مفاهیم اولیه شبکه

مجموعه‌ای از کامپیوترهای خود مختار متصل به هم که امکان تبادل اطلاعات بین آنها وجود دارد.
برخی از مزایای تشکیل شبکه ها عبارتند از:

- امکان ارتباط کامپیوترها در نقاط مختلف و حذف مسافت های فیزیکی
- امکان تبادل اطلاعات و منابع برای بهره برداری مشترک با اطمینان بالاتر
- افزایش کارائی، سرعت و دقت در تبادل اطلاعات
- امکان مدیریت متمرکز اطلاعات و اعمال سیاست های امنیتی

شبکه ها از نظر نوع ارتباط به دو دسته تقسیم می‌شوند:

- شبکهٔ نظیر به نظیر[۱]
- شبکهٔ مشتری‌کارگزار[۲]

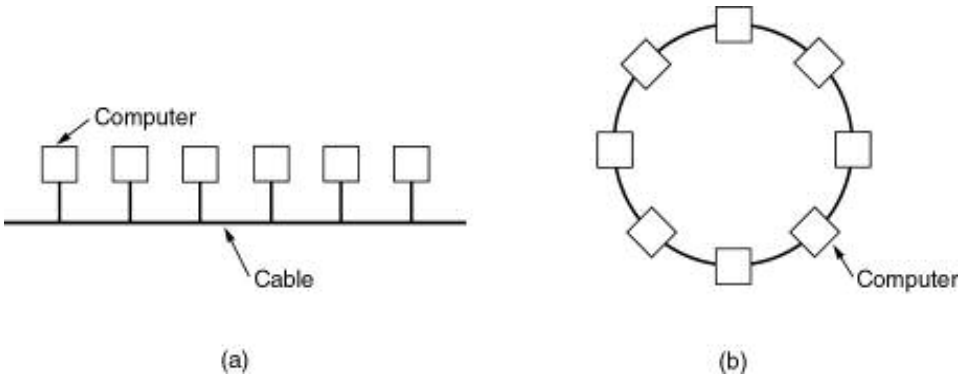
همچنین شبکه ها را از لحاظ گستردگی و وسعت نیز می توان به ترتیب زیر تقسیم نمود:
الف- شبکه های محلی[۳] یا LAN
ب- شبکه های بین‌شهری[۴] یا MAN
ج- شبکه های‌گسترده[۵] یا WAN
شبکه های درون سازمان اینترانت[۶] و اگر به شبکه بیرونی مثلا اینترنت وصل شود اکسترانت[۷] نامیده می شود.

---

[1] - Peer– to – Peer
[2] - Client /Server
[3] - Local Area Network
[4] - Metropolitan Area Network
[5] - Wide Area Network
[6] -Intranet
7 -Extranet

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

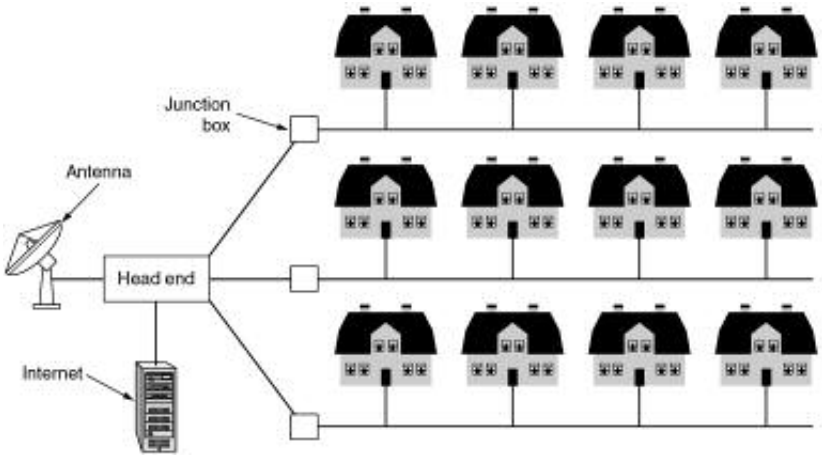
شبکه های محلی دارای سه خصوصیت متمایز کننده هستند:
اندازه مشخص دارند در نتیجه حداکثر تاخیر آنها مشخص است.
تکنولوژی انتقال در آنها بر اساس انتشار عمومی[1] می باشد.
معمولا همبندی یا توپولوژی Bus یا Ring دارند.



شکل ۲: (a) شبکه بر اساس توپولوژی BUS ، (b) شبکه بر اساس توپولوژی Ring

شبکه های شهری دارای یک یا چند مسیر و المان سوئیچینگ هستند لذا در این شبکه ها حداکثر میزان تاخیر به طور مشخص قابل تعیین نیست. شبکه اینترنت مجموعه ای از شبکه‌های شهری متصل به هم می باشد.

1 - Broadcast



الف ـ اجزای منطقی شبکه

پروتکل شبکه: به معنی قواعد و قوانین خاصی که ارتباط کامپیوترها بر اساس آن صورت می‌گیرد مانند پروتکل های TCP/IP و IPX / SPX.

سیستم عامل: سیستم عامل شبکه که بر روی سرور نصب شده و مدیریت شبکه را به عهده دارد.

ب ـ اجزای فیزیکی

اجزاء فیزیکی شبکه ها نیز به ترتیب زیر طبقه بندی می شوند:

کامپیوترهای سرور، ایستگاه های کاری و امکانات جانبی مانند چاپگر

محیط ارتباطی باسیم یا بی‌سیم

سایر اجزاء مانند: مودم، روتر، پل یا بریج، کارت شبکه، هاب، سوئیچ و غیره. که هر یک بر حسب اهمیت کاربرد در شبکه، تشریح می گردند.

کابل شبکه

کابل شبکه، رسانه ای است که از طریق آن اطلاعات از یک دستگاه موجود در شبکه به دستگاه دیگر انتقال می یابد. انواع مختلفی از کابل ها به طور معمول در شبکه های محلی استفاده می شوند. در برخی موارد شبکه تنها از یک نوع کابل استفاده می کند و در مواقعی نیز انواع مختلفی از کابل ها در شبکه به کار گرفته می شود. غیر از عامل توپولوژی، پروتکل و اندازه شبکه نیز در انتخاب کابل شبکه مؤثرند. آگاهی از ویژگی های انواع مختلف کابل ها و ارتباط آنها با دیگر

جنبه های شبکه برای توسعه یک شبکه موفق ضروری است. امروزه سه گروه از کابل ها، در ایجاد شبکه مطرح هستند:

کابل های هم محور یا کواکسیال؛ که زمانی بیشترین مصرف را در میان کابل های موجود در شبکه داشتند. چند دلیل اصلی برای استفاده زیاد از این نوع کابل وجود دارد:

- قیمت ارزان آن.
- سبکی و انعطاف پذیری.
- این نوع کابل به نسبت زیادی در برابر سیگنالهای مداخله گر مقاومت می نماید.
- مسافت بیشتری را بین دستگاه های موجود در شبکه، نسبت به کابل UTP پشتیبانی می نماید.

شکل ۴: تصویر کابل کواکسیال و اجزاء آن

اجزای کابل کواکسیال به شرح زیر می باشد:

- هسته مرکزی [1] که معمولاً از یک رشته سیم جامد مسی تشکیل می گردد.
- عایق [2] که معمولاً از جنس پی وی سی یا تفلون است.
- Copper WireMesh که از سیم های بافته شده تشکیل می شود و کار آن جمع آوری امواج الکترومغناطیسی است.
- Jacket که جنس ان اغلب از پلاستیک بوده و پوشش خارجی سیم در برابر خطرات فیزیکی است.

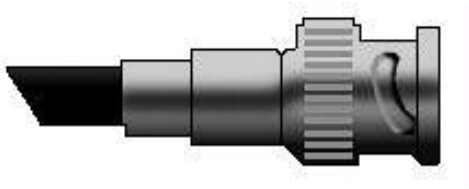
کابل کواکسیال به دو دسته تقسیم می شود:

- Thin net: کابلی است بسیار سبک، انعطاف پذیر و ارزان قیمت، قطر سیم در آن ۶ میلیمتر معادل ۰/۲۵ اینچ است. مقدار مسیری که توسط آن پشتیبانی می شود ۱۸۵ متر است.

[1] -Conducting Core
[2] - Insulation

- Thick net: این کابل قطری تقریباً ۲ برابر Thin net دارد. کابل مذکور، پوشش محافظی را (علاوه بر محافظ خود) داراست که از جنس پلاستیک بوده و بخار را از هسته مرکزی دور می سازد.

رایج ترین نوع اتصال دهنده مورد استفاده در کابل کواکسیال، BNC می باشد. انواع مختلفی از سازگارکننده ها برای BNC ها شامل: Barrel connector، Tconnector و Terminator وجود دارند. در شبکه هایی با توپولوژی Bus از کابل کواکسیال استفاده می شود.



شکل ۵: اتصال دهنده BNC

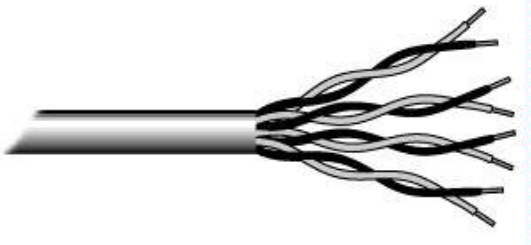
در طراحی جدید شبکه معمولا از کابل های زوج سیم به هم تابیده شده، استفاده می گردد. قیمت آن ارزان بوده و از نمونه های آن می توان به کابل تلفن اشاره کرد. کابل های مورد استفاده در شبکه های کامپیوتری که از چهار جفت سیم به هم تابیده تشکیل می گردد، خود به دو دسته تقسیم می شود:

UTP: کابل ارزان قیمتی است که نصب آسانی دارد و برای شبکه های محلی باسیم، بسیار مناسب است، همچنین نسبت به نوع دوم کم وزن تر و انعطاف پذیرتر است. مقدار سرعت دیتای عبوری از آن ۴ مگابیت در ثانیه تا ۱۰۹۰ مگابیت در ثانیه می باشد. این کابل می تواند تا مسافت حدوداً ۱۰۰ متر یا ۳۲۸ فوت را بدون افت سیگنال انتقال دهد. کابل مذکور نسبت به تداخل امواج الکترومغناطیس حساسیت بسیار بالایی دارد و در نتیجه در مکان های دارای امواج الکترومغناطیس، امکان استفاده از آن وجود ندارد.

در سیم تلفن که خود نوعی از این کابل است از اتصال دهنده RJ11 استفاده می شود، اما در کابل شبکه اتصال دهنده ای با شماره RJ45 بکار می رود که دارای هشت مکان برای چهار زوج سیم است.

شکل ۶: اتصال دهنده شبکه RJ45

کابل های زوج به هم تابیده[1] با توجه به ضخامت و میزان به هم تابیدگی آنها، در گروه های مختلفی که با CAT[2] شروع می شوند طبقه بندی شده‌اند. CAT1 یا نوع اول کابل UTP برای انتقال صدا بکار می رود، اما CAT2 تا CAT7 برای انتقال دیتا در شبکه های کامپیوتری مورد استفاده قرار می گیرند و سرعت انتقال دیتا در آنها به ترتیب عبارتست از: ۴ ، ۱۰ ، ۱۶، ۱۰۰ و ۱۰۰۰ مگابیت در ثانیه. لازم به ذکر است که برای شبکه های کوچک و خانگی استفاده از کابل CAT3 توصیه می شود.



شکل ۷: کابل هم محور CAT5

STP: در این کابل سیم های انتقال دیتا مانند UTP هشت سیم و یا چهار جفت دوتایی هستند. باید دانست که تفاوت آن با UTP در این است که پوسته ای به دور آن پیچیده شده که از اثرگذاری امواج بر روی دیتا جلوگیری می کند. از لحاظ قیمت، این کابل از UTP گران تر و از فیبر نوری ارزان تر است. مقدار مسافتی که کابل مذکور بدون افت سیگنال طی می کند برابر با ۵۰۰ متر معادل ۱۶۴۰ فوت است. در شبکه هایی با توپولوژی BUS و RING از دو نوع اخیر استفاده می شود. گفته شد که در این نوع کابل، ۴ جفت سیم به هم تابیده بکار می رود که از دو جفت آن یکی برای فرستادن اطلاعات و دیگری برای دریافت اطلاعات عمل می کند.

[1] - Twisted Pair
[2]- Category

دلیل تابیده بودن زوج ها در کابل های زوج بهم تابیده، کم کردن اثر نویز محیط است. زیرا دو کابل به هم تابیده به دلیل تاثیر مشابه از محیط، نویز مساوی دریافت نموده و بدین ترتیب در گیرنده، چون سیگنال منتقل شده، از تفاضل ولتاژ دو رشته حاصل می‌شود بنابراین نویز حذف می‌شود.

در شبکه هایی با نام اترنت سریع، دو نوع کابل به چشم می خورد:

100Base TX: یعنی شبکه ای که در آن از کابل UTP نوع CAT5 استفاده شده و عملاً دو زوج سیم در انتقال دیتا دخالت دارند (دو زوج دیگر فعلا بلا استفاده می باشد)، سرعت در آن ۱۰۰ مگابیت در ثانیه و روش انتقال مبتنی بر باند است.

100 Base T4: تنها تفاوت آن با نوع بالا این است که هر چهار جفت سیم در آن بکار گرفته می شوند.

شاخص کیفیت کابل CAT5 میزان تابیده بودن کابل ها به هم می باشد هرچه میزان تابیده بودن بیشتر باشد کابل از کیفیت بالاتری برخوردار می باشد. در کابل های UTP وجود یک نخ برای استحکام کابل ضروری و عدم وجود آن نشانگر عدم مرغوبیت کابل است.

اتصال Cross و مستقیم[1]، دو نوع اتصال روی کابل CAT5 است که رنگ بندی سیم ها در آن مطابق جدول ذیل است. کابل مستقیم، برای اتصال دو سیستم غیر هم جنس مانند کامپیوتر به سوئیچ استفاده شده و کابل Cross برای اتصال دو سیستم هم جنس مانند دو کامپیوترکاربرد دارد. رنگ بندی و نوع سیگنال ها در در شکل ذیل مشخص شده است.

