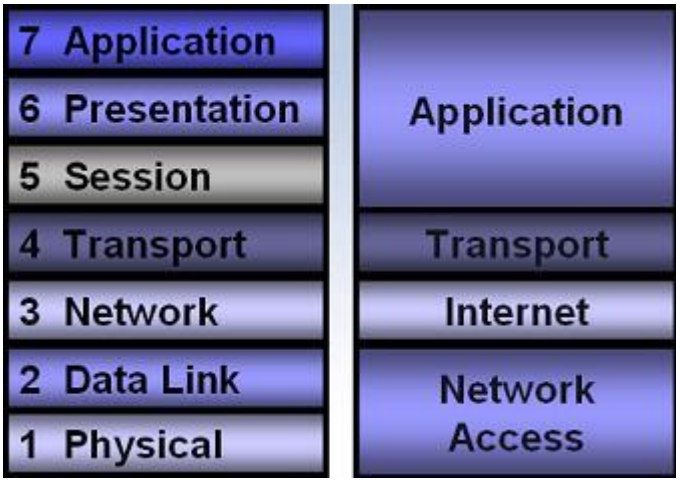
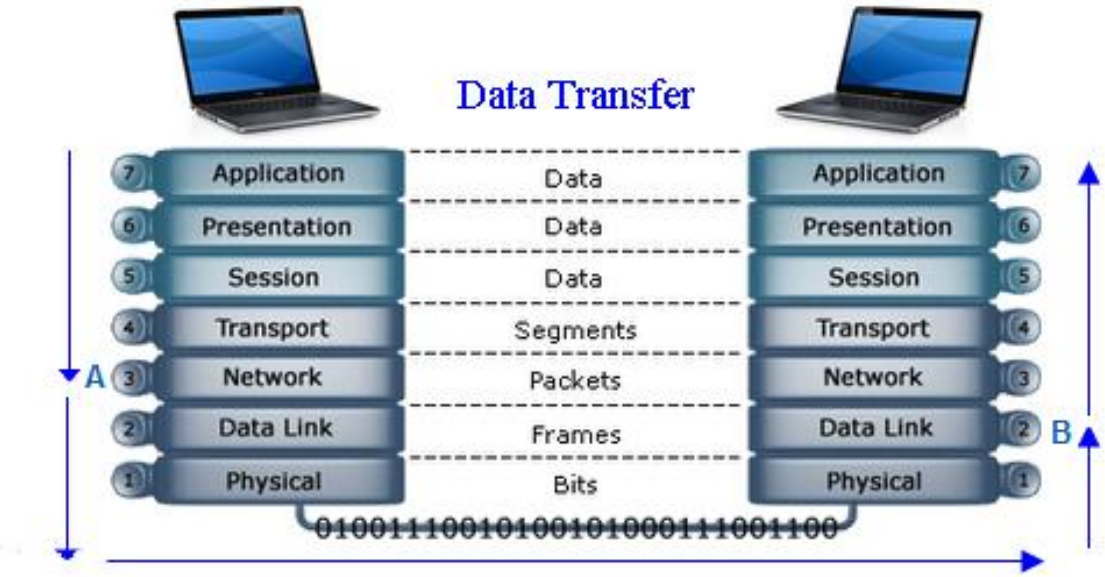
مدل های مرجع شبکه(لایه های OSI وTCP/IP)





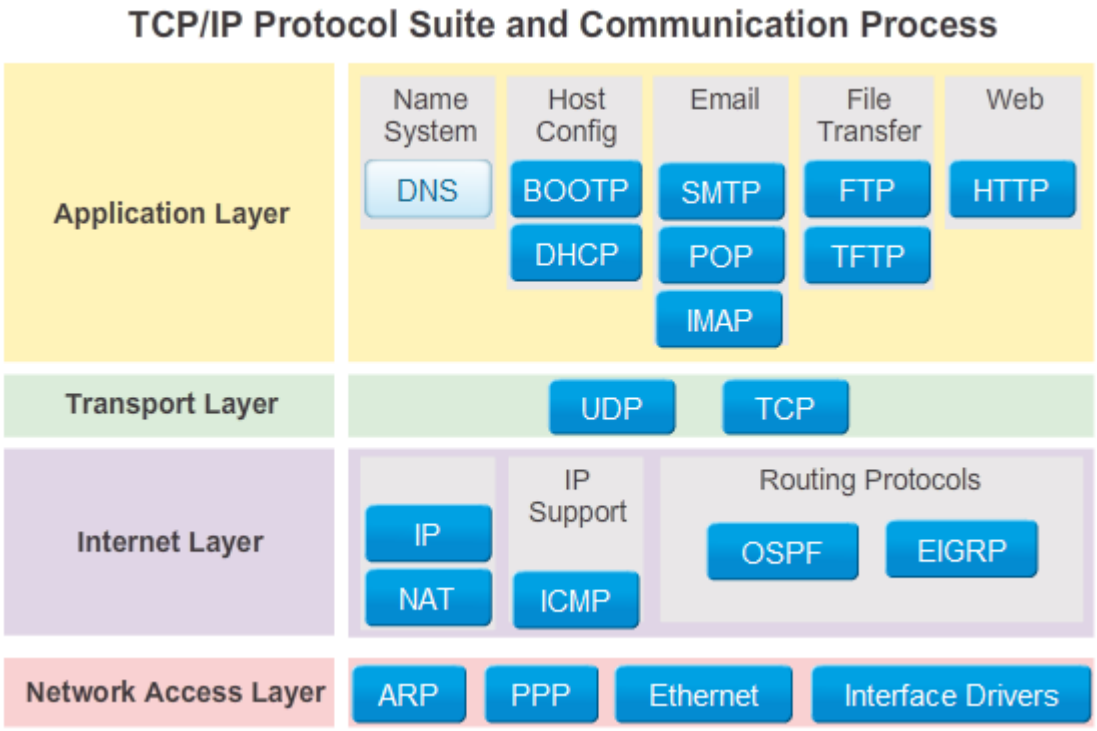
A: بعد از لایه ۴ در لایه ۳ عمل مسیریابی صورت میگیرد و آدرس آی میدا و مقصد در دیتا درج میشود

B: در کامپیوتر مقصد بعد از لایه ۲ بسته های اطلاعاتی از لایه ۳ یعنی آدرس آی پی مقصد از پکت جدا میشوند تا دیتا و اطلاعاتا اصلی به لایه ۷ کامپیوتر مقصد برسند

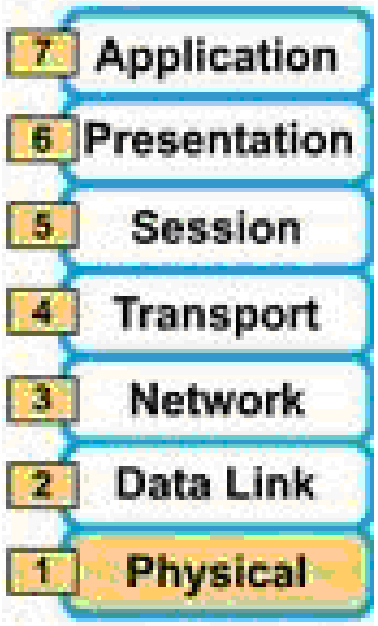
پروتکل های لایه OSI

OSI layers	Function	Data type	Protocols	Network components
Application layer	User Application Services ,Allows access to network services that support Applications. Handles network access, Flow control and error recovery.	User Data	DNS; NFS; BOOTP; DHCP; SNMP; RMON; FTP; TFTP; SMTP; POP3; IMAP; NNTP; HTTP; Telnet	Gateway
Presentation layer	Data Translation; Compression and Encryption. All different formats from all sources are made into a common uniform format that the rest of the OSI model can understand.	Encoded User Data	SSL; Shells and Redirectors MIME	Gateway , Redirector
Session layer	Session Establishment, Management And Termination. Manages who can transmit data at a certain time and for how long.	Sessions	NetBIOS, Sockets, Named Pipes, RPC	Gateway
Transport layer	Additional connection below the session layer Manages the flow control of data between parties across the network, Provides flow control and error-handling.	Datagram's /Segments	TCP and UDP; SPX; NetBEUI/NBF	Gateway , Advanced Cable tester Brouter
Network layer	Translates logical network address and names to their physical address (e.g. computer name to MAC address) Logical Addressing; Routing; Datagram Encapsulation; Fragmentation and Reassembly; Error Handling and Diagnostics	Datagram's / Packets	IP; IPv6; IP NAT; IPSec; Mobile IP; ICMP; IPX; DLC PLP; Routing protocols such as RIP and BGP	Brouter , Router, Frame Relay Device, ATM Switch, Advanced Cable Tester.
Data link layer	Handles data frames between the Network and Physical layers, The receiving end packages raw data from the Physical layer into data frames for delivery to the Network layer, Logical Link Control; Media Access Control; Data Framing; Addressing Error Detection and Handling; Defining Requirements of Physical Layer	Frames	IEEE 802.2 LLC, Ethernet Family; Token Ring; FDDI and CDDI; IEEE 802.11 (WLAN, Wi-Fi); HomePNA ;HomeRF; ATM; SLIP and PPP	Bridge , Switch, ISDN Router, Intelligent,Hub NIC,Advanced Cable Tester
Physical layer	Transmits raw bit stream over physical Cable, Defines cables, cards, and physical Aspects, Defines NIC attachments to hardware, how cable is attached to NIC. Encoding and Signalling; Physical Data Transmission; Hardware Specifications; Topology and Design.	Bits	EEE 802 IEEE 802.2 ISO 2110 ISDN	Repeater ; Multiplexer; Hubs TDR Oscilloscope Amplify

پروتکل های رایج در مدل TCP/IP



مدل OSI



مدل OSI یا Open System Interconnection یک مدل مرجع برای ارتباط بین دو کامپیوتر می باشد که در سال ۱۹۸۰ طراحی گردیده است. هر چند امروزه تغییراتی درآن به وجود آمده اما هنوز هم کاربردهای فراوانی در اینترنت و به خصوص در معماری پایه شبکه دارد. این مدل بر اساس لایه بندی قراردادهای برقراری ارتباط که همزمان روی دو سیستم مرتبط اجرا شده اند پایه ریزی شده است که این امر بسیار سرعت و دقت ارتباط را افزایش می دهد و این قراردادها بصورت طبقه طبقه در هفت لایه تنظیم شده اند که در زیر بررسی خواهند شد .

بررسی هفت لایه مدلOSI

لایه فیزیکی

این لایه که تنها تشکیل شده از سخت افزار می باشد و قراردادهای سخت افزاری در آن اجرا می شود وظیفه انتقال نهایی اطلاعات را دارد که این انتقال یصورت سیگنال و به صورت صفرو یک می باشد.

لایه پیوند داده ها

در این لایه اطلاعات، کشف خطا و اصلاح می شوند و بدون خطا و به صورت مطمئن به سوی مقصد ارسال می شوند.وظیفه دیگر این لایه مطمئن شدن از رسیدن اطلاعات به مقصد است که این کار توسط بیتهای , Parity check) checksum ,crc) انجام می پذیرد.که در صورت بروز خطا مجددا اطلاعات ارسال خواهند شد.

لایه شبکه

و اما پیچیده ترین لایه یعنی لایه شبکه که در آن قراردادهای شبکه بندی تعریف شده است. وظیفه این لایه انتقال تکنولوژی برقراری ارتباط برای دیگر شبکه های مستقل است که این امر این امکان را به osi می دهد که بتواند در زیر شبکه های مختلف فعالیت کند.

لایه انتقال

در این لایه قبل از ارسال اطلاعات یک بسته به سمت مقصد فرستاده می شود تا مقصد را برای دریافت اطلاعات آماده کند. همچنین این لایه وظیفه تکه تکه کردن بسته ها، شماره گذاری آنها و ترتیب و نظم دهی آنها را بر عهده دارد. که البته بسته ها در طرف گیرنده دوباره در همین لایه نظم دهی و قابل استفاده برای لایه های بالاتر خواهند شد.

لایه جلسه

در این لایه بر کارهایی از قبیل زمان ارسال و دریافت بسته ها مقدار رسیده و مقدار مانده از بسته ها نظارت می شود که به مدیریت بسته ها بسیار کمک می کند.

لایه ارائه

در این لایه استانداردهای رمز نگاری و فشرده سازی اطلاعات تعریف شده است که این لایه در امنیت بسیار مهم می باشد.

لایه کاربرد

استانداردهای ارتباط بین نرم افزارهای شبکه در این لایه قرار دارد که می توان از FTAM, CMIP, MHS VT :نام برد.

مدل TCP/IP یاInternet protocol /Transmission Control Protocol

مفهومTCP/IP

TCP/IPمجموعه قراردادهایی هستند که در جهت اتصال کامپیوتر ها در شبکه مورد استفاده قرار می گیرند. وبه تعریف دیگر قرارداد کنترل انتقال اطلاعات می باشد. مدل چهار لایه TCP/IP از لایه های زیر تشکیل شده است .

لایه کاربرد

لایه انتقال

لایه شبکه

لایه واسطه شبکه

لایه فیزیکی

لایه واسط شبکه

در این لایه تمام استانداردهای سخت افزاری و انواع پروتکل شبکه تعریف شده که خاصیت بزرگ این لایه این موضوع می باشد که در آن می توان بین نرم افزار و سخت افزار شبکه ارتباط برقرار کرد.

لایه شبکه

در این لایه پروتکل IP آدرس دهی و تنظیم می شود).توضیحات در قسمت (IP و همچنین دیگر پروتکل ها مانند ARP,ICMP,BOOTPکه در این میان نقش هیچکدام به اندازه IP , ICMP مهم نیست در کل وظیفه این لایه دادن اطلاعات در مورد شبکه و آدرس دهی در آن می باشد که مسیر یابها از آن بسیار استفاده می کنند.

لایه انتقال

ابتدایی ترین وظیف این لایه آگاهی از وضعیت بسته ها می باشد که بسیار مهم نیز هست. و در مرحله بعد وظیفه این لایه انتقال اطلاعاتی می باشد که نیاز به امنیت ندارند و سرعت برای آنها مهم تر است.

لایه کاربرد

این لایه دارای امکانات زیادی برای هنر نمایی متخصصان می باشد. در این لایه برنامه های کاربردی قرار دارند و در کل این لایه لایه ی نرم افزارهای شبکه می باشد و همچنین لایه پروتکل های نرم افزاری نیز می باشد. از مهم ترین نکات در خصوص این لایه قرارداشتن: انتقال فایل (FTP) و مدیریت پست (SMTP) و بقیه برنامه های کاربردی می باشد.

