بسم الله الرحمن الرحیم

بررسی شبکه‌های NGN و پروتکل‌های SIP&H.323

تهیه کنندگان:

مهندس یوسف قلی‌پور

مهندس ابوالفضل التجایی

«ن والقلم و ما یسطرون»

انتشارات
دانشگاه آزاد اسلامی یزد

۱۳۹۳

تقدیم به:

وجود مقدس آقا امام زمان(عج)

با تشکر از همه عزیزانی که ما را در این کار همراهی کردنـد؛ و همچنـین از اسـتاد عزیز و ارجمند جناب آقای مهندس امید توکلی برای راهنمایی‌هـا وکمـک‌هـای فـراوان ایشان، مراتب تقدیر و تشکر را داریم.

چکیده

مفهوم یک شبکه‌ی مجتمع باند وسیع در طول سال‌های اخیر بسط و گسترش یافته و با عنوان شبکه‌های نسل NGN[1]، نامگذاری شده است. در این راستا، ITU-T فعالیت‌های مربوط به استانداردسازی را با همکاری گروه‌ها و مؤسسات محلی دیگری رهبری نموده است.

با در نظر گرفتن طبیعت و ماهیت فراگیر اینترنت و زیرساخت‌های مرتبط با آن، و نیز کاربردهای مختلف آن نظیر: email، انتقال فایل و همچنین وب، می‌توان سیستم‌های مبتنی بر IP را به عنوان اساس و پایه NGN در نظر گرفت. لذا NGN در واقع یک شبکه مبتنی بر IP بهبود یافته خواهد بود. به طور کلی می‌توان‌پذیرفت که تفاوت اصلی بین سرویس‌های مرسوم مخابراتی کنونی و NGN، گذر از شبکه‌های مجزا و کاربرد محور به یک شبکه واحد با قابلیت انجام تمامی سرویس‌ها می‌باشد. در سرویس‌های تلفنی، این انتقال شامل گذر از یک شبکه Circuit-Switched به یک شبکه Packet-Switched می‌باشد. تمرکز و هدف نهایی فعالیت‌های در حال انجام و نیز انجام شده در زمینه NGN نوعی اطمینان حاصل کردن از توانایی‌های شبکه‌های مبتنی بر IP نسل آینده در رسیدن به استانداردهای سرویس‌های موجود شبکه‌های مخابراتی نه تنها برای سرویس‌های تلفنی بلکه برای مجموعه وسیعی از کاربردهای چندرسانه‌ای کنونی و آینده می‌باشد.

در این کتاب ساختار شبکه و اصول کلی NGN بررسی شده است و در این راستا مسایل خاصی که در طراحی این شبکه‌ها وجود دارد مورد مطالعه قرار می‌گیرد. برای این منظور موضوعاتی مانند VOIPو پروتکل‌های SIP&H.323، تامین کیفیت سرویس، ارتباط بین شبکه‌های سیمی و بی‌سیم بررسی شده و راه حل‌های موجود برای دستیابی به شبکه‌ای که بتواند سرویس‌های مورد نیاز کاربر را در هر زمان وهر مکان ارایه کند آورده شده است. در پایان نرم‌افزارهای شبیه‌ساز شبکه همچنین پروتکل‌های ارتباطی اجمالاً بررسی شده‌اند.

---

[1] Next Generation Networks (NGN)

مقدمه

در دهه‌ی گذشته پیشرفت قابل ملاحضه‌ای در مباحث مخابراتی و کامپیوتری صورت گرفته و این دو صنعت بیشتر از هر زمان دیگری به یکدیگر نزدیک شده‌اند به نحوی که امروزه به صورت گسترده‌ای شاهد مجتمع‌سازی و تلفیق تجهیزات کامپیوتری و شبکه‌های تلفنی با یکدیگر هستیم. با توجه به این که در شرایط فعلی تقاضاهای مشترکان شبکه‌های تلفنی از حد ارتباطات عادی فراتر رفته و به سمت توانایی‌های ارتباطی متنوع سوق پیدا کرده اپراتورها با ارائه‌ی سرویس‌های پهن باند سعی در پاسخ‌گویی به این تقاضا را دارند.

در این میان مفهوم جدیدی از شبکه‌های پهن باند با نام شبکه‌های نسل بعد (NGN) مطرح شده است که می‌توان ویژگی‌های اساسی آن را با توجه به مشکلاتی که پیش روی اپراتورهای شبکه قرار گرفته است تعریف کرد. مواردی مثل نیاز به یکپارچه‌سازی و ادغام سرویس‌های مختلف شبکه مثل دیتا، صوت، تلفن، چندرسانه‌ای و هم چنین ارائه‌ی سرویس‌های محبوب اینترنت مثل پیام‌های فوری، سرویس‌های پخش تلوزیونی، در نهایت ایجاد قابلیت دسترسی به سرویس‌ها در هر زمان و هر مکان برای مشترکان (مخصوصاً به صورت سیار) را می‌توان از جمله مواردی دانست که NGN به راحتی قادر به حل آن است. تا به حال پروتکل‌هایی برای شبکه‌های NGN ارائه و معرفی گردیده است که می‌توان به پروتکل‌هایی همچون SIP، H.323 و ... اشاره نمود.

در این کتاب ابتدا به طور مختصر درباره‌ی شبکه و ساختار آن صحبت می‌کنیم بعد از آن به NGN پرداخته سپس به معرفی VOIP و دو پروتکل استاندارد آن (SIP&H.323) می‌پردازیم. در ادامه، بررسی کیفییت سرویس را توضیح خواهیم داد، و پس از آن معرفی برنامه‌های کاربردی شبیه‌سازی و پروتکل‌های شبکه را ارائه کرده‌ایم.

امید است که گامی در جهت استغنای علمی ایران اسلامی برداشته باشیم.

در پایان از همه‌ی خوانندگان اعم از اساتید، دانشجویان و همه‌ی کارشناسان تقاضا می‌گردد کلیه‌ی نظرات و پیشنهادات خود و کمی‌ها وکاستی‌های این نوشته را از طریق ایمیل (y.gholipour@yahoo.com) با اینجانب در میان بگذارند.

تابستان ۱۳۹۳

فهرست مطالب

فصل اوّل
ساختار شبکه

شبکه

یک شبکه شامل مجموعه‌ای از دستگاه‌ها (کامپیوتر، چاپگر و ...) بوده که با استفاده از یک روش ارتباطی (کابل، امواج رادیویی، ماهواره) و به منظور اشتراک منابع فیزیکی (چاپگر) و اشتراک منابع منطقی (فایل) به یکدیگر متصل می‌شوند. شبکه‌ها می‌توانند با یکدیگر نیز مرتبط شده و شامل زیر شبکه‌هایی باشند.

شکل ۱.۱

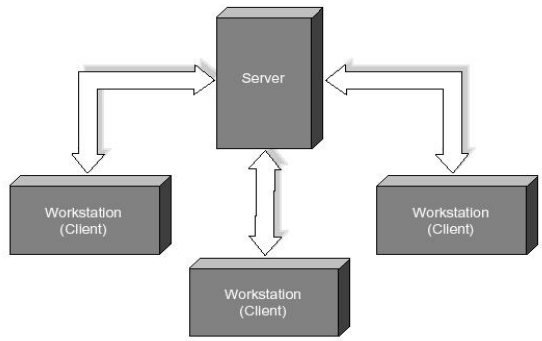
۱. ۱. تفسیم‌بندی شبکه ها

شبکه‌های کامپیوتری را بر اساس مؤلفه‌های متفاوتی تقسیم‌بندی می‌کنند. در ادامه به برخی از متداول‌ترین تقسیم بندی‌های موجود اشاره می‌گردد.

۱. ۱. ۱. تقسیم‌بندی بر اساس نوع وظایف

کامپیوترهای موجود در شبکه را با توجه به نوع وظایف مربوطه به دو گروه عمده: سرویس دهندگان[1] و یا سرویس گیرندگان[2] تقسیم می‌نمایند. کامپیوترهایی که در شبکه برای سایر کامپیوترها سرویس‌ها و خدماتی را ارائه می‌کنند، سرویس‌دهنده نامیده می‌شوند. کامپیوترهایی که از خدمات و سرویس‌های ارائه شده توسط سرویس دهندگان استفاده می‌کنند، سرویس‌گیرنده نامیده می‌شوند.

در شبکه‌های سرویس‌دهنده و سرویس‌گیرنده (Client-Server)، یک کامپیوتر در شبکه نمی‌تواند هم به عنوان سرویس‌دهنده و هم به عنوان سرویس‌گیرنده، انجام وظیفه نماید.

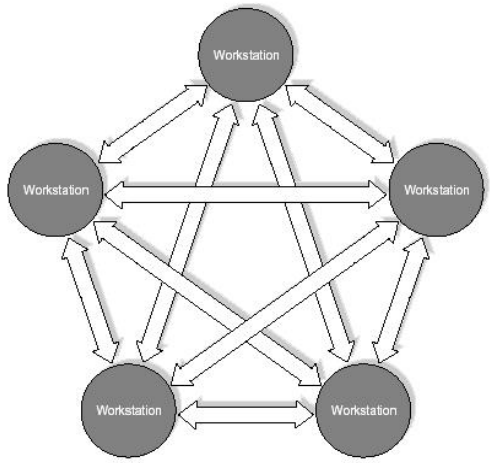


شکل ۱.۲

در شبکه‌های نظیر به نظیر، یک کامپیوتر می‌تواند هم به صورت سرویس‌دهنده و هم به صورت سرویس‌گیرنده انجام وظیفه نماید.

---

[1] Servers
[2] Clients



شکل ۳. ۱

یک شبکه محلی در ساده‌ترین حالت از اجزای زیر تشکیل شده است:

۱. دو کامپیوتر شخصی: یک شبکه می‌تواند شامل چند صد کامپیوتر باشد. حداقل یکی از کامپیوترها می‌بایست به عنوان سرویس‌دهنده مشخص گردد. (در صورتی که شبکه از نوع Client-Server باشد). سرویس‌دهنده، کامپیوتری است که هسته اساسی سیستم عامل بر روی آن نصب خواهد شد.

۲. یک عدد کارت شبکه (NIC) برای هر دستگاه: کارت شبکه نظیر کارت‌هایی است که برای مودم و صدا در کامپیوتر استفاده می‌گردد. کارت شبکه مسئول دریافت، انتقال، سازماندهی و ذخیره‌سازی موقت اطلاعات در طول شبکه است. به منظور انجام وظایف فوق کارت‌های شبکه دارای پردازنده، حافظه و گذرگاه اختصاصی خود هستند.

۲. ۱. ۱ تقسیم‌بندی بر اساس توپولوژی

الگوی هندسی استفاده شده جهت اتصال کامپیوترها، «توپولوژی» نامیده می‌شود. توپولوژی انتخاب شده برای پیاده‌سازی شبکه ها، عاملی مهم در جهت کشف و برطرف نمودن خطا در شبکه خواهد بود. انتخاب یک توپولوژی خاص نمی‌تواند بدون ارتباط با محیط انتقال و روش‌های استفاده از خط مطرح گردد. نوع توپولوژی انتخابی جهت

اتصال کامپیوترها به یکدیگر، مستقیماً بر نوع محیط انتقال و روش‌های استفاده از خط تأثیر می‌گذارد. با توجه به تأثیر مستقیم توپولوژی انتخابی در نوع کابل کشی و هزینه‌های مربوط به آن، می‌بایست با دقت و تأمل به انتخاب توپولوژی یک شبکه تلاش کرد. عوامل مختلفی جهت انتخاب یک توپولوژی بهینه مطرح می‌شود. مهمترین این عوامل شامل:

۱. هزینه: هر نوع محیط انتقال که برای شبکه LAN انتخاب گردد، در نهایت می‌بایست عملیات نصب شبکه در یک ساختمان پیاده‌سازی گردد. عملیات فوق فرآیندی طولانی جهت نصب کانال‌های مربوطه به کابل‌ها و محل عبور کابل‌ها در ساختمان است. در حالت ایده آل کابل کشی و ایجاد کانال‌های مربوطه می‌بایست قبل از تصرف و به کارگیری ساختمان انجام گرفته باشد. به هرحال می‌بایست هزینه نصب شبکه بهینه گردد.

۲. انعطاف‌پذیری: یکی از مزایای شبکه‌های LAN، توانایی پردازش داده‌ها و گستردگی و توزیع گره‌ها در یک محیط است. بدین ترتیب توان محاسباتی سیستم و منابع موجود در اختیار تمام استفاده کنندگان قرار خواهد گرفت. در ادارات همه چیز تغییر خواهد کرد. (لوازم اداری، اتاق‌ها و ...). توپولوژی انتخابی می‌بایست بسادگی امکان تغییر پیکربندی در شبکه را فراهم نماید. مثلا" ایستگاهی را از نقطه‌ای به نقطه دیگر انتقال و یا قادر به ایجاد یک ایستگاه جدید در شبکه باشیم.

سه نوع توپولوژی رایج در شبکه‌های LAN استفاده می‌شود:

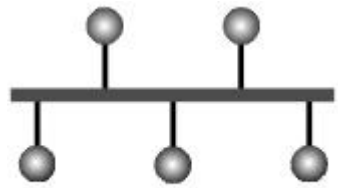
۱. گذرگاه (BUS)

۲. ستاره (STAR)

۳. حلقه (RING)

توپولوژی گذرگاه (BUS):

یکی از رایج‌ترین توپولوژی‌ها برای پیاده‌سازی شبکه‌های «LAN» است. در مدل بالا از یک کابل به عنوان ستون فقرات اصلی در شبکه استفاده شده و تمام کامپیوترهای موجود در شبکه شامل سرویس‌دهنده، سرویس‌گیرنده به آن متصل می‌شوند.



شکل ۱.۴

مزایای توپولوژی گذرگاه (BUS):

۱. کم بودن طول کابل: به دلیل استفاده از یک خط انتقال جهت اتصال تمام کامپیوترها، در توپولوژی فوق از کابل کمی استفاده می‌شود. این موضوع باعث پایین آمدن هزینه‌ی نصب و ایجاد تسهیلات لازم در جهت پشتیبانی شبکه خواهد بود.

۲. ساختار ساده: توپولوژی BUS دارای یک ساختار ساده است. در این مدل فقط از یک کابل برای انتقال اطلاعات استفاده می‌شود.

۳. توسعه آسان: یک کامپیوتر جدید را می‌توان به راحتی در نقطه‌ای از شبکه اضافه کرد. در صورت اضافه شدن ایستگاه‌های بیشتر در یک سگمنت، می‌توان از تقویت کننده‌هایی به نام «تکرارکننده‌ها» استفاده کرد.

معایب توپولوژی گذرگاه (BUS):

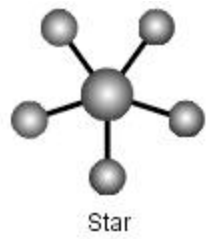
۱. مشکل بودن عیب‌یابی: با اینکه سادگی موجود در توپولوژی BUS امکان بروز اشتباه را کاهش می‌دهد، ولی در صورت ایجاد خطا کشف آن ساده نخواهد بود. در شبکه‌هایی که از توپولوژی فوق استفاده می‌کنند، کنترل شبکه در هر گره دارای مرکزیت نبوده و در صورت بروز خطا می‌بایست نقاط زیادی به منظور تشخیص خطا بازدید و بررسی شوند.

۲. ایزوله‌کردن خطا مشکل است: در صورتی که یک کامپیوتر در توپولوژی فوق دچار مشکل گردد، می‌بایست کامپیوتر را در محلی که به شبکه متصل است رفع عیب نمود. در موارد خاص می‌توان یک گره را از شبکه جدا کرد. در حالتی که اشکال در محیط انتقال باشد، تمام یک سگمنت می‌بایست از شبکه خارج شود.

۳. ماهیت تکرارکننده ها: در مواردی که برای توسعه شبکه از تکرارکننده‌ها استفاده می‌شود، ممکن است در ساختار شبکه تغییراتی نیز داده شود. این موضوع نیازمند به کارگیری کابل بیشتر و اضافه نمودن اتصالات مخصوص شبکه است.

توپولوژی ستاره (STAR):

در این نوع توپولوژی همان گونه که از نام آن مشخص است، از مدلی شبیه «ستاره» استفاده می‌گردد. در این مدل تمام کامپیوترهای موجود در شبکه معمولاً به یک دستگاه خاص با نام «هاب» متصل خواهند شد.



شکل۵. ۱

مزایای توپولوژی ستاره:

۱. سادگی سرویس شبکه: توپولوژی ستاره شامل تعدادی از نقاط اتصالی در یک نقطه‌ی مرکزی است. ویژگی فوق تغییر در ساختار و سرویس شبکه را آسان می‌نماید.

۲. در هر اتصال یک دستگاه: نقاط اتصالی در شبکه ذاتاً دارای توانایی و قابلیت اشکال هستند. در توپولوژی ستاره اشکال در یک اتصال، باعث خروج آن خط از شبکه و سرویس و اشکال زدایی خط مزبور است. عملیات فوق تأثیری در عملکرد سایر کامپیوترهای موجود در شبکه نخواهد گذاشت.

۳. کنترل مرکزی و عیب‌یابی: با توجه به این مسئله که نقطه‌ی مرکزی مستقیماً به هر ایستگاه موجود در شبکه متصل است، اشکال‌ها و ایرادها در شبکه به سادگی تشخیص و مهار خواهند گردید.

۴. روش‌های ساده دستیابی: هر اتصال در شبکه شامل یک نقطه‌ی مرکزی و یک گره‌ی

جانبی است. در چنین حالتی دستیابی به محیط انتقال جهت ارسال و دریافت اطلاعات دارای الگوریتمی ساده خواهد بود.

معایب توپولوژی ستاره:

۱. زیاد بودن طول کابل: به دلیل اتصال مستقیم هر گره به نقطه‌ی مرکزی، مقدار زیادی کابل مصرف می‌شود. با توجه به اینکه هزینه‌ی کابل نسبت به تمام شبکه، کم است، تراکم در کانال کشی جهت کابل‌ها و مسائل مربوط به نصب و پشتیبانی آنها به طور قابل توجهی هزینه‌ها را افزایش خواهد داد.

۲. مشکل بودن توسعه: اضافه نمودن یک گره‌ی جدید به شبکه مستلزم یک اتصال از نقطه‌ی مرکزی به گره‌ی جدید است. با اینکه در زمان کابل کشی پیش بینی‌های لازم جهت توسعه در نظر گرفته می‌شود، ولی در برخی حالات نظیر زمانی که طول زیادی از کابل مورد نیاز بوده، و یا اتصال مجموعه‌ای از گره‌های غیر قابل پیش بینی اولیه، توسعه شبکه را با مشکل مواجه خواهد کرد.

۳. وابستگی به نقطه مرکزی: در صورتی که نقطه‌ی مرکزی (هاب) در شبکه با مشکل مواجه شود، تمام شبکه غیرقابل استفاده خواهد بود.

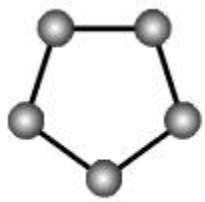
توپولوژی حلقه (RING):

در این نوع توپولوژی تمام کامپیوترها به صورت یک حلقه به یکدیگر مرتبط می‌گردند. تمام کامپیوترهای موجود در شبکه (سرویس‌دهنده، سرویس‌گیرنده) به یک کابل که به صورت یک دایره بسته است، متصل می‌گردند. در مدل فوق هر گره به دو و فقط دو همسایه‌ی مجاور خود متصل است. اطلاعات از گره‌ی مجاور دریافت و به گره‌ی بعدی ارسال می‌شوند. بنابراین داده‌ها فقط در یک جهت حرکت کرده و از ایستگاهی به ایستگاه دیگر انتقال پیدا می‌کنند.

مزایای توپولوژی حلقه:

۱. کم بودن طول کابل: طول کابلی که در این مدل به کار گرفته می‌شود، قابل مقایسه به توپولوژی BUS نبوده و طول کمی دارد. ویژگی فوق باعث کاهش تعداد اتصالات

(کانکتور) در شبکه شده و درصد اعتماد به شبکه را افزایش خواهد داد.



شکل ۶. ۱

۲. نیاز به فضایی خاص جهت انشعابات در کابل کشی نخواهد بود: به دلیل استفاده از یک کابل جهت اتصال هر گره به گره‌ی همسایه اش، اختصاص محل‌هایی خاص به منظور کابل کشی ضرورتی نخواهد داشت.

۳. مناسب جهت فیبر نوری: استفاده از فیبر نوری باعث بالا رفتن نرخ سرعت انتقال اطلاعات در شبکه است. چون در توپولوژی فوق ترافیک داده‌ها در یک جهت است، می‌توان از فیبر نوری به منظور محیط انتقال استفاده کرد. در صورت تمایل می‌توان در هر بخش ازشبکه، از یک نوع کابل به عنوان محیط انتقال استفاده کرد. مثلاً در محیط‌های اداری از مدل‌های مسی و در محیط کارخانه از فیبر نوری استفاده کرد.

معایب توپولوژی حلقه:

۱. اشکال در یک گره باعث اشکال در تمام شبکه می‌گردد: در صورت بروز اشکال در یک گره، تمام شبکه با اشکال مواجه خواهد شد. و تا زمانی که گره‌ی معیوب از شبکه خارج نگردد، هیچ گونه ترافیک اطلاعاتی را روی شبکه نمی‌توان داشت.

۲. اشکال زدایی مشکل است: بروز اشکال در یک گره می‌تواند روی تمام گره‌های دیگر تأثیر گذار باشد. به منظور عیب‌یابی می‌بایست چندین گره بررسی شود تا گره مورد نظر پیدا گردد.

۳. تغییر در ساختار شبکه مشکل است: در زمان گسترش و یا اصلاح حوزه‌ی جغرافیایی تحت پوشش شبکه، به دلیل ماهیت حلقوی شبکه مسائلی به وجود خواهد آمد.

٤. توپولوژی بر روی نوع دستیابی تأثیر می‌گذارد: هر گره در شبکه دارای مسئولیت عبوردادن داده‌ای است که از گره‌ی مجاور دریافت داشته است. قبل از اینکه یک گره بتواند داده‌ی خود را ارسال کند، می‌بایست به این اطمینان برسد که محیط انتقال برای استفاده قابل دستیابی است.

۳. ۱. ۱. تقسیم‌بندی بر اساس حوزه‌ی جغرافیایی تحت پوشش

شبکه‌های کامپیوتری با توجه به حوزه‌ی جغرافیایی تحت پوشش به سه گروه تقسیم می‌گردند:

۱. شبکه‌های محلی (کوچک) LAN

۲. شبکه‌های متوسط MAN

۳. شبکه‌های گسترده WAN

شبکه‌های محلی: حوزه‌ی جغرافیایی که توسط این نوع از شبکه‌ها پوشش داده می‌شود، یک محیط کوچک نظیر یک ساختمان اداری است. این نوع از شبکه‌ها دارای ویژگی‌های زیر می‌باشند:

۱. توانایی ارسال اطلاعات با سرعت بالا

۲. محدودیت فاصله

۳. قابلیت استفاده از محیط مخابراتی ارزان نظیر خطوط تلفن به منظور ارسال اطلاعات

۴. نرخ پایین خطا در ارسال اطلاعات با توجه به محدود بودن فاصله

شبکه‌های متوسط: حوزه جغرافیایی که توسط این نوع شبکه‌ها پوشش داده می‌شود، در حد و اندازه یک شهر و یا شهرستان است. ویژگی‌های این نوع از شبکه‌ها شامل:

۱. پیچیدگی بیشتر نسبت به شبکه‌های محلی

۲. قابلیت ارسال تصاویر و صدا

۳. قابلیت ایجاد ارتباط بین چندین شبکه

شبکه‌های گسترده: حوزه‌ی جغرافیایی که توسط این نوع شبکه‌ها پوشش داده می‌شود، در حد و اندازه‌ی کشور و قاره است. ویژگی این نوع شبکه‌ها عبارت است از است:

۱. قابلیت ارسال اطلاعات بین کشورها و قاره ها

۲. قابلیت ایجاد ارتباط بین شبکه‌های محلی
۳. سرعت پایین ارسال اطلاعات نسبت به شبکه‌های محلی
۴. نرخ خطای بالا با توجه به گستردگی محدوده تحت پوشش

انواع شبکه‌های بی سیم از نظر ابعاد و گستردگی:

WLAN[1]: امکان دستیابی کاربران ساکن در یک منطقه‌ی محدود نظیر محوطه یک دانشگاه و یا کتابخانه را به شبکه و یا اینترنت، فراهم می‌نماید.

WPAN[2]: امکان ارتباط بین دستگاه‌های شخصی در یک ناحیه‌ی محدود فراهم می‌شود. در این نوع شبکه‌ها از دو تکنولوژی Bluetooth و Infra Red استفاده می‌شود.

WMAN[3]: در این شبکه ها، امکان ارتباط بین چندین شبکه‌ی موجود در یک شهر بزرگ، فراهم خواهد شد که اغلب به عنوان شبکه‌های پشتیبان شبکه‌ی کابلی استفاده می‌شود.

WWAN[4]: در این شبکه‌ها، ارتباط بین شهرها و یا حتی کشورها از طریق سیستم‌های ماهواره‌ای متفاوت فراهم می‌شود.

۲. ۱. آشنایی با لایه‌های شبکه

۱. ۲. ۱. مدل هفت لایه‌ای (OSI[5]):

این مدل در سال ۱۹۸۴ استفاده شد. در ارسال، با این مدل عملیات از لایه هفت تا یک انجام می‌شود ودر گیرنده، این مراحل از لایه یک تا هفت انجام می‌گیرد.

---

[1] Wireless Local Area Networks
[2] Wireless Personal Area Networks
[3] Wireless Metropolitan Area Networks
[4] Wireless Wide Area Networks
[5] open system inter connection

۱. لایه‌ی هفت لایه‌ی کاربردی(Application):

این لایه با سیستم عامل و یا برنامه‌های کاربردی درارتباط است.

۲. لایه‌ی شش لایه‌ی ارائه (Presentation):

در این لایه تبدیل اطلاعات از قبیل:

۱-فشرده‌سازی ۲-رمز نگاری برای اطلاعات محرمانه ۳-رمزگشایی ۴-تبدیل کدها به یکدیگر که دو ماشین از استانداردهای مختلف استفاده می‌کنند.

این تبدیل اطلاعات به گونه‌ای صورت می‌گیرد که توسط سایر لایه‌ها قابل استفاده باشد.

۳. لایه‌ی پنج لایه‌ی جلسه (session):

این لایه مسئول ایجاد پشتیبانی وارتباطات مربوطه با دستگاه‌های دریافت کننده‌ی اطلاعات است.

۴. لایه‌ی چهار لایه‌ی انتقال (Transport):

یک سرویس انتقال اطلاعات بسیار مطمئن است. این لایه قبل از ارسال بسته ها، نرم‌افزار آن اقدام به ارسال یک بسته‌ی ویژه می‌نماید تا مطمئن شود ماشین گیرنده، آمادگی دریافت اطلاعات را دارد. اطلاعات به صورت بسته‌هایی شماره‌گذاری شده اند تا اطلاعات کم و یا دو بار دریافت نشوند.

واحد اطلاعات، سگمنت می‌باشد. در این لایه پیام‌های بزرگ به بسته‌های کوچکتر تقسیم می‌شوند.

وظایف این لایه ولایه‌های ۵ و ۶ و ۷ با استفاده از نرم‌افزار، پیاده‌سازی می‌شوند و فقط بر روی ماشین‌های نهایی (کاربران) وجود دارند. مراکز سوییچ به وظایف این لایه احتیاجی ندارند.

۵. لایه‌ی سه لایه‌ی شبکه (Network):

در این لایه، روش ارسال داده‌ها برای دستگاه گیرنده تعیین خواهد شد. آدرس‌دهی در این لایه انجام می‌شود. همچنین؛ در این لایه اطلاعات به صورت بسته‌هایی سازمان‌دهی و برای انتقال مطمئن، تحویل لایه دوم می‌شوند. با توجه به این که ممکن است بین دو

ماشین مسیرهای زیادی وجود داشته باشد این لایه وظیفه دارد اطلاعات را در مسیری هدایت کند که ترافیک اطلاعاتی به وجود نیاید.

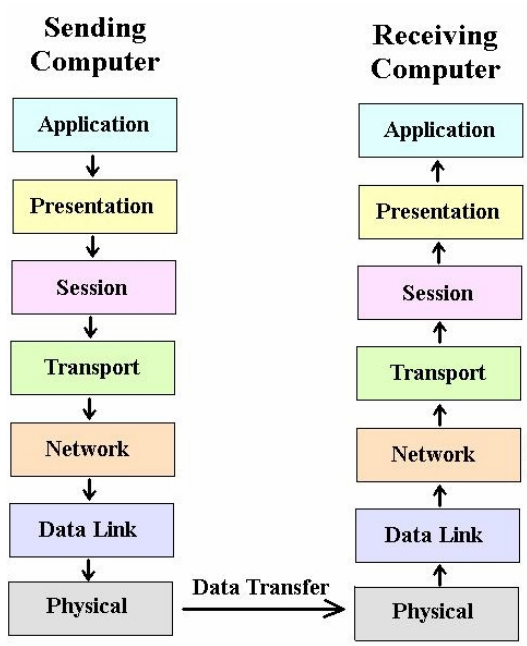
۶. لایه‌ی دو لایه‌ی اتصال اطلاعات (Data link):

در این لایه پروتکل‌های فیزیکی به داده اضافه خواهند شد. همچنین اگر اطلاعات صحیح نرسیده یا ناقص رسیده مجدداً پیام ارسال می‌شود که این خطایابی از طریق اضافه‌کردن بیت‌های کنترل خطا انجام می‌شود.

یکی دیگر از وظایف این لایه، وصول اطلاعات یا عدم وصول اطلاعات را به فرستنده اعلام می‌کند.

۷. لایه‌ی یک لایه‌ی فیزیکی (Physical):

این لایه در ارتباط مستقیم با سخت‌افزار بوده و خصایص فیزیکی شبکه نظیر: اتصالات-ولتاژ-زمان و ... را مشخص می‌کند. انتقال سیگنال از طریق این لایه انجام می‌گیرد.



شکل۷. ۱ لایه‌های شبکه. مدل هفت لایه ای

۲. ۲. ۱. مدل چهار لایه‌ای TCP/IP[1]

۱. لایه‌ی واسط شبکه (Network Access Layer):

این لایه ارتباط لازم با شبکه‌ی فیزیکی را فراهم می‌کند، داده‌ها را برای ارسال، حالت‌دهی می‌کند و داده‌ها را برای ارسال روی شبکه که سخت‌افزار هدف در آن قرار دارد، آدرس‌دهی می‌کند. این لایه همچنین کنترل خطا وجریان داده‌ها و جهت رسیدن اطلاعات در شبکه‌ی فیزیکی را هم تأمین می‌کند.

۲. لایه‌ی اینترنت یا لایه‌ی شبکه(Internet layer):

این لایه آدرس‌دهی منطقی و مستقل از سخت‌افزار را ممکن می‌سازد. بنابر این می‌توان داده‌ها را از بین زیر شبکه‌های کاملاً متنوع و ناسازگار عبور دهد. برای کاهش ترافیک و ایجاد امکان ارسال داده‌ها بین زیر شبکه‌ها مسیریابی انجام می‌دهد. این لایه‌ی ارتباط بین آدرس‌های فیزیکی (که در لایه‌ی واسط شبکه‌ی لایه‌ی قبل به کار می‌روند) و آدرس‌های منطقی برقرار می‌کند. به طور کلی می‌توان گفت این لایه، بسته‌های اطلاعاتی را روی شبکه هدایت می‌کند.

۳. لایه‌ی انتقال(Transport Layer):

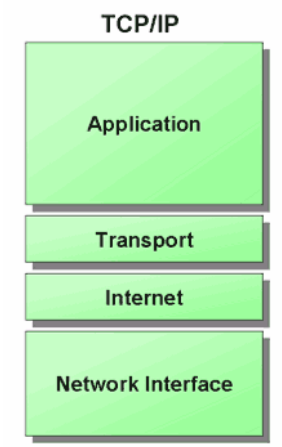
این لایه سرویس‌های کنترل جریان داده ها، خطاها و پاسخ‌دهی به دریافت داده‌ها را برای شبکه ارائه می‌کند و به عنوان واسطی با نرم‌افزارهای کاربردی، کاربرد شبکه را برای آنها تسهیل می‌کند.

۴. لایه‌ی کاربر(Application Layer):

این لایه ابزارهایی برای رفع اشکالات شبکه، انتقال فایل، کنترل از راه دور و کاربردهای اینترنتی ارائه می‌دهد که ما با این لایه در اینترنت سر و کار داریم و پروتکل‌های شبکه‌های نسل بعد مثل SIP,H.323 روی این لایه پیاده‌سازی می‌شوند.

---

[1] Transport Control Protocol/Internet Protocol



شکل۸. ۱ لایه‌های شبکه. مدل چهار لایه ای

۳. ۱. کابل‌های شبکه

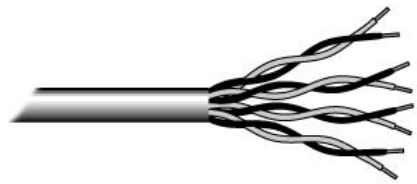
در شبکه‌های محلی، از کابل به عنوان محیط انتقال و به منظور ارسال اطلاعات استفاده می‌شود. ازچندین نوع کابل در شبکه‌های محلی استفاده می‌شود. در برخی موارد ممکن است در یک شبکه صرفاً از یک نوع کابل استفاده و یا با توجه به شرایط موجود از چندین نوع کابل استفاده شود. نوع کابل انتخاب شده برای یک شبکه به عوامل متفاوتی نظیر: توپولوژی شبکه، پروتکل و اندازه‌ی شبکه بستگی خواهد داشت. آگاهی از خصایص و ویژگی‌های متفاوت هر یک از کابل‌ها و تأثیر هر یک از آنها بر سایر ویژگی‌های شبکه، به منظور طراحی و پیاده‌سازی یک شبکه‌ی موفق بسیار لازم است.

۱. ۳. ۱. کابل دو رشته‌ای بدون محافظ UTP[1]

متداول‌ترین نوع کابلی که در انتقال اطلاعات استفاده می‌شود، کابل‌های به هم تابیده می‌باشند. این نوع کابل‌ها دارای دو رشته سیم به هم پیچیده بوده که هر دو نسبت به زمین، دارای یک امپدانس یکسان می‌باشند. بدین ترتیب امکان تأثیرپذیری این نوع کابل‌ها از کابل‌های مجاور و یا سایر منابع خارجی کاهش خواهد یافت. کابل‌های

[1] Unshielded Twist pairs

به هم تابیده دارای دو مدل متفاوت: (Shielded) روکش دار و (Unshielded) بدون روکش می‌باشند. کابل UTP نسبت به کابل STP به مراتب متداول تر بوده و در اکثر شبکه‌های محلی استفاده می‌گردد. کیفیت کابل‌های UTP متغیر بوده و از کابل‌های معمولی استفاده شده برای تلفن تا کابل‌های با سرعت بالا را شامل می‌گردد. کابل دارای چهار زوج سیم بوده و درون یک روکش قرار می‌گیرند. هر زوج با تعداد مشخصی پیچ تابانده شده (در واحد اینچ) تا تأثیرپذیری آن از سایر زوج‌ها و یاسایر دستگاه‌های الکتریکی کاهش یابد.



شکل۹. ۱

کابل‌های UTP دارای استانداردهای متعددی بوده که در گروه‌های (Categories) متفاوت زیر تقسیم شده‌اند:

جدول ۱.۱

Type	کاربرد
Cat 1	فقط صوت (کابل‌های تلفن)
Cat 2	داده با سرعت ۴ مگابیت در ثانیه
Cat 3	داده با سرعت ۱۰ مگابیت در ثانیه
Cat 4	داده با سرعت ۲۰ مگابیت در ثانیه
Cat 5	داده با سرعت ۱۰۰ مگابیت در ثانیه
Cat 6	داده با سرعت ۱۰۰۰ مگابیت در ثانیه
Cat 7	داده با سرعت ۱۰۰۰۰ مگابیت در ثانیه

مزایای کابل‌های به هم تابیده:

۱. سادگی و نصب آسان

۲. انعطاف‌پذیری مناسب

۳. دارای وزن کم بوده و به راحتی به هم تابیده می‌شوند.

معایب کابل‌های به هم تابیده:

۱. تضعیف فرکانس

۲. بدون استفاده از تکرارکننده‌ها، قادر به حمل سیگنال در مسافت‌های طولانی نمی‌باشند.

۳. پایین بودن پهنای باند

۴. به دلیل پذیرش پارازیت در محیط‌های الکتریکی سنگین، به خدمت گرفته نمی‌شوند.

کانکتور استاندارد برای کابل‌های UTP، از نوع RJ-45 می‌باشد. کانکتور فوق شباهت زیادی به کانکتورهای تلفن (RJ-11) دارد. هر یک از پین‌های کانکتور فوق می‌بایست به درستی پیکربندی شوند. (Jack Registered:RJ)

شکل ۱.۱۰

۲. ۳. ۱. کابل کواکسیال

یکی از مهمترین محیط‌های انتقال در مخابرات، کابل «کواکسیال» و یا «هم‌محور» می‌باشد. این نوع کابل‌ها از سال ۱۹۳۶ برای انتقال اخبار و اطلاعات در دنیا به کار گرفته شده اند. در این نوع کابل ها، دو سیم تشکیل دهنده‌ی یک زوج، از حالت متقارن خارج شده و هر زوج از یک سیم در مغز و یک لایه مسی بافته شده در اطراف آن تشکیل می‌گردد. در نوع دیگر کابل‌های کواکسیال، به جای لایه مسی بافته شده، از

تیوپ مسی استوانه‌ای استفاده می‌شود. ماده‌ای پلاستیکی این دو هادی را از یکدیگر جدا می‌کند. ماده‌ی پلاستیکی ممکن است به صورت دیسکهای پلاستیکی یا شیشه ای، در فواصل مختلف استفاده، و مانع از تماس دو هادی با یکدیگر شود و یا ممکن است دو هادی در تمام طول کابل به وسیله مواد پلاستیکی از یکدیگر جدا گردند.

شکل ۱.۱۱

مزایای کابل‌های کواکسیال:

۱. قابلیت اعتماد بالا
۲. ظرفیت بالای انتقال، حداکثر پهنای باند ۳۰۰ مگاهرتز
۳. دوام و پایداری خوب
۴. پایین بودن مخارج نگهداری
۵. قابل استفاده در سیستم‌های آنالوگ و دیجیتال
۶. هزینه پایین در زمان توسعه
۷. پهنای باند نسبتاً وسیع که مورد استفاده‌ی اکثر سرویس‌های مخابراتی از جمله تله کنفرانس صوتی و تصویری است.

معایب کابل‌های کواکسیال:

۱. مخارج بالای نصب
۲. نصب مشکل تر نسبت به کابل‌های به هم تابیده
۳. محدودیت فاصله
۴. نیاز به استفاده از عناصر خاص برای انشعابات

از کانکتورهای(Bayone –Neill -Concelman) **BNC** به همراه کابل‌های کواکسیال استفاده می‌گردد. اغلب کارت‌های شبکه دارای کانکتورهای لازم در این خصوص می‌باشند.

شکل ۱.۱۲

۱.۳.۳. فیبر نوری

یکی از جدیدترین محیط‌های انتقال در شبکه‌های کامپیوتری، فیبر نوری است. فیبر نوری از یک میله استوانه‌ای که هسته نامیده می‌شود و جنس آن از سیلیکات است تشکیل می‌گردد. شعاع استوانه بین دو تا سه میکرون است. روی هسته، استوانه‌ی دیگری (از همان جنس هسته) که غلاف نامیده می‌شود، استقرار می‌یابد. ضریب شکست هسته را با M1، و ضریب شکست غلاف را با M2، نشان داده و همواره M2<M1 است. در این نوع فیبرها، نور در اثر انعکاسات کلی در فصل مشترک هسته و غلاف، انتشار پیدا خواهد کرد. منابع نوری در این نوع کابل ها، دیود لیزری و یا دیودهای ساطع کننده نور می‌باشند. منابع فوق، سیگنال‌های الکتریکی را به نور تبدیل می‌نمایند.

شکل ۱.۱۳

مزایای فیبر نوری:

۱. حجم و وزن کم
۲. پهنای باند بالا
۳. تلفات سیگنال کم و در نتیجه فاصله‌ی تقویت کننده‌ها زیاد می‌گردد.
۴. فراوانی مواد تشکیل دهنده‌ی آنها
۵. مصون بودن از اثرات القاهای الکترو مغناطیسی مدارات دیگر
۶. آتش زا نبودن آنها به دلیل عدم وجود پالس الکتریکی در آنها
۷. مصون بودن در مقابل عوامل جوی و رطوبت
۸. سهولت در امر کابل کشی و نصب
۹. استفاده در شبکه‌های مخابراتی آنالوگ و دیجیتال
۱۰. مصونیت در مقابل پارازیت

معایب فیبر نوری:

۱. به راحتی شکسته شده و می‌بایست دارای یک پوشش مناسب باشند. این مسئله با ظهور فیبرهای تمام پلاستیکی و پلاستیکی- شیشه‌ای کاهش پیدا کرده است.

۲. اتصال دو بخش از فیبر یا اتصال یک منبع نور به فیبر، فرآیند دشواری است. در چنین حالتی می‌توان از فیبرهای ضخیم تر استفاده کرد اما این مسئله باعث تلفات زیاد و کم شدن پهنای باند می‌گردد.

۳. از اتصالات T شکل در فیبر نوری نمی‌توان جهت گرفتن انشعاب استفاده نمود. در چنین حالتی فیبر می‌بایست بریده شده و یک آشکار کننده اضافه گردد. این دستگاه می‌بایست توانایی دریافت و تکرار سیگنال را داشته باشد.

۴. تقویت سیگنال نوری یکی از مشکلات اساسی در زمینه‌ی فیبر نوری است. برای تقویت سیگنال می‌بایست سیگنال‌های نوری به سیگنال‌های الکتریکی تبدیل، تقویت و مجدداً به علائم نوری تبدیل شوند.

جدول ۲. ۱ کابل‌های استفاده شده در شبکه‌های اترنت

Maximum length	Cable Type	Specification
100 meters	Unshielded Twisted Pair	10BaseT
185 meters	Thin Coaxial	10Base2
500 meters	Thick Coaxial	10Base5
2000 meters	Fiber Optic	10BaseF
100 meters	Unshielded Twisted Pair	100BaseT
220 meters	Unshielded Twisted Pair	100BaseTX

۴. ۱. روتر[1]

روتر سخت‌افزار یا نرم‌افزاری است که به منظور مدیریت بسته‌های اطلاعاتی[2] و هدایت آنها پیش طراحی و ساخته شده است. روترها با استفاده از جدول مسیریابی در برقراری ارتباط بین کامپیوترها، چه در شبکه‌های شخصی در منازل و چه در شبکه‌های بزرگ و پیچیده، نقش حیاتی ایفا می‌کنند.

بخشی از تاخیر در اینترنت، در اثر وجود روتر در اینترنت می‌باشد که البته این تاخیر چندان زیاد نیست وقابل چشم پوشی می‌باشد.

شکل ۱۴. ۱ نمادهایی که تحت شبکه اینترنت با یکدیگر در ارتباط اند

[1] Router
[2] Data Packet

فصل دوّم
استانداردهای شبکه‌های نسل آینده (NGN)

۱. ۲. شبکه NGN

در این بخش، به بررسی تاریخچه، تعریف، ملزومات و آینده‌ی استانداردهای NGN می‌پردازیم. در این مسیر، جهت و حرکت استراتژیک استانداردها را به سمت یک شبکه‌ی NGN فراگیر با قابلیت همگرایی شبکه‌های موبایل و ثابت و تمامی وجوه مخابرات قرن بیست و یکم را مورد بررسی قرار می‌دهیم.

در طول ۱۰ سال اخیر، به طور فزاینده‌ای شاهد اجتماع و همگرایی شبکه‌های کامپیوتری و تلفنی بوده‌ایم. اپراتورهای عمومی شبکه (PNOها) شاهد کاهش در ترافیک تلفنی، شبکه‌های PSTN، خود در اثر محبوبیت در حال افزایش تلفن‌های موبایل و همچنین حرکت و انتقال سرویس‌ها از شبکه‌های تلفن به اینترنت بوده‌اند.

تقاضای مشتریان شبکه‌های تلفنی به تدریج از سرویس‌های مخابراتی محدود ارائه شده توسط فراهم کنندگان شبکه، (network providerها) به سمت سرویس‌های وسیع و متنوع اینترنت گرایش پیدا کرده‌است. پاسخ اپراتورهای شبکه‌های «ثابت» به این تقاضا، بهره برداری از تکنولوژی باند وسیع برای برآورده‌سازی نیاز مشتریان بوده است. این راه حل هر چند تقاضا و نیاز مشتریان را برآورده ساخته، اما در درون خود نوعی استقلال از سرویس و کاربرد را فراهم کرده است.

به عبارت دیگر؛ اپراتور شبکه، فقط وظیفه‌ی فراهم آوردن دسترسی به اینترنت (و یا حتی در حالت بدتر، دسترسی به ISPها) را بر عهده داشته است، در حالی که محتوای ارتباطی و سرویس‌های ارائه شده در اینترنت، مستقل از هزینه‌های ساخت و برقراری شبکه به مشتریان ارائه می‌گردد.

مشتریان در قبال سرویس که دریافت می‌کنند نه در قبال تکنولوژی مورد استفاده، پول پرداخت می‌کنند. لذا اگر سرویس‌هایی ارائه شوند که از تکنولوژی باند وسیع، بهره‌ی کافی را می‌برند به خاطر صرفه اقتصادی و سودآوری برای اپراتورهای شبکه، بسیار با اهمیت می‌باشند. بدین ترتیب، مفهوم یک شبکه‌ی باند وسیع مجتمع با عنوان شبکه نسل آینده (NGN) در طول سالهای اخیر توسعه پیدا کرده‌است.

مشخصات اصلی یک شبکه NGN در واقع از مسائل مواجه شده توسط اپراتورهای شبکه ناشی می‌شوند: نیاز به فراهم آوردن سرویس‌هایی بر روی نقاط دسترسی باند وسیع (به منظور افزایش سود اقتصادی)؛ نیاز به تلفیق سرویس‌های متنوع و پراکنده‌ی شبکه مانند: دیتا (جستجوی وب)، voice، ارتباطات تلفنی، چندرسانه‌ای و همچنین تلفیق سرویس‌های اینترنتی محبوبیت یافته مانند: ارسال پیام‌های لحظه‌ای[1] و سرویس‌های ارسالی همگانی[2]، تقاضای مشتریان برای دسترسی به سرویس‌ها در هر مکان دلخواه (ماهیت mobility). در این مسیر، به جای یک شبکه‌ای که یک راه حل خاص را فراهم می‌نماید (مانند PSTN)، مجموعه‌ای از شبکه‌ها با قابلیت پشتیبانی یک بستر انعطاف‌پذیر برای ارائه سرویس، مورد نیاز است.

یکی از مهمترین ویژگی‌های IP، استقلال لایه‌های پروتکل می‌باشد. این ویژگی مبنای اصلی شبکه‌های ارتباطی جهانی بوده است که در آن، ارتباط بین نقاط مختلف مستقل از نوع شبکه‌های زیرلایه، مانند: PSTN، ATM و یا Frame Relay برقرار می‌گردد. همچنین دسترسی باند وسیع مانند خطوط ADSL، قابلیت ارائه و استفاده از کاربردهای آنلاین را برای شبکه‌های جهانی فراهم کرده است.

