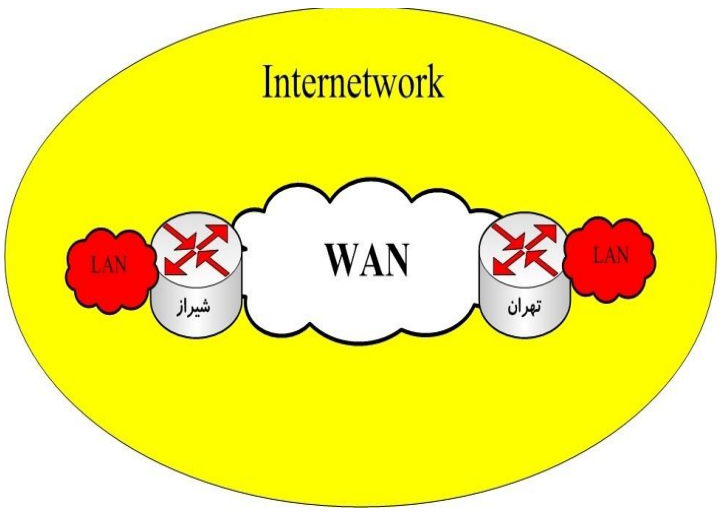
در ابتداچند اصطلاح را با هم تعریف می کنیم:

- **شبکه: بصورت ساده می توان گفت اتصال حداقل دو تا بینهایت کامپیوتر به نحوی که بتوانند از اطلاعات یکیدیگر استفاده کنند.**

- **Local Area Network (LAN): شبکه های محلی. منظور از محلی شبکه هاییست که از نظر جغرافیایی محدودند، مانند شبکه یک خانه، یک دفتر کاری یا یک ساختمان. بصورت ساده تا جایی که سیستم ها را بتوان به هم متصل کرد و نیازی به استفاده از بستر های مخابراتی نباشد شما دارای شبکه LAN هستید.**

- **Wide Area Network (WAN): شبکه های گشترده. شبکه هایی که شما برای بوجود آوردن آنها نیازمند بستر های مخابراتی هستید. عموماً زمانی این نوع شبکه مورد استفاده قرار می گیرد که سیستم های شما از نظر جغرافیایی از یکدیگر فاصله دارند.**

- **Internetwork: به مجموع شبکه های محلی (LAN) که توسط بستر های مخابراتی به یکدیگر متصل شده اند و یک شبکه یکپارچه را بوجود آورده اند گفته می شود.**



Media: تکنولوژی که بوسیله آن کامپیوتر ها با هم در ارتباطند که بصورت کلی به سه دسته تقسیم می شوند:

۱. **(Copper Base) کابلی**

۲. **(Fiber Optic) فیبر نوری**

۳. بی سیم (Wireless)

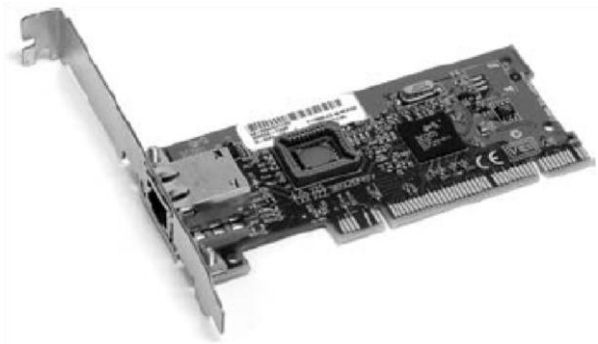
پروتوکل: قوانینی که تحت آن کامپیوتر ها به یکدیگر در ارتباط هستند.

واضح است که جهت ارتباط در شبکه کانالی برای انتقال اطلاعات نیاز است که غالباً امروزه از کابل های جفتی دوقلو (Twisted-Pair) استفاده می شود. این نوع کابل دو مدل دارد که یکی دارای روکش (STP) و دیگری بدون روکش (UTP) می باشد که نوع دوم آن بیشتر مورد استفاده قرار می گیرد. در شکل زیر نوع بدون روکش (UTP) آن را ملاحظه می فرمایید.

قطعه دیگری که در شبکه نیاز است،دستگاه جعبه ای شکلی است که به آن Hub گفته میشود. هر کامپیوتر با یک کابل مجزا از کارت شبکه خود به این دستگاه متصل شده است.

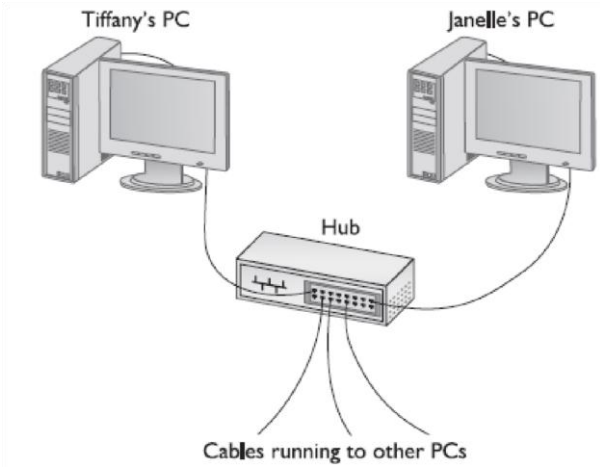
لایه یک شبکه نحوه انتقال اطلاعات بین کامپیوتر را بیان می کند و با این تعریف کابل و Hub در این لایه (Physical) جای می گیرند.

جادوی اصلی را در شبکه کارت های شبکه (NIC) به وجود آورده اند که به عنوان یک رابط (Interface) بین کامپیوتر و شبکه قرار گرفتند. (Interface در معنای لغوی رابط تعریف شده است اما برای فهم بهتر این کلمه از این تعریف استفاده می کنیم: هر قطعه یا دستگاهی که وظیفه ارسال و دریافت اطلاعات از شبکه را دارا باشد Interface نام دارد). کارت شبکه در شکل زیر نشان داده شده است.



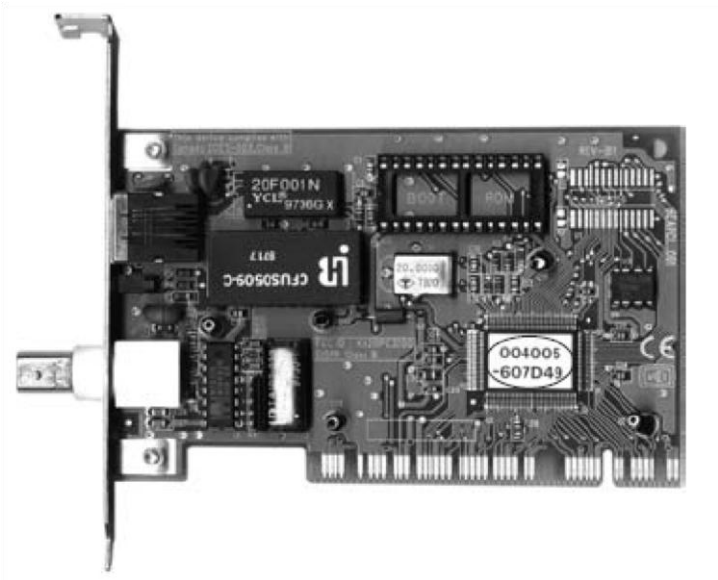
همانطورکه در شکل نیز میبینید کارت های شبکه در قدیم به صورت جدا و در صورت نیاز به سیستم ها وصل میشدند،اما امروزه بر روی تمام مادربردها تعبیه شده است و اگر شما بیش از آن را نیاز داشته باشید می توانید آن را جدا تهیه کرده و به سیستم خود اضافه نماید. در طراحی شبکه های امروزی یک رشته کابل از کارت شبکه به اتصالگر تعبیه شده بر روی دیوار (Wall Jack) متصل شده و یک رشته نیز از داخل دیوار تا Hub ادامه پیدا کرده است.

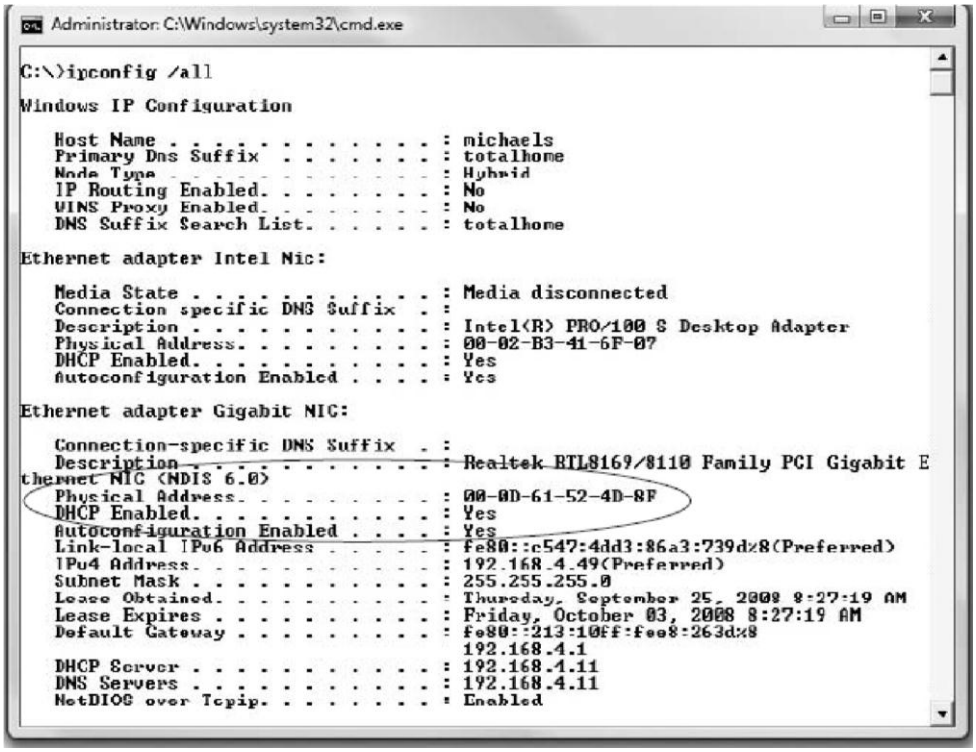
در اصل اتصالات شبکه به شکل زیر خواهد بود.



دستگاه کارت شبکه به علت فیزیکی بودن ظاهراً باید در لایه یک شبکه قرار گیرد اما، به علت نحوه عملکرد، آن را در لایه ۲ شبکه قرار داده اند. با نگاهی دقیق تر به کارت شبکه این موضوع روشن می شود.

آدرس دهی (مشخص کردن مبدأ و مقصد) در لایه دو شبکه بر عهده آدرسی است ۴۸ بیتی که در مبنای ۱۶ (Hex) نوشته می شود و به آن Media Access Control (MAC) **گفته می شود. این آدرس بر روی تمام** Interface **های دنیا وجود دارد و هیچ دو** Interface**ای در دنیا دارای آدرس** MAC **یکسان نیستند. ۲۴ بیت اول این آدرس کد کارخانه سازنده و ۲۴ بیت دوم کد دستگاه می باشد.**

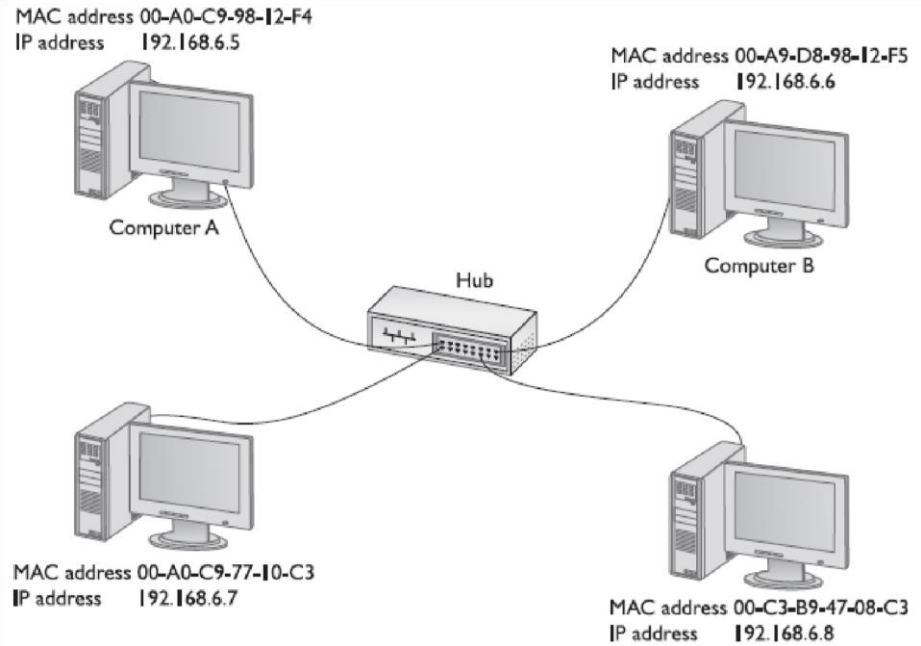




آدرس دهی در لایه ۲ شبکه بر اساس آدرس MAC می باشد و اگر جایی شنیدید که گفته شد فلان دستگاه در لایه ۲ شبکه کار می کند بدانید که منظور این است که نحوه آدرس دهی در آن (نشان دادن آدرس مبدأ و مقصد) با استفاده از MAC آدرس انجام می پذیرد.

IP همان آدرسی است که ما را از وابستگی زیاد به آدرس MAC جدا کرده و توانایی تقسیم کردن شبکه ها را به ما می دهد. IP آدرسی است ۳۲ بیتی که از چهار قسمت ۸ بیتی تشکیل شده که این قسمت های ۸ بیت در مبنای ۱۰ به صورت چهار عدد نوشته می شود که در محدوده 0 تا 255 تغییر می کنند، مانند 192.168.10.25

پس کامپیوتر های شبکه ما دارای دو آدرس شدند. اول آدرس MAC که در لایه دو شبکه (Data-Link) فعال است و بر روی کارت شبکه توسط کارخانه سازنده درج می شود و آدرس IP که در لایه ۳ شبکه فعال است و توسط کاربر تعیین می شود.