پروتکل اینترنت یاIP

حتما همه شما عزیزان واقف به این موضوع هستید که IP یکی از مهمترین قسمتهای TCP/IP و شاید بتوان گفت مهمترین قسمت آن زیرا تقریبا شما برای هر کاری نیاز به آن خواهید داشت لذا بسیار ضروری و حیاتی می باشد که شما اطلاعات خود را در زمینه این مهم افزون کنید IP .یک آدرس عددی است که برای ارتباط با شبکه به هر ماشینی در شبکه اختصاص داده می شود) چون IP برای وسایلی از قبیل ROUTER و MODEM و LAN و ... استفاده می شود

وظیفهIP

وظیفه پروتکل IP حمل و تردد بسته های حاوی اطلاعات و همچنین مسیر یابی آنها از مبدا تا مقصد است IP .پس از دریافت اطلاعات از TCP شروع به قطعه قطعه کردن آن به قطعه های کوچک به اسم FRAGMENT می نماید، پس از این مرحله برای هر FRAGMENT یک بسته IP می سازد که حاوی اطلاعات مورد نیاز بسته برای حرکت در طول شبکه می باشد و بسته IP را به بسته TCP اضافه می کند و شروع به ارسال بسته های تیکه تیکه شده (FRAGMENT)می نماید حال مسیر یابها بر اساس تنظیمات قسمت IP بسته ها را به مقصد خود هدایت می کنند و آن را داخل زیر شبکه ها هدایت می کنند.

خصوصیاتIP

بسته IP حد اکثر ۶۴ کیلوبایت فضا را اشغال خواهد کرد و بیشتر از آن نمی تواند باشد ولی موضوع جالب اینجاست که در حالت عادی حجم بسته حدود ۱۶۰۰ بایت بیشتر نمی شود IP .در تمامی سیستم های عامل با ساختار استانداردی که دارد به درستی کار می کنند و نیاز به هیچ نوع سخت افزار ندارد. بسته IP ساخته شده از تعدادی فیلد مجزا می باشد که هر کدام اطلاعاتی را در خود دارند که در زمان مورد نیاز این اطلاعات از داخل بسته ها استخراج می شود و مورد استفاده قرار می گیرد این اطلاعات شامل مواردی مثل:آدرس IP فرستنده. آدرس IP گیرنده و ..... می باشد.

آدرس های ویژهIP

این آدرسها نمونه هائی از آدرس های IP خاص هستند که از قبل برای مقاصد خاصی در نظر گرفته شده اند و در تعریف شبکه نمی توان از آنها به عنوان IP برای ماشینها استفاده کرد. از این آدرس در مواردی استفاده می شود که ماشین میزبان از IP خود بی اطلاع است.البته اگر از این آدرس به عنوان آدرس فرستنده استفاده شود هیچ جوابی برای فرستنده پس فرستاده نمی شود.

HostId.0

ین آدرس برای زمانی است که از آدرس خود در زیرشبکه بی اطلاع باشیم

255.255.255.255

از این آدرس برای ارسال پیامهای به صورت عمومی و فراگیر در شبکه استفاده می شود البته با استفاده از این آدرس می توان در زیر شبکه خود پیام فراگیر ارسال کرد.

NetId.255

از این آدرس برای ارسال پیامهای فراگیر در دیگر شبکه ها از خارج از آنها استفاده می شود.البته این سرویس تقریبا در بیشتر اوقات از سوی مدیران شبکه غیر فعال می شود.

مقایسه مدلهای OSI وTCP/IP

مدل OSI یاOpen System Interconnection یک مدل مرجع جهت رابطه بین دو کامپیوتر می باشد که در سال ۱۹۸۰ طراحی گردیده است. هر چند امروزه تغییراتی درآن به وجود آمده ولی هنوز هم کاربردهای فراوانی در اینترنت به خصوص در معماری پایه شبکه دارد .

۲. مثال : در لایه Network فقط پروتکل IP نیست , میتونه IPXو بقیه پروتکل ها هم باشه و در لایه Transport پرتکل TCP/UDP هست ولی میتونه SPXو غیره هم که مربوطه به ناول نتور , اپل تالک که پروتکل های DTE-DDPخودش رو داره.

۳. TCP/IPاومد نگاه کرد دید IPشده پروتکل استاندارد بزرگترین شبکه دنیا یعنی اینترنت (IP یعنی اینترنت پروتکل).

۴. TCP/IP یک مدل برای خود ساخت که این مدل دیگه پروتکل SPX,IPXو غیره رو نداره.

۵. تنها پروتکل لایه شبکه IP و تنها پروتکل لایه Transport فقط TCP/UDP هست یعنی محدودترش کرد.

۶. از طرف دیگه ۳ تا لایه(Application,Presentation,Session) لایه اپلیکیشنی هستن و Messageما عملا هیچ اتفاقی روش نمی افته و تغییر نمیکنه اولین جایی که تغییر میکنه Transportهستش اومد گفت من این ۳ تا لایه رو بعنوان لایه Applicationمیشناسم.

۷. لایه دیتالینک و فیزیکی چون جدا کردنشون خیلی کار سختیه تبدیل شدن به لایهLinkLayer.

۸. مدل OSI در لایه شبکه از هر دو نوع ارتباط اتصالگرا و غیر متصل پشتیبانی می کنند، ولی در لایه انتقال فقط سرویس اتصالگرا دارد، مدل TCP/IP در لایه شبکه فقط سرویس غیر متصل دارد ولی در لایه انتقال از هردو نوع ارتباط پشتیبانی می کند.

قبل از ایجاد مدل OSI پروتکلهای آن طراحی و ابداع شد. در نتیجه این مدل وابستگی و تعامل خاصی با هیچ مجموعه پروتکلی ندارد. اما در TCP/IPمسئله برعکس بود و این خود باعث شده که مدل TCP/IP تنها برای شبکه‌های تحت خود مناسب باشد.

۱۰. مدل OSI و) TCP/IP و پروتکل هایشان) هیچکدام کامل نیستند، و جا دارد برخی از نقاط ضعف آنها را برشماریم.در این قسمت، برخی از نقاط ضعف مدل های OSI و TCP/IPرا برسی خواهیم کرد.با مدل OSI شروع می کنیم.

در سال ۱۹۸۹، بسیاری متخصصان برجسته شبکه بر این باور بودند که آینده در بست متعلق به مدل OSI و پروتکل های آن است، و هیچ چیز نمی تواند در مقابل پیشرفت آن مقاومت کند.اما این اتفاق نیفتاد.چرا؟ نگاهی به گذشته درسهای بسیاری را برای چشمان عبرت بین دارد،که می توان آنها را چنین خلاصه کرد:

1.زمان نا مناسب

2.تکنولوژی نامناسب

3.پیاده سازی نامناسب

4.سیاست های نامناسب

زمان نامناسب

اولین عامل شکست مدل OSI زمان نامناسب بود.زمانی که یک استاندارد وضع می شود، اهمیت حیاتی در موفقیت و عدم موفقیت آن دارد.دیوید کلارک از دانشگاهM.I.T فرضیه ای در زمینه استانداردها دارد که ملاقات فیل ها معروف است

این شکل میزان فعالیت های حول یک موضوع جدید را نشان می دهد.وقتی موضوعی برای اولین بار کشف می شود، گرداگرد آن سیلی از فعالیت های تحقیقی (به شکل بحث، مقاله و سخنرانی) فرا می گیرد.بعد از مدتی این فروکش می کند و بعد از اینکه صنعت به این موضوع علاقه مند شد، موج سرمایه گذاری ها از پی می آید.

بسیار مهم است که در محل تلاقی این دو فیل (موج تحقیق و موج سرمایه گذری) استانداردها به طور کامل وضع شوند.اگر استاندارد زودتر از موعد(قبل از پایان تحقیقات) نوشته شود، خطر آن هست که موضوع به درستی درک نشده باشد و استاندارد ضعیف از آب در آید.اگر استاندارد دیرتر از موعد(بعد از شروع موج سرمایه گذاری) نوشته شود، شرکتهای بسیاری قبلا –از مسیرهای مختلف- در آن سرمایه گذاری کرده اند،و این خطر هست که استانداردهای آنها را نادیده بگیرد. اگر فاصله این دو فیل خیلی کم باشد (همه عجله داشته باشند که کار را زودتر شروع کنند)، خطر آن هست که استاندارد نویسان بین آنها له شوند.

اکنون معلوم شده است که پروتکل های استاندارد OSI بین فیل ها له شده اند.وقتی که پروتکل های OSI پا به عرصه وجود گذاشتند، پروتکل های رقیب (TCP/IP) مدت ها بود که در مراکز تحقیقاتی و دانشگاه ها پذیرفته شده بودند.با اینکه هنوز موج سرمایه گذاری صنعتی در TCP/IP شروع نشده بود.اما بازار آکادمیک آنقدر بزرگ بود که شرکتهای بسیاری را تشویق به تولید محصولات TCP/IP کند.و وقتی OSI بالاخره از راه رسید،کسی نبود که داوطلبانه از آن پشتیبانی کند.همه منتظر بودند دیگری قدم اول را بر دارد.، قدمی که هرگز برداشته نشد دOSI در نطفه خفه شد.

تـکنولوژی نامناسب

دلیل دیگری که OSI هرگز پا نگرفت آن بود که، این مدل و پروتکل های آن هر دو ناقص و معیوب بودند.انتخاب هفت لایه برای این مدل بیشتر یک انتخاب سیاسی بود تا فنی، و در حالی که دو لایه آن (نشست و نمایش) تقریبا خالی بودند،در لایه های دیگر (لینک داده و شبکه) جای نفس کشیدن نبود.

مدل) OSI و سرویس ها و پروتکل های آن) به طور باور نکردی پیچیده است.اگر کاغذهای چاپی این استاندارد را روی هم بچینید.ارتفاع آن از نیم متر هم بیشتر خواهد شد.پیاده سازی پروتکل های OSI بسیار دشوار، و عملکرد آنها ناقص است.در این رابطه، نقل جمله جالبی از پاول موکاپتریس1993) ، (Roseخالی از لطف نیست\:

سوال:از ترکیب یک گانگستر با یک استاندارد بین المللی چه چیزی بدست می آید؟

جواب:کسی پیشنهادی به شما می کند که از آن سر در نمی آورید.

مشکل دیگر مدل OSI ،علاوه بر غیر قابل فهم بودن آن، این است که برخی از عملکرد های آن (مانند آدرس دهی، کنترل جریان داده ها و کنترل خطا)در تمام لایه ها تکرار می شود.برای مثال، سالتزر و همکارانش (۱۹۸۴) نشان دادند که کنترل خطا باید در بالاترین لایه انجام شود تا بیشترین تاثیر را داشته باشد،بنابراین تکرار آن در لایه های پائین تر نه تنها غیر ضروری است، بلکه باعث افت کارایی هم خواهد شد.

پیاده سازی نامناسب

با توجه به پیچیدگی بیش از حد مدل OSI و پروتکل های آن ، جای تعجب نبود که اولین پیاده سازی های آن حجیم، سنگین و کند است.آنهایی که با این مدل کار کرده بودند، بزودی پشیمان شدند، و طولی نکشید که کلمه OSI مترادف شد با "کیفیت بد". بعد ها محصولات بهتری به بازار آمد،اما آوازه منفی OSI فراموش نشد.

از طرف دیگر، اولین پیاده سازی) TCP/IP که بخشی از سیستم عامل یونیکس برکلی بود) بسیار خوب از کار در آمد(و لازم به گفتن نیست که مجانی هم بود).افراد بسیار با سرعت شروع به استفاده از آن کردند،هواخاه آن شدند، آنرا توسعه دادند، و این باعث شد که باز هم به خیل طرفداران آن اضافه شود.در اینجا، بر خلاف OSI ، مارپیچ رو به بالا می رفت، نه پایین.

سیاست های نامناسب

دلیل استفاده پیاده سازی TCP/IP ، بسیاری از افراد (بویژه در محیط های دانشگاهی) تصور می کردند که TCP/IP جزئی از یونیکس است، و یونیکس هم در آن دوران محبوبیتی فوق العاده داشت.

از سوی دیگر، این عقیده رواج داشت که OSI یک مخلوق دولتی (مخصوصا دولتهای اروپایی و آمریکایی) است.البته این عقیده تا حدی درست بود، اما همین تصور هم که عده ای دیوان سالار دولتی بخواهد یک استاندارد دولتی را به زور به جا بیندازد، باعث شد تا برنامه نویسان و طراحان شبکه تمایلی از خود برای همکاری نشان ندهند.زبانهای برنامه نویسی) PL/1 که در دههٔ ۱۹۶۰ از سوی IBM بعنوان زبان آینده توسعه داده شد (و) ADa که وزارت دفاع آمریکا حامی آن بود) به همین دلیل دچار سرنوشتی مشابه شدند.

۱۱. مشکل دیگر مدل OSI ،علاوه بر غیر قابل فهم بودن آن، این است که برخی از عملکرد های آن (مانند آدرس دهی، کنترل جریان داده ها و کنترل خطا)در تمام لایه ها تکرار می شود.برای مثال، سالتزر و همکارانش (۱۹۸۴) نشان دادند که کنترل خطا باید در بالاترین لایه انجام شود تا بیشترین تاثیر را داشته باشد،بنابراین تکرار آن در لایه های پائین تر نه تنها غیر ضروری است، بلکه باعث افت کارایی هم خواهد شد.

۱۲. دلیل استفاده پیاده سازی TCP/IP ، بسیاری از افراد (بویژه در محیط های دانشگاهی) تصور می کردند که TCP/IP جزئی از یونیکس است، و یونیکس هم در آن دوران محبوبیتی فوق العاده داشت. از سوی دیگر، این عقیده رواج داشت که OSI یک مخلوق دولتی (مخصوصا دولتهای اروپایی و آمریکایی) است.البته این عقیده تا حدی درست بود، اما همین تصور هم که عده ای دیوان سالار دولتی بخواهد یک استاندارد دولتی را به زور به جا بیندازد، باعث شد تا برنامه نویسان و طراحان شبکه تمایلی از خود برای همکاری نشان ندهند.زبانهای برنامه نویسی) PL/1 که در دههٔ ۱۹۶۰ از سوی IBM بعنوان زبان آینده توسعه داده شد (و) ADa که وزارت دفاع آمریکا حامی آن بود) به همین دلیل دچار سرنوشتی مشابه شدند.

