدند تغییر کند، سرویس دهنده می‌تواند یک بسته ناخواسته پیکربندی افزاره با تاریخ زمان جدید برای بسته عضویت کانال ارسال کند.

جدول ۳- پروتکل در خواست عضویت کانال افزاره به سرویس دهنده

سرویس دهنده	⟷	افزاره
افزاره را در پایگاه داده پیدا می‌کند و کانال را شناسایی می‌کند.	→	بسته عضویت کانال را ارسال می‌کند.
اگر هیچ کانالی تعریف نشده یا افزاره عضوی از هیچ کانالی نمی‌باشد یا	←	تا تنظیم مجدد، عملیات را متوقف می‌کند.
بسته عضویت کانال را ارسال می‌کند.	←	عملیات را با پارامترهای جدید شروع می‌کند.

بسته عضویت کانال توسط سرویس دهنده مجدداً ارسال نمی‌شود. اگر افزاره بسته را دریافت نکند، دوباره آن را درخواست می‌کند.

زمانی‌که هرگونه تغییری در پیکربندی اتفاق می‌افتد، سرویس دهنده به هر یک از اعضا، این تغییرات را اطلاع می‌دهد.

سه نوع تغییر وجود دارد:

الف- یک افزاره به فهرست اضافه می‌شود.

ب- یک افزاره از فهرست حذف می‌شود.

پ- یک افزاره پیکربندی خود را تغییر می‌دهد که لازم است گره‌های دیگر، فهرست ارسال یا اطلاعات مسیریابی کانال برای آن گره را به‌روز رسانی کنند.

همه این حالت‌ها توسط سرویس دهنده مدیریت می‌شود که به تمامی افزاره‌ها، یک بسته ناخواسته پیکربندی افزاره با تاریخ/زمان به‌روز رسانی شده برای بسته عضویت کانال، ارسال می‌کند. پس از آن، افزاره یک بسته جدید عضویت کانال در خواست می‌کند. اگر گره‌ای که بسته را دریافت می‌کند، تشخیص دهد که آن بسته در عضویت کانال نیست، بسته‌های مسیریابی را متوقف می‌کند و منتظر بسته‌های پیکربندی بعدی می‌شود. اگر گره، یک فهرست عضویت کانال نداشته باشد، بدین معنی است که به تازگی به کانال اضافه شده است، لذا بسته‌های مسیریابی کانال یا بسته فهرست ارسال را درخواست می‌کند.

هر مدخل در بسته عضویت کانال شامل یک تاریخ/زمان است که آخرین تاریخ/زمان معتبر بسته مسیریابی کانال را نشان می‌دهد. همچنین شامل تاریخ/زمان فهرست ارسال که نشان‌دهنده آخرین زمان معتبر بسته فهرست ارسال و تاریخ/زمان درخواست افزاره که نشان‌دهنده آخرین زمان معتبر آن بسته برای افزاره است، می‌باشد. این تاریخ/زمان‌ها توسط افزاره برای درخواست اطلاعات جدید استفاده می‌شوند.

۸-۵-۶ فهرست ارسال

این تعامل اجازه می‌دهد تا افزاره، یک فهرست ارسال برای کانال به‌دست آورد.

اگر فهرست ارسال بعد از این‌که برخی از افزاره‌ها فعال شدند تغییر کند، پروتکل می‌تواند کارش را با ارسال یک بسته پیکربندی افزاره به عنوان یک پیام ناخواسته به سرویس‌دهنده شروع کند. (بند ۸-۵-۴ را مشاهده کنید)

فهرست ارسال، ابزاری اختیاری است که توسط آن مسیریاب‌ها می توانند بسته‌ها را ارسال کنند. با استفاده از فهرست‌های ارسال، سرویس دهنده پیکربندی می‌تواند به‌طور متمرکز، آدرس‌های چند پخشی برای یک کانال را مدیریت کند. سرویس دهنده‌ها باید ایجاد بسته‌های فهرست ارسال را پشتیبانی کنند و به درخواست‌های افزاره‌ها برای این بسته‌ها پاسخ دهند. پشتیبانی بسته‌های فهرست ارسال توسط افزاره‌ها اختیاری است و نیازی نیست که افزاره‌ها این بسته‌ها را از سرویس دهنده‌ها درخواست کنند.

این‌که چگونه فهرست ارسال در سرویس دهنده وابسته به پیاده سازی به‌دست می‌آید یا پیکربندی می‌شود، مبتنی بر سه روش مشخص شده در بند ۶ است. در نبود یک فهرست ارسال پیکربندی شده یا یک الگوریتم پیشرفته‌تر برای به‌دست آوردن آن، سرویس دهنده می‌تواند برای ایجاد یک فهرست ارسال، از الگوریتم زیر استفاده کند.

۸-۵-۶-۱ روش تولید فهرست ارسال

اگر و تنها اگر هر افزاره در کانال CNP/IP متعلق به گروه چند پخشی یکسانی باشد، از الگوریتم الف استفاده می‌کند، در غیراین صورت از الگوریتم ب استفاده می‌کند. توجه داشته باشید که گروه‌های چند پخشی که یک افزاره متعلق به آن‌ها است، بخشی از پیکربندی افزاره هستند که سرویس دهنده به‌طور کامل از آن‌ها آگاهی دارد. این آگاهی یا از طریق بسته ثبت افزاره ارسال شده از افزاره حاصل می‌آید یا از طریق بسته پیکربندی افزاره ارسال شده از سرویس دهنده به افزاره.

۸-۵-۶-۲ الگوریتم الف (بسیاربهینه)

یک گروه چندپخشی واحد که هر افزاره روی کانال CNP/IP متعلق به آن است را انتخاب کنید. از آدرس IP چند پخشی برای این گروه به‌عنوان تنها مدخل در فهرست ارسال استفاده کنید. توجه داشته باشید که این الگوریتم به هر افزاره در کانال CNP/IP متعلق به گروه چند پخشی مشخص شده در فهرست ارسال، بستگی دارد. اگر این امر به هر دلیلی صادق نباشد، در آن صورت فهرست ارسال باید مطابق آن تغییر یابد.

۸-۵-۶-۳ الگوریتم ب (نیروی شدید)

برای هر افزاره در فهرست عضویت کانال، آدرس IP تک پخشی مربوط به آن افزاره را به فهرست ارسال اضافه کنید. در این سناریو، فهرست ارسال باید تناظر یک به یک با فهرست عضویت کانال را حفظ کند. اگر افزاره‌ها به فهرست عضویت کانال اضافه یا از آن حذف شوند، فهرست ارسال باید مطابق آن تغیر یابد و در هنگام استفاده از فهرست‌های ارسال، هر بسته ارسال شده توسط یک افزاره، بدون شرط به هر آدرس در فهرست، ارسال می‌شود. افزاره به پورت‌ها و آدرس‌های مشخص شده در پیام‌های پیکربندی افزاره توجه می‌کنند.

جدول ۴- پروتکل درخواست فهرست ارسال افزاره به سرویس دهنده

سرویس دهنده	←→	افزاره
افزاره را در پایگاه داده پیدا می‌کند و فهرست ارسال را شناسایی می‌کند.	→	بسته در خواست فهرست ارسال را می‌فرستد.
ACK-DEVICE-REFUSED، اگر هیچ کانالی تعریف نشده یا افزاره عضوی از هیچ کانالی نمی‌باشد. یا	←	تا تنظیم مجدد عملیات را متوقف می‌سازد.
بسته فهرست ارسال را می‌فرستد.	←	عملیات را با پارامترهای جدید آغاز می‌کند.

بسته ارسال توسط سرویس دهنده، مجدداً ارسال نمی‌شود. اگر افزاره بسته را دریافت نکند، آن را دوباره درخواست می‌کند.

۸-۵-۷ مسیریابی کانال

۸-۵-۷-۱ کلیات

این تعامل به افزاره اجازه می‌دهد تا اطلاعات مسیریابی کانال را برای افزاره به‌دست آورد یا اجازه می‌دهد تا افزاره، اطلاعات مسیریابی کانال را برای توزیع به افزاره‌های دیگر به سرویس دهنده ارسال کند. این پروتکل در جدول‌های ۵ و ۶ نشان داده شده است.

این بسته‌ها مابین افزاره‌های CNP/IP مبادله می‌شوند و اطلاعات مسیریابی را برای افزاره اشاره شده در پیام، نشان می‌دهند. زمانی‌که یک سرویس دهنده پیکربندی، چند مورد از این بسته‌ها را ارسال می‌کند، هر آدرس IP تک پخشی، متناظر با یک آدرس IP در فهرست عضویت کانال است.

اطلاعات مسیریابی اشاره به آن گره دارد. آدرس های IP تمامی اعضای کانال باید منحصربه‌فرد باشند.

پشتیبانی از بسته‌های مسیریابی کانال اختیاری است.

به‌خصوص جدول‌های مسیریابی که شامل ماسک‌های[1] گروه و زیرشبکه هستند، در این بسته ارسال می‌شوند. اطلاعات ماسک گروه و زیرشبکه می‌توانند توسط مسیریاب‌ها استفاده شوند تا از ارسال هر بسته به هر مسیریاب دیگر جلوگیری کنند که در غیر این صورت، اگر به هر دلیلی در شبکه IP، آدرس‌دهی چندپخشی مابین مسیریاب‌ها میسر نباشد، ممکن است پهنای باند به هدر برود.

در صورتی‌که مسیریاب بتواند به بیش از یک دامنه CNP یا مانند یک پروکسی مسیریابی کند، SubnetMsk، GroupMsk و ساختار دامنه ممکن است در بسته تکرار شوند.

اگر اطلاعات مسیریابی کانال بعد از این‌که برخی از افزاره‌ها فعال شدند تغییر کند، پروتکل می‌تواند با ارسال یک پیام ناخواسته پیکربندی افزاره به سرویس دهنده، کارش را آغاز کند. (بند ۸-۵-۴ را مشاهده کنید).

زمانی‌که یک افزاره از بسته‌های مسیریابی کانال پشتیبانی می‌کند، و آن دارای اطلاعات جدید مسیریابی کانال است، افزاره یک بسته جدید مسیریابی کانال ایجاد می‌کند. سپس این بسته به سرویس دهنده ارسال می‌شود.

1- Mask

جدول ۵- پروتکل به‌روز رسانی مسیریابی کانال افزاره به سرویس دهنده

سرویس دهنده	←→	افزاره
افزاره را در پایگاه داده پیدا می‌کند و فهرست مسیریابی را شناسایی می‌کند	→	بسته مسیریابی کانال را می‌فرستد
ACK-DEVICE-REFUSED، اگر هیچ کانالی تعریف نشده یا افزاره عضوی از هیچ کانالی نباشد.	←	تا تنظیم مجدد، عملیات را متوقف می‌سازد
ACK-OK را ارسال می‌کند.	←	ارسال مجدد بسته‌های مسیریابی کانال را متوقف می‌کند.

هنگامی‌که یک افزاره از بسته‌های مسیریابی کانال پشتیبانی می‌کند، نیازمند بسته‌های مسیریابی کانال از افزاره‌های دیگر روی کانال است. افزاره، این بسته‌ها را به شیوه نشان داده شده در جدول ۶ به‌دست می‌آورد.

جدول ۶- پروتکل درخواست مسیریابی کانال افزاره به سرویس دهنده

سرویس دهنده	←→	افزاره
افزاره را در پایگاه داده پیدا می‌کند و فهرست مسیریابی را شناسایی می‌کند.	→	بسته درخواست مسیریابی کانال را می‌فرستد.
ACK-DEVICE-REFUSED، اگر هیچ کانالی تعریف نشده یا افزاره عضوی از هیچ کانالی نمی‌باشد	←	تا تنظیم مجدد، عملیات را متوقف می‌سازد.
بسته مسیریابی کانال را ارسال می‌کند.	←	عملیات را با پارامترهای جدید آغاز می‌کند.

ارسال توسط سرویس دهنده، تکرار نمی‌شود و هیچ ACKای به‌وسیله افزاره انجام نمی‌گیرد. اگر افزاره پیامی دریافت نکند، آن پیام را دوباره درخواست می‌کند.

پیام درخواست مسیریابی کانال در درخواست به سرویس دهنده، شامل دو فیلد است.

تاریخ/زمان: تاریخ/زمان نشان می‌دهد که اگر هر داده‌ای جدیدتر از این تاریخ/زمان باشد، آن داده باید ارسال شود. مقدار صفر نشان می‌دهد که داده همیشه ارسال می‌شود.

