

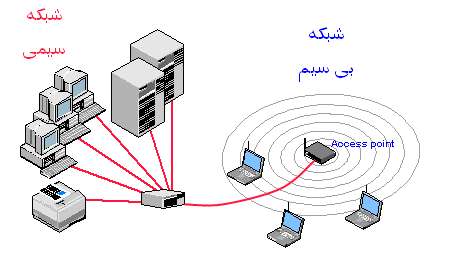
امنیت شبکه

استاد رحیمی

آذر 1390

یک شبکه رایانه‌ای *(به انگلیسی: Computer Network)*، که اغلب به طور خلاصه به آن شبکه گفته می‌شود، گروهی از رایانه‌ها و دستگاه‌هایی می‌باشد که توسط کانال‌های ارتباطی به هم متصل شده‌اند. شبکه رایانه‌ای باعث تسهیل ارتباطات میان کاربران شده و اجازه می‌دهد کاربران منابع خود را به اشتراک بگذارند.

**شبکه را برای چه منظوری راه اندازی می کنیم؟**

جهت سهولت در سرعت بالا و انتقال اطلاعات و کاهش هزینه و افزایش کارایی:

برای انتقال دو کامپیوتر دو روش وجود دارد: Wireless و Wire

**انواع شبکه‌های رایانه‌ای از نظر اندازه:[[1]](#footnote-2)**

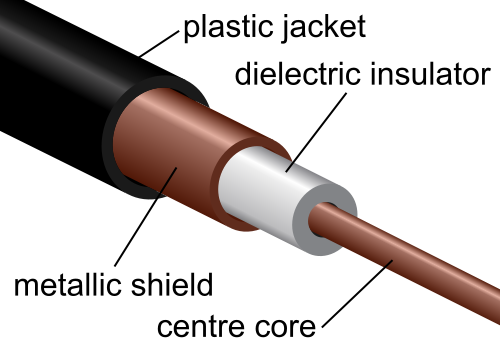
**«شبکه محلی» (Local Area Network)** یک «شبکه رایانه‌ای» است که محدوده جغرافیایی کوچکی مانند یک خانه، یک دفتر کار یا گروهی از ساختمان‌ها را پوشش می‌دهد.

**«شبکه کلان‌شهری» (Metropolitan Area Network)** یک «شبکه رایانه‌ای» بزرگ است که معمولاً در سطح یک شهر گسترده می‌شود.

**«شبکه گسترده» (Wide Area Network)** یک «شبکه رایانه‌ای» است که نسبتاً ناحیه جغرافیایی وسیعی را پوشش می‌دهد (برای نمونه از یک کشور به کشوری دیگر یا از یک قاره به قاره‌ای دیگر)

**انواع کابل در شبکه های رایانه ای**

1. **کابل هم‌محور یا کابل کواکسال**

کابل هم‌محور یا کابل کواکسال (به انگلیسی: Coaxial cable)، کابلی است که یک رسانای داخلی دارد که توسط یک عایق منعطف محصور شده است، که روی این لایهٔ منعطف نیز توسط یک رسانای نازک برای انعطاف کابل، به هم بافته شده است. همهٔ این اجزا، در داخل عایق دیگری جاسازی شده‌اند.

