

معرفی سامانه CGNAT

شرکت ایمن پردیس

فهرست

۲.....	معرفی شرکت ایمن پردیس
۵.....	معرفی راهکار ipCGN
۱۱.....	معرفی سیستم عامل NetOS



معرفی شرکت ایمن پردیس

شرکت «فناوری ارتباطات ایمن پردیس» توسط گروهی از متخصصین حوزه امنیت اطلاعات، شبکه و سیستم‌های مبتنی بر یونیکس فعالیت خود را با هدف ارائه خدمات تخصصی در زمینه پژوهش، مشاوره، طراحی و پیاده‌سازی خدمات مدیریت شده امنیت اطلاعات و توسعه سیستم‌های پربازده مبتنی بر شبکه آغاز نمود. این شرکت در حال حاضر مشغول به ارائه خدمات و تولید محصولات مورد نیاز شبکه‌های NGN به سازمان‌ها و شرکت‌های فعال در این حوزه‌ها می‌باشد.

رسالت شرکت، توسعه دانش بومی و انتقال دانش و تکنولوژی در حوزه‌های امنیت اطلاعات و زیرساخت‌های حساس، رفع نیاز کشور به متخصصین خارجی در حوزه امنیت از طریق تولید محصولات داخلی بوده و مأموریت‌های زیر برای شرکت در نظر گرفته شده است:

۱. انجام فعالیت‌های تخصصی در حوزه امنیت اطلاعات و زیرساخت‌های امن

۲. پژوهش و تولید محصولات مرتبط با حوزه تخصصی شرکت

۳. انتقال دانش تخصصی و نهادینه سازی دانش در سازمان‌ها

با توجه به رسالت شرکت، خدمات ارائه شده توسط این مجموعه دارای مزایای زیر در مقایسه با نمونه‌های خارجی می‌باشد:

- پشتیبانی تخصصی در محل به صورت ۲۴ ساعته در سه سطح مختلف
- همکاری و ارائه مشاوره به مشتریان در زمینه یکپارچه‌سازی محصولات شرکت با راهکارهای موجود
- امکان توسعه و اعمال تغییرات در محصولات مطابق نیازمندی مشتریان
- ارائه مزایای اقتصادی و کیفی رقابتی با محصولات خارجی

از خدمات شرکت ایمن پردیس می‌توان به موارد زیر اشاره نمود:

- طراحی و مجری موفق‌ترین پیام رسان مبتنی بر موبایل ایرانی (بیسفون) با بیش از دو میلیون کاربر. این پیام رسان با دیدگاه رفع نگرانی‌های امنیتی و حریم خصوصی در کشور طراحی و پیاده‌سازی شد. طی مدت انجام این پروژه، بیش از بیست نفر متخصص داخلی در حوزه پیاده‌سازی نرم‌افزارهای مبتنی بر تلفن همراه آموزش داده شدند.

- طراحی و مجری سیستم Carrier Grade NAT با نام تجاری ipCGN در سال ۱۳۹۲ به عنوان اولین نمونه در کشور، مورد استفاده در اپراتورهای اینترنت و موبایل کشور - این سامانه علاوه بر رفع مشکل کمبود آدرس‌های

IPv4، راهکاری جهت ثبت داده‌های ترافیک اینترنت و هویت کاربران جهت ارائه خدمات به قوه قضاییه و پلیس ارائه نموده است. همچنین با پیاده‌سازی استاندارد NAT64 در این محصول، بستر مناسب برای مهاجرت اپراتورها به IPv6 فراهم گردیده است.

- توسعه سیستم عامل NetOS مبتنی بر یونیکس به عنوان پایه محصولات و Appliance‌های تولید شده - این سیستم عامل علاوه بر ملاحظات امنیتی، مقیاس پذیری افقی و عمودی با ضریب بالا را فراهم می‌نماید. از مهمترین قابلیت‌های این سیستم عامل امکان پردازش ترافیک در مقیاس چند ده گیگابیت در ثانیه است که آن را برای پیاده سازی در شبکه‌های Carrier مناسب می‌سازد.

- توسعه سامانه ipDNS به عنوان DNS Resolver و Validator با پشتیبانی کامل از DNSSEC و بازدهی بالا (تا ۴۰۰ هزار درخواست در ثانیه) برای اپراتورهای اینترنت. همچنین با توجه به پیاده سازی استاندارد DNS64 در این محصول و امکان یکپارچگی آن با ipCGN، امکان مهاجرت ساده‌تر به پروتکل IPv6 در شبکه اپراتورها فراهم شده است.

- ارائه خدمات تخصصی پیاده‌سازی، انتقال دانش و مهاجرت به پروتکل IPv6

- توسعه نرم افزارهای خاص منظوره در زمینه NSM و امنیت شبکه در سطح Enterprise و Carrier

- طراحی و پیاده‌سازی حسگرها و پوششگرهای شبکه با ظرفیت‌های 1G و 10G

- طراحی و پیاده سازی حسگرهای امنیتی و کیفی شبکه و سیستم‌های جمع آوری و تقارن داده‌های حسگرها

- طراحی و پیاده سازی سامانه مدیریت ترافیک شبکه در سطح Carrier Grade به صورت توزیع شده و با مدیریت یکپارچه مرکزی

- ارائه خدمات مهاجرت به سیستم‌های باز متن و بهینه سازی سیستم‌های موجود مبتنی بر سیستم عامل‌های Solaris و HP-UX و انواع مختلف سیستم‌های UNIX در سطوح Enterprise و Carrier

- ارائه خدمات تخصصی و راهکارهای ذخیره سازی اطلاعات با فایل سیستم ZFS

- طراحی و پیاده‌سازی سیستم‌های خاص منظوره (Embedded) با قابلیت پردازش بالا در سطح Carrier Grade

- طراحی و پیاده‌سازی سیستم ipOSINT (جمع آوری اطلاعات، مرتبط سازی و داده کاوی اطلاعات شبکه در سطح IP, Port, AS Number, Domain Name و Packet) - مورد استفاده در مراکز CERT/CSIRT و SOC

- طراحی و پیاده سازی سیستم ipSpectator جهت انجام Passive Network Forensics (پردازش داده‌های ضبط شده شبکه و استخراج داده‌های کارآگاهی) - مورد استفاده در مراکز CERT/CSIRT و مراجع قضایی

- ارائه راهکارهای Load Balancing و Content Distribution

- ارایه راهکارهای Cloud Computing با استفاده از تکنولوژی های VMWare، Oracle Solaris و BSD BHyve
- طراحی و پیاده سازی مرکز عملیات امنیت شبکه (SOC) و مرکز پاسخگویی به رخدادهای امنیتی رایانه ای (CSIRT)

مشتریان

شرکت ایمن پردیس از بدو تاسیس خدمات تخصصی خود را به چندین سازمان و شرکت فعال در زمینه های مختلف شامل سازمان های دولتی، شرکت های خصوصی و ارایه دهندگان خدمات اینترنت ارایه نموده است.