---

[1] instant messaging
[2] broadcast

۲. ۲. ملزومات یک شبکه NGN

NGN از سال ۲۰۰۳ در استانداردها مورد بحث قرار گرفته است و مهمترین سؤال پرسیده شده در این زمینه این بوده است: «NGN چیست؟». همان طور که گفته شد، نیازهای تجاری و اقتصادی، نقطه‌ی شروع را در پاسخ به این سؤال مشخص نمودند.
گروه مطالعاتی ۱۳ ITU-T، تعریف NGN را در Recommendation Y. 2001 به این ترتیب مطرح نمود: «NGN یک شبکه‌ی مبتنی بر Packet می‌باشد که دارای قابلیت ارائه‌ی سرویس‌های مخابراتی و همچنین استفاده از تکنولوژی‌های انتقال باند وسیع با قابلیت QOS است و در آن، عملیات و فانکشن‌های مرتبط با سرویس، مستقل از تکنولوژی‌های مربوط به انتقال می‌باشند. در این شبکه، امکان دسترسی کاربران به شبکه‌ها و فراهم کنندگان سرویس و سرویس‌های مختلف وجود دارد.
این شبکه همچنین mobility تعمیم یافته را پشتیبانی می‌نماید که اجازه دسترسی به سرویس‌های مداوم (بدون وقفه) و موجود در هر مکان را به کاربران می‌دهد.
به علاوه Recommendation Y. 2001 شبکه NGN را با مشخصات اساسی زیر تعریف می‌کند:

۱. انتقال مبتنی بر Packet
۲. جداسازی فانکشن‌های کنترلی
۳. جداسازی سرویس از انتقال و فراهم‌سازی اینترفیس‌های باز
۴. پشتیبانی دامنه وسیعی از سرویس‌ها، کاربردها و مکانیزم‌های مبتنی بر سرویس‌ها (شامل سرویس‌های real-time، غیر real-time، streaming و چندرسانه‌ای)
۵. قابلیت‌های باند وسیع با end-to-end QOS
۶. Interworking با شبکه‌های متداول از طریق اینترفیس‌های باز
۷. Mobility تعمیم یافته
۸. دسترسی نامحدود توسط کاربران به فراهم کنندگان شبکه مختلف
۹. تنوع کافی در ساختارها و روش‌های شناسایی کاربر
۱۰. مشخصات واحد و یکسان برای یک سرویس خاص(از دید کاربر)
۱۱. سرویس‌های همگرا بین شبکه‌های موبایل و ثابت

۱۲. استقلال فانکشن‌های مرتبط با سرویس از تکنولوژی‌های انتقال مورد استفاده
۱۳. پشتیبانی تکنولوژی‌های مختلف last-mile
۱۴. تبعیت از تمامی ملزومات قانونی مانند: در نظر گرفتن مخابرات اضطراری، امنیت ارتباطات، Privacy و همچنین شنودها و تداخل‌های قانونی
۱۵. همچنین Recommendation Y. 2001، شبکه‌ی NGN را به تعدادی زمینه‌ی مطالعاتی تفکیک کرده است که هر یک نیاز به مطالعه به منظور بررسی ملزومات و ارائه راه حل می‌باشند.
این زمینه‌ها هم اکنون اساس و هسته‌ی اصلی فعالیت‌های مربوط به استانداردسازی در ITU-T و سایر مؤسسات توسعه استاندارد (SDO) را تشکیل می‌دهند:

چارچوب کلی و اصول ساختاری:

۱. قابلیت‌های سرویس‌دهی و معماری و ساختار سرویس‌ها
۲. قابلیت فعالیت و ارتباط بین سرویس‌ها و شبکه در NGN
۳. قابلیت‌های مخابراتی در مواقع بلایا و فجایع
۴. مدل‌های ساختاری و معماری برای NGN
۵. End-to-end QOS
۶. بسترهای سرویس‌دهی
۷. مدیریت شبکه
۸. امنیت شبکه
۹. قابلیت سیار بودن
۱۰. پروتکل‌ها و ساختارهای کنترل شبکه
۱۱. شماره‌گذاری، نام‌گذاری و آدرس‌دهی

ملزومات NGN هنوز در حال گسترش می‌باشند زیرا؛ NGN دارای ابعاد وسیع و گسترده‌ای است. ارائه‌ی سرویس‌های voice در بردارنده‌ی پیچیدگی‌های کنترل و مدیریت PSTN می‌باشد. mobility مستلزم همگرایی موبایل- ثابت (FMC) و جداسازی سرویس‌دهی از انتقال خواهد بود. در حالی که فراهم‌سازی اینترفیس‌های باز،

چالش‌هایی را نظیر وفق دادن ساختارهای مبتنی بر اینترنت با شبکه‌های امن و مطمئن مانند شبکه‌های تلفن معمولی، در پیش رو قرار می‌دهد.
نیاز دیگری که از سوی برخی از PNOها مطرح شد، استفاده از NGN برای جایگزینی با شبکه‌های تلفن معمولی (به طور کلی یا جزئی) بود. این جایگزینی مستلزم فراهم آوردن تمامی سرویس‌های شبکه‌های تلفن معمولی توسط NGN جایگزین شده می‌باشد. به عبارت دیگر؛ این جایگزینی باید کاملاً از دید مشتری تلفن معمولی قبلی نامحسوس باشد.

۳. ۲. استانداردهای NGN

موضوع شبکه‌های نسل بعد یا NGN در اواخر سال ۲۰۰۳ در استانداردهای جهانی مطرح شد و در نهایت گروه مطالعاتی شماره سیزده دفتر استانداردسازی مخابرات اتحادیه‌ی جهانی مخابرات یا همان ITU- TSG13 شبکه‌های نسل بعد را در توصیه نامه سری Y. 2001 (که هدف اصلی آن ارائه‌ی یک تعریف عمومی برای NGN بود) این گونه تعریف کرد: «یک شبکه‌ی مبتنی بر بسته‌های اطلاعاتی که قادر است سرویس‌های مخابراتی، امکان استفاده از باند پهن و فناوری‌های انتقال با قابلیت ارائه‌ی کیفیت سرویس را فراهم کند. هم چنین شبکه‌ای که در آن کارکردهای وابسته به سرویس، مستقل از فناوری‌های وابسته به انتقال است». این شبکه به کاربران اجازه می‌دهد که به شبکه ها، تامین کنندگان سرویس و یا سرویس‌های مختلف به صورت آزاد دسترسی داشته باشند و در کنار همه‌ی این موارد از تحرک فراگیر و عمومی نیز پشتیبانی می‌کند تا امکان استفاده از سرویس‌های یکپارچه را در هر مکان و هر زمانی برای کاربران فراهم کند. تحرک فراگیر نیز در توصیه نامه سری Y. 2001 اتحادیه جهانی مخابرات بدین صورت تعریف شده است: قابلیتی برای کاربر یا هر وسیله متحرک دیگر که برقراری ارتباط و استفاده از سرویس‌های دسترسی بدون در نظر گرفتن تغییر موقعیت مکانی و یا محیط فنی، برای آن فراهم شود. البته درجه‌ی در دسترس بودن سرویس ممکن است به عوامل زیادی از جمله توانایی‌های شبکه‌ی دسترسی، توافق نامه‌های سطح سرویس بین شبکه‌های خانگی کاربران و سایر شبکه‌ها و ... بستگی

داشته باشد. تحرک، در برگیرنده‌ی قابلیت برقراری ارتباط با و یا بدون پیوستگی سرویس نیز است.

در این بخش؛ به بررسی استانداردهای تهیه شده توسط ITU-T و موسسه استانداردهای مخابراتی اروپا (ETSI) در مورد شبکه‌های نسل بعد می‌پردازیم.

۲. ۴. فعالیت‌های استانداردسازی

در سال ۲۰۰۳، ITU-T SG13 گروهی را با نام NGN- JRG تشکیل داد که وظیفه‌ی آن شناسایی مباحث کلیدی و توسعه استانداردهایی مبنایی برای ساختن چارچوب‌های یک NGN، شامل ارائه یک تعریف در قالب ITU-T بود. فعالیت این گروه تا ماه ژوئن ۲۰۰۴ ادامه یافت و Y. 2001 و Y. 2011 حاصل کار گروه مذکور بوده و هم اکنون اساس مطالعات NGN در ITU-T می‌باشند.

۲. ۵. ETSI TISPAN

همزمان با ITU-T و به طور موازی با آن، ETSI نیز شروع به فعالیت‌های استانداردسازی منطقه‌ای نمود. دو کمیته موجود در ETSI در تابستان ۲۰۰۳ با یکدیگر ترکیب شدند. کمیته ETSI TIPHON در حال پژوهش بر روی ملزومات ارتباط شبکه‌های VOIP و PSTN بود و به موفقیت‌هایی نیز دست پیدا کرده بود. همچنین کمیته ETSI SPAN نیز مدتهای مدیدی بر روی استانداردهای مخابراتی اروپایی فعالیت می‌کرد. کمیته‌ی حاصله با نام TISPAN به یک طرح ساده برای برآورده ساختن نیاز فوری بازار دست یافت:

۱. ارائه‌ی تمامی سرویس‌های موجود در 3GPP IMS به مشتریان باند وسیع و تعدادی از سرویس‌های IMS به مشتریان PSTN/ISDN متصل به NGN.

۲. فراهم کردن اکثر سرویس‌های یک PSTN/ISDN موجود و همچنین اینترفیس‌هایی برای پشتیبانی جایگزینی PSTN/ISDN با NGN.

۳. بسط و گسترش 3GPP IMS برای پوشش زمینه‌هایی که 3GPP آنها را پوشش نداده است: به طور مشخص، تماسهای اضطراری و تداخل و شنود قانونی. همچنین،

TISPAN موظف بود که نشان دهد که ملاحظات و ملزومات مقرراتی برای خصوصی بودن قابل برآورده‌سازی است. (سرویس‌های مشابه 3GPP IMS(CLIP/CLIR بر اساس انتقال بسته‌ای استوار است؛ جداسازی فانکشن‌های کنترلی را پشتیبانی می‌نماید؛ سرویس‌دهی را از انتقال تفکیک می‌کند؛ اینترفیس‌های باز را فراهم می‌کند؛ و دامنه وسیعی از سرویس ها، کاربردها و مکانیزم‌ها را پشتیبانی می‌کند. همچنین، IMS قابلیت سیار بودن را نیز در خود دارد.

در راستای بحث جایگزینی شبکه‌های تلفن معمولی، دو نوع سرویس تلفن معمولی تعریف شده‌است: emulation و simulation. اولی به مفهوم پشتیبانی تجهیزات و اینترفیس‌های موجود مشتری به طریق کاملاً معادل با تلفن معمولی می‌باشد در حالی که دومی به مفهوم فراهم کردن انواع مشابهی از سرویس‌ها بر روی نقاط دسترسی باند وسیع برای تجهیزات جدید یا بهبود یافته مشتری است.

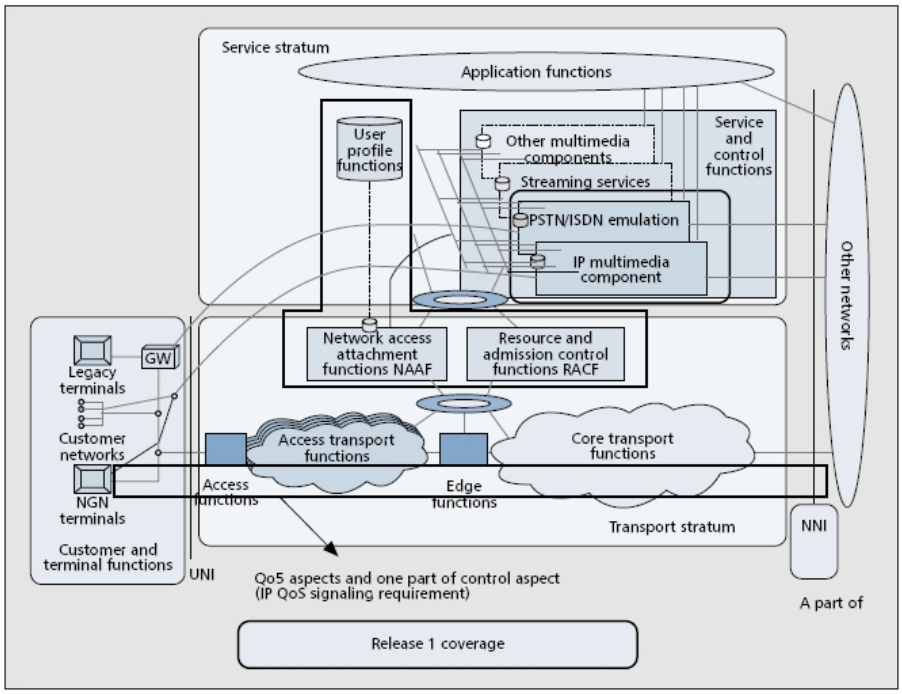
به این دلیل، اجزای TISPAN NGN به ترتیب زیر در نظر گرفته شدند:

۱. یک بستر کنترل سرویس‌دهی با قابلیت پشتیبانی سیستم‌های مختلف سرویس‌دهی
۲. یک بسته مجزا برای کاربردهای مختلف
۳. یک بستر انتقال مرکزی مبتنی بر تکنولوژی IP
۴. تلفیق با شبکه‌های مختلف دسترسی باند وسیع موجود
۵. امنیت شبکه، QOS و مدیریت شبکه

۶. ۲. ITU-T

از آنجایی که چندین مؤسسه استانداردسازی، طرح‌های خود را برای استاندارد NGN در ابتدای سال ۲۰۰۴ ارائه کردند، نگرانی‌هایی در صنعت در ارتباط با هماهنگی و عدم هماهنگی‌های احتمالی بین استانداردهای آینده NGN به وجود آمد. نگرانی‌های مذکور منجر به تشکیل یک گروه متمرکز در ITU-T به منظور فعالیت بر روی استانداردسازی NGN شد که با نام FGNGN شناخته می‌شود. در ادامه و پس از برگزاری جلسات مکرر، تصمیم بر این گرفته شد که ITU-T SG13 به عنوان گروه اصلی فعالیت کننده بر روی NGN در ITU-T فعالیت‌های FGNGN را ادامه دهد.

فعالیت‌های FGNGN تا ارائه Release 1 ادامه می‌یابد. شکل ۱ نمای کلی Release 1 را نشان می‌دهد. همان طور که در شکل ۱ دیده می‌شود، اگر در جهت افقی روی شکل حرکت کنیم، NGN به سه قسمت قابل تقسیم است: تجهیزات مشتری، تجهیزات شبکه و اتصال با شبکه‌های دیگر (شامل NGNهای دیگر).



شکل ۱. ۲ نمای کلی FGNGN Release 1

همچنین؛ در جهت عمودی می‌توان NGN را به دو ناحیه تقسیم نمود: لایه سرویس و لایه انتقال. لایه سرویس نیز به نوبه‌ی خود به فانکشن‌های کنترل و سرویس‌دهی و فانکشن‌های کاربرد[1] قابل تقسیم می‌باشد.

[1] application

۲.۷. ساختار شبکه‌های NGN

قبلاً اشاره کردیم که تفاوت اساسی بین NGN و سرویس‌های سنتی و مرسوم مخابراتی گذر از شبکه‌های جداگانه و مبتنی بر کاربرد خاص به یک شبکه واحد با قابلیت حمل و نقل تمامی سرویس‌ها می‌باشد. همچنین قبلاً به Recommendation Y. 2001 [1] اشاره کردیم که در آن، تعدادی از ویژگی‌ها و مشخصه‌های ضروری در یک NGN ارائه شده‌اند. به علاوه، ITU-T در Recommendation Y. 2011 یک چارچوب کلی را برای ساختار NGN به منظور رسیدن به ویژگی‌های مذکور در Y. 2001 مطرح می‌نماید.

۲.۸. ITU-T Recommendation Y. 2011

هدف اصلی Y. 2011 فراهم نمودن پایه و اساسی برای توسعه‌ی مدل‌های عملیاتی برای سرویس‌های مبتنی بر NGN می‌باشد.

ابتدا، در این Recommendation به تفاوت‌های بین سیستم‌های لایه‌بندی شده NGN و سیستم‌های هفت لایه OSI BRM [1] تعریف شده در ITU-T Recommendation X.200 اشاره می‌شود. به عنوان مثال، در رابطه با تعداد لایه‌ها و همچنین مشخصه‌های خاص هر لایه در OSI BRM با مسایل و مشکلاتی در NGN روبرو هستیم. در ارتباط با سیستم‌های NGN (سیستم‌های غیر OSI) ممکن است با برخی یا همه شرایط زیر روبرو شویم:

۱. تعداد لایه‌ها می‌تواند هفت نباشد.

۲. وظایف لایه‌های مختلف ممکن است با وظایف لایه‌های متناظر در OSI BRM یکسان نباشد.

۳. تعاریف و شرایط معینی که در OSI BRM تجویز می‌شود ممکن است که عملی نباشد.

۴. پروتکل‌های مورد استفاده با پروتکل‌های OSI تفاوت داشته باشد. (مانند IP)

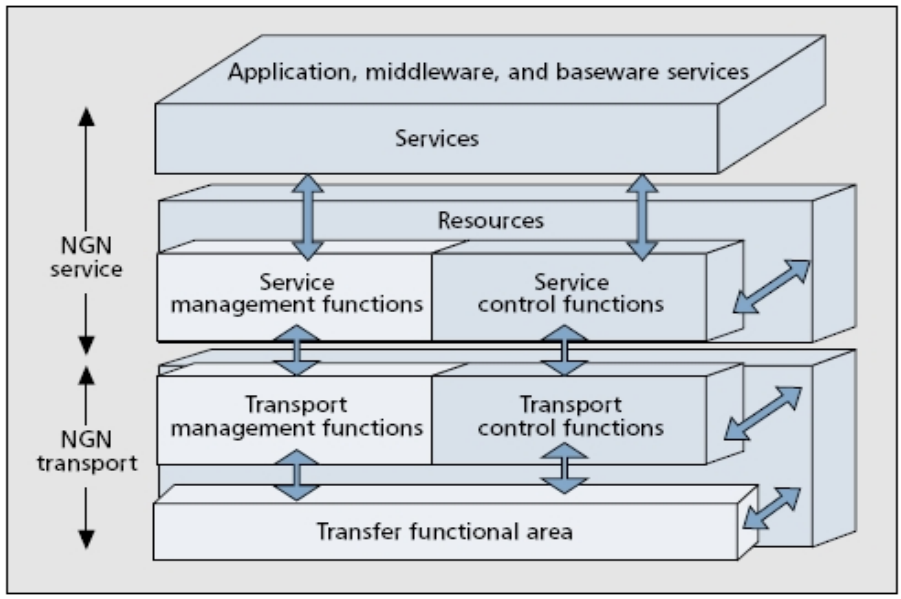
Annexهای Y. 2011 فرازهای مختلف OSI BRM را که به منظور استفاده در

[1] Open Systems Interconnection Basic Reference Model

NGN تغییر و تصحیح شده و همچنین بخش‌هایی را که غیر قابل استفاده در NGN می‌باشند را با جزئیات مشخص می‌نمایند.

سرویس‌ها و فانکشن‌ها با یکدیگر ارتباط دارند زیرا فانکشن‌ها در واقع برای ساختن و ایجاد سرویس‌ها مورد استفاده قرار می‌گیرند. مناسب است که فانکشن‌ها را به دو گروه متمایز، یا به عبارت دیگر به دو لایه تقسیم نماییم: گروه اول شامل تمامی فانکشن‌های کنترلی و دیگری شامل تمامی فانکشن‌های مدیریتی. با این تقسیم‌بندی می‌توان ارتباط و جریان اطلاعات بین فانکشن‌های درون یک گروه را تعریف نمود.

بدین ترتیب، Y. 2011 مدل سطح بالای نشان داده شده در شکل ۲ را توسعه داده است. این شکل نحوه گروه‌بندی فانکشن‌ها را به منظور توسعه سیستم نمایش می‌دهد. بلوک‌های فانکشنال را نیز می‌توان به نوبه خود به زیرگروه‌های نشان داده شده در شکل تقسیم نمود و بدین ترتیب به یک گروه‌بندی مناسب برای پیاده‌سازی و نمایش سیستم دست یافت.

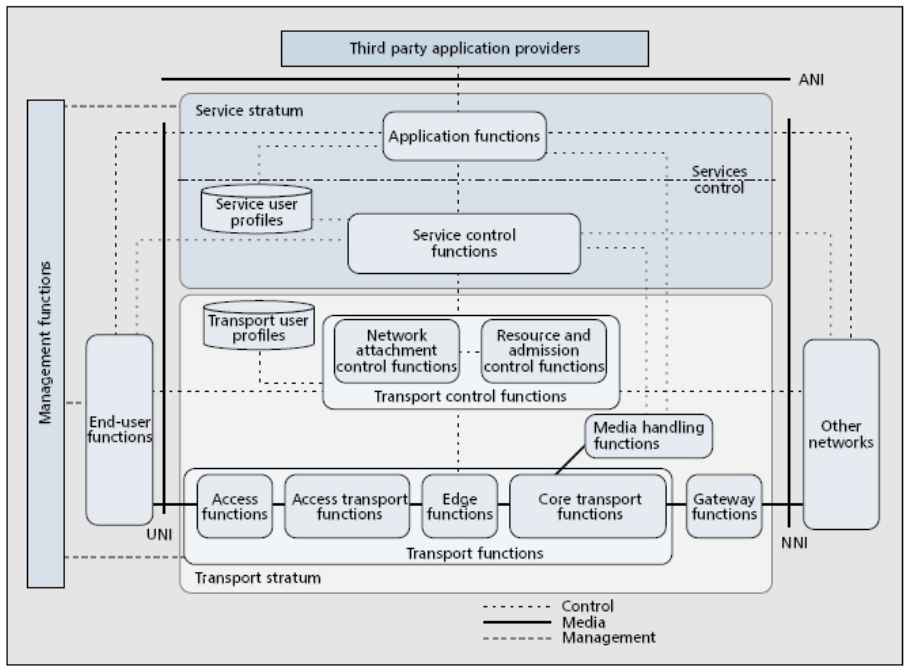


شکل ۲. ۲ مدل کلی فانکشنال برای NGN (مبتنی بر Y. 2001)

۹. ۲. FGNGN

در این بخش به ارائه ساختار NGN بر اساس طرح مطرح شده در FGNGN می‌پردازیم. البته لازم به ذکر است که ساختار نهایی بر اساس نتایج مطالعات بیشتر، قابل تغییر می‌باشد.

سرویس‌های NGN از سرویس‌های Session-based مانند: IP telephony، video conferencing، video chatting و سرویس‌های غیر session-based مانند video streaming و همچنین broadcasting تشکیل می‌شوند. علاوه بر آن، شبکه‌های NGN جایگزینی PSTN/ISDN را نیز پشتیبانی می‌نمایند.



شکل ۳. ۲ ساختار کلی NGN

شکل ۳ نمایی کلی از ساختار NGN را نمایش می‌دهد. فانکشن‌های NGN به دو لایه سرویس و انتقال (طبق Recommendation Y. 2011) تقسیم می‌شوند. در ادامه به توضیح فانکشن‌های NGN خواهیم پرداخت.

فانکشن‌های کاربر نهایی با استفاده از اینترفیس کاربر-شبکه (UNI) بـه NGN متـصل می‌شوند، در حالی که سایر شبکه‌ها از طریق اینترفیس شبکه-شبکه (NNI) به یکـدیگر متصلند.

تمایز قائل شدن بین UNI و NNI به منظور ایجاد قابلیـت اسـتفاده از بخـش وسـیع و متنوعی از تجهیزات مشتری و در عین حـال حفـظ کـردن مرزهـای تجـارت در محـیط NGN، از اهمیت بالایی برخوردار است. اینترفیس کاربرد-شبکه (ANI) تشکیل دهنـده مـرزی در مقابـل فـراهم کننـدگان کـاربرد third-party (third-party application providers) می‌باشد.

۱۰. ۲. فانکشن ها

۱. ۱۰. ۲. فانکشن‌های لایه انتقال

فانکشن‌های لایه‌ی انتقال، اتصال بین مؤلفـه‌هـا و فانکـشن‌هـای مجـزا را در درون NGN فراهم می‌نمایند. IP به عنوان محبوب‌ترین تکنولـوژی انتقـال در NGN در نظـر گرفته می‌شود. لذا، لایه انتقال، اتصال IP را هم برای تجهیزات کاربر نهـایی در خـارج از NGN و هم برای کنترل کننده‌های واقع در درون NGN فراهم خواهد کرد. لایه انتقال مسؤل فراهم کردن end-to-end QOS می‌باشد که همان مشخصه مطلـوب در NGN است. لایه‌ی انتقال به شبکه‌های دسترسی و شبکه‌ی هسته تقسیم می‌گردد کـه توسـط یک فانکشن با هم ارتباط دارند.

۲. ۱۰. ۲. فانکشن‌های دسترسی

فانکشن‌های دسترسی، دسترسی کـاربر نهـایی را بـه شـبکه مـدیریت مـی‌نماینـد. فانکـشن‌هـای دسترسـی بـه تکنولـوژی‌هـای دسترسـی ماننـد W-CDMA و ADSL وابسته‌اند. شبکه‌های دسترسی شامل فانکشن‌های مربوط به دسترسی کابلی، تکنولـوژی ADSL، بی سیم، اینترنت و دسترسی نوری می‌باشد.

۳. ۱۰. ۲. فانکشن‌های انتقال دسترسی

این فانکشن‌ها مسؤل انتقال اطلاعات در سراسر شبکه دسترسی می‌باشـند. وظیفـه

دیگر آنها فراهم نمودن مکانیزم‌های کنترل QOS با کنترل مستقیم ترافیک کاربر، شامل مدیریت بافر، صف و زمان بندی، فیلتر کردن بسته‌ها، طبقه‌بندی ترافیک، علامت‌گذاری، سیاست‌گذاری و شکل‌دهی است.

۴. ۱۰. ۲. فانکشن‌های لبه

فانکشن‌های لبه به منظور پردازش ترافیک در زمان تلفیق ترافیک دسترسی در شبکه‌ی هسته مورد استفاده قرار می‌گیرند.

۵. ۱۰. ۲. فانکشن‌های انتقال هسته

این فانکشن‌ها مسؤلیت اطمینان حاصل کردن از انتقال اطلاعات در سراسر شبکه‌ی هسته را بر عهده دارند. آنها ابزاری را برای تشخیص کیفیت انتقال در شبکه با استفاده از برقراری ارتباط با فانکشن‌های کنترل انتقال، فراهم می‌کنند. این فانکشن‌ها همچنین مکانیزم‌های QOS را با سر و کار داشتن مستقیم با ترافیک کاربر فراهم می‌نمایند که شامل مدیریت بافر، صف و زمان بندی، فیلتر کردن بسته، طبقه‌بندی ترافیک، علامت‌گذاری، سیاست‌گذاری و شکل دهی، کنترل دروازه و دیواره‌ی آتش می‌باشد.

۶. ۱۰. ۲. فانکشن‌های کنترل اتصال شبکه

این فانکشن‌ها رجیستریشن را در سطح دسترسی و initialization فانکشن‌های کاربر نهایی را برای دسترسی به سرویس‌های NGN فراهم می‌کنند. این فانکشن‌ها، مسؤل فراهم کردن شناسایی و صحت یابی[1] بوده و مدیریت فضای آدرس IP شبکه‌ی دسترسی و صحت‌یابی Sessionهای دسترسی را بر عهده دارند. آنها همچنین نقطه‌ی تماس سرویس NGN و فانکشن‌های کاربردی را به کاربر نهایی اعلام می‌کنند. این بدان معنی است که فانکشن‌های کنترل اتصال شبکه به تجهیزات نهایی در رجیستر کردن و آغاز استفاده از NGN کمک می‌نمایند.

---

[1] - identification / authentication

۷. ۱۰. ۲. فانکشن‌های کنترل منبع Admission [1]

RACFها فانکشن‌های کنترل admission و کنترل دروازه را تأمین می‌کنند که شامل کنترل NAPT [2] و DSCP [3] می‌باشد. کنترل admission مستلزم صحت‌یابی بر اساس پروفایل کاربر و از طریق فانکشن‌های کنترل اتصال شبکه می‌باشد.

همچنین، کنترل admission، عملیات اختیار دادن[4] بر اساس پروفایل کاربر و با توجه به قوانین و سیاست گذاری‌های اپراتور و موجودیت منابع را در بردارد. بررسی موجودیت منابع به معنی آن است که فانکشن کنترل admission تحقیق می‌کند که آیا یک تقاضای منبع به عنوان مثال، برای پهنای باند مجاز است یا خیر (با توجه به منابع باقیمانده و موجود).

RACFها به منظور کنترل یک یا چند مورد از فانکشن‌های زیر در لایه انتقال با فانکشن‌های انتقال کنش و واکنش دارند: فیلدینگ بسته، طبقه‌بندی ترافیک، علامت‌گذاری و سیاست‌گذاری، رزرواسیون و اختصاص پهنای باند، NAPT، NAPT/ FW traversal و اندازه گیری میزان استفاده.

۸. ۱۰. ۲. فانکشن‌های پروفایل کاربر انتقال

این بلوک فانکشنال نشان دهنده‌ی تلفیق اطلاعات کاربر و سایر اطلاعات کنترلی در یک فانکشن «پروفایل کاربر» در لایه‌ی انتقال است. این فانکشن را می‌توان به صورت مجموعه‌ای از دیتابیس‌های هماهنگ و مرتبط واقع در هر بخش NGN مشخص و پیاده‌سازی نمود.

۹. ۱۰. ۲. فانکشن‌های دروازه

این فانکشن فراهم کننده قابلیت interwork با سایر شبکه‌ها شامل اکثر شبکه-های موجود مانند شبکه‌های مبتنی بر PSTN/ISDN و همچنین اینترنت می‌باشد. این فانکشن‌ها حتی Interworking با سایر NGNهای متعلق به سایر administratorها

---

[1] - Resource and Admission Control Functions (RACF)
[2] - Network Address and Port Translation
[3] - Differentiated Services Field Code Point
[4] - Authorization

را پشتیبانی می‌کنند.
NNI بین یک شبکه و سایر شبکه‌ها در هر دو سطح کنترل و انتقال، شامل دروازه‌های مرزی، مورد استفاده قرار می‌گیرد. کنش و واکنش بین سطوح کنترل و انتقال می‌تواند به طور مستقیم و یا از طریق فانکشن کنترل انتقال، صورت‌پذیرد.

۱۰. ۱۰. ۲. فانکشن‌های Media Handling

مجموعه فانکشن‌های media handling شامل فرآیندهای منابع مدیا برای فراهم‌کردن سرویس‌هایی از قبیل تولید سیگنال‌های تن، ترانسکدینگ و conference bridging می‌باشد.

۱۱. ۱۰. ۲. فانکشن‌های لایه سرویس

این فانکشن‌ها فراهم کننده‌ی سرویس‌های session-based و غیر session-based شامل: subscribe/ notify برای اطلاعات حضور و یک روش پیام برای رد و بدل کردن پیام لحظه‌ای می‌باشند. فانکشن‌های لایه‌ی سرویس همچنین تمامی قابلیت‌های شبکه در ارتباط با سرویس موجود و قابلیت‌ها و اینترفیس‌های مرتبط با تجهیزات موجود مشتری را تأمین می‌نمایند.

۱۲. ۱۰. ۲. فانکشن‌های کنترل و سرویس

این فانکشن‌ها شامل فانکشن‌های کنترل session، یک فانکشن رجیستریشن، و فانکشن‌های صحت‌یابی و اختیاردهی در سطح سرویس هستند. این فانکشن‌ها همچنین می‌توانند شامل فانکشن‌های کنترل منابع مدیا (یعنی منابع تخصصی) باشند.

۱۳. ۱۰. ۲. فانکشن‌های پروفایل کاربر سرویس

این فانکشن‌ها نشان دهنده‌ی تلفیق اطلاعات کاربر و سایر اطلاعات کنترلی در یک فانکشن پروفایل کاربر در لایه سرویس هستند. این فانکشن را می‌توان به صورت مجموعه‌ای از دیتابیس‌های هماهنگ و مرتبط واقع در هر بخش NGN، مشخص و پیاده‌سازی نمود.

۱۴. ۱۰. ۲. فانکشن‌های کاربرد

شبکه‌های API NGNهای باز را پشتیبانی می‌نمایند که این امر سرویس دهندگان خارجی(third-party) را قادر می‌سازد تا قابلیت‌های NGN را برای به وجود آوردن سرویس‌های بهبود یافته برای کاربران NGN به کار گیرند. تمامی فانکشن‌های کاربرد (قابل اعتماد یا غیرقابل اعتماد) و همچنین سرویس دهندگان third-party از طریق سرورها یا دروازه‌ها در لایه سرویس به قابلیت‌های لایه سرویس NGN دسترسی دارند.

۱۵. ۱۰. ۲. فانکشن‌های مدیریتی

پشتیبانی مدیریت شبکه یک امر مبنایی در NGN به شمار می‌رود. فانکشن‌های مدیریتی اپراتور NGN را قادر می‌سازند تا شبکه را مدیریت کرده و سرویس‌های NGN را با کیفیت، امنیت و قابلیت اعتماد مورد نظر فراهم نماید.

این فانکشن‌ها به طور گسترده و توزیع شده در هر یک از مؤلفه‌های فانکشنال[1](FE) قرار گرفته‌اند. این فانکشن‌ها با FEهای مربوط به مدیریت المان‌های شبکه، مدیریت شبکه و مدیریت سرویس دارای ارتباط تنگاتنگ می‌باشند.

فانکشن‌های مدیریتی شامل فانکشن‌های charging و Billing می‌باشد. این فانکشن‌ها از طریق کنش و واکنش با یکدیگر در NGN اطلاعات accounting را جمع آوری کرده و بدین ترتیب اطلاعات میزان استفاده از منابع را برای اپراتور NGN فراهم می‌نمایند و اپراتور از طریق آن، قبض پرداخت برای کاربران صادر می‌نماید. این فانکشن‌ها دارای قابلیت جمع آوری اطلاعات هم برای پردازش تأخیری (offline charging) و هم پردازش near-real-time با کاربردهایی نظیر سرویس‌های پیش پرداخته (online charging) می‌باشند.

۱۶. ۱۰. ۲. فانکشن‌های End- User

اینترفیس‌های کاربر نهایی هم فیزیکال و هم فانکشال (کنترلی) می‌باشند (همان

[1] - Functional Entity

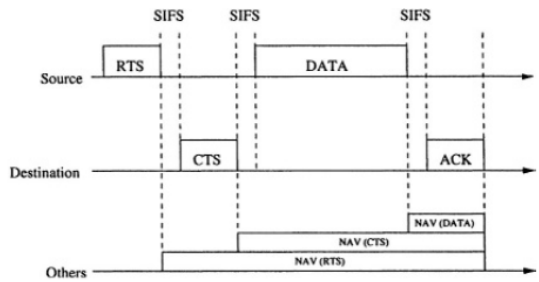
طور که در شکل ۳-۲ نشان داده شده است). هیچ گونه فرضی در مورد اینترفیس‌ها و شبکه‌های متنوع مشتری که ممکن است به شبکه دسترسی NGN متصل شوند، انجام نمی‌شود. تمامی تجهیزات مختلف مشتری در NGN پشتیبانی می‌شوند. این تجهیزات می‌توانند ثابت یا سیار باشند.

۱۷. ۱۰. ۲. فانکشن توزیع هماهنگی (DCF)

Distributed Coordination Function(DCF) سعی می‌کند که دسترسی یکسان را به تعداد بسته‌های اطلاعاتی به تمامی گره‌هایی که از shared media استفاده می‌کنند ایجاد کند. برای مثال در ساختار شالوده‌ای اگر تمام گره‌ها در یک سلول در دامنه ارسال یکدیگر باشند و هیچ منبع نویز دیگری هم وجود نداشته باشد، تمامی کاربرها و AP تعداد یکسان بسته ارسال خواهند کرد.

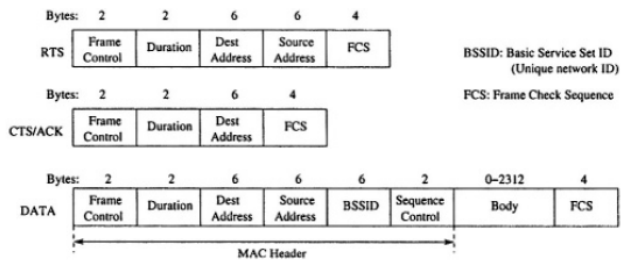
در شبکه‌های adhoc میزان توان عملیاتی که یک گره با استفاده از DCF به دست می‌آورد تابعی از تعداد همسایه‌ها و به وضعیت صف هر یک بستگی دارد که چه مقدار جمع شده باشند یا خیر. با توجه به اینکه میزان توان عملیاتی به وضعیت همسایه‌های یک گره بستگی دارد، یک مسئله جهانی در مقابل یک مسئله‌ی محلی تلقی می‌شود. لذا در یک شبکه‌ی adhoc که از DCF استفاده می‌کند، میزان توان عملیاتی، به توپولوژی شبکه بستگی دارد. نکته‌ی دیگر این که در DCF مکانیزمی برای دسترسی به هر گره آماده می‌شود و نه برای هر لینک.

در ادامه مکانیزم DCF به طور دقیق بررسی می‌شود. هر گره که بسته‌ای برای ارسال دارد یک برش زمانی را برای ارسال انتخاب می‌کند. در برش زمانی انتخاب شده بسته RTS ارسال می‌شود. گیرنده‌ای که برای ارسال داده آماده است با بسته CTS به آن جواب می‌دهد. به دنبال آن نیز فرستنده بسته اطلاعاتی خود را ارسال می‌کند. ارسال این بسته‌ها نیز با بازه‌های زمانی کوتاه به نام SIFS (Short Inter Frame Space) جدا می‌شود. این بازه این امکان را می‌دهد که بین ارسال و دریافت داده سوییچ کند. روال ارسال این بسته‌ها در شکل (۴. ۲) نشان داده شده است.



شکل ۴. ۲ روال DCF در IEEE 802.11

در بسته‌هایی که در لایه MAC برای این چهار بسته در نظر گرفته شده است بخشی با نام «دوره» وجود دارد که بیانگر زمان باقیمانده تا پایان دریافت پیغام Ack است. این پیامها در شکل (۲-۴) نشان داده شده است.



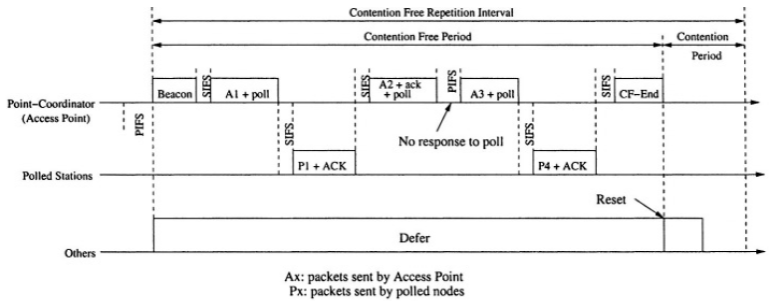
شکل ۵. ۲ ساختار بسته‌های DCF در IEEE 802.11

بر مبنای این داده‌ها گره‌های همسایه ساختار Network Allocation Vector (NAV) خود را به روز می‌کنند که برای نشان دادن زمان باقیمانده برای تعویق انداختن تمامی ارسالها را نشان می‌دهد.

اگر ارسال بسته با خطا مواجه شود، فرستنده طول contention window خود را زیاد می‌کند. تعداد دفعات ارسال برای بسته‌های کوچک به ۴ و برای بسته‌های بزرگ به ۷ محدود شده است. اگر در این تعداد دفعات بسته‌ای ارسال شود و هر بار با خطا مواجه شود طول contension window به مقدار اولیه خود برمیگردد. اگر ارسال بسته داده با موفقیت انجام شود در این حالت نیز طول contension window به مقدار حداقل خود برمی‌گردد.

۱۸. ۱۰. ۲. فانکشن نقطه هماهنگی(PCF)

PCF در حالت Infrastructure در استاندارد ,۱۱۸۰۲ عمل می‌کند. استاندارد ایجاب می‌کند که یک AP که در مود PCF پیاده شده است بایستی وضعیت خود را به حالت DCF تغییر بدهد. یعنی از حالت contention-free period به حالت contention period سوییچ کند. در حالت PCF هر AP بسته‌ها را به گره‌های دیگر می‌فرستد و لیست گره‌هایی که به آنها شانس ارسال را داده نظارت می‌کند. بر خلاف حالت DCF، این حالت تنها در صورتی می‌توانند ارسال کنند که به وسیله AP نظارت شده باشند. زمان آغاز contention free یعنی زمانی که PCF عمل می‌کند، به وسیله یک beacon و توسط AP نشانه‌گذاری می‌شود. در این نشانه‌گذاری طول زمان contention free نیز اعلام می‌شود. در این زمان زمان‌بندی ارسال به طور کامل توسط AP تعیین می‌گردد. زمان contention free در صورتی که AP بسته مخصوصی با نام CF-End را ارسال کند، کاهش می‌یابد. فرآیند Poll و acknowledgment به وسیله بسته‌های data حمل می‌شود. که در شکل (۲-۳) نشان داده شده است.



شکل ۶. ۲ Point Coordination Function

البته قبل از ارسال beacon، یک AP حداقل زمانی به اندازه (PIFS (PCF Inter Frame Space منتظر می‌ماند. این کار این اطمینان را ایجاد می‌کند که تمامی ارتباطاتی که مربوط به زمان contention free متوقف شده‌اند. این زمان همچنین برای انتظار یک پاسخ به poll توسط AP به کار می‌رود. بعد از گذشت این زمان، AP نتیجه می‌گیرد که گره‌ای که poll شده است بسته‌ای برای ارسال ندارد و یا poll را دریافت نکرده است. در ادامه نیز بعد از گذشت زمان PIFS به pollکردن گره دیگر می‌پردازد.

۱۱. ۲. ساختار IMS [1]

به عنوان تعریفی اولیه می‌توانیم IMS را ساختاری استاندارد برای پشتیبانی ارتباط چندرسانه‌ای در شبکه‌های نسل آینده[2]، NGN، بیان کنیم. در این بخش به بررسی ساختار IMS می‌پردازیم. لایه‌های مختلف تعریف شده در IMS و همچنین اجزای شبکه را بررسی می‌کنیم.

IMS مجموعه‌ای است از مؤلفه‌های فانکشنال و اینترفیس‌های شبکه هسته که توسط سرویس‌دهنده شبکه برای ارائه سرویس‌های مبتنی بر SIP به کاربران مورد استفاده قرار می‌گیرد. SIP [3] عبارت است از پروتکل راه اندازی جلسه که توسط IETF تعریف شده است. بخش عمده IMS از تکنولوژی شبکه دسترسی مستقل است. هر چند که ارتباطاتی بین IMS و فانکشن انتقال مربوطه وجود دارد که می‌تواند به نوع دسترسی وابسته باشد. یک IMS بر روی پروتکل‌های IETF بنا نهاده شده و دارای پروفایل‌ها و بهبودهای خاصی می‌باشد که نتیجه آن تأمین یک سیستم کامل و مقاوم چند رسانه‌ای می‌باشد. بهبودها و پروفایل‌های عملیاتی مذکور پشتیبانی کنترل اپراتور، شارژ، صورت حساب و همچنین امنیت را دربردارند.

علاوه بر بهبودها و پروفایل‌های فوق، IMS نیازمند مجموعه‌ای از اینترفیس‌های عمودی می‌باشد تا موارد زیر را فراهم نماید:

اینترفیس‌های مشترک به سرورهای کاربردی برای صورت حساب، امنیت، اطلاعات مشترکین، کنترل سرویس، و همچنین اینترفیس‌هایی به بلوک‌های سازنده سرویس مانندفانکشن‌های presence.

۱. QOS مدیریت شده و الزامی

۲. ایجاد دروازه‌ی مدیا مبتنی بر جلسه و تحت کنترل اپراتور

۳. charging , accounting توأم در میان لایه‌های سرویس، جلسه و انتقال

این توانایی‌ها، سبب تمایز IMSها از کاربردهای متداول اینترنت برای کنترل جلسه

---

[1] IP Multimedia Subsystems
[2] Next Generation Networks
[3] Session Initiation Protocol

می‌گردند. یک IMS بر اساس مدلی بنا شده است که در آن اپراتور شبکه و سرویس‌دهنده به ترتیب دسترسی به شبکه و دسترسی به سرویس‌های داده شده به مشتریان را کنترل می‌نمایند. این مفهوم در تقابل با مدل متداول اینترنت قرار دارد که در آن، شبکه از دید مشتری پنهان می‌باشد و تمامی سرویس‌ها توسط نقاط انتهایی (end point ها) فراهم می‌گردند. در نتیجه، به دلیل وجود چنین محیط کنترل شده‌ای، کاربران QOS مدیریت شده و پشتیبانی مشتری را، حداقل از دیدگاه تئوری، تجربه می‌نمایند.

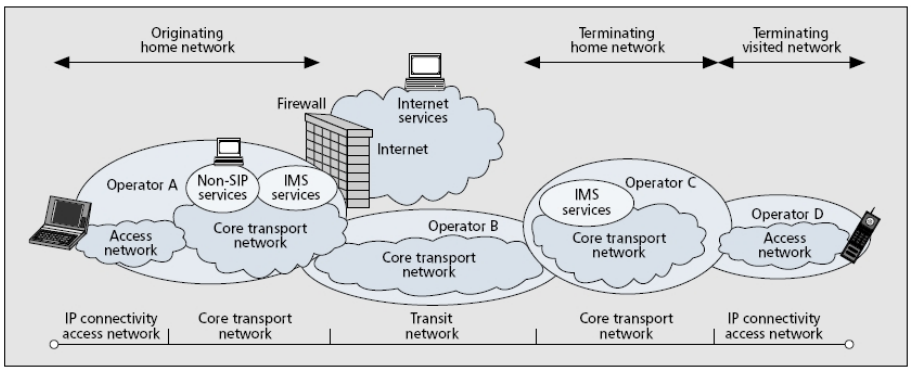
۱. ۱۱. ۲. شبکه‌های هسته و شبکه‌های دسترسی

همان طور که قبلاً ذکر شد، IMS مجموعه‌ای است از FEهای شبکه هسته که توسط سرویس‌دهنده شبکه برای ارائه سرویس به کاربران مورد استفاده قرار می‌گیرد که در آن، یک یا چند شبکه دسترسی رادیویی به یک هسته مشترک متصل می‌باشند. شبکه‌های دسترسی رادیویی اتصال ترمینال‌ها را به سرویس‌های فراهم شده در هسته برقرار می‌نمایند.

در IMS، شبکه دسترسی مجموعه‌ای است از مؤلفه‌هایی که اتصال انتقال IP بین domain کاربر و شبکه انتقال هسته را فراهم می‌نمایند. شبکه‌های دسترسی بر اساس تکنولوژی‌های مورد استفاده در آنها، و همچنین بر اساس اینکه هر شبکه به چه مؤسسه‌ای تعلق دارد، از یکدیگر تمایز پیدا می‌کنند.

شبکه‌ی هسته مجموعه‌ای است از مؤلفه‌هایی که اتصال انتقال IP را بین شبکه‌ی دسترسی و شبکه‌ی انتقال هسته‌ی دیگر، بین دو شبکه‌ی دسترسی و یا بین دو شبکه‌ی هسته‌ی دیگر فراهم می‌کنند. شبکه انتقال هسته همچنین اتصال به مؤلفه‌های لایه سرویس مانند IMS را فراهم می‌نماید. شبکه‌های هسته نیز بر اساس تعلق و تکنولوژی آنها از یکدیگر تفکیک می‌گردند. یکی از مشخصه‌های اساسی یک IMS، پشتیبانی حرکت کاربر می‌باشد. بنابراین، تمایز بین شبکه‌های هسته و دسترسی در راستای جداسازی فانکشن‌های مورد نیاز برای پشتیبانی یک IMS، مهم به نظر می‌رسد. شکل (۷. ۲) مثالی را از مجموعه تقسیم‌بندی شده شبکه‌های مذکور را نمایش می‌دهد. در خلال حرکت یک کاربر از یک شبکه دسترسی به شبکه دسترسی دیگر، قابلیت فراهم کردن سرویس‌های یکسان شبکه هسته امکان‌پذیر می‌باشد. این مفهوم هم برای

حرکت‌های غیر real-time مانند roaming و هم برای حرکت‌های real-time در زمانی که تکنولوژی دسترسی، حرکت را پشتیبانی می‌کند، مانند hand off، صادق می‌باشد.



شکل ۷. ۲ تفکیک شبکه

همان طور که در شکل(۶-۶) قابل مشاهده است، IMS مفهوم شبکه خانگی را نیز پشتیبانی می‌کند. مفهوم شبکه خانگی[1] در مقابل مفهوم شبکه‌ی ملاقات شونده[2] مطرح می‌شود. در این مفهوم، شبکه خانگی، شبکه‌ی هسته‌ای می‌باشد که سرویس‌های IMS را پشتیبانی نموده و مشترکین IMS را نگهداری می‌نماید. از دیگر سو، شبکه ملاقات شونده، شبکه‌ای است که در حال حاضر اتصال کاربر را با سرویس‌های IMS وی فراهم می‌کند. لذا، در شکل (۷. ۲)، اپراتور A صاحب شبکه خانگی کاربر لپ تاپ می‌باشد در حالی که اپراتور C صاحب شبکه خانگی کاربر تلفن همراه است که این کاربر نیز به نوبه خود در حال استفاده از خدمات roaming از اپراتور شبکه D می‌باشد.

۱۲. ۲. مقدمه‌ای بر QOS در شبکه‌های نسل آینده (NGN)

تأمین QOS در شبکه‌های مختلف یا ساختارهای متفاوت، خود به تنهایی مسأله‌ای پیچیده است. پیچیدگی مساله ذاتاً به عدم وجود مدل ریاضی ساده و سراسری برای

[1] - Home Network
[2] - Visited Network

شبکه‌های داده برمی‌گردد. گروه‌های تحقیقاتی متفاوت روشهای مختلفی را در برخورد با این مسأله در پیش می‌گیرند. بعضی گروه‌ها با ارائه مدل‌های ساده شده به تحلیل مسأله می‌پردازند و نهایتاً با ارائه شبیه سازی‌های نسبتاً ساده، قدرت الگوریتم‌های پیشنهادی خود را به اثبات می‌رسانند. گروه‌هایی نیز اساس کار را بر شبیه سازی‌هایی نسبتاً دقیق می‌گذارند و به نتایجی دست پیدا می‌کنند که ناگزیر نتایج نوعاً جزئی (ویژه آن شرایط شبیه‌سازی خاص) محسوب می‌شوند.

جدای از پیچیدگی مساله QOS، تامین آن در شبکه‌های NGN که مملو از مفاهیم نوپا و غیر دقیق است، بر پیچیدگی مسأله می‌افزاید. بنابراین به نظر نمی رسد که راه حل سراسری برای این مساله قابل ارائه باشد. با این وجود، در طول زمان اهمیت این مسئله (به ویژه در NGN) بر دشواری آن برتری یافته است و مقالات متعددی در جستجوی راه حل‌های کلی و جزئی منتشر شده است.

۱. ۱۲. ۲. تعریف QOS

تاکنون به طور خلاصه به مباحث مربوط به QOS اشاره شد. اما تعاریف دقیق آن چیست؟

در لایه‌های مختلف شبکه از QOS تعاریف مختلفی وجود دارد. در حد لایه فیزیکی، به نرخ داده و نرخ packet loss به عنوان متریک‌هایی که کیفیت کانال را توضیح می‌دهند، به عنوان QOS معرفی می‌شود. اگر کیفیت کانال به طور دائم تغییر کند، ثابت نگاه داشتن نرخ ارسال داده غیر ممکن خواهد بود. در حد لایه‌ی MAC به بخشی از زمان که یک گره به کانال دسترسی داشته و داده را ارسال می‌کند به عنوان QOS معرفی می‌شود. در حد لایه routing به متریک‌های QOS به متریک‌های هر hop در یک مسیر چند hop بستگی دارد. وظیفه لایه routing این است که مسیرهایی را که نیازهای QOS را ارضا می‌کنند، محاسبه و نگهداری نماید. این متریک‌ها بیشتر به طول عمر یک ارتباط مرتبط هستند. در لایه انتقال و لایه‌های بالاتر در صورتی که لایه routing نتواند به طور کامل به QOS بپردازد، بخش‌های تکمیلی QOS همراه خواهد شد.