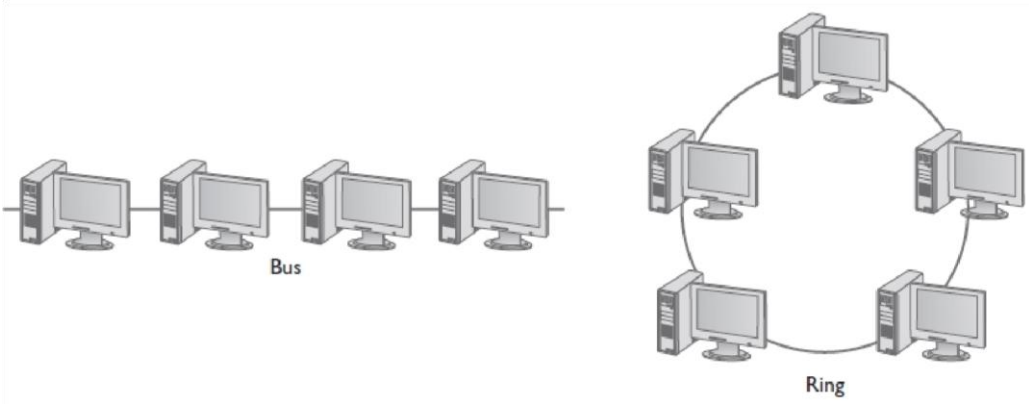
روتر ها جهت متصل کردن شبکه های مجزا به یکدیگر با استفاده از آدرس IP این کار را انجام می دهند و به دلیل وجود آدرس IP در لایه سه شبکه روتر ها و عملکرد آنها نیز در این لایه قرار می گیرد.

کابل کشی و توپولوژی

طبیعتاً در بحث شبکه باید بستری وجود داشته باشد که اطلاعات از روی آن، از یک سیستم به سیستم دیگر منتقل شود. غالباً امروزه از کابلها (مسی یا فیبر نوری) استفاده می شود و بعضی نیز از بستر بی سیم (Wireless) جهت این موضوع استفاده می کنند. استفاده از روش کابل کشی نیازمند داشتن دانش و مهارت می باشد تا بتوان یک کابل کشی منظم را ایجاد کرد.

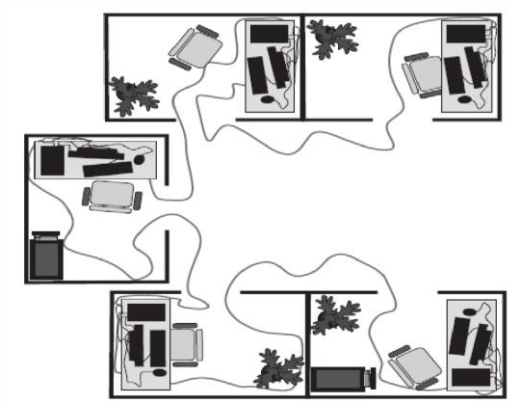
توپولوژی Bus و Ring

در توپولوژی Bus روش کار به این صورت بود که کامپیوتر ها به صورت پشت به پشت به یکدیگر متصل می شدند و ارتباط کامپیوتر ها با هم به صورت دست به دست شدن اطلاعات از مبدأ تا مقصد صورت می گرفت.

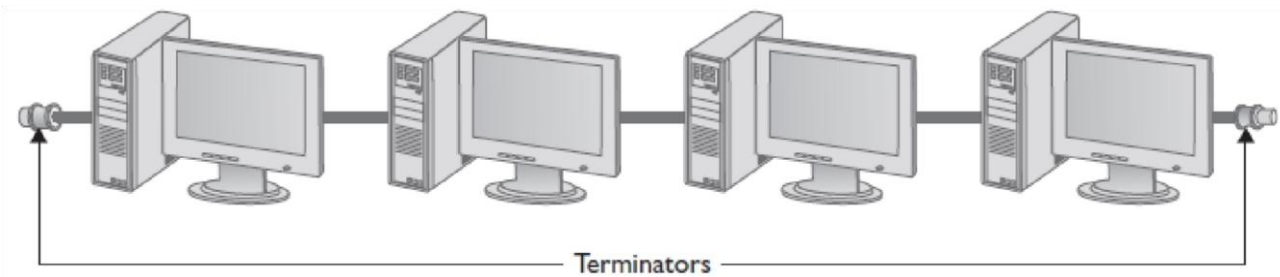


در توپولوژی Ring انتقال اطلاعات به صورت حلقه ای انجام می گرفت. البته به این نکته توجه کنید که ساختار انتقال اطلاعات به شکل حلقه بوده ولی ساختار فیزیکی شبکه به شکل حلقه نیست. یعنی اینطور نیست که ابتدا و انتهای رشته کابلی که کامپیوتر ها را به هم متصل کرده به یکدیگر وصل کنیم.

همانطور که در شکل زیر ملاحظه می فرمایید استفاده از توپولوژی Bus نیازمند متصل کردن کامپیوتر ها از یک اتاق به کامپیوتر های اتاق دیگر می باشد و می تواند مشکلات زیادی را برای ما به وجود آورد که البته این توپولوژی دیگر منسوخ شده و در شبکه های امروزی استفاده نمی شوند.



در توپولوژی Bus برایاینکه اطلاعات روی کابل دچار Loop نشوند در دو سرانتهاو ابتدای کابلها از Terminatorاستفاده می کردند تا داده های رسیده به انتها کابل دوباره به سمت فرستنده بر نگردد.

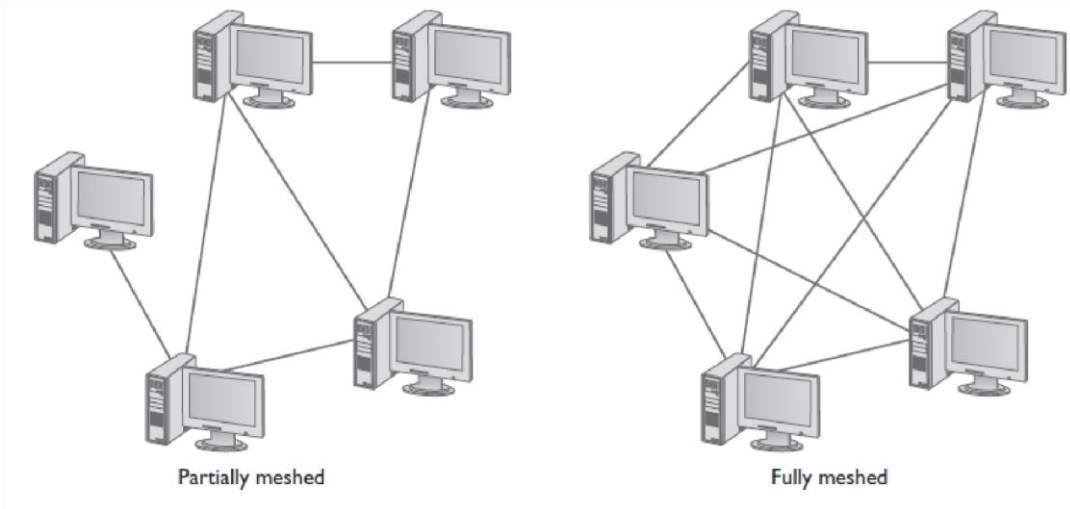


توپولوژی Star

در این توپولوژی یک جعبه تقسیم وظیفه اتصال کامپیوترها به یکدیگر را بر عهده دارد که سوئیچ نام دارد و جایگزین Hub های قدیمی شده است. دراین حالت اگر اتصال یک کامپیوتر با سوئیچ قطع شود، بر خلاف توپولوژی Bus، اتصال بقیه سیستم ها با یکدیگر قطع نمی شود و فقط همان کامپیوتر از مدار خارج می شود و خللی در روند کار بقیه سیستم ها ایجاد نمی شود.

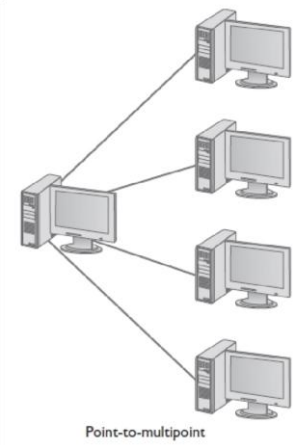
توپولوژی های Mesh و Point-to-Multipoint :

توپولوژی Mesh به دو حالت وجود دارد. یا کامپیوتر ها به بعضی از سیستم ها اتصال مستقیم دارند (Partial Mesh) و یا همه سیستم ها به بقیه ارتباط مستقیم دارند و استثنایی وجود ندارد که به آن Full Mesh گویند.



تعداد اتصالات در حالت Full Mesh برابر است با: $N(N-1)/2$ که در این فرمول N تعداد کامپیوتر هاست.

در توپولوژی Point-to-Multipoint همه سیستم ها به یک کامپیوتر مرکزی متصلند و این کامپیوتر ارتباط سایرین را بر قرار می کند.



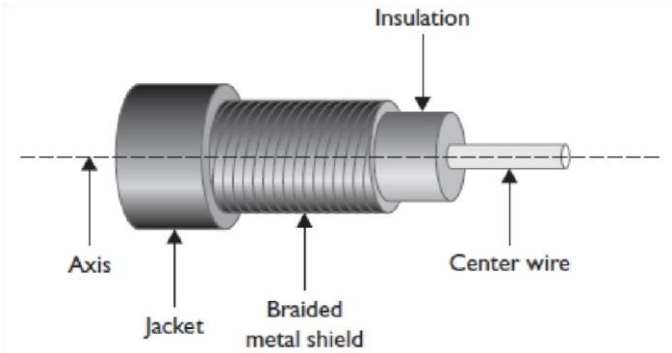
البته به خاطر داشته باشیم که این دو نوع توپولوژی (Mesh, Point-toPoint) در شبکه های WAN کاربرد دارند و نه در شبکه های LAN.

نوعی دیگر از توپولوژی نیز وجود دارد که باز هم در شبکه های WAN بیشترمورداستفاده قرارمی گیرد که در آن یک سیستم مستقیماً به سیستم دیگری متصل است که به آن Point-to-Point گویند.

کابل کشی توپولوژی ها

به طور معمول ما در توپولوژی های شبکه از سه نوع کابل استفاده می کینم: Coaxial، جفتی دوقولو (Twisted Pair) و فیبر نوری (Fiber Optic).

Coaxial



این نوع کابل در توپولوژی Bus مورد استفاده قرار می گرفت و شبیه همین کابل های آنتن است که ما امروزه جهت دریافت تصاویر تلویزیونی از آنها استفاده می کنیم. امروزه در شبکه ها از این نوع کابل استفاده نمی شود.

در توپولوژی Bus برای اتصال این نوع کابل به کامپیوتر ها از اتصالگر های BNC استفاده می شد.

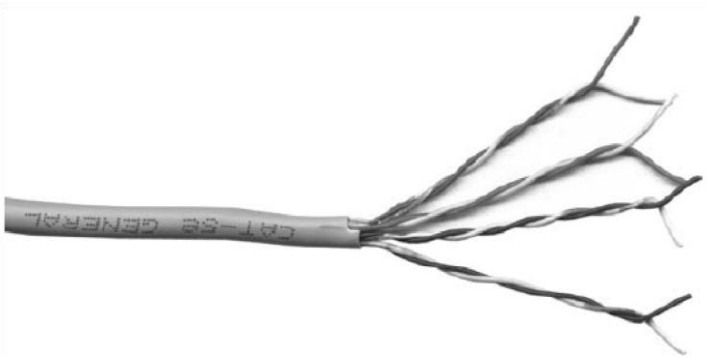
کابل های جفتی دوقلو: این نوع کابل های که امروزه متداول ترین نوع کابل جهت اتصال اجزاء مختلف شبکه به یکدیگر می باشد به دو نوع کلی تقسیم می شود. Shielded Twisted Pair (STP) , Unshielded Twisted Pair (UTP). در این نوع کابل از هشت رشته سیم مسی استفاده شده که وظیفه جابجایی اطلاعات را بر عهده دارند.

جفتی دوقلوی روکش دار (Shielded Twisted Pair)

نوع روکش دار جهت جلوگیری از تأثیر میادین مغناطیسی بر روی اطلاعات عبوری بر روی سیم های داخل کابل می باشد. این نوع روکش ها مانند عایق عمل می کنند و قیمت آن از نوع بدون روکش آن بیشتر است و تنها در مکان هایی استفاده می شود که احتمال تأثیر میدان مغناطیسی بر روی اطلاعات عبوری داده می شود که نمونه آن را در تصویر زیر مشاهده می فرمایید.

جفتی دوقلو بدون روکش (Unshielded Twisted Pair)

این نوع کابل روکش ندارد پس در برابر تأثیر میادین مغناطیسی مقاومت نوع قبل را نخواهد داشت ولی از نوع روکش دار ارزان تر است و امروزه در شبکه ها به صورت گسترده ای استفاده می شود.