Color	Cross	مستقیم	توضیحات
سبز / سفید	1	3	+ دریافت
سبز	2	6	- دریافت
سفید / نارنجی	3	1	+ ارسال
آبی	4	4	بدون استفاده
سفید / آبی	5	5	بدون استفاده
نارنجی	6	2	- ارسال
سفید / قهوای	7	7	بدون استفاده
قهوای	8	8	بدون استفاده

جدول ۱: رنگ بندی در دو نوع کابل Cross و مستقیم

[1] - Straight

سیم بندی کابل Straight و Cross در جدول ذیل مشخص شده است:

Pin1	Pin2	Pin3	Pin4	Pin5	Pin6	Pin7	Pin8
کابل Straight در هر دو سر کابل مطابق زیر(هر دو سر سیم بندی T568B)							
سفید نارنجی	نارنجی	سفید سبز	آبی	سفید آبی	سبز	سفید قهوه‌ای	قهوه‌ای
سفید نارنجی	نارنجی	سفید سبز	آبی	سفید آبی	سبز	سفید قهوه‌ای	قهوه‌ای
کابل Cross یک سر ردیف اول و سر دیگر ردیف دوم (یک سر T568B، سر دیگر T568A)							
سفید سبز	سبز	سفید نارنجی	آبی	سفید آبی	نارنجی	سفید قهوه‌ای	قهوه‌ای
سفید نارنجی	نارنجی	سفید سبز	آبی	سفید آبی	سبز	سفید قهوه‌ای	قهوه‌ای

جدول ۲: نحوه اتصال در کابل های Cross و مستقیم

کابل فیبر نوری کاملا متفاوت از نوع کواکسیال و زوج سیم به هم تابیده شده عمل می کند. به جای اینکه سیگنال الکتریکی در داخل سیم انتقال یابد، پالس هایی از نور در میان پلاستیک یا شیشه انتقال می یابد این کابل در برابر امواج الکترومغناطیس کاملا مقاومت می کند و نیز تأثیر افت سیگنال بر اثر انتقال در مسافت زیاد را بسیار کم در آن می توان دید. لازم به ذکر است که کابل فیبرنوری از جنس شیشه است و در هنگام کار و تماس با مغزی آن خطر بریدگی و نفوذ شیشه در بدن وجود دارد که مرگبار است.

شکل ۸: نمایی از فیبر نوری و قسمت های مختلف آن

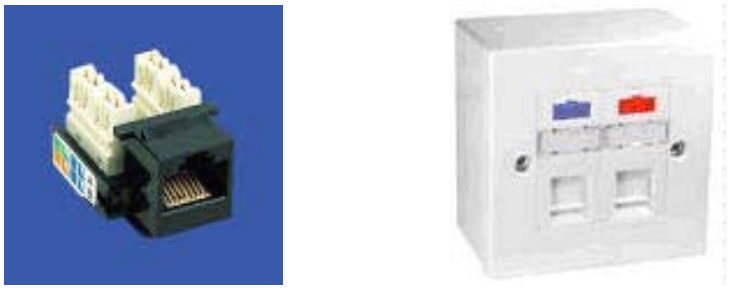
کابل کشی ساختار یافته

یک کابل کشی، منظم و قابل توسعه است که کشف و رفع خرابی در آن به سهولت انجام می پذیرد. در کابل کشی مبتنی بر کابل های CAT5 و یا CAT6 اجزاء زیر وجود دارد:

۱- پچ پانل[1] یک پانل شماره گذاری شده است که اتصالات مادگی[2] در آن قرار می‌گیرد و داخل رک[3] (قفسه فلزی) بسته می شوند.
۲- پچ کورد[4] که کابل رابط بین پچ پانل و سوئیچ یا هاب می باشد.
۳- یک اتصال مادگی دیگر که داخل پچ پانل قرار می‌گیرد.

شکل ۹: پچ پانل و پچ کورد متصل به آن

۴- جعبه ای عموما سفید رنگ[5] که یک عدد اتصال مادگی جهت اتصال کابل رابط کامپیوتر در آن قرار می‌گیرد.
۵- کابل رابط بین اتصال مادگی موجود در پچ پانل و اتصال مادگی درون جعبه سفید.
۶- پچ کورد دیگری که کابل رابط بین جعبه سفید و کامپیوتر خواهد بود.



شکل ۱۰: جعبه ای سفید رنگ و اتصال مادگی درون آن جهت اتصال کابل رابط

[1] - Patch Panel
[2] - Keystone
[3] - Rack
[4] - Patch Cord
[5] - Outlet

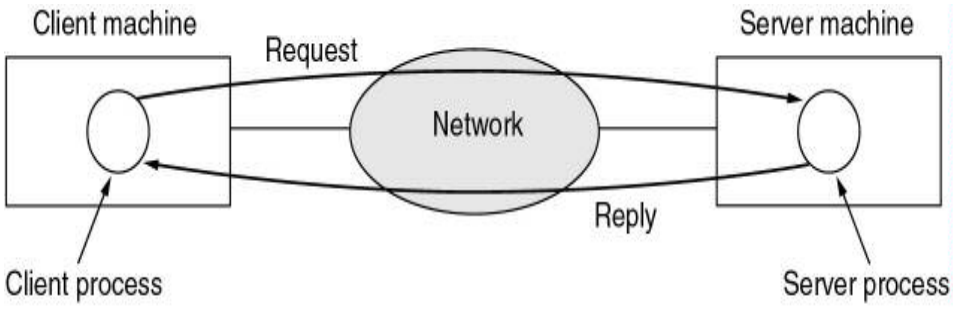
معمولا روی جعبه ها شماره معادل روی پچ پانل نوشته می‌شود تا رفع خرابی به سهولت انجام پذیرد. مدیر شبکه باید همیشه یک جدول از شماره جعبه ها و موقعیت آنها در ساختمان داشته باشد؛ تا به آسانی بتواند ارتباط فیزیکی یک کاربر مشخص را قطع و وصل نماید و یا در رفع خرابی وی اقدام نماید.

به طور کلی در هنگام کابل کشی توجه به نکات زیر لازم است:

- همیشه باید بیشتر از مقدار مورد نیاز کابل تهیه شود.
- هر بخشی از شبکه که نصب می گردد، آزمایش شود. زیرا ممکن است بخش هایی در شبکه وجود داشته باشند که خارج ساختن آنها پس از مدتی دشوار باشد.
- اگر کابل کشی در سطح زمین نیاز باشد لازم است تا کابل ها توسط محافظ مطمئن پوشانده شود.
- دو سر هر کابل باید نشانه گذاری و ترجیحا شماره گذاری گردد.

آشنایی با مفهوم Client / Server

در شبکه های کامپیوتری با ارزان شدن سخت افزار، الگوی شبکه از سیستم های مبتنی بر Mainframe که در آن یک کامپیوتر مرکزی همه پردازش ها را انجام می‌داد و ترمینال ها که توان پردازشی نداشته و فقط اطلاعات پردازش شده را از کامپیوتر مرکزی دریافت و نشان می دادند، به سیستم های مبتنی بر Client/Server منتقل شده است. در این الگو که عمدتا در شبکه مبتنی بر TCP/IP مطرح است یک دستگاه به عنوان سرویس دهنده بر روی یک نشانی IP و یک پورت سرویس دهی مشخص(مثلا ۸۰ برای وب)؛ که زوج IP و پورت اصلاحا سوکت نامیده می شود؛ آماده ارائه خدمات است. دستگاه سرویس گیرنده از نشانی IP خود و یک پورت که معمولا از شماره های بالای ۱۰۰۰ می باشد، درخواست خدمات خود را پس از ارسال درخواست برقراری ارتباط از سوکت خود به سوکت سرویس دهنده می کند. و پس از برقراری ارتباط اقدام به تبادل فرامین و دریافت نتایج آنها و در نتیجه دریافت سرویس مورد نظر می‌نماید.



شکل ۱۱: ارتباط بین پروسه ها در کلاینت و سرور

جهت مشاهده ارتباطات بین سوکت ها، بر روی دستگاهی که به شبکه متصل است، دستور netstat را در محیط DOS اجرا کنید.

آشنایی با تفاوت Dedicated و Non Dedicated و مقایسه آنها

در مدل Client/Server شبکه های کامپیوتری امکان توزیع و یا تخصیص سرویس های مختلف مانند فایل سرویس، Web، FTP ، Email و ... به Serverهای مختلف وجود دارد و مدیر شبکه با توجه به نیازها و منابع موجود سرویس ها را بین سرورها تقسیم می‌کند. این کار امکان توزیع بار را در میان سرورهای مختلف و همچنین ایجاد سرورهای پشتیبان برای خدمات حساس را فراهم می نماید. چنانچه فقط و فقط یک سرویس به یک سرور تخصیص یابد و آن سرور هیچ گونه خدمات دیگری را ارائه ندهد اصطلاحا به آن Dedicated Server گویند ولی چنانچه ارائه چندین سرویس به یک سرور محول گردد، به آن Non Dedicated گویند.

ایجاد شبکه که در آن تمام امور به صورت Dedicated انجام شود به علت نیاز به سرورهای متعدد بسیار پرهزینه است. در عمل مدیر شبکه با توجه به بار و حساسیت سرویس، اقدام به توزیع خدمات بین سرورها نموده و تنها سرویس هایی که بسیار مهم بوده و بار زیادی دارند را به صورت Dedicated اعمال می‌کنند.

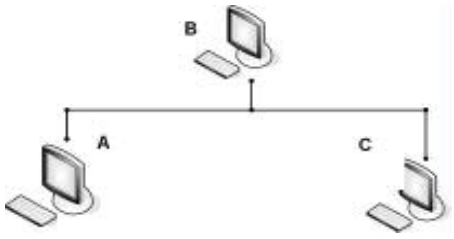
همانگونه که گفته شد پروتکل یکی از اجزاء منطقی شبکه و مجموعه ای از قراردادهای بین دو ماشین برای مشخص نمودن نحوه ارتباط با یکدیگر می باشد؛ و به دلیل اینکه پروتکل مورد استفاده و ساختار شبکه، به یکدیگر وابسته می باشند برخی از پروتکل های مهم به طور مختصر بیان می گردد.

۱- پروتکل NetBEUI

این پروتکل دارای خصوصیات زیر می باشد:

۱- این پروتکل بسیار ساده[1] است. وکافیست بعد از معرفی سخت افزار فقط نصب شود.
۲- برای شبکه های کوچک مناسب است.
۳- ارسال یا انتشار عمومی بسته[2] ترافیکی در شبکه ایجاد می کند.
با توجه به خصوصیاتی که می توان برای انواع پروتکل ها ذکر نمود، مدیر شبکه همیشه باید نکات بسیار مهمی را به عنوان ابزار، در شبکه مد نظر داشته باشد:
الف : admin، admin است چه بسا نام آن تعویض شده باشد؛ اما در حین حال همان وظایف و سطح دسترسی را دارا می باشد.
ب: به بیان بسیار ساده، اعلان یا انتشار عمومی بسته ها چیز بدی است؛ چون ترافیک شبکه را بالا برده و باعث مرگ تدریجی شبکه می گردد. اما در مواردی می توان گفت که انتشار عمومی بسته خوب و لازم است مثلا:
الف: وقتی می خواهیم اصطلاحا چشم بسته، چیزی را درون شبکه بیابیم.
ب: برای اعلان مطلبی عمومی به بقیه اعضاء شبکه می توان از آن استفاده نمود.

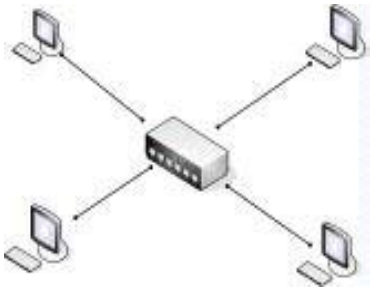
به عنوان مثال شبکه های زیر را در نظر بگیرید:
در شبکه ای به شکل ۱۲ وقتی ماشین A بسته ای را به طور خصوصی برای ماشینB ارسال نماید[3] C هم می تواند آن را بگیرد ولی آیا می تواند از آن استفاده نماید؟



شکل ۱۲ : یک شبکه ساده

در شبکه زیر اگر توزیع کننده ، هاب باشد و ماشینی بسته ای را برای ماشین دیگر، به شکل عمومی[4] ارسال کند، همه ماشین ها آن را دریافت می کنند. اما اگر توزیع کننده سوئیچ باشد فقط ماشین مقصد آن را دریافت می کند.

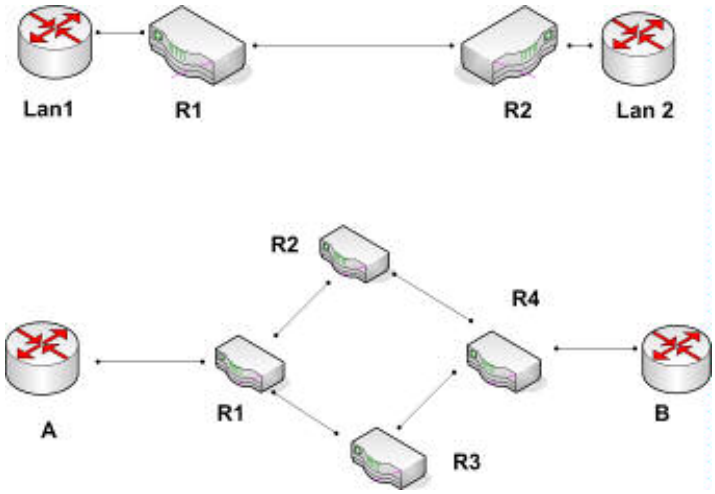
---
[1]- Very Simple Configuration
[2] - Broadcast
[3] - Unicast
4 - Broadcast



شکل ۱۳: شبکه با استفاده از هاب/سوئیچ

وقتی بسته ای به شکل عمومی ارسال می شود این بسته به همه کامپیوترها رسیده و آنها بسته را به لایه های بالاتر می دهند. اما وقتی بسته به طور خصوصی ارسال می شود سایر کامپیوترها اهمیت زیادی به آن نداده و لذا ترافیک کمتری ایجاد می گردد. اگر انتشار بسته به شکل عمومی از حد مشخصی بالاتر رود طوفان انتشار[1] ایجاد می گردد.

ذکر این نکته لازم است که پروتکل Net BEUI قابلیت مسیریابی ندارد[2]. به مثال زیر در این مورد دقت کنید:



شکل ۱۴- نحوه ارتباط در شبکه توسط پروتکل NetBEUI

این دو شبکه با پروتکل NetBEUI نمی توانند ارتباط برقرار کنند چون در این پروتکل مسیریابی پیش بینی نشده است. در این پروتکل تنها وسیله برای دریافت و ارسال اطلاعات، نام ماشین است.