پهنای باند و تاخیر و لرزش از جمله مهمترین پارامترهایی هستند که تاکنون در مبحث QOS به آنها پرداخته شده است. مشکل تأخیر اکثراً به دلیل طولانی شدن صف‌های داده در مسیریاب‌ها ایجاد می‌شود. مشکل jitter زمانی ایجاد می‌شود که بسته‌های با توالی معین با زمانهای مختلف به مقصد برسند. این مشکل در شبکه‌های VoIP که نیاز به حفظ توالی بسته‌های دارد بسیار مشکل ساز خواهد بود. در انتقال صوت و ویدئو نیز این مسأله به شدت حائز اهمیت است.

۲. ۱۲. ۲. تامین QOS در شبکه‌های IP

شبکه‌های نسل آینده به دلیل تکنیکی بودن، بر IP core استوار خواهند بود. شبکه‌های IP به طور سنتی فاقد امکانات تامین QOS برای کاربردهای خاص است. این مسأله از دیر باز مورد توجه بوده است و راه حل‌های متفاوتی در قالب RFCها برای آن ارائه شده است.

از بین این راه حل‌ها، الگوریتم مبتنی بر Diffserv در قالب Expedited Forwarding و Forwarding،Assured و نیز الگوریتم‌های مبتنی برIntserv [RFC 1633] در قالب RFC 2205-2210 از اهمیت بیشتری برخوردارند و به طور اجمالی (به ویژه RFC 1633, 2475) در این پروژه مورد مطالعه قرار گرفته‌اند و در صورت لزوم مطالعه دقیق‌تر روی آنها انجام خواهد شد. خلاصه این الگوریتم‌ها در مراجع مختلف موجود است و در اینجا به آن نخواهیم پرداخت.

۳. ۱۲. ۲. اجزاء مسأله QOS

دیدگاه ما در این پروژه بهینه‌سازی QOS در شبکه‌های نسل آینده مبتنی بر IP است. این مساله را می‌توان در چهار جزء ذیل مورد بررسی قرار داد:

الف. کلاس‌بندی ترافیک‌ها (traffic classification)

ترافیک یا flowهای مختلف از لحاظ کیفیتی که از آنها انتظار می‌رود متفاوتند. به همین دلیل اولین قدم در تامین QOS، طبقه‌بندی ترافیک‌ها بر حسب ضروریات کیفی (quality requirement) آنها بر حسب پارامترهای کیفیت از جمله end2end delay,

bit-rate، مینیمم، Jitter و غیره است. هر پروتکلی بر حسب نوع سرویس‌هایی که ارائه می‌دهد، طبقه بندی‌های متفاوتی از ترافیک‌های مجاز ارائه می‌دهد. این طبقه‌بندی نسبی است و بنابراین در مساله ما برای هر شبکه (Domain) ثابت و تعیین شده، فرض خواهد شد.

ب. جدول زمانی بسته‌ها (PS)

در این قسمت، نحوه برخورد با پاکت‌های داده متعلق به جریان‌های مختلف که که برای دسترسی به کانال صف بسته اند، بحث می‌شود. (Packet Scheduling)

ج. استراتژی صف

در این بخش به طور خلاصه، نحوه برخورد با پاکت‌های داده در صورت شلوغ شدن صف‌ها تعیین می‌شود. روش‌های مختلفی چون Drop-tail، Random Early Detection(RED) وRED Weighted در همین بخش مطرح می‌شود (Queuing Strategy).

د. شکل ترافیک

الگوریتم مطرح در این جزء سعی در حذف Burstiness ترافیک‌ها را دارند چرا که این ویژگی بوضوح منجر به تشدید Congestion در لینک‌ها و تضعیف QOS می‌گردد. الگوریتم‌های مطرح در این بخش، ترکیبی ازLeaky Bucket و Token Bucketها هستند (Traffic Shaping).

بدین ترتیب مساله QOS در یک کلام، انتخاب بهینه الگوریتم‌های بخش‌های (ب)، (ج) و (د) برای کلاس‌های تعریف شده در (الف) با هدف اپیتیم کردن شبکه است[1]. از جمله عواملی که در حل این مساله باید مد نظر قرار گیرد، پایین نگه داشتن سطح پیچیدگی محاسبات است.

[1] برای مثال الگوریتمهای مناسب برای ترافیك از کلاس Best Effort (که معمولا در تمام طبقه بندی‌های در نظر قرار می‌گیرد) به صورت (ب)FIFO ، (ج) Drop-tail و (د) Token Bucket است.

۴. ۱۲. ۲. معیارهای بهینگی

بهینگی از دیدگاه‌های مختلف می‌تواند معیارهای متفاوتی داشته باشد. از دید تامین کننده سرویس مجموعه الگوریتم‌های ارائه دهنده QOS زمانی بهینه خواهد بود که بیشترین بهره‌وری منابع شبکه و در نتیجه بیشترین سوددهی را بهمراه داشته باشد. از دیدگاه کاربر سرویس، شرایط اپتیم زمانی برقرار خواهد بود که به ازای یک سطح QOSتضمین شده، کمترین هزینه را برای ارائه سرویس پرداخت کند یا با پرداخت مشخص بیشترین رضایت یا QOS به او ارائه شود. بر این مبنا امکان تعریف مساله بهینه‌سازی فراهم خواهد آمد.

البته باید دقت شود که این دو دیدگاه لزوما متناقض نیستند. برای مثال نشان می‌دهد که با بالا بردن ضمانت در ارائه QOS به کاربران، اولاً آنها QOS بالاتر از میزان مطلوب خود دریافت نمی‌کنند (ولذا هزینه بیشتری نمی‌پردازند) ثانیا تامین کننده سرویس می‌تواند کاربران بیشتری را حمایت کند و در نتیجه سود بیشتری عاید خود نماید. دیدگاه ما در این پروژه استفاده از معیار بهره‌وری به عنوان معیار بهینگی خواهد بود.

۵. ۱۲. ۲. الگوریتم‌های جدول زمان‌بندی

تحقیقات متعددی در زمینه بهینه‌کردن نحوه تامین QOS در شبکه‌های مختلف انجام شده است. با این وجود در مورد روش جدول زمان‌بندی بسته تنوع کار بسیار بالاتر از سایر هزینه‌ها ست. این موضوع به دلیل سهم عمده این جزء در تامین QOS از طریق تسهیم منابع شبکه است. به همین دلیل جهت گیری عمده در این پروژه در این جزء از مساله خواهد بود و سعی خواهیم کرد الگوریتم‌های PS بهینه را برای شرایط متفاوت شناسایی کنیم.

در زیر چند نمونه از الگوریتمهای PS را عنوان می‌کنیم:

۱. Priority Queuing، که در آن، پاکت‌های داده بر حسب اولویت سرویس داده می‌شود.

۲. Weighted Fair Queuing (WFQ)، در این روش برای هر flow صفی فرض می‌شود و بسته به کلاسی که flow به آن متعلق است، وزنی برای آن صف تعیین

می‌شود. این وزن میزان سهم آن Flow را از پهنای باند تعیین می‌کند. این الگوریتم معمولا در ترکیب با PQ به کار می‌رود و نسخه‌های متفاوتی از آن تاکنون ارائه شده است، از جمله:

Start time fair Queuing
Hierarchical fair Queuing
Self-clocked fair Queuing
Worst-case fair weighted fair Queuing

مبنای تقدم سرویس در این روش deadline پاکت‌های داده است و دغدغه اصلی این الگوریتم‌ها تامین QOS از لحاظ تاخیر و تا حدی از لحاظ jitter است.

ارائه الگوریتمی کارا در این بخش می‌تواند یکی از پیشنهادات برای ادامه کار باشد. به ویژه روش‌های ترکیبی و بین لایه‌ای اخیرا مورد توجه قرار گرفته است که به علت فراهم نبودن مدل ریاضی اساسا مبتنی بر شبیه‌سازی هستند. مدل‌سازی و فرموله‌کردن این الگوریتم‌ها می‌تواند گام مهمی در راستای ارائه بهینه QOS باشد.

۶. ۱۲. ۲. الگوریتم‌های جدول زمان‌بندی در محیط بی سیم

شبکه‌های بی سیم به عنوان جزء لاینفک شبکه‌های NGN، توجه خاصی را در مساله QOS می‌طلبند. ویژگی‌هایی چون حضور کاربران متحرک و نیز کانال متغیر با زمان و error-prone موجب می‌شود که فرضیات اولیه الگوریتم‌های تخصیص منابع در شبکه‌های سیمی در مورد این شبکه‌ها فاقد کارایی باشند. همین مسأله باعث شده تا الگوریتمهای PS خاص محیط‌های بی‌سیم مورد مطالعه قرار گیرد. برخی از این کارها با فرض ATM Core انجام شده (طول پاکت‌های ثابت، QOS بالا،... .). مطالعه و تطبیق این کارها (که از پایه ریاضی خوبی برخوردار است) به IP Core می‌تواند یکی از زمینه‌های پیشنهادی برای ادامه کار باشد.

۷. ۱۲. ۲. تامین QOS در لایه دسترسی

تاکنون پروتکل‌های مختلفی برای لایه دسترسی شبکه‌های بی‌سیم پیشنهاد شده‌اند. این روش‌ها را به طور کلی می‌توان به دو دسته عمده Reservation-based و contention-based تقسیم کرد. البته روش‌هایی نیز وجود دارد که ترکیبی هستند که

ترکیبی از دو روش قبلی می‌باشند. و در نهایت روش‌هایی که به صورت cross layer به طراحی اقدام می‌کنند.

روش Reservation-based این حسن را دارد که collision-free است. زیرا هر گره داده‌های خود را در کانال اختصاص داده شده به آن ارسال می‌کند. پروتکل TDMA-based بر همین اساس معرفی شده است. در چنین شبکه‌ای گره‌ها به کلاسترهایی تقسیم می‌شوند و برای ارتباط با هم ابتدا به رزرو کردن Time slot برای ارسال و دریافت داده می‌پردازند. پروتکل‌هایی که بر اساس TDMA طراحی شده باشند دارای latency بالایی هستند. علاوه بر آن به همزمانی دقیقی نیز نیاز دارند.

الگوریتم‌های contention-based بر خلاف مدل قبلی به ساختار کلاستری نیاز ندارند. دسترسی گره‌ها به کانال بر اساس روش Carrier Sense است. این روش از نظر robustness و scalibility بسیار بهتر از روش اول است ولی به دلیل وجود collision مشکلات خاص خود را دارند. از طرفی نیز در چنین شبکه‌هایی داده‌های با همبستگی بالا و ترافیک ناگهانی در شبکه محتمل است.

از میان این الگوریتم‌ها می‌توان به IEEE 802.11 اشاره کرد. این روش به دلیل آنکه از لحاظ مصرف انرژی به صرفه نیست در شبکه‌های بی‌سیم کاربردی ندارد. تصحیحات بسیاری در WLAN MAC انجام شده است. از میان این مدل‌های پیشنهادی می‌توان به S-MAC و T-MAC اشاره کرد. در این مدل‌ها به بهای افزایش latency میزان مصرف توان کم شده است.

از جمله روش‌های hybrid می‌توان به IEEE 802.15.4 اشاره کرد که دو روش قبلی را با هم ترکیب کرده و روش CSMA/CA را معرفی کرده است. روش نهایی برای طراحی لایه MAC بر اساس Cross-Layer است. به عنوان مثال از این روش‌ها می‌توان به DMAC اشاره کرد که پروتکل پیشنهادی برای لایه MAC، به Routing نیز وابسته است.

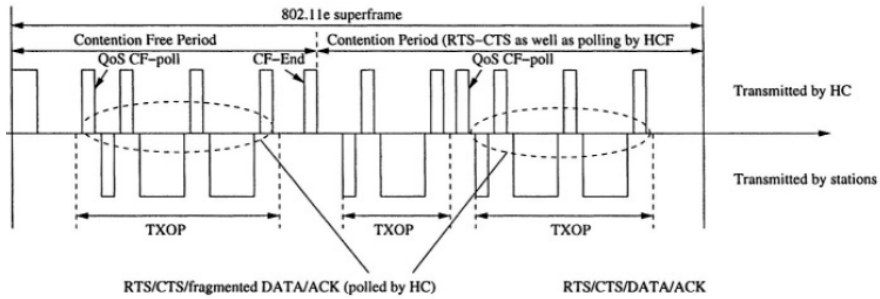
۸. ۱۲. ۲. QOS در IEEE 802.11e

در استاندارد IEEE 802.11e مکانیزم‌هایی برای اولویت‌بندی در شبکه ایجاد شده است. از آنجا که در شبکه اولویت دادن بسیار سخت است، این روال به صورت احتمالی

یا probabilistic بررسی شده است. این اولویت‌بندی را به عنوان یک متریک QOS می‌توان مطرح کرد.

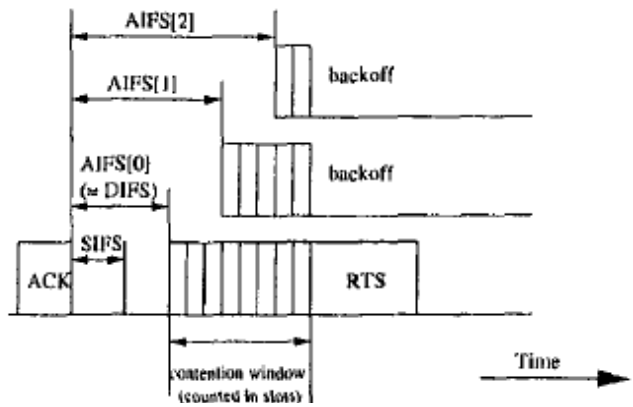
عملکرد DCF و PCF در استاندارد جدید بهبود یافته است و به صورت EDCF و HCF مطرح شده است. که در آنها مکانیزم‌هایی برای اولویت‌بندی اضافه شده است.

در شکل (۸. ۲) این عملکردها نشان داده شده است.



شکل۸. ۲ ساختار یک super frame در استاندارد IEEE 802.11e

در EDCF فریم‌هایی که وارد لایه MAC می‌شوند می‌توانند هشت سرویس با اولویت مختلف را تقاضا کنند. این اولویت‌ها به access categories مختلف نگاشته می‌شوند. هر AC می‌تواند مقدار متفاوتی برای یک بازه DIFS داشته باشد که در اینجا به آن AIFS می‌گویند. در شکل (۹. ۲) کلاسهای مختلف مقادیر AIFS نشان داده شده است.



شکل ۹. ۲ Backoff streamهایی با اولویتهای مختلف

این مقادیر می‌توانند به صورت خودکار به وسیله یک AP تنظیم شوند. گره‌ها نیز به وسیله beaconها از این مقادیر مطلع می‌شوند. مقادیر AIFS برای هر اولویت از بقیه مقادیر متمایز است.

HCF به یک هماهنگ کننده ترکیبی این اجازه را می‌دهد که وضعیت گره‌ها را حفظ کند و زمان contention free transmit opportunities را به شیوه آگاهانه جاگیری نماید. از میزان load per traffic نیز برای زمان‌بندی یک hybrid coordinator استفاده می‌شود. بر خلاف مود PCF یک hybrid coordinator می‌تواند گره‌ها را در زمان contention free نیز poll کند.

همان طور که در عملکرد PCF ذکر شد، این پروتوکل نیز به عملکرد centeralized نیاز دارد. برای آن که خواسته‌های QOS به تمامی ارضا شود هر AP ارسالها را در سلول خود هماهنگ میکند. این پروتوکل نیاز به توسعه دارد تا بتواند در حالت غیر centralized نیز کار کند.

۹. ۱۲. ۲. پشتیبانی از QOS بااستفاده از DCF بر اساس service differentiation

همان طور که تضمین QOS قطعی دشوار است، تضمین QOS نسبی به وسیله service differentiation فراهم شده است. با این کار می‌توان سیستمی را طراحی کرد که کاربران چندین گانه را پشتیبانی کند.

همان طور که در بخش‌های قبلی شرح داده شد، گره‌ها برای دسترسی به کانال با پارامترهای یکسان رقابت می‌کنند. در نتیجه اگر تمامی گره‌ها در دامنه ارتباطی یکدیگر باشند، استاندارد می‌تواند share عادلانه‌ای ایجاد کند. اگرچه برای ایجاد differentiated sevices نیاز به تصحیحاتی در استاندارد وجود دارد. سه شیوه اصلی برای این کار ارائه شده است که در آن عملکرد DCF مورد تصحیح قرار می‌گیرد. پارامترهایی که نیاز به تصحیح دارند عبارتند از:

۱. backoff increase function1: بعد از ارسال ناموفق RTS یا داده، حداکثر backoff time دو برابر می‌شود.

۲. DIFS: این پارامتر حداقل بازه مورد نیاز برای ارسال یک بسته جدید است. برای آن که اولویت یک بسته کم شود می‌توان DIFS را زیاد کرد.

۳. Maximum frame length: با افزایش این پارامتر می‌توان throughput کانال را زیاد کرد.

فصل سوّم
معرفی VOIP

با توجه به فراگیر شدن شبکه اینترنت دیگر سیستمهای مخابراتی نیز به تدریج به سمت ایجاد قابلیت اتصال به شبکه اینترنت سوق پیدا می‌کنند. با توجه به این که مهمترین مشخصه‌ی شبکه‌ی اینترنت این است که بر پایه‌ی ارسال بسته‌ای[1] قرار دارد، دیگر سیستم‌ها نیز سعی می‌کنند از این روش برای برقراری ارتباطات خود استفاده کنند. از طرف دیگر مهمترین مساله در سیستم‌های بر پایه ارسال بسته‌ی عدم تضمین کیفیت انتقال است. زیرا در شبکه‌هایی که بر پایه‌ی ارسال بسته‌ای قرار دارند ممکن است یک بسته مدت زیادی را در انتظار بماند و یا حتی از صف یک مسیردهنده[2] دور انداخته شود. در این شبکه‌ها همچنین، ممکن است با افزایش ترافیک شبکه نرخ ارسال هرکدام از کاربران افت پیدا کند. بنابراین مهمترین شاخص‌های کیفیت سرویس، یعنی ارسال با تاخیر کم و با نرخ مطمئن، در شبکه‌های با ارسال بسته‌ای با مشکل مواجه هستند. از آنجا که بحث کیفیت سرویس، یکی از مهمترین مباحث در زمینه‌ی ارسال صوت و ویدئو است، بنابراین بحث ارسال صوت و ویدئو از طریق شبکه، به صورت بحثی جداگانه در نظر گرفته می‌شود و سعی می‌شود ارسال بسته‌هایی که حاوی اطلاعات صوت یا ویدئو هستند با تاخیر و نرخ قابل اطمینانی ایجاد شود.

---

[1] Packet Based Transmission
[2] Router

از طرف دیگر باید توجه داشت که به طور سنتی، شبکه‌ی سوئیچ تلفنی،[1] برای برقراری ارتباط صوتی استفاده می‌شود. از آنجا که این شبکه به هر ارتباط که بین دو کاربر برقرار می‌شود، یک مسیر مستقل ارائه می‌دهد، کیفیت ارتباط بین دوکاربر تنها وابسته به کیفیت اجزائ سیستم است و مستقل از ترافیک شبکه بنابراین این شبکه به طور ذاتی برای ارتباط صوت و ویدئو مناسب است. اما با توجه به افزایش استفاده از امکانات مخابراتی برای ارسال داده و به وجود آمدن زیرساختهای مناسب برای ارسال بسته‌ای، اپراتورهای شبکه‌های بسته‌ای به فکر استفاده از زیرساخت موجود برای ارسال صوت و ویدئو افتادند. با توجه به هزینه کمتر ارتباط از طریق شبکه بسته‌ای به خصوص در ارتباطات بین کشورها و بین قاره‌ای، استفاده از شبکه‌های بسته‌ای برای تماس‌های تلفنی بین کشوری از طرف مردم مورد استقبال قرار گرفت و مشکلات ارتباط در مقابل هزینه‌ی کمتر نادیده گرفته شدند.

با توجه به آنچه گفته شد لازم است، شبکه به نحوی طراحی شود که امکان ارسال بسته‌ای صوت و ویدئو فراهم آید. به عبارت دیگر لازم است که تمامی لایه‌ها برای فریم یا بسته‌ای که حاوی اطلاعات صوت یا ویدئو است اولویت قایل شوند و آنرا با تاخیر و نرخ قابل قبول ارسال کنند. بنابراین، استانداردهایی که برای برقراری امکان ارسال صوت و ویدئو در شبکه به وجود آمده‌اند به نحوی در مورد کل ساختار شبکه نظر داده‌اند.

تا کنون روش‌های مختلفی برای فراهم‌کردن ارتباط صوت و ویدئو در شبکه‌های بسته‌ای ارائه شده است. در این فصل VOIP را معرفی و سپس به بررسی ساختار و عملکرد آن می‌پردازیم.

۱. ۳. معرفی VOIP و عملکرد آن

۱. ۱. ۳. VOIP چیست؟

VOIP مخفف Voice Over Internet Protocol است. این واژه بیانگر انتقال صوت (صدای انسان و فکس) از طریق بسته‌های IP[2] و مشخصاً اینترنت است. VOIP

[1] Public Switch Telephone Network (PSTN)
[1] Internet Protocol

می‌تواند به وسیله سخت‌افزارهایی متنوع مثل رایانه‌ی شخصی، تلفن IP و تلفن معمولی (که در این صورت آن را تلفن اینترنتی می‌نامند) محقق شود. به عبارت دیگر VOIP ابزاری است که صوت را در بسته‌هایی تحت یک شبکه اطلاعاتی بااستفاده از پروتکل اینترنت (IP)انتقال می‌دهد.

VoIP(وُیپ)، تلفن IP، تلفن اینترنتی، تلفن پهن‌باند، صدای پهن‌باند و صدا روی پهن‌باند(VOBB) نیز نامیده می‌شود.

معمولاً از شرکت‌های ارائه‌کننده‌ی سرویس‌های VoIP به‌عنوان تهیه‌کنندگان، و از پروتکل‌های استفاده شده برای حمل علایم صدا روی شبکه‌ی IP، به‌عنوان صدا روی IP یا پروتکل‌های VoIP یاد می‌شود. آن‌ها را می‌توان در اصل توسعه‌ی تجاری تجربه پروتکل صدا روی شبکه (۱۹۷۳) که توسط تهیه‌کنندگان نسل قدیمی اینترنت(ARPANET) اختراع شده بود، در نظر گرفت.

یکی از محاسن VOIP کاهش هزینه‌ها ست که برخی از کاهش هزینه‌ها تا حدودی به دلیل استفاده از یک شبکه‌ی منفرد برای حمل صدا و اطلاعات است، مخصوصاً در جایی که استفاده کنندگان به شبکه‌ای دسترسی دارند که از ظرفیت آن کمتر استفاده شده و می‌تواند VOIP را بدون هیچ هزینه‌ی اضافی حمل کند. تماس‌های VoIP به VoIP برخی اوقات مجانی هستند، در حالی که تماس VOIP به شبکه‌های تلفن معمولی(PSTN) ممکن است هزینه‌ای در بر داشته باشد که باید توسط استفاده کنندگان VoIP پرداخت شود.

بر قراری ارتباط در VOIP به دو صورت کلی تعریف می‌شود:

الف. برقراری ارتباط داخل یک حوزه

ب. برقراری ارتباط بین دو حوزه

۲. ۳. تاریخچه‌ی VOIP

در سال ۱۹۷۳برای اولین بار صدا تحت شبکه ارسال شد. به کمک تکنولوژی، مخابره‌ی صدا روی پروتکل اینترنت برای استفاده‌کنندگان نهایی از حداقل دهه‌ی ۱۹۹۰ در دسترس بوده‌است. امکان استفاده از شبکه‌ی اینترنت جهت حمل صوت در سال

۱۹۹۵ مطرح شد. سابقاً نرم‌افزار PC برای ایجاد ارتباطات بین رایانه‌ها از طریق شبکه‌ی اینترنت (با استفاده از روش Dia-up به یک ISP و با نرخ مکالمه محلی)وجود داشت. با ظهور VOIP این نرم‌افزار ارتقا داده شد تا این که اطلاعات صوتی به دیجیتال و بسته در آمد و از طریق اینترنت به صورت data، قابل ارسال گشت. طرف مقابل نیز اطلاعات بسته‌ای را توسط PC دریافت کرده و پس از متصل‌کردن بسته‌های صوتی و تبدیل آن به صوت توسط بلند گوهای رایانه قابل شنیدن می‌شد. به عنوان مثال در ۱۹۹۶، یک محصول نرم‌افزاری پیچیده‌ی فشرده شده که صدای اینترنتی Vocaltec نامیده می‌شد، VoIP را، به همراه نمای اضافی(از قبیل پست صوتی و نمایشگر ID) در اختیار قرار داد. در سال ۱۹۹۷ اولین سوییچ نرم‌افزاری ساخته شد، سافت‌سوئیچ‌ها یا همان سوییچ نرم‌افزاری، برای جایگزینی سخت‌افزار سنتی سوییچ بردها و برای خدمت‌رسانی بهتر، به‌عنوان راه بین دو شبکه‌ی تلفنی، طراحی و ساخته شده بودند.

با این که برقراری یک مکالمه با استفاده از چنین روشی امکان‌پذیر شد اما مشکلات فراوانی در این معماری وجود داشت ازجمله:

۱. کیفیت صوت پایین بود.

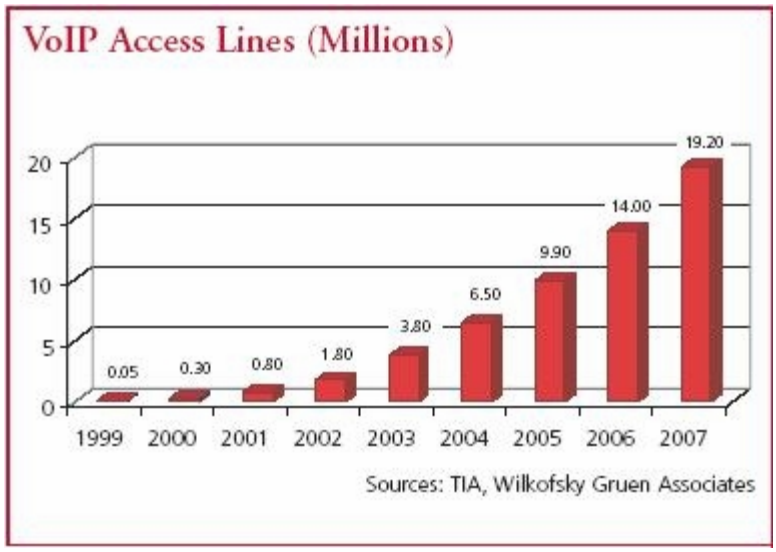
۲. هیچ گونه استانداردی مبنی بر این که چگونه صوت بسته‌بندی شود و این که چگونه اتصالات ایجاد و مدیریت شوند وجود نداشت.

۳. فقط از توپولوژی ساده‌ی شبکه‌ی تلفنی به صورت اتصالات نقطه به نقطه بین نشانی‌های IP شناخته شده پشتیبانی می‌شد.

۴. تنها سرویس‌های خیلی ساده‌ی صوتی قابل پشتیبانی بود.

که با توجه به مشکلات بالا مرحله‌ی بعدی تعریف معماریی بود که یک پارچه‌سازی بین شبکه‌ی تلفن معمولی و IP را پشتیبانی نماید. چندین گروه در این مورد شروع به کار کردند کاری که توسط این گروه‌ها انجام گرفت این بود که، آنها به یک معماری واحد جهت ارتباط شبکه‌ی تلفن معمولی با شبکه‌ی IP برای پشتیبانی از ترافیک صوت ویا هر نوع ترافیک دیگری دست یافتند. که در آخر تعدادی گره‌ی جدید معرفی شد و مسئولیت‌ها و عملکرد آنها تعریف شد.

VOIPیک تکنولوژی جدید است که اجازه می‌دهد صوت تحت اینترنت انتقال یابدVOIP از ارتباطات کامپیوتر به کامپیوتر[1] به ارتباطات تلفن به تلفن[2] رشد کرده است و با بر طرف شدن بعضی از مشکلات آن رفته رفته به کار بران آن افزوده می‌شود. جدول زیر روند روبه رشد کاربران VOIPرا بر اساس میلیون از سال ۱۹۹۹تا ۲۰۰۷ را نمایش می‌دهد.



نمودار۱. ۳ روند روبه رشد کاربران VOIP

[1] Pc-to-Pc
[2] Phone-to-Phone

نکته‌ای که باید در مورد سرویس VoIP به آن اشاره کرد این است که ارائه‌ی سرویس صوتی از طریق شبکه اینترنت نسبت به تلفن عادی، از کیفیت پایین‌تری برخوردار است؛ اما با توجه به هزینه‌ی بسیار کمتر VoIPنسبت به ارتباط تلفنی عادی و ارائه‌ی سرویس‌های متنوع تصویری و صوتی و متنی، که به سرویس VoIP اضافه شده است (VoIP به همراه سرویس‌های صوتی و تصویری و متنی سرویس تلفن اینترنتی[1] را به وجود می‌آورد)، میزان استفاده از این سرویس را به شدت در میان کاربران افزایش داده است و بازار جدیدی را در ارتباطات تلفنی ایجاد کرده است. میزان برقراری ارتباط در دنیا در سال ۲۰۰۶ بر اساس دقیقه در نمودار زیر نمایش داده شده است:

نمودار ۲. ۳ برقراری ارتباط در دنیا

۳. ۳. VOIP چگونه کار می‌کند؟

صوت یا صدای انسان سیگنالی آنالوگ است. بنابراین در مبدا، با استفاده از یک مبدل سیگنال آنالوگ به دیجیتال، تبدیل به یک سیگنال دیجیتال می‌شود. این کار به دلیل این که سیگنال آنالوگ در فواصل طولانی تحت تأثیر نویز و سیگنال‌های مزاحم، خواهد بود، انجام می‌پذیرد. از طرفی با توجه به این که صوت می‌بایست جهت انتقال از

[1] IP Telephony

طریق شبکه IP به بسته‌های دیتا تبدیل شود، دیجیتال شدن سیگنال صوت باید انجام‌پذیرد در انتهای انتقال نیز عمل عکس انجام خواهدپذیرفت. سیگنال دیجیتال که از طریق شبکه IP انتقال یافته، در مقصد و توسط یک تبدیل کننده از حالت یک سیگنال دیجیتال به آنالوگ تبدیل خواهد شد.

سیگنال دیجیتال بسیار ساده تر قابل کنترل است. فشرده سازی، مسیر یابی، تبدیل آن به فرمتی مناسب و مقاومت در برابر نویزاز مواردی است که کنترل آنها در حالت دیجیتال ساده تر انجام می‌پذیرد.

شبکه‌های مبتنی برIP، تولید کننده‌ی بسته‌های IP شامل یک سرآیند[1] (به منظور کنترل ارتباط) جهت انتقال هستند. VOIP از این سرآیند جهت انتقال از میان شبکه و رسیدن به مقصد استفاده می‌کند. شکل زیرنمایی از ارسال اطلاعات آنالوگ به سمت یک مقصد طبق توضیح بالا می‌باشد:

صوت(مبدأ) >ADC > اینترنت (شبکه IP) > DAC > صوت(مقصد)

شکل۱. ۳ انتقال صوت در VOIP

۴. ۳. مراحل برقراری ارتباط درVOIP

برقراری ارتباط در VOIP به دو شکل صورت می‌گیرد:

الف. برقراری ارتباط VOIP در سه مرحله:

گام اول: سیگنال‌های صوت آنالوگ با استفاده از یک مبدل آنالوگ به دیجیتال[2] دیجیتال می‌شوند. سیگنال‌های صوتی دیجیتال شده در مقابل نویز ایمن تر هستند راحت تر می‌توانند کنترل شوند و اگر بخواهیم به شکل دیگری تبدیل شوند.

---

[1] Header
[2] ADC

گام دوم: داده‌های دیجیتال به بسته‌هایی تقسیم می‌شوند. مکانیزم‌های پشتیبانی بلادرنگ و تحویل به موقع بسته‌ها باید انجام شود. پروتکل‌های سیگنالینگ[1] برای ایجاد لینک‌های ارتباطی بین تلفن‌ها مورد نیاز است.

گام سوم: بسته‌ها دریافت می‌شوند و داده‌های دیجیتال بازسازی می‌شوند. داده‌های دیجیتال ابتدا از حالت فشرده خارج شده سپس توسط یک مبدل دیجیتال به آنالوگ و به سیگنال صوتی تبدیل می‌شوند.

ب. نوع دیگری از دسته بندی

۱. استفاده از مبدل آنالوگ به دیجیتال (CODEC):

CODEC واژه‌ی رایجی است که معمولاً برای توصیف بعضی فرمهای سیستم فشرده‌سازی و نا فشرده‌سازی استفاده می‌شود. CODEC تلفیق دو واژه Code و Decode تشکیل شده است و در حالت رایج تر یک CODEC سیگنال‌های آنالوگ را به دیجیتال تبدیل می‌کند یا سیگنالهای دیجیتال را به فرم آنالوگ برمی گرداند. استانداردهای مختلف از تفاوت در پهنای باند مورد نیاز تکنیکهای فشرده‌سازی و کیفیت صوت ناشی شده است.

۲. فشرده سازی[2] بیت‌های سیگنال دیجیتال:

این عمل از مزایای استفاده از VOIP در جهت استفاده‌ی بهینه از پهنای باند است. پس از تبدیل شدن سیگنال آنالوگ به دیجیتال و آماده شدن سیگنال دیجیتال برای انتقال، فشرده‌سازی بیت‌های سیگنال انجام می‌پذیرد. الگوریتم فشرده‌سازی برای تبدیل داده دیجیتال به یک فرمت مناسب تر برای انتقال استفاده، می‌شود. الگوریتم‌های فشرده‌سازی مختلفی وجود دارند که کیفیت‌های متفاوتی از نظر زمان تاخیر و پهنای باند مورد نیاز ارائه می‌دهند. استانداردهای فشرده‌سازی با استفاده از استانداردهای مؤسسه ITU-T انجام می‌پذیرد. به عنوان مثال: یک کانال تلفنی معمولی، از ۶۴ کیلو بیت پهنای باند استفاده می‌کند. ولی استانداردهای مختلف می‌توانند این میزان پهنای

---

[1] Signaling
[2] Phone-to-Phone

باند را کاهش دهند که البته این کاهش، بر کیفیت صوت تأثیر منفی خواهد گذاشت. و یا استاندارد G.711، 64 K b و استاندارد G.729، 8 K b و استاندارد G.723 از 5. 3Kb تا 6. 5Kb پهنای باند استفاده می‌کنند.

الگوریتم فشرده‌سازی می‌تواند مزیتهای دیگری مثل توانایی بازیابی بسته‌های گم شده از روی بسته‌های دیگر را داشته باشد.

۳. واردکردن بسته صوتی در بسته دیتا با استفاده از یک پروتکل بلادرنگ (RTP):

پس از انجام عمل فشرده‌سازی و تبدیل سیگنال به حالت دیجیتال و تبدیل آن به بسته‌های دیتا (که به صورت بسته‌ای می‌باشد)، می‌بایست، عمل درج‌کردن این دیتا در بسته TCP / IP انجام گیرد. این عمل با استفاده از پروتکل RTP[1] انجام می‌پذیرد (این پروتکل در فصول بعدی توضیح داده خواهد شد). لازم به ذکر است VOIP به جای استفاده از TCP از UDP استفاده می‌کند.

و به طور کلی می‌توان گفت پروتکل RTP، کنترل دریافت بسته‌های حاوی صوت و صحت توالی آن را انجام می‌دهد.

۴. استفاده از یک پروتکل سیگنالینگ (H.323 ، SIP ، MGCP):

چطور جلسات مدیا به وجود آمده و چطور تمام می‌شود؟ چطور یک بخش بخش دیگر را برای برقراری یک تماس تعیین می‌کند؟ پاسخ این سوالها سیگنالینگ است.

در شبکه‌های تلفنی قدیمی پروتکل‌های سیگنالینگ خاصی وجود دارند که قبل و در طول یک تماس برای برقراری تماس ادامه یافتن آن و اتمام آن فراخوانی می‌شوند. در VOIPنیز پروتکل‌های سیگنالینگ برای چنین اهدافی لازم هستند.

دو استاندارد برجسته در VOIP وجود دارد که استانداردهای H.323 و SIP هستند. این پروتکل‌های سیگنالینگ رویه‌های تماس و روشهای قابلیت تبادل و پارامترهای جلسه مثل کدک را تعریف می‌کنند. این پروتکل‌ها زیر بنای پشتیبانی که برای عملیات در سیستمهای IP تلفنی لازم است را در بر دارند. این پروتکل‌ها در ادامه توضیح داده خواهند شد.

۵. دریافت بسته در مقصد:

---

[1] Compress

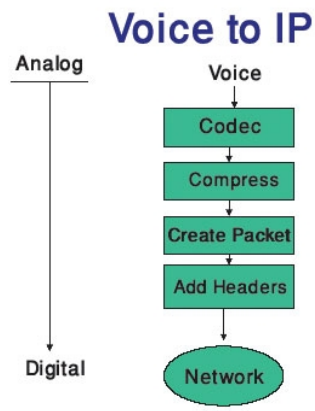
دریافت بسته در مقصد و استخراج صوت از بسته‌ی دیتا و تبدیل سیگنال دیجیتال به آنالوگ و ارسال آن به کارت صدا یا دستگاه تلفن.

۶. کنترل کیفیت سرویس QOS[1]

QOS اطمینانی است که معماری شبکه، برای تحویل بسته‌ها فراهم می‌کند. QOS می‌تواند توسط مجموعه‌ای از پارامترها تعریف شود که شامل نرخ داده‌ها تاخیر نرخ اشکال بیتی و ... باشد. برای کاربردهای IP تلفنی و بلادرنگ که تاخیرهای زیاد در انتقال بسته‌ها غیر قابل قبول است بسیار مهم می‌باشد.

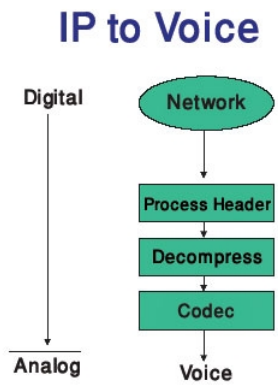
پروتکل دیگری که VOIP از آن استفاده می‌کند RSVP[2] است. این پروتکل وظیفه‌ی مدیریت کیفیت سرویس (QOS) را بر عهده دارد. RSVP پروتکل سیگنالینگی است که جهت اجتناب از تأخیر و تأمین کیفیت، از منابع شبکه، استفاده کرده و آنها را برای انتقال صوت رزرو می‌کند. مهمترین منبع شبکه که توسط این پروتکل مدیریت می‌شود، پهنای باند و ایجاد Dedicated Bandwidth است.

مراحل بالا در شکل‌های ۱ و ۲ در زیر رسم شده‌اند:



شکل۲. ۳

[1] Quality Of Service
[2] Resource Reservation protocol



شکل ۳. ۳

۵. ۳. برقراری یک مکالمه در VOIPبا استفاده از یک PBX[1]

فرض کنید که شرکت شما دستگاه مورد نظر به منطور استفاده از سرویس VoIP را خریداری و نصب کرده باشد. در شرکت مربوطه، صدها تلفن و یک PBX نیز نصب شده است. PBX سوئیچی است که از آن به منظور ارتباط مجموعه‌ای از تلفن‌ها به یکدیگر و به یک یا چندین خط خارج از شرکت استفاده می‌گردد. در اینجا PBX به صورت یک gateway است.

از gateway به منظور ارتباط دستگاه‌های موجود در دو شبکه متفاوت استفاده می‌گردد. PBX یک Gateway است. (چون سیگنال‌های استاندارد circuit-switching هر یک از تلفن‌ها را به داده‌های دیجیتال به منظور ارسال از طریق یک شبکه مبتنی بر IP و Packet Switching تبدیل می‌نماید). روش برقراری یک مکالمه از طریق یک شبکه Packet-Switching و با استفاده از VoIP به صورت زیر است:

۱. دریافت کننده را فعال تا از طریق آن یک سیگنال برای PBX ارسال گردد.

۲. PBX سیگنال را دریافت و یک بوق آزاد را برای فرستنده ارسال می‌دارد.

۳. فرستنده، اقدام به شماره گیری تلفن مخاطب مورد نظر می‌کند. شماره‌ی وارد شده در ادامه توسط PBX به صورت موقت ذخیره می‌گردد.

[1] Private Branch Exchange

۴. پس از مشخص نمودن شماره توسط فرستنده، PBX بمنظور اطمینان از صحت فرمت،آن را بررسی خواهد کرد.
۵. PBX در رابطه با نحوه‌ی تطبیق شماره دریافتی با شخص مورد نظر، اقدامات لازم را انجام خواهد داد. درفرآیند تطبیق، شماره‌ی مورد نظر به آدرس IP دستگاه دیگر که «میزبان IP» نامیده می‌گردد، ملحق می‌گردد. «میزبان IP»، سیستمی است که قصد برقراری ارتباط با آن وجود دارد.
۶. یک جلسه بین PBX اداره‌ی تماس گیرنده و «میزبان IP» برقرار می‌گردد. هر سیستم می‌بایست از پروتکل‌های مشابه بمنظور برقراری ارتباط استفاده نماید. سیستم ها، دو کانال برای هر جهت پیاده‌سازی خواهند کرد.
۷. مکالمه به مدت زمان مورد نظر انجام می‌گیرد. در زمان برقراری مکالمه، PBX شرکت شما و میزبان IP مخاطب، بسته‌های اطلاعاتی را ارسال و یا دریافت می‌دارند.
۸. مکالمه به اتمام رسیده و دریافت کننده غیرفعال می‌گردد.
۹. پس از قطع ارتباط، مدار(ارتباط) موجود بین تلفن تماس گیرنده و PBX آزاد می‌گردد.
۱۰. PBX سیگنالی را برای میزبان IP ارسال و خاتمه مکالمه را اعلام می‌نماید.
۱۱. پس از اتمام جلسه، دستگاه PBX شماره‌ی تلفن تطبیق داده شده به «میزبان IP» را از حافظه خود پاک می‌کند.
به منظور برقراری ارتباط از طریق تلفن با دستگاه‌هایی مانند: کامپیوتر در طول یک شبکه، می‌بایست از یک پروتکل مشترک استفاده گردد

۶. ۳. تجهیزات لازم برای برقراری ارتباط VOIP

۱. ۶. ۳. ATA (gateway) یا ATAdaptor

ساده‌ترین روش برقراری ارتباط VoIP با استفاده از ATAها[1] که gateway هم

[1] Analog Telephone Adaptor

نامیده می‌شوند، می‌باشد. این ابزارها این امکان را به شما می‌دهند که از تلفن‌های آنالوگ استاندارد فعلی تان استفاده کنید(اگر هنوز از تلفن‌های آنالوگ استفاده می‌کنید). به آسانی می‌توانید handset استاندارد خود را به ATA متصل کنید، سپس ATA را به کامپیوتر خود وصل کنید. با این کار قادر به برقراری ارتباط VoIP خواهید بود. ATA سیگنال آنالوگ را از تلفن استاندارد شما می‌گیرد و آن را به سیگنال دیجیتال آماده برای انتقال در بستر اینترنت تبدیل می‌کند. همراه برخی ATAها یک نرم‌افزار وجود دارد که روی کامپیوتر بارگذاری می‌شود و شما را قادر می‌سازد که آن را برای VoIP با دقت پیکربندی کنید.

شکل ۴. ۳ نحوه‌ی قرار گیری ATA

۲. ۶. ۳. تلفن‌های‌ای پی[1]

این تلفن‌های دستی کاملاً شبیه تلفن‌های دستی[2] استاندارد معمولی است. دارای یک کانکتور RJ 45 Ethernet به جای کانکتورهای استاندارد RJ 11 هستند. این تلفن‌ها تمام نرم‌افزارها و سخت‌افزارهای لازم برای برقراری ارتباطات VoIP را به صورت built-in دارند. مستقیماً به روتر شما وصل می‌شوند و یک ورودی سریع و مقرون به صرفه به دنیای VoIP فراهم می‌کنند.

[1] IP Phones
[2] Handset

شکل ۵. ۳ نمونه‌ای از Ip phone

۳. ۶. ۳. برنامه‌های نرم‌افزاری

این روش آسان‌ترین روش استفاده از تکنولوژی VoIP است. شرکت‌های زیادی هستند که نرم‌افزارهای مقرون به صرفه‌ای ارائه می‌دهند که می‌توانید برای این نوع VoIP از آن‌ها استفاده کنید. معمولاً تنها مبلغی که باید پرداخت کنید فقط هزینه ماهانه تامین کننده اینترنت است. تمام آن چه که نیاز دارید: یک میکروفون، بلندگو، یک کارت صدای مناسب و یک ارتباط اینترنت با سرعت مناسب؛ شرکت‌های تلفنی بزرگ امروزه با استفاده از VoIP هزاران تماس تلفنی راه دور را از طریق یک circuit Switch به درون یک IP gateway مسیردهی می‌کنند. این داده‌ها در طرف دیگر توسط یک gateway دریافت شده و سپس با یک circuit switch محلی دیگر مسیردهی می‌شود. هر روزه شرکت‌های بیش تری سیستم‌های تلفنی VoIP را نصب می‌کنند و تکنولوژی VoIP در حال رشد است.

۷. ۳. پروتکل‌های ارسال اطلاعات روی اینترنت

برای ارسال اطلاعات روی اینترنت معمولا از دو پروتکل TCP وUDP استفاده می‌کنند

۱. ۷. ۳. User Datagram Protocol(UDP)

یک پروتکل انتقال بدون اتصال است. ارسال بهتر و قابلیت اعتماد را ضمانت نمی کند. هیچ اتصالی را فراهم نمی کند فقط تحویل سریعتری را با سرآیندهای کمتر نسبت به TCP فراهم می‌کند.

۲. ۷. ۳. پروتکل کنترل انتقال[1] (TCP)

یک پروتکل انتقال اتصال گرا است. یک اتصال را در طول جلسه برقرار می‌کند و بسته‌های گم شده را دوباره می‌فرستد. TCPتحویل بسته‌ها را ضمانت می‌کند.
برای انتقال صوت در VOIP از پروتکل UDP به جای TCP استفاده می‌شود. در یک گفتگو گم شدن یک یا دو بسته از صوت در حقیقت خیلی مهم نیست چون معمولاً از بسته‌های خیلی کوچک 40ms تا ۱۰ ms استفاده می‌شود. از طرف دیگر صوت به شدت حساس به تاخیر است. متاسفانه برقراری ارتباط در TCP و بازگشت یک درخواست (ACK)تاخیراتی تولید می‌کند. حتی بدتر از این حالتی است که بسته‌ها گم می‌شوند. TCP بسته را دوباره ارسال می‌کند و تاخیر بیشتری تولید می‌کند. در انتقال صوت تحمل چند بسته گم شده بسیار بهتر از تاخیر است. اگر بسته‌ها گم شوند یا در زمانی که باید رمزگشایی شوند به مقصد نرسند این عمل باعث می‌شود که یک وقفه مانند لکنت در گفتار بوجود آید یا یک موج کوچک مثل اکو یا تجزیه داده روی دهد که باعث تضعیف اتصال تلفنی می‌شود.

۸. ۳. چه پیش می‌آید اگر بسته‌ها به ترتیب غلط به مقصد برسند؟

UDP مفهومی به نام ترتیب بسته ندارد. هر چند که بیشتر بسته‌ها به ترتیب می‌رسند چون در تمام بسته‌ها در یک جلسه معین یک مسسیر را از مبدا تا مقصد طی می‌کنند. البته ممکن است که بسته‌های مختلف مسیرهای متفاوتی طی کنندااما این حالت فقط وقتی اتفاق می‌افتدکه یا یک لینک(ارتباط) از بین برود یا تراکم رخ دهد و یا تغییراتی در توپولوژی شبکه ایجاد شود. احتمال وقوع چنین اتفاقاتی در طول مدت

[1] Transmission Control Protocol

یک جلسه بسیار کم است. به علاوه تکنیک‌های مدیریت QOS می‌توانند یک مجموعه مسیر را در سراسر شبکه برای یک جلسه معین برقرار کنندکه امکان رسیدن بسته‌ها به ترتیب غلط را کاهش می‌دهد. یکی دیگر از روش‌ها شماره‌گذاری بسته‌های ارسالی می‌باشد که اگر درمسیر بسته‌هایی گم شوند و به مقصد نرسند ویا به ترتیب نرسند تشخیص داده شوند.

۹. ۳. دسته‌بندی سرویس‌های VOIP

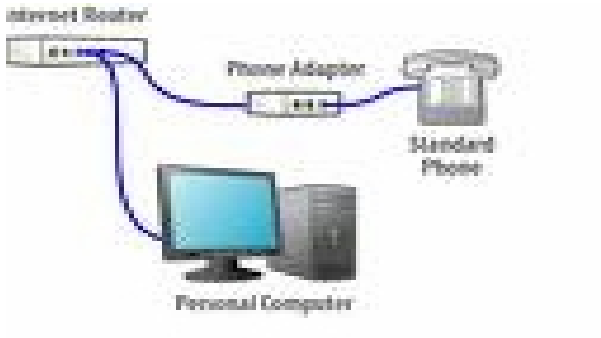
۱. ۹. ۳. تماس کامپیوتر با کامپیوتر

این روش توسط کاربرانی که امکان ارتباط با اینترنت را دارند، مناسب است. استفاده از امکانات رایانه شخصی به همراه سرویس‌های اینترنتی وب، پست الکترونیکی و مسنجر از مزایای این روش است. هزینه‌ی این روش بسیار اندک و کیفیت سرویس پایین است.

شکل ۶. ۳ ارتباط pc to pc

۲. ۹. ۳. تماس کامپیوتر با تلفن

این روش، حالت پیشرفته‌ی روش قبل است. در این روش هزینه‌ی برقراری ارتباط با یک سرویس‌دهنده می‌بایست در نظر گرفته شود.