کاربرد NAP یا Network Access Protection چیست ؟

NAPبه منظور محافظت از دسترسی به شبکه یکی از ویژگی های ویندوز سرور ۲۰۰۸ است که به منظور کنترل دسترسی ها به منابع شبکه براساس هویت Client ها و سیاست های درج شده در شبکه ها می باشد.این مجوزها میتواند شامل مواردی از قبیل :

۱. داشتن آنتی ویروس
۲. به روز بودن آنتی ویروس
۳. آپدیت بودن ویندوز
۴. براساس سرویس پک ویندوز
۵. غیرفعال بودن فایروال
۶. و شرایط دیگر...

NAPدر واقع یک گزارش ازوضعیت سلامت کلاینت ها طبق مجوزهای گفته شده میگیرد و در صورتی که این مجوزها برای کلاینتی

تأیید شد اجازه دسترسی و ورود به شبکه داخلی را میدهد. در صورتی که کلاینتی این شرایط را تا حدودی نداشت و موفق به کسب تأیید نشود به شبکه ای دیگر به نام Remediation Network وارد میشود که این شبکه شامل یکسری سرویس برای عملیات آپدیت و اعمال گروپ پالیسی های خاص و فعال کردن فایروال است.در صورتی که کلاینتی این شرایط را تا اصلا نداشت و موفق به کسب تأیید نشود به شبکه ای دیگر به نام Guest Network وارد میشود که این شبکه شامل سرویس خاصی نیست و معمولا یک Web Proxy دارد.در واقع کلاینتی که به این شبکه وارد شود از سرویس های شبکه داخلی ما بهره ای نمیبرد NAP .برای اعمال تأیید و یا عدم تأیید کلاینت ها از روش Enforcement استفاده میکند : Enforcement Type.راهکاری برای جلوگیری از دسترسی کلاینت های تأیید نشده میباشد که در ۴ سطح میتوان اعمال کرد :

- IP Sec
- 802.1 X
- VPN
- DHCP

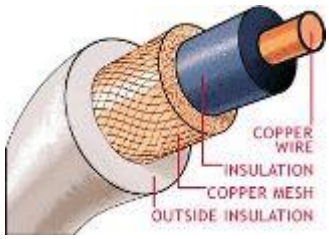
نکته قابل توجه : از NAP نمیتوان به عنوان یک راهکار امنیتی نام برد واستفاده کرد .با توجه به شرایطی که در بالا ذکر شد چنانچه کلاینتی تمام مجوزهای گفته شده را داشته باشد میتواند از NAP به راحتی بگذرد و به شبکه ما وارد شود NAP . تنها راهکاریست برای چک کردن سلامت سیستم ها ..

کابل شبکه (مسی و فیبر نوری)

کابل کواکسیال

یکی از مهمترین محیط های انتقال در مخابرات کابل کواکسیال و یا هم محور می باشد . این نوع کابل ها از سال ۱۹۳۶ برای انتقال اخبار و اطلاعات در دنیار به کار گرفته شده اند. در این نوع کابل ها، دو سیم تشکیل دهنده یک زوج ، از حالت متقارن خارج شده و هر زوج از یک سیم در مغز و یک لایه مسی بافته شده در اطراف آن تشکیل می گردد. در نوع دیگر کابل های کواکسیال ، به حای لایه مسی بافته شده ، از تیوپ مسی استوانه ای استفاده می شود. ماده ای پلاستیکی این دو هادی را از

یکدیگر جدا می کند. ماده پلاستیکی ممکن است بصورت دیسکهای پلاستیکی یا شیشه ای در فواصل مختلف استفاده و مانع از تماس دو هادی با یکدیگر شود و یا ممکن است دو هادی در تمام طول کابل بوسیله مواد پلاستیکی از یکدیگر جدا گردند.



کابل کواکسیالی که به عنوان ستون فقرات استفاده می گردد Thick Ethernet نامیده می شود. در سیستم فوق ، از تمامی پهنای باند به منظور انتقال اطلاعات استفاده می گردد . موسسه IEEE در سال۱۹۸۳، نسخه رسمی استاندارد اترنت را با نام IEEE ۸۰۲,۳ و در سال ۱۹۸۵ ، نسخه شماره دو را با نام IEEE۸۰۲,۳ a ارائه نمود .

از سال ۱۹۸۳ تاکنون ، استانداردهای متفاوتی ارائه شده است که یکی از اهداف مهم آنان ، تامین پهنای باند مناسب به منظور انتقال اطلاعات است . ما امروزه شاهد رسیدن به مرز گیگابیت در شبکه های کامپیوتری می باشیم.

کانکتور استاندارد برای کابل های کواکسیال، از نوع **BNC** (Bayone -Neill - Concelman) می باشد.

کابل های (**UTP (Unshielded Twisted Pair**

کابل UTP یکی از متداولترین کابل های استفاده شده در شبکه های مخابراتی و کامپیوتری است. از کابل های فوق، علاوه بر شبکه های کامپیوتری در سیستم های تلفن نیز استفاده می گردد (.(CAT1شش نوع کابل UTP متفاوت وجود داشته که می توان با توجه به نوع شبکه و اهداف مورد نظر از آنان استفاده نمود. کابل CAT5، متداولترین نوع کابل UTP محسوب می گردد.

مشخصه های کابل UTP

با توجه به مشخصه های کابل های UTP، امکان استفاده، نصب و توسعه سریع و آسان آنان، فراهم می شود.

در زیر انواع کابل های UTP معرفی شده است:

گروه :CAT1سیستم های قدیمی تلفن، ISDN و مودم سرعت انتقال اطلاعات حداکثر تا یک Mb/s

گروه :CAT2شبکه های Token Ring سرعت انتقال اطلاعات حداکثر تا چهار Mb/s

گروه :CAT3شبکه های Token ring و ۱۰ BASE-T سرعت انتقال اطلاعات حداکثر تا ده Mb/s

گروه :CAT4شبکه های Token Ring سرعت انتقال اطلاعات حداکثر تا شانزده Mb/s

گروه :CAT5اترنت ۱۰Mb/s، اترنت سریع ۱۰۰Mb/s و شبکه های Token Ring با سرعت ۱۶Mb/s سرعت انتقال اطلاعات حداکثر تا یکصد Mb/s

گروه :CAT5eشبکه های Gigabit Ethernet سرعت انتقال اطلاعات حداکثر تا یکهزار Mb/s

گروه :CAT6شبکه های Gigabit Ethernet سرعت انتقال اطلاعات حداکثر تا یکهزار Mb/s

گروه :CAT7شبکه های ۱۰G با سرعت انتقال داده تا ده هزار Mb/s

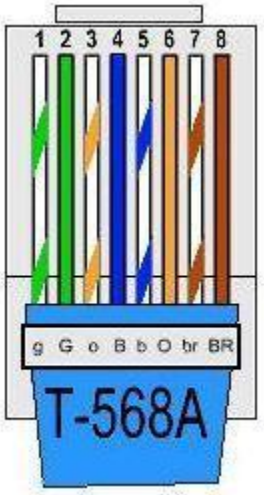
کابل های CAT6 مشابه کابل های CAT5 بوده ولی بین ۴ زوج کابل آنان از یک جداکننده فیزیکی به منظور کاهش پارازیت های الکترومغناطیسی استفاده شده و سرعتی بالغ بر یکهزار Mb/s را ارائه می نمایند.

شرکت های بزرگ در شبکه LAN، کابل CAT6 از نوع UTP را برای مسافت های زیر ۱۰۰ متر و برای بالاتر از ۱۰۰ متر از نوع SFTP استفاده می کنند.

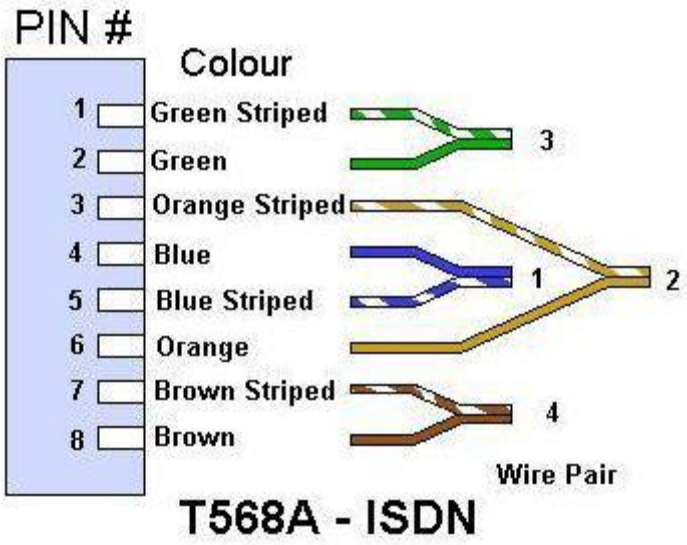
کابل های بهم تابیده دارای انواع بدون شیلد UTP، فویل آلومینیومی FTP و شیلد دار STP و گاهی فویل و شیلد دار SFTP در رنگهای مختلف و با دو نوع ژاکت PVC و LSZH عرضه می شوند که نوع آخری فاقد هالوژن می باشد و در هنگام آتش سوزی دود سمی تولید نمی کند.

استاندارد اتصالات کابلها در شبکه

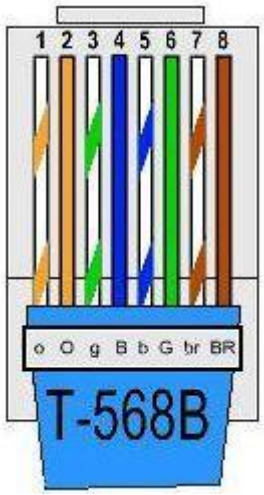
رنگ بندی رشته های کابل شبکه اولیه و استاندارد در سیستم CAT5 و CAT6 نوع A



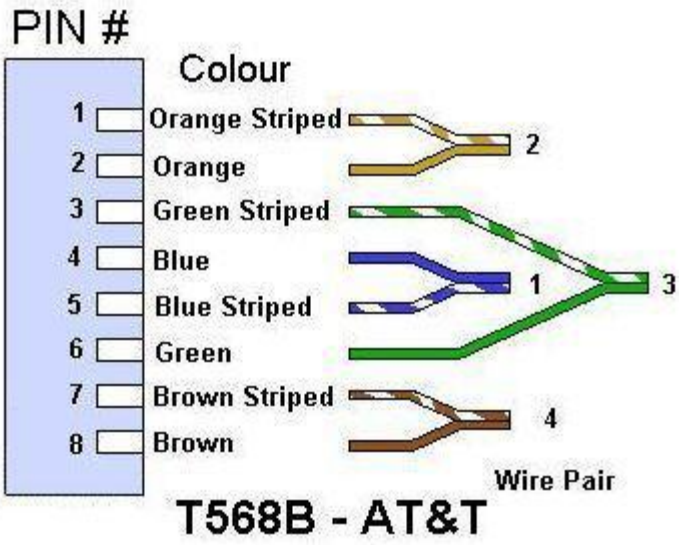
۱- سفید سبز
۲- سبز
۳- سفید نارنجی
۴- آبی
۵- سفید آبی
۶- نارنجی
۷- سفید قهوه ای
۸- قهوه ای



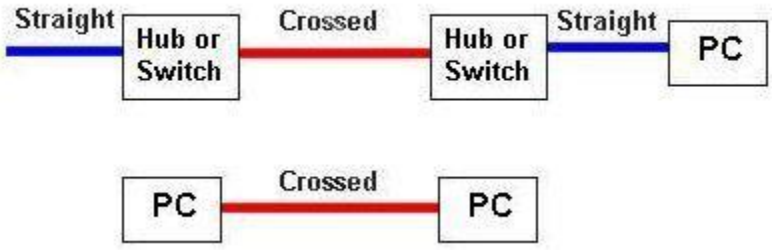
رنگ بندی رشته های کابل شبکه اولیه و استاندارد در سیستم CAT5 و CAT6 نوع B



۱- سفید نارنجی
۲- نارنجی
۳- سفید سبز
۴- آبی
۵- سفید آبی
۶- سبز
۷- سفید قهوه ای
۸- قهوه ای

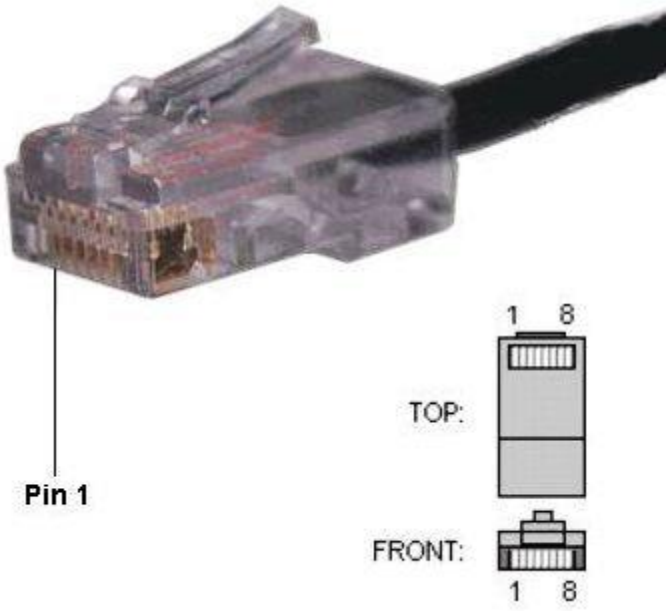


این نوع اتصال برای یک شبکه که از چند کامپیوتر و بوسیله سوئیچ صورت می گیرد و هر دو سر سیم متناظر و ۱ به ۱ بهم اتصال پیدا می کنند.