تصویر 1اجزا کابل کواکسیال

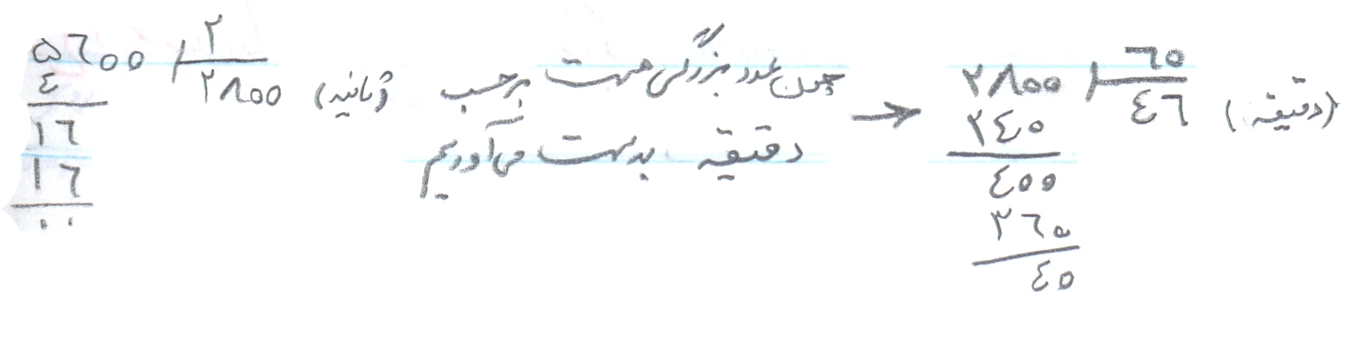
این کابل‌ها دارای امپدانس[[2]](#footnote-3) مخصوص به خود هستند. مثلا کابل 50 اهمی یا 75 اهمی . کابل مورد استفاده در آنتن ماهواره‌های خانگی و تلویزیون‌ها همگی از نوع کواکسیال 75 اهمی هستند و کابل های مورد استفاده در شبکه های رایانه ای 50 اهمی می باشند. اگر به بدنه آن‌ها دقت کرده باشید، امپدانس و برخی اصطلاحات دیگر آن نوشته شده است .

یکی از مشخصات بارز کابل کواکسیال این است که در حالت گیرندگی هیچ نویزی نمی تواند در طول خط انتقال وارد آن شود و در حالت فرستندگی هیچ تشعشع و تابشی در طول کابل دیده نمی شود . یعنی موج انتقالی کاملا محافظت می‌شود .

**مثال:** بسته ای داریم به حجم 700 MB اگر بخواهیم از طریق کابل کواکسیل انتقال اطلاعات داشته باشیم چقدر زمان نیاز است؟ (سرعت کابل کواکسیل 2 mbps می باشد)

700 mB 🡪 5600,000,000 b

2 mb 🡪 2,000,000 b



**جواب:** 46 دقیقه و 40 ثانیه

(اختلاف 1 MB با 1 mB هفت میلیون بیت می باشد)

1. **کابل زوج به‌هم‌تابیده**

زوج به ‌هم ‌تابیده (به انگلیسی: Twisted pair)، فرمی از سیم‌کشی است که در آن سیم‌های هادی دو به دو به هم پیچ خورده‌اند تا اختلالات الکترومغناطیسی حاصل از منابع خارجی را خنثی سازند. سوکتی که برای این نوع کابل ها استفاده می شود RJ 11 در تلفن و RJ 45 در شبکه می باشد.

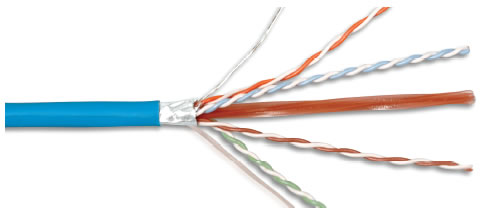
تصویر 2 هر زوج سیم برای کاهش اختلالات مغناطیسی بدور هم تابانیده شده است

در این کابل ها به دلیل سرعت بالای انتقال اطلاعات، بین کابل ها یک پلاستیکی خاص جهت خنک کردن سیم ها قرار می دهند.

انواع زوج به ‌هم ‌تابیده شامل روکش دار و بدون روکش[[3]](#footnote-4) می باشد.

زوج سیم‌های به هم تابیده روکش دار (به انگلیسی: Shielded twisted pair) معمولا توسط غلافی در برابر افزایش اختلالات الکترو مغناطیسی محافظت می‌شوند. همچنین نوع دیگری از این سیم ها دارای ورقه ی فلزی[[4]](#footnote-5) می باشد که جهت خنک نگه داشتن و جلوگیری از افت سرعت در متراژ های بالا مفید است.

