به نام خدا

آزمایشگاه شبکه و امنیت

آشنایی با شبکه

مروری بر پروتکل‌ها و مفاهیم شبکه

شبکه چیست؟

شبکه شامل دو یا چند کامپیوتر است که برای به اشتراک گذاشتن منابع خود (مثل چاپگر وCD-ROM)، ردوبدل کردن فایل ها و یا ارتباط با یکدیگر متصل شده اند. در واقع شبکه با اتصال کامپیوترها به روش های گوناگون شرایطی را فراهم می آورد که برای انتقال اطلاعات هزینه ها کاهش یافته و سرعت و ریسک انتقال نیز پایین بیاید.

مزایای استفاده از شبکه عبارتند از:

- اشتراک منابع
- کاهش هزینه‌ها
- افزایش کارایی سیستم
- حذف محدودیت‌های جغرافیایی در تبادل داده‌ها

اجزای اصلی موجود در شبکه

- Client :کامپیوتر سرویس گیرنده که از خدمات موجود در شبکه استفاده می کند.
- Servers :کامپیوتر سرویس دهنده که خدمات متفاوت را در اختیار دیگر کامپیوترها قرار می دهد.
- Media :تمامی موارد ارتباط دهنده بین کامپیوترها شامل کابل، کانکتور و تجهیزات ارتباطی می باشد.
- Resources : شامل تمام منابع موجود در شبکه مانند مانیتور،اسکنر، صفحه کلید،چاپگر و ... می باشد.
- Shared Resources : به کلیه منابعی گفته می شود که کامپیوتر سرویس دهنده در اختیار کامپیوتر سرویس گیرنده قرار می دهد، مثل چاپگر ، اسکنر و... .

انواع شبکه

- از نظر گستردگی و موقعیت فیزیکی و جغرافیایی
  - Local area network (LAN)
  - Metropolitan area network (MAN)
  - Wide area network (WAN) (به عنوان مثال، اینترنت یک شبکه WAN است.)
- از نظر مدل سرویس دهی
  - شبکه‌های نظیر به نظیر (Peer-to-Peer)

در این شبکه ایستگاه ویژه‌ای جهت نگهداری فایل‌های اشتراکی و سیستم‌عامل شبکه وجود ندارد. هر ایستگاه می‌تواند به منابع سایر ایستگاه‌های شبکه دسترسی پیدا کند.

- شبکه‌های مبتنی بر سرویس‌دهنده (Server Based)

در این مدل شبکه، یک کامپیوتر به عنوان سرویس‌دهنده کلیه فایل‌ها ونرم‌افزارهای اشتراکی نظیر واژه پردازها، کامپایلرها، بانک‌های اطلاعاتی و سیستم‌عامل شبکه را در خود نگهداری می‌کند. یک کاربر به سرویس‌دهنده متصل شده و فایلها و اطلاعات خود را بر می‌دارد.

- مدل سرویس‌دهنده/سرویس گیرنده (Client/Server)

در این مدل یک ایستگاه درخواست انجام کارش را به سرویس دهنده ارائه می کند و سرویس دهنده پس از اجرای وظیفه محوله نتایج را به ایستگاه مورد نظر بر می‌گرداند.

- از نظر تکنولوژی انتقال داده
  - Broadcast

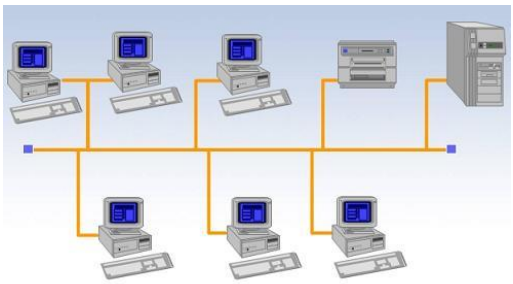
یک کانل مخابراتی مشترک بین همه کامپیوترهای شبکه وجود دارد که ارسال پیام در قالب بسته های کوچکی توسط هر کامپیوتر صورت می گیرد که آدرس مقصد بخشی از پیام است و بسته توسط همه کامپیوتر ها دریافت ودر صورت تعلق به خود بسته پردازش و در صورت عدم تعلق بسته نادیده گرفته می شود. در این شبکه هر کامپیوتر آدرس یکتا دارد.

  - Point to Point

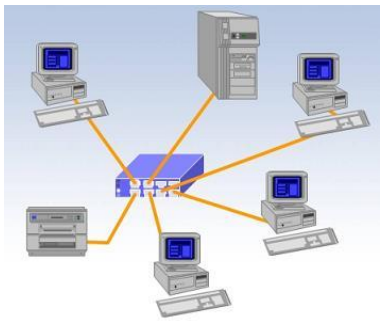
بین دو ماشین در شبکه، یک کانال فیزیکی و مستقیم وجود دارد و هیچ ماشین دیگری به آن کانال متصل نخواهد بود.

