به نام خدا

پدافند غیر عامل باید همچون شعله‌ای بلند شود.

مقام معظم رهبری

پدافند غیر عامل – شبکه های PAP

فهرست

مقدمه

امروزه استفاده از اینترنت با پهنای باند بالا به عنوان یکی از معیارهای توسعه جامعه مدنی شناخته می‌شود و دولت ها سعی می‌کنند در راستای رسیدن به دولت الکترونیکی و استفاده از ابزارهای نوین فناوری حداکثر تلاش خود را مبذول نمایند.

استفاده از سرویس های بی شماری که در سایه دولت الکترونیک به افراد جامعه داده می‌شود، همواره باعث می‌شود که متقاضیان به این گونه سرویس ها افزایش یابند و در سایه افزایش این سرویس ها عملاً امکان پرداخت هزینه های سنگین اینترنتی برای کاربران وجود ندارد و در عین حال اتصال تلفنی به اینترنت نیز باعث کندی بیش از حد سرویس دهی می‌گردد.

در این راستا شرکت های بزرگ ارائه خدمات اختصاصی[۱] در زمینه ارتباطات که در حال حاضر تعداد آنها به یازده می‌رسد، تجهیزات رایانه‌ای و ارتباطی را جهت جذب این گروه از کاربران خریداری کرده و در اکثر مراکز مخابراتی مستقر کرده اند. شبکه های یازده گانه تحت مدیریت شرکت های PAP تدارک و مدیریت ارتباط ADSL[۲] در سطح کشور را به عهده دارند. بسیاری از ادارات، بانک ها، شرکت های خصوصی و منازل شخصی از طریق

---

[۱] . PAP: Private Access Provider

[۲] Asymmetric Digital Subscriber Line

این شبکه ها به یکدیگر و یا به شبکه اینترنت متصل شده اند. در حال حاضر بیش از یکصد هزار پورت با پهنای باندهای مختلف در سطح کشور فعال است و پیش بینی می شود این تعداد به سرعت افزایش یابد. تکنولوژی اطلاعات و ارتباطات و پیشرفت های چشمگیر بوجود آمده در این حوزه باعث شده تا دولت ها را وادار سازد ضمن توسعه و ارتقاء این تکنولوژی، ساز و کار نظارت و امنیت این نوع ارتباطات را در رئوس کارهای خود قرار دهد. به دلیل محدودیت منابع شرکت های خصوصی یازده گانه در سرمایه گذاری، در حال حاضر هیچگونه تدابیر امنیتی خاصی برای محافظت از این شبکه ها لحاظ نشده است و در صورت اختلال در این شبکه ها زیان های شدیدی بوجود خواهد آمد. اهمیت این موضوع با توجه به ضرورت انتقال شبکه های بانکی از زیر ساخت های ارتباطی ماهواره ایی به زیر ساخت کابلی افزایش پیدا می کند. تنها جایگزین شبکه های ماهواره ایی، شبکه های ADSL ایجاد شده توسط شرکت های PAP می باشد. راه حل اصلی در این زمینه ایجاد مرکز کنترل امنیتی اختصاصی خطوط ADSL (با توجه به ماهیت و معماری خاص این سیستم ها) می باشد.

فصل ۱. بررسی تکنولوژی ADSL

به دنبال پیشرفت دانش و فناوری اطلاعات و ارتباطات وگسترش شبکه‌های اطلاع رسانی و اینترنت با پهنای باند وسیع و در نتیجه بروز و ظهور نیازهای ارتباطی و خدمات مخابراتی در جوامع مختلف نیاز به ارسال اخبار، گزارش، پیام، منابع اطلاعاتی و غیره هر چه بیشتر افزایش یافت. بنابراین با ظهور اینترنت و اتصال رایانه‌ها به یکدیگر به صورت یک شبکه جهانی بحث انتقال داده‌ها بین نقاط مختلف جهان در کمترین زمان ممکن مطرح گردیده است. از آنجا که عموم کاربران، خانگی و تجاری بوده و از طرفی توانایی پرداخت هزینه‌های سنگین توسط این گروه ازکاربران وجود ندارد شرکت‌های بزرگ طراح و سازنده تجهیزات رایانه‌ای و ارتباطی جهت جذب این گروه از کاربران همواره به دنبال راه حل های اساسی در جهت طراحی، ساخت و تأمین تجهیزات و ابزارهای مناسب و ارزان قیمت بدون استفاده از زیر ساخت‌های ارتباطی قبلی (سیم مسی) بوده و هستند. لذا این‌گونه شرکت‌ها غالباً به دنبال روش‌هایی بوده‌اند تا بتوان با استفاده از تجهیزات و امکانات موجود و قدیمی خدمات جدید ارتباطی را فراهم ساخت.

بنابراین با توجه به انجام و گسترش کابل کشی تلفن (وجود سیم مسی) از اوایل قرن بیستم تا به حال که تقریباً تمامی منازل، ادارات،

سازمان‌ها و مراکز اجتماعی دارای آن هستند تحقیقات زیادی به منظور استفاده از زوج سیم کابل مسی جهت رسیدن به سرعت‌های بالاتر انتقال اطلاعات صورت گرفت که نتیجه آن تحت عنوان فناوری DSL و ADSL مطرح شد.

در اغلب منازل و ادارات برخی از کشورهای دنیا ، کاربران از یک DSL نامتقارن (ADSL) استفاده می نمایند. تکنولوژی ADSL در واقع نوعی از DSL ها می باشد که ارتباط آن نامتقارن است، یعنی سرعت ارسال داده در ثانیه کمتر از دریافت آن می باشد. تکنولوژی ADSL فرکانس های قابل دسترس دریک خط را تقسیم می نماید تا کاربران اینترنت قادر به دریافت و ارسال اطلاعات باشند.

تکنولوژی ADSL با سایر تکنولوژی های مربوط به دستیابی به اینترنت نظیر مودم های کابلی و اینترنت ماهواره ای رقابت می نماید. بر طبق آمار اخذ شده در سال ۱۹۹۹، بیش از ۳۳۰۰۰۰ منزل در امریکا از ADSL استفاده کرده اند. تعداد کاربران استفاده از مودم های کابلی تا سال ۱۹۹۹ به مرز ۱۳۵۰۰۰۰ کاربر رسیده است. بر این اساس تا اواخر سال ۲۰۰۳، تعداد مشترکین مودم های کابلی به مرز ۸.۹۸۰.۰۰۰ و مشترکین DSL به ۹.۳۰۰.۰۰۰ رسیده اند.