1 - BroadCast Storm
2 -Non Routable

در این شبکه روتر اجازه عبور بسته را نمی دهد البته می تواند بسته های اطلاعاتی را برای همه پخش کند. ولی این اجازه از آن گرفته شده است. زیرا در این صورت در اینترنت همه افراد، اطلاعات بقیه را می دانستند.

۲- IPX/SPX

این پروتکل در شبکه های ناول استفاده می گردید. البته ناول جدید از پروتکلTCP/IP استفاده می کند.

این پروتکل خصوصیات زیر را دارا می باشد:

پیکر بندی آن ساده، قابلیت مسیریابی داشته، هر زمان لازم باشد بسته اطلاعاتی را به صورت عمومی و هر جا لازم باشد آن را به شکل خصوصی منتشر می کند.

در توپولوژی شبکه های کوچک و بزرگ استفاده می شود.

با تمام مزایای ذکر شده در فوق به دلیل عدم سرمایه گذاری روی آن، پروتکل TCP/IP عرف گردید و لذا از آن در شبکه ها استفاده نمی گردد.

با استفاده از این پروتکل به دو طریق ارسال اطلاعات داریم:

IPX ➔ ۱- بدون تضمین Connection less عادی

SPX ➔ ۲- با تضمین Connection Oriented سفارشی

در حالت سفارشی، یک رسید[1] به دست فرستنده می رسد که اگر رسید در هر صورت دریافت نشود، بسته دوباره ارسال می گردد.

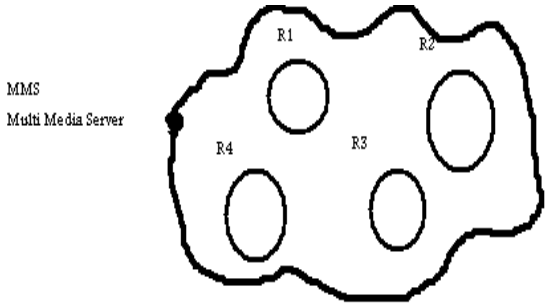
همچنین می توان از IPX/ SPX خواست که بسته را با کدام سرویس ارسال نماید، در شبکه ناول دستوری به نام Rconsole با پروتکل SPX و دستور file Transfer با پروتکل IPX کار می کند.

لازم به ذکر است که در صورت استفاده از پروتکل SPX ، ترافیک شبکه بالا می رود.

1 - Acknowledge

۳- پروتکل TCP/IP

این پروتکل پیکربندی پیچیده ای داشته و سرویس های فراوان و متنوعی را فراهم می کند. یعنی پیچیدگی آن به تنوع سرویس هایش بر می گردد.
این پروتکل در سیستم عامل یونیکس متولد شد ولی در همه سیستم عامل ها استفاده می شود. در شبکه های کوچک قابلیت پیکربندی اتوماتیک و در شبکه های بزرگ قابلیت مسیریابی را نیز دارد. علاوه بر خصوصیات پروتکل های قبلی، قابلیت ارسال بسته به گروهی خاص[1] را نیز دارد.



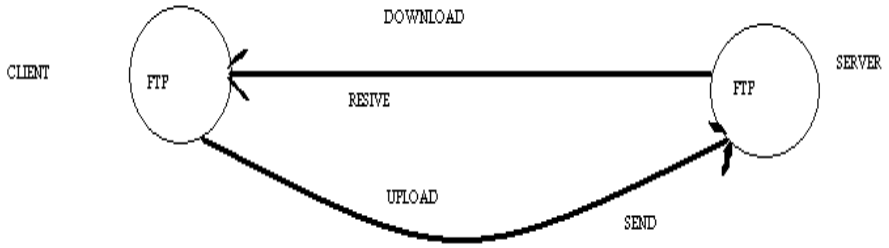
شکل ۱۵: استفاده از Multicast برای ارسال پیام

به عنوان مثال در شبکه فوق بسته ای باید برای ۲۰ ماشین ارسال شود. پس باید برای هر کدام به شکل خصوصی ارسال شده، که کار دشواری است و یا باید به شکل عمومی پخش گردد که در این صورت همه به آن دسترسی دارند و از طرف دیگر ترافیک شبکه نیز بسیار بالا می رود. در این حالت می توان از قابلیت ارسال بسته به گروهی خاص استفاده نمود.
باید اذعان داشت که TCP/IP مجموعه ای از سرویس هاست، لذا باید فلسفه و هدف از اجرای شبکه را دانست به عنوان مثال اهداف زیر را می توان در نظر داشت:
- اشتراک منابع جهت استفاده از سرویس های متعدد
- کنترل و عملیات از راه دور
- ارسال پیغام برای اعضاء شبکه

سرویس های TCP/IP

FTP : File Transfer Protocol که برای انتقال فایل بین دو ماشین استفاده می گردد. چنین سرویسی هم در سمت سرویس دهنده و هم در سرویس گیرنده وجود دارد.

1 - Multicasting



شکل ۱۶: نحوه استفاده از سرویس FTP

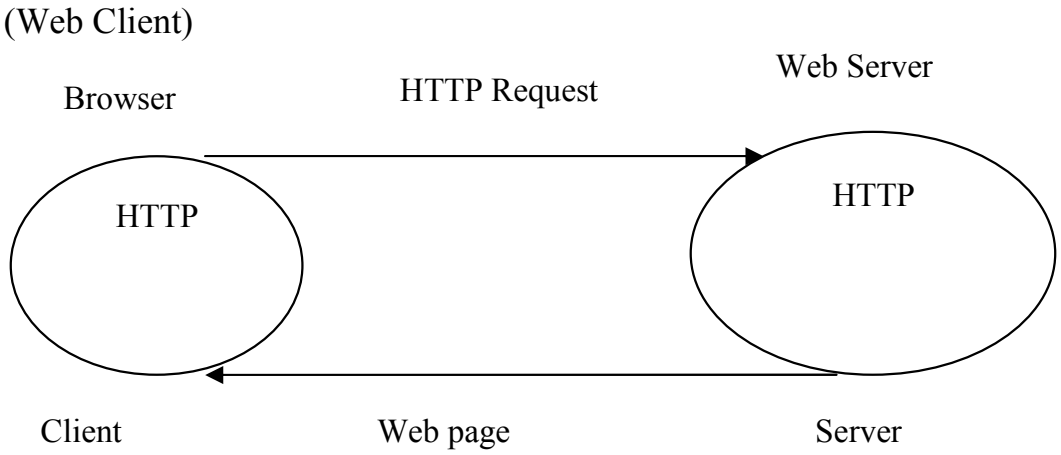
برای FTP Client می توان به نرم افزار Internet Explorer اشاره نمود که به شکل زیر بکار گرفته می شود: Ftp: //.....

به عنوان مثال دیگر می توان نرم افزار Ftp.exe را نام برد که از طریق Command ویندوز قابل اجرا می باشد.

از طرف دیگر در Windows 2000 سرویسی به نام FTP Server وجود دارد.

(Hyper Text Transfer Protocol) HTTP

این پروتکل، سرویسی برای انتقال اطلاعات است. و می توان بلوک دیاگرامی به شکل زیـر بـرای آن متصور شد.



شکل ۱۷: نحوه استفاده از سرویس HTTP

که HTTP Request ممکن است یکی از موارد زیر باشد:

- درخواست صفحات HTML باشد.
- اجرای یک برنامه کاربردی مانند جستجو در میان صفحات وب باشد.
- انتقال یک فایل باشد که این مطلب را می توان در زمان دانلود یا ایمیل دید.

پس بنابراین می توان گفت که پروتکل HTTP یک پروتکل همه کاره است.

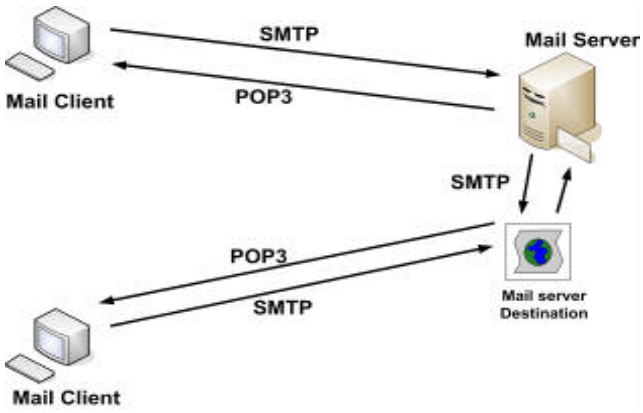
پروتکل های مورد استفاده در ایمیل

سه پروتکلی معروفی که در ایمیل استفاده می شود به شرح ذیل می باشد:

Simple Mail Transfer Protocol: SMTP
Post Office Protocol v3: Pop3
Internet Mail (message) Access Protocol: IMAP4

نرم افزارهای ایمیل هم به دو گروه سرویس دهنده[1] و سرویس گیرنده[2] تقسیم می شوند.

از نرم افزارهای سرویس گیرنده ها می توان به Outlook Express و از سرویس دهنده ها به نرم افزارهای MD Daemon، I Mail و Web Mail اشاره نمود.

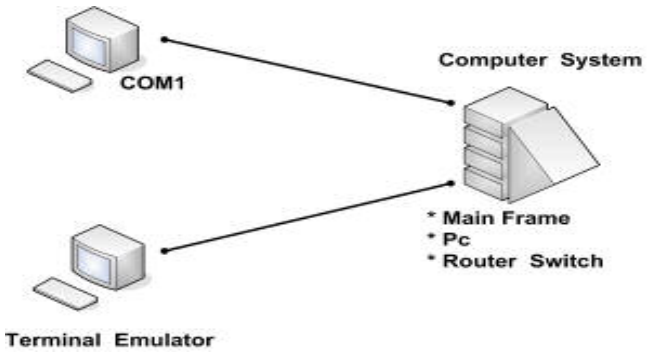


شکل ۱۸: نحوه استفاده از پروتکل های ایمیل در شبکه

Telnet

ترمینال یک وسیله ورودی یا خروجی بوده و بر دو نوع متنی و گرافیکی می باشد.

[1] - Mail Server
[2] - Mail Client



شکل ۱۹: ارتباط بین دو سیستم از طریق شبکه

Telnet : اگر ارتباط بین ترمینال و سیستم کنترل از طریق شبکه بوده و پروتکل مورد استفاده TCP باشد در این صورت Telnet یک Terminal Emulator Text تعریف می شود. بعضی از ترمینال ها به قرار زیر هستند:

Hyper Terminal, RAdmin, Term95, PC Anywhere

Simple Network Management Protocol **: SNMP**

از این پروتکل که از نوع UDP می باشد برای مدیریت شبکه استفاده می شود. در جهت تحقق این کار بر روی هر ماشین شبکه، باید نرم افزاری[۱] نصب نمود تا اطلاعات مدیریتی را از آن ماشین جمع آوری نموده و در یک بانک اطلاعاتی قرار دهد. مدیر سیستم نیز نرم افزار دیگری[۲] جهت مشاهده بانک اطلاعاتی استفاده می نماید.

مایکروسافت چنین نرم افزاری نداشته و از سرویس های بقیه کمپانی ها استفاده می کند. برخی از این نرم افزارها به شرح ذیل می باشند:

Cisco Works - What's Up Gold - Hp Open View - Solar Winds

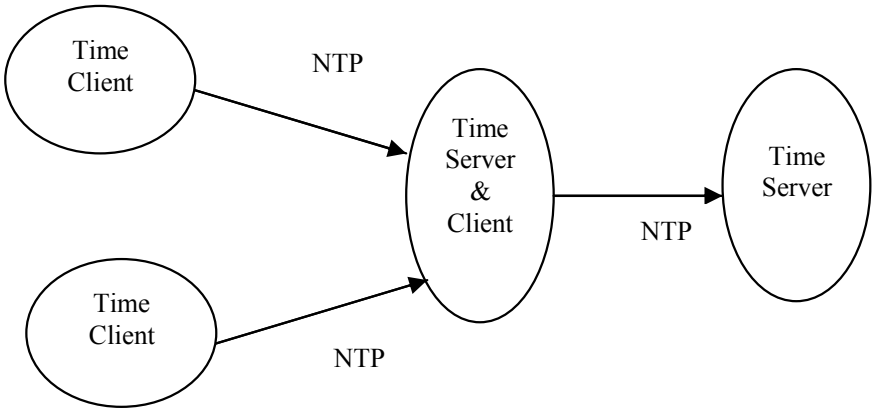
Simple Network Time Protocol : SNTP

این پروتکل قابلیت همزمان نمودن ساعت را در بین تمام اجزاء شبکه فراهم می کند.

---

[1] - SNMP Agent

[2] - Management Information Base (MTB)



بلوک دیاگرام کاربرد پروتکل SNTP

در مایکروسافت چنین سرویسی به نام Windows time در مسیر زیر وجود دارد:

Administrator tools → Service

این سرویس را می توان با اجرای دستورات زیر در Command ویندوز مشاهده نمود:

Net time /query sntp

و با دستور زیر پیکربندی نمود:

Net time/set sntp:192.168.10.1
(Server)

Time.nist.gov

۱- در یک شبکه مبتنی بر ویندوز 2000 که کامپیوترها در گروه کاری قرار دارند به صورت پیش فرض سرویس Windows Time غیر فعال است.

۲- در یک شبکه مبتنی بر ویندوز 2000 که کامپیوترها در یک حوزه قرار دارند به صورت پیش فرض این سرویس فعال است. و در این صورت Domain Control به عنوان Time Server و بقیه کامپیوترها به عنوان Time Client عضو این حوزه هستند.

۳- در سیستم عامل های ویندوز 2003 وXP چه در گروه کاری و چه در حوزه این سرویس فعال است.

۴- برای کارکرد صحیح سرویس Windows time اختلاف ساعت بین سرویس دهنده و سرویس گیرنده نباید از ۱۲ساعت بیشتر باشد یعنی باید گزینه Date در پنجره Time Zoneیکسان باشد.

TCP/IP Host

ماشین هایی که بتوان توسط آنها با TCP/IP ارتباط برقرار نمود TCP/IP Client نامیده می شوند. هر Host روی TCP/IP دو مشخصه دارد.