- انواع توپولوژی (روش اتصال فیزیکی کامپیوترها) در شبکه های LAN

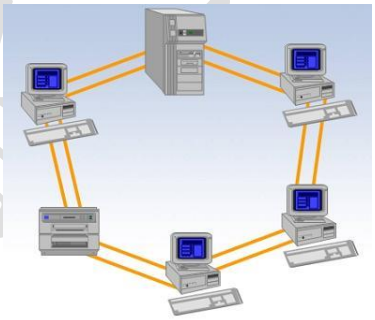
۱. خطی یا سری (bus)　　۲. روش ستاره ای یا متمرکز (star)

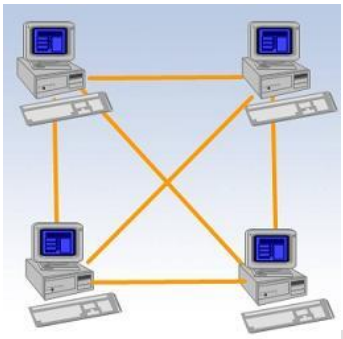


۳. روش حلقه ای (ring)

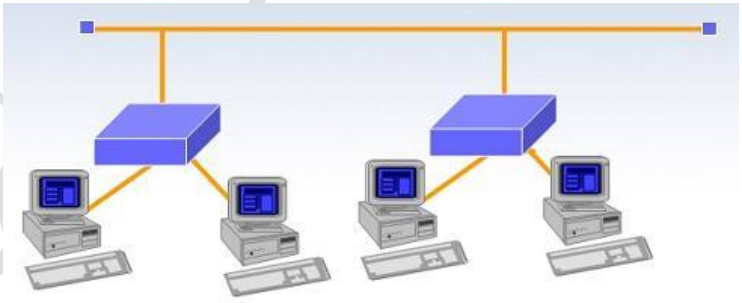


۴. روش پوششی (mesh)



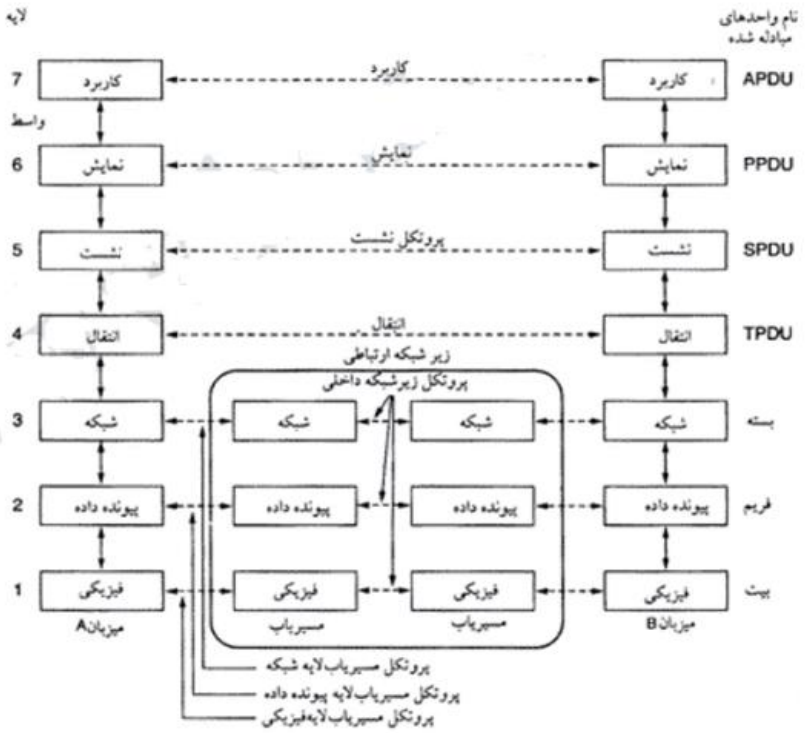


۵ . روش ترکیبی (hybrid) (به عنوان نمونه خطی- ستاره ای)



مدل OSI (Open System Interconnection)

مدل مرجع OSI چگونگی ارتباطات بین کامپیوتری در سطح شبکه را به هفت لایه یا سطح تقسیم می کند.



مدل مرجع OSI

لایه فیزیکی : وظیفه ی انتقال بیت های خام را از طریق کانال ارتباطی بر عهده دارد.

لایه پیوند داده ها: با شکستن داده های ورودی به بسته های کوچک (فریم) ، خط فیزیکی پر خطا را به خط ارتباطی عاری از خطا برای لایه ی شبکه تبدیل میکند.

آدرس دهی در شبکه ها به دو صورت است: (الف)آدرس دهی فیزیکی که توسط MAC Address انجام می شود. (ب) آدرس دهی logical که توسط IP و ... در پروتکل های مختلف انجام می شود.آدرس دهی MAC در لایه پیوند داده انجام می شود.

لایه شبکه : عملکرد زیر شبکه را کنترل میکند. از مسائل مطرح در این لایه آدرس دهی و مسیر یابی بسته ها(packet) می باشد. آدرس دهی در این لایه به صورت logical است.

لایه انتقال : این لایه برای تهیه جریان ارتباطی قابل اعتماد بین دو سیستم که شامل انتقال دوباره پیامهای گمشده، قرار دادن آنها در جای مناسب و نظارت و بازرسی خطاهاست(عمل error recovery)، استفاده می شود.قابل ذکر است تاییدیه دریافت اطلاعات به صورت صحیح (Ack) توسط این لایه ایجاد و به کامپیوتر ارسال کننده، انتقال داده می شود.

لایه نشست : وظیفه برقراری یک ارتباط منطقی بین نرم افزارهای دو کامپیوتری که به یکدیگر متصل هستند به عهده این لایه است. در واقع وظیفه این لایه فراهم آوردن شرایط یک جلسه همانند ورود به سیستم از راه دور ، احراز هویت طرفین ،مشخص نمودن اعتبار پیامها ، اتمام جلسه ، حسابداری مشتری ها می باشد.