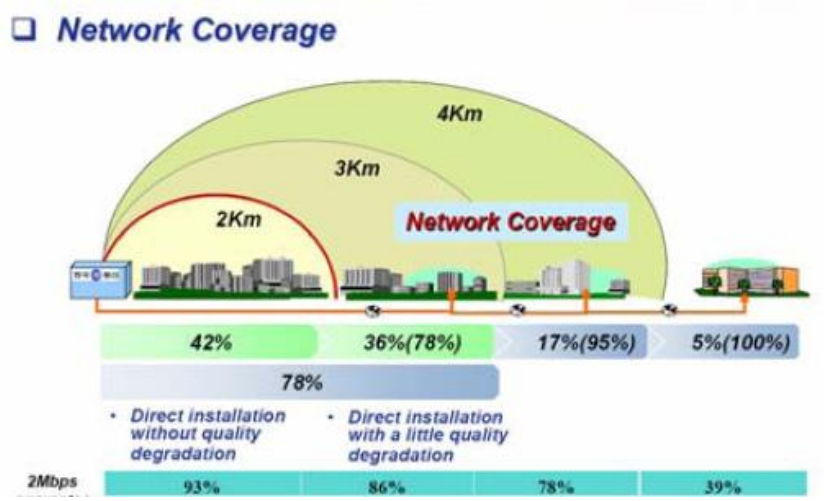
تکنولوژی ADSL پهنای باند ۱.۱ مگاهرتزی خطوط مسی را به کانال های ۴ کیلوهرتزی تقسیم می کند و آخرین کانال را جهت

ارسال صدا و فاکس معمولی تخصیص می دهد و ۲۵۶ کانال دیگر را برای انتقال دو طرفه اطلاعات استفاده می کند. به این ترتیب که ۶۴ کانال را برای خط ارسال اطلاعات و ۱۲۸ کانال دیگر را جهت دریافت اطلاعات استفاده می کند. در بهترین حالت اگر ۱۹۲ کانال ۴ کیلو هرتزی موجود را استفاده کند، در تئوری سرعت باید به حدود ۹ مگابیت در ثانیه برسد. این خطوط از تمامی پهنای موجود در خطوط مسی دوطرفه استفاده می‌کنند تا بالاترین سرعت ممکن در ثانیه را بر خلاف خطوط معمول ارائه دهند. تکنولوژی ADSL همچنین به صورت یک ارتباط دایمی[۱] است به طوری که استفاده کننده قادر می باشد به صورت ۲۴ساعته و ۷ روز هفته از ارتباط با شبکه (اینترنت) بهره مند شود.

ADSL از یک تکنولوژی با نام " تکنولوژی حساس به مسافت " استفاده می نماید. در این تکنولوژی متناسب با افزایش طول خط ارتباطی، کیفیت سیگنال افت و سرعت خط ارتباطی کاهش پیدا می نماید. ADSL دارای محدودیت ۱۸۰۰۰ فوت (۵۴۶۰ متر) است. کاربرانی که در مجاورت و نزدیکی شرکت ارائه دهنده سرویس DSL قرار دارند، دارای کیفیت و سرعت مناسبی بوده و متناسب با افزایش مسافت، کاربران اینترنت از نظر کیفیت و سرعت دچار افت

[۱] Always – on

خواهند شد. تکنولوژی ADSL قادر به ارائه بالاترین سرعت در حالت " از اینترنت به کاربر۱ " تا ۸ مگابیت در ثانیه است . (در چنین حالتی حداکثر مسافت ۶۰۰۰ فوت و یا ۱۸۲۰ متر خواهد بود.) البته سرعت انتقال اطلاعات در محدوده ذکر شده علاوه بر عامل فاصله ارتباطی به نوع سیم استفاده شده نیز، بستگی دارد.



۱. Downstream

فصل ۲. سرویسهای قابل ارائه توسط شرکتهای PAP

شرکت های PAP با توجه به تجهیزات و توپولوژی که برای ارائه خدمات به مشترکین دایر می‌کنند می توانند علاوه بر ارائه خدمات اینترنت پر سرعت سرویس های دیگری مبتنی بر همین بستر ارائه دهند.

یکی از این سرویس ها که تقریبا در تمامی شبکه های PAP عمومیت دارد معروف به سرویس سه گانه شرکت های PAP می باشد. منظور از سرویس‌های سه‌گانه، ارائه اینترنت پرسرعت، تلفن و تلویزیون اینترنتی در قالب یک بسته[۱] به مشترکان است. مسلماً هر یک از این سرویس‌ها، کاربردها و جذابیت‌های خود را دارد که ارائه همه آنها با هم و با قیمت مناسب، بر جذابیت‌های آنها می‌افزاید.

۱. سرویس های ویدئو

به ارسال و پخش برنامه‌های ویدئویی یا تلویزیونی برای مشترکان از طریق زیرساخت باند وسیع و توسط پروتکل اینترنت سرویس تلویزیون اینترنتی یا IP-TV گفته می‌شود. این سرویس معمولاً با

۱. Package

سرویس‌های دیگری مانند ویدئو بر طبق تقاضا و تلفن اینترنتی و اینترنت پرسرعت، در قالب یک"بسته" به مشترکین ارائه می‌شود.

سرویس های ویوئو در قالب سرویس های زیر قابل ارائه است :

❖ ویدئو بر اساس تقاضا[۱]

در سرویس ویدئو بر اساس تقاضا یا VoD، مشترکین بر اساس درخواست به تصاویر مورد نظر دسترسی خواهند داشت.

❖ انتشار ویدئو[۲]

با ارائه این سرویس کاربران می توانند به ارسال تصاویر بر روی شبکه به صورت همگانی بدون نیاز به اشغال پهنای باند اختصاصی بپردازند. مانند پخش شبکه های صدا و سیما جهت مشترکین. با پشتیبانی از تکنولوژی Broadcasting، دیگر نیازی به اضافه نمودن پهنای باند برای تمامی مشترکین نیست، در این روش تجهیزات شبکه خود از داده ها به تعداد کاربران کپی سازی نموده و به تمامی کاربران با کیفیتی عالی بدون در نظر گرفتن تعداد آنها سرویس می دهد.