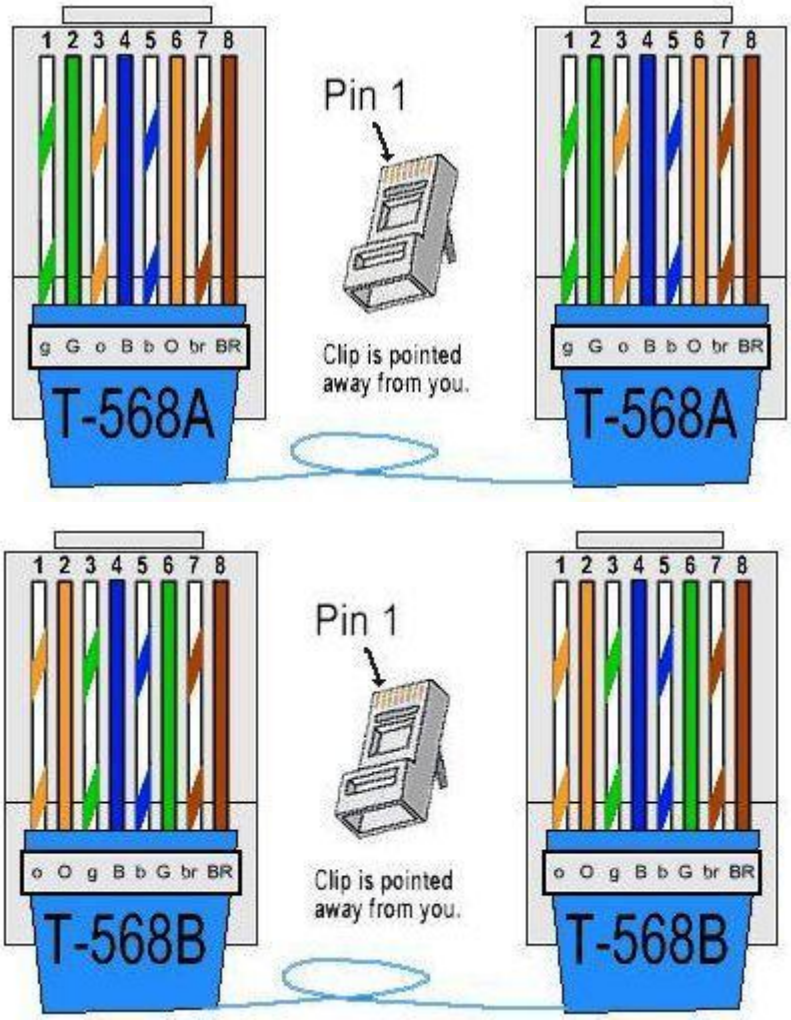


برای اتصال دو دستگاه همجنس مثل دو کامپیوتر یا دو سوئیچ به هم، اتصال Cross استفاده میشود که در این اتصال یک سر بصورت معمولی و در سر دیگر کابل، سیم ۱ به ۳ و ۲ به ۶ وصل میشود. رشته های کابل با توجه به شماره آنها در سوکت قرار داده شده و سوکت پرس می شود.

تذکر: شماره گذاری وقتی طرف تخت سوکت به سمت شماست و از سمت چپ به راست صورت می گیرد.

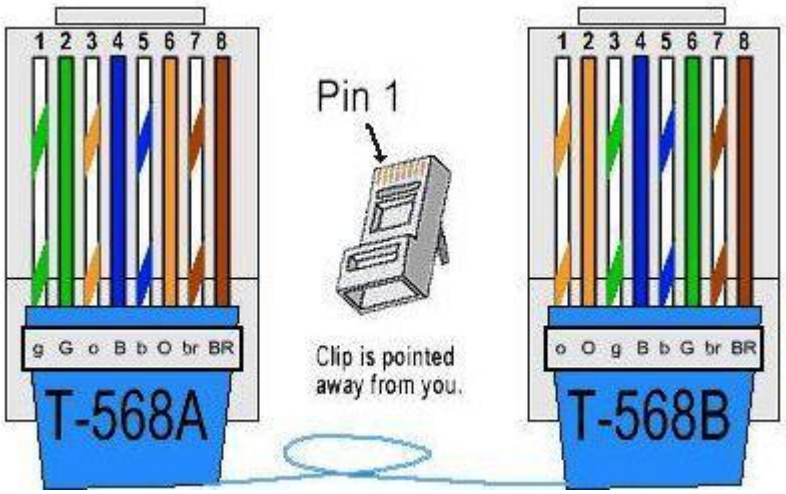


اتصال به صورت استرایت یا مستقیم

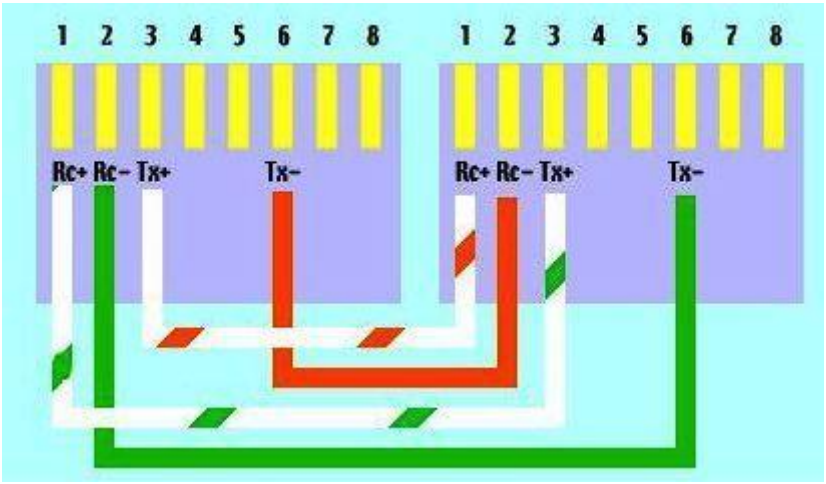


اتصال به صورت کراس

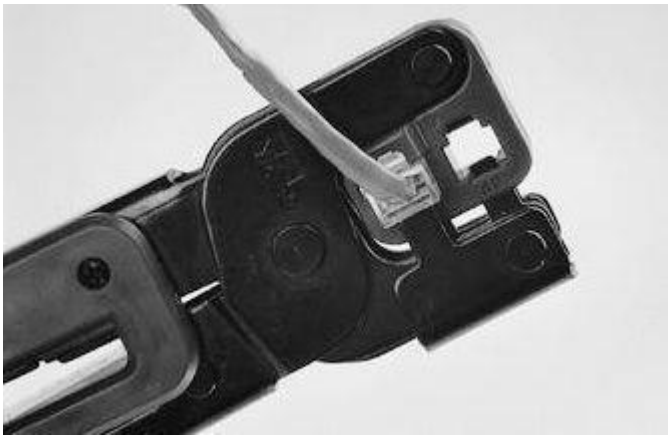
وقتی دو دستگاه همجنس مثل دو کامپیوتر یا دو سوئیچ را بخواهیم به هم متصل کنیم، از اتصال متقاطع یا کراس (Crossover cable) استفاده می کنیم. برای ساخت این کابل یک سر را بصورت مستقیم به کانکتور متصل می کنیم و در سر دیگر جای TX و RX را عوض می کنیم، یعنی سیم ۱ به ۳ و ۲ به ۶ وصل میشود.



در این تصویر به صورت فنی به این نوع سیم کشی پرداخته شده است و سیستم فرستندگی و گیرندگی را نشان می دهد.

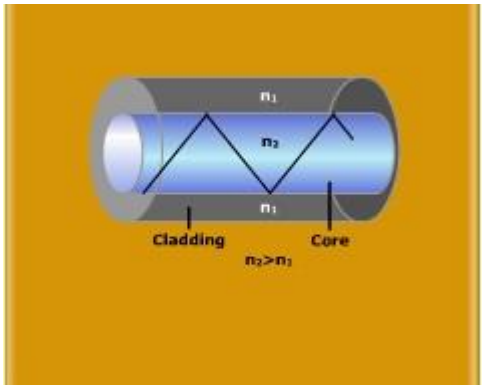


در تصویر زیر آچار مخصوص اتصال را مشاهده می کنید:



فیبر نوری

یکی از محیط های انتقال در شبکه های کامپیوتری، فیبر نوری است. فیبر نوری را هنگامی استفاده می کنیم که نیاز به ارتباط بین مسافت های بیش از ۱۰۰ متر و پهنای باند زیاد داریم. در این فیبرها، نور در اثر انعکاسات کلی در فصل مشترک هسته((coreو غلاف ((cladding، انتشار پیدا خواهد کرد. منابع نوری در این نوع کابل ها، دیود لیزری و یا دیودهای ساطع کننده نور می باشند.

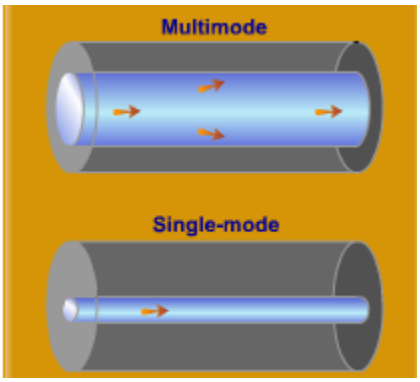


فیبرهای نوری از نظر ژاکت به انواع مختلف از قبیل ضد جونده، وایر استیل آرمورد، ضد آتش، ضد دود و ... تقسیم می شوند. همچنین متناسب با محل استفاده به سه گروه مصارف داخل ساختمانی Indoor ، مصارف داخل ساختمان و کانالهای پلاستیکی و فلزیIndoor/Outdoor و برای استفاده در فضای آزاد و دفن در زیر زمین Outdoor تقسیم می شوند.

فیبر های نوری در دو گروه عمده ارائه می گردند:

فیبرهای تک حالته (Single-Mode): بمنظور ارسال یک سیگنال در هر فیبر استفاده می شود.

فیبرهای چندحالته (Multi-Mode) : بمنظور ارسال چندین سیگنال در یک فیبر استفاده می شود.



فیبرهای تک حالته دارای یک هسته کوچک (۸ و ۹ میکرون قطر) بوده و قادر به ارسال نور لیزری مادون قرمز (طول موج از ۱۳۰۰ تا ۱۵۵۰ نانومتر) می باشند. فیبرهای چند حالته دارای هسته بزرگتر (۵۰ و ۶۲/۵ میکرون قطر) و قادر به ارسال نورمادون قرمز از طریق LED می باشند.

فیبرهای مالتی مود می‌تواند در سرعت ۱۰۰ مگابیت با ۲ کیلومتر مسافت را پاسخگو باشد. اما در سرعتهای گیگابیتی، فیبرهای مالتی مود ۶۲/۵ فقط در حدود ۳۰۰ متر و مالتی مود ۵۰ فقط در حدود ۵۵۰ متر را پشتیبانی می‌کند. فیبرهای سینگل مود تا سرعت ۱۰۰ مگابیت را تا مسافت ۱۰۰ کیلومتر می تواند پشتیبانی کند. البته این محدودیتها به دلیل عدم توانایی تجهیزات اکتیو می باشد.

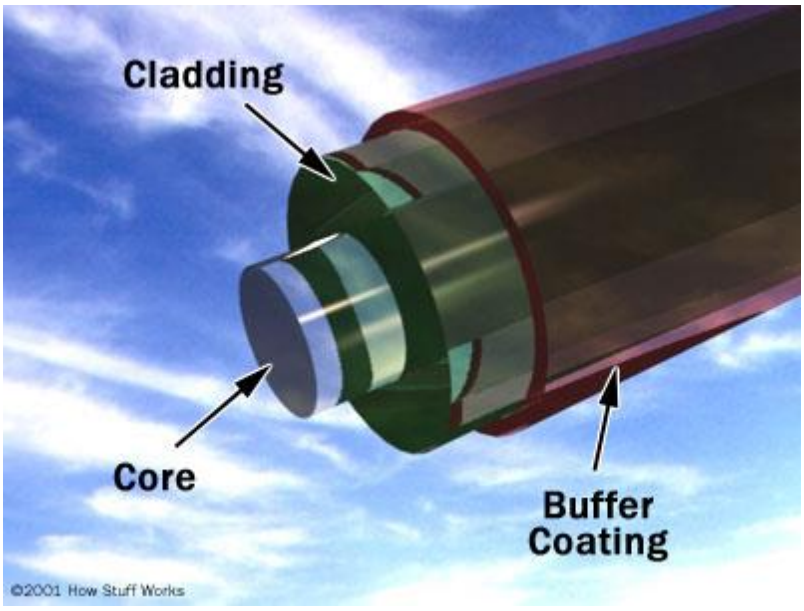
یک فیبر نوری از سه بخش متفاوت تشکیل شده است:

هسته (Core): هسته نازک شیشه ای در مرکز فیبر که سیگنا ل های نوری در آن حرکت می نمایند.

روکش (Cladding): بخش خارجی فیبر بوده که دورتادور هسته را احاطه کرده و باعث برگشت نورمنعکس شده به هسته می گردد.

بافر رویه (Buffer Coating): روکش پلاستیکی که باعث حفاظت فیبر در مقابل رطوبت و سایر موارد آسیب پذیر، است .

صدها و هزاران نمونه از رشته های نوری فوق در دسته هائی سازماندهی شده و کابل های نوری را بوجود می آورند. هر یک از کلاف های فیبر نوری توسط یک روکش هائی با نام Jacket محافظت می گردند.



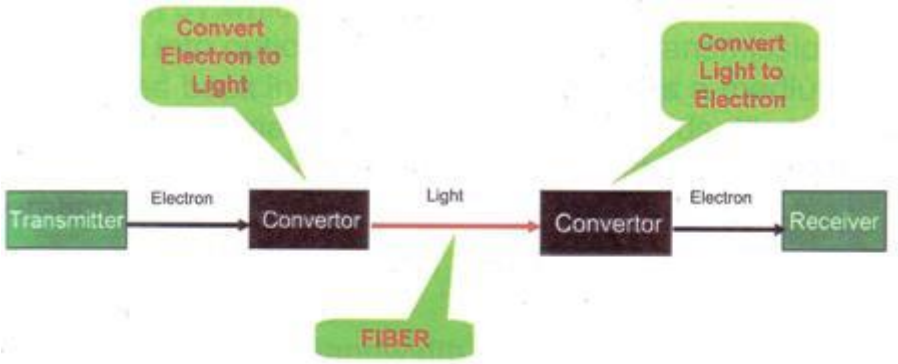
سیستم رله فیبر نوری

سیستم رله فیبر نوری از عناصر زیر تشکیل شده است:

فرستنده: مسئول تولید و رمزنگاری سیگنال های نوری است .

فیبر نوری: انتقال سیگنال های نوری را برعهده دارد.

دریافت کننده نوری: سیگنالهای نوری را دریافت و رمزگشائی می نماید.



