بسمه تعالی

عنوان مقاله:

شبکه های مخابراتی *IMS_BASED*

و

CSCF ها

توسط : علی ثاقب موفق

فروردین ۱۳۹۱

مقدمه:

شرکت ها و سازمان های مخابراتی برای حفظ لبه رقابتی خود همواره به دنبال روشهایی برای نوآوری و گسترش سرویس های خود به مشترکین می باشند به طوریکه افزایش سرعت وکاهش هزینه را به همراه داشته باشد. لذا بسیاری از شرکتهای مخابراتی ابداعات و سایر کاربردهای انتهایی خود را به سمت IP سوق داده اند .

تکنولوژی VOIP به لحاظ اینکه چندین پاکت اطلاعاتی را تحت مسیرهای مختلف در یک زمان عبور می دهد باعث می شود که شرکتها بتوانند انبوهی از اطلاعات را بطور موثرتر و کم هزینه تر نسبت به شبکه های سوئیچینگ مداری سنتی عبور دهند. تکنولوژی VOIP بطور همزمان صدا، داده و فیلم را انتقال می دهد و پهنای باند را بین کاربردهای مختلف تقسیم و به اشتراک می گذارد لذا نسبت به TDM از منابع شبکه موثرتر و بهینه استفاده میکند .

امروزه همه شرکتها در تلاش هستند تا بهترین حرکت از نقطه A یعنی TDM را به سمت نقطه B یعنی IP داشته باشند و این مهاجرت بدون شناخت کامل CSCF ها امکان پذیر نمی باشد.

سرویسهای *CSCF*

سرویس CSCF یک فانکشن و قطعه مرکزی برای سیگنالینگ و کنترل در IMS است که به سه بخش , serving CSCF Interrogating CSCF , Proxy CSC*F* تقسیم می شود که هر کدام عملکرد خاص خود را دارند. مثلا P-CSCF برای پیام های sip یک پراکسی بوده و برای ارتباط مستقیم با لایه Transport می باشد. ضمن اینکه اولین نقطه سیگنالینگ در IMS برای هر نقطه پایانی محسوب می شود.

زمانیکه یک دستگاه واقع در نقطه پایانی شبکه مثل گوشی موبایل به یک شبکه ip مثل GPRS دسترسی می یابد در این نقطه یک رویداد را خواهد داشت که توسط اولین سیگنالینگ به P-CSCF واقع می شود . همانگونه که از نام P-CSCF پیداست، یک پراکسی برای همه پیام های SIP از نقطه پایانی تا بقیه شبکه است و معمولا در شبکه خانگی است اما در شبکه قابل رویت نیز قرار می گیرد . (Home network – visited network)

پراکسی P-CSCF از DNS Lookup برای اینکه بفهمد چه *I-CSCF* ی پیام های sip می فرستد استفاده می کند به طوریکه یک *I-CSCF* ممکن است در خود شبکه و یا در شبکه دیگری باشد (domain , I-CSCF).

پراکسیP-CSCF تصمیمات سیاستگذاری را نیز پاسخگوست. S-CSCF برای ارتباط با AS یا همان Application Server در بخش request و تقاضاها متعهد است و براساس دریافت یک تقاضای ثبت پیام sip از یک I-CSCF از سرویس S-CSCF کمک گرفته و برای ثبت از HSS پرسش می کند . مهم است که بدانیم چه S-CSCF هایی باید برای کنترل نشست پایانه پاسخگو باشد. کار اصلی I-CSCF این است که پراکسی بین P-CSCF بعنوان نقطه ورودی و S-CSCF بعنوان نقطه کنترل برای تقاضاها و کاربردها در بخش application باشد.

فرایند ثبت مکالمه

سرویس p-cscf یک درخواست پیام sip دریافت کرده و جستجوی DNS را برای یافتن I-CSCF مناسب انجام می دهد تا پیام را مسیر دهی نماید.

زمانیکه I-CSCF پیام SIP را دریافت کرد یک HSS را برای تعیین *s-cscf* مرتبط با ترمینال پایانی اجرا خواهد کرد. (home subscriber server) و سپس پیام sip را به s-cscf جهت رفتار بعدی forward می کند . بعلاوه اینکه s-cscf می تواند بعنوان یک ثبت کننده عمل کرده و برای مسیریابی همه پیام های sip به سرور برنامه های کاربردی یا AS مسئول بوده و اجازه می دهد تا کنترل نشست سطح کنترل با منطق کاربردی سطح کاربرد تعامل داشته باشد.

برای انجام اینکار S-CSCF از اطلاعات بدست آمده از HSS به شکل IFC *(* initial filter criteria *)* استفاده می کند. FC شامل قوانینی است که در سطح Application قرار دارند و نحوه تعامل و محل پیام *های*sip را تعریف می کند که باید به AS های مختلف مسیردهی شوند. پراکسی S-CSCF ممکن است بعنوان secondary filter criteria *(*SFC*)* عمل کند که از AS حاصل شده و در طی course پیام رسانی با آنها به CSCF نزدیک است . عناصر شبکه ای AS و HSS مهم هستند.