---

[۱] Video On Demand

[۲] Video Broadcasting

❖ کاربردهای سرویس ویدئو

۱. پخش دیجیتالی تلویزیون
۲. ویدئو بر طبق تقاضا
۳. آموزش از راه دور

۲. سرویس تلفن اینترنتی

با توجه به اینکه روش‌های برقراری ارتباط تلفنی در حال تغییر است، امروزه برای برقراری ارتباط تلفنی راه دور اغلب از تکنولوژیی به نام سرویس تلفن اینترنتی یا VoIP[۱] استفاده می‌شود. سرویس VoIP یک روش برای تبدیل سیگنال‌های آنالوگ صوت به داده‌های دیجیتال است که از طریق اینترنت منتقل می‌شوند. سرویس VoIP می‌تواند یک ارتباط اینترنت استاندارد را به یک روش مجازاً رایگان برای برقرای ارتباطات تلفنی در هر جای دنیا تبدیل کند.

۳. سرویس بازی های شبکه[۲]

بوسیله تجهیزات شرکت های PAP، سرویس دهنده با استفاده از حداقل پهنای باند ممکن می تواند به ارائه سرویس بازی های تحت شبکه بپردازد. این تجهیزات با تشخیص سیگنالهای مخصوص

---

۱ Voice Over IP

۲ GAME NETWORK

بازی ها، آنها را کپی کرده و به کاربران بازی به صورت همزمان ارسال می کند. بدین وسیله با حداقل پهنای باند بین مراکز برترین کیفیت سرویس بوجود می آید.

۴. سرویس اینترنت

امروزه اینترنت رفته رفته جزء لاینفکی از زندگی انسان‌ها در این عصر می‌شود. بدون شک هر فردی به نقش وسیع اینترنت و شبکه‌های اطلاع رسانی داده ها و اهمیت آن در تجارت الکترونیکی، آموزش الکترونیکی، دولت الکترونیکی، پول الکترونیکی و دیگر نیازهای روز پی خواهد برد. اما در این بین نحوه اتصال وکیفیت این نوع ارتباط اهمیت قابل ملاحظه‌ای دارد. فناوری ADSL امکان ارتباط پر سرعت کاربر را با شبکه جهانی اینترنت فراهم می‌سازد به طوری که کاربر با استفاده از خط تلفن موجود درمحل کار و یا منزل بدون این‌که خط اشتغال گردد می‌تواند ارتباطی پرسرعت و دایمی را با بهترین کیفیت با شبکه اینترنت و شبکه‌های اطلاع رسانی داشته باشد.

فصل ۳. معماری شبکه های ADSL

امروزه در دنیا شرکت‌های موجود در امور مخابراتی، توسط میلیون‌ها کیلومتر کابل، فیبر و بسترهای آماده و فراهم خود از یک طرف و شرکت‌های ارائه دهنده خدمات شبکه اینترنت با اتکا به فناوری ها و روش‌های نوین از طرف دیگر، پا به عرصه گذاشته‌اند تا بتوانند با مشارکت یکدیگر و استفاده از تکنیک ها و ابزار فن آوری اطلاعات و ارتباطات، خدمات شبکه با پهنای باند بالا را برای تمامی اقشار، ادارات و جوامع فراهم آورند.

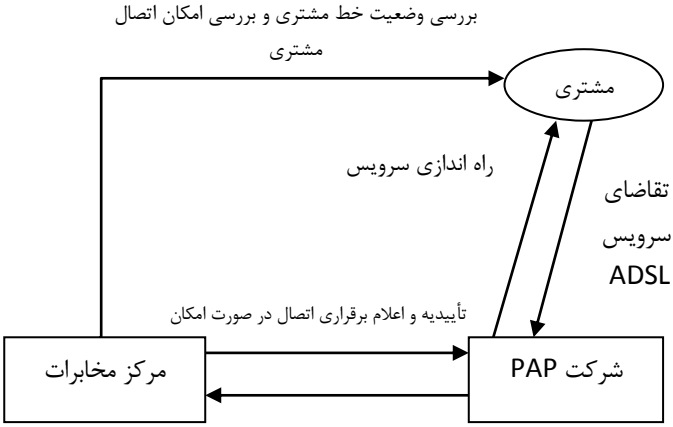
تکنولوژی ADSL فرق چندانی با سایر گزینه‌های متداول دسترسی پرسرعت همچون مودم‌های کابلی ندارد. مهم‌ترین مشخصه این شبکه‌ها، ترکیب و تجمیع ترافیک ارتباطی گروه بزرگی از مشترکان در لبه شبکه[۱] و ارسال این ترافیک یکپارچه به سمت هسته اینترنت[۲] از طریق لینک‌های بسیار سریع مخابراتی است. لبه شبکه علاوه بر تجمیع ترافیک‌ها، بسیاری از عملیات مدیریتی و امنیتی را نیز برعهده دارد و از این لحاظ یکی از مهم‌ترین عناصر این ساختار به‌شمار می‌رود.

---

۱. Edge Network

۲. Internet Core

شکل زیر نحوه ارتباط شرکت های PAP با مراکز مخابراتی و نحوه درخواست سرویس توسط مشتری را نشان می دهد.



نحوه ارتباط شرکت های **PAP**و مخابرات و مشتری

برای بهره گیری از تکنولوژی ADSL در حالت عمومی و نگاه کلی باید از وجود دو دستگاه خاص برای این منظور استفاده نمود. یکی از این دستگاه ها باید در محل مشترکین و دستگاه دیگر در محل ارائه دهنده خدمات ADSL، نصب گردد. در محل مشترکین

از یک ترانسیور ADSL استفاده می‌گردد. شرکت ارائه دهنده خدمات ADSL از یک دستگاه با نام DSLAM[1] استفاده می نماید

تجهیزات و تمهیداتی که برای برقراری ارتباط کاربر تا شرکت PAP مورد نیاز است عبارتند از:

الف ـ سمت کاربر:

۱. مودم های ADSL
۲. تضمین اینکه خط کاربر از نوع تقسیم فرکانسی نباشد.