آدرس IP تک پخشی: این IP اگر غیرصفر باشد، نشان می‌دهد که تنها مسیریابی کانال برای این افزاره، ارسال می‌شود. اگر صفر باشد نشان می‌دهد که تمامی اطلاعات مسیریابی کانال برای همه اعضای کانال، ارسال می‌شود.

این گزینه‌ها می‌توانند به‌منظور بهینه سازی درخواست‌ها به سرویس دهنده استفاده شوند. به‌عنوان مثال، اگر یک مسیریاب فهرست عضویت کانال را در خواست کند و افزاره جدیدی در این فهرست بیابد، می‌تواند اطلاعات مسیریابی کانال را تنها برای آن افزاره در خواست کند.

۸-۵-۷-۲ مسیریابی به آدرس‌های زیرشبکه/گره

بسته مسیریابی کانال شامل فهرستی از آدرس‌های زیرشبکه/گره، همچنین فهرستی از دامنه‌ها با ماسک‌های زیرشبکه می‌باشد. این‌ها می‌توانند توسط یک مسیریاب استفاده شوند تا به شیوه زیر، مسیریابی بهینه را اجرا کنند.

پیام‌های زیرشبکه/گره آدرس دهی شده به یک آدرس دامنه/زیرشبکه/گره به افزاره مربوطه می‌روند. پیام‌های شناسه منحصربه‌فرد سرراست زیرشبکه و پخشی زیرشبکه، به تمامی گره‌های پیکربندی شده در آن زیرشبکه می‌روند. چنین زیرشبکه‌هایی در ماسک زیرشبکه، تنظیم نخواهند شد. آدرس‌های دامنه/ زیرشبکه/ گره معمولاً منحصربه‌فرد خواهند بود اما در برخی موارد (حالت‌های خطا یا شرایط ناپایدار) امکان دارد چندین افزاره، آدرس یکسانی را بخواهند. در چنین مواردی، پیام‌ها باید به چندین افزاره مسیریابی شوند.

۸-۵-۷-۳ معانی برای درخواست تمامی چندپخشی‌ها

فیلد پرچم‌های CNP از بسته مسیریابی کانال، شامل بیتی بنام WANTS_ALL_BROADCASTS است. وضعیت‌های این فیلد، به‌صورت زیر مسیریابی را بهینه می‌کند:

تمامی افزاره‌ها، حداقل یک گره CNP قابل آدرس‌دهی را نشان خواهند داد. به‌عنوان مثال، برای مسیریاب‌های CNP/IP، این گره، سمت مسیریاب متصل به کانال IP است. اگر افزاره دارای حداقل یک گره CNP قابل آدرس دهی که در وضعیت غیرپیکربندی است باشد، باید گزارش کند که با وجود شناسه دامنه در پیام پخشی، نیازمند تمامی پخش‌ها (دامنه گسترده یا زیرشبکه) است. علت این است که گره‌های CNP برخلاف شناسه دامنه، زمانی‌که در حالت غیرپیکربندی هستند، به تمامی پخش‌ها پاسخ می‌دهند.

۸-۶ پیام‌های متفرقه وضعیت

۸-۶-۱ کلیات

این پیام‌ها بدین دلیل در نظر گرفته می‌شوند که به ابزارهای شبکه اجازه دهند تا اطلاعات را از یک افزاره به‌منظور کمک به مدیریت و اشکال‌زدایی افزاره‌های روی یک شبکه، استخراج کنند. به‌طور کلی تمامی اطلاعات موجود در مورد سلامت، آمار و پیکربندی افزاره می‌توانند توسط پیام‌های شرح داده شده در این بند به‌دست آیند. آن‌ها به‌منظور استفاده برای پیکربندی افزاره‌ها یا جایگزینی با عملیات فعلی تعریف شده برای سرویس‌دهنده پیکربندی، در نظر گرفته نشده‌اند.

از عملیات‌های عمومی زیر پشتیبانی به عمل می‌آید:

الف- درخواست سلامت/وضعیت عمومی افزاره CNP/IP؛

ب- درخواست سلامت/وضعیت/آمار عمومی افزاره CNP/IP و داشتن آمار واضحی از ارسال آن‌ها به درخواست کننده؛

پ- درخواست پیکربندی یک افزاره؛

ت- درخواست فهرست ارسال یک افزاره؛

ث- درخواست عضویت کانال یک افزاره؛

ج- درخواست اطلاعات مسیریابی کانال یک افزاره.

همه این عملیات‌ها به حالت یک تراکنش شکل ۱ تکامل درخواست/پاسخ ساده هستند. فرمت‌های مناسب پیام که قبلاً برای تعامل‌های سرویس‌گیرنده/سرویس دهنده تعریف شده‌اند، در این‌جا استفاده می‌شوند. در هر یک از تراکنش‌های درخواست/پاسخ شرح داده شده در این بند، توجه به این نکته اهمیت دارد که افزاره‌ای که سرویس دهنده پیکربندی نیست، نباید به درخواست‌هایی که مربوط به افزاره مورد تقاضا نیست پاسخ دهد. به‌عنوان مثال، افزاره الف نباید به درخواست برای اطلاعات در مورد افزاره ب پاسخ دهد، مگر اینکه افزاره الف یک سرویس دهنده پیکربندی باشد.

۸-۶-۲ وضعیت افزاره CNP/IP

۸-۶-۲-۱ کلیات

تمامی این اطلاعات اختیاری هستند. وسیله تأمین این اطلاعات در هیچ روشی بیان نشده است. قابلیت‌های دسترسی به این اطلاعات شامل موارد زیر هستند، اما تنها به این موارد محدود نمی‌شوند.

الف- خط سریال محلی روی مسیریاب؛

ب- دسترسی پارامترهای CNP؛

پ- دسترسی متغیر شبکه CNP؛

ت- پیام‌های (تاکنون تعریف شده) خصوصی بر روی IP؛

ث- اجرای سرویس دهنده HTML در مسیریاب؛

این داده‌ها برای تکثیر یا مانع شدن از هر پشتیبانی اختیاری برای SNMP MIB-II در پشته TCP/IP مسیریاب در نظر گرفته نمی‌شوند.

۸-۶-۲-۲ اطلاعات وضعیت

به‌طور کلی، اطلاعات آماری در فرمت درجه ثابت صحیح ۳۲ بیتی بدون علامت تهیه می‌شود. اگر آماری پشتیبانی نشود، مقدار آن آمار، 0xFFFFFFFF قرار داده می‌شود. اگر یک آمار در وضعیت سرریز است، مقدارش به 0xFFFFFFFE تنظیم می‌شود. پشتیبانی از هر آمار فردی، اختیاری است، اما هر گره CNP/IP باید با این بسته، به درخواست برای اطلاعات پاسخ دهد. فروشندگان آزاد هستند تا آمارهای ویژه پیاده سازی را به‌عنوان یک بسته پاسخ اضافی، اضافه کنند. برای کسب اطلاعات در مورد تعمیم‌های خاص فروشنده، به بند ۸-۷ مراجعه کنید.

الف- زمان پس از اینکه شمارنده، آخرین بار مجدداً تنظیم می‌شود (فرمت: عدد صحیح ۳۲ بیتی بدون علامت بر حسب ثانیه)

ب- زمان آخرین تنظیم مجدد شمارنده. (در GMT) (فرمت: تاریخ زمان، به بند ۴-۹ مراجعه کنید)؛

پ- تعداد اعضای روی کانال (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ت- تعداد اعضای روی کانالی که پیام‌ها در گذشته اخیر، در آن ارسال شده‌اند (روش اندازه گیری، تعریف نشده است). (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ث- بسته‌های CNP دریافت شده. (بسته‌های دریافت شده از کانال CNP).(فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ج- بسته‌های CNP دریافت شده اما به دلیل ارسال انتخابی حذف شده. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

چ- کل بایت‌های CNP دریافت شده. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ح- بسته‌های CNP ارسال شده. (بسته‌های ارسال شده به کانال CNP). (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

خ- بایت‌های CNP ارسال شده. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

د- بسته‌های CNP ارسال شده به کانال IP. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ذ- بایت‌های CNP ارسال شده به کانال IP. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ر- بسته‌های CNP دریافت شده از کانال IP. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ز- بایت‌های CNP دریافت شده از کانال IP. (فرمت: عدد صحیح ۳۲ بیتی بدون علامت)؛

ژ- بسته‌های IP حاوی بسته‌های LT بر روی شبکه IP. (فرمت: عدد صحیح ۳۲ بیتی بدون علامت)؛

س- بسته‌های IP حاوی بسته‌های LT از شبکه IP. (فرمت: عدد صحیح ۳۲ بیتی بدون علامت)

ش- میانگین تراکم بر روی کانال IP. (مقدار به‌صورت جفت عدد صحیح ۳۲ بیتی بدون علامت بیان می‌شود. جمع بسته‌های LT<۱۰>/جمع بسته‌های IP<۱۴>)

ص- میانگین تراکم ازکانال IP. (مقدار به‌صورت جفت عدد صحیح ۳۲ بیتی بدون علامت بیان می‌شود. جمع بسته‌های LT<۱۲>/جمع بسته‌های IP<۱۵>). (چون تمامی این پارامترها اختیاری هستند، لزوماً شکل‌های تکراری داده، مسئله نمی‌باشد. یکی ممکن است ۱۲ و۱۴ را پشتیبانی نکند و به‌جای آن ۱۷ را پشتیبانی کند.)؛

ض- تعداد بسته‌های UDP ارسال شده (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ط- تعداد بسته‌های TCP ارسال شده (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ظ- تعداد بسته‌های چند پخشی ارسال شده (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ع- بسته‌های LT منقضی که از IP حذف شده‌اند. (منقضی به این معنی است که بیش از حد طولانی در شبکه IP، بوده‌اند.) (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

غ- تعداد قطعی‌ها در ارتباط TCP (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ف- تعداد میزبان‌های مختلفی که قطعی‌های موجود در ارتباط TCP را تجربه می‌کنند. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ق- تعداد پیام‌های پیکربندی مسیریاب ارسال شده (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

ک- تعداد پیام‌های پیکربندی مسیریاب دریافت شده (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)؛

گ- تعداد تغییرات پیکربندی. (فرمت: مقدار صحیح ۳۲ بیتی)؛

ل- میانگین تعداد اجرای ارسال بسته‌های UDP در هر ثانیه. (فرمت: عدد صحیح ۳۲ بیتی)؛

م- میانگین تعداد اجرای دریافت بسته‌های UDP در هر ثانیه. (فرمت: عدد صحیح ۳۲ بیتی)؛

ن- میانگین تعداد اجرای ارسال بسته‌های TCP در هر ثانیه. (فرمت: عدد صحیح ۳۲ بیتی)؛

و- میانگین تعداد اجرای دریافت بسته‌های TCP در هر ثانیه.(فرمت: عدد صحیح ۳۲ بیتی).

۸-۶-۳ پیکربندی افزاره

ممکن است پیکربندی افزاره توسط برخی از میزبان‌ها درخواست شود. در صورتی‌که افزاره، دریافت کننده درخواست را مشخص می‌کند به چنین درخواستی باید پاسخ داده شود.

تراکنش‌های در خواست/پاسخ پیکربندی افزاره همانطور که در ۸-۵-۴ شرح داده شده، از بسته‌های یکسانی استفاده می‌کنند، از سوی دیگر از تعامل ساده‌تر نشان داده شده در جدول ۷ استفاده می‌کنند.

جدول۷- پروتکل برای درخواست پیکربندی یک افزاره

افزاره	←→	میزبان IP
صحت درخواست را تائید می‌کند	→	بسته درخواست پیکربندی را ارسال می‌کند
در حالت رد کردن،ACK-DEVICE-REFUSED یا	←	انجام یافته
بسته پیکربندی افزاره را ارسال می‌کند	←	انجام یافته

۸-۶-۴ فهرست ارسال افزاره

فهرست ارسال یک افزاره، ممکن است توسط برخی از میزبان‌ها درخواست شود. در صورتی‌که افزاره دریافت کننده درخواست را مشخص می‌کند، به چنین درخواستی باید پاسخ داده شود.

تراکنش‌های درخواست/پاسخ فهرست ارسال همان‌طور که در بند ۸-۵-۶ شرح داده شده، از بسته‌های یکسانی استفاده می‌کنند، از سوی دیگر از تعامل ساده‌تر نشان داده شده در جدول ۸ استفاده می‌کنند.