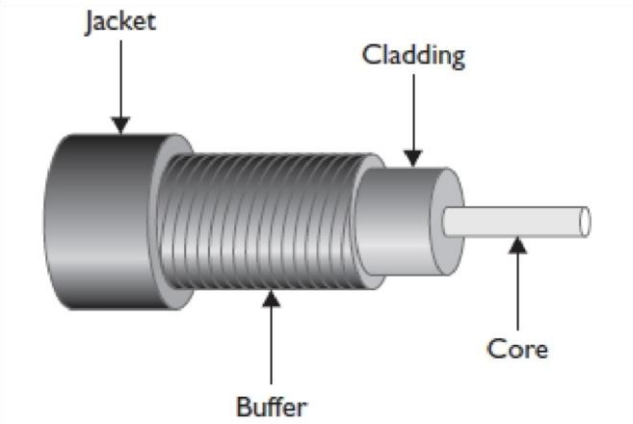
کابل های جفتی دوقلو براساس فرکانس وپهنایباندی کهارائه می دهند دستهبندیشده اندکهبه این دسته بندیها Category گفته می شود و در شبکه های امروزی CAT6, CAT5e, CAT5 مورد استفاده قرار می گیرند.

CAT Rating	Max Frequency	Max Bandwidth	Status with TIA/EIA
CAT 1	< 1 MHz	Analog phone lines only	No longer recognized
CAT 2	4 MHz	4 Mbps	No longer recognized
CAT 3	16 MHz	16 Mbps	Recognized
CAT 4	20 MHz	20 Mbps	No longer recognized
CAT 5	100 MHz	100 Mbps	No longer recognized
CAT 5e	100 MHz	1000 Mbps	Recognized
CAT 6	250 MHz	10000 Mbps	Recognized

کابلهای جفتی دوقلو دارای محدودیت طول ۱۰۰ متر هستند که بهتر است شما در کابل کشی و جهت اطمینان بیشتر این محدودیت را ۹۰ متر در نظر بگیرید.

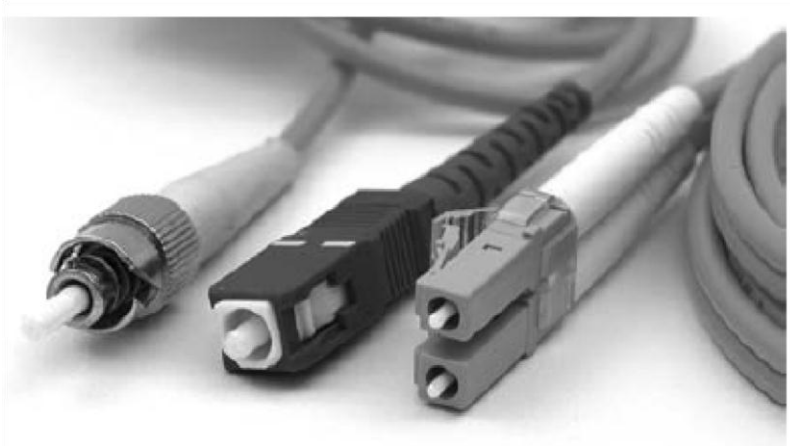
کابل فیبر نوری

در این نوع کابل اطلاعات به صورت پالس های نوری فرستاده می شود و غالباً اطلاعات را در طول های بیشتری جابجا می کنند.



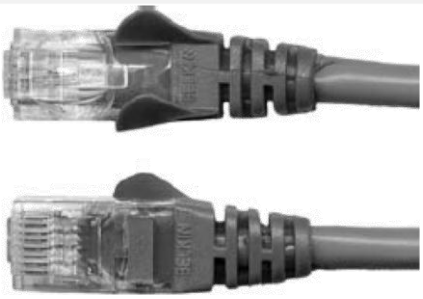
هسته مرکزی این نوع کابل (Core) و روکش آن (Cladding) با قطر های مختلفی ساخته می شوند که متداول ترین آن دارای قطر *125/5.62 µm* می باشد. در کابل های فیبر نوری که دو رشته ای هستند همیشه یک رشته فرستنده و رشته دیگر گیرنده می باشد که در بعضی از انواع کابل فیبر نوری دو رشته را در یک اتصالگر نصب کرده اند که بازهم یکی فرستنده و رشته دیگر گیرنده می باشد. نمونه ای از این نوع کابل را در تصویر زیر می بینید که از اتصالگر MT-RJ استفاده کرده است.

کابل های فیبر نوری به دو دسته تقسیم می شوند. دسته اول Multimode **که جهت ارسال اطلاعات از** LED **استفاده می کند و دسته دوم** Single Mode **که جهت ارسال اطلاعات از لیزر استفاده می نماید. در تصویر زیر انواع اتصالگر های فیبر را ملاحظه می فرمایید که از چپ به راست** ST،SC **و** LC **می باشند.**

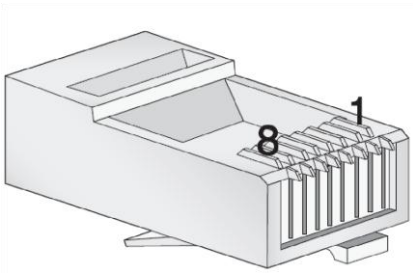


شبکه های Ethernet قدیمی

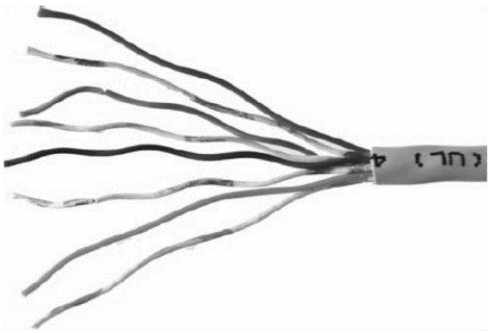
در اوایل دهه ۹۰ میلادی IEEE**، بهینه شده** Ethernet **را با نام** BaseT10 **به بازار عرضه کرد که از کابل های جفتی دوقلو، اتصالگر های** RJ-45 **و** Hub **استفاده می شد. در عبارت** BaseT10 **عدد ۱۰ نشان دهنده سرعت** 10Mbps**،** Base **مخفف کلمه** Baseband **و** T **به معنای** Twisted-Pair **می باشد. نمونه ای از** Hub **ها را در تصویر زیر ملاحظه**



اتصالگر های RJ-45 **دارای هشت** Pin **هستند که ازچپ به راستمانند تصویر زیر شماره گذاری می شوند.**

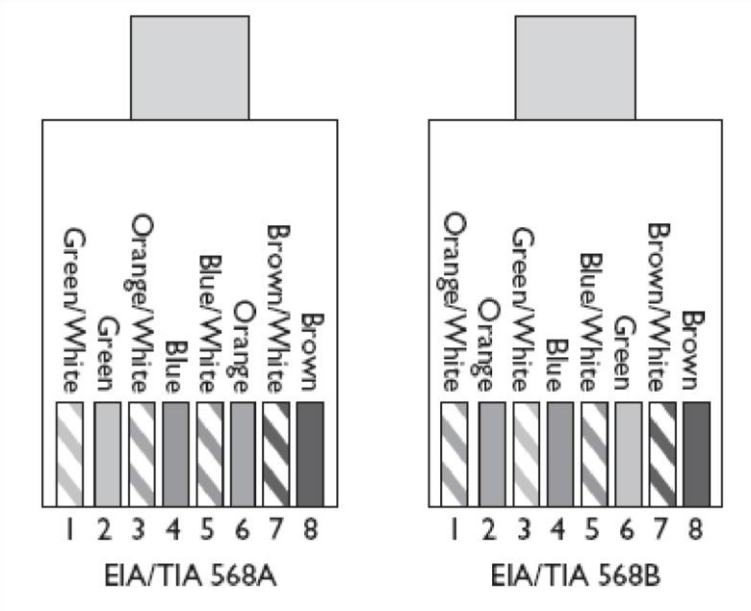


ما با استفاده از رنگ بندی استاندارد هشت رشته سیم در کابل جفتی دوقلو را داخل اتصالگر های RJ-45 **قرار می دهیم و با استفاده از آچار شبکه** (Crimper) **آن را پانچ می کنیم.**



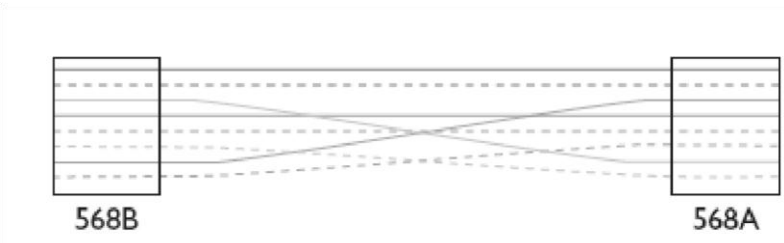
بر طبق مصوبه TIA/EIA **ما دارای دو استاندارد برای رنگ بندی کابل های جفتی دوقلو هستیم که عبارتند از:**

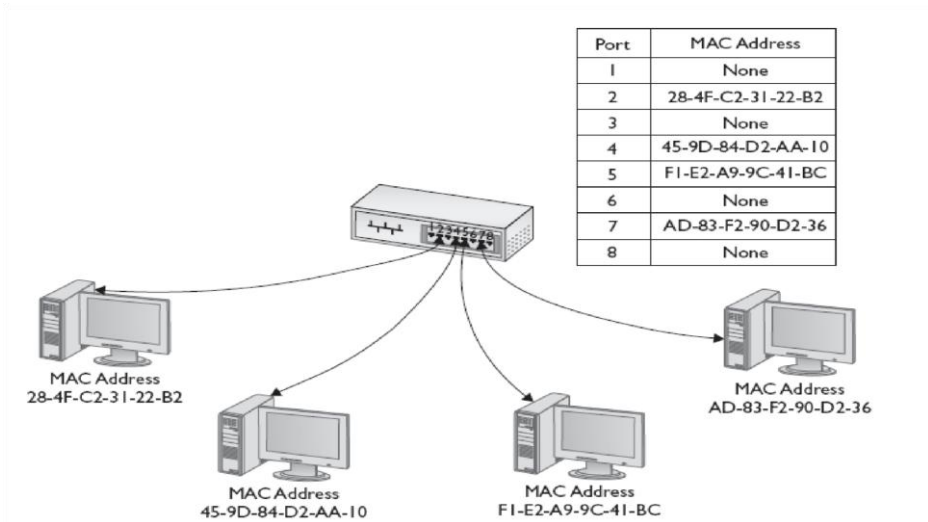
TIA/EIA 568A and TIA/EIA 568B **و در تصویر زیر نیز این رنگ بندی را ملاحظه می فرمایید.**



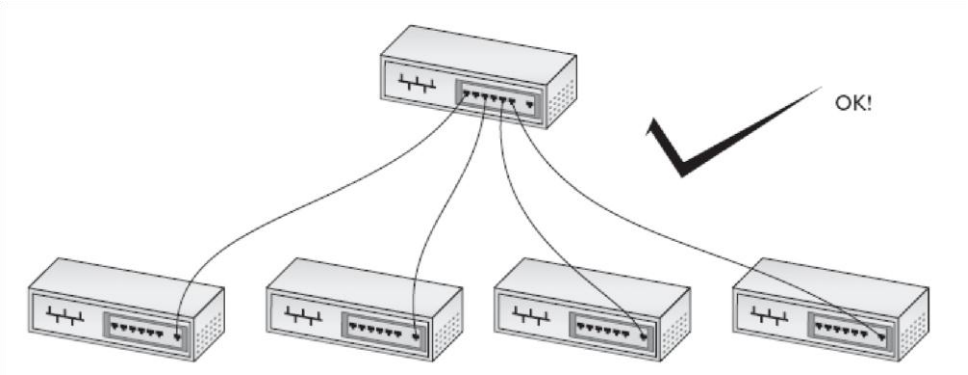
بر طبق استاندارد برای اتصال دو دستگاه مشابه مانند PC **به** PC**، روتر به روتر، سوئیچ به سوئیچ و روتر به** PC **اتصال ما باید از نوع** Cross-Over **باشد و برای اتصال دو دستگاه غیر مشابه مانند** PC **به سوئیچ، روتر به سوئیچ و ... اتصال باید از نوع** Straight **باشد. اگر دو سر کابل ما زمان اتصال به اتصالگر های** RJ-45 **از یک استاندارد تبعیت کند کابل ما** Straight **و اگر یک سر کابل از استاندارد** 568B **و سر دیگر** 568A **باشد کابل ما از نوع** Cross-Over **می باشد.**

هنگامی که از حالت Cross-Over **استفاده می کنیددر واقع** Pin 1 **از یک سر کابل به** Pin 3 **سر دیگر و** Pin 2 **به** Pin 6 **سر دیگر کابل متصل است.**





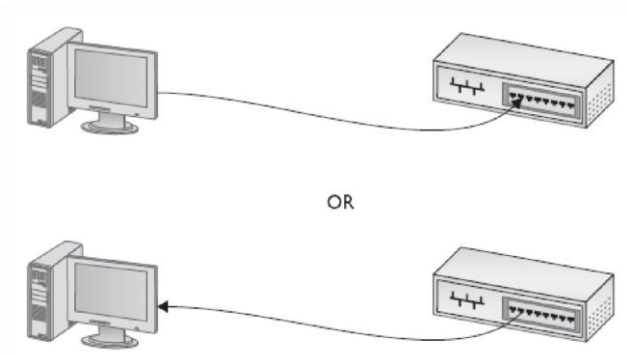
از دیگر مزیت های سوئیچ ها این است که جهت اتصال به سایر سوئیچ ها تنها محدود به پورت های Uplink نیستند و هر کدام از پورت های سوئیچ می توانند جهت Uplink استفاده شوند. البته در دنیای حرفه ای شبکه به جای عبارت Uplink از لفظ Trunk استفاده می شود.



همانطور که در تصویر زیر ملاحظه می فرمایید Hub و سوئیچ از نظر ظاهری شبیه به هم هستند ولی نحوه عملکرد آنه با هم فرق می کند. در تصویر زیر در بالا Hub و در پایین سوئیچ قرار دارد.