مزایا و معایب شبکه بی سیم نسبت به شبکه های کابلیLAN

مزایا:

۱. عدم نیاز به سیم کشی
۲. شبکه های کابلی در مقیاس هایی همچون یک شهر قابل اجرا نیست ولی شبکه های بی سیم تا ده ها و در مواردی تا صد ها کیلومتر قابل پیاده سازی می باشد.
۳. نصب سریع و آسان (در مقایسه با سختی های کابل کشی)

معایب:

۱. در شبکه های کابلی میزان انتقال اطلاعات بین ۱۰ مگابیت تا ۱۰۰۰ مگابیت بر ثانیه (نسبت به نوع تجهیزات و تنظیمات) می باشد که این رقم در شبکه های بی سیم بین ۱ مگابیت تا ۳۰۰ مگابیت (نسبت به تجهیزات و تنظیمات و فاصله) می باشد. لازم به ذکر است که در صورتی که هدف شما از برقراری لینک وایرلس استفاده از شبکه اینترنت می باشد در این زمینه هیچ نگرانی نخواهید داشت زیرا تجهیزات استفاده شده توسط شرکت رسانه جواب گوی نیاز شما خواهد بود.
۲. قطعاً شبکه های کابلی پایدارتر از شبکه های بی سیم هستند اما به دلیل محدودیت های اجرای شبکه کابلی عملاً شبکه بی سیم بهترین گزینه خواهد بود.

پنج سازمان از مهمترین سازمانهای استاندارد سازی

استانداردهای سری IEEE 802.X

802.3 : استاندارد شبکه‌های محلی باس

IEEE 802.4 : استاندارد شبکه‌های محلی توکن باس

IEEE 802.5 : استاندارد شبکه‌های محلی حلقه

IEEE 802.11: استاندارد شبکه‌های بی‌سیم

استاندارد آی‌ئی‌ئی‌ئی ۸۰۲/۳

وقتی ایستگاهی مایل به انتقال باشد به کابل گوش می‌کند. اگر کابل اشغال باشد ایستگاه منتظر می‌ماند تا آزاد شود وگرنه فوراً عمل انتقال را انجام میدهد. اگر دو یا چند ایستگاه در کابل بیکار همزمان شروع به انتقال کنند باهم برخورد خواهند کرد. تمام ایستگاههای برخوردکننده به انتقال خاتمه می‌دهند، مدتی منتظر می‌مانند و کل فرایند را مجدداً تکرار می‌کنند.

در حال حاضر اترنت رایج‌ترین معماری شبکه است. این معماری *baseband* که از توپولوژی خطی استفاده می‌کند معمولاً دارای سرعت انتقال *10 Mbps* است و با روش دسترسی *CSMA/CD* ترافیک روی کابل اصلی شبکه را منظم می‌نماید.

رسانهٔ اترنت غیرفعال است، بدین مفهوم که از کامپیوتر برق می‌گیرد و بخوبی کار می‌کند مگر اینکه از لحاظ فیزیکی قطع گردد و یا به اشتباه توسط ترمینیتور بسته نشود.

در لیست زیر ویژگیهای اترنت خلاصه شده است.

توپولوژی غالب	خطی
سایر توپولوژی‌ها	ستاره‌ای خطی
نوع معماری	*baseband*
روش دسترسی	*CSMA/CD*
مشخصات	*10* یا *100* مگابیت در ثانیه
نوع کابل	*UTP/Thinnet/Thicknet*

تکنولوژیهای مختلف اترنت :

10 BASE 2برای انتقال داده ها از کابل های کواکسیال THINNETاستفاده میکند
در ۵۱۰ BASE از کابل کواکسیال THICKNET برای اتصال کامپیوترها به یکدیگر استفاده میشود .
برای راه اندازی شبکه 10 BASE Tاز کابلهای) Twisted Pairزوج به هم تابیده) استفاده میشود که حداکثر سرعت آن 10 MBPSاست .
10 BASE FLیکی از خصوصیات شبکه اترنتی است که برای انتقال اطلاعات از فیبر نوری استفاده میکند.
ساختار شبکه 100BASE Xهمانند شبکه 10BASE Tاست . (سرعت این شبکه 100MBPSاست) با این تفاوت که 100 BAE Xبا سه مدل کابل کشی متفاوت مورد استفاده قرار میگیرد
۱۰۰۰ BASE Xاین استاندارد شبکه ای را توضیح میدهد که درآن سرعت انتقال اطلاعات یک گیگابایت در ثانیه است
۱۰۰۰ BASE T

در این استاندارد ، از کابل های زوج به هم تابیده برای راه اندازی شبکه ای با سرعت یک گیگابیت در ثانیه استفاده میشود

پروتکل CSMACD در تکنولوژی اترنت به عنوان ابزاری برای کنترل ارسال دیتا در یک مدیا و یا یک collision domainمشترک است به نحوی که فریم ها در طول شبکه بدون وقوع collision ارسال گردند. در این پروتکل دیگر نیازی به وجود یک arbitration central برای صدور مجوز ارسال *دیتا از طریق تخصیص token و یا timeslot ها به ایستگاه ها نمی باشد.در این حالت هر کارت شبکه به تنهایی نحوه دسترسی به مدیا را بدون حضور collision کنترل می کند.*

پروتکل های TCP و UDP چه تفاوتی با هم دارند ؟

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

ITPro.ir - انجمن تخصصی فناوری اطلاعات ایران

tcpچیست؟

) Tcpپروتکل کنترل انتقال) یک پروتکل ارتباطی اصلی مورد استفاده در شبکه های IP است. پروتکل TCP شامل لایه انتقال از مدل OSI است TCP .ارتباط کرا بود که فابلیل اطمینان با اعتباری را داراست.با روش اتصال گرا، دو گره از شبکه می توانند مخابره داشته باشند. با استفاده از TCP آنها باید ابتدا پروتکلی یا فرایندی با نام) Handshaking تکان دادن دست) را کامل کرده تا یک اتصال را ایجاد کنند.زمانی می گوییم که TCP قابلیت اطمینان با اعتباری را فراهم می کند یعنی اینکه TCP شامل مکانیزمی برای خطایابی و تصحیح خطا بین مبدا و مقصد است.این خصوصیت از TCPمغایر UDP است که غیراتصال گرا و غیرقابل اعتماد است. پروتکل‌های لایه بالاتری که از TCP شامل SMTP, HTTP, NNTP, FTP, TelNet, SSH, LDAPاست .

UDPچیست ؟

پروتکل دیتاگرام کاربر یا UDP یک بخش از مجموعه پروتکل اینترنت است. با استفاده از آن برنامه ها بر کامپیوترهای مختلف یک شبکه می توانند پیام کوتاه را به شکل یه دیتاگرام به یکدیگر ارسال کنند UDP .می‌تواند در شبکه هایی که TCPبه صورت سنتی استفاده می‌شود استفاده گردد اما هیچ تعهدی بر اعتبار یا درستی ترتیب داده‌ها ندارد. دیتاگرامها ممکن است بدون اطلاع خراب شوند یا به محلی برسد که برایش ارسال نشده بود.اگرچه با دیدن این فاکتورها UDP به نظر پروتکل مفیدی به نظر نمی‌رسد. اما آن راه حل مناسبی برای استقاده در مکانهایی هستند که سرعت مهمتر از قابلیت اطمینان یا اعتماد بوده و اهمیت بیشتر دارد. از آنجایی که UDP سربار چک کردن اینکه داده به مقصد در هر بار ارسال داده را ندارد این مورد از UDP پروتکلی سریعتر و موثرتر می‌سازد. این پروتکل اغلب برای برنامه‌هایی با اهمیت‌دهی بالا به زمان که از بین رفتن داده‌ها مقدم‌تر از نرسیدن آنها است مورد استفاده قرار می‌گیرد UDP.یک پروتکل بی‌مرز است که برای سرورهای سفارش شده در پاسخگویی به درخواست‌های کوتاه به تعداد زیادی کلاینت هستند مفید است. در حالیکه TCP بیشتر برای اتصال میان یک سرور و یک کلاینت تنها استفاده می‌شود .

IPچیست و چه کاربردی دارد؟

نشانی پروتکل اینترنت (Internet Protocol Address)یا به اختصار نشانی آی‌پی (IP Address)نشانی عددی است که به هریک از دستگاه ها و رایانه‌های متصل به شبکهٔ رایانه ای که بر مبنای نمایه TCP/IPکار می‌کند، اختصاص داده می‌شوند. پیام‌هایی که دیگر رایانه‌ها برای این رایانه می‌فرستند با این نشانهٔ عددی همراه است و راه یاب های شبکه آن را مانند «نشانی گیرنده» در نامه‌های پستی تعبیر می‌کنند، تا بالاخره پیام به رابط شبکه رایانه مورد نظر برسد.دو نسخه IP درحال استفاده می باشد : آی‌پی نسخه ۴ و آی‌پی نسخه ۶ که هر یک نشانی آی‌پی را به روش متفاوتی ارائه می نمایند.

انواع کلاس های **IP address**:

کلاس A

شبکه های کلاس A برای شبکه هایی که تعداد شبکه هایشان کم ,ولیکن تعداد میزبانهایشان زیاد است و معمولا برای استفاده توسط انستیتوهای دولتی و آموزشی انتخاب میشوند مناسب هستند

در یک آدرس شبکه کلاس , Aبخش نخست آن نشان دهنده آدرس شبکه (network address)و سه بخش دیگر نیز نشاندهنده آدرس میزبان (host address)در شبکه است.

بطور مثال IP 10.20.20.20 عدد ۱۰ به آدرس شبکه و عدد ۲۰,۲۰,۲۰ به آدرس میزبان تعلق دارد

در آدرس دهی کلاس A اولین بیت صفر میباشد.

01111111 = 0 + 64 + 32+ 16+ 8+ 4+ 2+ 1 = 127

کلاس B

شبکه های کلاس B برای شبکه هایی که تعداد شبکه هایشان بین شبکه های بسیار بزرگ و بسیار کوچک است در نظر گرفته شده است

در یک آدرس شبکه کلاس B دو بخش نخست آن نشان دهنده آدرس شبکه و دو بخش دیگر نشاندهنده آدرس میزبان است

بطور مثال IP 172.16.10.10 عدد ۱۷۲,۱۶ به آدرس شبکه تعلق دارد و عدد ۱۰,۱۰ به آدرس میزبان تعلق دارد

در آدرس دهی کلاس B دومین بیت صفر میباشد.

10111111 = 128+ 0+ 32+ 16+ 8+ 4+ 2+ 1 = 191

کلاس C

شبکه های کلاس C برای شبکه هایی که تعداد شبکه های زیادی دارند اما میزبان کمتری دارند تدارک داده شده است

در یک آدرس شبکه کلاس C , سه بخش نخست آن نشان دهنده آدرس شبکه و بخش آخر به آدرس میزبان تعلق دارد

بطور مثال IP 192.168.10.20 عدد ۱۹۲,۱۶۸,۱۰ به آدرس شبکه و ۲۰ به آدرس میزبان تعلق دارد

در ای پی آدرس دهی کلاس C , سومین بیت صفر میباشد.

11011111 = 128 + 64+ 0+ 16+ 8+ 4 + 2+ 1 = 223

کلاس D

آدرس کلاس D برای Multicasting استفاده میشود

بدلیل اینکه این آدرس رزو شده است بهمین دلیل از بحث درباره آن خوداری میکنیم

در کلاس D چهارمین بیت صفر میباشد.

=۱۱۱۰۱۱۱۱ ۲۳۹=۱۲۸+۶۴+۳۲+۰+۸+۴+۲+۱

کلاس E

آدرسهای کلاس E برای research and Development استفاده میشود.

IP نسخه ۴ چیست؟

در ابتدا که استاندارد های شبکه وب تعریف گردید، از اعدادی بر مبنای ۳۲ بیت برای ایجاد شماره های IP استفاده شد که به آن، آدرس های اینترنتی نسخه ۴ می گویند (IPv4 یا Internet Protocol Version 4)، در این نسخه که هم اکنون نیز در حال استفاده است، از ترکیب اعداد بر مبنای ۳۲ بیت نهایتا تا سقف ۴,۳ میلیارد (۴,۲۹۴,۹۶۷,۲۹۶) آدرس اختصاصی قابل ایجاد است، از طرفی در این نسخه از آدرس های پروتکل اینترنت تعداد ۱۸ میلیون آدرس برای شبکه های شخصی (private networks شامل سری ۱۰,۰,۰,۰ الی ۱۰,۲۵۵,۲۵۵,۲۵۵ تعداد ۱۶۷۷۷۲۱۶ آی پی آدرس، ۱۷۲,۱۶,۰,۰ الی ۱۷۲,۳۱,۲۵۵,۲۵۵ تعداد ۱۰۴۸۵۷۶ آی پی آدرس و ۱۹۲,۱۶۸,۰,۰ الی ۱۹۲,۱۶۸,۲۵۵,۲۵۵ تعداد ۶۵۵۳۶ آی پی آدرس) و ۲۷۰ میلیون آدرس نیز برای کامپیوترهای میزبان شبکه (multicast) اختصاص داده شد (multicast به طور ساده به معنی تکنیکی است که در آن با اختصاص یک IP به یک ابر سرور، امکان پشتیبانی از تعداد زیادی سرورهای زیر مجموعه با آن

فراهم می شود، multicast ها در واقع به نوعی سرورهای اصلی وب محسوب می شوند).

IP نسخه ۶ چیست؟

گسترش روز افزون اینترنت و نیاز به آدرس های بسیار بیشتر تیم IETF (Internet Engineering Task Force) را برآن داشت تا به فکر تکنولوژی های جدیدی باشند تا امکان تعریف آدرس های آی پی بیشتری فرآهم گردد. بهترین راه ساخت مجدد نشانی پروتکل اینترنت بود.

در سال ۱۹۹۵ میلادی نسخه جدید نشانی پروتکل اینترنت با نام IP Ver. 6.0 معرفی گردید .

اندازه آدرس از ۳۲ بیت به ۱۲۸ بیت افزایش یافت و امکان آدرس دهی تا ۲۱۲۸ آدرس افزایش یافت.

این کار تنها تعداد آدرس های اینترنتی را گسترش نداد، بلکه باعث خواهد شد جدول مسیریاب های اینترنتی (روترها) کوچکتر شود.

کلیه سیستم‌عامل‌های جدید سرور و خانگی از جمله ویندوز ویستا به طور کامل پشیبانی می‌شود ولی متاسفانه هنوز توسط بسیاری از مسیریاب های شبکه های خانگی و تجهیزات شبکه عادی پشتیبانی نشده است.

IP ایستا ((Staticو پویا ((Dynamic

IP پویا ((Dynamicبا هر بار وصل‌شدن به شبکهٔ داخلی و یا اینترنت تغییر می‌کند. اما IP ایستا ((Staticاینطور نیست.