جدول۸-پروتکل برای درخواست فهرست ارسال یک افزاره

دستگاه	←→	میزبان IP
صحت درخواست را تائید می‌کند.	→	بسته درخواست فهرست ارسال را می‌فرستد.
در حالت رد کردن،ACK-DEVICE-REFUSED یا	←	انجام یافته
بسته فهرست ارسال را می‌فرستد.	←	انجام یافته

۸-۶-۵ فهرست عضویت کانال

ممکن است فهرست عضویت کانال یک افزاره، توسط برخی از میزبان‌ها درخواست شود. در صورتی‌که آن افزاره، دریافت کننده درخواست را مشخص می‌کند، به چنین درخواستی باید پاسخ داده شود.

تراکنش‌های درخواست/پاسخ فهرست عضویت کانال افزاره، همان‌طور که در بند ۸-۵-۵ شرح داده شد، از بسته‌های مشابهی استفاده می‌کنند، از سوی دیگر از تعامل ساده‌تر نشان داده شده در جدول ۹ استفاده می‌کنند.

جدول ۹- پروتکل برای درخواست تعریف کانال یک افزاره

افزاره	⟷	میزبان IP
درستی درخواست را تائید می‌کند	→	بسته درخواست عضویت کانال را ارسال می‌کند
در حالت رد کردن، ACK-DEVICE- یا REFUSED	←	انجام یافته
بسته عضویت کانال را ارسال می‌کند	←	انجام یافته

۸-۶-۶ اطلاعات مسیریابی کانال

اطلاعات مسیریابی کانال یک افزاره، ممکن است توسط برخی از میزبان‌ها درخواست شود. اگر چنین پیامی نشان دهد که افزاره در حال دریافت درخواست است، باید به این پیام پاسخ داد.

تراکنش‌های درخواست/پاسخ پیکربندی افزاره، همان‌طور که در بند ۸-۵-۷ شرح داده شد، از بسته‌های مشابهی استفاده می‌کنند، از سوی دیگر از تعامل ساده‌تر نشان داده شده در جدول ۱۰ استفاده می‌کنند.

جدول ۱۰- پروتکل برای درخواست اطلاعات مسیریابی کانال یک دستگاه

افزاره	⟷	میزبان IP
درستی درخواست را تائید می‌کند.	→	بسته ی درخواست مسیریابی کانال را ارسال می‌کند.
در حالت رد کردن، ACK-DEVICE-REFUSED یا	←	انجام یافته
بسته مسیریابی کانال را ارسال می‌کند.	←	انجام یافته

۸-۷ پیام‌های مختص فروشنده

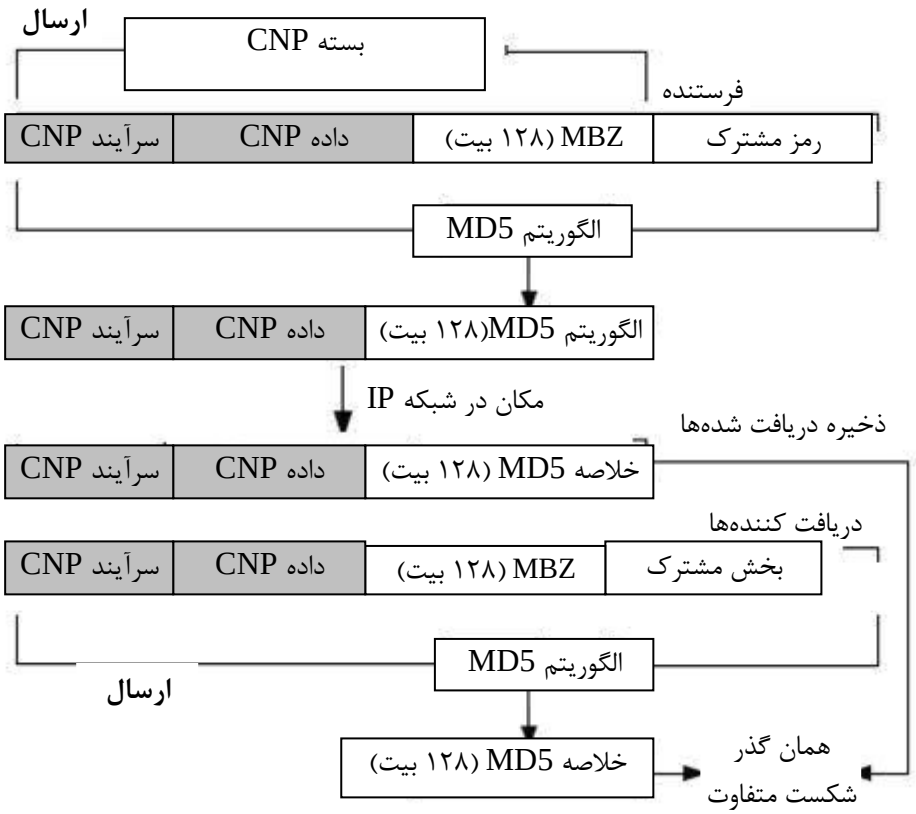
کد فروشنده در سرآیند عمومی بسته، بسته‌های مختص فروشنده را ممکن می‌سازد. این مقدار برای تمامی بسته‌های استاندارد تعریف شده، مطابق با این مشخصه، صفر است. بسته‌های مختص فروشنده توسط کد فروشنده (مقدار بزرگتر از صفر) شناسایی می‌شوند.

یک کد منحصر به‌فرد نوع بسته، به هر تابع توضیح داده شده در بند ۹-۱ اختصاص می‌یابد. کدهای استاندارد نوع بسته‌ای که در این مشخصه تعریف شده‌اند، در بازه 0x00 تا 0x7F می‌باشند. بسته‌های مختص فروشنده که اطلاعات را مانند قالب تابع استاندارد تعریف شده در این مشخصه حمل می‌کنند، می‌توانند از کد نوع بسته یکسان با آن تابع استاندارد استفاده کنند. اما کد فروشنده باید شناسه منحصربه‌فرد برای آن فروشنده

باشد. بسته‌های مختص فروشنده‌ای که با توابع استاندارد موجود تعریف شده در این مشخصه رابطه‌ای ندارند، باید از یک کد نوع بسته در محدوده 0x80 تا 0xFF استفاده کنند.
بسته‌های مختص فروشنده‌ای که توسط افزاره‌هایی دریافت می‌شوند که ترکیب کد فروشنده/نوع بسته را درک نمی‌کنند، باید حذف شوند.

۸-۸ تصدیق بسته‌های CNP

امنیت در افزاره‌های CNP/IP اختیاری است. اگر بیت امنیت در فیلد پرچم‌های پروتکل‌های سرآیند CNP/IP، مقداردهی شود (به بند ۹-۲، سرآیند عمومی CNP/IP مراجعه کنید) در آن‌صورت طرح تصدیق زیر باید به‌صورت شرح داده شده در این بند پیاده سازی شود.
سطح امنیت شرح داده شده در این بند، تصدیق شده است. پیام‌های ارسال شده با استفاده از طرح شرح داده شده در این‌جا، به‌عنوان پیام‌های رسیده از منبع قابل اطمینان، تصدیق شده‌اند.
اطلاعات داخل پیام‌ها رمزگذاری نمی‌شوند و از بازرسی پنهان نمی‌مانند. این طرح تضمین می‌کند که فرستنده، بسته‌ها را با استفاده از رمز معتبر اشتراکی تشکیل داده و آن بسته پس از ارسال دستکاری نشده است. برای اطلاعات بیشتر در مورد این طرح، می‌توانید به "الگوریتم پیام- خلاصه[1] MD5" مراجعه کرده و RFC1321 را مشاهده کنید.



شکل ۴- رمز گذاری و رمزگشایی بسته‌های تصدیق CNP

1- Message -Digest

شکل۴، روال رمزگذاری و رمزگشایی بسته‌هایی را نشان می‌دهد که در آن‌ها بیت امنیت در سرآیند CNP، مقداردهی شده است.
قبل از انتقال یک پیام امن، فرستنده یک رمز اشتراکی به پیام اضافه می‌کند که در زیر نشان داده شده است. "رمز اشتراکی" باید مقداری را نشان دهد که حداقل شامل ۱۲۸ درجه آزادی است. به‌عنوان مثال، یک آرایه ۱۶ بایتی که تمامی بیت‌ها برای انتخاب، موجود هستند یا یک رشته ۲۲ بایتی که ۶ بیت در هر بایت موجود هستند، که هر دو مثال حداقل نیاز برای یک "رمز اشتراکی"CNP را برآورده می‌سازند. با این حال "رمز اشتراکی" CNP ۱۲۸ درجه آزادی محدود نشده است و می‌تواند بیشتر باشد.
نیازهای دیگر "رمز اشتراکی" عبارتند از:
-"رمز اشتراکی" نباید به‌صورت باز در شبکه انتقال یابد.
-افزاره‌های CNP باید به ابزارهای امنیت دستی، اجازه تنظیم و به‌روزرسانی رمزهای افزاره را دهند.
-اگر و تنها اگر تصدیق در پیاده‌سازی افزاره ارائه شود، یک افزاره CNP باید حداقل یک "رمز اشتراکی" واحد که می‌تواند برای تائید درستی درخواست‌ها استفاده شود، فراهم کند.
-تولیدکنندگان به‌صورت اختیاری می‌توانند در ابتدا محصولات را با یک "رمز اشتراکی" پیش فرض تولید کنند که این رمز می تواند بعداً با استفاده از پیام‌های امن شبکه، به‌روز رسانی شود.
سپس خلاصه‌ای از بسته با به‌کاربردن الگوریتم خلاصه-پیام MD5 (RFC 1321 را مشاهده کنید)، برای کامل کردن بسته CNP/IP به‌علاوه "رمز اشتراکی" تولید می‌شود.
خلاصه MD5 تولید شده در فیلد کلیدی MBZ درج می‌شود و بسته بدون مخفی‌کاری به شبکه منتقل می‌شود.
یک افزاره گیرنده، روال مشابهی را روی بسته دریافتی اجرا می‌کند.
الف - خلاصه دریافتی را ذخیره می کند و فیلد خلاصه را باصفر جایگزین می‌کند؛
ب- خلاصه‌ای از بسته را با "رمز اشتراکی" خودش اجرا می‌کند؛
پ- خلاصه دریافتی را با خلاصه جدیدی که آن تولید کرده است، مقایسه می‌کند؛
ت- یکسان بودن خلاصه‌های MD5، درستی بسته‌ها را نشان می‌دهد؛
ث- بسته‌های تصدیق نشده باید حذف شوند و ممکن است توسط افزاره CNP ثبت شوند.

۹ فرمت‌های بسته

۹-۱ انواع بسته

این بند، شرح مفصلی از محتواها و فرمت‌های بسته CNP/IP را ارائه می‌دهد. خواننده برای پی بردن به اینکه چگونه بسته‌های متنوع شرح داده شده در این بند به‌کار می‌روند، باید به بند ۶ مراجعه کند.
تمامی بسته‌های CNP/IP از یک سرآیند به همراه یک بخش داده، تشکیل شده‌اند. فرمت سرآیند برای تمامی بسته‌های CNP/IP، یکسان است. بخش داده وابسته به نوع بسته CNP/IP است. همه فیلدها در شبکه به‌ترتیب بایت هستند به جز مواردی که ذکر شده است.

جدول ۱۱ یک مرجع متقابل برای تمامی بسته‌های استفاده شده در سامانه است. علامت‌های اختصاری زیر برای نشان دادن مجموعه‌های متنوع داده، استفاده می‌شوند.

DC- پیکربندی افزاره؛

CM- فهرست عضویت کانال؛

SL- فهرست ارسال؛

CR-مسیریابی کانال.