اسامی تعدادی از مشتریان شرکت به شرح زیر است:

- سازمان تنظیم مقررات و ارتباطات رادیویی
- سازمان فناوری اطلاعات ایران
- شرکت ارتباطات زیرساخت
- ارتباطات کهکشان
- شرکت رایتل
- بزرگ نت آریا
- شرکت داده پردازی رسپینا
- شرکت گیلان کامپیوتر
- توسعه فناوری اطلاعات خوارزمی
- شرکت تالیا
- شرکت تراشه سبز تهران (بیستاک)
- شرکت زعیم
- شرکت U2Telecom
- شرکت نوین مهر
- گلوبال پتروتک کیش
- شرکت تجارت الکترونیک صبا (آپارات و کلوب)

معرفی راهکار ipCGN

مقدمه

رشد بی سابقه تلفن های همراه هوشمند و افزایش تعداد کاربران اینترنت در سالهای اخیر، ارایه دهندگان خدمات اینترنت را مجبور به سرمایه گذاری قابل توجهی در بخش زیر ساخت، به منظور ارایه و پشتیبانی از ترافیک رو به رشد و همچنین ارایه سرویسهای نوین نموده است. این موضوع سبب استفاده بسیار زیاد از IPv4 شده و در نتیجه معضل کمبود IPv4 از مشکلات و چالشهای حال حاضر می باشد.

در سوم ماه فوریه سال ۲۰۱۱، سازمان IANA آخرین پنج آدرس ۸/ را به ثبت کنندگان محلی اینترنت Regional Internet Registries (RIR) اختصاص داد. از ماه آوریل سال ۲۰۱۴ طرح تخصیص IP سازمان ARIN وارد فاز نهایی خود گردید و این سازمان قادر به پاسخگویی به درخواستهای جدید نمی باشد.

از طرف دیگر محتوای دیجیتال و ترافیک اینترنت در حال رشد تصاعدی می باشند و تمایل روزافزون به استفاده از اینترنت در تمامی بخشها و ایجاد شدن مباحثی همچون Internet of Things سبب گردیده تعداد تجهیزات متصل به اینترنت تا پایان این دهه میلادی به ۲۰ میلیارد دستگاه برسد و این خود به معنای تقاضای بیشتر برای آدرسهای IP است.

به منظور پیشبرد وضعیت کنونی و آماده شدن برای توسعه طولانی مدت، مهاجرت به IPv6 به امری اجتناب ناپذیر برای ارایه دهندگان خدمات بدل گشته است.

از آنجاییکه پروتکل IPv6 به طوری ذاتی با IPv4 سازگار نیست، سرویس دهندگان مجبور به ارایه طرحی برای پیاده سازی تواماً IPv4 و IPv6 در کنار هم به منظور ادامه فعالیت کنونی و همچنین آماده سازی برای توسعه در آینده می باشند.

شرکت ایمن پردیس با ارایه راهکار جامع مهاجرت از IPv4 به IPv6، این امکان را برای ارایه دهندگان خدمات به وجود آورده است تا با تکیه بر زیرساخت کنونی مبتنی بر IPv4 خود، زمان بیشتری به منظور آمادگی انتقال به زیرساخت جدید IPv6 داشته باشند. این راهکار علاوه بر رفع مشکل کمبود آدرسهای IPv4 با استفاده از NAT44، مسیر مهاجرت به پروتکل IPv6 را از طریق NAT64 امکانپذیر می سازد.

لازم به ذکر است به جهت حفظ زیرساختهای موجود و کاهش هزینههای سربار اپراتورها، این سیستم به گونه ای طراحی شده است که در طی پروسه Integration نیاز به اعمال تغییر در زیرساختهای شبکه اپراتور و همچنین نرم افزارهای موجود (مانند نرم افزار Billing) نباشد.

چالشهای سرویس دهندگان

سازمان IANA مسئولیت هماهنگی جهانی آدرس دهی و پروتکل های اینترنتی را بر عهده دارد. نقش این سازمان اختصاص آدرس های استفاده نشده به ثبت کنندگان محلی اینترنت (RIR) با توجه به نیازشان می باشد. در حال حاضر آدرس های موجود در IANA رو به کاهش است و ثبت کنندگان محلی اینترنت نیز به سرعت IP های خود را مصرف می کنند.

افزایش سریع تعداد تجهیزات متصل به اینترنت موجب کاهش فضای آدرس دهی IPv4 گردیده است و در عین حال

ارایه دهندگان خدمات با تقاضاهای زیادی جهت اتصال به اینترنت مواجه هستند. با اینکه مهاجرت به IPv6 به خدمات دهندگان در جهت توسعه زیرساخت کمک می‌نماید اما مهاجرت ناگهانی و یکباره نیز راه حل منطقی نبوده و در عمل امکانپذیر نمی‌باشد. به علاوه، با توجه به ناسازگاری پروتکل‌های IPv4 و IPv6، فرایند ترجمه آدرس نیز باعث ایجاد اختلال در بعضی پروتکلها و برنامه‌ها می‌شود.

پایداری ارتباط، از جمله اولویتهای هر ارایه دهنده خدمات به حساب می‌آید و اپراتورها به دنبال اطمینان از صحت کارکرد برنامه‌های اجرا شده توسط کاربران خود می‌باشند. سرویس دهندگان جهت ادامه فعالیت کنونی خود و آمادگی برای ایجاد توسعه و پایبندی به توافقنامه سطح خدمات (SLA)، با چالشهای زیر روبرو هستند:

- **حفظ زیر ساخت‌های موجود:** سرویس دهندگان دارای زیرساختهای گسترده مبتنی بر IPv4 می‌باشند و تمایل دارند ضمن حفظ این زیرساخت موجود، بدون اعمال تغییرات پرهزینه و ایجاد اختلال در سرویس دهی، برای طرحهای توسعه‌ای آینده آماده شوند.