زوج سیم‌های به هم تابیده بدون روکش کابل هایی هستند فاقد غلاف که در شبکه‌های اترنت (ethernet) و سیستم های تلفن یافت می‌شوند.

تصویر 3 کابل زوج به هم تابیده بدون روکش

تصویر 4 کابل زوج به هم تابیده روکش دار

جدول زیر لیست انواع کابل های UTP می باشد:

|  |  |  |
| --- | --- | --- |
| **موارد استفاده** | **سرعت انتقال اطلاعات** | **گروه** |
| سيستم های قديمی تلفن ، ISDN و مودم | حداکثر تا يک مگابيت در ثانيه | CAT1 |
| شبکه های Token Ring | حداکثر تا چهار مگابيت در ثانيه | CAT2 |
| شبکه های Token ring و 10BASE-T | حداکثر تا ده مگابيت در ثانيه | CAT3 |
| شبکه های Token Ring | حداکثر تا شانزده مگابيت در ثانيه | CAT4 |
| اترنت ( ده مگابيت در ثانيه ) ، اترنت سريع ( يکصد مگابيت در ثانيه ) و شبکه های Token Ring ( شانزده مگابيت در ثانيه ) | حداکثر تا يکصد مگابيت در ثانيه | CAT5 |
| شبکه های Gigabit Ethernet | حداکثر  تا يکهزار مگابيت در ثانيه | CAT5e |
| شبکه های Gigabit Ethernet | حداکثر  تا يکهزار مگابيت در ثانيه | CAT6 |

**کارت شبکه (Network Interface Card)**

کارت شبکه، يکی از مهمترين عناصر سخت افزاری در زمان پياده سازی يک شبکه کامپیوتری است. هر کامپيوتر موجود در شبکه ( سرويس گيرندگان و سرويس دهندگان )، نيازمند استفاده از يک کارت شبکه است. کارت شبکه، ارتباط بين کامپيوتر و محيط انتقال ( نظير کابل ها ی مسی و يا فيبر نوری ) را فراهم می نمايد.

هر کارت شبکه دارای یک آدرس فیزیکی[[5]](#footnote-6) (MAC) است. آدرس فوق يک عدد شش بايتي بوده که سه بايت اول آن مشخص کننده سازنده کارت شبکه و سه بايت دوم، شماره سريال کارت شبکه است.



تصویر 5 کارت شبکه بیسیم

تصویر 6 کارت شبکه با پورت RJ-45

**MAC Address چيست**

آدرس سخت‌افزاری یا آدرس MAC، آدرس عددی است که به صورت سخت‌افزاری در کارت شبکه در کارخانه حک شده‌است. این نوع آدرس‌دهی موجب شناسایی منحصر به فرد کارت شبکه در بین کارت‌ها می‌شود. طول این آدرس ۶ بایت است.

-------------------

**سوئیچ شبکه**

دستگاهی است که در قلب هر شبکه مبتنی بر توپولوژی[[6]](#footnote-7) ستاره ای است. با استفاده از سوئيچ، چندين کاربر قادر به ارسال اطلاعات از طريق شبکه در يک لحظه خواهند بود. در سوییچ ها سرعت ارسال اطلاعات هر يک از کاربران بر سرعت دستيابي ساير کاربران شبکه تاثير نخواهد گذاشت.سوئیچ ها معمولا در لایه 2 مدل OSI هستند و با تعداد پورت 5 ، 8 ، 16 ، 24 و گاهی 36 و 48 پورت نیز تولید می شوند. سرعت آنها معمولاً 10، 100 و یا 1000 مگابیت بر ثانیه است. سوئیچ ها دارای پورتهایR j- 45 و یا فیبر نوری و یا ترکیبی از هر دو هستند.