به صورت کلی شبکه های Ethernet دارای سرعت های 10,100,1000 (1G), 10000 (10G) Mbps هستند که امروزه سرعت 10Mbps دیگر وجور ندارد و سرعت 100Mbps نیز آرام آرام از رده خارج می شود. در شبکه قانونی وجود دارد به نام Flow Control که بر طبق این قانون سیستمی که می تواند با سرعت بالاتری انتقال اطلاعات انجام دهد باید خود را با سیستمی که سرعت پایین تری دارد منطبق کند.

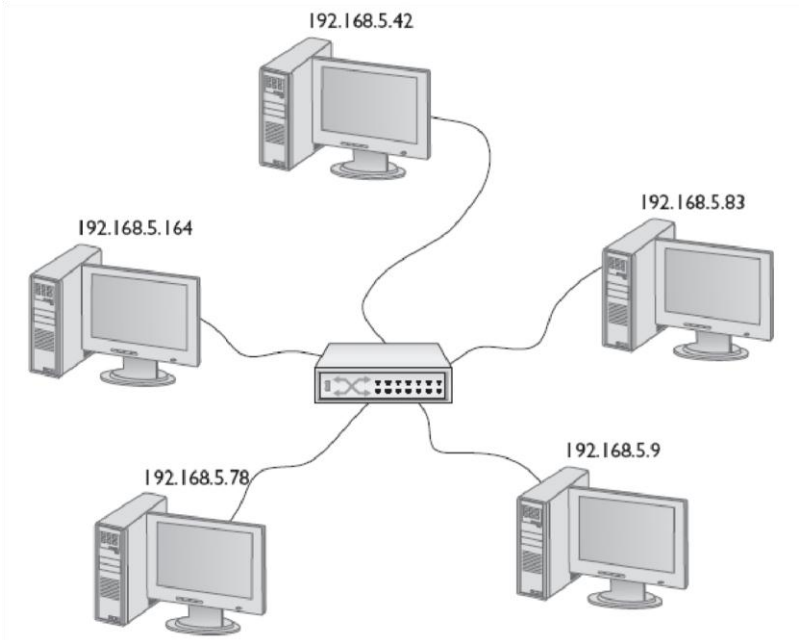
از دیگر قوانین شبکه Duplex می باشد که به دو حالت Half و Full می تواند وجود داشته باشد. در حالت Half Duplex همیشه یک سیستم فرستنده و سیستم دیگر گیرنده می باشد که طبیعتاً سرعت انتقال به نصف کاهش می یابد.



در حالت Full Duplex که حالت ایده آل برای ما محسوب می شود هر دو سیستم همزمان هم فرستنده و هم گیرنده هستند.

TCP/IP

همانطور که قبلاً دیدیم زمانی که در مورد لایه های شبکه و نحوه آدرس دهی هر کدام از لایه ها بحث شد گفتیم که آدرس دهی در لایه سه شبکه با IP می باشد. IP آدرسی است ۳۲ بیتی در مبنای ۱۰ که به صورت چهار عدد که با نقطه (Dot) از یکدیگر جدا می شوند نوشته می شود. این چهار عدد می توانند بین 0 تا 255 تغییر کنند. بر طبق قانون شبکه هر سیستم فعال در شبکه باید دارای یک آدرس واحد و منحصر به فرد باشد و دو سیستم با یک آدرس IP پذیرفته نیست.



آدرس IPای که ما هم اکنون در مورد آن صحبت می کنیم نسخه ۴ از IP است که البته نسخه ۶ آن نیز وجود دارد که در فصول بعد به آن اشاره خواهد شد. IP نسخه ۴ به صورت استاندارد به پنج کلاس دسته بندی می شود که ۲ تای آن جهت استفاده خاص از بحث ما خارج می شوند و ۳ کلاس باقی مانده مورد بحث ما خواهند بود. دو کلاسی که از حوزه بحث ما خارج هستند کلاس D (استفاده می شود جهت ارسال ترافیک Multicast) و کلاس E که جهت تحقیقات رزرو شده است. کلاس های A,B,C جهت انتقال اطلاعات به حالت Unicast که عمده ترافیک یک شبکه را شامل می شود بکار می رود.

	First Decimal Value	Addresses	Hosts per Network ID
Class A	1–126	1.0.0.0–126.255.255.255	16,277,214
Class B	128–191	128.0.0.0–191.255.255.255	65,534
Class C	192–223	192.0.0.0–223.255.255.255	254
Class D	224–239	224.0.0.0–239.255.255.255	Multicast
Class E	240–255	240.0.0.0–255.255.255.255	Reserved

همانطور که در جدول نیز دیده می شود عدد ۱۲۷ بین کلاس A وB حذف شده. آدرس IPیی که با ۱۲۷ شروع شود (معروف ترین آن127.0.0.1) به عنوان آدرس Loopback استفاده می شود. بسته اطلاعاتی که به مقصد آدرس Loopback فرستاده شود هیچگاه از کارت شبکه فرستنده خارج نمی شود.

در بحث آدرس IP علاوه بر خود IP عبارتی به نام Subnet mask نیز وجود دارد. Subnet mask محدوده تغییرات IP را نشان می دهد. Subnet mask نیز مانند IP از چهار عدد تشکیل شده که با نقطه از یکدیگر جدا شده اند. سه کلاس IP که مورد بحث ما هستند دارای Subnet mask های پیش فرض خود هستند که در پایین به آنها اشاره شده است. هر کدام از قسمت های Subnet mask محدوده تغییرات قسمت متناظر آن را در IP نشان می دهد. یعنی مثلاً عدد سوم از Subnet mask محدوده تغییرات قسمت سوم آدرس IP را نشان می دهد.

Class A: **255.0.0.0**
Class B: **255.255.0.0**
Class C: **255.255.255.0**

Subnet mask های نوشته شده در بالا پیش فرض هر کلاس از IP است و می بینید به صورت استاندارد 0 یا 255 می باشند. البته جلوتر خواهیم دید که به جزء این دو عدد، اعداد دیگری نیز می توانند باشند. آن چه در Subnet mask جهت آدرس دهی صحیح حائز اهمیت است تبدیل آن از مبنای ۱۰ به مبنای ۲ می باشد. تبدیل Subnet mask پیش فرض هر کلاس از مبنای ۱۰ به مبنای ۲ خروجی زیر را به ما خواهد داد.

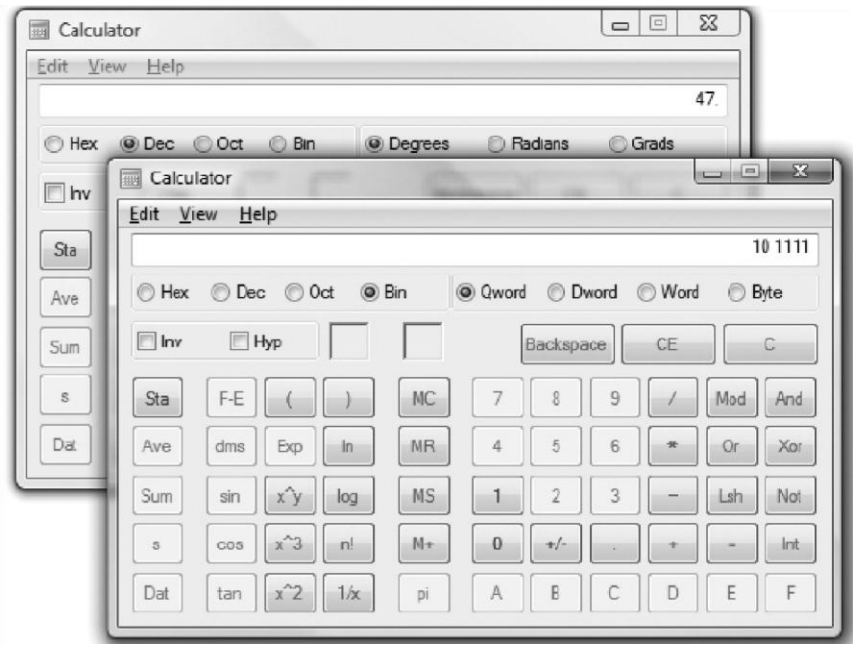
Class A: 11111111 . 00000000 . 00000000 . 00000000 /8
Class B: 11111111 . 11111111 . 00000000 . 00000000 /16
Class C: 11111111 . 11111111 . 11111111 . 00000000 /24

به صورت استاندارد می گوییم آن قسمت از Subnet mask که دارای بیت های یک باشد قسمت Network ID و آن قسمت از Subnet mask که دارای بیت های صفر است Host ID نام دارد. Network ID معرف تعداد شبکه و قسمت

Host ID معرف تعداد کاربرانی است که در آن شبکه می توانند حضور داشته باشند. پس همانطور که از وضعیت بیتهای صفر و یک کلاس ها مشخص است، وقتی از کلاس A که به سمت کلاس C حرکت می کنیم قسمت Network ID بزرگتر و قسمت Host ID کوچکتر می شود. پس از سمت A به سمت کلاس C تعداد شبکه های افزایش ولی تعدادکاربرانی که در هر شبکه می توانند باشند کمتر می شود. اعدادی را نیز که بعد از بیت های Subnet mask با " / " نشانداده شده اند Prefix Length نام دارد و در واقع تعداد کل یک های Subnet mask را نشان می دهد. از این پس می توانید به جای نوشتن Subnet mask از Prefix Length استفاده کنید.

مثلاً به جای نوشتن 255.255.255.0 (192.168.1.0) می توان نوشت (192.168.1.0/24) که این Prefix Length در واقع نشان دهنده همان Subnet mask است و شما با این کار Subnet mask را خلاصه کرده و به صورت یک عدد درپشت IP نمایش می دهید.

جهت تبدیل اعداد از مبنای ۱۰ به مبنای ۲ می توانیم از تقسیمات متوالی بر ۲ استفاده کنیم. تقسیم متوالی عدد ۲۵۵ بر ۲ معادل ۱۱۱۱۱۱۱۱ خواهد بود. البته از حالت مهندسی ماشین حساب Windows نیز می توانید استفاده کنید، اما به هر حال به عنوان مهندس شبکه دانستن روش تبدیل بهتر است. در تصویر زیر تبدیل عدد ۴۷ از مبنای ۱۰ به مبنای ۲ با استفاده از ماشین حساب Windows Vista دیده می شود.



بر اساس استاندارد هر قسمت از Subnet mask که دارای عدد 1 باشد به عنوان Network ID و هر قسمت از آن کهدارای عدد 0 باشد به عنوا ن Host ID شناخته می شود. قسمت Network ID نشان دهنده تعداد شبکه و قسمت Host

ID نشان دهنده تعداد کاربران هر شبکه می باش ـد. بـا ایـن حـساب در کـلاس A قـسمت اول Subnet mask کـلاً دارای ۱ است پس Network ID محسوب می شود و با در نظر گرفتن ۱۲۶ عددی که در قسمت اول IP در ایـن کـلاسوجود دارد ما می توانیم در کلاس A از IP، دارای ۱۲۶ شبکه باشیم که در هر کدام از آنها ۲۱۶ ۷۷۲ ۱۶ کـار بـر وجـودداشته باشد.

به یاد داشته باشیم که آدرس های IP از نظر نوع کارکرد به دو دسته عمده تقسیم می شوند: Public و Private آدرس های Public جهت استفاده بر روی اینترنت استفاده می شوند و مدیریت این نوع آدرس های IP بر عهده موسسه IANA می باشد. جهت استفاده از این نوع آدرس باید وجهی را پرداخت نمایید و IP مورد نظر را اجاره کنید. نوع دوم آدرس های Private می باشند که جهت استفاده در شبکه های داخلی بکار می روند و به صورت آزاد در تمام دنیا و بدون محدودیت می توان از آنها استفاده کرد. مدیریت این نوع از IP در اختیار ماست، پس ما هم روی صحبت خود را بر روی این نوع استاندارد از آدرس های IP می گذاریم. آدرس های Private در زیر آورده شده است. سایر IP هایی که در لیست زیر نیستند جزء IP های Public هستند و ما به آنها کاری نداریم. از هر کدام از سه کلاس A,B,C نماینده هایی جهت IP های Private جدا کرده اند و مابقی Public محسوب می شوند.