Address: IP Address
Name: نام ماشین

در این پروتکل ملاک عمل IP می باشد؛ زیرا نام کامپیوتر ممکن است در شبکه تکراری باشد:

www.usb.ac.ir

Fully Qualified Domain Name (FQDN)

اسامی کامپیوتر ها از چند قسمت تشکیل شده است:

WWW.Host Role.mail

نقشی که اعمال می کند

Site Name .usb .com

دامنه فعالیت و یا وابستگی

Computer Name یا Net Bios Name نام کامپیوتر بوده که حداکثر ۱۵ کاراکتر بوده و معمولا در زمان نصب سیستم عامل ویندوز به کامپیوتر داده می شود. لازم به ذکر است کـه علامـت نقطـه در نامگذاری مجاز نیست.

Net Bios Name = Computer Name
TCP/IP Name = Full Computer Name

اما هنگامی که در نظر است یک کامپیوتر در شبکه ای دیگر قابل دسترسی باشد باید FQDN را توسط IP Address تصحیح نمود. که این کار توسط سرویسی به نام DNS انجام می گیرد. در ادامه و به تفصیل در مورد آن توضیح داده خواهد شد.

اما IP Address که ملاک عمل می باشد یک عدد ۴ بایتی به شکل زیر است:

W. X. Y. Z 0 < { W. X. Y. Z } < 255

که به این نوع IP Address ، IP.V4 گویند. نوع دیگری از IP که ۱۲۸ بیت یا ۱۶ بایتی است به IPNGیا IPV6 معروف است.

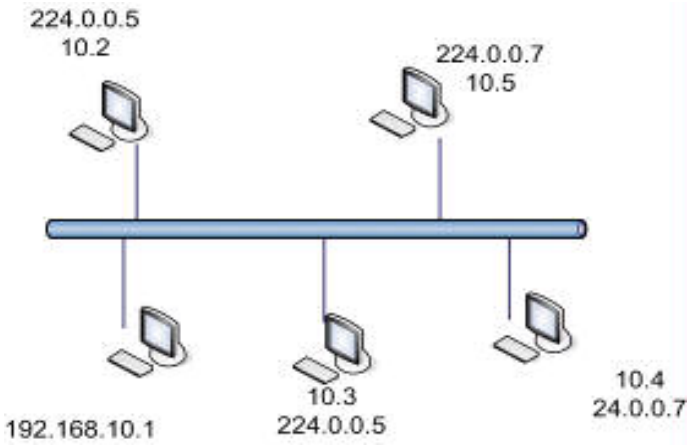
هر IP Address از دو قسمت Network ID و Host ID تشکیل شده است. این آدرس ها به کلاس هایی به ترتیب زیر طبقه بندی شده اند:

Host ID	Network ID	Class	W
3 byte	1 byte	A	0-126
2 byte	2 byte	B	128-191
1 byte	3 byte	C	192-223
	Multicast	D	224-239
		E	240-255

جدول ۳: کلاس بندی آدرس های مختلف با فرمت W. X. Y. Z

به آدرس 127. X. Y. Z، Loop Back Adders گفته می شود که برای بررسی کامپیوترهای شخصی استفاده می شود. یعنی با دستور Ping 127.0.0.1 می توان TCP/IP هر کامپیوتر را چک نمود.

برای مثال شبکه زیر را در نظر بگیرید:



شکل ۲۰: شبکه ای که در آن یک سرویس گیرنده دو آدرس دارد.

در این شبکه می توان دید که یک سرویس گیرنده دو آدرس IP داشته، که از یکی از آنها برای ارسال بسته به گروهی خاص استفاده می شود. حال این سوال پیش می آید که از چه کلاس آدرسی باید در هر شبکه استفاده نمود؟ واضح است که کلاس شبکه به تعداد ماشین های موجود در شبکه بستگی دارد.

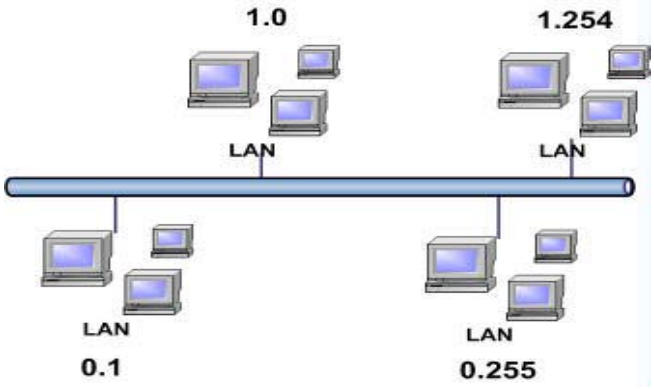
به عنوان مثال برای یک شرکت که ۲۰ کامپیوتر داشته و تا چند سال دیگر قرار است به ۲۵ عدد برسد بهتر است از کلاس C استفاده نمود.
ذکر این نکته ضروری است که بایت های Host ID نمی تواند همگی با هم صفر یا همگی با هم ۲۵۵ باشد. اگر بایت های Host ID همگی با هم ۲۵۵ باشد به آن انتشار عمومی[1] گفته می شود.
به آدرس های صحیح(■) و نادرست(×) در جدول زیر دقت نمائید:

192.168.0.1	■	18.255.0.255	■	10.0.0.0	×
192.168.10.0	×	۱92.168.10.255	×	172.16.255.255	×
130.145.0.0	×	172.16.255.255	×	172.16.255.0	■
10.0.0.0	×	10.255.255.255	×	18.0.0.255	■
18.0.255.0	■	172.16.0.255	■		

جدول ۴: مثال هایی از آدرس های مجاز و غیرمجاز

برای حدود ۱۰۰ ماشین که در آینده به ۵۰۰۰ عدد می رسد می توان از کلاس B استفاده نمود.
اگر در این حالت از چند کلاس C استفاده شود در این صورت از دیدگاه شبکه، کامپیوترهای موجود به چند شبکه مجزا تقسیم شده و نمی توانند همدیگر را پیدا نمایند.

N.I : 140.150.X.Y
N.N : 140.150.0.0



شکل ۲۱: استفاده از چند کلاس مختلف برای یک شبکه

[1]- BroadCast

در کلاسB حداکثر Network	2^{14} =۶۴*۲۵۶	در کلاس Bحداکثر Host ها	$2^{16} - 2$
در کلاس A حداکثرNetwork	۱۲۶	در کلاس AحداکثرHost ها	$2^{24} - 2$
در کلاس C حداکثر Network	2^{21}	در کلاسCحداکثرHost ها	$2^{8} - 2$

Subnet mask: فرض کنید شبکه ای ۵۰۰۰ کامپیوتر داشته، لذا از کلاس B به شکل 130.131.X.Y استفاده می گردد. در این صورت تعداد زیادی آدرس از دست می رود. زیرا فقط با ۱۳ بیت می توان ۵۰۰۰ کامپیوتر را آدرس دهی نمود و بقیه بیت ها را به Net ID اضافه و تعداد شبکه ها بیشتری را آدرس دهی کرد. به این نوع آدرس دهی، Classless و به حالت نرمال آن Full Class گفته می شود.

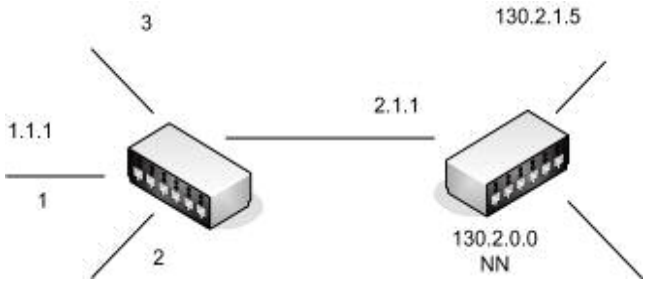
TCP از روی Subnet mask پی می برد که از ۳۲ بیت مربوط به آدرس چند بیت Net ID و چند بیت Host ID است. بدین ترتیب که بیت های صفر آن مربوط به Host ID و بیت های یک آن مربوط به Net ID است.

همواره باید نکات زیر را مورد توجه قرار داد:

- همه بایت های Net ID نمی تواند با هم صفر یا ۲۵۵ شود.
- برای این که کلیه Host ها مستقیما بتوانند با هم ارتباط برقرار کنند لازم است تا Net ID آنها یکسان باشد.
- IP Address برای هر ماشین باید منحصر به فرد باشد.

شروع مکانیزم ارسال اطلاعات در TCP/IP

شبکه های زیر را در نظر بگیرید:



شکل ۲۲: نحوه تبادل بسته در دو شبکه مختلف

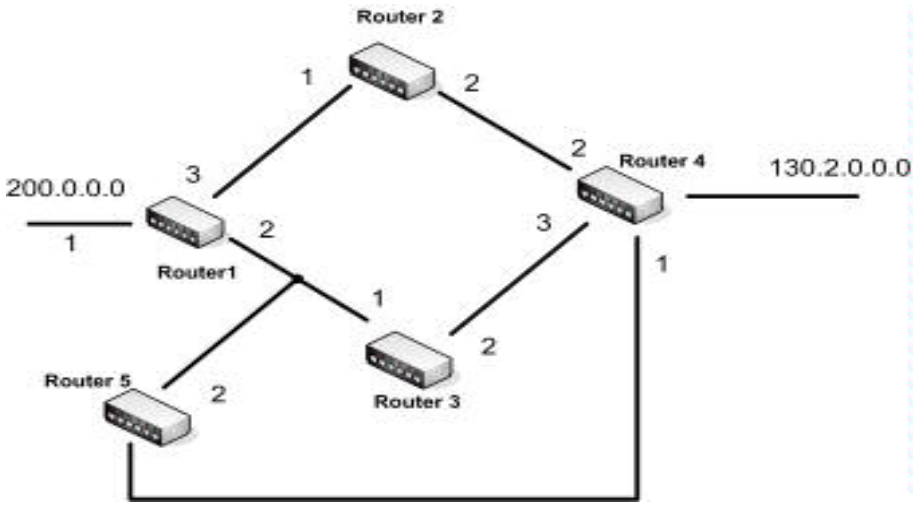
در شکل فوق بسته ای را فرض کنید که قرار است از آدرس 130.1.1.2 بـه یـک Web server بـه آدرس http://130.2.1.5 ارسال گردد. در این صورت اولین کاری که ماشین مبدا انجـام مـی دهـد این است که آدرس شبکه مقصد را نگاه کرده و با آدرس شبکه خودش مقایسه می کنـد. اگـر ایـن پارامتر یکسان باشد می توان فهمید که ماشین مبدا و مقصد در یک شبکه قرار دارند. در غیـر ایـن صورت آن را به روتر ارسال می کند. روتر ها جدولی به نام جدول مسیریابی[1] به شکل زیر داشـته و از روی آن می فهمد که بسته را به چه مقصدی ارسال نماید.

شماره پورت	شماره شبکه
۲	۱۳۰.۲.۱.۵

جدول ۵: مثالی از جدول مسیریابی

به عنوان مثالی دیگر، شبکه شکل ۲۳ را در نظر بگیرید:
در این شبکه برای ارسال داده کدام یک از دو پورت ۲ یا ۳ بهتر است؟
ارزش مسیر[2] پارامتر دیگری در شبکه می باشد؛ هر چه این عدد کوچکتر باشد مسیر بهتر بوده و ترافیک آن کمتر است. پس با توجه به این مسئله ارسال از پورت ۲ بهتر به نظر می رسد.

[1] - Routing Table
[2]- metric



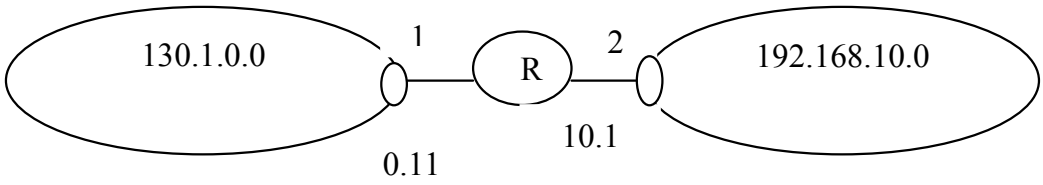
شکل ۲۳: چندین شبکه که توسط روترهای مختلف در ارتباطند.

روتر	ارزش مسیر	شماره پورت	شماره شبکه
R5	1	2	130.2.0.0
R3	20	3	130.2.0.0

در مثال فوق اگر روتر R5 اضافه شود مسیریابی چگونه انجام می شود؟

در این حالت چون بعد از این که بسته از پورت ۲ خارج گردید، باید مشخص شود که باید از کدام روتر عبور نماید لذا پارامتر دیگری نیز اضافه می شود و آن روتر گیرنده اطلاعات است. همچنین می توان به جای آدرس روتر، IP آنرا داد و می توان به جای شماره پورت، IP اینترفیسی را که به آن وصل شده را وارد نمود. اگر ارزش دو مسیر یکسان باشد دیگر مهم نیست بسته ها از چه مسیری ارسال گردد. و حتی می تواند در هر دو مسیر اطلاعات ارسال گردد.

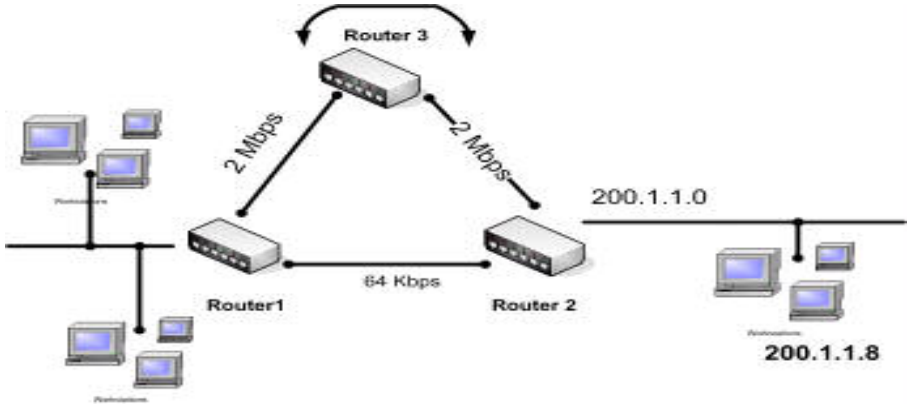
سوال دیگری که ممکن است به ذهن خطور کند این است که جدول مسیریابی چگونه و کی ساخته می شود؟



شکل ۲۴: نمای کلی یک شبکه با جدول مسیریابی به شکل زیر

N.N	Port ID	Metric	N.R
192.168.10.0/24	2	1	-
130.1.0.0/16	1	1	-

جدول مسیریابی می تواند به صورت استاتیک توسط مدیر شبکه کامل شده و یا در حین کار به صورت دینامیکی ساخته و بروز شود که در این صورت پروتکل مسیریابی[1] مطرح می شود.
در مثال قبل اگر بین روتر های R2 و R1 هیچ سرویس گیرنده ای نباشد، لازم نیست روترها حتی IP داشته باشند.
در ادامه مثال فوق، فرض کنید R2 اینترفیسی برای جاهای دیگر دارد.