لایه نمایش یا ارائه : این لایه چگونگی نمایش المانهای داده برای ارسال از جمله منظم کردن بیتها و بایتها در اعداد، فرمت بندی اعداد نمایی و همانند آن را بر عهده دارد.همچنین compression و encryption و همچنین Redirectory(RDR) از وظایف این لایه است.

لایه کاربرد: این لایه بعنوان پنجره ای به کانال ارتباطی برای برنامه کاربردی و البته با توصیف داده ها و تبدیل آنها به اطلاعات با مفهوم برای برنامه های کاربردی عمل میکند.در عین حال، نظارت بر error recovery و flow control در هنگام ارسال و دریافت اطلاعات به عهده دارد.

تعریف پروتکل :

مجموعه ای از قوانین است که دو دستگاه برای انتقال موفق داده، از آنها پیروی می کنند. برخی از مواردی که یک پروتکل آنها را مشخص می کند عبارتند از:

- نحوه تشخیص خطا و تصحیح خطاهای احتمالی که حین تبادل داده ممکن است اتفاق بیفتد.
- روش متراکم سازی داده ها
- چگونگی اعلان پایان یک فریم داده توسط فرستنده
- چگونگی اعلان دریافت یک فریم داده توسط گیرنده و نحوه ادامه ارسال داده در صورت عدم موفقیت گیرنده، در دریافت صحیح داده ها
- طول هر فریم داده

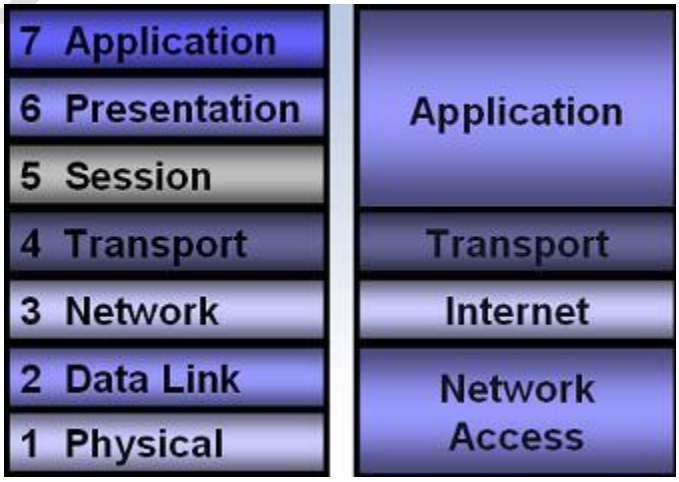
تا کنون انواع مختلفی از پروتکلها برای استفاده های مختلف طراحی شده اند و هر کدام دارای معایب و مزایایی هستند برخی از پروتکلها ساده، برخی با قابلیت اطمینان بیشتر و برخی دارای سرعت بالاتر هستند. برخی از پروتکلهای متداول عبارتند از: TCP/IP، UDP، FTP ، PPP و ... . توضیحات کامل در مورد عملکرد هر پروتکل در متن‌هایی با نام RFC توسط IETF انتشار می یابند (مثلا RFC شماره ۷۹۱، اطلاعات جامعی را در مورد پروتکل IP ارائه می‌کند).

مدل لایه ای TCP/IP

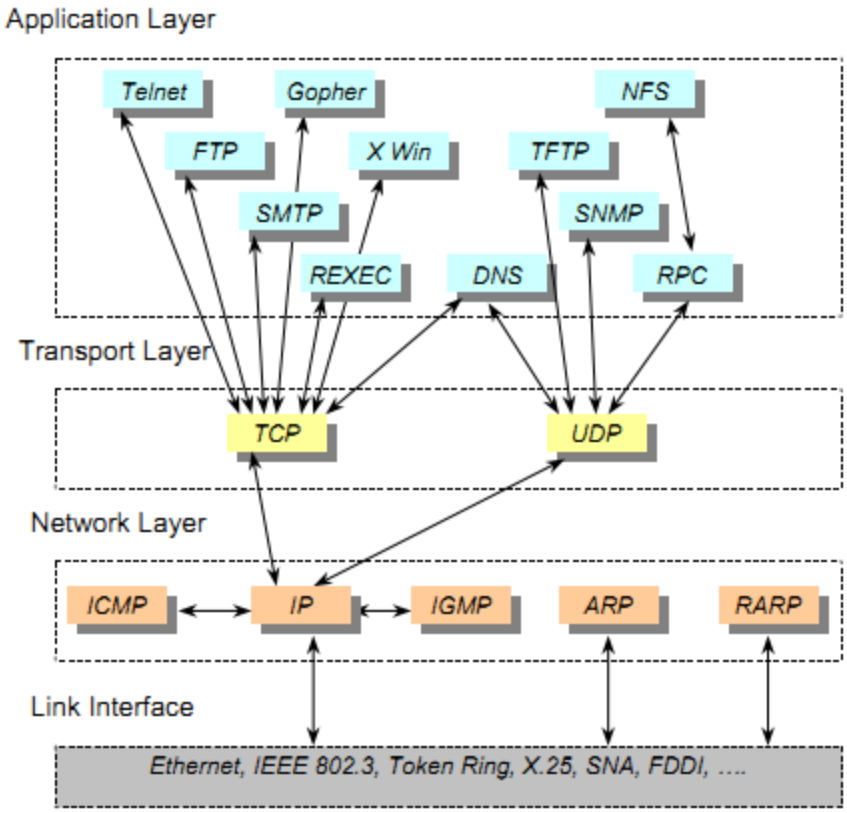
پروتکلی استاندارد برای ارتباط کامپیوترهای موجود در یک شبکه اینترنت است. از این پروتکل ، به منظور ارتباط در شبکه های بزرگ استفاده می‌شود. برقراری ارتباط از طریق پروتکل های متعددی که در چهارلایه مجزا سازماندهی شده اند، میسر می گردد.