- **آمادگی برای رشد آنی تعداد کاربران:** ارایه دهندگان خدمات همچنین به دنبال راههای مشخصی جهت مواجهه با تقاضاهای رو به رشد متقاضیان اتصال به اینترنت می‌باشند. به علاوه مادامی که آنها جهت انتقال به بستر IPv6 آماده می‌شوند، تمایل دارند از انتقال بدون مشکل و بدون اختلال و نیز برطرف کردن مشکلات سازگاری با بستر IPv4 کنونی نیز مطمئن باشند.

- **پایبندی به توافقنامه سطح خدمات (SLA):** فعالیت اقتصادی ارایه دهندگان خدمات به میزان زیادی به پایداری و برقراری سرویس آنها بستگی دارد. قطعی سرویس برای خدمات دهندگان قابل قبول نیست، چرا که موجب ضرر مالی، نارضایتی کاربران و کاهش اعتبار حرفه‌ای آنها می‌شود.

راه حل، ایجاد یک برنامه جایگزین با در نظر گرفتن فضای کلی IPv6 و استفاده از راهکارهای مهاجرت می‌باشد. با این وجود سیستم‌های مبتنی بر IPv4 تا سالها وجود خواهند داشت و ضروری است که زیرساخت‌های IPv4 و IPv6 در کنار یکدیگر وجود داشته باشند.

راهکارهای گوناگونی جهت توسعه شبکه‌های IPv4 و مهاجرت مرحله به مرحله به IPv6 وجود دارند. معروفترین و معمولترین این راهکارها شامل موارد زیر هستند:

توضیح	راهکار
به منظور صرفه جویی IPv4 در مقیاس بالا و با استفاده از تکنولوژیهای NAT44/NAT444	CGNAT یا LSN
ایجاد دسترسی به IPv4 از طریق شبکه IPv6	DS-Lite (Dual-Stack Lite)
پیاده‌سازی IPv6 در یک شبکه مبتنی بر IPv4	6rd (IPv6 Rapid Deployment)

توضیح	راهکار
ایجاد ارتباط کاربران IPv6 به اینترنت مبتنی بر IPv4	DNS64 + NAT64

راهکار ipCGN

راهکار CGN ارایه شده توسط شرکت ایمن پردیس (ipCGN)، با انجام ترجمه آدرس و پورت (NAT/PAT) با راندمان بالا این امکان را برای ارایه دهندگان خدمات به وجود آورده است تا علاوه بر استفاده از شبکه IPv4، به طور همزمان آمادگی لازم جهت مهاجرت به IPv6 را کسب نمایند. ipCGN بر پایه سیستم عامل NetOS طراحی شده که ویژگی‌هایی همچون راندمان بالا، توسعه پذیری، صرفه جویی در IPv4، مهاجرت به IPv6 و امنیت را فراهم می‌آورد. در این راهکار، نیازمندی‌های امنیتی و قانونی اپراتورها به منظور پاسخگویی به مراجع قضایی نیز به طور کامل در نظر گرفته شده است.

افزایش عمر زیرساخت‌های IPv4

محصول شرکت ایمن پردیس (ipCGN) مطابق با استانداردهای موجود در زمینه CGNAT ساخته شده است. CGNAT با استفاده از ترجمه آدرس و پورت در مقیاس بزرگ علاوه بر پایان دادن به مصرف بیش از حد IPv4، به افزایش عمر سرویس دهی شبکه‌های مبتنی بر IPv4 نیز کمک می‌کند.

اصولاً تعداد آدرس‌های Private و Public در شبکه سرویس دهندگان بسیار زیاد بوده و انجام ترجمه آدرس، از نظر امکانات پردازی، فرایندی بسیار پیچیده و پرهزینه می‌باشد. به همین منظور، ipCGN از ابتدا با هدف ارایه سرویس CGNAT با راندمان بالا و قابلیت توسعه پذیری، طراحی و ساخته شده است. به علاوه ipCGN از ویژگی نگهداری و پردازش Log پیشرفته‌ای برخوردار است که ضمن نگهداری اطلاعات مربوط به فعالیت کاربران، پاسخگوی درخواستهای مراجع قانونی مربوطه می‌باشد.

همانطور که در تصویر ۱ نشان داده شده است، راهکار ipCGN، این امکان را برای ارایه دهندگان خدمات فراهم می‌آورد تا عمر زیرساخت‌های مبتنی بر IPv4 خود را افزایش داده و ضمن صرفه جویی در هزینه‌های مالی، فرصت کافی جهت اجرای برنامه مهاجرت به IPv6 را نیز پیدا کنند.

یکپارچگی با زیرساخت‌های موجود

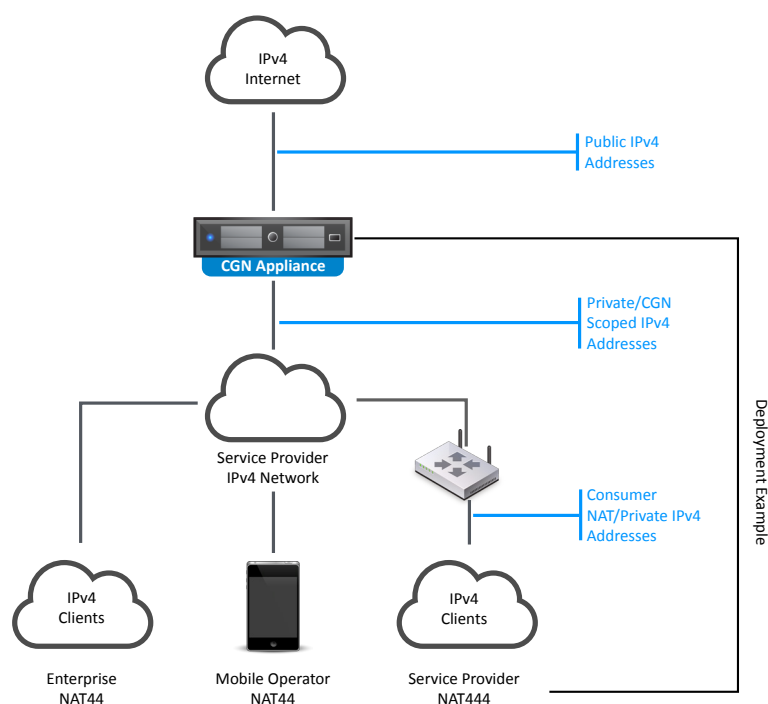
ورود یک سامانه جدید به قلب شبکه اپراتورها امری حساس بوده و همواره با نگرانی‌های اپراتورها همراه است. یکپارچگی با توپولوژی موجود و نیاز به حداقل تغییرات در طراحی فعلی شبکه، از اهداف شرکت ایمن پردیس در طراحی سیستم ipCGN بوده است. همچنین در صورت لزوم امکان اعمال تغییرات در محصول به منظور یکپارچگی آسانتر با شبکه اپراتور فراهم می‌باشد. برای مثال، امکان مسیریابی توسط پروتکل‌های OSPF و BGP در سیستم در نظر گرفته شده تا یکپارچگی سیستم با شبکه موجود با کمترین تغییرات در توپولوژی شبکه اپراتور امکانپذیر گردد. همچنین یکپارچگی با راهکارهای BSS موجود به منظور دریافت داده‌های هویتی کاربران (در صورت نیاز) به صورت Passive و با دریافت یک نسخه از پروتکل Radius موجود در شبکه امکانپذیر می‌باشد. بنابراین اپراتور نیازی به