شکل ۷. ۳ ارتباط pc to phone

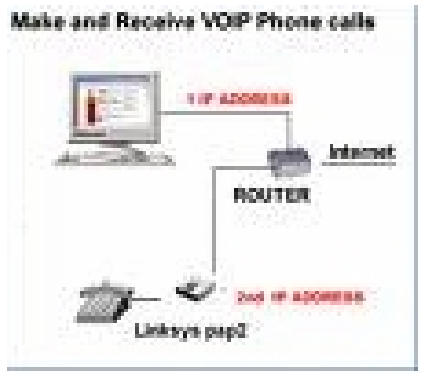
۳. ۹. ۳. تماس تلفن با تلفن

این روش (که IP Telephony نیز گفته می‌شود) جذاب‌ترین روش ارتباطی VOIP است. پایین‌ترین هزینه و بهترین کیفیت صوت با این روش محقق می‌شود. تنها هزینه‌ی این روش، هزینه‌ی برقراری ارتباط است.

شکل۸. ۳ ارتباط Phone to pc

۴. ۹. ۳. تماس تلفن با کامپیوتر

این روش، جهت ارتباط کاربران شبکه عمومی تلفن با کاربران اینترنتی است. هزینه‌ی ارتباط با یک سرویس‌دهنده، تنها هزینه‌ی این روش است.



شکل ۹. ۳ ارتباط phone to pc

۱۰. ۳. مقایسه‌ی VOIP وشبکه تلفن معمولی و مزایای آن

در شبکه‌ی تلفن معمولی شرکت‌های تلفن بیش از یکصد سال است که از تکنولوژی circuit switch استفاده می‌نمایند.

۱. ۱۰. ۳. Circuit switching

در این روش به محض برقراری ارتباط بین دو نفر در تمام مدت زمان مکالمه یک مدار اختصاصی برای آنها در نظر گرفته خواهد شد. بدین ترتیب برای دو نقطه مربوطه یک ارتباط دو سویه ایجاد می‌گردد،نحوه برقراری ارتباط در این سیستم به قرار زیر است:

۱. پس از برداشتن گوشی تلفن یک بوق شنیده می‌شود. بوق فوق به منزله برقراری ارتباط با شرکت تلفن (مرکز تلفن) است.

۲. با استفاده از سیستم تلفن، اقدام به شماره گیری می‌شود.

۳. ارتباط مورد نظر از طریق مجموعه‌ای از سوئیچ‌ها عبور داده شده تا به مخاطب مورد نظر برسد.

۴. یک ارتباط بین تلفن شما و مخاطب برقرار و یک مدار فعال می‌گردد. مکالمه با مخاطب مورد نظر در مدت زمان دلخواه انجام می‌گیرد و پس از قطع مکالمه، مدار فعال شده بین شما و مخاطب غیر فعال خواهد شد.

فرض کنید مدت زمان مکالمه شما ده دقیقه باشد، در طول مدت زمان فوق، مدار ایجاد شده بین دو تلفن به صورت پیوسته فعال خواهد بود. در سیستم‌های قدیمی مخابراتی، مکالمه تلفنی با نرخ انتقال اطلاعات ثابت ۶۴ کیلو بیت در ثانیه و یا ۱۰۲۴ بیت در ثانیه در هر جهت انجام می‌گرفت(مجموع نرخ انتقال اطلاعات ۱۲۸ کیلوبیت در ثانیه). با توجه به اینکه در هر کیلوبایت، هشت کیلوبیت وجود دارد، بنابراین در هر ثانیه ۱۶ کیلو بایت و یا در هر دقیقه ۹۶۰ کیلوبایت اطلاعات ارسال می‌گردد(زمانی که مدار فعال است). بنابراین در مدت زمان ده دقیقه ارتباط تلفنی، مجموع اطلاعات ارسال شده ۹۶۰۰ کیلو بایت (۹/۴ مگابایت) خواهد بود. در یک مکالمه تلفنی اکثر داده‌های ارسال شده بیهوده می‌باشند. زمانی که شما حرف می‌زنید، مخاطب صرفاً گوش می‌دهد. این بدان معنی است که در هر مقطع زمانی، ازنصف خط ارتباطی بیشتر استفاده نمی گردد. (سکوت موجود بر روی خط در مدت زمان برقراری ارتباط زیاد خواهد بود) در این حالت حجم اطلاعات ارسال شده، به ۴/۷ مگابایت تنزل پیدا خواهد کرد.

شبکه‌های مبتنی بر داده از روش Circuit switching استفاده نکرده و در مقابل، از روش Packet Switching استفاده می‌گردد.

۲. ۱۰. ۳. Packet Switching

در روش Packet Switching بر خلاف Circuit Switching که به صورت پیوسته ارتباط را فعال نگه می‌دارد، صرفاً در زمان ارسال اطلاعات (یک بخش کوچک داده که به آن بسته گفته می‌شود) ارتباط فعال خواهد شد. اطلاعات مربوط به فرستنده به مجموعه‌ای از بسته‌ها تقسیم می‌گردد. در هر یک از بسته‌های اطلاعاتی آدرس فرستنده و دریافت کننده اطلاعات قرار خواهد گرفت. دریافت کننده بسته‌های اطلاعاتی، اطلاعات را به یکدیگر ملحق تا اطلاعات اولیه بوجود آیند. روش فوق بسیار کارآ بوده و زمان فعال بودن ارتباط بین فرستنده و گیرنده را به حداقل مقدار خود می‌رساند. بدین ترتیب ترافیک موجود بر روی شبکه نیز کاهش خواهد یافت. کامپیوترهای فرستنده و گیرنده در زمان ارتباط با یکدیگر قادر به دریافت و یا ارسال اطلاعات برای سایر کامپیوترها نیز خواهند بود.

تکنولوژی VoIP از روش Packet Switching استفاده می‌کند. با استفاده از روش فوق امکان برقراری چندین مکالمه تلفنی فراهم می‌گردد. با استفاده از تلفن‌های معمولی، یک مکالمه ده دقیقه ای، ده دقیقه کامل از زمان انتقال با نرخ ۱۲۸ کیلوبیت در ثانیه را اشغال خواهد کرد. در روش VoIP، مکالمه ده دقیقه‌ای اشاره شده صرفاً ۵/۳ دقیقه زمان انتقال را با نرخ ۶۴ کیلوبیت در ثانیه اشغال خواهد کرد. در این حالت ۶۴ کیلوبیت در ثانیه برای مدت ۵/۳ دقیقه، و ۱۲۸ کیلوبیت در ثانیه برای زمان باقیمانده ۵ /۶دقیقه آزاد خواهد ماند.

در هنگام استفاده از تلفن معمولی، شما باید هزینه زمان استفاده از خط تلفن را بپردازید و زمان بیشتر و فاصله دورتر برابر با هزینه بیشتر است. بعلاوه شما در یک زمان نمی‌توانید با بیش از یک نفر صحبت کنید. همچنین هنگام برقراری تماس تلفنی، یک خط مخابراتی اختصاصاً استفاده می‌شود. در مقابل مکانیزم‌های VOIP شما را قادر می‌سازد تا با چند نفر همزمان صحبت کنید. در این فرآیند، فاصله دور تأثیری ندارد. بعلاوه در هنگام صحبت می‌توانید به مباد له‌ی دیتا (تصویر، گراف، ویدئوو ...) بپردازید.

۳. ۱۰. ۳. مقایسه شبکه‌های مخابراتی سنتی و آینده از زوایای مختلف

۱. استاندارد برقرارکننده ارتباط در شبکه‌های تلفنی VOIP پروتکل‌ها و بسته‌های داده هستند (مانند شبکه‌های IP) در حالی‌که در شبکه‌های مخابراتی سنتی واسطه‌های ارتباطی استاندارد (سوئیچ مدارهای درون شبکه) تعریف شده‌اند.

۲. با در نظر گرفتن ماهیت فن‌آوری VOIP و خصوصیات شبکه IP، متوجه خواهیم شد که این شبکه‌ها از پیچیدگی‌های داخلی بسیار کمتری نسبت به یک شبکه مخابراتی سنتی برخوردار هستند. همین امر سبب می‌شود که نگهداری این‌گونه شبکه‌ها بسیار آسان‌تر و کم هزینه‌تر باشد.

۳. در شبکه‌های مخابراتی، سرویس‌های مخابراتی درون شبکه مخابراتی (تجهیزات داخلی) مستقر می‌شوند، یعنی برای داشتن یک سرویس خاص باید مرکز مخابراتی پشتیبانی کننده‌ی آن سرویس باشد. به عبارت دیگر تجهیزات کاربر در این نوع سرویس‌ها چنان‌چه نیاز به دریافت خدمات خاصی باشد، تا زمانی‌که آن سرویس از

طرف مرکز مخابرات ارائه نشود، امکان استفاده از آن وجود ندارد. برعکس، در شبکه‌های مخابراتی بر پایه پروتکل IP، سیستم‌های نهایی در صورتی که یک سرویس جدید را پشتیبانی کنند، می‌توانند با یکدیگر (بدون نیاز به تغییر در شبکه مخابراتی) و با استفاده از آن سرویس ارتباط برقرار کنند.

۴. دیگر ویژگی سیستم‌های مخابراتی مبتنی بر IP پویایی و تحول سریع آنهاست. این سیستم‌ها به‌عنوان زیر مجموعه‌ای از علم کامپیوتر و فن‌آوری دیجیتال مشمول قانون مور می‌شوند. به بیان دیگر باید حدود هر ۱۸ ماه منتظر پیشرفتی در ابعاد دو برابر سابق در این‌گونه سیستم‌ها باشیم، در حالی‌که شبکه‌های مخابراتی قدیمی مدت زیادی است که همان شکل سابق را حفظ کرده‌اند و به‌ندرت دستخوش تغییرات می‌شوند. نگاهی گذرا بر تاریخ تحولات شبکه‌های مخابراتی نشان می‌دهد که پس از حدود هر ۳۰ سال شاهد تحولاتی محسوس در آنها هستیم که در مقایسه با تحولات شبکه‌های مخابراتی آینده در عمل ناچیز است.

۵. سرعت برقراری ارتباط VOIP که به وسیله سوئیچ بسته‌های داده کار می‌کنند به مراتب سریع‌تر از برقراری ارتباط در شبکه‌های سوئیچ‌کننده مدار (شبکه‌های مخابراتی کنونی) است.

۶. در سیستم‌های مخابراتی آینده (VOIP) ارائه‌کنندگان خدمات مخابراتی در عمل نقش واضح و تعریف شده‌ای ندارند، زیرا ارکان اصلی برقراری ارتباط دو طرف مکالمه‌کننده هستند. پیش‌بینی می‌شود که مراکز مخابراتی آینده از طریق ارائه راهکارهای متنوع به‌منظور بهبود برقراری ارتباط فعالیت کنند که این خدمات ممکن است بین دو مرکز مخابراتی، به‌طور کامل متفاوت باشد.

۴. ۱۰. ۳. به طور کلی برخی از مزایای VOIP را می‌توان به صورت زیر لیست نمود

۱. کاهش هزینه‌های تماس راه دور
۲. استفاده از امکانات اینترنتی و تجارت الکترونیکی
۳. یکپارچگی شبکه‌های دیتا و تلفن
۴. ارسال فکس

۵. اشتراک منابع و کاهش هزینه سرمایه گذاری
۶. استفاده از تلفن معمولی و یا رایانه شخصی
۷. کیفیت بسیار بالای صوت و ...

۱۱. ۳. مشکلات VOIP

برخی از مشکلات VOIP به قرار زیر می‌باشد:

- امنیت
- انعکاس صدا
- کیفیت صوت باید قابل مقایسه با شبکه عمومی تلفن باشد.
- از بین رفتن بسته‌های دیتا (Packet Lost)
- عدم پذیرش بسته (Dropt Packet)
- تاخیر (Delay)
- Jitter و سکوت

در ادامه برخی از مشکلات را به صور مختصر توضیح می‌دهیم:

Delay:

این مشکل زمانی رخ می‌دهد که تأخیر مبدأ تا مقصد از ۵۰ میلی ثانیه بیشتر شود. تاخیر ناشی از تکرار[1] و روی هم افتادن کلمات است.

روش‌ها و استانداردهای حذف تکرار، مثل G.168 سازمان ITU-T مشکل تکرار را مرتفع می‌نمایند. مشکل دیگر یعنی روی هم افتادن کلمات نیز زمانی بروز می‌نماید که تأخیر در یک جهت بیش از ۲۵۰ میلی ثانیه طول بکشد.

به طور کلی منابع تاخیر را می‌توان به شکل زیر دسته‌بندی کرد:

- تاخیر حس‌کردن حامل (Carrier sense delay): وقتی تعریف می‌شود که فرستنده در حال حس‌کردن حامل می‌باشد. مقدار آن توسط اندازه پنجره‌ی رقابت[2] تعیین می‌شود.

---

[1] Echo
[2] contention window

- تاخیر بازگشت (Backoff delay): وقتی اتفاق می‌افتد که حس کردن carrier موفقیت آمیز نباشد یا ارسال دیگری تشخیص داده شده و یا برخورد اتفاق افتاده با شد.
- تاخیر انتقال (Transmission delay): توسط عرض باند کانال، طول packet و طرح کدینگ اختیار شده تعیین می‌شود.
- تاخیر انتشار(Propagation delay): توسط فاصله بین نودهای فرستنده و گیرنده تعیین می شود.
- تاخیر پردازش (Processing delay): گیرنده باید قبل از ارسال packet به hop بعدی آن را پردازش کند. این تاخیر بطور عمده به توان محاسباتی نود و بازدهی الگوریتم پردازش داخل شبکه‌ای داده بستگی دارد.
- تاخیر صف‌بندی (Queuing delay): به بار ترافیکی بستگی دارد. در مواقع ترافیک سنگین این تاخیر فاکتور غالب است.

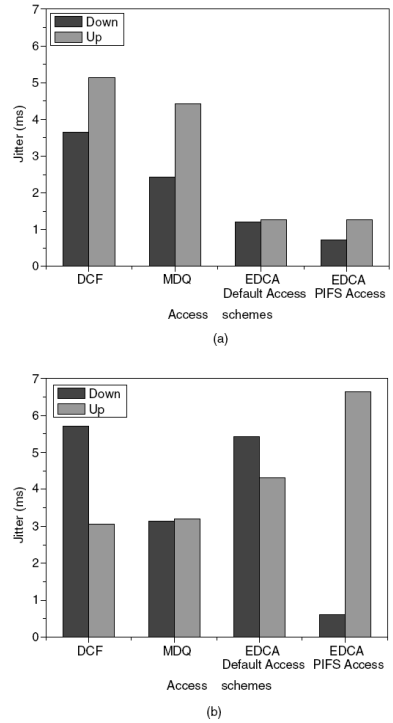
Jitter:

تفاوت در زمان‌های رسیدن بسته‌های صوت را «jitter» می‌گویند یا به عبارت دیگر تغییر در تاخیر را Jitter گویند. جهت رفع آن از بافر استفاده می‌شود تا با ذخیره‌سازی و ارسال بسته‌ها، توالی بسته‌ها رعایت شود. در بافر اگر بسته‌های صوتی بعدی دریافت نشوند همه‌ی بسته‌های صوتی‌ای را که دریافت کرده است را ارسال نمی‌کند و تاخیر بین بسته‌ها را افزایش می‌دهد که این کار بافر، خود باعث ایجاد تأخیر (Delay) بیشتر می‌شود.

بررسی جیتر در استاندارد IEEE 802.11

جیتر در شبکه‌های VoIP به همراه تاخیر دو پارامتر عمده در بررسی کیفیت شبکه هستند. برای بررسی جیتر در چهار نوع access scheme در شبکه بیسیم مبتنی بر IEEE 802.11، شامل DCF, MDQ, EDCA, EDCA PIFS شبیه سازیهایی انجام شد. در این شبیه سازیها ۱ تا ۱۰ VoIP Session بر روی ۵ رشته TCP اجرا شد.

در شکل (۳. ۱۰) کارآیی جیتر در این موارد مشاهده می‌شود. می‌توان تصور کرد که دو فاکتور عمده وجود دارد که جیتر را در شبکه IEEE 802.11 افزایش می‌دهد. این دو فاکتور عبارتند از contention/collision که در بقیه ایستگاهها باعث تاخیر اتفاقی در داخل صف‌ها می‌شود. در ابتدا زمانی که یک جلسه VoIP وجود دارد، EDCA scheme به صورت از قبل تعریف شده و دسترسی به صورت PIFS عملکرد بهتری از نظر جیتر نسبت به DCF schemeها نشان می‌دهد. این به دلیل داشتن پارامترهای دسترسی کانال کوچکتر است. در توصیف این رفتار می‌توان گفت، زمانی که یک جلسه VoIPبرقرار باشد، TCP می‌تواند از درصد پهنای باند بیشتری برای هر کانال استفاده کند. در این شرایط AC_VO در EDCA shemeها که پارامترهای دسترسی کوچکتری را استفاده می‌کند، می‌تواند رقابت در ایستگاههای TCP و AC_BE در QAP را کاهش دهد. با این روال جیتر کاهش خواهد یافت. از طرف دیگر در زمانی که ۱۰جلسه VoIPبرقرار باشد، نتیجه با آنچه که در حالت قبلی ذکر شد کاملا متفاوت می‌شود. در این شرایط CWmin[AC_VO] برای EDCA به اندازه کافی بزرگ نیست تا از collision جلوگیری کند. در این شرایط collisionهای بسیاری رخ می‌دهد که در نتیجه جیتر را بسیار بالا می‌برد. اگرچه برای مقدار جیتر برای downlink VoIP در حالت دسترسی EDCA PIFS همچنان کم می‌ماند. این به دلیل آن است که downlink AC_VO می‌تواند به طور کامل از contention با station TCPها و AC_BE در AP جلوگیری کند. میزان جیتر در تمامی دسترسی‌ها به جز برای EDCA PIFS زیاد می‌شود. این نیز به دلیل رندم بودن میزان تاخیر در صف‌ها است.



شکل ۱۰. ۳ Jitter performances of four access schemes: (a) 1 VoIP session; (b) 10 VoIP sessions.

از آنچه تاکنون انجام شده است می‌توان نتیجه گرفت که در صورتی که VoIP sessionهای کم وجود دارد، عملکرد EDCA نسبت به DCF/MDQ بهتر است. ولی این نتیجه در صورتی که تعداد جلسه‌ها زیاد باشد برعکس خواهد بود.

گم شدن بسته‌ها:

عامل اصلی گم شدن بسته‌ها ازدحام است با توجه به این که VOIP برای بالا بردن سرعت از UDP / IP استفاده می‌کند؛ لذا امکان تکرار بسته‌های دیتای از دست رفته وجود ندارد. اگر در شبکه‌ای میزان از دست رفتن بسته بیش از ۱۰ ٪ باشد آن شبکه غیر قابل اطمینان است. از روش‌های کنترل کیفیت سرویس (QOS) در حل این مشکل استفاده می‌شود. از آنجایی که UDP نمی‌تواند یک ساز و کار برای اطمینان از این که

بسته‌های اطلاعاتی به‌صورت دایمی و منظم تحویل داده می‌شوند یا ضمانت‌های کیفیت سرویس را(که به عنوان QOS شناخته شده‌اند) تهیه کند، اجرای VOIP با مسایل نهفتگی و ناپایداری سیگنال مواجه‌است. این یک واقعیت است به‌ویژه هنگامی که تاخیر انتشار مدار ماهواره‌ای، ناشی از سفر چرخشی طولانی، حادث می‌شود(۴۰۰ میلی‌ثانیه تا ۶۰۰ میلی‌ثانیه برای ماهواره‌های ثابت). برای رفع این مشکل گره‌های دریافت‌کننده باید بسته‌های IP را که ممکن است خارج از دستور، تاخیردار یا گم شده باشند(با توجه به این که جریان صوت یک سازگاری زمان مناسب را می‌طلبد)، بازسازی کنند.

انعکاس صدا:

علل مشترک بازگشت یا انعکاس صدا،عدم تطبیق امپدانس در مدار آنالوگ می‌باشد.

قطعی برق:

تلفن‌های معمولی به‌طور مستقیم به خطوط تلفن شرکت‌های تلفن متصل هستند، در هنگام قطع برق به‌وسیلهٔ تولیدکنندگان، بک‌آپ یا باتری‌های قرار داده شده است که ارتباط برقرار باقی بماندولی یکی از موضوعات مطرح ودر حال بررسی در VOIP قطعی برق می‌باشد.

مشکل در ارسال Fax:

پشتیبانی از ارسال دورنویس روی VoIP هنوز محدود است. وسایل رمزگذار صدای موجود، برای مخابره‌ی دورنویس طراحی نشده‌اند. تلاشی برای حل این مشکل به‌وسیله‌ی تعریف یک راه حل مبتنی بر IP متناوب برای تحویل دورنویس روی IP، به نام پروتکل T. 38 در حال انجام است. راه حل ممکن دیگر برای چیره‌شدن بر این مشکل، برخورد با سامانه دورنویس به‌عنوان یک سامانه سوییچینگ (مسیریابی) پیام است(که به مخابره‌ی داده در زمان آنی نیاز ندارد).

تماس‌های اورژانسی:

طبیعت IP به گونه‌ای است که مکان‌یابی جغرافیایی را برای کاربران شبکه مشکل می‌سازد. در حوادثی که تماس گیرنده قادر به دادن آدرس نیست، سرویس‌های

اضطراری ممکن است قادر به مکان‌یابی آن‌ها به هیچ طریقی نباشند. برای همین یک حامل VoIP بزرگ، نیاز به ثبت آدرس فیزیکی جایی که خط VoIP استفاده خواهد شد را دارد. هنگامی که شما با شماره‌ی اورژانس کشورتان تماس می‌گیرید، آن‌ها آن را برای سامانه محلی منا سب، مسیریابی خواهند کرد. در سیستم VOIP باید اطلاعات به طور کامل ثبت شود و در دسترس مراکز قانونی قرار گیرد.

سکوت:

سکوت فاصله خالی میان صحبت است که ۵۰ ٪ تا ۶۰ ٪ کل زمان تماس را تشکیل می‌دهد. روش Call Client Suppression و روش Comfort Noise جهت رفع آن به کار می‌روند.

البته این نکته را نباید از نظر دور داشت که روز به روز از مشکلات VOIP کاسته می‌شود وبه کیفیت آن افزوده می‌گردد. همین طور که در ادامه توضیح خواهیم داد در ابتدا پروتکل H.323 تحت استاندارد ITU ارائه شد. یک پروتکل پیشرفته و پیچیده است. پروتکل فوق مشخصات لازم برای ویدئوکنفرانس‌های محاوره‌ای و اشتراک داده و نرم‌افزارهای صوتی نظیر IP تلفنی را تعریف می‌کند.

۱۲. ۳. تلفن‌های سیار وتجهیزات دستی

شرکت‌های تلفن و مصرف‌کنندگان، میلیاردها دلار در تجهیزات تلفن سیار سرمایه‌گذاری کرده‌اند. در کشورهای توسعه یافته، خطوط موبایل تقریباً به نفوذ کامل در بازار دست یافته‌اند، و بسیاری از مردم خطوط زمینی‌شان(خطوط ارتباطی با کابل) را رها و منحصراً از خطوط سیار استفاده می‌کنند. در چنین موقعیتی، تقاضای فراگیر برای استفاده از VoIP در میان مصرف‌کنندگان کاملاً محرز نیست که مجموعه شرکت‌های شبکه‌های بی‌سیم به طور کامل همه‌ی مناطق جغرافیایی را پوشش دهند که یک شبکه‌ی سلولی داشته باشیم(ایجاد خطوط VoIP سیار به این وسیله امکان‌پذیر می‌شود)یا به عبارت دیگر می‌توان گفت با داشتن اینترنت بی سیم با پهنای باند زیاد و سر عت بالای دسترسی به VOIP سیار بسیار تسهیل می‌گردد. به‌هر حال، مجموعهٔ تلفن‌هایی که تحویل ارتباط بدون انقطاع را بین یک شبکه‌ی سلولار و یک شبکه‌ی

WiFi را ممکن می‌سازند، برای کمک به رواج بیشتر VoIP مورد انتظار هستند.
تلفن‌هایی شبیه به NEC N900iL، و مدل‌های بعد از آن(Nokia E60, 61)، اولین مجموعه تلفن‌های دو نمایه‌ی قادر به تحویل VoIP سیار بوده‌اند. با بیشتر و بیشتر شدن خطوط سیار و تجهیزات دستی استفاده‌کنندگانVoIP، اسامی مستعار MoIP و MVoip(موبایل VoIP) به این کاربردهای سیار انتساب یافته‌اند.
وسایل دستی نوع دیگری از وسایل هستند که به وسیله آن شما می‌توانید از خدمات VoIP استفاده کنید. از این‌رو بیشتر این وسایل با توجه به استفاده از انواع GSM/GPRS وسایل ارتباط، محدود شده‌اند، تقریباً همه‌ی وسایل دستی از WiFiهای برخی گونه‌ها استفاده می‌کنند.
وسایل دستی دیگر، وسایل نوع بارکد استحکام یافته هستند که در انبارها و محیط‌های خرده‌فروشی استفاده می‌شوند. این نوع وسایل در چهار چوب VoIP که به دنیای خارجی متصل نمی‌شوند و منحصراً برای ارتباطات یک کارمند به کارمند دیگر استفاده می‌شوند، تکیه می‌کنند و به عبارت دیگر می‌توان گفت این نوع ارتباط یک نوع ارتباط داخلی می‌باشد. در زیر چند مدل از تلفن‌های VOIP را می‌بینید:

VoIP Phone 4625Avaya

1140E VoIP Phone

1535 VoIP Video Phone

VOIP phoneCisco

شکل ۱۱. ۳ چند مدل از تلفن‌های VOIP

۱۳. ۳. امنیت در VOIP

۱. ۱۳. ۳. چالش‌های امنیتی VoIP

تصور کنید یک مهاجم به طور پنهانی به شبکه VoIP شما راه یافته و به تمامی مکالمات مورد نظر خود گوش داده و سپس اطلاعات حساس، اسرار شرکت یا حتی جزییات مورد نیاز مدیر ارشد اجرایی ما را استخراج نماید. با توجه به این که فن آوری VoIP در ارتباط با اتصال اینترنت است و از آن استفاده می‌نماید، مشکلات و مسائل امنیتی در ارتباط با کامپیوتر متصل شده به اینترنت می‌تواند سرویس فوق را نیز تحت تاثیر قرار دهد. فن آوری VoIP هنوز جوان است و بحث‌های مختلفی در خصوص ظرفیت ریسک‌پذیری آن وجود دارد. مهاجمان ممکن است قادر به انجام فعالیت‌هایی نظیر قطع مکالمه تلفنی، استراق سمع، برنامه ریزی و هدایت حملات مبتنی بر مهندسی اجتماعی با بررسی کالرای دی[1] و در نهایت از کار انداختن این سرویس باشند. فعالیت‌هایی که مستلزم استفاده از حجم بالایی از منابع شبکه است، نظیر دریافت فایل‌های حجیم، بازی‌های آن لاین، استفاده از محتویات چندرسانه‌ای (صوت و تصویر)، می‌تواند سرویس VoIP را تحت تاثیر قرار دهد.

در زمان استفاده از فن آوری VoIP ممکن با مسائل دیگری که در ارتباط با روتینگ تلفن بر روی اتصال پهن باند اینترنت است نیز برخورد نماییم. برخلاف خطوط تلفن سنتی، که امکان استفاده از آنان حتی در صورت قطع برق وجود دارد، سرویس VoIP در چنین مواردی غیرقابل استفاده می‌گردد و ممکن است مسایل خاصی را برای سیستم‌های امنیتی منازل و یا دستیابی به شماره تلفن‌های اضطراری به دنبال داشته باشد.

۲. ۱۳. ۳. نحوه‌ی حفاظت

در زمان استفاده از این سرویس لازم است به موارد زیر توجه گردد:

۱. به هنگام نگه داشتن نرم‌افزارها(update): در صورتی که تولید کنندگان نرم‌افزار

[1] Caller ID

برای سیستم عامل دستگاه مورد نظر نسخه‌های بهنگام شده‌ای را ارایه داده اند، می‌بایست در اولین فرصت نسبت به نصب آنان اقدام گردد. نسخه‌های بهنگام شده ممکن است فرآیند به هنگام‌سازی را در سطح Firmware انجام دهند. با به هنگام‌سازی نرم‌افزارهای موجود، پیشگیری لازم در خصوص برخی حملات برنامه ریزی شده با هدف بهره گیری از نقاط آسیب‌پذیر انجام خواهد شد.

۲. استفاده و به هنگام‌سازی نرم‌افزارهای ضد[1] ویروس: برنامه‌های ضد ویروس قادر به تشخیص و حفاظت کامپیوتر شما در مقابل ویروس‌های شناخته شده می‌باشند. با توجه به این واقعیت که مهاجمان به صورت مستمر اقدام به نوشتن ویروس‌های جدید می‌نمایند، لازم است که این نوع نرم‌افزارها همواره به هنگام باشند.

۳. استفاده از گزینه‌ها و تنظیمات امنیتی: برخی از ارائه دهندگان سرویس VoIP، امکان رمزنگاری اطلاعات را نیز به عنوان یک سرویس دیگر در اختیار مشتریان خود قرار می‌دهند. در صورت وجود نگرانی در خصوص تعرض به حریم خصوصی خود، می‌توان از این ویژگی و سایر گزینه‌های موجود در این رابطه استفاده نمود.

۴. نصب و یا فعال نمودن یک دیوار آتش: دیوارهای آتش با بررسی بسته‌های اطلاعاتی می‌توانند یک سطح حفاظتی مناسب در خصوص فیلتر نمودن برخی کدهای مخرب جهت ورود به سیستم شما را انجام دهند. برخی از سیستم‌های عامل به همراه یک دیوار آتش ارائه می‌گردند. در چنین مواردی لازم است از فعال بودن آنان اطمینان حاصل نمود.

۵. بررسی تنظیمات امنیتی: هم کامپیوتر شما و هم تجهیزات و نرم‌افزارهای ارایه شده جهت استفاده از سرویس VoIP، امکانات و گزینه‌های متفاوتی را در اختیار شما قرار می‌دهند. فعال نمودن برخی گزینه‌ها ممکن است ضریب آسیب‌پذیری شما را در مقابل حملات افزایش دهد. بنابراین لازم است گزینه‌های غیرضروری را غیرفعال نمود. پیشنهاد می‌گردد تنظیمات امنیتی به دقت بررسی گردد و صرفاً گزینه‌هایی انتخاب شود که علاوه بر تامین اهداف عملیاتی، باعث افزایش ضریب آسیب‌پذیری شما نگردد.

---

[1] Anti

۳. ۱۳. ۳. تعیین هویت تماس گیرنده

تعیین هویت تماس گیرنده از سوی تهیه‌کنندگان VoIP به طور متفاوت پشتیبانی می‌شود، هر چند اکثریت تهیه‌کنندگان VoIP حالا تعیین هویت کامل تماس گیرنده(با نام، یا یادآوری تماس‌های گرفته شده) را پیشنهاد می‌کنند اما هنوز هنگام تماس یک شمارهٔ تلفن سنتی، از سوی برخی تهیه‌کنندگان VoIP، تعیین هویت تماس‌گیرنده پشتیبانی نمی‌شود. در حالات بسیار اندکی، تهیه‌کنندگان VoIP اجازه‌ی کلاهبرداری از اطلاعات تعیین هویت تماس گیرنده را به یک تماس‌گیرنده می‌دهند، این امر زمانی اتفاق می‌افتد که هر از چندگاهی آن‌ها از یک شماره‌ی متفاوت تماس می‌گیرند. تجهیزات VoIP و نرم‌افزارهای موجود در بازار، اغلب امکان تصحیح اطلاعات تعیین هویت تماس‌گیرنده را تسهیل می‌کنند. اگر چه این امر می‌تواند انعطاف بسیار زیاد تجاری ایجاد کند، اما راه را برای سو استفاده نیز باز می‌گذارد.

۱۴. ۳. اشخاص حقیقی و شرکت‌های استفاده‌کننده از ارتباطات راه دور

اگر چه محیط‌های دفتری کمی و حتی خانه‌های کمتری از یک زیرساخت VoIP ناب استفاده می‌کنند، تهیه‌کنندگان ارتباطات راه دور هر روز از علم تلفن IPبرای اتصال ایستگاه‌های سوییچینگ(راه‌گزینی سیگنال‌های صدای تبدیل یافته به بسته‌ها و برعکس(استفاده می‌کنند. نتیجه، ایجاد یک شبکه‌ی دیجیتال دیتای خلاصه شده‌ی مجزاست که تهیه‌کننده می‌تواند به‌راحتی برای اهداف چندگانه مورد استفاده قرار دهد و آن‌را ارتقا بخشد. مزیت استفاده از این تلفن، نیاز به فقط یک کلاس اتصال مدار(حوزه- مسیر) و استفاده‌ی بهتر از پهنای باند است. شرکت‌ها می‌توانند گیت‌وی‌های خودشان را برای حذف هزینه‌های بخش سوم که در برخی موقعیت‌ها ارزنده‌است، پیدا کنند.

VoIP به‌طور گسترده به‌وسیله‌ی حامل‌ها، مخصوصاً برای تماس‌های تلفنی بین‌المللی به‌خدمت گرفته شده‌است.

بسیاری از شرکت‌های ارتباط از راه دور چند رسانه‌ای IP(IMS)،به دنبال این هستندکه تکنولوژی‌های اینترنت را با دنیای موبایل یکی خواهد کنند(استفاده از یک زیرساخت

VoIP خالص). این تکنولوژی، آن‌ها را برای ارتقا بخشیدن به سامانه‌های موجودشان هنگام‌پذیرفتن تکنولوژی‌های اینترنت از قبیل ایمیل، وب، پیام فوری، حضور و کنفرانس‌های ویدیویی تواناتر خواهد ساخت.

۱۵. ۳. کنترل کیفیت QOS

QOS اطمینانی است که معماری شبکه برای تحویل بسته‌ها فراهم می‌کند. QOS می‌تواند توسط مجموعه‌ای از پارامترها تعریف شود که شامل نرخ داده‌ها تاخیر نرخ اشکال بیتی و ... باشد. برای کاربردهای IP تلفنی و بلا درنگ که تاخیرهای زیاد در انتقال بسته‌ها غیر قابل قبول است بسیار مهم است.

پس از انجام عمل فشرده‌سازی و تبدیل سیگنال به حالت دیجیتال و تبدیل آن به بسته‌های دیتا (که به صورت Packet می‌باشد) می‌بایست، عمل درج‌کردن این دیتا در بسته TCP / IP انجام گیرد. این عمل با استفاده از پروتکل RTP انجام می‌پذیرد. لازم به ذکر است VOIP بجای استفاده از TCP از UDP استفاده می‌کند.

پروتکل RTP، کنترل دریافت بسته‌های حاوی صوت و صحت توالی آن را انجام می‌دهد. پروتکل دیگری که VOIP از آن استفاده می‌کند RSVP[1] است. این پروتکل وظیفه مدیریت کیفیت سرویس را بر عهده دارد. RSVP پروتکل سیگنالینگی است که جهت اجتناب از تأخیر و تأمین کیفیت از منابع شبکه استفاده کرده و آنها را برای انتقال صوت رزرو می‌کند. مهمترین منبع شبکه که توسط این پروتکل مدیریت می‌شود، پهنای باند و ایجاد Dedicated Bandwidth است.

۱۶. ۳. مسایل قانونی در کشورهای مختلف

با افزایش محبوبیت VOIPدر میان کاربران، کاربران VOIP نسبت به کاربران PSTN در حال افزایش هستند و دولت‌ها نیز برای قانون مند بودن و تحت کنترل بودن این خدمات دست به تشویق انحصارگران تلفن تحت قیمومیت دولت زده است.

[1] Resource Reservation Protocol

در آمریکا کمیتهٔ ارتباطات فدرال هم اکنون از همهٔ اپراتورهای VoIP پشتیبانی نمی‌کند. FCC(سازمان آمریکایی مسئول منظم‌کردن ارتباطات) اخیراً به اپراتورهای VoIP برای حمایت از عاملیت استراق سمع CALEA نیاز دارد. پیمان ارتباطات از راه دور ۲۰۰۵ افزودن بیشتر مقررات تلفن سنتی، از قبیل قابلیت انتقال شماره‌ی محلی و حقوق لازمه‌ی سرویس جهانی را پیشنهاد می‌دهد. مسائل دیگر قانونی آینده شبیه به: شمولیت قوانین در مقابل استراق سمع، و بی‌طرفی شبکه هستند.

برخی از کشورهای آمریکای لاتین و وابسته به دریای کارائیب، برای خدمات تلفنی ایالت‌های خودشان، که محدودیت‌هایی روی استفاده از VoIP تحمیل شده‌است، بیمناک هستند، شامل پاناما، جایی که برای VoIPمالیات وضع شده‌است. در اتیوپی، جایی که حکومت تنها سرویس‌دهنده‌ی ارتباط از راه دور است، و پیشنهاد برای استفاده از خدمات VoIP یک گناه مجرمانه‌است. در برخی از کشورها، دیوارهای آتش را برای جلوگیری از تماس‌های بین‌المللی ایجاد شده با استفاده از VoIPرا نصب کرده‌اند.

معمولاً یک تمایز عمومی بین خدمات VoIP روی شبکه‌های مدیریت شده(از طریق اتصالات پهن‌باند) و خدمات VoIP روی شبکه‌های مدیریت نشده(الزاماً، اینترنت) وجود دارد.

خدمات VoIP که روی شبکه‌های مدیریت شده عمل می‌کنند اغلب یک جایگزین پایدار برای خدمات تلفن PSTN(با وجود مسائل قطع برق و فقدان اطلاعات جغرافیایی) محسوب می‌گردند. که البته اپراتورهایی که این خدمات را ارائه می‌دهند می‌توانند محدوده‌ی خودشان را به‌وسیله‌ی کنترل قیمت و یا جداسازی تعرفه‌ها از تعرفه‌های

تلفن‌های معمولی کنترل و مدیریت کنند.

خدمات VoIP که روی شبکه‌های مدیریت نشده عمل می‌کنند اغلب آنچنان از نظر کیفیت فقیر در نظر گرفته می‌شوند که یک جانشین قابل دوام برای خدمات PSTN نمی‌باشند. و به طور کلی ممکن است شبکه‌های مدیریت نشده بدون هیچ وظیفه‌ی مشخصی تهیه شده باشند، حتی اگر یک تهیه‌کننده‌ی قدرتمندی نیز داشته باشند.

در هند، استفاده از VoIP قانونی است، اما داشتن Gatewayهای VoIP در داخل هند غیر قانونی است. این به‌طور مشخص به این معناست که افرادی که PC دارند می‌توانند از آن برای ایجاد یک تماس VoIP روی هر شماره‌ای که بخواهند استفاده کنند، اما اگر طرف دوم یک تلفن معمولی است، دروازه‌ای که تماس VoIP را برای یک تماس تلفن معمولی تبدیل می‌کند نباید داخل هند باشد.

در امارات متحده عربی، استفاده از هر شکل VoIP، برای وسعتی که وب‌سایت‌های Skype و پروژه‌ی جیزمو کار نمی‌کنند، غیر قانونی است. Skype و پروژه‌ی جیزمو دو VOIP بسیار قدرتمند می‌باشند.

در جمهوری کره، فقط تهیه‌کنندگان ثبت شده توسط حکومت برای پیشنهاد خدمات VoIP مجاز هستند. بیشتر تهیه‌کنندگان VoIP در کره نرخ‌های یکسان پیشنهاد می‌کنند. خدمات VoIP کره‌ای‌ها به‌طور معمول در نرخ‌هایی شبیه به تماس‌های زمینی اندازه‌گیری و شارژ می‌شوند. تهیه‌کنندگان VoIP خارجی از قبیل Vonage، با موانع بسیار برای ثبت نام حکومتی روبرو می‌شوند. این مسئله در سال ۲۰۰۶، هنگامی که تهیه‌کنندگان سرویس اینترنتی خدمات اینترنت شخصی دارای قرارداد برای اعضای نیروهای ایالت‌های متحد کره، مقیم در پایانه‌های USFK، تهدید کردند که دسترسی به خدمات VoIP را که به‌وسیله‌ی اعضای USFK به‌عنوان یک راه اقتصادی برای تماس با خانواده‌هایشان در ایالت متحده استفاده می‌شد، مسدود می‌کنند، در زمینه‌هایی که تهیه‌کنندگان سرویس VoIP اعضای ثبت نشده بودند، به اوج رسید. یک مصالحه بین USFK و مقامات رسمی ارتباطات از راه دور کره در ژانویه‌ی ۲۰۰۷ حاصل شد، جایی که اعضای سرویس USFK قبل از یکم ژانویه‌ی ۲۰۰۷ به کره آمده بودند و امکان تصدیق خدمات ISP بر پایه‌ی استفاده‌ی اشتراک VoIP مبتنی بر

آمریکا(مرکز آن در کشور آمریکا)، ادامه یابد، اما برای ورودی‌هایی که بعد از تاریخ مورد توافق به کره می‌آمدند باید از یک تهیه‌کننده‌ی VoIP مبتنی بر کره‌ای استفاده می‌کردند(مرکز آن در کشور کره)، که به‌وسیله‌ی قرارداد، قیمتی شبیه به نرخ‌های یکدست ارایه شده به‌وسیله‌ی تهیه‌کنندگان VoIP آمریکا، پیشنهاد شد.

۱. ۱۶. ۳. تلفن IP در ژاپن

در ژاپن تلفن IP(IP電話, IP Denwa?) به‌عنوان یک سرویس کاربردی تکنولوژی VoIP، به‌عنوان تمام یا یک بخش از خط تلفن در نظر گرفته می‌شود. از سال ۲۰۰۳(شروع تلفن IP)، سرویس تلفن IP به اعضایی که آمادگی داشتند، تلفن واگذار شد. صدا تنها سرویس تلفن IP نیست، بلکه سرویس تلفن ویدیو نیز وجود دارد. بر اساس قانون تجارت ارتباط از راه دور، تقسیم‌بندی سرویس برای تلفن IP، بر سرویس تهیه شده از طریق اینترنت نیز که به هیچ عضو تلفنی واگذار نشده، دلالت می‌کند. تلفن IP به‌طور پایه‌ای، به‌وسیلهٔ وزارت امور داخلی و ارتباطات(MIC)، به‌عنوان یک سرویس ارتباط از راه دور در نظر گرفته شده‌است. اپراتورها مجبور به افشای اطلاعات ضروری روی کیفیت، و دیگر مسائل آن و اولویت برای عقد قرارداد با مشتریان هستند، و برای پاسخ به شکایات آن‌ها از صمیم قلب، اصرار دارند.

بسیاری از تهیه‌کنندگان خدمت اینترنت(ISPها)، خدمات تلفن IP را ارائه می‌دهند. از این رو، تهیه‌کننده، که سرویس تلفن IP را ارایه می‌دهد، «ITSP(تهیه‌کننده‌ی سرویس تلفن اینترنت)» نامیده می‌شود. اخیراً، رقابت بین ITSPها، به‌وسیله‌ی انتخاب گزینه‌ای یا مجموعه‌ی فروش، همراه با خدمات ADSL یا FTTH فعال شده‌است.

سامانه‌ی تعرفه‌ی معمولی استفاده شده برای تلفن IP ژاپنی‌ها، به‌شرح عناوین زیر گرایش دارد:

۱. تماس بین مشترکین تلفن IP، محدود شده به همان گروه، اغلب بدون هزینه‌است.

۲. تماس از مشترکین تلفن IP به خطوط ثابت یا PHS، بیشتر نرخ ثابت و یکسان روی کل کشور دارد. بین ITSP، هزینه‌ی تماس داخلی بیشتر در حد VoIP نگهداری می‌شود.

۳. در صورت واگذاری تلفن IP به عضو تلفن معمولی(AB – J۰)، تماس داخلی همانند تلفن معمولی در نظر گرفته می‌شود.
۴. در صورت واگذاری تلفن IP به عضو تلفن ویژه(۰۵۰)، تماس داخلی همانند زیر در نظر گرفته می‌شود:
تماس داخلی بعضی اوقات هزینه‌دار است(و برخی زمان‌ها، بدون هزینه). در حالت بدون هزینه، بیشتر، ترافیک‌ها از طریق اتصال P2P با همان استاندارد VoIP مبادله می‌شوند. در غیر این صورت محاوره‌ی مشخص(تماس با گوشی)، نیازمند به نقطه‌ی گیت‌وی VoIP است، که به هزینه‌های اجرایی نیاز دارد.

۲. ۱۶. ۳. شماره تلفن برای تلفن IP در ژاپن

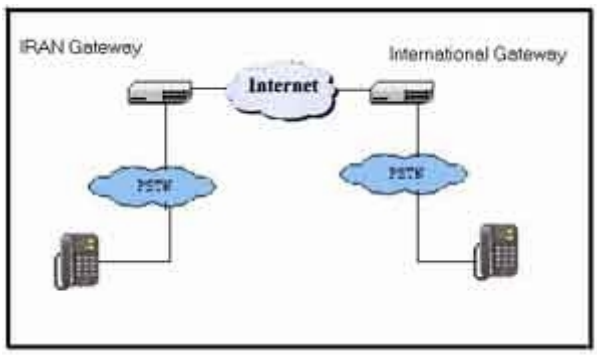
از سپتامبر ۲۰۰۲، MIC تلفن IP را در حالتی که سرویس آن در داخل طبقه‌بندی‌های خواسته شدهٔ مشخص کیفیت می‌افتد، به اعضای تلفن، واگذار کرده‌است. تلفن IP با کیفیت بالا به یک عضو تلفن واگذار می‌شود. به‌طور معمول شماره با عدد ۰۵۰ شروع می‌شود. اما هنگامی که کیفیت آنچنان بالاست که مشتری تقریباً نمی‌تواند تفاوت بین آن و یک تلفن معمولی را بیان کند و هنگامی که تهیه‌کننده شماره‌ی آن‌را با یک مکان گزارش می‌دهد(محل قرار گرفتن طرف مقابل) و اتصال را با امکانات برقراری تماس اضطراری ارائه می‌کند، در این حالت تهیه‌کننده VOIP اجازه دارد یک شماره تلفن معمولی را، که یک شماره‌ی «AB-J۰» نامیده می‌شود، به عنوان شماره‌ی VOIP واگذار کند.

۳. ۱۶. ۳. وضعیت ارائه سرویس VOIP در کشور

سرویس VOIPرا از حدود ۳ تا ۴ سال پیش، برخی از شرکت‌های خصوصی در داخل کشور ارائه می‌کنند. بدین صورت که این شرکت‌ها با اجاره کردن یک یا چند خط E1 دوطرفه (خطوطی که امکان برقراری ارتباط از هر دو طرف خط امکان‌پذیر می‌باشد)، امکان برقراری مکالمه تلفنی را با تعداد زیادی مشترک تلفنی ایجاد می‌کردند. در مرحله بعد، قراردادی را با یک شرکت خارجی که به شبکه VoIP متصل است، منعقد می‌کردند تا Gateway (تجهیزاتی که در انتهای یک شبکه قرار می‌گیرد تا

ارتباط این شبکه با شبکه دیگر در نقطه‌ای دیگر از دنیا را امکان‌پذیر سازد و عملیات تطبیق سیگنالینگ بین شبکه‌های مختلف را انجام دهد) که در ایران قرار دارد بتواند با Gateway که در خارج از ایران است، ارتباط برقرار نماید. سناریوی عملکرد این شرکت‌ها جهت برقراری ارتباط مشترکین تلفنی داخلی با خارج کشور و برعکس، به این صورت بود که کاربران از طریق خط تلفن و شبکه تلفن معمولی، به تجهیزات خاصی در ISPها مرتبط می‌شدند. در ISPها تجهیزات خاصی به نام Media Gateway، ماهیت آنالوگ صوت را به ماهیت بسته‌ای IP تبدیل می‌کردند و از طریق مسیریاب‌های بسته‌ای، این اطلاعات به سمت دروازه‌هایی که در خارج از کشور قرار دارند، هدایت می‌شد و در شبکه VoIP قرار می‌گرفت. پس از مسیریابی این اطلاعات در شبکه، در نزدیک‌ترین Media Gateway واقع در مقصد، این اطلاعات صوتی به صورت صوت آنالوگ تبدیل می‌شد و از طریق شبکه PSTN محلی، ارتباط تلفنی برقرار می‌گردید.

این عملیات به صورت دوطرفه انجام می‌شود؛ یعنی دروازه‌های داخل ایران نیز ترافیک صوتی را از دروازه خارجی دریافت کرده، با تبدیل آن به صوت آنالوگ، از طریق شبکه PSTN اقدام به برقراری ارتباط صوتی می‌نمودند. حالت اول که دروازه داخل کشور اطلاعات صوتی را به خارج ارسال می‌کند، «Origination» نام دارد و به حالت دوم که اطلاعات را از دروازه‌ی خارجی جهت برقراری ارتباط دریافت می‌کند، «Termination» گویند.



شکل ۱۲. ۳

۱۷. ۳. مشکلاتی در ارتباط با نظارت بر شبکه VoIP

یکی از امکاناتی که تلفن عادی دارد، این است که به راحتی می‌توان مکالمات را کنترل کرد و بر آن نظارت داشت. اما شبکه VoIP، به دلیل اینکه بسته‌های اطلاعاتی در آن، به هزاران کاربر مرتبط می‌شود، به سادگی شبکه تلفنی رایج قابل کنترل نیست و دست‌کم، نیاز به سخت‌افزارهای پیچیده‌ای جهت ردیابی و کنترل مکالمات تلفنی دارد.

۱۸. ۳. چرا تاکنون از این فن آوری در ابعاد گسترده‌ای استفاده نشده است ؟

ارتباط و هماهنگی بین معماری VoIP و اینترنت مبادله‌ی داده‌ی صوتی می‌بایست به صورت بلادرنگ و بدون توقف انجام گردد و این موضوع با معماری ناهمگن اینترنت که ممکن است از تعدادی روتر به منظور مسیریابی بسته‌های اطلاعاتی استفاده نماید، همخوانی نداشته و می‌تواند باعث بروز مسایل خاصی نظیر افزایش زمان RTT[1] گردد. بنابراین، می‌بایست با اعمال تغییرات لازم و به کارگیری فن آوری‌های دیگر، زمینه‌ی استفاده‌ی موثر از فن آوری VoIP را فراهم نمود.

[1] Round Trip Time

فصل چهارم
بررسی پروتکل‌های SIP & H.323

دو استاندارد اصلی در رقابت برای VoIP، استاندارد IETF،SIP و استاندارد ITUT،H.323 هستند.