در زمان ایجاد یک ارتباط ، ممکن است در یک لحظه تعداد زیادی از برنامه ها ، با یکدیگر ارتباط برقرار نمایند، این پروتکل دارای قابلیت تفکیک و تمایز یک برنامه موجود بر روی یک کامپیوتر با سایر برنامه ها بوده و پس از دریافت داده ها از یک برنامه ، آنها را برای برنامه متناظر موجود بر روی کامپیوتر دیگر ارسال می نماید. نحوه ارسال داده توسط پروتکل از محلی به محل دیگر ، با فرآیند ارسال یک نامه از شهری به شهری دیگر، قابل مقایسه است.

برقراری ارتباط با فعال شدن یک برنامه بر روی کامپیوتر مبدا آغاز می گردد . برنامه فوق ،داده های مورد نظر جهت ارسال را بگونه ای آماده و فرمت بندی می نماید که برای کامپیوتر مقصد قابل خواندن و استفاده باشند. (مشابه نوشتن نامه با زبانی که دریافت کننده ، قادر به مطالعه آن باشد) . در ادامه آدرس کامپیوتر مقصد ، به داده های مربوطه اضافه می گردد (مشابه آدرس گیرنده که بر روی یک نامه مشخص می گردد) . پس از انجام عملیات فوق ، داده به همراه اطلاعات اضافی (درخواستی برای تائید دریافت در مقصد) ، در طول شبکه به حرکت درآمده تا به مقصد مورد نظر برسد. عملیات فوق ، ارتباطی به محیط انتقال شبکه به منظور انتقال اطلاعات نداشته و تحقق عملیات فوق با رویکردی مستقل نسبت به محیط انتقال ، انجام خواهد شد.



لایه ها را در مدل مرجع OSI و TCP/IP

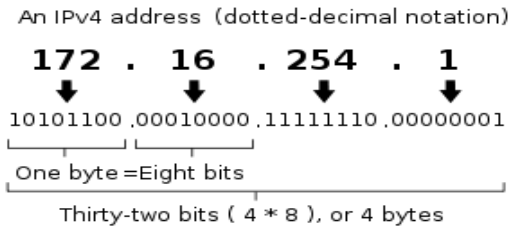


➢ پروتکل IP

یکی از پروتکل های مهم موجود در لایه internet که مسئولیت آدرس دهی logical را به عهده دارد، IP می باشد.

در اینجا قالب بسته های IP را بررسی میکنیم:

هر آدرس IP یک عدد ۳۲ بیتی است که به ۴ قسمت ۸ بیتی ،که octet نامیده می شود، تقسیم می شود و به صورت ۴ عدد دهدهی نمایش داده می شود که با نقطه از هم جدا شده اند.

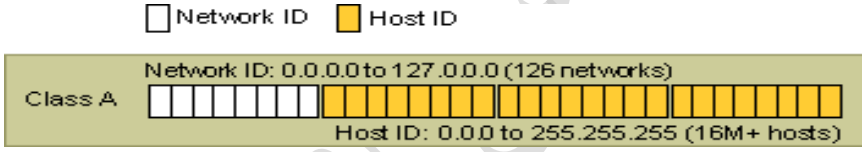


کلاسهای مختلف IP نسخه ی ٤ :

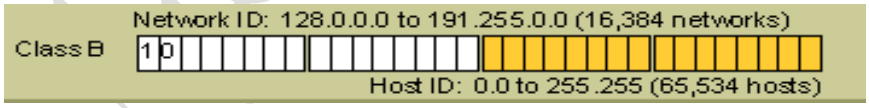
سه کلاسِ پایه‌ایِ مختلفِ نشانی‌دهیِ آی‌پی، برای شبکه‌های بزرگ، متوسط و کوچک وجود دارد. کلاس A برای شبکه‌های بزرگ، کلاس B برای شبکه‌های متوسط و کلاس C برای شبکه‌های کوچک است. علاوه بر این سه کلاس، کلاس D برای پخش چندگانه، ارسال اطلاعات به گروهی از رایانه‌ها، و کلاس E برای کارهای تحقیقاتی وجود دارند.

Subnet mask	CIDR	پایان	شروع	کلاس
255.0.0.0	/8	127.255.255.255	0.0.0.0	Class A
255.255.0.0	/16	191.255.255.255	128.0.0.0	Class B
255.255.255.0	/24	223.255.255.255	192.0.0.0	Class C
Not defined	/4	239.255.255.255	224.0.0.0	Class D(multicast)
Not defined	/4	255.255.255.255	240.0.0.0	Class E(reserved)

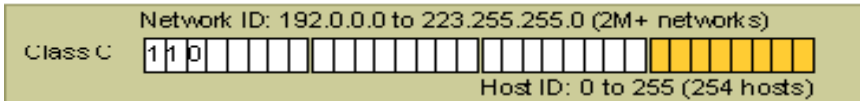
- در کلاس A آدرس های IP با عددی بین ۱ تا ۱۲۶ شروع می شوند و آدرس میزبان در سه جزء آخر قرار می گیرد.