تغییر راهکار Billing موجود یا استفاده از نرم افزارهای خاص را در این مورد نخواهد داشت.

ضریب اطمینان پروتکل های لایه Application

محصول CGN شرکت ایمن پردیس (ipCGN) با فراهم آوردن شرایط برقراری برنامه ها و پایداری ارتباط، این امکان را به وجود می آورد که سرویس ها در طول فرایند آدرس دهی، در دسترس بوده و بدون هیچ مشکلی به فعالیت خود ادامه دهند.

بسیاری از برنامه ها همچنان با تکیه بر اطلاعات لایه شبکه و اپلیکیشن (۳ تا ۷) فعالیت می کنند. برنامه هایی که اطلاعات مربوط به شبکه و سایر موارد را در Payload بسته های خود قرار می دهند با انجام فرایند NAT دچار وقفه می شوند. محصول ipCGN با فراهم آوردن قابلیت Application Layer Gateway (ALG) این امکان را فراهم کرده تا پروتکل هایی همچون ICMP، DNS، SIP، PPTP، RSTP، TFTP، FTP و H.323 حتی با انجام فرایند NAT نیز به کار خود ادامه دهند. به علاوه ویژگی های پیشرفته ای همچون Endpoint Independent Mapping (EIM) با قابل پیش بینی کردن رفتار NAT، باعث می شود کل فرایند تأثیری بر فعالیت اپراتور نداشته باشد.



تصویر ۱ - جایگزاری CGN در شبکه اپراتور

تنوع در روش های مهاجرت به IPv6

شبکه های سرویس دهندگان از نظر انواع خدمات بسیار متنوع بوده و تکنولوژی های متفاوتی به طور همزمان در آنها پیاده سازی شده است. محصول ipCGN انتخاب گسترده ای از راهکارها را فراهم می آورد تا انتقال به IPv6 به سادگی و سهولت انجام پذیرد. همچنین شرکت ایمن پردیس خود را موظف می داند همکاری های لازم در راستای

همفکری و ارایه راهکار به اپراتور به منظور اعمال حداقل تغییرات در شبکه موجود و یکپارچه سازی راهکار ipCGN در شبکه اپراتور ارایه نماید.

تکنولوژیهای (IPv6 Rapid Deployment (6rd یا Light Weight 4 over 6 (LW4o6 این امکان را برای تجهیزاتی IPv6 فراهم می آورند تا از طریق یک شبکه مبتنی بر IPv4 به اینترنت متصل شوند.

تجهیزاتی که فقط با IPv6 کار می کنند احتیاج به راهی برای اتصال به اینترنت IPv4 دارند و راهکارهای NAT64 / DNS64 این امکان را برای آنها فراهم می آورند. قابلیت ترجمه آدرسهای IPv6 به IPv4 در نسل جدید ipCGN، امکان مهاجرت قدم به قدم به پروتکل IPv6 را فراهم نموده است.

به علاوه، محصول ipCGN این اطمینان خاطر را برای مشتریان فراهم می سازد که آنها می توانند تکنولوژیهای مهاجرت را به طور همزمان پیاده سازی نمایند و درعین حال ipCGN نیز با همه آنها سازگار بوده و این امکان را برای ارایه دهندگان خدمات فراهم می آورد تا به صورت مرحله به مرحله برای انتقال به IPv6 برنامه ریزی نمایند. به عنوان مثال ابتدا به منظور صرفه جویی در مصرف IPv4 از CGNAT استفاده نمایند و سپس اقدام به پیاده سازی NAT64 / DNS64 نمایند تا کاربران IPv6 نیز بتوانند به اینترنت IPv4 متصل شوند.

با توجه به موارد گفته شده، محصول ایمن پردیس (ipCGN) ویژگیهای جامع و کاملی همچون ALG، CGNAT و تکنیکهای گوناگون مهاجرت به IPv6 را یکجا فراهم آورده است.



مزایای ipCGN

طراحی آدرس دهی شبکه و مهاجرت به IPv6 در هر سازمان و شبکه متفاوت است. سرویس دهندگان نیازمند راهکاری می باشند که بیشترین سازگاری و پشتیبانی را از ملزومات استاندارد آدرس دهی و مهاجرت داشته باشند. شرکت ایمن پردیس با ارایه محصول ipCGN توانسته ویژگیهای پیشرفته ای را بطور یکجا ارایه داده است که سبب فراهم آمدن فواید گوناگونی شده است:

- **افزایش عمر زیرساختهای IPv4:** محصول ipCGN با فراهم آوردن امکان ترجمه آدرس و پورت با بازدهی بالا، این قابلیت را برای ارایه دهندگان خدمات فراهم آورده است که مدت زمان بیشتری بتوانند از زیر ساخت IPv4 خود استفاده نمایند.

- **ضریب بالای کارایی برنامه‌ها:** محصول ipCGN برقراری برنامه‌ها و پایداری ارتباطات را فراهم می‌آورد. پشتیبانی ALG از پروتکل‌های پرکاربرد موجود، باعث افزایش تداوم سرویس ارائه دهندگان خدمات، ارائه SLA بهتر و افزایش رضایت کاربران می‌شود.