در ابتدا H.323 عمومی‌ترین پروتکل بود، اگر چه در حال حاظر SIP از آن پیش افتاده‌است. این مقدمهٔ لازم برای پیمایش بهتر NAT و دیوارهای آتش بود، اگر چه تغییرات اخیر معرفی شده برای H.323 این مزیت را جابه جا کرده‌است.

به هر حال، در شبکه‌های صدای استحکام یافته(ارسال مطمئن صدا)(backbone)، جایی که هر چیز زیر کنترل عملگر شبکه یا ارتباط از راه دور است، H.323 پروتکل انتخابی است. بسیاری از بزرگترین حمل کنندگان، از H.323 در مرکز پشتیبان استفاده می‌کنند.

جایی که VoIP از میان سوئیچ‌های نرم تهیه‌کنندگان متعدد عبور می‌کند، مفاهیم رسانهٔ کامل و علامت‌دهی مهم هستند. در H.323، داده، از سه جریان داده به دست می‌آید:

۱. علامت‌دهی تماس

H.225 .۲

H.245 .۳

بنابراین، اگر شما در لندن هستید، تهیه‌کننده‌ی VOIP شما در استرالیاست و شما

می‌خواهید که با آمریکا تماس بگیرید، پس در این حالت پروکسی کامل، هر سه جریان نیمی از دور دنیا را طی خواهند کرد و تأخیر بالا(۵۰۰ تا ۶۰۰ میلی ثانیه) و فقدان بسته زیاد خواهد بود. برای جلوگیری از این مشکل، علامت‌دهی از طرف تهیه کننده‌ی VOIP انجام می‌شود که با این روش تاخیر به ۱۲۰ تا ۱۵۰ میلی ثانیه کاهش داده خواهد شد.

یکی از مسائل کلیدی همه‌ی پروتکل‌های VoIP سنتی، پهنای باند تلف شده‌ی استفاده شده برای سرآیند بسته‌هاست. به‌طور معمول، برای ارسال یک G.723. 1 با روش شنیداری فشرده شده‌ی ۵/۶ کیلوبیت بر ثانیه، به پهنای باند ۱۸ کیلوبیت بر ثانیه نیاز است. اختلاف بین ۵/۶ کیلوبیت بر ثانیه و ۱۸ کیلوبیت بر ثانیه سرآیندها می‌باشد. تعدادی تکنیک‌های بهینه‌سازی پهنای باند استفاده شده از قبیل منع سکوت و فشرده‌سازی سرآیند وجود دارد. این می‌تواند به‌طور عادی ۳۵٪ پهنای باند استفاده شده را، ذخیره کند.

VOIP CONNECTION

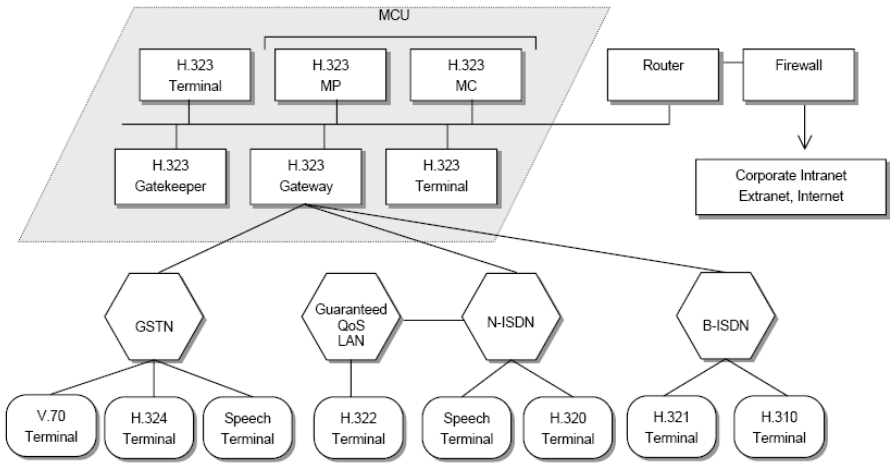
شکل۱. ۴

تکنیک‌های تهویه‌ی VoIP از قبیل TDMoIP می‌تواند سربار پهنای باند را تا دو برابر بیشتر به‌وسیله‌ی انتقال چندتایی پیام‌های محاورات چندگانه که برای همان مقصد عنوان‌گذاری می‌شوند و آن‌ها را به‌داخل همان بسته‌ها کپسول می‌کند، کاهش دهد. یا به عبارت دیگر با انتقال چندین پیام به طور همزمان که دارای یک مقصد می‌باشند، از پهنای باند به طور بهینه استفاده می‌شود.

در ادامه ابتدا پروتکل H.323 و پس از آن پروتکل SIP را توضیح خواهیم داد.
H.323 دارای مجموعه‌ای از سایر پروتکل‌ها بوده که هر یک دارای کاربرد خاص خود می‌باشند. پس از آن پروتکل دیگری با کیفیت وقابلیت‌های بالاتری به نام SIP[1] توسط IETF ارائه شد. SIP نسبت به H.323 دارای کارایی به مراتب بیشتری بوده و صرفاً برای IP تلفنی طراحی و پیاده‌سازی شده است.

۱. ۴. پروتکل H.323

این استاندارد مشخصات ترمینال‌ها و دیگر اجزاء شبکه، که قرار است امکان برقراری ارتباط چندرسانه‌ای[2] در شبکه‌های با ارسال بسته‌ای را فراهم کنند، توضیح می‌دهد. اجزاء تبعیت کننده از این استاندارد، امکان ارسال بسته‌ها به صورت زمان واقعی، و همچنین ارسال داده را فراهم می‌آورند. پشتیبانی از انتقال زمان واقعی صوت در این استاندارد اجباری است، ولی انتقال ویدئو و داده به صورت اختیاری می‌باشد. ساختار کلی این استاندارد به صورت شکل زیر می‌باشد.



شکل ۲. ۴ ساختار استاندارد H.323

[1] Session Initiation Protocol
[2] Multimedia

با توجه به شکل ۳. ۱۴ ملاحظه می‌شود که ترمینال‌هایی که از استاندارد H.323 تبعیت کنند می‌توانند به شبکه‌های مختلفی مانند ISDN[1] و GSTN[2] اتصال پیدا کنند. در زیر فصل بررسی ساختار H.323، اجزاء شبکه‌ای که استاندارد H.323 را پشتیبانی می‌کند را با جزییات بیشتری بررسی می‌کنیم.

۲. ۴. تاریخچه H.323

نسخه اول H.323 نظریه سیستم‌های تلفن مجازی و تجهیزاتی برایLAN هایی که هیچ ضمانتی برای QOS فراهم نمی کردند بود و در اکتبر ۱۹۹۶پذیرفته شد.
با پیشرفت VOIP نیازهای جدیدی مثل مهیا کردن ارتباط بین یک PC based Phone و یکPhone روی یک شبکه مدار سوییچ سنتی (SCN) ضرورت پیدا کرد. این گونه نیازها وجود یک استاندارد برایIP تلفنی را ضروری کرد. نسخه دوم H.323 برای مهیا کردن این نیازمندی‌ها تعریف شد و در ژانویه ۱۹۹۸پذیرفته شد. خصوصیات زیادی به استاندارد H.323 اضافه شده شامل فکس تحت شبکه‌های مبتنی بر Packet ارتباطات gatekeeper-gatekeeper و مکانیزمهای اتصال سریع بود. H.323 و ارتباط آن با سایر استانداردهای خانواده H.32X استاندارد H.323 بخشی از خانواده H.32X است که توسط ITU-T پیشنهاد شده است سایر نظریه‌های این خانواده سرویس‌های ارتباط مولتی مدیا تحت شبکه‌های مختلف را فراهم می‌کند.

H.320 تحت Integrated Services Digital Network(ISDN)

H.321 تحت Broandband ISDN(B-ISDN)

H.322 تحت LAN هاییکه QOS را ضمانت می‌کنند.

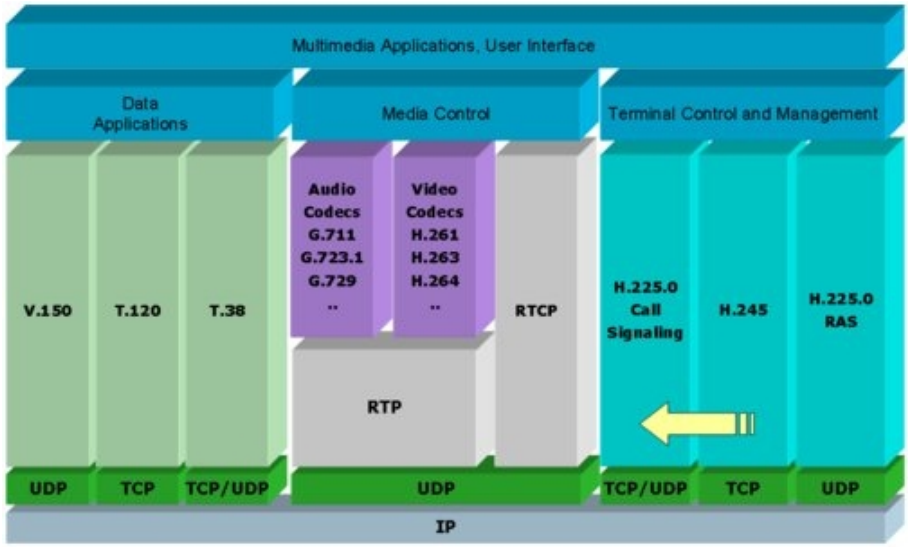
H.324 تحت Switched Circuit Network(SCN)

یکی از اهداف اولیه استاندارد H.323 سازگاری آن با سایر شبکه‌های مولتی مدیا بود این سازگاری با استفاده از gateway فراهم می‌شود یک gateway هر نوع ترجمه سیگنالی را برای سازگار شدن فراهم می‌کند.

---

[1] Integrated Services Digital Network
[2] General Switch Telephone Network

شکل زیر پشته پروتکل H.323 را با جزئیات کامل نمایش می‌دهد.



شکل ۳. ۴ پشته پروتکل H.323

۳. ۴. مزایای اصلی H.323

الف. استقلال از نوع شبکه

H.323 به نحوی طراحی شده که بتواند برای تمامی ساختارهای موجود برای شبکه‌ها قرار گیرد. این ساختار می‌تواند از کلیه سیستم‌های جدیدتری که قابلیت‌های بیشتری نسبت به سیستم‌های قبلی دارند استفاده کند.

ب. مدیریت پهنای باند

صوت و تصویر به پهنای باندی که در اختیار دارند حساس هستند و اگر پهنای باندی که در اختیار آنها قرار می‌گیرد به طور مناسب کنترل نشود، عملکرد سیستم با مشکل مواجه می‌شود. H.323 امکان کنترل تعداد ارتباطات صوتی و ویدئویی یک کاربر را می‌دهد. همچنین امکان کنترل پهنای باندی که در یک کاربرد خاص استفاده شده را فراهم می‌آورد. در حقیقت هر ترمینال H.323 امکان کنترل پهنای باند در هر

sessionای که تشکیل می‌شود را دارد. این مکانیسم که ABA[1] نامیده می‌شود می‌تواند نرخ ارسال یک کاربرد (مثلا دریافت یک فیلم) را با توجه به وضعیت شبکه، کنترل کند.

ج. برقراری ارتباط چند نقطه‌ای

یکی دیگر از امکانات فراهم شده توسط H.323، برقراری ارتباط بین چند نقطه است که این موضوع می‌تواند توسط یک کنترل کننده مرکزی، MCU[2]، یا به صورت توزیع یافته[3] فراهم گردد

د) استانداردهای Codec

H.323 استانداردهایی را برای فشرده‌سازی صوت و ویدئو تهیه می‌کند. این استانداردها باعث می‌شود که اجزاء تهیه شده توسط سازندگان مختلف بتوانند با یکدیگر کار کنند.

۴. ۴. معماری H.323

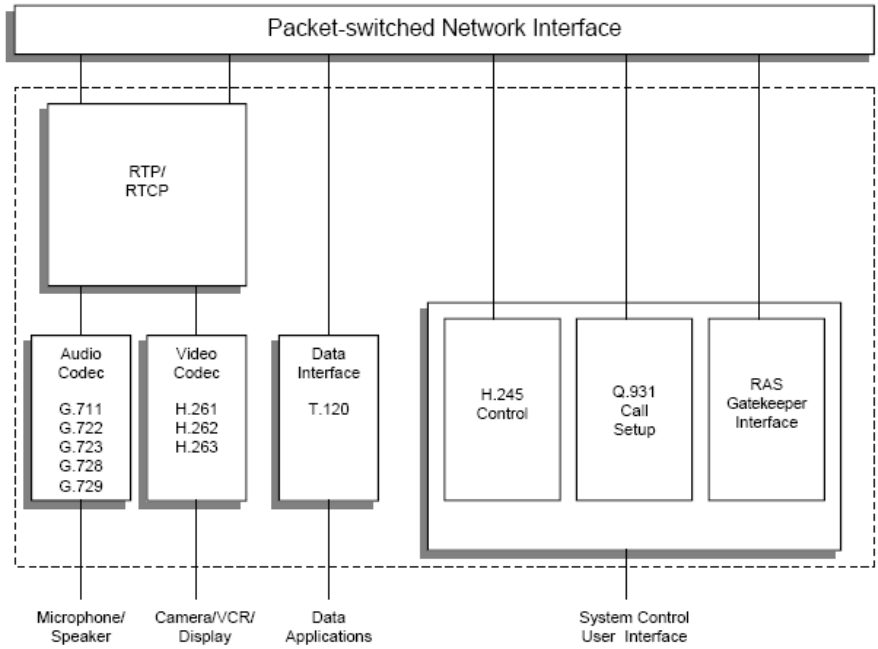
H.323 چهار نوع از اجزاء را تعریف می‌کند که وقتی که با هم شبکه می‌شوند سرویس‌های ارتباطی مولتی مدیای نقطه به نقطه و یک نقطه به چند نقطه را مهیا می‌کنند. بعضی از عناصر اجباری هستند و بعضی اختیاری در زیر هریک از این بخش‌ها را به طور دقیق‌تری بررسی می‌کنیم:

الف. ترمینال

ترمینال H.323 آخرین نقطه‌ی شبکه است که با یک ترمینال، Gateway یا کنترل کننده که با چند نقطه به صورت یک طرفه یا دوطرفه ارتباط دارد. این ارتباط شامل کنترل و ارسال صوت، ویدئو و داده می‌باشد. یک ترمینال ممکن است تنها پشتیبانی کننده صوت، صوت و ویدئو، صوت و داده یا هر سه آنها شود. همه ترمینال‌های H.323 باید استاندارد H.245 را نیز پشتیبانی کنند. این استاندارد استفاده از کانال و

[1] Automatic Bandwidth Adjustment
[2] Multipoint Control Unit
[3] Distributed

قابلیت‌های آن را به اطلاع دیگر بخش‌ها می‌رساند. بخش‌های مختلف یک ترمینال برای برقراری ارتباط با یک شبکه بسته‌ای در شکل ۴. ۴ آمده است.



شکل ۴. ۴ بخش‌های مختلف ترمینال H.323

ملاحظه می‌شود که ترمینال از استاندارد Q.931 برای سیگنالینگ ارتباط و برقراری ارتباط[1] استفاده می‌کند. همچنین برای برقراری ارتباط با Gatekeeper از پروتکل RAS[2] استفاده می‌کند. همان طور که ملاحظه می‌شود از پروتکل T.120 برای برقراری ارتباط داده بهره‌برداری می‌گردد.

ب. دروازه[3]

دلیل استفاده از دروازه، برقراری ارتباط بین دو نقطه‌ی انتهایی است، که یکی از آنها

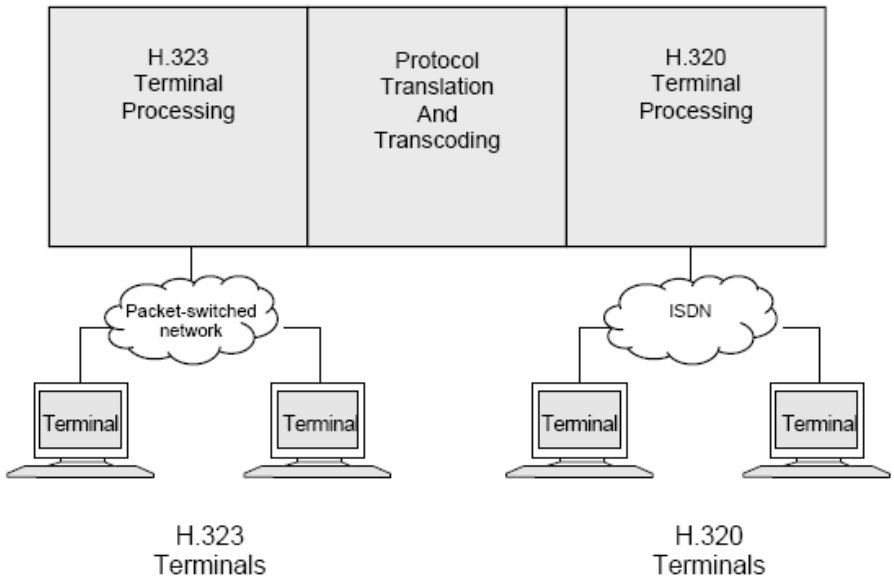
[1] Call Setup
[2] Registration/Admission/Status
[3] Gateway

ترمینال H.323 است و دیگری H.323 را پشتیبانی نمی‌کند. کاربردهای اصلی دروازه عبارتند از:

- برقراری ارتباط[1] صوتی با ترمینال‌های آنالوگ و دیجیتال.
- برقرارکردن لینک با ترمینال‌هایی که H.323 را پشتیبانی نمی‌کنند.

در حقیقت اگر ارتباط با اجزاء دیگر استانداردها لازم نبود نیازی به استفاده از دروازه نمی‌شد. همچنین دروازه یک بخش غیر اجباری در حالت برقراری کنفرانس است که سرویس‌های مختلفی را ارایه می‌کند. از جمله این سرویس‌ها ترجمه ارتباط بین نقاط انتهایی برقرار کننده کنفرانس و ترمینال‌ها است. این بخش همچنین وظیفه‌ی ترجمه بین روش‌های کدک را نیز بر عهده دارد.

یک نکته‌ی دیگر این است که تعداد ترمینال‌هایی که می‌توانند به یک دروازه متصل شوند در استاندارد محدود نشده و بر عهده سازنده قرار گرفته است. شکل ۵. ۴ ساختاری از یک دروازه را نشان می‌دهد.



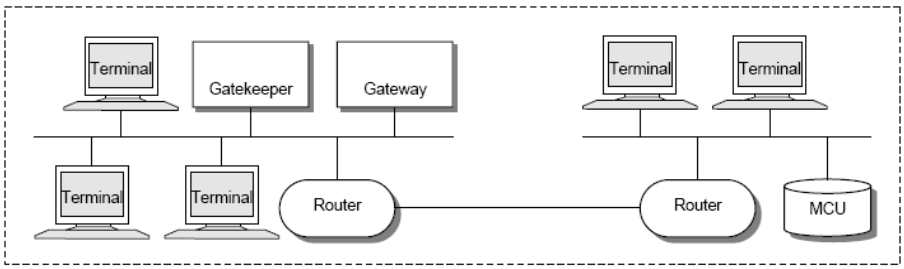
شکل ۵. ۴ ساختار یک Gateway

[1] Call Establishment

ج. دروازه بان(Gatekeeper)

یکی از مهمترین بخش‌های H.323 بخش گیت کیپر است. این بخش وظیفه‌ی کنترل دسترسی را برعهده دارد و از ورود کاربران بدون اجازه به کنفرانس ویدئویی یا تشکیل ویدئو کنفرانس‌ها بدون اجازه جلوگیری می‌کند. وظیفه‌ی دیگر این قسمت کنترل پهنای باند است. به عنوان مثال تعداد ویدئو کنفرانس‌های همزمان در یک شبکه توسط این قسمت کنترل می‌گردد و هنگامی که تعداد کنفرانس‌ها به یک سطح آستانه رسید اجازه ایجاد کنفرانس جدید داده نمی‌شود. با این روش کل پهنای باندی که به کنفرانس‌ها اختصاص می‌یابد محدود می‌شود و بنابراین بقیه پهنای باند باقی‌مانده برای دیگر کاربردها مانند ارسال فایل استفاده می‌شود. باید توجه داشت که وجود گیت کیپر در یک شبکه H.323 اجباری نیست اما اگر وجود داشته باشد، لازم است ترمینال‌ها از آن استفاده کنند.

یکی دیگر از کاربردهای گیت کیپر ایجاد یک گروه از ترمینال ها، دروازه‌ها و MCUها است که از بیرون به صورت یک گروه واحد ملاحظه شوند. به این گروه یک منطقه H.323 گفته می‌شود. در شکل ۶. ۴ یک نمونه آمده است.



شکل ۶. ۴ یک منطقه H.323

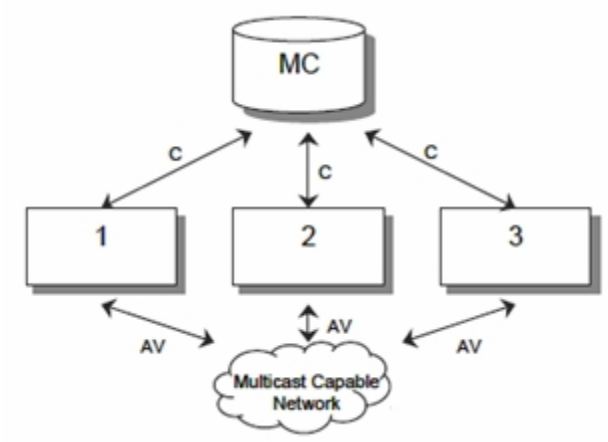
د. واحد کنترل چند نقطه‌ای[1]

واحد کنترل کننده‌ی چند نقطه‌ای (MCU) وظیفه‌ی برقراری کنفرانس بین ۳ یا تعداد بیشتری نقاط انتهایی را برعهده دارد. یک MCU شامل یک کنترل کننده چند نقطه‌ای

[1] Multipoint Control Unit

(MC) می‌باشد. این واحد همچنین می‌تواند شامل پردازشگر چندنقطه‌ای[1] نیز باشد. یک MC مباحثه بین ترمینال‌ها را بر عهده دارد تا قابلیت‌های پردازشی ترمینال‌ها را از نظر صوت و ویدئو معلوم کند. MC همچنین منابع کنفرانس را کنترل می‌کند تا معلوم کند که کدامیک از ارتباطات صوتی یا ویدئویی به صورت پخش چندگانه[2] باشد. MC به طور مستقیم به پردازش هیچ کدام از جریان‌های صوت یا ویدئو نمی‌پردازد بلکه این کار را به MP واگذار می‌کند.

کنفرانس‌های چند نقطه‌ای به دو گونه متفاوت می‌توانند باشند: الف. کنفرانس با کنترل کننده مرکزی ب. کنفرانس پخش شده[3].



شکل۷. ۴ کنفرانس چند نقطه‌ای با کنترل کننده‌ی مرکزی

در کنفرانس چند نقطه‌ای با کنترل کننده‌ی مرکزی از یک MCU استفاده می‌شود. در این حالت تمامی ترمینال‌ها اطلاعات خود، شامل صوت، ویدئو یا داده را از طریق MCU انتقال می‌دهند. MCU کنفرانسها را از طریق پروتکل H.245 کنترل می‌کند. این پروتکل قابلیت‌های ترمینال‌ها را نیز تعیین می‌کند. بخش MP وظیفه میکس‌کردن صوت و تصویر و همچنین توزیع آنها بین شرکت کنندگان در کنفرانس را بر عهده دارد.

[1] Multipoint Processor
[2] Multicast
[3] Distributed

بنابراین هر MCU که وظیفه کنترل کنفرانس‌ها به طور مرکزی را بر عهده دارد شامل یک MC و یک MP می‌شود.
کنفرانس‌های چند نقطه‌ای توزیع شده از روش پخش چندگانه استفاده می‌کنند. با این روش ترمینال‌های شرکت کننده در کنفرانس می‌توانند بدون آن که صوت یا اطلاعات خود را به MCU انتقال دهند آنرا برای دیگر شرکت کنندگان کنفرانس ارسال کنند. باید توجه داشت که در این حالت نیز پردازش اطلاعات به صورت مرکزی و توسط MC انجام می‌گردد و اطلاعات کنترلی H.245 از طریق ارتباط مستقیم انجام می‌شود.

۵. ۴. پروتکل‌های تعیین شده توسط H.323

پروتکل‌های تعیین شده توسط H.323 در زیر لیست شده اند. H.323 از شبکه‌ای بر مبنای packet تشکیل شده است و پروتکل‌های انتقال و اجرا شده روی آن مستقل هستند و آنها را تعیین نمی کند.

Audio CODECs
Video CODECs
H.225 registration, admission, and status(RAS)
H.225 call signaling
H.245 control signaling
Real-time transfer Protocol(RTP)
Real-time control Protocol(RTCP)

کدک صدا[1]

یک Audio CODEC سیگنال audio ی دریافتی از میکرفون را برای انتقال به ترمینال فرستنده ی H.323 کدگذاری می‌کند و کد audio دریافتی را برای ارسال به speaker در ترمینال گیرنده‌ی H.323 دی کد می‌کند. از آنجایی که audio حداقل سرویس ارائه شده توسط استاندارد H.323 است، تمام ترمینال‌های H.323 باید حداقل یک audio CODEC را پشتیبانی کنند.

[1] Audio CODEC

کدک تصویر[1]

یک Video CODEC سیگنال‌های videoدریافتی از دوربین را برای انتقال به ترمینال فرستنده‌ی H.323کدگذاری می‌کند و کد دریافتی را که باید به نمایشگر ویدئو در ترمینال گیرنده‌ی H.323ارسال شود دی کد می‌کند. از آنجایی که H.323 به صورت اختیاری می‌تواندvideo را پشتیبانی کند و یا نکند در نتیجه پشتیبانی از video CODECنیز اختیاری است.

به هر حال هر ترمینالH.323 که ارتباطات ویدئو را مهیا کند باید کدگذاری و دی کد کردن video را مثل آنچه که توسط نظریه یITU-T H.261تعیین شده، پشتیبانی کند.

H۲۲۵. ثبت، تصدیق و وضعیت (RAS[2])

یک پروتکل بین نقاط انتهایی ترمینال‌ها و(gateway) و Gatekeeper که آنها را کنترل می‌کند، است. این پروتکل یک پروتکل سیگنالینگ است که از طریق آنgateway نقاط انتهایی ناحیه خودش را کنترل می‌کند. توجه کنید که gateway در H.323اختیاری است پس سیگنالینگRAS نیز اختیاری است. از سیگنالینگ RAS برای انجام ثبت، کنترل پذیرش، تغییرات پهنای باند و نمایش وضعیت بین نقاط انتهایی وgatekeeper ها استفاده می‌شود و از نظر برپایی بر تمام کانال‌های دیگر تقدم دارد.

سیگنالینگ تماس(H.225 call Signaling)

برای برپایی و اتمام یک تماس بین دو H.323 نقطه انتهایی به کار می‌رود. این کار توسط تبادل پیغام‌های پروتکلH.225 روی یک کانال سیگنالینگ تماس انجام می‌شود. یک کانال سیگنالینگ تماس بین دو H.323 ویک نقطه انتهایی و یا بین یک نقطه انتهایی و یکgatekeeper می‌باشد.

---

[1] Video CODEC
[2] Registration,Admission and Status

سیگنالینگ کنترل(H.245 control Signaling)

یک پروتکل کنترل است که بین دو یا چند end-point استفاده می‌شود. هدف اصلی از H.245 مدیریت جریانهای مدیا بین اعضای جلسه‌ی H.323است. H.245 از طریق برقراری یک یا چند کانال منطقی بین end-point ها عمل می‌کند. پیامهای کنترل مبادله شده توسط این کانال اطلاعات مربوط به قابلیت تبادل، باز و بسته کردن کانال منطقی جریان رسانه‌ی کنترل جریان و دستورات کلی و نشانه‌ها را حمل می‌کنند.

۴.۶. خصوصیات ترمینال‌ها

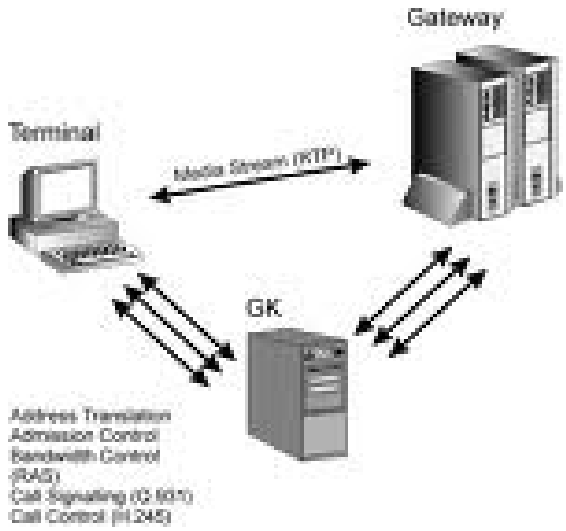
ترمینال‌های H.323 باید موارد زیر را پشتیبانی کنند:

H.245 برای تبادل قابلیت‌های ترمینال و ایجاد کانال‌های مدیای H.225 برای سیگنالینگ تماس و برپای call Rasبرای ثبت و کنترل تصدیق با یک gatekeeper RTP/RTCPبرای توالی بسته‌های audioو video ترمینال های H.323باید CODECصوتی G.711 را پشتیبانی کنند. اجزای اختیاری در یک ترمینال H.323،CODECهایی ویدئویی،پروتکل‌های data-conferencing T.120و قابلیت‌های MCU است.

۴.۷. خصوصیات Gateway و Gatekeeper

یک دروازه‌ی ترجمه‌ی پروتکل‌ها برای برپایی و خاتمه‌ی تماس، تبدیل فرمت‌های چند رسانه‌ای بین شبکه‌های مختلف و انتقال اطلاعات بین شبکه‌های مختلف و انتقال اطلاعات بین شبکه‌های H.323و غیرH.323 را مهیا می‌کند. یک کاربرد از دروازه‌ی H.323 درIP تلفنی است جایی که یک شبکه‌ی IP و یک شبکه‌ی تلفن معمولی به هم متصل می‌شوند.

Gatekeeperها سرویس‌های کنترل تماس، مثل ترجمه‌ی آدرس و مدیریت پهنای باندکه در RAS تعریف شد، را برای نقاط انتهایی مهیا می‌کنندGatekeeper ها در شبکهH.323 اختیاری هستند. اگر آنها در یک شبکه وجود داشته باشند،ترمینال‌ها و gatewayها باید سرویس‌های آنها را استفاده کنند.



شکل۸. ۴ موقعیت‌های یک Gatekeeper و Gateway

۱. ۷. ۴. وظایف اجباری Gatekeeper

- ترجمه آدرس
- کنترل پذیرش
- کنترل پهنای باند
- مدیریت ناحیه

۲. ۷. ۴. وظایف اختیاری Gatekeeper

- کنترل سیگنالینگ تماس
- اجازه تماس
- مدیریت مکالمه
- کار با سایر شبکه ها

پروتکل H.323 طوری تعیین شده که با سایر شبکه‌ها کار کند. رایج‌ترین کاربرد H.323، IPتلفنی است.

H.323 دارای مجموعه‌ای از سایر پروتکل‌ها بوده که هر یک دارای کاربرد خاص خود می‌باشند. تعدادی از این پروتکل‌ها در جدول زیر ارئه شده است.

جدول ۱. ۴

H.323 Protocol			
Transport	**Data**	**Audio**	**Video**
H.225 H.235 H.245 H.450. 1 H.450. 2 H.450. 3 RTP X.224. 0	T.122 T.124 T.125 T.126 T.127	G.711 G.722 G.723. 1 G.728 G.729	H.261 H.263

۸. ۴. سیستم معماری خدمات H.323

۱. ۸. ۴. دسته‌بندی مشخصات در H.323

مشخصه‌ها در H.323 می‌تواند به ۳ گروه تقسیم گردد: مشخصه‌های محلی، مشخصه‌های شبکه‌ای و خدمات تکمیلی مشخصه‌های محلی می‌توانند در نقاط پایانی بدون نیاز به سیگنال خاص صورت‌پذیرد.

مثال‌ها برای مشخصه‌های محلی چنین هستند: تکرار فراخوان، تاریخچه‌ی فراخوان، فهرست‌های فراخوان کتاب، آدرس فراخوان، شماره گیر سرعت، عملکردهای خصوصی مثل عدم مزاحمت و غیره. یک جفت از مشخصه‌ها وجود دارد که نیاز به کنترل دارد. این مشخصه‌های شبکه‌ای در یک روتر مرکزی نگهداشته و تکمیل می‌شوند. مثالاً حل مشکلات آدرس، پذیرش فراخوان، ثبت جزئیات فراخوان، قطع نام یا عدد شماره و غیره می‌باشد.

گروه سوم از مشخصه‌ها، مجموعه خدمات تکمیلی می‌باشد. این، مشخصه‌هایی هستند که نیاز به سیگنال خاص میان واحدهای مربوطه دارند. مثالاً برای خدمات تکمیلی شامل پیشروی فراخوان، انتقال فراخوان، تکمیل فراخوان، نگهداری فراخوان و غیره می‌باشد.

۲. ۸. ۴. فلسفه طرح H.450

سیستم معماری خدمات تکمیلی H.450 از یک عملکرد مرکزی تا جای ممکن استفاده می‌کند. واحدهای مشابه بطور مستقیم با استفاده از سیگنال H.450 بدون دارا بودن کنترل شبکه مرکزی ارتباط برقرار می‌کنند. برای این مشخصه‌ها که به کنترل مرکزی نیاز دارند، یک سرویس‌دهنده مشخصه استفاده می‌گردد که شکل خاصی از یک نقطه پایانی M. 323/H.450 می‌باشد. مثال‌هایی که یک سرویس‌دهنده مشخصه به آن نیاز دارد شامل کاربر بدون وکیل، سرویس‌دهنده پیام گیر، سرویس‌دهنده ACD مشخصه‌ی گروهی می‌باشد.

علاوه بر کنترل مشخصه‌ی توزیع یافته، H.450 نیز یک نمونه را توصیف می‌کند که H.450 می‌تواند به جای نقطه‌ی نهایی انتقال یابد. یکی از مهمترین نیازهای طراحی H.450 ساده‌سازی مشخصه‌ها با شبکه‌های خصوصی و عمومی می‌باشد.

علاوه بر این،H.450 برای پروتکل‌های وسیع که در بخش بعد توصیف می‌گردد، طراحی شده بود. این H.450 شامل چند مکانیزم برای تضمین عملکرد میان نقاط نهایی با تفاوت سیستم‌ها می‌باشد که یک پیش شرایط برای استقرار و عملکرد مشخصه جدید می‌باشد.

۳. ۸. ۴. گسترش H.450

H.450 فقط یک مجموعه خدمات تکمیلی نیست، بلکه چند مکانیزم را ارائه می‌دهد که به گسترش آسان این مجموعه مشخصات اجازه می‌دهد.

۴. ۸. ۴. کنترل مشخصه‌ی همزمان با استفاده از H.323 Annexl

کنترل مشخصه‌ی همزمان روش مخالف می‌باشد همان طور که برای سیستم معماری H.450 مقایسه شده است. سرویس‌دهنده کنترل مشخصه‌ی همزمان روش مخالف می‌باشد همان طور که برای کنترل مشخصه‌ها در نقاط نهایی استفاده شده است. این روش در H.323 Annexl مشخص شده است. نقاط نهایی برای H.323 Annexl هنوز از سیگنال عملکرد برای کنترل فراخوان اصلی استفاده می‌گردد. این قابلیت عملکرد درونی فراخوان اصلی با نقاط نهایی H.323/H.450 عملکرد نتیجه

می‌دهد. این شامل شیره اصلی برای کنترل عملکردهای رابط کاربر مثل مرحله کلیدی، پیام‌های نمایشی و نشانگرهای مشخصه می‌باشد. هوشمندی کمی در نقاط انتهایی وجود دارد. راه‌هایی منطقی در سرویس‌دهنده‌ی متمرکز مشخص می‌باشد. این امر گسترش مشخصه‌ها را ممکن می‌سازد. تنها سرویس‌دهنده‌ی مشخصه باید امروزی گردد و نقاط پایانی نباید تغییر کنند، از سوی دیگر هیچ علم معناشناسی استاندارد شده‌ای برای مشخصات و ویژگی‌ها وجود ندارد. علم معناشناسی وابسته به اجزا می‌باشند. برنامه‌های کاربردی که می‌خواهند از عملکرد مشخصه و ویژگی برای اولین گروه کنترل فراخوانی استفاده کنند، نیاز به رابط عملکردی (API) دارند که نمی‌تواند به راحتی با استفاده از شیوه‌ی محرک ارائه شده باشد. یک کنترل محرک رو به پایین بیشتر مساله درجه‌بندی و سنجش به دلیل ویژگی پردازش بر روی مولفه‌های شبکه متمرکز می‌باشد.

۵. ۸. ۴. کنترل همه برنامه‌های کاربردی بااستفاده از H.323 Annex k

H.323 Annex k یک راه اختیاری را برای کنترل‌کردن سرویس‌ها در H.323 مشخص و تعریف می‌کند. H.323 Annex k توسعه و گسترش سرویس‌های جدید را بدون به روز آمد کردن نقاط پایانی H.323 را ممکن می‌سازد. Annex k یک مرحله خدماتی را با روی حد و پایه کنترل فراخونی H.323 ارائه می‌کند. جلسه کنترل سرویس و خدمات می‌تواند پس از مبادله‌کردن اطلاعات مربوطه در پیام‌های H.225-CC یا RAS تشکیل شود. این مکانیزم برای کنترل سرویس مستقل از فراخوانی و مرتبط با فراخوانی می‌باشد. جلسات کنترل خدمات و سرویس می‌توانند بین نقاط پایانی یا بین نقاط پایانی و شبکه (مثلاً GLC) نگه داشته شوند. قرارداد HTTP در کانال کنترل خدمات برای پیشنهادکردن (ارائه شده)، انتخاب‌کردن و فعال‌کردن سرویس‌ها به کاربرده شده است. منطق سرویس و خدمات در صفحات، نسخه‌ها HTML توصیف شده است که از طریق قرارداد HTTP منتقل شده اند. بنابراین این مشخصات و ویژگی‌ها می‌توانند از دستگاه حرکت دهنده یک جستجوگر وب (شامل PDAS کنترل شده است) باشند.

برنامه‌های کاربردی نمونه ممکن است شامل انتقال صفحات XML احتمالاً شامل زبان برنامه نویسی و جاوا، بارگذاری‌کردن اطلاعات و آگهی ها، یا منتقل‌کردن زبان‌های برنامه

نویسی، پردازش فراخوانی از سرویس‌گیرنده به GIL باشد.

۹.۴. SIP[1]

SIP یک پروتکل لایه‌ی کاربر است که توانایی ایجاد، اصلاح و پایان یک جلسه‌ی چند رسانه‌ای (ویدئو کنفرانس) و یا یک تلفن اینترنتی را دارد. SIP به طور مشخص حمایت می‌کند و سرویس می‌دهد به کاربرانی که ثبت شده اند و اشخاص را به طور پویا و متحرک حمایت می‌کند کاربران می‌توانند یک هویت مشخصی صرفنظر از مکان خود داشته باشند.

SIP یک سیستم ارتباطی بسته نیست. SIP می‌تواند با پروتکل‌هایی که تحت استاندارد IETF معماری شده اند ارتباط برقرار کند. مانند پروتکل های:

- RSVP: برای انتقال بلادرنگ داده
- RSTP: برای کنترل تأخیر رسانه
- SAP: برای اعلام نشست‌های چند رسانه‌ای

SIP، پروتکلی کنترلی در لایه کاربر و مبتنی بر کدگذاری اسکی است که می‌تواند برای برقراری، نگهداری و خاتمه تماس بین دو یا بیشتراز دو نقطه انتهایی استفاده شود.

همانند دیگر پروتکل‌های VOIP، SIP نیز برای آدرس‌دهی کاربردهای سیگنالینگ و مدیریت نشست‌ها در یک شبکه تلفنی طراحی شده است. سیگنالینگ اجازه می‌دهد اطلاعات تماس در شبکه منتقل شود و مدیریت نشست قابلیت کنترل یک تماس را فراهم می‌آورد.

وقتی یک تماس SIP ایجاد می‌شود ابتدا تماس گیرنده مکان سرور مناسب را پیدا می‌کند و در خواست خود را برای آن می‌فرستد دو طرف تماس با آدرس‌های SIP تعیین هویت می‌شوند.

بدیهی است که قابلیت‌های پروتکل SIP در شبکه‌هایی که به صورت نقطه به نقطه از پروتکل IP استفاده نمی‌کنند قابل اعمال نیست و در این شبکه‌ها از پروتکل MEGACO جهت اعمال کنترل‌های لازم استفاده می‌شود.

---

[1] Session Initiation Protocol

SIP با هر دو پروتکل ورژن IPV6 و IPV4 کار می‌کند.
به طور کلی SIP توانایی‌های زیر را فراهم می‌کند:
۱. مشخص‌کردن موقعیت مقصد نهایی: SIP قابلیت تحلیل آدرس، نگاشت نام و تغییر مسیر تماس را فراهم می‌کند.
۲. مشخص‌کردن خصوصیات و قابلیت‌های نقطه‌های تماس: SIP قادر است از طریق پروتکل توصیف نشست یا SDP سرویس‌هایی که یک نقطه تماس می‌تواند ارائه دهد را مشخص کند.
۳. مشخص‌کردن در دسترس بودن نقطه تماس و علت آن: اگر تماس نتواند به علت در دسترس نبودن نقطه انتهایی برقرار شود، SIP می‌تواند مشخص کند که آیا این تماس به علت مشغول بودن برقرار نشده است یا بعد از تعداد مشخصی زنگ خوردن پاسخی دریافت نشده است.
۴. برقراری نشست بین نقطه شروع و انتهایی تماس: اگر تماس بتواند تکمیل شود، SIP نشستی بین نقاط ابتدایی و انتهایی دایر می‌کند. SIP همچنین تغییرات در حین تماس از جمله اضافه‌کردن یک نقطه جدید به کنفرانس چندرسانه‌ای، تغییر خصوصیات رسانه و نحوه کدگذاری را پشتیبانی می‌کند.
۵. انتقال و اتمام تماس ها: SIP از انتقال تماس از یک نقطه به نقطه‌ای دیگر پشتیبانی می‌کند. SIP به سادگی یک نشست بین واگذار کننده و نقطه جدید برقرار می‌کند و همچنین به نشست‌های بین واگذار کننده و نقطه انتهایی در صورت لزوم پایان می‌دهد.
توجه: اصطلاح کنفرانس به معنی یک نشست (تماس) برقرار شده بین دو یا چندین نقطه انتهایی است. کنفرانس می‌تواند دو یا چندین کاربر را شامل شود و با استفاده از یک نشست چند پخشی[1] یا چندین نشست تک پخشی[2] برقرار شود.

۱۰. ۴. معماری SIP

SIP یک پروتکل سیگنالیگ است که برپایی، اصلاح و تغییر و خاتمه جلسات مولتی مدیا را اداره می‌کند. SIP در ترکیب با سایر پروتکلها، برای توصیف خصوصیات

[1] Multicast
[2] Unicast

جلسه به کار می‌رود.
سیگنالیک SIP باید مجزا از جریان مدیای آن فرض شود در واقع یک تفکیک منطقی بین سیگنالیگ و داده‌ی جاری در جلسه وجود دارد. این تفکیک مهم، مانند یک سیگنالیگ می‌تواند از طریق یک یا چند پروکسی سرور یا ریدایرکت سرور انتقال یابد و این در حالی است که جریان مدیا یک مسیر مستقیم دارد.
مثل H.323، کنترل SIP براساس مدل کنترل توزیع شده می‌باشد.
یک طرح اخیراً منتشر شده که یک چارچوب ویژه را برای بسطهای کنترل فراخوانی در رابطه با مشخصاتی مثل انتقال تماس، کنفرانس ها، Piclcup (A) Call Monitoring Call Parkipi , پیشنهاد می‌دهد. مولفان می‌خواهند مطمئن شوند که سرویس‌ها و خدمات تکمیلی به طور واحدی مجزا مشخص شده اند و از همدیگر مجزا شده اند. این امر تائید استاندارد شده انتقال خدمات تکمیلی وکنترل فراخوانی را ممکن می‌سازد. در این بررسی، SIP WG تنها انتقال فراخوانی Call Dinersion ,Mcssay Waiting نمایش بر اساس این چارچوب طراحی شده است. این امر، تکامل SIP به سوی تعریف سرویس‌ها و خدمات تکمیلی H.323,H.450 را نشان می‌دهد.
برای انتقالی که SIP ارائه می‌کند، سه احتمال وجود دارد. برای اطمینان که سرآیندهای جدید SIP نشان دهنده مشخصه جدید، توسط سرویس‌دهنده شناخته شده اند، SIP، سرآیند اطلاعات را ارائه می‌کند. مشخصات و ویژگی‌های شناسائی شده توسط سرآیندهای جدید توسط نامشان مشخص شده اند برای انتقال بحث براساس شیوه‌های جدید (پیامهای درخواست)، سرآیند Allow می‌تواند در یک درخواست SIP افزوده شود. سرصفحه Supproteol، مشخصات سرویس‌دهنده‌ها را نشان می‌دهد که این مشخصات و ویژگی‌ها توسط سرویس‌گیرنده‌ها تائید شده اند.
انتقال دادن یک مجموعه پیام به جز SIP ممکن است نیز به عنوان یک بسط در نظر گرفته شده باشد. برای مثال، مجموعه پیام ممکن است شامل صفحه وب نشان دهنده نقشه و طرح با موقعیت کنونی فراخوانده شده باشد.

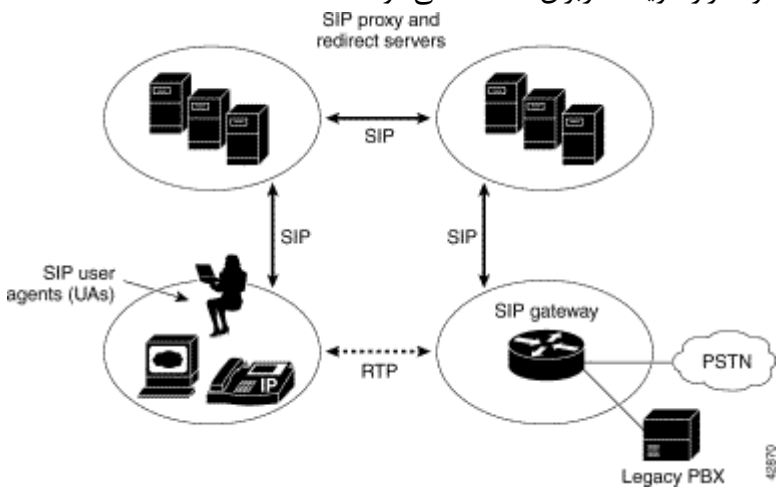
۱۱. ۴. اجزای شبکه‌ی SIP

از نقطه نظر معماری، اجزای فیزیکی یک شبکهSIP می‌تواند در دو مجموعه

طبقه‌بندی شود:

مشتری‌ها و سرورها که به آنها UAC [1] وUAS [2] نیز گفته می‌شود. یک نقطه نهـایی SIP قادر است هر دو نقش UAC و UAS را ایفا کند، اما در هر انتقال فقط باید یـک نقـش داشته باشد. اینکه یک نقطه انتهایی به عنوان UAS یا UAC عمل کند وابسته به UA است که تقاضا را شروع کرده است.

توجه: سرورهای SIP می‌توانند با دیگر سرویس‌های کاربردی از جملـه LDAP، XML و برنامه‌های پایگاه داده ارتباط برقرار کنند. از این سـرویس‌هـا بـرای خـدماتی از قبیـل مدیریت و احراز هویت کاربران استفاده می‌شود.



شکل۹. ۴ ساختار SIP

الف. مشتری‌های SIP

یک مشتری (که به آنUser Agent Client نیز گفته می‌شو د) یک برنامه‌ی کاربردی است که درخواست sip را می‌فرستد وشامل موارد زیر است:

تلفن ها: تلفن‌ها می‌توانند به عنوان یک UAC یا UAS عمل کنند.

تلفن‌های نرم‌افزاری(PCهایی که قابلیت phone را نصب کـرده انـد) و Cisco SIP IP

[1] User Agent Client
[2] User Agent Server

phoneها می‌توانند درخواست SIP را آغاز کنند و به آن پاسخ دهند.
Gateway: کنترل تماس را فراهم می‌کند. Gatewayها سرویس‌های بسیاری مهیا می‌کنند. رایج‌ترین آنها عملیات ترجمه بین نقاط انتهایی SIP و انواع ترمینال‌های دیگر در یک گفتگو است.این عمل شامل ترجمه‌ی فرمت‌های انتقال وپردازه‌های ارتباط است.

ب. سرورهای SIP

چهار نوع مختلف server وجود دارد:

۱- PROXY Serve

یک وسیله‌ی واسط است که در خواست‌های SIP ا از یک مشتری دریافت می‌کند و سپس یا آنها را خودش مدیریت می‌کند و یا، بعد از فراهم‌کردن برخی ترجمه ها، به یک server دیگر ارسال می‌کند. proxy که در خواست‌ها را دریافت کرده و آنها را می‌فرستد، در واقع هر دو نقش client وserver را ایفا می‌کند Proxy server ها می‌توانند اعمالی نظیر تصدیق، اجازه کنترل و دسترسی به شبکه، مسیریابی، ارسال مجدد درخواست به صورت معتبر و امنیت را میسر کند.

۲- redirect server

یک redirect server ، سروری است که درخواست‌های SIP را می‌پذیرد، آدرس مقصد را به آدرس جدید تبدیل می‌کند، و آن را به درخواست کننده بر می‌گرداند. سپس، درخواست کننده درخواست را به آدرس برگردانده شده از redirect server می‌فرستد. یک redirect server هیچ درخواست SIP را خودش شروع نمی کند.