Class	IP اول رنج	IP آخر رنج	تعداد شبکه مجاز
A	**10.0.0.0**	**10.255.255.255**	۱
B	**172.16.0.0**	**172.31.255.255**	۱۶
C	**192.168.0.0**	**192.168.255.255**	۲۵۶

آنچه تا به حال دیدیم حالت استاندارد IP های موجود می باشد. آن چیزی که در محاسبه شـبکه هـایبـزرگ مطـرح مـیشود این است که ما برای محدود کردن ترافیک Broadcast که ترافیک مزاحم برای ما محسوب می شود باید پای خـودرا از حدود پیش فرض و استاندارد فراتر بگذاریم. مثلاً به کلاس A از IP های Private توجه بفرمایید. در ایـن محـدودهIP ما می توانیم یک شبکه داشته باشیم بـا ۲۱۶ ۷۷۲ ۱۶ تعـداد IP کـه ایـنتمـاممجموعـه بـزرگ زیـر مجموعـه یـکBroadcast Domain محسوب می شود و ایـن بـا محـدود کـردن ترافیـک Broadcast منافـات دا رد زیـرا کـه در ایـن جمعیت میلیونی اگر یکی از کاربران بسته اطلاعاتی خود را به صورت Broadcast بر روی شبکه بفرستد با اینکه مخاطـباو ممک ن است یک نفر و یک IP واحد و مشخص می باشد ۲۱۴ ۷۷۲ ۱۶ کامپیوتر باید این بسته اطلاعاتی را کـه

بـه آنهـامربوط نمی شود دریافت کرده و بی جهت پردازش کنند. Broadcast Domain **محدوده ایست که اگر یکی از کـامپیوت ر های موجود در آن بسته اطلاعاتی خود را به حالت** Broadcast **بر روی شبکه بفرستد به دست تمام اعضای ایـن محـدودهخواهد رسید و برای جلوگیری از این موضوع باید** Broadcast Domain **ها را به اندازه های معقول تقـسیم بنـدی کنـیم. توجه به این موضوع الزامیست که جدا کردن سیستم ها از یکدیگر و قرار دادن آنها در** Broadcast Domain **های مجزا به منزله قطع ارتباط بین آنها نیست بلکه فقط اجـازه عبـور ترافیـک** Broadcast **بـین دو قـسمت را نمـی دهـیم و ارتبـاط**Unicast **به قوت خود می تواند وجود داشته باشد. تنها تفاوت این حالت با زمانی که همه سیـستم هـا زیـر مجموعـه یـک**Broadcast Domain **بودند این است که برای برقراری ارتباط بین** Broadcast Domain **های جدا شـده بایـد از روتـراستفاده کنیم. برای آشنایی با روش کار به مثال زیر توجه فرمایید.**

رنج آدرس 192.168.1.0 **با** subnet mask **برابر با** 255.255.255.0 **را در نظر بگیرید. مجموعه آدرس یک شبکه را نشان می دهد که در برگیرنده ۲۵۶ آدرس** IP **می باشد. فرض کنید که ما بخواهیم این مجموعه را به چهار شبکه مجزا تقسیم کنیم. از دو فرمول زیر استفاده می کنیم. علامت " ^ " به معنای *توان* می باشد. ما می خواهیم این مجموعه ۲۵۶ کاربر که یک** Broadcast Domain **محسوب می شود را به چهار قسمت مساوی تقسیم کنیم.**

تعداد شبکه ها = 2^N

تعداد کاربران هر شبکه = 2^H

حال که این شبکه قرار است به چهار قسمت مجزا تقسیم شود از فرمول 2^N **استفاده می کنیم.**

2^N = 4 _ _ _▸ N = 2

N **تعداد صفرهایی از** Subnet Mask **پیش فرض می باشد که *باید به یک تبدیل شوند* و** H **تعداد صفر هایی هـستند کـه**

بعـد از تـشکیل N **در** Subnet mask **مـی تواننـد صـفر بـاقی بماننـد. مجموعـه آدرس تعیـین شـده بـرای ایـن سـناریو** 0.1.168.192 **می باشد که به صورت پیش فرض دارای** Subnet mask**ی برابـر بـا** 255.255.255.0 **یـا همـان** /24 **مـیباشد. برای راحتی کار باید** Subnet mask **را از مبنای ده به مبنای دو تغییر دهیم.**

آن= 255.255.255.0 11111111 . 11111111 . 11111111 . ***00000000***

قسمتی از Subnet mask **که ما برای حل این گونه صورت مسئله ها می توانیم استفاده کنیم قسمتی است که دارای بیت های *صفر* است و آن قسمتی که دارای بیت های یک است قابل دستکاری نیست و دیگر از کنترل ما خارج شده است.**

پس ما فقط دارای هشت عدد بیت صفر هستیم که می توانیم روی آن مانور انجام دهیم. بر طبق تعریف N **ما می توانیم دو تا از صفر های** Subnet mask **را به یک تبدیل کنیم پس خواهیم داشت:**

11111111 . 11111111 . 11111111 . ***11000000***

با انجام این تبدیل که حاصل استفاده از فرمول 2^N **بود تعداد صفر های باقی مانده برای ما شش می باشد که این صفر های باقی مانده همان** H **را تشکیل می دهد. پس خواهیم داشت:**

2^6 = 64

این فرمول به ما نشان می دهد که ما در چهار شبکه ای که داریم می توانیم در هر کدام ۶۴ آدرس IP **و در حقیقت ۶۴ کاربر داشته باشیم. توجه به این نکته الزامیست که ما دو بیت از صفرهای** Subnet mask **را به یک تبدیل کردیم پس قاعدتاً قسمت آخر** Subnet mask **دیگر نمی تواند عدد "0" باشد. با تبدیل بیت های** 11000000 **به مبنای ده خواهیم داشت** 192**. پس** Subnet mask **جدید ما خواهد بود** ***192***.255.255.255..

مرحله بعد تعیین محدوده IP **های هر کدام از این چهار قسمت می باشد. جهت انجام صحیح این کار می توانید عدد ۱۹۲ در** Subnet mask **جدید را از عدد ۲۵۶ کسر کنید تا محدوده تغییرات هر کدام از این چهار قسمت مشخص شود.**

256 – 192 = 64

پس محدوده تغییرات هر کدام از این قسمت ها ۶۴ تایی خواهد بود. پس شروع می کینم.

192.168.1.0 ► 192.168.1.63

192.168.1.64 - - ► 192.168.1.127

- - ►

192.168.1.128 192.168.1.191

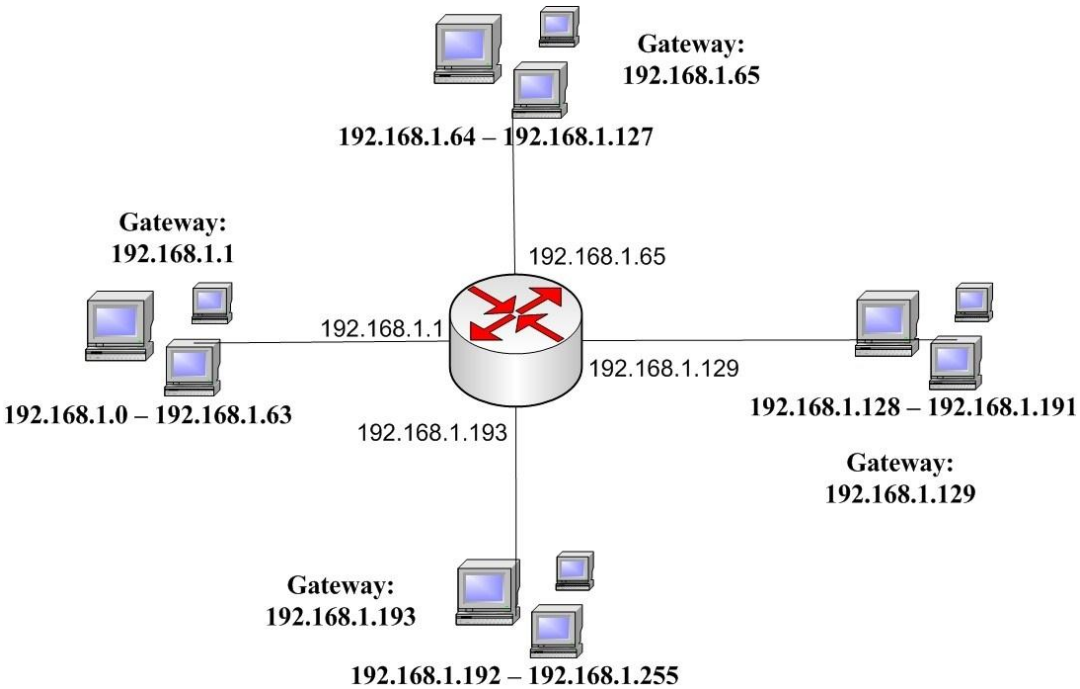
- - ►

192.168.1.192 -192.168.1.255

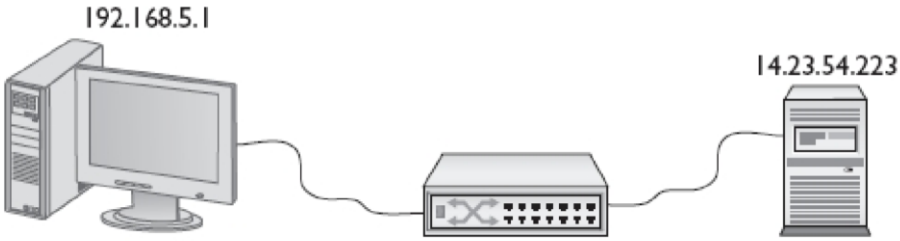
به این ترتیب شما دارای چهار شبکه هستید که در هر کدام ۶۴ آدرس IP **وجود دارد. توجه داشته باشد که عبارت** Subnet mask **برای هر چهار قسمت یکسان است** (Static Length Subnet Mask) **و برابر است با** (/26) **که همان** 255.255.255.192. **است و یا** prefix Length

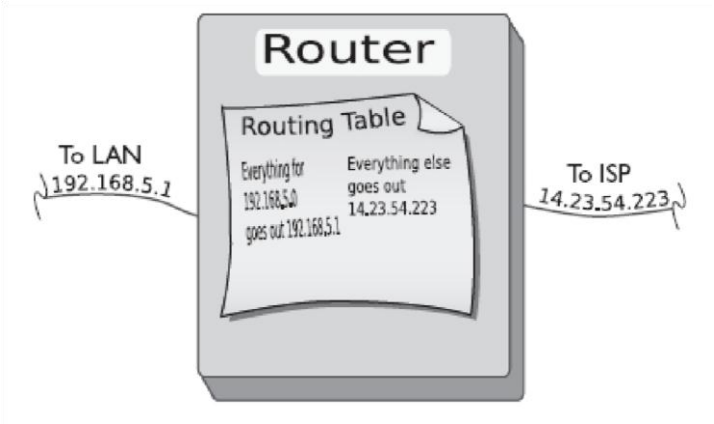
تبصره: در هر محدوده شما از IP اول و IP آخر نمی توانید استفاده کنید. IP اول به عنوان معرف مجموعه (Net ID) و IP آخر جهت انجام عملیات Broadcast (Broadcast IP) استفاده می شود. پس از مجموع ۶۴ تا IP ی موجود در هر مجموعه ۶۲ تای آن قابل استفاده است و می تواند بر روی کامپیوتر ها تنظیم شود.

همانطور که پیش تر هم گفته شد جهت اتصال شبکه های مختلف به یکدیگر ما به دستگاهی به نام روتر نیازمندیم که این اتصالات را برای ما فراهم کند. مثلاً برای سناریوی قبل که چهار شبکه ۶۴ تایی به وجود آمد برای اتصال این شبکه ها بهیکدیگر به یک روتر با چهار کارت شبکه (Interface) نیاز داریم. هر کدام از این Interface ها به عنوان خروجی(Gateway) برای یکی از این شبکه ها منظور می شود. آدرس IP یی که به هر کدام از این Interface های روتر میدهید جهت Gateway یک شبکهبودن حتماً باید دارای آدرسی در رنج همان شبکه باشد. مثلاً برایاینکه فلانInterface برای شبکه اول Gateway باشد باید یک از IP های محدوده 192.168.1.1 – 192.168.1.62 را به خود اختصاص دهد. بیاد داشته باشیم که آدرس اول و آخر هر رنج قابل استفاده نیست.



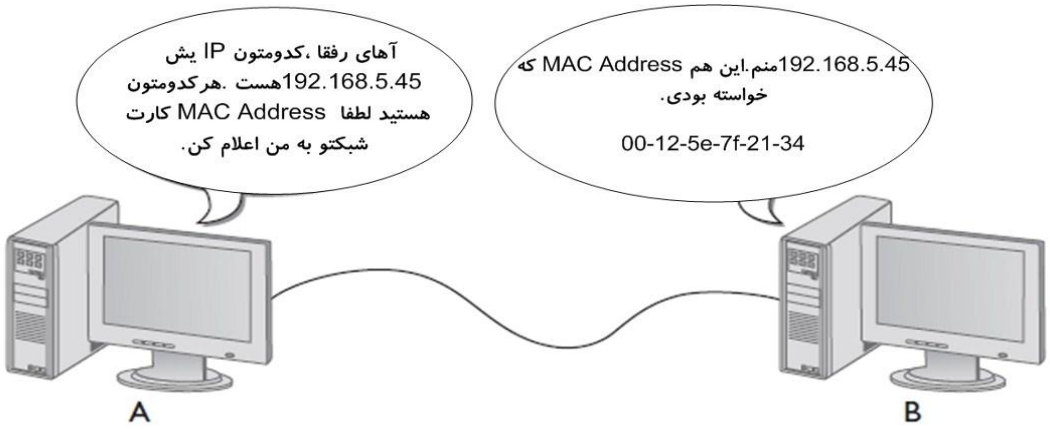
روترها جهت پیدا کردن مقصد و دسترسی به آن دارای جدولی هستند با نام جدول مسیر یابی (Routing Table) که این جدول به آنها بهترین مسیر به مقصد را نشان می دهد.