تصویر 7 دو نمونه سوئیچ

**مسیریاب (Router)**

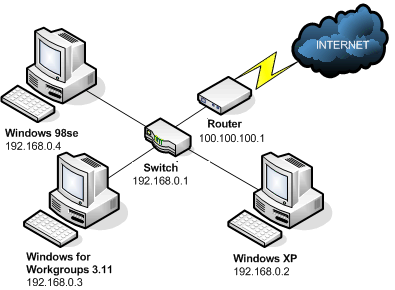
مسیریاب یا روتر های سخت افزاری

روترها دستگاه های لايه سوم ( مدل مرجع OSI ) می باشند. مسیریاب ها، شبکه هایی که دارای یک رنج آدرس شبکه (IP Address) نیستند را به هم متصل می کنند. مانند ارتباط کامپیوترهای یک شبکه به سرورهای اینترنت.

هر روتر حداقل دارای یک پورت LAN جهت اتصال به شبکه محلی و یک پورت WAN جهت اتصال به شبکه دور دست می باشد. مسیریاب ها بهترین مسیر را برای فرستادن بسته ها به مقصد انتخاب می کند و چک می کند تا ببیند آیا بسته ها به مقصد رسیده اند یا نه.

بر اساس مقصد داده ها، بسته ها از یک مسیر یاب دیگر از طریق بهترین راه فرستاده می شوند. این موضوع باعث می شود تا به عنوان یک وسیله ی قدرتمند در شبکه های پیچیده مثل اینترنت استفاده شود، در واقع می توان اینترنت را به عنوان شبکه ای از مسیر یاب ها توصیف کرد.

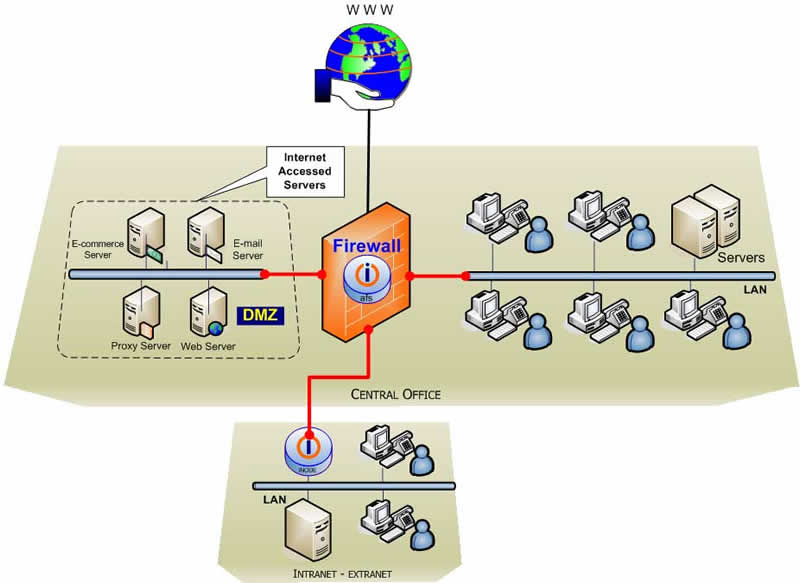
مسیریاب یا روتر های نرم افزاری

روترهای نرم افزاری دارای عملکردی مشابه با روترهای سخت افزاری بوده و مسئوليت اصلی آنان نيز ارسال داده از يک شبکه به شبکه ديگر است. يک روتر نرم افزاری می تواند يک سرويس دهنده NT، يک سرويس دهنده نت ور و يا يک سرويس دهنده لينوکس باشد. تمامی سيستم های عامل شبکه ای مطرح ،دارای قابليت های روتينگ از قبل تعبيه شده می باشند. در اکثر موارد از روترها به عنوان فايروال و يا gateway اينترنت، استفاده می گردد.

**دیوار آتش یا Firewall**

یک فایروال شبکه را در برابر ترافیک ناخواسته و همچنین نفوذ دیگران به کامپیوترها حفاظت می کند. توابع اولیه یک فایروال به این صورت است که اجازه می دهد ترافیک خوب عبور کند و ترافیک بد را مسدود می کند.