۳- User agent server

serverی است که درخواست‌های SIPرا دریافت کرده و با کاربر ارتباط برقرار می‌کند. (در واقع یک وسیله SIPمثل یک تلفن با قابلیت SIP که هم به عنوان یک UAC و هم به عنوان یک UAS عمل خواهد کرد)، در صورتی که بتواند درخواست‌های SIPرا آغاز کند؛ به عنوان یک UAC عمل می‌کند و در صورتی که بتواند؛ درخواست‌ها را دریافت کرده و به انها پاسخ دهد، به عنوان یک UAS عمل می‌کند.

۴- Register server

serverی است که درخواست‌های SIP Register را می‌پذیرد. SIPمفهومی به نام ثبت کاربر دارد به این معنی که یک کاربر تعیین می‌کند که در شبکه با یک آدرس خاص در دسترس باشد یا نباشد. این ثبت از طریق انتشار یک درخواست از طرف کاربر به register server انجام می‌شود. یکregister server می‌تواند با یک Proxy serverیا redirect server ترکیب شود.

۱۲. ۴. آدرس‌دهی در SIP

اربران در یک شبکه SIP به وسیله آدرس‌های SIP یکتا شناخته می‌شوند. یک آدرس SIP مشابه یک آدرس ایمیل و به فرمت sip:userid@gateway. com است. شناسه کاربری می‌تواند یک نام کاربری یا یک آدرس E.164 باشد.

یک کاربر نهایی SIP ممکن است بین سیستم‌ها حرکت کند. موقعیت یک کاربر نهایی می‌تواند به صورت پویا در یک سرور SIP ثبت شود. سرور می‌تواند یک یا چندین پروتکل از جمله finger، rwhoise، LDAP را برای تعیین محل کاربر نهایی استفاده کند.

چون کاربر نهایی می‌تواند در بیش از یک محل login کند، و چون سرور موقعیت یاب ممکن است برخی مواقع اطلاعات نادرستی داشته باشد، ممکن است بیش از یک آدرس برای کاربر نهایی برگرداند. اگر درخواست از طرف یک سرور پروکسی SIP آمده باشد، سرور پروکسی هر یک از آدرس‌ها را چک می‌کند تا زمانی که موقعیت کاربر نهایی را پیدا کند ولی اگر درخواست از یک SIP redirect Server آمده باشد، تمامی آدرس‌ها را در هدر فیلد ارتباط به تماس گیرنده ارسال می‌کند.

alice@yahoo. com for e-mail
alice@atlanta. com for sip

۱۳. ۴. پیام‌های SIP

IP مانند پروتکل انتقال متن بر اساس متن است.

پیغام SIP یک درخواست از مشتری SIP به سرور و یا یک پاسخ از سرور به یک مشتری SIP می‌باشد.

هر دو نوع پیام شامل یک خط شروع، یک یا چند رشته‌ی پیش رو (header field) و پس از آن یک خط خالی که پایان header field را نشان می‌دهد و پیام که به صورت‌های مختلف می‌باشد.

شکل کلی پیام:

خط شروع (Start line)

سرآیند یا پیام پیش رو (message header)

خط خالی

پیام (message body)

خط شروع (start line) و خط پیام پیش رو (message header) و خط خالی همیشه پشت سر هم و با هم باید قرار بگیرند حتی اگر پیام وجود نداشته باشد.

۱. ۱۳. ۴. درخواست‌ها (Requests)

درخواست‌های SIP با داشتن یک خط درخواست برای خط شروع تشخیص داده می‌شوند.

یک خط درخواست شامل یک روش فراخوانی، یک درخواست به همراه آدرس و تفکیک ورژن پروتکل می‌باشد.

شکل خط درخواست:

Method Request – URL SIP – Version

روش فراخوانی به شش روش انجام می‌شود

۱. دعوت (Invite): دعوت به تشکیل جلسه

۲. درخواست(Ack): درخواست دعوت را مخاطب دریافت کرده است

۳. اختیارات(Option): درخواست اطلاعات درباره‌ی توانایی‌ها

۴. اتمام(Bye): تقاضای قطع ارتباط

۵. صرفنظر کردن(Cancel): درخواست صرفنظرکردن از ارتباط در حالی که درخواست هنوز کامل نشده است

۶. ثبت اطلاعات(Register): انتقال اطلاعات مربوط به محل کاربر به سرور SIP
درخواست URL نشان دهنده‌ی آدرس کاربر یا سرویس درخواست شده است.
ورژن SIP:
هر دو پیام درخواست و پاسخ شامل ورژن SIP در حال استفاده می‌باشند.
هر درخواست باید شامل ورژن SIP باشد.

۲. ۱۳. ۴. پاسخ‌ها (Responses)

پاسخ‌های SIP از درخواست‌ها به وسیله‌ی یک خط وضعیت مثل خط شروع تشخیص داده می‌شوند.
یک خط وضعیت شامل ورژن پروتکل و عدد کد وضعیت و عبارت متنی که بین این سه پارامتریک کاراکتر فاصله وجود دارد.
نمونه‌ای از خط وضعیت یا پاسخ:

SIP Version Status – Code Reason – Phrase خط وضعیت یا پاسخ

Status – Code: کد وضعیت
یک کد سه رقمی است که نشان دهنده‌ی نوع پیام است
Reason – Phrase عبارت متنی:
یک Text که نمایش دهنده‌ی موقعیت کد است. یک مشتری SIP نیاز به امتحان‌کردن و یا نمایش Reason – Phrase ندارد و این پیام‌ها بین سرورها می‌باشد.
اولین رقم از کد وضعیت (Status – Code) کلاس پاسخ را تعریف می‌کند و دو رقم دیگر در طبقه‌ی خاصی قرار نمی‌گیرند. برای پاسخ‌های دو رقم دیگر از 00 تا 99 می‌توانند قرار بگیرند.
این کدها دارای ۶ کلاس می‌باشند.
1xx: اطلاعات درخواست دریافت شد و مورد پردازش قرار گرفت.
2xx: موفقیت. عمل با موفقیت انجام‌پذیرفت؛ فهمیدن وپذیرفتن
3xx: تغییر جهت. Redirection اطلاعات بیشتری برای تکمیل درخواست مورد نیاز است.
4xx: خطای مشتری. درخواست ناهماهنگ و یا این درخواست در این سرور نمی‌تواند

انجام شود و یا درخواست دارای ترکیب اشتباه می‌باشد.

5xx: خطای سرور. سرور در انجام یک درخواست معتبر صحیح شکست می‌خورد و نمی‌تواند درخواست را اجرا کند.

6xx: خرابی‌های عمده (عمومی). درخواست نمی‌تواند در هیچ سروری انجام شود.

در زیر نمونه‌هایی از کدهای پاسخ آورده شده‌اند:

100 Trying	416 Unsupported URI Scheme
180 Ringing	420 Bad Extension
181 Call Is Being Forwarded	421 Extension Required
182 Queued	423 Interval Too Brief
183 Session Progress	480 Temporarily Unavailable
200 OK	481 Call/Transaction Does Not Exist
300 Multiple Choices	483 Too Many Hops
301 Moved Permanently	484 Address Incomplete
302 Moved Temporarily	485 Ambiguous
305 Use Proxy	487 Request Terminated
380 Alternative Service	488 Not Acceptable Here
400 Bad Request	491 Request Pending
401 Unauthorized	493 Undecipherable
402 Payment Required	500 Server Internal Error
403 Forbidden	501 Not Implemented
404 Not Found	502 Bad Gateway
405 Method Not Allowed	503 Service Unavailable
406 Not Acceptable	504 Server Time-out
407 Proxy Authentication Required	505 Version Not Supported
408 Request Timeout	513 Message Too Large
410 Gone	600 Busy Everywhere

جدول ۲. ۴ کدهای پاسخ

۳. ۱۳. ۴. سرآیندها (header fields)

سرآیندهای SIP شبیه سرآیندهای HTTP می‌باشند. خصوصاً سرآیندهای SIP (header field) از تعریف هماهنگی برای پیام‌های پیش رو (message header) و قاعده‌ای برای ادامه‌ی سرآیندها روی چندین خط دارند.

همچنین چندین هدرفیلد که با یک کاما (،) از هم جدا شده اند را می‌توان در یک هدر فیلد ترکیب کرد.

شکل کلی سرآیندها (header field) به صورت زیر می‌باشد:

جایگاه فیلد: اسم فیلد

باید اسم فیلد با یک دو نقطه (colon) از جایگاه فیلد جدا شود. جایگاه فیلد می‌تواند با فاصله از دو نقطه قرار گیرد یا بلافاصله بعد از دو نقطه بیاید یا دو نقطه از اسم فیلد با فاصله بیاید یا بلافاصله بعد از اسم فیلد وارد شود که البته هیچ فرقی ندارد اما بهتر است که همه بلافاصله و پشت سر هم بیایند.

به عنوان مثال:

Subject: lunch
Subject: lunch
Subject : lunch
Subject : lunch
Subject: lunch

که البته شکل آخر ترجیح داده می‌شود.

اگر جایگاه فیلد طولانی باشد می‌توان آنها را در چند خط شکست ولی در خط بعدی باید زیر

شروع جایگاه فیلد باید ادامه‌ی جایگاه فیلد را نوشت به مثال زیر توجه کنید.

Subject: I know you’re there , pick up the phone and talk to me .

که ما این پیام را می‌توانیم به صورت زیر بنویسیم.

Subject: I know you’re there ,
Pick up the phone
and talk to me .

نمونه‌ای از هدر فیلدها که در چند خط نوشته شده اند و با یکدیگر تفاوتی ندارند.

Route: < sip: alice @ atlanta. com>
Subject: Lunch
Route: < sip: bob @ biloxi. com>
Route: < sip: carol @ chicago. com>
Route: < sip: alice @ atlanta. com> , sip: bob @ biloxi. com>
Route: < sip: carol @ chicago. com>
Subject: Lunch
Route: < sip: alice @ atlanta. com> , sip: bob @ biloxi. com>,
< sip: carol @ chicago. com>
Subject: Lunch

نمونه‌های زیر مجاز هستند ولی معادل یکدیگر نیستند چون مسیرهای آنها با هم متفاوت هستند.

Route: < sip: alice @ atlanta. com>
Route: < sip: bob @ biloxi. com>
Route: < sip: carol @ chicago. com>
Route: < sip: bob @ biloxi. com>
Route: < sip: alice @ atlanta. com>
Route: < sip: carol @ chicago. com>
Route: < sip: bob @ biloxi. com> , < sip: carol @ chicago. com>,
< sip: alice @ atlanta. com>

هدر فیلدها به کوچک یا بزرگ بودن حروف غیرحساس هستند ولی به آنچه در آنها نقل شده

حساس می‌باشد به مثال زیر توجه فرمایید.

Contact: < sip: alice @ Atlanta. com>; expires = 3600
CONTACT: < SIP: ALICE @ ATLANTA. COM> ; EXPRIES = 3600

دو نمونه‌ی فوق با یکدیگر تفاوتی ندارند و معادل یکدیگر هستند.

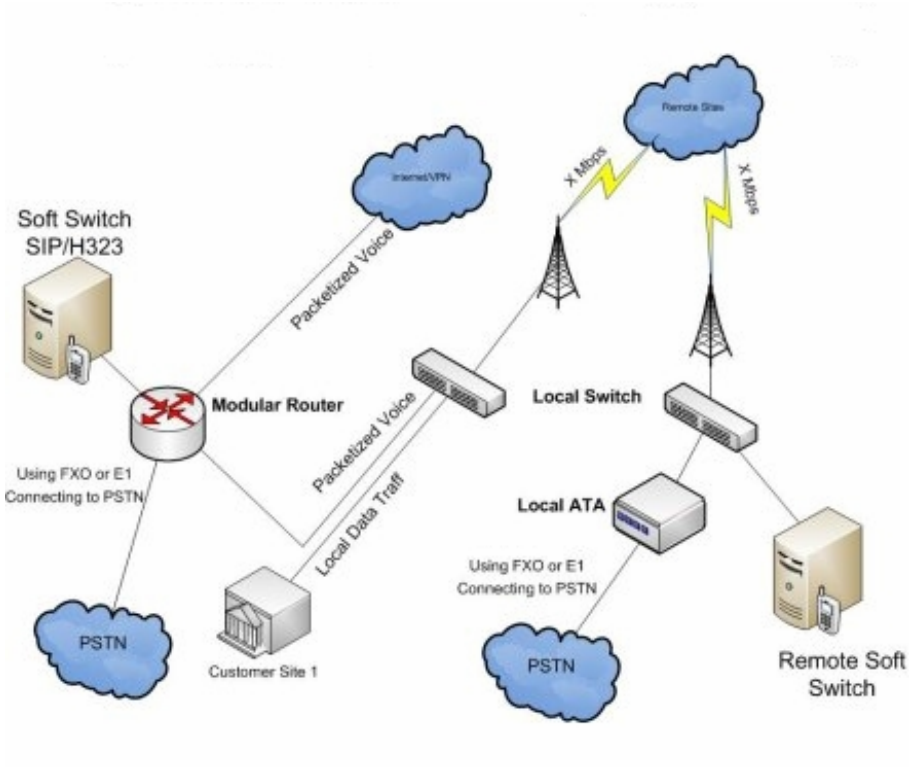
۱۴. ۴. به وجود آوردن یک جلسه

وقتی یک کاربر خواستار به وجود آوردن یک جلسه مثل جلسه‌ی صوتی، تصویری و یا بازی است آن با یک درخواست دعوت تنظیم می‌شود. درخواست دعوت از سرور درخواست آغاز جلسه را دارد. این درخواست ممکن است توسط پرکسی‌ها ارسال شود و

سرانجام دریافت شود در یک یا چند UAS که قابلیت پردازش دعوت را دارند. اگر پاسخ 2xx ارسال شود، جلسه آغاز می‌گردد و اگر پاسخ‌های 3xx , 4xx , 5xx , 6xx ارسال شوند دعوت‌پذیرفته نشده است که می‌تواند دلایل مختلفی داشته باشد.

URL تهیه شده در هدر فیلد تماس باید URL یک SIP باشد. اگر درخواست شروع مکالمه URL یک SIP را در بر داشته باشد باید URL آن SIP موجود باشد.

باید URLها آدرس‌های جهانی باشند مثل آدرس‌های اینترنتی.



شکل ۱۰. ۴ برقراری ارتباط در یک شبکه VOIP

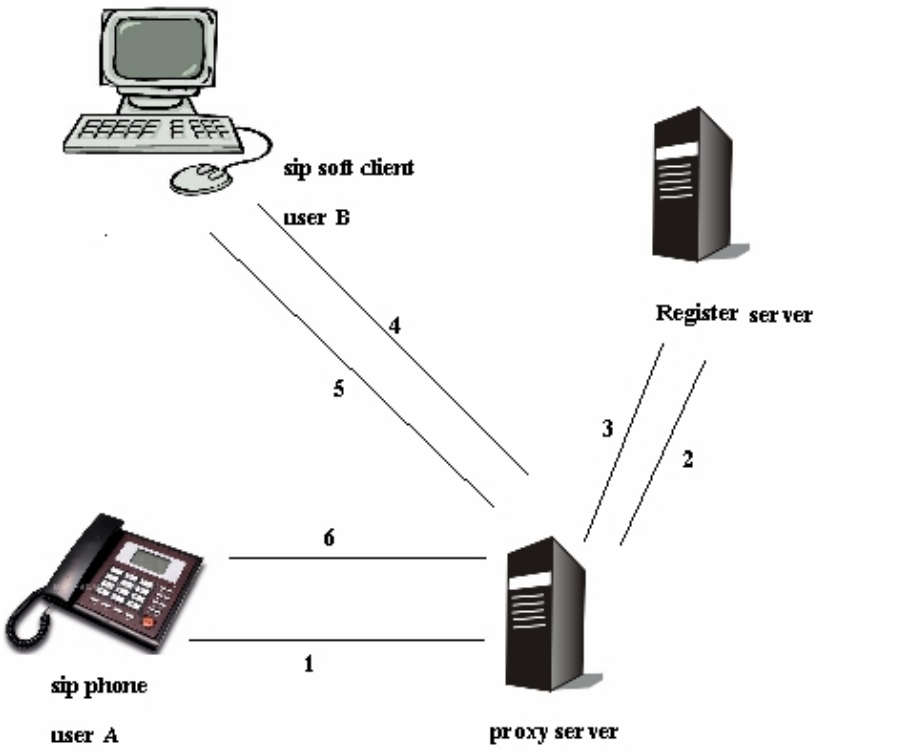
۱۵. ۴. نحوه‌ی برقراری مکالمه در SIP

۱. ۱۵. ۴. برقراری مکالمه داخل یک حوزه

برقراری مکالمه بین دو مشترک که از یک ISP سرویس می‌گیرند و در یک حوزه

قرار دارند در شکل زیر نمایش داده شده است. کاربر ۱ دارای یک تلفن SIPو کاربر ۲ دارای یک رایانه با نرم‌افزار پشتیبانی صوت و تصویر است. هر دو کاربر مشخصات و نشانی IPخود را در یک سرورپروکسی شبکه‌ی ISPثبت کرده اند. کاربر ۱ به سرور پروکسی اعلام می‌کند که خواهان برقراری ارتباط با مشترک ۲ است، سرور پروکسی نشانی کاربر ۲ را از سرور رجیستر دریافت می‌کند و دعوت مشترک ۱ را به مشترک ۲ انتقال می‌دهد. کاربر ۲ به سرور پروکسی اطلاع می‌دهد که دعوت کاربر ۱ مورد قبول وآماده‌ی دریافت پیام است.

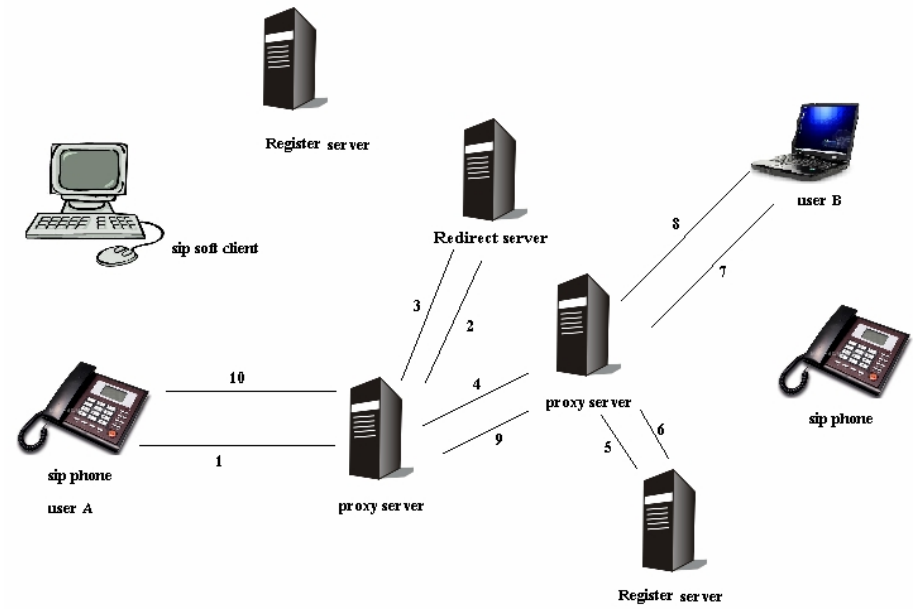
سرور پروکسی این مسئله را به کاربر ۱ اعلام می‌کند و کاربران یک ارتباط نقطه به نقطه برقرار می‌کنند.



شکل۱۱. ۴ ارتباط داخل یک حوزه

۲. ۱۵. ۴. برقراری مکالمه بین دو حوزه

در این حالت سرور پروکسی متوجه می‌شود که کاربر ۲ خارج از حوزه قرار دارد بنابراین از سرور Redirect(که می‌تواند داخل یا خارج از حوزه باشد)نشانی IPکاربر ۲ را سوال می‌کند و پاسخ را به سرور پروکسی حوزه‌ی ۲ ارسال می‌کند. سرور پروکسی ۲ دعوت کاربر ۱ را به کاربر ۲ ارسال و پیام تصدیق او را از همان مسیر به سرور پروکسی ۱ ارسال می‌کند. جزئیات بیشتر را در شکل زیر ببینید:



شکل۱۲. ۴ ارتباط بین دو حوزه

۱۶. ۴. امنیت در SIP

موضع SIPدر یک شبکه IP در معرض انواع تهدیدها مثل ID و ... قرار دارد. ID صحیح شخصی که تقاضای تماس دارد یک درخواست قانونی برای شرکت تلفنی است و در صورت جعل ID آنها این امنیت از بین می‌رود. اما علت تهدیدات اینترنت این است که هرگز حفاظهای کافی و تجهیزاتی که یک شبکه را در کل بر روی اینترنت امن و بی خطر نگه دارد وجود ندارد.

سیگنالینگ SIP دارای آسیب‌پذیری‌های متنوعی است که می‌توان دو نوع دسته‌بندی را به شکل زیر برای آن‌ها در نظر گرفت:

الف.

۱- بر اساس شبکه ی IP نظیر حملات sniffing, Spoofing, DOS, replay, middle man می‌باشد.

۲- به علت طبیعت و ساختار SIP در لایه کاربرد نظیر bogus terminate, bogus register است.

۳- شامل حملاتی ناشی از ترکیب استفاده از SIP در شبکه و آسیب‌پذیری‌های مختلف شبکه VOIP و رسانه‌های کاربردی نظیر buffer overflow, SQL injection می‌باشد.

در ادامه بعضی از حملات در این سیگنالینگ را با توضیح مختصری تشریح می‌نماییم:

DOS

حملات DOS پهنای باند سیستم را اشغال می‌کند، زمان پردازش اضافی به سیستم تحمیل می‌نماید و باعث می‌شود سیستم کارایی خود را از دست بدهد زیرا درگیر تعداد زیادی پیام ناقص می‌شود. در ضمن حمله‌کننده به پیام‌های ارسال شده از سرور SIP پاسخی نمی‌دهد و تنها آدرس‌های منابع SIP در این پیام‌ها را شنود نموده و از آن برای DOS بهره می‌برد.

Voice trapping

شنود ترافیک در سیگنالینگ SIP به دلیل عدم رمزنگاری پیام‌ها امکان‌پذیر است.

Voice spam/Predicate call

مهاجم، پیام‌های invite متعدد را برای مزاحمت کاربری و یا برای فروش محصول خود ارسال می‌نماید. وجود Spam در این شبکه مزاحمت بیشتری دارد. زیرا spam پست الکترونیکی به دلیل این که on-line چک نمی‌شود و هرگاه فرصت دست داد چک می‌شود، آزاردهنده نیست، اما ماهیت بلادرنگ voip باعث پاسخ‌گویی به تمام invite های رسیده می‌شود.

Bogus terminate

برای از کار انداختن یک نشست در SIP با ارسال پیام‌های جعلیcancel و یا bye به سرورSIP مکالمه را بدون اطلاع کاربر قطع می‌نمایند.

Malformed message

داخل نمودن یک سری کدهای نامعتبر و اضافی درون پیام‌های ارسالی، سرریز بافر ویا SQL injection از حملاتی است که می‌تواند انجام شود و از کد نویسی در بخش‌هایی از هدر SIP استفاده می‌نماید.

Phishing

در این حمله از شناسه‌های شبکه سو استفاده می‌شود. به این مفهوم که شناسه‌ی یک کاربر مجاز را استفاده نموده و به سرورSIP متصل می‌شوند تا اطلاعات لازم را از ارتباط ایجاد شده دریافت نمایند. یا آدرس خود را به عنوان یک سرور پروکسی مجازSIP در وب سایت وارد نموده و کاربر به سرور جعلی که آدرس آن وارد شده است، متصل می‌شود.

Replay attack

تکرار اطلاعات درست و حقیقی یک پیام ارسال شده در شبکه‌ی درون پیامی جعلی توسط حمله‌کننده را حمله تکرار می‌نامند. در این حمله ابتدا شنود انجام می‌شود و اطلاعات به دست آمده از پیام تحت فرمت جدید دوباره در شبکه ارسال می‌شود.

در این قسمت به راه‌حل‌هایی، برای مقابله با این حملات اشاره می‌کنیم. از مکانیزم‌هایی که امنیت SIP را افزایش می‌دهند می‌توان به موارد زیر اشاره نمود:

۱. اضافه نمودن IPsec به سیگنالینگSIP دشوار و پرزحمت است زیرا منجر به تحمیل سرباز اضافی به دلیل رمزنگاری به روشIPsec-ESP می‌شود.

۲. احراز هویت در لایه انتقال (TLS) همان HTTPS,SIPSمی‌باشد. این روش سربار کمتری نسبت به IPsecایجاد می‌کند و از الگوریتمPKI بهره می‌برد. باید از TCP برای انتقال استفاده شود.

۳. استفاده از پروتکل که SRTPبا رمز نگاری، محرمانگی و نیز احراز هویت که می‌تواند با گذاشتن یک nonce از حمله تکرارreplay جلوگیری نماید.

۴. استفاده از سیستم‌های NIDS در شبکه‌هایVOIP کاربرد دارد.

جدول زیر نگاشتی از حملات و تهدیدها به همراه راه حل‌های ارائه شده در هر مورد را نشان می‌دهد.

جدول ۳. ۴ سد حملات سیگنالینگ SIP با استفاده از مکانیزم‌های امنیتی مختلف

Solution		HTTP Authen.	S/MIME	SIP URI	IPSec	Spam Score	SRTP	Authen. Identity Body	Intrusion detection	Firewall	RELOAD
Security Property	Security Threat										
Availability	DoS								X	X	
	Bogus Terminate	X	X	X	X			X			X
	Voice Spam					X			X	X	
	Malformed Message		X	X	X			X			X
	Lookup and Routing		X	X	X			X			X
	Free Riding		X	X	X			X			X
Availability & Confidentiality	Bogus Register	X	X	X	X			X			X
	Sybil Attack		X	X	X			X			X
Confidentiality	Voice Trapping		X	X	X		X				X
Confidentiality & Integrity	Phishing	X	X	X	X						X
	Replay Attack		X	X	X		X	X			X

ب.

در دسته‌بندی حملات نوع **(ب)**داریم:

در نوع دیگری از دسته‌بندی در یک حالت کلی یک شبکه که بر اساس پروتکل SIP باشد با دو نوع تهدیدات داخلی و خارجی روبرو خواهد شد. تهدیدات خارجی توسط

مهاجم‌هایی راه اندازی می‌شوند که در ارتباط واقعی بر اساس SIP شرکت ندارند. تهدیدات خارجی زمانی رخ می‌دهد که اطلاعات از مرزها یا شبکه‌هایی عبور می‌کنند که ممکن است شامل شرکت کننده‌ی سوم یا شبکه‌های غیر قابل اعتماد باشد. اما تهدیدات داخلی اغلب توسط یک شرکت کننده در جلسه‌ی SIP رخ می‌دهد. اگر شرکت کننده در جلسه‌ی SIP موجب ایجاد حمله شود این شرکت کننده دیگر معتبر نخواهد بود.

از آنجایی که شبکه توسط دیوارهای آتش محافظ می‌شود بنابراین بیشتر مقابله با حملاتی که از درون شبکه صورت می‌گیرد مهم خواهد بود. این حملات بسیار پیچیده بوده و یافتن منبع آنها بسیار دشوار می‌باشد.

در زیر به برخی از این حملات اشاره می‌کنیم:

۱. حمله‌ی عدم پذیرش سرویس(DNS):

این حمله به این معنی است که توسط ارسال انواع زیادی از بسته‌های ناشناس، ناقص و غیره به سرور یا گیت، این کامپیوتر می‌تواند پاسخگویی را متوقف کند.

راه حل:پیکربندی،تنظیم و نصب نرم‌افزار و سخت‌افزار بر روی وسیله به منظور جلوگیری از بسته‌های خاص.

۲. کلاه برداری در بسته ها:

حمله کننده با ارسال بسته‌های جعلی وانمود می‌کند که شخص دیگری است.

راه حل:ارسال تصدیق آدرس(استفاده از کدهای خاص بیان صحیح بودن ارسال آدرس)بین دو شرکت کننده در مکالمه.

۳. استراق سمع:

حمله کننده اطلاعات ارسال شده به سمت دیگر را به دست می‌آورد.

راه حل:داده پیام رمزدار شده مانند RTP امن،از این نوع حمله جلوگیری می‌کند.

۴. درستی پیغام:

پیغامی که دریافت می‌شود معلوم نیست دقیقا همان پیغامی باشد که در محل اولیه ارسال شده است. حمله کننده می‌تواند محتوای پیغام را در حین انتقال تغییر دهد.

راه حل:پیغامهای معتبر و تصدیق شده.

SIPمکانیزم‌های مختلفی را به منظور امنیت شبکه برای اطلاعات حساس رمزدار شده نقطه به نقطه و مسیر به مسیر(hop) در رشته‌های سرانداز(header) و بدنه‌ی پیغام پیشنهاد می‌کند. بسیاری از این مشخصات که SIP شامل آنها است عبارتند از: روشهای مختلف و متنوع تصدیق HTTP یا ضمایم امنیتی،امنیت لایه انتقال ویا انتقال شبکه،ترافیک سیگنالینگ SIP را رمز دار می‌کند و ضمایم پیغام‌ها به صورت درست و قابل اعتماد بر عهده دارد. یکی از مکانیزم‌های امنیت عمومی که امنیت لایه‌ی انتقال آن را تامین می‌کند امنیت IP(IP-Sec) می‌باشد.

گروه کاری IETF که روی SIP کار می‌کنند،یک سری مسائل اصلی امنیت را به طور جامع توسعه داده اند تا از SIP در مقابل شنود، سرقت جلسه، حمله‌های فعال و همچنین درستی هویت کاربر محافظت کنند. این کار با استفاده از پروتکل SRTP برای حفاظت مدیا و HTTPS برای امنیت تنظیمات انجام می‌شود و این‌ها یک سطح امنیت مناسب را مهیا می‌کنند و می‌توانند قسمت به قسمت توسعه داده شوند و اغلب برای کار با کامپیوترها با یکدیگر در دوره‌ی توسعه،توسط SIPIT مورد آزمایش قرار
می گیرند.

SIPمثل HTTP،می تواند توسط TLS [1]حمل شود. SIP توسط TLS،رمز نگاری و پیام‌ها را برای کانال ارتباطی مهیا می‌کند و سرور بعدی را نیز شناسایی می‌کند. بر خلاف HTTP درخواست SIP قبل از این که به مقصد نهایی برسد،می تواند از چند hop عبور کند. ویژگی SIP یک رویه‌ی خاص را تعریف می‌کند که مشابه HTTPS است. برنامه‌ی SIP طوری طراحی شده است تا اطمینان دهدکه هر hop از TLS استفاده می‌کند و هر سرور، سرور بعدی را شناسایی می‌کند.

چندین راه حل برای اجرای SIP روی TLS وجود دارد. البته همه‌ی آنها به مرحله‌ی اجرا نرسیده اند.

STRP یک مشخصه برای ایجاد رمز نگاری و درستی پیام‌ها برای RTP و ترافیک RTCP است.

---

[1] Transport Layer Security

SRTP نیاز دارد هر دو طرف یک کلید محرمانه برای رمز نگاری و رمزگشایی داشته باشند. این اطلاعات که است(یا تعریف این که چگونه این کلید را بدست آوریم)باید در جلسه تعریف شود.

سرویس دهندگان اینترنت نیاز دارنددقیقاً شماره‌ی تماس گیرنده را به مقصد حمل کنند،حتی زمانی که تماس گیرنده بخواهد ناشناس باقی بماند. مکانیزمی که در حال حاضر SIP برای انتقال شماره‌ی تماس گیرنده استفاده می‌کند،-header asserted p- Identity است، اما متاسفانه این ساز وکار نیاز دارد domainهای زیادی به همدیگر اطمینان کنند تا اطلاعات هویتی دقیقی به دست آید. گروه کاری SIP برای حل این مشکل یک سرویس به نام «تشخیص هویت[1]» را توسعه داده اند که به صورت یک پروکسی SIP اجرا می‌شود. یک سرور تشخیص هویت یک امضای دیجیتالی به آدرس SIP اضافه می‌کند، که نشان می‌دهد فرستنده‌ی درخواست احراز هویت شده است و نامی که در قسمت from از header قرار دارد، می‌تواند به عنوان یک هویت واقعی مورد اطمینان قرار بگیرد. فقط سرور تشخیص هویت لازم است تا هر چیزی را بنویسد و بقیه سرورهای SIP می‌توانند شناسایی کنند که امضای دیجیتالی معتبر است.

به طور کلی حمله‌های شایع در این سیگنالینگ(SIP) را می‌توانDos ,flooding دانست.

۱۷. ۴. زبانهای برنامه نویسی سرویس

در کل، خلقت و ساختن در SIP می‌تواند با استفاده از زبان‌های برنامه نویسی انجام شود. ساختن به معنای اجراکردن منطقی سرویس و خدماتی است که H.450 را کنترل می‌کند یا روی یک درخواست پیام واکنش می‌دهد. سرویس‌دهنده‌های IETE، زبان‌های برنامه نویسی زیادی را طراحی کرده اند که می‌تواند برای اجرای خدمات آغاز شده توسط درخواست‌های پیام به کار برده شوند. IETF عموماً کاربران مطمئن و غیر مطمئن را متمایز می‌کند. برای کاربران غیر مطمئن یعنی کاربران نهایی، زبان پردازش

[1] Identity

فراخوانی (CPL)،شیوه‌هایی را برای چگونه کنترل‌کردن گردش کار SIPINVITE راارائه می‌کند. این به معنا است که تصمیم گیری شود؛ درخواست ورودی باید رد شود، پیش رود یا پروکسی شود، می‌باشد به عنوان یک توصیه به کاربران بی تجربه می‌توان خاطر نشان کرد که عملکردهای CPL بسیار محدوداست و برای جلوگیری از مسائل و مشکلات اجرا و امنیت می‌باشد. دو شیوه برای ایجاد خدمات، برای کاربران نهایی مثل مجریان سرویس‌دهنده پیشنهاد شده است: SIP-CGI, SIP SERVLETS زبان‌های برنامه نویسی SIP-CGI از زبانهای برنامه نویسی HTTP-CGI، زبانهای برنامه نویسی SIP-CGI می‌تواند برای کنترل‌کردن جریان کامل گردش کار SIP به کارگیری شوند. در حالی که زبان‌های برنامه نویسی SIP CGI مستقل از هر زبان برنامه نویسی می‌باشند.

SIP SERVLETS نیاز به محیط JSVS مثل HAVA SERVLETS دارند. به طوری که از برنامه نویسی وب مشخص است، SIP SERVLETS می‌تواند توسط پیام‌های ورودی فراخوانده شوند و چگونگی کنترل درخواست‌ها را بر سرویس‌دهنده‌های SIP دستور دهند.

در این شیوه، SIP، مکانیزم‌هایی را برای برنامه نویسی سرویس (خدماتی) ارائه می‌کند که همه به سادگی به کار برده می‌شوند. این مزیت بزرگی است که با استفاده از شیوه‌های برنامه نویسی محیط‌های مختلف می‌توان شبکه‌های هوشمند تلفنی ایجاد کرد. برای اجرای تمام خدمات روی سرویس‌دهنده‌های پروکسی SIP،باید اطمینان حاصل شود که درخواست مسئولیت پروکسی SIP از سرور عبور کند(بگذرد). زمانی که شبکه‌هایی IP از مسیر آگاه نباشند، SIP، سر آیند مسیر را برای تعیین‌کردن راهی که پیام باید برود را ارائه می‌کند.

یک شیوه جدید برنامه نویسی استفاده از ریز برنامه‌های JAVA (جاوا) که در درخواستهای SIP به کار برده شده است را پیشنهاد می‌کند.

۱۸. ۴. مقایسه H.323 وSIP

H.323 وSIP شباهت‌ها و تفاوت‌های بسیاری دارند. هر دوی آنها می‌توانند تماس‌های مستقیم یا کنفرانسی بین کامپیوترها و تلفن‌های معمولی برقرار کنند. هردو از مذاکره برای تعیین پارامترهای تماس، رمز نگاری و پروتکل‌های RTP/RTCP پشتیبانی می‌کنند. با وجود شباهت‌های ظاهری،این دو پروتکل از نظر فلسفه‌ی وجودی بسیار با هم تفاوت دارند.

H.323 پروتکلی است بزرگ، پیچیده و استاندارد صنعت تلفن، که دقیقا مشخص کرده چه چیزهای مجازند و چه چیزهای ممنوع. در این رهیافت همه چیز کاملاً مشخص و تعریف شده، و ارتباط بین سیستم‌های مختلف به سادگی امکان‌پذیر است. بهایی که برای سادگی باید پرداخت، عبارت است از، پیچیدگی و انعطاف‌پذیری کم، که انطباق این پروتکل با نیازهای آینده را دشوار کرده است.

از طرف دیگر،SIP یک پروتکل سبک و معمولی اینترنتی است که با مبادله‌ی پیام‌های متنی کار می‌کند، و سازگاری خوبی با پروتکل‌های موجود در اینترنت دارد، ولی در زمینه‌ی ارتباط با پروتکل‌های سیگنالینگ تلفن چندان قوی نیست. از آنجایی که IETF مدل VOIP خود را به صورت کاملاً مدولار تعریف کرده، این پروتکل انعطاف‌پذیری بالایی دارد و به راحتی می‌توان آن را با نیازهای آتی انطباق داد. نقطه ضعف این پروتکل مشکلات ناشی از ناسازگاری سیستم هاست، که IETF سعی کرده است با برپایی سمینارهای متعدد و تبادل آرا بین سازندگان مختلف آن را به حداقل برساند. در جدول زیر برخی از موارد SIP و H.323 مقایسه شده‌اند:

جدول ۴. ۴

SIP	H.323	آیتم
IETF	ITUT	مسئول طراحی
تا حد زیاد	بلی	سازگاری باPSTN
بلی	خیر	سازگاری با اینترنت
ماژولار	یکپارچه	معماری
فقط برقراری تماس	پشته پروتکل کامل	کامل بودن
بلی	بلی	مذاکره پارامترها
SIPرویTCPیاUDP	Q.931رویTCP	سیگنالینک تماس
متنی	باینری	فرمت پیام
RTP/RTCP	RTP/RTCP	انتقال رسانه
بلی	بلی	تماس چند طرفه
بلی	بلی	کنفرانس چند رسانه ای
URL	شماره تلفن با میزبان	آدرس دهی
صریح یا بعد از انقضای زمان	صریح یا رها کردنTCP	پایان تماس
بلی	خیر	پیام رسانی فوری
بلی	بلی	رمز نگاری
۲۵۰ صفحه	۱۴۰۰ صفحه	اندازه استاندارد
متوسط	بزرگ وپیچیده	پیاده سازی
در حال رشد	کاربرد گسترده	وضعیت فعلی

فصل پنجم
نرم‌افزارهای شبیه سازی

۱. ۵. معرفی شبیه ساز شبکه NS-2

نرم‌افزار شبیه ساز شبکه[۱] (NS) یک نرم‌افزار شبیه‌سازی مبتنی بر رویداد[۲] شبکه است که به صورت کُدِ باز[۳] و به عنوان قسمتی از پروژه ی VINT[4] توسط UC،Berkeley،AT&T، Xerox و ETH در سال ۱۹۹۵ ارائه گردید. هسته‌ی اصلی این شبیه ساز با استفاده از C++ نوشته شد. اما نسخه‌ی دوم آن (NS2) به یک زبان متنی[۵] استاندارد، به نام OTcl برای ایجاد ارتباط ساده‌تر با کاربر مجهز گردید. با آن که این پروژه در محیط Linux طراحی و توسعه داده شده، اما امکان اجرای آن در محیط ویندوز نیز فراهم گردیده است.

این نرم‌افزار می‌تواند برای مقاصد مختلفی همچون:

ارزیابی کارایی پروتکل‌های یک شبکه‌ی موجود

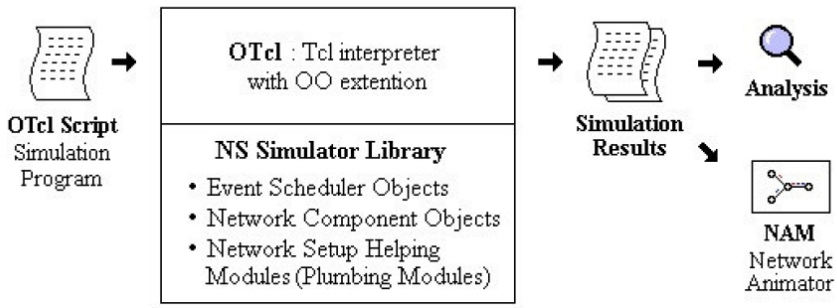
ارزیابی کارایی پروتکلهای جدیدِ طراحی شده قبل از پیاده‌سازی روی شبکه

انجام آزمایش‌هایی با مقیاسِ بزرگ، که به صورت عملی ممکن نمی‌باشند

---

[1] Network Simulator
[2] Event-based
[3] Open source
[4] Virtual Internet Testbed (VINT)
[5] Script-based

شبیه‌سازی رفتار انواع مختلف شبکه‌های مبتنی بر IP به کار گرفته شود.
علاوه بر این یک نرم‌افزار پویا نمایی[1] به نام Nam برای NS توسعه داده شده است تا بتوان رویدادهای شبکه را پس از انجام شبیه‌سازی به صورت تصویری نیز دنبال نمود.
NS-2 در حقیقت یک مفسر[2] زبان متنی Object Oriented Tcl (OTcl) است که می‌تواند سازماندهی رویدادها[3] را برای یک شبکه‌ی طراحی و سرپا شده با کمک اشیا از پیش تعریف شده در کتابخانه، را انجام دهد. شکل (۱-۲) بطور ساده، نحوه‌ی کار با NS-2 را نشان می‌دهد.



شکل۱. ۵ نمای ساده شده‌ی نحوه‌ی عملکردِ NS-2

در حقیقت به کمک کدهای Tcl با هسته‌ی اصلی NS که C++ است ارتباط برقرار می‌کنیم. قسمت‌های زیر از NS با C++ نوشته و ترجمه شده است:

۱. اجزای پایه و ابتدایی یک شبکه
۲. سازمان دهنده‌ی رویدادها

و با کمک کدهای Tcl قادر به انجام موارد زیر هستیم:

۱. تعریف توپولوژی شبکه با عناصر از پیش تعریف شده
۲. تعریف ترافیک برای یک توپولوژی موجود
۳. تعریف رویدادها و راه اندازی سازمان دهنده‌ی رویدادها

---

[1] Animator
[2] Interpreter
[3] Event schedule

به طور خلاصه ویژگی‌های زیر در NS-2 پیاده‌سازی شده و پشتیبانی می‌شوند:

۱. امکان تعریف توپولوژی و نحوه‌ی جریان یافتنِ بست ها

۲. ارسال به یک یا چند مقصد

۳. امکان شبیه‌سازی شبکه‌های بی سیم

۴. امکان شبیه‌سازی رفتار منابع ترافیکی همچون www، CBR[1] و VBR[2]

۵. پشتیبانی از پروتکل‌های لایه‌ی انتقالِ TCP و UDP

۶. مسیریابی تکنیک‌های مدیریت صف در مسیریاب‌ها (DropTail, RED, CBQ)

کاربردهایی همچون FTP، Telnet و Ping

۷. امکان ره گیری بسته‌ها در تمامی خطوط

از دیگر ویژگی‌های منحصر به فردِ NS امکان استفاده از عناصر از پیش تعریف شده‌ی Pcap/BPF است که با کمک آنها می‌توان به شبکه‌ی واقعی متصل شد و بدین ترتیب قسمتی از شبیه‌سازی را به شکل واقعی روی شبکه انجام داد.

نحوهٔ استفاده از NS-2 معمولاً نوشتن یک کد Tcl با یک ویرایشگر متن ساده و اجرای آن با برنامه‌ی NS-2 است. مادامی‌که از عناصر از پیش تعریف شده‌ی NS-2 استفاده می‌کنیم تنها با کدهای Tcl سر و کار خواهیم داشت. اما چنانچه نیاز به تعریف پروتکل‌ها و عناصر خاصی داشته باشیم ناگزیریم که آن را به شکل کد C نوشته و NS را دوباره کامپایل کنیم.

خروجی اسکریپت اجرا شده توسط NS، می‌تواند یک پیام در stdout، یک فایل Trace که می‌تواند برای بررسی نتیجه‌ی یک یا چند رویداد و یا نحوه‌ی رفتار شبکه مورد استفاده قرار گیرد و یا شکل نمایشی (Visual) رخدادها با استفاده از Nam باشد.

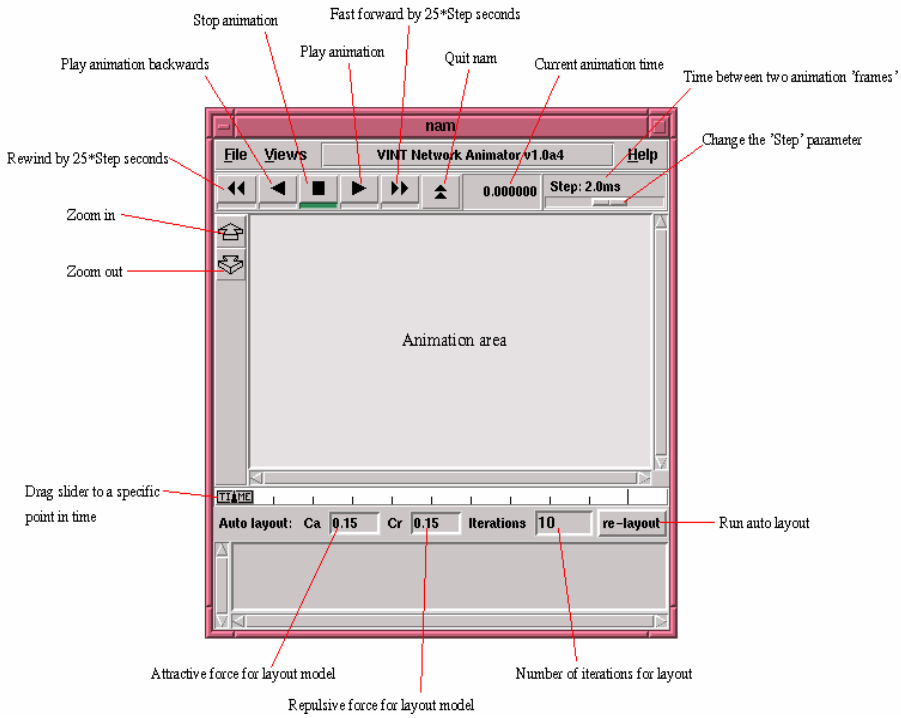
۱. ۱. ۵. معرفی Nam[3]

Nam یک نمایش دهنده‌ی نموداری توپولوژی شبکه و جریان داده است. با استفاده از این ابزار می‌توان مسیر تک تک بسته‌ها و حتی نوع و طول آنها را در حین

---

[1] Constant Bit Rate
[2] Variable Bit Rate
[3] Network Animator

عملکرد سیستم مشاهده کرد.



شکل۲. ۵ معرفی محیط ابزار Network Animator

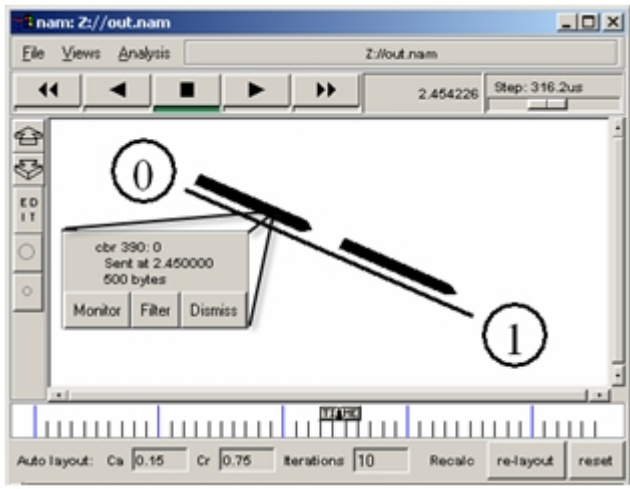
شکل (۲-۵) محیط ابزار Nam را نشان می‌دهد. با این نرم‌افزار می‌توان علاوه بر نمایش نتیجه‌ی شبیه‌سازی، توپولوژی‌های ساده را نیز تولید نمود. ابزارهای بهتری نیز نظیر Nscript برای تولید توپولوژی و ترافیک شبکه وجود دارند که از GUI[1] مناسبی برخودار هستند و تا حد زیادی کاربر را از نوشتن کدهایTcl بی‌نیاز می‌کنند. با این وجود کُد Tcl کارامدترین روش پیاده‌سازی شبکه‌های پیچیده بوده و امکانات بیشتری را در اختیار کاربر قرار می‌دهد. شکل زیر یک نمونه کُدِ Script و تصویری از نمایشِ در حال جریانِ NAM از این ارسال داده‌ی ساده را نمایش می‌دهد.

[1] Graphical User Interface

جدول ۱. ۵

loaded duplex connection-Tcl Code

#Create a simulator object
set ns [new Simulator]
#Open the nam trace file
set nf [open out. nam w]
$ns namtrace-all $nf
#Define a 'finish' procedure
proc finish {} {
global ns nf
$ns flush-trace
close $nf
exec nam out. nam &
exit 0
}
#Create two nodes
set n0 [$ns node]
set n1 [$ns node]
#Create a duplex link between the nodes
$ns duplex-link $n0 $n1 1Mb 10ms DropTail
#Create a UDP agent and attach it to node n0
set udp0 [new Agent/UDP]
$ns attach-agent $n0 $udp0
# Create a CBR traffic and attach it to udp0 	
set cbr0 [new Application/Traffic/CBR]
$cbr0 set packetSize_ 500
$cbr0 set interval_ 0. 005
$cbr0 attach-agent $udp0
#Create a traffic sink and attach it to node n1
set null0 [new Agent/Null]
$ns attach-agent $n1 $null0
#Connect the traffic source to the traffic sink
$ns connect $udp0 $null0
#Schedule events for the CBR agent
$ns at 0. 5 "$cbr0 start"
$ns at 4. 5 "$cbr0 stop"
#Call the finish procedure after 5 seconds of #simulation time
$ns at 5. 0 "finish"
#Run the simulation
$ns run



شکل ۳. ۵ خروجی Tcl Code در Nam. بسته‌ها به صورت پیکان‌هایی نمایش داده می‌شوند

در NS امکان تعریف پهنای باند، تاخیر، نوع پروتکل لایه‌ی Data link (مانند ARQ)، نوع مدیریت صف برای هر خط و نوع آدرس‌دهی (MAC) و نحوه‌ی ارسال داده روی خط مشترک (CSMA/CD) نیز وجود دارد. امکان اعمال رویداد در حین شبیه‌سازی و پویا نمودن شبیه‌سازی نیز وجود دارد. برای مثال می‌توان یک اتصال را در لحظه‌ای مشخص قطع نمود و یا یک خط lossy تعریف نمود.