شکل ۲۵: نحوه ارسال بسته به ماشینی که آدرس آن در جدول مسیریاب نیست.

در این صورت بسته ای که به روتر ۱ می رسد و قرار است به آدرس 124.4.7.3 برود چون در جدول مسیریاب مشخص نشده پیغام Destination Host unResearchable ظاهر می شود (یعنی به روتر دسترسی داشته ولی پاسخی دریافت نمی گردد) و برای مقاصد 180.1.1.7 و 215.43.21.2 هم چنین مشکلی وجود دارد. بنابراین باید این آدرس ها را نیز در جدول مسیریاب وارد نمود که وقتی تعداد این مسیرها زیاد شود، دیگر انجام این کار مشکل می باشد. لذا مشخص می گردد که اگر بسته ی به R1 رسید و ندانست کجا برود، آن را به بعدی ارسال نماید که به آن 0.0.0.0 یا Default gateway گفته می شود.

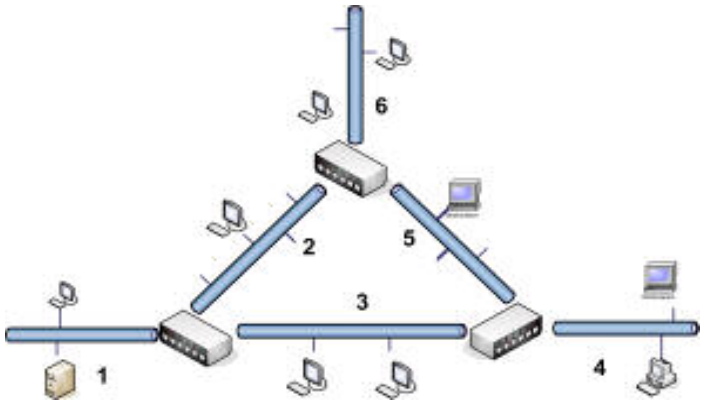
[1] - Routing protocol

حال اگر در شبکه قبل R3 را نیز داشته و در نظر است بسته ای سریعا به یک ماشین مشخص به آدرس 200.1.1018 ارسال گردد و مسیر نیز مشخص باشد در این صورت آن را وارد جدول مسیریاب می کنیم.

N.N	Port ID	Metric	NR
200.1.1.8/32	3	1	R3

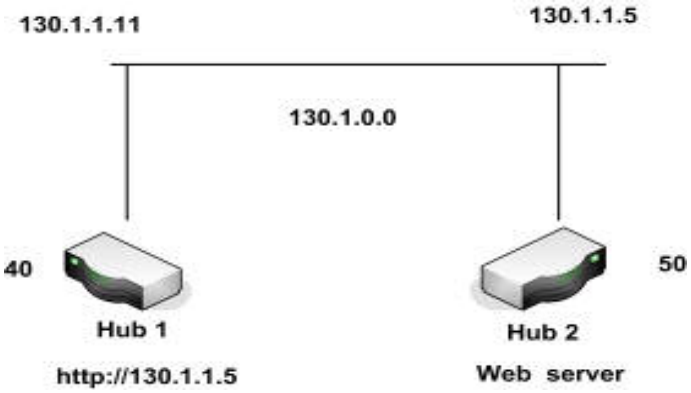
جدول مسیریاب را می توان از طریق Command ویندوز با اجرای دستورات زیر مشاهده نمود.

C:\netstat –r
C:\route print



شکل ۲۶: شبکه ای مبتنی بر سوئیچ هایی با قابلیت مسیریابی

شکل ۲۶ در صورتی شبکه می باشد که سوئیچ ها، روتر هم باشند که در این صورت به آنها سوئیچ لایه سه گویند. در این بخش به بررسی چگونگی دریافت بسته در کارت شبکه پرداخته می شود. به عنوان مثال شبکه زیر را در نظر بگیرید:



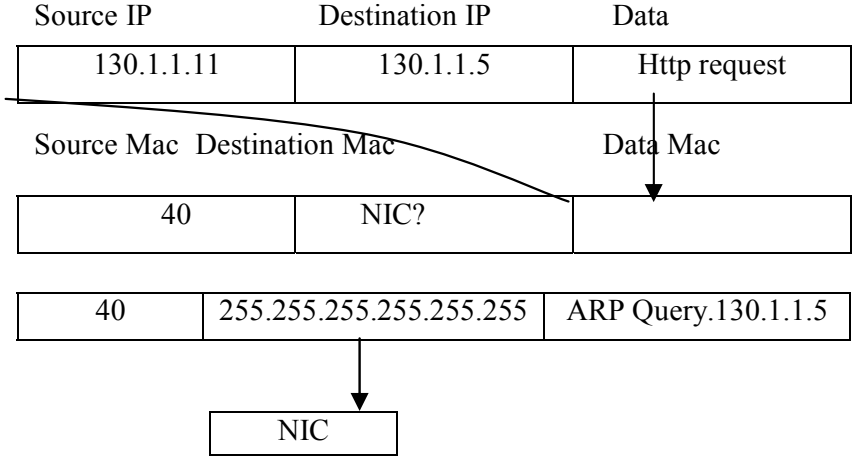
شکل ۲۷: مثالی از ارسال یک بسته TCP/IP

یک بسته TCP/IP مانند شکل ۲۸ می باشد. یعنی یک بسته برای ارسال به ماشینی با IP مشخص ابتدا باید به کارت شبکه ارسال گردد. اما این کار امکان پذیر نیست زیرا کارت شبکه مفهوم IP را نمی فهمد و فقط آدرس فیزیکی[1] را می داند. لذا به کمک آن، اقدام به ارسال بسته می نماید.

هر کارت شبکه اعم از باسیم و بی سیم دارای یک شماره سریال شش بایتی منحصر به فرد جهانی به نام آدرس فیزیکی است که در زمان تولید کارت شبکه در آن تعریف می‌شود. به هر شرکت تولید کننده یک رنج بزرگ از سریال ها تخصیص داده شده است که آن شرکت فقط مجاز است از رنج مشخص شده، سریالی به کارت های تولیدی خود اختصاص دهد. این آدرس در پروتکل شبکه، در لایه فیزیکی قرارگرفته است و به همین دلیل به آن آدرس فیزیکی گفته می شود.

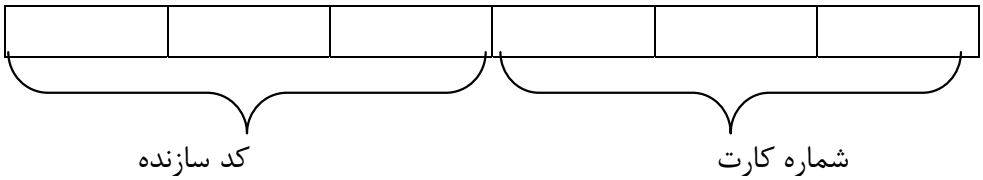
آدرس فیزیکی یا منطقی، به آدرس سیستم در لایه های بالاتر شبکه گفته می شود.

نکته کلیدی و متمایز کننده شبکه محلی و شهری در این است که در شبکه محلی سیستم های کامپیوتری برای ارتباط با یکدیگر باید آدرس فیزیکی یکدیگر را به ترتیب زیر یافته و در لایه فیزیکی مستقیما با هم ارتباط برقرار کنند.



شکل ۲۸: یک بسته TCP/IP که قرار است از طریق کارت شبکه ارسال گردد.

آدرس فیزیکی هر ماشین در شبکه به شکل زیر است:



[1] - Mac Address

از روی کد سازنده می توان فهمید کارت شبکه محصول چه شرکتی است.
آدرس فیزیکی کارت شبکه را می توان با اجرای دستور IPConfig /all در محیط DOS، مشاهده نمود. آدرس فیزیکی در قسمت Physical Address نتیجه اجرای دستور فوق، با یک مقدار ۶ بایتی و به صورت هگزا دسیمال نمایش داده می‌شود.
قبل از آنکه TCP/IP بسته ای را به کارت شبکه تحویل دهد، باید IP Address را به آدرس فیزیکی تبدیل نماید که به این عمل Address Regulation گفته می شود.
سه روش برای یافتن آدرس فیزیکی مقصد وجود دارد:
اول این که روی ماشین مبدا جدولی شامل کلیه آدرس های فیزیکی ماشین های شبکه موجود باشد. روش دوم این است که به کمک فراخوان یا اعلان عمومی، آدرس فیزیکی آن را جویا شد. و در نهایت روش سوم بدین ترتیب است که کامپیوتری به عنوان سرور وجود داشته باشد و در صورت نیاز برای یافتن آدرس فیزیکی خاصی، به آن مراجعه نمود.

پروتکل ARP (Address Resolution Protocol)

این پروتکل جهت مشخص کردن نشانی آدرس فیزیکی از روی آدرس IP بکار می‌رود. هر کامپیوتر یک جدول به نام جدولARP در حافظه خود دارد که نشانی IP و آدرس فیزیکی کامپیوترهایی را که اخیرا با آنها کار کرده است را برای یک مدت کوتاه نگهداری می‌کند. چنانچه کامپیوتر بخواهد با کامپیوتری دیگر که در جدول ARP رکوردی برای آن وجود ندارد کار کند، یک درخواست برای تمام کامپیوترهای شبکه ارسال و آدرس فیزیکی مرتبط با IP را سوال می‌کند. دستگاهی که آدرس IP مورد نظر را داراست به عنوان پاسخ، آدرس فیزیکی خود را اعلام می کند و دستگاه متقاضی ارتباط، پس از اضافه کردن یک رکورد برای آن در جدولARP خود، از نشانی فیزیکی برای ارتباط با دستگاه مقابل بهره می‌برد.
در شبکه های مبتنی بر مایکروسافت هر ۱۰ دقیقه یک بار درخواست خود برای تمام کامپیوترهای شبکه ارسال می کند و در شبکه های مبتنی بر 3Com هر ۱۵ دقیقه این عمل انجام می گیرد. که این موضوع به دلیل افزایش ترافیک شبکه، یک نقطه ضعف محسوب می گردد. بنابراین این زمان را که به Time out معروف است باید (البته روی هر سیستم جداگانه) زیاد گردد. که عملی وقت گیر است.
جدول ARP هر دستگاه با اجرای دستور ذیل قابل مشاهده می باشد:

```
C:\arp –a
```

چنانچه می‌خواهید آدرس فیزیکی یک IP مشخص (مثلا 10.10.10.5) را در شبکه محلی خود پیدا کنید ابتدا دستور ذیل را اجرا کرده و سپس دستور قبل را وارد نمایید:

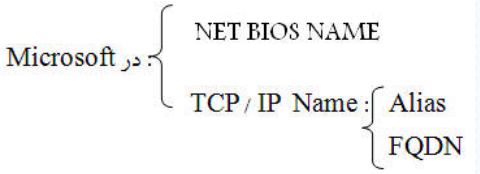
C:\ping 10.10.10.5

در ادامه مثالی را فرض کنید که در آن وب سرور در شبکه دیگری است. پس باید آدرس فیزیکی روتر را یافته و فریم را تحویل روتر داد. روتر این فریم را گرفته و با توجه به قسمت دیتای فریم، بسته را به ماشینی به IP Address مقصد تحویل می دهد.

همانطور که گفته شد به کمک دستور arp –a می توان جدول آدرس های فیزیکی[1] را مشاهده کرد. برای وارد نمودن این آدرس ها در این جدول به صورت استاتیکی، از دستور arp -s می توان استفاده نمود.

حال اگر آدرسIP بین چند ماشین تکراری باشد هر ماشینی که زودتر به درخواست عمومی پاسخ دهد بسته را دریافت می کند. پس از ۱۰دقیقه دوباره درخواست عمومی ارسال می گردد و در این مرحله ممکن است ماشین بعدی به آن پاسخ دهد، لذا در شبکه اختلال ایجاد شود.

برای ارتباط در شبکه ها باید نام کامپیوتر به آدرسIP تبدیل شود، اسامی کامپیوترها به دو شکل زیر هستند:



این دو را تفکیک نموده و هر کدام را با درخواست[2] مربوط به خودش به یکی از دو شکل زیر می توان یافت.

۱- از درون فایلی درون خود کامپیوتر در مسیر زیر:

Windows Directory\System32\Drivers\etc\hosts

۲- از سرویس دهنده ای به نام DNS Server

۳- توسط درخواست عمومی از کلیه ماشین های شبکه سوال شود.

که روش ایده آل این است که همه کامپیوترهای شبکه به سراغ DSN Server بروند.

برای یافتن اسامی Net Bios Name نیز سه روش وجود دارد :

الف: از درون فایلی درون خود کامپیوتر در مسیر زیر:

[1] - Mac Address Table
[2] -TCP/IP Request

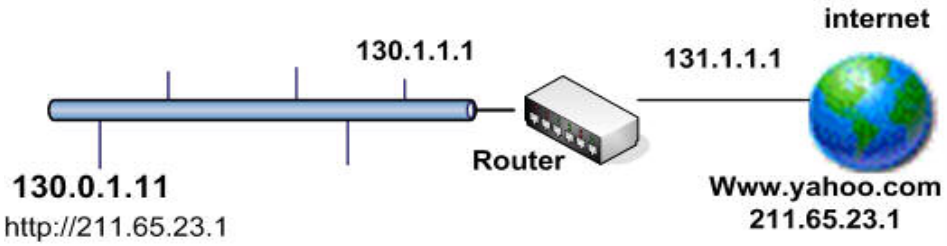
Windows Directory\System32\Drivers\etc\lmhosts

ب: از یک کامپیوتر سروری به نام Wins server

ج: توسط درخواست عمومی از کلیه ماشین های شبکه سوال شود.

نکاتی دیگر در مورد IP Address

هر ماشین در شبکه ی مبتنی بر پروتکل TCP/IP برای ارتباط نیازمند استفاده از IP Address می باشد. شبکه زیر را در نظر بگیرید:



شکل ۲۹: اختصاص آدرس های IP

دو نوع IP Address معتبر[1] و غیرمعتبر[2] وجود دارد. با توجه به تعداد کامپیوترهای موجود در شبکه، یک رنج IP ثبت شده از شرکت ثبت کننده منطقه‌ای یا RIR گرفته و به عنوان IP معتبر به هر ماشین اختصاص داده می شود. این روش آدرس دهی دو مشکل دارد:

اولا باید هزینه زیادی برای ثبت IP صرف نمود.