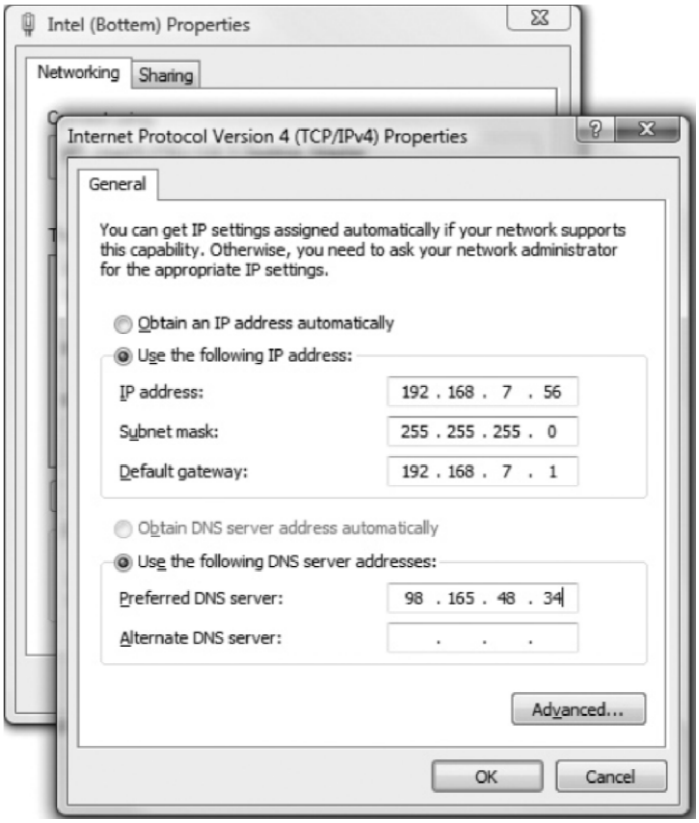


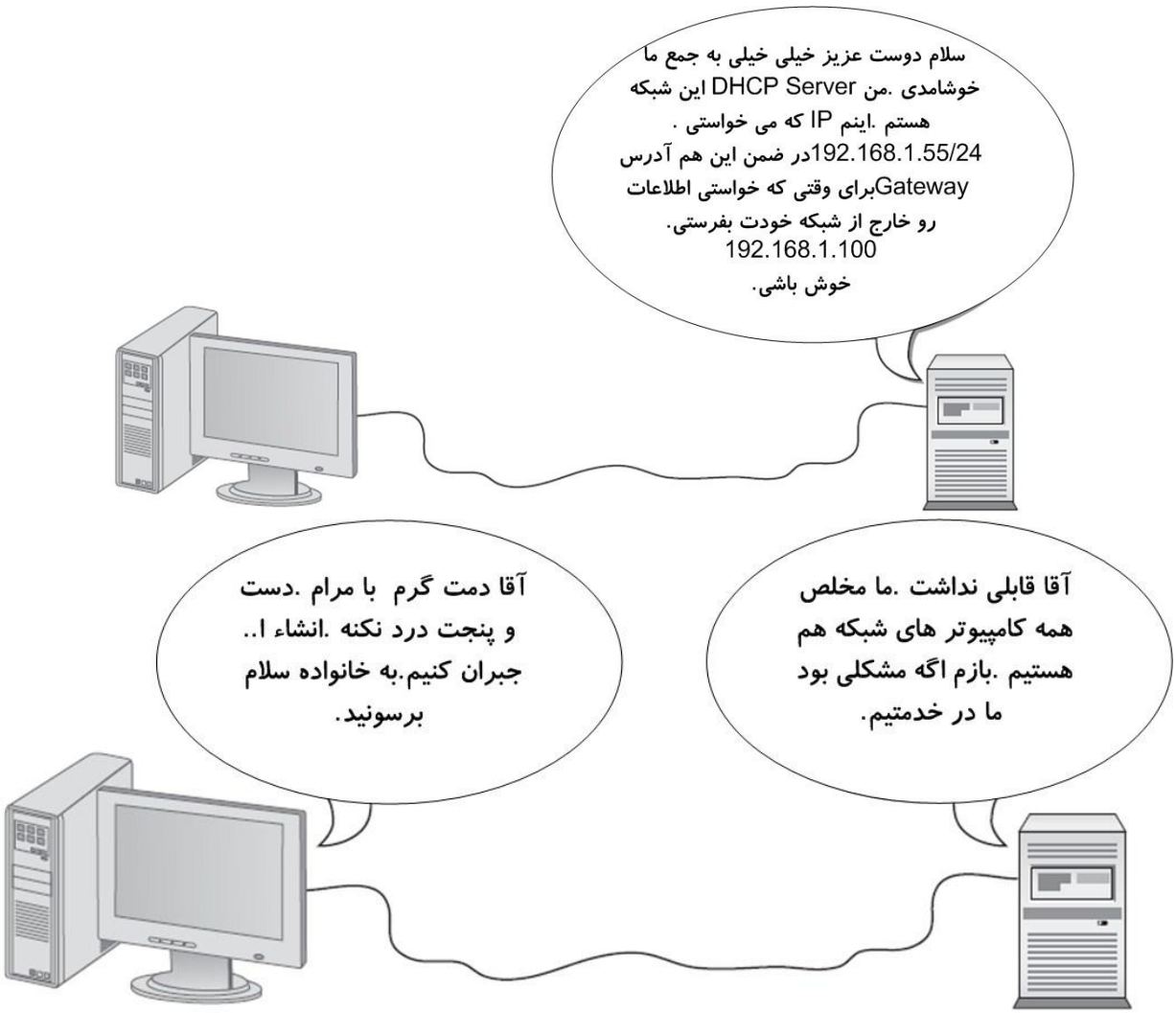
کامپیوتر ها جهت رسیدن به مقصد مورد نظر خود که خارج از شبکه (Subnet) **خود آنهاست بسته های اطلاعاتی را برای روتر خود** (Default Gateway) **می فرستند و روتر های موجود در طول مسیر نیز با استفاده از جدول مسیر یابی خود و دست به دست کردن بسته های اطلاعاتی آنها را به سمت مقصد رهنمون می کنند.**

از دیگر عملیات های موجود در TCP/IP **بحث** ARP **می باشد. کامپیوتر ها برای برقراری ارتباط بین یکدیگر نیازمند دانستن آدرس** MAC **سیستم مقصد می باشند. کامپیوتر فرستنده جهت پیدا کردن آدرس** MAC **سیستم مقصد از پروتوکل** Address Resolution Protocol (ARP) **استفاده می کند. کامپیوتر فرستنده درخواست خود را به صورت** Broadcast **بر روی شبکه می فرستد و سیستم مخاطب نیز پس از دریافت درخواست، آدرس** MAC **خود را برای متقاضی ارسال می کند.**



کامپیوتر هایی که در شبکه می خواهند کار کنند باید دارای آدرس IP باشند. این آدرس می تواند توسط شما به سیستم داده شود (Static) و یا به کمک DHCP server این کار انجام شود. DCHP سرویسی است بر روی سیستم عامل سرور که می تواند در صورت درخواست کامپیوتر جهت داشتن IP، آدرسی را برای آنها صادر کند و شما نیازی به تنظیم IP بر روی تک تک سیستم ها نداشته باشید و این کار به صورت خود کار انجام پذیرد. در تصویر زیر تنظیم IP به صورت دستی (Static) نشان داده شده است.





به یاد داشته باشیم که اگر یک کامپیوتر به هر دلیلی نتواند از DHCP SERVER آدرس بگیرد خودش برای خودش یک IP تصادفی صادر می کند. این آدرس در محدوده 169.254.0.0/16 می باشد. به این عملکرد کامپیوتر ها آدرس دهی خودکار یا همان Automatic Private IP Addressing (APIPA) می گوییم.

دستور Netstat **به شما کمک می کند تا از وضعیت اتصالات** TCP **و پورت های مورد استفاده برروی سیستم شما از مبدأ به مقصد اطلاع حاصل کنید.**

```
C:\>netstat -n
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    192.168.4.27:57913     209.29.33.25:80        ESTABLISHED
  TCP    192.168.4.27:61707     192.168.4.10:445       ESTABLISHED
C:\>
```

همچنین دستور Netstat –an **وضعیت پورت هایی که در حالت** Listening **هستند را نیز نمایش می دهد.**

```
C:\>netstat -an
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:7              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:990            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:27015        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:52144        127.0.0.1:52145        ESTABLISHED
  TCP    127.0.0.1:52145        127.0.0.1:52144        ESTABLISHED
  TCP    127.0.0.1:52146        127.0.0.1:52147        ESTABLISHED
  TCP    127.0.0.1:52147        127.0.0.1:52146        ESTABLISHED
  TCP    192.168.4.27:139       0.0.0.0:0              LISTENING
  TCP    192.168.4.27:52312     74.125.47.108:80       TIME_WAIT
  TCP    192.168.4.27:57913     63.246.140.18:80       CLOSE_WAIT
  TCP    192.168.4.27:61707     192.168.4.10:445       ESTABLISHED
```

Internet Control Management Protocol(ICMP) پروتوکلی است که وظیفه چک کردن اتصالات شبکه را برعهده دا رد. یکی از مهمترین و کاربردی ترین دستوراتی که ما در دنیای شبکه استفاده می کنیم Ping **می باشد.**

پروتکلهای کاربردی :

Application	TCP/UDP	Port	Notes
HTTP	TCP	80	The Web
HTTPS	TCP	443	The Web, securely
Telnet	TCP	23	Terminal emulation
SSH	TCP	22	Secure terminal emulation
SMTP	TCP	25	Sending e-mail
POP3	TCP	110	E-mail delivery
IMAP4	TCP	143	E-mail delivery
FTP	TCP	20/21	File transfer
TFTP	UDP	69	File transfer

همانطور که در جدول بالا ملاحظه می فرمایید تعدادی از پروتوکل ها و سرویس هایی مطرح شبکه ها که کاربرد زیادی دارند به همراه نوع پروتوکل و شماره پورتی که استفاده می کنند نمایش داده شده است.

HTTP: جهت باز کردن صفحات WEB.

HTTPS: بازکردن و انتقال اطلاعات به صورت ایمن در صفحات Web. HTTPS **از تلفیق** HTTP **و** SSL **پدید می آید.**

Secure Socket Layer (SSL) بر روی TCP 344 **فعال است.** Telnet**: اتصال از یک سیستم به سیستم دیگر از طریق خط دستوری** (Command Prompt) **و اجرای دستورات بر روی سیستم مقصد.**

SSH: شبیه به Telnet **عمل می کند اما اطلاعاتی که از مبدا به سمت مقصد جابجا می شود به صورت کد گذاری شده منتقل می شود.**

SMTP: پروتوکل انتقال E-mail.

POP3: پروتوکلی که بین کاربر و Mail-Server **برقرار است. این پروتوکل به کاربر کمک می کند که جهت دسترسی به** E-Mail **های خود به صندوق پستی وصل شده و تمام نامه ها بر روی سیستم کاربر ذخیره می شوند و او می تواند بدون نیاز به اتصال به اینترنت نامه های خود را بخواند. از معروف ترین نرم افزار هایی که این کار را انجام می دهد می توان به** Outlook Express **اشاره کرد.** IMAP4**: پروتوکلی که بین کاربر و** Mail-Server **برقرار است. این پروتوکل نامه های الکترونیکی کاربران را بر روی سرور نگه دارای می کند و کاربر جهت خواندن نامه های خود باید به اینترنت متصل باشد.**

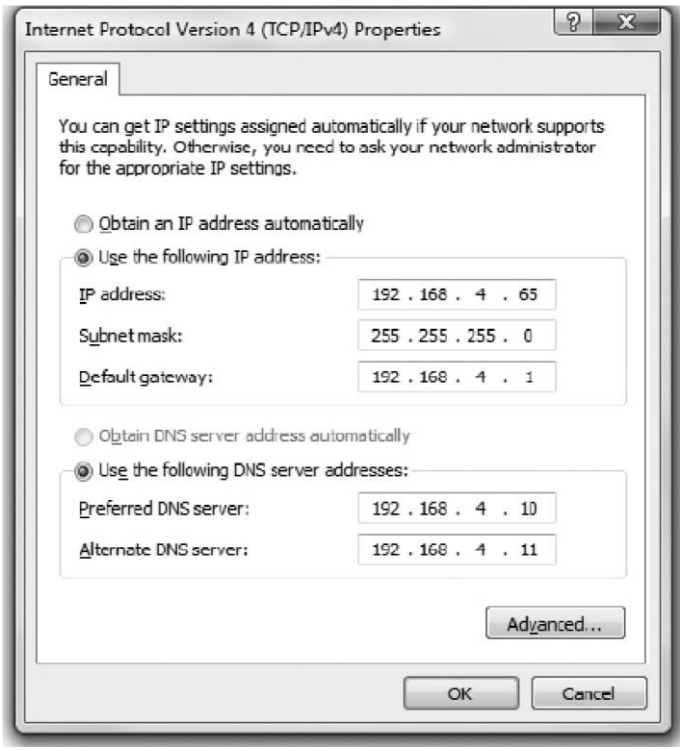
همچنین قدرت حذف نامه ها، جستجو در نامه ها جهت یافتن یک کلمه کلیدی و ساختن پوشه بر روی سرور جهت نگه دارای نامه های الکترونیکی را دارد.

FTP: وظیفه جابجایی اطلاعات از منبع به مقصدی را دارد.

تبدیل اسم به آدرس (Name Resolution) با استفاده از DNS

سیستم ها برای برقراری ارتباط و انتقال اطلاعات با آدرس IP کار می کنند. اما برای ما انسانها به خاطر سپردن اسم بسیار راحت تر از بخاطر سپردن چهار عدد (آدرس IP) می باشد. برای اینکه نامی را که ما بخاطر می سپاریم و به سیستم می دهیم به زبان قابل فهم برای کامپیوتر ها تبدیل شود (آدرس IP) از سرویسی استفاده می کنیم به نام Domain Name System (DNS)**. سرویس DNS عملیاتی با نام** Name Resolution **را انجام میدهد. این کار یعنی تبدیل اسم به IP و بالعکس.**

DNS Server (Name Server): سروری است که سرویس DNS بر روی آن فعال شده و سرویس دهی به شبکه را بر عهده دارد.



همانطور که در تصویر بالا نیز ملاحظه می فرمایید در صفحه تنظیمات TCP/IP **در انتهای صفحه دو فضا برای وارد کردن آدرس** DNS Server **تعبیه شده است که شما به وسیله این قسمت به سیستم خود می گویید که جهت پرسیدن سوال در**

مورد تبدیل اسم به IP یا تبدیل IP به اسم از کدام سیستم میتواند کمک بگیرد. این که دو آدرس DNS را می توان به سیستم داد جهت این است که اگر کامپیوتر ما برای سوال خود از DNS اول (Preferred) نتوانست جوابی دریافت کند می تواند از آدرس DNS دوم (Alternate) اقدام کند.