سرویس SBC

سرویس SBC یک مجموعه عملیات استاندارد نیست بلکه طیف وسیعی از مباحثی است که با سرویس VOICE و Multimedia بر روی زیرساخت ip رخ می دهد و شامل :

- امنیت و جلوگیری از استفاده بد از سرویس جهت حصول اطمینان از کیفیت سرویس(QOS)
- نظارت و مونیتورینگ اهداف صورتحساب گیری و regulatory
- حفظ حریم خصوصی حامل و اطلاعات کاربر
- بررسی و تحلیل مشکلات پروتکل voip که از استفاده گسترده firewall ها و NAT رخ می دهد و آرایه ای از پروتکل های مختلف و لهجه های مورد استفاده در شبکه های VOIP را پشتیبانی می کند.

دستگاهی که در شبکه دسترسی یا Access است تعین هویت کاربر اولیه را انجام می دهد. دستگاه واقع در EDGE، سیاست دسترسی را به محدود نمودن حمله DOS اجبار نموده و از دزدی پهنای باند جلوگیری می کند و نهایتا دستگاه واقع در CORE یا هسته ممکن است استفاده کلی را برای یک گروه خاص کاربران محدود کند و حملات DOS توزیع شده را نیز کشف نماید.

SBC می تواند امنیت و پشتیبانی را در مقابل موارد ذیل فراهم کند:

- دسترسی غیرمجاز به شبکه مطمئن
- تلفن های نامعتبر و بد مثل حملات از کارانداختن سرویس یا DOS
- دزدی پهنای باند توسط کاربران مجاز
- شرایط غیر معمول شبکه مثل یک بحران بزرگ

منابع معمولی که به پشتیبانی نیاز دارند عبارتند از پهنای باند لینک های دسترسی و ظرفیت پردازش روی سرورهای شبکه و به طور کلی پیوندهای شبکه هسته CORE به جهت جلوگیری از bottle neck شدن به طور ارزان و بیش از اندازه مهیا می شوند. همچنین برای فراهم سازی امنیت فوق ، SBC باید :

- شناسائی و تعیین هویت هر کاربر و تعیین اولویت هر مکالمه را انجام دهد.
- محدودیت میزان CALL و استفاده از منابع برای جلوگیری از overload را انجام دهد.
- اعتباردهی هر جریان رسانه و طبقه بندی و مسیردهی داده برای اطمینان از QOS مناسب
- جلوگیری از دسترسی غیر مجاز برای سیگنالینگ و ترافیک رسانه

کیفیت سرویس

عملیات کیفیت سرویس QOS بطور نرمال با مکانیزم طبقه بندی بهم پیوسته انجام می شود . برای مثال Diff serv که overhead رزرو پهنای باند را برای هر جریان خاص برمی دارد.

بنا بر دلایل رگولاتوری مثل QOS و wire tapping و دلایل تجاری مثل صورتحساب و کشف دزدی، استفاده از شبکه ممکن است به نظارت و مونیتورینگ نیاز داشته باشد. تجهیزات مونیتورینگ به هوشمندی مناسبی برای درک سیگنالینگ و پروتکل رسانه نیاز دارند . آنها از میان جریان و سیگنالینگ رسانه در نقطه ای قرار می گیرند. SBC این نیازمندیها را برای همه ترافیک عبوری از میان SBC جهت ورود به شبکه برآورده می سازد. آنها یک راه حل توزیع شده مقیاس پذیر را برای این فعالیت متمرکز برروی پردازش فراهم می کنند.

حفظ حریم خصوصی :

دو نوع از اطلاعات زیر بایستی که محافظت شوند :

- اطلاعات راجع به شبکه هسته CORE که ممکن است دارای اطلاعات حساس تجاری برای رقبا محسوب شود و یا اینکه به حمل شبکه کمک کند.
- اطلاعات کاربری که نمی خواهد اطلاعاتش عمومی گردد.

SBC می تواند اطلاعات محرمانه را قبل از ترک شبکه هسته، از پیام بردارد. این اطلاعات شامل جزئیات توپولوژی شبکه داخلی و مسیریابی سیگنالینگ از میان شبکه هسته است. همچنین می تواند از طریق سیگنالینگ یا relay ، آدرس واقعی کاربر را مخفی کند.