دیوار آتش سیستمی سخت افزاری یا نرم افزاری است که بین کامپیوتر شما یا یک شبکه LAN و شبکه بیرونی (مثلا اینترنت) قرار گرفته و ضمن نظارت بر دسترسی به منابع resource سیستم ، در تمام سطوح ورود و خروج اطلاعات را تحت نظر دارد. هر سازمان یا نهادی که بخواهد ورود و خروج اطلاعات شبکه خود را کنترل کند موظف است تمام ارتباطات مستقیم شبکه خود را با دنیای خارج قطع نموده و هر گونه ارتباط خارجی از طریق یک دروازه که دیوار آتش یا فیلتر نام دارد، انجام شود.



تصویر 8 - نمایی از سه شبکه مجزا که از طریق یک فایروال مرکزی به اینترنت متصل هستند

**انواع استاندارد کارت شبکه از نظر سرعت:**

**Ethernet[[7]](#footnote-8) 10 Mbit/s**

**Fast Ethernet 100 Mbit/s**

**Gigabit Ethernet 1000 Mbit/s**

**نکته:** در شبکه به دلیل عدم توانایی یکسان سازی دستگاه های با سرعت بیت پایین، با دستگاه های با سرعت بیت بالا، همیشه پایین ترین سرعت بیت کارت های شبکه و کابل را در نظر گرفته می شود.

**تذکر:**

به خدمات سخت افزاری چون کابل کشی، نصب سوئیچ و... را Passive و به خدمات نرم افزاری مانند نصب سیستم عامل مدیریت شبکه، شناسایی توپولوژی مناسب، پشتیبانی شبکه و... را خدمات Active می گوییم.

**چگونگی مشاهده مشخصات کارت شبکه**

روش اول:

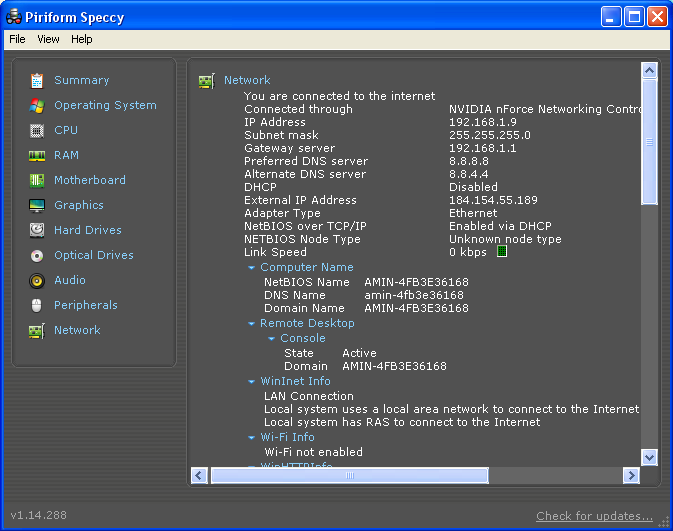
روش اول: استفاده از برنامه های کاربردی

نرم افزار هایی جهت نمایش مشخصات دقیق سخت افزار ها وجود دارد که از بین آن ها می توان به Speccy، CPU-Z و Sandra Lite اشاره کرد.

مزیت عمده استفاده از این نرم افزار ها، ارائه اختیارات بیشتر نسبت به روش های داخلی سیستم عامل است.

وبسایت های برنامه های یاد شده

: **Speccy:** www.piriform.com/speccy



**برای دیدن مدل و سرعت کارت شبکه:**

**Right Click on Desktop -> Properties -> Customize ->  My Network Plases -> OK**

**وقتی روی صفحه اومد روش Right Click می کنیم و Properties که در آنجا آیکنی داریم به نام Local Area Connection که در اصل همان کارت شبکه ما می شود، که نوع آن را هم همان جا نوشته است.**

**اگر این آیکن در این صفحه نبود مشکل چیست؟ یا کارت شبکه نداریم یا نصب نیست.**

**برای دیدن این مورد:**

**Right Click on My Computer -> Properties -> Hardware -> Device Manager**

**اگر در این لیست گزینه ای داریم به نام Network Adapter که علامت سوال یا تعجب زرد داشت یعنی کارت شبکه داریم ولی نصب نیست ولی اگر نبود یعنی کارت شبکه نداریم. و اگر نصب باشد نوع و استاندارد آن را می نویسد.**