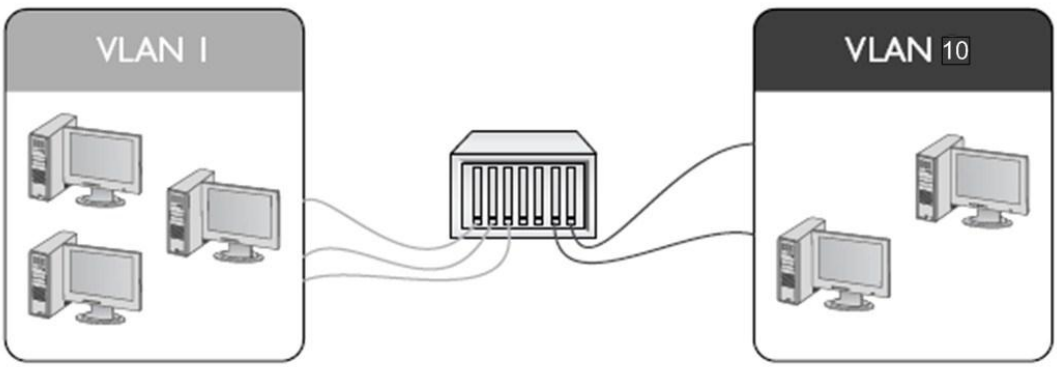
Spanning-Tree Protocol (STP):

استفاده از پروتوکل STP برای این منظور است که این حالت بدون استفاده از تمهیدات خاص شبکه ما را دچارLoop می کند که این موضوع می توان بسیار دردسر ساز باشد. STP جلوی ایجاد حلقه (Loop) را در شبکه ما میگیرد.

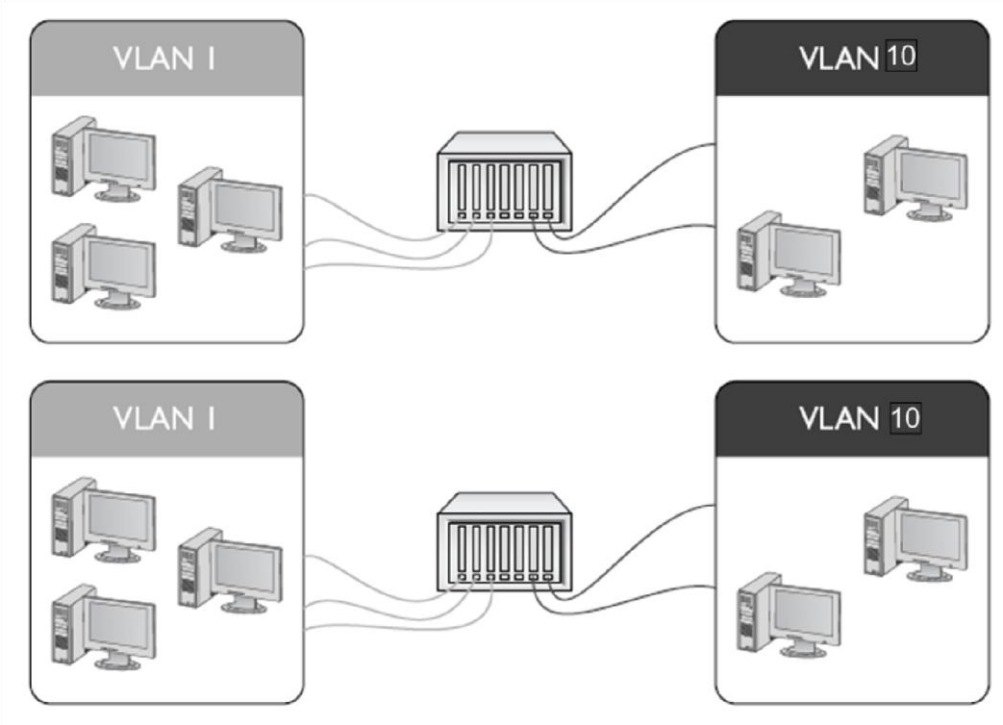
VLAN

استفاده از روش Virtual Local Area Network(VLAN) جهت محدود کردن ترافیک Broadcast امروزه در تمام شبکه ها وجود دارد و استفاده می شود. در این روش پایه جدا کردن VLAN ها از هم پورت های روی سوئیچ می باشد.

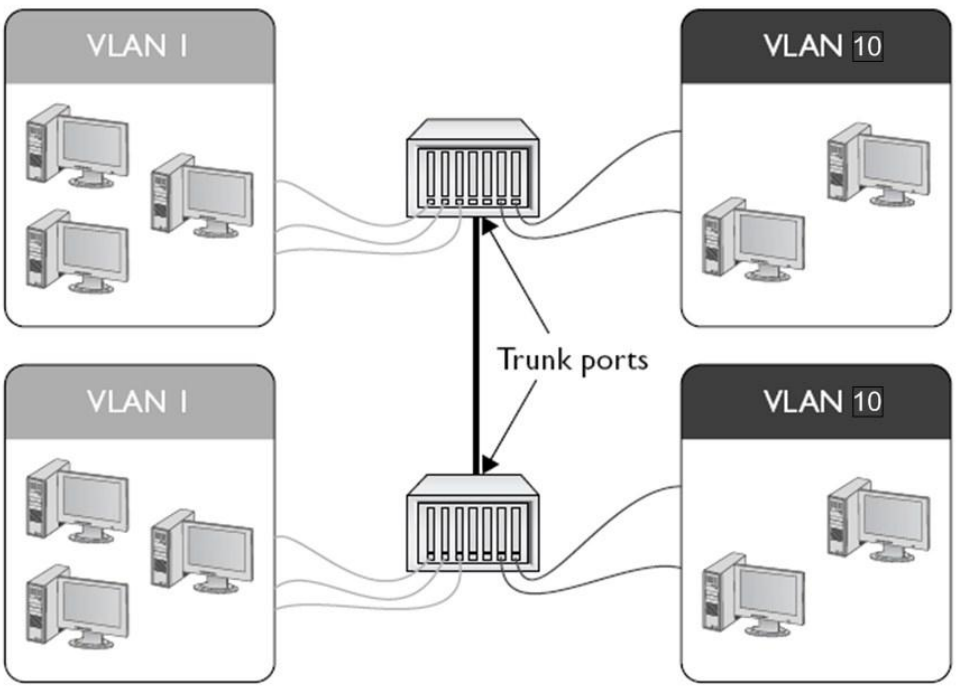
شما می توانید پورت های روی سوئیچ را به عضویت VLAN های مختلفی دربیاورید. سیستم شما بر اساس اینکه به کدام یک از پورت های روی سوئیچ متصل است عضویتش در آن VLAN می باشد.



زمانی که شبکه شما بزرگ می شود و تعداد سوئیچ های شما و در نتیجه تعداد VLAN ها افزایش میابد باید پلی ارتباطی بین سوئیچ ها باشد تا این اتصالات توانایی انتقال اطلاعات از چند VLAN را داشته باشد. پورت هایی که عضو VLAN خاصی هستند فقط اطلاعات مربوط به اعضای همان VLAN را از خود عبور می دهند.

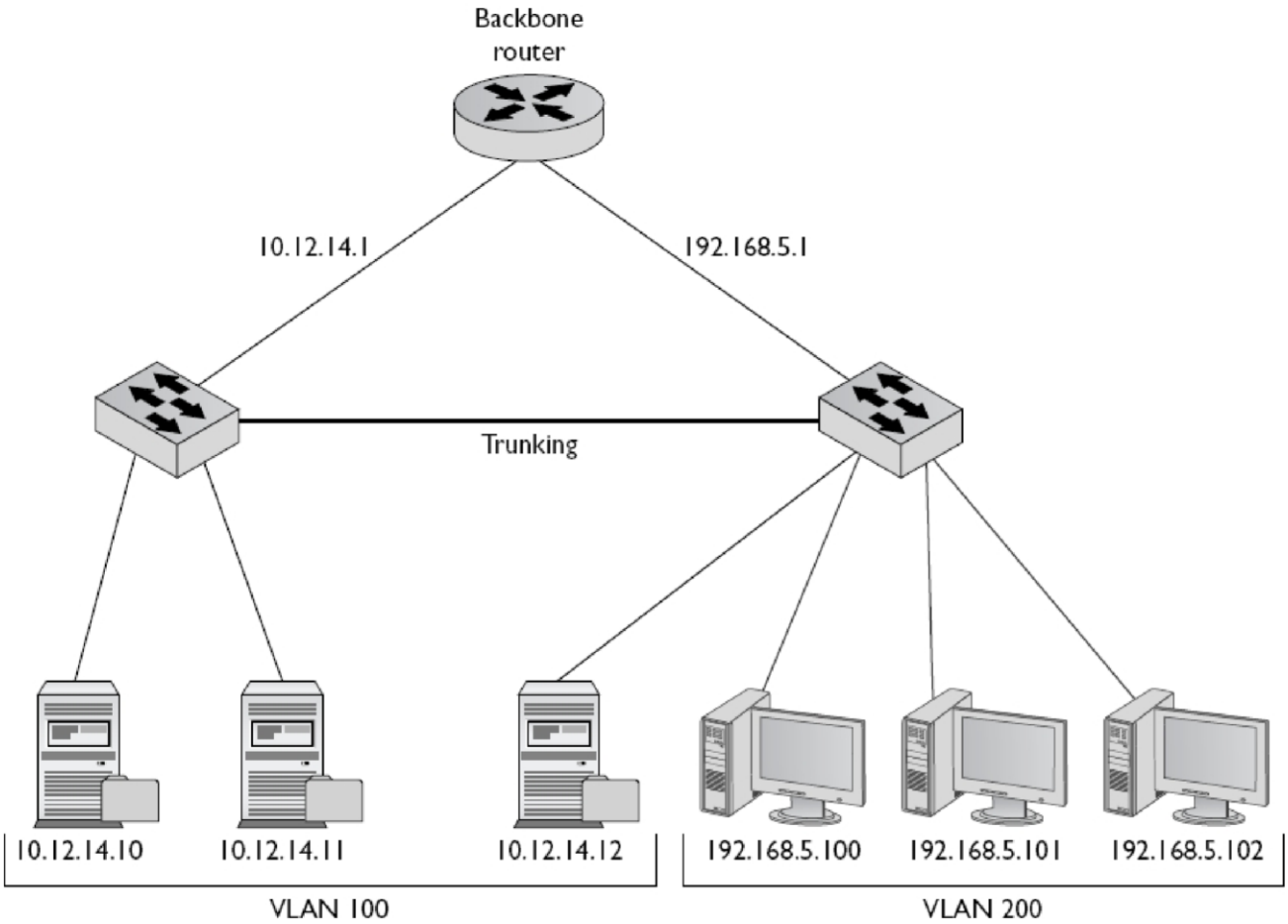


اتصالاتی که توانایی انتقال اطلاعات از چند VLAN را داشته باشد و بین سوئیچ ها تعبیه می شوند Trunk نام دارند و پورت هایی که سوئیچ ها را به هم متصل می کنند Trunk Port نامیده می شوند. اتصالات Trunk عضو هیچکدام از VLAN ها نیستند و اطلاعات هر نوع VLANی را از خود عبور می دهند.



هر VLAN یک Broadcast Domain مجزا محسوب می شود و طبق معمول برای متصل کردن Broadcast Domain ها جهت انتقال ترافیک Unicast از روتر یا هر دستگاهی که در لایه ۳ از شبکه کار کند نیاز داریم. جهت برقراری ارتباط

بین VLANها باید به ازای هر VLAN یک رنج آدرس IP نیز در نظر گرفت.



گفتیم که علاوه برروتر ها هر دستگاهی که در لایه ۳ از شبکه کار کند توانایی برقراری ارتباط بین VLAN ها را دا رد. از آن جمله می توانیم به سوئیچ ها لایه ۳ اشاره کنیم که جهت اتصال بین VLAN ها بسیار استفاده می شوند. یـک نمونـه ازآنها را در تصویر زیر ملاحظه می فرمایید(Cisco Catalyst 3560).

IPv6

این نوع آدرس IP، ۱۲۸ بیتی است که در مبنای ۱۶ (Hex) نوشته می شود. این نوع جدید از IP بدلیل کمبود تعداد IPv4 طراحی شده و به تدریج جایگاه خود را در شبکه ها پیدا خواهد کرد. همانطور که گفته شد ۱۲۸ بیتی بودن این IP می توانند دغدغه های کمبود آدرس (مخصوصاً آدرس های Public) را از بین ببرد. نمونه ای از این IP را در زیر ملاحظه می فرمایید.

2001:0000:0000:3210:0800:200C:00CF:1234

FEDC::CF:0:BA98:1234/64

همانطور که از ظاهر IP ها مشخص است دارای طول زیادی هستند و خیلی هم چه از جهت نوشتن و چه از جهت بخاطر سپردن کار راحتی نداریم. جهت بهبود وضعیت IP از لحاظ نوشتاری قوانینی وضع شده تا ما بتوانیم از شرایط خلاصه نویسی در IP ها استفاده کنیم. روش کار بدین صورت است که از مجموع ۸ بخش ۱۶ بیتی (مجموعاً ۱۲۸ بیت) آن ۱۶ بیتی هایی که صفر هستند می توانند حذف شوند و بجای آنها یک دو نقطه ":" گذاشته شود. در مثال بعد زیر قسمت هایی که قابل حذف هستند خط کشیده شده است. به مثال زیر توجه بفرمایید:

2001:0000:0000:3210:0800:0000:0000:1234

بر طبق قانون مطرح شده آدرس IP بالا را می توانیم به حالت زیر خلاصه کنیم.

2001::3210:0800::1234

می بینیم که بعد از حذف ۱۶ بیتی هایی که همه صفر بودند و بجای قسمت های حذف شده از دو نقطه استفاده شده است.