ب ـ مراکز مخابراتی

۱. Splitter + Micro Filter[2]
۲. DSLAM

ج ـ شرکت های PAP

۱. فایروال های سخت افزاری و نرم افزاری
۲. مسیریاب های توزیع اینترنت

شبکه های ADSL از نقطه محل مشترک شروع و با استفاده از زوج سیم مسی مخابرات به مرکز مخابرات منتقل می‌گردد. در مرکز

[1] Digital Subscriber Line Access Multiplexer

[2] جداکننده

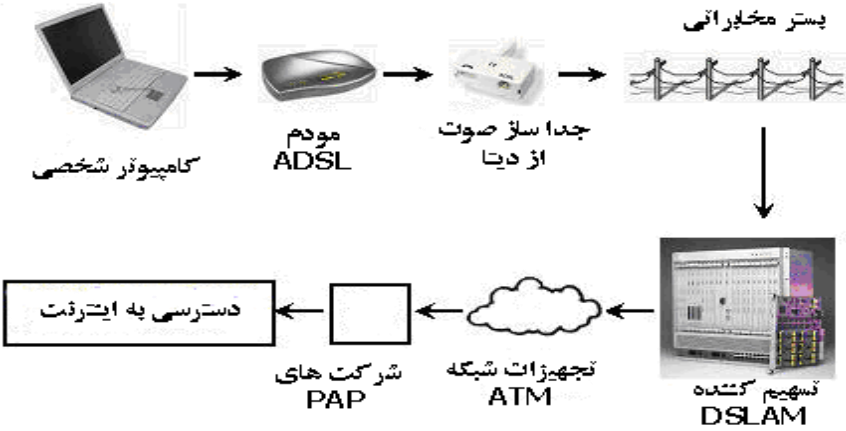
مخابرات سر کابل مشترک توسط یک جدا کننده به دو بخش ارایه خدمات تلفن صوتی و بخش ارایه خدمات دیتا تقسیم می‌گردد.

کاربران با به کارگیری جداکننده‌های[۱] نسبتاً ارزان قیمت در محل خود قادر به استفاده همزمان از سیم تلفن خود برای اتصال به گوشی تلفن و مودم خواهند بود.

بخش ارایه خدمات دیتا در نهایت توسط بستر ارتباطی و تجهیزات مستقر در مرکز مخابرات به DSLAM ها و تجهیزات شرکت های PAP برای ارایه خدمات شبکه به کاربران متصل می‌گردد.

برای بررسی موضوع و تجهیزات مورد استفاده، شکل ۲ که بیانگر شیوه ارتباطی و ساختار شبکه ADSL می باشد، ترسیم شده است. در ادامه هر یک از اجزا این شبکه بررسی خواهند شد.

۱. Splitter



شکل ۲. شیوه ارتباطی و ساختار شبکه **ADSL**

مودم ADSL

مودم ADSL دستگاهی است که می تواند یک کامپیوتر یا یک مسیریاب را از طریق خط DSL برای بهره گیری از خدمات ADSL به مرکز خدمات دهنده متصل کند. مودم های ADSL نیز همانند تمامی مودم ها وظیفه اصلی دریافت و ارسال اطلاعات[۱] را به عهده دارند. در واقع این مودمها امواج فرکانس بالا[۲] را (در محدوده ۲۵ KHz تا ۱ MHz)[۳] برای ارسال به DSLAM ها مدوله[۴] کرده و

---

[۱] Transceiver

[۲] high-frequency tones

[۳] Voice bands are in ۰-۴ kHz range

[۴] modulate

امواج دریافتی از DSLAM ها را در محل کاربر مجدداً رمزگشایی[۱] و به صورت دیتا به کامپیوتر کاربر منتقل می‌کند. مودم های ADSL قادر هستند با در اختیار داشتن مسیریاب DSL[۲]، مدیریت اتصال به شبکه و نحوه اشتراک گذاری ارتباط و منابع را نیز مدیریت کنند.

تسهیم کننده DSLAM

تسهیم کننده های DSLAM که اغلب با نام Dee-slam شناخته می شوند، ابزاری هستند که چندین کانال انتقال با سرعت پایین تر را در کانالی با سرعت بالا در انتهای یک اتصال برای دسترسی پرسرعت مشترکین یک شرکت PAP ترکیب می کند. (تسهیم کننده دیگری در انتهای دیگر اتصال، این فرآیند را معکوس می سازد تا کانالهای با سرعت پایین را مجدداً تولیدکند.)

تصویر تسهیم کننده Siemens DSLAM SURPASS hiX ۵۶۲۵ شرکت زیمنس را که در بخش Passive تجهیزات ADSL شرکت های PAP به کار رفته است در شکل ۳ نشان داده شده است.

---

۱ Demodulate

۲ DSL Router

شکل ۳- تصویر تسهیم کننده Siemens DSLAM SURPASS hiX ۵۶۲۵

بعلاوه DSLAM می‌تواند امکاناتی همچون مسیریابی یا تخصیص آدرس دینامیکی IP را نیز برای مشترکین فراهم کند. در واقع DSLAM را می‌توان دلیل اصلی تفاوت بین سرویس‌دهی از طریق ADSL و از طریق مودم کابلی به حساب آورد.

در این ارتباط‌ها DSLAM خطوط ارتباطی جهت یافته از سوی تعداد زیادی از مشترکین را دریافت نموده و آن‌ها را روی یک خط ارتباطی با ظرفیت بالا به اینترنت منتقل می‌کند. دستگاه‌های DSLAM قادر به پشتیبانی چندین نوع DSL یک مرکز تلفن واحد و تعداد گوناگونی از پروتکل‌ها و روش‌های مدوله سازی هستند. تصاویر رک و کارت های DSLAM در شکل های ۴و۵ نشان داده شده اند.

شکل ۴- DSLAM rack

همچنین شکل زیر کارت های DSLAM را به صورت مجزا و درون رک نمایش می دهند.

شکل ۵- کارت های DSLAM

مسیر رسیدن دیتا به تسهیم کننده های DSLAM :

۱. محل کاربر که از طریق مودم ADSL متصل می گردد.

۲. مسیر کابل[۱] از محل کاربر تا مرکز مخابرات که اغلب Last Mile نامیده می‌شود.