IP پویا ((Dynamicدر هر شبکه توسط کارساز پروتکل پیکربندی پویای میزبان ((DHCP Serverبه رایانه‌ها در شبکه اختصاص داده می‌شود. یعنی وقتی شما به اینترنت و یا شبکهٔ داخلی وصل می‌شوید، کارساز پروتکل پیکربندی پویای

میزبان به شما یک نشانی آی‌پی اختصاص می‌دهد.

DHCP Server می‌تواند یک سرویس در سیستم‌عامل‌های سرور باشد یا یک قطعهٔ سخت‌افزاری مانند مسیریاب (Router) و یا نقطهٔ دسترسی (Access Point) در شبکه باشد.

استانداردهای شبکه بیسیم

یکسری استانداردها برای شبکه های بی سیم تعریف شده است که در زیر نام آنها را می بینید :

a - 802.11b - 802.11g - 802.11n۸۰۲,۱۱

اینها معروفترین استانداردهای شبکه بی سیم هستند گر چه امروزه بیشتر استانداردهای g۸۰۲,۱۱ و n۸۰۲,۱۱ رایج هستند . در موارد بسیار کمیاب نیز ممکن است هنوز از استاندارد b۸۰۲,۱۱ استفاده شود ولی a۸۰۲,۱۱ در هیچ کجا کاربرد ندارد .

استاندارد a۸۰۲,۱۱

از فرکانس ۵ گیگا هرتز استفاده می کند و تا ۵۴ مگابیت بر ثانیه نرخ انتقال داده سرعت دارد . توجه داشته باشید که این نرخ انتقال داده در بهترین حالت ممکن به دست می آید . چنین سوالی مطرح می شود که اگر این استاندارد داده را با سرعت ۵۴ مگابیت بر ثانیه منتقل می کند , چرا دیگر کاربردی ندارد ؟

دلیل این است که تا مسافت ۱۰۰ فیت بورد دارد و به راحتی سیگنال آن مسدود می شود . همچنین مسافت اگر کمی افزایش یابد مثلا فاصله به ۲۰ یا ۳۰ فیت برسد سرعت انتقال به طرز باورنکردنی کاهش می یابد .پس استفاده از آن با مشکلات زیادی روبرو است .

استاندارد b۸۰۲,۱۱

یکی از اولین استانداردهایی بود که به سرعت عمومی شد . از فرکانس ۲,۴ گیگاهرتز استفاده می کند . یکی از مشکلات بزرگی که استفاده از این استاندارد در شبکه بوجود می آورد این است که دیوایس های بی سیم زیادی همچون دوربین ها و تلفن های بی سیم و... از این استاندارد استفاده می کنند و این امر موجب پدید آمدن تداخل سیگنال بین دو دیوایس شده . همچنین این استاندارد نرخ انتقال داده با سرعت ۱۱ مگابیت بر ثانیه را دارد گرچه سرعت بالایی نیست ولی به دلیل این که اکثر افراد برای استفاده از اینترنت در خانه از آن استفاده می کنند , نیاز آنها را برطرف می کند . همچنین این استاندارد مسافت ۳۰۰ فیت در فضای باز و ۱۰۰ فیت در فضای داخل را انتقال می دهد و دلیل این تفاوت این است که در فضای بسته داخل دیوار ها و سقف ها مانعی برای عبور سیگنال محسوب می شوند .

استاندار g۸۰۲,۱۱

جایگزین مناسبی برای b۸۰۲,۱۱ بود و جالب است بدانید که g۸۰۲,۱۱ قابلیت سازگاری و بازگشت به b۸۰۲,۱۱ را دارد به همین دلیل است که بر روی بسیاری از دیوایس های نوشته شده است g&b۸۰۲,۱۱ به این معنی که توانایی استفاده از هر دو سیگنال را دارد . این ویژگی باعث شد که در صورتی شما یک مودم وایرلس g۸۰۲,۱۱ خریداری کردید , نیازی به تعویض کلیه دیوایس های دیگر خود همچون کارت شبکه لپ تاپ نشوید . این استاندارد از فرکانس ۲,۴ گیگا هرتز استفاده می کند و سرعت انتقال آن ۵۴ مگابیت برثانیه است همچنین مسافت ۱۰۰ فیت داخل و ۳۰۰ فیت فضای باز را انتقال می دهد .

استاندارد n۸۰۲,۱۱

آخرین استانداردی که وجود دارد n۸۰۲,۱۱ می باشد . این استاندارد یک تکنولوژی جالب توجه است زیرا از هر دو فرکانس ۲,۴ و ۵ گیگا هرتز استفاده می کند . همچنین نرخ انتقال داده ۱۰۰ مگابیت برثانیه را دارد ولی واقعیت این است که در یک سناریوی کامل (در صورتی که همه چیز به خوبی تنظیم شده باشد و تداخل سیگنال را کاهش دهید و مسافت را کاهش دهید

, همه کانال ها را در اختیار داشته باشید) به صورت تئوری سرعت تا ۶۰۰ مگابیت بر ثانیه نیز عبور می کند . همچنین این استاندارد تا مسافت ۱۰۰۰ فیت را انتقال می دهد .

این استاندارد از تکنولوژی به نام MIMO استفاده می کند . مخفف Multiple In Multiple Out و به این معنی است که در آن واحد و در یک لحظه بیش از یک سیگنال ارسال و دریافت شود و از این طریق سرعت بالاتری را خواهیم داشت .

Collision چیست

Collisionیا همان تصادف زمانی اتفاق می افتد که دو دستگاه در یک شبکه Ethernet می خواهند بصورت همزمان سیگنال های خودر ار ارسال و دریافت کنند و این سیگنال ها قرار است بر روی همان Shared Media ارسال شود ، با توجه به اینکه در Shared Media ها ارسال Full-Duplex یا دو طرفه همزمان وجود ندارد و ارتباطات half-Duplex هستند این فرآیند در این ساختار شبکه پشتیبانی نمی شود و در نهایت Collision در شبکه شما به وجود می آید ، یعنی دو سیگنال در لحظه در شبکه ای قرار می گیرند که امکان پشتیبانی در دو سیگنال در لحظه را ندارد. برای جلوگیری از به وجود آمدن Collision در چنین ساختارهایی از الگوریتمی به نام CSMA/CD برای شناسایی و جلوگیری از به وجود آمدن Collision استفاده می شود . البته نباید به collision به عنوان یک مشکل حاد نگاه کرد ، امروزه Collision به عنوان یک اتفاق عادی در شبکه هایی که بر اساس ساختار Half-Duplex کار می کنند شناخته می شود Collision .

Domainدر واقع به هر Segment از شبکه شما گفته می شود که در آن Collision رخ می دهد که معمولا در شبکه های اترنت است. به زبان دیگر Collision Domain در محدوده همه دستگاه هایی ممکن است رخ دهد که به یک Shared Mediaمتصل شده اند .

دیتا سنتر و استانداردها

به طور کلی محلی برای نگهداری از داده ها می باشد، و از آنجا که این داده ها در تجهیزاتی مثل سرورها قرار دارند به صورت خودکار دیتاسنتر محلی برای نگهداری سرورها و تجهیزات لازم برای ایجاد دسترسی به داده ها می باشد.

طبق استاندارد TIA942 ساختمان یا بخشی از یک ساختمان که وظیفه اصلی آن جادادن اتاق کامپیوتر و نواحی پشتیبانی است را دیتا سنتر گویند.

البته با ظهور پدیده هایی مثل دیتاسنترهای ماژولار که اتاقکهای (کانتینر) از پیش ساخته شده و قابل نصب در فضای باز یا هر محل دیگری هستند این تعریف همچون استاندارد قدیمی TIA942 نیاز به اصلاح دارد.

یکی از مهمرتین و اساسی ترین سوالات کلاس یا تییر Tier مورد نیاز است در این دیتاسنتر تییر مورد نظر کدام است؟ تفاوت تییر یا کلاس در دیتا سنتر بر اساس اهمیت مشخص می شود و Tier یک دیتاسنتر نشان دهنده این است که تا چه حد این دیتاسنتر در شرایط مختلف می تواند پایدار باشد در حال حاضر ۴ کلاس یا تییر برای دیتاسنتر تعریف شده و وجه تمایز اصلی آنها افزونگی یا Redundancy است که هر چه این مورد بیشتر باشد هزینه بالاتری را نیز طلب میکند.

الگوریتم های مسیر یابی و پروتکل های مسیریابی

الگوریتم کوتاه‌ترین مسیر

ساده‌ترین روش مسیریابی، روش کوتاه‌ترین مسیر است. هدف اصلی از این الگوریتم، این است که گراف زیرشبکه را طوری تشکیل بدهیم که در آن هر گره را یک مسیریاب فرض کنیم و هر یال را یک خط ارتباطی میان دو مسیریاب. در این حالت، هر یال یک وزن خواهد داشت و با توجه به الگوریتم کوتاه‌ترین مسیر دایجسترا(۸) می‌توان کوتاه‌ترین مسیر ممکن را محاسبه کرد.

الگوریتم سیل‌آسا

راهکارهای پیشنهادی برای این روش، استفاده از یک شمارنده گام است.

الگوریتم بردار فاصله

در این روش، مسیریاب‌ها در خود جدولی (برداری) ذخیره می‌کنند با عنوان بردار فاصله که در آن بهترین فاصله تا هر مسیریاب دیگر در شبکه را ذخیره می‌کنند. در این صورت، تصمیم‌گیری بهتری هنگام مسیریابی اتخاذ می‌شود.

الگوریتم حالت لینک

مسیریابی بردار فاصله مسیریابی خوبی بود و حتی در شبکه آرپانت(۱۰) تا سال ۱۹۷۹ نیز عملیاتی بود، اما دو مشکل اساسی داشت. نخست اینکه معیار تاخیر در این الگوریتم، طول صفی از مسیریاب‌ها بود و دوم اینکه پهنای باند هر یک از خطوط در محاسبات دخالت داده نمی‌شد. بنابراین حتی اگر جای فاصله را با پهنای باند در جداول مسیریاب عوض می‌کردند، زمان همگرایی این مسیریاب‌ها به یک نتیجه درست، به بی‌نهایت میل می‌کرد.

الگوریتم حالت لینک، ساده است و می‌توان به‌صورت زیر آن را بیان کرد:

1. هر مسیریاب باید همسایه‌های خود را شناسایی کرده و آدرس‌های شبکه‌شان را داشته باشد.
2. میزان هزینه و یا تاخیر همسایه‌های خود را بداند.
3. اطلاعاتی که از همسایه‌ها بدست آورده است را برای تمام مسیریاب‌های دیگر بفرستد.
4. کوتاه‌ترین مسیر برای رسیدن به دیگر مسیریاب‌ها را محاسبه کند.

شناسایی همسایه‌ها به‌این صورت انجام می‌گیرد که پس از راه‌اندازی مسیریاب (بوت‌شدن) یک بسته سلام(۱۱) به تمام همسایه‌ها ارسال می‌شود. مسیریاب‌های همسایه مشخصات خود را برای این مسیریاب می‌فرستند.

برای تخمین هزینه و تاخیر همسایه‌ها، از بسته‌ای به نام Echo استفاده می‌شود. وقتی مسیریاب این بسته را برای همسایه می‌فرستد، آن مسیریاب فورا باید پاسخ آن را ارسال کند، پس از محاسبه زمان رفت و برگشت و تقسیم آن بر عدد ۲، میزان

نسبی تاخیر بدست می‌آید. سپس این اطلاعات را در قالب بسته‌ای برای دیگر مسیریاب‌ها ارسال می‌کند تا آنها نیز از وضعیت این مسیریاب مطلع باشند.

بدین ترتیب هر مسیریاب با دریافت اطلاعات کامل از تمام مسیریاب‌های شبکه، می‌تواند همواره بهترین مسیر را انتخاب کند و کوتاه‌ترین مسیر ممکن را برای ارسال بسته‌ها در نظر بگیرد و شش شرط یک الگوریتم را رعایت کند. روش‌های دیگر مسیریابی نیز وجود دارند که به آنها نیز خواهیم پرداخت.

مقایسه انواع پروتکل های مسیریابی

قایسه انواع پروتکل های مسیریابی. پروتکلهای مسیر یابی و به عبارتی نحوه مسیر یابی در دنیای شبکه به چند طریق گروه بندی می گرد.

اولین دسته بندی رایج و موجود در مسیر یابی ۲ گروه زیر هستند:

- Static Route
- Dynamic Route

Static Route

استاتیک روت روشی است که در آن ادمین شبکه برای تمامی مسیر های مورد نیاز مسیر را به صورت دستی تعریف میکند. در این روش مشکل زمانی به وجود می آید که یکی از مسیر یا IP یکی از روتر ها تغییر کرده و یا یک لینک ارتباطی به هر دلیلی قطع شود آنگاه ادمین تمامی خطوط مسیریابی که در روتر ها ثبت شده است را باید ویرایش و یا اصلاح کند.

این روش مسیر یابی برای شبکه های کوچک مناسب می باشد.

Dynamic Route

داینامیک روت به معنی استفاده از پروتکل های مسیر یابی است که بسته به نوع شبکه و صلاح دید ادمین یکی از پروتکل های موجود انتخاب و اعمال می گردد.

Dynamic Routeرا می توان به دو دسته زیر تقسیم کرد:

- IGP
- EGP

IGP :

این گروه شامل دسته ای از پروتکل های مسیر یابی می گردد که درون AS استفاده و به ۳ گروه زیر تقسیم می گردد:

- Distance Vector => RIP , IGRP
- Link State => ISIS , OSPF
- Hybrid => EIDRP

EGP :

این گروه شامل پروتکل های مسیر یابی ای می گردد که در شبکه های بزرگی مانند اینترنت بین AS استفاده می گردند مانند:

- BGP

پروتکل RIP

RIPیکی از پروتکل های مسر یابی بوده که توسط تمامی برندهای روتر موجوده پشتیبانی می گردد. یکی از معایب این پروتکل Class Less بودن آن است، به این معنی که تمامی IP هایی که روتر جهت اعلام به روتر های همسایه خود اعلام

می کند تمامی در کلاس اصلی خود به روتر های مجاور اعلام می گردد. به همین دلیل اگر شما در شبکه Sub net بندی انجام داده باشید ممکن است در زمان استفاده از این پروتکل با مشکل هایی مواجه شوید.