اما قانون خلاصه سازی دارای تبصره هایی است، از جمله:

عملیات حذف ۱۶ بیتی های صفر فقط در یک بخش IP می تواند انجام شود. به زبان ساده تر در ساختار IPv6 دو بار دو نقطه در ساختار IP پذیرفته نیست. پس خلاصه سازی که ما در بالا انجام دادیم صحیح نیست و ما فقط از یک دو نقطه در IP می توانیم استفاده کنیم. 2001::3210:0800::1234. این که کدام بخش از صفرهای موجود می توانند حذف شوند اختیاری است و در مثال بالا و بعد از خلاصه سازی یکی از حالات زیر مورد قبول است.

1. **2001::3210:0800:0000:0000:1234**
2. **2001:0000:0000:3210:0800::1234**

۳. همانطور که ملاحظه می فرمایید ساختار صحیح IPv6 فقط یک بار دو نقطه را می پذیرد. این موضوع به این خاطر است که شما با دیدن یک IPv6 بتوانید تشخیص دهید در صورت بروز خلاصه سازی چند بیت از مجموع ۱۲۸ بیت خلاصه شده است. می توانید بجای صفرهایی که نمی توانند خلاصه شوند بجای **0000** تنها یک **0** بگذارید. مثلاً اگر خلاصه سازی حالت اول را مد نظر بگیریم می توانیم بجای صفر های قسمت ششم و هفتم فقط یک صفر بگذاریم ولی گذاشتن این صفر ها الزامی است و حذف کلی آنها مورد قبول نیست و خواهیم داشت:

2001::3210:0800:0:0:1234

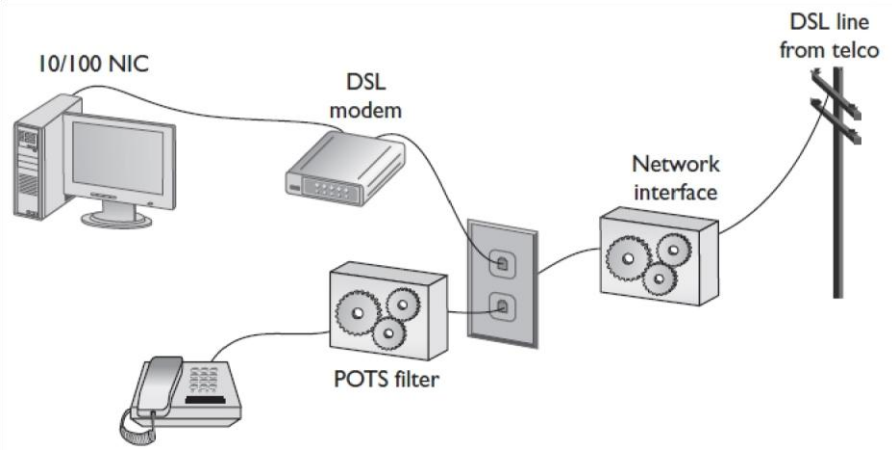
- تبصره بعد در خلاصه سازی IPv6 این است که اگر در قسمت های ۱۶ بیتی همه بیتها صفر نبود آیا باز هم می توان خلاصه سازی انجام داد. به مثال زیر توجه کنید:

FE80:12CC:0025:ABCD:A000:1111:4567:AABB. در این مثال قسمت های سوم و پنجم دارای بیت های صفر هستند، آیا این صفر ها را نیز می توان حذف کرد؟ جواب آن است که بله، به شرط آنکه صفر ها در سمت چپ اعداد یا حروف قرار گرفته باشند و در صورت حضور آنها در سمت راست اعداد یا حروف قابل حذف نیستند. با این تفاسیر فقط صفر های قسمت سوم که در سمت راست قرار گرفته اجازه حذف شدن دارند و صفر های قسمت پنجم را نمی توان حذف کرد و تنها می توان با یک صفر نشان داد. **FE80:12CC:25:ABCD:A0:1111:4567:AABB**

- در IPv6 دیگری چیزی به عنوان Subnet Mask وجود ندارد و شما تعداد بیت های ثابت (Network ID) را با Prefix Length (قرار دادن عددی پشت IP) نشان می دهید. **64**/2001::12:0:0:0800:321034 در تصویر زیر نمونه ای از IPv6 تنظیم شده در ویندوز Vista را ملاحظه می فرمایید.

Digital Subscribe Line (DSL) نوعی از اتصالات Broadband می باشد که دارای انواع حالات است و معروف ترین آن که نامش با گوش ما آشناست ADSL است که بر روی آن اینترنت به کاربران داده می شود. ساختار اتصال از محل

کاربر تا بستر مخابراتی و در نهایت ISP در تصویر زیر نشان داده شده است. در استفاده از ADSL علاوه بر دیتای اینترنتی شما می توانید از تلفن نیز جهت انجام مکالمات خود استفاده کنید پس، یک اتصال Broadband محسوب می شود.



جهت استفاده از خطوط ADSL نیازمند مودم های مخصوص این تکنولوژی هستیم که نمونه ای از آن مربوط به شرکت سیسکو را در تصویر زیر ملاحظه می فرمایید.

جهت انجام تنظیمات احتمالی بر روی مودم ADSL می توانید از محیط گرافیکی آن با استفاده از Internet Explorer بهره ببرید. تصویر زیر نمونه ای از این صفحه می باشد.

شبکه های بی سیم (wireless)

شبکه های بی سیم نیز مانند شبکه های سیمی با همان استاندارد های ۷ لایه شبکه و ... کار می کنند و تنها تفاوتشان ارسال اطلاعات است بصورت امواج رادیویی ولی از نظر ساختار عملکرد شبکه به همان صورت کار می کنند. شبکه های بی سیم با حالت های مختلفی طی سال های اخیر به بازار عرضه شده اند اما آنچه امروزه فراگیر تر است حالت Wi-Fi می باشد که

توسط IEEE ارائه شده است. مجموعه IEEE استاندارد های مربوط به شبکه های بی سیم را با 802.11 مشخص می کند.

انواع استانداردهای 802.11 را با خواص مختلف ملاحظه می فرمایید.

Standard	Frequency	Spectrum	Speed	Range	Compatibility
802.11b	2.4 GHz	DSSS	11 Mbps	~300'	802.11b

Standard	Frequency	Spectrum	Speed	Range	Compatibility
802.11a	5.0 GHz	DSSS	54 Mbps	~150'	802.11a

Standard	Frequency	Spectrum	Speed	Range	Compatibility
802.11g	2.4 GHz	OFDM	54 Mbps	~300'	802.11b/g

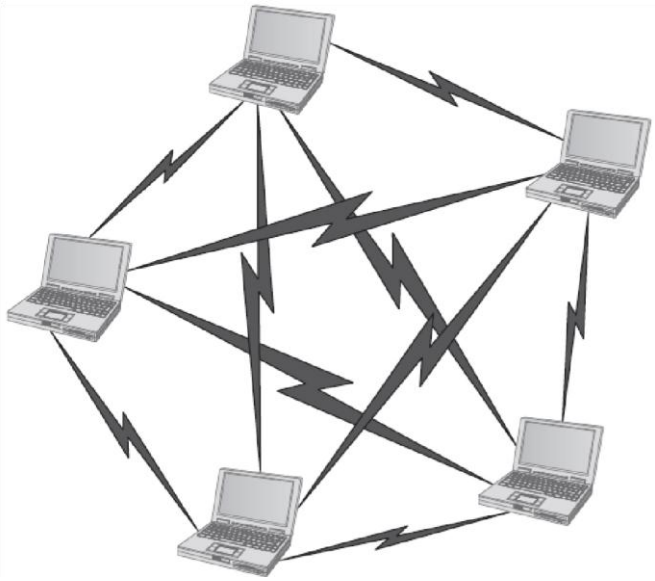
Standard	Frequency	Spectrum	Speed	Range	Compatibility
802.11n	2.4 GHz[1]	OFDM	100+ Mbps	~300'	802.11b/g/n[2]

[1] Dual-band 802.11n devices can function simultaneously at both 2.4- and 5.0-GHz bands.
[2] Many dual-band 802.11n WAPs support 802.11a devices as well as 802.11b/g/n devices. This is not part of the standard, but something manufacturers have implemented.

برای کارکرد سیستم های ما تحت شبکه های Wireless نیازمند تجهیزات دریافت و ارسال مخصوص به این نوع شبکه ها هستیم. استفاده از کارت شبکه های Wireless بر روی کامپیوتر های ما الزامیست. کارت شبکه ای را که در تصویر زیر ملاحظه می فرمایید جهت نصب در داخل کامپیوتر و به صورت Internal می باشد.

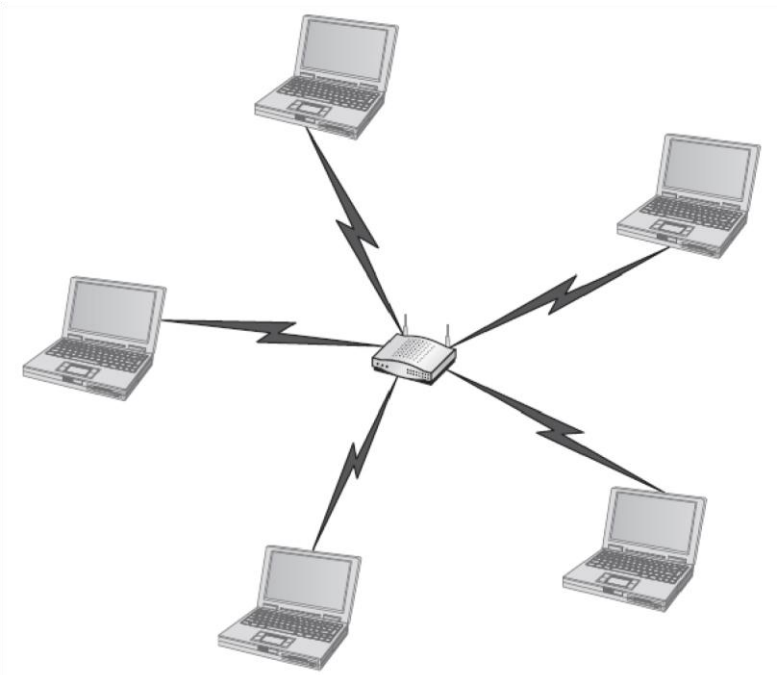
کارت شبکه های خارجی (External) هم جهت استفاده در شبکه های بی سیم وجود دارند که نمونه ای از آن را در تصویر زیر ملاحظه می فرمایید.

عملکرد کامپیوتر ها در شبکه های بی سیم به دو صورت انجام می پذیرد. اول آنکه کامپیوتر ها مستقیم و با استفاده از کارت شبکه های خود و بدون هیچ دستگاه واسطه ای به یکدیگر متصل شوند. به این حالت شبکه های بی سم AD Hoc **گفته می شود.**



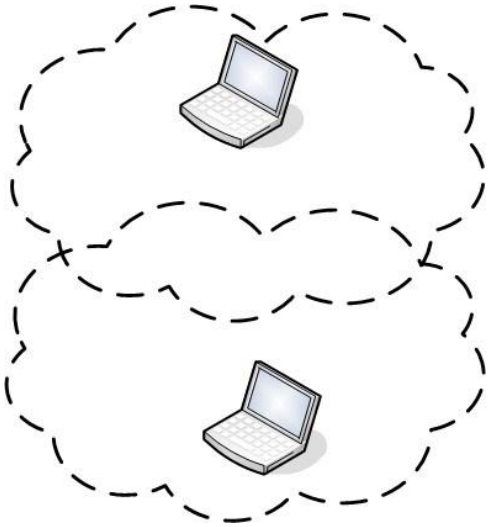
این روش مشکلات زیادی را در بر دارد از جمله آنکه کامپیوتر ها تا فواصل معینی بیشتر نمی توانند از هم دور شوند. امروزه این روش کاربردی ندارد وبا وجود بزرگ شدن شبکه ها و وجود تعداد زیادی کامپیوتر در شبکه های بی سیم کارایی خود را از دست داده است. امروزه برای اتصال کامپیوتر های داخل شبکه بی سیم از دستگاه هایی به نام Wireless Access Point (WAP) **استفاده می شود.**

این Access Point **ها مانند سوئیچ های شبکه های کابلی عمل می کنند یعنی، اطلاعات را از سیستم مبدأ می گیرند و به سیستم مقصد تحویل می دهند. وجود** Access Point **ها باعث قابلیت بزرگتر شدن شبکه ها می شوند. می توان برای تحت پوشش گرفتن مساحت بیشتر در فواصل مختلف** Access Point **هایی را تعبیه کرد.**



در مورد استفاده از تجهیزات بی سیم دو فاکتور بسیار حائز اهمیت است؛ یکی فضایی (مساحت) را که تجهیزات بی سیم میتوانند پوشش دهند و دوم سرعتی که این تجهیزات می توانند تحت آن کار کنند.

فضایی را که تجهیزات بی سیم می توانند پوشش دهند را Basic Service Set (BSS) **می گویند.**



تجهیزات بی سیم برای ارتباط با یکدیگر باید دارای فضای همپوشانی باشند یعنی، فضایی از BSSی را که پوشش می دهند روی هم بیافتد. به این فضای همپوشانی Basic Service Area (BSA) **می گویند.**

Access Point **ها خود دارای آنتن هایی هستند که غالباً امواج رادیویی را تا ۲ دسیبل منتشر می کنند. برای انتقال بیشتر و قوی کردن سیگنال ها می توانید بجای آنته های خود** Access Point **از آنتن های متحرک استفاده کنید که غالباً قوی تر از آنتن های خود** Access Point **ها هستند.**

با آرزوی توفیق روز افزون برای همه عزیزان