۳. تسهیم کننده DSLAM که وظیفه دریافت و ارسال اطلاعات از کاربر را به عهده دارد. این دستگاه همچنین وظیفه تلفیق اطلاعات و صدا را بر روی خط ارتباطی کاربر بر عهده دارد. در آن سوی خط وظیفه جداسازی صدا و اطلاعات و ارسال اطلاعات به شبکه های دیتا و ارسال صدا به سوییچ های مخابراتی را باید انجام دهد.

۴. مرکز MDF[۲] که در واقع یک رک[۳] برای اتصال خطوط مشترکین از خارج مرکز مخابرات به داخل مرکز می باشد. از این مرکز برای اتصال خطوط مشترکین به خطوط تجهیزات شبکه استفاده می‌شود. مراکز MDF معمولاً در مجاورت مراکز سوییچ مخابراتی بنا می شوند و فاصله چندانی از یکدیگر ندارند.

---

۱ Local Loop

۲ Main Distribution Frame

۳ Rack

شکل ۶- مرکز MDF شرکت مخابرات

پروتکل های ارتباطی شبکه های ADSL

برای رفع چالش هایی که در خصوص بکارگیری سرویس های ADSL وجود دارد، اجرای یک پروتکل مشخص بین کاربر و فراهم‌کننده خدمات توصیه می‌شود. این پروتکل از نوع پروتکل‌های محلی است که به منظور شناسایی وظایف مشخص میان دو نقطه اجرا می‌شود و در ارتباطات خارج از آن حوزه نقش ندارند. در حال حاضر چهار گزینه در این خصوص وجود دارد که هر یک مزایا و نقاط ضعف منحصر به خود را دارند و عبارتند از :

آدرس دهی ثابت IP [۱]

اولین و در واقع ابتدایی‌ترین راه حل، تخصیص یک آدرس **IP** به هر کاربر است که خود به تنظیم آن روی کامپیوتر خود اقدام می‌کند. این روش اساساً یک پروتکل نیست، تنها یک راه‌حل سریع برای مشکل است که از ابعادی گسترده برخوردار است. برای مثال، مشکل استفاده همزمان چند کامپیوتر و یک کاربر از ارتباط ADSL به این ترتیب حل نمی‌شود.

پروتکل پیکربندی پویای میزبان (DHCP [۲])

این روش برای این منظور طراحی شده است که پیکربندی IP را روی کامپیوتر کاربران به صورت خودکار انجام دهد. این پروتکل در شبکه‌های محلی سازمانی نیز از کاربرد گسترده‌ای برخوردار است. به‌ویژه در مورد پایانه‌هایی که به طور موقت به این شبکه‌ها متصل می‌گردند (برای مثال کامپیوترهای Laptop). پروتکل DHCP در حقیقت یک جهش محسوس نسبت به روش آدرس‌دهی ثابت محسوب می‌شود.

---

[۱] Static IP Address

[۲] Dynamic Host Configuration Protocol

پروتکل تونل‌زنی لایه۲ (L۲TP [۱])

پروتکل L۲TP، به عنوان یک گزینه نسبتاً جدیدتر برای شبکه‌های دسترسی باند پهن مطرح است و با ایجاد یک تونل مجازی از داخل شبکه اینترنت، کاربر را به هر نقطه مشخصی متصل می‌کند و کلیه تنظیمات لازم برای برقراری سرویس از داخل این تونل بر تجهیزات کاربر اعمال می‌گردد. پروتکل L۲TP در عمل یک شبکه مجازی یا VPN [۲] روی شبکه فراهم کننده ایجاد می‌کند که از امنیت خوبی نیز برخوردار است، ولی درعوض پیچیدگی و سربار بیشتری دارد. به‌ویژه در شبکه‌های بزرگ دسترسی با چندین هزار کاربر، مدیریت این تونل‌ها دشوار خواهد بود.

پروتکل نقطه به نقطه روی ATM (PPPoA [۳]) و پروتکل نقطه به نقطه روی اترنت(PPPoE [۴])

این پروتکل ترکیبی است از پروتکل های PPTP [۵] و L۲F [۶] که توسط شرکت سیسکو توسعه یافته است. این پروتکل ترکیبی است

---

[۱] Layer ۲ Tunneling Protocol

[۲] Virtual Private Network

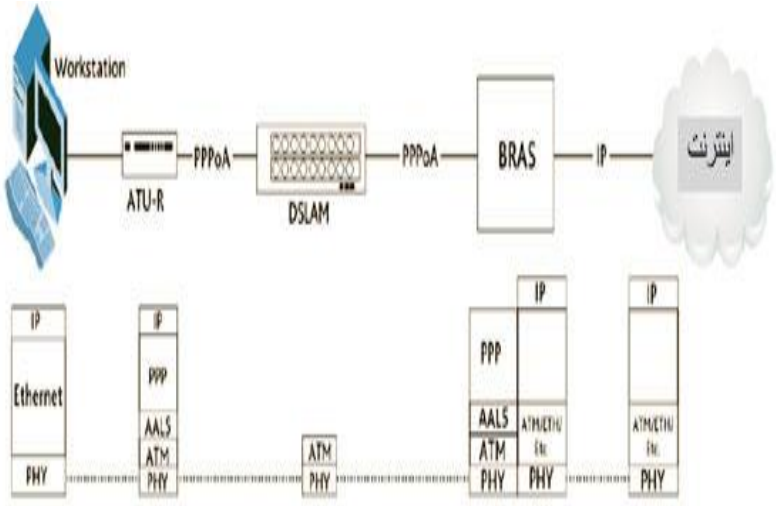
[۳] Point to Point Protocol over ATM

[۴] Point to Point Protocol over Ethernet

[۵] Point to Point Tunneling Protocol

[۶] Layer ۲ Forwarding

از بهترین خصوصیات موجود در L۲F و PPTP. این پروتکل فریم های PPP را برای ارسال بر روی شبکه های IP مانند اینترنت و علاوه بر این برای شبکه های مبتنی بر X.۲۵، Frame Relay و یا ATM کپسوله می کند. هنگامی که اینترنت به عنوان زیر ساخت تبادل اطلاعات استفاده می گردد، L۲TP می تواند به عنوان پروتکل Tunneling از طریق اینترنت مورد استفاده قرار گیرد.