جدول۱۱-مرجع متقابل نوع پیام

نوع بسته	فرمت (بند۹)	تراکنش‌های استفاده شده (بند ۸)	کد
بسته داده	۹-۴	مبادله بسته داده CNP (۸-۴)	0x01
درخواست پیکربندی بسته	۹-۸	درخواست DC به سرویس دهنده (۸-۵-۴) درخواست DC به افزاره (۸-۶-۳)	0x63
ثبت افزاره	۹-۵	ثبت افزاره با سرویس دهنده (۸-۵-۴)	0x03
پیکربندی افزاره	۹-۵	پاسخ DC از سرویس دهنده (۸-۵-۴) پاسخ DC از افزاره (۸-۵-۳) به‌روزرسانی ناخواسته سرویس دهنده پیکربندی افزاره(۸-۵-۱-۲)	0x71
درخواست عضویت کانال	۹-۸	درخواست CM به سرویس دهنده (۸-۵-۵) درخواست CMبه افزاره (۸-۶-۵)	0x64
عضویت کانال	۹-۶	پاسخ CM از سرویس دهنده (۸-۵-۵) پاسخ CM از افزاره (۸-۶-۵)	0x04
ارسال درخواست فهرست	۹-۸	درخواست SL به سرویس دهنده (۸-۵-۶) درخواست SL به افزاره (۸-۶-۴)	0x66
فهرست ارسال	۹-۱۰	پاسخ SL از سرویس دهنده(۸-۵-۶) پاسخ SL به افزاره (۸-۶-۴)	0x06
درخواست مسیریابی کانال	۹-۸	درخواست CR به سرویس دهنده (۸-۵-۷) درخواست CR به افزاره(۸-۶-۶)	0x68
مسیریابی کانال	۹-۷	پاسخ CR از سرویس دهنده (۸-۵-۷) پاسخ CR به افزاره (۸-۶-۶)	0x08
تصدیق کردن	۹-۹	۸-۵-۳	0x07
قطعه بندی کردن	۹-۳	تمامی تراکنش‌های SL،CM وCR در ۸-۵ و۸-۶	0x7f
درخواست وضعیت/سلامت/آمار	۹-۸	درخواست وضعیت به افزاره(۸-۶-۲)	0x60
پاسخ وضعیت/سلامت/آمار	۹-۱۱	پاسخ وضعیت از افزاره (۸-۶-۲)	0x70

۹-۲ سرآیند مشترک CNP/IP

تمامی افزاره‌های CNP/IP دارای سرآیند مشترک نشان داده شده در جدول ۱۲ می‌باشند.

جدول ۱۲- قالب سرآیند مشترک بسته

بایت ۳	بایت۲	بایت۱	بایت۰
نوع بسته	نسخه	طول بسته داده	
کد فروشنده(۱۶بیت)	پرچم‌های پروتکل	اندازه سرآیند توسعه‌یافته	
شناسه جلسه			
شماره ترتیب			
نشان زمانی			

این سرآیند در تمامی بسته‌ها ارائه شده است. موارد زیر، توضیحی درباره هر فیلد است.

۹-۲-۱ نسخه

این مورد، شماره نسخه بسته می‌باشد. چنین فرض می‌شود که بسته‌های دارای شماره نسخه یکسان، همیشه می‌توانند تجزیه شوند. اگر گرهی، سرآیندی با شماره نسخه‌ای که قابل فهم نیست را دریافت کند، آن گره بسته را بدون پردازش بیشتر محتواهای بسته حذف خواهد کرد. شماره نسخه فعلی، 0x01 می‌باشد. شماره نسخه، ۵ بیت پایین‌تر از این بایت است. ۳ بیت بالا به‌صورت زیر تعریف می‌شوند:

بیت۵-۶: رزرو شده، MBZ

بیت ۷: بسته مشتری خاص، بسته‌ای از این بیت تبعیت می‌کند که شامل کد مشتری دیگری است و بدین معنی است که با این بسته پردازش می‌شود.

۹-۲-۲ پرچم‌های پروتکل

این‌ها پرچم‌های بیتی هستند که برای نشان دادن جنبه‌های متفاوت پروتکل تونل‌زنی به‌کار می‌روند. بیت-های زیر مورد استفاده قرار می‌گیرند:

بیت۷: رزرو شده، MBZ

بیت۶: رزرو شده،MBZ

بیت ۵: بیت امنیت، اگر مقدار این بیت ۱ باشد، این بسته شامل اطلاعات تصدیق شرح داده شده در بند ۸-۸ می‌باشد.

بیت‌های ۴-۰: کد پروتکل: این فیلد، پروتکلی که در درون بسته، تونل‌زنی می‌شود را مشخص می‌کند. پروتکل‌های زیر، مورد پشتیبانی قرار می‌گیرند:

0x00-EIA-709
0x01-EIA-600
0x02-CNP

۹-۲-۳ کد فروشنده

این فیلد برای نشان دادن کدهای خاص فروشنده استفاده می شود. مقدار 0x0000 نشان می‌دهد که این بسته، یک بسته سازگار مشخص شده در این سند است. هر مقداری غیر از 0x0000 نشان می‌دهد که این بسته، یک بسته مختص فروشنده است. برای اطلاعات بیشتر در مورد بسته‌های مختص فروشنده، بند ۸-۷ را مشاهده کنید.

هر کد فروشنده توسط انجمن اختصاصی صنعت، تخصیص خواهد یافت و مدیریت خواهد شد. کدهای فروشنده، لازم است فقط داخل یک پروتکل خاص، منحصر به‌فرد باشند.

۹-۲-۴ نوع بسته

این بخش، نوع بسته را تعیین می‌کند. کدهای نوع بسته تعریف شده در این مشخصه، در بازه 0x00 تا 0x7F هستند. بسته‌های مختص فروشنده که اطلاعات را مانند قالب تابع استاندارد تعریف‌شده در این مشخصه حمل می‌کند، می‌توانند کد نوع بسته یکسانی با آن تابع استاندارد را به‌کار ببرند، اما کد فروشنده باید شناسه منحصربه‌فرد آن فروشنده باشد. بسته‌های مختص فروشنده‌ای که رابطه‌ای با توابع استاندارد موجود تعریف شده در این مشخصه ندارند، باید از یک کد نوع بسته در بازه 0x80 تا 0xFF استفاده کنند. برای اطلاعات بیشتر در مورد پیام‌های فروشنده خاص، بخش ۸-۷ را مشاهده کنید.

۹-۲-۵ طول بسته داده

این فیلد، طول بسته برحسب بایت است که شامل بایت‌ها در سرآیند عمومی بسته نیز می‌باشد. مقدار این فیلد اضافه شده به آدرس نسخه، آفستی از فیلد نسخه بعدی از بسته بعدی می‌باشد، در صورتی‌که بیش از یکی، در قاب جاری وجود داشته باشد.

۹-۲-۶ اندازه سرآیند تعمیم‌یافته

این فیلد، طول سرآیند بسته به تعداد چهار بایت رکورد افزون بر اندازه سرآیند استاندارد می‌باشد. اگر هیچ تعمیمی به سرآیند مشترک وجود نداشته باشد، این فیلد صفر می‌باشد. همچنین این اشاره دارد به اینکه سرآیندها باید مضربی از چهاربایت باشند و باید روی مرزهای چهار بایت ردیف شوند. این فیلد اجازه تجدیدنظر این پروتکل را در آینده می‌دهد.

لیکن اجازه تجدیدنظر، در صورت سازگاری رو به عقب می‌باشد. تمامی بسته‌های تولید شده‌ای که مربوط به نسخه ۱ این پروتکل می‌باشند، باید مقدار اندازه سرآیندشان صفر باشد.

۹-۲-۷ شناسه جلسه

شناسه جلسه در همکاری با شماره ترتیب کار می‌کند تا تضمین کند که بسته‌ها به ترتیبی دریافت می‌شوند که روی یک کانال UDP استاندارد ارسال شده‌اند. هر گره CNP/IP، یک شناسه جلسه انتخاب‌شده را به‌صورت تصادفی نگه می‌دارد. اگر گره CNP/IP، راه اندازی مجدد، یا تنظیم و یا غیره شود و شماره‌های ترتیبی را به‌کار رفته را فراموش کند، گره با یک شناسه جلسه جدید، پیام‌های بعدی‌اش را به هر مقصد

ارسال خواهد کرد. همچنین شناسه جلسه جدید به‌صورت تصادفی انتخاب می‌شود با این محدودیت که با شناسه جلسه‌ای که توسط گره، قبل از وقوع راه اندازی مجدد/ تنظیم مجدد استفاده می‌شد، یکسان نیست.
زمانی‌که گره از یک منبع، پیامی دریافت می‌کند که شناسه جلسه‌ای متفاوت از شناسه‌ای دارد که در پیام قبلی آن منبع استفاده می‌شد، گره چنین فرض می‌کند که پیام ضمیمه، مرتب است. به‌علاوه گیرنده برای حفظ ترتیب پیام‌های بعدی، جفت عدد شناسه جلسه/ترتیب موجود در پیام جدید را به خاطر می‌سپارد.

۹-۲-۸ شماره ترتیب

شماره ترتیب برای بسته فعلی است. برای جزئیات الگوریتم، بندهای ۸-۴-۲ تا ۸-۴-۴ را مشاهده کنید.

۹-۲-۹ نشان زمانی

نشان زمانی برای بسته فعلی، در صورتی‌که هیچ نشان زمانی به بسته تخصیص نشده باشد، صفر است. این نشان زمانی، زمانی را نشان می‌دهد که این بسته روی کانال IP ایجاد شده است.
فیلد نشان زمانی همیشه برای بسته‌های پیکربندی صفر است. این فیلد فقط برای بسته‌های داده معتبر است.

۹-۳ بسته داده

این بسته برای محصور کردن سایر بسته‌های CNP/IP که اندازه آنها بیش از اندازه یک نمودار داده واحد UDP است، استفاده می‌شود.
بسته قطعه، قالب ارائه شده در جدول ۱۳ را دارد.

جدول ۱۳-فرمت بسته قطعه

بایت۳	بایت۲	بایت۱	بایت۰
سرآیند عمومی بسته			
تاریخ/زمان			
شناسه قطعه	شناسه درخواست		پرچم‌ها
بایت‌های بار	بایت‌های بار	بایت‌های بار	بایت‌های بار
بایت‌های بار	بایت‌های بار	بایت‌های بار	بایت‌های بار
بایت‌های بار	بایت‌های بار	بایت‌های بار	بایت‌های بار
بایت‌های بار	بایت‌های بار	بایت‌های بار	بایت‌های بار
بایت‌های بار	بایت‌های بار	بایت‌های بار	بایت‌های بار

شرح تمامی فیلدها در این بسته، در زیر آمده است.

۹-۳-۱ نوع بسته

به بند ۹-۱ مراجعه کنید.

۹-۳-۲ تاریخ/زمان

برای جزئیات قالب تاریخ زمان، بند ۹-۵ را مشاهده کنید. فیلد تاریخ/زمان از تاریخ/زمان بسته محصور شده، کپی گرفته شده است. تمامی قطعات برای بسته محصور شده‌ای که با تمامی عناصرهای داده مرتبط هستند، تاریخ/زمان یکسانی دارند. اگر هر یک از داده‌های تشکیل شده از بسته محصور شده در طول انتقال قطعه-

بندی آن بسته تغییر کنند، در آن صورت تاریخ/زمان در بسته‌های قطعه تحت متأثر، تغییر خواهد کرد تا داده جدید مقداردهی شود.

۹-۳-۳ پرچم‌ها

بیت ۷: معتبر؛ مقداردهی این بیت نشان می‌دهد که داده معتبر، دربسته‌ای که شناسه قطعه موردنظر را نشان می‌دهد وجود دارد.

بیت ۶: نهایی؛ مقداردهی این بیت نشان می‌دهد که هیچ داده‌ای برای مقادیر شناسه قطعه بزرگ‌تر از آن مقدار برگشتی در این بسته، وجود ندارد.

بیت‌های ۵ الی ۰: برای استفاده‌های آتی ذخیره می‌شوند.

۹-۳-۴ شناسه درخواست

کپی از مقدار شناسه درخواست از پیام درخواستی، که موجب ایجاد این پاسخ شده است.

۹-۳-۵ شناسه قطعه

کپی از مقدار شناسه قطعه از پیام درخواستی که موجب ایجاد این پاسخ شده است. این شناسه داده‌ای است که در این پاسخ موجود است.

۹-۴ بسته‌های داده CNP

بسته‌های داده CNP/IP، فرمت قالب ارائه شده در جدول ۱۴ را دارند.

جدول ۱۴- فرمت بسته داده

بسته داده CNP	سرآیند عمومی CNP/IP

۹-۴-۱ سرآیند CNP/IP

بند ۹-۲ را مشاهده کنید.

۹-۴-۲ بسته داده CNP

این بسته "PDU" کامل شرح داده شده در بند ۶-۴ از استاندارد CNP است. تعداد بایت‌های تشکیل دهنده PDU برابر است با "اندازه بسته منهای اندازه سرآیند".