- **ترجمه IPv6:** محصول ipCGN از راهکارهای گوناگون مهاجرت به IPv6 پشتیبانی می‌کند و وجود همزمان این تکنولوژی‌ها با همدیگر، امکان مهاجرت آسانتر را برای سرویس دهندگان فراهم می‌آورد. سازگاری و هماهنگی بین CGNAT و تکنولوژی‌های مهاجرت به IPv6، امکان انتقال مرحله به مرحله و همچنین وجود هر دو نسخه IPv4 و IPv6 در شبکه را بدون احتیاج به تجهیزات مختلف را فراهم می‌سازد.

معرفی سیستم عامل NetOS

تحولات تکنولوژی های Application Networking

با روی کار آمدن و فراگیر شدن روزافزون تکنولوژیهای موبایل و رایانش ابری، دیتاسنترهای مدرن دائماً در حال تغییر شکل و ماهیت ناشی از نیازمندی های این تکنولوژی ها هستند. افزایش سریع ترافیک دیتاسنترها به چالشی جدید برای سرویس دهندگان و شبکه های بزرگ بدل شده است که آنها را به سمت توسعه و استفاده از زیرساخت های مقیاس پذیر با بازدهی بالا سوق می دهد. برای همسو شدن با این روند و به جهت بهبود بازدهی و امنیت معماری دیتاسنترها، تکنولوژیهای Application Networking نیز تغییرات زیادی را تجربه کرده اند.

برای مثال افزایش ناگهانی ترافیک شبکه ها که از اپلیکیشن های موبایل، کلان داده و ترافیک وب ناشی شده است، چالشهای جدی در مقیاس پذیری و بازدهی سیستمهای Application Networking به وجود آورده است. به منظور انطباق با این رشد، سیستم های Application Networking مقیاس پذیر و با ضریب اطمینان بالا مورد نیاز است تا امکان ارائه خدمات با سطح کیفی مطلوب امکانپذیر گردد.

طی شش سال گذشته، معماری پردازنده های چند منظوره که توسط سازندگان سیستمهای Application Networking استفاده می شده است از پردازنده های تک هسته ای ۳۲ بیتی، به پردازنده های چند هسته ای ۶۴ بیتی تغییر پیدا کرده است. ولی با این وجود، معماری نرم افزارهای Application Networking به منظور سازگاری با این پردازنده های جدید بهینه سازی نشده و بعضی از سازندگان، در زمان کوتاه قادر به تطبیق محصولات خود برای مواجهه با افزایش ترافیک دیتاسنتر نبوده اند. به منظور رفع این مشکل، لازم است معماری سطح بالای این سیستم ها مورد بازنگری کلی قرار گرفته تا تغییرات مورد نیاز در کیفیت عملکرد سیستمهای Application Networking انجام پذیرد. این معماری مجدد در پلتفرم NetOS شرکت «ایمن پردیس» انجام پذیرفته است.

دوران پردازنده های چند هسته ای

سیستمهای سنتی شبکه (مانند سوئیچها و روترها) که فقط نیاز به پردازش بخش کوچکی از header ترافیک شبکه را دارند، این عمل را با استفاده از پردازشگرهای ASIC و با بازدهی بالا انجام می دهند. طبیعی است که این سیستم ها قادر به ارائه و پیاده سازی پردازش های کاربردی تر و عمیق تر بر روی ترافیک نمی باشند.

از سوی دیگر سیستمهای Application Networking مانند ADC^۱، با بررسی عمیق تر بسته ها و رفتار هوشمندانه تر نسبت به ترافیک، توانایی پیاده سازی پردازش های پیچیده روی ترافیک شبکه را دارند. به همین منظور، سیستمهای Application Networking به حافظه و پردازشگرهای چند منظوره وابسته هستند تا بتوانند هر گونه پردازش را بدون محدودیتهای موجود در ASIC انجام دهند. صنعت ساخت پردازنده، نقش کلیدی را در چرخه توسعه Application Networking ایفا می کند. پیش از این، بازدهی پردازنده ها با افزایش سرعت clock آنها افزایش می یافت. اما بالا بردن سرعت clock، از سوی دیگر منجر به افزایش مصرف انرژی می گردید. در سال ۲۰۰۵ به منظور رفع این مشکل، پردازنده های چند هسته ای با دو یا چند CPU بر روی یک چیپ سیلیکونی، با هدف افزایش سرعت، کاهش مصرف، کاهش فضا و کاهش هزینه تمام شده ارائه شدند. اما چندین پردازنده، الزاماً به معنی افزایش خطی راندمان پردازش نبوده و در حقیقت، افزایش بازدهی در یک سیستم چند هسته ای کاملاً به معماری

1- Application Delivery Controller

نرم افزار وابسته است.

در سطح سیستمی، دوبرابر کردن تعداد پردازنده ها به طور خودکار باعث دوبرابر شدن بازدهی نمی شود، بلکه تغییرات اساسی در طراحی نرم افزار لازم است و بدون این تغییرات، عملاً بخش عمده ای از توان این پردازنده های گرانقیمت چند هسته ای به هدر می رود.

در طراحی یک سیستم چند هسته ای، موضوع حائز اهمیت، عدم هماهنگی سرعت پردازنده و دیگر اجزای سیستم (مانند حافظه و I/O) است که معمولاً مهمترین دلیل بازدهی پایین سیستم می باشد. به علاوه سیستم های چند هسته ای بدون وجود معماری نرم افزاری که بتواند از پردازش موازی پشتیبانی کند، قادر به استفاده بهینه از پردازنده های چند هسته ای نمی باشند. خوشبختانه این محدودیتها قابل برطرف کردن بوده و با ترکیب درستی از معماری صحیح نرم افزار و طراحی بهینه در مدل دسترسی به حافظه می توان بازدهی اینگونه سیستم ها را افزایش داد.

چالشهای طراحی سیستم های چند هسته ای

پردازنده های چند هسته ای، در عین فراهم کردن امکانات و قابلیت های جدید به منظور افزایش بازدهی سیستم، چالشهای جدیدی را نیز در زمینه طراحی سیستم های Application Networking به وجود آورده اند. در این راستا طراحان این سیستم ها با چالشهای زیر در زمینه طراحی روبرو خواهند شد:

۱. **حافظه:** با توجه به این موضوع که سرعت درگاه حافظه همیشه کمتر از سرعت پردازنده است، در صورت بهینه نبودن روش دسترسی به حافظه، این عدم هماهنگی باعث کاهش بازدهی سیستم می گردد. چرا که زمان پردازنده در حین دسترسی به حافظه به دلیل این ناهماهنگی به هدر خواهد رفت. در یک سیستم چند هسته ای، دسترسی همزمان به بخشی از حافظه توسط چند پردازنده مختلف می تواند باعث ایجاد گلوگاه در دسترسی به حافظه شده و تأثیر منفی روی بازدهی کلی سیستم داشته باشد.