- در کلاس B آدرس های IP با عددی میان ۱۲۸ تا ۱۹۱ شروع می شوند و با عددی که توسط موسسه اختصاص دهنده IP تعیین می شود، ادامه می یابند. دو جزء آخر متغیر هستند.



- در کلاس C آدرس های IP با عددی بین ۱۹۲ تا ۲۲۳ شروع می شوند و با دو عددی که توسط موسسه اختصاص دهنده IP تعیین می گردند، ادامه می یابند. جزء آخر متغیر خواهد بود.



آدرسهای خاص:

- آدرس ۲۵۵.۲۵۵.۲۵۵.۲۵۵:

اگر بخواهیم بصورت باینری بگوییم می‌شود آدرسی که تمام ارقامش یک باشد. این IP برای انتشار پیام به شبکه محلی است که در نتیجه توسط هر میزبان IP قابل رویت است یا به عبارتی دیگر برای ارسال پیام‌های فراگیر برای تمام ماشینهای میزبان بر روی شبکه محلی، که ماشین فرستنده در آن شبکه قرار دارد، به کار می رود.

- آدرس ۰.۰.۰.۰:

هر ماشین میزبان که آدرس IP خود را نداند، این آدرس را بعنوان آدرس خود فرض می‌کند. مثل اینکه برای کسی نامه بفرستید ولی آدرس خود را بعنوان نویسنده ننوشته باشید، در نتیجه گیرنده پاسخی نمی‌تواند بدهد.

حالتی که تمام بیت‌های ID شبکه صفر (یعنی همه بایت‌های آن ۰) باشد ولی ID میزبان معتبر باشد: این آدرس برای وقتی است که آدرس میزبان، آدرس مربوط به شبکه خودش را نداند ! مثال: ۰.۰.۱۲۳.۵۴ برای کلاسB

حالتی که ID شبکه معتبر باشد ولی تمام بیت‌های ID میزبان یک (یعنی همه بایت‌هاش ۲۵۵) باشد: این آدرس برای ارسال پیام کلی برای کامپیوترهای یک شبکه در صورتی که کامپیوتر فرستنده جزو آن شبکه نباشد، کاربرد دارد. همچنین برای انتشار پیام مستقیم و هدایت شده. مثال ۱۷۲.۱۶.۲۵۵.۲۵۵

- حالتی‌که IP با یک یا چند بایت با مقدار ۲۵۵ شروع شود:

هیچ IDشبکه ای نمی‌تواند اینگونه باشد. این گونه آدرس‌ها برای الگوهای زیر شبکه (Subnet Mask) استفاده شده اند.

مثال: ۲۵۵.۲۵۵.۰.۰

حالتی که بایت اول آدرس IP عدد ۱۲۷ باشد:

اگر دقت کرده باشید عدد ۱۲۷ برای بایت اول در هیچ کدام از کلاس‌ها موجود نبود زیرا این عدد برای IDهای شبکه قابل دسترس نیست. این آدرس برای تشخیص هویت و اهداف مشکل‌زدایی (مثلا از نرم‌افزارهای شبکه‌ای) استفاده می‌شود .بسته‌ای که به این گونه آدرس‌ها فرستاده شود، به خود کامپیوتر فرستنده بر خواهد گشت!

مثال: ۱۲۷.۰.۰.۱

- **پروتکل TCP**

TCP به این منظور طراحی شد تا یک دنباله از بایت ها را به صورت مطمئن و عاری از خطا بین دو نقطه ی پایانی از شبکه ای که نامطمئن و مستعد خطاست، منتقل نماید.

در شکل زیر ساختار یک قطعه ی TCP را مشاهده می کنید. فیلد های پورت مبدا و پورت مقصد نقاط انتهایی دو طرف یک اتصال را مشخص می نمایند. ترتیب قطعه ی داده و اعلام وصول داده ها با فیلد های sequence number و acknowledgment number مشخص می شوند.

TCP Header

Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Source port																Destination port															
32	Sequence number																															
64	Acknowledgment number (if ACK set)																															
96	Data offset				Reserved			NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
128	Checksum																Urgent pointer (if URG set)															
160 …	Options (if Data Offset > 5) …																								padding							

در ادامه توضیح پرچم‌های تک بیتی Urg,ACK,PSH,PST,SYN,FIN ,NS,CWR,ECE داده می شود:

بیت NS(ECN): برای محافظت در برابر پنهانکاری عمدی یا تصادفی بسته های TCP فرستنده استفاده می شود. با جلوگیری از بهره برداری ECN برای بدست آوردن سهم ناعادلانه از پهنای باند، با باعث بهبود کنترل ازدحام می شود. کاربرد صحیح ECN نیازمند همکاری گیرنده در فرستادن سیگنال پاسخ Congestion Experienced به فرستنده است اما این پروتکل مکانیزمی برای الزام این همکاری ندارد.

بیت ECE(ECN Echo): اگر بیت SYN، set شده باشد، این بیت نشان دهنده ی این است که بسته tcp قابلیت ECN دارد. اگر بیت SYN ، صفر باشد این بیت نشان می دهد که بسته ای دارای پرچم ست شده ی Congestion Experienced در سرایند بسته ی IP بوده، در طول مبادله اطلاعات، دریافت شده است.

بیت CWR(Congestion Window Reduced): توسط فرستنده برای نشان دادن دریافت یک segment که پرچم ECE آن set شده و به مکانیزم کنترل ازدحام جواب داده، set می شود.

بیت URG :در صورتی که در این بیت عدد ۱ قرار گیرد معین می شود که در فیلد Urgent Pointer مقدار قابل معتبری قرار دارد و بایستی مورد پردازش قرار گیرد.