تصویر زیر شبکه مورد مثال ما در پیاده سازی پروتکل RIP می باشد.

همانطور که در تصویر زیر مشاهده میکنید شما باید Networkمربوط به IP هر کدام از اینترفیس های موجود در روتر را با کامند هایی مانند زیر اعلام کنید. فرامین زیر مربوط به روتر Router0 می باشد

معرفی پروتکل مسیریابی Open Shortest Path First یاOSPF

پروتکل مسیریابی Open Shortest Path First که به اختصار OSPF نامیده می شود یک **پروتکل مسیریابی Link state**است که می تواند ترافیک های مربوط به پروتکل IP را مدیریت کند .OSPF نسخه های مختلفی دارد که در حال حاضر از نسخه ۲ آن بیشتر استفاده می شود OSPF.بر خلاف برخی پروتکل ها که بصورت انحصاری توسط شرکت ها ارائه می شوند یک پروتکل کاملا جامع و بدون وابستگی به هیچ برند خاصی است ، تقریبا همه روترهایی که در دنیا وجود دارند از پروتکل OSPFپشتیبانی می کنند .**پروتکل مسیریابی** Open Shortest Path First یا OSPFاز الگوریتم Shortest Path Firstیا SPF که توسط Dijkstra طراحی شده است برای جلوگیری از بوجود آمدن **Routing Loop**در توپولوژی شبکه ها استفاده می کند و به نوع یک شبکه Loop Free ایجاد می کند OSPF .فرآیند **Convergence**سریعی دارد و از طرفی قابلیت Incremental Update را نیز با استفاده از **Link State Advertisement**یا **LSA**فراهم می کند OSPF .

یک پروتکل Classless است و به شما این اجازه را می دهد که برای طراحی یک ساختار سلسله مراتبی شبکه از **VLSM**و **Route Summarization**براحتی استفاده کنید .

مهمترین معایبی که در OSPF وجود دارد این است که OSPF برای نگهداری لیست OSPF Neighbor ها ، توپوپولوژی شبکه که شامل یک دیتابیس از تمامی روترها و Route های موجود در آنهاست و همچنین Routing Table خود روتر به حافظه RAM نسبتا بیشتری در مقایسه با **پروتکل های Distance Vector** نیاز دارد ، همچنین OSPF به قدرت پردازشی یا CPU بیشتری برای اجرا کردن الگوریتم SPF نیاز دارد و همین موارد باعث می شود که OSPF در رده بندی پروتکل های مسیریابی پیچیده یا Complex Protocol قرار بگیرد. دو مفهوم بسیار مهم در مواردی که می خواهید از OSPFاستفاده کنید وجود دارند که اولین مفهوم **Autonomous System**و دومین **مفهوم Area** می باشد .

Areaدر OSPF برای ایجاد کردن ساختار مسیریابی سلسله مراتبی یا موروثری (Hierarchical Routing) در یک **Autonomous System**استفاده می شود **Area** .ها تعیین کننده این هستند که چگونه و به چه اندازه اطلاعات مربوط به Routing بایستی در شبکه به اشتراک گذاشته شود OSPF .دو لایه وراثت یا Hierarchy دارد ، لایه Backbone یا **Area 0**و لایه های خارج از Backbone یا **Area**های بین عدد ۱ تا ۶۵۵۳۵ ، ایندو دو **Area**ای متفاوت هستند که می توان در بین آنها اطلاعات مسیریابی را **Summarize**کرد **Route Summarization** .به ما کمک می کند که بتوانیم Routing Table های خود را فشرده سازی و کوچکتر کنیم. تمامی **Area**ها بایستی به **Area 0**متصل شوند و تمامی روترها در این **Area**از یک توپولوژی یکسان استفاده می کنند .

معرفی پروتکل مسیریابی**EIGRP**

تاریخچه پیدایشEIGRP

پروتکل EIGRP در سال ۱۳۹۳ توسط شرکت سیسکو ارائه شد و در واقع نسخه بهینه پروتکل IGRP می باشد که در اواسط دهه ۸۰ ارائه شد که محدودیت های RIP را نداشت.پروتکل EIGRP تا سال ۲۰۱۳ به عنوان پروتکل اختصاص سیسکو بود و تنها رو تجهیزات این شرکت قابل استفاده بود . اما از در سال ۲۰۱۳ توسط شرکت سیسکو به عنوان یک پروتکل استاندارد معرفی شد و در حال حاضر روی برخی از تجهیزات دیگر قابل استفاده است .

VLANچیست

Virtual Local Area Network تکنولوژی است که در سوئیچها و تجهیزات لایه ۲ و ۳ ممکن است دیده باشید. از یک مثال ساده شروع میکنم. فرض کنید یک سوئیچ سیسکو ۲۹۶۰ داریم. یک پهنای باند ۴ مگی داریم به همراه ۸ آدرس که gateway ما روتر سرویس دهنده ماست. با هر منطقی به این نتیجه میرسیم که تمامی دستگاههای خود را به سوئیچ متصل کرده و کابل روتر سرویس دهنده را نیز به آن متصل کنیم.

حال یکی از تجهیزات ما یک روتر است که عمل NAT را انجام می دهد که به ۱۰ PC سرویس میدهد. اگر تمامی آن PCها را به سوئیچ متصل کنیم کلاینتهای ما میتواند آزادانه با تنظیم کردن آدرسهای VALID ما از اینترنت استفاده کنند. بسیاری از سرویس دهنده های اینترنت به این مشکل مبتلا هستند که اگر مقداری کلاینت آنها باهوش باشد کار آنها ساخته است. خب اولین راه حل این است که از ۲ عدد سوئیچ استفاده کنیم. که منطقی است. اما شما هزینه اضافه پرداخت کرده اید.برای این کار میتوان به سادگی از VLAN استفاده نمود و سوئیچ خود را تبدیل به ۲ یا چند سوئیچ مجزا کرد.

InterVLAN Routing

یک سوئیچ لایه دو می تواند با اتصال به یک روتر ارتباط بینVLAN ها را برقرار کند و این برقراری ارتباط می تواند توسط لینک های جداگانه برای هر VLAN انجام شود و یا با استفاده از یک لینک Trunkاز سوئیچ به روتر انجام پذیرد .

با توجه به تعداد محدود پورت رو روتر معمولا از یک لینک ترانک برای برقراری ارتباط بینVLAN های استفاده می شود و به ان Router on Stick گفته می شود .

- نکته : با تمام سوئیچ هایی که از VLAN پشتیبانی می کنند می توان این ویژگی را پیاده سازی کرد.
- نکته : کل ترافیک بین VLAN ها روی یک لینک منتقل می شود و در صورت قطع شدن یا وجود ترافیک زیاد (بیشتر از ظرفیت لینک) ، باعث ایجاد مشکل در ارتباط بین VLAN ها خواهد شد.
- نکته : این ویژگی در دنیای واقعی کاربرد بسیار زیادی دارد چون روی روترها تعداد پورت ها کم هستند و در صورت نیاز به پورت بیشتر نیاز به خرید ماژول می باشد که این کار مقرون به صرفه نیست در نتیجه با استفاده از این ویژگی این کمبود پورت جبران می شود .

مدیا کانورتر

مدیا کانورترها یک سیگنال از کابل مسی را میگیرند آن را تبدیل به یک سیگنال نوری سبک میکنند و از طریق فیبر نوری آن را انتقال میدهند. آن سوی دیگردر انتهای فیبر نوری، گیرنده مدیا کانورتر سیگنال نوری را دریافت کرده و مجددا آن را به سیگنال مسی برمیگرداند.

برای مثال اگر یک سیگنال اترنت وارد فرستنده فیبر نوری شود، همین سیگنال اترنت در آن سوی فیبر نوری از طرف گیرنده دریافت شده و به همان صورتی که بود به شما تحویل داده میشود. همین روند برای سیگنالهای دیتا مانند RS232 و Rs485و Rs422 و به همان خوبی برای سیگنالهای دوربین های CCTV نیز صدق میکند. مدیا کانورترها به صورت جفت می باشند که یکی در ابتدا و دیگری در انتهای لینک فیبر نوری قرار می گیرند.

پروتکل **SMTP** چیست؟

پست الکترونیکی یکی از مهمترین سرویس های اینترنت است که شباهت زیادی به پست معمولی دارد .این سرویس، اتصال غیر هم زمان رابرای افراد پدید می آورد .بدین معنا که افراد هر زمان مایل باشند می توانند اقدام به ارسال و یا مطالعه ی نامه های خود نمایند، بدون این که نیاز باشد این اعمال را با زمان و برنامه ریزی دیگران منطبق کنند .هنگامی که یک نامه ی الکترونیکی ارسال می شود، انتظار این است که سرویس دهنده ی پست الکترونیکی، آن نامه را به درستی به مقصدارسال نماید .مراحل ارسال بدون توجه به سخت افزار و نرم افزار و تنها با استفاده از پروتکل های انتقال پست الکترونیکی انجام می شود.

SMTP مهمترین پروتکل انتقال پست الکترونیکی می باشد. پروتکل SMTP مخفف **SIMPLE MAIL TRANSFER PROTOCOL** بوده که از این پروتکل برای ارسال پیام‌های الکترونیکیE-mail استفاده می‌شود. . تا قبل از آن از پروتکلUUCP(Unix-to-Unix Copy) برای ارسال پیام‌های الکترونیکیE-mail استفاده می‌شد.

این پروتکل دارای ویژگی های بسیار زیادی است که آن را به یکی از مهمترین پروتکلهای اینترنت تبدیل کرده است .اما با این وجود، این پروتکل محدودیت هایی از قبیل محدودکردن بدنه ی نامه های الکترونیکی به هفت بیت کد اسکی را از زمان گذشته

با خود به همراه دارد .این محدودیت تا اوایل دهه1980 میلادی که انتقال و ارسال نامه های الکترونیکی بسیار کم و به ندرت بود، مشکلی ایجاد نمی کرد .اما امروزه و در عصر رسانه های چند منظوره، محدودیت هفت بیت کد اسکی دردسرساز است .زیرا نیاز دارد که داد ه های مالتی مدیای باینری، قبل از ارسال از طریق SMTPبه کد اسکی تبدیل شوند و پس از انتقال از طریق این پروتکل از اسکی به باینری برگردانده شوند.

پروتکل smtp به دلیل محدودیت‌هایی در نگهداری نامه‌ها، معمولا با پروتکل‌های POP3 یا (post office protocol3) یا IMAP (internet message access protocol) استفاده می‌شود که برای کاربران امکان ذخیره نامه‌ها را روی یک سرور یا دانلود آنها را از سرور فراهم می‌کند. در حقیقت می‌توان گفت، SMTP برای ارسال نامه‌ها و POP3 یا IMAP برای دریافت نامه‌ها به کار می‌روند. به عبارت ساده‌تر، سرور SMTP، مانند وب سرور یک رایانه است که مانند مسیریاب عمل می‌کند. هنگامی که پیام‌های پست الکترونیکی از کاربران را دریافت می‌کند آنها را به گیرندگان مورد نظر می‌فرستند. SMTPفقط به نام کاربری و دامنه نیاز دارد تا مستقیم پیغام را به سمت گیرنده مسیریابی کند و به طور پیشفرض بر روی پورت ۲۵ قرار دارد. البته مدیران سرور برای افزایش امنیت می توانند پورت آن را تغییر دهند.

تعریف BACH BON (بک بون)

به مفهومی اطلاق می شود که امکان برقراری بین سگمنت های دیگر موجود در یک LAN را برقرار می سازد. در حالت کلی محلی می باشد که از آنجا شبکه به قسمت ها و انشعابهای مختلف تقسیم می شود.

Split Horizonچیست

Split Horizonبا اتکا به اصلی بسیار ساده و کارا ، از بروز چرخه یا loop در شبکه جلوگیری میکند

تفاوت اصلی روش های مسیریابی Link State و Distance Vector چیست؟

در پروتکل های مسیر یابی Distance Vector هر روتر تنها تا روترهای همسایه را می بیند و هیچ اطلاعی از توپولوژی شبکه ندارد. اما در پروتکل های Link-State هر روتر جزئیات توپولوژی شبکه را می داند.

SLIP , PPP

پروتکل خط سری اینترنت SLIP مخفف کلمات Serial Line Protocol و پروتکل نقطه به نقطه PPP مخفف کلمات Point - to - Point دو نوع حساب اینترنت هستند که اغلب کاربران اینترنت به آنها روی آوردند .

SLIPقدیمی تر است SLIP .به شما اجازه میدهد. که از طریق خط ارتباط سری مانند خط تلفن به فراهم کننده سرویس اینترنت ISP منتقل شوید .

PPPکه بعد از SLIP توسعه یافت نیز طبعی سری دارد.

انواع استاندارد برای سوکت زنی

استاندارد نوع T-568A : خط سبز، سبز، خط زرد،ابی، خط ابی، زرد، خط قهوه ای ، قهوه ای

استاندارد نوع T-568B : خط زرد، زرد، خط سبز،ابی، خط ابی، سبز، خط قهوه ای ، قهوه ای

انواع رک

رک های دیواری: رک های دیواری معمولا دارای ارتفاع های ۵ ، ۶ ، ۷ ، ۹ یونیت هستند و از یک طرف درش باز می شود

رک های ایستاده : در این رکها، انواع پچ پنل، سوئیچ، سرور و سایر قطعات رکمونت ۱۹ اینچی قرار می گیرد. از بالا و پائین این نوع رکها می توان کابلها را عبور داد و همچنین از چهار طرف باز می شوند.

تعریف پچ پنل

در تعریف ها اومده که برای سازماندهی کابل های داخل رک از پچ پنل استفاده می کنند.

وظیفه اصلیش این هست که بین نقاط انتهایی کابلهای شبکه و تجهیزات شبکه ای (هاب، روتر، ...) قرار میگیره و بجای اینکه کابلهای شبکه مستقیما" به این تجهیزات وصل بشن از طریق اون وصل میشن. بعبارت دیگه وجودش بهیچوجه الزامی نیست ولی بکار بردنش در شبکه هایی که در طی زمان گسترش و تغییرات دارن کار رو راحت میکنه.