بررسی مسائل پروتکل VOIP :

سیستم SBC بعنوان Gateway برای شبکه های غیر متجانس عمل می کند و تفاوت پروتکل های مورد استفاده در شبکه های دسترسی و هسته را مخفی می کند که شامل موارد ذیل است :

- مخفی سازی توپولوژی شبکه دسترسی شامل پیچیدگی مسیردهی از میان firewall , NAT و همپوشانی فضاهای آدرس VPN یا فضاهای آدرس IP اختصاصی است.
- تعامل بین دستگاهها و شبکه هایی با قابلیت های مختلف مثل تبدیل بین SIP و سیگنالینگ H.۳۲۳ یا بین IPV۴ و *IP*V۶ یا حتی نسخه های مختلف *H.*۳۲۳
- تبدیل جریان های رسانه بین codec های ناسازگار

بازنگری IMS

IMS معماری کنترلی ۳Gpp برای شبکه مخابراتی نسل آتی است. این معماری برای محدوده وسیعی از سرویس های packet based و realtime اپراتورها طراحی شده است که شارژینگ time based را بخوبی شارژینگ سرویس و پاکت انجام می دهد. همچنین کیفیت سرویس، مکانیزم های شارژینگ انعطاف پذیر و پذیرش LI را انجام می دهد.

معماری IMS چندین ابزار عمومی مثل call control و حافظه پیکربندی در اختیار می دهد که برای توسعه کار و سرویس جدید نیاز کمی به کار توسعه ای خواهیم داشت. در نتیجه IMS می تواند سرویس های جدید را سریعتر و ارزان تر گزارش دهد(در مقایسه با سرویس های تلفنی و طرحهای یکپارچه سنتی). IMS فرمت و قالبی را برای توسعه سرویس های مکالمه و سرویس های پیشرفته فراهم می کند که شامل پیام دهی چند رسانه تجمیع وب سرویس مبتنی بر حضور *Push to* talk است.

استفاده از اینترفیس های استاندارد رقابت بین عرضه کنندگان را افزایش می دهد بطوریکه اپراتورها به یک اینترفیس خاص مقید نمی شوند . معماری ۳Gpp به سه لایه اصلی تقسیم می شود هر کدام از لایه ها یا سطوح با یک تعداد نام های مشابه استفاده می شوند سطح کاربردی یا سرویس، سطح کنترل یا سیگنالینگ و سطح انتقال یا کاربر.

سطح کاربردی

سطح کاربردی یک زیرساخت برای تدارک و مدیریت سرویس ها فراهم میکند و اینترفیس های استاندارد را برای فانکشنالیتی مشترک طبق ذیل تعریف می کند:

- حافظه پیکربندی ، مدیریت هویت ، وضعیت کاربر (مثل حضور و موقعیت) که توسط HSS نگهداری می شود.

- سرویس های صورتحساب گیری که توسط CGF فراهم شده است (charging geateway function)
- کنترل مکالمات صوت و ویدئو و پیام رسانی که توسط سطح کنترل فراهم می شود.

این سطح شبکه IPV۶ قابلیت QOS آن فعال شده است. این زیرساخت برای فراهم نمودن محدوده وسیعی از سرویس های p۲p و چند رسانه ای سروری ip طراحی شده است. اگر چه IPV۶ برای این سطح انتقال تعریف شده ، بسیاری از توسعه های اصلی بر مبنای IPV۴ موجود و آدرس های IPV۴ خصوصی ساخته شده است به طوریکه NAT را در مرزهای هر دامین آدرس و مسیریابی و پیچیدگی های همراه با آن را در مرزها معرفی می کند.

سطح کنترل :

سطح کنترل بین سطح انتقال و کاربردی است و همه سیگنالینگهای تلفنی را مسیردهی می کند و به سطح سیگنال می گوید که چه ترافیکی را اجازه داده تا رد شود. همچنین اطلاعات صورتحساب را برای استفاده شبکه تولید می کند .

در هسته این سطح کنترل ، *CSCF* ها قرار دارند که شامل عملکردهای زیر است :

P-CSCF اولین نقطه تماس برای کاربران با IMS است و امنیت پیامها بین شبکه و کاربر و تخصیص منابع برای جریان رسانه را انجام می دهد.

I-CSCF اولین نقطه تماس از شبکه های هم نظیر است ، *I*-CSCF برای پرسش از HSS جهت تعیین *S*-CSCF برای کاربر مسئول بوده و ممکن است توپولوژی اپراتور را از شبکه های نظیر مخفی کند. *S*-CSCF یا Saving – CSCF مغز مرکزی است . s-cscf پردازش موارد ثبت شده، موقعیت کاربر تعیین هویت شده و پردازش مکالمه را انجام می دهد که شامل مسیردهی مکالمات به برنامه های کاربردی است. همچنین عملیات*s*-cscf توسط سیاستهای ذخیره شده در HSS کنترل می گردد.

این معماری توزیع شده راه حل مقیاس پذیر و انعطاف پذیر را فراهم می کند . برای مثال هر تابع CSCF می تواند اطلاعات صورتحساب را برای هر عمل تولید کند.

جریان های سیگنالینگ تلفنی از تلفن زننده و از میان *P*-CSCF شبکه رویت شده به *S*-CSCF خانگی او عبور می کند . این سیگنالینگ سپس به بخش فراخوانی شده از طریق *S*-CSCF عبور می یابد. سطح کنترل ، ترافیک کاربری را از میان RACS کنترل می کند که شامل تابع تصمیم گیری سیاست (PDF) است که سیاست داخلی را روی منابع پیاده سازی می کند .