۲. **پردازش موازی:** پردازش موازی می تواند با اجرا کردن instruction های متفاوت بر روی چند پردازنده، باعث افزایش راندمان شود. اما معماریهای سنتی نرم افزار که به منظور استفاده از یک پردازنده به وجود آمده اند نمی توانند از این مزیت بهره مند شوند. معماری نرم افزار یک سیستم چند هسته ای باید به گونه ای طراحی شود تا بتواند به صورت بهینه، همزمانی (Concurrency) و دسترسی به منابع مشترک را مدیریت نماید. بدون همچنین تغییری در معماری، مزایای پردازش موازی در پردازنده های چند هسته ای، قابل استفاده نخواهد بود.

۳. **ارتباط بین پروسس ها (IPC^۲):** پردازش موازی نیازمند ارتباط بین پردازنده ها به منظور تبادل اطلاعات مربوط به وضعیت سیستم می باشد تا تمامی هسته ها همزمان مشغول پردازش و انجام کارها شوند و همه کارها به شکل نامطلوبی روی یک هسته انجام نگیرد. در یک سیستم چند هسته ای با پردازش موازی، دشواری و هزینه تعویض و تخصیص حافظه در بین هسته ها، به صورت نمایی با افزایش تعداد هسته ها افزایش می یابد و باعث کاهش بازدهی کلی می شود.

طراحی سیستم های پردازش موازی به طور معمول به دو دسته SMP^۳ و MPP^۴ تقسیم بندی می شود. در سیستم های

2- Inter-Process Communications

3- Symmetric Multi-Processing

4- Massively Parallel Processing

مبتنی بر SMP چندین پردازنده، سیستم عامل، حافظه و دیگر منابع I/O را با یکدیگر به اشتراک می‌گذارند. سیستم عامل، به منظور بهبود بازدهی، taskها را به طور مساوی بین پردازنده‌ها تقسیم می‌نماید. ولی به دلیل سربار نسبتاً زیاد ناشی از Locking منابع مورد استفاده مانند حافظه، این سیستم‌ها دارای محدودیت‌هایی در مقیاس پذیری می‌باشند.

از سوی دیگر، سیستم‌های MPP منابع را در میان پردازنده‌ها به اشتراک نمی‌گذارند. هر پردازنده در MPP، مالک بخش مشخصی از منابع حافظه و سیستم عامل است و به هر پردازنده وظیفه متفاوت و مشخصی داده می‌شود تا بازدهی سیستم به شکل مناسبی افزایش پیدا کند. با وجود این، به دلیل عدم توزیع مناسب بار در سیستم‌های MPP و هزینه بسیار بالای ارتباطات IPC، این سیستم‌ها مقیاس پذیری و افزایش بازدهی قابل قبولی را ارائه نمی‌دهند.

همچنانکه ضریب نفوذ و میزان به کارگیری پردازنده‌های چند هسته‌ای افزایش می‌یابد، طراحی‌های SMP و MPP به خاطر محدودیت‌هایی که بیان شد نمی‌توانند از قابلیت‌های موجود در آن استفاده کنند. بدین منظور لازم است نرم‌افزارهای سیستمی که نیازمند به بازدهی بالا هستند، چالش‌های مرتبط با معماریهای چند هسته‌ای را برطرف نمایند. معماری‌های مورد استفاده در نرم‌افزار که به منظور استفاده از پردازنده‌های تک هسته‌ای به وجود آمده‌اند، می‌باید با در نظر گرفتن پردازش موازی و به منظور کاهش هزینه‌های Locking و IPC بازطراحی شوند. همچنین به طور ویژه، معماری دسترسی به حافظه باید به طور جدی مورد بازبینی و طراحی مجدد قرار گیرد.

طراحی‌های سنتی سیستم معمولاً یکی از روش‌های زیر را به منظور به اشتراک گذاری حافظه، بین هسته‌های پردازشگر در یک سیستم چند هسته‌ای، به کار می‌گیرند:

۱. **حافظه توزیع شده**^۵: در این نوع از سیستم، هر پردازنده دارای فضای حافظه مختص به خود بوده و تبادل داده‌ها بین پردازنده‌ها به صورت داخلی صورت می‌گیرد. اینگونه طراحی به منظور تبادل داده‌ها نیاز به مکانیزم‌های IPC دارد. به همین منظور لازم است داده‌ها قبل از تبادل توسط IPC، آماده سازی شوند که این امر دارای هزینه سربار بالایی می‌باشد. همچنین با توجه به اینکه هر پردازنده دارای حافظه مختص به خود است، لازم است بعضی از داده‌ها در قسمت‌های مختلف کپی شوند که باعث بروز Data Duplication شده و در نتیجه منجر به استفاده ناکارآمد از حافظه و ایجاد محدودیت در مقیاس پذیری سیستم می‌شود.

۲. **حافظه اشتراکی**^۶: در این نوع از طراحی سیستم، تمامی پردازنده‌ها به یک حافظه مشترک دسترسی دارند و می‌توانند بدون در نظر گرفتن موقعیت فیزیکی خود، به آن حافظه دسترسی پیدا کنند. از آنجاییکه هر پردازنده بدون احتیاج به IPC می‌تواند به کل حافظه دسترسی داشته باشد، بنابراین بار اضافی روی بازدهی سیستم تحمیل نخواهد شد. با این وجود، در سیستم‌های حافظه اشتراکی سنتی، به دلیل استفاده همزمان از بلوک‌های حافظه توسط پردازنده‌ها، بین آنها تصادم به وجود می‌آید. در نتیجه منابع حافظه می‌بایستی در هر زمانی که هر کدام از پردازنده‌ها به آنها دسترسی پیدا می‌کند، برای بقیه پردازنده‌ها غیر قابل دسترس شوند. این مشکل که سیستم‌های حافظه اشتراکی سنتی از آن رنج می‌برند، در سیستم‌های چند هسته‌ای، چند برابر می‌شود.

بسیاری از سیستم‌های Application Networking به منظور استفاده از معماری قدیمی، از روش اول استفاده نموده و نرم‌افزار را روی چند هسته اجرا می‌نمایند. اما این روش به دلیل هزینه سربار استفاده از IPC و استفاده نامناسب از حافظه، قابلیت توسعه پذیری لازم را ندارد.