بیت ACK : اگر در این بیت عدد ۱ قرار داشته باشد به این معنا است که در فیلد Acknowledgment numberعدد معتبری قرار دارد . بیتهایACK و SYN نقش دیگری نیز دارند که در ادامه بدان اشاره خواهد شد.

بیت PSH :اگر در این بیت مقدرا ۱ قرار گرفته باشد، از گیرند تقاضا می شود که دادهای موجود را بافر نکرده و در اسرع وقت تحویل داده شود.

بیت RST :اگر در این بیت عدد ۱ قرار گرفته شود به این معن است که این ارتباط به صورت یک طرفه خاتمه یافته است.

بیت SYN :این بیت نقش اساسی در ار تباط یک بسته TCP بازی می کند . برقراری ارتباط یک طرفه TCP از روند زیر تبعیت می کند.

شروع کننده ارتباط یک بسته TCPبدون هیچ داده ای و با تنظیم بیتهای ۱ =SYN و ACK=0 تقاضای یک ارتباط جدید می کند.

در صورتی که طرف مقابل تمایل به بر قراری ارتباط داشته باشد برای طرف مقابل یک بسته با قرار دادن بیتهای ۱ =SYN و ACK=1 می فرستد. بنابراین، تمایل خود را برای برقراری ارتباط به طرف مقابل اعلام می کند.

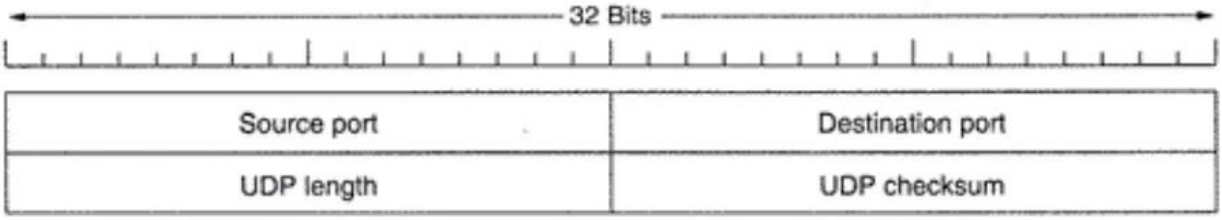
بیت FIN : اگر یکی از طرفین هیچ داد دیگر برای فرستادن نداشته باشد، این بیت را در آخرین بسته برابر ۱

قرار می دهد و ارتباط را یک طرفه قطع می کند. باید توجه داشته که ارتباط هنوز به طور کامل قطه نشده است و باید طرف مقابل نیز در آخرین بسته خود این فیلد را برابر ۱ قرار داده تا ارتباط کامل قطع شود.

➢ پروتکل UDP

UDP یا User Datagram Protocol یک پروتکل بدون اتصال در لایه انتقال است. UDP اطلاعات را از طریق پروتکل IP منتقل می‌کند، اما به دلیل اینکه از Sequence Number و سیستمی مانند Three Way Handshake که در پروتکل TCP استفاده می‌شود، پشتیبانی نمی‌کند پروتکل چندان قابل اطمینانی نیست. به این معنا که درستی تحویل پیام‌ها در این پروتکل مورد بررسی قرار نمی‌گیرد اما تضمین می کند که حداکثر تلاش خود را برای تحویل اطلاعات انجام می دهد. بنابراین این قرارداد رسیدن اطلاعات را در مقصد بررسی نمی کند و لذا نرخ ارسال آن به مراتب بالاتر از قرارداد TCPمی باشد.

UDP داده ها را در قالب قطعاتی ارسال می کند که در ابتدای آنها ۸ بایت سرایند و سپس داده های لایه ی کاربرد قرار می گیرند. این سرایند در شکل زیر نشان داده شده است. دو فیلد شماره ی پورت به منظور شناسایی نقاط پایانی(پروسه های نهایی) در ماشین های مبدا و مقصد به کار می آید.



➢ پروتکل ICMP

این پروتکل امکانات لازم در خصوص اشکال زدائی و گزارش خطاء در رابطه با بسته های اطلاعاتی غیرقابل توزیع را فراهم می نماید. با استفاده از ICMP، کامپیوترها و روترها که از IPبه منظور ارتباطات استفاده می نمایند ، قادر به گزارش خطاء و مبادله اطلاعاتی محدود در رابطه وضعیت بوجود آمده می باشند. مثلا" در صورتیکه IP، قادر به توزیع یک بسته اطلاعاتی به مقصد مورد نظر نباشد ، ICMPیک پیام مبتنی بر غیرقابل دسترس بودن را برای کامپیوتر مبداء ارسال می دارد . با اینکه پروتکل IPبمنظور انتقال داده بین روترهای متعدد استفاده می گردد ، ولی ICMP به نمایندگی از TCP/IP، مسئول ارائه گزارش خطاء و یا

پیام های کنترلی است . تلاش ICMP، در این جهت نیست که پروتکل IPرا بعنوان یک پروتکل مطمئن مطرح نماید ، چون پیام های ICMPدارای هیچگونه محتویاتی مبنی بر اعلام وصول پیام (Acknowledgment)بسته اطلاعاتی نمی باشند ICMP . ، صرفا" سعی در گزارش خطاء و ارائه فیدبک های لازم در رابطه با تحقق یک وضعیت خاص را می نماید. این پروتکل مسئول انجام کارهای زیر می باشد:

- Echo Request و Echo Reply برای کنترل امکان ارتباط با یک دستگاه مرتبط با شبکه مبتی بر IP
- Source quench message برای اطلاع دادن buffer over flow به کامپیوتر ارسال کننده اطلاعات
- Destination unreachable که نمایش دهنده عدم امکان ارتباط با مقصد مورد نظر می باشد
- یک سیستم میتواند از این پروتکل برای امتحان اینکه آیا سیستم دیگر فعال است یا خیر با فرستادن ping استفاده کند. اگر سیستم ping شده فعال باشد به فرستادن پیام پاسخ واکنش نشان میدهد.