شکل ۷- ترکیب پروتکل ها در ارتباطات مبتنی بر PPPoE/oA

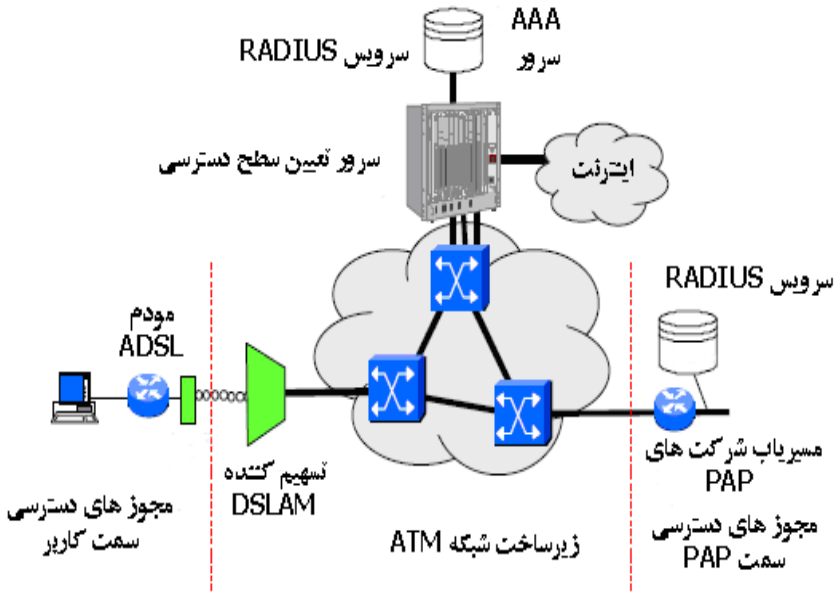
فصل ۴. نقاط آسیب پذیر شبکه های ADSL

با توجه به ساختار معماری شبکه های ADSL نقاط آسیب پذیر می تواند هر یک از تجهیزات فعال و غیر فعال به کار گرفته شده در ساختار شبکه ADSL باشد.

تجهیزات غیر فعال شبکه های ADSL شامل ساختمان ها و مکان های استقرار تجهیزات مربوطه، بستر رسانه، تجهیزات اتصال و ... می باشد. نقاط آسیب پذیر تجهیزات غیرفعال شبکه های ADSL و تدوین ملاحظات پدافند غیر عامل برای این بخش از تجهیزات در مبحث امنیت فیزیکی مورد بررسی قرار می گیرد.

تجهیزات فعال شبکه های ADSL از جمله مودم های ADSL، تسهیم کننده های DSLAM، مسیریاب ها، پروتکل های ارتباطی، سرور های AAA[۱] ، اگر مطابق سیاست صحیح و برنامه ریزی شده ای تهیه و بومی سازی نشده باشند هنگام بروز مخاصمات بین الملل یا جنگ های سایبری و فیزیکی به شدت در معرض آسیب پذیری هستند به علاوه در صورت عدم تنظیم صحیح در مواقع تهدیدات امنیتی نیز می توانند مورد هجوم و آسیب قرار گیرند.

[۱] AAA Server: Authentication Authorization Accounting server



مودم های ADSL

با توجه به پروتکل های ارتباطی و شیوه های اتصال به شبکه ADSL که در بخش قبلی مورد بحث قرار گرفت، از آنجایی که برای دسترسی و اتصال به شبکه ADSL معمولاً نام کاربری و رمز عبور مورد استفاده قرار می گیرد، اولین خطری که در استفاده از مودم ها، کاربران شبکه را مورد تهدید قرار می‌دهد، دسترسی به این اطلاعات می باشد.

از آنجا که کاربران معمولا برای انتقال نام کاربری و رمز عبور خود از مودم استفاده می کنند، باید اطمینان داشته باشند که مودم و برنامهٔ سرویس دهندهٔ آن به درستی نصب شده اند، صحیح عمل می کنند، و دقیقا آنچه را که مورد انتظار است انجام می دهند.
بعضی از مودم ها می توانند حاوی کدها و دستورالعمل های خاص برای نفوذ به شبکه یا کامپیوتر کاربران یا حاوی دستورالعمل هایی برای ارسال اطلاعات به نقاط دیگر باشد.

بنابراین اولین گام در امنیت شبکه های ADSL استفاده از مودم های امن که مورد بررسی و ممیزی قرار گرفته اند می باشد. گام بعدی استفاده از مودم هایی است که به طور داخلی به کارگیری از رمزکننده ها را برای ارسال اطلاعاتی نظیر نام کاربری و رمز عبور به کار می گیرند.

خطوط ارتباطی مخابراتی

عمل شنود بر روی سیم‌های مسی، چه در انواع Coax و چه زوج‌های بهم تابیده، هم‌اکنون نیز از راه‌های نفوذ به شمار می‌آیند. با استفاده از شنود و اطلاعات بدست آمده می توان تلاش برای نفوذ در سیستم‌های کامپیوتری را گسترش داد و به جمع‌بندی مناسبی برای حمله رسید. هرچند که می‌توان سیم‌ها را نیز به گونه‌ای مورد

محافظت قرار داد تا کمترین احتمال برای شنود و یا حتی تخریب فیزیکی وجود داشته باشد، ولی در حال حاضر، امن ترین روش ارتباطی در لایه‌ی فیزیکی، استفاده از فیبرهای نوری است. در این روش به دلیل نبود سیگنال‌های الکتریکی، هیچگونه تشعشعی از نوع الکترومغناطیسی وجود ندارد، لذا امکان استفاده از روش‌های معمول شنود به پایین‌ترین حد خود نسبت به استفاده از سیم در ارتباطات می‌شود.

بنابراین یکی از نقاط آسیب پذیر در شبکه های ADSL مسیر کابل و نحوه انجام آن می باشد. باید با توجه به روش های عبور کابل از مسیر حفاظت شده و امن نظیر عبور از داکت های فولادی و مستحکم با توجه به حساسیت مراکز، نسبت به ایمن کردن تجهیزات اتصال مسیر، اقدام نمود.