5- Distributed Memory

6- Shared Memory

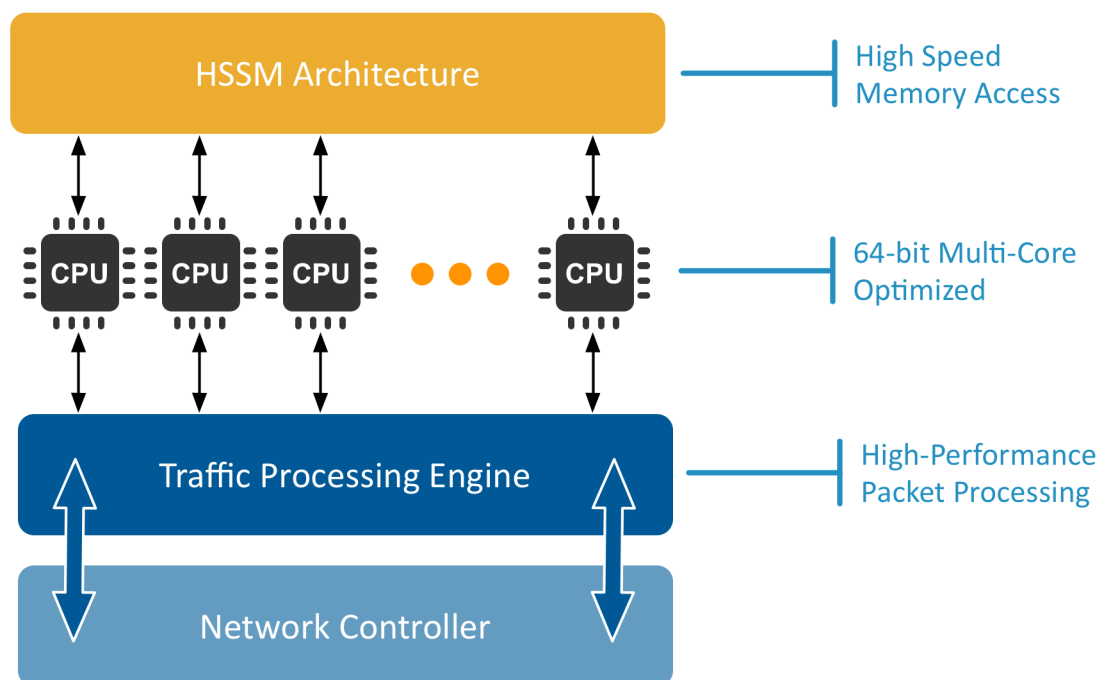
سیستمهای Application Networking مدرن می باید آمادگی لازم را به منظور پردازش ترافیک با سرعت های بالا را داشته باشند که این امر فقط با استفاده از نرم افزارهای بهینه شده برای سیستم های چند هسته ای که برای دسترسی سریع به حافظه بهینه سازی شده باشند امکان پذیر است.

معماری HSSM در NetOS

سیستم «NetOS»، از ابتدا به منظور مقیاس پذیری بر مبنای پردازنده های چند هسته ای بهینه سازی شده است. معماری NetOS، نقاط ضعف و محدودیتهای هر دو مدل طراحی سنتی حافظه که پیشتر اشاره شد را برطرف ساخته و امکان استفاده از تکنولوژی پیشرفته در طراحی سیستم های پردازنده چند هسته ای را فراهم می آورد.

HSSM^۷ یا معماری حافظه اشتراکی با سرعت بالا، محدودیتهای طراحی سنتی را از بین برده و بازدهی سیستم را به طور خطی و بر اساس معماری پردازنده چند هسته ای افزایش می دهد.

همچنین، معماری NetOS مسیر ترافیک عبوری را از مسیر ترافیک مدیریتی جدا می کند. برای ارسال ترافیک اصلی، چندین پردازنده اختصاصی به منظور پردازش موازی و با راندمان بالا در نظر گرفته شده اند. برای کاربری مدیریتی، NetOS یک یا چند پردازنده را متناسب نیاز، به این امر اختصاص می دهد. در نتیجه مدیر شبکه می تواند حتی در زمان اوج ترافیک، بدون نگرانی بازیابی های سیستمی خود را به منظور آگاهی از وضعیت و سلامت سیستم انجام دهد. جداسازی ترافیک اصلی و ترافیک مدیریتی بر روی هسته های جداگانه باعث افزایش انعطاف پذیری و پایداری کلی سیستم می شود.



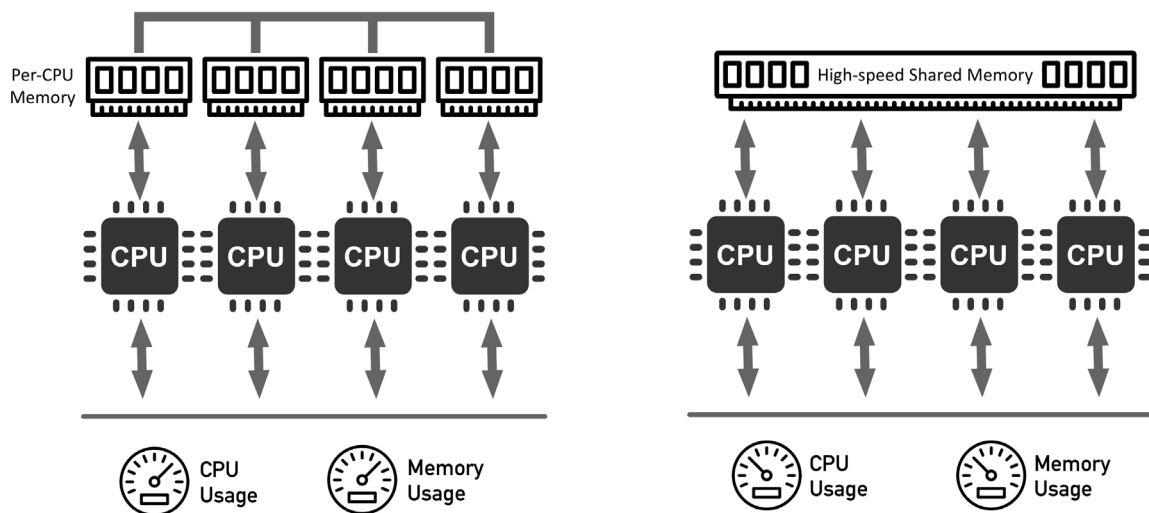
تصویر یک - معماری سطح بالای NetOS

معماری حافظه اشتراکی سرعت بالای NetOS، نیاز به ارتباطات IPC را از میان برده و دیگر نیازی به کپی کردن

7- High-Speed Shared Memory

محتوای حافظه نخواهد بود که این موضوع باعث می شود پردازنده ها با قدرت بیشتری، مهمترین وظایف خود را که پردازش ترافیک است انجام دهند. (مزایای حافظه اشتراکی NetOS در تصویر دو نمایش داده شده است.)