ثانیا این که با توجه به محدودیت این آدرس ها در جهان، مشکل کمبود IP به وجود می آید.

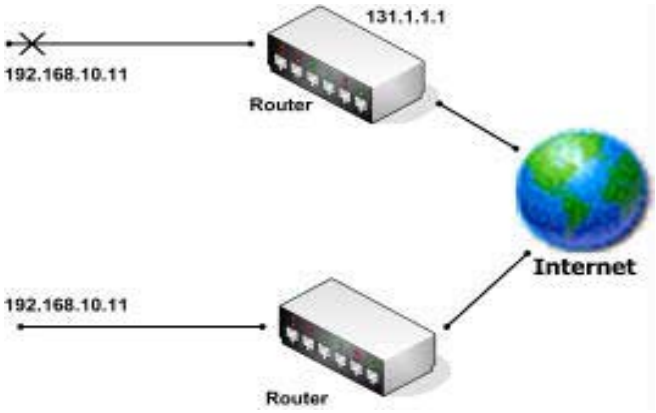
اما می توان بدون صرف هزینه به کامپیوترهای شبکه IP اختصاص داد. برای این کار می توان از IP های غیر معتبر استفاده نمود. این IP Address به شکل زیر در کلاس های مختلف طبقه بندی شده اند و هرگز رجیستر نمی گردد و می توان آنها را در شبکه متعدد استفاده نمود.

A: 10.X.Y.Z
B: 172.16.X.Y
C: 192.168.0.X

.
.
.
.

192.168.255.X

[1] - Valid IP Address
[2] - Invalid IP Address



شکل ۳۰: استفاده از آدرس های غیرمعتبر در شبکه

درشبکه های داخلی مانند شبکه فوق ازIP غیر معتبر برای آدرس دهی استفاده شده است و فقط برای ارتباط با شبکه خارجی نظیر اینترنت با استفاده از عملیاتی به نام NAT[1] از IPهای معتبر استفاده می شود؛ که طی آن یکIP غیر معتبر داخلی بهIP معتبر ترجمه شده و ارتباط با اینترنت از طریق آن انجام می‌پذیرد. بدین صورت که روتر IP خود را که یک آدرس معتبر می باشد روی بسته قرار داده و ارسال می کند. پاسخ دریافت شده از شبکه خارجی نیز به روتر ارسال می گردد. لذا با نصب NAT می توان آدرس های غیر معتبر را به آدرس معتبر تبدیل نمود. این کار سرعت انتقال داده را در شبکه کاهش می دهد اما مزایایی فراوانی هم دارد. NAT در مواردی که تعداد IP های معتبر در دسترس، کم است و نیاز به برقراری ارتباط تعداد زیادی دستگاه با اینترنت است کاربرد دارد. همچنین به عنوان یک روش مناسب جهت ایمن سازی شبکه قابل استفاده است زیرا کامپیوتری که از طریق NAT با شبکه اینترنت در ارتباط است به دلیل عدم ارتباط مستقیم از امنیت بیشتری برخوردار خواهد بود.

برای آگاهی از این مسئله که IP یک کامپیوتر معتبر می باشد یا نه، کافی است پس از اتصال به شبکه دستور ذیل را اجرا نمود:

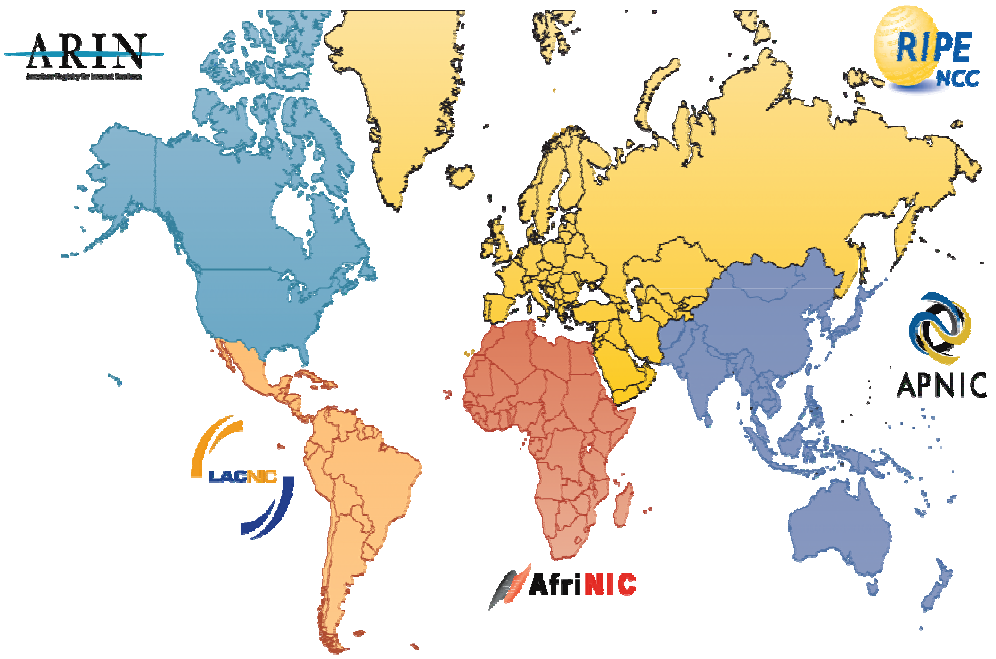
C:\ipconfig

همچنین برای کشف IP معتبری که خدمات را به کامپیوتر ما ارائه می‌دهد می توان به سایت www.myipaddress.com رجوع نمود.

[1] - Network Address Translation

مدیریت فضای IP در جهان

فضای IP در جهان توسط چهار سازمان منطقه‌ای که اصطلاحا ثبت کننده منطقه‌ای[1] RIR نامیده می‌شوند مدیریت می شود. این سازمان ها که به صورت جغرافیایی عمل می کنند در محدوده جغرافیایی خود مسولیت تخصیص و مدیریت IPها را برعهده دارند. در هر کشوری سرویس دهندگان اینترنت[2] پس از عضویت در سازمان مربوط به منطقه جغرافیایی خود به عنوان یک تخصیص دهنده محلی[3] می توانند از طریق RIR نشانی ها را دریافت کرده و در اختیار کاربران خود قرار دهند. لیست RIR ها در جدول ۶ به تفکیک منطقه جغرافیای تحت پوشش آورده شده است.



شکل ۳۱: چهار سازمان ثبت کننده منطقه‌ای IP در جهان

جهت اطلاع از اینکه یک نشانی IP معتبر واقعا به نام چه شبکه ای ثبت شده است می توان با توجه به جدول زیر و منطقه ای که در آنجا نشانی IP فعال شده است به نشانی های اینترنتی مشخص شده مراجعه نمود و آدرس IP مورد نظر را در قسمت جستجو آن سایت وارد کرد.

---

[1] - Regional Internet Registry
2 - Internet Service Provider
3 - Local Internet Registry (LRI)

RIRs	Region	Site
AFRINIC	Africa	www.afrinic.net
APNIC	Asian Pacific Network Information Center	www.apnic.net
ARIN	American Registry for Internet Numbers	www.arin.net
LACNIC	Latin American and Caribbean Internet Address Registry	www.lacnic.net
RIPE NCC	Europe, the Middle East and parts of Central Asia	www.ripe.net

جدول ۶: لیست RIR ها به تفکیک منطقه جغرافیای

DHCP Server مسأله ای دیگر در TCP/ IP

در صورتی که تعداد ماشین در یک شبکه کم باشد می توان پیکربندی شبکه را به صورت دستی انجام داد و هرIP را به یک کامپیوتر مشخص اختصاص داد. اما اگر تعداد ماشین های شبکه زیاد بود این کار باید به صورت اتوماتیک صورت گیرد. این وظیفه را DHCP Server بر عهده دارد.

پس برای پیکربندی ماشین های سرویس گیرنده دانستن فرامین زیر ضروری به نظر می رسد:

۱- فرمان IP Config

۲- فرمان Ping

با دستور Ping می توان از شکل و نحوه سلامت ارتباط مطلع گردید و همچنین توسط آن می توان ارتباط دو ماشین و کامپیوترهای موجود در مسیر آنها را چک نمود. این فرمان به صورت زیر اجرا می گردد:

$$Ping \begin{bmatrix} name \\ IP \end{bmatrix}$$

مثال: Ping 192. 168. 10. 1

با استفاده از دستور زیر نیز می توان از سالم بودن کارت شبکه کامپیوتر مطمئن شد.

$$\begin{Bmatrix} ping & 127.0.0.1 \\ ping & local\ Host \end{Bmatrix}$$

و به کمک دستور زیر مدت زمانی برحسب میلی ثانیه برای دریافت پاسخ تعیین می گردد.

$$Ping\ -w \begin{bmatrix} name \\ IP \end{bmatrix}$$

بعضی مواقع ممکن است یک شرکت فراهم کننده اینترنت، پروتکل Ping را مسدود کرده باشند. در این صورت سیستم به Ping جواب نمی دهد ولی به http پاسخ خواهد داد.

استفاده از دستور زیر سبب می گردد تا هنگام دریافت پاسخ سیستم نسبت به ارسال بسته به صورت نامحدود اقدام نماید.

$$Ping \ -t \begin{bmatrix} name \\ IP \end{bmatrix}$$

و حتی توسط دستور ذکر شده در زیر می توان تعداد بسته های ارسالی را هم مشخص نمود:

$$ping\ -n \quad \begin{bmatrix} name \\ IP \end{bmatrix}$$

دستور زیر طول بسته ارسالی را برحسب بایت نیز مشخص می کند:

$$ping \quad -L \begin{bmatrix} name \\ IP \end{bmatrix}$$

و این دستور نام ماشین را ارسال می نماید:

ping -a IP Address

برای travel shooting و ردگیری شبکه WAN و پی بردن به روترهای موجود در مسیر می توان از دستورهای زیر استفاده نمود:

$$Tracert \begin{Bmatrix} Name \\ IP \end{Bmatrix}$$

Tracert -d WWW.Yahoo.com

برای آگاهی از وضعیت سرویس گیرنده ها و پورت ها نیز می توان از دستورهای زیر استفاده نمود.

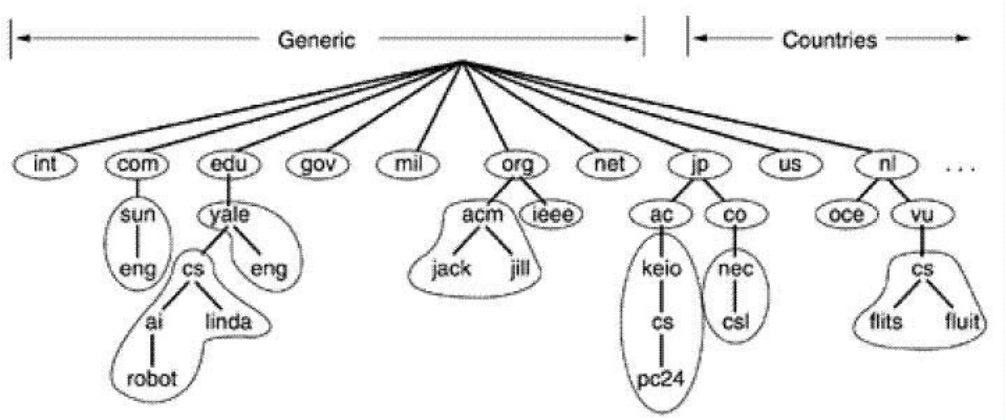
arp -a
netstat -n
netstat -a

سرویس DNS

همان گونه که در ابتدا بیان گردید DNS[1] یکی از سرویس های اصلی و پایه در شبکه‌های مبتنی بر IP و از جمله اینترنت است. به گونه‌ای که بدون وجود آن عملا کلیه سرویس های دیگر از کار خواهند افتاد. به همین جهت یکی از چهار پارامتر اصلی[2] در تنظیمات شبکه مبتنی برTCP/IP، تعریف یا مشخص کردن سرویس دهنده DNS است.

[1] - Domain Name Service
[2] - IP ،Subnet ،Gateway ,DNS

فسفله اصلی سرویسDNS جهت حل مسائل آدرس دهی است. سیستم های کامپیوتری از اعداد برای آدرس دهی استفاده می کنند در حالی که انسان ها با اسامی راحت تر هستند؛ بنابراین سرویس DNS مانند یک دفترچه تلفن برای اینترنت است که در آن اسامی افراد با اسامی مقصدها و شماره تلفن ها با نشانی های IP متناظرند. سرویس دهنده DNS نام سایتی مانند www.yahoo.com را دریافت نموده و نشانی IP متناظر آن، مثلا 87.248.113.14 را برمی گرداند. DNS در حقیقت یک پایگاه داده توزیع شده است. به این معنی که اطلاعات آن در تعداد زیادی دستگاه در سراسر جهان پخش شده‌اند به همین جهت، این ساختار قابل توسعه است. نحوه اسم گذاری و مدیریت اسامی دارای ساختاری سلسله مراتبی و درختی است که در شکل ذیل نمایش داده شده است.



شکل ۳۲: ساختار درختی در نام گذاری اینترنتی

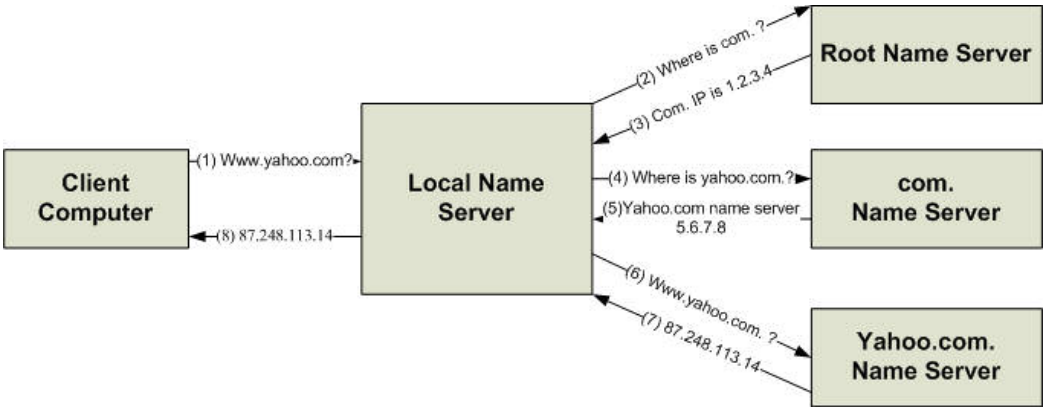
همان طور که در **شکل ۳۲** نشان داده شده است نام گذاری از یک ریشه شروع می شود که آن را با نقطه (.) نشان می دهند و به دو شکل نام گذاری عمومی و کشوری انشعاب می یابد:

در نام گذاری عمومی، با توجه به موضوع، پسوند خاصی تعریف می شود برخی پسوندهای معروف عبارتند از COM؛ مخفف Commercial برای نشانی های تجاری، org مخفف Organization برای سازمان ها، NET مخفف Network برای شبکه‌ها و سرویس دهنده‌ها، EDU برای دانشگاه ها و....