تسهیم کننده ها (DSLAM)

با توجه به عملکرد و وظیفه تسهیم کننده ها، همانند آنچه که در مورد مودم های ADSL در مورد کدهای مخفی برای نفوذ و ارسال اطلاعات به نقاط خارج از شبکه اشاره شد، در این مورد نیز مورد توجه و ارزیابی قرار گیرد. اصولاً باید در مورد این تجهیزات نیز

ممیزی و دقت لازم در مورد به کارگیری تجهیزات مطمئن و بومی شده، صورت پذیرد.

نکته دوم در مورد این تجهیزات بررسی و اطمینان از عدم وجود دستورات کنترلی در این تجهیزات می باشد. توسط دستورات کنترلی می توان از طریق شبکه و از راه دور عملکرد این تجهیزات را تغییر داد و یا کارکرد آن ها را مختل نمود.
از آنجایی که یکی از اهداف امنیت و ملاحظات پدافند غیر عامل، پایداری در ارائه سرویس می باشد باید موضوع تهدید را در مورد این تجهیزات به دقت مورد توجه قرار داد.

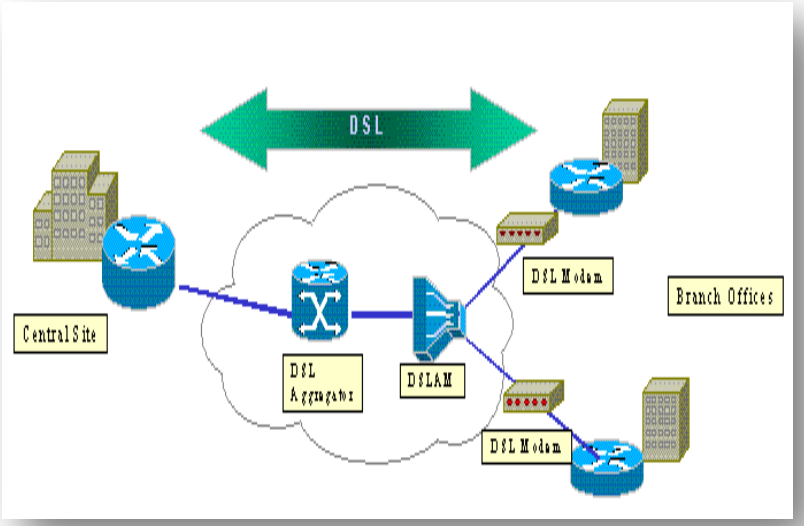
در بازدیدهای صورت گرفته از شرکت های مخابراتی مستقر در شهر تهران موارد زیر حائز اهمیت می باشند:

- تجهیزات passive شرکت های PAP در محوطه های باز و پیرامونی مراکز مخابراتی و درون کانکس هایی که دارای هیچ گونه امنیت فیزیکی نمی باشد، قرار گرفته است و امکان نفوذ به آنها به سادگی وجود دارد.

- تعداد بسیار زیادی از پورت های شرکت های PAP بدون استفاده (نداشتن کاربر) مانده است.

- پرسنل مراکز مخابراتی دانشی در خصوص این تجهیزات ندارند و در صورت بروز مشکل صرفا با مراجعه متخصصین شرکت های PAP مشکل رفع خواهد شد.

- کابل های همه رک های شرکت ها بدون رعایت نکات امنیتی به اتاق های MDF مراکز مخابراتی رفته است.



فصل ۵. تهدیدات و حملات علیه شبکه های ADSL

سیستم های شبکه های کامپیوتری از طریق راه های بسیار زیادی می توانند مورد حمله واقع و متحمل خسارات بسیار زیادی گردند. این حملات می توانند به صور زیر باشند:

ممانعت از ارائه سرویس (DOS[۱])

هکرها از طریق قطع جریان اطلاعات به وسیله قطع کردن دستگاههای مهم و حیاتی مثل سرور، روتر و دیوار آتش و یا با ارسال بیش از حد بسته های اطلاعاتی به سرورها اقدام به خارج کردن آنها و عدم سرویس دهی آنها می نمایند. همچنین در صورت بروز مخاصمات بین الملل شرکت ها و کشورهای سازنده تجهیزات ممکن است برای ضربه زدن به کشور در مورد تجهیزاتی که از آنها در شبکه وجود دارد، اقدام به خارج کردن از سرویس دهی این نوع از تجهیزات از راه دور و مبتنی بر شبکه اینترنت نمایند. در این نوع حمله، کاربر دیگر نمی‌تواند از منابع و اطلاعات و ارتباطات استفاده کند. این حمله از نوع فعال است و میتواند توسط کاربر داخلی و یا خارجی صورت گیرد.

[۱] Denial of Service

سرقت اطلاعات

هکر ها و حمله کنندگان برای دست یابی به اطلاعات اختصاصی سازمانها و تخریب آن با روشهایی همچون استراق سمع و نفوذ به داخل سازمان و یا بهره گیری از برنامه های کامپیوتری جهت شناسایی و یافتن کلمه عبور کاربران مجاز اقدام به سرقت اطلاعات می نمایند.

تخریب داده ها

حمله کننده ها به داده های ذخیره شده بر روی دیسک ها در زمان انتقال بین شبکه خسارت وارد می نمایند. این حمله یک حمله فعال است که در آن جامعیت و صحت اطلاعات را با تغییرات غیر مجاز بهم می زند و باعث اختلال جدی در عملکرد صحیح شبکه می‌شود.

تحلیل ترافیک

در این نوع حمله مهاجم براساس بسته های اطلاعاتی ترافیک شبکه را تحلیل کرده و اطلاعات ارزشمندی را کسب میکند. این حمله یک نوع حمله غیر فعال است و اکثراً توسط کاربران خارجی صورت می گیرد. با بدست آوردن این نوع تحلیل می توانند برای شناسایی و از کار انداختن شریانهای اصلی کشور بهره بگیرند.

جعل هویت

این نوع حمله یک نوع حمله فعال است که در آن هکر هویت یک فرد مجاز شبکه را جعل می کند و برای اختلال در صحت عملکرد شبکه یا برای دریافت اطلاعات از آن بهره می گیرد.