یک شبکه‌ی محلی و شبکه محلی بی سیم در NS به عنوان یک نود در نظر گرفته می‌شوند، چرا که در توپولوژی LAN تمامی رایانه‌ها به یک خط واحد متصل هستند که می‌توان آن را یک نود میانی تصور نمود. بنابراین نوع دیگری از نود به نام LAN node در NS تعریف شده است که امکان شبیه‌سازی شبکه‌های محلی را فراهم می‌کند.

مسیریابی به طور پیش فرض توسط NS انجام می‌شود. NS برای آدرس‌دهی و راه‌یابی در شبکه، از یک سیستم تعیین آدرسِ خاص استفاده می‌کند. آدرس در NS بطور پیش فرض یک رشته‌ی ۶۴ بیتی است که ۳۲ بیت با ارزش کمتر[1] آن معرف port-id و از ۳۲ بیت نیمه‌ی بالاتر، بیت با ارزش بالاتر برای مقصود چند پخشی و ۳۱ بیت بقیه برای مشخص نمودن node-id به کار می‌رود. کاربر معمولاً با این آدرس‌دهی درونی، سر و

[1] Least Significant Bits

کار ندارد چراکه نام نود ها، معرف آدرس آنهاست.
Xgraph وسیله رسم نمودار در NS است. این ابزار همانند Nam بر روی فایل خروجی حاصل از شبیه‌سازی عمل می‌کند. Xgraph با استفاده از فایل trace تولید شده توسط NS قادر است مقادیر عددی را به شکل نموداری نشان دهد. این ابزار تنها برای نسخهٔ Linux، تهیه شده و کاربران Windows باید از ابزار وابسته به MATLAB به نام Gnuplot و یا Tracegraph استفاده نمایند.

۲. ۱. ۵. امکانات شبیه‌سازی توپولوژی‌های بی سیم در NS-2

پروتکل‌های Wireless در NS2 تعریف شده است. NS2 امکان تنظیم بسیاری از پارامترهای ریزِ را در توپولوژی‌های بی سیم در اختیار قرار می‌دهد. برای مثال می‌توان مدل انتشاری محیطی که شبیه‌سازی در آن صورت می‌گیرد را از بین مدل‌های افت فضای آزاد (Free Space) و Two-Ray به همراه Shadowing انتخاب نمود. تنها پترن آنتن تعریف شده برای NS، Omni-Directional است. با توجه به ماهیت Open-Source بودن NS، انواع دیگر آنتن و کانال قابل تعریف است.
همچنین انواع مختلفی از پروتکل‌های مسیریابی برای شبکه‌های بی سیم تعریف شده است که از آن جمله می‌توان به Destination Sequence Distance Vector (DSDV)، Dynamic Source Routing (DSR)، Temporally ordered Routing Algorithm (TORA) و Adhoc On-demand Distance Vector (AODV) اشاره نمود.
یکی از ویژگی‌های منحصر به فرد NS، امکان ایجاد تحرک در شبیه‌سازی شبکه‌های بیسیم است. بدین معنی که با تعریف موقعیت مکانی اولیهٔ Station ها، سرعت و در نهایت بردار جهت حرکت آنها، می‌توان در حین شبیه سازی، گیرنده و فرستنده‌ها را جابه جا نمود. NS خود با در نظر گرفتن تاخیر ذاتی مسیر بین نودها و مدل افت محیط، توان دریافتی (میزان خطا) و سایر پارامترهای شبیه‌سازی را لحظه به لحظه محاسبه می‌کند. می‌توان برای یک چند رسانه‌ای یک مدل خطا نیز در نظر گرفت (Error Model). علاوه بر این امکان تعریف حرکت تصادفی (به صورت آماری) نیز برای

ایستگاه‌ها وجود دارد.

پروتکل DCF[1] لایه‌ی MAC برای IEEE 802.11 در NS2 پیاده‌سازی شده است. این پروتکل برای حالت تک پخشی از الگوی RTS/CTS/DATA/ACK استفاده می‌کند (حالت معمولی) و برای حالت پخش، بسته را به همهٔ گیرنده‌ها ارسال می‌کند. علاوه بر این پروتکل، پروتکلی بنام TDMA-MAC نیز برای لایهٔ MAC طراحی شده است که در دست توسعه می‌باشد. در این روش، پروتکل، بازه‌های زمانی متفاوتی را در یک فریم برای ارسال و دریافت داده‌های نودها استفاده می‌کند.

برای شبیه‌سازی شبکه‌های مرکب (بی سیم + با سیم) مجموعه رویه‌هایی به NS اضافه گردید که از آن جمله نودِ «BaseStationNode» است که مانند یک دروازه بین شبکه‌ی Wired و Wireless عمل می‌کند. با تعریف این شئ، هر مجموعه از ایستگاه‌های بی سیم در یک دامنه با یک شماره مشخصه‌ی یکتا قرار می‌گیرند و BaseStationNode آن حوزه، مسوول رساندن بسته‌ها به مقاصد بی سیم می‌باشد. پس از تعریف این شئ، امکان پیاده‌سازی پروتکل‌های مسیریابی در توپولوژی‌های مختلط (سیمی و بیسیم) میسر شده و نیز پروتکل‌هایی مانند MobileIP برای شبکه‌ی Wireless تعمیم داده شد (پروتکل MobileIP توسط SUN Micro Systems ابتدا برای توپولوژی‌های با سیم تعریف و پیاده‌سازی شده بود).

در مجموع امکانات NS برای شبیه‌سازی بی سیم محدود می‌باشد. اگرچه بعضی ویژگی‌های آن همانند قابلیت تحرک کاربران منحصر به فرد می‌باشد، اما همهٔ حالات ممکن، (مثلاً Roaming) در آن لحاظ نشده است. علاوه بر این، NS انواع اندکی از ترافیک‌های از پیش تعریف شده (مانند CBR، VBR، FTP و ...) را در اختیار قرار می‌دهد و با توجه به رابط کاربری مبتنی بر text آن، ایجاد توپولوژی یک شبکهٔ بزرگ و شبیه‌سازی ترافیک نزدیک به واقعیت روی آن بسیار پیچیده و وقت گیر خواهد بود.

۲. ۵. نرم‌افزار شبیه‌سازی تخصصی شبکه‌های مخابراتی OPNET

در این بخش به معرفی نرم‌افزار تخصصی OPNET که اغلب توسط سازمان‌های

[1] Distributed coordination function (DCF)

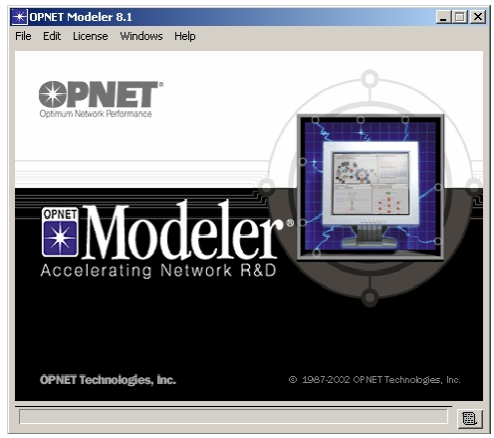
بزرگ جهانی برای طراحی، مدل‌سازی و شبیه‌سازی عملکرد شبکه بزرگ مخابراتی مورد استفاده قرار می‌گیرد، خواهیم پرداخت. نرم‌افزار OPNET در سازمان بین المللی OPNET در کشور ایالات متحده آمریکا و توسط جمع کثیری از فارغ التحصیلان مقاطع تحصیلی کارشناسی ارشد و دکتری مهندسی برق مخابرات و کامپیوتر دانشگاه MIT در ماساچوست طراحی گردیده است.

OPNET یک نرم‌افزار تجاری بوده و حق امتیاز به کارگیری آن در اختیار سازمان‌های بزرگ مانند نیروهای آمریکا، پنتاگون، سازمان فضایی آمریکا NASA، سازمان کنترل استانداردهای ITU و اتحادیه اروپا و سازمان جهانی کنترل استانداردهای مخابراتی در کشور آمریکا و دانشگاه‌های آمریکا، مانند دانشگاه MIT، دانشگاه Stanford، دانشگاه Berkeley در کالیفرنیا و دانشگاه McGill در کبک کانادا قرار دارد. OPNET دارای نسخه‌های متعددی با قابلیت‌های مختلف و در عین حال کنترل شده می‌باشد. برای فعال‌سازی هر بخش از نرم‌افزار نیاز به اخذ مجوز و license مشخصی از سازمان OPNET می‌باشد. دو نسخه اصلی این نرم‌افزار که برای شبیه سازی‌های تخصصی و حرفه‌ای به کارگرفته می‌شود، OPNET Modeler و OPNET IT Guru می‌باشد. مدل نخست کامل‌ترین و جامع‌ترین مدل در جهان بشمار می‌رود و برای فعال‌سازی همه بخش‌های آن نیاز به اخذ در حدود ۴۸۰ عدد license می‌باشد. با در نظرگیری این حجم از لایسنس‌ها براحتی می‌توان پیش بینی کرد که حجم بالایی از حافظه، برای نصب و راه اندازی آن مورد نیاز است.

۱. ۲. ۵. راه‌اندازی و کار با OPNET

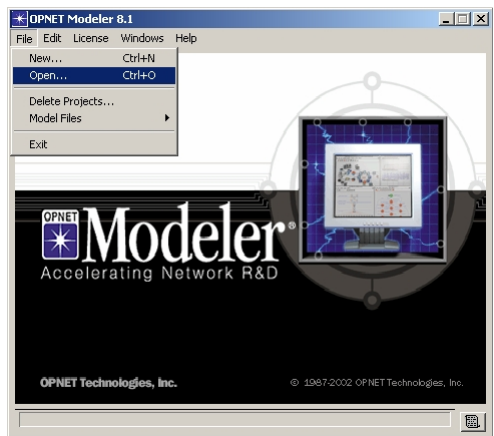
برای راه‌اندازی آن حجم فضای مورد نیاز در حدود یک گیگابایت و حافظه‌ی مجازی سیستم باید در حدود 2GB در نظر گرفته شود. علت این امر بدان دلیل است که برای ثبت حرکت بسته‌ها و مدیریت مجموعه Eventهای رخ داده در طول شبیه‌سازی، در نظرگیری فضای مناسب به عنوان حافظه‌ی مجازی امری است حیاتی، به نحوی که با سایر برنامه‌های درحال اجرا در سیستم هیچ تداخلی نداشته باشد. با این مقدمه مناسب است که در این مرحله به نحوه راه‌اندازی و معرفی اجمالی برنامه OPNET بپردازیم.

پس از نصب OPNET و با کلیک نمودن Icon آن بر روی Desktop سیستم عامل (توجه کنید که OPNET دارای نسخه‌های مخصوص به سیستم عامل‌های ویندوز، لینوکس، FreeBSD و Gentoo می‌باشد) برنامه اجرا گردیده و به صورت ذیل آماده دریافت فرمان خواهد بود.



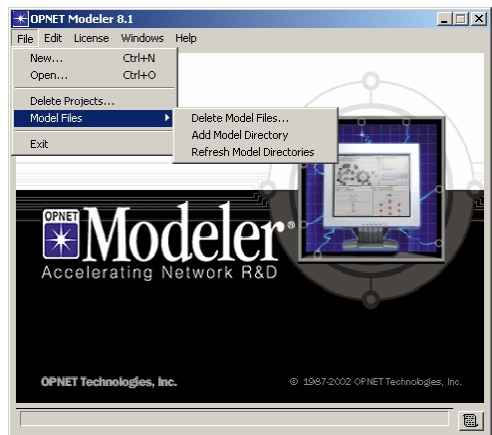
شکل۴. ۵ساختار کلی

برای باز نمودن پروژه‌های از پیش تعریف شده از منوی File → Open استفاده می‌شود و برای تعریف یک پروژه جدید از فرمان File → New بهره گیری می‌نماییم. برای حذف پروژه‌های قدیمی از گزینه Delete Projects استفاده می‌شود.



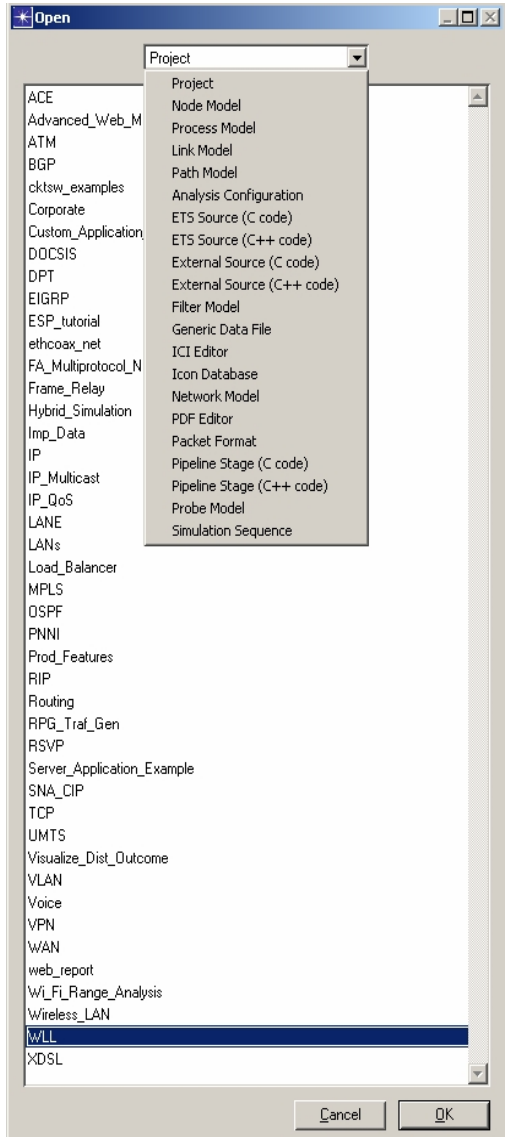
شکل۵. ۵ باز کردن فایل

برای اعمال تغییرات لازم در ارتباط با فایلهای پروژه‌های موجود ازگزینه File → Model Files بهره گیری می‌شود. سایر منوها در حال حاضر مورد استفاده این بخش نبوده و در جا و مکان مناسب به معرفی آنان خواهیم پرداخت.



شکل۶. ۵ فایل‌های مدل

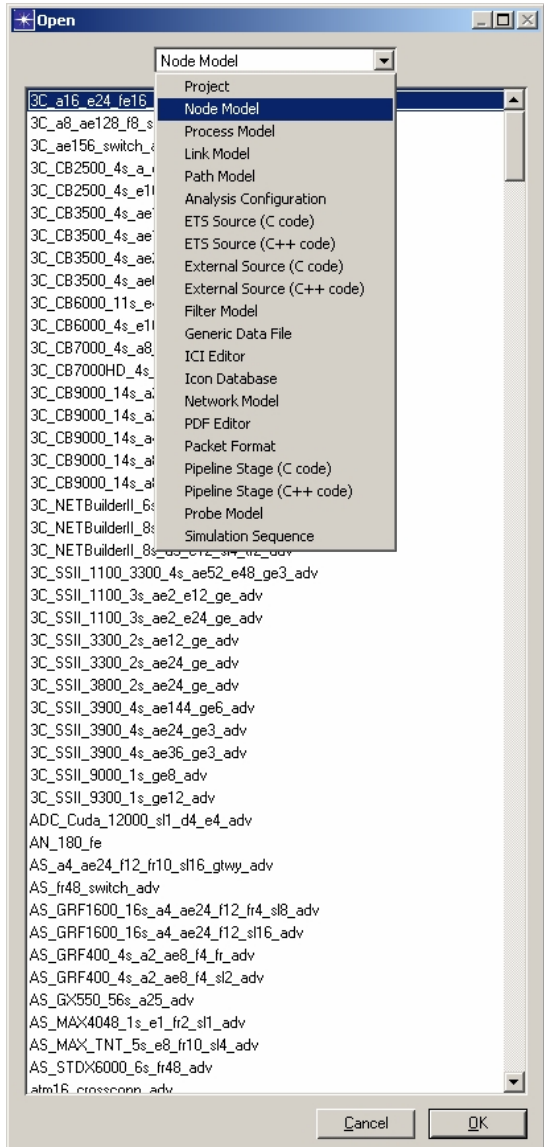
این پنجره دارای یک Combo Box است که با کلیک بر روی آن یک زیرمنو نمایان می‌گردد. گزینه‌هایی چون Node Model، Project و گزینه‌های متنوع دیگری در اختیارتان قرارخواهد گرفت. در این مجموعه هدف معرفی همه گزینه‌های فوق نبوده و تنها به بررسی برخی از آنان بسنده می‌کنیم. گزینه Project (همان طور که در شکل نیز فعال است) برای انتخاب و بازنمودن پروژه‌های از پیش طراحی شده مورد استفاده قرار می‌گیرد.



شکل۷. ۵ تعریف پروژه

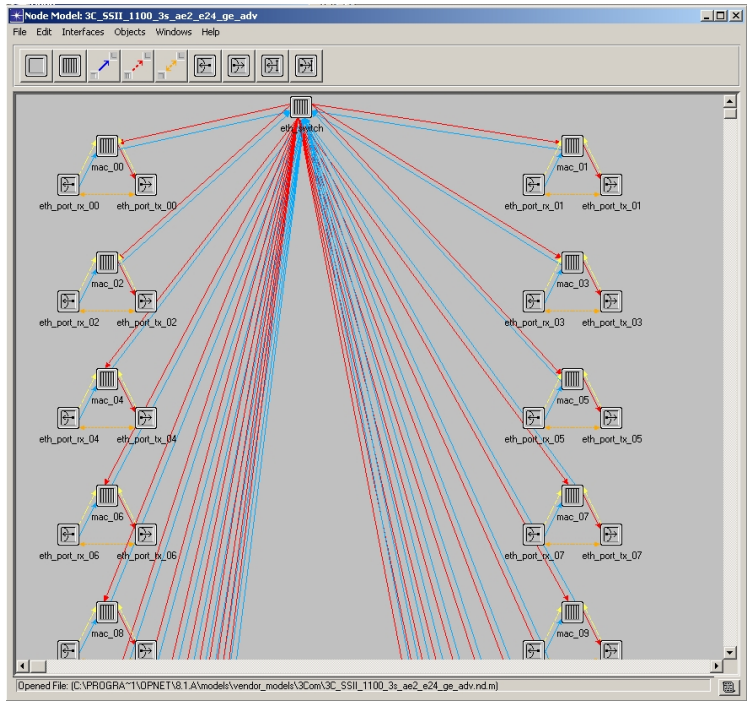
گزینه Node Model برای باز نمودن و انتخاب یکی از مدل‌های Node مورد استفاده قرار می‌گیرد. به عنوان مثال برای انتخاب مدل سخت‌افزاری سوییچ لایه سه شرکت 3Com که دارای ۳ پورت سریال، ۲ پورت نا همزمان ATM و ۲۴ پورت Ethernet و

در عین حال دارای یک پورت Gigabit Ethernet می‌باشد، می‌توان گزینه 3C-SSII-1100-3S-ae2-224-ge-adv را انتخاب نمود. با انتخاب نام آن و کلیک کردن OK، پنجره شکل باز می‌شود.

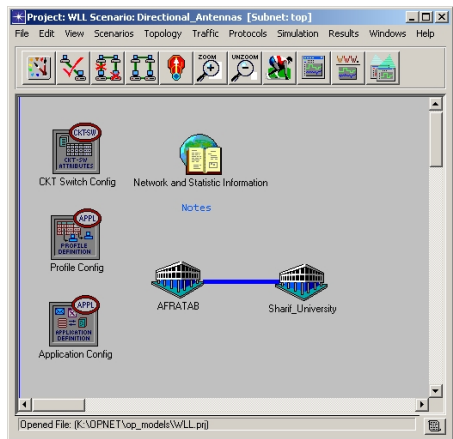


شکل۸. ۵ تعریف نود

همان طور که در شکل ۵. ۹ دیده می‌شود مدل سوییچ به قدری بزرگ و پیچیده است که در صفحه‌ی کامل، امکان نمایش آن نبوده و نیاز به Scroll نمودن مکرر خواهد بود.



شکل۹. ۵ مدل سوییچ

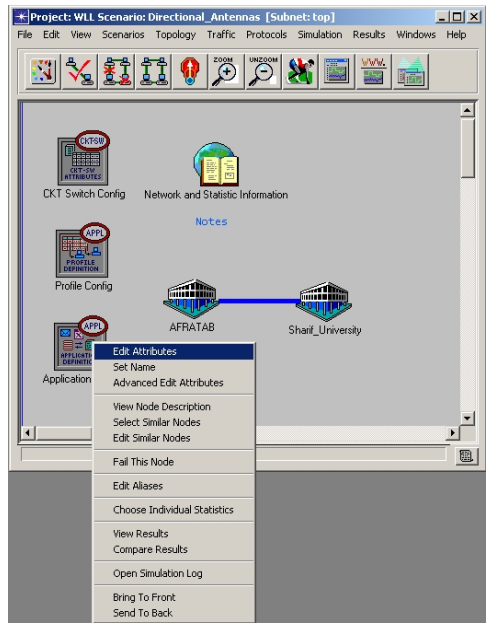


شکل ۱۰. ۵ مدلی نمادین از یک شبکه‌ی دانشگاهی مرتبط با شبکه خارجی

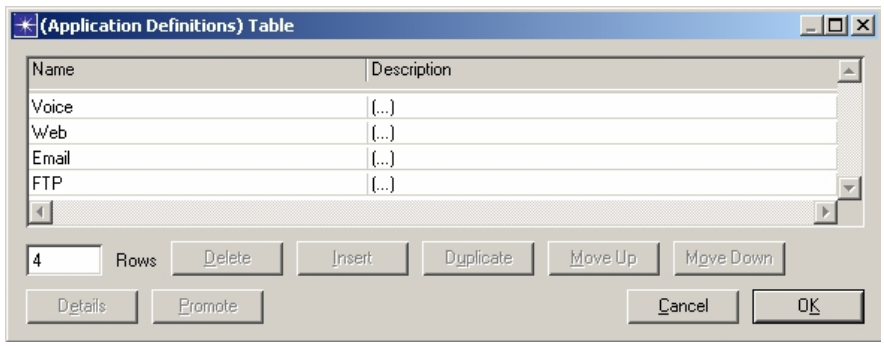
در این مجموعه هدف معرفی همه بخش‌ها نبوده و تنها به ارائه قابلیت‌های OPNET اکتفا می‌نمائیم. باز می‌گردیم به منوی Project و یک مدل مثالی از شبکه دانشگاه شریف را باز می‌نماییم. گزینه WLL را به عنوان نام پروژه در انتهای لیست را انتخاب و پنجره شکل ۱۰. ۵ نمایان می‌شود.

در این اینترفیس، ۳ بلوک در سمت چپ قرار دارد که به ترتیب از بالا به پایین برای تعریف پیکربندی تنظیمات شبکه‌های Circuit Switch، پیکربندی و تعریف پروفایل‌های ترافیکی مورد استفاده Nodeهای شبکه‌ها و پیکربندی تنظیمات مربوط به انواع ترافیک‌های مختلف موجود در سیستم به کار می‌روند. در بلوک Application می‌توان ترافیک‌های گوناگونی چون Web Browsing و Email، FTP، Database Accoss و کنترلی را مورد انتخاب قرار داده و یا به صورت ترکیبی با یکدیگر Mix نمود.

Icon مربوط به Application Config را با کلید سمت راست کلیک نموده و گزینه اول را انتخاب می‌نماییم. حال گزینه Value از بخش Application Definition را انتخاب و گزینه Edit را انتخاب کنید. پنجره‌ی ذیل باز می‌گردد. ۴ نوع ترافیک Voice (برای مدل‌سازی VoIP)، Web Browsing، Email، FTP تعریف گردیده است. ترافیک Voice با کیفیت‌های مختلفی فایل تنظیم می‌باشد که بخشی از آن در شکل ذیل نشان داده شده است:

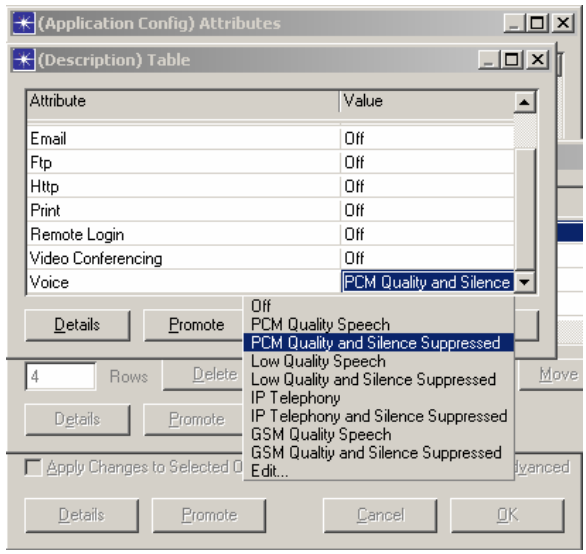


شکل۱۱. ۵تنظیم پارامترها



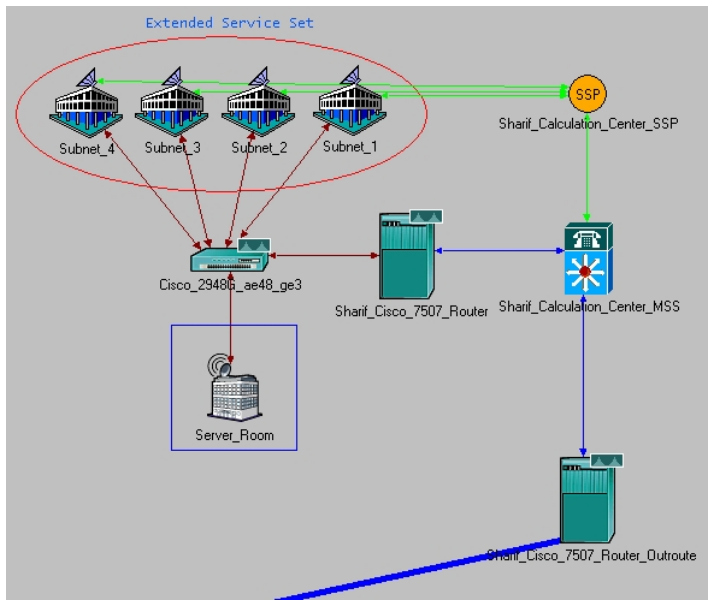
شکل ۱۲. ۵ انواع ترافیک

برای شبیه سازی‌های انجام گرفته می‌توان کیفیت صدا را به طرق مختلفی تنظیم نمـود. حتی این امکان وجود دارد که کدر و دی کدر صوت و پارامترهای متنوع دیگـری را نیـز تنظیم نمود. مـی‌تـوان از اسـتانداردهای گونـاگونی ماننـد G.729 و یـا G.711 و دهـا استاندارد دیگر بهره جست. با به کارگیری بلوک Profile Config امکان ترکیـب‌سـازی ترافیک‌های گوناگون وجود دارد.



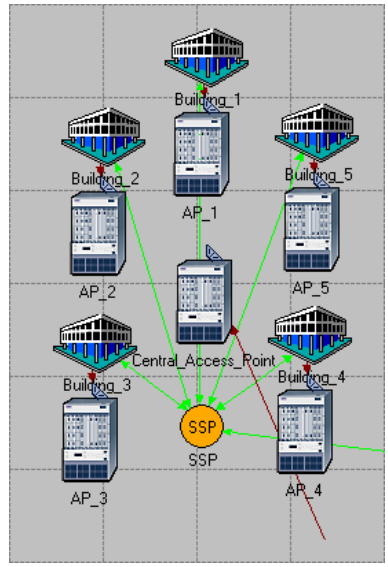
شکل ۱۳. ۵ انواع کدینگ صوت

برای نمایش قابلیت‌های OPNET اجازه دهید نگاهی اجمالی به یک شبکه نمونه داشته باشیم:



شکل۱۴. ۵جزئیات یک شبکه نمونه

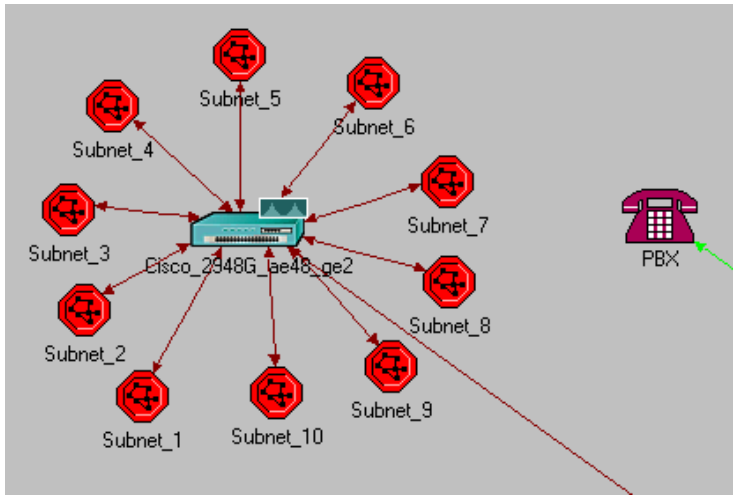
چهار زیرشبکه بی سیم که هر یک به وسیله‌ی یک AccessPoinT با آنتن جهت دار(Directional Antenna) و پنج ساختمان بزرگ محوطه، که هر یک دارای ۱۰ زیرشبکه‌ی بی سیم که هر یک به طور متوسط ۱۰ کاربر فعال داراست. درشکل به صورت یک ESS (Extended Service Set) نشان داده شده است. هر یک از ۵ ساختمان موجود در هر یک از ۴ زیرشبکه اصلی دارای یک PBX است که در حدود ۳۰ کانال فعال تلفنی و ظرفیت ۱۰۰ کانال (حداکثر) را داراست می‌باشد.



شکل ۱۵. ۵جزئیات زیرشبکه ها

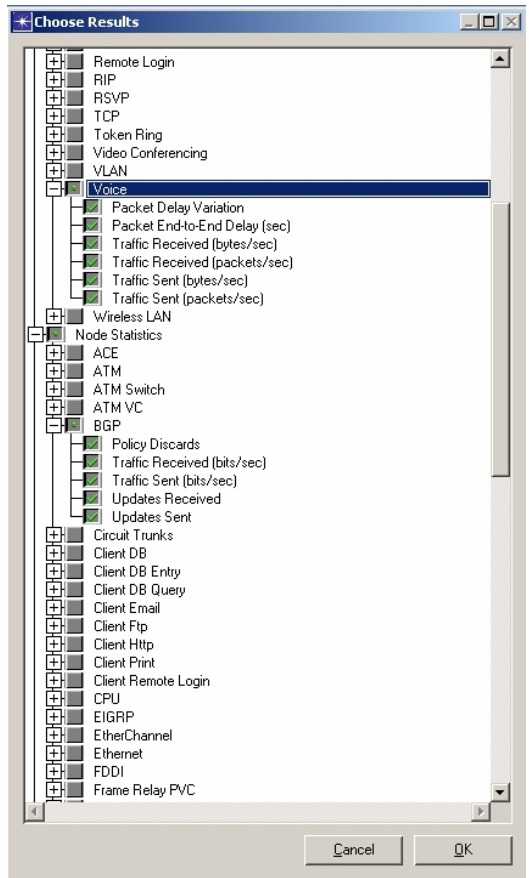
داخل یکی از Subnetهای چهارگانه را در شکل(۱۵-۵) می‌توان مشاهده نمود. ۵ ساختمان که بر روی هر یک، یک عدد آنتن Station قرار دارد به همراه یک آنتن جهت دار مرکزی به صورت نقاط دسترسی نشان داده شده است. ۵ آنتن روی هر ساختمان به صورت Station۸۰۲,11 و آنتن اصلی مرکزی به صورت نقاط دسترسی خواهد بود. هر ساختمان (و به تبعیت آن، ترافیک هر ساختمان) به صورت بی سیم به آنتن اصلی مرکزی منتقل شده و از طریق کابل 100 Base-T به سوییچ لایه چهارم Cisco که در شکل (۱۶-۵) نشان داده شده است انتقال داده شده و متصل می‌گردد.

شکل (۱۶-۵) داخل هر یک از ساختمان‌ها را نمایش می‌دهد. هر زیرشبکه که به صورت یک آیکون قرمز رنگ نشان داده شده است، حاوی ۱۰ کاربر فعال می‌باشد. PBX داخل هر ساختمان به SSP مرکزی آن ساختمان وصل و (شکل (۱۴-۵)) SSP همه‌ی ساختمان‌ها در ۴ زیرشبکه‌ی اصلی به SSP وصل می‌گردد. (شکل ۱۶. ۵)



شکل ۱۶. ۵جزئیات داخل ساختمان

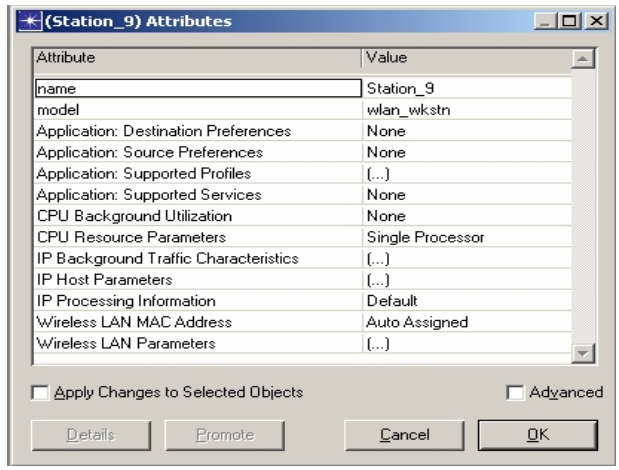
برای اطلاعات بیشتر در مورد نحوه اتصال ادوات به کاررفته و علت طراحی هر بخش به شکلی که در بالا بدان اشاره شد، به بخش طراحی کلی و جزئی سیستم مراجعه فرمائید. به دلیل اینکه که در این بخش هدف ارائه معرفی قابلیت‌های وسیع OPNET است اجازه دهید تا نگاهی به امکانات متنوعی که OPNET در جمع آوری و ثبت آمارهای گوناگون شبکه در اختیار طراح قرار می‌دهد، بیاندازیم. شکل ۱۷. ۵ پنجره‌ی Choose Result برنامه را نمایش می‌دهد. برای کاربرد کنونی هدف بررسی کیفیت صدا از قبیل Packet Deley Voriation و Packet End –To-End Delay و ترافیک مبادله شده مابین ۲ عدد کاربر نهایی می‌باشد بنابراین پارامترهای مربوط را در پنجره Choose Result انتخاب می‌کنیم. بطور کلی آرماگانهای مختلفی را می‌توان گزینش نمود که در این مثال پارامترهای مربوط به پروتکل BGP را نیز انتخاب کرده‌ایم.



شکل۱۷. ۵ ثبت آمارگانهای گوناگون

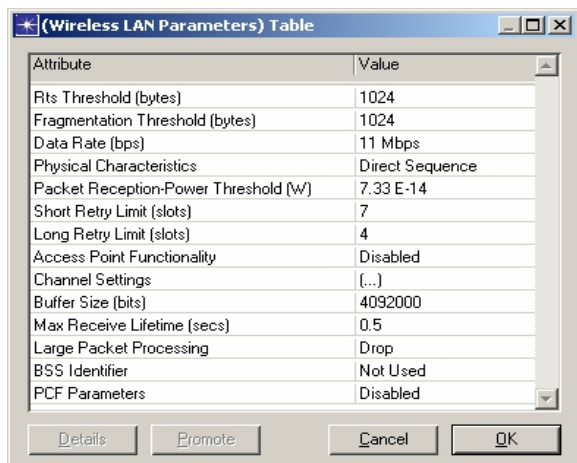
برای معرفی قابلیت‌های OPNET در تنظیم پارامترهای گوناگون یک Work Station ساده از نوع 11802, شکل (۱۸-۵) را که در آن پارامترهای لایه‌های فیزیکی، شبکه، اتصال اطلاعات، انتقال و کاربرد نشان داده شده را در نظر بگیرید.

گزینه اول نام ترمینال می‌باشد که باید به صورت یکتا و منحصر به فرد در کل سیستم هر زیرشبکه بدان نسبت داده شده باشد گزینه‌های سوم تا ششم مربوط به سرویس‌های لایه کاربرد می‌باشد. در این گزینه‌ها می‌توان تعیین نمود که ترمینال چه نوع ترافیک‌ها و چه نوع پروفایل ترافیکی را مورد استفاده قرار داده و چه نوع سرویس‌هایی را در شبکه ارایه می‌نماید.



شکل ۱۸. ۵پارامترهای لایه‌های فیزیکی

گزینه‌های مربوط به CPU، نوع سخت‌افزار موجود در ترمینال را تعیین و میزان بار اعمال شده به حافظه و پردازنده مرکزی آن را تنظیم می‌نماید. گزینه‌های مربوط به IP پارامترهای لایه شبکه را پیکربندی می‌نمایند و سرانجام گزینه‌های مربوط به Wireless LAN پارامترهای MAC Address و لایه MAC را پیکربندی می‌کند. شکل ۱۹. ۵ پنجره‌ی مربوط به پارامترهای لایه‌ی فیزیکی ۱۱۸۰۲, را نمایش می‌دهد.

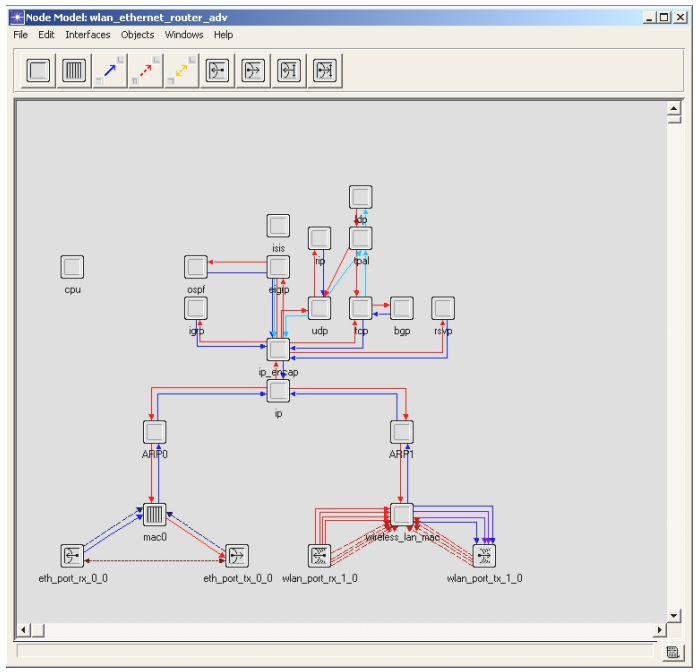


شکل ۱۹. ۵پارامترهای لایه فیزیکی

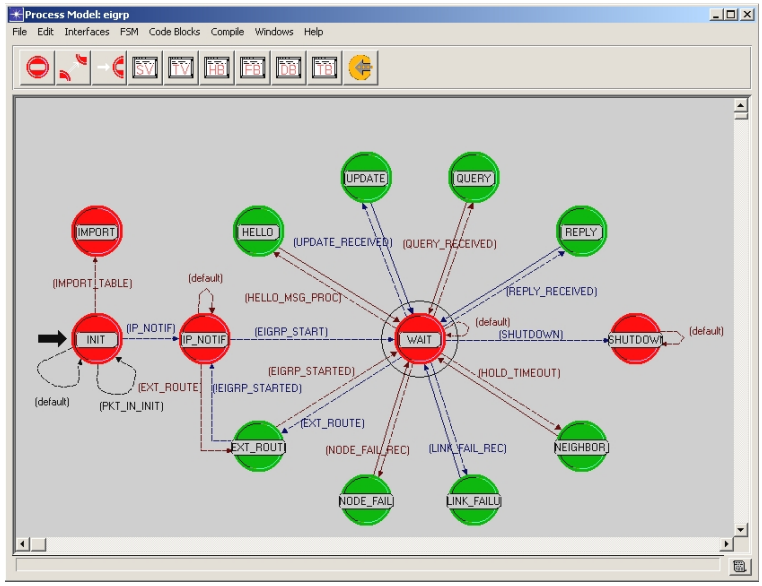
گزینه Rts Threshold میزان آستانه بکاررفته برای تعیین زمانی است که بسته‌های کنترلی RTS/CTS در مبادله اطلاعات مورد استفاده قرار می‌گیرد و توسط طراح تعیین می‌گردد. گزینه Fragmentation Threshold میزان آستانه‌ی لازم برای قطعه‌سازی فریم‌های ,۱۱۸۰۲ در تبادل اطلاعات بین ترمینال‌های گوناگون را معین می‌سازد. گزینه سوم نرخ بیت و گزینه چهارم نوع مدولاسیون مربوط به استاندار ,۱۱۸۰۲ را مشخص می‌نماید. گزینه پنجم یعنی Reception-Power (Watt) Packet حداقل میزان توان لازم برای دریافت معتبر بسته در گیرنده را برحسب وات را مشخص می‌نماید. دو گزینه بعد Retry Limitهای به کار رفته در استاندارد ,۱۱۸۰۲ را تنظیم می‌کند در حالی که Access Point Function را مشخص می‌کند. تنظیمات کانال از جمله پهنای باند هر زیرکانال و فرکانس مرکزی آن در گزینه بعد معین می‌گردد. اندازه بافر در این مثال برابر ۴۰۹۲۰۰۰ بیت قرار داده شده که می‌توان اعداد متنوعی را انتخاب نمود. گزینه Max Receive Lifetime حداکثر زمان مجاز برای ذخیره‌سازی فریم‌های ,۱۱۸۰۲ در صف[1] را معین می‌سازد. برای جلوگیری از Wireless Networks Attacks که با تولید مکرر بسته‌های بزرگ برای Overload نمودن آن صورت می‌گیرد. گزینه Drop را انتخاب می‌کنیم. گزینه آخر برای تعیین نوع Access Scheme یعنی DCF یا PCF را مشخص می‌نماید.

شکل ۲۰. ۵ Protocol Stack یک Wireless Access Poitn را نشان می‌دهد. هر یک از بلوک‌های نشان داده شده یک ماشین حالت پیچیده است که بعنوان مثال State Machine مربوط به EIGRP در شکل ۲۱. ۵ نشان داده شده است. اگر یکی از دایره‌های موجود در State Machine را دوبار کلیک کنیم، پنجره‌ای باز می‌گردد که کدهای مربوط به آن در آن نشان داده می‌شود.

[1] Queue

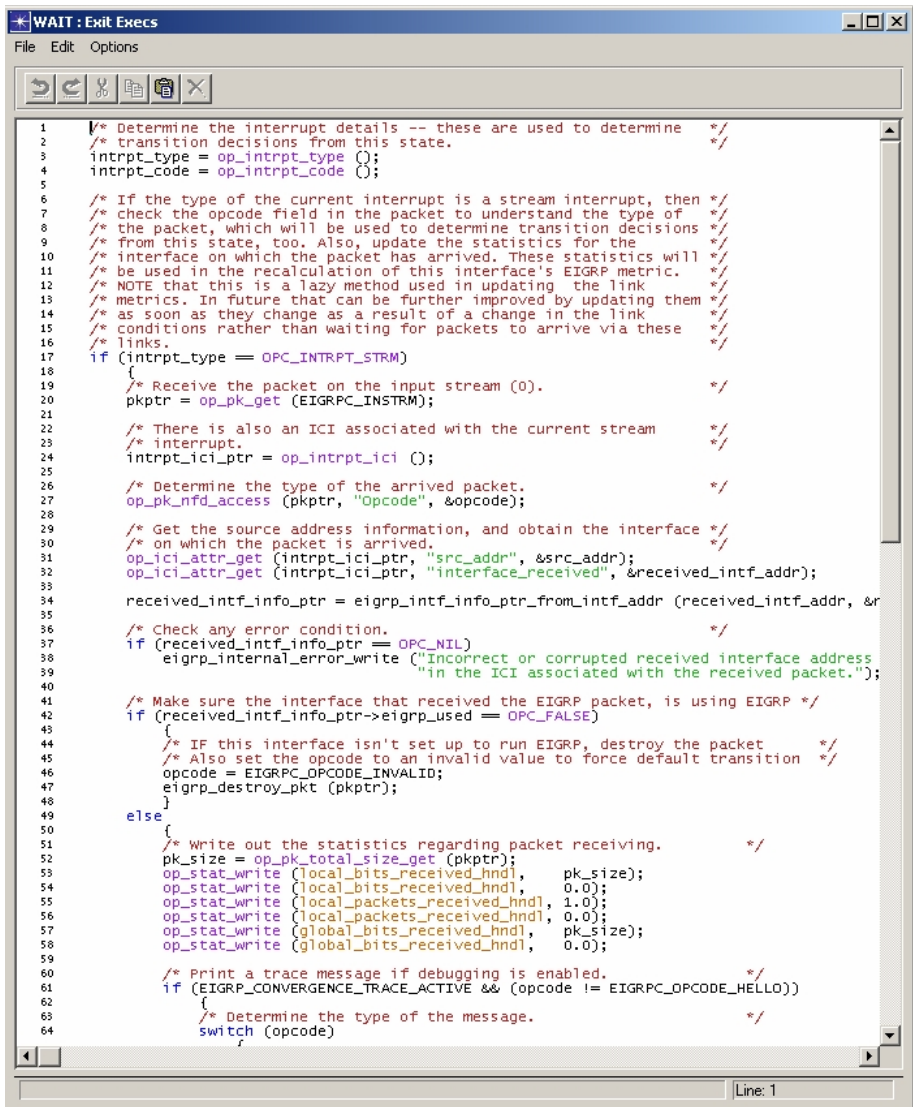


شکل ۵ .۲۰ Protocol Stack



شکل۵ .۲۱ State Machine

شکل ۲۲. ۵ تنها بخش ناچیزی از این کدها مربوط به یک State از State Machine بلوک EIGRP را نشان می‌دهد.



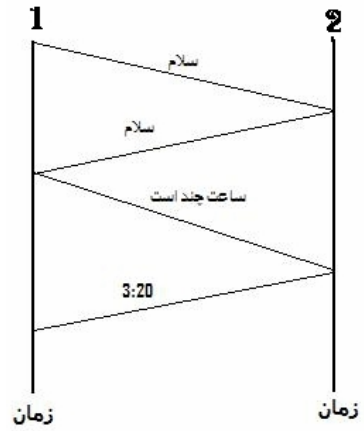
شکل ۲۲. ۵ مثالی از کدهای مربوط به یک State

فصل ششم
مروری بر انواع پروتکل‌های شبکه

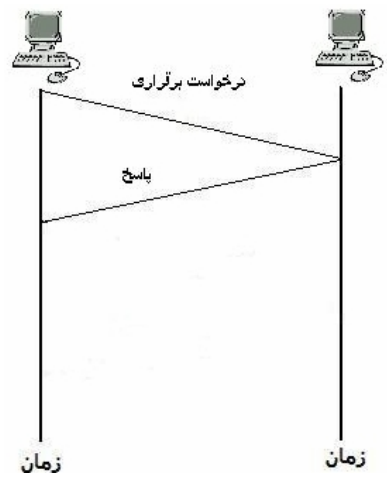
مفهوم پروتکل

شبکه‌ی کامپیوتری گروهی از کامپوترها هستند که به هم متصل می‌باشند. در واقع در شبکه‌های کامپیوتری بین نمادهای مختلف ارتباط برقرار می‌شود. (نماد: هر چیزی که بتواند ارتباط برقرار کند(علاوه بر تجهیزات، به مجموعه‌ای از قوانین نیاز است. مجموعه‌ای از قوانین که ارتباط بین نمادها را مدیریت می‌کند «پروتکل» نام دارد. پروتکل مشخص می‌کند چه نمادی ارتباط برقرار کرد، چگونه ارتباط برقرار شود، و ارتباط چه زمانی برقرار شود. پروتکل شبکه را با پروتکل‌هایی که انسان‌ها روزانه با آن‌ها سر و کار دارند مقایسه می‌کنیم. فرض کنید ساعت را در اختیار ندارید و می‌خواهید زمان فعلی را از کسی بپرسید. شما باید فعالیتی را شروع کنید سلام، ارتباط برقرار می‌شود. دومی با پیام سلام پاسخ می‌دهد شما از جواب سلام متوجه می‌شوید که می‌توانید به ارتباط ادامه دهید و می‌توانید ساعت را سوال کنید. پاسخی مثل مزاحم نشوید، من وقت ندارم و امثال اینها نشان از عدم امکان برقراری ارتباط می‌باشد. اگر افراد از پروتکل‌های مختلف استفاده کنند(مثل زبان‌های مختلف) امکان برقراری ارتباط وجود ندارد. پروتکل شبکه‌های کامپیوتر شبیه پروتکل انسانی است با این تفاوت که نمادهایی که پیام‌هایی را مبادله می‌کنند و فعالیت‌هایی را انجام می‌دهند قطعات سخت‌افزاری و نرم‌افزاری دستگاه‌هایی مثل کامپیوترها هستند. تمام فعالیت‌های موجود

در شبکه که برای برقراری ارتباط انجام می‌گیرند توسط پروتکل‌ها اداره می‌شوند.



شکل۱. ۶ پروتکل انسانی



شکل ۲. ۶ پروتکل شبکه

در این بخش تعدادی از پروتکل‌ها را معرفی می‌کنیم.