توجه کنید همان‌طور که در بند ۸-۴-۲ شرح داده شد، بسته‌های داده CNP باید در همان ترتیبی که ایجاد شده‌اند، پردازش شوند. بنابراین بسته‌های IPای که خارج از ترتیب رسیده باشند، باید قبل از این‌که به پشته پروتکل CNP تحویل داده شوند، دوباره مرتب شوند. اگر مرتب‌سازی مجدد پشتیبانی نشده است، بسته‌هایی که خارج از ترتیب رسیده‌اند، باید نادیده گرفته شوند.

۹-۵ بسته‌های پیکربندی/ ثبت افزاره CNP

اگر از یک سرویس دهنده پیکربندی استفاده شود، افزاره‌های CNP/IP، بسته ثبت افزاره را به سرویس دهنده ارسال می‌کنند تا وجود آن‌ها را به اطلاع برسانند. پس از آن سرویس دهنده با بسته پیکربندی افزاره پاسخ می‌دهد. این بسته ثبت توسط سرویس دهنده استفاده خواهد شد تا هم افزاره CNP/IP را پیکربندی کند و هم احتمالاً فهرستی از تمامی افزاره‌های CNP/IP روی کانال IP را نگهداری کند.

بسته پیکربندی افزاره تنها بسته‌ای است که ناخواسته توسط سرویس دهنده پیکربندی به یک افزاره ارسال می‌شود.

بسته‌های ثبت افزاره CNP/IP و پیکربندی افزاره دارای فرمت نشان داده شده در جدول ۱۵ می‌باشند.

جدول ۱۵- فرمت بسته پیکربندی/ثبت افزاره

<table>
<tr><th>بایت۰</th><th>بایت۱</th><th>بایت۲</th><th>بایت۳</th></tr>
<tr><td colspan="4">سرآیند عمومی بسته</td></tr>
<tr><td colspan="4">تاریخ زمان</td></tr>
<tr><td colspan="2">پرچم‌های IP</td><td>نوع مسیریاب</td><td>پرچم‌های CNP</td><td>نوع گره</td></tr>
<tr><td colspan="2">تعداد آدرس MAC [M]</td><td>MBZ</td><td colspan="2">مهلت زمانی کانال</td></tr>
<tr><td colspan="2">جمع کل بایت‌های شناسه منحصربه‌فرد[U]</td><td colspan="2">پورت تک پخشی IP</td></tr>
<tr><td colspan="4">آدرس تک پخشی IP</td></tr>
<tr><td colspan="4">تاریخ زمان عضویت کانال</td></tr>
<tr><td colspan="4">تاریخ زمان فهرست ارسال</td></tr>
<tr><td colspan="4">آدرس IP سرویس دهنده پیکربندی</td></tr>
<tr><td colspan="4">آدرس IP سرویس دهنده اصلی زمان</td></tr>
<tr><td colspan="4">آدرس IP سرویس دهنده فرعی زمان</td></tr>
<tr><td colspan="2">پورت IP سرویس دهنده پیکربندی</td><td colspan="2">پورت IP سرویس دهنده اصلی زمان</td></tr>
<tr><td colspan="2">پورت IPسرویس دهنده فرعی زمان</td><td colspan="2">MBZ</td></tr>
<tr><td colspan="4">آدرسIP MC [0]</td></tr>
<tr><td colspan="2">پورت چند پخشی IP [0]</td><td colspan="2">MBZ[0]</td></tr>
<tr><td colspan="4">آدرسIP MC [M-1]</td></tr>
<tr><td colspan="2">پورت چند پخشی IP [M-1]</td><td colspan="2">MBZ[0]</td></tr>
<tr><td>شناسه منحصربه‌فرد [0]</td><td>شناسه منحصربه‌فرد [1]</td><td>شناسه منحصربه-فرد [2]</td><td>شناسه منحصربه‌فرد [3]</td></tr>
<tr><td>شناسه منحصربه‌فرد [4]</td><td>شناسه منحصربه‌فرد [5]</td><td>شناسه منحصربه-فرد [6]</td><td>شناسه منحصربه‌فرد [U-1]</td></tr>
<tr><td>طول نام[N]</td><td>نام[0]</td><td>نام[1]</td><td>نام[2]</td></tr>
<tr><td>نام[3]</td><td>نام[4]</td><td>نام[5]</td><td>...[6]</td></tr>
</table>

یادآوری- کروشه‌ها حاوی اندیس یک فیلد در آرایه می‌باشند.

۹-۵-۱ نوع بسته

به بند ۹-۱ مراجعه کنید.

۹-۵-۲ تاریخ/زمان

این بخش، تاریخ و زمانی است که بر مبنای آن، داده معتبر است. نسخه‌های جدیدتر یا قدیمی‌تر این داده می‌توانند با دقت ۱ ثانیه، با جستجو در این فیلد تعیین شوند. این فیلد محدود شده است طوری‌که اگر بیش از یک نسخه داده در ثانیه یکسانی ایجاد شوند، هر یک از آن‌ها دارای مقادیر منحصربه‌فرد و فزاینده برای این فیلد هستند.

در صورتی‌که شبکه، SNTP یا NTP را پشتیبانی کند، مقدار تاریخ/زمان، بخشی ثانیه‌های تاریخ زمان NTP از RFC1305 خواهد بود. این تعداد ثانیه‌ها پس از ۱ ژانویه ۱۹۰۰ می‌باشد. این زمان در سال ۲۰۳۶ به پایان خواهد رسید. برای جزئیات بیشتر، بند ۳ از RFC 2030 را مشاهده کنید.

اگر شبکه، پروتکل SNTP یا NTP راپشتیبانی نکند، ممکن است تاریخ/زمان یک مقدار صحیح کوچک بدون صفر باشد آشکار است که این تاریخ‌ها در اوایل دهه ۱۹۰۰، منطبق با ساعت معمول نیستند، اما همان‌طور که پیشتر ذکر شد، ملزم به پیروی از شرایط یگانگی برای هر نوع زمان هستند. به‌عبارت دیگر این مقادیر که توسط چنین افزاره‌ای منتشر می‌شوند، هرگز داده‌های متفاوت را شامل نشده یا در مورد آنها تکرار نمی‌شوند.

۹-۵-۳ پرچم‌های IP

مقادیر ماسک عبارتند از:

0x01-UDP پشتیبانی شده

0x02-TCP پشتیبانی شده

0x04-چند پخشی پشتیبانی شده

۹-۵-۴ نوع مسیریاب CNP

در حالت کلی که نوع گره افزاره، یک مسیریاب است، این فیلد به حالت‌های عمل زیر دلالت می‌کند:

0x00: پیکربندی: برای هر دامنه مشخص شده، اگر مقدار بیت subnet mask صفر باشد، گره/ زیرشبکه، پیام‌های شناسه منحصربه‌فرد مستقیم زیرشبکه و چند پخشی زیرشبکه (زیرشبکه غیر صفر) را به افزاره ارسال می‌کند. در حالتی که زیرشبکه در هر یک از پیام‌های بالا ۰ است، اگر بیت ۰ زیرشبکه به ۱ مقداردهی شود، پیام باید ارسال گردد. برای پیام‌های گروه، در صورتی ارسال می‌کند که بیت در group mask، مقداردهی شده باشد.

0x01: یادگیری: برای هر دامنه مشخص شده، اگر مقدار بیت subnet mask صفر باشد، گره/ زیرشبکه، پیامهای شناسه منحصربه‌فرد مستقیم زیرشبکه و چند پخشی زیر شبکه (زیر شبکه غیر صفر) را به افزاره ارسال می‌کند. در حالتی که زیرشبکه در هر یک از پیام‌های بالا ۰ است، اگر بیت ۰ زیر شبکه در ماسک به ۱ مقداردهی شود، پیام باید ارسال گردد. بیت‌های subnet mask برای زیر شبکه‌هایی مقداردهی می‌شوند که روی "سمت دیگر" هستند یا می‌توانند باشند و برای زیرشبکه‌هایی که معروف به بودن روی "این سمت" هستند، مقداردهی نمی‌شوند. پیام‌های گروه‌ها همیشه ارسال می‌شوند (بیت‌های گروه نادیده گرفته می‌شوند).

0x02: پل: برای هر دامنه مشخص شده، تمامی پیام‌ها را ارسال می‌کند (بیت‌های زیرشبکه گره نادیده گرفته می‌شوند.)
0x03: تکرار کننده: همه پیام‌ها را ارسال می‌کند (دامنه/ زیر شبکه/اطلاعات گروه نادیده گرفته می‌شوند)

۹-۵-۵ پرچم‌های CNP

مقادیر ماسک عبارتند از:
0x01: WANTS-ALL-BROADCAST. برای شرح این تابع، بند ۸-۵-۷-۳ را مشاهده کنید.
0x02: امنیت شرح داده شده در بند ۸-۸ را پشتیبانی می‌کند.

۹-۵-۶ نوع گره

نوع افزاره. رفتار بعضی از این انواع نامشخص باقی می‌ماند.
0x01: کانال غیر IP به مسیریاب کانال IP
0x02: گره کانال IP
0x03: پراکسی کانال IP
0x04: کانال IP به مسیریاب کانال

۹-۵-۷ تعداد آدرس mc

تعداد آدرس‌های IP چندپخشی و پورت‌ها

۹-۵-۸ مهلت زمانی کانال

مقدار برحسب میلی ثانیه مهلت زمانی در بندهای ۸-۴-۴ و ۸-۴-۲ بحث شده است. مقادیر ۱ میلی ثانیه تا ۱۵۰۰ میلی ثانیه معتبر هستند. با این حال، این پارامتر می‌تواند کمتر از ۱ میلی ثانیه نیز تعیین شود. به دلیل ماهیت SNTP، این سطح دقت را نمی‌توان تضمین کرد و انتظار آن را نیز نباید داشت.
سطح عملی‌تر حداقل دقت، در بازه ۱۰ میلی ثانیه تا ۱۶ میلی ثانیه می‌باشد.

۹-۵-۹ تعداد کل بایت‌های شناسه منحصربه‌فرد

از تعداد کل بایت‌های شناسه‌های منحصربه‌فرد تبعیت می‌شود. اندازه یک شناسه منحصربه‌فرد باید مضربی از ۶ بایت باشد. حداقل باید یک مدخل وجود داشته باشد. اگر افزاره یک گره باشد، شناسه منحصربه‌فرد متناظر با شناسه منحصربه‌فرد تعریف شده در بند ۸- ۱ خواهد بود. یک افزاره مسیریاب می‌تواند حداکثر سه شناسه منحصربه‌فرد داشته باشد، یکی برای هر کناره مسیریاب و یکی برای اهداف پیکربندی. شناسه‌ای که لازم است در این فیلد مشخص شود، شناسه مربوط به کناره مسیریاب است که مستقیماً به کانال CNP/IP مورد نظر وصل شده است.

۹-۵-۱۰ پورت IP تک‌پخشی

شماره پورتی که افزاره CNP/IP، هنگام گوش دادن به پیام‌های IP تک‌پخشی، به کار می‌برد.

۹-۵-۱۱ آدرس IP تک‌پخشی

آدرس IP تک‌پخشی افزاره CNP/IP در ترتیب بایت شبکه. افزاره CNP/IP روی این آدرس، به پیام‌های IP تک‌پخشی وارد شونده گوش خواهد کرد.

۹-۵-۱۲ تاریخ/زمان عضویت کانال

تاریخ/زمان جدیدترین بسته عضویت کانال از سرویس‌دهنده. این تاریخ زمان بدین منظور استفاده می‌شود که تعیین کند هنگامی‌که افزاره، یک بسته ناخواسته پاسخ افزاره از سرویس دهنده دریافت می‌کند، آیا باید یک بسته جدید عضویت کانال از سرویس دهنده پیکربندی درخواست شود. زمانی‌که یک بسته از افزاره به سرویس دهنده ارسال می‌شود، محتوای معنی‌داری ندارد.

۹-۵-۱۳ تاریخ/زمان فهرست ارسال

تاریخ/زمان بسته جدید فهرست ارسال برای این افزاره این تاریخ زمان بدین منظور استفاده می‌شود که تعیین کند هنگامی‌که افزاره، یک بسته ناخواسته پاسخ افزاره از سرویس دهنده دریافت می‌کند، آیا باید یک بسته جدید فهرست ارسال از سرویس دهنده پیکربندی درخواست شود.