در نام گذاری کشوری به هر کشور دو کاراکتر اختصاص داده می شود و سطح اول نام گذاری با این دو کاراکتر مشخص می شود. مانند ir برای ایران، ca برای کانادا، uk برای انگلستان و .... سطح دوم نام گذاری مشابه حالت عمومی با توجه به موضوع پسوند داده می شود. مثلا برای تجاری com و برای دانشگاهی ac.

نام گذاری عمومی توسط سازمان های جهانی مدیریت می شوند و برای این که بتوان یک نام از این گروه در اختیار گرفت باید از طریق این سازمان ها یا کارگزاران آنها اقدام به ثبت دامنه[1] نمود. نام گذاری کشوری توسط خود همان کشور مدیریت می شود به عنوان مثال در ایران ir توسط مرکز تحقیقات فیزیک نظری مدیریت شده و برای ثبت دامنه می باید از طریق آن یا کارگزاران آن اقدام نمود برای اطلاع بیشتر به سایت www.nic.ir رجوع کنید.

نحوه مدیریت اطلاعات DNS مشابه نام گذاری، یک مدیریت سلسله مراتبی است به این معنی که در سطح اول Name Server های ریشه قرار دارند برای اسامی با ساختار عمومی که به صورت جهانی مدیریت می شوند درحال حاضر ۱۳ Name Server وجود دارند که با اسامی a.root-servers.net الی m.root-servers.net مشخص می شوند. این سرورها در نقاط مختلف جهان قرارگرفته اند و در هر لحظه یک کپی از اطلاعات سطح اول اسامی را در بر دارند. اطلاعات سطح اول مشخص می کند که نشانی های IP مربوط به هر یک از سرورهای اسامی سطح بالا[2] مانند com. ، org. ، net. و.... در کجا قرار دارند. این سرورهای اسامی سطح بالا، نیز هرکدام نشانی‌های IP مربوط به Name Server های Domain های تعریف شده را نگه می دارند مثلا TLD Server مربوط به com نشانی یا نشانی های IP تمام Domain هایی که با com ختم می شوند را در بردارد. در سطح آخر، Name Server های Domain ها قرار دارند مانند Name Server سایت yahoo.com این Name Server ها توسط خود سازمان یا شرکت مربوطه مدیریت می شوند و شرکت می تواند برای خود اسامی مختلف با نشانی IP متناظر ایجاد کند مثلا www.yahoo.com را تعریف نماید. با توجه به توضیحات فوق در شکل ۳۳ مراحل تبدیل یک اسم اینترنتی، به IP مشخص شده است.



شکل ۳۳: مراحل تبدیل یک اسم اینترنتی به IP

[1] - Domain Registration
[2] - Top Lever Domains

همان طور که در شکل فوق مشخص گردیده است تبدیل یک نام به IP که ا صطلاحا Resolve گفته می شود در ۸ مرحله انجام می‌پذیرد:

۱.دستگاه سرویس گیرنده تقاضای تبدیل نام (مثلا www.yahoo.com) به IP را به DNS Server محلی خود، که همان IP می باشد که در تنظیمات شبکه دستگاه Client به عنوان DNS Server تعریف شده است، ارسال می کند.

۲. Name Server محلی، از Root Server تقاضای ارسال نشانی IP مربوط به Name Server Com را می کند.

۳. Root Server در پاسخ نشانی TLD Name Server COM را بر می گرداند.

۴. Name Server محلی، از Name Server COM می‌خواهد تا نشانی Name Server Yahoo.com را ارسال کند.

۵. Name Server COM نشانیName Server Yahoo.com را بر می گرداند.

۶. Name Server محلی، از Name Server Yahoo.com نشانی IP مربوط به www.yahoo.com را سوال می کند.

۷. Name Server Yahoo.com نشانی IP متناظر باwww.yahoo.com را بر می گرداند.

۸. Name Server محلی، نشانی یافته شده را در اختیار Client قرار می‌دهد.

لایه های شبکه در مدل مرجع OSI

مدل OSI[1] که در حدود سال های 1983 توسط ISO[2] مطرح شد سعی دارد تا یک الگوی جامع ارائه نماید تا شبکه‌های کامپیوتری بتوانند از طریق آن با یکدیگر ارتباط برقرار کنند. (چنین شبکه های کامپیوتری را که تمایل به برقراری ارتباط با هم دارند اصطلاحا سیستم های باز[3] نامیده‌اند) در مدل OSI بر اساس اصول ذیل لایه بندی انجام گرفته است:

وقتی یک سطح جدید از انتزاع نیاز باشد یک لایه جدید تعریف می شود.

هرلایه باید یک عملکرد به خوبی تعریف شده داشته باشد.

عملیات های هر لایه با دیدگاه ایجاد یک استاندارد جهانی تعریف شوند.

مرز بین لایه ها باید به گونه ای انجام شود که حداقل تبادل اطلاعات بین آنها نیاز باشد.

---

[1] - Open Systems Interconnection
[2] - International Standard Organization
[3] - Open System

تعداد لایه ها باید به اندازه ای باشد که نیاز به قراردادن عملیات های قابل تفکیک در یک لایه وجود نداشته باشد و از طرفی تعداد لایه ها آنقدر زیاد نباشد که باعث شود معماری ارائه شده بیش از حد لایه بندی گردد (تعداد لایه ها باید لازم و کافی باشد).
از آنجا که دانستن اینکه هر یک از تجهیزات شبکه در چه لایه ای از شبکه و چگونه کار می نماید ضروری می باشد لذا در این بخش به مدل OSI که شبکه را به هفت لایه به ترتیب زیر تقسیم می کند اشاره می گردد.

7- Application
6- Presentation
5- Session
4- Transport
3- Network
2- Data link
1- Physical

وظایف هر کدام به طور مختصر به شرح زیر می باشد:
لایه ۷: این لایه وظیفه برقراری ارتباط کاربر یا برنامه کاربردی را با شبکه بر عهده دارد. این لایه مجموعه متنوعی از پروتکل ها را شامل می شود در واقع هر کاربردی برای خود یک پروتکل دارد.
نمونه های متداول کاربردها مانند Web (http)، FTP ، Telnet، Email و .... همگی در این لایه مطرح می شوند.
لایه ۶: عملیات اصلی این لایه امکان برقراری ارتباط میان دو سیستم با ساختار اطلاعات متفاوت است (مثلا یک طرف از ساختار عدد صحیح و طرف دیگر از ساختار Character Set استفاده کند). در این لایه مجموعه‌ای از ساختارهای داده‌ای انتزاعی[1] ایجاد می گردد که اطلاعات در سمت فرستنده از فرمت فرستنده به آن تبدیل شده و در سمت گیرنده از فرمت انتزاعی به فرمت گیرنده. به عبارت دیگر در این لایه نحوه کدینگ و نمایش اطلاعات مشخص می گردد و در همین لایه، رمزنگاری هم انجام می شود.
لایه ۵: این لایه آداب و رسوم یک ارتباط را بر عهده دارد و از آنجائی که شروع ارتباط ممکن است با نام کاربری وکلمه عبور باشد لذا امنیت نیز در این لایه مطرح می شود.
لایه ۴: این لایه که به لایه انتقال معروف است، نحوه انتقال اطلاعات[2] را مشخص می کند. در این لایه واحد انتقال اطلاعات، قطعه[1] می باشد. عمل اصلی در این لایه دریافت اطلاعات از لایه

[1] - abstract data structures
[2] - Connection Oriented Connection Less

Session و تبدیل آن به قطعه یا قطعات (شکستن بسته اطلاعاتی لایه Session در صورت لزوم) دیگر است.

لایه ۳: وظیفه این لایه مسیریابی و کنترل عملیات Subnet در شبکه می باشد. در این لایه واحد انتقال اطلاعات، بسته[۲] می باشد. محور اصلی عملکرد، مسیریابی بسته‌ها می باشد که این کار می تواند به صورت ثابت و از پیش تعریف شده[۳]، در ابتدای هر اتصال و یا به صورت کاملا پویا[۴] عمل کند.

مساله مدیریت ازدحام[۵] که به واسطه ایجاد تراکم بسته‌ها در گلوگاه‌ها حاصل می‌گردد؛ همچنین تضمین کیفیت سرویس QOS[۶] برعهده این لایه است.

باید توجه داشت که در شبکه هایی با تکنولوژی انتقال Broadcast، این لایه بسیار نازک بوده و یا اصلا وجود ندارد (زیرا همان گونه که قبلا گفته شد دراین شبکه‌ها بحث مسیریابی مطرح نیست و همه پیام را دریافت می‌کنند)

لایه ۲: در این لایه فریم تشکیل و مکانیزمی برای تشخیص خطا[۷] در فریم فراهم می شود. یعنی در این لایه داده ها در فریم منتقل می شوند. فریم ها به صورت فریم های داده یا فریم های تائیدیه[۸] می باشند.

برای مشخص کردن فریم ها از یک سری الگوهای بیتی خاص به نام جداکننده[۹] استفاده می شود.

مشکلات مربوط به انتقال فریم ها مانند گم شدن، تخریب و یا تکراری شدن آنها (که به واسطه از دست رفتن تائیدیه حاصل می شود) باید در این لایه حل شوند. در این لایه همچنین مکانیزم هایی جهت همگام کردن دو طرف لینک به صورت Flow Regulation وجود دارد.

در شبکه‌هایی که از تکنولوژی Broadcast استفاده می کنند یک زیر لایه به نام Media Access Sub layer اضافه می شود که مسولیت مدیریت محیط انتقال مشترک را برعهده دارد.

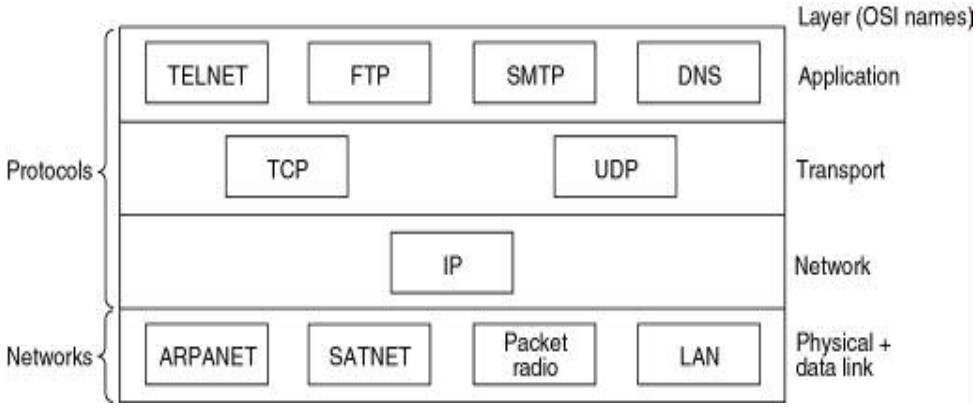
لایه ۱: واحد انتقال اطلاعات در این لایه بیت می باشد یعنی در این لایه فریم تبدیل به بیت و سپس به سیگنال تبدیل می شود. کلیه مسائل در این لایه حول موضوع نحوه انتقال بیت های خام روی محیط فیزیکی انتقال، واسط های مکانیکی و الکتریکی می باشد.

---

[1] - Segment
[2] - Packet
[3] - static routing
[4] -Dynamic routing
[5] - Congestion
[6] - Quality of Service
[7] - Error Detection
[8] - Acknowledge
[9] - Delimiter

مدل TCP/IP

مدل کاربردی امروزی است که شبکه اینترنت بر آن استوار است، این مدل TCP/IP از شبکه ARPANET برگرفته شده که نخستین بار در سال ۱۹۷۴ مطرح شد. مدل اساسا توسط وزارت دفاع آمریکا طراحی شد و هدف اصلی آن ایجاد شبکه ای بود که در شرایط سخت و حتی بروز جنگ هسته ای ازکار نیفتد؛ یعنی با قطع یک نقطه از شبکه، کل شبکه مختل نشود. این امر منجر به طراحی یک شبکه، مبتنی بر سوئیچ بسته ای[1] شد که با گسترش و توسعه آن در کل دنیا امروزه به شبکه اینترنت تبدیل شده است.



شکل ۳۴: لایه های شبکه بر اساس مدل TCP/IP

مدل TCP/IP که درشکل ۳۴ مشخص شده است دارای چهار لایه است:

لایه Host-to-Network: در این لایه ارتباط یک سیستم با شبکه به طوری که قابلیت تبادل بسته IP را داشته باشد تامین می گردد. در این لایه که تلفیق دو لایه فیزیکی و لینک داده در مدل OSI است استاندارد عمومی را TCP/IPتعریف نمی کند و شرایط از شبکه به شبکه دیگر و سیستم به سیستم دیگر متدوال است لذا TCP/IP به لحاظ تعریف ساختاری، در این لایه بسیار مبهم است.

لایه شبکه یا Network:

این لایه یک لایه بدون اتصال است[2] می باشد. پروتکل این لایه IP[3] نام دارد و ساختار بسته ها در قالب IP Packet مشخص می شوند. متقابلا با مدل OSI مساله مسیر یابی بسته‌ها، موضوع اصلی این لایه است.