تحریم

یکی دیگر از تهدیداتی که متوجه عملکرد صحیح شبکه و توسعه آن است، وضع تحریم ها و عدم ارائه تجهیزات و قطعات و خدمات فنی در رابطه با تجهیزات فنی شبکه نظیر تسهیم کننده‌های DSLAM، مسیریابها و ... می باشد.

حملات ضد امنیتی مسیریاب‌ها

حمله به مسیریاب‌ها و سوئیچ‌های شبکه بخش مهمی از حملات منطقی را تشکیل می‌دهند. حملات ضد امنیتی منطقی برای مسیریاب‌ها و دیگر تجهیزات فعال شبکه، مانند سوئیچ‌ها، را می‌توان به سه دسته‌ی اصلی تقسیم نمود:

۱- حمله برای غیرفعال سازی کامل

۲- حمله به قصد دستیابی به سطح کنترل

۳- حمله برای ایجاد نقص در سرویس‌دهی

در یک شبکه که شامل مجموعه ای از نقاط است وجود تأسیسات کافی و غیر قابل نفوذ امنیتی در یک نقطه و از سوی دیگر نبود امنیت کافی در نقاط دیگر شبکه شبیه به آن است که یک محافظ در جلوی میز کامپیوتر واقع شده باشد حال آنکه کامپیوتر کاملا در دسترس باشد این مسئله حاکی از آن است که چنانچه بخشی از شبکه غیر قابل نفوذ و سایر نقاط آسیب پذیر باشد در عمل گویی کل شبکه با مشکل امنیتی مواجه است.

فصل ۶. ملاحظات پدافند غیر عامل در شبکه هایPAP

به منظور حفاظت از تجهیزات شرکت هایPAP و برقراری امنیت خدمات شبکه های ADSL با رویکرد پدافند غیر عامل و به منظور دست یافتن به اهداف ترسیم شده در اسناد پدافند غیر عامل موارد زیر می تواند تا حدود زیادی مشکلات مهم را در این حوزه برطرف نماید :

۱. تجهیزاتی که دارای بیشترین نیاز امنیتی هستند، در امن ترین منطقه قرار گیرند و اجازه دسترسی عمومی به آنها و یا از سایر شبکه های دیگر به این منطقه داده نشود. دسترسی ها باید با کمک یک فایروال و یا سایر امکانات امنیتی مانند دسترسی از راه دور[۱] به طور امن کنترل شود. همچنین کنترل شناسایی و احراز هویت و مجاز یا غیر مجاز بودن در این منطقه باید با درجه امنیت بالایی انجام شود.

۲. سرورهایی که در این شبکه ها مورد استفاده و دسترسی هستند، در منطقه ای جداگانه و دارای ضریب امنیتی بالاتر نسبت به سایر بخش ها قرار گیرند تا در صورت مورد حمله قرار گرفتن یکی،

---

۱. RAS: Remote Access Control

سایرین مورد تهدید قرار نگیرند. به این مناطق مناطق خارج از تهدیدات نظامی[۱] گفته می‌شود.

۳. از فایروال ها به صورت لایه ای استفاده شود، استفاده از فایروال ها به شکل لایه ای و به کارگیری فایروال های مختلف سبب می‌شود تا درصورت وجود یک اشکال امنیتی در یک فایروال، کل شبکه به مخاطره نیفتاده و امکان استفاده از کد های جاسوسی و خرابکارانه نیز به حداقل برسد.

۴. امکان استفاده از تهدیدات مربوط به استراق سمع که طی آن دشمن می تواند بدون اطلاع طرفین، اطلاعات و پیامها را شنود کند، به حداقل برسد. استفاده از فضاهای امن در قسمت های passive و active می تواند به این مساله کمک کند.

۵. حملات مرتبط با تحلیل ترافیک که طی آن بر اساس یک سری بسته های اطلاعاتی، مهاجم می تواند ترافیک شبکه را تحلیل کرده و اطلاعات ارزشمندی را کسب کند، شناسایی شود. این حملات از نوع غیر فعال است و اکثراً توسط کاربران خارجی صورت می گیرد.

۶. امکان دستکاری پیامها و داده ها که بر اساس آن مهاجم می تواند جامعیت و صحت اطلاعات را با تغییرات غیر مجاز برهم

---

۱. DMZ: Demilitarized Zone

زند از بین برود. این نوع حملات نیز توسط کاربران خارجی صورت می‌گیرد. همچنین امکان جعل هویت که طی آن مهاجم هویت یک فرد مجاز شبکه را جعل می کند به حداقل میزان ممکن برسد.

۷. امنیت ارتباطات که در آن با استفاده از فایروال ها، سیستمهای ضد ویروس، سرورهای کنترل دسترسی و احراز هویت، نرم افزارهای مانیتورینگ، ثبت و تحلیل رویدادها می توان به تشخیص هویت و کنترل کاربران پرداخت، به وجود می آید.

۸. امنیت سیستم ها که در آن با بهره گیری از پویشگرهای امنیتی، آنتی ویروسها، **IDS**[۱] و**IPS**[۲] به ثبت و کنترل دسترسی کاربران به منابع پرداخته می‌شود، لحاظ شود.

۹. سطوحی از امنیت کاربردها به وجود آید که طی آن با بهره گیری از سیستمهای **IDS**، آنتی ویروس، پویشگر امنیتی و فیلترهای محتوا بر دسترسی کاربران نظارت می‌شود.

۱۰. از مدل هایی از مسیریاب ها استفاده شود که سیاست های امنیتی در قبال کلاینت ها در آنها کاملا رعایت شده است و همچنین در مسیریابها، سعی شود که تهدیدها شناسایی شده و از دسترسی شبکه های ناشناس جلوگیری گردد.

---

۱ Intrusion Detection System

۲ Intrusion Prevention System

۱۱. از دیواره های آتش[۱] برای رسیدن به امنیت برای کاربران استفاده شود که این امر در بسیاری از مسیریابها تعبیه شده است.

۱۲. ایجاد مکانیزم تولید و تغییر کلید رمز کننده اطلاعات[۲] داخل مسیریابها برای بالابردن ضریب ایمنی لحاظ شود و همچنین تشخیص و شناسایی حملات خطرناک از طریق پست الکترونیکی و سایر روشها مورد نظر قرار گیرد.

۱. Firewall

۲ IKE: Internet Key Exchange