۹-۵-۱۴ آدرس IP سرویس‌دهنده پیکربند

آدرس IP سرویس دهنده پیکربندی. یک سرویس دهنده پیکربندی جدید برای این کانال، می‌تواند تنظیمات بسته پیکربندی افزاره را به آدرس IP و پورت سرویس‌دهنده پیکربندی و سرویس‌دهنده زمان ارسال کند.

۹-۵-۱۵ آدرس IP سرویس دهنده اصلی/ فرعی

آدرس IP سرویس دهنده‌های NTP زمان. همان‌طور که در بالا بحث شد، این‌ها توسط سرویس دهنده پیکربندی تعیین می‌شوند. در صورتی‌که افزاره بتواند به سرویس دهنده اصلی دسترسی پیدا کند، این سرویس دهنده را به کار می‌برد، در غیر این صورت از سرویس دهنده فرعی استفاده می‌کند. این فرایند تضمین می‌کند که افزاره‌ها از یک سرویس‌دهنده قابل پیش‌بینی استفاده خواهند کرد.

۹-۵-۱۶ پورت IP سرویس‌دهنده پیکربند

شماره پورت IP برای سرویس‌دهنده پیکربندی است. همانند بالا تنظیم شود.

۹-۵-۱۷ پورت‌های IP سرویس دهنده اصلی/ فرعی زمان

شماره‌های پورت IP برای سرویس‌دهنده‌های زمان می‌باشد. باید پورت استاندارد NTP (۱۲۳) را به کار برد، مگر این‌که شرایط کاهش‌دهنده مانع این امر شود.

۹-۵-۱۸ آدرس IP چندپخشی

این بند، معرف آدرس IP چندپخشی افزاره CNP/IP می‌باشد. تعداد McAddress، در صورت پشتیبانی نشدن صفر است. افزاره CNP/IP به بسته‌های IP چندپخشی وارد شده، بر روی این آدرس توجه خواهد کرد. ۸ بایت آدرس، پورت، MBZ، به تعداد دفعات McAddress تکرار می‌شوند.

۹-۵-۱۹ پورت IP چندپخشی

شماره پورت افزاره CNP/IP هنگام توجه به بسته‌های IP چند پخشی است.

۹-۵-۲۰ شناسه‌های منحصربه‌فرد

شناسه‌های منحصربه‌فرد با هم بسته‌بندی می‌شوند، هر یک شامل ۶ بایت هستند و در ترتیب بایت شبکه CNP ارائه می‌شوند.

۹-۵-۲۱ طول نام

از طول نام پیروی می‌شود. نام باید به صفر ختم شود و در محاسبه طول نام، صفر نیز در نظر گرفته می‌شود.

۹-۵-۲۲ نام

متغیری است که بدون در نظر گرفتن خاتمه‌دهنده صفر، طول آن حداکثر ۱۲۸ بایت می‌باشد. این متغیر مربوط به افزاره است. نیازی نیست که نام مابین افزاره‌ها منحصربه‌فرد باشد.

۹-۶ بسته عضویت کانال

این بسته توسط یک سرویس‌دهنده پیکربندی برای آگاه کردن یک افزاره از عضویت کانال به کار می‌رود. برای سادگی، این پیام‌ها شامل آدرس IP و شماره پورت تمامی افزاره‌های CNP/IP در کانال است. به محض این‌که افزاره، فهرستی از آدرس‌های IP را داشته باشد، می‌تواند یک پیام درخواست به هر افزاره در فهرست ارسال کند تا پیکربندی کامل آن را درخواست کند.
بسته عضویت کانال، قالب ارائه شده در جدول ۱۶ را دارد.

جدول ۱۶- قالب بسته عضویت کانال

<table>
<tr><th>بایت۰</th><th>بایت۱</th><th>بایت۲</th><th>بایت۳</th></tr>
<tr><td colspan="4">سرآیند عمومی بسته</td></tr>
<tr><td colspan="4">تاریخ زمان</td></tr>
<tr><td colspan="4">تاریخ زمان فهرست ارسال</td></tr>
<tr><td colspan="4">MBZ</td></tr>
<tr><td colspan="2">اندازه فهرست</td><td colspan="2">MBZ</td></tr>
<tr><td colspan="4">فیلدهای زیر یک‌بار برای هر افزاره CNP/IP تکرار می‌شوند</td></tr>
<tr><td colspan="4">آدرس IP تک پخشی</td></tr>
<tr><td colspan="2">پورت IPتک پخشی</td><td colspan="2">MBZ</td></tr>
<tr><td colspan="4">تاریخ زمان بسته مسیریابی کانال برای افزاره</td></tr>
</table>

در زیر شرحی از تمامی فیلدهای موجود در این بسته آمده است.

۹-۶-۱ تاریخ/زمان

تاریخ/زمان ایجاد بسته عضویت کانال برای این کانال است. بخش ۹-۴ را مشاهده کنید.

۹-۶-۲ تاریخ/زمان فهرست ارسال

تاریخ/زمان ایجاد بسته فهرست ارسال برای این افزاره است. بخش ۹-۴ را مشاهده کنید.

۹-۶-۳ MBZ

تعداد افزاره‌ها در جدول افزاره‌های CNP/IP می‌باشد.

۹-۶-۴ اندازه فهرست

تعداد افزاره‌هایی که در جدول افزاره‌های CNP/IP هستند.

۹-۶-۵ آدرس IP تک‌پخشی

آدرس IP تک‌پخشی افزاره CNP/IP در ترتیب بایت شبکه است. افزاره CNP/IP روی این آدرس به بسته-های IP تک‌پخشی وارد شده توجه خواهد کرد.

۹-۶-۶ پورت IP تک‌پخشی

شماره پورتی که افزاره CNP/IP، هنگام توجه به پیام‌های IP تک پخشی استفاده می‌کند.

۹-۶-۷ تاریخ/زمان بسته مسیریابی کانال برای افزاره

این، تاریخ/زمان جدیدترین بسته مسیریابی کانال برای افزاره‌ای است که در دسترس سرویس‌دهنده پیکربندی می‌باشد. این تاریخ/زمان بدین منظور به کار می‌رود که تعیین کند آیا باید یک بسته جدید مسیریابی کانال از سرویس‌دهنده پیکربندی درخواست کرد.

۹-۷ بسته مسیریابی کانال

بسته مسیریابی کانال، دارای قالب نشان داده شده در جدول ۱۷ است.

جدول ۱۷- قالب‌های بسته مسیریابی کانال

<table>
<tr><th>بایت۰</th><th>بایت۱</th><th>بایت۲</th><th>بایت۳</th></tr>
<tr><td colspan="4">سرآیند عمومی بسته با نوع بسته (0x08)</td></tr>
<tr><td colspan="4">تاریخ زمان</td></tr>
<tr><td colspan="2">پورت IP چند پخشی</td><td colspan="2">پورت IP تک پخشی</td></tr>
<tr><td colspan="4">آدرس IPMC</td></tr>
<tr><td colspan="4">آدرس IP چند پخشی</td></tr>
<tr><td>پرچم‌های IP</td><td>نوع مسیریاب CNP</td><td>پرچم‌های CNP</td><td>نوع گره</td></tr>
<tr><td colspan="2">تعداد کل بایت‌های شناسه منحصربه‌فرد [U]</td><td colspan="2">تعداد کل بایت‌های دامنه [D]</td></tr>
<tr><td>شناسه منحصربه‌فرد [0]</td><td>شناسه منحصربه‌فرد [1]</td><td>شناسه منحصربه‌فرد [2]</td><td>شناسه منحصربه‌فرد [3]</td></tr>
<tr><td>شناسه منحصربه‌فرد [4]</td><td>شناسه منحصربه‌فرد [5]</td><td>شناسه منحصربه‌فرد [6]</td><td>شناسه منحصربه‌فرد [U-1]</td></tr>
<tr><td colspan="4">برای آدرس هر گره (آدرس‌های گره CNP) فیلدهای زیر تکرار می‌شوند.</td></tr>
<tr><td>شماره زیرشبکه [0]</td><td>شماره گره[0]</td><td colspan="2">شاخص دامنه[0]</td></tr>
<tr><td colspan="2">شاخص شناسه منحصربه‌فرد[0]</td><td>شماره زیر شبکه[1]</td><td>شماره دامنه[1]</td></tr>
<tr><td colspan="2">شاخص دامنه[1]</td><td colspan="2">شاخص شناسه منحصربه‌فرد[1]</td></tr>
<tr><td>شماره زیرشبکه[S-1]</td><td>شماره گره[S-1]</td><td colspan="2">شاخص دامنه [S-1]</td></tr>
<tr><td colspan="2">شاخص شناسه منحصربه‌فرد</td><td>.....</td><td>.....</td></tr>
</table>

ادامه جدول ۱۷

برای هر دامنه (فهرست دامنه CNP)، فیلدهای زیر یک‌بار تکرار می‌شوند			
SubnetMsk[0]	SubnetMsk[1]	SubnetMsk[2]	SubnetMsk[3]
SubnetMsk[4]	SubnetMsk[5]	SubnetMsk[6]	SubnetMsk[7]
...	....	....	....
SubnetMsk[28]	SubnetMsk[29]	SubnetMsk[30]	SubnetMsk[31]
GroupMsk[0]	GroupMsk[1]	GroupMsk[2]	GroupMsk[3]
...	...	...	...
GroupMsk[28]	GroupMsk[29]	GroupMsk[30]	GroupMsk[31]
طول دامنه	MBZ	دامنه[0]	دامنه[1]
دامنه[2]	دامنه[3]	دامنه[4]	دامنه[5]

یادآوری- کروشه‌ها، حاوی اندیس فیلد در یک آرایه هستند.

شرحی از فیلدهای این بسته در زیر آمده است.

۹-۷-۱ تاریخ/زمان

برای شرح این فیلد، بند ۹-۴ را مشاهده کنید.

۹-۷-۲ پورت IP چندپخشی

شماره پورتی که افزاره CNP/IP، هنگام توجه به پیام‌های چندپخشی، در آن مستقر است.

۹-۷-۳ پورت IP تک‌پخشی

شماره پورتی که افزاره CNP/IP، هنگام توجه به پیام‌های تک‌پخشی، استفاده می‌کند.

۹-۷-۴ آدرس IP چندپخشی

آدرس IP چندپخشی افزاره CNP/IP در صورتی‌که پشتیبانی نشود، صفر است. افزاره CNP/IP روی این آدرس به بسته‌های IP چندپخشی وارد شده توجه می‌کند.

۹-۷-۵ آدرس IP تک‌پخشی

آدرس IP تک پخشی افزاره CNP/IP در ترتیب بایت شبکه. افزاره CNP/IP روی این آدرس، به بسته‌های IP تک پخشی وارد شده توجه می‌کند.

۹-۷-۶ پرچم‌های IP

قابلیت IP پشتیبانی شده را نشان می‌دهد. بخش ۹-۵ را مشاهده کنید.

۹-۷-۷ نوع مسیریاب CNP

در صورتی‌که نوع گره یک مسیریاب است، نوع مسیریاب را نشان می‌دهد. بند ۹-۵ را مشاهده کنید.

۹-۷-۸ پرچم‌های CNP

ماسک پرچم‌های CNP است. بند ۹-۵ را مشاهده کنید.

۹-۷-۹ نوع گره

نوع افزاره را نشان می‌دهد. بند ۹-۵ را مشاهده کنید.

۹-۷-۱۰ تعداد کل بایت‌های شناسه منحصربه‌فرد

تعداد بایت‌های شناسه‌های منحصربه‌فردی که پیگیری می‌شود. باید اندازه یک شناسه منحصربه‌فرد مضربی از ۶ بایت باشد. مقدار صفر نیز مجاز است.

۹-۷-۱۱ تعداد کل بایت‌های گره زیرشبکه

تعدا کل بایت‌ها برای عناصر گره زیرشبکه CNP که پیگیری می‌شود. اندازه عنصر گره زیرشبکه باید مضربی از ۶ بایت باشد. مقدار صفر نیز مجاز است.

۹-۷-۱۲ تعداد کل بایت‌های دامنه

اندازه عناصر دامنه در پیام را نشان می‌دهد. در صورت لزوم ممکن است دامنه‌های زیادی نشان داده شوند. در مورد بسته‌های ارسالی بیشتر از ۵۴۸ بایت، بند ۸-۳ را مشاهده کنید. هر عنصر دامنه ۳۲+۳۲+۲+۶=۷۲ بایت است و طول ثابتی دارد.