---

[1] - Packet Switched Network
[2] - Connection Less
[3] - Internet Protocol

لایه انتقال یا Transport:

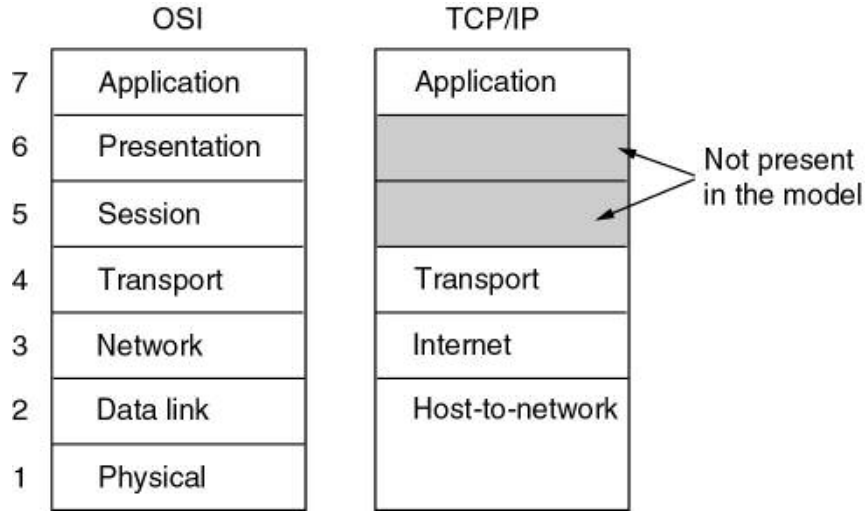
در این لایه ارتباط به صورت انتها به انتها[1] مطرح است و دو نوع پروتکل در این لایه وجود دارد:

TCP[2]: که یک ارتباط از نوع اتصال محور مطمئن[3] ایجاد می کند.

UDP[4]: یک ارتباط از نوع ارتباط بدون اتصال غیر مطمئن[5] ایجاد می کند.

لایه کاربرد یا Application:

شامل تمامی پروتکل های لایه بالا مانند: FTP (پروتکل انتقال فایل)، SMTP (پروتکل انتقال mail)، DNS (پروتکل تبدیل اسامی به IP)، NNTP (پروتکل سرویس News)، HTTP (پروتکل Web) و ....



شکل ۳۵: مقایسه دو مدل OSI و TCP/IP

مقایسه OSI و TCP/IP :

مدل TCP/IP دارای ۴ لایه است ولی OSI دارای ۷ لایه می باشد.

در OSI سه مفهوم Protocol، Interface، Service به طور صریح از هم تفکیک شده اما در TCP/IP آنقدر صریح نیست.

در OSI ابتدا لایه‌ها طراحی شده و سپس پروتکل ها بر اساس آن تعریف شده اند ولی در TCP/IP ابتدا پروتکل ها طراحی شده‌اند و سپس لایه‌ها با آنها تطابق یافته اند.

---

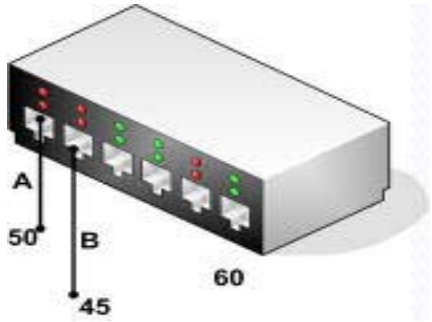
[1] - End-to-End
[2] - Transmission Control Protocol
[3] - Reliable Connection-Oriented
[4] - User Datagram Protocol
[5] - Unreliable Connection-less

در OSI لایه شبکه هم امکان هر دو سرویس بدون اتصال و با اتصال را فراهم می کند ولی در TCP/IP لایه شبکه فقط بدون اتصال است و این لایه انتقال است که این دو سرویس را فراهم می کند. در این مدل لایه بندی به خوبی انجام شده ولی پروتکل ها بر خلاف مدل TCP/IP آن طور که باید، توصیف و پیاده سازی نشده اند.

لازم است بدانید که روتر در لایه ۱، ۲ و ۳ کار می کند. سوئیچ هم وقتی یک فریم به آن می رسد آدرس فیزیکی مقصد را چک کرده و سپس آن را ارسال می کند. پس سوئیچ در لایه۲ , ۱ کار نموده، کارت شبکه و مودم هم در لایه ۱ و ۲ کار می کنند. و از آنجا که وقتی یک فریم به هاب و تکرار کننده می رسد، آن را به همه جا ارسال می کند لذا می توان فهمید که هاب در لایه یک کار می کند. تکرارکننده[1] وظیفه تقویت سیگنال را برعهده دارد. در تکنولوژی Bus اگر فاصله از ۱۸۵ متر بیشتر باشد از تکرارکننده استفاده می گردد.

نحوه عملکرد سوئیچ در شبکه

نحوه عمل سوئیچ در ابتدای کار، همانند هاب بوده یعنی در هنگام ارسال بسته تمام پورت های آن باز می باشد. اما در همان لحظه آدرس فیزیکی هر پورت را دانسته و جدول آدرس های فیزیکی خود را جهت ارسال داده های در دفعات بعدی کامل می کند. به مثال زیر دقت نمائید:



Mac Address Table	
50	1
60	8

شکل ۳۶: یک سوئیچ با جدول آدرس های فیزیکی

ظرفیت جدول آدرس های فیزیکی سوئیچ در کاتالوگ آن نوشته شده است.

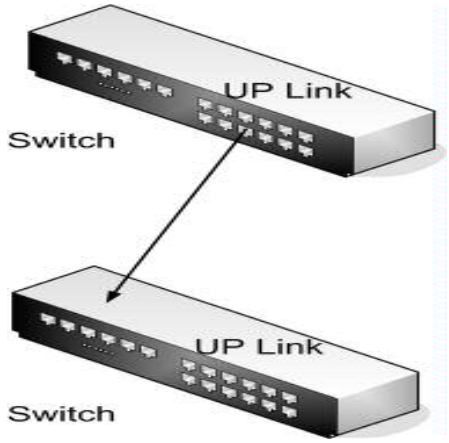
در نظر بگیرید که یک هکر روی یک پورت نشسته و جدول آدرس های فیزیکی را در سوئیچ به هم بریزد لذا بحث امنیت در سوئیچ هم مطرح می باشد.

[1] - Repeater

سوئیچ های عادی را سوئیچ لایه۲ گویند و این سوئیچ ها روی آدرس فیزیکی تصمیم می گیرند اما سوئیچ های دیگری معروف به سوئیچ لایه ۳ وجود دارد که روی IPAddress تصمیم می گیرند.
هنگام انتخاب سوئیچ و کارت شبکه موارد زیر را باید در نظر گرفت:

۱- سرعت و تعداد پورت ها
۲ - قابلیت توسعه و ارتباط با ماشین های دیگر[1]
۳- مدیریت[2]
۴ – روش های دسترسی به سوئیچ

در صورتی که در نظر است سوئیچ های یک رک به هم متصل گردد از قابلیت توسعه آنها استفاده می شود. لازم به ذکر است که پورتی به نام UPLINK به همین منظور در سوئیچ ها تعبیه شده است. ممکن است این اتصال توسط پورتی بجز UPLINK هم به صورت سالم و بدون خطا برقرار شود که به این حالت سوئیچ ها AutoSence هستند.



شکل ۳۷: نحوه اتصال سوئیچ توسط پورتی به نام UPLINK

به عنوان مثال توسط سوئیچ های 3 com مدل ۴۴۰۰ حداکثر ۸ قابل توسعه دارند به شرطی که مجموع پورت ها از ۱۹۲ عدد بیشتر نشود.
ویژگی بعدی سوئیچ ها، قابل مدیریت و برنامه ریزی بودن و نیز همچنین هوشمند یا غیر هوشمند بودن آنهاست.
یک دیگر از ویژگی های سوئیچ، چگونگی دستیابی ماشین ها به محیط انتقال[3] است. برای این کار روش های متعددی وجود دارد. نخستین روش Carrier Sense می باشد یعنی اگر خط آزاد بود

[1] - Stackable
[2] - Management
[3] -Access method

داده ارسال می گردد. روش دیگر CDMA بوده که این روش به دلیل اینکه قابل پیش بینی نبوده، فاقد نظم است و مدیریتی روی آن نیست، اولویتی ندارد.

پیکربندی سوئیچ

با استفاده از پورت کنسول RS232 و همچنین سرویس های RMON , SNMP , HTTP , Telnet می توان سوئیچ ها را پیکربندی نمود. موارد مهمی که در پیکربندی یک سوئیچ باید مورد توجه قرار گیرند به شرح زیر می باشد:

هوشمند بودن[1] سوئیچ: یعنی این که اگر یک کامپیوتر به کمک کارت شبکه به یک سوئیچ متصل گردد و به هر دلیلی کارت شبکه معیوب شود به طوری که باعث ایجاد تصادم[2] شود هاب و سوئیچ هوشمند این تصادم را منتقل نمی کند.

ارسال و دریافت همزمان[3] در سوئیچ

نکته دیگر در مورد سوئیچ ها، قابلیت ارسال و دریافت همزمان داده در آنها طبق بلوک دیاگرام زیر است:

NIC ←→ NIC
FDX
SW ←→ SW

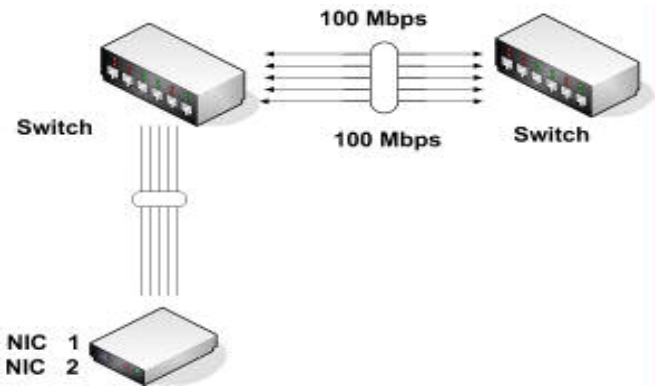
لازم به ذکر است که هاب از چنین خصوصیتی برخوردار نیست زیرا چون در تکنولوژی هاب وقتی یک ماشین داده ارسال می کند، تمام پورت های آن باز است و نمی تواند هم زمان داده ای دیگر را دریافت نماید. ضمن این که این خاصیت زمانی خوب کار می کند که تمامی تجهیزات مدنظر محصول یک کارخانه باشد.

Port Trunking

این قابلیت فقط مختص سوئیچ می باشد. این ویژگی اجازه می دهد بین دو سوئیچ مطابق شکل زیر دو لینک یا بیشتر داشته داشته تا تشکیل کانال دهیم.

---

1 -Smart
2 -Collision
3 -Full Doublex



شکل ۳۸: استفاده از قابلیت Port Trunking برای اتصال دو سوئیچ

اندازه فیزیکی سوئیچ

سوئیچ ها را از نظر اندازه فیزیکی یه دو دسته رومیزی[1] و قابل نصب در رک[2] وجود دارد.

اولویت بندی ترافیک شبکه[3]

این سرویس اجازه می دهد تا ترافیکی را که به سوئیچ می رسد بررسی نموده و آن را اولویت بندی نماید. برای این کار در سوئیچ ها چند صف تشکیل می دهد (به عنوان مثال درسوئیچ های 3Com چهار صف) و ترافیک اولویت بندی شده در صف ها ارسال می گردد. معمولا ترافیک های صدا و تصویر در اولویت بالاتر قرار دارند.

رمزنگاری[4]

بعضی سوئیچ ها قابلیت رمزنگاری دارند. کارت شبکه نیز می تواند از چنین قابلیتی برخوردار باشد.
اکنون چند سوال مهم مطرح و به آنها پاسخ داده می شود.

در شبکه زیر اگر لینک ارتباطی ۱۰۰۰ مگا بیت در ثانیه، به ۱۰۰ تبدیل شود چه تاثیری در کل شبکه دارد؟

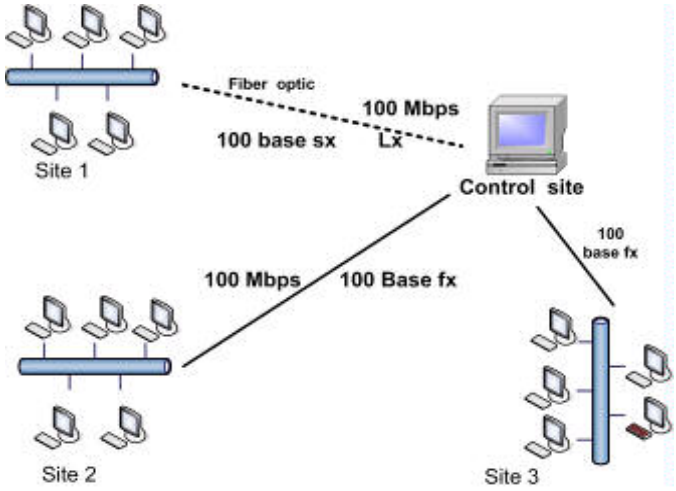
پاسخ: چون ترافیک Broadcast روی سایت ۱ زیاد است وقتی سرعت بالامی رود Broadcast نیز با سرعت بیشتری به Control Site می رسد لذا باید به فکر کاهش Broadcast بود.

---

[1] -Desktop
[2] -Rack Mount
[3] -Quality of Service
[4] -Encryption

سوال: آیا خرابی یا کثیف بودن یک کانکتور تاثیری در سرعت شبکه دارد؟

پاسخ: خرابی کانکتور باعث می شود که برای فرستادن بسته، دوباره سعی شود[1]. و این کار باعث کندی شبکه می شود.



شکل ۳۹: مثالی از یک شبکه جهت بررسی مشکلات احتمالی

سوال: آیا یک فن کویل در شبکه تاثیر دارد؟

پاسخ: هر چیزی که سیم پیچ داشته باشد در شبکه موثر است. به همین خاطر توصیه شده که فاصله بین سیم های برق و کابل شبکه حداقل ۲۰ الی ۳۰ سانتی متر باشد.

برای داشتن یک شبکه خوب توجه به نکات زیر ضروری است:

طراحی توپولوژی در آن به درستی انجام شود یعنی تجهیزات اکتیو و پسیو به درستی انتخاب شوند.

قطعات و تجهیزات، اعم از اکتیو و پسیو به دقت نصب شود و نگهداری و نظافت آنها نیز طبق دستورالعملی در فواصل زمانی مشخص ادامه داشته باشد.

یک سوکت RG45 اگر به طور کامل پرس نگردد نویز و پارازیت، مخصوصا در فرکانس های ۱۰۰ و۱۰۰۰ ایجاد می گردد.

- پیکربندی تجهیزات اکتیو و مونیتورینگ آنها به دقت و مستمر انجام شود.
- نوع پروتکل، سیستم عامل ایستگاه ها، سرورها، نوع نرم افزار و سرویس ها به دقت انتخاب و نصب شود و پیکربندی آنها بر اساس نیاز صورت پذیرفته و به طور مستمر مانیتور شوند.

[1] - Retry