➢ پروتکل ARP

ازاین پروتکل به منظور تبدیل آدرسهای IP به آدرسهای فیزیکی (MAC address) استفاده می شود. در واقع به این کار name resolve گویند. روش کار این پروتکل بدین صورت است که آدرس هر میزبان به عنوان یک عضو در شبکه در جدولی به نام جدول ARP یا حافظه ARP نگهداری میشود. جدول ARP رابط بین آدرسهای فیزیکی و آدرسهای IP در یک شبکه است.زمانیکه یک میزبان بر روی شبکه قصد فرستادن یک پیام به میزبان دیگری روی شبکه دارد میزبان اول آدرس فیزیکی مقصد را از روی جدولARP معین میکند اگر آدرس مقصد در جدول موجود نباشد فرستنده یا مرجع یک پخش بر روی شبکه می فرستد.این درخواست حاوی آدرس IP نامشخصی میباشد.تمام میزبانها در شبکه درخواست ARP را دریافت میکنند و میزبانی که آدرس IP نامشخص متعلق به آن است ، آدرس فیزیکی خود را به مرجع یا میزبان اول می فرستد.جدول ARP ارتباط جدید را به عنوان یک آدرس جدید در خود نگهداری میکند.

برای استفاده از پروتکل ARP از دستور ARP در COMMAND PROMPT استفاده میکنیم. به عنوان مثال دستور "arp -a" لیست آدرس های فیزیکی به همراه آدرس های IP آنها را نشان میدهد.

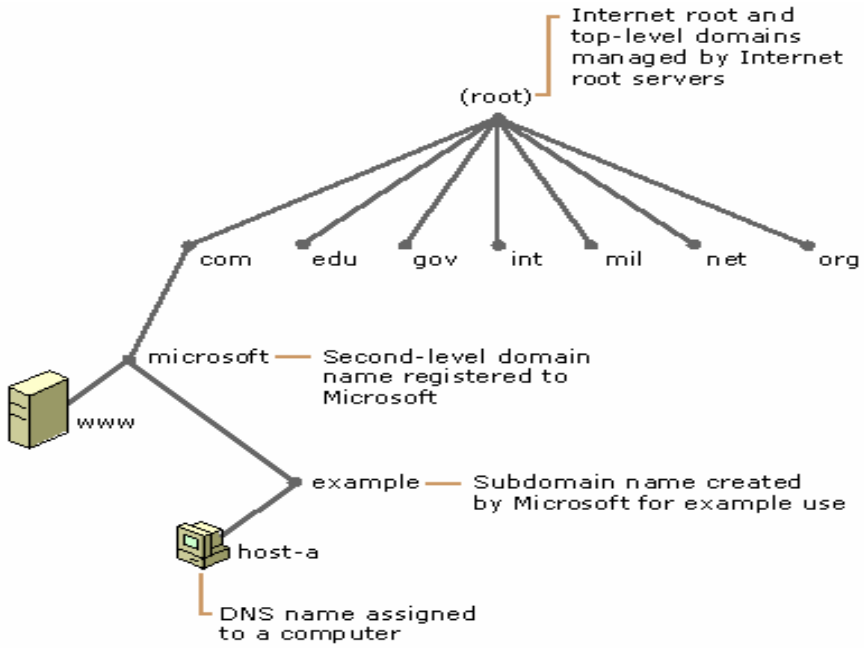
از دستورات دیگر می توان "arp -s" را نام برد که به صورت استاتیک یک درایه به جدول ARP اضافه میکند. نحوه ی استفاده از آن در مثال زیر آمده است:

```
Arp –s   172.16.1.8   00-16-E6-48-2D-9F
```

برای مشاهده ی دیگر فرمت های این دستور از help در command prompt استفاده می شود.
نحوه ی بکارگیری help در دستور کار ذکر شده است.

- **پروتکل DNS**

DNS یک پایگاه سلسله مراتبی است که در جهان بطور گسترده برای ذخیره سازی انواع مختلفی از اطلاعات شامل آدرس های IP، نام حوزه ها و اطلاعات سرویس دهنده پست الکترونیک مورد استفاده قرار میگیرد.
روش کار DNS بطور خلاصه این چنین است: برای تبدیل یک نام به آدرس IP، برنامه یک تابع کتابخانه ای به نام تبدیل کننده (resolver) را فراخوانی می کند، و نام مورد نظر را بصورت پارامتر به آن می دهد. تبدیل کننده یک بسته ی UDP را به سرویس دهنده ی DNS محلی می فرستد، که این DNS آدرس IP معادل نام خواسته شده را یافته و به تبدیل کننده بر می گرداند. که آن هم به نوبه ی خود، آدرس برنامه را به فراخوانی کننده تحویل می دهد. برنامه هم پس از بدست آوردن آدرس IP کامپیوتر مقصد، می تواند با آن ارتباط TCP برقرار کرده یا بسته های UDP به آن بفرستد.
همانطور که درشکل صفحه بعد مشاهده میکنید در بالای سلسله مراتب این درخت ریشه سرورهای DNS وجود دارد. این درخت شامل اطلاعات در مورد سرورهای DNS در مراحل سطوح پایین تر سلسله مراتب میباشد. مراحل پایین سلسله مراتب DNS شامل سرورهای DNS برای نام حوزه های org,.net,.com. می باشد.
برای استفاده از پروتکل DNS از دستور nslookup استفاده میکنیم، که در دستور کار با نحوه ی استفاده از آن آشنا خواهید شد.