۹-۷-۱۳ شناسه‌های منحصربه‌فرد

شناسه‌های منحصربه‌فرد با هم بسته‌بندی می‌شوند، هر کدام ۶ بایت دارند و در ترتیب بایت شبکه CNP نشان داده می‌شود.

۹-۷-۱۴ آدرس‌های گره CNP

این آدرس، فهرستی از آدرس‌های گره CNP است و هرکدام در یک ساختار می‌باشند. فیلدها عبارتند از:

الف- شماره زیر شبکه CNP (بایت)

ب- شماره گره CNP (بایت)

پ- شاخص به فهرست دامنه پیروی شده (کلمه ۱۶ بیتی)

ت- شاخص به فهرست شناسه منحصربه‌فرد قبلی

توجه داشته باشید در صورتی‌که تمامی چهار بخش در نظر گرفته شوند، هر مدخل در جدول باید منحصربه‌فرد باشد. اگر هر بخش متفاوت باشد، هر کدام از بخش‌های دیگر می‌توانند مابین مدخل‌ها تکرار شوند. به‌عنوان مثال یک (دامنه، زیر شبکه، گره) اگر شاخص شناسه منحصربه‌فرد متفاوت باشد، می‌تواند بیش از یک بار ظاهر شود. این نشان می‌دهد که این آدرس CNP دارای بیش از یک شناسه منحصربه‌فرد است. این قانونی است اما به ندرت استفاده می‌شود. مدخل‌های با شناسه منحصربفرد یکسان، اما با بخش‌های N و S و D متفاوت، نشان‌دهنده آدرس‌های چندگانه (دامنه، زیر شبکه، گره) برای شناسه منحصربه‌فرد یکسان هستند. این امر مرسوم است.

۹-۷-۱۵ فهرست دامنه CNP

فهرستی از دامنه‌ها دنبال می‌شوند. هر دامنه توسط یک ماسک زیر شبکه، ماسک گروه و شناسه دامنه نشان داده می‌شود. تعداد دامنه‌ها به‌وسیله فیلد بایت‌های دامنه تقسیم بر اندازه ساختار دامنه (۷۲ بایت) پیام نشان داده می‌شود. به شرط محدودیت‌های اندازه پیام، هر تعداد دامنه در پیام می‌تواند وجود داشته باشد. در مورد

قطعه‌بندی پیام‌های طولانی، به بند ۸-۳ مراجعه کنید. هر دامنه در ساختاری با طول ثابت ۷۲ بایت نشان داده می‌شود.

۹-۷-۱۶ ماسک زیر شبکه (ماسک زیر شبکه CNP)

آرایه ماسک زیر شبکه، آرایه‌ای از ۲۵۶ بیت (۳۲ بایت) است که هر کدام مربوط به یک زیرشبکه CNP است. اگر بیتی در آرایه مقداردهی شود، مسیریاب بسته‌ها را از میان کانال IP خود به آن زیر شبکه ارسال می‌کند.

۹-۷-۱۷ ماسک گروه (ماسک گروه CNP)

آرایه ماسک گروه، آرایه‌ای متشکل از ۲۵۶ بیت است که هر کدام مربوط به یک آدرس گروه CNP می‌باشد. اگر بیتی در آرایه مقداردهی شود، مسیریاب بسته‌ها را از میان کانال IP خود به آن گروه ارسال می‌کند.

۹-۷-۱۸ طول دامنه (طول دامنه CNP)

طول دامنه یکی از مقادیر ۰،۱، ۳ یا ۶ است و متناظر با طول شناسه دامنه CNP بر حسب بایت می‌باشد.

۹-۷-۱۹ دامنه (شناسه دامنه CNP)

شناسه دامنه CNP آرایه‌ای متشکل از ۶ بایت نشان داده شده در ترتیب بایت شبکه CNP است. اگر طول دامنه کمتر از ۶ بایت باشد، بایت‌های استفاده نشده دامنه که بعد از شناسه خالی هستند، با مقادیر صفر پر می‌شوند.

۹-۸ بسته درخواست

جدول ۱۸، قالب بسته درخواست پیکربندی را نشان می‌دهد. مقدار نوع بسته در سرآیند عمومی بسته با توجه به ساختار داده‌ای که درخواست می‌شود، متغیر است.

جدول ۱۸- قالب بسته درخواست پیکربندی

بایت۰	بایت۱	بایت۲	بایت۳
سرآیند عمومی بسته			
تاریخ زمان			
علت	شناسه درخواست		شناسه قطعه
تاریخ زمان پس از			
آدرس IPتک پخشی			

۹-۸-۱ تاریخ/زمان

برای شرح این فیلد، بخش ۹-۴ را مشاهده کنید.

۹-۸-۲ پرچم‌ها

بیت‌های ۰و۱: علت

کد علت، درخواست را همان‌طور که در جدول ۱۹ نشان داده شده، تغییر می‌دهد.

جدول ۱۹- کدهای علت درخواست

کد علت	شرح	کد
درخواست- معمولی	درخواست معمولی اگر داده جدیدتر باشد یا تاریخ صفر باشد، داده ارسال می‌شود.	0x00
درخواست-تایید کردن	درخواست برای تائید درستی داده. داده همیشه ارسال می شود.	0x01

بیت۲: درخواست همه

کد علت، درخواست را همان‌طور که در جدول ۲۰ نشان داده شده، تغییر می‌دهد.

جدول ۲۰-کدهای مقدار درخواست

کد علت	شرح	کد
درخواست- یکی	درخواست یک قطعه، در صورتی‌که بیش از یک قطعه مورد نیاز باشد.	0x00
درخواست-همه	درخواست تمامی قطعه‌ها تا فورا ارسال شوند.	0x01

بیت ۳: درخواست و حذف

کد علت، درخواست را همان‌طور که در جدول ۱۲ نشان داده شده، تغییر می‌دهد.

جدول۲۱- کدهای عمل درخواست

کد علت	شرح	کد
درخواست- کپی	آمار را کپی می کند	0x00
درخواست-انتقال	آمار را کپی و حذف می‌کند.	0x01

بیت ۴ تا ۷: برای استفاده در آینده رزرو شده است.

۹-۸-۳ شناسه درخواست

یک مقدار دارای علامت است که توسط منبع این درخواست مورد استفاده قرار می‌گیرد تا بتواند به‌صورتی منحصربه‌فرد، پاسخ به این درخواست را متمایز سازد. به بند ۸-۳ مراجعه کنید.

۹-۸-۴ شناسه قطعه

در اطلاعات درخواست‌شده‌ای استفاده می‌شود که امکان دارد شامل بیش از یک بسته پاسخ باشد. به بند ۸-۲-۳ مراجعه کنید.

۹-۸-۵ از تاریخ/زمان

برای شرح این فیلد، به بند ۹-۴ مراجعه کنید. به گیرنده نشان می‌دهد در صورتی‌که داده در دسترس، جدیدتر از این تاریخ/زمان است، آن را ارسال کند. مقدار صفر نشان می‌دهد که همیشه داده درخواست شده ارسال می‌شود.

۹-۸-۶ آدرس IP تک‌پخشی

این آدرس تنها برای پیام‌های درخواست مسیریابی کانال استفاده می‌شود. در غیر این صورت MBZ به کار می‌رود. این آدرس نشان می‌دهد که فقط مسیریابی کانال برای این افزاره خاص فرستاده می‌شود. مقدار صفر نشان می‌دهد که تمامی اطلاعات مسیریابی کانال ارسال می‌شود. (این گزینه تنها زمانی درست است که TCP برای ارتباط با سرویس دهنده پیکربندی استفاده می‌شود)

۹-۹ بسته تصدیق

این پیام‌ها توسط افزاره‌های CNP/IP در پاسخ به پیام دریافت شده از افزاره‌های دیگر استفاده می‌شوند. پیام تصدیق دارای قالب نشان داده شده در جدول ۲۲ است. در مورد استفاده از ACKها روی ارتباطات TCP، بند ۸-۵-۳-۲ را مشاهده کنید.

جدول ۲۲- قالب‌های بسته تصدیق

بایت۳	بایت۲	بایت۱	بایت۰
سرآیند عمومی بسته با نوع بسته			
تاریخ/زمان			
شناسه قطعه	شناسه درخواست		نوع ACK

شرح فیلدهای این بسته در زیر آمده است.

۹-۹-۱ تاریخ/زمان

برای شرح این فیلد، بخش ۹-۴ را مشاهده کنید.

۹-۹-۲ نوع ACK

این پارامتر توسط افزاره‌های CNP/IP استفاده می‌شود تا درخواست‌های بیشتری روی سرویس‌دهنده انجام دهند. مقادیر معتبر عبارتند از:

- ACK_OK (0);
- ACK_FIXED (1);
- ACK_BAD_MESSAGE (2);
- ACK_CANT_COMPLY (3);
- ACK_DEVICE_REFUSED (4);
- ACK_not_SUPPORTED (5);

۹-۹-۳ شناسه درخواست

یک مقدار علامت‌دار بازگشتی از درخواست است تا بتواند پاسخ به این درخواست را به‌صورت منحصربه‌فرد، متمایز کند. به بند ۸-۳ مراجعه کنید. این مقدار در صورتی‌که استفاده نشود، معادل صفر است.

۹-۹-۴ شناسه قطعه

نتیجه درخواست تا تناظر را درخواست‌کننده میسر سازد. به بند ۸-۳ مراجعه کنید. این مقدار در صورتی‌که استفاده نشود، معادل صفر است.

۹-۱۰ بسته فهرست ارسال

این پیام توسط سرویس‌دهنده پیکربندی در درخواست یک افزاره برای به دست آوردن فهرست ارسال در افزاره‌های CNP/IP، ارسال می‌شود.

جدول ۲۳-قالب بسته‌ی فهرست ارسال

بایت۳	بایت۲	بایت۱	بایت۰
سرآیند عمومی بسته			
تاریخ/زمان			
MBZ		MBZ	جفت شماره پورت، آدرس IP
فیلدهای زیر برای هر جفت پورت/آدرس یکبار تکرار می شود			
آدرس IP			
MBZ		پورت IP	

شرح فیلدهای این بسته در زیر آمده است.

۹-۷-۱ تاریخ/زمان

بخش ۹-۴ را مشاهده کنید.

۹-۷-۲ جفت شماره پورت، آدرس IP

جفت شماره پورت، آدرس IPای که افزاره CNP/IP در فهرست ارسال دارد. مقدار صفر مجاز است. در اینجا هم آدرس‌های چندپخشی و هم تک‌پخشی ارائه می‌شوند.

۹-۷-۳ آدرس IP

آدرس IP یک افزاره CNP/IP یا آدرس چندپخشی است. افزاره CNP/IP بسته‌ها را به این آدرس ارسال خواهد کرد.

۹-۷-۴ پورت IP

شماره پورتی که افزاره CNP/IP هنگام ارسال بسته‌ها، استفاده می‌کند.

۹-۱۱ پیام پاسخ وضعیت/سلامت/آمار گره

بسته وضعیت دارای قالب نشان داده شده در جدول ۲۴ است.

جدول ۲۴- پیام پاسخ وضعیت/ سلامت/آمار گره

بایت۳	بایت۲	بایت۱	بایت۰
سرآیند عمومی بسته			
۱- زمان پس از اینکه شمارنده آخرین بار مجدداً تنظیم می شود. (فرمت:عدد صحیح ۳۲ بیتی بدون علامت بر حسب ثانیه)			
۲- زمان آخرین تنظیم مجدد شمارنده. (در GMT) (قالب: تاریخ/زمان، ۹-۴ را مشاهده کنید)			
۳- تعداد اعضای روی کانال			

۴- تعدا اعضای روی کانالی که پیام‌ها در گذشته اخیر، در آن ارسال شده‌اند.
۵- بسته‌های CNP دریافت شده
۶- بسته‌های CNP دریافت شده اما به دلیل ارسال انتخابی حذف شده
۷- کل بایت‌های CNP دریافت شده.
۸- بسته‌های CNP ارسال شده
۹- کل بایت‌های CNP ارسال شده.
۱۰- بسته‌های CNP ارسال شده به کانال IP.
۱۱- بایت‌های CNP ارسال شده به کانال IP.
۱۲- بسته‌های CNP دریافت شده از کانال IP.
۱۳- بایت‌های CNP دریافت شده از کانال IP.
۱۴- بسته‌های IP حاوی بسته‌های LT بر روی شبکه IP.
۱۵- بسته‌های IP حاوی بسته های LT از شبکه IP.
۱۶- میانگین تراکم بر روی کانال IP.
۱۷- میانگین تراکم ازکانال IP.
۱۸- تعداد بسته‌های UDP ارسال شده.
۱۹- تعداد بسته‌های TCP ارسال شده.
۲۰- تعداد بسته‌های چند پخشی ارسال شده.
۲۱- بسته های LT منقضی که از IP حذف شده اند.
۲۲- تعداد شکست‌های ارتباط TCP.
۲۳- تعداد میزبان‌های مختلفی که شکست‌های ارتباط TCP را تجربه می‌کنند.
۲۴- تعداد پیام‌های پیکربندی مسیریاب ارسال شده.
۲۵- تعداد پیام‌های پیکربندی مسیریاب دریافت شده.
۲۶- تعداد تغییرات پیکربندی.
۲۷- میانگین تعداد اجرای ارسال بسته‌های UDP در هر ثانیه.
۲۸- میانگین تعداد اجرای دریافت بسته‌های UDP در هر ثانیه.
۲۹- میانگین تعداد اجرای ارسال بسته‌های TCP در هر ثانیه.
۳۰- میانگین تعداد اجرای دریافت بسته‌های TCP در هر ثانیه.