پروتکل‌ها را به پنج بخش به شرح زیر تقسیم‌بندی می‌کنیم:

۱. پروتکل لایه کاربردی

۲. پروتکل لایه جلسه

۳. پروتکل لایه انتقال
۴. پروتکل لایه شبکه
۵. پروتکل لایه پیوند داده
در ادامه تعدادی از این پروتکل‌ها را توضیح می‌دهیم:

۱. ۶. پروتکل‌های لایه کاربردی

پروتکل H.245

از این پروتکل جهت تبادل پیام‌های کنترلی به صورت نقطه به نقطه بین نقاط انتهایی درگیر در یک ارتباط استفاده می‌شود و برای تبادل اطلاعات در موارد زیر به کار می‌رود:
۱. تبادل قابلیت‌ها
۲. کنترل کانال‌های منطقی
۳. پروتکل‌های مربوط به کدکننده‌های تصویری
پشتیبانی از سرویس‌های تصویری در استاندارد H.323 به طور اختیاری تعریف شده است، بنابراین پشتیبانی از کد کننده‌های تصویری نیز اختیاری خواهد بود، پایانه‌های H.323 ارائه دهنده سرویس‌های تصویری بایستی از استانداردهای H.261 و H.263 برای کدکردن پشتیبانی نمایند.

پروتکل Q.931 یا H.225

پروتکل Q.931 که به نام H.225 نیز معروف است و برای برقراری اتصال بین نقاط انتهایی H.323 (پایانه‌ها و گیت وی ها) مورد استفاده قرار می‌گیرد.

پروتکلDNS

از کلمات Domain Name System اقتباس و یک پروتکل شناخته شده در عرصه شبکه‌های کامپیوتری خصوصاً اینترنت است. از پروتکل فوق به منظور ترجمه اسامی کامپیوترهای میزبان و دامنه به آدرس‌های IPاستفاده می‌گردد.

تاریخچه‌ی DNS

DNS، زمانی که اینترنت تا به این اندازه گسترش پیدا نکرده بود و صرفاً در حد و اندازه یک شبکه کوچک بود، استفاده می‌گردید. در آن زمان، اسامی کامپیوترهای میزبان به صورت دستی در فایلی با نام HOSTS درج می‌گردید. فایل فوق بر روی یک سرویس‌دهنده مرکزی قرار می‌گرفت. هر سایت و یا کامپیوتر که نیازمند ترجمه‌ی اسامی کامپیوترهای میزبان بود، می‌بایست از فایل فوق استفاده می‌نمود. همزمان با گسترش اینترنت و افزایش تعداد کامپیوترهای میزبان، حجم فایل فوق نیز افزایش و امکان استفاده از آن با مشکل مواجه گردید (افزایش ترافیک شبکه). با توجه به مسائل فوق، در سال ۱۹۸۴تکنولوژیDNSمعرفی گردید.

DNS، یک «بانک اطلاعاتی توزیع شده» است که بر روی ماشین‌های متعددی مستقر می‌شود (مشابه ریشه‌های یک درخت که از ریشه اصلی انشعاب می‌شوند). امروزه اکثر شرکت‌ها و موسسات دارای یک سرویس‌دهنده DNS کوچک در سازمان خود می‌باشند تا این اطمینان ایجاد گردد که کامپیوترها بدون بروز هیچ گونه مشکلی، یکدیگر را پیدا می‌نمایند. در صورتی که از ویندوز ۲۰۰۰ و اکتیو دایرکتوری استفاده می‌نمائید، قطعاً از DNS به منظور ترجمه ی اسامی کامپیوترها به آدرس‌های IP، استفاده می‌شود. شرکت مایکروسافت در ابتدا نسخه‌ی اختصاصی سرویس‌دهنده DNS خود را با نام (WINS Windows Internet Name Service) طراحی و پیاده‌سازی نمود. این سرویس‌دهنده مبتنی بر تکنولوژی‌های قدیمی بود و از پروتکل‌هایی استفاده می‌گردید که هرگز دارای کارایی مشابه DNS نبودند. بنابراین طبیعی بود که شرکت مایکروسافت از WINS فاصله گرفته و به سمت DNS حرکت کند.

پروتکل[1] LDAP

یک پروتکل مبتنی بر شبکه برای دسترسی به سرویس‌های دایرکتوری روی شبکه است. این پروتکل دارای مستندات RFC2251 و RFC3377 است. به علت آن که دایرکتوری‌های موجود روی شبکه یکتا نیستند و هر یک ممکن است براساس یک

[1] Lightweight Directory Access Protocol

سکوی سیستم عاملی و ساختار متفاوت باشند، پروتکل LDAP امکان برقراری ارتباط و مدیریت آن‌ها را فراهم می‌کند.

پروتکل IMAP [۱]

این پروتکل به کاربر اجازه می‌دهد نامه‌های مورد نظر را از سرویس‌دهنده دریافت کند. در حالی که این نامه هنوز روی سرور باقی مانده است.

پروتکل HTTP[۲]

یکی از متداول‌ترین پروتکل‌های لایه‌ی کاربردی است که مسئولیت ارتباط بین سرویس گیرندگان و سرویس دهندگان وب را برعهده دارد.

پروتکل SMTP [۳]

پروتکل ساده و در عین حال مهم و اساسی برای انتقال ایمیل است. این اصطلاح از آن رو به کار می‌رود که نسبت به سایر پروتکل‌های ایمیل قبلی بسیار ساده عمل می‌کند SMTP. فقط به نام کاربری و دامنه نیاز دارد تا مستقیم پیغام را به سمت گیرنده مسیریابی کند. SMTPیک پروتکل ارسال است و برای دریافت مناسب به همین دلیل برای دریافت ایمیل به جای SMTP از پروتکل‌های دریافت ایمیل مثل IMAP و POP3استفاده می‌شود.

پروتکل FTP [۴]

یکی از ضروری‌ترین کارهایی که اغلب کاربران در شبکه به آن نیاز دارند انتقال فایل است TCP/IP . مستقیماً دارای سرویسی است که انتقال فایل را به راحتی بین ماشین‌های مختلف و سخت‌افزارهای متنوع و سیستم عامل‌های گوناگون امکان‌پذیر می‌سازد و آن FTP است.

---

[1] Internet Message Access Protocol
[2] Hyper Text Transfer Protocol
[3] Simple Mail Transfer Protocol
[4] File Transfer Protocol

پروتکل SSH

پروتکل SSH ابزاری برای مدیریت و دسترسی به شبکه از راه دور است. این پروتکل، داده‌ها را به صورت رمز شده میان دو میزبان انتقال می‌دهد. پروتکل SSH ابتدا برای سیستم‌های عامل یونیک و لینوکس ساخته شد تا جایگزینی برای TelNEt و دیگر ابزارهای ناامن راه دور باشد.

پروتکل NetBios

این پروتکل از جمله پروتکل‌های بسیار متداول است. از این پروتکل برای یافتن گره‌های شبکه براساس نام آن استفاده می‌شود. این پروتکل از سیستم نام گذاری (Naming System)کمک می‌گیرد.

پروتکل RADIUS

برگرفته شده از Remote Authentication Dial-In User Service، استانداردی برای طراحی و پیاده‌سازی سرویس دهندگانی است که مسئولیت تایید و مدیریت کاربران را برعهده خواهند گرفت. مشخصات و نحوه‌ی عملکرد پروتکل RADIUSدر RFC 2865 و RFC 2866 تعریف شده است.

پروتکل SOAP

پروتکل ارتباطی وب سرویس براساسXML می‌باشد. یکی از ویژگی های SOAP نحوه‌ی تشریح نمایش داده های کاربردها در قالب XML و نحوه انجام فراخوانی روال های راه دور(RPC) می‌باشد. بدین صورت که یک پیام SOAP (شامل فراخوانی یک تابع و ارسال پارامترها به آن تابع) از سمت کاربر ارسال می‌گردد و سرویس‌دهنده در پاسخ به این پیام با اجرای آن تابع نتیجه بدست آمده را در قالب یک پیام SOAP دیگر باز می گرداند.

پروتکل RAS

پروتکل RAS بخشی از توصیه نامه H.323 بوده و پروتکلی است که از آن بین نقاط انتهایی (پایانه‌ها و گیت وی ها) و GateKeeper استفاده می‌شود. کانال RAS

قبل از هر کانال دیگری باز می‌شود و مستقل از کانال برقراری مکالمه و انتقال رسانه است. RAS از درگاه 1719 – UDP استفاده می‌نماید. گیت وی‌ها از دو روش زیر برای شناسایی GateKepper استفاده می‌کنند:

الف. شناسایی Unicast:

در این روش از درگاه 1718 – UDP استفاده می‌شود و نقاط انتهایی با آدرس Gate Keeper , IP پیکربندی می‌شوند و می‌توانند فوراً ثبت شوند.

ب. شناسایی به صورت Multicast

این روش از آدرس Multicast برابر 224. 0. 1. 41 استفاده می‌کند، چون نقاط پایانی نیازی به پیکربندی به صورت ایستا ندارند، بنابراین سریع تر است.

پروتکل DHCP

یک پروتکل که در سخت‌افزارهای موجود در شبکه به کاربرده شده و برای عملیات در پروتکل اینترنت ضروری است. این پروتکل حجم فعالیت مدیریت سیستم را کاهش داده و به سخت‌افزارهای موجود در شبکه اجازه داده شده که به صورت دستی تنظیم گردند.

پروتکلBitTorrent

BitTorrent پروتکلی است که به منظور ارسال فایل طراحی شده است. در واقع نوعی ارتباطpeer-to-peer می‌باشد که کاربران مستقیماً به یکدیگر متصل می‌شوند و به ارسال و دریافت قسمتی از فایل می‌پردازند. گر چه فعالیت‌های تمامی کاربران توسط یک سرور مرکزی به نام Tracker هماهنگ می‌شود، اما این سرور از محتویات فایل‌هایی که منتقل می‌شود بی اطلاع است.

پروتکلSNMP(Simple Network Management Protocol)

یکی از مسایل مهمی که هر Administrator در شبکه‌های متوسط و بزرگ با آن مواجه است، مدیریت شبکه به شکل جامع و تا حد امکان یکپارچه است.

پروتکل NNPT(Network News Transfer Protocol)

سرویس دسترسی به گروه‌های خبری(News Groups) ، به زبان ساده NNTP سرویسی است برای دسترسی به اطلاعاتی که توسط افراد مختلف ارسال شده و به طور مشترک مورد استفاده قرار می‌گیرد.

پروتکل TFTP(Trivial File Transfer Protocol, a simple file transfer protocol)

T.F.T.P یک پروتکل ساده انتقال فایل است. این پروتکل اولین بار در سال ۱۹۸۰ معرفی شده و روی پورت ۶۹ کار می‌کند.

پروتکل RTP (Real-time Transport Protocol)

پروتکل RTP یا پروتکل انتقال بلادرنگ همان طور که از نام آن معلوم است برای حمل سرویس‌هایی که تأخیر زمانی در ارسال آن‌ها نقش حیاتی ایفاد می‌کند، به کار گرفته می‌شود. پروتکل RTP برای پشتیبانی از حمل صوت و تصویر به صورت بلادرنگ به صورت استاندارد درآمده و در لایه‌ی انتقال نیز، معمولاً از پروتکل UDP استفاده می‌کند. این پروتکل با مشخص نمودن نوع Pay load در سرآیند خود می‌تواند اولویت‌دهی به بسته‌ها را به کار گرفته و برای ترتیب رسیدن بسته‌ها به مقصد نیز از شماره‌ی سریال اختصاصی به هر سرویس بهره مند شود. همچنین با اختصاص زمان در بسته‌ها به صورت Time Stamping و رعایت این پارامتر در مسیردهی بین گره ها، ارسال بسته‌ها را بین مبدأ و مقصد کنترل نماید.

RTP خودش به تنهایی در خصوص موضوعات مربوط به کیفیت محموله‌ی بلادرنگ کاری انجام نمی‌دهد و به سادگی اطلاعات کافی برای لایه‌ی بالاتر کاربرد تهیه می‌نماید، تا تصمیم معقولی در خصوص این که چگونه امکان حمل دیتا در تراز کیفی موردنظر انجام‌پذیر باشد، اتخاذ شود. پروتکل RTP یکی از مهم‌ترین و اساسی‌ترین پروتکل‌ها در شبکه‌های نسل بعد می‌باشند و علاوه بر UDP از پروتکل‌های دیگری نیز در لایه‌ی انتقال می‌تواند استفاده نماید.

RTP قابلیت رزرو آدرس‌ها را ندارد و Qos را نیز تضمین نمی‌کند. این پروتکل برای نظارت بر ارسال صحیح اطلاعات به خصوص در شبکه‌های چند پخشی بزرگ است.

RTP و RTCP به گونه‌ای طراحی شده اند که از شبکه‌ی انتقال و لایه‌های شبکه مستقل هستند. شکل زیر ساختار کلی RTP را نشان می‌دهد. وظایف RTP عبارت اند از:

۱. جمع آوری اطلاعات در مورد نوع رسانه (Media)
۲. جمع آوری اطلاعات در مورد تعداد مکالمات
۳. جمع آوری اطلاعات در مورد شناسایی ارسال کننده
۴. هم زمانی
۵. آشکارسازی تلفات
۶. تکه تکه‌کردن اطلاعات و جمع آوری مجدد آن‌ها
۷. امنیت و رمز نگاری

پروتکل RTCP

این پروتکل، مکمل پروتکل RTP بوده و وظیفه‌ی تأمین سرویس‌های کنترلی را بر روی گره‌های موجود در داخل شبکه به عهده دارد. این کار با برقراری ارتباط با گره‌ها و آگاهی از کیفیت انتقال در آن‌ها انجام می‌گیرد. با استفاده از این پروتکل اطلاعات مورد نیاز جهت ایجاد هم زمانی بین صوت و تصویر در پایانه‌های بین مسیر مهیا می‌شود.

این پروتکل بسته‌های اطلاعاتی را به صورت دوره‌ای به تمامی شرکت کنندگان در جلسات دقیقاً با مکانیزم ارسال اطلاعات، ارسال می‌کند. وظایف مهم این پروتکل عبارت اند از:

۱. جداکردن بسته‌های متناسب با شماره‌ی درگاه
۲. تبادل اطلاعات در مورد تلفات و تأخیرها بین دو نقطه‌ی پایانی
۳. امکان ارسال بسته‌ها با فاصله بر اساس شماره سیستم پایانی و پهنای باند موجود

گزارش‌های ارسالی توسط این پروتکل شامل اطلاعات زیر است:

اطلاعات در مورد اطلاعات ارسالی و هم زمانی می‌باشد.

۱. دریافتی شامل اطلاعاتی در مورد اطلاعات دریافتی، تلفات، Jitter و گزارش‌های تأخیر
۲. شرح منابع
۳. اسم، ایمیل، شماره تلفن و شناسایی

۶. ۲. پروتکل‌های لایه جلسه

پروتکل SMB

مخفف Server Message Block بوده و پروتکلی برای اشتراک فایل، چاپگر و در بعضی مواقع اشتراک پورت‌های com است. SMB یک پروتکل مهم در لایه کاربرد است. SMB یک پروتکل سرویس‌گیرنده/دهنده و درخواست/پاسخ است و منظور از سرویس‌گیرنده/ دهنده این است که یک ماشین منابع را به اشتراک می‌گذارد (سرویس‌دهنده) و ماشینی دیگر از منابع اشتراکی استفاده می‌کند (سرویس‌گیرنده) و منظور از درخواست/پاسخ این است که سرویس‌گیرنده یک درخواست به سرویس‌دهنده ارسال می‌کند و سرویس‌دهنده پس از بررسی درخواست پاسخ مناسب را برای سرویس‌گیرنده ارسال می‌کند.

P9: Distributed file system protocol developed originally as part of Plan9

سیستم پرونده روشی برای ذخیره و سازمان‌دهی پرونده‌های رایانه‌ای و داده هایشان است تا یافتن و دسترسی به آن‌ها را آسان کند. سیستم‌های پرونده می‌توانند از یک وسیله‌ی ذخیره‌ی اطلاعات مانند دیسک سخت یا سی دی رام استفاده کنند و مکان فیزیکی پرونده‌ها را نگهداری کنند و می‌توانند دسترسی به داده‌های یک پرونده‌ی خادم (سرور) را با رفتار به عنوان مشتری (کلاینت) برای یک پروتکل شبکه (مانند: کلاینت‌های NFS، SMBیا P9) فراهم کنند یا ممکن است مجازی باشند و تنها به عنوان روشی برای دسترسی به داده‌های مجازی (مانندprocfs :)وجود داشته باشند. این با خدمات دایرکتوری و رجیستری متفاوت است.

در شکل رسمی تر، یک سیستم پرونده یک پایگاه داده تک منظوره برای ذخیره، سازمان دهی، دستکاری و بازیابی داده‌ها است.

۶. ۳. پروتکل‌های لایه انتقال

پروتکل TCP

یکی از پروتکل‌های استاندارد TCP/IP است که امکان توزیع و عرضه

اطلاعات(سرویس ها) بین صرفاً دو کامپیوتر، با ضریب اعتماد بالا را فراهم می‌نماید چنین ارتباطی(صرفاً بین دو نقطه)،Unicastنامیده می‌شود.
در ارتباطات با رویکرد اتصال گرا، می‌بایست قبل از ارسال داده، ارتباط بین دو کامپیوتر برقرارگردد پس از برقراری ارتباط، امکان ارسال اطلاعات برای صرفاً اتصال ایجاد شده، فراهم می‌گردد.
ارتباطات از این نوع،بسیار مطمئن می‌باشند، علت این امر به تضمین توزیع اطلاعات برای مقصد مورد نظر برمی گردد.

پروتکل UDP[1]

پروتکلی در سطح لایه‌ی «حمل» بوده که برنامه مقصد در شبکه را مشخص نموده و از نوع بدون اتصال است. این پروتکل، امکان توزیع اطلاعات با سرعت مناسب را ارائه ولی در رابطه با تضمین صحت ارسال اطلاعات، سطح مطلوبی از اطمینان را به وجود نمی آورد.

پروتکلSPX

این پروتکل توسط شرکت ناول(Novell)عرضه شده و روشی قابل اطمینان برای انتقال داده‌ها ارائه می‌کند. این پروتکل برای بررسی انتقال صحیح داده ها، محاسباتی بر روی داده‌ها در کامپیوتر مبدأ و مقصد انجام می‌دهد. برای یک فرآیند انتقال صحیح مقادیر محاسبه شده در کامپیوتر مبدا قبل از ارسال باید با مقادیر محاسبه شده در کامپیوتر مقصد پس از دریافت داده ها، یکسان باشد. SPX قابلیت ردیابی انتقال صحیح داده‌ها را نیز دارد.

پروتکل GRE

GRE برگرفته شده ازGeneric Routing Encapsulation می‌باشد. این پروتکل توسط سیسکو برای حمل بسته‌ها داخل یک بسته دیگر ارائه شد. کافی است دو سمتی که GRE با هم صحبت می‌کنند؛ به هم مسیر داشته باشند، شبکه داخلی هر یک از این دو به یکدیگر متصل می‌شود.

[1] User Datagram Protocol

۴. ۶. پروتکل‌های مبتنی بر رقابت (contention-based)

در پروتکل‌های مبتنی بر رقابت نودها می‌توانند در هر لحظه تصادفی یک ارسال را شروع کنند و باید برای کانال با یکدیگر رقابت کنند. مسئله مهم در پروتکل‌های مبتنی بر رقابت کاهش مصرف انرژی ناشی از برخوردها، overhearing و گوش‌کردن غیر فعال است. پروتکل‌های CSMA/CA به طرز مؤثری مشکل برخورد را حل می‌کنند و برای جلوگیری از مقدار زیادی سربار[1] (یعنی خاموش کردن رادیو در زمان ارسال دیگری) می‌توانند به کار روند.

پروتکل‌های زمان‌بندی شده (Slotted)

سه پروتکل زمان‌بندی شده موجود (S-MAC, T-MAC , DMAC) هر سه از پروتکل‌های قدیمی مبتنی بر رقابت استخراج شده اند. این پروتکل‌ها سربارهٔ ذاتی ناشی از گوش‌کردن غیر فعال را با سنکرون کردن نودها و ایجاد یک چرخه کاری در هر بازه زمانی، جبران می‌کنند. در شروع هر بازه زمانی، همه نودها بیدار می‌شوند و هر نودی که بخواهد پیامی ارسال کند، باید برای کانال رقابت کند. این رفتار سنکرونیزه شده احتمال برخورد را در مقایسه با ساختار تصادفی پروتکل‌های CSMA بهینه شده از نظر انرژی که در بخش قبل به آنها اشاره شد، افزایش می‌دهد. برای جبران سربار ناشی از افزایش برخورد، S-MAC و T-MAC دارای سیگنال‌های RTS / CTS می‌باشند، اما DMAC این کار را بدون در نظر گرفتن سربار ایجاد شده انجام می‌دهد. این سه پروتکل زمان‌بندی شده همچنین در تصمیم گیری در زمان سوییچ کردن بعد از حالت فعال به حالت خواب، متفاوت می‌باشند.

پروتکل‌های مبتنی بر TDMA

TDMA یک contention-less MAC Scheme می‌باشد که در آن نودهای مختلف در بازه‌های مختلف زمانی به محیط دسترسی پیدا می‌کنند. بزرگترین مزیت TDMA بر دیگر MAC Schemeها توانایی آن در خاموش کردن یک نود در بیشتر

[1] Overhearing

اوقات می‌باشد و تنها در بازه‌های زمانی مشخص شده آن را روشن می‌کند. در نتیجه، زمان گوش کردن غیر فعال نیز به صورت قابل توجهی کم می‌شود. بزرگترین نیازی که در مورد TDMA وجود دارد احتیاج به سنکرونیزاسیون زمانی می‌باشد.

پروتکل‌های MAC که بر اساس self-organizing (خود آرایش) می‌باشند (پروتکل‌های SMACS)، بر اساس TDMA استوار می‌باشند که مشکل سنکرون بودن تمام نودها را با تقسیم نودها به زیر شبکه‌ها و سنکرون ساختن آنها تنها در یک زیر شبکه حل کرده‌اند. برای توانا ساختن نودهای متحرک یا نودهای جدید برای تولید ارتباط جدید، نودهای ساکن پیام‌های BI (Broadcast Interval) را در زمانهای نسبتاً منظم منتشر می‌کنند و به پاسخ نودهای متحرک یا نودهای جدید گوش می‌کنند. نودهای متحرک که به صورت منظم کانال را کنترل می‌کنند، به راحتی این پیام را می‌شنوند و تنها در صورتی که ارتباط جدید مورد نیاز باشد، پاسخ می‌دهند.

نکته‌ی قابل توجه در مورد پروتکل‌های TDMA طراحی شده کنونی آن است که این پروتکل‌ها برای ذخیره انرژی نودهای ساکن طراحی شده است، زیرا فرض می‌شود نودهای متحرک میزان زیادی انرژی دارند. در نتیجه وقتی نودهای متحرک ساکن هستند، نمی‌توانند مانند دیگر نودهای ساکن برای حفظ انرژی کار کنند زیرا نودهای متحرک زمان‌بندی متفاوتی از نودهای ساکن دارند. لذا این پروتکل‌ها در مواردی که نودهای متحرک هم انرژی محدود دارند، نمی‌تواند به کار برود.

از مهمترین ویژگی‌های یک پروتکل TDMA که آن را از دیگر پروتکل‌ها متمایز می‌کند، یکی آن است که این پروتکل‌ها به صورت ذاتی برخورد ندارند و دیگر آن که در این پروتکل‌ها گوش‌کردن غیر فعال می‌تواند حذف شود زیرا نودها از پیش می‌دانند که چه زمانی انتظار داده‌ی آمده را داشته باشند. در زیر به طور خلاصه به تشریح روش‌های مختلفی که در پروتکل‌های مبتنی بر زمان‌بندی مورد استفاده قرار می‌گیرند می‌پردازیم.

الف. جدول‌بندی براساس Sink (Sink-based Scheduling)

در این روش کل شبکه به clusterهای بزرگی تقسیم‌بندی می‌شود، به گونه‌ای که در آن ترافیک multi-hop ممکن می‌باشد. ترافیک موجود در هر cluster با یک نود sink

که به شبکه زمینه با اتصال سیمی متصل است و لذا به منابع زیادی مجهز است، جدول‌بندی می‌شود. در اینجا هدف بهینه کردن عمر شبکه می‌باشد و لذا sink در هنگام تصمیم گیری اینکه کدام نود باید حس کند، کدام نود باید بفرستد و کدام نود باید بخوابد، سطح انرژی هر نود را در نظر می‌گیرد. جدول زمان‌بندی TDMA به صورت پریودیک عوض می‌شود تا با تغییرات تطبیق یابد. این امر ایجاب می‌کند که همه نودها بتوانند به صورت مستقیم با نود sink ارتباط برقرار کنند (در ماکزیمم توان ارسالی)، که این مسا له مقیاس‌پذیری شبکه را محدود می‌کند. به علاوه، طول فریم TDMA ثابت می‌باشد، بنابراین قبل از اجرا باید تعداد نودها معلوم باشد.

ب. جدول‌بندی استاتیک static scheduling))

پروتکل SS-TDMA (self stabilizing) که بر اساس این روش عمل می‌کند، در تمام طول عمر شبکه از یک جدول ثابت استفاده می‌کند، که به طور کامل نیاز به یک کنترل کننده جدول مرکزی را از بین می‌برد. SS-TDMA در توپولوژی منظم مثل شبکه‌های مربعی یا شش ضلعی عمل کرده و ترافیک را در تمام شبکه سنکرون می‌کند. تمام سطرهای زوج پیام را به سمت با لا، تمام سطرهای فرد پیام را به سمت پایین ارسال می‌کنند. **می‌توان** نشان داد چنین جداول استاتیکی می‌توانند باعث کارایی قابل قبولی برای روش‌های ارتباطی معمول (broadcast، convergecast و Localgossip) شود، اما محدودیت آنها در محل نودها این روش را در بسیاری از سناریوها غیرعملی می‌سازد.

ج. وظایف گردان ((Rotating duties

هنگامی که چگالی نودها بالاست، هزینه‌ی سرویس دادن توسط یک نود مرکزی می‌تواند بین یک تعداد نود با چرخاندن این وظیفه بین آنها تقسیم شود. پروتکل PACT از clusterبندی غیرفعال برای تقسیم‌بندی شبکه به تعدادی cluster که با نودهای مرزی به هم متصل شده اند، استفاده می‌کند. چرخیدن و تغییر مدیران و نودهای مرزی cluster، براساس اطلاعاتی است که روی پیام‌های کنترلی مبادله شونده در فاز کنترل ترافیک جدول TDMA، سوار شده اند. پروتکل BMA از روش موجود

در LEACH برای مدیریت شکل‌دهی و چرخش clusterها استفاده می‌کند. در شروع یک فریم TDMA، هر نود یک بیت اطلاعات به مدیر cluster خود broadcast می‌کند که اعلام می‌کند که آیا داده‌ای برای ارسال دارد یا نه. براساس این اطلاعات مدیر cluster تعداد slotهای داده مورد نیاز و نوع slotها را تعیین و آن را به تمام نودهای تحت کنترل broadcast می‌کند. نکته مورد توجه این است که علائم ترافیک به صورت بیتی نیاز به هم زمانی بسیار دقیق بین نودهای یک cluster دارند.

د. جدول‌بندی تقسیم شده (partitioned scheduling):

در پروتکل EMACS وظایف جدول‌بندی براساس شماره‌ی slot تقسیم می‌شود. هر slot به عنوان یک مینی فریم TDMA عمل می‌کند و شامل یک فاز رقابت، یک قسمت کنترل ترافیک و یک قسمت داده می‌باشد. یک نود فعال که مالک یک slot می‌باشد، همیشه در slot خودش ارسال می‌کند. بنابراین، یک نود n از آنجا که ممکن است گیرنده داده هر یک از همسایه هایش باشد، باید به قسمت‌های کنترل ترافیک تمام آنها گوش کند. فاز رقابت برای سرویس دادن به نودهای غیر فعال که مالک هیچ slotای نیستند، قرار داده شده است. ایده این است که تنها بعضی از نودها باید فعال باشند تا یک شبکه backbone تشکیل دهند که این شبکه آماده استفاده توسط نودهای غیر فعال در زمانی که آنها رویدادی را دریافت می‌کنند، باشد. در بسیاری از سناریوها، رویدادها به ندرت اتفاق می‌افتند، لذا انرژی مصرف شده در گوش کردن برای در خواست، منبع اصلی سرباره را تشکیل می‌دهد. لذا پروتکل LMAC شامل بازه رقابت نمی باشد. در مقایسه با دیگر پروتکل‌های TDMA-based، هر دو پروتکل EMACS و LMAC دارای مزیت کنترل کردن حرکت نودها می‌باشند که به وضوح زمینه‌های کاربرد آنها را زیاد می‌کند.

جدول‌بندی تقسیم شده و تکرار شده بیشتر به پروتکل‌های slotted ومبتنی بر رقابت از آن جهت که نودها مستقل عمل می‌کنند، شبیه می‌باشد که باعث می‌شود نصب و عملکرد آنها آسان و در مقابل از بین رفتن نودها مقاوم باشند.

هـ کپی کردن و تکرار جدول (Replicated Scheduling):

ایده مورد استفاده در TRAMA این است که فرآیند جدول‌بندی در تمام نودهای یک شبکه تکرار شود. نودها به طور منظم اطلاعات ترافیک‌های طولانی مدت route شده از آنها و نیز ویژگی‌های همسایه‌های با فاصله یک hop را broadcast می‌کنند. این باعث می‌شود هر نودی درباره درخواست‌های همسایه‌های با فاصله یک hop و ویژگی همسایه‌های با فاصله دو hop آگاه شود. این اطلاعات برای تعیین نوع slotها با هدف جلوگیری از برخورد، توسط تابعی که برنده (فرستنده) را در هر slot براساس مشخصه نود و شماره slot محاسبه می‌کند، کافی می‌باشد. در هنگام اجرا، جدول می‌تواند با توجه به ترافیک موجود تطبیق داده شود و لذا نودهای با ترافیک کم slot هایشان را برای بقیه فریم آزاد کنند تا توسط نودهای دیگر استفاده شود. گرچه TRAMA استفاده بهینه از کانال (high channel utilization) به عمل می‌آورد، اما این عمل را به ازاء تأخیر زیاد و پیچیدگی الگوریتم انجام می‌دهد.

۵. ۶. پروتکل‌های لایه شبکه

پروتکلIPv4

IPv4 یا IP از پایه‌های پروتکل ارتباطیTCP/IP می‌باشد که برای انتقال بسته‌های داده، صوت و تصویر از طریق اینترنت استفاده می‌شود. IPV6 پروتکل نسل آینده شبکه‌های کامپیوتری می‌باشد که برای جایگزین شدن پروتکل فعلی استاندارد شده است.

پروتکلIPv6

مخفف عبارت Internet Protocol Version 6 یا نگارش ۶ پروتکل اینترنت، پروتکل نسل بعدی برای اینترنت هست که توسط IETF or Internet Engineering Task Forceبه منظور جایگزین نمودن نگارش جاری پروتکل اینترنت IPv4طراحی شده است.

پروتکل H.450

سیستم معماری خدمات تکمیلی H.450 از یک عملکرد مرکزی تا جای ممکن استفاده می‌کند. واحدهای مشابه به طور مستقیم با استفاده از سیگنال H.450 بدون دارا بودن کنترل شبکه مرکزی ارتباط برقرار می‌کنند. برای این مشخصه‌ها که به کنترل مرکزی نیاز دارند، یک سرویس‌دهنده مشخصه استفاده می‌گردد که شکل خاصی از یک نقطه پایانی M. 323/H.450 می‌باشد.

پروتکل RSVP

RSVP به منظور کاهش تأخیر، و افزایش QOS در VoIP از سوی IETF معرفی شده است. RSVP ترافیک رشته‌های IP را اولویت‌بندی کرده و شبکه‌های IP را قادر می‌سازد، صوت را با همان کیفیت سوییچ‌های دیجیتال منتقل کنند. به عبارتی دیگر با پیدایش RSVP، VOIP به واقعیت پیوسته است.

با فعال‌کردن پروتکل RSVP می‌توان ارتباطات صوتی را با تأخیر قابل قبول بر روی شبکه‌ی دیتا منتقل کرد. RSVP یک پروتکل مسیریابی نیست ولی برای کار با پروتکل‌های مسیریابی تک پخشی وچند پخشی طراحی شده است. RSVP دارای خصوصیات زیر است:

۱. جهت آن به سمت گیرنده است.

۲. از تک پخشی و چند پخشی پشتیبانی می‌کند.

۳. می توان این پروتکل را از مسیریاب‌هایی که این پروتکل را پردازش نمی‌کنند عبور داد.

۴. برنامه‌های کاربردی می‌توانند با استفاده از این پروتکل و به منظور بالا بردن QOS از پهنای باند به صورت پویا استفاده کنند.

پروتکل SDP

این پروتکل نیز مانند SIP مبتنی بر متن است و در هر سطر خود خصوصیاتی از جلسه و رسانه‌ی قابل انتقال در جلسه را مشخص می‌کند. شروع کننده‌ی جلسه ابتدا خصوصیات رسانه‌های مورد نظر در جلسه را به طرف مقابل ارسال می‌دارد، طرف مقابل

یا از بین توصیفات ارسالی شروع کننده مکالمه تعدادی را انتخاب می‌نماید و یا قابلیت‌های پیشنهادی را رد می‌کند، در هر صورت توافق و یا عدم توافق پس از دو یا چند بار ار سال بدنه‌ی پیغام، قابلیت‌های مورد قبول دو طرف مشخص می‌گردد. در RFC2327 ساختار پیغام‌ها در SDP توضیح داده شده است.

پروتکل BGP

BGP پروتکل مسیریابی در شبکه یا گروهی از شبکه‌ها که دارای خط مشی یکسان هستند، است. وظیفه‌ی BGP تبادل اطلاعات مسیریابی در اینترنت است و بین ISPها استفاده می‌شود، ولی شبکه‌های تجاری و یا دانشگاه‌ها معمولاً از پروتکل داخلی IGP نظیر RIP یا OSPF برای مسیریابی درون شبکه استفاده می‌کنند. اگر از این پروتکل برای ارتباط بین دو شبکه استفاده شود به آن EBGP و اگر در داخل یک شبکه استفاده شود به آن IBGP می‌گویند.

BGP یکی از پروتکل‌های قدرتمند با قابلیت مقیاس‌پذیری بالا است و به همین دلیل برای مسیریابی در شبکه‌ی اینترنت استفاده می‌شود. پایگاه داده‌های مسیریابی BGP در حال حاضر دارای بیش از ۹۰۰۰۰ مسیر است. به منظور تعیین سیاست و مدیریت مسیرها برای هر یک از این رکوردها پارامترهای مختلفی تعریف شده است.

پروتکل DiffServ

Diffservها بر خلاف IntServ ترافیک شبکه را به کلاس‌های مختلف دسته‌بندی می‌کنند و به هر کلاس (COS) پارامترهای QoS را نسبت می‌دهند، در صورتی که IntServ با کنترل تمام اجزای شبکه، Qos بالا را به صورت End – To – End ارائه می‌دهند. Intserv بر مبنای RSVP و به منظور نگهداری QoS در سطح دلخواه برای تمام بسته‌های مبادله شده در شبکه است. Diffserv از طریق یک الگوی شش بیتی که به اول بسته‌های اطلاعاتی اضافه می‌شوند، نوع سرویس را مشخص می‌کنند.

بسته‌های اطلاعاتی در هر یک از اجزای شبکه دسته‌بندی شده و با روش‌های خاصی موسوم به PHP ارسال می‌شوند. این روش‌ها پهنای باند، حد تأخیر و حد Jitter بسته‌ها را مشخص می‌کنند، تلفیق علامت‌گذاری بسته‌ها و تعریف درست PHP موجب می‌شود،

که کلیه‌ی بسته‌ها و برنامه‌های کاربردی با QOS مناسب ارسال شوند. بنابراین DiffServ سیگنالینگ برای QOS حذف شده و تعداد حالت‌های مورد نیاز برای هر جز شبکه کاهش می‌یابد.

پروتکل EGP (ExteriorGatewayProtocol)

EGPمسیرها را بین AS های مختلف توزیع می‌کند وروترها را در درون یک AS برای انتخاب بهترین مسیر برای خروج از AS جهت دیتایی که نیاز مبرم به مسیردهی دارند قادر می‌سازد.

پروتکل AS

اینترنت به منظور عملیات مسیریابی به سیستم‌های مستقلی به نام AUTONOMOUS SYSTEM: AS تقسیم‌بندی می‌شود. یک AS یک گروه از روترهایی می‌باشد که تحت کنترل یک مدیریت واحد بوده و از یک پروتکل مسیریابی مشترک استفاده می‌کنند.

پروتکل IGRP [1]

IGRPبرگرفته شده از (Interior Gateway Routing Protocol) یکی از پروتکل روتینگ distance-vector طراحی شده توسط شرکت سیسکو است. این بدان معنی است در صورت استفاده از پروتکل فوق در یک شبکه، می‌بایست تمامی روترها از نوع سیسکو باشند. شرکت سیسکو هدف از ایجاد پروتکل IGRP را غلبه بر برخی محدودیت‌های پروتکلRIP عنوان کرده است.

پروتکل EIGRP

پروتکل EIGRP دارای مجموعه، پتانسیل‌هایی است که آن را با سایر پروتکل‌های روتینگ نظیر IGRP کاملاً متمایز می‌نماید. برخی از این ویژگی‌ها عبارتند از:

۱. حمایت ازIP ، IPXو AppelTalk از طریقPDM، برگرفته شده از-Protocol Dependent Modules

[1] Interior Gateway Routing Protocol

۲. ارتباط از طریق RTP، برگرفته شده از Reliable Transport Protocol
۳. انتخاب بهترین مسیر از طریق DUAL، برگرفته شده از diffusing update algorithm
۴. حمایت از چندین سیستم خودمختار AS
۵. حمایت از خلاصه‌سازی VLSM، برگرفته شده از Variable Length Subnet Masking

پروتکل IPSec

در پشته‌ی پروتکل TCP/IP هر لایه دارای یک یا چند پروتکل می‌باشد که هر پروتکل وظایف خاص خود را دارد. بر همین اساس جهت ایجاد امنیت در هر لایه بنا به اصول طراحی زیر پروتکل‌ها یک یا چند پروتکل امنیتی تعبیه می‌شود. مطابق اصول طراحی زیر لایه، هر لایه وظیفه‌ای را بر عهده دارد که منحصر بفرد می‌باشد و در هر لایه نیز، هر پروتکل می‌تواند مطابق با قراردادی خاص، عملیات خاصی را بر عهده بگیرد، بر همین اساس امنیت در لایه شبکه بر عهده IPSec است.

۶. ۶. پروتکل لایه پیوند داده

پروتکل CDP

پروتکل CDP برگرفته شده از(Cisco Discovery Protocol)خلاصه اطلاعاتی را در خصوص دستگاه‌هایی که به طور مستقیم متصل شده اند، نمایش می‌دهد و در لایه Data Link کار می‌کند.

اما در پایان لازم می‌دانم که مفهوم RFC را توضیح دهم چون این اصطلاح در متون مربوط به شبکه زیاد استفاده می‌شود.

RFC چیست؟

متون بسیار کامل ولی خشک و سنگین که در مورد مفاهیم مختلف شبکه بحث می‌کنند. این فایل‌ها به صورت متنی و با پسوند txt هستند و به عنوان مرجع (برای مراجعه و نه مطالعه کامل) کاربرد دارند. این فایل‌ها یک بار منتشر شده و هرگز تغییر داده نمی‌شوند (حتی اگر حاوی اشتباه باشند).

ضمیمه الف

امروزه اهمیت شبکه‌های رایانه بر هیچ کس پوشیده نیست. با توجه به مزیت‌های مختلف آنها (کاهش هزینه، صرفه جویی در وقت، حذف محدودیت‌های جغرافیایی و ...)، شاهد پیشرفت روزافزون این شاخه علمی هستیم. به همین دلیل لازم دانستیم اصطلاحات رایج در شبکه را به عنوان ضمیمه در این کتاب بیاوریم.

DTE (Data Terminal Equipment):

منبع و گیرنده داده‌ها را در شبکه‌های رایانه‌ای DTE می‌گویند.

DCE (Data Communication Equipment):

تجهیزاتی که مشخصات الکتریکی داده‌ها را با مشخصات کانال داده‌ها تطبیق می‌دهد مانند مودم.

B.W (Band width):

پهنای باند یا محدوده‌ای که در آن امواج آنالوگ بدون هیچ افتی حرکت می‌کنند.

Noise:

نویز یا پارازیت به امواج الکتریکی مزاحم می‌گویند که موجب اختلال در انتقال داده‌ها می‌شود.

Bps:

سرعت انتقال داده‌ها یا بیت در ثانیه.

Network:
شبکه.

Share:
به اشتراک‌گذاری داده‌ها و منابع سخت‌افزاری برای استفاده همه‌ی کامپیوترهای موجود در شبکه.

Time Sharing:
نوعی شبکه در قدیم که از یک Main Frame به عنوان سرور استفاده می‌کردند.

LAN (Local area network):
شبکه‌های محلی و کوچک.

MAN (Metropolition area network):
شبکه‌های شهری.

WAN (Wide area network):
شبکه‌های گسترده همانند اینترنت.

Node:
به هر کامپیوتر وصل به شبکه Node یا گره می‌گویند.

Server:
سرویس‌دهنده.

Client:
سرویس‌گیرنده.

Peer - to - Peer:
شبکه‌های نظیر به نظیر که در آن هر کامپیوتری هم سرویس‌دهنده است و هم سرویس‌گیرنده.

Server – Based:
شبکه‌هایی بر اساس سرویس‌دهنده که در آن یک یا چند کامپیوتر فقط سرویس‌دهنده و بقیه کامپیوترها سرویس‌گیرنده هستند.

Topology:
توپولوژی به طرح فیزیکی شبکه و نحوه‌ی آرایش رایانه‌ها در کنار یکدیگر توپولوژی می‌گویند.

Collision:
برخورد یا لرزش سیگنال‌ها.

NIC:
کارت شبکه.

Fiber Optic:
کابل فیبر نوری که در برپایی شبکه‌ها به کار می‌رود و سرعت بسیار بالایی (بیش از ۱ گیگا بیت در ثانیه) دارد.

Thinnet:
کابل کواکسیال (هم محور) نازک با پشتیبانی ۱۸۵ متر بدون تقویت کننده.

Thiknet:
کابل کواکسیال (هم محور) ضخیم با پشتیبانی ۵۰۰ متر بدون تقویت کننده.

STP (Shielded T.P):
نوعی کابل زوج به هم تابیده دارای حفاظ می‌باشد.

Rack:
در شبکه‌های T.P. بزرگ برای جلوگیری از اشغال فضای زیاد توسط کابل‌ها مورد استفاده قرار می‌گیرد.

Patch panel:

دستگاهی که بین هاب و کابل قرار می‌گیرد.

RJ45:

فیش‌های مربوط به کابل‌های T.P. هستند.

IRQ:

وقفه.

Base I/O Port:

آدرس پایه ورودی و خروجی.

Base Memory:

آدرس پایه حافظه.

Boot ROM:

قطعه‌ای برای بالا آوردن شبکه‌هایی که در آن هیچ گونه دیسکی برای بالا آوردن نیست (شبکه‌های Disk less)

AP (Access Point):

دستگاهی که یک کامپیوتر بی سیم را به یک شبکه LAN وصل می‌کند.

Cell:

محدوده‌ای را که یک AP تحت پوشش دارد را سلول(Cell) می‌گویند.

Protocol:

پروتکل ها، قوانین و روال‌هایی برای ارتباط هستند و یک شبکه برای برقراری ارتباط از این قوانین استفاده می‌کند.

پروتکل ۸۰۲:
نوعی پروتکل برای اجزای فیزیکی شبکه‌های LAN می‌باشد.

:CSMA/CD
نوعی روش دسترسی به خط با استفاده از روش گوش دادن به خط.

:Token Ring
روش عبور نشانه که در شبکه‌های حلقوی به کار می‌رود، از انواع روش دسترسی به خط است.

:MAU
وسیله‌ای مانند هاب، اما در شبکه‌های حلقوی به کار می‌رود.

:Novell Netware
نوعی سیستم عامل برای شبکه.

:Unix
نوعی سیستم عامل برای شبکه.

:Advanced Server
نوعی سیستم عامل برای شبکه.

:Search Engine
موتور جستجو.

معماری شبکه:
به ترکیبی از استانداردها، پروتکل‌ها و توپولوژی‌ها معماری شبکه می‌گویند.

INDEX

Charging	تامین اعتبارکردن
CODEC	کدک
Call	تماس
COMPRESS	فشرده‌سازی
Circuit-switching	سوییچ مداری
Caller ID	شماره تماس گیرنده
Call Transfer	انتقال تماس
Collision	برخورد
D	
Data Packet	بسته‌های اطلاعاتی
Data link	پیوند داده
Dial-up	اینترنت خانگی
DAC	مبدل دیجیتال به آنالوگ
Decode	دی کد
Dropt Packet	از دست رفتن بسته‌ها
Digital	دیجیتال
Delay	تاخیر
Duration	در طی دوره
E	
End point	نقطه انتهایی
End-to-end	کاربران نهایی، نقاط انتهایی
ETSI	گروه استانداردسازی
End-user	کاربر نهایی-کاربر انتهایی
Echo	اکو
F	
Fax	فکس

G

Gatekeeper	سرور اصلی در H.323
Gateway	مترجم بین پروتکل‌ها
General Switch Telephone Network (GSTN)	سوییچ شبکه تلفن

H

Handset	تلفن دستی
Hand off	دست نزدن-استفاده نکردن
H.323	پروتکل استاندارد ارتباطی
Header	سرآیند

I

Internet layer	لایه اینترنت
IP	بسته‌ای پی
ITU-T	گروه استانداردسازی
IMS	پیام‌های فوری
IP Telephony	تلفن‌ای پی
ISP	سرویس‌دهنده اینترنت
Invite	دعوت برای یک جلسه

J

Jitter	لرزش

L

Layer	لایه
Load	بارگذاری
Laptop	لپ تاپ

M

Mobility	سیار
Media Handling	مدیریت مدیا
MCU	واحد کنترل چند نقطه‌ای

MOIP	موبایل ویپ
Message	پیام
Message header	سرآیند پیام
Message body	بدنه پیام
Method	روش
Monitoring	نگاه‌کردن –بررسی‌کردن
N	
Network	شبکه
Network Topology	توپولوژی شبکه
Network Access Layer	لایه دسترسی شبکه
NGN	شبکه‌های نسل بعد
O	
Origination	رفتن اطلاعات به سرور خارج از کشور
OSI	مدل هفت لایه‌ای شبکه
P	
Physical	فیزیکی
Presentation	ارائه-نمایش
Packet	بسته
PSTN	تلفن معمولی
Protocol	پروتکل
Packet Switching	پکت سوییچ
PBX	مرکز تلفن- پ ب ایکس
Packet Based Transmission	انتقال اطلاعات به صورت بسته‌ای
Phone-to- Phone	ارتباط تلفن با تلفن
Phone-to- PC	ارتباط تلفن با کامپیوتر
Packet Lost	از دست رفتن بسته‌ها
Point-to-Multipoint	ارتباط یک نقطه با چندین نقطه

	Q
QOS	سرویس کیفیت خدمات
	R
Register	ثبت‌کردن
Redirect server	سرور باز گرداننده - سرور غیر مستقیم
Request	درخواست
Responses	پاسخ
Real-time	زمان واقعی
Route	مسیر
Ring	حلقه
	S
Segment	واحد اطلاعات
Server	سرور
Session	جلسه
SIP	پروتکل ارتباطی
Signaling	سیگنالینگ
Soft switch	سوییچ نرم‌افزاری
Star	ستاره
Start line	خط شروع
Speaker	بلند گو
Subject	موضوع
	T
Talker Overlap	روی هم افتادن کلمات
Termination	ورواطلاعات از سرور خارجی به سرور داخلی
TCP/IP	پروتکل اینترنت
Transport	انتقال
Transport Layer	لایه انتقال

U	
UDP	پروتکل انتقال
User Agent Client (UAC)	کاربر
User agent server (UAS)	سرور
Update	به روزرسانی
V	
Version	ورژن
Voice	صدا
VOBB	نام دیگر ویپ
VOIP	ویپ
Video	ویدئو-تصویر
Video conferencing	کنفرانس ویدئویی
W	
Wireless	بی سیم

مراجع

[1]. Content Networking Architecture, Protocols, and Practice; Markus Hofmann and Leland R. Beaumont; Elsevier; 2005.

[2]. Fundamentals of Telecommunications. Roger L. Freeman; John Wiley & Sons, Inc; 1999.

[3]. Introduction to telecommunications network engineering; Tarmo Anttalainen. 2nd ed; ARTECH HOUSE, INC. ; 2003.

[4]. Telecommunications and data communications handbook; Ray Horak; John Wiley & Sons, Inc; 2007.

[5]. The ENCYCLOPEDIA OF NETWORKING; WERNER F EIBEL; Network Press; 1996.

[6]. Next Generation Networks: Perspectives and Potentials; Jingming Li Salina, Pascal Salina; Wily; ISBN: 0470516496; 2008.

[7]. NGN Architectures, Protocols and Services; Toni Janeveski; John Wiley & Sons, Inc. ; 2014.

[8]. Hacking VoIP Protocols, Attacks, and Countermeasures; Himanshu Dwivedi; No Starch Press; ISBN:978-1-59327-163-3; 2008.

[9]. Packet Guide to Voice Over IP; Bruce Hartpence; Publisher O'Reilly Media; ISBN: 978-1-4493-3967-8; 2013.

[۱۰].شبکه‌های نسل بعدNGN(۱۳۸۵) ناقوس اندیشه، حسن جند، بابک احسنت،

[۱۱].شبکه TCP/IP(۱۳۸۲) رایانه سبز، عین الله جعفر نژاد قمی: آموزش joe casad_TCP/IP

[۱۲]. (۱۳۸۳)، مهران گرمه ای، رضا اکبر زاده_

[۱۳]. (۱۳۸۹)، علی اصغر عمیدیان،سید علی علویان،حسن جند_ شبکه‌های نسل جدید انقلابی در صنعت ارتباطات

[14]. http://www.cs.columbia.edu/sip

[15]. http://www.ietf.org