تجهیزات شبکه و حدود عملکرد آنها:

- Hub : در این دستگاه که در حد لایه physical عمل می کند، سیگنال ها پس از دریافت بدون هیچگونه تحلیلی سریعا ارسال می شوند.این دستگاه به عنوان یک واسط برای ارتباط بین دستگاه ها عمل می‌کند. هر سیگنال پس از دریافت به تمام پورت ها غیر از پورت مبدا ارسال می گردد. روش عملکرد Hub همواره Half Duplex می باشد.
- Switch : در این دستگاه علاوه بر دریافت و ارسال سیگنال کارهای دیگری نیز انجام می شود.در حقیقت حدود عملیاتی که در switch انجام می شوند لایه Datalink می باشد. یعنی سوئیچ در دو لایه پایینی OSI کار می کند.Switch سیگنالها را دریافت کرده و پس از دریافت سیگنال ها یک Frame به صورت کامل،ابتدا اقدام به کنترل CRC و سپس آدرس مبدا و مقصد(MAC Address) آن می نماید. با کنترل آدرس مبدا، شماره پورت و MAC Address مربوط به کامپیوتر ارسال کننده در جدول Filter/Forward Table ثبت می گردد و اطلاعات صرفا به همان پورتی که مقصد به آن متصل است ارسال می شود. در صورت وجود نداشتن آدرس کامپیوتر مقصد در جدول مذکور، Frame دریافت شده توسط switch به تمام پورت ها ارسال شده یا اصطلاحا Flood می شود. ضمنا در صورتی که یک Frame از نوع Broadcast به switch برسد به تمام پورت ها Flood می شود.

- Bridge : این دستگاه به switch شباهت دارد و از نظر لایه های کاری نیز در دو لایه پایینی کار می کند. تمام موارد کاری آن شبیه switch است با این تفاوت که تعداد پورت های آن معمولا دو تا و در برخی موارد چهارتا می باشد و برای اتصال شبکه های Bus به یکدیگر طراحی شده است.
- Router : این دستگاه یک لایه بالاتر از switch کار می کند. در حقیقت این دستگاه در سه لایه پایینی از OSI کار می‌کند و از آدرس‌های logical برای تشخیص مسیر ارسال packet استفاده می‌کند. برخلاف switch که در صورت دریافت Frame از نوع broadcast آن را Flood می کند، Router اجازه عبور آن را نمی دهد.

تعدادی از دستور های مفید خط فرمان در windows

- **ipconfig**

برای نشان دادن اطلاعات IP

  - **ipconfig/all** جزئیات بیشتری مانند DNS SERVER ها را نشان می دهد.
  - **ipconfig/renew** برای تجدید آدرس IP یک کارت شبکه ی مشخص.

برای مشاهده ی دیگر OPTION های این دستور از HELP خط فرمان استفاده کنید.

- **netsh**

netsh به شما اجازه می دهد تا به صورت Local و یا Remote تنظیمات شبکه ی کامپیوتری که netsh را اجرا می کند را تغییر و یا نمایش دهید.

netsh همچنین از طریق Scripting این اجازه را به شما می دهد تا گروهی از دستورات را به حالت Batchبرای کامپیوترهای مشخصی اجرا نمایید. netsh همچنین این امکان را در اختیار شما قرار می‌دهد تا تنظیمات را در قالب یک فایل متنی به منظور پیکر بندی سیستم های دیگر ذخیره کنید .

به عنوان مثال دستور زیر کارت شبکه ای به نام local area connection را با آدرس IP، ۱۹۲.۱۶۸.۰.۱۰۰ و subnet mask، ۲۵۵.۲۵۵.۲۵۵.۰ و default gateway، ۱۹۲.۱۶۸.۰.۱ پیکر بندی می کند.

```
netsh interface ip set address name="Local Area Connection" static 192.168.0.100
255.255.255.0 192.168.0.1 1
```

با استفاده از دستور زیر می توان از DHCP، IP جدید گرفت.

```
netsh interface ip set address "Local Area Connection" dhcp
```

برای تنظیم DNS server به صورت static از دستور زیر استفاده می کنیم:

```
netsh interface ip set dns name="Local Area Connection" source=static
addr=192.168.0.2 register=none
```

برای تنظیم DNS server به صورت Dynamic از دستور زیر استفاده می کنیم:

```
netsh interface ip set dns name="Local Area Connection" source=dhcp
```

- **netstat**

این دستورnetwork connectionهای ورودی و خروجی و جدول های مسیر یابی و... را نشان میدهد.

از دستور netstat -a برای مشاهده ی connection ها و پورت هایUDP و TCP در حال شنود استفاده می شود..

از دستور netstat -r برای مشاهده ی جدول مسیر یابی استفاده می شود.

از دستور netstat –p ”protocol” برای مشاهده ی connectionها با پروتکل خاص استفاده می‌شود.