۱- زمان پس از این‌که شمارنده آخرین بار مجددا نتظیم می شود.(فرمت:عدد صحیح ۳۲ بیتی بدون علامت بر حسب ثانیه)

۲- زمان آخرین تنظیم مجدد شمارنده. (در GMT)(قالب: تاریخ/زمان، ۹-۴ را مشاهده کنید)

۳- تعداد اعضای روی کانال (قالب: مقدار صحیح ۳۲ بیتی بدون علامت)

۴- تعداد اعضای روی کانالی که پیام‌ها در گذشته اخیر، در آن ارسال شده‌اند (روش اندازه‌گیری، تعریف نشده است). (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)

۵- بسته‌های CNP دریافت شده. (بسته‌های دریافت شده از کانال CNP).(فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)

۶- بسته‌های CNP دریافت شده اما به دلیل ارسال انتخابی حذف شده. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۷- کل بایت‌های CNP دریافت شده. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۸- بسته‌های CNP ارسال شده.(بسته‌های ارسال شده به کانال CNP). (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۹- کل بایت‌های CNP ارسال شده. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۱۰- بسته‌های CNP ارسال شده به کانال IP. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۱۱- بایت‌های CNP ارسال شده به کانال IP. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۱۲- بسته‌های CNP دریافت شده از کانال IP. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۱۳- بایت‌های CNP دریافت شده از کانال IP. (فرمت: عدد صحیح ۳۲ بیتی بدون علامت)
۱۴- بسته‌های IP حاوی بسته‌های LT بر روی شبکه IP. (فرمت: عدد صحیح ۳۲ بیتی بدون علامت)
۱۵- بسته‌های IP حاوی بسته‌های LT از شبکه IP. (فرمت: عدد صحیح ۳۲ بیتی بدون علامت)
۱۶- میانگین تراکم بر روی کانال IP.(مقدار به‌صورت جفت عدد صحیح ۳۲ بیتی بدون علامت بیان می‌شود. جمع بسته‌های LT<۱۰>/جمع بسته‌های IP<۱۴>)
۱۷- میانگین تراکم ازکانال IP.(مقدار به‌صورت جفت عدد صحیح ۳۲ بیتی بدون علامت بیان می‌شود. جمع بسته‌های LT<۱۲>/جمع بسته‌های IP<۱۵>).(چون تمامی این پارامترها اختیاری هستند، لزوماً شکل‌های تکراری داده، مسئله نمی‌باشد. یکی ممکن است ۱۲ و۱۴ را پشتیبانی نکند و بجای آن ۱۷ را پشتیبانی کند.)
۱۸- تعداد بسته‌های UDP ارسال شده (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۱۹- تعداد بسته‌های TCP ارسال شده (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۲۰- تعداد بسته‌های چند پخشی ارسال شده (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۲۱- بسته‌های LT منقضی که از IP حذف شده اند. (منقضی به این معنی است که بیش از حد طولانی در شبکه IP، بوده‌اند.) (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۲۲- تعداد شکست‌های ارتباط TCP (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۲۳- تعداد میزبان‌های مختلفی که عدم برقراری ارتباط TCP را تجربه می‌کنند. (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۲۴- تعداد پیام‌های پیکربندی مسیریاب ارسال شده (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۲۵- تعداد پیام‌های پیکربندی مسیریاب دریافت شده (فرمت: مقدار صحیح ۳۲ بیتی بدون علامت)
۲۶- تعداد تغییرات پیکربندی.(فرمت: مقدار صحیح ۳۲ بیتی)
۲۷- میانگین تعداد اجرای ارسال بسته‌های UDP در هر ثانیه.(فرمت: عدد صحیح ۳۲ بیتی)
۲۸- میانگین تعداد اجرای دریافت بسته‌های UDP در هر ثانیه.(فرمت: عدد صحیح ۳۲ بیتی)
۲۹- میانگین تعداد اجرای ارسال بسته‌های TCP در هر ثانیه.(فرمت: عدد صحیح ۳۲ بیتی)
۳۰- میانگین تعداد اجرای دریافت بسته‌های TCP در هر ثانیه.(فرمت: عدد صحیح ۳۲ بیتی)

پیوست الف

(الزامی)

مشخصات استاندارد CNP

قالب بسته‌های محصور سازی توسط تونل IP، شامل فیلد L2Hdr از طریق فیلد جامع CRC است. این قالب شامل فیلدهای Preamble، Bit Sync یا ByteSynce یا بیت‌های نقش کد خط نمی‌باشد. مشخصه این بسته‌ها را می‌توان در ISO-IEC 14908-1 یافت. طرح‌های آدرس‌دهی‌ای که در زیر آمده و در این مشخصه ارجاع داده شده‌اند، بر اساس تعریف RFC 2131 پشتیبانی می‌شوند.

الف-۱ شناسه منحصربه‌فرد در افزاره-شناسه Neuron؛

الف-۲ شناسه دامنه- شناسه دامنه؛

الف-۳ شناسه زیر شبکه- شناسه زیر شبکه؛

الف-۴ شناسه گروه- شناسه گروه.

ملاحظات همگام‌سازی هنگام استفاده CNP

CNP یک پروتکل ارتباطی طراحی شده برای کنترل بی درنگ افزاره‌ها است. به این ترتیب انتظار می‌رود که پیام‌ها در مقدار محدود زمانی (مطابق با نیازهای کاربرد) و با حداقل انحراف زمان حول آن زمان محدود شده، دریافت شوند. به‌عنوان بخش تشخیص/ ترمیم خطای پروتکل، قابلیت تشخیص پیام تکراری وجود دارد طوری‌که برخلاف تعداد پیام‌های دریافت شده در تراکنش پیام واحد، پیام‌ها تنها یکبار کار می‌کنند.

تشخیص تکرار در CNP، الگوریتمی است که هم در فرستنده و هم در گیرنده اجرا می شود. الگوریتم به‌طور کامل در آن استاندارد شرح داده شده است، اما در اینجا از دید سطح بالاتری ارائه می‌شود تا به توضیح مسئله همگام‌سازی زمان کمک کند.

زمانی‌که فرستنده پیامی می‌نویسد، در پیکربندی خود نگاه می‌کند تا سرویس پروتکل را تعیین کند. اگر سرویس پروتکل، تشخیص تکرار را مشخص کند، فرستنده یک شماره تراکنشی که به تازگی هنگام ارتباط با آدرس گیرنده، توسط این فرستنده استفاده نشده است را تخصیص می‌دهد.

پس از این، پیام با آن شماره تراکنش ارسال می‌شود. همچنین فرستنده یک زمان‌سنج به نام زمان‌سنج تراکنش را آغاز می‌کند که بعد از انقضای آن، امتحان مجدد پیام رخ خواهد داد مگر این‌که تعداد پیکربندی امتحان مجدد به پایان رسیده باشد یا پاسخ دریافت شده باشد. پس از دریافت پیام، گیرنده نگاه می‌کند که آیا تراکنشی برای آن پیام وجود دارد. اگر وجود داشت، پیام تکراری است و به آن پاسخ داده می‌شود؛ اگر وجود نداشته باشد بعد از آن کار نمی‌کند و یک تراکنش جدید با مقداردهی زمان‌سنج دریافتی تخصیص داده می‌شود. زمانی‌که زمان‌سنج دریافتی منقضی شود، تراکنش حذف می‌شود. به محض این‌که تراکنش حذف شد، هر پیام جدیدی باشماره تراکنش یکسان با تراکنش حذف شده، به‌عنوان پیام جدید مورد ملاحظه قرار می‌گیرد.

شبکه‌های IP با کنترل بی‌درنگ طراحی نشده‌اند. برای پشتیبانی از کاربردهای بی‌درنگ حساس روی IP همچون صدا، پروتکل IP با بیت‌های QOS (کیفیت سرویس) در سرآیند قاب، توسعه یافته است. متأسفانه محتوای بیت‌ها استاندارد نیست و تمامی مسیریاب‌ها روی بیت‌ها به‌طور مناسب عمل نمی‌کنند. در این متن، کسی نمی‌تواند به‌طور قابل اعتماد، بیت‌های QOS را در یک بسته مقداردهی کند و آن بسته را روی اینترنت عمومی ارسال کند و تأخیر پایین، سرویس انحراف زمانی کم انتها به انتها را به‌دست آورد.

اگر بسته‌های CNP روی شبکه IPای که تأخیر زمانی تصادفی روی برخی از بسته‌ها تحمیل می‌کند، تونل زنی شوند، شکست‌های پروتکل CNP رخ خواهد داد به این دلیل که تحویل پیام‌های منقضی شده، به جای بسته‌های تکراری به‌عنوان بسته‌های جدید توسط گیرنده تفسیر می‌شوند. این شکست‌ها می‌توانند برای کاربرد اساسی، جدی باشند. به‌منظور جلوگیری از این شکست‌های پروتکل، گزینه همگام‌سازی زمان تمامی گره‌ها طبق دستورات این استاندارد، امکان پذیر است. برای تعیین صحت چگونگی همگام‌سازی، باید زمان-سنج‌های پروتکل CNP در حال استفاده در میان قطعه IP که ممکن است تأخیر تصادفی به‌وجود آورد، بررسی شوند. جدول ب-۳، CNP دارای مجموعه کاملی از مقادیر زمان‌سنج برای یک شبکه CNP است. حداکثر انحراف مجاز، توسط معادله زیر محاسبه می‌شود:

((مقدار زمان سنج تراکنش امتحان های مجدد) – مقدار زمان سنج تراکنش دریافتی در حال استفاده)min

محلی که در آن تمامی جفت گره‌هایی که در سراسر کانال IP ارتباط برقرار می‌کنند، بررسی می‌شوند و حداقل انحراف زمانی که می‌تواند تحمل شود، توسط تنظیمات زمان‌سنج‌های پیکربندی آن‌ها، تعیین می-گردد. با این کار، می‌توان تعیین کرد که چگونه زمان دقیق، در میان تمامی گره‌های شبکه به‌دست می‌آید. اجرای این محاسبه نیازمند آگاهی از پیکربندی تمامی گره‌های CNPای است که از طریق کانال IP ارتباط برقرار می‌کنند. این اشاره به این دارد که برخی از انواع پایگاه داده شبکه با تمامی اطلاعات پیکربندی، داخل آن است. در نبود این اطلاعات می‌توان روش دیگری را برای جلوگیری از مشکل تشخیص بسته منقضی، دنبال کرد. اگر سرویس‌دهنده زمان روی هر قطعه LAN متصل به اینترنت، وجود داشته باشد که از یک ماهواره یا منبع رادیویی، زمان تجزیه ناپذیر را به‌دست می‌آورد و آن را به گره‌های روی LAN، سرویس‌دهی می‌کند، هر قطعه LAN می‌تواند دید خیلی دقیقی از زمان داشته باشد که این موجب می‌شود مشکل تشخیص ندادن بسته‌های منقضی، مشکل‌آفرین نشود.

پیوست ب

(الزامی)

مشخصات برای CNP

افزاره CNP باید یکی از شماره‌های پورت زیر را که توسط IANA تخصیص داده شده است، استفاده کند.

- 1628/tcp
- 1628/udp
- 1629/tcp
- 1629/udp-