سوییچ و انواع ان

سوئیچ یک ارتباط بین دو سگمنت ایجاد می نماید. سوئیچهای لایه ۲ باتعداد ۵، ۸، ۱۶، ۲۴ و گاهی ۳۶ و ۴۸ پورت نیز تولید می شود امروزه سرعت آنها ۱۰۰/۱۰ و یا ۱۰۰۰ مگابیت بر ثانیه است. سوئیچها دارای پورتهای ۴۵آرجی ویا فیبرنوری و یا ترکیبی از هر دو هستند. در دو نوع رومیزی و رکمونت و یا رمیزی با قابلیت رکمونتجهت نصبدررکها ۱۹ اینچ استاندارد وجود دارد سرعت سوئیچ کردن از مهمترین مشخصات یک سوئیچ است.

تعریف روتر

شبکه ها را روترها (مسیر یابها) به هم متصل می کنند .تمام دنیا توسط روترها به هم متصل شده و بدین صورت شبکه اینترنت شکل گرفته است . این دستگاهها کارکرد پیچیده ای داشته و نیاز به تنظیمات نرم افزاری دارند .

انواع کابل شبکه :

- کابل cross-over : اتصال دوکامپیوتر با هم - اتصال دوهاب و یا دو سوئیچ به هم بدون استفاده از پورت uplink
- کابل straight : اتصال یک کامپیوتر با یک هاب و یا یک سوئیچ - اتصال دوهاب و یا دو سوئیچ با استفاده ازپورت uplink

فیبرنوری چیست و مزایا آن

- فیبرنوری را هنگامی استفاده می کنیم که نیاز به ارتباط بین مسافت های زیاد یا نیاز به پهنای باند زیاد داریم . فیبرهای نوری که در کار شبکه استفاده می شود باید دارای ۲ رشته و یا ضریبی از ۲ باشند .
- مزایا فیبرنوری : قیمت ارزان – وزن کم – امنیت بالا – پهنای باند وسیع

تعریف DHCP و ویژگی های آن

DHCP یا یک پروتکل ارتباطی درشبکه محلی است که به مدیر شبکه امکان اختصاص IP به رایانه ها به صورت خودکار و از طریق یک سروررا فراهم می کند .هر دستگاهی که بخواهد به اینترنت متصل شود یک IP یکتا لازم دارد . بنا براین در یک شبکه برای اتصال به اینترنت همه دستگاهها بایدIP داشته باشند. اگر ازDHCP استفاده نشود؛ باید برای تک تک رایانه ها به صورت دستی IP وارد کرد ولی استفاده از DHCP باعث می شود که اختصاص IP به دستگاهها به صورت خود کار انجام شود. ویژگی های آن عبارتند :

- جلوگیری از Conflict
- سرعت بخشیدن به کارها
- مدیریت متمرکز

- ضرورت

تعریف **DNS** و ویژگی های آن

DNS یک پروتکل شناخته شده در عرصه شبکه های کامپیوتری خصوصا" اینترنت است. از پروتکل فوق به منظور ترجمه اسامی کامپیوترهای میزبان و Domain به آدرس های IP استفاده می گردد. زمانی که شما آدرس یک سایت را در مرورگر خود تایپ می نمایید نام فوق به یک آدرس IP و براساس یک درخواست خاص گزارش که از جانب کامپیوتر شما صادر می شود، ترجمه می گردد.

برخی نکات خلاصه جهت یاد آوری

انواع آدرسهای IP

- برای آدرس دادن به ماشین های میزبان بهتر است ۳۲ بایت آدرس IP به قسمت های زیر تقسیم شود:

۱. آدرس شبکه

۲. آدرس زیرشبکه(در صورت لزوم)

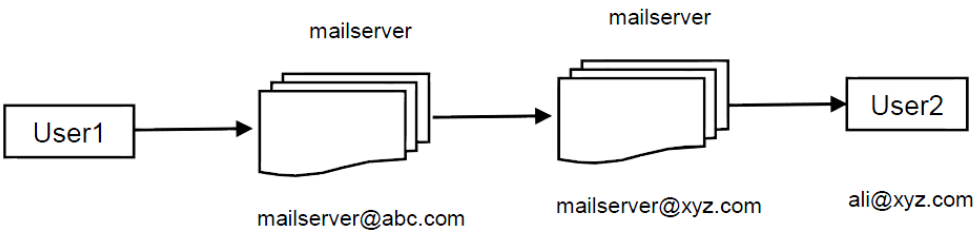
۳. آدرس ماشین میزبان

- آدرس های IP در پنج کلاس A, B,C,D,E معرفی شده اند.

پروتکل های رایج در مدل TCP/IP

- پروتکلهائی که در این لایه استفاده می‌شوند عبارتند از:
- IP , IGMP , BOOTP , ARP , RARP , RIP , ICMP

SMTP پروتکل ساده انتقال نامه‌های الکترونیکی



از پروتکل SMTP برای هل دادن استفاده می‌کنیم. برای ارسال نامه از این پروتکل استفاده می‌شود. برای دریافت نامه از PoP3 و Imap استفاده می‌کنیم.

تکرار کننده یا Repeater :

ابزاری است که سیگنال دیجیتال ورودی را دریافت کرده و پس از تشخیص صفر و یک‌ها (از طریق خطوط ولتاژ) آنها را از نو در خروجی خود به صورت سیگنال دیجیتال عاری از نویز بازتولید می‌کند. تکرار کننده‌ها هیچ درکی از فریم، بسته و حتی بایت ندارند و صرفاً با مفهوم بیت و سطوح ولتاژ آشنایی دارند.

هـاب :

یک هاب معمولاً دارای تعدادی خط ورودی است که از لحاظ الکتریکی از درون بهم متصل شده‌اند. فریمی که از یک خط ورودی دریافت می‌شود بی‌قید و شرط بر روی تمام خطوط دیگر ارسال و منتشر خواهد شد.

تجهیزات Active و Passive در شبکه‌های کامپیوتری :

قطعاتی که معمولاً به برق متصل شده و در تولید، هدایت و یا تربیت سیگنال‌ها نقش دارند در اصطلاح به خودی خود فعالیت دارند قطعات فعال یا **Active** گفته می‌شوند. مثل بی‌سیم، سوئیچ، مودم

قطعاتی که معمولاً به برق متصل شده و در تولید، هدایت و یا تربیت سیگنال‌ها نقش ندارند در اصطلاح به خودی خود فعالیت ندارند قطعات غیرفعال یا **Passive** گفته می‌شوند. مثل کابل، داکت، رک

VLAN

مخفف عبارت Virtual LAN یا LANهای مجازی می‌باشد که باعث جدانمودن ترافیک بخش‌های مختلف و ایجاد حوزه‌های Broadcast Domain (پخش همگانی) مستقل برای محدود کردن ترافیک Broadcast می‌باشد. هر VLAN با یک شماره که به VLAN ID معروف می‌باشد شناسایی می‌شود که رنجی بین یک تا 1005 می‌باشد و VLAN1، VLAN1002، VLAN1003، VLAN1004 و VLAN1005 رزرو می‌باشند.

VLAN1 معروف به Default VLAN می‌باشد و به صورت پیش فرض بر روی کلیه سوئیچ‌ها ایجاد شده و کلیه پورت‌های سوئیچ در عضویت VLAN1 می‌باشد.

فصل سوم: لایه IP در شبکه اینترنت

لایه IP : هدایت بسته‌های اطلاعاتی از شبکه‌ای به شبکه‌های دیگر

آدرسهای MAC

- آدرسهای قابل تعریف در لایه اول (لایه فیزیکی) جهت انتقال فریمها روی کانال

در پروتکل CSMA/CD شبکه (Ethernet) MAC آدرس = 6 بایت

- وابسته به ساختار شبکه

در پروتکل SLIP فیلد آدرس MAC وجود ندارد

بسته IP : واحد اطلاعاتی که درون فیلد داده از فریم فیزیکی قرار گرفته و با عبور از یک شبکه به شبکه دیگر تغییر نمی‌کند.

آدرس IP : آدرس جهانی و مشخص کننده ماشین به صورت یکتا و فارغ از ساختار شبکه‌ای

مسیریاب (Router)

- ماشینی با تعدادی ورودی و خروجی
- دریافت بسته‌های اطلاعاتی از ورودی و هدایت و انتخاب کانال خروجی مناسب بر اساس آدرس مقصد

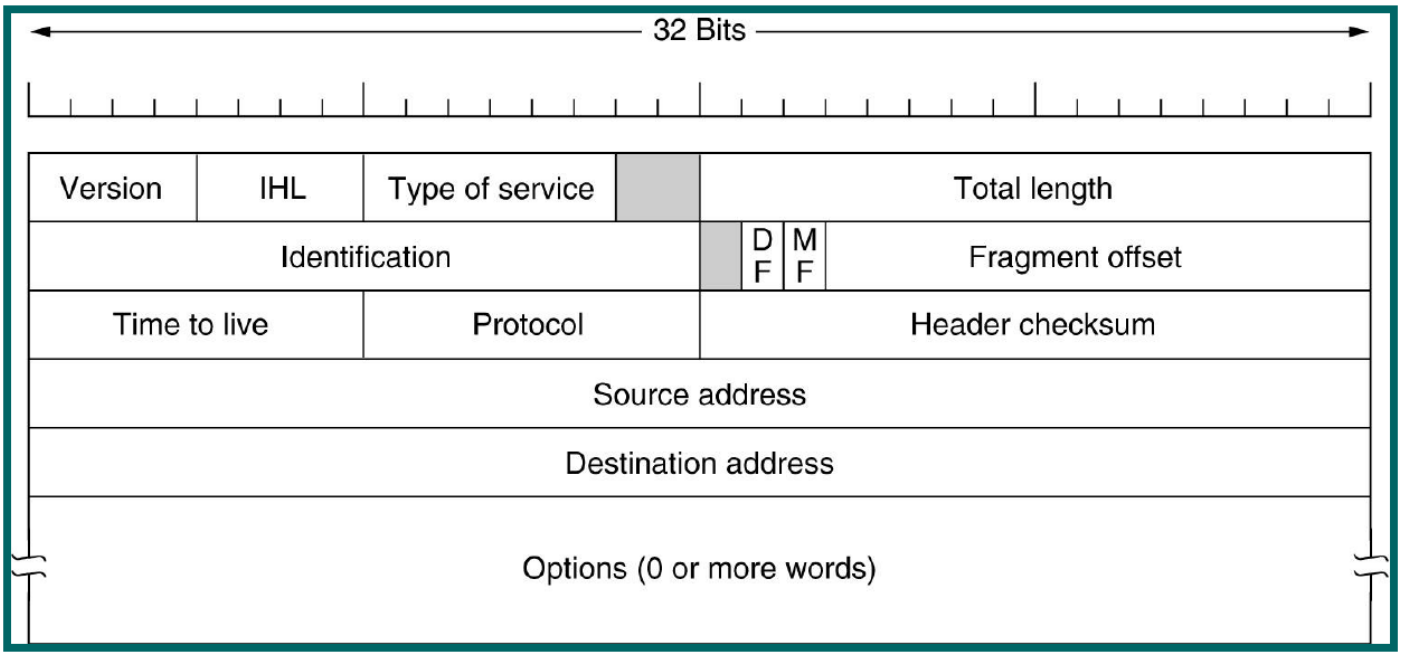
پروتکل IP

- قرارداد حمل و تردد بسته‌های اطلاعاتی
- مدیریت و سازماندهی مسیریابی صحیح بسته‌ها از مبدأ به مقصد

دیتاگرام

واحد اطلاعات که به صورت یکجا از لایه IP به لایه انتقال تحویل داده می‌شود یا بالعکس لایه انتقال آنرا جهت ارسال روی شبکه به لایه IP تحویل داده و ممکن است شکسته شود.

قالب بسته IP



مالتی پلکس یا تسهیم : تقسیم پهنای باند یک کانال بین چند ایستگاه

- تسهیم در میدان فرکانس یا FDM مخفف Frequency Division Multiplexing
- **تسهیم در میدان زمان** یا TDM مخفف Time Division Multiplexing

FDM : تقسیم پهنای باند فرکانسی به N باند مجزا (N تعداد ایستگاه موجود در شبکه)

TDM : تقسیم زمان به بازه‌های کوچک (ارسال اطلاعات بر روی کانال توسط هر ایستگاه فقط در بازه زمانی مشخص)

انواع خطا در شبکه‌های کامپیوتری

- نویز حرارتی
- شوک‌های الکتریکی
- نویز کیهانی

روشهای کشف خطا

- اضافه کردن بیت توازن به داده‌ها
- روش Checksum
- کدهای کشف خطای CRC

مشخصات فیزیکی استاندارد IEEE 802.3

- سرعت : 10 مگابیت بر ثانیه
- کدینگ : "منچستر"
- سطوح ولتاژ : 0.85 V_ و +
- کانال : کابل کواکس 50 اهم یا زوج سیم
- حداکثر طول کانال : 500 متر با کابل کوآکس ضخیم و 185 متر با کابل کوآکس نازک و 100 متر با زوج سیم.

پهنای باند:

توانایی و ظرفیت کانال در ارسال اطلاعات با نرخ B بیت در هر ثانیه

طول موج : فاصله ای است که موج در یک سیکل در زمان یک دوره یا پریود طی میکند.در حقیقت طول موج فاصله میان 2 نقطه هم فاز از دو سیکل پی در پی از موج میباشد.

دسته بندی سخت افزار شبکه‌های کامپیوتری

- **از دیدگاه تکنولوژی انتقال**

1. شبکه‌های پخش فراگیر
2. شبکه‌های نقطه به نقطه

- **از دیدگاه مقیاس بزرگی**

1. شبکه های LAN
2. شبکه های MAN
3. شبکه های WAN

شبکه پخش فراگیر(Broadcast)

انتقال اطلاعات از طریق یک کانال فیزیکی مشترک توسط تمام ایستگاهها

شبکه محلی LAN

- فواصل جغرافیایی محدود (حداکثر تا چند کیلومتر)
- تعداد ایستگاهها کم
- کوتاه بودن طول کانال انتقال

محاسن شبکه‌های LAN

- افت سیگنال کم, نرخ خطای پایین, نرخ ارسال بالا و تأخیر انتشار بسیـار ناچیـز به دلیل کوتاه‌بودن طول کانال
- مدیریت آسانتر شبکه به علت محدود بودن تعداد ایستگاهها
- هزینه پایین نصب و راه‌اندازی این نوع شبکه.

شبکه های بی سیم (Wireless)

موارد استفاده:

- ایجاد شبکه‌ای با وجود ایستگاههای متحرک
- استفاده در مکانهایی که کابل‌کشی در آن مقرون به صرفه و یا عقلانی نیست.

مزایا

- ساده بودن نصب و راه اندازی این نوع شبکه