**برای انتقال اطلاعات بین دو کامپیوتر علاوه بر کابل و NIC نیاز به IP (Internet Protocol)هم داریم.**

**Protocol قانون یا قوانینی که جهت انتقال اطلاعات بین کامپیوتر ها استفاده می شود. دو پروتکل مهم TCP و UDP می باشد.**

**TCP مثل این هست که برای ارسال بسته ها یک پیک بگیریم و بسته را بهش بدهیم و ازش بخواهیم تا در صورت تمایل بسته، یک امضا از گیرنده بگیرد و برای ما بیاورد.**

**UDP بسته را می دهیم به پیک ببرد و بهش می گوییم که اگر بود بسته را بهش بده و اگر نبود بسهت را بنداز جلو در و برگرد.**

**پس TCP یک بسته را می برد و برای هر بسته تاییدیه می گیرد. (Acknowledgement) و بر می گرداند اگر بسته در مقصد به هر دلیلی دریافت نشد اینقدر این بسته ارسال می شود تا برسد. اصطلاحاً می گویند TCP یک کانکشن مطمئن است. مثل دانلود یک فایل که حتی اگر 1 درصد آن هم مانده باشد قابل اجرا نیست.**

**UDP سریع می رود و برایش تحویل بسته مهم نیست به این ارتباط Connectionless می گویند و امنیت ندارد. UDP، Live هست و در لحظه مثل پخش های زنده دوربین مدار بسته.**

**IP یک عدد است بین 0 تا 255 و 4 Octed دارد. \_\_\_.\_\_\_.\_\_\_.\_\_\_**

**هر IP از دو بخش HostID.NetID تشکیل شده است. بخش HostID متغییر است ولی NetID همواره ثابت می باشد.**

**سه نوع کلاس داریم:**

**A: 1 to 126**

**B: 128 to 191**

**C: 192 to 223**

**نکته: 127 برای Loop Back می باشد.**

**جهت شناسایی کلاس IP کافی است که فقط به octed اول IP Address ها توجه کنیم.**

**برای اینکه در شبکه، کامپیوتر ها همدیگر را ببینند NetID ها باید یکسان باشند.**

**NetID HostID Subnet Mask**

**A: \_\_\_.\_\_\_.\_\_\_.\_\_\_ 255.0.0.0**

**B: \_\_\_.\_\_\_.\_\_\_.\_\_\_ 255.255.0.0**

**C: \_\_\_.\_\_\_.\_\_\_.\_\_\_ 255.255.255.0**

**شماره IP در سرعت تاثیر ندارد بلکه به تعداد کامپیوتر ها بستگی دارد.**

1. در برخی از کتاب های شبکه از شبکه شخصی (PAN)، شبکه متصل (Internetwork)، شبکه داخلی (Intranet)، شبکه خارجی (Extranet) و شبکه اینترنت (Internet) نیز یاد شده است. [↑](#footnote-ref-2)
2. مقدار مخالفت در برابر جریان الکتریکی که با زمان تغییر می‌کند در یک مدار [↑](#footnote-ref-3)
3. Unshielded twisted pair (UTP) [↑](#footnote-ref-4)
4. Foil [↑](#footnote-ref-5)
5. Media Access Control [↑](#footnote-ref-6)
6. همبندی یا توپولوژی (به انگلیسی: Topology) به معنای چگونگی پیکربندی و ایجاد اتصالات بین دستگاه‌های یک شبکه رایانه‌ای است. [↑](#footnote-ref-7)
7. اترنت(به انگلیسی: Ethernet) یکی از فناوری‌های مبتنی بر Frame در شبکه‌های رایانه برای شبکه‌های محلی (LAN) می‌باشد. این نام از مفهوم فیزیکی ether گرفته شده‌است. [↑](#footnote-ref-8)