معماری حافظه اشتراکی NetOS استفاده از پردازنده های چند هسته ای گرانتیست و منابع حافظه را بهینه نموده و در مقایسه با سیستم های رایج، اجزای سخت افزاری کمتری احتیاج دارد. اجزای کمتر، کارایی عملیاتی و ضریب اطمینان کلی سیستم را افزایش می دهد.



تصویر دو - مقایسه معماری HSSM و Distributed Memory

مزایای NetOS

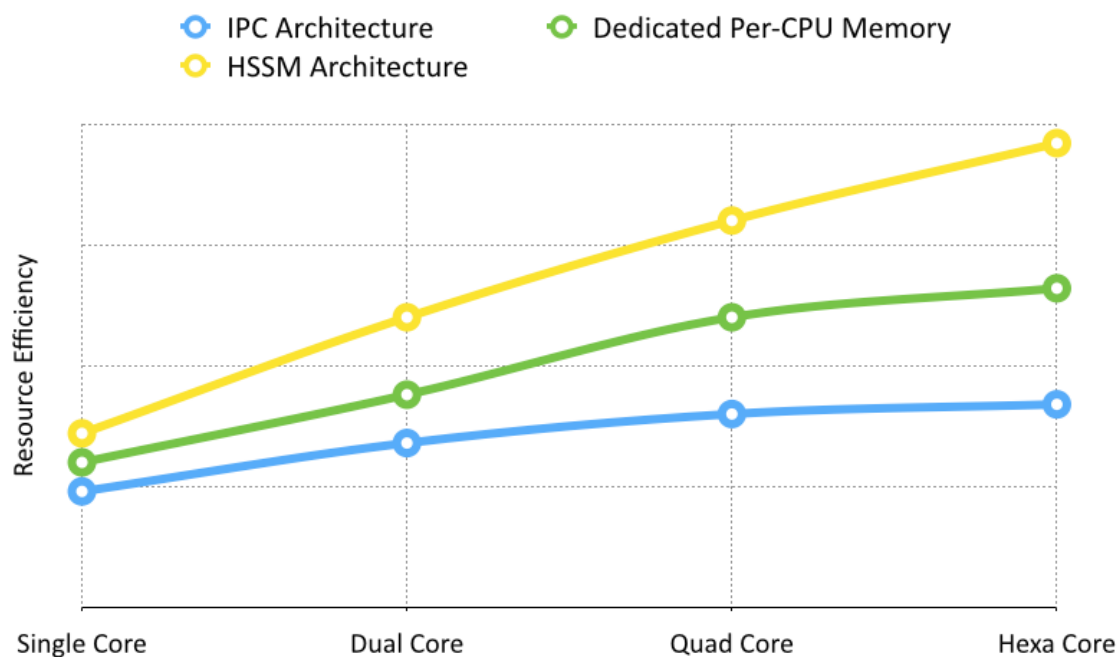
یکی از نتایج استفاده از معماری حافظه اشتراکی سرعت بالای NetOS، نیاز به سخت افزار (پردازنده و حافظه) کمتر است تا به توانایی و راندمان یکسان در حالت طراحی سنتی با معماری سنتی برسند.

پلتفرم NetOS علاوه بر رشد بازدهی و مقیاس پذیری به صورت خطی، ویژگی های دیگری را نیز فراهم می آورد:

- **افزایش بازدهی نرم افزارها:** NetOS به مقدار قابل ملاحظه ای ضریب دسترسی برنامه ها را افزایش داده و همچنین باعث بهبود در سرعت پاسخگویی نرم افزارهای میانی می گردد که نتیجه آن، تجربه کاربری بهتر برای کاربر نهایی می باشد.
- **بازدهی قابل پیش بینی:** NetOS بازدهی را به طور خطی افزایش می دهد که باعث ارایه سطح کیفی مناسب حتی در صورت رشد ترافیک می گردد.
- **کاهش پیچیدگی:** بازدهی بالا و توسعه پذیری سیستم باعث عدم نیاز به اضافه نمودن سخت افزار پیچیده و شبکه را داشته و مدیریت سیستم را به سادگی امکان پذیر می نماید.
- **محافظت از سرمایه گذاری اپراتورها:** با افزایش ترافیک شبکه، سرویس دهندگان می توانند خدمات خود

را توسعه دهند و در عین حال با استفاده از زیربنای موجود، از سرمایه گذاری خود محافظت کنند.

- **کاهش هزینه‌های سرمایه گذاری:** راندمان و کارایی بیشتر نسبت به تجهیزات مشابه، به سرویس دهندگان این امکان را می‌دهد از هزینه اولیه خود بهره بیشتری ببرند.
- **کارایی بیشتر دیتاسنتر و بازده اقتصادی بهتر:** کاهش میزان برق مصرفی، سرمایش و فضای مورد نیاز کمتر باعث کاهش هزینه‌ها می‌شود.



تصویر سه - مقیاس پذیری خطی در معماری HSSM

جمع بندی

پلتفرم NetOS ابتدا بر پایه اصول طراحی مدرن و حافظه اشتراکی سرعت بالا ساخته شده است تا بتواند پاسخگوی نیاز روزافزون Application Networking باشد. NetOS در سیستمهای پردازنده چند هسته‌ای، راندمان را به صورت خطی افزایش داده و در مقایسه با طراحیهای سنتی مشابه، سخت افزار کمتری را برای رسیدن به نتایج مشابه نیاز دارد.

در نتیجه، سرویس دهندگان می‌توانند سیستم کارآمدتری را در اختیار داشته باشند که می‌تواند بازدهی بیشتری را فراهم نماید و این به منزله فراهم کردن تجربه بهتر برای کاربران و بازده اقتصادی بهتر از نظر هزینه و بودجه می‌باشد.